

# NVR700W NVR510

ルーター

Rev.15.00.24, Rev.15.01.25



## コマンドリファレンス

ヤマハ製品をお買い上げいただきありがとうございます。

お使いになる前に本書をよくお読みになり、正しく設置、設定を行ってください。

本書中の警告や注意を必ず守り、正しく安全にお使いください。

本書はなくさないように、大切に保管してください。

# 目次

序文：はじめに.....	25
<b>第 1 章：コマンドリファレンスの見方.....</b>	<b>26</b>
1.1 対応するプログラムのリビジョン.....	26
1.2 コマンドリファレンスの見方.....	26
1.3 インターフェース名について.....	26
1.4 no で始まるコマンドの入力形式について.....	27
1.5 コマンドの入力文字数とエスケープシーケンスについて.....	27
1.6 工場出荷設定値について.....	27
<b>第 2 章：コマンドの使い方.....</b>	<b>28</b>
2.1 コンソールについて.....	28
2.1.1 コンソールによる設定手順.....	28
2.1.2 CONSOLE ポートからの設定.....	29
2.1.3 TELNET による設定.....	29
2.2 SSH サーバーについて.....	30
2.2.1 SSH サーバー機能の使用に当たっての注意事項.....	30
2.2.2 SSH サーバーの設定.....	31
2.3 TFTP について.....	31
2.3.1 TFTP による設定手順.....	32
2.3.2 設定ファイルの読み出し.....	32
2.3.3 設定ファイルの書き込み.....	33
2.4 コンソール使用時のキーボード操作について.....	33
2.5 「show」で始まるコマンド.....	34
2.5.1 show コマンドの表示内容から検索パターンに一致する内容だけを抜き出す.....	34
2.5.2 show コマンドの表示内容を見やすくする.....	36
2.5.3 外部メモリへのリダイレクト機能.....	36
<b>第 3 章：ヘルプ.....</b>	<b>38</b>
3.1 コンソールに対する簡易説明の表示.....	38
3.2 コマンド一覧の表示.....	38
<b>第 4 章：機器の設定.....</b>	<b>39</b>
4.1 ログインパスワードの設定.....	39
4.2 ログインパスワードの暗号化保存.....	39
4.3 管理パスワードの設定.....	39
4.4 管理パスワードの暗号化保存.....	39
4.5 一般ユーザー名とログインパスワードの設定.....	40
4.6 ログイン時のパスワード認証に RADIUS を使用するか否かの設定.....	40
4.7 管理ユーザーへの移行時のパスワード認証に RADIUS を使用するか否かの設定.....	41
4.8 ユーザーの属性を設定.....	41
4.9 他のユーザーの接続の強制切断.....	44
4.10 ログインタイマの設定.....	44
4.11 INIT スイッチによるパスワード再入力機能の設定.....	45
4.12 セキュリティークラスの設定.....	45
4.13 CPU 使用率の閾値の設定.....	46
4.14 メモリ使用率の閾値の設定.....	47
4.15 パケットバッファのパラメーターを変更する.....	47
4.16 環境変数の設定.....	48
4.17 エイリアスの設定.....	48
4.18 マクロの設定.....	49

4.19 EMFS ファイルの作成、削除.....	50
4.20 タイムゾーンの設定.....	51
4.21 現在の日付けの設定.....	51
4.22 現在の時刻の設定.....	51
4.23 リモートホストによる時計の設定.....	52
4.24 NTP による時計の設定.....	52
4.25 NTP パケットを送信するときの始点 IP アドレスの設定.....	53
4.26 Stratum 0 の NTP サーバーとの時刻同期を許可する設定.....	53
4.27 コンソールのプロンプト表示の設定.....	53
4.28 コンソールの言語とコードの設定.....	54
4.29 コンソールの表示文字数の設定.....	54
4.30 コンソールの表示行数の設定.....	55
4.31 コンソールにシステムメッセージを表示するか否かの設定.....	55
4.32 SYSLOG を受けるホストの IP アドレスの設定.....	55
4.33 SYSLOG ファシリティの設定.....	56
4.34 NOTICE タイプの SYSLOG を出力するか否かの設定.....	56
4.35 INFO タイプの SYSLOG 出力の設定.....	57
4.36 DEBUG タイプの SYSLOG を出力するか否かの設定.....	57
4.37 SYSLOG を送信する時の始点 IP アドレスの設定.....	57
4.38 SYSLOG パケットの始点ポート番号の設定.....	58
4.39 SYSLOG に実行コマンドを出力するか否かの設定.....	58
4.40 TCP のコネクションレベルの syslog を出力するか否かの設定.....	58
4.41 インターフェースパケットのダンプを SYSLOG へ出力するか否かの設定.....	61
4.42 TELNET サーバー機能の ON/OFF の設定.....	61
4.43 TELNET サーバー機能の listen ポートの設定.....	62
4.44 TELNET サーバーへアクセスできるホストの設定.....	62
4.45 TELNET サーバーへ同時に接続できるユーザー数の設定.....	63
4.46 ファストパス機能の設定.....	63
4.47 LAN インターフェースの動作設定.....	64
4.48 LAN インターフェースのリンクアップ後の送信抑制時間の設定.....	64
4.49 ポートミラーリング機能の設定.....	65
4.50 LAN インターフェースの動作タイプの設定.....	65
4.51 インターフェースまたはシステムの説明の設定.....	70
4.52 ONU インターフェースの動作タイプの設定.....	70
4.53 ONU インターフェースの動作設定.....	71
4.54 ONU インターフェースのリンクアップ後の送信抑制時間の設定.....	72
4.55 TFTP によりアクセスできるホストの設定.....	72
4.56 SFTP サーバーへアクセスできるホストの設定.....	73
4.57 Magic Packet を LAN に中継するか否かの設定.....	74
4.58 HTTP リビジョンアップ実行を許可するか否かの設定.....	75
4.59 HTTP リビジョンアップ用 URL の設定.....	75
4.60 HTTP リビジョンアップ用 Proxy サーバーの設定.....	75
4.61 HTTP リビジョンアップ処理のタイムアウトの設定.....	76
4.62 リビジョンダウンを許可するか否かの設定.....	76
4.63 DOWNLOAD ボタンによるリビジョンアップ操作を許可するか否かの設定.....	76
4.64 リビジョンアップ実行のスケジュール.....	77
4.65 SSH サーバー機能の ON/OFF の設定.....	78
4.66 SSH サーバー機能の listen ポートの設定.....	78
4.67 SSH サーバーへアクセスできるホストの設定.....	79
4.68 SSH サーバーへ同時に接続できるユーザー数の設定.....	80
4.69 SSH サーバーホスト鍵の設定.....	80
4.70 SSH サーバーホスト鍵の表示.....	80
4.71 SSH サーバーで利用可能な暗号アルゴリズムの設定.....	81
4.72 SSH クライアントの生存確認.....	82
4.73 SSH サーバー応答に含まれる OpenSSH のバージョン情報の非表示設定.....	82
4.74 SSH サーバーで利用可能な認証方式の設定.....	83
4.75 SSH サーバーの公開鍵認証に用いる公開鍵情報を保存するファイルの設定.....	83
4.76 SSH サーバーの公開鍵認証に用いる公開鍵の設定.....	84
4.77 SSH サーバーの公開鍵認証に用いる公開鍵の表示.....	85
4.78 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定.....	86
4.79 TEL ポートでの接続・切断時にアラーム音を鳴らすか否かの設定.....	86

4.80 データ通信での接続・切断時にアラーム音を鳴らすか否かの設定	86
4.81 攻撃を検知した時にアラーム音を鳴らすか否かの設定	87
4.82 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定	87
4.83 microSD 機能に関連するアラームを鳴らすか否かの設定	88
4.84 内蔵無線 WAN 機能に関連するアラーム音を鳴らすか否かの設定	88
4.85 バッチファイル実行機能に関連するアラーム音を鳴らすか否かの設定	88
4.86 起動時のアラーム音を鳴らすか否かの設定	89
4.87 HTTP リビジョンアップ機能に関連するアラームを鳴らすか否かの設定	89
4.88 エコーキャンセラー制御方法の設定	89
4.89 エコーキャンセラーの NLP 閾値の設定	91
4.90 エコーキャンセラーを無効にする音の設定	91
4.91 ジッタバッファ制御方法の設定	92
4.92 RTP パケットのパケット長を設定	93
4.93 RTP/RTCP で使用するポート番号の設定	93
4.94 SCP クライアント	93
4.95 SSH クライアント	94
4.96 SSH クライアントで利用可能な暗号アルゴリズムの設定	95
4.97 SSH サーバーの公開鍵情報を保存するファイルの設定	96

## 第 5 章 : ヤマハルーター用ファイルシステム RTFS.....97

5.1 RTFS のフォーマット	97
5.2 RTFS のガベージコレクション	97

## 第 6 章 : IP の設定.....98

6.1 インターフェース共通の設定	98
6.1.1 IP パケットを扱うか否かの設定	98
6.1.2 IP アドレスの設定	98
6.1.3 セカンダリ IP アドレスの設定	99
6.1.4 インターフェースの MTU の設定	100
6.1.5 同一インターフェースに折り返すパケットを送信するか否かの設定	101
6.1.6 echo,discard,time サービスを動作させるか否かの設定	101
6.1.7 IP の静的経路情報の設定	101
6.1.8 DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定	104
6.1.9 DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定	104
6.1.10 PDP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定	105
6.1.11 PDP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定	105
6.1.12 IP パケットのフィルターの設定	106
6.1.13 フィルタセットの定義	109
6.1.14 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定	110
6.1.15 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定	110
6.1.16 動的フィルターの定義	111
6.1.17 動的フィルターのタイムアウトの設定	112
6.1.18 FQDN フィルターで使用するキャッシュのタイマーの設定	113
6.1.19 侵入検知機能の動作の設定	114
6.1.20 1 秒間に侵入検知情報を通知する頻度の設定	115
6.1.21 重複する侵入検知情報の通知抑制の設定	115
6.1.22 侵入検知情報の最大表示件数の設定	116
6.1.23 TCP セッションの MSS 制限の設定	116
6.1.24 TCP ウィンドウ・スケール・オプションを変更する	117
6.1.25 ルーターが端点となる TCP のセッション数の設定	117
6.1.26 IPv4 の経路情報に変化があった時にログに記録するか否かの設定	118
6.1.27 フィルタリングによるセキュリティーの設定	118
6.1.28 ルールに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定	119
6.1.29 IP パケットの TOS フィールドの書き換えの設定	120
6.1.30 代理 ARP の設定	121
6.1.31 ARP エントリの寿命の設定	121
6.1.32 静的 ARP エントリの設定	122
6.1.33 ARP が解決されるまでの間に送信を保留しておくパケットの数を制御する	122
6.1.34 ARP エントリの変化をログに残すか否かの設定	123

6.1.35 ネットワーク監視機能の設定.....	123
6.1.36 implicit 経路の優先度の設定.....	125
6.1.37 フローテーブルの各エントリの寿命を設定する.....	126
6.1.38 フローテーブルのエントリー数の設定.....	126
6.1.39 フラグメントパケットを再構成するために保持しておく時間を設定.....	127
6.1.40 IP パケットの DS フィールドの書き換えの設定.....	127
6.2 PP 側の設定.....	128
6.2.1 PP 側 IP アドレスの設定.....	128
6.2.2 リモート IP アドレスプールの設定.....	129
6.2.3 PP 経由のキープアライブの時間間隔の設定.....	130
6.2.4 PP 経由のキープアライブを使用するか否かの設定.....	131
6.2.5 PP 経由のキープアライブのログをとるか否かの設定.....	132
6.3 RIP の設定.....	132
6.3.1 RIP を使用するか否かの設定.....	132
6.3.2 RIP に関して信用できるゲートウェイの設定.....	133
6.3.3 RIP による経路の優先度の設定.....	133
6.3.4 RIP パケットの送信に関する設定.....	134
6.3.5 RIP パケットの受信に関する設定.....	134
6.3.6 RIP のフィルタリングの設定.....	135
6.3.7 RIP で加算するホップ数の設定.....	136
6.3.8 RIP2 での認証の設定.....	136
6.3.9 RIP2 での認証キーの設定.....	137
6.3.10 RIPv2 での広告動作モードの設定.....	137
6.3.11 回線切断時の経路保持の設定.....	138
6.3.12 回線接続時の PP 側の RIP の動作の設定.....	138
6.3.13 回線接続時の PP 側の RIP 送出の時間間隔の設定.....	139
6.3.14 回線切断時の PP 側の RIP の動作の設定.....	139
6.3.15 回線切断時の PP 側の RIP 送出の時間間隔の設定.....	140
6.3.16 バックアップ時の RIP の送信元インターフェース切り替えの設定.....	140
6.3.17 RIP で強制的に経路を広告する.....	140
6.3.18 RIP2 でのフィルターの比較方法.....	141
6.3.19 RIP のタイマを調整する.....	142
6.4 VRRP の設定.....	142
6.4.1 インターフェース毎の VRRP の設定.....	142
6.4.2 シャットダウントリガーの設定.....	143
6.5 バックアップの設定.....	145
6.5.1 プロバイダー接続がダウンした時に PP バックアップする接続先の指定.....	145
6.5.2 バックアップからの復帰待ち時間の設定.....	146
6.5.3 LAN 経由でのプロバイダー接続がダウンした時にバックアップする接続先の指定.....	146
6.5.4 バックアップからの復帰待ち時間の設定.....	147
6.5.5 LAN 経由のキープアライブを使用するか否かの設定.....	147
6.5.6 LAN 経由のキープアライブの時間間隔の設定.....	148
6.5.7 LAN 経由のキープアライブのログをとるか否かの設定.....	149
6.5.8 ONU 経由でのプロバイダー接続がダウンした時にバックアップする接続先の指定.....	149
6.5.9 バックアップからの復帰待ち時間の設定.....	150
6.5.10 ONU 経由のキープアライブを使用するか否かの設定.....	150
6.5.11 ONU 経由のキープアライブの時間間隔の設定.....	151
6.5.12 ONU 経由のキープアライブのログをとるか否かの設定.....	151
6.6 パケット転送フィルターの設定.....	152
6.6.1 パケット転送フィルターの定義.....	152
6.6.2 インターフェースへのパケット転送フィルターの適用.....	153

## 第 7 章 : イーサネットフィルターの設定.....154

7.1 フィルター定義の設定.....	154
7.2 インターフェースへの適用の設定.....	156
7.3 イーサネットフィルターの状態の表示.....	156

## 第 8 章 : URL フィルターの設定.....158

8.1 フィルター定義の設定.....	158
---------------------	-----

8.2 URL フィルターのインターフェースへの適用.....	159
8.3 URL フィルターでチェックを行う HTTP のポート番号の設定.....	159
8.4 URL フィルターを使用するか否かの設定.....	159
8.5 URL フィルターで破棄するパケットの送信元に HTTP レスポンスを返す動作の設定.....	160
8.6 フィルターにマッチした際にログを出力するか否かの設定.....	161

## 第 9 章 : PPP の設定.....162

9.1 相手の名前とパスワードの設定.....	162
9.2 受け入れる認証タイプの設定.....	162
9.3 要求する認証タイプの設定.....	163
9.4 自分の名前とパスワードの設定.....	163
9.5 同一 username を持つ相手からの二重接続を禁止するか否かの設定.....	164
9.6 常時接続の設定.....	164
9.7 LCP 関連の設定.....	165
9.7.1 Address and Control Field Compression オプション使用の設定.....	165
9.7.2 Magic Number オプション使用の設定.....	166
9.7.3 Maximum Receive Unit オプション使用の設定.....	166
9.7.4 Protocol Field Compression オプション使用の設定.....	166
9.7.5 lcp-restart パラメーターの設定.....	167
9.7.6 lcp-max-terminate パラメーターの設定.....	167
9.7.7 lcp-max-configure パラメーターの設定.....	167
9.7.8 lcp-max-failure パラメーターの設定.....	168
9.7.9 Configure-Request をすぐに送信するか否かの設定.....	168
9.8 PAP 関連の設定.....	168
9.8.1 pap-restart パラメーターの設定.....	168
9.8.2 pap-max-authreq パラメーターの設定.....	169
9.9 CHAP 関連の設定.....	169
9.9.1 chap-restart パラメーターの設定.....	169
9.9.2 chap-max-challenge パラメーターの設定.....	169
9.10 IPCP 関連の設定.....	170
9.10.1 Van Jacobson Compressed TCP/IP 使用の設定.....	170
9.10.2 PP 側 IP アドレスのネゴシエーションの設定.....	170
9.10.3 ipcp-restart パラメーターの設定.....	170
9.10.4 ipcp-max-terminate パラメーターの設定.....	171
9.10.5 ipcp-max-configure パラメーターの設定.....	171
9.10.6 ipcp-max-failure パラメーターの設定.....	171
9.10.7 WINS サーバーの IP アドレスの設定.....	171
9.10.8 IPCP の MS 拡張オプションを使うか否かの設定.....	172
9.10.9 ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定.....	172
9.11 MSCBCP 関連の設定.....	172
9.11.1 mscbcpr-restart パラメーターの設定.....	172
9.11.2 mscbcpr-maxretry パラメーターの設定.....	173
9.12 CCP 関連の設定.....	173
9.12.1 全パケットの圧縮タイプの設定.....	173
9.12.2 ccp-restart パラメーターの設定.....	174
9.12.3 ccp-max-terminate パラメーターの設定.....	174
9.12.4 ccp-max-configure パラメーターの設定.....	174
9.12.5 ccp-max-failure パラメーターの設定.....	175
9.13 IPV6CP 関連の設定.....	175
9.13.1 IPV6CP を使用するか否かの設定.....	175
9.14 PPPoE 関連の設定.....	175
9.14.1 PPPoE で使用する LAN インターフェースの指定.....	175
9.14.2 アクセスコンセントレータ名の設定.....	176
9.14.3 セッションの自動接続の設定.....	176
9.14.4 セッションの自動切断の設定.....	176
9.14.5 PADI パケットの最大再送回数の設定.....	177
9.14.6 PADI パケットの再送時間の設定.....	177
9.14.7 PADR パケットの最大再送回数の設定.....	177
9.14.8 PADR パケットの再送時間の設定.....	177
9.14.9 PPPoE セッションの切断タイマの設定.....	178

9.14.10 サービス名の指定.....	178
9.14.11 TCP パケットの MSS の制限の有無とサイズの指定.....	178
9.14.12 ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定.....	179
9.14.13 認証失敗の最大回数を設定する.....	179
9.14.14 PPPoE フレームを中継するインターフェースの指定.....	180
<b>第 10 章 : DHCP の設定.....</b>	<b>181</b>
10.1 DHCP サーバー・リレーエージェント機能.....	181
10.1.1 DHCP の動作の設定.....	181
10.1.2 RFC2131 対応動作の設定.....	182
10.1.3 リースする IP アドレスの重複をチェックするか否かの設定.....	183
10.1.4 DHCP スコープの定義.....	184
10.1.5 DHCP 予約アドレスの設定.....	185
10.1.6 DHCP アドレス割り当て動作の設定.....	187
10.1.7 DHCP 割り当て情報を元にした予約設定の生成.....	188
10.1.8 DHCP オプションの設定.....	189
10.1.9 DHCP リース情報の手動追加.....	190
10.1.10 DHCP リース情報の手動削除.....	190
10.1.11 DHCP サーバーの指定の設定.....	191
10.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定.....	191
10.1.13 DHCP サーバーの選択方法の設定.....	191
10.1.14 DHCP BOOTREQUEST パケットの中継基準の設定.....	192
10.1.15 インターフェース毎の DHCP の動作の設定.....	192
10.2 DHCP クライアント機能.....	193
10.2.1 DHCP クライアントのホスト名の設定.....	193
10.2.2 要求する IP アドレスリース期間の設定.....	193
10.2.3 IP アドレス取得要求の再送回数と間隔の設定.....	194
10.2.4 DHCP クライアント ID オプションの設定.....	194
10.2.5 DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定.....	195
10.2.6 リンクダウンした時に情報を解放するか否かの設定.....	196
<b>第 11 章 : ICMP の設定.....</b>	<b>198</b>
11.1 IPv4 の設定.....	198
11.1.1 ICMP Echo Reply を送信するか否かの設定.....	198
11.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定.....	198
11.1.3 ICMP Mask Reply を送信するか否かの設定.....	198
11.1.4 ICMP Parameter Problem を送信するか否かの設定.....	199
11.1.5 ICMP Redirect を送信するか否かの設定.....	199
11.1.6 ICMP Redirect 受信時の処理の設定.....	199
11.1.7 ICMP Time Exceeded を送信するか否かの設定.....	200
11.1.8 ICMP Timestamp Reply を送信するか否かの設定.....	200
11.1.9 ICMP Destination Unreachable を送信するか否かの設定.....	201
11.1.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定.....	201
11.1.11 受信した ICMP のログを記録するか否かの設定.....	202
11.1.12 ステルス機能の設定.....	202
11.2 IPv6 の設定.....	203
11.2.1 ICMP Echo Reply を送信するか否かの設定.....	203
11.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定.....	203
11.2.3 ICMP Parameter Problem を送信するか否かの設定.....	204
11.2.4 ICMP Redirect を送信するか否かの設定.....	204
11.2.5 ICMP Redirect 受信時の処理の設定.....	204
11.2.6 ICMP Time Exceeded を送信するか否かの設定.....	205
11.2.7 ICMP Destination Unreachable を送信するか否かの設定.....	205
11.2.8 受信した ICMP のログを記録するか否かの設定.....	206
11.2.9 ICMP Packet-Too-Big を送信するか否かの設定.....	206
11.2.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定.....	206
11.2.11 ステルス機能の設定.....	207

<b>第 12 章 : トンネリング</b> .....	<b>209</b>
12.1 トンネルインターフェースの使用許可の設定.....	209
12.2 トンネルインターフェースの使用不許可の設定.....	209
12.3 トンネルインターフェースの接続種別の設定.....	210
12.4 トンネルインターフェースの種別の設定.....	210
12.5 トンネルインターフェースの IPv4 アドレスの設定.....	211
12.6 トンネルインターフェースの相手側の IPv4 アドレスの設定.....	211
12.7 相手側トンネルインターフェースの端点 IP アドレスの設定.....	212
12.8 自分側トンネルインターフェースの端点 IP アドレスの設定.....	212
12.9 トンネルインターフェースの端点 IP アドレスの設定.....	213
12.10 トンネルの端点の名前の設定.....	213
12.11 マルチポイントトンネルのサーバーの設定.....	214
12.12 マルチポイントトンネルで使用する自分の名前の設定.....	214
12.13 トンネルインターフェースの MAP-E 種別の設定.....	215
12.14 トンネルインターフェースの変換種別の設定.....	215
<b>第 13 章 : IPsec の設定</b> .....	<b>217</b>
13.1 IPsec の動作の設定.....	218
13.2 IKE バージョンの設定.....	218
13.3 IKE の認証方式の設定.....	218
13.4 事前共有鍵の登録.....	219
13.5 IKEv2 の認証に使用する PKI ファイルの設定.....	220
13.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定.....	220
13.7 EAP-MD5 によるユーザー認証の設定.....	221
13.8 EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定.....	221
13.9 IKE の鍵交換を始動するか否かの設定.....	222
13.10 設定が異なる場合に鍵交換を拒否するか否かの設定.....	223
13.11 IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定.....	223
13.12 鍵交換の再送回数と間隔の設定.....	224
13.13 相手側のセキュリティー・ゲートウェイの名前の設定.....	224
13.14 相手側セキュリティー・ゲートウェイの IP アドレスの設定.....	225
13.15 相手側の ID の設定.....	226
13.16 自分側のセキュリティー・ゲートウェイの名前の設定.....	227
13.17 自分側セキュリティー・ゲートウェイの IP アドレスの設定.....	227
13.18 自分側の ID の設定.....	228
13.19 IKE キープアライブ機能の設定.....	229
13.20 IKE キープアライブに関する SYSLOG を出力するか否かの設定.....	231
13.21 IKE が用いる暗号アルゴリズムの設定.....	231
13.22 受信した IKE パケットを蓄積するキューの長さの設定.....	232
13.23 IKE が用いるグループの設定.....	232
13.24 IKE が用いるハッシュアルゴリズムの設定.....	233
13.25 受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定.....	234
13.26 IKE ペイロードのタイプの設定.....	235
13.27 IKEv1 鍵交換タイプの設定.....	235
13.28 IKE の情報ペイロードを送信するか否かの設定.....	236
13.29 PFS を用いるか否かの設定.....	236
13.30 XAUTH の設定.....	237
13.31 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の設定.....	237
13.32 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の属性の設定.....	238
13.33 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの設定.....	239
13.34 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの属性の設定.....	239
13.35 XAUTH によるユーザー認証の設定.....	240
13.36 内部 IP アドレスプールの設定.....	241
13.37 IKE XAUTH Mode-Cfg メソッドの設定.....	241
13.38 IPsec クライアントに割り当てる内部 IP アドレスプールの設定.....	242
13.39 IKE のログの種類の設定.....	243
13.40 ESP を UDP でカプセル化して送受信するか否かの設定.....	243
13.41 折衝パラメーターを制限するか否かの設定.....	244



13.42 IKE のメッセージ ID 管理の設定.....	245
13.43 CHILD SA 作成方法の設定.....	245
13.44 鍵交換の始動パケットを受信するか否かの設定.....	246
13.45 SA 関連の設定.....	246
13.45.1 SA の寿命の設定.....	246
13.45.2 SA のポリシーの定義.....	248
13.45.3 SA の手動更新.....	250
13.45.4 ダングリング SA の動作の設定.....	250
13.45.5 IPsec NAT トラバーサルを利用するための設定.....	251
13.45.6 SA の削除.....	252
13.46 トンネルインターフェース関連の設定.....	253
13.46.1 IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定.....	253
13.46.2 IPsec トンネルの外側の IPv4 パケットに対する DF ビットの制御の設定.....	253
13.46.3 使用する SA のポリシーの設定.....	254
13.46.4 IPComp によるデータ圧縮の設定.....	254
13.46.5 トンネルバックアップの設定.....	255
13.46.6 トンネルテンプレートの設定.....	256
13.47 トランスポートモード関連の設定.....	258
13.47.1 トランスポートモードの定義.....	258
13.47.2 トランスポートモードのテンプレートの設定.....	258
13.48 PKI 関連の設定.....	259
13.48.1 証明書ファイルの設定.....	259
13.48.2 CRL ファイルの設定.....	260
<b>第 14 章 : L2TP 機能の設定.....</b>	<b>261</b>
14.1 L2TP を動作させるか否かの設定.....	261
14.2 L2TP トンネル認証に関する設定.....	262
14.3 L2TP トンネルの切断タイマの設定.....	262
14.4 L2TP キープアライブの設定.....	263
14.5 L2TP キープアライブのログ設定.....	263
14.6 L2TP のコネクション制御の syslog を出力するか否かの設定.....	264
14.7 L2TPv3 の常時接続の設定.....	264
14.8 L2TP トンネルのホスト名の設定.....	265
14.9 L2TPv3 の Local Router ID の設定.....	265
14.10 L2TPv3 の Remote Router ID の設定.....	266
14.11 L2TPv3 の Remote End ID の設定.....	266
<b>第 15 章 : PPTP 機能の設定.....</b>	<b>267</b>
15.1 共通の設定.....	267
15.1.1 PPTP サーバーを動作させるか否かの設定.....	267
15.1.2 相手先情報番号にバインドされるトンネルインターフェースの設定.....	267
15.1.3 PPTP の動作タイプの設定.....	268
15.1.4 PPTP ホスト名の設定.....	268
15.1.5 PPTP ホスト名の設定.....	268
15.1.6 PPTP パケットのウィンドウサイズの設定.....	269
15.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定.....	269
15.1.8 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定.....	270
15.1.9 PPTP のコネクション制御の syslog を出力するか否かの設定.....	270
15.2 リモートアクセス VPN 機能.....	271
15.2.1 PPTP トンネルの出力切断タイマの設定.....	271
15.2.2 PPTP キープアライブの設定.....	271
15.2.3 PPTP キープアライブのログ設定.....	271
15.2.4 PPTP キープアライブを出すインターバルとカウントの設定.....	272
15.2.5 PPTP 接続において暗号化の有無により接続を許可するか否かの設定.....	272
<b>第 16 章 : IPIP トンネリング機能の設定.....</b>	<b>273</b>
16.1 IPIP キープアライブの設定.....	273
16.2 IPIP キープアライブのログ設定.....	273

<b>第 17 章 : クラウドサービスとの VPN 接続設定機能の設定</b> .....	<b>275</b>
17.1 VPN 接続するクラウドサービスの指定.....	275
17.2 クラウドサービスとの VPN 接続設定に必要なパラメーターの設定.....	275
17.3 クラウドサービスとの VPN 接続設定の名称の設定.....	276
17.4 クラウドサービスとの VPN 接続を設定するトンネルインターフェースの指定.....	276
17.5 クラウドサービスとの VPN 接続設定に使用するオプションの設定.....	277
17.6 クラウドサービスとの VPN 接続設定の手動実行.....	277
17.7 クラウドサービスとの VPN 接続設定の状態の表示.....	278
17.8 クラウドサービス接続時の詳細情報を SYSLOG に表示.....	278
<b>第 18 章 : SNMP の設定</b> .....	<b>280</b>
18.1 SNMPv1 によるアクセスを許可するホストの設定.....	280
18.2 SNMPv1 の読み出し専用のコミュニティ名の設定.....	281
18.3 SNMPv1 の読み書き可能なコミュニティ名の設定.....	281
18.4 SNMPv1 トラップの送信先の設定.....	281
18.5 SNMPv1 トラップのコミュニティ名の設定.....	282
18.6 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定.....	282
18.7 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定.....	282
18.8 SNMPv2c によるアクセスを許可するホストの設定.....	283
18.9 SNMPv2c の読み出し専用のコミュニティ名の設定.....	283
18.10 SNMPv2c の読み書き可能なコミュニティ名の設定.....	284
18.11 SNMPv2c トラップの送信先の設定.....	284
18.12 SNMPv2c トラップのコミュニティ名の設定.....	284
18.13 SNMPv3 エンジン ID の設定.....	285
18.14 SNMPv3 コンテキスト名の設定.....	285
18.15 SNMPv3 USM で管理するユーザーの設定.....	285
18.16 SNMPv3 によるアクセスを許可するホストの設定.....	286
18.17 SNMPv3 VACM で管理する MIB ビューファミリの設定.....	287
18.18 SNMPv3 VACM で管理するアクセスポリシーの設定.....	288
18.19 SNMPv3 トラップの送信先の設定.....	288
18.20 SNMP 送信パケットの始点アドレスの設定.....	289
18.21 sysContact の設定.....	289
18.22 sysLocation の設定.....	289
18.23 sysName の設定.....	290
18.24 SNMP 標準トラップを送信するか否かの設定.....	290
18.25 SNMP トラップの送信の遅延時間の設定.....	291
18.26 SNMP の linkDown トラップの送信制御の設定.....	291
18.27 PP インターフェースの情報を MIB2 の範囲で表示するか否かの設定.....	292
18.28 トンネルインターフェースの情報を MIB2 の範囲で表示するか否かの設定.....	292
18.29 スイッチのインターフェースの情報を MIB2 の範囲で表示するか否かの設定.....	293
18.30 内蔵無線 WAN インターフェースの情報を MIB2 の範囲で表示するか否かの設定.....	293
18.31 PP インターフェースのアドレスの強制表示の設定.....	294
18.32 LAN インターフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設 定.....	294
18.33 電波強度トラップを送信するか否かの設定.....	295
18.34 内蔵無線 WAN モジュールの電波強度トラップを送信するか否かの設定.....	295
18.35 スイッチへ静的に付与するインターフェース番号の設定.....	296
18.36 スイッチへ静的に付与するスイッチ番号の設定.....	296
18.37 スイッチの状態による SNMP トラップの条件の設定.....	297
18.38 スイッチで共通の SNMP トラップの条件の設定.....	298
<b>第 19 章 : RADIUS の設定</b> .....	<b>299</b>
19.1 RADIUS による認証を使用するか否かの設定.....	299
19.2 RADIUS によるアカウントを使用するか否かの設定.....	299
19.3 RADIUS サーバーの指定.....	300
19.4 RADIUS 認証サーバーの指定.....	300
19.5 RADIUS アカウントサーバーの指定.....	301

19.6 RADIUS 認証サーバーの UDP ポートの設定.....	301
19.7 RADIUS アカウントサーバーの UDP ポートの設定.....	301
19.8 RADIUS シークレットの設定.....	302
19.9 RADIUS 再送信パラメーターの設定.....	302
<b>第 20 章 : NAT 機能.....</b>	<b>303</b>
20.1 NAT 機能の動作タイプの設定.....	303
20.2 インターフェースへの NAT ディスクリプター適用の設定.....	303
20.3 NAT ディスクリプターの動作タイプの設定.....	304
20.4 NAT 処理の外側 IP アドレスの設定.....	305
20.5 NAT 処理の内側 IP アドレスの設定.....	306
20.6 静的 NAT エントリの設定.....	306
20.7 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定.....	307
20.8 静的 IP マスカレードエントリの設定.....	307
20.9 NAT の IP アドレスマップの消去タイマの設定.....	308
20.10 IP マスカレードテーブルの TTL 処理方式の設定.....	309
20.11 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定.....	309
20.12 IP マスカレードで利用するポートの範囲の設定.....	310
20.13 FTP として認識するポート番号の設定.....	311
20.14 IP マスカレードで変換しないポート番号の範囲の設定.....	311
20.15 NAT のアドレス割当をログに記録するか否かの設定.....	311
20.16 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定.....	312
20.17 IP マスカレード変換時に DF ビットを削除するか否かの設定.....	312
20.18 IP マスカレードで変換するホスト毎のセッション数の設定.....	313
20.19 IP マスカレードで変換する合計セッション数の設定.....	313
<b>第 21 章 : DNS の設定.....</b>	<b>314</b>
21.1 DNS を利用するか否かの設定.....	314
21.2 ルーター自身の FQDN の設定.....	314
21.3 DNS サーバーの IP アドレスの設定.....	315
21.4 DNS ドメイン名の設定.....	316
21.5 DNS サーバーを通知してもらう相手先情報番号の設定.....	316
21.6 DNS サーバーアドレスを取得するインターフェースの設定.....	317
21.7 DNS サーバーアドレスを取得するインターフェースの設定.....	318
21.8 DHCP/DHCPv6/PCP MS 拡張で DNS サーバーを通知する順序の設定.....	318
21.9 プライベートアドレスに対する問い合わせを処理するか否かの設定.....	319
21.10 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定.....	319
21.11 SYSLOG 表示で DNS により名前解決するか否かの設定.....	320
21.12 DNS 問い合わせの内容に応じた DNS サーバーの選択.....	320
21.13 静的 DNS レコードの登録.....	323
21.14 DNS 問い合わせパケットの始点ポート番号の設定.....	324
21.15 DNS サーバーへアクセスできるホストの設定.....	324
21.16 DNS キャッシュを使用するか否かの設定.....	325
21.17 DNS キャッシュの最大エントリ数の設定.....	326
21.18 DNS フォールバック機能を使用するか否かの設定.....	326
<b>第 22 章 : NAT46/DNS46 機能.....</b>	<b>327</b>
22.1 NAT46 機能で使用する IPv4 アドレスプールの設定.....	327
22.2 NAT46 機能で使用する IPv6 プレフィックスの設定.....	327
22.3 NAT46 機能で使用する宛先アドレスを静的に対応づける設定.....	328
22.4 NAT46 エントリーの表示.....	328
<b>第 23 章 : 優先制御 / 帯域制御.....</b>	<b>330</b>
23.1 インターフェース速度の設定.....	330
23.2 クラス分けのためのフィルター設定.....	330
23.3 キューイングアルゴリズムタイプの選択.....	333
23.4 クラス分けフィルターの適用.....	334

23.5 クラス毎のキュー長の設定.....	335
23.6 デフォルトクラスの設定.....	335
23.7 クラスの属性の設定.....	336
23.8 動的なクラス変更 (Dynamic Class Control) の設定.....	336
<b>第 24 章 : 連携機能.....</b>	<b>339</b>
24.1 連携動作を行うか否かの設定.....	339
24.2 連携動作で使用するポート番号の設定.....	339
24.3 帯域測定で連携動作を行う相手毎の動作の設定.....	340
24.4 負荷監視通知で連携動作を行う相手毎の動作の設定.....	341
24.5 負荷監視サーバーとしての動作トリガの設定.....	343
24.6 負荷監視クライアントとしての動作の設定.....	344
24.7 連携動作の手動実行.....	345
<b>第 25 章 : OSPF.....</b>	<b>346</b>
25.1 OSPF の有効設定.....	346
25.2 OSPF の使用設定.....	346
25.3 OSPF による経路の優先度設定.....	346
25.4 OSPF のルーター ID 設定.....	347
25.5 OSPF で受け取った経路をルーティングテーブルに反映させるか否かの設定.....	347
25.6 外部プロトコルによる経路導入.....	348
25.7 OSPF で受け取った経路をどう扱うかのフィルターの設定.....	348
25.8 外部経路導入に適用するフィルター定義.....	350
25.9 OSPF エリア設定.....	351
25.10 エリアへの経路広告.....	352
25.11 スタブ的接続の広告.....	353
25.12 仮想リンク設定.....	353
25.13 指定インターフェースの OSPF エリア設定.....	354
25.14 非ブロードキャスト型ネットワークに接続されている OSPF ルーターの指定.....	358
25.15 スタブが存在する時のネットワーク経路の扱いの設定.....	358
25.16 OSPF の状態遷移とパケットの送受信をログに記録するか否かの設定.....	358
25.17 インターフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定.....	359
<b>第 26 章 : BGP.....</b>	<b>360</b>
26.1 BGP の起動の設定.....	360
26.2 経路の集約の設定.....	360
26.3 経路を集約するためのフィルターの設定.....	360
26.4 AS 番号の設定.....	361
26.5 ルーター ID の設定.....	361
26.6 BGP による経路の優先度の設定.....	362
26.7 BGP で受信した経路に対するフィルターの適用.....	362
26.8 BGP で受信する経路に適用するフィルターの設定.....	363
26.9 BGP に導入する経路に対するフィルターの適用.....	364
26.10 BGP の設定の有効化.....	365
26.11 BGP に導入する経路に適用するフィルターの設定.....	365
26.12 BGP による接続先の設定.....	366
26.13 BGP のログの設定.....	367
26.14 インターフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定.....	368
26.15 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値の設定.....	368
26.16 BGP で受信した経路に対する経路選択の優先順位の規則を設定.....	369
<b>第 27 章 : IPv6.....</b>	<b>371</b>
27.1 共通の設定.....	371
27.1.1 IPv6 パケットを扱うか否かの設定.....	371
27.1.2 IPv6 インターフェースのリンク MTU の設定.....	371
27.1.3 TCP セッションの MSS 制限の設定.....	372
27.1.4 TCP ウィンドウ・スケール・オプションを変更する.....	372

27.1.5 タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かの設定	373
27.1.6 IPv6 ファストパス機能の設定	373
27.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケット数の設定	374
27.1.8 近隣キャッシュの最大エントリ数の設定	374
27.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定	375
27.1.10 IPv6 パケットの DS フィールドの書き換えの設定	375
27.2 IPv6 アドレスの管理	376
27.2.1 インターフェースの IPv6 アドレスの設定	376
27.2.2 インターフェースのプレフィックスに基づく IPv6 アドレスの設定	378
27.2.3 IPv6 プレフィックスに変化があった時にログに記録するか否かの設定	379
27.2.4 DHCPv6 の動作の設定	380
27.2.5 DAD (Duplicate Address Detection) の送信回数数の設定	381
27.2.6 自動的に設定される IPv6 アドレスの最大数の設定	381
27.2.7 始点 IPv6 アドレスを選択する規則の設定	382
27.3 近隣探索	382
27.3.1 ルーター広告で配布するプレフィックスの定義	382
27.3.2 ルーター広告で配布する RDNSS オプションの定義	384
27.3.3 ルーター広告の送信の制御	385
27.3.4 ルーター要請の再送機能の設定	386
27.4 経路制御	387
27.4.1 IPv6 の経路情報の追加	387
27.4.2 IPv6 の経路情報に変化があった時にログに記録するか否かの設定	389
27.5 RIPng	389
27.5.1 RIPng の使用の設定	389
27.5.2 インターフェースにおける RIPng の送信ポリシーの設定	389
27.5.3 インターフェースにおける RIPng の受信ポリシーの設定	390
27.5.4 RIPng の加算ホップ数の設定	390
27.5.5 インターフェースにおける信頼できる RIPng ゲートウェイの設定	391
27.5.6 RIPng で送受信する経路に対するフィルタリングの設定	391
27.5.7 回線接続時の PP 側の RIPng の動作の設定	392
27.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定	392
27.5.9 回線切断時の PP 側の RIPng の動作の設定	393
27.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定	393
27.5.11 RIPng による経路を回線切断時に保持するか否かの設定	393
27.5.12 RIPng による経路の優先度の設定	394
27.6 VRRPv3 の設定	394
27.6.1 インターフェース毎の VRRPv3 の設定	394
27.6.2 シャットダウントリガーの設定	395
27.7 フィルターの設定	396
27.7.1 IPv6 フィルターの定義	396
27.7.2 IPv6 フィルターの適用	398
27.7.3 IPv6 動的フィルターの定義	399
27.8 IPv6 マルチキャストパケットの転送の設定	400
27.8.1 MLD の動作の設定	401
27.8.2 MLD の静的な設定	402
27.9 近隣要請	403
27.9.1 アドレス重複チェックをトリガーに近隣要請を行うか否かの設定	403

## 第 28 章 : OSPFv3.....404

28.1 OSPFv3 の有効設定	404
28.2 OSPFv3 の使用設定	404
28.3 OSPFv3 のルーター ID 設定	404
28.4 OSPFv3 エリア設定	405
28.5 エリアへの経路広告	405
28.6 指定インターフェースの OSPFv3 エリア設定	406
28.7 仮想リンク設定	408
28.8 OSPFv3 による経路の優先度設定	409
28.9 OSPFv3 で受け取った経路をルーティングテーブルに反映させるか否かの設定	409
28.10 OSPFv3 で受け取った経路をどう扱うかのフィルターの設定	410

28.11 外部プロトコルによる経路導入.....	411
28.12 外部経路導入に適用するフィルター定義.....	412
28.13 OSPFv3 のログ出力設定.....	413

## 第 29 章 : アナログ通信機能の設定.....414

29.1 キー操作とコンソールコマンドの対応.....	414
29.2 TEL ポートごとの設定.....	415
29.2.1 TEL ポートを使うか否かの設定.....	415
29.2.2 TEL ポートのダイヤルイン番号の設定.....	416
29.2.3 TEL ポートに接続する機器の設定.....	416
29.2.4 TEL ポートの発信者番号を通知するか否かの設定.....	417
29.2.5 相手先番号による即時発信を許可するか否かの設定.....	418
29.2.6 ダイヤル完了ボタンの設定.....	418
29.2.7 グローバル着信を許可するか否かの設定.....	419
29.2.8 TEL ポートでの識別着信をするか否かの設定.....	419
29.2.9 識別着信リストの登録.....	420
29.2.10 サブアドレス無し着信を許可するか否かの設定.....	421
29.2.11 サブアドレスにかかわらず着信を許可するか否かの設定.....	421
29.2.12 異なる種類の通信機器からの着信を許可するか否かの設定.....	422
29.2.13 話中着信を許可するか否かの設定.....	422
29.2.14 着信ベルリストの登録.....	423
29.2.15 ナンバー・ディスプレイの設定.....	424
29.2.16 指定した TEL ポートの優先着信順位を設定.....	424
29.2.17 ダイヤル桁間タイマの設定.....	425
29.2.18 フッキングを判定する時間の設定.....	425
29.2.19 フッキング後にキー操作を受け入れる時間の設定.....	426
29.2.20 フッキング及びオンフック検出を無効と判断する時間の設定.....	426
29.2.21 オフフックを検出するまでの遅延時間の設定.....	427
29.2.22 オフフック/オンフックを検出する閾値の設定.....	427
29.2.23 インピーダンスの設定.....	428
29.2.24 保留音の種類の設定.....	428
29.2.25 TEL ポートの再呼出時間設定.....	429
29.2.26 フレックスホン機能の使用パターンの設定.....	429
29.2.27 着信転送先アドレスの設定.....	430
29.2.28 着信転送を起動するタイミングの設定.....	430
29.2.29 着信転送トーカーの設定.....	431
29.2.30 着信転送が拒否された時の動作の設定.....	432
29.2.31 送話 PAD の設定.....	432
29.2.32 受話 PAD の設定.....	433
29.2.33 MP 時に電話発着信のために 1B チャネルに落とすか否かの設定.....	434
29.2.34 TEL ポートへの切断信号の送付の設定.....	434
29.2.35 アザーダイヤルトーンを出すか否かの設定.....	435
29.2.36 着信時の着信ベル鳴動モードの設定.....	435
29.2.37 緊急番号の処理方式の設定.....	436
29.2.38 i・ナンバーサービスのポート番号の設定.....	436
29.2.39 アナログダイヤルインと無鳴動着信機能の設定.....	437
29.2.40 PB ダイヤルインの一次応答検出タイミングの設定.....	438
29.2.41 発番号情報なし着信機能の設定.....	439
29.2.42 RTP 音声の受話 PAD の設定.....	439
29.2.43 RTP 音声の送話 PAD の設定.....	440
29.2.44 ポーズを判定する時間の設定.....	441
29.2.45 TEL ポートに対する電力供給の設定.....	441
29.2.46 オフフックで発信する相手先電話番号の設定.....	442

## 第 30 章 : カスケード接続機能の設定.....443

30.1 カスケード接続モードの設定.....	443
30.2 カスケード接続に利用する IP アドレス取得インターフェースの設定.....	443
30.3 アナログ親機となる機器の設定.....	444
30.4 アナログ親機となる機器の設定.....	444

30.5 アナログ子機受け入れモードの設定.....	445
30.6 アナログ子機受け入れモードの設定.....	445
30.7 アナログ子機受け入れモードの設定.....	446
30.8 カスケード接続のログを記録するか否かの設定.....	446

## 第 31 章 : SIP 機能の設定.....448

31.1 共通の設定.....	448
31.1.1 SIP による VoIP 機能を使用するか否かの設定.....	448
31.1.2 SIP による発信時に使用する IP プロトコルの選択.....	448
31.1.3 SIP による VoIP 機能で利用可能な音声コーデックの設定.....	448
31.1.4 SIP のリクエスト再送タイムアウト値の設定.....	449
31.1.5 ネットボランチ電話で使用するドメイン名の設定.....	450
31.1.6 ネットボランチ電話で SIP ユーザー名として付与する番号桁数の設定.....	450
31.1.7 特定のダイヤルに対応する SIP による発信先の設定.....	451
31.1.8 SIP の session-timer 機能のタイマ値の設定.....	451
31.1.9 SIP による発信時に 100rel をサポートするか否かの設定.....	452
31.1.10 送信する SIP パケットに User-Agent ヘッダを付加する設定.....	453
31.1.11 着信可能なポートがない場合に返す SIP のレスポンスコードの設定.....	453
31.1.12 SIP による着信時の INVITE に refresher 指定がない場合の設定.....	453
31.1.13 インターネット電話着信時におけるネーム・ディスプレイ情報通知設定.....	454
31.1.14 SIP による着信時に P-N-UAType ヘッダをサポートするか否かの設定.....	454
31.1.15 着信時のセッションタイマのリクエストを設定.....	455
31.1.16 SIP 着信時に SIP ユーザー名を検証するかどうかの設定.....	455
31.1.17 SIP で使用する IP アドレスの設定.....	456
31.1.18 SIP メッセージのログを記録するか否かの設定.....	456
31.2 SIP サーバー毎の設定.....	456
31.2.1 SIP サーバーの設定.....	456
31.2.2 SIP サーバー毎の先頭に付加された 184/186 の扱いの設定.....	457
31.2.3 SIP サーバー毎の発信時に使用する自己 SIP ディスプレイ名の設定.....	458
31.2.4 SIP サーバー毎の発信時の相手 SIP アドレスのドメイン名の設定.....	458
31.2.5 SIP サーバー毎の session-timer 機能のタイマ値の設定.....	459
31.2.6 SIP サーバー毎の発信時に 100rel をサポートするか否かの設定.....	460
31.2.7 SIP サーバー毎の REGISTER リクエストの更新間隔の設定.....	460
31.2.8 SIP サーバー毎の REGISTER リクエストの Request-URI の設定.....	461
31.2.9 SIP サーバー毎の REGISTER リクエストの Contact ヘッダに付加する q 値の設定.....	461
31.2.10 SIP サーバー毎の着信時の発番号情報通知ルールの設定.....	461
31.2.11 SIP サーバー経由接続時におけるアナログ付加サービス設定.....	462
31.2.12 SIP サーバーへの接続状態に応じて発信するか否かの設定.....	463
31.2.13 SIP サーバーへの発信に番号以外を使えないように制限する設定.....	463
31.2.14 自分自身の SIP アドレスへの発信を許可するかどうかの設定.....	464
31.2.15 SIP サーバー毎の代表 SIP アドレスの設定.....	464
31.2.16 発信時の 5xx エラーをサーバー障害とするか否かの設定.....	464
31.2.17 SIP サーバー毎の REGISTER リクエストの Contact ヘッダの設定.....	465
31.3 TEL ポートの設定.....	465
31.3.1 TEL ポートからの SIP による発信の制限の設定.....	465
31.3.2 TEL ポートからの SIP による発信で使用する自己 SIP ユーザー名の設定.....	466
31.3.3 TEL ポートからの SIP による発信で使用する自己 SIP ディスプレイ名の設定.....	467
31.3.4 TEL ポートにおける宛先 SIP アドレスによる着信制限の設定.....	467
31.3.5 TEL ポートにおける SIP の着信識別で使用する自己 SIP アドレスの設定.....	468
31.3.6 TEL ポートにおける SIP の着信に対するアナログダイヤルインと無鳴動着信機能の設定.....	468
31.3.7 TEL ポートにおける特定のプレフィックスによる発呼経路選択の設定.....	469
31.3.8 TEL ポートでの識別着信をするか否かの設定.....	471
31.3.9 識別着信リストの登録.....	472
31.3.10 発番号情報なし SIP 着信機能の設定.....	473
31.4 電話番号ルーティングの設定.....	473
31.4.1 ダイヤル番号によって発呼経路を自動選択するテーブルの設定.....	473
31.4.2 ダイヤル番号と発呼経路との関連付けの設定.....	474
31.5 ひかり電話の設定.....	476
31.5.1 NGN 網に接続するインターフェースの設定.....	476

31.5.2 NGN 網を介したリナンバリング発生時に LAN インターフェースを一時的にリンクダウンするか否かの設定.....	476
31.5.3 NGN 網接続情報の表示.....	477
31.6 データコネク ト接続機能の設定.....	477
31.6.1 NGN 網を介したトンネルインターフェースの切断タイマの設定.....	477
31.6.2 NGN 網を介したトンネルインターフェースの帯域の設定.....	478
31.6.3 NGN 網を介したトンネルインターフェースの着信許可の設定.....	478
31.6.4 NGN 網を介したトンネルインターフェースの発信許可の設定.....	479
31.6.5 NGN 網を介したトンネルインターフェースで使用する LAN インターフェースの設定.....	479
31.6.6 NGN 網を介したトンネルインターフェースで接続に失敗した場合に接続を試みる相手番号の設定.....	479
31.6.7 NGN 電話番号を RADIUS で認証するか否かの設定.....	480
31.6.8 NGN 電話番号を RADIUS で認証するとき使用するパスワードの設定.....	480
31.6.9 NGN 網への発信時に RADIUS アカウンティングを使用するか否かの設定.....	481
31.6.10 NGN 網からの着信時に RADIUS アカウンティングを使用するか否かの設定.....	481
<b>第 32 章 : トリガによるメール通知機能.....</b>	<b>483</b>
32.1 メール設定識別名の設定.....	483
32.2 SMTP メールサーバーの設定.....	483
32.3 POP メールサーバーの設定.....	484
32.4 メール処理のタイムアウト値の設定.....	485
32.5 メールの送信時に使用するテンプレートの設定.....	485
32.6 メール通知のトリガの設定.....	487
<b>第 33 章 : HTTP サーバー機能.....</b>	<b>490</b>
33.1 共通の設定.....	490
33.1.1 HTTP サーバー機能の有無の設定.....	490
33.1.2 HTTP サーバーへアクセスできるホストの設定.....	490
33.1.3 HTTP サーバーのセッションタイムアウト時間の設定.....	491
33.1.4 HTTP サーバー機能の listen ポートの設定.....	491
33.1.5 PP インターフェースとトンネルインターフェースの名前の設定.....	491
<b>第 34 章 : ネットボランチ DNS サービスの設定.....</b>	<b>493</b>
34.1 ネットボランチ DNS サービスの使用の可否.....	493
34.2 ネットボランチ DNS サーバーへの手動更新.....	493
34.3 ネットボランチ DNS サーバーからの削除.....	494
34.4 ネットボランチ DNS サービスで使用するポート番号の設定.....	494
34.5 ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得.....	494
34.6 ホスト名の登録.....	495
34.7 電話アドレスの設定.....	496
34.8 通信タイムアウトの設定.....	496
34.9 ホスト名を自動生成するか否かの設定.....	496
34.10 NetVolante インターネット電話用ホスト名の使用の可否.....	497
34.11 シリアル番号を使ったホスト名登録コマンドの設定.....	498
34.12 ネットボランチ DNS サーバーの設定.....	498
34.13 ネットボランチ DNS サーバーアドレス更新機能の ON/OFF の設定.....	499
34.14 ネットボランチ DNS サーバーアドレス更新機能のポート番号の設定.....	499
34.15 自動更新に失敗した場合のリトライ間隔と回数の設定.....	500
34.16 ネットボランチ DNS 登録の定期更新間隔の設定.....	500
34.17 ネットボランチ DNS の自動登録に成功したとき設定を保存するファイルの設定.....	501
<b>第 35 章 : UPnP の設定.....</b>	<b>502</b>
35.1 UPnP を使用するかどうかの設定.....	502
35.2 UPnP に使用する IP アドレスを取得するインターフェースの設定.....	502
35.3 UPnP のポートマッピング用消去タイマのタイプの設定.....	503
35.4 UPnP のポートマッピングの消去タイマの設定.....	503
35.5 UPnP の syslog を出力するか否かの設定.....	503



<b>第 36 章 : スケジュール</b> .....	<b>505</b>
36.1 スケジュールの設定.....	505
<b>第 37 章 : VLAN の設定</b> .....	<b>508</b>
37.1 VLAN ID の設定.....	508
37.2 スイッチングハブのポートが所属する VLAN の設定.....	508
<b>第 38 章 : 生存通知機能</b> .....	<b>510</b>
38.1 生存通知の共有鍵の設定.....	510
38.2 生存通知を受信するか否かの設定.....	510
38.3 生存通知の実行.....	511
<b>第 39 章 : 生存通知機能 リリース 2</b> .....	<b>512</b>
39.1 通知名称の設定.....	512
39.2 通知設定の定義.....	512
39.3 通知設定の有効化.....	513
39.4 通知間隔の設定.....	513
39.5 通知を送信した際にログを記録するか否かの設定.....	514
39.6 受信設定の定義.....	514
39.7 受信設定の有効化.....	515
39.8 受信間隔の監視設定.....	515
39.9 通知を受信した際にログを記録するか否かの設定.....	516
39.10 同時に保持できる生存情報の最大数の設定.....	516
39.11 生存通知の状態のクリア.....	516
<b>第 40 章 : SNMP サーバー機能</b> .....	<b>518</b>
40.1 SNMP サーバー機能を有効にするか否かの設定.....	518
40.2 SNMP サーバーへのアクセスを許可するホストの設定.....	518
<b>第 41 章 : 外部メモリ機能</b> .....	<b>520</b>
41.1 USB ホスト機能を使うか否かの設定.....	520
41.2 USB バスで過電流保護機能が働くまでの時間の設定.....	521
41.3 microSD カードスロットを使うか否かの設定.....	521
41.4 外部メモリ用キャッシュメモリの動作モードの設定.....	521
41.5 ファイルアクセス高速化用キャッシュメモリのサイズの設定.....	522
41.6 外部メモリに保存する統計情報のファイル名のプレフィックスの設定.....	523
41.7 外部メモリに保存する SYSLOG ファイル名の指定.....	525
41.8 外部メモリボタンと DOWNLOAD ボタンの同時押下による設定ファイル、ファームウェアファイル のコピー操作を許可するか否かの設定.....	526
41.9 外部メモリ内のファイルからの起動を許可するか否かの設定.....	526
41.10 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する.....	527
41.11 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定.....	527
41.12 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、設定ファイル名の指定.....	528
41.13 ファイル検索時のタイムアウトを設定する.....	530
41.14 バッチファイルを実行する.....	530
41.15 バッチファイルと実行結果ファイルの設定.....	530
41.16 外部メモリ性能測定コマンド.....	531
41.17 DOWNLOAD ボタンを押した時に実行する機能の設定.....	532
41.18 DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定.....	532
41.19 シグネチャーを保存する外部メモリのディレクトリーの設定.....	533

<b>第 42 章 : 内蔵無線 WAN 機能.....</b>	<b>534</b>
42.1 内蔵無線 WAN モジュールを使用するか否かの設定.....	534
42.2 内蔵無線 WAN モジュールの無線通信機能を使うか否かの設定.....	535
42.3 電波の受信レベル取得機能の設定.....	535
42.4 電波の受信レベルの取得.....	536
42.5 内蔵無線 WAN モジュールに対する詳細な SYSLOG を出力するか否かの設定.....	536
42.6 内蔵無線 WAN インターフェースの選択.....	537
42.7 内蔵無線 WAN インターフェースの使用許可の設定.....	537
42.8 内蔵無線 WAN インターフェースの使用不許可の設定.....	538
42.9 内蔵無線 WAN の常時接続の設定.....	538
42.10 内蔵無線 WAN の発信先アクセスポイントの設定.....	538
42.11 内蔵無線 WAN の接続時の認証タイプの設定.....	539
42.12 内蔵無線 WAN でのユーザー名とパスワードの設定.....	539
42.13 内蔵無線 WAN からの自動発信設定.....	540
42.14 入力がないときに内蔵無線 WAN を切断するタイマの設定.....	540
42.15 出力がないときに内蔵無線 WAN を切断するタイマの設定.....	540
42.16 内蔵無線 WAN を切断するタイマの設定.....	541
42.17 内蔵無線 WAN での接続毎パケット通信量制限の設定.....	541
42.18 内蔵無線 WAN での接続毎パケット通信時間制限の設定.....	542
42.19 内蔵無線 WAN での通信制限の累積期間の設定.....	542
42.20 内蔵無線 WAN でのパケット通信量制限の設定.....	543
42.21 内蔵無線 WAN でのパケット通信時間制限の設定.....	543
42.22 内蔵無線 WAN で使用する通信方式とバンドの設定.....	544
42.23 内蔵無線 WAN に入力する PIN コードの設定.....	545
42.24 内蔵無線 WAN の PIN 認証を有効にする.....	546
42.25 内蔵無線 WAN の PIN 認証を無効にする.....	546
42.26 内蔵無線 WAN モジュールで使用する PIN コードの変更.....	546
42.27 内蔵無線 WAN モジュールの PIN ロック解除コードの入力.....	547
42.28 指定した相手に対して発信制限を解除する.....	547
42.29 定期実行で取得した電波の受信レベルの表示.....	548
42.30 外部メモリから内蔵無線 WAN モジュールのファームウェアを更新する.....	548
42.31 HTTP を利用した内蔵無線 WAN モジュールファームウェアのチェックおよび更新の実行.....	549
42.32 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新用 URL の設定.....	549
42.33 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新を許可するか否かの設定.....	550
42.34 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新のタイムアウトの設定.....	550
<b>第 43 章 : モバイルインターネット接続機能.....</b>	<b>551</b>
43.1 携帯端末を使用するか否かの設定.....	551
43.2 携帯端末に入力する PIN コードの設定.....	552
43.3 モバイルインターネット接続機能の発信方式の設定.....	552
43.4 携帯端末または内蔵無線 WAN モジュールに直接コマンドを発行する.....	553
43.5 指定した相手に対して発信制限を解除する.....	553
43.6 PP で使用するインターフェースの設定.....	554
43.7 携帯端末からの自動発信設定.....	554
43.8 携帯端末を切断するタイマの設定.....	554
43.9 携帯端末を入力がないときに切断するタイマの設定.....	555
43.10 携帯端末を出力がないときに切断するタイマの設定.....	555
43.11 発信先アクセスポイントの設定.....	555
43.12 携帯端末に指示する発信先の設定.....	556
43.13 パケット通信量制限の設定.....	556
43.14 パケット通信時間制限の設定.....	557
43.15 同じ発信先に対して連続して認証に失敗できる回数数の設定.....	558
43.16 LCP の Async Control Character Map オプション使用の設定.....	559
43.17 発信者番号通知 (186) を付加するかどうかの設定.....	559
43.18 詳細な SYSLOG を出力するか否かの設定.....	560
43.19 接続毎パケット通信量制限の設定.....	560
43.20 接続毎パケット通信時間制限の設定.....	561
43.21 通信制限の累積期間の設定.....	561

43.22 携帯端末でパケット着信機能を使用するか否かの設定.....	562
43.23 モバイルインターネット機能の着信許可の設定.....	562
43.24 電波の受信レベルの取得.....	563
43.25 電波の受信レベル取得機能の設定.....	563
43.26 定期実行で取得した電波の受信レベルの表示.....	564
43.27 USB ポートに接続した機器の初期化に使う AT コマンドの設定.....	564
43.28 USB ポートに接続した機器のフロー制御を行うか否かの設定.....	565
43.29 携帯端末のファームウェア更新.....	565
43.30 携帯端末のネットワーク事業者モードの設定.....	566
43.31 自分の名前とパスワードの設定.....	566
43.32 WAN で使用するインターフェースの設定.....	567
43.33 携帯端末からの自動発信設定.....	567
43.34 携帯端末を切断するタイマの設定.....	568
43.35 携帯端末を入力がないときに切断するタイマの設定.....	568
43.36 携帯端末を出力がないときに切断するタイマの設定.....	569
43.37 常時接続の設定.....	569
43.38 発信先アクセスポイントの設定.....	570
43.39 パケット通信量制限の設定.....	570
43.40 パケット通信時間制限の設定.....	571
43.41 接続毎パケット通信量制限の設定.....	572
43.42 接続毎パケット通信時間制限の設定.....	573
43.43 通信制限の累積期間の設定.....	574
<b>第 44 章 : ブリッジインターフェース (ブリッジ機能).....</b>	<b>575</b>
44.1 ブリッジインターフェースに收容する実インターフェースを設定する.....	575
44.2 自動的なラーニングを行うか否かの設定.....	576
44.3 ブリッジがラーニングした情報の消去タイマの設定.....	576
44.4 静的なラーニング情報の設定.....	577
<b>第 45 章 : Lua スクリプト機能.....</b>	<b>578</b>
45.1 Lua スクリプト機能を有効にするか否かの設定.....	578
45.2 Lua スクリプトの実行.....	578
45.3 Lua コンパイラの実行.....	579
45.4 Lua スクリプトの走行状態の表示.....	579
45.5 Lua スクリプトの強制終了.....	580
45.6 Lua スクリプト機能に関連するアラーム音を鳴らすか否かの設定.....	581
<b>第 46 章 : カスタム GUI.....</b>	<b>582</b>
46.1 カスタム GUI を使用するか否かの設定.....	582
46.2 カスタム GUI を使用するユーザーの設定.....	582
46.3 カスタム GUI の API を使用するか否かの設定.....	583
46.4 カスタム GUI の API にアクセスするためのパスワードの設定.....	583
<b>第 47 章 : 診断.....</b>	<b>584</b>
47.1 ポートの開閉状態の診断.....	584
47.2 ポートへ到達可能なアクセス範囲の診断.....	585
47.3 ポートの開閉状態の診断で検出可能な通過パケットの最大数の設定.....	585
47.4 ポートの開閉状態の診断結果の履歴数の設定.....	586
47.5 ポートの開閉状態の診断結果の表示.....	586
47.6 ポートへ到達可能なアクセス範囲の診断結果の表示.....	586
47.7 ポートの開閉状態の診断結果の消去.....	586
<b>第 48 章 : 統計.....</b>	<b>587</b>
48.1 統計機能を有効にするか否かの設定.....	587

<b>第 49 章 : DPI</b> .....	<b>588</b>
49.1 DPI を使用するか否かの設定.....	588
49.2 IPv4 の DPI フィルターの設定.....	589
49.3 IPv6 の DPI フィルタの設定.....	590
49.4 DPI のフィルターのインターフェースへの適用.....	591
49.5 DPI のアプリケーショングループの作成.....	592
49.6 シグネチャのダウンロードの手動実行.....	593
49.7 シグネチャのダウンロード先 URL の設定.....	594
49.8 アプリケーションの識別に関するログを出力するか否かの設定.....	594
49.9 DPI の統計情報の表示.....	595
49.10 DPI の統計情報のクリア.....	596
49.11 識別結果のキャッシュの表示.....	597
49.12 識別結果のキャッシュのクリア.....	597
49.13 アプリケーションを表すニーモニック一覧の表示.....	597
49.14 カテゴリーを表すニーモニック一覧の表示.....	598
49.15 DPI の動作状態、およびシグネチャの状態の表示.....	599
<b>第 50 章 : L2MS</b> .....	<b>601</b>
50.1 共通の設定.....	601
50.1.1 L2MS の動作モードの設定.....	601
50.1.2 L2MS を使用するか否かの設定.....	602
50.1.3 エージェントの監視時間間隔の設定.....	603
50.1.4 端末情報の監視時間間隔の設定.....	603
50.1.5 スナップショット機能を使用するか否かの設定.....	604
50.1.6 スナップショットファイルを作成する.....	605
50.1.7 LAN マップの SYSLOG 出力の設定.....	605
50.1.8 LAN マップで使用する機器名の設定.....	606
50.2 スイッチの制御.....	606
50.2.1 スイッチの選択.....	606
50.2.2 スイッチが持つ機能の設定.....	606
50.2.3 スイッチが持つ機能の設定内容や動作状態の取得.....	607
50.2.4 スイッチに対して特定の動作を実行.....	607
50.2.5 スイッチの設定の削除.....	608
50.2.6 スイッチのファームウェアの更新.....	608
50.2.7 LAN ケーブル二重化機能の設定.....	609
50.2.8 スイッチの設定ファイルを格納するディレクトリの指定.....	610
50.2.9 スイッチの設定を保存するファイル名の指定.....	610
50.2.10 スイッチの設定の取得.....	611
50.2.11 スイッチの設定の復元.....	611
50.2.12 スイッチのゼロコンフィグ機能を使用するか否かの設定.....	612
50.3 スイッチの機能.....	612
50.3.1 システム.....	613
50.3.2 ポート.....	617
50.3.3 MAC アドレステーブル.....	623
50.3.4 VLAN.....	625
50.3.5 QoS.....	630
50.3.6 ミラーリング.....	634
50.3.7 カウンタ.....	637
50.3.8 ループ検出.....	643
50.3.9 PoE 給電.....	647
50.4 アクセスポイントの制御.....	651
50.4.1 アクセスポイントの選択.....	651
50.4.2 アクセスポイントの設定ファイルを格納するディレクトリの指定.....	652
50.4.3 アクセスポイントの設定を保存するファイル名の指定.....	652
50.4.4 アクセスポイントの設定のバックアップ実行.....	652
50.4.5 アクセスポイントの設定の復元実行.....	653
50.4.6 アクセスポイントの設定の削除.....	653
50.4.7 アクセスポイント設定のゼロコンフィグ機能を使用するか否かの設定.....	654

50.4.8	アクセスポイントの HTTP リビジョンアップ機能の実行.....	654
50.4.9	アクセスポイント制御用の HTTP プロキシの使用.....	655
50.4.10	アクセスポイント制御用の HTTP プロキシのタイムアウト時間の設定.....	655
50.5	ルーターの制御.....	655
50.5.1	HTTP プロキシ経由での Web GUI へのアクセスを許可するか否かの設定.....	655
<b>第 51 章</b>	<b>: YNO エージェント.....</b>	<b>657</b>
51.1	YN0 エージェント機能を使用するか否かの設定.....	657
51.2	YN0 マネージャー接続用のアクセスコードの設定.....	657
51.3	YN0 エージェント機能に関する追加の SYSLOG を出力するか否かの設定.....	658
51.4	YN0 マネージャーに表示される自身の機器説明の設定.....	658
51.5	YN0 で使用する HTTPS プロキシサーバーの設定.....	659
51.6	GUI Forwarder 接続のタイムアウト時間の設定.....	659
51.7	YN0 のゼロコンフィグの設定.....	659
51.8	YN0 エージェント機能の動作状態の表示.....	660
51.9	LAS (Log Analysis Service).....	662
51.9.1	SYSLOG 送信キューの長さの設定.....	662
51.9.2	LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間の設定.....	662
51.9.3	LAS クライアントがリクエストの送信を再試行する回数の設定.....	662
51.9.4	LAS サーバーとのコネクションに対するキープアライブの設定.....	663
51.9.5	LAS の動作状態の表示.....	663
51.10	XMPP サーバーとのキープアライブの時間間隔の設定.....	664
<b>第 52 章</b>	<b>: ダッシュボード.....</b>	<b>665</b>
52.1	ダッシュボードのデータを蓄積するか否かの設定.....	665
<b>第 53 章</b>	<b>: 操作.....</b>	<b>666</b>
53.1	相手先情報番号の選択.....	666
53.2	トンネルインターフェース番号の選択.....	666
53.3	設定に関する操作.....	667
53.3.1	管理ユーザーへの移行.....	667
53.3.2	終了.....	667
53.3.3	設定内容の保存.....	667
53.3.4	設定ファイルの複製.....	668
53.3.5	ファームウェアファイルを内蔵フラッシュ ROM にコピー.....	669
53.3.6	設定ファイルの削除.....	670
53.3.7	実行形式ファームウェアファイルの削除.....	671
53.3.8	デフォルト設定ファイルの設定.....	671
53.3.9	デフォルトファームウェアファイルの設定.....	671
53.3.10	シリアルポートのボーレートの設定.....	671
53.3.11	設定の初期化.....	672
53.3.12	遠隔地のルーターからの設定に対する制限.....	672
53.4	動的情報のクリア操作.....	672
53.4.1	アカウントのクリア.....	672
53.4.2	TEL ポートに関するアカウントのクリア.....	673
53.4.3	ARP テーブルのクリア.....	674
53.4.4	IP の動的経路情報のクリア.....	674
53.4.5	ブリッジのラーニング情報のクリア.....	674
53.4.6	ログのクリア.....	674
53.4.7	DNS キャッシュのクリア.....	674
53.4.8	インターフェースのカウンタ情報のクリア.....	675
53.4.9	NAT アドレステーブルのクリア.....	675
53.4.10	インターフェースの NAT アドレステーブルのクリア.....	676
53.4.11	IP マスカレードで管理しているセッションの統計情報のクリア.....	676
53.4.12	PPPoE パススルー機能がラーニングした情報のクリア.....	676
53.4.13	IPv6 の動的経路情報の消去.....	677
53.4.14	近隣キャッシュの消去.....	677

53.4.15 起動情報の履歴を削除する.....	677
53.4.16 外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除.....	677
53.5 ファイル、ディレクトリの操作.....	678
53.5.1 ディレクトリの作成.....	678
53.5.2 ファイルまたはディレクトリの削除.....	678
53.5.3 ファイルまたはディレクトリの複製.....	678
53.5.4 ファイル名またはディレクトリ名の変更.....	679
53.6 その他の操作.....	679
53.6.1 相手先の使用許可の設定.....	679
53.6.2 相手先の使用不許可の設定.....	680
53.6.3 再起動.....	680
53.6.4 インターフェースの再起動.....	681
53.6.5 内蔵無線 WAN モジュールの再起動.....	681
53.6.6 発信.....	682
53.6.7 切断.....	682
53.6.8 ping.....	683
53.6.9 ping6 の実行.....	683
53.6.10 traceroute.....	684
53.6.11 traceroute6 の実行.....	685
53.6.12 nslookup.....	685
53.6.13 SIP サーバーに対し手動で接続.....	685
53.6.14 SIP サーバーに対し手動で切断.....	686
53.6.15 IPv4 動的フィルターの接続管理情報の削除.....	686
53.6.16 IPv6 動的フィルターの接続管理情報の削除.....	686
53.6.17 TELNET クライアント.....	687
53.6.18 スイッチングハブ MAC アドレステーブルの消去.....	688
53.6.19 Magic Packet の送信.....	688
53.6.20 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行.....	689
53.6.21 URL フィルターの統計情報のクリア.....	689
53.6.22 メール通知の実行.....	690
53.6.23 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ).....	690
53.6.24 ライセンス認証の実行.....	691
53.6.25 ライセンス認証のリトライの間隔と回数設定.....	691
53.6.26 設定の一括更新.....	691
53.6.27 ロールバックタイマーの起動.....	693
53.6.28 設定の確認.....	693
53.6.29 ファイルをマクロとして実行する.....	693
53.6.30 echo.....	694

## 第 54 章 : 設定の表示.....695

54.1 機器設定の表示.....	695
54.2 すべての設定内容の表示.....	695
54.3 指定した AP の設定内容の表示.....	695
54.4 指定した PP の設定内容の表示.....	696
54.5 指定したスイッチの設定内容の表示.....	696
54.6 指定したトンネルの設定内容の表示.....	696
54.7 指定した WWAN の設定内容の表示.....	697
54.8 設定の差分の表示.....	697
54.9 設定ファイルの一覧.....	698
54.10 アナログ親機に登録された各 TEL ポート設定内容の表示.....	698
54.11 ファイル情報の一覧の表示.....	698
54.12 インターフェースに付与されている IPv6 アドレスの表示.....	699
54.13 SSH サーバー公開鍵の表示.....	700
54.14 指定したインターフェースのフィルター内容の表示.....	700
54.15 指定したインターフェースの IPv6 フィルター内容の表示.....	700
54.16 ファームウェアファイルの一覧.....	701
54.17 環境変数の表示.....	701
54.18 エイリアスの表示.....	701
54.19 マクロの表示.....	702

<b>第 55 章 : 状態の表示</b> .....	<b>703</b>
55.1 ARP テーブルの表示.....	703
55.2 インターフェースの状態の表示.....	703
55.3 各相手先の状態の表示.....	703
55.4 IP の経路情報テーブルの表示.....	704
55.5 RIP で得られた経路情報の表示.....	705
55.6 IPv6 の経路情報の表示.....	705
55.7 IPv6 の RIP テーブルの表示.....	705
55.8 近隣キャッシュの表示.....	705
55.9 ブリッジのラーニング情報の表示.....	706
55.10 IPsec の SA の表示.....	706
55.11 証明書の情報の表示.....	707
55.12 CRL ファイルの情報の表示.....	707
55.13 VRRP の情報の表示.....	707
55.14 動的 NAT ディスクリプターのアドレスマップの表示.....	708
55.15 動作中の NAT ディスクリプターの適用リストの表示.....	708
55.16 LAN インターフェースの NAT ディスクリプターのアドレスマップの表示.....	708
55.17 IP マスカレードで使用しているポート番号の個数の表示.....	709
55.18 IP マスカレードで使用しているセッション数の表示.....	709
55.19 IP マスカレードで管理しているセッションの統計情報の表示.....	710
55.20 L2TP の状態の表示.....	710
55.21 PPTP の状態の表示.....	710
55.22 IPIP トンネリングの状態の表示.....	711
55.23 OSPF 情報の表示.....	711
55.24 BGP の状態の表示.....	711
55.25 DHCP サーバーの状態の表示.....	712
55.26 DHCP クライアントの状態の表示.....	712
55.27 DHCPv6 の状態の表示.....	713
55.28 バックアップ状態の表示.....	713
55.29 動的フィルターによって管理されている接続の表示.....	713
55.30 IPv6 の動的フィルターによって管理されている接続の表示.....	714
55.31 ネットワーク監視機能の状態の表示.....	715
55.32 侵入情報の履歴の表示.....	715
55.33 相手先ごとの接続時間情報の表示.....	715
55.34 PPPoE パススルー機能がラーニングした情報の表示.....	716
55.35 ネットボランチ DNS サービスに関する設定の表示.....	716
55.36 スイッチングハブ MAC アドレステーブルの表示.....	717
55.37 UPnP に関するステータス情報の表示.....	717
55.38 トンネルインターフェースの状態の表示.....	717
55.39 VLAN インターフェースの状態の表示.....	718
55.40 トリガによるメール通知機能の状態の表示.....	718
55.41 MLD のグループ管理情報の表示.....	719
55.42 IPv6 マルチキャストの経路情報の表示.....	719
55.43 ログインしているユーザー情報の表示.....	719
55.44 ログインしたユーザーのログイン履歴の表示.....	720
55.45 パケットバッファの状態の表示.....	720
55.46 QoS ステータスの表示.....	721
55.47 連携動作の状態の表示.....	721
55.48 OSPFv3 情報の表示.....	722
55.49 URL フィルターの情報の表示.....	722
55.50 生存通知の状態の表示.....	723
55.51 生存通知の状態の表示.....	723
55.52 リモートセットアップ機能に関する接続情報の表示.....	724
55.53 技術情報の表示.....	724
55.54 USB ホスト機能の動作状態を表示.....	724
55.55 microSD スロットの動作状態を表示.....	725
55.56 内蔵無線 WAN モジュールの動作状態を表示.....	725
55.57 外部メモリの動作状態を表示.....	726
55.58 RTFS の状態の表示.....	726

55.59 ルーターへのサインイン状態の表示.....	726
55.60 SIP サーバーとの接続状態の表示.....	726
55.61 アナログ関係の状態の表示.....	727
55.62 カスケード接続の状態表示.....	727
55.63 起動情報を表示する.....	728
55.64 起動情報の履歴の詳細を表示する.....	728
55.65 起動情報の履歴の一覧を表示する.....	728
55.66 エージェント一覧の表示.....	728
55.67 LAN ケーブル二重化機能の動作状態を表示.....	730
55.68 DNS キャッシュの表示.....	730
55.69 ライセンス情報の表示.....	730
55.70 ライセンス認証の状態の表示.....	731
55.71 STATUS LED の情報の表示.....	731
55.72 LAN マップの状態を表示する.....	732
55.73 コピーライトの表示.....	734
55.74 音声通話の接続状態の表示.....	734
55.75 小型 ONU の状態の表示.....	734

## 第 56 章 : ロギング.....736

56.1 ログの表示.....	736
56.2 アカウントの表示.....	736
56.3 PP アカウントの表示.....	737
56.4 アナログ関係のアカウントの表示.....	737
56.5 SIP のアカウントの表示.....	737
56.6 ひかり電話のアカウントの表示.....	738
56.7 データコネクタのアカウントの表示.....	738
56.8 モバイル回線のアカウントの表示.....	738
56.9 内蔵無線 WAN のアカウントの表示.....	738
56.10 通信履歴の表示.....	739
56.11 コマンド履歴の表示.....	739

## 索引.....740



---

# 序文

---

## はじめに

---

- 本書の記載内容の一部または全部を無断で転載することを禁じます。
- 本書の記載内容は将来予告なく変更されることがあります。
- 本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。保証は本製品物損の範囲に限ります。予めご了承ください。
- 本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいようお願い致します。
- 本書に記載されている会社名、製品名は各社の登録商標あるいは商標です。

# 第 1 章

## コマンドリファレンスの見方

### 1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、以下のリビジョンに対応しています。

モデル	リビジョン
NVR700W	Rev.15.00.24
NVR510	Rev.15.01.25

このコマンドリファレンスの印刷より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。

<http://www.rtpro.yamaha.co.jp>

### 1.2 コマンドリファレンスの見方

このコマンドリファレンスは、ルーターのコンソールから入力するコマンドを説明しています。

1 つ 1 つのコマンドは次の項目の組合せで説明します。

[書式]	コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。
	コマンドの名称部分は太字 ( <b>Bold face</b> ) で示します。
	パラメーター部分は斜体 ( <i>Italic face</i> ) で示します。
	キーワードは標準文字で示します。
	括弧 ([ ]) で囲まれたパラメーターは省略可能であることを示します。
[設定値]	コマンドの設定値の種類とその意味を説明します。
[説明]	コマンドの解説部分です。
[ノート]	コマンドを使用する場合に特に注意すべき事柄を示します。
[設定例]	コマンドの具体例を示します。

### 1.3 インターフェース名について

コマンドの入力形式において、ルーターの各インターフェースを指定するためにインターフェース名を利用します。インターフェース名は、インターフェース種別とインターフェース番号を間にスペースを入れずに続けて表記します。インターフェース種別には、"lan"、"wan"、"onu" があります。

lan インターフェースについては、LAN 分割機能を適用した場合に分割された LAN はピリオド (.) でつなげた形式となります。

NVR700W では LAN 分割機能の拡張機能として VLAN インターフェースが使用できます。

タグ VLAN はスラッシュ (/) でつなげた形式となります。

例

インターフェースの種類	インターフェース名
LAN、WAN	lan1, lan2
タグ VLAN	lan1/1, lan1/2, ...
LAN 分割機能の LAN	lan1.1, lan1.2, ...
LAN 分割機能の拡張機能の LAN	vlan1,vlan2, ...

インターフェースの種類	インターフェース名
イーサネット方式 (NDIS) による USB 接続型データ端末、内蔵無線 WAN	wan1
ONU	onu1

また、仮想的なインターフェースである loopback インターフェースと null インターフェースを指定できます。

インターフェースの種類	インターフェース名
LOOPBACK	loopback1, loopback2, ...loopback9
NULL	null

NVR700W では、仮想的なインターフェースであるブリッジインターフェースを指定できます。

インターフェースの種類	インターフェース名
BRIDGE	bridge1

## 1.4 no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のものがあり、並記されているコマンドが多数あります。no で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、初期値に戻します。

また、**show config** コマンドでの表示からも外します。言い換えれば、no で始まる形式を使わない限り、入力されたコマンドは、たとえ初期値をそのまま設定する場合でも、**show config** コマンドでの表示の対象となります。

コマンドの入力形式で、no で始まるものに対して、省略可能なパラメーターが記載されていることがあります。これらは、パラメーターを指定してもエラーにならないという意味で、パラメーターとして与えられた値は no コマンドの動作になんら影響を与えません。

## 1.5 コマンドの入力文字数とエスケープシーケンスについて

1つのコマンドとして入力できる文字数は、コマンド本体とパラメーター部分とスペースを含めて最大半角 4095 文字以内、キーワードの合計が 1024 個以内です。

また、コマンドのパラメーター部分に以下の特殊文字を入力する場合には表に示す方法で入力してください。

特殊文字	入力
?	\?, '?', "?"
#	\#, '#', "#"
	\ , ' ', " "
>	\>, '>', ">"
\	\\
'	\', ""
"	\", ""
空白	\の後ろに空白、' ', ""

## 1.6 工場出荷設定値について

お買い上げ頂いた状態および **cold start** コマンドを実行した直後の状態は、本書に記載されたコマンドの初期値が適用されるわけではなく、以下に示す工場出荷設定になっています。

```
ip lan1 address 192.168.100.1/24
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 192.168.100.2-192.168.100.191/24
dns private name setup.netvolante.jp
analog supplementary-service pseudo call-waiting
analog extension dial prefix sip prefix="9#"
```

NVR700W は Rev.15.00.11 以降、NVR510 は Rev.15.01.10 以降で **telnetd host lan** コマンドも設定されています。

## 第 2 章

### コマンドの使い方

NVR700W, NVR510 に直接コマンドを 1 つ 1 つ送って機能を設定したり操作したりする方法と、必要なコマンド一식을記述したファイルを送信して設定する方法の 2 種類をサポートしています。LAN インターフェースが使用できない場合は、CONSOLE ポートを使ってコマンドを実行し、復旧などの必要な操作を行うことができます。

対話的に設定する手段をコンソールと呼び、コマンドを 1 つ 1 つ実行して設定や操作を行うことができます。必要なコマンド一식을記述したファイルを設定ファイル (Config) と呼び、TFTP により NVR700W, NVR510 にアクセスできる環境から設定ファイルを送信したり受信したりすることが可能です。

#### 2.1 コンソールについて

各種の設定を行うためには、NVR700W, NVR510 の CONSOLE ポートにシリアル端末を接続する方法と、LAN 上のホストから TELNET、または SSH でログインする方法の 2 つがあります。

NVR700W, NVR510 へのアクセス方法
CONSOLE ポートに接続した端末からアクセス
LAN 上のホストから TELNET または SSH でログイン

NVR700W, NVR510 へは、それぞれに対して 1 ユーザーがアクセスすることができます。またその中で管理ユーザーになれるのは同時に 1 ユーザーだけです。例えば、シリアル端末でアクセスしているユーザーが管理ユーザーとして設定を行っている場合には、別のユーザーが一般ユーザーとしてアクセスすることはできません。

TELNET または SSH による同時アクセスが最大 8 ユーザーまで可能です。また複数のユーザーが同時に管理ユーザーになることができ、異なるホストから同時に設定を行うこともできます。そのほか、各ユーザーは現在アクセスしている全ユーザーのアクセス状況を確認することができ、管理ユーザーならば他のユーザーの接続を強制的に切断させることもできます。

##### 2.1.1 コンソールによる設定手順

CONSOLE ポートから設定を行う場合は、まず NVR700W, NVR510 の CONSOLE ポートとパソコンをクロスタイプのシリアルケーブルで接続します。シリアルケーブルの両端のコネクタはパソコンに適合したタイプをご使用ください。

パソコンではターミナルソフトを使います。Windows をお使いの場合には、ターミナル機能のあるソフトウェアを用意してください。macOS をお使いの場合は、OS に付属の『ターミナル』アプリケーションを使用します。

TELNET で設定を行う場合は、パソコンでは TELNET アプリケーションを使います。Windows をお使いの場合は OS に付属の『TELNET』ソフトウェアを使用します。macOS をお使いの場合は、OS に付属の『ターミナル』アプリケーションで `telnet` コマンドを実行します。

コンソールコマンドの具体的な内容については、本書の第 3 章以降をご覧ください。

コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。設定後に意図した動作をするかどうか、必ずご確認ください。

コンソールに表示される文字セットは初期値ではシフト JIS です。これは、`console character` コマンドを使用して端末の文字表示の能力に応じて選択できます。いずれの場合でもコマンドの入力文字は ASCII で共通であることに注意してください。

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザーとしてログインした後、`administrator` コマンドで管理ユーザーとしてアクセスします。この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。
2. 回線を接続していない相手の相手先情報を変更する場合には、`pp disable` コマンドを実行してから相手先情報の内容を変更してください。回線が接続されている場合には、`disconnect` コマンドでまず回線を手動切断しておきます。
3. 各種コマンドを使用して、相手先情報の内容を変更します。
4. `pp enable` コマンドを実行します。
5. `save` コマンドを実行して、不揮発性メモリに設定内容を保存します。



**注:** Ctrl キーを押しながら S キーを押すと、コンソール出力を一時停止します。この状態でキーを押しても画面上は無反応に見えますが、キー入力は処理されます。コンソール出力を再開するには Ctrl キーを押しながら Q キーを押します。

セキュリティの観点から、コンソールにキー入力がない時には、自動的に 300 秒 (初期値) でログアウトするように設定されています。この時間は **login timer** コマンドを使用して変更することができます。

新たに管理ユーザーになって設定コマンドを実行すると、その内容はすぐに動作に反映されますが、**save** コマンドを実行しないと不揮発性メモリに書き込まれません。



**注意:** ご購入直後の起動や **cold start** 後にはログインパスワードも管理パスワードも設定されていません。セキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。

- NVR700W, NVR510 のご購入直後の起動でコンソールから各種の設定が行える状態になりますが、実際にパケットを配送する動作は行いません。
- セキュリティの設定や、詳細な各種パラメーターなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。

## 2.1.2 CONSOLE ポートからの設定

ターミナルソフトウェアの使用方法については、各ソフトウェアの取扱説明書をご覧ください。シリアルケーブルの接続は事前にすませておきます。

1. 「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。

※設定しユーザー名でログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザー名の入力待ち状態となります。ここで、設定したユーザー名を入力して Enter キーを押し、続いてユーザーパスワードを入力します。

何も表示されないときは、1 度 Enter キーを押します。

「>」が表示されると、コンソールコマンドを入力できるようになります。



**注:**

- **help** と入力してから Enter キーを押すと、キー操作の説明が表示されます。
- **show command** と入力してから Enter キーを押すと、コマンド一覧が表示されます。

2. **administrator** と入力してから、Enter キーを押します。

3. 「Password:」と表示されたら、管理パスワードを入力します。

「#」が表示されると、各種のコンソールコマンドを入力できます。

4. コンソールコマンドを入力して、設定を行います

5. 設定が終わったら、**save** と入力してから Enter キーを押します。

コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。

6. 設定を終了するには、**quit** と入力してから Enter キーを押します。

7. コンソール画面を終了するには、もう 1 度 **quit** と入力してから Enter キーを押します。

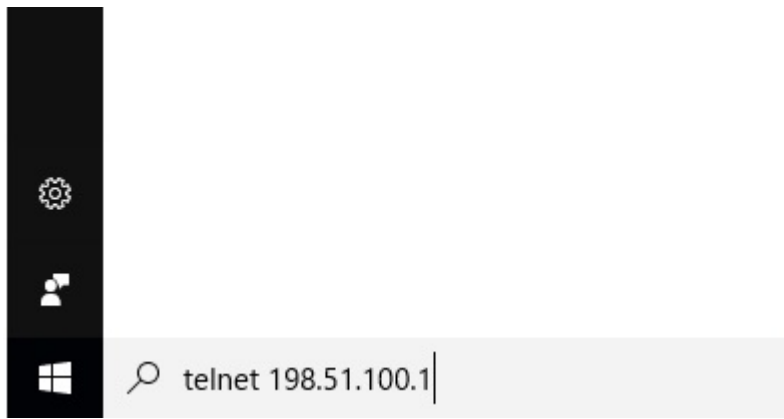
## 2.1.3 TELNET による設定

ここでは、Windows の TELNET を使用する場合を例に説明します。NVR700W, NVR510 の IP アドレスは 198.51.100.1 とした場合の例です。

Windows では、あらかじめ次の方法で TELNET を有効にする必要があります。「コントロールパネル」-「プログラム」-「プログラムと機能」で、「Windows の機能の有効化または無効化」を選ぶと表示される「Windows の機能」画面で、「Telnet クライアント」にチェックを付けてから「OK」をクリックします。

1. [スタート]メニューから「telnet 198.51.100.1」と入力します。

実際には「198.51.100.1」のかわりに本機に設定されている IP アドレスを入力します。



2. 「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。

※設定した名前ありユーザーでログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザー名の入力待ち状態となります。ここで、設定したユーザー名を入力して Enter キーを押し、続いてユーザーパスワードを入力します。

何も表示されないときは、1 度 Enter キーを押します。「>」が表示されると、コンソールコマンドを入力できるようになります。

 A screenshot of a Telnet session window titled 'Telnet 198.51.100.1'. The terminal output is as follows:
 

```

Password:

NVR700W Rev. 15.00.22 (Thu Apr 15 20:41:58 2021)
Copyright (c) 1994-2021 Yamaha Corporation. All Rights Reserved.
To display the software copyright statement, use 'show copyright' command.
00:a0:de:e6:21:d4, 00:a0:de:e6:21:d5
Memory 256Mbytes, 2LAN, 1ONU, 1WWAN

The login password is factory default setting. Please request an administrator to change the password by the 'login password' command.
> administrator
Password:
The administrator password is factory default setting. Please change the password by the 'administrator password' command.
#
# quit
>
  
```

#### 👉 注:

- **help** と入力してから Enter キーを押すと、キー操作の説明が表示されます。
- **show command** と入力してから Enter キーを押すと、コマンド一覧が表示されます。

3. **administrator** と入力してから、Enter キーを押します。
4. 「Password:」と表示されたら、管理パスワードを入力します。  
「#」が表示されると、各種のコンソールコマンドを入力できます。
5. コンソールコマンドを入力して、設定を行います
6. 設定が終わったら、**save** と入力してから Enter キーを押します。  
コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。
7. 設定を終了するには、**quit** と入力してから Enter キーを押します。
8. コンソール画面を終了するには、もう 1 度 **quit** と入力してから Enter キーを押します。

## 2.2 SSH サーバーについて

NVR700W, NVR510 では、LAN 上のホストから SSH でログインして設定することができます。このときホスト側で使用する SSH クライアントは、macOS の『ターミナル』アプリケーションや UNIX 環境では標準的に搭載されており、実行することができますが、Windows 系 OS では標準では搭載されていません。SSH クライアントが搭載されていない環境では、フリーソフトなどで SSH クライアント機能のあるものを用意してください。

## 2.2.1 SSH サーバー機能の使用に当たっての注意事項

SSH サーバー機能では以下の機能をサポートしていないことに注意してください。

- SSH プロトコルバージョン 1
- パスワード認証以外のユーザー認証 ( ホストベース認証、公開鍵認証(※)、チャレンジ・レスポンス認証、GSSAPI 認証 )

※以下の機種およびファームウェアでは公開鍵認証をサポートしています。

- NVR700W Rev.15.00.17 以降
- NVR510 Rev.15.01.16 以降
- ポートフォワーディング ( X11/TCP 転送 )
- Gateway Ports ( ポート中継 )
- 空パスワードの許可

## 2.2.2 SSH サーバーの設定

SSH サーバー機能は、工場出荷設定では使用しないよう設定されています。SSH サーバー機能を使用できるようにするまでの設定手順は以下の通りです。

1. **login user** コマンドで名前ありユーザーを登録します。SSH ではログイン時のユーザー名の入力が必要となるため、事前に必ず名前ありユーザーを登録しなければなりません。
2. 次に、**sshd host key generate** コマンドで SSH サーバーのホスト鍵を生成します。このコマンドによって DSA または RSA の公開鍵、および秘密鍵のペアが生成されます。ただし機種によってはこのコマンドの処理に数十秒ほど時間がかかる場合があります。
3. 最後に **sshd service** コマンドで SSH サーバー機能を有効にします。

```

Telnet 198.51.100.1
> administrator
Password:
The administrator password is factory default setting. Please change the password by the 'administrator password' command.
# login user RTuser himitsu
Password Strength : Weak
# sshd host key generate
Update to new host key ? (Y/N)Y
Generating public/private dsa key pair ...
*****
Generating public/private rsa key pair ...
*****
# sshd service on
# save
Saving ... CONFIGO Done .
# quit
>

```

## 2.3 TFTP について

NVR700W, NVR510 に設定した項目は、TFTP により LAN 上のホストから設定ファイルとして読み出すことができます。またホスト上の設定ファイルを本機に読み込ませて設定を行うこともできます。

TFTP は、Windows や macOS の『ターミナル』アプリケーション、UNIX 環境で標準的に搭載されており、実行することができます。TFTP が搭載されていない環境では、フリーソフトなどで TFTP クライアント機能のあるものを用意してください。この時、NVR700W, NVR510 は TFTP サーバーとして動作します。

設定ファイルは全体の設定を記述したものであり、特定部分の設定だけを読み出したり差分点だけを書き込んだりすることはできません。設定ファイルは Windows のメモ帳等で直接編集できるテキストファイル ( シフト JIS、CRLF 改行 ) です。

TFTP では、平文の設定ファイルと暗号化された設定ファイルを扱うことができます。対応している暗号化形式は、AES128 及び、AES256 です。パスワードを指定して暗号化されたファイルは利用できません。RT-Tftp Client では暗号化に対応していません。

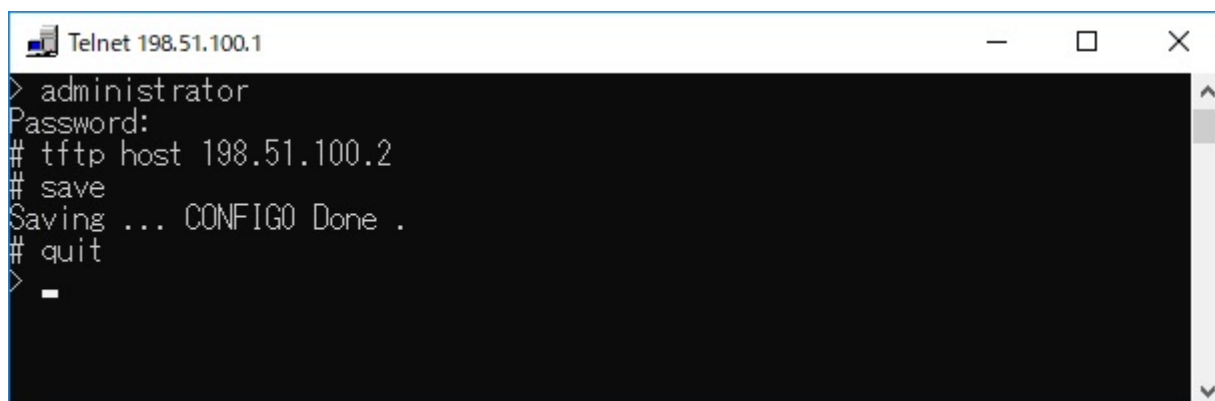


注意：

- 設定ファイルの内容はコマンドの書式やパラメーターの指定などの内容が正しく記述されている必要があります。間違った書式や内容があった場合には、その内容は動作に反映されず無視されます。

### 2.3.1 TFTP による設定手順

TFTP により設定ファイルをやりとりするためには、NVR700W, NVR510 側にあらかじめアクセス許可するための設定が必要です。まず **tftp host** コマンドを使用し、本機にアクセスできるホストを設定します。工場出荷設定ではどのホストからもアクセスできない設定になっていることに注意してください。



```

Telnet 198.51.100.1
> administrator
Password:
# tftp host 198.51.100.2
# save
Saving ... CONFIGO Done .
# quit
>

```

次に、LAN 上のホストから TFTP コマンドを実行します。使用するコマンドの形式は、そのホストの OS に依存します。次の点に注意して実行してください。

- 本機の IP アドレス
- 転送モードは“アスキー”、“ascii”または“文字”にします。  
暗号化された設定ファイルを扱う場合は“バイナリ”、“binary”にします。
- 本機に管理パスワードが設定されている場合には、ファイル名称の後ろに管理パスワードを指定する必要があります。
- 起動中の設定ファイルを読み出したり書き込んだりする場合は、設定ファイル名は、“config”と指定します。

### 2.3.2 設定ファイルの読み出し

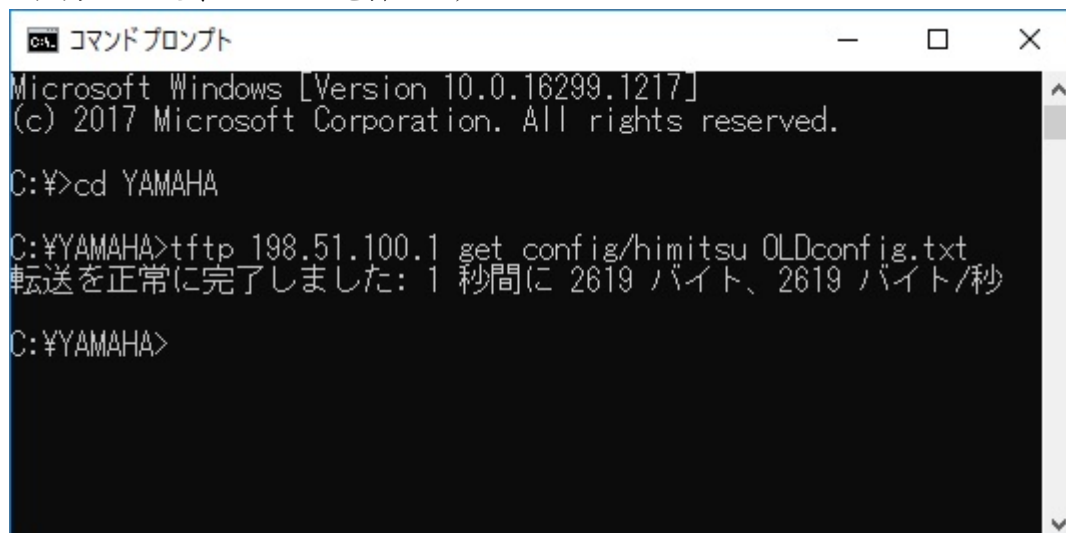
ここでは、Windows から設定ファイルを読み出す場合の例を示します。NVR700W, NVR510 のコンソール操作ではないことに注意してください。この例では、NVR700W, NVR510 の IP アドレスを 198.51.100.1、管理パスワードは“himitsu”、Windows に新しくできるファイルの名称を“OLDconfig.txt”とします。

- [スタート]メニューから[Windows システム ツール]-[コマンドプロンプト]を選びます。
- 設定ファイルを保存するディレクトリに移動します。
- tftp 198.51.100.1 get config/himitsu OLDconfig.txt** と入力してから、Enter キーを押します。

設定ファイルを暗号化して読み出す場合は、ファイル名の後に“-encryption”オプションを指定します。暗号化形式を指定する場合は、“-encryption”の後に“-aes128”または“-aes256”をオプションを指定します。暗号化形式を省略した場合は、AES256 が暗号化形式として使用されます。暗号化形式を AES128 として設定ファイルを暗号化して読み出す場合は、

**tftp -i 198.51.100.1 get config-encryption-aes128/himitsu OLDconfig.txt**

と入力してから、Enter キーを押します



```

コマンドプロンプト
Microsoft Windows [Version 10.0.16299.1217]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥>cd YAMAHA

C:¥YAMAHA>tftp 198.51.100.1 get config/himitsu OLDconfig.txt
転送を正常に完了しました: 1 秒間に 2619 バイト、2619 バイト/秒

C:¥YAMAHA>

```



### 2.3.3 設定ファイルの書き込み

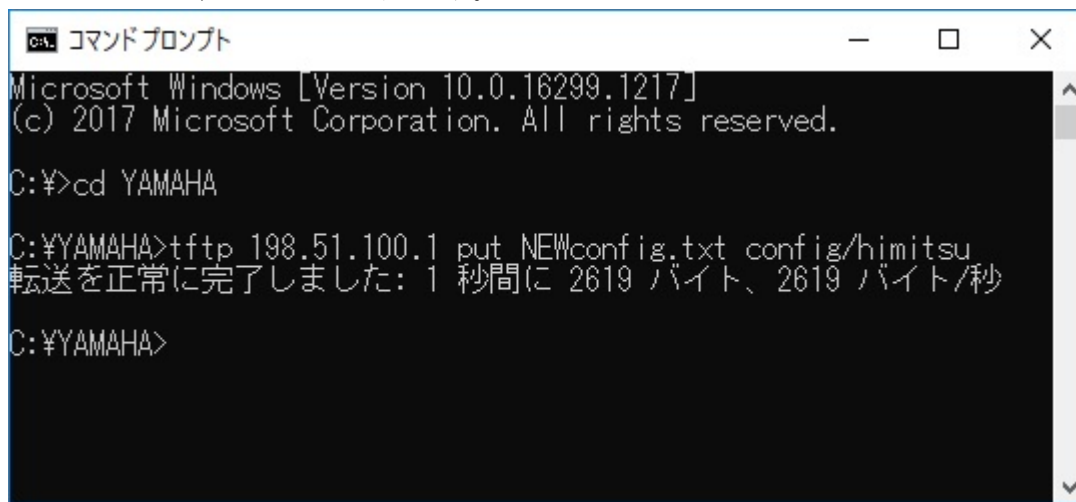
ここでは、Windows から設定ファイルを書き込む場合の例を示します。NVR700W, NVR510 のコンソール操作ではないことに注意してください。この例では、NVR700W, NVR510 の IP アドレスを 198.51.100.1、管理パスワードは“himitsu”、書き込むべき Windows 上のファイルの名称を“NEWconfig.txt”とします。

1. [スタート]メニューから[Windows システム ツール]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tfpt 198.51.100.1 put NEWconfig.txt config/himitsu** と入力してから、Enter キーを押します。

暗号化された設定されたファイル"NEWconfig.rtf"を設定ファイルに書き込む場合は、通常の設定ファイルの書き込みと同様に、

**tfpt -i 198.51.100.1 put NEWconfig.rtf config/himitsu**

と入力してから、Enter キーを押します。



### 2.4 コンソール使用時のキーボード操作について

一画面に収まらない行数の情報を表示する場合は、**console lines** コマンドで設定された行数分を表示した段階で表示をストップさせ、画面下に「--- つづく ---」と表示されます。

この状態から残りを表示させる場合には、スペースキーを押します。Enter キーを押すと新しい一行を表示します。これらの操作を繰り返し、最後まで表示すると自動的にコマンド入力ができる状態にもどります。

最後まで表示せずにこの段階で表示を終了させたい場合には、q キーを押します。この後コマンドが入力できる状態にもどります。

一画面に収まらない行数の情報を表示する場合にもストップさせたくなければ、**console lines infinity** コマンドを実行します。

キーボード操作	説明・備考
SPACE	1 画面先に進める
ENTER	1 行先に進める
RETURN	
q	終了
Ctrl-C	

**show config**、**show config list**、**show config pp**、**show config tunnel**、**show config switch**、**show config ap**、**show file list**、**show log** と同じ内容を、UNIX コマンドの less 風に表示する場合には、それぞれ、**less config**、**less config list**、**less config pp**、**less config tunnel**、**less config switch**、**less config ap**、**less file list**、**less log** コマンドを使用します。

キーボード操作	説明・備考
{n} f	{n}画面先に進める
{n} Ctrl-F	
{n} SPACE	

キーボード操作	説明・備考
{n} b	{n}画面後ろに戻る
{n} Ctrl-B	
{n} j	{n}行先に進める
{n} Ctrl-J	
{n} Ctrl-E	
{n} Ctrl-M	
{n} ENTER	
{n} RETURN	{n}行後ろに戻る
{n} k	
{n} Ctrl-K	
{n} y	
{n} Ctrl-Y	
{n} Ctrl-P	{n}半画面先に進める
{n} d	
{n} Ctrl-D	{n}半画面後ろに戻る
{n} u	
{n} Ctrl-U	{n}行目へ移動 {n}省略時は先頭行
{n} g	
{n} G	{n}行目へ移動 {n}省略時は末尾行
{n} r	現在の画面の書き直し
{n} Ctrl-R	
{n} Ctrl-L	
q	終了
Ctrl-C	

説明:

- n: 数字のキー入力で整数値を表します。省略時は '1' です。
- Ctrl-X:[Ctrl]キーを押しながら[X]キーを押すことを示します。

## 2.5 「show」で始まるコマンド

「show」で始まるコマンドが表示する内容から、指定した検索パターンに一致する内容だけを抜き出して表示することができます。あるいは「show」で始まるコマンドが表示する内容をページ単位で表示しながら、後ろに戻ったり、指定した検索パターンに一致する内容を検索したりすることができます。これらの機能は「show」で始まるすべてのコマンドで利用できます。

### 2.5.1 show コマンドの表示内容から検索パターンに一致する内容だけを抜き出す

[書式]

```
show [...] | grep [-i] [-v] [-w] pattern
```

[設定値及び初期値]

- -i: pattern 中の英大文字 / 小文字を区別せず検索する
- [初期値]: -

- `-v`: *pattern* に一致しなかった行を表示する
  - [初期値]: -
- `-w`: *pattern* が単語に一致する時だけ表示する
  - [初期値]: -
- *pattern*
  - [設定値]: 検索パターン
  - [初期値]: -

**[説明]**

**show** コマンドの表示内容から検索パターンである *pattern* に一致する行だけを抜き出して表示する。  
`-i` オプションを指定した時には、*pattern* 中の英大文字/小文字を区別せずに検索する。例えば `-i` オプションがある時には `'abc'` という *pattern* は `'abc'` や `'ABC'`、`'aBc'`、`'ABc'` などと一致する。一方、`-i` オプションがなければ、`'abc'` は `'abc'` としか一致しない。

`-v` オプションを指定した時には、*pattern* に一致しない行を表示する。  
`-w` オプションを指定した時には、*pattern* に一致するのは単語だけとなる。例えば、`-w` オプションがある時には `'IP'` という *pattern* は `'IPv4'` や `'IPv6'` とは一致しないが、`'IP '` (前後に空白がある) や `'[IP]'` には一致する。一方、`-w` オプションが無ければ先に上げた例にはすべて一致する。

*pattern* は限定された正規表現である。一般的な正規表現では多くの特殊文字を使って多様な検索パターンを構成できるが、ここで実装されているのは以下の特殊文字のみである。

文字	意味	使用例	一致する文字列の例
.	任意の 1 文字に一致する	a.b	aab、aXb、a-b
?	直前の文字が 0 回または 1 回出現するパターンに一致する	b?c	ac、abc
*	直前の文字が 0 回以上繰り返し返すパターンに一致する	ab*c	ac、abc、abbc、abbbbbbbbc
+	直前の文字が 1 回以上繰り返し返すパターンに一致する	ab+c	abc、abbc、abbbbbbbbc
	前後の文字のいずれかに一致する	ab cd	abd、acd
[ ]	[ ] 内の文字のいずれかに一致する	a[bc]d	abd、acd
[^ ]	[ ] 内の文字以外のものに一致する	a[^bc]d	aad、axd
^	行の先頭に一致する	^abc	abc で始まる行
\$	行の末尾に一致する	abc\$	abc で終わる行
( )	文字列などをグループとして扱う	(ab cd)	ab、cd
\	続く特殊文字の効果を打ち消す	a\.c	a.c

また、**grep** は一行に繰り返し指定することもできる。更に、**less** コマンドと同時に使用することもできる。  
*pattern* 中の文字として `'\','?','|'` を使用する場合は、それらの文字の前に `'\'` をもう一つ重ねて入力しなければならない。

コマンド実行時に `"Searching ..."` と表示され、対象文字列の検索中に `Ctrl-C` を入力すると表示を中止できる。

```
例 )
# show command | grep nat
Searching ...
clear nat descriptor dynamic: 動的な NAT 情報を削除します
^C
#
```

## [設定例]

```
show config | grep ip | grep lan
show config | grep ip | less
```

## [適用モデル]

NVR700W, NVR510

## 2.5.2 show コマンドの表示内容を見やすくする

## [書式]

```
show [...] | less
```

## [説明]

**show** コマンドの表示内容を1画面単位で表示し、最終行でコマンドを受け付ける。

表示内容が1画面に満たない場合には、すべての内容を表示して終了する。

コマンドは、数値プレフィックスとコマンド文字を入力することで実行される。数値プレフィックスはオプションで省略できる。数値プレフィックスを省略した場合には1と見なされる。検索コマンドでは、コマンド文字の後に検索文字列を入力できる。

コマンドには以下の種類がある。

コマンド	内容 (数値プレフィックスをNとする)
q	less を終了する。
スペース	N 画面先に進む。
b	N 画面後ろに戻る。
j、ENTER	N 行先に進む。
k	N 行後ろに戻る。
g	N 行目にジャンプする。
G	N 行目にジャンプする。ただし、数値プレフィックスを省略した時には、最終行にジャンプする。
/	コマンド文字後に入力された検索パターンを前方に検索する。検索パターンは <b>grep</b> コマンドと同じものである。
?	コマンド文字後に入力された検索パターンを後方に検索する。検索パターンは <b>grep</b> コマンドと同じものである。
n	最後に入力された/ <b>、あるいは?</b> と同じ検索パターンで同じ方向に検索する。
N	最後に入力された/ <b>、あるいは?</b> と同じ検索パターンで逆方向に検索する。

## [適用モデル]

NVR700W, NVR510

## 2.5.3 外部メモリへのリダイレクト機能

## [書式]

```
show [...] > name
```

```
show [...] >> name
```

## [設定値及び初期値]

- *name*: ファイル名
- [設定値]:

設定値	説明
usb1:filename	USB メモリ内のファイル
sd1:filename	microSD カード内のファイル

- [初期値]:-

## [説明]

**show** コマンドの実行結果を外部メモリに保存させることができるリダイレクト (>) により指定されたファイルは、常に新規ファイルとして生成される。このため、同名のファイルが外部メモリ中に存在している場合、ファイルは置き換えられる。

保存ファイルの暗号化には対応していない。

パイプ (|) と併用することで必要な行のみをファイルとして保存させることができる。

```
# show log | grep IKE > usb1:log.txt
```

外部メモリの既存ファイルに対してリダイレクト記号 '>' を使用することで、コマンドの実行結果を既存ファイルに追加できる。

```
# show log > usb1:log.txt          ... 新規ファイル
# show log >> usb1:(既存)log.txt    ... ファイルの末尾に追加
```

また、リダイレクト記号 '>' を使用し、出力先ファイルに既存ファイル名を指定すると、ファイルを上書きしてよいかの確認メッセージが表示される。

```
# show log > usb1:(既存)log.txt
# 指定したファイルは既に存在しています。上書きしますか? (Y/N)
```

ただし、GUI のコマンド入力ページ、カスタム GUI、Lua の `rt.command` から実行した場合は確認メッセージが表示されず、強制的に上書きされる。

## [ノート]

リダイレクトの後にパイプ (|) は指定できない。

リダイレクトを複数回指定できない。

**show** 以外から始まるコマンド、**less** から始まるコマンドは適用外となる。

外部メモリについて、以下の状態では本機能は実行できない。

- 接続されていない状態
- ボタンを押された状態
- 使用を禁止されている状態

メモリの容量が不足している場合、書き込みに成功したサイズ分のファイルが生成される。

## [設定例]

**show log** の内容を USB メモリに保存

```
# show log > usb1:log.txt
```

**show techinfo** の内容を microSD カードに保存

```
# show techinfo > sd1:techinfo.txt
```

## [適用モデル]

NVR700W, NVR510

## 第3章

---

### ヘルプ

---

#### 3.1 コンソールに対する簡易説明の表示

---

[書式]

**help**

[説明]

コンソールの使用方法の簡単な説明を表示する。

[適用モデル]

NVR700W, NVR510

#### 3.2 コマンド一覧の表示

---

[書式]

**show command**

[説明]

コマンドの名称とその簡単な説明を一覧表示する。

[適用モデル]

NVR700W, NVR510

## 第 4 章

### 機器の設定

#### 4.1 ログインパスワードの設定

[書式]

**login password**

[説明]

無名ユーザーとしてログインするためのパスワードを 32 文字以内で設定する。パラメーターはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

NVR700W, NVR510

#### 4.2 ログインパスワードの暗号化保存

[書式]

**login password encrypted**

[説明]

無名ユーザーのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメーターはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[ノート]

パスワードを暗号化して保存する場合は本コマンドを、平文で保存する場合は **login password** コマンドを使用する。

[適用モデル]

NVR700W, NVR510

#### 4.3 管理パスワードの設定

[書式]

**administrator password**

[説明]

管理ユーザーとしてルーターの設定を変更するための管理パスワードを 32 文字以内で設定する。パラメーターはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

NVR700W, NVR510

#### 4.4 管理パスワードの暗号化保存

[書式]

**administrator password encrypted**

[説明]

管理ユーザーのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメーターはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

## [ノート]

パスワードを暗号化して保存する場合は本コマンドを、平文で保存する場合は **administrator password** コマンドを使用する。

## [適用モデル]

NVR700W, NVR510

## 4.5 一般ユーザー名とログインパスワードの設定

---

## [書式]

**login user** *user* [*password*]

**login user** *user* encrypted *password*

**no login user** *user* [*password*]

## [設定値及び初期値]

- *user*
  - [設定値]: ユーザー名 (32 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (32 文字以内)
  - [初期値]: -

## [説明]

一般ユーザー名とパスワードを設定する。

登録できるユーザーは最大 32 人。

ユーザー名に使用できる文字は、半角英数字およびハイフン (-)、アンダーバー(\_)

第 1 書式では、パスワードは平文で入力し、暗号化して保存される。また、パスワードを省略すると、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

第 2 書式では、*password* に暗号化されたパスワードを入力する。

TFTP で設定を取得した場合は、パスワードが暗号化されて保存されているため、常に第 2 書式の形で表示される。

## [ノート]

同一のユーザー名を複数登録することはできない。

既に登録されているユーザー名で設定を行った場合は、元の設定が上書きされる。

**syslog execute command** を on に設定している場合には、設定パスワードがログに残ることを防ぐために、パスワードを省略した書式で入力するか、一時的に **syslog execute command** を off に設定する、さもなければ **clear log** を実行するなどの操作を行うことが望ましい。

## [適用モデル]

NVR700W, NVR510

## 4.6 ログイン時のパスワード認証に RADIUS を使用するか否かの設定

---

## [書式]

**login radius use** *use*

**no login radius use**

## [設定値及び初期値]

- *use*
  - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off



**[説明]**

ログイン時のパスワード認証に RADIUS を使用するか否かを設定する。

**[ノート]**

RADIUS 認証サーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius auth**
- **radius auth server**
- **radius auth port**
- **radius secret**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 4.7 管理ユーザーへの移行時のパスワード認証に RADIUS を使用するか否かの設定

---

**[書式]**

```
administrator radius auth use
no administrator radius auth [use]
```

**[設定値及び初期値]**

- *use*
- [設定値]:

設定値	説明
on	ローカル認証と RADIUS 認証を併用する
only	RADIUS 認証のみ使用する
off	使用しない

- [初期値]: off

**[説明]**

**administrator** コマンドで管理ユーザーへ移行する際のパスワード認証に RADIUS を使用するか否かを設定する。

on の場合、最初に **administrator password** コマンドで設定された管理パスワードとの比較を行い、一致しなかった場合に RADIUS サーバーへの問い合わせを行う。only の場合、RADIUS サーバーへの問い合わせのみを行う。

**[ノート]**

RADIUS 認証サーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius auth**
- **radius auth server**
- **radius auth port**
- **radius secret**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 4.8 ユーザーの属性を設定

---

**[書式]**

```
user attribute [user] attribute=value [attribute=value...]
no user attribute [user...]
```

**[設定値及び初期値]**

- *user*
- [設定値]:

設定値	説明
ユーザー名	登録されているユーザー名
*radius	RADIUS 認証でログインするすべてのユーザー (NVR510 では Rev.15.01.03 以降で指定可能)
*	すべてのユーザー

- [初期値]: -
- `attribute=value`: ユーザー属性
- [設定値]:
  - `administrator`: 管理者モードを使えるかどうかを示す属性

設定値	説明
on	<code>administrator</code> コマンドにより管理ユーザーに昇格することができる。また GUI の管理者ページへ接続することができる。管理者パスワードを用いて SFTP 接続を行うことができる。
off	<code>administrator</code> コマンドにより管理ユーザーに昇格することができない。また GUI の管理者ページへ接続することができない。管理者パスワードを用いて SFTP 接続を行うことができない。

- `connection`: ルーターへのアクセス方法を示す属性

設定値	説明
off	すべての接続を禁止する。
all	すべての接続を許可する。
serial	シリアルコンソールからの接続を許可する。
telnet	TELNET による接続を許可する。
ssh	SSH による接続を許可する。
sftp	SFTP による接続を許可する。
remote	リモートセットアップによる接続を許可する。
http	GUI 設定画面への接続を許可する。

- `gui-page`: ログインユーザーに対して閲覧を許可する GUI 画面の種別を示す属性

設定値	説明
all	ログインユーザーでアクセスできるすべての画面の閲覧を許可する。
dashboard	ダッシュボード画面の閲覧を許可する。
lan-map	LAN マップ画面の閲覧を許可する。
config	かんたん設定画面、詳細設定画面、管理画面、CONFIG 画面および TECHINFO 画面の閲覧を許可する。

- `host`: ルーターへのアクセスホストを指定する属性

設定値	説明
IP アドレス	指定したホストからの接続を許可する。
any	すべてのホストからの接続を許可する。
インターフェース名	指定したインターフェースからの接続を許可する。

- `multi-session`: 複数接続を許可するかどうかを示す属性

設定値	説明
on	同一ユーザー名による TELNET、SSH、HTTP での複数接続を許可する。
off	同一ユーザー名による TELNET、SSH、HTTP での複数接続を禁止する。

- login-timer : ログインタイマの指定

設定値	説明
120..21474836	キー入力がない場合に自動的にログアウトするまでの秒数。
clear	ログインタイマを設定しない。

- [初期値]:
  - administrator=on
  - connection=serial,telnet,remote,ssh,sftp,http
  - gui-page=all
  - host=any
  - multi-session=on
  - login-timer=300

### [説明]

ユーザーの属性を設定する。

*user* を省略した場合は、無名ユーザーの属性を設定する。

*user* に \*radius を指定した場合は、RADIUS 認証でログインするすべてのユーザーの属性を設定する。NVR510 では Rev.15.01.03 以降で指定可能。

*user* にアスタリスク (\*) を指定した場合は、すべてのユーザーに対して設定を有効にする。ただし、ユーザー名を指定した設定がされている場合は、その設定が優先される。

すでに管理ユーザーに昇格しているユーザーに対して、このコマンドで administrator 属性を off に変更しても、そのユーザーは **exit** コマンドにより一般ユーザーに降格するか、あるいはログアウトするまでは管理ユーザーで居続けることができる。

connection 属性では、off、all 以外の値はコンマ (,) でつないで複数指定することができる。

すでに接続しているユーザーに対して、このコマンドで connection 属性または host 属性により接続を禁止しても、そのユーザーは切断するまでは接続を維持し続けることができる。

gui-page 属性では、all 以外の値はコンマ(,)でつないで複数指定することができる。本属性で設定した設定内容は、ログインユーザーとしてログインしたときのみ有効となる。管理ユーザーとしてログインした場合は、本属性の設定にかかわらず、常に GUI 上のすべての画面を閲覧する権限を持つ。すでに GUI に接続中のユーザーに対してこのコマンドで本属性の設定が変更された場合、次に GUI 上のページにアクセスした時点から新しい設定が反映される。

host 属性では、TELNET、SSH、SFTP 及び HTTP で接続できるホストを設定する。指定できる IP アドレスは、1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらをコンマ (,) でつないだものである。

multi-session 属性では、TELNET、SSH、HTTP での複数接続の可否を設定する。この属性を off に変更しても、シリアルと TELNET やリモートセットアップと SSH など、接続方法が異なる場合は同じユーザー名で接続することができる。

すでに複数の接続があるユーザーに対して、このコマンドで multi-session 属性を off に変更しても、そのユーザーは切断するまでは接続を維持し続けることができる。

無名ユーザーに対しては SSH、SFTP による接続を許可することができない。

無名ユーザーに対しては TELNET での複数接続はできない。

TELNET、SSH、SFTP、HTTP で接続した場合、login-timer 属性の値が clear に設定されていても、タイマ値は 300 秒として扱う。

**login timer** コマンドの設定値よりも、本コマンドの login-timer 属性の設定値が優先される。

### [ノート]

本コマンドにより、すべてのユーザーの接続を禁止する、またはすべてのユーザーが管理ユーザーに昇格できないといった設定を行った場合、ルーターの設定変更や状態確認などができなくなるので注意する必要がある。

### [適用モデル]

NVR700W, NVR510

## 4.9 他のユーザーの接続の強制切断

### [書式]

```
disconnect user user [/connection[no]]
```

```
disconnect user [user]/connection[no]
```

### [設定値及び初期値]

- *user*
  - [設定値]: ユーザー名
  - [初期値]: -
- *connection*: 接続種別
  - [設定値]:

設定値	説明
telnet	TELNET による接続
serial	シリアルコンソールからの接続
remote	リモートセットアップによる接続
ssh	SSH による接続
sftp	SFTP による接続
http	GUI 設定画面への接続

- [初期値]: -
- *no*
  - [設定値]: 接続番号
  - [初期値]: -

### [説明]

他ユーザーの接続を切断する。

**show status user** コマンドで表示された接続状況からパラメーターを指定する。

無名ユーザーを切断する場合は、第二書式で **user** を省略した形で指定する。

パラメーターを省略した場合は、指定したパラメーターと一致するすべての接続を切断する。

### [ノート]

自分自身のセッションを切断することはできない。

### [設定例]

例 1) ユーザー名「test」でログインしているすべての接続を切断する。

```
# disconnect user test
```

例 2) TELNET で接続しているすべてのユーザーを切断する。

```
# disconnect user /telnet
```

### [適用モデル]

NVR700W, NVR510

## 4.10 ログインタイマの設定

### [書式]

```
login timer time
```

```
no login timer [time]
```

### [設定値及び初期値]

- *time*
  - [設定値]:

設定値	説明
120..21474836	キー入力がない場合に自動的にログアウトするまでの秒数
clear	ログインタイマを設定しない

- [初期値]: 300

**[説明]**

キー入力がない場合に自動的にログアウトするまでの時間を設定する。

**[ノート]**

TELNET、SSH、SFTP、HTTP で接続した場合、clear が設定されていてもタイマ値は 300 秒として扱う。

**[適用モデル]**

NVR700W, NVR510

## 4.11 INIT スイッチによるパスワード再入力機能の設定

**[書式]**

**password reenter** *reenter*

**no password reenter**

**[設定値及び初期値]**

- *reenter*
- [設定値]:

設定値	説明
enable	パスワード再入力機能を許可する
disable	パスワード再入力機能を許可しない

- [初期値]: enable

**[説明]**

起動完了後に INIT スイッチを 10 秒以上押し続けると、その後 10 分間はパスワードを再入力可能にする機能を許可するか否かを設定する。再入力可能な 10 分間は、TELENET やシリアル経由でもパスワードなしでログインが可能。なお、パスワードを再入力可能にする機能は、電源投入後 1 回のみ実行可能。

**[適用モデル]**

NVR700W, NVR510

## 4.12 セキュリティークラスの設定

**[書式]**

**security class** *level* *forget* [*telnet* [*ssh*]]

**no security class** [*level* *forget* [*telnet* [*ssh*]]]

**[設定値及び初期値]**

- *level*
- [設定値]:

設定値	説明
1	シリアルでも、TELNET、SSH でも遠隔地のルーターからでもログインできる
2	シリアルと TELNET と SSH からは設定できるが、遠隔地のルーターからはログインできない
3	シリアルからのみログインできる

- [初期値]: 1
- *forget*
- [設定値]:

設定値	説明
on	設定したパスワードの代わりに "w,lXlma" (ダブルユー、カンマ、エル、エックス、エル、エム、エー)でもログインでき、設定の変更も可能になる。ただしシリアルのみ
off	パスワードを入力しないとログインできない

- [初期値]: on
- *telnet*
- [設定値]:

設定値	説明
on	TELNET クライアントとして <b>telnet</b> コマンドが使用できる
off	<b>telnet</b> コマンドは使用できない

- [初期値]: off
- *ssh*
- [設定値]:

設定値	説明
on	SSH クライアントとして <b>ssh</b> コマンドが使用できる
off	<b>ssh</b> コマンドは使用できない

- [初期値]: off

#### [説明]

セキュリティークラスを設定する。

ただし、本コマンドによる設定は Web GUI は対象外である。

#### [ノート]

**remote setup accept** コマンドにより、遠隔地のルーターからのログイン (**remote setup**) を細かくアクセス制限することができる。遠隔地のルーターからのログイン機能は、回線交換あるいは専用線を利用するため、それらに接続できる機種だけが持つ機能である。設定を変更したときに変更した値よりも多くのユーザーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー数が設定値より少なくなるまで新たな接続は許可しない。

#### [適用モデル]

NVR700W, NVR510

## 4.13 CPU 使用率の閾値の設定

#### [書式]

```
system cpu threshold cpu1 cpu2
no system cpu threshold [cpu1 [cpu2]]
```

#### [設定値及び初期値]

- *cpu1*
  - [設定値]: 警告を発する CPU 使用率の閾値の上限 (0..100 %)
  - [初期値]: -
- *cpu2*
  - [設定値]: 警告を発する CPU 使用率の閾値の下限 (0..100 %)
  - [初期値]: -

#### [説明]

CPU 使用率を監視して、*cpu1* 以上または *cpu2* 以下の使用率になると SYSLOG や SNMP トラップで警告を発する。SNMP トラップ送信するためには **snmp trap cpu threshold on** を設定する必要がある。

NVR700W は Rev.15.00.16 以降で使用可能。NVR510 は Rev.15.01.15 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 4.14 メモリ使用率の閾値の設定

### [書式]

```
system memory threshold memory1 memory2
no system memory threshold [memory1 [memory2]]
```

### [設定値及び初期値]

- *memory1*
  - [設定値]: 警告を発するメモリ使用率の閾値の上限 (0..100 %)
  - [初期値]: -
- *memory2*
  - [設定値]: 警告を発するメモリ使用率の閾値の下限 (0..100 %)
  - [初期値]: -

### [説明]

メモリ使用率を監視して、*memory1* 以上または *memory2* 以下の使用率になると SYSLOG や SNMP トラップで警告を発する。

SNMP トラップ送信するためには `snmp trap memory threshold on` を設定する必要がある。

NVR700W は Rev.15.00.16 以降で使用可能。 NVR510 は Rev.15.01.15 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 4.15 パケットバッファのパラメーターを変更する

### [書式]

```
system packet-buffer group parameter=value [parameter=value ...]
no system packet-buffer group [parameter=value ...]
```

### [設定値及び初期値]

- *group*: パケットバッファのグループを指定する。
  - [設定値]: グループ名 ( small, middle, large, huge )
  - [初期値]: -
- *parameter*: 変更するパラメーターを指定する。
  - [設定値]:

設定値	説明
max-buffer	パケットバッファの最大割り当て数
max-free	フリーリストの最大値
min-free	フリーリストの最小値
buffer-in-chunk	チャンク内のパケットバッファ数
init-chunk	起動時に確保するチャンク数

- [初期値]: -
- *value*
  - [設定値]: 変更する値を指定する。
  - [初期値]:

NVR700W, NVR510

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
huge	20	0	0	1	0

**[説明]**

パケットバッファの管理パラメーターを変更する。

パラメーターに指定できる値は、**huge** ブロックとそれ以外で異なる。**huge** ブロック以外のブロックでは、パラメーターには 1 以上の整数を指定できる。同時に、各パラメーターは以下に示す条件をすべて満たす必要がある。

- $\text{max-buffer} \geq \text{max-free}$
- $\text{max-free} > \text{min-free}$
- $\text{max\_free} \geq \text{buffer-in-chunk}$
- $\text{max\_free} \geq \text{buffer-in-chunk} \times \text{init-chunk}$

**huge** ブロックでは、**max-free**、**min-free**、**init-chunk** には 0 以上の整数を、**max-buffer**、**buffer-in-chunk** には 1 以上の整数を指定できる。**max-free**、**min-free**、**init-chunk** に 0 を指定する場合には、3 つのパラメーターがすべて 0 でなければならない。**max-free**、**min-free**、**init-chunk** が 1 以上の場合には、各パラメーターは他のグループと同様、上記の条件を満たす必要がある。

**[設定例]**

```
# system packet-buffer small max-buffer=3000 max-free=1000
# system packet-buffer large min-free=100
```

**[適用モデル]**

NVR700W, NVR510

## 4.16 環境変数の設定

---

**[書式]**

```
set name=value
no set name[=value]
```

**[設定値及び初期値]**

- *name*
  - [設定値]: 環境変数名
  - [初期値]: -
- *value*
  - [設定値]: 設定値
  - [初期値]: -

**[説明]**

ルーターの環境変数を設定する。

環境変数名の命名規則は次の通りである。

半角の英数字とアンダースコア '\_' が使用できるが、アンダースコアまたは数字を最初の文字にすることはできない。

変数名の長さに制限はないが、**set** コマンドはコマンドラインの最大長 (4095 文字) を超えて実行できない。

英字の大文字、小文字を区別する。例えば、**abc** と **Abc** は別の変数として扱われる。

*value* に空白等の特殊文字を含む場合は、*value* 全体を引用符で囲む必要がある。

**[適用モデル]**

NVR700W, NVR510

## 4.17 エイリアスの設定

---

**[書式]**

```
alias name=value
no alias name[=value]
```

**[設定値及び初期値]**

- *name*
  - [設定値]: エイリアス名



- [初期値]:-
- *value*
  - [設定値]: 設定値
  - [初期値]:-

**[説明]**

エイリアスを設定する。

エイリアスの命名規則は次の通りである。  
 半角の英数字とアンダースコア '\_' が使用でき、先頭は必ず英文字でなければならない。  
 英文字の大文字、小文字を区別する。例えば、*abc* と *Abc* は別のエイリアスとして扱われる。  
*value* に空白等の特殊文字を含む場合は、*value* 全体を引用符で囲む必要がある。

**[ノート]**

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 4.18 マクロの設定

---

**[書式]**

```
macro [-v] [-x] name <<eom
no macro [-v] [-x] name [<<eom]
```

**[設定値及び初期値]**

- -v
  - [設定値]: 展開前の内容を表示しながら実行する
  - [初期値]:-
- -x
  - [設定値]: 展開した後の行を表示しながら実行する
  - [初期値]:-
- *name*
  - [設定値]: マクロ名
  - [初期値]:-
- *eom*
  - [設定値]: マクロの終端文字列
  - [初期値]:-

**[説明]**

マクロを設定する。

このコマンド入力後はマクロ入力状態になるので、マクロの内容を入力していく。マクロの最後には、*eom* で指定した終端文字列だけを入力すれば、マクロ入力が終了する。  
 マクロ入力中でも、Ctrl-C を入力すればコマンドを中断できる。

-v オプションを指定すると、マクロを実行するときに実行する各行について、環境変数とエイリアスの展開前の内容を表示しながら実行する。

-x オプションは、環境変数とエイリアスを展開した後の行を表示しながらマクロを実行する。

*name* に使用できる文字は、半角の英大文字、英小文字、数字、アンダースコア ( \_ ) のみで、先頭は必ず英文字でなければならない。

実行例は以下の通り。

```
# macro sample <<EOM
show ip route
show ip connection
```

```
EOM
#
```

### [ノート]

複数行からなるコマンドに対応していないため、**schedule at** コマンドからは実行できない。

Lua スクリプトの `rt.command()` で複数行からなるコマンドを実行する場合には、各行を改行文字 ('\n') で連結した文字列をコマンドとして渡す。改行文字は '\n' でなくてはならず、'\r' や '\r\n' ではエラーとなる。実行例は以下の通り。

```
rtn, err = rt.command("macro sample <<EOM\nnecho This is sample\nEOM")
```

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

### [適用モデル]

NVR700W, NVR510

## 4.19 EMFS ファイルの作成、削除

### [書式]

```
embedded file [-b] filename <<eof
no embedded file [-b] filename [<<eof]
```

### [設定値及び初期値]

- *-b*
  - [設定値]: BASE64 形式を指定
  - [初期値]: -
- *filename*
  - [設定値]: ファイル名
  - [初期値]: -
- *eof*
  - [設定値]: 終端文字列
  - [初期値]: -

### [説明]

EMFS 上のファイルを作成、削除する。

**embedded file** コマンドを投入すると、コンソールはファイルの内容を入力するモードとなる。*eof* で指定した EOF 文字列が入力されるまでが、ファイルの内容となる。**no embedded file** コマンドでファイルを削除できる。

*-b* オプションを指定した場合は、入力されたファイルの内容は BASE64 形式であるものとして処理される。BASE64 形式として不正な内容の場合はエラーとなる。バイナリーファイルを保存する場合は、BASE64 形式でなければならない。*-b* オプションが省略された場合は、入力された内容がそのままテキストファイルとして保存される。

EOF 文字列として利用できる文字種は、半角英数字 (A-Z、a-z、0-9) のみである。英大文字、小文字は区別される。

実行例は以下の通り。

```
# embedded file sample.txt <<EOF
show ip route
show ip connection
EOF
#
```

### [ノート]

複数行からなるコマンドに対応していないため、**schedule at** コマンドからは実行できない。

Lua スクリプトの `rt.command()` で複数行からなるコマンドを実行する場合には、各行を改行文字 ('`\n`') で連結した文字列をコマンドとして渡す。改行文字は '`\n`' でなくてはならず、'`\r`' や '`\r\n`' ではエラーとなる。実行例は以下の通り。

```
rtn, err = rt.command("embedded file sample <<EOF\nnecho This is sample\nEOF")
```

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

[適用モデル]

NVR700W, NVR510

## 4.20 タイムゾーンの設定

[書式]

**timezone** *timezone*

**no timezone** [*timezone*]

[設定値及び初期値]

- *timezone* : その地域と世界標準時との差
- [設定値] :

設定値	説明
jst	日本標準時 (+09:00)
utc	世界標準時 (+00:00)
任意の時刻 : 分	時刻 : 分 (-12:00..+11:59)

- [初期値] : jst

[説明]

タイムゾーンを設定する。

[適用モデル]

NVR700W, NVR510

## 4.21 現在の日付けの設定

[書式]

**date** *date*

[設定値及び初期値]

- *date*
- [設定値] : yyyy-mm-dd または yyyy/mm/dd
- [初期値] : -

[説明]

現在の日付けを設定する。

[適用モデル]

NVR700W, NVR510

## 4.22 現在の時刻の設定

[書式]

**time** *time*

[設定値及び初期値]

- *time*
- [設定値] : hh:mm:ss
- [初期値] : -

**[説明]**

現在の時刻を設定する。

**[適用モデル]**

NVR700W, NVR510

## 4.23 リモートホストによる時計の設定

---

**[書式]**

```
rdate host [syslog]
```

**[設定値及び初期値]**

- *host*

- [設定値]:

設定値	説明
IP アドレス	リモートホストの IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
名前	ホストの名称

- [初期値]:-

- *syslog*: 出力結果を SYSLOG へ出力することを示すキーワード

- [初期値]:-

**[説明]**

ルーターの時計を、パラメーターで指定したホストの時間に合わせる。  
このコマンドが実行されるとホストの TCP の 37 番ポートに接続する。

**[ノート]**

ヤマハルーターシリーズ および、多くの UNIX コンピュータをリモートホストに指定できる。  
*syslog* キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

**[適用モデル]**

NVR700W, NVR510

## 4.24 NTP による時計の設定

---

**[書式]**

```
ntpdate ntp_server [syslog]
```

**[設定値及び初期値]**

- *ntp\_server*

- [設定値]:

設定値	説明
IP アドレス	NTP サーバーの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
IPv6 アドレス	NTP サーバーの IPv6 アドレス (xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx (xxxx は十六進数))
名前	NTP サーバーの名称

- [初期値]:-

- *syslog*: 出力結果を SYSLOG へ出力することを示すキーワード

- [初期値]:-

**[説明]**

NTP を利用してルーターの時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。

**[ノート]**

インターネットに接続している場合には、**rddate** コマンドを使用した場合よりも精密な時計合わせが可能になる。NTP サーバーはできるだけ近くのを指定した方が良い。利用可能な NTP サーバーについてはプロバイダーに問い合わせること。

syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

**[適用モデル]**

NVR700W, NVR510

## 4.25 NTP パケットを送信するときの始点 IP アドレスの設定

---

**[書式]**

```
ntp local address ip_address
```

```
no ntp local address
```

**[設定値及び初期値]**

- *ip\_address*
  - [設定値]: IP アドレス
  - [初期値]: -

**[説明]**

NTP パケットを送信するときの始点 IP アドレスを設定する。

始点 IP アドレスが設定されていないときは、通常の UDP パケットの送信ルールに従い、出力インターフェースの IP アドレスを利用する。

**[適用モデル]**

NVR700W, NVR510

## 4.26 Stratum 0 の NTP サーバーとの時刻同期を許可する設定

---

**[書式]**

```
ntp backward-compatibility comp
```

```
no ntp backward-compatibility [comp]
```

**[設定値及び初期値]**

- *comp*
  - [設定値]:

設定値	説明
accept-stratum-0	Stratum 0 の NTP サーバーとの時刻同期を許可する

- [初期値]: -

**[説明]**

Stratum 0 の NTP サーバーとの時刻同期を許可する。

**[ノート]**

外部クロックに同期した NTP サーバーでない限り、Stratum 0 にはならない。

**[適用モデル]**

NVR700W, NVR510

## 4.27 コンソールのプロンプト表示の設定

### [書式]

**console prompt** *prompt*

**no console prompt** [*prompt*]

### [設定値及び初期値]

- *prompt*
  - [設定値]: コンソールのプロンプトの先頭文字列 (64 文字以内)
  - [初期値]: -

### [説明]

コンソールのプロンプト表示を設定する。空文字列も設定できる。

### [適用モデル]

NVR700W, NVR510

## 4.28 コンソールの言語とコードの設定

### [書式]

**console character** *code*

**no console character** [*code*]

### [設定値及び初期値]

- *code*
  - [設定値]:

設定値	説明
en.ascii	英語で表示する、文字コードは ASCII
ja.sjis	日本語で表示する、文字コードはシフト JIS
ja.euc	日本語で表示する、文字コードは EUC
ja.utf8	日本語で表示する、文字コードは UTF-8

- [初期値]: ja.sjis

### [説明]

コンソールに表示する言語とコードを設定する。  
本コマンドは一般ユーザーでも実行できる。

### [適用モデル]

NVR700W, NVR510

## 4.29 コンソールの表示文字数の設定

### [書式]

**console columns** *col*

**no console columns** [*col*]

### [設定値及び初期値]

- *col*
  - [設定値]: コンソールの表示文字数
  - [設定値]:
    - 80..4096 (NVR700W Rev.15.00.17 以降、NVR510 Rev.15.01.16 以降)
    - 80..200 (上記以外)
  - [初期値]: 80

**[説明]**

コンソールの 1 行あたりの表示文字数を設定する。  
本コマンドは一般ユーザーでも実行できる。

**[適用モデル]**

NVR700W, NVR510

**4.30 コンソールの表示行数の設定****[書式]**

**console lines** *lines*  
**no console lines** [*lines*]

**[設定値及び初期値]**

- *lines*
  - [設定値]:

設定値	説明
10..100	表示行数
infinity	スクロールを止めない

- [初期値]: 24

**[説明]**

コンソールの表示行数を設定する。  
このコマンドは一般ユーザーでも実行できる。

**[適用モデル]**

NVR700W, NVR510

**4.31 コンソールにシステムメッセージを表示するか否かの設定****[書式]**

**console info** *info*  
**no console info** [*info*]

**[設定値及び初期値]**

- *info*
  - [設定値]:

設定値	説明
on	表示する
off	表示しない

- [初期値]: off

**[説明]**

コンソールにシステムメッセージを表示するか否かを設定する。

**[ノート]**

キーボード入力中にシステムメッセージがあると表示画面が乱れるが、[Ctrl]+r で入力中の文字列を再表示できる。

**[適用モデル]**

NVR700W, NVR510

**4.32 SYSLOG を受けるホストの IP アドレスの設定****[書式]**

**syslog host** *host*  
**no syslog host** [*host*]

**[設定値及び初期値]**

- *host*
  - [設定値]: SYSLOG を受けるホストの IP アドレス (空白で区切って最大 4 ヶ所まで設定可能)
  - [初期値]: -

**[説明]**

SYSLOG を受けるホストの IP アドレスを設定する。

IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。

**syslog debug** コマンドが on に設定されている場合、大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。

**[適用モデル]**

NVR700W, NVR510

### 4.33 SYSLOG ファシリティの設定

---

**[書式]**

**syslog facility** *facility*

**no syslog facility** [*facility*]

**[設定値及び初期値]**

- *facility*
  - [設定値]:

設定値	説明
0..23	facility 値
user	1
local0..local7	16..23

- [初期値]: user

**[説明]**

SYSLOG のファシリティを設定する。

**[ノート]**

ファシリティ番号の意味づけは、各 SYSLOG サーバーで独自に行う。

**[適用モデル]**

NVR700W, NVR510

### 4.34 NOTICE タイプの SYSLOG を出力するか否かの設定

---

**[書式]**

**syslog notice** *notice*

**no syslog notice** [*notice*]

**[設定値及び初期値]**

- *notice*
  - [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

**[説明]**

各種フィルター機能等で検出したパケット情報を SYSLOG で出力するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510



### 4.35 INFO タイプの SYSLOG 出力の設定

#### [書式]

```
syslog info info
no syslog info [info]
```

#### [設定値及び初期値]

- *info*
- [設定値]:

設定値	説明
on	出力する
off	出力する、ただし SYSLOG ホストへの送信は行わない

- [初期値]: on

#### [説明]

ルーターの動作状況に関する SYSLOG 出力の設定をする。

#### [ノート]

INFO タイプのログは *info* パラメーターの on/off にかかわらずルーター内部に保持される。**syslog host** コマンドで設定するホストへの送信は、*info* パラメーターが on の場合にのみ行われる。

#### [適用モデル]

NVR700W, NVR510

### 4.36 DEBUG タイプの SYSLOG を出力するか否かの設定

#### [書式]

```
syslog debug debug
no syslog debug [debug]
```

#### [設定値及び初期値]

- *debug*
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

#### [説明]

ルーターのデバッグ情報を SYSLOG で出力するか否かを設定する。

#### [ノート]

*debug* パラメーターを on にすると、大量のデバッグメッセージを送信するため、**syslog host** コマンドで設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに off にする。

#### [適用モデル]

NVR700W, NVR510

### 4.37 SYSLOG を送信する時の始点 IP アドレスの設定

#### [書式]

```
syslog local address address
no syslog local address [address]
```

#### [設定値及び初期値]

- *address*
- [設定値]: 始点 IP アドレス

- [初期値]: -

#### [説明]

SYSLOG パケットを送信する時の始点 IP アドレスを設定する。始点 IP アドレスが設定されていない時は、通常の UDP パケット送信ルールに従い、出力インターフェースの IP アドレスを利用する。

#### [適用モデル]

NVR700W, NVR510

### 4.38 SYSLOG パケットの始点ポート番号の設定

#### [書式]

```
syslog srcport port
no syslog srcport [port]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 514

#### [説明]

本機が送信する SYSLOG パケットの始点ポート番号を設定する。

#### [適用モデル]

NVR700W, NVR510

### 4.39 SYSLOG に実行コマンドを出力するか否かの設定

#### [書式]

```
syslog execute command switch
no syslog execute command [switch]
```

#### [設定値及び初期値]

- *switch*
  - [設定値]:

設定値	説明
on	実行されたコマンドをログに残す
off	実行されたコマンドをログに残さない

- [初期値]: off

#### [説明]

実行されたコマンドを SYSLOG で出力するか否かを設定する。

#### [ノート]

コマンド実行に成功した場合、そのコマンド入力をログに出力する。

#### [適用モデル]

NVR700W, NVR510

### 4.40 TCP のコネクションレベルの syslog を出力するか否かの設定

#### [書式]

```
tcp log switch [src_addr[/mask] [dst_addr[/mask] [tcpflag[src_port_list [dst_port_list]]]]]
no tcp log [...]
```

#### [設定値及び初期値]

- *switch*
  - [設定値]:

設定値	説明
on	TCP コネクションの syslog を出力する

設定値	説明
off	TCP コネクションの syslog を出力しない

- [初期値]: off
- *src\_addr*: 始点アドレス
- [設定値]:
  - IP アドレス
    - xxx.xxx.xxx.xxx は
      - 10 進数
      - \*(ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
    - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定
    - , を区切りとして複数設定することができる。
  - FQDN
    - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
    - \* から始まる FQDN は \* より後ろの文字列を後方一致条件として判断する 例えば \*.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
    - , を区切りとして複数設定することができる。
    - \*(すべての IP アドレス)
- [初期値]: -
- *dst\_addr*: 終点アドレス
- [設定値]:
  - *src\_addr* と同じ形式
  - 省略時は 1 個の \* と同じ
- [初期値]: -
- *mask*: IP アドレスのビットマスク。 *src\_addr* および *dst\_addr* がネットワークアドレスの場合にのみ指定可能。
- [設定値]:
  - "0xffffffff" のような 16 進表記
  - "/24" のようなビット数表記
  - 省略時は 0xffffffff と同じ
- [初期値]: -
- *tcpflag*: フィルタリングする TCP パケットの種類
- [設定値]:
  - プロトコルを表す 10 進数 (6 のみ)
  - プロトコルを表すニーモニック

ニーモニック	10 進数	説明
tcp	6	すべての TCP パケット
tcpsyn	-	SYN フラグの立っているパケット
tcpfin	-	FIN フラグの立っているパケット
tcprst	-	RST フラグの立っているパケット
established	-	ACK フラグの立っているパケット

- *tcpflag=flag\_value/flag\_mask*、または *tcpflag!=flag\_value/flag\_mask*
  - *flag\_value*, *flag\_mask* は 16 進表記
  - 参考フラグ値

0x0001	FIN
0x0002	SYN
0x0004	RST

0x0008	PSH
0x0010	ACK
0x0020	URG

- \*(すべての TCP パケット。ニーモニックに tcp を指定したときと同じ)
- 省略時は \* と同じ
- [初期値]:-
- *src\_port\_list*: TCP のソースポート番号
- [設定値]:
  - ポート番号、タイプを表す 10 進数
  - ポート番号を表すニーモニック

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- \*(すべてのポート、タイプ)
- 省略時は \* と同じ
- [初期値]:-
- *dest\_port\_list*: TCP のデスティネーションポート番号
  - [設定値]: *src\_port\_list* と同じ形式
  - [初期値]:-

#### [説明]

TCP の syslog を出力する。 **syslog debug on** も設定されている必要がある。IPv4 のみに対応している。システムに負荷がかかるため、トラブルシュート等の一時的な使用にしか推奨されない。

## [ノート]

*src\_addr* および *dest\_addr* への FQDN の指定は NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.13 以降のファームウェアで指定可能。

## [設定例]

```
tcp log on * * tcpsyn * 1723 (PPTP のポートに SYN が来ているか )
tcp log on * * tcpflag!=0x0000/0x0007 (FIN,RST,SYN の立った TCP パケット )
tcp log on ( すべての TCP パケット。tcp log on * * * * * と同じ )
```

## [適用モデル]

NVR700W, NVR510

## 4.41 インターフェースパケットのダンプを SYSLOG へ出力するか否かの設定

## [書式]

**packetdump** *interface count*

**packetdump pp** *peer\_num count*

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *count*
  - [設定値]:

設定値	説明
1..21474836	回数
off	ダンプを行わない
infinity	回数制限をかけない

- [初期値]: off

## [説明]

**syslog debug on** が設定されている場合のみ、指定したインターフェースのパケットをダンプする。

## [ノート]

本コマンドの設定は、**show config** コマンドで表示されない。

本コマンドの設定は、**save** コマンドで保存されない。電源再投入や再起動により、本コマンドの設定がクリアされる。

*count* パラメータを *infinity* にすると、大量のパケットダンプメッセージが出力されるため機器の負荷が高くなる。

すべてのパケットがダンプされるわけではない。パケットロスすることもある。

ファストパスで処理されたパケットは出力されない。

## [適用モデル]

NVR700W, NVR510

## 4.42 TELNET サーバー機能の ON/OFF の設定

## [書式]

**telnetd service** *service*

**no telnetd service**

**[設定値及び初期値]**

- *service*
  - [設定値]:

設定値	説明
on	TELNET サーバー機能を有効にする
off	TELNET サーバー機能を停止させる

- [初期値]: on

**[説明]**

TELNET サーバー機能の利用を選択する。

**[ノート]**

TELNET サーバーが停止している場合、TELNET サーバーはアクセス要求に一切応答しない。

**[適用モデル]**

NVR700W, NVR510

## 4.43 TELNET サーバー機能の listen ポートの設定

---

**[書式]**

**telnetd listen port**

**no telnetd listen**

**[設定値及び初期値]**

- *port*
  - [設定値]: TELNET サーバー機能の待ち受け (listen) ポート番号 (1..65535)
  - [初期値]: 23

**[説明]**

TELNET サーバー機能の listen ポートを選択する。

**[ノート]**

telnetd は、TCP の 23 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。ただし、待ち受けポートを変更した場合には、ポート番号が変更されても、TELNET オプションのネゴシエーションが行える TELNET クライアントを用いる必要がある。

**[適用モデル]**

NVR700W, NVR510

## 4.44 TELNET サーバーへアクセスできるホストの設定

---

**[書式]**

**telnetd host ip\_range [ip\_range...]**

**telnetd host any**

**telnetd host none**

**telnetd host lan**

**no telnetd host**

**[設定値及び初期値]**

- *ip\_range*: TELNET サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
  - [設定値]:

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
onu1	ONU インターフェースからのアクセスを許可する

設定値	説明
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
  - [設定値]: すべてのホストからのアクセスを許可する
  - [初期値]: any
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: -
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: -

**[説明]**

TELNET サーバーへのアクセスを許可するホストを設定する。

**[ノート]**

設定後の新しい TELNET 接続から適用される。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

lan キーワードと WAN インターフェースは NVR700W の Rev.15.00.03 以降、NVR510 の Rev.15.01.03 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 4.45 TELNET サーバーへ同時に接続できるユーザー数の設定

---

**[書式]**

```
telnetd session num
no telnetd session
```

**[設定値及び初期値]**

- *num*
  - [設定値]: 同時接続数 (1...8)
  - [初期値]: 8

**[説明]**

TELNET に同時に接続できるユーザー数を設定する。

**[ノート]**

設定を変更したときに変更した値よりも多くのユーザーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー数が設定値より少なくなるまで新たな接続は許可しない。

**[適用モデル]**

NVR700W, NVR510

## 4.46 ファストパス機能の設定

---

**[書式]**

```
ip routing process process
no ip routing process
```

**[設定値及び初期値]**

- *process*
  - [設定値]:

設定値	説明
fast	ファストパス機能を利用する
normal	ファストパス機能を利用せず、すべてのパケットをノーマルパスで処理する

- [初期値]: fast

**[説明]**

パケット転送をファストパス機能で処理するか、ノーマルパス機能で処理するかを設定する。

**[ノート]**

ファストパスでは使用できる機能に制限は無いが、取り扱うパケットの種類によってはファストパスで処理されずノーマルパスで処理されることもある。

**[適用モデル]**

NVR700W, NVR510

## 4.47 LAN インターフェースの動作設定

---

**[書式]**

**lan shutdown interface** [port...]

**no lan shutdown interface** [port...]

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *port*
  - [設定値]: ポート番号 (*interface* が lan1 の場合のみ有効)
  - [初期値]: -

**[説明]**

LAN インターフェースを利用できないようにする。このコマンドを設定した LAN インターフェース、あるいはスイッチングハブのポートでは、LAN ケーブルを接続してもリンクアップしなくなる。

**[ノート]**

lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インターフェースが同時にリセットされる。

**[適用モデル]**

NVR700W, NVR510

## 4.48 LAN インターフェースのリンクアップ後の送信抑制時間の設定

---

**[書式]**

**lan linkup send-wait-time interface** time

**no lan linkup send-wait-time interface** [time]

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *time*
  - [設定値]: 送信抑制秒数 (0..10)
  - [初期値]: 0 (抑制しない)



**[説明]**

リンクアップ後の送信抑制時間を設定し、パケットの送信を抑制する。送信を抑制されたパケットはキューに保存され、リンクアップから設定秒数の経過後に送信される。保存先のキュー長は **queue interface length** コマンドの設定に従う。

**[ノート]**

リンクアップ直後に Gratuitous ARP や IPv6 neighbor solicitation 等のパケットがルーターから送信されるが、その送信が早過ぎるために対向機器側で受信できない場合は、この抑制時間を適宜設定し送信を遅延させることで対向機器側で受信できるようになる。

**[適用モデル]**

NVR700W, NVR510

## 4.49 ポートミラーリング機能の設定

**[書式]**

```
lan port-mirroring interface mirror direction port ... [direction port ...]
```

```
no lan port-mirroring interface
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *mirror*
  - [設定値]: ミラーリングパケットを送出させるポート番号
  - [初期値]: -
- *direction*: 観測対象のパケットの方向
  - [設定値]:

設定値	説明
in	入る方向
out	出る方向

- [初期値]: -
- *port*
  - [設定値]: 観測対象とするポート番号
  - [初期値]: -

**[説明]**

スイッチングハブインターフェースにおいて、特定ポートでの通信を他のポートで観測できる機能を設定する。LAN インターフェース名にはスイッチングハブを持つインターフェースだけが指定可能である。

**[ノート]**

LAN 分割機能との併用はできない。

スニファースポートから送出されるパケットの送出レートが回線速度を超えないようにする必要がある。ミラーリングパケットがスニファースポートから送出しきれない場合、他のポート間での通信に影響を与えることがある。

このコマンドを実行すると、lan1 および lan2 インターフェースが同時にリセットされる。

**[設定例]**

例 1) ポート 4 でポート 1 受信パケットを観測

```
# lan port-mirroring lan1 4 in 1
```

例 2) ポート 4 でポート 1 送受信パケットとポート 2 送信パケットを観測

```
# lan port-mirroring lan1 4 in 1 out 1 2
```

**[適用モデル]**

NVR700W

## 4.50 LAN インターフェースの動作タイプの設定

## [書式]

```
lan type interface_with_swhub speed [port] [speed [port]...] [option=value...]
```

```
lan type interface_with_swhub option=value [option=value...]
```

```
lan type interface_without_swhub speed [option=value...]
```

```
lan type interface_without_swhub option=value [option=value...]
```

```
lan type interface mtu=mtu
```

```
no lan type interface [...]
```

## [設定値及び初期値]

- *interface\_with\_swhub*
  - [設定値]: スイッチングハブを持つ LAN インターフェース名
  - [初期値]: -
- *interface\_without\_swhub*
  - [設定値]: スイッチングハブを持たない LAN インターフェース名
  - [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *speed*: リンク速度および動作モード
  - [設定値]:

設定値	説明
auto	速度自動判別
1000-fdx	1000BASE-T 全二重
100-fdx	100BASE-TX 全二重
100-hdx	100BASE-TX 半二重
10-fdx	10BASE-T 全二重
10-hdx	10BASE-T 半二重
省略	省略時は auto

- [初期値]: auto
- *port*
  - [設定値]:

設定値	説明
1..4	スイッチングハブのポート番号
省略	省略時は全ポート

- [初期値]: -
- *option=value*: オプション機能
  - [設定値]:
    - mtu
      - インターフェースで送受信できる最大データ長 (64..1500)
    - auto-crossover
      - オートクロスオーバー機能

設定値	説明
on	オートクロスオーバー機能を有効にする
off	オートクロスオーバー機能を無効にする

- *macaddress-aging*
  - MAC アドレスエージング機能

設定値	説明
秒数	エージング時間 (1..3825)
off	MAC アドレスエージング機能を無効にする

- port-based-option
  - LAN 分割機能、ポート分離機能

設定値	説明
divide-network	LAN 分割機能を有効にする
split-into-split_pattern	ポート分離機能を有効にする(基本機能)
X1,X2,X3,X4(X1..X4 は 1..4 の数字を羅列し末尾に"+"もしくは "-"をつけたもの)	ポート分離機能を有効にする(拡張機能)
off	LAN 分割機能、ポート分離機能を無効にする

- speed-downshift
  - 速度ダウンシフト機能

設定値	説明
on	速度ダウンシフト機能を有効にする
off	速度ダウンシフト機能を無効にする

- energy-saving
  - 省電力機能

設定値	説明
on	省電力機能を有効にする
off	省電力機能を無効にする

- [初期値]:
  - mtu=1500
  - auto-crossover=on
  - macaddress-aging=300
  - port-based-option=off
  - speed-downshift=on
  - energy-saving=off

## [説明]

指定した LAN インターフェースの速度と動作モードの種類、およびオプション機能について設定する。スイッチングハブを持つ LAN インターフェースについては、ポート毎に速度と動作モードを指定できる。

### ○mtu

インターフェースで送受信できる最大データ長を指定する。データ長には MAC ヘッダと FCS は含まれない。また、タグ VLAN 時のタグ長 (4 バイト) も含まれない。

指定できるデータ長の範囲は 64~1500 の範囲となる。

インターフェースの *mtu* を設定して、かつ、**ip mtu** コマンドまたは **ipv6 mtu** コマンドの設定が初期値のままの場合、IPv4 や IPv6 での MTU にはインターフェースの *mtu* が利用される。一方、**ip mtu** コマンドまたは **ipv6 mtu** コマンドが設定されていて、かつ、その設定値がインターフェースの *mtu* より小さい場合、**ip mtu** コマンドまたは **ipv6 mtu** コマンドの設定値が MTU として利用される。インターフェースの *mtu* も含めてすべて設定されていない時には、初期値である 1500 が利用される。

### ○オートクロスオーバー機能

LAN ケーブルがストレートケーブルかクロスケーブルかを自動的に判定して接続する機能。この機能が有効になっていると、ケーブルのタイプがどのようなものであるかを気にする必要がなくなる。

### ○MAC アドレスエージング機能

スイッチングハブを持つ LAN インターフェースでのみ利用できる。  
 スwitchングハブが持つ MAC アドレステーブル内のエントリを一定時間で消去していく機能。この機能を off にすると、一度スイッチングハブが記憶した MAC アドレスは自動的に消去されないのはもちろん、**clear switching-hub macaddress** コマンドを実行しても消去されない。エントリが消去されるのは、この機能を再度有効にした時だけになる。

コマンドの設定値と実際に消去されるまでの時間に誤差が生じる場合がある。特に、本機では 13 秒未満の値を設定しても、実際に消去される時間が 13 秒より短くなることはない。

MAC アドレステーブルには最大で 8192 個のエントリを格納できる。

#### ○LAN 分割機能

スイッチングハブを持つ LAN インターフェースでのみ利用できる。  
 このオプションは NVR510 では利用できない。

LAN 分割機能には基本機能と拡張機能があり、基本機能では、スイッチングハブの各ポートが個別の LAN インターフェースとして動作する。各インターフェースにはそれぞれ個別の IP アドレスを付与でき、その間でのルーティグも可能になる。

例えば、通常は LAN インターフェースを 2 つ持つルーターなのだが、LAN 分割機能を使えば LAN インターフェースを最大 5 個利用できることになる。

拡張機能では、スイッチングハブの各ポートを自由に組み合わせて 1 つの LAN インターフェース (VLAN インターフェース) とすることができる。

同一の VLAN インターフェースに所属するポート間はスイッチとして動作する。

LAN 分割で使用するインターフェース名は基本機能と拡張機能で異なる。

基本機能における LAN インターフェースのインターフェース名は元の LAN インターフェース名にピリオドとポート番号をつなげることで表される。

例えば、lan1 が 4 ポートのスイッチングハブを持つ LAN インターフェースなので、以下の LAN インターフェースが使用できるようになる。

ポート番号	インターフェース名
1	lan1.1
2	lan1.2
3	lan1.3
4	lan1.4

拡張機能では、LAN インターフェースのインターフェース名として vlan1、vlan2、vlan3・・・(VLAN インターフェース) を使用する。基本機能とは異なり、VLAN インターフェースは特定のポートと関連付けられてはいない。

**vlan port mapping** コマンドを用いて、スイッチングハブの各ポートがどの VLAN インターフェースに所属するかを設定することで、分割方法を自由に変更することができる。

VLAN インターフェースは同時に 4 つ使用することができる (vlan1-vlan4)。

LAN 分割機能を有効にした場合、lan1 インターフェースに対する設定は、lan1.1 (基本機能の場合) もしくは vlan1 (拡張機能の場合) に引き継がれる。

LAN 分割で使用する LAN インターフェースの MAC アドレスは元の LAN インターフェースの MAC アドレスに一致する。したがって上記の例では、lan1.1-lan1.4 や vlan1-vlan4 の MAC アドレスはすべて lan1 と同一になる。

#### ○ポート分離機能

スイッチングハブを持つ LAN インターフェースでのみ利用できる。  
 このオプションは NVR510 では利用できない。

通常は、スイッチングハブの各ポートは他のポートと制限無く通信できるが、ポート分離機能を利用すると、ポート間での通信を制限することができる。

ポート分離機能には基本機能と拡張機能があり、基本機能ではポート間での通信を制限しつつ、ルーターを経由した通信が可能であり、拡張機能では指定ポートからのルーターを経由した通信も制限することができる。

基本機能では、ポートをグループに分離し、グループ内の通信およびルーターとの通信は可能としつつ、他のグループのポートとは通信を制限できる。

LAN 分割機能とは異なり、ポート分離機能によって LAN インターフェースが増減することはない。分離されたポートはすべて同じ LAN インターフェースとして認識され、同一の IP アドレスを持つ。

ポートの分離パターンは、ポート番号の数字の並びで分離する部分に ":" を入れて記述する。例を以下に示す。

split_pattern	ポ ー ト				説明
	1	2	3	4	
1 : 234	↔	←	→	↔	ポート 1 とその他
1 : 2 : 34	↔	↔	←	→	ポート 1、ポート 2 とその他
1 : 2 : 3 : 4	↔	↔	↔	↔	全ポートを分離

省略形でコマンドを入力しても、**show config** コマンドの出力には省略しない形で表示される。

同一 LAN インターフェースにおけるプライマリアドレスのネットワークとセカンダリアドレスのネットワーク間の通信はルーターを経由するので、他のグループとの通信も可能である。

拡張機能では、ポート毎に受信したパケットを転送するポートを指定することで、ポート間やルーター自身、ルーターを経由した通信を制限することができる。具体的には、以下のように設定する。

```
lan type lan1 port-based-option=X1,X2,X3,X4
```

Xn(n=1..4)にはポート n で受信したパケットを転送するポート番号を羅列し、ルーター自身との通信・ルーターを経由した通信を許可する場合は"+", 禁止する場合は "-" を末尾につける。ただし "+" は省略可能である。

"-"を指定した場合、そのポートで受信したパケットはルーティングされなくなる。またそのポートに接続された機器はルーターとの通信ができなくなる。

例えば以下の設定の場合、ポート 1 から 3 で受信したパケットはポート 4 とルーターに転送され、ポート 4 で受信したパケットはポート 1 から 3 に転送されるがルーターには転送されない。つまり、ポート 1 と 4、ポート 2 と 4、ポート 3 と 4 の 3 つのグループに分離された状態となり、ポート 1 から 3 はお互いのポートと通信できずポート 4 とのみ通信可能になる。また、ポート 1 から 3 はルーターと通信可能だが、ポート 4 は通信不可であり受信パケットもルーティングされない。

```
lan type lan1 port-based-option=4,4,4,123-
```

#### ○速度ダウンシフト機能

on に設定すると 1000BASE-T で使用できないケーブルを接続された時に、速度を落としてリンクを試みる機能である。

#### ○省電力機能

on に設定すると EEE (Energy Efficient Ethernet) により通信していない LAN ポートで消費電力を抑えることができる。

この機能を使用するには、接続する機器も EEE をサポートしている必要がある。

#### [ノート]

LAN インターフェースが使用できる場合、本コマンドの実行後、LAN インターフェースのリセットが自動で行われ、その後に設定が有効となる。LAN インターフェースが使用できない場合、設定の変更のみが行われる。

lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インターフェースが同時にリセットされる。

#### [設定例]

スイッチングハブを持つ LAN インターフェースで、ポート 1、2 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続する。

```
# lan type lan1 100-fdx 1 2
```

#### [適用モデル]

NVR700W, NVR510

## 4.51 インターフェースまたはシステムの説明の設定

---

### [書式]

```
description id description
no description id [description]
description interface description
no description interface [description]
```

### [設定値及び初期値]

- *id*
  - [設定値]: システム全体の説明を記述する場合の ID (1..21474836)
  - [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、'pp'、'tunnel'、'wwan' のいずれか
  - [初期値]: -
- *description*
  - [設定値]: 説明の文字列 (最大 64 文字/ASCII、32 文字/シフト JIS)
  - [初期値]: -

### [説明]

システム全体の説明、あるいはインターフェースの説明を設定しておく。設定内容はあくまで説明のためだけであり、動作には影響を与えない。

システム全体の説明の場合は、ID の値を変えることで複数行の説明を設定できる。インターフェースの説明は一行に限定される。

*interface* として 'pp' あるいは 'tunnel'、'wwan' を指示したときにはそれぞれ、**pp select** あるいは **tunnel select**、**wwan select** で選択したインターフェースの説明となる。

設定内容は **show config** コマンドで表示される。また、インターフェースに対する設定内容はインターフェースに対する **show status** コマンドでも表示される。

システム全体の説明は、**show config** コマンドではすべての設定よりも先に、ID 順に表示される。

説明には、ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 (半角カタカナを除く) も使用できる。ただし、**console character** コマンドの設定が sjis の場合にのみ、正しく設定、表示でき、他の設定の場合には文字化けすることがある。

### [ノート]

wwan 指定は NVR700W で指定可能。

### [適用モデル]

NVR700W, NVR510

## 4.52 ONU インターフェースの動作タイプの設定

---

### [書式]

```
onu type interface speed [option=value...]
onu type interface option=value [option=value]
no onu type interface [...]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: ONU インターフェース名
  - [初期値]: -
- *speed*: リンク速度および動作モード
  - [設定値]:

設定値	説明
auto	速度自動判別
1000-fdx	1000BASE-X 全二重
省略	省略時は auto

- [初期値]: auto
- *option=value*: オプション機能
  - [設定値]:
    - mtu
      - インターフェースで送受信できる最大データ長 (64..1500)
    - energy-saving
      - 省電力機能

設定値	説明
on	省電力機能を有効にする
off	省電力機能を無効にする

- [初期値]:
  - mtu=1500
  - energy-saving=off

**[説明]**

指定した ONU インターフェースの速度と動作モードの種類、およびオプション機能について設定する。

○*mtu*

インターフェースで送受信できる最大データ長を指定する。データ長には MAC ヘッダと FCS は含まれない。

指定できるデータ長の範囲は 64～1500 の範囲となる。

インターフェースの *mtu* を設定して、かつ、**ip mtu** コマンドまたは **ipv6 mtu** コマンドが設定されずデフォルトのままの場合、IPv4 や IPv6 での *mtu* としてはインターフェースの *mtu* が利用される。一方、**ip mtu** コマンドまたは **ipv6 mtu** コマンドが設定されている場合には、インターフェースの *mtu* の設定にかかわらず、**ip mtu** コマンドまたは **ipv6 mtu** コマンドの設定値が *mtu* として利用される。インターフェースの *mtu* も含めてすべて設定されていない時には、デフォルト値である 1500 が利用される。

○省電力機能

on に設定すると EEE (Energy Efficient Ethernet) により通信していない ONU ポートで消費電力を抑えることができる。

この機能を使用するには、接続する機器も EEE をサポートしている必要がある。

**[ノート]**

ONU インターフェースが使用できる場合、本コマンドの実行後、ONU インターフェースのリセットが自動で行われ、その後に設定が有効となる。ONU インターフェースが使用できない場合、本コマンドを実行しても、インターフェースのリセットは行われず、設定の変更のみが行われる。

**[適用モデル]**

NVR700W, NVR510

## 4.53 ONU インターフェースの動作設定

**[書式]**

```
onu shutdown interface
no onu shutdown interface
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: ONU インターフェース名
  - [初期値]: -

**[説明]**

ONU インターフェースを利用できないようにする。このコマンドを設定した ONU インターフェースでは、小型 ONU を接続してもリンクアップしなくなる。

**[適用モデル]**

NVR700W, NVR510

## 4.54 ONU インターフェースのリンクアップ後の送信抑制時間の設定

---

**[書式]**

```
onu linkup send-wait-time interface time
no onu linkup send-wait-time interface [time]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: ONU インターフェース名
  - [初期値]: -
- *time*
  - [設定値]: 送信抑制秒数 (0..10)
  - [初期値]: 0 (抑制しない)

**[説明]**

リンクアップ後の送信抑制時間を設定し、パケットの送信を抑制する。送信を抑制されたパケットはキューに保存され、リンクアップから設定秒数の経過後に送信される。保存先のキュー長は **queue interface length** コマンドの設定に従う。

**[ノート]**

リンクアップ直後に Gratuitous ARP や IPv6 neighbor solicitation 等のパケットがルーターから送信されるが、その送信が早過ぎるために対向機器側で受信できない場合は、この抑制時間を適宜設定し送信を遅延させることで対向機器側で受信できるようになる。

**[適用モデル]**

NVR700W, NVR510

## 4.55 TFTP によりアクセスできるホストの設定

---

**[書式]**

```
tftp host ip_range [ip_range...]
tftp host any
tftp host none
tftp host lan
no tftp host
```

**[設定値及び初期値]**

- *ip\_range*: TFTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
onu1	ONU インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する



設定値	説明
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
  - [設定値]: すべてのホストからのアクセスを許可する
  - [初期値]: -
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: none
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: -

**[説明]**

TFTP サーバーへのアクセスを許可するホストを設定する。

**[ノート]**

セキュリティの観点から、プログラムのリビジョンアップや設定ファイルの読み書きが終了したらすぐに *none* にする。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。  
 IP アドレスの範囲、LAN インターフェース、WAN インターフェース、タグ VLAN インターフェース、lan キーワードは、NVR700W Rev.15.00.03 以降、NVR510 Rev.15.01.03 以降のファームウェアで指定可能。  
 ブリッジインターフェースは NVR700W の Rev.15.00.03 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 4.56 SFTP サーバーへアクセスできるホストの設定

**[書式]**

- ```
sftpd host ip_range [ip_range...]
sftpd host any
sftpd host none
sftpd host lan
no sftpd host
```

**[設定値及び初期値]**

- *ip\_range*: SFTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
  - [設定値]:

| 設定値                                                            | 説明                           |
|----------------------------------------------------------------|------------------------------|
| 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの | 指定したホストからのアクセスを許可する          |
| lanN                                                           | LAN インターフェースからのアクセスを許可する     |
| onu1                                                           | ONU インターフェースからのアクセスを許可する     |
| wan1                                                           | WAN インターフェースからのアクセスを許可する     |
| bridge1                                                        | ブリッジインターフェースからのアクセスを許可する     |
| vlanN                                                          | VLAN インターフェースからのアクセスを許可する    |
| lanN/M                                                         | タグ VLAN インターフェースからのアクセスを許可する |

- [初期値]: -

- *any*
  - [設定値]: すべてのホストからのアクセスを許可する
  - [初期値]: -
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: none
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: -

**[説明]**

SFTP サーバーへのアクセスを許可するホストを設定する。

**[ノート]**

対象となるホストは **sshd host** コマンドでもアクセスが許可されていないなければならない。  
設定後の新しい SFTP 接続から適用される。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

lan キーワードと WAN インターフェースは NVR700W の Rev.15.00.03 以降、NVR510 の Rev.15.01.03 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 4.57 Magic Packet を LAN に中継するか否かの設定

**[書式]**

```
ip interface wol relay relay
```

```
no ip interface wol relay
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *relay*
  - [設定値]:

| 設定値       | 説明                                |
|-----------|-----------------------------------|
| broadcast | Magic Packet をブロードキャストパケットとして中継する |
| unicast   | Magic Packet をユニキャストパケットとして中継する   |
| off       | Magic Packet かどうか検査しない            |

- [初期値]: off

**[説明]**

遠隔地から送信された、ディレクティッドブロードキャスト宛の IPv4 パケットとして構成された MagicPacket を指定した LAN インターフェースに中継する。IPv4 パケットの終点 IP アドレスは指定した LAN インターフェースのディレクティッドブロードキャスト宛でなくてはならない。

broadcast または unicast を指定した場合には、受信したパケットの内容をチェックし、Magic Packet データシーケンスが存在する場合にのみパケットを中継する。

broadcast を指定した場合には、MagicPacket をブロードキャストパケットとして LAN インターフェースに送信する。

unicast を指定した場合には Magic Packet データシーケンスから MAC アドレスを抜きだし、それを終点 MAC アドレスとしたユニキャストパケットとして送信する。

off を指定した場合には、Magic Packet かどうかの検査は行わない。

## [ノート]

いずれの場合も、Magic Packet として中継されなかった場合の packets は、**ip filter directed-broadcast** コマンドの設定に基づき処理される。

## [適用モデル]

NVR700W, NVR510

## 4.58 HTTP リビジョンアップ実行を許可するか否かの設定

## [書式]

```
http revision-up permit permit
no http revision-up permit [permit]
```

## [設定値及び初期値]

- *permit*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

## [説明]

HTTP リビジョンアップを許可するか否かを設定する。

## [ノート]

このコマンドの設定は、コマンドによる直接の HTTP リビジョンアップ、Web GUI からのリビジョンアップ、DOWNLOAD ボタンによるリビジョンアップに影響する。

## [適用モデル]

NVR700W, NVR510

## 4.59 HTTP リビジョンアップ用 URL の設定

## [書式]

```
http revision-up url url
no http revision-up url [url]
```

## [設定値及び初期値]

- *url*
  - [設定値]: ファームウェアが置いてある URL を設定する
  - [初期値]: `http://www.rtpro.yamaha.co.jp/firmware/revision-up/(機種名).bin`

## [説明]

HTTP リビジョンアップとしてファームウェアが置いてある URL を設定する。

入力形式は“`http://サーバーの IP アドレスあるいはホスト名/パス名`”という形式となる。

サーバーのポート番号が 80 以外の場合は、“`http://サーバーの IP アドレスあるいはホスト名:ポート番号/パス名`”という形式で、URL の中に指定する必要がある。

## [適用モデル]

NVR700W, NVR510

## 4.60 HTTP リビジョンアップ用 Proxy サーバーの設定

## [書式]

```
http revision-up proxy proxy_server [port]
no http revision-up proxy [proxy_server [port]]
```

## [設定値及び初期値]

- *proxy\_server*

- [設定値]: HTTP リビジョンアップ時に使用する Proxy サーバー
- [初期値]: -
- *port*
  - [設定値]: Proxy サーバーのポート番号
  - [初期値]: -

**[説明]**

Proxy サーバーのホスト名または、IP アドレスとポート番号を指定する。

**[適用モデル]**

NVR700W, NVR510

## 4.61 HTTP リビジョンアップ処理のタイムアウトの設定

---

**[書式]**

```
http revision-up timeout time
no http revision-up timeout [time]
```

**[設定値及び初期値]**

- *time*
  - [設定値]: タイムアウト時間 (秒)
  - [初期値]: 30

**[説明]**

HTTP リビジョンアップ処理のタイムアウト時間を設定する。

**[適用モデル]**

NVR700W, NVR510

## 4.62 リビジョンダウンを許可するか否かの設定

---

**[書式]**

```
http revision-down permit permit
no http revision-down permit [permit]
```

**[設定値及び初期値]**

- *permit*
  - [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | 現在のリビジョンより古いリビジョンへのリビジョンダウンを許可する  |
| off | 現在のリビジョンより古いリビジョンへのリビジョンダウンを許可しない |

- [初期値]: off

**[説明]**

HTTP リビジョンアップ機能にて、現在のリビジョンよりも古いリビジョンへのファームウェアのリビジョンダウンを許可するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 4.63 DOWNLOAD ボタンによるリビジョンアップ操作を許可するか否かの設定

---

**[書式]**

```
operation http revision-up permit permit
no operation http revision-up permit [permit]
```

**[設定値及び初期値]**

- *permit*

- [設定値]:

| 設定値 | 説明                              |
|-----|---------------------------------|
| on  | DOWNLOAD ボタンによるリビジョンアップ操作を許可する  |
| off | DOWNLOAD ボタンによるリビジョンアップ操作を許可しない |

- [初期値]: off

**[説明]**

DOWNLOAD ボタンによりファームウェアのリビジョンアップ機能を使用するか否かを設定する。

**[ノート]**

リビジョンアップ機能は HTTP リビジョンアップ機能に準ずる。

**[適用モデル]**

NVR700W, NVR510

## 4.64 リビジョンアップ実行のスケジュール

**[書式]**

```
http revision-up schedule period time1 time2
http revision-up schedule startup
no http revision-up schedule [period time1 time2]
no http revision-up schedule startup
```

**[設定値及び初期値]**

- *period*: ファームウェアのリビジョンアップを試みるスケジュールを設定する。

- [設定値]:

| 設定値                 | 説明                                                                 |
|---------------------|--------------------------------------------------------------------|
| daily               | 毎日                                                                 |
| weekly <i>day</i>   | 毎週<br><i>day</i> は曜日を表す文字列で、以下のいずれか<br>sun,mon,tue,wed,thu,fri,sat |
| monthly <i>date</i> | 毎月<br><i>date</i> は 1~31 の数字で月内の日を表す                               |

- [初期値]: -
- *time1,time2*: リビジョンアップを試みる時間帯を設定する。
  - [設定値]: *time1,time2* は 24 時間制で、HH:MM 形式で指定する。
  - [初期値]: -

**[説明]**

ファームウェアのリビジョンアップを試みるスケジュールを設定する。

*period* ではリビジョンアップを試みる間隔を指定する。毎日、毎週、毎月の指定をそれぞれ、daily、weekly、monthly で指定する。weekly、monthly の場合はそれぞれ曜日、日の指定が必要になる。

monthly の場合で、指定した日とその月に存在しない場合には、その月にはリビジョンアップは試みられない。たとえば、'monthly 31' と指定した場合、31 日が存在しない 2 月、4 月、6 月、9 月、11 月にはリビジョンアップは試みられない。

*time1*、*time2* ではリビジョンアップを試みる時間帯を設定する。*time1* で指定した時刻から *time2* で指定した時刻の間のランダムな時刻に 1 回だけ、リビジョンアップを試みる。そこでリビジョンアップできなかった場合には、次の日/週/月までリビジョンアップは行われない。

*time1* で指定した時刻が *time2* で指定した時刻より遅い場合には、*time2* は翌日の時刻と解釈される。

**http revision-up schedule startup** コマンドでは起動時に 1 回だけ、リビジョンアップを試みる。そこでリビジョンアップできなかつた場合には、次の起動までリビジョンアップは行われない。

**http revision-up permit** コマンドで HTTP リビジョンアップを許可されていない時は、ファームウェアのリビジョンアップは行わない。

**http revision-down permit** コマンドでリビジョンダウンが許可されている場合は、WEB サーバーにおいてあるファームウェアが現在のファームウェアよりも古いリビジョンであってもファームウェアの書き換えを行う。

なお、WEB サーバーにおいてあるファームウェアが現在のファームウェアと同一リビジョンの場合には、ファームウェアの書き換えは行わない。

[ノート]

startup は NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降のファームウェアで使用可能。

[設定例]

```
http revision-up schedule daily 23:00 02:00 # 毎日、23 時から翌日 2 時までの間
http revision-up schedule weekly sun 12:00 13:00 # 日曜日の昼 12 時から 13 時までの間
http revision-up schedule monthly 1 23:00 0:00 # 毎月 1 日の 23 時から 24 時までの間
http revision-up schedule startup # 起動時
```

[適用モデル]

NVR700W, NVR510

## 4.65 SSH サーバー機能の ON/OFF の設定

[書式]

```
ssh service service
```

```
no ssh service [service]
```

[設定値及び初期値]

- service*

- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | SSH サーバー機能を有効にする |
| off | SSH サーバー機能を停止させる |

- [初期値]: off

[説明]

SSH サーバー機能の利用を選択する。

[ノート]

SSH サーバー機能が停止している場合、SSH サーバーはアクセス要求に一切応答しない。

[適用モデル]

NVR700W, NVR510

## 4.66 SSH サーバー機能の listen ポートの設定

[書式]

```
ssh listen port
```

```
no ssh listen [port]
```

[設定値及び初期値]

- port*

- [設定値]: SSH サーバー機能の待ち受け (listen) ポート番号 (1..65535)

- [初期値]: 22

[説明]

SSH サーバーの listen ポートを選択する。

## [ノート]

SSH サーバーは、TCP の 22 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。

## [適用モデル]

NVR700W, NVR510

## 4.67 SSH サーバーへアクセスできるホストの設定

## [書式]

**sshd host** *ip\_range* [*ip\_range...*]

**sshd host** *any*

**sshd host** *none*

**sshd host** *lan*

**no sshd host**

## [設定値及び初期値]

- *ip\_range* : SSH サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値] :

| 設定値                                                            | 説明                           |
|----------------------------------------------------------------|------------------------------|
| 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの | 指定したホストからのアクセスを許可する          |
| lanN                                                           | LAN インターフェースからのアクセスを許可する     |
| onu1                                                           | ONU インターフェースからのアクセスを許可する     |
| wan1                                                           | WAN インターフェースからのアクセスを許可する     |
| bridge1                                                        | ブリッジインターフェースからのアクセスを許可する     |
| vlanN                                                          | VLAN インターフェースからのアクセスを許可する    |
| lanN/M                                                         | タグ VLAN インターフェースからのアクセスを許可する |

- [初期値] : -
- *any*
  - [設定値] : すべてのホストからのアクセスを許可する
  - [初期値] : *any*
- *none*
  - [設定値] : すべてのホストからのアクセスを禁止する
  - [初期値] : -
- *lan*
  - [設定値] : すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値] : -

## [説明]

SSH サーバーへのアクセスを許可するホストを設定する。

## [ノート]

設定後の新しい SSH 接続から適用される。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

lan キーワードと WAN インターフェースは NVR700W の Rev.15.00.03 以降、NVR510 の Rev.15.01.03 以降で指定可能。

## [適用モデル]

NVR700W, NVR510

## 4.68 SSH サーバーへ同時に接続できるユーザー数の設定

---

### [書式]

```
ssh session num
no ssh session [num]
```

### [設定値及び初期値]

- *num*
  - [設定値]: 同時接続数 (1..8)
  - [初期値]: 8

### [説明]

SSH に同時に接続できるユーザー数を設定する。

### [ノート]

設定を変更したときに変更した値よりも多くのユーザーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー数が設定値より少なくなるまで新たな接続は許可しない。

### [適用モデル]

NVR700W, NVR510

## 4.69 SSH サーバーホスト鍵の設定

---

### [書式]

```
ssh host key generate [bit=bit]
no ssh host key generate [...]
```

### [設定値及び初期値]

- *bit*
  - [設定値]: 鍵のビット長(1024, 2048)
  - [初期値]: 2048

### [説明]

SSH サーバーのホスト鍵を設定する。

bit パラメーターによって、生成する鍵のビット数を指定できる。

### [ノート]

SSH サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。

既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザーに対してホスト鍵を更新するか否かを確認する。

ホスト鍵の生成には、機種によって異なるが、1024 ビット鍵では数秒から 数分程度、2048 ビット鍵では数分から十数分程度の時間がかかる。

TFTP で設定を取得した場合は、**ssh host key generate [bit=bit] KEY1 KEY2 KEY3** という形式で保存される。

KEY1 ~ KEY3 は、秘密鍵を機器固有の方式で暗号化した文字列である。

### [適用モデル]

NVR700W, NVR510

## 4.70 SSH サーバーホスト鍵の表示

---

### [書式]

```
show sshd host key [type=fingerprint [hash_algorithm]]
```

### [設定値及び初期値]

- *fingerprint*: 鍵指紋を表示することを示すキーワード
  - [初期値]: -
- *hash\_algorithm*: 鍵指紋を表示する際に使用するハッシュ関数のアルゴリズム



- [設定値]:

| 設定値    | 説明      |
|--------|---------|
| md5    | MD5     |
| sha256 | SHA-256 |

- [初期値]: sha256

#### [説明]

SSH サーバーのホスト鍵を表示する。

*fingerprint* キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

NVR510 は Rev.15.01.16 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 4.71 SSH サーバーで利用可能な暗号アルゴリズムの設定

#### [書式]

```
sshd encrypt algorithm algorithm [algorithm ...]
```

```
no sshd encrypt algorithm [...]
```

#### [設定値及び初期値]

- *algorithm*: 暗号アルゴリズム (空白で区切って複数指定可能)

- [設定値]:

| 設定値          | 説明                                                                           |
|--------------|------------------------------------------------------------------------------|
| aes128-ctr   | AES128-CTR                                                                   |
| aes192-ctr   | AES192-CTR                                                                   |
| aes256-ctr   | AES256-CTR                                                                   |
| aes128-cbc   | AES128-CBC                                                                   |
| aes192-cbc   | AES192-CBC                                                                   |
| aes256-cbc   | AES256-CBC                                                                   |
| 3des-cbc     | 3DES-CBC                                                                     |
| blowfish-cbc | Blowfish-CBC (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応) |
| cast128-cbc  | CAST-128-CBC (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応) |
| arcfour      | Arcfour (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応)      |

- [初期値]: aes128-ctr aes192-ctr aes256-ctr

#### [説明]

SSH サーバーで利用可能な暗号アルゴリズムを設定する。

*algorithm* で指定した暗号アルゴリズムのリストを SSH 接続時にクライアントへ提案する。

#### [ノート]

*algorithm* で指定した暗号アルゴリズムをクライアントがサポートしていない場合には、そのクライアントと SSH による接続ができない。

[適用モデル]  
NVR700W, NVR510

## 4.72 SSH クライアントの生存確認

### [書式]

```
sshd client alive switch [interval [count]]
no sshd client alive [switch ...]
```

### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | クライアントの生存確認を行う   |
| off | クライアントの生存確認を行わない |

- [初期値]: off
- *interval*
  - [設定値]: 送信間隔の秒数 (1..2147483647)
  - [初期値]: 100
- *count*
  - [設定値]: 試行回数 (1..2147483647)
  - [初期値]: 3

### [説明]

クライアントの生存確認を行うか否かを設定する。

クライアントに *interval* で設定した間隔で応答を要求するメッセージを送る。 *count* で指定した回数だけ連続して応答がなかったら、このクライアントとの接続を切り、セッションを終了する。

[適用モデル]  
NVR700W, NVR510

## 4.73 SSH サーバー応答に含まれる OpenSSH のバージョン情報の非表示設定

### [書式]

```
sshd hide openssh version use
no sshd hide openssh version [use]
```

### [設定値及び初期値]

- *use*
  - [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | SSH バージョン情報を表示しない |
| off | SSH バージョン情報を表示する  |

- [初期値]: off

### [説明]

SSH 接続時のサーバー応答に含まれる OpenSSH のバージョン情報を表示するか否かを設定する。このコマンドはセキュリティ目的として OpenSSH のバージョン情報を隠したい場合に使用する。このコマンドを on に設定した場合は、"SSH-2.0-OpenSSH" と通知する。

### [ノート]

このバージョン情報は、SSH 接続時にサーバーとクライアントのプロトコルの互換性を調整するために使用される。このコマンドを ON に設定することにより、クライアントソフトによっては、接続できなくなる可能性がある。その場合には、クライアントソフトを変更するか、このコマンドを OFF に設定する。

[適用モデル]  
NVR700W, NVR510

## 4.74 SSH サーバーで利用可能な認証方式の設定

### [書式]

```
sshd auth method all
sshd auth method method [method]
no sshd auth method [...]
```

### [設定値及び初期値]

- *all*: パスワード認証、および、公開鍵認証を受け入れる
  - [初期値]: all
- *method*
  - [設定値]:

| 設定値       | 説明            |
|-----------|---------------|
| password  | パスワード認証を受け入れる |
| publickey | 公開鍵認証を受け入れる   |

- [初期値]: -

### [説明]

SSH サーバーで利用可能な認証方式を設定する。  
パスワード認証より公開鍵認証が安全な認証方式である。

### [ノート]

本コマンドが使用できないファームでは、**sshd auth method password** 相当の動作となります。  
NVR700W は Rev.15.00.17 以降で使用可能。  
NVR510 は Rev.15.01.16 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 4.75 SSH サーバーの公開鍵認証に用いる公開鍵情報を保存するファイルの設定

### [書式]

```
sshd authorized-keys filename [user] path=path
no sshd authorized-keys filename [user] [path=path]
```

### [設定値及び初期値]

- *user*: 登録されているユーザー名
  - [初期値]: -
- *path*: SSH クライアントの公開鍵を格納したファイル名
  - [初期値]:
    - /ssh/authorized\_keys/ユーザー名 (登録されているユーザーの場合)
    - /ssh/authorized\_keys/no.name (無名ユーザーの場合)

### [説明]

SSH クライアントの公開鍵を格納したファイル (authorized\_keys ファイル) を設定する。ユーザーが公開鍵認証する際に使用する。

本コマンドを設定する場合、無名ユーザー以外は事前に **login user** コマンドでユーザーを登録しておく必要がある。登録されていないユーザーに対して本コマンドを設定するとエラーになる。

*user* を省略した場合は、無名ユーザーに対する設定となる。

公開鍵認証を使用する場合は、あらかじめ許可する SSH クライアントの公開鍵をファイルに格納しておく必要がある。対応しているファイルのフォーマットは以下のとおり。

- 各行にひとつの公開鍵を格納する。
- 1つの公開鍵は、"(公開鍵の種類) (base64 エンコードされた鍵本体) (鍵のコメント)"の順に記載する。
- ファイルには 33 個まで公開鍵を登録できる。34 個目以降の公開鍵は無視する。
- 空行や#で始まる行は無視する。
- 1行の長さは、4094 文字 (改行コードを除く) まで対応する。4094 文字より長い行は無視する。
- 改行コードは、CR+LF、LF、CR に対応する。最終行の場合は改行がなくてもよい。
- ファイルの文字コードは、ASCII に対応する。
- 公開鍵の種類には、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384、ecdsa-sha2-nistp521、ssh-ed25519、ssh-dss、ssh-rsa(\*) を設定できる。
  - ※ssh-rsa の鍵長は、1024bit、2048bit、4096bit に対応する。
- OpenSSH の authorized\_keys ファイルではオプションを指定できるが対応しない。オプションの記載は無視する。

[サンプル]

例:RSA 2048bit の公開鍵の場合

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAp3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
1ZyaKDKf8BiiCsKnvFsLI fSgcOejllflBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNwCYCa1Y0Ign8u8O
zVx1dx1QABZuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkggrMxg40feB+0hjS
+K2eY49uqqwqYUYCdNw6bTIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmtl0//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

例:ECDSA 256bit の公開鍵の場合

```
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP211Vy
IP8Bg+r8rZhNmRq+ber0+sOaYCsvm5TN1CGt5WpCNkpwkV3c3rxwA6GAgGxuJsSn4J6Bo1mABhHg+YH
M= user2
```

**login user** コマンドで登録されていないユーザーから接続された場合は、無名ユーザーとして公開鍵認証を試みる。

[ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

NVR510 は Rev.15.01.16 以降で使用可能。

[適用モデル]

NVR700W, NVR510

## 4.76 SSH サーバーの公開鍵認証に用いる公開鍵の設定

[書式]

```
import sshd authorized-keys [user]
```

[設定値及び初期値]

- *user*
  - [設定値]: 登録されているユーザー名
  - [初期値]: -

[説明]

SSH クライアントの公開鍵を格納したファイル (authorized\_keys ファイル) に設定を追加する。

本コマンドを実行する場合、無名ユーザー以外は事前に **login user** コマンドでユーザーを登録しておく必要がある。登録されていないユーザーに対して本コマンドを設定するとエラーになる。

*user* を省略した場合は、無名ユーザーに対する設定となる。

**sshd authorized-keys filename** コマンドで指定した authorized\_keys ファイルに対して設定を追加する。

authorized\_keys ファイルやディレクトリが存在しない場合は、新規に作成する。

コマンド入力後にプロンプトに応じて公開鍵を 1 つ入力する。入力した公開鍵が、authorized\_keys ファイルに追加書き込みされる。公開鍵は、"(公開鍵の種類) (base64 エンコードされた鍵本体) (鍵のコメント)"の順に記載する。4094 文字まで入力できる。

公開鍵のフォーマットは、**sshd authorized-keys filename** コマンドと同様である。

authorized\_keys ファイルを削除または初期化したいときは、**delete** コマンドを使用する。

## [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

NVR510 は Rev.15.01.16 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 4.77 SSH サーバーの公開鍵認証に用いる公開鍵の表示

## [書式]

```
show sshd authorized-keys [user] [type=fingerprint [hash_algorithm]]
```

```
show sshd authorized-keys * [type=fingerprint [hash_algorithm]]
```

## [設定値及び初期値]

- *user* : 登録されているユーザー名
  - [初期値] :-
- *fingerprint* : 鍵指紋を表示することを示すキーワード
  - [初期値] :-
- *hash\_algorithm* : 鍵指紋を表示する際に使用するハッシュ関数のアルゴリズム
  - [設定値] :

| 設定値    | 説明      |
|--------|---------|
| md5    | MD5     |
| sha256 | SHA-256 |

- [初期値] : sha256
- \* : 全ユーザー
  - [初期値] :-

## [説明]

SSH クライアントの公開鍵を格納したファイル (*authorized\_keys* ファイル) を表示する。

*fingerprint* を指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

第 1 書式では、ユーザーに対応した *authorized\_keys* ファイルを表示する。*user* を省略した場合は、無名ユーザーの情報を表示する。

第 2 書式では、全ユーザーの *authorized\_keys* ファイルを表示する。

## [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

NVR510 は Rev.15.01.16 以降で使用可能。

## [設定例]

例: RSA 2048bit の公開鍵を表示する場合

```
# show sshd authorized-keys user1
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAp3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
1ZyaKDKf8BiiCsKnvFsLI fSgcOejllf1BtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNWcYCaLY0Ign8u8O
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hjs
+K2eY49uqqwqYUYCdNw6bTIIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmt10//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

例:RSA 2048bit の公開鍵の鍵指紋を SHA-256 で表示した場合

```
# show sshd authorized-keys user1 type=fingerprint sha256
2048 SHA256:uk2janKfeZXBsUniTmdNwL2fhdcAdfY0MsGSsCtpg8E user1 (RSA)
```

例:RSA 2048bit の公開鍵の鍵指紋を MD5 で表示した場合

```
# show sshd authorized-keys user1 type=fingerprint md5
2048 MD5:6e:fe:21:cc:d2:a4:55:78:07:7f:7f:f7:59:17:56:3a user1 (RSA)
```

例:全ユーザーを表示した場合

```
# 無名ユーザーと user1, user2, user3 が存在している。
# user2 は、sshd authorized-keys filename コマンドでファイルの置き場所を変更している。
# user3 は、authorized_keys ファイルが存在しない。

# show sshd authorized-keys * type=fingerprint sha256
(noname) /ssh/authorized_keys/no.name
2048 SHA256:fMlGwY5YlQvz9xEObkDXaO7TuvIlgFIAkmV0K2MGbyU (RSA)

user1 /ssh/authorized_keys/user1
2048 SHA256:uk2janKfeZXBsUnitMdNwL2fhdcAdfy0MsGSsCtpg8E user1 (RSA)

user2 /pub-key
2048 SHA256:Ul7sScopCUNPA5IndPWzHhkANqr3PkD2k3GMv0qS5NA user2 (RSA)

user3 /ssh/authorized_keys/user3
/ssh/authorized_keys/user3 : ファイルデータの読み込みに失敗しました。 : No such
file or directory
```

## [適用モデル]

NVR700W, NVR510

## 4.78 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定

## [書式]

**alarm entire switch****no alarm entire**

## [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

## [説明]

有効になっているアラーム音を鳴らすか全く鳴らさないかを選択する。

## [適用モデル]

NVR700W, NVR510

## 4.79 TEL ポートでの接続・切断時にアラーム音を鳴らすか否かの設定

## [書式]

**alarm connection analog switch****no alarm connection analog**

## [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: off

## [説明]

TEL ポートでの内線通話を除く接続・切断時にアラーム音を鳴らすか否かを選択する。

## [適用モデル]

NVR700W, NVR510

## 4.80 データ通信での接続・切断時にアラーム音を鳴らすか否かの設定

### [書式]

**alarm connection data** *switch*

**no alarm connection data**

### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

### [説明]

データ通信での接続・切断時にアラーム音を鳴らすか否かを選択する。

### [適用モデル]

NVR700W, NVR510

## 4.81 攻撃を検知した時にアラーム音を鳴らすか否かの設定

### [書式]

**alarm intrusion** *switch*

**no alarm intrusion**

### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

### [説明]

攻撃を検知した時にアラーム音を鳴らすか否かを選択する。

### [適用モデル]

NVR700W, NVR510

## 4.82 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定

### [書式]

**alarm usbhost** *switch*

**no alarm usbhost**

### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

### [説明]

USB ホスト機能に関連するアラーム音を鳴らすか否かを選択する。

[適用モデル]  
NVR700W, NVR510

#### 4.83 microSD 機能に関連するアラームを鳴らすか否かの設定

[書式]

**alarm sd** *switch*  
**no alarm sd** [*switch*]

[設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

[説明]

microSD 機能に関連するアラームを鳴らすかどうかを設定する。

[適用モデル]  
NVR700W, NVR510

#### 4.84 内蔵無線 WAN 機能に関連するアラーム音を鳴らすか否かの設定

[書式]

**alarm wwan** *switch*  
**no alarm wwan**

[設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

[説明]

内蔵無線 WAN 機能に関連するアラーム音を鳴らすか否かを選択する。

[適用モデル]  
NVR700W

#### 4.85 バッチファイル実行機能に関連するアラーム音を鳴らすか否かの設定

[書式]

**alarm batch** *switch*  
**no alarm batch**

[設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on



**[説明]**

バッチファイル実行機能に関連するアラーム音を鳴らすか否かを選択する。

**[適用モデル]**

NVR700W, NVR510

**4.86 起動時のアラーム音を鳴らすか否かの設定****[書式]**

**alarm startup switch** [*pattern*]

**no alarm startup** [*switch*]

**[設定値及び初期値]**• *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

• *pattern*

- [設定値]: アラーム音のパターン (1...3、省略時は 1)
- [初期値]: -

**[説明]**

起動時にアラーム音を鳴らすか否かを選択する。

**[適用モデル]**

NVR700W, NVR510

**4.87 HTTP リビジョンアップ機能に関連するアラームを鳴らすか否かの設定****[書式]**

**alarm http revision-up switch**

**no alarm http revision-up** [*switch*]

**[設定値及び初期値]**• *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

**[説明]**

HTTP リビジョンアップ機能に関連するアラームを鳴らすかどうかを設定する。

**[適用モデル]**

NVR700W, NVR510

**4.88 エコーキャンセラー制御方法の設定****[書式]**

**audio echo-canceller port=*port* mode [*length* [*nlp=*nlp*]*] [*cng=*cng*]*] [*nlc=*nlc*]*]**

**no audio echo-canceller port=*port***

**[設定値及び初期値]**• *port*

- [設定値]:

| 設定値  | 説明       |
|------|----------|
| tel1 | TEL1 ポート |
| tel2 | TEL2 ポート |

- [初期値]: -
- *mode*
- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| auto | 自動設定          |
| off  | エコーキャンセラー OFF |

- [初期値]: auto
- *length*
- [設定値]: エコーキャンセラーテール長( 16..128: ミリ秒)
- [初期値]: 16
- *nlp*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | NLP 機能有効 |
| off | NLP 機能無効 |
| 省略  | 省略時は on  |

- [初期値]: on
- *cng*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | CNG 機能有効 |
| off | CNG 機能無効 |
| 省略  | 省略時は on  |

- [初期値]: on
- *nlc*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | NLC 機能有効 |
| off | NLC 機能無効 |
| 省略  | 省略時は on  |

- [初期値]: on

#### [説明]

ポート毎のエコーキャンセラー制御方法を設定する。

*mode* パラメーターを *auto* に指定した場合、通常はエコーキャンセラー機能が ON で動作して、ファックスの開始音を検出したときには、その呼が終了するまではエコーキャンセラー機能が OFF で動作する。

NLP (NonLinear Processing) 機能を *on* に指定すると、対向からの音声がある場合には、TEL ポートから対向に送られる音声を抑制する。

CNG(Comfort Noise Generation) 機能を *on* に指定すると、対向からの音声があるときに TEL ポートから対向に送られる音声を抑制した場合に、対向に送られる音声に環境雑音と同程度のノイズを加えることによって、音声抑制切替による不自然さを軽減することができる。

NLC(Non-Linearity Corrector) 機能を *on* に指定すると、エコーキャンセラー機能で処理される音に歪みがあっても処理できる。

## [ノート]

*nlp* のパラメーターを省略した場合、**nlp=on** で設定される。  
*cng* のパラメーターを省略した場合、**cng=on** で設定される。  
*nlc* のパラメーターを省略した場合、**nlc=on** で設定される。

従来機種とは *length* パラメーターの設定範囲が異なる。  
 従来機種の設定を流用する場合、設定値そのままでは読み込むことのできない場合があるので注意が必要。

## [設定例]

- TEL1 ポートのエコーキャンセラーを OFF とする  

```
# audio echo-canceller port=tel1 off
```
- TEL1 ポートのエコーキャンセラーの設定値をデフォルト値に戻す  

```
# no audio echo-canceller port=tel1
```

## [適用モデル]

NVR700W, NVR510

## 4.89 エコーキャンセラーの NLP 閾値の設定

## [書式]

```
audio echo-canceller nlp threshold port=port threshold
```

```
no audio echo-canceller nlp threshold port=port
```

## [設定値及び初期値]

- *threshold*
  - [設定値]: 閾値 (-10db..-60db)
  - [初期値]: -35db
- *port*
  - [設定値]:

| 設定値  | 説明       |
|------|----------|
| tel1 | TEL1 ポート |
| tel2 | TEL2 ポート |

- [初期値]: -

## [説明]

エコーキャンセラーの NLP(NonLinear Processing) 閾値を設定する。

## [ノート]

NLP 閾値はポート毎の設定となる。

従来機種とは *threshold* パラメーターの設定範囲が異なる。  
 従来機種の設定を流用する場合、設定値そのままでは読み込むことができないので注意が必要。

## [設定例]

TEL1 ポートのエコーキャンセラーの NLP 閾値を -60db に設定する。

```
audio echo-canceller nlp threshold port=tel1 -60db
```

## [適用モデル]

NVR700W, NVR510

## 4.90 エコーキャンセラーを無効にする音の設定

## [書式]

```
audio echo-canceller disabler mode
```

```
no audio echo-canceller disabler
```

## [設定値及び初期値]

- *mode*

- [設定値]:

| 設定値                 | 説明                            |
|---------------------|-------------------------------|
| 2100hz              | 2100Hz 検出でエコーキャンセラー無効         |
| with-phase-reversal | 位相反転ありの 2100Hz 検出でエコーキャンセラー無効 |

- [初期値]: 2100hz

#### [説明]

エコーキャンセラーを無効にする音の種類を設定する。

#### [ノート]

音の種類は機器全体で単一の設定となる。

#### [適用モデル]

NVR700W, NVR510

## 4.91 ジッタバッファ制御方法の設定

#### [書式]

```
audio jitter-buffer port=port mode length [min=min]
```

```
no audio jitter-buffer port=port
```

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値  | 説明       |
|------|----------|
| tel1 | TEL1 ポート |
| tel2 | TEL2 ポート |

- [初期値]: -

- *mode*

- [設定値]:

| 設定値  | 説明   |
|------|------|
| auto | 自動設定 |
| fix  | 固定長  |

- [初期値]: auto

- *length*

- [設定値]: ジッタバッファ長パラメーター( 10..500: ミリ秒単位)

- [初期値]: 250

- *min*

- [設定値]: 最小ジッタバッファ長パラメーター( 0..500: ミリ秒単位)

- [初期値]: 10

#### [説明]

ポート毎のジッタバッファ制御方法を設定する。

#### [ノート]

auto の場合、通常は適応バッファモードで制御を行い、ファックスの開始音を検出したら、その呼が終了するまで固定長モードで動作する。

*length* で設定する値は、fix の場合ジッタバッファ長の収束値となり、auto の場合ジッタバッファ長の初期値に反映される。

*min* で設定する値は、auto の場合の最小ジッタバッファ長になる。

#### [設定例]

- TEL1 ポートのジッタバッファを固定、収束値を 200 ミリ秒とする

```
# audio jitter-buffer port=tell fix 200
```

- TEL1 インターフェースのジッタバッファの設定値を初期値に戻す

```
# no audio jitter-buffer port=tell
```

#### [適用モデル]

NVR700W, NVR510

## 4.92 RTP パケットのパケット長を設定

---

### [書式]

```
audio rtp segsize length
```

```
no audio rtp segsize
```

### [設定値及び初期値]

- *length*
  - [設定値]: RTP パケット長(msec) (10 / 20 / 30)
  - [初期値]: 20

### [説明]

RTP パケットのパケット長を設定する。

### [ノート]

インターネット電話・カスケード接続すべての RTP パケット長が一律に設定される。カスケード接続を使用して、カスケード子機からインターネット電話を行う場合、親機・子機共に同じパケット長に設定しておく必要がある。

従来機種とは *length* パラメーターの設定範囲が異なる。

従来機種の設定を流用する場合、設定値そのままでは読み込むことができないので注意が必要。

### [設定例]

- RTP のパケット長を 30msec に設定する

```
# audio rtp segsize 30
```

#### [適用モデル]

NVR700W, NVR510

## 4.93 RTP/RTCP で使用するポート番号の設定

---

### [書式]

```
audio rtp port port
```

```
no audio rtp port
```

### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号 (6000 ... 65000)
  - [初期値]: 5004

### [説明]

RTP および RTCP で使用するポート番号を設定する。

設定したポート番号から機器で必要な分のポート数を確保する。

設定できるポート番号は偶数に限る。

他のアプリケーション等で使用するポート番号と重ならないように注意する必要がある。

また、この設定を変更した場合は、NAT や FILTER の設定を見直す必要がある。

通話中は設定を変更できない。

#### [適用モデル]

NVR700W, NVR510

## 4.94 SCP クライアント

### [書式]

```
scp [[user@]host:]file1 [[user@]host:]file2 [port]
```

### [設定値及び初期値]

- *user*
  - [設定値]: リモートホストにログインする際に使用するユーザー名
  - [初期値]: -
- *host*
  - [設定値]: リモートホストのホスト名、または IP アドレス
  - [初期値]: -
- *file1*
  - [設定値]: 転送元ファイル名
  - [初期値]: -
- *file2*
  - [設定値]: 転送先ファイル名
  - [初期値]: -
- *port*
  - [設定値]: リモートホストのポート番号
  - [初期値]: 22

### [説明]

SCP を実行する。

*file1* または *file2* のどちらか一方はリモートホスト上のファイルを指定し、もう一方にはルーターのファイルシステムにあるファイルを指定する。

*file1*、*file2* の両方にリモートホストのファイルを指定することはできない。

同様に *file1*、*file2* の両方にルーターのファイルシステムにあるファイルを指定することはできない。

RTFS および外部メモリにあるファイルを指定する場合、*user* および *host* を省略し *file* のみを絶対パスで指定する。

ルーターの設定ファイル (*config*、*config0*~*config4*) やファームウェア (*exec*、*exec0*、*exec1*) を指定する場合には、*file* に "*config*" や "*exec0*" のようにファイル名のみを指定する。

*host* に IPv6 アドレスを指定する場合には、"*[*"、"*]*" で IP アドレスを囲む。

実行例は以下の通り。

リモートホスト (192.168.1.1) から、ルーターの *exec0* にファイルをコピーする。

```
# scp user@192.168.1.1:nvr700w.bin exec0
```

ルーター上のファイル *usb1:/log.txt* を、リモートホスト (2001:1::1) へコピーする。

```
# scp usb1:/log.txt user@[2001:1::1]:log.txt
```

### [適用モデル]

NVR700W, NVR510

## 4.95 SSH クライアント

### [書式]

```
ssh [-p port] [-e escape] [user@]host
```

### [設定値及び初期値]

- *port*
  - [設定値]: リモートホストのポート番号
  - [初期値]: 22
- *escape*
  - [設定値]: エスケープ文字の文字コード (0 ... 255)
  - [初期値]: 126 (~)
- *user*

- [設定値]: リモートホストにログインする際に使用するユーザー名
- [初期値]: -
- *host*
  - [設定値]: リモートホストのホスト名、または IP アドレス
  - [初期値]: -

**[説明]**

SSH を実行し、指定したホストにリモートログインする。

*user* を省略した場合、ルーターにログインした際に入力したユーザー名を使用して SSH サーバーへのアクセスを試みる。

*host* に IPv6 アドレスを指定する場合には、"`[`"、"`]`" で IP アドレスを囲む。

*escape* で指定したエスケープ文字は行頭に入力されたときだけ、エスケープ文字として認識される。エスケープ文字に続けてピリオド(.)が入力された場合、強制的に接続を閉じる。行頭からエスケープ文字を 2 回続けて入力した場合には、この文字が 1 回だけサーバーに送られる。

実行例は以下の通り。

リモートホスト (192.168.1.1、ポート:10022) へアクセスする。

```
# ssh -p 10022 user@192.168.1.1
```

リモートホスト (2001:1::1) へアクセスする。

```
# ssh user@[2001:1::1]
```

**[適用モデル]**

NVR700W, NVR510

## 4.96 SSH クライアントで利用可能な暗号アルゴリズムの設定

**[書式]**

`ssh encrypt algorithm algorithm [algorithm...]`

`no ssh encrypt algorithm [algorithm...]`

**[設定値及び初期値]**

- *algorithm*: 暗号アルゴリズム(空白で区切って複数指定可能)
- [設定値]:

| 設定値          | 説明                                                                           |
|--------------|------------------------------------------------------------------------------|
| aes128-ctr   | AES128-CTR                                                                   |
| aes192-ctr   | AES192-CTR                                                                   |
| aes256-ctr   | AES256-CTR                                                                   |
| aes128-cbc   | AES128-CBC                                                                   |
| aes192-cbc   | AES192-CBC                                                                   |
| aes256-cbc   | AES256-CBC                                                                   |
| 3des-cbc     | 3DES-CBC                                                                     |
| blowfish-cbc | Blowfish-CBC (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応) |
| cast128-cbc  | CAST-128-CBC (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応) |
| arcfour      | Arcfour (NVR700W の Rev.15.00.16 以降、および、NVR510 の Rev.15.01.15 以降 では 非対応)      |

- [初期値]: aes128-ctr aes192-ctr aes256-ctr

**[説明]**

SCP クライアントで利用可能な暗号アルゴリズムを設定する。

*algorithm* で指定した暗号アルゴリズムのリストを SSH 接続時にサーバーに提案する。

[ノート]

*algorithm* で指定した暗号アルゴリズムをサーバーがサポートしていない場合には、そのサーバーと SSH による接続ができない。

[適用モデル]

NVR700W, NVR510

## 4.97 SSH サーバーの公開鍵情報を保存するファイルの設定

---

[書式]

**ssh known hosts** *file*

**no ssh known hosts** [*file*]

[設定値及び初期値]

- *file*
  - [設定値]: SSH サーバーの公開鍵情報を保存するファイル名
  - [初期値]: /ssh/known\_hosts

[説明]

SSH サーバーの公開鍵情報を保存するファイルを指定する。

[適用モデル]

NVR700W, NVR510



## 第 5 章

### ヤマハルーター用ファイルシステム RTFS

RTFS は、ルーターの内蔵フラッシュ ROM に構築されるファイルシステムです。一般的な PC のファイルシステムと同様、内蔵フラッシュ ROM に任意のデータを保存しファイル名を付けて管理することができます。またディレクトリ構造も実現されています。内蔵フラッシュ ROM にはファームウェア (exec) や設定ファイル (config) など様々なデータが保存されていますが、それらとは独立した特定の領域を RTFS として使用します。

ファイルやディレクトリを指定するコマンドでは、プレフィックスなしの "/" から始まるパスを入力すると RTFS 領域を参照することができます。

Lua スクリプト機能のスクリプトファイルやカスタム GUI の HTML ファイルなど、読み出し専用データを保存する用途として RTFS を使用してください。ログファイルの記録など、RTFS 領域への定期的な書き込みはフラッシュ ROM の消耗を早めます。頻繁に書き込みを行ったことが原因でフラッシュ ROM の故障に至った場合は、保証期間内であっても無償修理の保証対象外になります。

#### 5.1 RTFS のフォーマット

##### [書式]

`rtfs format`

##### [説明]

内蔵フラッシュ ROM の RTFS 領域をフォーマットし、すべてのデータを削除する。工場出荷状態に戻した場合にもフォーマットが行われる。

##### [ノート]

フォーマットを実行するとデータは完全に削除され、復元することができない。

##### [適用モデル]

NVR700W, NVR510

#### 5.2 RTFS のガベージコレクション

##### [書式]

`rtfs garbage-collect`

##### [説明]

内蔵フラッシュ ROM の RTFS 領域にある不要なデータを削除し、空き容量を増やす。

ガベージコレクションは通常必要なときに自動で実行されるが、処理に数十秒かかるため、事前に行っておきたい場合にこのコマンドを実行する。

##### [ノート]

ガベージコレクションによってファイルが削除されたり上書きされたりすることはない。

##### [適用モデル]

NVR700W, NVR510

## 第 6 章

### IP の設定

#### 6.1 インターフェース共通の設定

##### 6.1.1 IP パケットを扱うか否かの設定

###### [書式]

```
ip routing routing
no ip routing [routing]
```

###### [設定値及び初期値]

- *routing*
  - [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | IP パケットを処理対象として扱う   |
| off | IP パケットを処理対象として扱わない |

- [初期値]: on

###### [説明]

IP パケットをルーティングするかどうかを設定する。

###### [ノート]

off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。

###### [適用モデル]

NVR700W, NVR510

##### 6.1.2 IP アドレスの設定

###### [書式]

```
ip interface address ip_address/mask [broadcast broadcast_ip]
ip interface address dhcp
ip wan address pdp
ip pp address ip_address[/mask]
ip loopback address ip_address[/mask]
ip bridge_interface address ip_address/mask [broadcast broadcast_ip]
ip bridge_interface address dhcp [autoip=switch]
no ip interface address [ip_address/mask [broadcast broadcast_ip]]
no ip interface address [dhcp]
no ip wan address [pdp]
no ip pp address [ip_address[/mask]]
no ip loopback address [ip_address[/mask]]
no ip bridge_interface address [ip_address/mask [broadcast broadcast_ip]]
no ip bridge_interface address [dhcp]
```

###### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *wan*
  - [設定値]: WAN インターフェース名
  - [初期値]: -
- *loopback*
  - [設定値]: LOOPBACK インターフェース名

- [初期値]:-
- *bridge\_interface*
  - [設定値]:ブリッジインターフェース名
  - [初期値]:-
- *ip\_address*
  - [設定値]:IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
  - [初期値]:-
- *dhcp*: DHCP クライアントとして IP アドレスを取得することを示すキーワード
  - [初期値]:-
- *pdp*: 内蔵無線 WAN モジュールから IP アドレスを取得することを示すキーワード
  - [初期値]:-
- *mask*
  - [設定値]:
    - xxx.xxx.xxx.xxx(xxx は十進数)
    - 0x に続く十六進数
    - マスクビット数
  - [初期値]:-
- *broadcast\_ip*
  - [設定値]:ブロードキャスト IP アドレス
  - [初期値]:-
- *switch*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | AutoIP 機能を使う   |
| off | AutoIP 機能を使わない |

- [初期値]: off

**[説明]**

インターフェースの IP アドレスとネットマスクを設定する。“broadcast *broadcast\_ip*” を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。  
*dhcp* を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。また *dhcp* を指定している場合に **no ip interface address** を入力すると、取得していた IP アドレスの開放メッセージを DHCP サーバーに送る。

**[ノート]**

LAN インターフェースと ONU インターフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。  
 PP インターフェースに IP アドレスを設定していない場合には、そのインターフェースは **unnumbered** として動作する。  
 DHCP クライアントとして動作させた場合に取得したクライアント ID は、**show status dhcp** コマンドで確認することができる。  
 第 3 書式、および、ブリッジインターフェースは NVR700W で指定可能。

工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 工場出荷設定値について」を参照してください。

**[適用モデル]**

NVR700W, NVR510

### 6.1.3 セカンダリ IP アドレスの設定

**[書式]**

- ip interface secondary address** *ip\_address*[/*mask*]
- ip interface secondary address** *dhcp*
- no ip interface secondary address** [*ip\_address*/*mask*]

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *ip\_address*
  - [設定値]: セカンダリ IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
  - [初期値]: -
- *dhcp*: DHCP クライアントとして IP アドレスを取得することを示すキーワード
  - [初期値]: -
- *mask*
  - [設定値]:
    - xxx.xxx.xxx.xxx(xxx は十進数)
    - 0x に続く十六進数
    - マスクビット数
  - [初期値]: -

**[説明]**

LAN 側のセカンダリ IP アドレスとネットマスクを設定する。  
 dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。

**[ノート]**

セカンダリのネットワークでのブロードキャストアドレスは必ずディレクティッドブロードキャストアドレスが使われる。

**[適用モデル]**

NVR700W, NVR510

## 6.1.4 インターフェースの MTU の設定

---

**[書式]**

```
ip interface mtu mtu0
ip pp mtu mtu1
ip tunnel mtu mtu2
no ip interface mtu [mtu0]
no ip pp mtu [mtu1]
no ip tunnel mtu [mtu2]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *mtu0,mtu1,mtu2*
  - [設定値]: MTU の値 (64..1500)
  - [初期値]:
    - mtu0=1500
    - mtu1=1500
    - mtu2=1280

**[説明]**

各インターフェースの MTU の値を設定する。

**[ノート]**

実際にはこの設定が適用されるのは IP パケットだけである。他のプロトコルには適用されず、それらではデフォルトのまま 1500 の MTU となる。

**[適用モデル]**

NVR700W, NVR510

## 6.1.5 同一インターフェースに折り返すパケットを送信するか否かの設定

### [書式]

```
ip interface rebound switch
ip pp rebound switch
ip tunnel rebound switch
no ip interface rebound [switch]
no ip pp rebound [switch]
no ip tunnel rebound [switch]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | 折り返すパケットを送信する  |
| off | 折り返すパケットを送信しない |

- [初期値]:
  - off (PP インターフェースの場合)
  - on (その他のインターフェースの場合)

### [説明]

同一インターフェースに折り返すパケットを送信するか否かを設定する。折り返すパケットを送信しない場合にはそのパケットを廃棄し、送信元へ ICMP Destination Unreachable を送信する。

### [適用モデル]

NVR700W, NVR510

## 6.1.6 echo,discard,time サービスを動作させるか否かの設定

### [書式]

```
ip simple-service service
no ip simple-service [service]
```

### [設定値及び初期値]

- *service*
  - [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | TCP/UDP の各種サービスを動作させる |
| off | サービスを停止させる            |

- [初期値]: off

### [説明]

TCP/UDP の echo(7)、discard(9)、time(37) の各種サービスを動作させるか否かを設定する。サービスを停止すると該当のポートも閉じる。

### [適用モデル]

NVR700W, NVR510

## 6.1.7 IP の静的経路情報の設定

### [書式]

```
ip route network gateway gateway1 [parameter] [gateway gateway2 [parameter]...]
```

**no ip route network [gateway...]**

**[設定値及び初期値]**

• *network*

• [設定値]:

| 設定値     | 説明                       |
|---------|--------------------------|
| default | デフォルト経路                  |
| IP アドレス | 送り先のホスト/マスクビット数(省略時は 32) |

• [初期値]: -

• *gateway1, gateway2*

• [設定値]:

- IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
- pp *peer\_num* : PP インターフェースへの経路
  - *peer\_num*:相手先情報番号
- pp anonymous name=*name*

| 設定値         | 説明             |
|-------------|----------------|
| <i>name</i> | PAP/CHAP による名前 |

• *dhcp interface*

| 設定値              | 説明                                                                                                       |
|------------------|----------------------------------------------------------------------------------------------------------|
| <i>interface</i> | DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、ブリッジインターフェース名 |

• *pdp interface*

| 設定値              | 説明                                                   |
|------------------|------------------------------------------------------|
| <i>interface</i> | 内蔵無線 WAN モジュールから与えられるデフォルトゲートウェイを使う場合の、WAN インターフェース名 |

• tunnel *tunnel\_num* : トンネルインターフェースへの経路

• LOOPBACK インターフェース名、NULL インターフェース名

• [初期値]: -

• *parameter* : 以下のパラメーターを空白で区切り複数設定可能

• [設定値]:

| 設定値                             | 説明                                                                                                                                                                           |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>filter number [number..]</i> | フィルター型経路の指定 <ul style="list-style-type: none"> <li>• <i>number</i> <ul style="list-style-type: none"> <li>• フィルターの番号 (1..21474836) (空白で区切り複数設定可能)</li> </ul> </li> </ul>     |
| <i>dpi number [number..]</i>    | フィルタ型経路の指定 <ul style="list-style-type: none"> <li>• <i>number</i> <ul style="list-style-type: none"> <li>• DPI フィルタの番号 (1..2147483647) (空白で区切り複数設定可能)</li> </ul> </li> </ul> |
| <i>metric metric</i>            | メトリックの指定 <ul style="list-style-type: none"> <li>• <i>metric</i> <ul style="list-style-type: none"> <li>• メトリック値 (1..15)</li> <li>• 省略時は 1</li> </ul> </li> </ul>             |

| 設定値                           | 説明                                                                                                                                                                                                               |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hide                          | 出カインターフェースが LAN インターフェース、または WAN インターフェース、PP インターフェース、TUNNEL インターフェースの場合のみ有効なオプションで、相手先が接続されている場合だけ経路が有効になることを意味する                                                                                               |
| weight <i>weight</i>          | 異なる経路間の比率を表す値 <ul style="list-style-type: none"> <li>• <i>weight</i> <ul style="list-style-type: none"> <li>• 経路への重み (NVR700W では 0..2147483647、NVR510 では 1..2147483647)</li> <li>• 省略時は 1</li> </ul> </li> </ul> |
| keepalive <i>keepalive_id</i> | <i>gateway1</i> に到達性のあるときにだけ有効となる <ul style="list-style-type: none"> <li>• <i>keepalive_id</i> <ul style="list-style-type: none"> <li>• キープアライブの識別子 (1..100)</li> </ul> </li> </ul>                              |

- [初期値]:-

### [説明]

IP の静的経路を設定する。

*gateway* のパラメーターとしてフィルター型経路を指定した場合には、記述されている順にフィルターを適用していき、適合したゲートウェイが選択される。

適合するゲートウェイが存在しない場合や、フィルター型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルター型経路が指定されていないゲートウェイが選択される。

フィルター型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。

フィルター型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。

*filter* が指定されていないゲートウェイが複数記述されている場合で、それらの経路を使うべき時にどちらを使うかは、始点/終点 IP アドレス、プロトコル、始点/終点ポート番号により識別されるストリームにより決定される。同じストリームのパケットは必ず同じゲートウェイに送出される。*weight* で値 (例えば回線速度の比率) が指定されている場合には、その値の他のゲートウェイの *weight* 値に対する比率に比例して、その経路に送出されるストリームの比率が上がる。

いずれの場合でも、*hide* キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。なお LOOPBACK インターフェース、NULL インターフェースは常にアップ状態なので、*hide* オプションは指定はできるものの意味はない。

複数のゲートウェイを設定した時に、ロードバランスをせずに特定のゲートウェイだけを優先的に使用するには、*weight* オプションで 0 を設定する。

### [ノート]

既に存在する経路を上書きすることができる。

*keepalive* オプションは NVR700W で指定可能。

ブリッジインターフェースは NVR700W で指定可能。

*pdp interface* 指定は NVR700W で指定可能。

*parameter* パラメータの *dpi* キーワードは NVR700W の Rev.15.00.17 以降のファームウェアで指定可能。

最初の *gateway* キーワードより後のキーワードとパラメーターは合計 129 個まで設定可能。

### [設定例]

- デフォルトゲートウェイを 192.168.0.1 とする。

```
# ip route default gateway 192.168.0.1
```

- PP1 で接続している相手のネットワークは 192.168.1.0/24 である。

```
# ip route 192.168.1.0/24 gateway pp 1
```

- PP1 が有効な時には PP1 のみが使われる。PP1 がダウンすると PP2 が使われる。

```
# ip route 192.168.0.1/24 gateway pp 1 hide gateway pp 2 weight 0
```

- ソフトウェア更新関係の packets は PP1 インターフェース経由で、その他は TUNNEL1 経由で送信する。

```
# dpi group set 100 name=sw_update
windows_update,apple_update,ios_ota_update,adobe_update
# ip dpi filter 1 pass * * 100
# ip route default gateway pp 1 dpi 1 gateway tunnel 1
```

#### [適用モデル]

NVR700W, NVR510

## 6.1.8 DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定

### [書式]

```
ip interface dhcp auto default-route-add switch
```

```
no ip interface dhcp auto default-route-add [switch]
```

### [設定値及び初期値]

- interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- switch*
  - [設定値]:

| 設定値 | 説明                                      |
|-----|-----------------------------------------|
| on  | DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加する  |
| off | DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加しない |

- [初期値]: on

### [説明]

指定したインターフェースを使用中、DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定する。

すでに DHCP で IP アドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次に DHCP で IP アドレスを取得した時点から新しい設定が反映される。

### [ノート]

NVR700W は Rev.15.00.14 以降で使用可能。 NVR510 は Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 6.1.9 DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定

### [書式]

```
ip interface dhcp auto interface-route-add switch
```

```
no ip interface dhcp auto interface-route-add [switch]
```

### [設定値及び初期値]

- interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- switch*
  - [設定値]:

| 設定値 | 説明                                          |
|-----|---------------------------------------------|
| on  | DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加する |



| 設定値 | 説明                                           |
|-----|----------------------------------------------|
| off | DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加しない |

- [初期値]: on

#### [説明]

指定したインターフェースを使用中、DHCP で IP アドレスを取得したときにアドレスを取得したインターフェースの implicit なネットワーク経路を自動的に追加するか否かを設定する。  
すでに DHCP で IP アドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次に DHCP で IP アドレスを取得した時点から新しい設定が反映される。

#### [ノート]

NVR700W は Rev.15.00.14 以降で使用可能。NVR510 は Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 6.1.10 PDP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定

#### [書式]

```
ip interface pdp auto default-route-add switch
no ip interface pdp auto default-route-add [switch]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -
- *switch*

- [設定値]:

| 設定値 | 説明                                     |
|-----|----------------------------------------|
| on  | PDP で IP アドレスを取得したときにデフォルト経路を自動的に追加する  |
| off | PDP で IP アドレスを取得したときにデフォルト経路を自動的に追加しない |

- [初期値]: on

#### [説明]

指定した WAN インターフェースを使用中、PDP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定する。  
すでに PDP で IP アドレスを取得している WAN インターフェースに対してこのコマンドの設定が変更された場合、次に PDP で IP アドレスを取得した時点から新しい設定が反映される。

#### [ノート]

Rev.15.00.03 以降で使用可能。

#### [適用モデル]

NVR700W

### 6.1.11 PDP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定

#### [書式]

```
ip interface pdp auto interface-route-add switch
no ip interface pdp auto interface-route-add [switch]
```

**[設定値及び初期値]**• *interface*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

• *switch*

- [設定値]:

| 設定値 | 説明                                          |
|-----|---------------------------------------------|
| on  | PDP で IP アドレスを取得したときに implicit 経路を自動的に追加する  |
| off | PDP で IP アドレスを取得したときに implicit 経路を自動的に追加しない |

- [初期値]: on

**[説明]**

指定したインターフェースを使用中、PDP で IP アドレスを取得したときにアドレスを取得したインターフェースの implicit なネットワーク経路を自動的に追加するか否かを設定する。

すでに PDP で IP アドレスを取得している WAN インターフェースに対してこのコマンドの設定が変更された場合、次に PDP で IP アドレスを取得した時点から新しい設定が反映される。

**[ノート]**

Rev.15.00.03 以降で使用可能。

**[適用モデル]**

NVR700W

**6.1.12 IP パケットのフィルターの設定****[書式]**

```
ip filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [protocol [src_port_list [dest_port_list]]]]
no ip filter filter_num [pass_reject]
```

**[設定値及び初期値]**• *filter\_num*

- [設定値]: 静的フィルター番号 (1..21474836)
- [初期値]: -

• *pass\_reject*

- [設定値]:

| 設定値          | 説明                                           |
|--------------|----------------------------------------------|
| pass         | 一致すれば通す (ログに記録しない)                           |
| pass-log     | 一致すれば通す (ログに記録する)                            |
| pass-nolog   | 一致すれば通す (ログに記録しない)                           |
| reject       | 一致すれば破棄する (ログに記録する)                          |
| reject-log   | 一致すれば破棄する (ログに記録する)                          |
| reject-nolog | 一致すれば破棄する (ログに記録しない)                         |
| restrict     | 回線が接続されていれば通し、切断されていれば破棄する (破棄する場合のみログに記録する) |
| restrict-log | 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)         |

| 設定値            | 説明                                    |
|----------------|---------------------------------------|
| restrict-nolog | 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない) |

- [初期値]: -
- *src\_addr*: IP パケットの始点アドレス
- [設定値]:
  - IP アドレス
    - A.B.C.D (A~D: 0~255 もしくは\*)
      - 上記表記で A~D を\*とすると、該当する 8 ビット分についてはすべての値に対応する
      - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
      - , を区切りとして複数設定する事が出来る。
    - FQDN
      - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われる為、使用できない)
      - \* から始まる FQDN は \* より後ろの文字列を後方一致条件として判断する 例えば \*.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
      - , を区切りとして複数設定する事が出来る。
    - map-e
      - MAP-E により付与されたグローバル IPv4 アドレスを表すキーワード
      - \* (すべての IP アドレスに対応)
  - [初期値]: -
  - *dest\_addr*: IP パケットの終点アドレス
  - [設定値]:
    - *src\_addr* と同じ形式
    - 省略した場合は一個の \* と同じ
  - [初期値]: -
  - *mask*: IP アドレスのビットマスク (*src\_addr* および *dest\_addr* がネットワークアドレスの場合のみ指定可)
  - [設定値]:
    - A.B.C.D (A~D: 0~255)
    - 0x に続く十六進数
    - マスクビット数
    - 省略時は 0xffffffff と同じ
  - [初期値]: -
  - *protocol*: フィルタリングするパケットの種類
  - [設定値]:
    - プロトコルを表す十進数 (0..255)
    - プロトコルを表すニーモニック

| ニーモニック | 十進数 | 説明         |
|--------|-----|------------|
| icmp   | 1   | ICMP パケット  |
| tcp    | 6   | TCP パケット   |
| udp    | 17  | UDP パケット   |
| ipv6   | 41  | IPv6 パケット  |
| gre    | 47  | GRE パケット   |
| esp    | 50  | ESP パケット   |
| ah     | 51  | AH パケット    |
| icmp6  | 58  | ICMP6 パケット |

- 上項目のカンマで区切った並び
- 特殊指定

|                     |                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------|
| icmp-error          | TYPE が 3、4、5、11、12、31、32 のいずれかである ICMP パケット                                                             |
| icmp-info           | TYPE が 0、8~10、13~18、30、33~36 のいずれかである ICMP パケット                                                         |
| tcpsyn              | SYN フラグの立っている tcp パケット                                                                                  |
| tcpfin              | FIN フラグの立っている tcp パケット                                                                                  |
| tcprst              | RST フラグの立っている tcp パケット                                                                                  |
| established         | ACK フラグの立っている tcp パケット内から外への接続は許可するが、外から内への接続は拒否する機能                                                    |
| tcpflag=value/mask  | TCP フラグの値と mask の値の論理積 (AND) が、value に一致、または不一致である TCP パケット<br>value と mask は 0x に続く十六進数で 0x0000~0xffff |
| tcpflag!=value/mask |                                                                                                         |
| *                   | すべてのプロトコル                                                                                               |

- 省略時は \* と同じ。
- [初期値] :-
- *src\_port\_list : protocol* に、TCP(tcp/tcpsyn/tcpfin/tcprst/established/tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDP のソースポート番号。*protocol* が ICMP(icmp) 単独の場合には、ICMP タイプ。
- [設定値] :
  - ポート番号、タイプを表す十進数
  - ポート番号を表すニーモニック (一部)

| ニーモニック     | ポート番号 |
|------------|-------|
| ftp        | 20,21 |
| ftpdata    | 20    |
| telnet     | 23    |
| smtp       | 25    |
| domain     | 53    |
| gopher     | 70    |
| finger     | 79    |
| www        | 80    |
| pop3       | 110   |
| sunrpc     | 111   |
| ident      | 113   |
| ntp        | 123   |
| nntp       | 119   |
| snmp       | 161   |
| syslog     | 514   |
| printer    | 515   |
| talk       | 517   |
| route      | 520   |
| uucp       | 540   |
| submission | 587   |

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

- 上項目のカンマで区切った並び (10 個以内)
- \* (すべてのポート、タイプ)
- 省略時は \* と同じ。
- [初期値]:-
- *dest\_port\_list*
  - [設定値]: *protocol* に、TCP(*tcp/tcpsyn/tcpfin/tcprst/established/tcpflag*)、UDP(*udp*) のいずれかが含まれる場合は、TCP/UDP のデスティネーションポート番号。 *protocol* が ICMP(*icmp*) 単独の場合には、ICMP コード
  - [初期値]:-

#### [説明]

IP パケットのフィルターを設定する。本コマンドで設定されたフィルターは **ip interface secure filter**、**ip filter set**、**ip filter dynamic**、および **ip interface rip filter** コマンドで用いられる。

#### [ノート]

*restrict-log* 及び *restrict-nolog* を使ったフィルターは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに有効である。例えば、時計を合わせるための NTP パケットがこれに該当する。ICMP パケットに対して、ICMP タイプと ICMP コードをフィルターでチェックしたい場合には、*protocol* には 'icmp' だけを単独で指定する。*protocol* が 'icmp' 単独である場合にのみ、*src\_port\_list* は ICMP タイプ、*dest\_port\_list* は ICMP コードと見なされる。*protocol* に 'icmp' と他のプロトコルを列挙した場合には *src\_port\_list* と *dest\_port\_list* の指定は TCP/UDP のポート番号と見なされ、ICMP パケットとの比較は行われぬ。また、*protocol* に 'icmp-error' や 'icmpinfo' を指定した場合には、*src\_port\_list* と *dst\_port\_list* の指定は無視される。*protocol* に '\*' を指定するか、TCP/UDP を含む複数のプロトコルを列挙している場合には、*src\_port\_list* と *dest\_port\_list* の指定は TCP/UDP のポート番号と見なされ、パケットが TCP または UDP である場合のみポート番号がフィルターが比較される。パケットがその他のプロトコル (ICMP を含む) の場合には、*src\_port\_list* と *dest\_port\_list* の指定は存在しないものとしてフィルターと比較される。

*src\_addr* および *dest\_addr* は IP アドレス と FQDN と map-e を混合することも可能。

*src\_addr* および *dest\_addr* への FQDN の指定は NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.13 以降のファームウェアで指定可能。

*src\_addr* および *dest\_addr* に FQDN を指定することによって、固定 IP アドレスではないサーバーや 1 つの FQDN に対して複数の固定 IP アドレスを持つサーバーを対象にしたフィルタリングを行う事が出来る。FQDN を使用する場合、ルーター自身が DNS リカーシブサーバーとして動作し、ルータ配下の端末は、DNS サーバーとして本機を指定する必要がある。

指定した FQDN に一致する通信が発生した場合、設定した FQDN に該当する IP アドレスの情報が保持される。保持される期間は、**ip filter fqdn timer** コマンドで指定できる。

*src\_addr* および *dest\_addr* への map-e の指定は NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降のファームウェアで指定可能。

#### [設定例]

LAN1 で送受信される IPv4 ICMP ECHO/REPLY を pass-log で記録する

```
# ip lan1 secure filter in 1 2 100
# ip lan1 secure filter out 1 2 100
# ip filter 1 pass-log * * icmp 8
# ip filter 2 pass-log * * icmp 0
# ip filter 100 pass * *
```

LAN2 から送信される IPv4 Redirect のうち、"for the Host" だけを通さない

```
# ip lan2 secure filter out 1 100
# ip filter 1 reject * * icmp 5 1
# ip filter 100 pass * *
```

#### [適用モデル]

NVR700W, NVR510

## 6.1.13 フィルタセットの定義

#### [書式]

```
ip filter set name direction filter_list [filter_list ...]
```

```
no ip filter set name [direction ...]
```

**[設定値及び初期値]**

- *name*
  - [設定値]: フィルタセットの名前を表す文字列
  - [初期値]: -
- *direction*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| in  | 入力方向のフィルター |
| out | 出力方向のフィルター |

- [初期値]: -
- *filter\_list*
  - [設定値]: 空白で区切られたフィルター番号の並び (1001 個以内)
  - [初期値]: -

**[説明]**

フィルタセットを定義する。フィルタセットは、in/out のフィルターをそれぞれ定義し、**ip interface secure filter** コマンドによりインターフェースに適用される。

**[適用モデル]**

NVR700W, NVR510

### 6.1.14 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定

---

**[書式]**

```
ip filter source-route filter_out
no ip filter source-route [filter_out]
```

**[設定値及び初期値]**

- *filter\_out*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | フィルタアウトする  |
| off | フィルタアウトしない |

- [初期値]: on

**[説明]**

Source-route オプション付き IP パケットをフィルタアウトするか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 6.1.15 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定

---

**[書式]**

```
ip filter directed-broadcast filter_out
ip filter directed-broadcast filter filter_num [filter_num ...]
no ip filter directed-broadcast
```

**[設定値及び初期値]**

- *filter\_out*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | フィルタアウトする  |
| off | フィルタアウトしない |

- [初期値]: on

- *filter\_num*
  - [設定値]: 静的フィルター番号 (1..21474836)
  - [初期値]: -

#### [説明]

終点 IP アドレスがディレクテッドブロードキャストアドレス宛になっている IP パケットをルーターが接続されているネットワークにブロードキャストするか否かを設定する。

*on* を指定した場合には、ディレクテッドブロードキャストパケットはすべて破棄する。

*off* を指定した場合には、ディレクテッドブロードキャストパケットはすべて通過させる。

*filter* を指定した場合には、**ip filter** コマンドで設定したフィルターでパケットを検査し、PASS フィルターにマッチした場合のみパケットを通過させる。

#### [ノート]

このコマンドでのチェックよりも、**ip interface wol relay** コマンドのチェックの方が優先される。**ip interface wol relay** コマンドでのチェックにより通過させることができなかったパケットのみが、このコマンドでのチェックを受ける。いわゆる smurf 攻撃を防止するためには *on* にしておく。

#### [適用モデル]

NVR700W, NVR510

## 6.1.16 動的フィルターの定義

#### [書式]

```
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] protocol [option ...]
```

```
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] filter filter_list [in filter_list] [out filter_list] [option...]
```

```
no ip filter dynamic dyn_filter_num
```

#### [設定値及び初期値]

- *dyn\_filter\_num*
  - [設定値]: 動的フィルター番号 (1..21474836)
  - [初期値]: -
- *srcaddr*: IP パケットの始点アドレス
  - [設定値]:
    - **ip filter** コマンドの *src\_addr* と同じ形式
  - [初期値]: -
- *dstaddr*: IP パケットの終点アドレス
  - [設定値]:
    - *srcaddr* と同じ形式
  - [初期値]: -
- *mask*: IP アドレスのビットマスク (*srcaddr* および *dstaddr* がネットワークアドレスの場合のみ指定可)
  - [初期値]: -
- *protocol*: プロトコルのニーモニック
  - [設定値]:
    - echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/
    - tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/
    - netbios\_ns/netbios\_dgm/netbios\_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
    - https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
    - ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
    - ping/ping6/tcp/udp/submission/netmeeting

以下のニーモニックは設定できますが、動的フィルターとして動作しません

- dhcpc/dhcps/dhcpv6c/dhcpv6s
  - [初期値]: -
- *filter\_list*
  - [設定値]: **ip filter** コマンドで登録されたフィルター番号のリスト

- [初期値]: -
- *option*
- [設定値]:
  - *syslog=switch*

| 設定値 | 説明                        |
|-----|---------------------------|
| on  | コネクションの通信履歴を SYSLOG に残す   |
| off | コネクションの通信履歴を SYSLOG に残さない |

- *timeout=time*

| 設定値  | 説明                               |
|------|----------------------------------|
| time | データが流れなくなったときにコネクション情報を解放するまでの秒数 |

- [初期値]: *syslog=on*

### [説明]

動的フィルターを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザーがアクセス制御のルールを記述する。キーワードの *filter*、*in*、*out* の後には、**ip filter** コマンドで定義されたフィルター番号を設定する。

*filter* キーワードの後に記述されたフィルターに該当するコネクション (トリガー) を検出したら、それ以降 *in* キーワードと *out* キーワードの後に記述されたフィルターに該当するコネクションを通過させる。*in* キーワードはトリガーの方向に対して逆方向のアクセスを制御し、*out* キーワードは動的フィルターと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。*pass/reject* の引数も同様に無視される。

プロトコルとして *tcp* や *udp* を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。

### [ノート]

*srcaddr* および *dstaddr* は IP アドレスと FQDN と *map-e* を混合することも可能。

*srcaddr* および *dstaddr* への FQDN の指定は NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.13 以降で指定可能。

*srcaddr* および *dstaddr* への *map-e* の指定は NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で指定可能。

### [設定例]

```
# ip filter 10 pass * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

### [適用モデル]

NVR700W, NVR510

## 6.1.17 動的フィルターのタイムアウトの設定

### [書式]

```
ip filter dynamic timer option=timeout [option=timeout...]
no ip filter dynamic timer
```

### [設定値及び初期値]

- *option*: オプション名
- [設定値]:

| 設定値                    | 説明                                          |
|------------------------|---------------------------------------------|
| <i>tcp-syn-timeout</i> | SYN を受けてから設定された時間内にコネクションが確立しなければセッションを切断する |
| <i>tcp-fin-timeout</i> | FIN を受けてから設定された時間が経てばコネクションを強制的に解放する        |



| 設定値           | 説明                                         |
|---------------|--------------------------------------------|
| tcp-idle-time | 設定された時間内に TCP コネクションのデータが流れなければコネクションを切断する |
| udp-idle-time | 設定された時間内に UDP コネクションのデータが流れなければコネクションを切断する |
| dns-timeout   | DNS の要求を受けてから設定された時間内に応答を受けなければコネクションを切断する |

- [初期値]:
  - tcp-syn-timeout=30
  - tcp-fin-timeout=5
  - tcp-idle-time=3600
  - udp-idle-time=30
  - dns-timeout=5
- *timeout*
  - [設定値]: 待ち時間 ( 秒 )
  - [初期値]: -

**[説明]**

動的フィルターのタイムアウトを設定する。

**[ノート]**

本設定はすべての検査において共通に使用される。

**[適用モデル]**

NVR700W, NVR510

### 6.1.18 FQDN フィルターで使用するキャッシュのタイマーの設定

**[書式]**

```
ip filter fqdn timer time [auto=switch]
no ip filter fqdn timer [time]
```

**[設定値及び初期値]**

- *time*
  - [設定値]: 秒数 (1..2147483647)
  - [初期値]: 600
- *switch*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | 自動設定を使用する  |
| off | 自動設定を使用しない |

- [初期値]: on

**[説明]**

FQDN フィルターで使用するキャッシュのタイマーを設定する。

**ip filter** コマンドで、始点アドレスおよび、終点アドレスに FQDN を設定している場合、指定した FQDN に一致する通信が発生したとき、タイマーが動作する。*time* に指定した秒数の間、FQDN フィルターに一致する通信がない場合、FQDN と IP アドレスを対応づけるキャッシュを削除する。

auto=on の場合、タイマーには以下の値が設定される。

- ファストパスを使用する通信のとき、ファストパスのフローテーブルで使用されるタイマーの中で、最も大きい値が本タイマーの値として自動で設定される。
- ファストパスを使用しない通信のとき、*time* の値がタイマーとして設定される。

auto=off の場合は、常に *time* の値がタイマーとして設定される。

## [ノート]

NVR700W は Rev.15.00.10 以降、NVR510 は Rev.15.01.13 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 6.1.19 侵入検知機能の動作の設定

## [書式]

**ip interface intrusion detection direction [type] switch [option]**

**ip pp intrusion detection direction [type] switch [option]**

**ip tunnel intrusion detection direction [type] switch [option]**

**no ip interface intrusion detection direction [type] switch [option]**

**no ip pp intrusion detection direction [type] switch [option]**

**no ip tunnel intrusion detection direction [type] switch [option]**

## [設定値及び初期値]

## • interface

- [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
- [初期値]: -

## • direction: 観察するパケット・コネクションの方向

- [設定値]:

| 設定値 | 説明           |
|-----|--------------|
| in  | インターフェースの内向き |
| out | インターフェースの外向き |

- [初期値]: -

## • type: 観察するパケット・コネクションの種類

- [設定値]:

| 設定値       | 説明           |
|-----------|--------------|
| ip        | IP ヘッダ       |
| ip-option | IP オプションヘッダ  |
| fragment  | フラグメント       |
| icmp      | ICMP         |
| udp       | UDP          |
| tcp       | TCP          |
| ftp       | FTP          |
| winny     | Winny        |
| share     | Share        |
| default   | 設定していないものすべて |

- [初期値]: -

## • switch

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 実行する  |
| off | 実行しない |

- [初期値]:

- TYPE を指定しないとき=off
- TYPE を指定したとき=on

## • option

- [設定値]:

| 設定値        | 説明            |
|------------|---------------|
| reject=on  | 不正なパケットを破棄する  |
| reject=off | 不正なパケットを破棄しない |

- [初期値]: off

#### [説明]

指定したインターフェースで、指定された向きのパケットやコネクションについて異常を検知する。  
*type* オプションを省略したときには、侵入検知機能の全体についての設定になる。

#### [ノート]

危険性の高い攻撃については、*reject* オプションの設定に関わらず、常にパケットを破棄する。  
Winny については、バージョン 2 の検知が可能であり、それ以前のバージョンには対応していない。  
Share については、バージョン 1.0 EX2 (ShareTCP 版) の検知が可能であり、それ以前のバージョンには対応していない。

#### [適用モデル]

NVR700W, NVR510

### 6.1.20 1 秒間に侵入検知情報を通知する頻度の設定

#### [書式]

**ip interface intrusion detection notice-interval *frequency***

**ip pp intrusion detection notice-interval *frequency***

**ip tunnel intrusion detection notice-interval *frequency***

**no ip interface intrusion detection notice-interval**

**no ip pp intrusion detection notice-interval**

**no ip tunnel intrusion detection notice-interval**

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *frequency*
  - [設定値]: 頻度 (1...1000)
  - [初期値]: 1

#### [説明]

1 秒間に侵入検知情報を通知する頻度を設定する。

#### [適用モデル]

NVR700W, NVR510

### 6.1.21 重複する侵入検知情報の通知抑制の設定

#### [書式]

**ip interface intrusion detection repeat-control *time***

**ip pp intrusion detection repeat-control *time***

**ip tunnel intrusion detection repeat-control *time***

**no ip interface intrusion detection repeat-control**

**no ip pp intrusion detection repeat-control**

**no ip tunnel intrusion detection repeat-control**

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *time*

- [設定値]: 秒数 (1..1000)
- [初期値]: 60

**[説明]**

同じホストに対する同じ種類の攻撃を、*time* 秒に 1 回のみ通知するよう抑制する。

**[適用モデル]**

NVR700W, NVR510

## 6.1.22 侵入検知情報の最大表示件数の設定

---

**[書式]**

**ip interface intrusion detection report num**

**ip pp intrusion detection report num**

**ip tunnel intrusion detection report num**

**no ip interface intrusion detection report**

**no ip pp intrusion detection report**

**no ip tunnel intrusion detection report**

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *num*
  - [設定値]: 件数 (1..1000)
  - [初期値]: 50

**[説明]**

**show ip intrusion detection** コマンドで表示される侵入検知情報の最大件数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 6.1.23 TCP セッションの MSS 制限の設定

---

**[書式]**

**ip interface tcp mss limit mss**

**ip pp tcp mss limit mss**

**ip tunnel tcp mss limit mss**

**no ip interface tcp mss limit [mss]**

**no ip pp tcp mss limit [mss]**

**no ip tunnel tcp mss limit [mss]**

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *mss*
  - [設定値]:

| 設定値       | 説明       |
|-----------|----------|
| 536..1460 | MSS の最大長 |
| auto      | 自動設定     |
| off       | 設定しない    |

- [初期値]:
  - off(Rev.15.00.07 以前、Rev.15.01.06 以前)
  - auto(Rev.15.00.10 以降、Rev.15.01.09 以降)

**[説明]**

インターフェースを通過する TCP セッションの MSS を制限する。インターフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード `auto` を指定した場合には、インターフェースの MTU、もしくは PP インターフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

**[ノート]**

PPPoE 用の PP インターフェースに対しては、`pppoe tcp mss limit` コマンドでも TCP セッションの MSS を制限することができる。このコマンドと `pppoe tcp mss limit` コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

**[適用モデル]**

NVR700W, NVR510

### 6.1.24 TCP ウィンドウ・スケール・オプションを変更する

**[書式]**

```
ip interface tcp window-scale sw
ip pp tcp window-scale sw
ip tunnel tcp window-scale sw
no ip interface tcp window-scale [...]
no ip pp tcp window-scale [...]
no ip tunnel tcp window-scale [...]
```

**[設定値及び初期値]**

- `interface`
  - [設定値]: LAN インターフェース名、WAN インターフェース名
  - [初期値]: -
- `sw`
  - [設定値]:

| 設定値    | 説明                        |
|--------|---------------------------|
| off    | 何もしない                     |
| remove | TCP ウィンドウ・スケール・オプションを削除する |

- [初期値]: off

**[説明]**

インターフェースを通過する TCP パケットのウィンドウ・スケール・オプションを強制的に変更する。`remove` を指定すると、ウィンドウ・スケール・オプションが有効になっていた場合には、無効にして転送する。

**[ノート]**

NVR700W は Rev.15.00.03 以降、NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 6.1.25 ルーターが端点となる TCP のセッション数の設定

**[書式]**

```
tcp session limit limit
no tcp session limit [limit]
```

**[設定値及び初期値]**

- `limit`: 制限値
- [設定値]:

| 設定値      | 説明     |
|----------|--------|
| 32~65535 | セッション数 |

| 設定値  | 説明    |
|------|-------|
| none | 制限しない |

- [初期値]: 15000

#### [説明]

ルーターが端点となる TCP のセッション数を制限する。

none を選択した場合には制限を設けない。

#### [ノート]

ルーターと直接通信しない場合にはこの制限は適用されない。

#### [適用モデル]

NVR700W, NVR510

### 6.1.26 IPv4 の経路情報に変化があった時にログに記録するか否かの設定

#### [書式]

**ip route change log log**

**no ip route change log [log]**

#### [設定値及び初期値]

- log
- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | IPv4 経路の変化をログに記録する  |
| off | IPv4 経路の変化をログに記録しない |

- [初期値]: off

#### [説明]

IPv4 の経路情報に変化があった時にそれをログに記録するか否かを設定する。

ログは INFO レベルで記録される。

#### [適用モデル]

NVR700W, NVR510

### 6.1.27 フィルタリングによるセキュリティーの設定

#### [書式]

**ip interface secure filter direction [filter\_list...] [dynamic filter\_list...]**

**ip pp secure filter direction [filter\_list...] [dynamic filter\_list...]**

**ip tunnel secure filter direction [filter\_list...] [dynamic filter\_list...]**

**ip interface secure filter name set\_name**

**ip pp secure filter name set\_name**

**ip tunnel secure filter name set\_name**

**no ip interface secure filter direction [filter\_list]**

**no ip pp secure filter direction [filter\_list]**

**no ip tunnel secure filter direction [filter\_list]**

**no ip interface secure filter name [set\_name]**

**no ip pp secure filter name [set\_name]**

**no ip tunnel secure filter name [set\_name]**

#### [設定値及び初期値]

- interface
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、LOOPBACK インターフェース名、NULL インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- direction

- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| in  | 受信したパケットのフィルタリング |
| out | 送信するパケットのフィルタリング |

- [初期値]:-
- *filter\_list*
  - [設定値]: 空白で区切られたフィルター番号の並び (静的フィルターと動的フィルターの数の合計として 129 個以内)
  - [初期値]:-
- *set\_name*
  - [設定値]: フィルターセットの名前を表す文字列
  - [初期値]:-
- *dynamic*: キーワード後に動的フィルターの番号を記述する
  - [初期値]:-

### [説明]

**ip filter** コマンドによるパケットのフィルターを組み合わせ、インターフェースで送受信するパケットの種類を制限する

方向を指定する書式では、それぞれの方向に対して適用するフィルター列をフィルター番号で指定する。指定された番号のフィルターが順番に適用され、パケットにマッチするフィルターが見つければそのフィルターにより通過/破棄が決定する。それ以降のフィルターは調べられない。すべてのフィルターにマッチしないパケットは破棄される。

フィルターセットの名前を指定する書式では、指定されたフィルターセットが適用される。フィルターを調べる順序などは方向を指定する書式の方法に準ずる。定義されていないフィルターセットの名前が指定された場合には、フィルターは設定されていないものとして動作する。

### [ノート]

フィルターリストを走査して、一致すると通過、破棄が決定する。

```
# ip filter 1 pass 192.168.0.0/24 *
# ip filter 2 reject 192.168.0.1
# ip lan1 secure filter in 1 2
```

この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルター 1 で通過が決定してしまうため、フィルター 2 での検査は行われない。そのため、フィルター 2 は何も意味を持たない。フィルターリストを操作した結果、どのフィルターにも一致しないパケットは破棄される。

PP Anonymous で認証に RADIUS を利用する場合で、RADIUS サーバーから送られた Access-Response にアトリビュート 'Filter-Id' が付いていた場合には、その値に指定されたフィルターセットを適用し、**ip pp secure filter** コマンドの設定は無視される。

ただしアトリビュート "Filter-Id" が存在しない場合には、**ip pp secure filter** コマンドの設定がフィルターとして利用される。

LOOPBACK インターフェースと NULL インターフェースでは動的フィルターは使用できない。

NULL インターフェースで *direction* に 'in' は指定できない。

ブリッジインターフェースは NVR700W で指定可能。

### [適用モデル]

NVR700W, NVR510

## 6.1.28 ルールに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定

### [書式]

```
ip fragment remove df-bit rule
no ip fragment remove df-bit [rule]
```

### [設定値及び初期値]

- *rule*

- [設定値]:

| 設定値                      | 説明                                                     |
|--------------------------|--------------------------------------------------------|
| filter <i>filter_num</i> | <i>filter_num</i> は <b>ip filter</b> コマンドで登録されたフィルター番号 |

- [初期値]:-

#### [説明]

フォワーディングする IP パケットの内、*rule* に一致するものは DF ビットを 0 に書き換える。

#### [ノート]

DF ビットは経路 MTU 探索アルゴリズムで利用されるが、経路の途中に ICMP パケットをフィルターするファイアウォールなどがあるとアルゴリズムがうまく動作せず、特定の通信相手とだけは通信ができないなどの現象になることがある。このような現象は、「経路 MTU 探索ブラックホール (Path MTU Discovery Blackhole)」と呼ばれている。この経路 MTU 探索ブラックホールがある場合には、このコマンドでそのような相手との通信に関して DF ビットを 0 に書き換えてしまえば、経路 MTU 探索は正しく動作しなくなるものの、通信できなくなるということはない。

#### [適用モデル]

NVR700W, NVR510

## 6.1.29 IP パケットの TOS フィールドの書き換えの設定

#### [書式]

```
ip tos supersede id tos [precedence=precedence] filter_num [filter_num_list]
no ip tos supersede id [tos]
```

#### [設定値及び初期値]

- *id*
  - [設定値]: 識別番号 (1..65535)
  - [初期値]: -
- *tos*
  - [設定値]:
    - 書き換える TOS 値 (0..15)
    - 以下のニーモニックが利用できる

| ニーモニック            | TOS 値 |
|-------------------|-------|
| normal            | 0     |
| min-monetary-cost | 1     |
| max-reliability   | 2     |
| max-throughput    | 4     |
| min-delay         | 8     |

- [初期値]:-
- *precedence*
  - [設定値]:
    - precedence 値 (0..7)
    - precedence を省略した場合、PRECEDENCE 値は変更しない
  - [初期値]: -
- *filter\_num*
  - [設定値]: 静的フィルターの番号 (1..21474836)
  - [初期値]: -
- *filter\_num\_list*
  - [設定値]: 静的フィルターの番号 (1..21474836) の並び
  - [初期値]: -



**[説明]**

IP パケットを中継する場合に TOS フィールドを指定した値に書き換える。  
 識別番号順にリストをチェックし、*filter\_num* リストのフィルターを順次適用していく。そして、最初にマッチした IP フィルターが *pass*、*pass-log*、*pass-nolog*、*restrict*、*restrict-log*、*restrict-nolog* のいずれかであれば TOS フィールドが書き換えられる。  
*reject*、*reject-log* または *reject-nolog* である場合は書き換えずに処理を終わる。

**ip dscp supersede** コマンドの設定と本コマンドの設定で条件が同じ場合、**ip dscp supersede** コマンドの設定が優先される。

**[適用モデル]**  
 NVR700W

**6.1.30 代理 ARP の設定****[書式]**

```
ip interface proxyarp proxyarp
ip interface proxyarp vrrp vrid
no ip interface proxyarp [proxyarp]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *proxyarp*
  - [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | 代理 ARP 動作をする  |
| off | 代理 ARP 動作をしない |

- [初期値]: off
- *vrid*
  - [設定値]: VRRP グループ ID (1..255)
  - [初期値]: -

**[説明]**

代理 ARP 動作をするか否か設定する。**on** を設定した時には、代理 ARP 動作を行う。この時利用する MAC アドレスは、LAN インターフェースまたは ONU インターフェースの実 MAC アドレスとなる。ブリッジインターフェースを指定した時には、ブリッジインターフェースに収容された実 LAN インターフェースにおいて、代理 ARP 動作をするか否か設定する。この時利用する MAC アドレスは ARP を受信した実 LAN インターフェースの MAC アドレスとなる。

第 2 書式を設定した時には、指定された **VRID** での VRRP の状態がマスターである場合のみ代理 ARP 動作を行う。利用する MAC アドレスは指定された **VRID** の仮想 MAC アドレスとなる。

**[ノート]**

第 2 書式、および、ブリッジインターフェースは NVR700W で指定可能。

**[適用モデル]**  
 NVR700W, NVR510

**6.1.31 ARP エントリの寿命の設定****[書式]**

```
ip arp timer timer [retry]
no ip arp timer [timer [retry]]
```

**[設定値及び初期値]**

- *timer*

- [設定値]: ARP エントリの寿命秒数 (30..32767)
- [初期値]: 1200
- *retry*
  - [設定値]: ARP リクエスト再送回数 (4..100)
  - [初期値]: 4

**[説明]**

ARP エントリの寿命を設定する。ARP 手順で得られた IP アドレスと MAC アドレスの組は ARP エントリとして記憶されるが、このコマンドで設定した時間だけ経過するとエントリは消される。ただしエントリが消される前に再度 ARP 手順が実行され、その ARP に応答が無い場合にエントリは消される。

*retry* パラメーターで ARP リクエストの再送回数を設定できる。ARP リクエストの再送間隔は初回は 2 秒、その後は 1 秒である。

*retry* パラメーターについては、通常は初期値から変更する必要はない。

**[適用モデル]**

NVR700W, NVR510

**6.1.32 静的 ARP エントリの設定**

---

**[書式]**

```
ip interface arp static ip_address mac_address
no ip interface arp static ip_address[...]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *ip\_address*
  - [設定値]: IP アドレス
  - [初期値]: -
- *mac\_address*
  - [設定値]: MAC アドレス
  - [初期値]: -

**[説明]**

ARP エントリを静的に設定する。このコマンドで設定された ARP エントリは、**show arp** コマンドで TTL が 'permanent' と表示され、常に有効となる。また、**clear arp** コマンドを実行してもエントリは消えない。

**[適用モデル]**

NVR700W, NVR510

**6.1.33 ARP が解決されるまでの間に送信を保留しておくパケットの数を制御する**

---

**[書式]**

```
ip interface arp queue length len
no ip interface arp queue length [len]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *len*
  - [設定値]: キュー長 (0..10000)
  - [初期値]:
    - 200 (NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降)
    - 40 (上記以外)

**[説明]**

ARP が解決していないホストに対してパケットを送信しようとした時に、ARP が解決するか、タイムアウトにより ARP が解決できないことが確定するまで、インターフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。

0 を設定するとパケットを保留しなくなるため、例えば ARP が解決していない相手に ping を実行すると必ず最初の 1 パケットは失敗するようになる。

**[適用モデル]**

NVR700W, NVR510

**6.1.34 ARP エントリの変化をログに残すか否かの設定****[書式]**

```
ip interface arp log switch
```

```
no ip interface arp log [switch]
```

**[設定値及び初期値]**• *interface*

- [設定値]: LAN インターフェース名、ONU インターフェース名
- [初期値]: -

• *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 記録する  |
| off | 記録しない |

- [初期値]: off

**[説明]**

ARP エントリの変更をログに記録するか否かを設定する

**[ノート]**

show log | grep ARP: を実行することによって、過去の ARP エントリ履歴を確認することができる。

**[適用モデル]**

NVR700W, NVR510

**6.1.35 ネットワーク監視機能の設定****[書式]**

```
ip keepalive num kind interval count gateway [gateway ...] [option=value ...]
```

```
no ip keepalive num
```

**[設定値及び初期値]**• *num*

- [設定値]: このコマンドの識別番号 (1..100)
- [初期値]: -

• *kind*: 監視方式

- [設定値]:

| 設定値       | 説明              |
|-----------|-----------------|
| icmp-echo | ICMP Echo を使用する |

- [初期値]: -

• *interval*

- [設定値]: キープアライブの送信間隔秒数 (1..65535)
- [初期値]: -

• *count*

- [設定値]: 到達性がないと判断するまでに送信する回数(3..100)

- [初期値] :-
- *gateway* : 複数指定可 (10 個以内)
- [設定値] :

| 設定値                   | 説明                                                                                            |
|-----------------------|-----------------------------------------------------------------------------------------------|
| IP アドレス               | xxx.xxx.xxx.xxx (xxx は十進数)                                                                    |
| <i>dhcp interface</i> | DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インターフェース名、ONU インターフェース名または WAN インターフェース名 |
| <i>pdp interface</i>  | 内蔵無線 WAN モジュールから与えられるデフォルトゲートウェイを使う場合の、WAN インターフェース名                                          |

- [初期値] :-
- *option=value* 列
- [設定値] :

| <i>option</i>          | <i>value</i>       | 説明                                                                                  |
|------------------------|--------------------|-------------------------------------------------------------------------------------|
| log                    | on                 | SYSLOG を出力する                                                                        |
|                        | off                | SYSLOG を出力しない                                                                       |
| upwait                 | 秒数                 | 到達性があると判断するまでの待機時間 (1..1000000)                                                     |
| downwait               | 秒数                 | 到達性がないと判断するまでの待機秒数 (1..1000000)                                                     |
| length                 | バイト                | ICMP Echo パケットの長さ (64-1500)                                                         |
| local-address          | IP アドレス            | 始点 IP アドレス                                                                          |
| ipsec-refresh          | セキュリティー・ゲートウェイの識別子 | DOWN→UP または UP→DOWN に状態が変化した場合に、指定のセキュリティー・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る) |
| ipsec-refresh-up       | セキュリティー・ゲートウェイの識別子 | DOWN→UP に状態が変化した場合のみ、指定のセキュリティー・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)            |
| ipsec-refresh-down     | セキュリティー・ゲートウェイの識別子 | UP→DOWN に状態が変化した場合のみ、指定のセキュリティー・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)            |
| gateway-selection-rule | head               | ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていても、必ず最初に指定されたゲートウェイへ送出する                |
|                        | normal             | ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていたら、通常の規則に従い送出ゲートウェイを選択する                |

- [初期値] :

- log=off
- upwait=5
- downwait=5
- length=64
- gateway-selection-rule=head

#### [説明]

指定したゲートウェイに対して ICMP Echo を送信し、その返事を受信できるかどうかを判定する。keepalive に失敗した場合、フロントパネルの STATUS LED が橙色に点灯する。

#### [ノート]

length パラメーターで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。

local-address、ipsec-refresh、ipsec-refresh-up、ipsec-refresh-down、gateway-selection-rule パラメーターは NVR700W で指定可能。

ipsec-refresh、ipsec-refresh-up、ipsec-refresh-down パラメーターは、ネットワークバックアップ機能の主系/従系回線の切り替え時において、IPsec 通信の復旧時間を短縮させる際に有効である。

gateway パラメーターの pdp 指定は NVR700W で指定可能。

#### [設定例]

下記の設定は、NVR700W の設定例です。

設定例の **ip route** コマンドの keepalive や、**ip keepalive** コマンドの ipsec-refresh-up、gateway-selection-rule は、NVR510 では指定できません。

ネットワークバックアップ機能で従系回線 pp11 から主系回線 pp10 へ復旧する際に、IPsec 接続で使用しているセキュリティ・ゲートウェイの識別子 3 に属する SA を強制的に更新させる。

```
# ip route 172.16.0.0/24 gateway pp 10 keepalive 1 gateway pp 11 weight 0
# ip keepalive 1 icmp-echo 5 5 172.16.0.1 ipsec-refresh-up=3
```

ネットワークバックアップ機能を利用して、IP キープアライブ 1 がダウンしたのをトリガーにして経路 172.16.224.0/24 を活性化させる。

```
# ip route 172.16.112.0/24 gateway null keepalive 1 gateway 172.16.0.1 weight 0
# ip route 172.16.224.0/24 gateway 172.16.112.1 keepalive 2
# ip keepalive 1 icmp-echo 5 5 192.168.100.101
# ip keepalive 2 icmp-echo 5 5 172.16.112.1 gateway-selection-rule=normal
```

#### [適用モデル]

NVR700W, NVR510

## 6.1.36 implicit 経路の優先度の設定

#### [書式]

```
ip implicit-route preference preference
no ip implicit-route preference [preference]
```

#### [設定値及び初期値]

- preference
  - [設定値]: implicit 経路の優先度 (1..2147483647)
  - [初期値]: 10000

#### [説明]

implicit 経路の優先度を設定する。

優先度は 1 以上の整数で示され、数字が大きいほど優先度が高い。

implicit 経路が動的経路制御プロトコルで得られた経路または **ip route** コマンドで設定された静的な経路と食い違う場合には、優先度が高い方が採用される。静的な経路と優先度が同じ場合には、静的な経路が優先される。

動的経路制御プロトコルで得られた経路と優先度が同じ場合には、時間的に先に採用された経路が有効となる。

なお、**ip implicit-route preference** コマンドで implicit 経路の優先度を変更しても、その時点で既にルーティングテーブルに登録されている implicit 経路の優先度の変更されない。

**[ノート]**

implicit 経路とは、IP アドレスを設定したインターフェースが有効な状態になったときに暗黙のうちに登録されるそのインターフェースを経由する経路のことである。例えば、IP アドレスを設定した LAN インターフェースがリンクアップ状態のときには、設定した IP アドレスとネットマスクの組み合わせから決定されるネットワークアドレスが、その LAN インターフェースを経由する implicit 経路として登録されている。

**[適用モデル]**

NVR700W

**6.1.37 フローテーブルの各エントリの寿命を設定する****[書式]****ip flow timer protocol time****no ip flow timer protocol [time]****[設定値及び初期値]**

- *protocol* : 寿命を指定するプロトコル

- [設定値] :

| 設定値  | 説明                          |
|------|-----------------------------|
| tcp  | TCP パケット                    |
| udp  | UDP パケット                    |
| icmp | ICMP パケット                   |
| slow | FIN/RST ビットのセットされた TCP パケット |

- [初期値] :

- tcp = 900
- udp = 30
- icmp = 30
- slow = 30

- *time*

- [設定値] : 秒数 (1-21474836)
- [初期値] : -

**[説明]**

フローテーブルの各エントリの寿命をプロトコル毎に設定する。

FIN/RST の通過したエントリには 'slow' が適用される。

NAT や動的フィルターを使用している場合には、それらのエントリの寿命が適用される。

**[適用モデル]**

NVR700W, NVR510

**6.1.38 フローテーブルのエントリー数の設定****[書式]****ip flow limit limit****no ip flow limit [limit]****[設定値及び初期値]**

- *limit*

- [設定値] : 制限値 (10-131072)
- [初期値] : 131072

**[説明]**

IPv4 ファストパスまたは IPv6 ファストパスのそれぞれで使用可能なフローテーブルのエントリー数を設定する。

ファストパス機能使用時でも本制限値を超える分のフローはノーマルパスで処理される。

[適用モデル]  
NVR700W, NVR510

### 6.1.39 フラグメントパケットを再構成するために保持しておく時間を設定

#### [書式]

```
ip reassembly hold-time time
no ip reassembly hold-time [time]
```

#### [設定値及び初期値]

- *time*
- [設定値]:

| 設定値             | 説明                          |
|-----------------|-----------------------------|
| 秒数 ( 1 .. 255 ) | フラグメントパケットを再構成するために保持しておく時間 |

- [初期値]: 15 秒

#### [説明]

IPv4 のフラグメントパケットを再構成するために保持しておく時間。  
設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。  
コマンド実行時にすでに保持していたパケットについては変更しない。

#### [ノート]

NVR700W は Rev.15.00.16 以降で使用可能。  
NVR510 は Rev.15.01.15 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 6.1.40 IP パケットの DS フィールドの書き換えの設定

#### [書式]

```
ip dscp supersede id dscp filter_num [filter_num_list]
no ip dscp supersede id [dscp]
```

#### [設定値及び初期値]

- *id*
  - [設定値]: 識別番号 (1..65535)
  - [初期値]: -
- *dscp*
  - [設定値]:
    - 書き換える DSCP 値 (0..63)
    - 以下のニーモニックが利用できる

| ニーモニック  | DSCP 値 |
|---------|--------|
| default | 0      |
| cs1     | 8      |
| cs2     | 16     |
| cs3     | 24     |
| cs4     | 32     |
| cs5     | 40     |
| cs6     | 48     |
| cs7     | 56     |

| ニーモニック | DSCP 値 |
|--------|--------|
| af11   | 10     |
| af12   | 12     |
| af13   | 14     |
| af21   | 18     |
| af22   | 20     |
| af23   | 22     |
| af31   | 26     |
| af32   | 28     |
| af33   | 30     |
| af41   | 34     |
| af42   | 36     |
| af43   | 38     |
| ef     | 46     |

- [初期値]: -
- *filter\_num*
  - [設定値]: 静的フィルターの番号 (1..21474836)
  - [初期値]: -
- *filter\_num\_list*
  - [設定値]: 静的フィルターの番号 (1..21474836) の並び
  - [初期値]: -

#### [説明]

IP パケットを中継する場合に DS フィールドを指定した値に書き換える。識別番号順にリストをチェックし、*filter\_num* リストのフィルターを順次適用していく。そして、最初にマッチした IP フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

**ip tos supersede** の設定と本コマンドの設定で条件が同じ場合、本コマンドの設定が優先される。

#### [ノート]

NVR700W は Rev.15.00.24 以降で使用可能。

[適用モデル]  
NVR700W

## 6.2 PP 側の設定

### 6.2.1 PP 側 IP アドレスの設定

#### [書式]

```
ip pp remote address ip_address
ip pp remote address dhcpc [interface]
no ip pp remote address [ip_address]
```

#### [設定値及び初期値]

- *ip\_address*
  - [設定値]:



| 設定値     | 説明                         |
|---------|----------------------------|
| IP アドレス | xxx.xxx.xxx.xxx (xxx は十進数) |
| dhcp    | DHCP クライアントを利用することを示すキーワード |

- [初期値]: -
- `dhcp`: DHCP クライアントを利用することを示すキーワード
  - [初期値]: -
- `interface`
  - [設定値]:
    - DHCP クライアントとして動作する LAN インターフェース名
    - 省略時は `lan1`
  - [初期値]: -

#### [説明]

選択されている相手の PP 側の IP アドレスを設定する。

`dhcp` を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。

`dhcp` を設定した場合は、`interface` で指定した LAN インターフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、`0.0.0.0` を割り当てる。

#### [設定例]

ルーター A 側が

```
no ip pp remote address
ppp ipcp ipaddress on
```

と設定し、接続するルーター B 側が

```
ip pp remote address yyy.yyy.yyy.yyy
```

と設定している場合には、実際のルーター A の PP 側の IP アドレスは "`yyy.yyy.yyy.yyy`" になる。

#### [適用モデル]

NVR700W, NVR510

## 6.2.2 リモート IP アドレスプールの設定

#### [書式]

```
ip pp remote address pool ip_address [ip_address...]
ip pp remote address pool ip_address-ip_address
ip pp remote address pool dhcp
ip pp remote address pool dhcpc [interface]
no ip pp remote address pool
```

#### [設定値及び初期値]

- `ip_address`
  - [設定値]: `anonymous` のためにプールする IP アドレス
  - [初期値]: -
- `ip_address-ip_address`
  - [設定値]: IP アドレスの範囲
  - [初期値]: -
- `dhcp`: 自分自身の DHCP サーバー機能を利用することを示すキーワード
  - [初期値]: -
- `dhcpc`: DHCP クライアントを利用することを示すキーワード
  - [初期値]: -
- `interface`
  - [設定値]:

- DHCP クライアントとして動作する LAN インターフェース名、または ONU インターフェース名
- 省略時は `lan1`
- [初期値]:-

**[説明]**

`anonymous` で相手に割り当てるための IP アドレスプールを設定する。PP として `anonymous` が選択された場合のみ有効である。

`dhcp` を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。

`dhcpc` を設定した場合は、`interface` で指定した LAN インターフェース、または ONU インターフェースが DHCP クライアントとして IP アドレス情報のみを取得し、そのアドレスを割り当てる。取得できなかった場合は、`0.0.0.0` を割り当てる。

**[ノート]**

`ip_address` として設定できる数は下記の通り。

| 機種      | ファームウェア         | 最大設定可能数 |
|---------|-----------------|---------|
| NVR700W | Rev.15.00.10 以降 | 33      |
|         | 上記以外            | 19      |
| NVR510  | Rev.15.01.03 以降 | 14      |
|         | 上記以外            | 10      |

**[適用モデル]**

NVR700W, NVR510

### 6.2.3 PP 経由のキープアライブの時間間隔の設定

**[書式]**

**pp keepalive interval** *interval* [`retry-interval=retry-interval`] [`count=count`] [`time=time`]

**no pp keepalive interval** [*interval* [*count*]]

**[設定値及び初期値]**

- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..65535)
  - [初期値]: 30
- *retry-interval*
  - [設定値]:
    - キープアライブパケットの確認に一度失敗した後の送信間隔[秒] (1..65535)
    - キープアライブパケットが確認できれば、送信間隔はまた *interval* に戻る
  - [初期値]: 1
- *count*
  - [設定値]: この回数連続して応答がなければ相手側のルーターをダウンしたと判定する (3..100)
  - [初期値]: 6
- *time*
  - [設定値]:
    - キープアライブパケットの確認に失敗するようになってから回線断と判断するまでの時間[秒] ( $(interval + 1) \cdot 65535$ )
    - *count* パラメーターとは同時には指定できない
  - [初期値]:-

**[説明]**

PP インターフェースでのキープアライブパケットの送信間隔と、回線断と判定するまでの再送回数および時間を設定する。

送信したキープアライブパケットに対して返事が返ってきている間は *interval* で指定した間隔でキープアライブパケットを送信する。一度、返事が確認できなかった時には送信間隔が *retry-interval* パラメーターの値に変更される。*count* パラメーターに示された回数だけ連続して返事が確認できなかった時には回線断と判定する。

回線断判定までの時間を *time* パラメーターで指定した場合には、少なくとも指定した時間の間、キープアライブパケットの返事が連続して確認できない時に回線断と判定する。

[ノート]

*time* パラメーターを指定した場合には、その値はキープアライブの間隔と再送回数によって再計算されるため、設定値とは異なる値が **show config** で表示されることがある。

[適用モデル]

NVR700W, NVR510

## 6.2.4 PP 経由のキープアライブを使用するか否かの設定

[書式]

```
pp keepalive use lcp-echo
pp keepalive use icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]
pp keepalive use lcp-echo icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]
pp keepalive use off
no pp keepalive use
```

[設定値及び初期値]

- lcp-echo : LCP Echo Request/Reply を用いる
  - [初期値] : -
- icmp-echo : ICMP Echo/Reply を用いる
  - [初期値] : -
- dest\_ip
  - [設定値] : キープアライブ確認先の IP アドレス
  - [初期値] : -
- option=value 列
  - [設定値] :

| option     | value | 説明                          |
|------------|-------|-----------------------------|
| upwait     | ミリ秒   | アップ検知のための許容応答時間 (1..10000)  |
| downwait   | ミリ秒   | ダウン検知のための許容応答時間 (1..10000)  |
| disconnect | 秒     | 無応答切断時間 (1..21474836)       |
| length     | バイト   | ICMP Echo パケットの長さ (64-1500) |

- [初期値] : -

[初期設定]

pp keepalive use off

[説明]

選択した相手先に対する接続のキープアライブ動作を設定する。

lcp-echo 指定で、LCP Echo Request/Reply を用い、icmp-echo も指定すれば ICMP Echo/Reply も同時に用いる。icmp-echo を使用する場合には、IP アドレスの設定が必要である。

[ノート]

このコマンドを設定していない場合でも、**pp always-on** コマンドで on と設定していれば、LCP Echo によるキープアライブが実行される。

icmp-echo で確認する IP アドレスに対する経路は、設定される PP インターフェースが送出先となるよう設定される必要がある。

downwait パラメーターで応答時間を制限する場合でも、**pp keepalive interval** コマンドの設定値の方が小さい場合には、**pp keepalive interval** コマンドの設定値が優先される。downwait、upwait パラメーターのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。

disconnect パラメーターは、PPPoE で使用する場合に PPPoE レベルでの再接続が必要な場合に使用する。disconnect パラメーターが設定されている場合に、設定時間内に icmp-echo の応答がない場合、PPPoE レベルで一度切断操作を行うため、**pp always-on** コマンドとの併用により再接続を行うことができる。

他のパラメーターがデフォルト値の場合、disconnect パラメーターは 70 秒程度に設定しておくこと、ダウン検出後の切断動作が確実に行われる。

length パラメーターで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。

**[適用モデル]**

NVR700W, NVR510

## 6.2.5 PP 経由のキープアライブのログをとるか否かの設定

**[書式]**

```
pp keepalive log log
no pp keepalive log [log]
```

**[設定値及び初期値]**

- log
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | ログをとる   |
| off | ログをとらない |

- [初期値]: off

**[説明]**

PP 経由のキープアライブをログにとるか否かを設定する。

**[ノート]**

この設定は、すべての PP で共通に用いられる。

**[適用モデル]**

NVR700W, NVR510

## 6.3 RIP の設定

### 6.3.1 RIP を使用するか否かの設定

**[書式]**

```
rip use use
no rip use [use]
```

**[設定値及び初期値]**

- use
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | RIP を使用する  |
| off | RIP を使用しない |

- [初期値]: off

**[説明]**

RIP を使用するか否かを設定する。この機能を OFF にすると、すべてのインターフェースに対して RIP パケットを送信することはなくなり、受信した RIP パケットは無視される。

**[適用モデル]**

NVR700W, NVR510

### 6.3.2 RIP に関して信用できるゲートウェイの設定

#### [書式]

```
ip interface rip trust gateway [except] gateway [gateway...]
ip pp rip trust gateway [except] gateway [gateway...]
ip tunnel rip trust gateway [except] gateway [gateway...]
no ip interface rip trust gateway [[except] gateway [gateway...]]
no ip pp rip trust gateway [[except] gateway [gateway...]]
no ip tunnel rip trust gateway [[except] gateway [gateway...]]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *gateway*
  - [設定値]: IP アドレス
  - [初期値]: -

#### [説明]

RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。

*except* キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

*except* キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

*gateway* は 10 個まで指定可能。

#### [ノート]

信用できる、あるいは信用できないゲートウェイは設定されておらず、すべてのホストからの RIP を信用できるものとして扱う。

#### [適用モデル]

NVR700W, NVR510

### 6.3.3 RIP による経路の優先度の設定

#### [書式]

```
rip preference preference [invalid-route-reactivate=switch]
no rip preference [preference [invalid-route-reactivate=switch]]
```

#### [設定値及び初期値]

- *preference*
  - [設定値]: 1 以上の数値
  - [初期値]: 1000
- *switch*
  - [設定値]:

| 設定値 | 説明                     |
|-----|------------------------|
| on  | 無効となった RIP 由来の経路を削除しない |
| off | 無効となった RIP 由来の経路を削除する  |

- [初期値]: off

#### [説明]

RIP により得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

RIP で他のルーターから経路を受信しているとき、スタティックや OSPF など RIP より優先度が高く設定されたルーティングプロトコルで同じ経路を受信した場合、通常 RIP により受信した経路は無効となって削除されるが、*invalid-*

`route-reactivate` オプションを *on* で指定している場合、優先度が高い経路が消滅したときに無効になっていた RIP 由来の経路を再有効化する。

#### [ノート]

スタティック経路の優先度は 10000 で固定である。

`invalid-route-reactivate` オプションを *on* で指定しているとき、再有効化した経路を RIP の発信元が広告しなくなっても当該経路がルーティングテーブル上に残り続けることがあるため、`invalid-route-reactivate` オプションは *off* にすることが望ましい。

なお、上記のルーティングテーブルに残った経路は、RIP の使用を停止することで削除できる。

#### [適用モデル]

NVR700W, NVR510

### 6.3.4 RIP パケットの送信に関する設定

#### [書式]

```
ip interface rip send send [version version [broadcast]]
ip pp rip send send [version version [broadcast]]
ip tunnel rip send send [version version [broadcast]]
no ip interface rip send [send...]
no ip pp rip send [send...]
no ip tunnel rip send [send...]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *send*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | RIP パケットを送信する  |
| off | RIP パケットを送信しない |

- [初期値]:
  - off (トンネルインターフェースの場合)
  - on (その他のインターフェースの場合)
- *version*
  - [設定値]: 送信する RIP のバージョン (1,2)
  - [初期値]: 1 (トンネルインターフェース以外の場合)
- *broadcast*
  - [設定値]: `ip interface address` コマンドで指定したブロードキャスト IP アドレス
  - [初期値]: -

#### [説明]

指定したインターフェースに対し、RIP パケットを送信するか否かを設定する。

"`version version`" で送信する RIP のバージョンを指定できる。

#### [適用モデル]

NVR700W, NVR510

### 6.3.5 RIP パケットの受信に関する設定

#### [書式]

```
ip interface rip receive receive [version version [version]]
ip pp rip receive receive [version version [version]]
ip tunnel rip receive receive [version version [version]]
```

**no ip interface rip receive** [*receive...*]

**no ip pp rip receive** [*receive...*]

**no ip tunnel rip receive** [*receive...*]

#### [設定値及び初期値]

- *interface*

- [設定値]: LAN インターフェース名、ONU インターフェース名
- [初期値]: -

- *receive*

- [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | RIP パケットを受信する  |
| off | RIP パケットを受信しない |

- [初期値]:

- off (トンネルインターフェースの場合)
- on (その他のインターフェースの場合)

- *version*

- [設定値]: 受信する RIP のバージョン (1,2)
- [初期値]: 1 2 (トンネルインターフェース以外の場合)

#### [説明]

指定したインターフェースに対し、RIP パケットを受信するか否かを設定する。

"version *version*" で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 ともに受信する。

#### [適用モデル]

NVR700W, NVR510

### 6.3.6 RIP のフィルタリングの設定

#### [書式]

**ip interface rip filter direction filter\_list**

**ip pp rip filter direction filter\_list**

**ip tunnel rip filter direction filter\_list**

**no ip interface rip filter direction [filter\_list]**

**no ip pp rip filter direction filter\_list**

**no ip tunnel rip filter direction filter\_list**

#### [設定値及び初期値]

- *interface*

- [設定値]: LAN インターフェース名、ONU インターフェース名
- [初期値]: -

- *direction*

- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| in  | 受信した RIP のフィルタリング |
| out | 送信する RIP のフィルタリング |

- [初期値]: -

- *filter\_list*

- [設定値]: 空白で区切られた静的フィルター番号の並び (100 個以内)
- [初期値]: -

## [説明]

インターフェースで送受信する RIP のフィルタリングを設定する。

**ip filter** コマンドで設定されたフィルターの始点 IP アドレスが、送受信する RIP の経路情報にマッチする場合は、フィルターが **pass** であればそれを処理し、**reject** であればその経路情報だけを破棄する。

## [適用モデル]

NVR700W, NVR510

### 6.3.7 RIP で加算するホップ数の設定

## [書式]

**ip interface rip hop direction hop**

**ip pp rip hop direction hop**

**ip tunnel rip hop direction hop**

**no ip interface rip hop direction hop**

**no ip pp rip hop direction hop**

**no ip tunnel rip hop direction hop**

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *direction*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| in  | 受信した RIP に加算する |
| out | 送信する RIP に加算する |

- [初期値]: -
- *hop*
  - [設定値]: 加算する値 (0..15)
  - [初期値]: 0

## [説明]

インターフェースで送受信する RIP に加算するホップ数を設定する。

## [適用モデル]

NVR700W, NVR510

### 6.3.8 RIP2 での認証の設定

## [書式]

**ip interface rip auth type type**

**ip pp rip auth type type**

**ip tunnel rip auth type type**

**no ip interface rip auth type [type]**

**no ip pp rip auth type [type]**

**no ip tunnel rip auth type [type]**

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *type*
  - [設定値]:



| 設定値  | 説明          |
|------|-------------|
| text | テキスト型の認証を行う |

- [初期値]:-

#### [説明]

RIP2 を使用する場合のインターフェースでの認証の設定をする。text の場合はテキスト型の認証を行う。

#### [適用モデル]

NVR700W, NVR510

### 6.3.9 RIP2 での認証キーの設定

#### [書式]

```
ip interface rip auth key hex_key
ip pp rip auth key hex_key
ip tunnel rip auth key hex_key
ip interface rip auth key text text_key
ip pp rip auth key text text_key
ip tunnel rip auth key text text_key
no ip interface rip auth key
no ip pp rip auth key
no ip tunnel rip auth key
no ip interface rip auth key text
no ip pp rip auth key text
no ip tunnel rip auth key text
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]:-
- *hex\_key*
  - [設定値]: 十六進数の列で表現された認証キー
  - [初期値]:-
- *text\_key*
  - [設定値]: 文字列で表現された認証キー
  - [初期値]:-

#### [説明]

RIP2 を使用する場合のインターフェースの認証キーを設定する。

#### [設定例]

```
# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

#### [適用モデル]

NVR700W, NVR510

### 6.3.10 RIPv2 での広告動作モードの設定

#### [書式]

```
rip advertise mode mode
no rip advertise mode [mode]
```

#### [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値 | 説明                                                                                |
|-----|-----------------------------------------------------------------------------------|
| 1   | RIP の送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告しない。 |
| 2   | RIP の送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告する。  |

- [初期値]: 1

#### [説明]

RIPv2 で RIP 送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合、当該経路の広告動作を MODE の設定値によって変更する。

本コマンドに対応していないリビジョンでは、MODE の設定値が 1 のときの動作をする。  
RIPv1 の動作には影響はない。

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。NVR510 は Rev.15.01.16 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 6.3.11 回線切断時の経路保持の設定

#### [書式]

```
ip pp rip hold routing rip_hold
no ip pp rip hold routing [rip_hold]
```

#### [設定値及び初期値]

- *rip\_hold*
- [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 回線が切断されても RIP による経路を保持し続ける |
| off | 回線が切断されたら RIP による経路を破棄する   |

- [初期値]: off

#### [説明]

PP インターフェースから RIP で得られた経路を、回線が切断された場合に保持し続けるかどうかを設定する。

#### [適用モデル]

NVR700W, NVR510

### 6.3.12 回線接続時の PP 側の RIP の動作の設定

#### [書式]

```
ip pp rip connect send rip_action
no ip pp rip connect send [rip_action]
```

#### [設定値及び初期値]

- *rip\_action*
- [設定値]:

| 設定値      | 説明                                                          |
|----------|-------------------------------------------------------------|
| interval | <b>ip pp rip connect interval</b> コマンドで設定された時間間隔で RIP を送出する |

| 設定値    | 説明                       |
|--------|--------------------------|
| update | 経路情報が変わった場合にのみ RIP を送出する |
| none   | RIP を送出しない               |

- [初期値] : update

#### [説明]

選択されている相手について回線接続時に RIP を送出する条件を設定する。

#### [設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

#### [適用モデル]

NVR700W, NVR510

### 6.3.13 回線接続時の PP 側の RIP 送出の時間間隔の設定

#### [書式]

```
ip pp rip connect interval time
no ip pp rip connect interval [time]
```

#### [設定値及び初期値]

- *time*
  - [設定値] : 秒数 (30..21474836)
  - [初期値] : 30

#### [説明]

選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。

**ip pp rip send** と **ip pp rip receive** コマンドが on、**ip pp rip connect send** コマンドが interval の時に有効である。

#### [設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

#### [適用モデル]

NVR700W, NVR510

### 6.3.14 回線切断時の PP 側の RIP の動作の設定

#### [書式]

```
ip pp rip disconnect send rip_action
no ip pp rip disconnect send [rip_action]
```

#### [設定値及び初期値]

- *rip\_action*
  - [設定値] :

| 設定値      | 説明                                                             |
|----------|----------------------------------------------------------------|
| none     | 回線切断時に RIP を送出しない                                              |
| interval | <b>ip pp rip disconnect interval</b> コマンドで設定された時間間隔で RIP を送出する |
| update   | 経路情報が変わった時にのみ RIP を送出する                                        |

- [初期値] : none

#### [説明]

選択されている相手について回線切断時に RIP を送出する条件を設定する。

**[設定例]**

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

**[適用モデル]**

NVR700W, NVR510

**6.3.15 回線切断時の PP 側の RIP 送出の時間間隔の設定****[書式]**

```
ip pp rip disconnect interval time
no ip pp rip disconnect interval [time]
```

**[設定値及び初期値]**

- *time*
  - [設定値]: 秒数 (30..21474836)
  - [初期値]: 3600

**[説明]**

選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。

**ip pp rip send** と **ip pp rip receive** コマンドが on、**ip pp rip disconnect send** コマンドで interval の時に有効である。

**[設定例]**

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

**[適用モデル]**

NVR700W, NVR510

**6.3.16 バックアップ時の RIP の送信元インターフェース切り替えの設定****[書式]**

```
ip pp rip backup interface switch
no ip pp rip backup interface
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明     |
|-----|--------|
| on  | 切り替える  |
| off | 切り替えない |

- [初期値]: off

**[説明]**

バックアップ時に RIP の送信元インターフェースを切り替えるか否かを設定する。RIP の送信元インターフェースは、off のときには、バックアップ元のインターフェースであり、on のときには、バックアップ先のインターフェースとなる。

**[ノート]**

両者の違いは、送信元の IP アドレスの違いとなって現れる。off のときには、バックアップ元のインターフェースのアドレスが選ばれ、on のときには、バックアップ先のインターフェースのアドレスが選ばれる。なお、どちらの場合にも、バックアップ回線を通じて RIP が送信される。

**[適用モデル]**

NVR700W

**6.3.17 RIP で強制的に経路を広告する****[書式]**

```
ip interface rip force-to-advertise ip-address/netmask [metric metric]
```

```

ip pp rip force-to-advertise ip-address/netmask [metric metric]
ip tunnel rip force-to-advertise ip-address/netmask [metric metric]
no ip interface rip force-to-advertise ip-address/netmask [metric metric]
no ip pp rip force-to-advertise ip-address/netmask [metric metric]
no ip tunnel rip force-to-advertise ip-address/netmask [metric metric]

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *ip-address/netmask*
  - [設定値]: 強制的に広告したい経路のネットワークアドレスとネットマスク長、または 'default'
  - [初期値]: -
- *metric*
  - [設定値]: 広告する際のメトリック値 (1~15)
  - [初期値]: 1

#### [説明]

設定した経路が経路テーブルに存在しない場合でも、指定されたインターフェースに対し、RIP で経路を強制的に広告する。経路として 'default' を指定した場合にはデフォルト経路が広告される。

#### [設定例]

LAN1 側に、LAN2 の一部のホストだけを広告する。

```

ip lan1 address 192.168.0.1/24
ip lan2 address 192.168.1.1/24

```

```

rip use on
rip filter rule with-netmask
ip lan1 rip send on version 2
ip lan1 rip receive on version 2

```

```

ip filter 1 reject 192.168.1.0/24
ip filter 100 pass *
ip lan1 rip filter out 1 100

```

```

ip lan1 rip force-to-advertise 192.168.1.28/30
ip lan1 rip force-to-advertise 192.168.1.100/32
ip lan1 rip force-to-advertise 192.168.1.101/32

```

#### [適用モデル]

NVR700W, NVR510

### 6.3.18 RIP2 でのフィルターの比較方法

#### [書式]

```

rip filter rule rule
no rip filter rule [rule]

```

#### [設定値及び初期値]

- *rule*
  - [設定値]:

| 設定値          | 説明                                 |
|--------------|------------------------------------|
| address-only | ネットワークアドレスだけを比較対象とする               |
| with-netmask | RIP2 の場合、ネットワークアドレスとネットマスクを比較対象とする |

- [初期値]: address-only

## [説明]

RIP フィルターで、設定されたフィルターと RIP エントリの内容の比較方法を設定する。

| rip filter rule コマンド | プロトコル | 比較方法                                                           |
|----------------------|-------|----------------------------------------------------------------|
| address-only         | RIP1  | ネットマスク型のフィルターは範囲指定と解釈され、RIP エントリのアドレス部がその範囲に入っているかどうかを比較する。    |
|                      | RIP2  |                                                                |
| with-netmask         | RIP1  | ネットマスク型のフィルターの、アドレスとネットマスク、RIP エントリのアドレス、ネットマスクと一致するかどうかを比較する。 |
|                      | RIP2  |                                                                |

## [適用モデル]

NVR700W, NVR510

## 6.3.19 RIP のタイマを調整する

## [書式]

```
rip timer update [invalid [holddown]]
```

```
no rip timer [update]
```

## [設定値及び初期値]

- *update*
  - [設定値]: 定期的な広告の送信間隔 (10~60 (秒))
  - [初期値]: 30 秒
- *invalid*
  - [設定値]: 広告を受け取れなくなってから経路を削除するまでの時間 (30~360 (秒))
  - [初期値]: update×6 (180 秒)
- *holddown*
  - [設定値]: 経路が削除されたときにメトリック 16 で経路を広告する時間 (20~240 (秒))
  - [初期値]: update×4 (120 秒)

## [説明]

RIP のタイマ値を設定する。

*update*、*invalid*、*holddown* の各値の間には以下の不等式が成立している必要がある。

$$\begin{aligned} update \times 3 &\leq invalid \leq update \times 6 \\ update \times 2 &\leq holddown \leq update \times 4 \end{aligned}$$

## [ノート]

PP インターフェースに対し、**ip pp rip connect/disconnect interval** コマンドが設定されているときは、そのコマンドの設定値が **rip timer** コマンドに優先する。ただし、**ip pp rip connect/disconnect interval** コマンドは *update* タイマと *invalid* タイマの値に影響するが、*holddown* タイマの値には影響しない。**ip pp rip connect/disconnect interval** コマンドの設定値を T とした場合、各タイマは以下ようになる。

|                 |                                         |
|-----------------|-----------------------------------------|
| <i>update</i>   | T                                       |
| <i>invalid</i>  | T×6                                     |
| <i>holddown</i> | <b>rip timer</b> コマンドの設定値 (デフォルト 120 秒) |

PP インターフェース以外は該当するコマンドがないため、常に **rip timer** コマンドの設定値が有効である。

## [適用モデル]

NVR700W, NVR510

## 6.4 VRRP の設定

## 6.4.1 インターフェース毎の VRRP の設定

### [書式]

```
ip interface vrrp vrid ip_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
```

```
no ip interface vrrp vrid [vrid...]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*
  - [設定値]: VRRP グループ ID (1..255)
  - [初期値]: -
- *ip\_address*
  - [設定値]: 仮想ルーターの IP アドレス
  - [初期値]: -
- *priority*
  - [設定値]: 優先度 (1..254)
  - [初期値]: 100
- *preempt*: プリエンプトモード
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *auth*
  - [設定値]: テキスト認証文字列 (8 文字以内)
  - [初期値]: -
- *time1*
  - [設定値]: VRRP 広告の送信間隔 (1..60 秒)
  - [初期値]: 1
- *time2*
  - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
  - [初期値]: 3

### [説明]

指定した VRRP グループを利用することを設定する。

同じ VRRP グループに所属するルーターの間では、VRID および仮想ルーターの IP アドレスを一致させておかななくてはならない。これらが食い違った場合の動作は予測できない。

*auth* パラメーターを指定しない場合には、認証なしとして動作する。

*time1* および *time2* パラメーターで、マスターが VRRP 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRP ルーターで一致している必要がある。

### [ノート]

*priority* および *preempt* パラメーターの設定は、仮想ルーターの IP アドレスとして自分自身の LAN インターフェースに付与されているアドレスを指定している場合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。

### [適用モデル]

NVR700W

## 6.4.2 シャットダウントリガーの設定

## [書式]

```

ip interface vrrp shutdown trigger vrid interface
ip interface vrrp shutdown trigger vrid pp peer_num
ip interface vrrp shutdown trigger vrid tunnel tunnel_num
ip interface vrrp shutdown trigger vrid route network [nexthop]
no ip interface vrrp shutdown trigger vrid interface
no ip interface vrrp shutdown trigger vrid pp peer_num
no ip interface vrrp shutdown trigger vrid tunnel tunnel_num
no ip interface vrrp shutdown trigger vrid route network

```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*
  - [設定値]: VRRP グループ ID (1..255)
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: tunnel インターフェース番号
  - [初期値]: -
- *network*
  - [設定値]:
    - ネットワークアドレス
    - IP アドレス/マスク長
    - default
  - [初期値]: -
- *nexthop*
  - [設定値]:
    - インターフェース名
    - IP アドレス
  - [初期値]: -

## [説明]

設定した VRRP グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

| 形式             | 説明                                                                                                                                                                                 |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN インターフェース形式 | 指定した LAN インターフェースがリンクダウンするか、あるいは <b>lan keepalive</b> でダウンが検知されると、シャットダウンする。                                                                                                       |
| pp 形式          | 指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。 <ul style="list-style-type: none"> <li>• <b>pp keepalive use</b> 設定によりダウンが検出された場合</li> </ul> |



| 形式        | 説明                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tunnel 形式 | <p>指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。</p> <ul style="list-style-type: none"> <li>• IPsec トンネルで、<b>ipsec ike keepalive use</b> 設定によりダウンが検出された場合</li> <li>• L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、<b>l2tp keepalive use</b> 設定によりダウンが検出された場合</li> <li>• PPTP トンネルで、<b>pptp keepalive use</b> 設定によりダウンが検出された場合</li> <li>• IPIP トンネルで、<b>ipip keepalive use</b> 設定によりダウンが検出された場合</li> </ul> |
| route 形式  | <p>指定した経路が経路テーブルに存在しないか、<i>nexthop</i> で指定したインターフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。<i>nexthop</i> を省略した場合には、経路がどのような先に向いていても存在する限りはシャットダウンしない。</p>                                                                                                                                                                                                                                           |

[ノート]

tunnel インターフェースは Rev.15.00.14 以降のファームウェアで使用可能。

[適用モデル]

NVR700W

## 6.5 バックアップの設定

### 6.5.1 プロバイダー接続がダウンした時に PP バックアップする接続先の指定

[書式]

```

pp backup none
pp backup pp peer_num [ipsec-fast-recovery=action]
pp backup interface ip_address
pp backup wan_interface
pp backup tunnel tunnel_num
no pp backup
    
```

[設定値及び初期値]

- none : バックアップ動作しない
  - [初期値] : none
- peer\_num
  - [設定値] : バックアップ先として PP を使用する場合の相手先情報番号
  - [初期値] : -
- action : バックアップから復帰した直後に SA の再構築を実施するか否か
  - [設定値] :

| 設定値 | 説明     |
|-----|--------|
| on  | 再構築する  |
| off | 再構築しない |

- [初期値] : off
- interface
  - [設定値] : バックアップ先として使用する LAN インターフェース、ONU インターフェース
  - [初期値] : -
- wan\_interface
  - [設定値] : バックアップ先として使用する WAN インターフェース
  - [初期値] : -

- *ip\_address*
  - [設定値]: ゲートウェイの IP アドレス
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

**[説明]**

PP インターフェースが切断されたときにバックアップするインターフェースを指定する。バックアップ先のインターフェースが PP インターフェースの場合には、`ipsec-fast-recovery` オプションを設定できる。このオプションで `on` を設定したときには、バックアップから復帰した直後に IPsec の SA をすぐに再構築するため、IPsec の通信が可能になるまでの時間を短縮できる。

**[ノート]**

このコマンドは PP インターフェースごとに設定できる。  
PP インターフェースの切断を検知するために `pp always-on` コマンドで `on` を設定する必要がある。

**[適用モデル]**  
NVR700W

## 6.5.2 バックアップからの復帰待ち時間の設定

---

**[書式]**

```
pp backup recovery time time
no pp backup recovery time [time]
```

**[設定値及び初期値]**

- *time*
  - [設定値]:

| 設定値         | 説明    |
|-------------|-------|
| 1..21474836 | 秒数    |
| off         | すぐに復帰 |

- [初期値]: off

**[説明]**

バックアップから復帰する場合には、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

**[ノート]**

この設定は、すべての PP で共通に用いられる。

**[適用モデル]**  
NVR700W

## 6.5.3 LAN 経由でのプロバイダー接続がダウンした時にバックアップする接続先の指定

---

**[書式]**

```
lan backup interface none
lan backup interface pp peer_num
lan backup interface backup_interface ip_address
lan backup interface backup_wan_interface
lan backup interface tunnel tunnel_num
no lan backup interface
```

**[設定値及び初期値]**

- none : バックアップ動作しない
  - [初期値]: none

- *interface*
  - [設定値]: バックアップ対象の LAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: バックアップとして *pp* を使用する場合の相手先情報番号
  - [初期値]: -
- *backup\_interface*
  - [設定値]: バックアップとして使用する LAN インターフェースまたは ONU インターフェース
  - [初期値]: -
- *backup\_wan\_interface*
  - [設定値]: バックアップとして使用する WAN インターフェース
  - [初期値]: -
- *ip\_address*
  - [設定値]: ゲートウェイの IP アドレス
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

指定する LAN インターフェースに対して、LAN 経由でのプロバイダー接続がダウンした場合にバックアップするインターフェース情報を設定する。

#### [ノート]

バックアップ動作のためには、LAN 経由での接続のダウンを検知するために **lan keepalive use** コマンドでの設定が併せて必要である。

#### [適用モデル]

NVR700W

### 6.5.4 バックアップからの復帰待ち時間の設定

---

#### [書式]

```
lan backup recovery time interface time
no lan backup recovery time interface [time]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: バックアップ対象の LAN インターフェース名
  - [初期値]: -
- *time*
  - [設定値]:
    - 秒数 (1..21474836)
    - off
  - [初期値]: off

#### [説明]

指定する LAN インターフェースに対して、バックアップから復帰する場合に、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

#### [適用モデル]

NVR700W

### 6.5.5 LAN 経由のキープアライブを使用するか否かの設定

---

#### [書式]

```
lan keepalive use interface icmp-echo dest_ip [option=value...] [dest_ip [option=value...]]
```

**lan keepalive use interface arp dest\_ip [dest\_ip...]**

**lan keepalive use interface icmp-echo dest\_ip [option=value...] [dest\_ip [option=value...]...] arp dest\_ip [dest\_ip...]**

**lan keepalive use interface off**

**no lan keepalive use interface [...]**

#### [設定値及び初期値]

- *interface*
  - [設定値]: バックアップ対象の LAN インターフェース名
  - [初期値]: -
- *dest\_ip*
  - [設定値]: キープアライブ確認先の IP アドレス
  - [初期値]: -
- *option = value 列*
  - [設定値]:

| <i>option</i> | <i>value</i> | 説明                          |
|---------------|--------------|-----------------------------|
| upwait        | ミリ秒          | アップ検知のための許容応答時間 (1..10000)  |
| downwait      | ミリ秒          | ダウン検知のための許容応答時間 (1..10000)  |
| length        | バイト          | ICMP Echo パケットの長さ (64-1500) |

- [初期値]: -

#### [説明]

指定する LAN インターフェースに対して、キープアライブ動作を行うか否かを設定する。icmp-echo を指定すれば ICMP Echo/Reply を用い、arp を指定すれば ARP Request/Reply を用いる。併記することで併用も可能である。

#### [ノート]

icmp-echo で確認する IP アドレスに対する経路は、バックアップをする LAN インターフェースに向くことが必要である。

downwait パラメーターで応答時間を制限する場合でも、lan keepalive interval コマンドの設定値の方が小さい場合には、lan keepalive interval コマンドの設定値が優先される。downwait、upwait パラメーターのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。

length パラメーターで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。

#### [適用モデル]

NVR700W

## 6.5.6 LAN 経由のキープアライブの時間間隔の設定

#### [書式]

**lan keepalive interval interface interval [count]**

**no lan keepalive interval interface**

#### [設定値及び初期値]

- *interface*
  - [設定値]: バックアップ対象の LAN インターフェース名
  - [初期値]: -
- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔 (1..65535)
  - [初期値]: 30
- *count*
  - [設定値]: ダウン検出を判定する回数 (3..100)
  - [初期値]: 6

**[説明]**

指定する LAN インターフェースに対して、キープアライブパケットの送出間隔とダウン検出を判定する回数を設定する。 *count* に設定した回数だけ連続して応答パケットを検出できない場合に、ダウンと判定する。

一度応答が返ってこないことを検出したら、その後のキープアライブパケットの送出間隔は 1 秒に短縮される。そのため、デフォルトの設定値の場合でもダウン検出に要する時間は 35 秒程度である。

**[適用モデル]**

NVR700W

**6.5.7 LAN 経由のキープアライブのログをとるか否かの設定****[書式]**

**lan keepalive log** *interface log*

**no lan keepalive log** *interface*

**[設定値及び初期値]**

- *interface*
  - [設定値]: バックアップ対象の LAN インターフェース名
  - [初期値]: -
- *log*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | ログをとる   |
| off | ログをとらない |

- [初期値]: off

**[説明]**

キープアライブパケットのログをとるか否かを設定する。

**[適用モデル]**

NVR700W

**6.5.8 ONU 経由でのプロバイダー接続がダウンした時にバックアップする接続先の指定****[書式]**

**onu backup** *interface none*

**onu backup** *interface pp peer\_num*

**onu backup** *interface backup\_interface ip\_address*

**onu backup** *interface backup\_wan\_interface*

**onu backup** *interface tunnel tunnel\_num*

**no onu backup** *interface*

**[設定値及び初期値]**

- *none*: バックアップ動作しない
  - [初期値]: none
- *interface*
  - [設定値]: バックアップ対象の ONU インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: バックアップとして *pp* を使用する場合の相手先情報番号
  - [初期値]: -
- *backup\_interface*
  - [設定値]: バックアップとして使用する LAN インターフェースまたは ONU インターフェース
  - [初期値]: -
- *backup\_wan\_interface*
  - [設定値]: バックアップとして使用する WAN インターフェース
  - [初期値]: -

- *ip\_address*
  - [設定値]: ゲートウェイの IP アドレス
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

**[説明]**

指定する ONU インターフェースに対して、ONU 経由でのプロバイダ接続がダウンした場合にバックアップするインターフェース情報を設定する。

**[ノート]**

バックアップ動作のためには、ONU 経由での接続のダウンを検知するために **onu keepalive use** コマンドの設定が併せて必要である。

**[適用モデル]**

NVR700W

## 6.5.9 バックアップからの復帰待ち時間の設定

---

**[書式]**

```
onu backup recovery time interface time
no onu backup recovery time interface [time]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: バックアップ対象の ONU インターフェース名
  - [初期値]: -
- *time*
  - [設定値]:
    - 秒数 (1..21474836)
    - off
  - [初期値]: off

**[説明]**

指定する ONU インターフェースに対して、バックアップから復帰する場合に、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

**[適用モデル]**

NVR700W

## 6.5.10 ONU 経由のキープアライブを使用するか否かの設定

---

**[書式]**

```
onu keepalive use interface icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]
onu keepalive use interface arp dest_ip [dest_ip...]
onu keepalive use interface icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...] arp dest_ip [dest_ip...]
onu keepalive use interface off
no onu keepalive use interface [...]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: バックアップ対象の ONU インターフェース名
  - [初期値]: -
- *dest\_ip*
  - [設定値]: キープアライブ確認先の IP アドレス
  - [初期値]: -
- *option = value 列*

- [設定値]:

| option   | value | 説明                          |
|----------|-------|-----------------------------|
| upwait   | ミリ秒   | アップ検知のための許容応答時間 (1..10000)  |
| downwait | ミリ秒   | ダウン検知のための許容応答時間 (1..10000)  |
| length   | バイト   | ICMP Echo パケットの長さ (64-1500) |

- [初期値]: -

#### [説明]

指定する ONU インターフェースに対して、キープアライブ動作を行うか否かを設定する。icmp-echo を指定すれば ICMP Echo/Reply を用い、arp を指定すれば ARP Request/Reply を用いる。併記することで併用も可能である。

#### [ノート]

icmp-echo で確認する IP アドレスに対する経路は、バックアップをする ONU インターフェースに向くことが必要である。

downwait パラメーターで応答時間を制限する場合でも、**onu keepalive interval** コマンドの設定値の方が小さい場合には、**onu keepalive interval** コマンドの設定値が優先される。downwait、upwait パラメーターのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。

length パラメーターで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。

#### [適用モデル]

NVR700W, NVR510

### 6.5.11 ONU 経由のキープアライブの時間間隔の設定

#### [書式]

**onu keepalive interval** *interface interval* [*count*]

**no onu keepalive interval** *interface*

#### [設定値及び初期値]

- *interface*
  - [設定値]: バックアップ対象の onu インターフェース名
  - [初期値]: -
- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔 (1..65535)
  - [初期値]: 30
- *count*
  - [設定値]: ダウン検出を判定する回数 (3..100)
  - [初期値]: 6

#### [説明]

指定する ONU インターフェースに対して、キープアライブパケットの送出間隔とダウン検出を判定する回数を設定する。*count* に設定した回数だけ連続して応答パケットを検出できない場合に、ダウンと判定する。

一度応答が返ってこないことを検出したら、その後のキープアライブパケットの送出間隔は 1 秒に短縮される。そのため、デフォルトの設定値の場合でもダウン検出に要する時間は 35 秒程度である。

#### [適用モデル]

NVR700W, NVR510

### 6.5.12 ONU 経由のキープアライブのログをとるか否かの設定

#### [書式]

**onu keepalive log** *interface log*

**no onu keepalive log** *interface*

**[設定値及び初期値]**

- *interface*
  - [設定値]: バックアップ対象の ONU インターフェース名
  - [初期値]: -
- *log*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | ログをとる   |
| off | ログをとらない |

- [初期値]: off

**[説明]**

キーペアライブパケットのログをとるか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 6.6 パケット転送フィルターの設定

---

### 6.6.1 パケット転送フィルターの定義

---

**[書式]**

```
ip forward filter id order gateway gateway filter filter_id ... [keepalive keepalive_id ]
no ip forward filter id order[gateway gateway [filter filter_id ...] [keepalive keepalive_id ]]
```

**[設定値及び初期値]**

- *id*
  - [設定値]: パケット転送フィルターの識別子 (1..255)
  - [初期値]: -
- *order*
  - [設定値]: 評価の順番 (1..255)
  - [初期値]: -
- *gateway*
  - [設定値]:

| 設定値       | 説明                       |
|-----------|--------------------------|
| IP アドレス   | パケットを転送するゲートウェイの IP アドレス |
| wan1      | WAN インターフェース             |
| pp 番号     | PP インターフェース              |
| tunnel 番号 | TUNNEL インターフェース          |

- [初期値]: -
- *filter\_id*
  - [設定値]: **ip filter** コマンドの識別子
  - [初期値]: -
- *keepalive\_id*
  - [設定値]: **ip keepalive** コマンドの識別子
  - [初期値]: -

**[説明]**

パケット転送フィルターを定義する。

*id* パラメーターは、複数のパケット転送フィルターをグループ化するための識別子である。

同じインターフェースに対して複数のパケット転送フィルターを設定するときには、それらのすべてに対して、同じ番号を指定しなければならない。



*order* パラメーターは、評価の順番を示すもので、若い番号を持つものほど優先的に採用される。

*filter\_id* パラメーターとしては、**ip filter** コマンドの識別子を最大 16 個まで指定できる。

複数の識別子を指定したときには、前にあるものが優先的に評価される。

前から順に対応する **ip filter** コマンドを調べ、パケットの内容と合致すれば、その **ip filter** コマンドの設定を採用する。

**ip filter** コマンドの動作が **reject** であれば、パケットを転送せずに破棄し、そうでなければ、*gateway* パラメーターで指定したゲートウェイにパケットを転送する。

*keepalive\_id* には、**ip keepalive** コマンドの識別子を指定する。

ここで指定した IP キープアライブの結果が **down** であれば、このゲートウェイを使用しない。

つまり、該当する **ip filter** コマンドがあったとしても、該当しなかったものとして扱う。

なお、実際に動作させるためには、**ip interface forward filter** コマンドも設定する必要がある。

[適用モデル]

NVR700W

## 6.6.2 インターフェースへのパケット転送フィルターの適用

---

[書式]

**ip interface forward filter** *id*

**ip pp forward filter** *id*

**ip tunnel forward filter** *id*

**ip local forward filter** *id*

**no ip interface forward filter** [*id*]

**no ip pp forward filter** [*id*]

**no ip tunnel forward filter** [*id*]

**no ip local forward filter** [*id*]

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *id*
  - [設定値]: **ip forward filter** コマンドで指定したパケット転送フィルターの識別子 (1..255)
  - [初期値]: -

[説明]

インターフェースにパケット転送フィルターを適用する。

指定したインターフェースで受信したパケットを、指定したパケット転送フィルターの設定と比較し、転送先のゲートウェイを決定する。

**ip local forward filter** コマンドは自分自身が送信するパケットを対象にするときに指定する。

[適用モデル]

NVR700W

## 第 7 章

### イーサネットフィルターの設定

#### 7.1 フィルター定義の設定

##### [書式]

```
ethernet filter num kind src_mac [dst_mac [offset byte_list]]
```

```
ethernet filter num kind type [scope] [offset byte_list]
```

```
no ethernet filter num [kind ...]
```

##### [設定値及び初期値]

- *num*
  - [設定値]: 静的フィルターの番号 ( 1-512 )
  - [初期値]: -
- *kind*
  - [設定値]:

| 設定値                  | 説明                     |
|----------------------|------------------------|
| pass, pass-nolog     | 一致すれば通す ( ログに記録しない )   |
| pass-log             | 一致すれば通す ( ログに記録する )    |
| reject, reject-nolog | 一致すれば破棄する ( ログに記録しない ) |
| reject-log           | 一致すれば破棄する ( ログに記録する )  |

- [初期値]: -
- *src\_mac*
  - [設定値]:
    - 始点 MAC アドレス
    - xx:xx:xx:xx:xx:xx (xx は 16 進数、または \*)
    - \*(すべての MAC アドレスに対応)
  - [初期値]: -
- *dst\_mac*
  - [設定値]:
    - 終点 MAC アドレス
    - 始点 MAC アドレス *src\_mac* と同じ形式
    - 省略時は一個の \* と同じ
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値           | 説明                                  |
|---------------|-------------------------------------|
| dhcp-bind     | 指定された DHCP スコープで予約設定されているホストを対象にする  |
| dhcp-not-bind | 指定された DHCP スコープで予約設定されていないホストを対象にする |

- [初期値]: -
- *scope*
  - [設定値]:
    - DHCP スコープ
    - 1..65535 の整数
    - DHCP スコープのリース範囲に含まれる IP アドレス
  - [初期値]: -
- *offset*

- [設定値]: オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とする)
- [初期値]: -
- *byte\_list*
  - [設定値]:
    - バイト列
    - xx(2 桁の 16 進数) あるいは \*(任意のバイト) をカンマで区切った並び (16 個以内)
  - [初期値]: -

### [説明]

イーサネットフレームのフィルターを設定する。本コマンドで設定されたフィルターは、**ethernet lan filter** コマンドで用いられる。

通常型のフィルターでは、始点 MAC アドレス、終点 MAC アドレスなどで送受信するイーサネットフレームにフィルターを適用する。

dhcp-bind 型のフィルターでは、以下のイーサネットフレームにフィルターを適用する。対象とならないイーサネットフレームはフィルターに合致しないものとして扱う。

- 以下のいずれかに該当する、IPv4 パケットの場合
- イーサネットタイプが IPv4(0x0800)
- PPPoE 環境で、イーサネットタイプが PPPoE データフレーム (0x8864)、プロトコル ID が IPv4(0x0800)
- 802.1Q タグ VLAN 環境で、TPID が 802.1Q タグ (0x8100)、イーサネットタイプが IPv4(0x0800)

イーサネットフレームの始点 MAC アドレスと始点 IP アドレスの組が、対象となる DHCP スコープで予約されているならフィルターに合致するとみなす。

- イーサネットタイプが、以下のいずれかの場合
- ARP(0x0806)
- RARP(0x8035)
- PPPoE 制御パケット (0x8863)
- MAC レイヤ制御パケット (0x8808)

イーサネットフレームの始点 MAC アドレスが、対象となる DHCP スコープで予約されているならフィルターに合致するとみなす。

dhcp-not-bind 型のフィルターでは、以下のイーサネットフレームにフィルターを適用する。対象とならないイーサネットフレームはフィルターに合致しないものとして扱う。

- イーサネットタイプが IPv4(0x0800) である場合

dhcp-bind、dhcp-not-bind 型のフィルターで対象とする DHCP スコープは、*scope* パラメーターで指定する。

*scope* パラメーターとしては DHCP スコープ番号を指定することもできるし、DHCP スコープが定義されているサブネットに含まれる IP アドレスで指定することもできる。IP アドレスで DHCP スコープを指定する場合には、複数の DHCP スコープが該当する時には、その中で最も長いネットマスク長を持つ DHCP スコープを選択する。

*scope* パラメーターを省略した場合には、フィルターが適用されるインターフェースで使用される DHCP スコープがすべて対象となる。

dhcp-bind、dhcp-not-bind 型のフィルターが DHCP リレーエージェントとして動作しているルーターに設定された場合、DHCP サーバーから DHCP スコープとその DHCP スコープにおけるクライアントの予約情報を取得し、フィルターの適用時に参照する。DHCP サーバーからの DHCP スコープおよび予約情報の取得は、DHCP メッセージをリレーする際、DHCP メッセージのオプション部に予約情報を書き込んで通知することにより行われる。

### [ノート]

LAN 分割機能を使用する場合には、ルーター内部でイーサネットタイプとして 0x8100~0x810f の値を使用しているため、それらのイーサネットフレームをフィルターして送受信できないようにすると、LAN 分割機能を使用しているポートで通信できなくなるので注意が必要である。

dhcp-bind、dhcp-not-bind 型のフィルターでは、イーサネットフレームの始点 MAC アドレスや始点 IP アドレスを用いてフィルターの判定をするため、**ethernet lan filter** コマンドでは通常 in 方向にのみ使用することになる。out 方向の場合、始点 MAC アドレスはルーター自身の MAC アドレスになるため、DHCP の予約情報もしくはリースしたアドレスと一致することはない。

dhcp-bind 型フィルターは、予約もしくはアドレスがリースされているクライアントだけを通過させる、という形になるため、通常は pass 等と組み合わせて使用する。一方、dhcp-not-bind 型フィルターは、予約もしくはアドレスが

リースされていないクライアントを破棄する、という形になるため、通常は `reject` 等と組み合わせて使用することになる。

**[適用モデル]**

NVR700W, NVR510

## 7.2 インターフェースへの適用の設定

**[書式]**

`ethernet interface filter dir list`

`no ethernet interface filter dir [list]`

**[設定値及び初期値]**

- `interface`
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- `dir`
  - [設定値]:

| 設定値 | 説明                       |
|-----|--------------------------|
| in  | LAN 側から入ってくるパケットのフィルタリング |
| out | LAN 側に出ていくパケットのフィルタリング   |

- [初期値]: -
- `list`
  - [設定値]: 空白で区切られた静的フィルター番号の並び (512 個以内)
  - [初期値]: -

**[説明]**

LAN 側を通るパケットについて、`ethernet filter` コマンドによるパケットのフィルターを組み合わせ、通過するパケットの種類を制限する。

**[ノート]**

NVR510 では LAN インターフェース名に VLAN インターフェースは指定できない。

**[適用モデル]**

NVR700W, NVR510

## 7.3 イーサネットフィルターの状態の表示

**[書式]**

`show status ethernet filter type [scope]`

**[設定値及び初期値]**

- `type`
  - [設定値]:

| 設定値        | 説明                               |
|------------|----------------------------------|
| dhcp-bind  | 指定された DHCP スコープで予約設定されているホスト     |
| dhcp-scope | 指定された DHCP スコープでアドレスがリースされているホスト |

- [初期値]: -
- `scope`
  - [設定値]: スコープ番号 (1-65535)
  - [初期値]: -

**[説明]**

イーサネットフィルターの情報を表示する。

[適用モデル]  
NVR700W, NVR510

## 第 8 章

### URL フィルターの設定

#### 8.1 フィルター定義の設定

##### [書式]

```
url filter id kind keyword [src_addr[/mask]]
```

```
no url filter id
```

##### [設定値及び初期値]

- *id*
  - [設定値]: フィルター番号 (1..21474836)
  - [初期値]: -
- *kind*
  - [設定値]:

| 設定値                | 説明                   |
|--------------------|----------------------|
| pass, pass-nolog   | 一致すれば通す (ログに記録しない)   |
| pass-log           | 一致すれば通す (ログに記録する)    |
| reject, reject-log | 一致すれば破棄する (ログに記録する)  |
| reject-nolog       | 一致すれば破棄する (ログに記録しない) |

- [初期値]: -
- *keyword*
  - [設定値]:

| 設定値    | 説明                                    |
|--------|---------------------------------------|
| 任意の文字列 | フィルタリングする URL の全部もしくは一部 (半角 255 文字以内) |
| *      | すべての URL に対応                          |

- [初期値]: -
- *src\_addr*: IP パケットの始点 IP アドレス
  - [設定値]:

| 設定値           | 説明                                                                          |
|---------------|-----------------------------------------------------------------------------|
| 任意の IPv4 アドレス | 1 個の IPv4 アドレス                                                              |
| 範囲指定          | 間に - (ハイフン) を挟んだ 2 つの IP アドレス、- を後ろにつけた IP アドレス、または - を前につけた IP アドレス (範囲指定) |
| *             | すべての IP アドレスに対応                                                             |
| 省略            | 省略時は * と同じ                                                                  |

- [初期値]: -
- *mask*
  - [設定値]: ネットマスク長 (*src\_addr* がネットワークアドレスの場合のみ指定可)
  - [初期値]: -

##### [説明]

URL によるフィルターを設定する。本コマンドで設定されたフィルターは、**url interface filter** コマンドで用いられる。

指定されたキーワードに、大文字のアルファベットが含まれる場合、それらを小文字に変換して保存する。

## [ノート]

`src_addr` はコンマ (,) で区切って複数指定することができる。

## [適用モデル]

NVR700W

## 8.2 URL フィルターのインターフェースへの適用

## [書式]

```
url interface filter dir list
```

```
url pp filter dir list
```

```
url tunnel filter dir list
```

```
no url interface filter dir
```

```
no url pp filter dir
```

```
no url tunnel filter dir
```

## [設定値及び初期値]

- `interface`
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- `dir`
  - [設定値]:

| 設定値 | 説明                          |
|-----|-----------------------------|
| in  | 入力方向の HTTP コネクションをフィルタリングする |
| out | 出力方向の HTTP コネクションをフィルタリングする |

- [初期値]: -
- `list`
  - [設定値]: 空白で区切られた URL フィルター番号の並び (128 個以内)
  - [初期値]: -

## [説明]

`url filter` コマンドで設定したフィルターを組み合わせ、インターフェースで送受信する HTTP パケットの URL によって制限を行う。

設定できるフィルターの数は、128 個以内、またはコマンドライン文字列長 (4095 文字) で入力できる範囲内である。指定されたすべてのフィルターにマッチしないパケットは破棄される。

## [適用モデル]

NVR700W

## 8.3 URL フィルターでチェックを行う HTTP のポート番号の設定

## [書式]

```
url filter port list
```

```
no url filter port
```

## [設定値及び初期値]

- `list`
  - [設定値]: 空白で区切られたポート番号の並び (4 個以内)
  - [初期値]: 80

## [説明]

URL フィルターでチェックを行う HTTP のポート番号を設定する。

## [適用モデル]

NVR700W

## 8.4 URL フィルターを使用するか否かの設定

### [書式]

```
url filter use switch
```

```
no url filter use
```

### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | URL フィルターを使用する  |
| off | URL フィルターを使用しない |

- [初期値]: on

### [説明]

URL フィルターを使用するか否かを設定する。

### [適用モデル]

NVR700W

## 8.5 URL フィルターで破棄するパケットの送信元に HTTP レスポンスを返す動作の設定

### [書式]

```
url filter reject redirect
```

```
url filter reject redirect url
```

```
url filter reject off
```

```
no url filter reject [action]
```

### [設定値及び初期値]

- *redirect*: HTTP リダイレクトの HTTP レスポンスを返し、ブロック画面へ転送する
  - [初期値]: *redirect*
- *off*: HTTP レスポンスは返さずに、TCP RST によって TCP セッションを終了する
  - [初期値]: -
- *url*
  - [設定値]: リダイレクトする URL(<http://> または <https://> で始まる文字列で、半角 255 文字以内)
  - [初期値]: -
- *action*
  - [設定値]:
    - *redirect*
    - *off*
  - [初期値]: -

### [説明]

URL フィルターで破棄するパケットの送信元に HTTP レスポンスを返す動作を設定する。ブロック画面には、一致したキーワードまたは、アクセスを遮断した理由を表示する。

*url* を指定した場合、実際にリダイレクトするときには指定した *url* の後ろに "?" に続けて以下の内容のクエリを付加する。

- アクセスを遮断した URL
- マッチしたフィルターに設定されているキーワード

*url* に <http://> または <https://> で始まる文字列以外を設定することはできない。

### [ノート]

*redirect* を設定して Web ブラウザにブロック画面を表示する場合、**httpd service on** コマンドの設定が必要である。



[適用モデル]  
NVR700W

## 8.6 フィルターにマッチした際にログを出力するか否かの設定

---

[書式]

`url filter log switch`

`no url filter log`

[設定値及び初期値]

• `switch`

• [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | フィルターにマッチした際にログを出力する  |
| off | フィルターにマッチした際にログを出力しない |

• [初期値]: on

[説明]

フィルターにマッチした際にログを出力するか否かを設定する。

[ノート]

onを設定した場合でも、`url filter` コマンドで `kind` に `pass`、`pass-nolog`、または `reject-nolog` を指定したフィルターにマッチした場合はログを出力しない。

[適用モデル]  
NVR700W

## 第 9 章

### PPP の設定

#### 9.1 相手の名前とパスワードの設定

##### [書式]

```
pp auth username username password [myname myname mypass] [ip_address] [ip6_prefix]
no pp auth username username [password...]
```

##### [設定値及び初期値]

- *username*
  - [設定値]: 名前 (64 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (64 文字以内)
  - [初期値]: -
- *myname*: 自分側の設定を入力するためのキーワード
  - [初期値]: -
- *myname*
  - [設定値]: 自分側のユーザー名
  - [初期値]: -
- *mypass*
  - [設定値]: 自分側のパスワード
  - [初期値]: -
- *ip\_address*
  - [設定値]: 相手に割り当てる IP アドレス
  - [初期値]: -
- *ip6\_prefix*
  - [設定値]: ユーザーに割り当てるプレフィックス
  - [初期値]: -

##### [説明]

相手の名前とパスワードを設定する。複数の設定が可能。オプションで自分側の設定も入力ができる。

双方向で認証を行う場合には、相手のユーザー名が確定してから自分を相手に認証させるプロセスが動き始める。これらのパラメーターが設定されていない場合には、**pp auth myname** コマンドの設定が参照される。

##### [適用モデル]

NVR700W, NVR510

#### 9.2 受け入れる認証タイプの設定

##### [書式]

```
pp auth accept accept [accept]
no pp auth accept [accept]
```

##### [設定値及び初期値]

- *accept*
  - [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| pap | PAP による認証を受け入れる |

| 設定値       | 説明                          |
|-----------|-----------------------------|
| chap      | CHAP による認証を受け入れる            |
| mschap    | MSCHAP による認証を受け入れる          |
| mschap-v2 | MSCHAP Version2 による認証を受け入れる |

- [初期値]: 認証を受け入れない

#### [説明]

相手からの PPP 認証要求を受け入れるかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。

このコマンドで認証を受け入れる設定になっていても、**pp auth myname** コマンドで自分の名前とパスワードが設定されていなければ、認証を拒否する。

PP 毎のコマンドである。

#### [適用モデル]

NVR700W, NVR510

## 9.3 要求する認証タイプの設定

#### [書式]

```
pp auth request auth [arrive-only]
```

```
no pp auth request [auth[arrive-only]]
```

#### [設定値及び初期値]

- *auth*

- [設定値]:

| 設定値       | 説明                         |
|-----------|----------------------------|
| pap       | PAP による認証を要求する             |
| chap      | CHAP による認証を要求する            |
| mschap    | MSCHAP による認証を要求する          |
| mschap-v2 | MSCHAP Version2 による認証を要求する |
| chap-pap  | CHAP もしくは PAP による認証を要求する   |

- [初期値]: -

#### [説明]

選択された相手について PAP と CHAP による認証を要求するかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。

chap-pap キーワードの場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。

arrive-only キーワードが指定された場合には、着信時にのみ PPP による認証を要求するようになり、発信時には要求しない。

#### [適用モデル]

NVR700W, NVR510

## 9.4 自分の名前とパスワードの設定

### [書式]

```
pp auth myname myname password
no pp auth myname [myname password]
```

### [設定値及び初期値]

- *myname*
  - [設定値]: 名前 (64 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (64 文字以内)
  - [初期値]: -

### [説明]

PAP または CHAP で相手に送信する自分の名前とパスワードを設定する。  
PP 毎のコマンドである。

### [適用モデル]

NVR700W, NVR510

## 9.5 同一 username を持つ相手からの二重接続を禁止するか否かの設定

### [書式]

```
pp auth multi connect prohibit prohibit
no pp auth multi connect prohibit [prohibit]
```

### [設定値及び初期値]

- *prohibit*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 禁止する  |
| off | 禁止しない |

- [初期値]: off

### [説明]

**pp auth username** コマンドで登録した同一 *username* を持つ相手からの二重接続を禁止するか否かを設定する。

### [ノート]

定額制プロバイダーを営む場合に便利である。ユーザー管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバーの方で対処する必要がある。  
*anonymous* が選択された場合のみ有効である。  
なお、NVR510 では RADIUS を使用したログインユーザーの管理はできない。

### [適用モデル]

NVR700W, NVR510

## 9.6 常時接続の設定

### [書式]

```
pp always-on switch [time]
no pp always-on
```

### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 常時接続する  |
| off | 常時接続しない |

- [初期値]: off
- *time*
  - [設定値]: 再接続を要求するまでの秒数 (60..21474836)
  - [初期値]: -

#### [説明]

選択されている相手について常時接続するか否かを設定する。また、常時接続での通信終了時に再接続を要求するまでの時間間隔を指定する。

常時接続に設定されている場合には、起動時に接続を起動し、通信終了時には再接続を起動し、キープアライブ機能により接続相手のダウン検出を行う。接続失敗時あるいは通信の異常終了時には *time* に設定された時間間隔を待った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。*switch* が on に設定されている場合には、*time* の設定が有効となる。*time* が設定されていない場合、*time* は 60 になる。

以下のコマンドが設定されている場合、*switch* を on に設定した時点で接続処理が行われる。

- PPPoE 接続
  - **pppoe use**
  - **pp enable**
- モバイルインターネット接続 (携帯端末を PP (USB モデム) として制御するタイプ)
  - **pp bind usb1**
  - **pp enable**
  - **mobile use**

また、上記の設定に依らず、*switch* を off に設定した時点で切断処理が行われる。

#### [ノート]

PP 毎のコマンドである。

PP として *anonymous* が選択された時には無効である。

#### [適用モデル]

NVR700W, NVR510

## 9.7 LCP 関連の設定

### 9.7.1 Address and Control Field Compression オプション使用の設定

#### [書式]

```
ppp lcp acfc acfc
no ppp lcp acfc [acfc]
```

#### [設定値及び初期値]

- *acfc*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: off

#### [説明]

選択されている相手について[PPP,LCP]の Address and Control Field Compression オプションを用いるか否かを設定する。

## [ノート]

on を設定していても相手に拒否された場合は用いない。

## [適用モデル]

NVR700W, NVR510

## 9.7.2 Magic Number オプション使用の設定

## [書式]

```
ppp lcp magicnumber magicnumber
```

```
no ppp lcp magicnumber [magicnumber]
```

## [設定値及び初期値]

- *magicnumber*

- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: on

## [説明]

選択されている相手について[PPP,LCP]の Magic Number オプションを用いるか否かを設定する。

## [ノート]

on を設定していても相手に拒否された場合は用いない。

## [適用モデル]

NVR700W, NVR510

## 9.7.3 Maximum Receive Unit オプション使用の設定

## [書式]

```
ppp lcp mru mru [length]
```

```
no ppp lcp mru [mru [length]]
```

## [設定値及び初期値]

- *mru*

- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: on

- *length*

- [設定値]: MRU の値 (1280..1792)

- [初期値]: 1792

## [説明]

選択されている相手について[PPP,LCP]の Maximum Receive Unit オプションを用いるか否かと、MRU の値を設定する。

## [ノート]

on を設定していても相手に拒否された場合は用いない。一般には on でよいが、このオプションをつけると接続できないルーターに接続する場合には off にする。

データ圧縮を利用する設定の場合には、*length* パラメーターの設定は常に 1792 として動作する。

## [適用モデル]

NVR700W, NVR510

## 9.7.4 Protocol Field Compression オプション使用の設定

### [書式]

```
ppp lcp pfc pf
no ppp lcp pfc [pf]
```

### [設定値及び初期値]

- *pf*
- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: off

### [説明]

選択されている相手について[PPP,LCP]の Protocol Field Compression オプションを用いるか否かを設定する。

### [ノート]

on を設定していても相手に拒否された場合は用いない。

### [適用モデル]

NVR700W, NVR510

## 9.7.5 lcp-restart パラメーターの設定

### [書式]

```
ppp lcp restart time
no ppp lcp restart [time]
```

### [設定値及び初期値]

- *time*
- [設定値]: ミリ秒 (20..10000)
- [初期値]: 3000

### [説明]

選択されている相手について[PPP,LCP]の configure-request、terminate-request の再送時間を設定する。

### [適用モデル]

NVR700W, NVR510

## 9.7.6 lcp-max-terminate パラメーターの設定

### [書式]

```
ppp lcp maxterminate count
no ppp lcp maxterminate [count]
```

### [設定値及び初期値]

- *count*
- [設定値]: 回数 (1..10)
- [初期値]: 2

### [説明]

選択されている相手について[PPP,LCP]の terminate-request の送信回数を設定する。

### [適用モデル]

NVR700W, NVR510

## 9.7.7 lcp-max-configure パラメーターの設定

### [書式]

```
ppp lcp maxconfigure count
no ppp lcp maxconfigure [count]
```

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,LCP]の configure-request の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.7.8 lcp-max-failure パラメーターの設定

---

**[書式]**

```
ppp lcp maxfailure count
no ppp lcp maxfailure [count]
```

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,LCP]の configure-nak の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.7.9 Configure-Request をすぐに送信するか否かの設定

---

**[書式]**

```
ppp lcp silent switch
no ppp lcp silent [switch]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明                                                                          |
|-----|-----------------------------------------------------------------------------|
| on  | PPP/LCP で、回線接続直後の Configure-Request の送信を、相手から Configure-Request を受信するまで遅らせる |
| off | PPP/LCP で、回線接続直後に Configure-Request を送信する                                   |

- [初期値]: off

**[説明]**

PPP/LCP で、回線接続後 Configure-Request をすぐに送信するか、あるいは相手から Configure-Request を受信するまで遅らせるかを設定する。通常は回線接続直後に Configure-Request を送信して構わないが、接続相手によってはこれを遅らせた方がよいものがある。

**[適用モデル]**

NVR700W, NVR510

## 9.8 PAP 関連の設定

---

### 9.8.1 pap-restart パラメーターの設定

---

**[書式]**

```
ppp pap restart time
no ppp pap restart [time]
```



**[設定値及び初期値]**

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

選択されている相手について[PPP,PAP]authenticate-request の再送時間を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.8.2 pap-max-authreq パラメーターの設定

---

**[書式]**

```
ppp pap maxauthreq count  
no ppp pap maxauthreq [count]
```

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,PAP]authenticate-request の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.9 CHAP 関連の設定

---

### 9.9.1 chap-restart パラメーターの設定

---

**[書式]**

```
ppp chap restart time  
no ppp chap restart [time]
```

**[設定値及び初期値]**

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

選択されている相手について[PPP,CHAP]challenge の再送時間を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.9.2 chap-max-challenge パラメーターの設定

---

**[書式]**

```
ppp chap maxchallenge count  
no ppp chap maxchallenge [count]
```

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,CHAP]challenge の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.10 IPCP 関連の設定

### 9.10.1 Van Jacobson Compressed TCP/IP 使用の設定

#### [書式]

```
ppp ipcp vjc compression
no ppp ipcp vjc [compression]
```

#### [設定値及び初期値]

- *compression*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

#### [説明]

選択されている相手について[PPP,IPCP]Van Jacobson Compressed TCP/IP を使用するか否かを設定する。

#### [ノート]

on を設定していても相手に拒否された場合は用いない。

#### [適用モデル]

NVR700W, NVR510

### 9.10.2 PP 側 IP アドレスのネゴシエーションの設定

#### [書式]

```
ppp ipcp ipaddress negotiation
no ppp ipcp ipaddress [negotiation]
```

#### [設定値及び初期値]

- *negotiation*

- [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| on  | ネゴシエーションする  |
| off | ネゴシエーションしない |

- [初期値]: off

#### [説明]

選択されている相手について PP 側 IP アドレスのネゴシエーションをするか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

### 9.10.3 ipcp-restart パラメーターの設定

#### [書式]

```
ppp ipcp restart time
no ppp ipcp restart [time]
```

#### [設定値及び初期値]

- *time*

- [設定値]: ミリ秒 (20..10000)
- [初期値]: 3000

#### [説明]

選択されている相手について[PPP,IPCP]の configure-request、terminate-request の再送時間を設定する。

[適用モデル]  
NVR700W, NVR510

#### 9.10.4 ipcp-max-terminate パラメーターの設定

---

[書式]

```
ppp ipcp maxterminate count
no ppp ipcp maxterminate [count]
```

[設定値及び初期値]

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 2

[説明]

選択されている相手について[PPP,IPCP]の terminate-request の送信回数を設定する。

[適用モデル]  
NVR700W, NVR510

#### 9.10.5 ipcp-max-configure パラメーターの設定

---

[書式]

```
ppp ipcp maxconfigure count
no ppp ipcp maxconfigure [count]
```

[設定値及び初期値]

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

[説明]

選択されている相手について[PPP,IPCP]の configure-request の送信回数を設定する。

[適用モデル]  
NVR700W, NVR510

#### 9.10.6 ipcp-max-failure パラメーターの設定

---

[書式]

```
ppp ipcp maxfailure count
no ppp ipcp maxfailure [count]
```

[設定値及び初期値]

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

[説明]

選択されている相手について[PPP,IPCP]の configure-nak の送信回数を設定する。

[適用モデル]  
NVR700W, NVR510

#### 9.10.7 WINS サーバーの IP アドレスの設定

---

[書式]

```
wins server server1 [server2]
no wins server [server1 [server2]]
```

[設定値及び初期値]

- *server1*, *server2*
  - [設定値]: IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
  - [初期値]: -

**[説明]**

WINS(Windows Internet Name Service) サーバーの IP アドレスを設定する。

**[ノート]**

IPCP の MS 拡張オプションおよび DHCP でクライアントに渡すための WINS サーバーの IP アドレスを設定する。ルーターはこのサーバーに対し WINS クライアントとしての動作は一切行わない。

**[適用モデル]**

NVR700W, NVR510

### 9.10.8 IPCP の MS 拡張オプションを使うか否かの設定

---

**[書式]**

```
ppp ipcp msex msex
```

```
no ppp ipcp msex [msex]
```

**[設定値及び初期値]**

- *msex*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

選択されている相手について、[PPP,IPCP]の MS 拡張オプションを使うか否かを設定する。

IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバーの IP アドレスと WINS(Windows Internet Name Service) サーバーの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバーや WINS サーバーの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。

off の場合は、DNS サーバーや WINS サーバーのアドレスを渡されても受け取らない。

**[適用モデル]**

NVR700W, NVR510

### 9.10.9 ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定

---

**[書式]**

```
ppp ipcp remote address check sw
```

```
no ppp ipcp remote address check [sw]
```

**[設定値及び初期値]**

- *sw*

- [設定値]:

| 設定値 | 説明                          |
|-----|-----------------------------|
| on  | 通知された相手の PP 側 IP アドレスを拒否する  |
| off | 通知された相手の PP 側 IP アドレスを受け入れる |

- [初期値]: on

**[説明]**

他の PP 経由のホスト経路が既に存在している IP アドレスを PP 接続時に相手側 IP アドレスとして通知されたときに、その IP アドレスを受け入れるか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.11 MSCBCP 関連の設定

---

### 9.11.1 mscbcp-restart パラメーターの設定

#### [書式]

```
ppp mscbcp restart time
no ppp mscbcp restart [time]
```

#### [設定値及び初期値]

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 1000

#### [説明]

選択されている相手について[PPP,MSCBCP]の request/Response の再送時間を設定する。

#### [適用モデル]

NVR700W, NVR510

### 9.11.2 mscbcp-maxretry パラメーターの設定

#### [書式]

```
ppp mscbcp maxretry count
no ppp mscbcp maxretry [count]
```

#### [設定値及び初期値]

- *count*
  - [設定値]: 回数 (1..30)
  - [初期値]: 30

#### [説明]

選択されている相手について[PPP,MSCBCP]の request/Response の再送回数を設定する。

#### [適用モデル]

NVR700W, NVR510

## 9.12 CCP 関連の設定

### 9.12.1 全パケットの圧縮タイプの設定

#### [書式]

```
ppp ccp type type
no ppp ccp type [type]
```

#### [設定値及び初期値]

- *type*
  - [設定値]:

| 設定値      | 説明                                     |
|----------|----------------------------------------|
| stac0    | Stac LZS で圧縮する                         |
| stac     | Stac LZS で圧縮する                         |
| cstac    | Stac LZS で圧縮する ( 接続相手が Cisco ルーターの場合 ) |
| mppe-40  | 40bit MPPE で暗号化する                      |
| mppe-128 | 128bit MPPE で暗号化する                     |
| mppe-any | 40bit,128bit MPPE いずれかの暗号化を行う          |
| none     | 圧縮しない                                  |

- [初期値]: stac

#### [説明]

選択されている相手について[PPP,CCP]圧縮方式を選択する。

**[ノート]**

Van Jacobson Compressed TCP/IP との併用も可能である。

*type* に *stac* を指定した時、回線状態が悪い場合や、高負荷で、パケットロスが頻繁に起きると、通信が正常に行えなくなることがある。このような場合、自動的に「圧縮なし」になる。その後、リスタートまで「圧縮なし」のままである。このような状況が改善できない時は、*stac0* を指定すればよい。ただしその時は接続先も *stac0* に対応していなければならない。*stac0* は *stac* よりも圧縮効率は落ちる。

接続相手が Cisco ルーターの場合に *stac* を適用すると通信できないことがある。そのような場合には、設定を *cstac* に変更すると通信が可能になることがある。

*mppe-40*, *mppe-128*, *mppe-any* の場合には 1 パケット毎に鍵交換される。MPPE は Microsoft Point-To-Point Encryption(Protocol) の略で CCP を拡張したものであり、暗号アルゴリズムとして RC4 を採用し、鍵長 40bit または 128bit を使う。暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 と合わせて設定する。

**[適用モデル]**

NVR700W, NVR510

**9.12.2 ccp-restart パラメーターの設定**

---

**[書式]**

**ppp ccp restart *time***

**no ppp ccp restart [*time*]**

**[設定値及び初期値]**

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

選択されている相手について[PPP,CCP]の *configure-request*、*terminate-request* の再送時間を設定する。

**[適用モデル]**

NVR700W, NVR510

**9.12.3 ccp-max-terminate パラメーターの設定**

---

**[書式]**

**ppp ccp maxterminate *count***

**no ppp ccp maxterminate [*count*]**

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 2

**[説明]**

選択されている相手について[PPP,CCP]の *terminate-request* の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

**9.12.4 ccp-max-configure パラメーターの設定**

---

**[書式]**

**ppp ccp maxconfigure *count***

**no ppp ccp maxconfigure [*count*]**

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,CCP]の `configure-request` の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.12.5 ccp-max-failure パラメーターの設定

---

**[書式]**

```
ppp ccp maxfailure count
no ppp ccp maxfailure [count]
```

**[設定値及び初期値]**

- `count`
  - [設定値]: 回数 (1..10)
  - [初期値]: 10

**[説明]**

選択されている相手について[PPP,CCP]の `configure-nak` の送信回数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 9.13 IPV6CP 関連の設定

---

### 9.13.1 IPV6CP を使用するか否かの設定

---

**[書式]**

```
ppp ipv6cp use use
no ppp ipv6cp use [use]
```

**[設定値及び初期値]**

- `use`
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on

**[説明]**

選択されている相手について IPV6CP を使用するか否かを選択する。

**[適用モデル]**

NVR700W, NVR510

## 9.14 PPPoE 関連の設定

---

### 9.14.1 PPPoE で使用する LAN インターフェースの指定

---

**[書式]**

```
pppoe use interface
no pppoe use
```

**[設定値及び初期値]**

- `interface`
  - [設定値]: LAN インターフェース名、ONU インターフェース名、VLAN インターフェース名
  - [初期値]: -

**[説明]**

選択されている相手に対して、PPPoE で使用するインターフェースを指定する。設定がない場合は、PPPoE は使われない。

**[ノート]**

VLAN インターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

### 9.14.2 アクセスコンセントレータ名の設定

---

**[書式]**

**pppoe access concentrator** *name*

**no pppoe access concentrator**

**[設定値及び初期値]**

- *name*
  - [設定値]: アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII)
  - [初期値]: -

**[説明]**

選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを指定するために使用する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.3 セッションの自動接続の設定

---

**[書式]**

**pppoe auto connect** *switch*

**no pppoe auto connect**

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 自動接続する  |
| off | 自動接続しない |

- [初期値]: on

**[説明]**

選択されている相手に対して、PPPoE のセッションを自動で接続するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.4 セッションの自動切断の設定

---

**[書式]**

**pppoe auto disconnect** *switch*

**no pppoe auto disconnect**

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 自動切断する  |
| off | 自動切断しない |



- [初期値]: on

**[説明]**

選択されている相手に対して、PPPoE のセッションを自動で切断するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.5 PADI パケットの最大再送回数の設定

---

**[書式]**

```
pppoe padi maxretry times  
no pppoe padi maxretry
```

**[設定値及び初期値]**

- *times*
  - [設定値]: 回数 (1..10)
  - [初期値]: 5

**[説明]**

PPPoE プロトコルにおける PADI パケットの最大再送回数を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.6 PADI パケットの再送時間の設定

---

**[書式]**

```
pppoe padi restart time  
no pppoe padi restart
```

**[設定値及び初期値]**

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

PPPoE プロトコルにおける PADI パケットの再送時間を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.7 PADR パケットの最大再送回数の設定

---

**[書式]**

```
pppoe padr maxretry times  
no pppoe padr maxretry
```

**[設定値及び初期値]**

- *times*
  - [設定値]: 回数 (1..10)
  - [初期値]: 5

**[説明]**

PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.8 PADR パケットの再送時間の設定

---

**[書式]**

```
pppoe padr restart time  
no pppoe padr restart
```

**[設定値及び初期値]**

- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

PPPoE プロトコルにおける PADR パケットの再送時間を設定する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.9 PPPoE セッションの切断タイマの設定

---

**[書式]**

**pppoe disconnect time *time***

**no pppoe disconnect time**

**[設定値及び初期値]**

- *time*
  - [設定値]:

| 設定値         | 説明        |
|-------------|-----------|
| 1..21474836 | 秒数        |
| off         | タイマを設定しない |

- [初期値]: off

**[説明]**

選択されている相手に対して、タイムアウトにより PPPoE セッションを自動切断する時間を設定する。

**[ノート]**

LCP と NCP パケットは監視対象外。

**[適用モデル]**

NVR700W, NVR510

### 9.14.10 サービス名の指定

---

**[書式]**

**pppoe service-name *name***

**no pppoe service-name**

**[設定値及び初期値]**

- *name*
  - [設定値]: サービス名を表す文字列 (7bit US-ASCII、255 文字以内)
  - [初期値]: -

**[説明]**

選択されている相手について PPPoE で要求するサービス名を設定する。

接続できるアクセスコンセントレータが複数ある場合に、要求するサービスを提供することが可能なアクセスコンセントレータを選択して接続するために使用する。

**[適用モデル]**

NVR700W, NVR510

### 9.14.11 TCP パケットの MSS の制限の有無とサイズの指定

---

**[書式]**

**pppoe tcp mss limit *length***

**no pppoe tcp mss limit**

## [設定値及び初期値]

• *length*

- [設定値]:

| 設定値        | 説明                   |
|------------|----------------------|
| 1240..1452 | データ長                 |
| auto       | MSS を MTU の値に応じて制限する |
| off        | MSS を制限しない           |

- [初期値]: auto

## [説明]

PPPoE セッション上で TCP パケットの MSS(Maximum Segment Size) を制限するか否かを設定する。

## [ノート]

このコマンドと **ip interface tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

## [適用モデル]

NVR700W, NVR510

### 9.14.12 ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定

## [書式]

**pppoe invalid-session forced close** *sw*

**no pppoe invalid-session forced close**

## [設定値及び初期値]

• *sw*

- [設定値]:

| 設定値 | 説明                                 |
|-----|------------------------------------|
| on  | ルーター側には存在しない PPPoE セッションを強制的に切断する  |
| off | ルーター側には存在しない PPPoE セッションを強制的に切断しない |

- [初期値]: on

## [説明]

ルーター側には存在しない PPPoE セッションを強制的に切断するか否かを設定します。

## [適用モデル]

NVR700W, NVR510

### 9.14.13 認証失敗の最大回数を設定する

## [書式]

**pppoe call prohibit auth-error count** *count*

**no pppoe call prohibit auth-error count**

## [設定値及び初期値]

• *count*

- [設定値]:

| 設定値         | 説明        |
|-------------|-----------|
| 1..21474836 | 認証失敗の最大回数 |
| off         | 発信制限をかけない |

- [初期値]: 15

**[説明]**

選択されている相手に対し、認証が失敗できる最大回数を設定する。  
 なお、以下のコマンドを実行すると、再び発呼が可能となる。

**pp auth accept / pp auth request / pp auth myname / pp auth username / no pp auth accept / no pp auth request / no pp auth myname / no pp auth username**

**[適用モデル]**

NVR510

**9.14.14 PPPoE フレームを中継するインターフェースの指定****[書式]**

**pppoe pass-through member interface interface [interface...]**

**no pppoe pass-through member [...]**

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -

**[説明]**

PPPoE パススルー機能を使用するインターフェースを指定する。

指定したインターフェース間で PPPoE フレームが中継される。

LAN インターフェース名には、物理 LAN インターフェースおよび LAN 分割機能で使用するインターフェースを指定できる。

**[ノート]**

指定した LAN インターフェース、ONU インターフェースはプロミスキャスモードで動作する。

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

設定できる *interface* の数は下記の通り。

| 機種      | 最大設定可能数 |  |
|---------|---------|--|
| NVR700W | 5       |  |
| NVR510  | 2       |  |

**[適用モデル]**

NVR700W, NVR510

## 第 10 章

### DHCP の設定

本機は DHCP(\*1) 機能として、DHCP サーバー機能、DHCP リレーエージェント機能、DHCP クライアント機能を実装しています。

DHCP 機能の利用により、基本的なネットワーク環境の自動設定を実現します。

DHCP クライアント機能は Windows 等の OS に実装されており、これらと本機の DHCP サーバー機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

ルーターが DHCP サーバーとして機能するか DHCP リレーエージェントとして機能するか、どちらとしても機能させないかは **dhcp service** コマンドにより設定します。現在の設定は、**show status dhcp** コマンドにより知ることができます。

DHCP サーバー機能は、DHCP クライアントからのコンフィギュレーション要求を受けて IP アドレスの割り当て (リース) や、ネットマスク、DNS サーバーの情報等を提供します。

割り当てる IP アドレスの範囲とリース期間は **dhcp scope** コマンドにより設定されたものが使用されます。IP アドレスの範囲は複数の設定が可能であり、それぞれの範囲を DHCP スコープ番号で管理します。DHCP クライアントからの設定要求があると DHCP サーバーは DHCP スコープの中で未割り当ての IP アドレスを自動的に通知します。なお、特定の DHCP クライアントに特定の IP アドレスを固定的にリースする場合には、**dhcp scope** コマンドで定義したスコープ番号を用いて **dhcp scope bind** コマンドで予約します。予約の解除は **no dhcp scope bind** コマンドで行います。IP アドレスのリース期間には時間指定と無期限の両方が可能であり、これは **dhcp scope** コマンドの **expire** および **maxexpire** キーワードのパラメーターで指定します。リース状況は **show status dhcp** コマンドにより知ることができます。DHCP クライアントに通知する DNS サーバーの IP アドレス情報は、**dns server** コマンドで設定されたものを使用します。

DHCP リレーエージェント機能は、ローカルセグメントの DHCP クライアントからの要求を、予め設定されたリモートのネットワークセグメントにある DHCP サーバーへ転送します。リモートセグメントの DHCP サーバーは **dhcp relay server** コマンドで設定します。DHCP サーバーが複数ある場合には、**dhcp relay select** コマンドにより選択方式を指定することができます。

また DHCP クライアント機能により、インターフェースの IP アドレスやデフォルト経路情報などを外部の DHCP サーバーから受けることができます。ルーターを DHCP クライアントとして機能させるかどうかは、**ip interface address**、**ip interface secondary address**、**ip pp remote address**、**ip pp remote address pool** の各コマンドの設定値により決定されます。設定されている内容は、**show status dhcp** コマンドにより知ることができます。

(\*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

#### 10.1 DHCP サーバー・リレーエージェント機能

##### 10.1.1 DHCP の動作の設定

[書式]

```
dhcp service type
no dhcp service [type]
```

[設定値及び初期値]

- *type*
- [設定値]:

| 設定値    | 説明                     |
|--------|------------------------|
| server | DHCP サーバーとして機能させる      |
| relay  | DHCP リレーエージェントとして機能させる |

- [初期値]:-

## [説明]

DHCP に関する機能を設定する。

DHCP リレーエージェント機能使用時には、NAT 機能を使用することはできない。

## [ノート]

工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 工場出荷設定値について」を参照してください。

## [適用モデル]

NVR700W, NVR510

## 10.1.2 RFC2131 対応動作の設定

## [書式]

```
dhcp server rfc2131 compliant comp
```

```
dhcp server rfc2131 compliant [except] function [function..]
```

```
no dhcp server rfc2131 compliant
```

## [設定値及び初期値]

- *comp*

- [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | RFC2131 準拠 |
| off | RFC1541 準拠 |

- [初期値]: on
- *except*: 指定した機能以外が RFC2131 対応となるキーワード

- [初期値]: -

- *function*

- [設定値]:

| 設定値              | 説明                                      |
|------------------|-----------------------------------------|
| broadcast-nak    | DHCPNAK をブロードキャストで送る                    |
| none-domain-null | ドメイン名の最後に NULL 文字を付加しない                 |
| remain-silent    | リース情報を持たないクライアントからの DHCPREQUEST を無視する   |
| reply-ack        | DHCPNAK の代わりに許容値を格納した DHCPACK を返す       |
| use-clientid     | クライアントの識別に Client-Identifier オプションを優先する |

- [初期値]: -

## [説明]

DHCP サーバーの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。

また RFC1541 をベースとして RFC2131 記述の個別機能のみを対応させる場合には以下のパラメーターで指定する。これらのパラメーターはスペースで区切り複数指定できる。except キーワードを指示すると、指定したパラメーター以外の機能が RFC2131 対応となる。

|               |                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------|
| broadcast-nak | 同じサブネット上のクライアントに対しては DHCPNAK はブロードキャストで送る。DHCPREQUEST をクライアントが INIT-REBOOT state で送られてきたものに対しては、giaddr 宛であれば Bbit を立てる。 |
|---------------|-------------------------------------------------------------------------------------------------------------------------|

|                  |                                                                                                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none-domain-null | 本ドメイン名の最後に NULL 文字を付加しない。<br>RFC1541 ではドメイン名の最後に NULL 文字を付加するかどうかは明確ではなかったが、RFC2131 では禁止された。一方、Windows NT/2000 の DHCP サーバーは NULL 文字を付加している。そのため、Windows 系の OS での DHCP クライアントは NULL 文字があることを期待している節があり、NULL 文字がない場合には winipcfg.exe での表示が乱れるなどの問題が起きる可能性がある。 |
| remain-silent    | クライアントから DHCPREQUEST を受信した場合に、そのクライアントのリース情報を持っていない場合には DHCPNAK を送らないようにする。                                                                                                                                                                                |
| reply-ack        | クライアントから、リース期間などで許容できないオプション値 (リクエスト IP アドレスは除く) を要求された場合でも、DHCPNAK を返さずに許容値を格納した DHCPACK を返す。                                                                                                                                                             |
| use-clientid     | クライアントの識別に chaddr フィールドより Client-Identifier オプションを優先して使用する。                                                                                                                                                                                                |

[ノート]

工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 工場出荷設定値について」を参照してください。

[適用モデル]

NVR700W, NVR510

### 10.1.3 リースする IP アドレスの重複をチェックするか否かの設定

[書式]

**dhcp duplicate check** *check1 check2*

**no dhcp duplicate check**

[設定値及び初期値]

- *check1* : LAN 内を対象とするチェックの確認用待ち時間

- [設定値] :

| 設定値     | 説明                   |
|---------|----------------------|
| 1..1000 | ミリ秒                  |
| off     | LAN 内を対象とするチェックを行わない |

- [初期値] : 100

- *check2* : LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間

- [設定値] :

| 設定値     | 説明                                       |
|---------|------------------------------------------|
| 1..3000 | ミリ秒                                      |
| off     | LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない |

- [初期値] : 500

[説明]

DHCP サーバーとして機能する場合、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。

[ノート]

LAN 内のスコープに対しては ARP を、DHCP リレーエージェント経由のスコープに対しては PING を使ってチェックする。

[適用モデル]

NVR700W, NVR510

## 10.1.4 DHCP スコープの定義

### [書式]

```
dhcp scope scope_num ip_address-ip_address/netmask [except ex_ip ...] [gateway gw_ip] [expire time] [maxexpire time]
no dhcp scope scope_num [ip_address-ip_address/netmask [except ex_ip...]] [gateway gw_ip] [expire time] [maxexpire time]]
```

### [設定値及び初期値]

- *scope\_num*
  - [設定値]: スコープ番号 (1..65535)
  - [初期値]: -
- *ip\_address-ip\_address*
  - [設定値]: 対象となるサブネットで割り当てる IP アドレスの範囲
  - [初期値]: -
- *netmask*
  - [設定値]:
    - xxx.xxx.xxx.xxx (xxx は十進数)
    - 0x に続く十六進数
    - マスクビット数
  - [初期値]: -
- *ex\_ip*
  - [設定値]: IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能、'|' を使用して範囲指定も可能)
  - [初期値]: -
- *gw\_ip*
  - [設定値]: IP アドレス対象ネットワークのゲートウェイの IP アドレス
  - [初期値]: -
- *time*: 時間
  - [設定値]:
    - expire time: DHCP クライアントからリース期間要求がない場合のリース期間
    - maxexpire time: DHCP クライアントからリース期間要求がある場合の許容最大リース期間

| 設定値           | 説明                                              |
|---------------|-------------------------------------------------|
| 1..21474836   | 分 (NVR700W Rev.15.00.14、NVR510 Rev.15.01.13 以降) |
| 1..2147483647 | 分 (上記以外)                                        |
| xx:xx         | 時間:分                                            |
| infinity      | 無期限リース                                          |

- [初期値]:
  - expire time=72:00
  - maxexpire time=72:00

### [説明]

DHCP サーバーとして割り当てる IP アドレスのスコープを設定する。除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。

### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降では、同一ネットワークの DHCP スコープを複数設定できる。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。DHCP リレーエージェントを経由しない DHCP クライアントに対して gateway キーワードによる設定パラメータが



省略されている場合にはルーター自身の IP アドレスを通知する。

`expire` の設定値は `maxexpire` の設定値以下でなければならない。

工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 工場出荷設定値について」を参照してください。

NVR700W の Rev.15.00.07 以前、NVR510 の Rev.15.01.06 以前では、**dhcp scope** コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- **dhcp scope bind**
- **dhcp scope option**

[適用モデル]

NVR700W, NVR510

### 10.1.5 DHCP 予約アドレスの設定

[書式]

```
dhcp scope bind scope_num ip_address [type] id
dhcp scope bind scope_num ip_address mac_address
dhcp scope bind scope_num ip_address ipcp
dhcp scope bind scope_num ip_address-ip_address mac_address
no dhcp scope bind scope_num ip_address
no dhcp scope bind scope_num ip_address-ip_address
```

[設定値及び初期値]

- `scope_num`
  - [設定値]: スコープ番号 (1..65535)
  - [初期値]: -
- `ip_address`
  - [設定値]:

| 設定値             | 説明                      |
|-----------------|-------------------------|
| xxx.xxx.xxx.xxx | (xxx は十進数) 予約する IP アドレス |
| *               | 割り当てる IP アドレスを指定しない     |

- [初期値]: -
- `type`: Client-Identifier オプションの `type` フィールドを決定する
  - [設定値]:

| 設定値      | 説明   |
|----------|------|
| text     | 0x00 |
| ethernet | 0x01 |

- [初期値]: -
- `id`

- [設定値]:

| 設定値                              | 説明                                    |
|----------------------------------|---------------------------------------|
| <code>type</code> が ethernet の場合 | MAC アドレス                              |
| <code>type</code> が text の場合     | 文字列                                   |
| <code>type</code> が省略された場合       | 2 桁十六進数の列で先頭は <code>type</code> フィールド |

- [初期値]: -
- `mac_address`
  - [設定値]:
    - xx:xx:xx:xx:xx:xx (xx は十六進数) 予約 DHCP クライアントの MAC アドレス
    - xx:xx:xx:\* のように下位 3 オクテットをアスタリスク (\*) にすることで、OUI(ベンダー ID) のみの指定となる
  - [初期値]: -

- `ipcp` : IPCP でリモート側に与えることを示すキーワード
  - [初期値] :-

### [説明]

IP アドレスを割り当てる DHCP クライアントを固定的に設定する。

IP アドレスを固定せずにクライアントだけを指定することもできる。この形式を削除する場合はクライアント識別子を省略できない。

### [ノート]

IP アドレスは、`scope_num` パラメータで指定された DHCP スコープ範囲内でなければならない。1つの DHCP スコープ内では、1つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。

IPCP で与えるアドレスは LAN 側のスコープから選択される。

コマンドの第 1 書式を使う場合は、あらかじめ `dhcp server rfc2131 compliant on` あるいは `use-clientid` 機能を使用するよう設定されていなければならない。また `dhcp server rfc2131 compliant off` あるいは `use-clientid` 機能を使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

コマンドの第 1 書式でのクライアント識別子は、クライアントがオプションで送ってくる値を設定する。`type` パラメーターを省略した場合には、`type` フィールドの値も含めて入力する。`type` パラメーターにキーワードを指定する場合には `type` フィールド値は一意に決定されるので Client-Identifier フィールドの値のみを入力する。

コマンドの第 2 書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの `chaddr` フィールドを用いる。この形の予約機能は、RT の設定が `dhcp server rfc2131 compliant off` あるいは `use-clientid` 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないと動作しない。

クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 書式での予約は、`dhcp server rfc2131 compliant on` あるいは `use-clientid` パラメーターが指定された場合には無効になるため、新たに Client-Identifier オプションで送られる値で予約し直す必要がある。

コマンドの第 2 書式で 1 つの OUI(ベンダー ID) を複数設定することができる。OUI(ベンダー ID) 設定と MAC アドレス設定の両方がある場合、MAC アドレス設定を優先する。

OUI(ベンダー ID)設定は以下のファームウェアで指定可能。

NVR700W Rev.15.00.14 以降

NVR510 Rev.15.01.13 以降

NVR700W の Rev.15.00.07 以前、NVR510 の Rev.15.01.06 以前では、`dhcp scope` コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- `dhcp scope bind`
- `dhcp scope option`

### [設定例]

```
A. # dhcp scope bind 1 192.168.100.2 ethernet 00:a0:de:01:23:45
B. # dhcp scope bind 1 192.168.100.2 text client01
C. # dhcp scope bind 1 192.168.100.2 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind 1 192.168.100.2 00:a0:de:01:23:45
E. # dhcp scope bind 1 192.168.100.2-192.168.100.19 00:a0:de:*
```

#### 1. `dhcp server rfc2131 compliant on` あるいは `use-clientid` 機能を使用する設定の場合

- A. B. C. の書式では、クライアントの識別に Client-Identifier オプションを使用する。
- D. の書式では DHCP パケットの `chaddr` フィールドを使用する。ただし、Client-Identifier オプションが存在する場合、この設定は無視される。

DHCP サーバーは `chaddr` フィールドの値より Client-Identifier オプションの値の方が優先して使用される。

`show status dhcp` コマンドを実行してクライアントの識別子を確認することで、クライアントが Client-Identifier オプションを使っているか否かを判別することも可能である。

- リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用していない

- リースしているクライアントとして十六進数の文字列、あるいは文字列が表示されていれば、Client-Identifier オプションが使われている Client-Identifier オプションを使うクライアントへの予約は、ここに表示される十六進数の文字列あるいは文字列を使用する

2. **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能を使用しない場合

- A. B. C. の書式では指定できない。Client-Identifier オプションは無視される。
- D. の書式では DHCP パケットの chaddr フィールドを使用する。

なお、クライアントとの相互動作に関して以下の留意点がある。

- 個々の機能を単独で用いるとクライアント側で思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant on** あるいは **dhcp server rfc2131 compliant off** で使用することを推奨する。
- ルーターの再起動やスコープの再設定によりリース情報が消去されている場合、アドレスの延長要求をした時やリース期間内のクライアントを再起動した時にクライアントが使用する IP アドレスは変わることがある。

これを防ぐためには **dhcp server rfc2131 compliant on** (あるいは **remain-silent** 機能を有効にする) 設定がある。この設定にすると、ヤマハルーターがリース情報を持たないクライアントからの DHCPREQUEST に対して DHCPNAK を返さず無視するようになる。この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースすることができる。

E. の書式では、OUI(ベンダー ID)のみ指定し、その OUI(ベンダー ID)を持つ機器にのみ IP アドレスを割り当てることができる。

[適用モデル]  
NVR700W, NVR510

### 10.1.6 DHCP アドレス割り当て動作の設定

[書式]

```
dhcp scope lease type scope_num type [fallback=fallback_scope_num]
no dhcp scope lease type scope_num [type ...]
```

[設定値及び初期値]

- scope\_num, fallback\_scope\_num
  - [設定値]: スコープ番号 (1-65535)
  - [初期値]: -
- type: 割り当ての動作
  - [設定値]:

| 設定値           | 説明               |
|---------------|------------------|
| bind-priority | 予約情報を優先して割り当てる   |
| bind-only     | 予約情報だけに制限して割り当てる |

- [初期値]: bind-priority

[説明]

scope\_num で指定した DHCP スコープにおける、アドレスの割り当て方法を制御する。

type に bind-priority を指定した場合には、**dhcp scope bind** コマンドで予約されたクライアントには予約どおりの IP アドレスを、予約されていないクライアントには他のクライアントに予約されていない空きアドレスがスコープ内にある限りそれを割り当てる。

type に bind-priority を指定した場合には、fallback オプションは指定できない。

type に bind-only を指定した場合は、fallback オプションでフォールバックスコープを指定しているかどうかによって動作が変わる。

fallback オプションの指定が無い場合、**dhcp scope bind** コマンドで予約されているクライアントにのみ IP アドレスを割り当て、予約されていないクライアントにはたとえスコープに空きがあっても IP アドレスを割り当てない。

type に bind-only を指定し、同時に fallback オプションでフォールバックスコープを指定している場合には、以下のような動作になる。

1. クライアントが、スコープで IP アドレスを予約されている時には、予約どおりの IP アドレスを割り当てる。

2. クライアントが、スコープでは IP アドレスが予約されていないが、フォールバックスコープでは予約されている時には、フォールバックスコープでの予約どおりの IP アドレスを割り当てる。
3. クライアントが、スコープ、フォールバックスコープのいずれでも IP アドレスを予約されていない時には、フォールバックスコープに対する **dhcp scope lease type** コマンドの設定によって動作が変わる。
  - a. フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が **bind-priority** になっている時には、クライアントにはフォールバックスコープに空きアドレスがある限りそれを割り当てる。
  - b. フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が **bind-only** になっている時には、クライアントには IP アドレスは割り当てられない。

いずれの場合も、リース期間は各 DHCP スコープの定義に従う。

**[適用モデル]**

NVR700W, NVR510

## 10.1.7 DHCP 割り当て情報を元にした予約設定の生成

**[書式]**

**dhcp convert lease to bind scope\_n [except] [idx [...]]**

**[設定値及び初期値]**

- *scope\_n*
  - [設定値]: スコープ番号 (1-65535)
  - [初期値]: -
- *idx*
  - [設定値]:

| 設定値 | 説明                                                          |
|-----|-------------------------------------------------------------|
| 番号  | <b>show status dhcp summary</b> コマンドで表示されるインデックス番号、最大 100 個 |
| all | 割り当て中の情報全てを対象とする                                            |
| 省略  | 省略時は all                                                    |

- [初期値]: -

**[説明]**

現在の割り当て情報を元に予約設定を作成する。except キーワードを指示すると、指定した番号以外の情報が予約設定に反映される。

**[ノート]**

以下の変換規則で IP アドレス割り当て情報が予約設定に変換される。

| IP アドレス割り当て情報のクライアント識別種別 (show status dhcp で表示される名称) | クライアント識別情報例               | 予約設定情報例                       |
|------------------------------------------------------|---------------------------|-------------------------------|
| クライアントイーサネットアドレス                                     | 00:a0:de:01:02:03         | ethernet 00:a0:de:01:02:03 ※1 |
|                                                      |                           | 00:a0:de:01:02:03 ※2          |
| クライアント ID                                            | (01) 00 a0 de 01 02 03    | ethernet 00:a0:de:01:02:03    |
|                                                      | (01) 00 a0 de 01 02 03 04 | 01 00 a0 de 01 02 03 04       |
|                                                      | (01) 31 32 33             | 00 31 32 33                   |

※1 : rfc2131 compliant on あるいは use-clientid ありの場合、このような IP アドレス割り当て情報の表示は ARP チェックの結果である可能性が高く、通常の割り当て時にはクライアント ID オプションが使われるため、この形式で予約設定をする。ただし、MAC アドレスと異なるクライアント ID を使うホストが存在する場合はこの自動変換による予約は有効に機能しないため、そのようなホストに対する予約設定は別途、手動で行う必要がある

※2 : rfc2131 compliant off あるいは use-clientid なしの場合、chaddr フィールドを使用する

コマンド実行時点での割り当て情報を元に予約設定を作成する。サマリ表示からこの変換コマンドの実行までに時間が経過した場合には、本コマンド実行後に意図したペアの予約が作成されていることを **show config** で確認すべきである

[適用モデル]  
NVR700W, NVR510

## 10.1.8 DHCP オプションの設定

### [書式]

```
dhcp scope option scope_num option=value [option=value...]
no dhcp scope option scope_num [...]
```

### [設定値及び初期値]

- *scope\_num*
  - [設定値]: スコープ番号 (1..65535)
  - [初期値]: -
- *option*
  - [設定値]:
    - オプション番号
      - 1..49,62..254
    - 主なニーモニック

|             |    |
|-------------|----|
| router      | 3  |
| dns         | 6  |
| hostname    | 12 |
| domain      | 15 |
| wins_server | 44 |

- [初期値]: -
- *value*: オプション値
  - [設定値]:
    - 値としては以下の種類があり、どれが使えるかはオプション番号で決まる。例えば、'router','dns','winsserver' は IP アドレスの配列であり、'hostname','domain' は文字列である。

|              |                          |
|--------------|--------------------------|
| 1 オクテット整数    | 0..255                   |
| 2 オクテット整数    | 0..65535                 |
| 2 オクテット整数の配列 | 2 オクテット整数をコンマ (,) で並べたもの |
| 4 オクテット整数    | 0..2147483647            |
| IP アドレス      | IP アドレス                  |
| IP アドレスの配列   | IP アドレスをコンマ (,) で並べたもの   |
| 文字列          | 文字列                      |
| スイッチ         | "on","off","1","0" のいずれか |
| バイナリ         | 2 桁十六進数をコンマ (,) で並べたもの   |

- [初期値]: -

### [説明]

スコープに対して送信する DHCP オプションを設定する。**dns server** コマンドや **wins server** コマンドなどでも暗黙のうちに DHCP オプションを送信していたが、それを明示的に指定できる。また、暗黙の DHCP オプションではスコープでオプションの値を変更することはできないが、このコマンドを使えばそれも可能になる。

### [ノート]

NVR700W の Rev.15.00.07 以前、NVR510 の Rev.15.01.06 以前では、**dhcp scope** コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- **dhcp scope bind**
- **dhcp scope option**

[適用モデル]  
NVR700W, NVR510

## 10.1.9 DHCP リース情報の手動追加

### [書式]

```
dhcp manual lease ip_address [type] id
dhcp manual lease ip_address mac_address
dhcp manual lease ip_address ipcp
```

### [設定値及び初期値]

- *ip\_address*
  - [設定値]: リースする IP アドレス
  - [初期値]: -
- *type*: Client-Identifier オプションの *type* フィールドを決定する
  - [設定値]:

| 設定値      | 説明   |
|----------|------|
| text     | 0x00 |
| ethernet | 0x01 |

- [初期値]: -
- *id*
  - [設定値]:

| 設定値                        | 説明                              |
|----------------------------|---------------------------------|
| <i>type</i> が text の場合     | 文字列                             |
| <i>type</i> が ethernet の場合 | MAC アドレス                        |
| <i>type</i> が省略された場合       | 2 桁十六進数の列で先頭は <i>type</i> フィールド |

- [初期値]: -
- *mac\_address*
  - [設定値]: XX:XX:XX:XX:XX:XX (XX は十六進数) DHCP クライアントの MAC アドレス
  - [初期値]: -
- *ipcp*: IPCP でリモート側に与えたものとするキーワード
  - [初期値]: -

### [説明]

手動で、特定 IP アドレスのリース情報を追加する。

### [ノート]

本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を追加したい場合を除いて、使用するべきではない。

### [適用モデル]

NVR700W, NVR510

## 10.1.10 DHCP リース情報の手動削除

### [書式]

```
dhcp manual release ip_address
```

### [設定値及び初期値]

- *ip\_address*
  - [設定値]: 解放する IP アドレス
  - [初期値]: -

### [説明]

手動で、特定 IP アドレスのリース情報を削除する。

### [ノート]

本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を削除したい場合を除いて、使用するべきではない。

[適用モデル]  
NVR700W, NVR510

### 10.1.11 DHCP サーバーの指定の設定

#### [書式]

```
dhcp relay server host1 [host2 [host3 [host4]]]
no dhcp relay server
```

#### [設定値及び初期値]

- *host1..host4*
  - [設定値]: DHCP サーバーの IP アドレス
  - [初期値]: -

#### [説明]

DHCP BOOTREQUEST パケットを中継するサーバーを最大 4 つまで設定する。  
サーバーが複数指定された場合は、BOOTREQUEST パケットを複製してすべてのサーバーに中継するか、あるいは 1 つだけサーバーを選択して中継するかは **dhcp relay select** コマンドの設定で決定される。

[適用モデル]  
NVR700W, NVR510

### 10.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定

#### [書式]

```
dhcp relay srcport port
no dhcp relay srcport [port]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 68

#### [説明]

DHCP リレーエージェント機能で使用する始点ポート番号を設定する。

#### [ノート]

NVR700W Rev.15.00.17 以降、および NVR510 Rev.15.01.16 以降で指定可能。

[適用モデル]  
NVR700W, NVR510

### 10.1.13 DHCP サーバーの選択方法の設定

#### [書式]

```
dhcp relay select type
no dhcp relay select [type]
```

#### [設定値及び初期値]

- *type*
  - [設定値]:

| 設定値  | 説明                        |
|------|---------------------------|
| hash | Hash 関数を利用して一つだけサーバーを選択する |
| all  | すべてのサーバーを選択する             |

- [初期値]: hash

#### [説明]

**dhcp relay server** コマンドで設定された複数のサーバーの取り扱いを設定する。  
hash が指定された場合は、Hash 関数を利用して一つだけサーバーが選択されてパケットが中継される。この Hash

関数は、DHCP メッセージの `chaddr` フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバーが選択されるはずである。all が指定された場合は、パケットはすべてのサーバーに対し複写中継される。

**[適用モデル]**

NVR700W, NVR510

### 10.1.14 DHCP BOOTREQUEST パケットの中継基準の設定

**[書式]**

**dhcp relay threshold** *time*

**no dhcp relay threshold** [*time*]

**[設定値及び初期値]**

- *time*
  - [設定値]: 秒数 (0..65535)
  - [初期値]: 0

**[説明]**

DHCP BOOTREQUEST パケットの `secs` フィールドとこのコマンドによる秒数を比較し、設定値より小さな `secs` フィールドを持つ DHCP BOOTREQUEST パケットはサーバーに中継しないようにする。

これにより、同一 LAN 上に別の DHCP サーバーがあるにも関わらず遠隔地の DHCP サーバーにパケットを中継してしまうのを避けることができる。

**[適用モデル]**

NVR700W, NVR510

### 10.1.15 インターフェース毎の DHCP の動作の設定

**[書式]**

**ip interface dhcp service** *type* [*host1* [*host2* [*host3* [*host4*]]]]

**no ip interface dhcp service**

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値    | 説明                                    |
|--------|---------------------------------------|
| off    | DHCP サーバーとしても DHCP リレーエージェントとしても機能しない |
| server | DHCP サーバーとして機能させる                     |
| relay  | DHCP リレーエージェントとして機能させる                |

- [初期値]: -
- *host1..host4*
  - [設定値]: DHCP サーバーの IP アドレス
  - [初期値]: -

**[説明]**

インターフェース毎に DHCP の動作を設定する。

DHCP サーバーを設定した場合には、ネットワークアドレスが合致する DHCP スコープから IP アドレスを 1 つ割り当てる。

DHCP リレーエージェントを設定した場合には、HOST を設定する必要がある、この HOST へ DHCP DISCOVER パケットおよび DHCP REQUEST パケットを転送する。

off に設定した場合には、DHCP サーバーとしても DHCP リレーエージェントとしても動作しない。DHCP パケットは破棄されます。



本設定が無い場合は、`dhcp service` コマンドの設定に従う。`dhcp service` コマンドの設定と本設定の両方がある場合には、本設定が優先される。

#### [ノート]

ブリッジインターフェースは NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 10.2 DHCP クライアント機能

---

### 10.2.1 DHCP クライアントのホスト名の設定

---

#### [書式]

```
dhcp client hostname interface primary host
dhcp client hostname interface secondary host
dhcp client hostname pp peer_num host
dhcp client hostname pool pool_num host
no dhcp client hostname interface primary [host]
no dhcp client hostname interface secondary [host]
no dhcp client hostname pp peer_num [host]
no dhcp client hostname pool pool_num [host]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *pool\_num*
  - [設定値]: **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool\_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)
  - [初期値]: -
- *host*
  - [設定値]: DHCP クライアントのホスト名
  - [初期値]: -

#### [説明]

DHCP クライアントのホスト名を設定する。

#### [ノート]

WAN インターフェースを設定した時には、`secondary` は指定できない。

ブリッジインターフェースは NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

### 10.2.2 要求する IP アドレスリース期間の設定

---

#### [書式]

```
ip interface dhcp lease time time
no ip interface dhcp lease time [time]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *time*
  - [設定値]: 分数 (1..21474836)
  - [初期値]: -

**[説明]**

DHCP クライアントが要求する IP アドレスのリース期間を設定する。

**[ノート]**

リース期間の要求が受け入れられなかった場合、要求しなかった場合は、DHCP サーバーからのリース期間を利用する。

ブリッジインターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

### 10.2.3 IP アドレス取得要求の再送回数と間隔の設定

---

**[書式]**

```
ip interface dhcp retry retry interval
no ip interface dhcp retry [retry interval]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *retry*
  - [設定値]:

| 設定値      | 説明  |
|----------|-----|
| 1..100   | 回数  |
| infinity | 無制限 |

- [初期値]: infinity
- *interval*
  - [設定値]: 秒数 (1..100)
  - [初期値]: 5

**[説明]**

IP アドレスの取得に失敗したときにリトライする回数とその間隔を設定する。

**[ノート]**

ブリッジインターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

### 10.2.4 DHCP クライアント ID オプションの設定

---

**[書式]**

```
dhcp client client-identifier interface primary [type type] id
dhcp client client-identifier interface secondary [type type] id
dhcp client client-identifier pp peer_num [type type] id
dhcp client client-identifier pool pool_num [type type] id
```

```
no dhcp client client-identifier interface primary
no dhcp client client-identifier interface secondary
no dhcp client client-identifier pp peer_num
no dhcp client client-identifier pool pool_num
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *type*: ID オプションの *type* フィールドの値を設定することを示すキーワード
  - [初期値]: -
- *type*
  - [設定値]: ID オプションの *type* フィールドの値
  - [初期値]: 1
- *id*
  - [設定値]:
    - ASCII 文字列で表した ID
    - 2 桁の十六進数列で表した ID
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *pool\_num*
  - [設定値]: **ip pp remote address pool dhcp** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcp** コマンドで IP アドレスを 2 個取得できる機種で、*pool\_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcp** コマンドで取得できる IP アドレスの最大数)
  - [初期値]: -

#### [説明]

DHCP クライアント ID オプションの *type* フィールドと ID を設定する。

#### [ノート]

ブリッジインターフェースは NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 10.2.5 DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定

#### [書式]

```
dhcp client option interface primary option=value
dhcp client option interface secondary option=value
dhcp client option pp peer_num option=value
dhcp client option pool pool_num option=value
no dhcp client option interface primary [option=value]
no dhcp client option interface secondary [option=value]
no dhcp client option pp peer_num [option=value]
no dhcp client option pool pool_num [option=value]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *option*

- [設定値]: オプション番号 (十進数)
- [初期値]: -
- *value*
  - [設定値]: 格納するオプション値 (十六進数、";" で区切って複数指定可能) なおオプション長情報は入力の必要はない
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *pool\_num*
  - [設定値]: **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool\_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)
  - [初期値]: -

**[説明]**

DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションを設定する。

**[ノート]**

このコマンドはサーバーとの相互接続に必要な場合にのみ設定する。  
得られたオプション値は内部では利用されない。  
WAN インターフェースを設定した時には、secondary は指定できない。

ブリッジインターフェースは NVR700W で指定可能。

**[設定例]**

- LAN2 プライマリアドレスを DHCP サーバーから得る場合に特定アドレス (192.168.0.128) を要求する。

```
# dhcp client option lan2 primary 50=c0,a8,00,80
# ip lan2 address dhcp
(注: ただし、この場合でも要求アドレスがサーバーから与えられるか否かはサーバー次第である。)
```

**[適用モデル]**

NVR700W, NVR510

**10.2.6 リンクダウンした時に情報を解放するか否かの設定****[書式]**

```
dhcp client release linkdown switch [time]
no dhcp client release linkdown [switch [time]]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明                                                 |
|-----|----------------------------------------------------|
| on  | インターフェースのリンクダウンが <i>time</i> 秒間継続すると、取得していた情報を解放する |
| off | インターフェースがリンクダウンしても情報は保持する                          |

- [初期値]: off
- *time*
  - [設定値]: 秒数 (0..259200)
  - [初期値]: 3

**[説明]**

DHCP クライアントとして DHCP サーバーから IP アドレスを得ているインターフェースがリンクダウンした時に、DHCP サーバーから得ていた情報を解放するか否かを設定する。リンクダウンするとタイマが働き、*time* の秒数だけリンクダウン状態が継続すると情報を解放する。*time* が設定されていない場合には *time* は 3 秒となる。情報が解放されると、次にリンクアップした時に情報の取得を試みる。

**[ノート]**

タイマの値を長く設定すると、不安定なリンク状態の影響を避けることができる。本コマンドの設定は、コマンド実行後に発生したリンクダウン以降で有効になる。タイマの満了前にリンクアップした場合にはタイマはクリアされ、情報を解放しない。タイマの満了前に情報のリース期間が満了した場合には、タイマはクリアされ、情報は解放される。以下のコマンド実行時には、動作中のタイマはクリアされる。

**ip interface address, ip pp remote address, ip pp remote address pool, dhcp client release linkdown**

**[適用モデル]**

NVR700W, NVR510

## 第 11 章

### ICMP の設定

#### 11.1 IPv4 の設定

##### 11.1.1 ICMP Echo Reply を送信するか否かの設定

[書式]

```
ip icmp echo-reply send send
no ip icmp echo-reply send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

[説明]

ICMP Echo を受信した場合に、ICMP Echo Reply を返すか否かを設定する。

[適用モデル]

NVR700W, NVR510

##### 11.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

[書式]

```
ip icmp echo-reply send-only-linkup send
no ip icmp echo-reply send-only-linkup [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | リンクアップしている時だけ ICMP Echo Reply を返す |
| off | リンクの状態に関わらず ICMP Echo Reply を返す   |

- [初期値]: off

[説明]

リンクダウンしているインターフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[適用モデル]

NVR700W, NVR510

##### 11.1.3 ICMP Mask Reply を送信するか否かの設定

[書式]

```
ip icmp mask-reply send send
no ip icmp mask-reply send [send]
```

**[設定値及び初期値]**

- *send*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

ICMP Mask Request を受信した場合に、ICMP Mask Reply を返すか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**11.1.4 ICMP Parameter Problem を送信するか否かの設定****[書式]**

```
ip icmp parameter-problem send send
no ip icmp parameter-problem send [send]
```

**[設定値及び初期値]**

- *send*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: off

**[説明]**

受信した IP パケットの IP オプションにエラーを検出した場合に、ICMP Parameter Problem を送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**11.1.5 ICMP Redirect を送信するか否かの設定****[書式]**

```
ip icmp redirect send send
no ip icmp redirect send [send]
```

**[設定値及び初期値]**

- *send*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

他のゲートウェイ宛の IP パケットを受信して、そのパケットを適切なゲートウェイに回送した場合に、同時にパケットの送信元に対して ICMP Redirect を送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 11.1.6 ICMP Redirect 受信時の処理の設定

#### [書式]

```
ip icmp redirect receive action
no ip icmp redirect receive [action]
```

#### [設定値及び初期値]

- *action*
- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 処理する |
| off | 無視する |

- [初期値]: off

#### [説明]

ICMP Redirect を受信した場合に、それを処理して自分の経路テーブルに反映させるか、あるいは無視するかを設定する。

#### [適用モデル]

NVR700W, NVR510

### 11.1.7 ICMP Time Exceeded を送信するか否かの設定

#### [書式]

```
ip icmp time-exceeded send send [rebound=sw]
no ip icmp time-exceeded send [send [rebound=sw]]
```

#### [設定値及び初期値]

- *send*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on
- *sw*
- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | 受信インターフェースから送信する |
| off | 経路に従って送信する       |

- [初期値]: off

#### [説明]

受信した IP パケットの TTL が 0 になってしまったため、そのパケットを破棄した場合に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。  
rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

#### [適用モデル]

NVR700W, NVR510

### 11.1.8 ICMP Timestamp Reply を送信するか否かの設定

#### [書式]

```
ip icmp timestamp-reply send send
no ip icmp timestamp-reply send [send]
```



**[設定値及び初期値]**

- *send*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

ICMP Timestamp を受信した場合に、ICMP Timestamp Reply を返すか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**11.1.9 ICMP Destination Unreachable を送信するか否かの設定****[書式]**

```
ip icmp unreachable send send [rebound=sw]
```

```
no ip icmp unreachable send [send [rebound=sw]]
```

**[設定値及び初期値]**

- *send*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

- *sw*

- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | 受信インターフェースから送信する |
| off | 経路に従って送信する       |

- [初期値]: off

**[説明]**

経路テーブルに宛先が見つからない場合や、あるいは ARP が解決できなくて IP パケットを破棄することになった場合に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するか否かを設定する。rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

**[適用モデル]**

NVR700W, NVR510

**11.1.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定****[書式]**

```
ip icmp error-decryptd-ipsec send switch
```

```
no ip icmp error-decryptd-ipsec send [switch]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | IPsec で復号したパケットに対して ICMP エラーを送る   |
| off | IPsec で復号したパケットに対して ICMP エラーを送らない |

- [初期値] : on

#### [説明]

IPsec で復号したパケットに対して ICMP エラーを送るか否か設定する。

#### [ノート]

ICMP エラーには復号したパケットの先頭部分が含まれるため、ICMP エラーが送信元に返送される時にも IPsec で処理されないようになっており、本来 IPsec で保護したい通信が保護されずにネットワークに流れてしまう可能性がある。特に、フィルター型ルーティングでプロトコルによって IPsec で処理するかどうか切替えている場合には注意が必要となる。

ICMP エラーを送らないように設定すると、tracertoute に対して反応がなくなるなどの現象になる。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 11.1.11 受信した ICMP のログを記録するか否かの設定

#### [書式]

```
ip icmp log log
no ip icmp log [log]
```

#### [設定値及び初期値]

- log
  - [設定値] :

| 設定値 | 説明    |
|-----|-------|
| on  | 記録する  |
| off | 記録しない |

- [初期値] : off

#### [説明]

受信した ICMP エラーを DEBUG レベルのログに記録するか否かを設定する。Echo Request や Echo Reply のログは記録しない。

#### [適用モデル]

NVR700W, NVR510

### 11.1.12 ステルス機能の設定

#### [書式]

```
ip stealth all
ip stealth interface [interface...]
no ip stealth [...]
```

#### [設定値及び初期値]

- all : すべての論理インターフェースからのパケットに対してステルス動作を行う
  - [初期値] : -
- interface
  - [設定値] : 指定した論理インターフェースからのパケットに対してステルス動作を行う
  - [初期値] : -

**[説明]**

このコマンドを設定すると、指定されたインターフェースから自分宛に来たパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインターフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくことでそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

**[ノート]**

指定されたインターフェースからの PING にも答えなくなるので注意が必要である。

自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ip icmp \*** コマンド群を用いる必要がある。

ブリッジインターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 11.2 IPv6 の設定

---

### 11.2.1 ICMP Echo Reply を送信するか否かの設定

---

**[書式]**

```
ipv6 icmp echo-reply send send
no ipv6 icmp echo-reply send [send]
```

**[設定値及び初期値]**

- *send*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

ICMP Echo Reply を送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 11.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

---

**[書式]**

```
ipv6 icmp echo-reply send-only-linkup send
no ipv6 icmp echo-reply send-only-linkup [send]
```

**[設定値及び初期値]**

- *send*
- [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | リンクアップしている時だけ ICMP Echo Reply を返す |
| off | リンクの状態に関わらず ICMP Echo Reply を返す   |

- [初期値]: off

**[説明]**

リンクダウンしているインターフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

**[適用モデル]**

NVR700W, NVR510

**11.2.3 ICMP Parameter Problem を送信するか否かの設定**

---

**[書式]**

**ipv6 icmp parameter-problem send *send***

**no ipv6 icmp parameter-problem send [*send*]**

**[設定値及び初期値]**

- *send*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: off

**[説明]**

ICMP Parameter Problem を送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**11.2.4 ICMP Redirect を送信するか否かの設定**

---

**[書式]**

**ipv6 icmp redirect send *send***

**no ipv6 icmp redirect send [*send*]**

**[設定値及び初期値]**

- *send*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

ICMP Redirect を出すか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**11.2.5 ICMP Redirect 受信時の処理の設定**

---

**[書式]**

**ipv6 icmp redirect receive *action***

**no ipv6 icmp redirect receive [*action*]**

**[設定値及び初期値]**

- *action*

- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 処理する |
| off | 無視する |

- [初期値] : off

**[説明]**

ICMP Redirect を受けた場合に処理するか無視するかを設定する。

**[適用モデル]**

NVR700W, NVR510

### 11.2.6 ICMP Time Exceeded を送信するか否かの設定

**[書式]**

**ipv6 icmp time-exceeded send *send* [rebound=*sw*]**

**no ipv6 icmp time-exceeded send [*send* [rebound=*sw*]]**

**[設定値及び初期値]**

- *send*

- [設定値] :

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値] : on

- *sw*

- [設定値] :

| 設定値 | 説明               |
|-----|------------------|
| on  | 受信インターフェースから送信する |
| off | 経路に従って送信する       |

- [初期値] : off

**[説明]**

ICMP Time Exceeded を出すか否かを設定する。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

**[適用モデル]**

NVR700W, NVR510

### 11.2.7 ICMP Destination Unreachable を送信するか否かの設定

**[書式]**

**ipv6 icmp unreachable send *send* [rebound=*sw*]**

**no ipv6 icmp unreachable send [*send* rebound=*sw*]**

**[設定値及び初期値]**

- *send*

- [設定値] :

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値] : on

- *sw*

- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | 受信インターフェースから送信する |
| off | 経路に従って送信する       |

- [初期値]: off

#### [説明]

ICMP Destination Unreachable を出すか否かを設定する。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

#### [適用モデル]

NVR700W, NVR510

## 11.2.8 受信した ICMP のログを記録するか否かの設定

#### [書式]

```
ipv6 icmp log log
no ipv6 icmp log [log]
```

#### [設定値及び初期値]

- *log*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 記録する  |
| off | 記録しない |

- [初期値]: off

#### [説明]

受信した ICMP を DEBUG タイプのログに記録するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 11.2.9 ICMP Packet-Too-Big を送信するか否かの設定

#### [書式]

```
ipv6 icmp packet-too-big send send
no ipv6 icmp packet-too-big send [send]
```

#### [設定値及び初期値]

- *send*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

#### [説明]

ICMP Packet-Too-Big を出すか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 11.2.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定

### [書式]

```
ipv6 icmp error-decryptd-ipsec send switch
no ipv6 icmp error-decryptd-ipsec send [switch]
```

### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | IPsec で復号したパケットに対して ICMP エラーを送る   |
| off | IPsec で復号したパケットに対して ICMP エラーを送らない |

- [初期値]: on

### [説明]

IPsec で復号したパケットに対して ICMP エラーを送るか否か設定する。

### [ノート]

ICMP エラーには復号したパケットの先頭部分が含まれるため、ICMP エラーが送信元に返送される時にも IPsec で処理されないようになっており、本来 IPsec で保護したい通信が保護されずにネットワークに流れてしまう可能性がある。特に、フィルター型ルーティングでプロトコルによって IPsec で処理するかどうか切替えている場合には注意が必要となる。

ICMP エラーを送らないように設定すると、tracertoute に対して反応がなくなるなどの現象になる。

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 11.2.11 ステルス機能の設定

### [書式]

```
ipv6 stealth all
ipv6 stealth interface [interface...]
no ipv6 stealth [...]
```

### [設定値及び初期値]

- all: すべての論理インターフェースからのパケットに対してステルス動作を行う
  - [初期値]: -
- *interface*
  - [設定値]: 指定した論理インターフェースからのパケットに対してステルス動作を行う
  - [初期値]: -

### [説明]

このコマンドを設定すると、指定されたインターフェースから自分宛に来たパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインターフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくことでそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

### [ノート]

指定されたインターフェースからの PING にも答えなくなるので注意が必要である。

自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ipv6 icmp \*** コマンド群を用いる必要がある。

ブリッジインターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510



## 第 12 章

### トンネリング

#### 12.1 トンネルインターフェースの使用許可の設定

##### [書式]

**tunnel enable** *tunnel\_num* [*tunnel\_num* ...]

**no tunnel enable** *tunnel\_num*

##### [設定値及び初期値]

- *tunnel\_num*
- [設定値]:

| 設定値       | 説明                            |
|-----------|-------------------------------|
| 番号        | トンネルインターフェース番号                |
| 番号 1-番号 2 | 番号 1 から番号 2 までのトンネルインターフェース番号 |
| 番号 1-     | 番号 1 以上のすべてのトンネルインターフェース番号    |
| -番号 1     | 番号 1 以下のすべてのトンネルインターフェース番号    |
| all       | すべてのトンネルインターフェース              |

- [初期値]:-

##### [説明]

トンネルインターフェースを使用できる状態にする。

工場出荷時は、すべてのトンネルインターフェースは **disable** 状態であり、使用する場合は本コマンドにより、インターフェースを有効にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。複数指定は、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

#### 12.2 トンネルインターフェースの使用不許可の設定

##### [書式]

**tunnel disable** *tunnel\_num*

##### [設定値及び初期値]

- *tunnel\_num*
- [設定値]:

| 設定値       | 説明                            |
|-----------|-------------------------------|
| 番号        | トンネルインターフェース番号                |
| 番号 1-番号 2 | 番号 1 から番号 2 までのトンネルインターフェース番号 |
| 番号 1-     | 番号 1 以上のすべてのトンネルインターフェース番号    |
| -番号 1     | 番号 1 以下のすべてのトンネルインターフェース番号    |
| all       | すべてのトンネルインターフェース              |

- [初期値]:-

#### [説明]

トンネルインターフェースを使用できない状態にする。  
トンネル先の設定を行う場合は、**disable** 状態で行うのが望ましい。  
複数指定した場合には、その全てで使用できない状態になる。複数指定は、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 12.3 トンネルインターフェースの接続種別の設定

#### [書式]

**tunnel type** *type* [*role*]

**no tunnel type** [*type* [*role*]]

#### [設定値及び初期値]

- *type*

- [設定値]:

| 設定値            | 説明                       |
|----------------|--------------------------|
| point-to-point | point-to-point トンネル      |
| multipoint     | point-to-multipoint トンネル |

- [初期値]: point-to-point

- *role*

- [設定値]:

| 設定値    | 説明              |
|--------|-----------------|
| client | クライアントの役割を割り当てる |

- [初期値]: client

#### [説明]

トンネルインターフェースの接続種別を、接続先を 1 箇所だけ持つ **point-to-point** トンネル、もしくは、複数の接続先を持つ **point-to-multipoint** トンネル（マルチポイントトンネル）に設定する。

*role* オプションは *type* に **multipoint** を設定した場合のみ設定可能なオプションで、マルチポイントトンネルでは同一のトンネルに接続する複数のルーターの中から **server** と **client** をそれぞれ 1 台以上指定する必要がある。

#### [ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターの *role* オプションのみに **server** を指定する。なお、NVR700W は、**server** を指定できない。

NVR700W は、Rev.15.00.10 以降で使用可能。

#### [適用モデル]

NVR700W

## 12.4 トンネルインターフェースの種別の設定

#### [書式]

**tunnel encapsulation** *type*

**no tunnel encapsulation**

#### [設定値及び初期値]

- *type*

- [設定値]:

| 設定値        | 説明                                                                                 |
|------------|------------------------------------------------------------------------------------|
| ipsec      | IPsec トンネル                                                                         |
| ipip       | IPv6 over IPv4 トンネル、IPv4 over IPv6 トンネル、IPv4 over IPv4 トンネルまたは IPv6 over IPv6 トンネル |
| pptp       | PPTP トンネル                                                                          |
| l2tp       | L2TP/IPsec トンネル                                                                    |
| l2tpv3-raw | L2TPv3 トンネル                                                                        |
| l2tpv3     | L2TPv3/IPsec トンネル                                                                  |
| ipudp      | IPUDP トンネル                                                                         |
| map-e      | MAP-E トンネル                                                                         |

- [初期値]:
  - ipsec (NVR700W)
  - ipip (NVR510)

#### [説明]

トンネルインターフェースの種別を設定する。

#### [ノート]

トンネリングと NAT を併用する場合には **tunnel endpoint address** コマンドにより始点 IP アドレスを設定することが望ましい。

ipsec、l2tpv3-raw、および l2tpv3 は NVR700W で使用可能。NVR510 は Rev.15.01.03 以降で l2tp を指定可能。IPUDP トンネルは、データコネクタ接続以外では使用できない。

map-e キーワードは、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 12.5 トンネルインターフェースの IPv4 アドレスの設定

#### [書式]

```
ip tunnel address ip_address[/mask]
```

```
no ip tunnel address [ip_address[/mask]]
```

#### [設定値及び初期値]

- *ip\_address*
  - [設定値]: IPv4 アドレス
  - [初期値]: -
- *mask*
  - [設定値]:
    - xxx.xxx.xxx.xxx(xxx は十進数)
    - 0x に続く十六進数
    - マスクビット数
  - [初期値]: -

#### [説明]

トンネルインターフェースの IPv4 アドレスとネットマスクを設定する。

NVR700W では、このコマンドの設定によりトンネルインターフェースを経由して BGP のコネクションを確立できるようになる。

#### [適用モデル]

NVR700W, NVR510

## 12.6 トンネルインターフェースの相手側の IPv4 アドレスの設定

---

### [書式]

```
ip tunnel remote address ip_address
no ip tunnel remote address [ip_address]
```

### [設定値及び初期値]

- *ip\_address*
  - [設定値]: IPv4 アドレス
  - [初期値]: -

### [説明]

トンネルインターフェースの相手側の IPv4 アドレスを設定する。

NVR700W では、このコマンドの設定によりトンネルインターフェースを経由して BGP のコネクションを確立できるようになる。

### [適用モデル]

NVR700W, NVR510

## 12.7 相手側トンネルインターフェースの端点 IP アドレスの設定

---

### [書式]

```
tunnel endpoint remote address remote
no tunnel endpoint remote address [remote]
```

### [設定値及び初期値]

- *remote*
  - [設定値]: 相手側のトンネルインターフェース端点の IP アドレス、またはホスト名(半角 64 文字以内)
  - [初期値]: -

### [説明]

相手側のトンネルインターフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。トンネルインターフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

**tunnel endpoint local address** コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、ローカルエンドポイントアドレスに適切なインターフェースの IP アドレスが利用される。また、本コマンドでホスト名を設定し、**tunnel endpoint local address** コマンドで IP アドレスを設定した場合、**tunnel endpoint local address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

### [ノート]

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が *ipip* の場合である。本コマンドが設定されている場合、**tunnel endpoint address** コマンドおよび **tunnel endpoint name** コマンドの設定は利用されない。本コマンドは NVR700W の Rev.15.00.10 以降、NVR510 の Rev.15.01.09 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 12.8 自分側トンネルインターフェースの端点 IP アドレスの設定

---

### [書式]

```
tunnel endpoint local address local
no tunnel endpoint local address [local]
```

### [設定値及び初期値]

- *local*
  - [設定値]: 自分側のトンネルインターフェース端点の IP アドレス、またはホスト名(半角 64 文字以内)
  - [初期値]: -

**[説明]**

自分側のトンネルインターフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。トンネルインターフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

**tunnel endpoint remote address** コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、本コマンドの設定は反映されない。また、本コマンドでホスト名を設定し、**tunnel endpoint remote address** コマンドで IP アドレスを設定した場合、**tunnel endpoint remote address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

**[ノート]**

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が *ipip* の場合である。

NVR700W は Rev.15.00.10 以降で使用可能。

NVR510 は Rev.15.01.09 以降で使用可能。

IPv6 のダイナミックアドレスは NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 12.9 トンネルインターフェースの端点 IP アドレスの設定

---

**[書式]**

```
tunnel endpoint address [local] remote
no tunnel endpoint address [[local] remote]
```

**[設定値及び初期値]**

- *local*
  - [設定値]: 自分側のトンネルインターフェース端点の IP アドレス
  - [初期値]: -
- *remote*
  - [設定値]: 相手側のトンネルインターフェース端点の IP アドレス
  - [初期値]: -

**[説明]**

トンネルインターフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、*local* と *remote* では IPv4/IPv6 の種別が揃っていないといけない。トンネルインターフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

*local* を省略した場合は、適当なインターフェースの IP アドレスが利用される。

**[ノート]**

このコマンドにより設定した IP アドレスが利用されるのは、**tunnel encapsulation** コマンドの設定値が *pptp*、*l2tp*、*l2tpv3-raw*、*l2tpv3*、*ipip* の場合である。IPsec トンネルでは、トンネル端点は **ipsec ike local address** および **ipsec ike remote address** コマンドにより設定される。

PPTP サーバー、L2TP/IPsec サーバーの Anonymous で受ける場合には設定する必要はない。

**[適用モデル]**

NVR700W, NVR510

## 12.10 トンネルの端点の名前の設定

---

**[書式]**

```
tunnel endpoint name [local_name] remote_name [type]
no tunnel endpoint name [[local_name] remote_name [type]]
```

**[設定値及び初期値]**

- *local\_name*

- [設定値]: 自分側端点
- [初期値]: -
- *remote\_name*
  - [設定値]: 相手側端点
  - [初期値]: -
- *type*: 名前の種類
  - [設定値]:

| 設定値  | 説明        |
|------|-----------|
| fqdn | FQDN      |
| tel  | NGN 網電話番号 |

- [初期値]: fqdn

#### [説明]

トンネル端点の名前を指定する。

#### [ノート]

**tunnel endpoint address** コマンドが設定されている場合には、そちらが優先される。

このコマンドが利用されるのは、**tunnel encapsulation** コマンドの設定値が ptp、l2tpv3-raw、l2tpv3、ipip、ipudp の場合である。

ptp、l2tpv3-raw、l2tpv3、ipip トンネルの場合、名前にはドメイン名 (FQDN) を指定する。

ipudp トンネルの場合、名前には NGN 網電話番号を指定する。ハイフン無しで記述する。

ipip トンネルの名前指定は、NVR700W の Rev.15.00.10 以降、NVR510 の Rev.15.01.09 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 12.11 マルチポイントトンネルのサーバーの設定

#### [書式]

```
tunnel multipoint server id ip_address
```

```
no tunnel multipoint server id [ip_address]
```

#### [設定値及び初期値]

- *id*
  - [設定値]: サーバー識別子 (1 .. 3)
  - [初期値]: -
- *ip\_address*
  - [設定値]: IPv4 / IPv6 アドレスまたはホスト名
  - [初期値]: -

#### [説明]

マルチポイントトンネルにおいて、サーバーの役割が割り当てられているルーターのアドレスを設定する。本コマンドは **tunnel type** コマンドで接続種別に **multipoint**、**role** オプションに **client** が設定されているトンネルインターフェース (マルチポイントトンネルのクライアント側のトンネルインターフェース) で有効になる。

本コマンドを複数設定し、複数のサーバーを指定している場合は、接続可能なサーバーすべてに対してトンネルが接続される。最大で 3 台のサーバーを指定できる。

#### [ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターがサーバーとなる。

NVR700W は Rev.15.00.10 以降で使用可能。

#### [適用モデル]

NVR700W

## 12.12 マルチポイントトンネルで使用する自分の名前を設定

### [書式]

```
tunnel multipoint local name name
no tunnel multipoint local name [name]
```

### [設定値及び初期値]

- *name*
  - [設定値]: 名前（半角で 64 文字以内、全角で 32 文字以内）
  - [初期値]: -

### [説明]

マルチポイントトンネルで使用する自分の名前を設定する。

本コマンドで設定した名前はトンネル接続後に接続相手にも通知され、接続相手側でもトンネルの識別情報として SYSLOG 等で利用される。

### [ノート]

NVR700W は Rev.15.00.10 以降で使用可能。

### [適用モデル]

NVR700W

## 12.13 トンネルインタフェースの MAP-E 種別を設定

### [書式]

```
tunnel map-e type type
no tunnel map-e type [type]
```

### [設定値及び初期値]

- *type*
  - [設定値]:

| 設定値        | 説明                 |
|------------|--------------------|
| v6plus     | v6 プラス             |
| ocn        | OCN バーチャルコネクタサービス  |
| ipv6option | BIGLOBE IPv6 オプション |

- [初期値]: v6plus

### [説明]

トンネルインタフェースの MAP-E 種別を設定する。

**tunnel encapsulation** コマンドを *map-e* に設定したときに、どの MAP-E サービスを利用するかを設定する。

### [ノート]

NVR700W は、Rev.15.00.16 以降で使用可能。

NVR510 は、Rev.15.01.15 以降で使用可能。

ipv6option キーワードは、NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 12.14 トンネルインタフェースの変換種別を設定

### [書式]

```
tunnel translation type
no tunnel translation [type]
```

## [設定値及び初期値]

• *type*

## • [設定値]:

| 設定値   | 説明         |
|-------|------------|
| nat46 | NAT46 トンネル |

## • [初期値]:-

## [説明]

トンネルインタフェースの変換種別を設定する。

## [ノート]

**tunnel encapsulation** コマンドとの併用はできず、後から入力したコマンドが有効となる。

NVR700W Rev.15.00.23 以降で使用可能。

NVR510 Rev.15.01.23 以降で使用可能。

## [適用モデル]

NVR700W, NVR510



# 第 13 章

## IPsec の設定

NVR700W では、暗号化により IP 通信に対するセキュリティーを保証する IPsec 機能を実装しています。IPsec では、鍵交換プロトコル IKE (Internet Key Exchange) を使用します。必要な鍵は IKE により自動的に生成されますが、鍵の種類となる事前共有鍵は **ipsec ike pre-shared-key** コマンドで事前に登録しておく必要があります。この鍵はセキュリティー・ゲートウェイごとに設定できます。また、鍵交換の要求に応じるかどうかは、**ipsec ike remote address** コマンドで設定します。

鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA (Security Association) で管理します。SA を区別する ID は自動的に付与されます。SA の ID や状態は **show ipsec sa** コマンドで確認することができます。SA には、鍵の寿命に合わせた寿命があります。SA の属性のうちユーザーが指定可能なパラメーターをポリシーと呼びます。またその番号はポリシー ID と呼び、**ipsec sa policy** コマンドで定義し、**ipsec ike duration ipsec-sa**、**ipsec ike duration isakmp-sa** コマンドで寿命を設定します。

SA の削除は **ipsec sa delete** コマンドで、SA の初期化は **ipsec refresh sa** コマンドで行います。**ipsec auto refresh** コマンドにより、SA を自動更新させることも可能です。

IPsec による通信には、大きく分けてトンネルモードとトランスポートモードの 2 種類があります。

トンネルモードは IPsec による VPN (Virtual Private Network) を利用するためのモードです。ルーターがセキュリティー・ゲートウェイとなり、LAN 上に流れる IP パケットデータを暗号化して対向のセキュリティー・ゲートウェイとの間でやりとりします。ルーターが IPsec に必要な処理をすべて行うので、LAN 上の始点や終点となるホストには特別な設定を必要としません。

トンネルモードを用いる場合は、トンネルインターフェースという仮想的なインターフェースを定義し、処理すべき IP パケットがトンネルインターフェースに流れるように経路を設定します。個々のトンネルインターフェースはトンネルインターフェース番号で管理されます。設定のためにトンネル番号を切替えるには **tunnel select** コマンドを使用します。トンネルインターフェースを使用するか使用しないかは、それぞれ **tunnel enable**、**tunnel disable** コマンドを使用します。

| 相手先情報番号による設定                                                                                                                  |     | トンネルインターフェース番号による設定                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------|-----|-------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• <b>pp enable</b></li> <li>• <b>pp disable</b></li> <li>• <b>pp select</b></li> </ul> | <=> | <ul style="list-style-type: none"> <li>• <b>tunnel enable</b></li> <li>• <b>tunnel disable</b></li> <li>• <b>tunnel select</b></li> </ul> |

トランスポートモードは特殊なモードであり、ルーター自身が始点または終点になる通信に対してセキュリティーを保証するモードです。ルーターからリモートのルーターへ TELNET で入るなどの特殊な場合に利用できます。トランスポートモードを使用するには **ipsec transport** コマンドで定義を行い、使用をやめるには **no ipsec transport** コマンドで定義を削除します。

セキュリティー・ゲートウェイの識別子とトンネルインターフェース番号は、以下の表のようになります。

| モデル     | セキュリティー・ゲートウェイの識別子                                                                               | トンネルインターフェース番号                                                                                   |
|---------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| NVR700W | <ul style="list-style-type: none"> <li>• 1-20 (Rev.15.00.10 以降)</li> <li>• 1-6 (上記以外)</li> </ul> | <ul style="list-style-type: none"> <li>• 1-20 (Rev.15.00.10 以降)</li> <li>• 1-6 (上記以外)</li> </ul> |

本機はメインモード (main mode) とアグレッシブモード (aggressive mode) に対応しています。VPN を構成する両方のルーターが固定のグローバルアドレスを持つときにはメインモードを使用し、一方のルーターしか固定のグローバルアドレスを持たないときにはアグレッシブモードを使用します。

メインモードを使用するためには、**ipsec ike remote address** コマンドで対向のルーターの IP アドレスを設定する必要があります。アグレッシブモードを使用するときには、固定のグローバルアドレスを持つかどうかによって設定が異なります。固定のグローバルアドレスを持つルーターには、**ipsec ike remote name** コマンドを設定し、**ipsec ike remote address** コマンドで any を設定します。固定のグローバルアドレスを持たないルーターでは、**ipsec ike local name** コマンドを設定し、**ipsec ike remote address** コマンドで IP アドレスを設定します。

メインモードでは、**ipsec ike local name** コマンドや **ipsec ike remote name** コマンドを設定することはできません。また、アグレッシブモードでは、**ipsec ike local name** コマンドと **ipsec ike remote name** コマンドの両方を同時に設定することはできません。このように設定した場合には、正しく動作しない可能性があります。

## 13.1 IPsec の動作の設定

### [書式]

```
ipsec use use
no ipsec use [use]
```

### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明     |
|-----|--------|
| on  | 動作させる  |
| off | 動作させない |

- [初期値]: on

### [説明]

IPsec を動作させるか否かを設定する。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 13.2 IKE バージョンの設定

### [書式]

```
ipsec ike version gateway_id version
no ipsec version gateway_id [version]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *version*
  - [設定値]: 使用する IKE のバージョン
  - [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| 1   | IKE バージョン 1 |
| 2   | IKE バージョン 2 |

- [初期値]: 1

### [説明]

セキュリティー・ゲートウェイで使用する IKE のバージョンを設定する。

### [ノート]

*version* で指定したバージョン以外での接続以外は受け付けない。

### [適用モデル]

NVR700W

## 13.3 IKE の認証方式の設定

### [書式]

```
ipsec ike auth method gateway_id method
no ipsec ike auth method gateway_id [method]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *method*
  - [設定値]:

| 設定値            | 説明            |
|----------------|---------------|
| auto           | 認証方式を自動的に選択する |
| pre-shared-key | 事前共有鍵         |
| certificate    | デジタル署名        |
| eap-md5        | EAP-MD5       |

- [初期値]:
  - auto

**[説明]**

IKE の認証方式を設定する。

METHOD に auto を設定した場合、以下の条件にしたがって認証方式が決定される。

- 事前共有鍵方式
  - **ipsec ike pre-shared-key** コマンドが設定されている場合。
- デジタル署名方式
 

次の条件をすべて満たしている場合

  - **ipsec ike pki file** コマンドで指定した場所に証明書が保存されている。
  - **ipsec ike eap request** コマンドおよび **ipsec ike eap myname** コマンドが設定されていない。
- EAP-MD5 方式
 

次の条件をすべて満たしている場合

  - **ipsec ike pki file** コマンドで指定した場所に証明書が保存されている。
  - **ipsec ike eap request** コマンド、または **ipsec ike eap myname** コマンドが設定されていない。

上記、認証方式を決定する条件のうち、複数の条件に合致する場合、次の順番で認証方式が優先される。

1. 事前共有鍵方式
2. デジタル署名方式
3. EAP-MD5 方式

*method* に auto 以外を指定した場合、上記の認証方式を決定する条件にかかわらず、*method* に指定した方式で認証を行う。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

**[適用モデル]**

NVR700W

## 13.4 事前共有鍵の登録

---

**[書式]**

```
ipsec ike pre-shared-key gateway_id key
ipsec ike pre-shared-key gateway_id text text
no ipsec ike pre-shared-key gateway_id [...]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *key*
  - [設定値]: 鍵となる 0x ではじまる十六進数列 (128 バイト以内)

- [初期値]: -
- *text*
  - [設定値]: ASCII 文字列で表した鍵 (128 文字以内)
  - [初期値]: -

**[説明]**

鍵交換に必要な事前共有鍵を登録する。設定されていない場合には、鍵交換は行われない。鍵交換を行う相手ルーターには同じ事前共有鍵が設定されている必要がある。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[設定例]**

```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDCD0CDEDCD
```

**[適用モデル]**

NVR700W, NVR510

## 13.5 IKEv2 の認証に使用する PKI ファイルの設定

---

**[書式]**

```
ipsec ike pki file gateway_id certificate=cert_id [crl=crl_id]
no ipsec ike pki file gateway_id [...]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *cert\_id*
  - [設定値]: 証明書ファイルの識別子 (1..8)
  - [初期値]: -
- *crl\_id*
  - [設定値]: CRL ファイルの識別子 (1..8)
  - [初期値]: -

**[説明]**

IKEv2 の認証に使用する PKI ファイルを設定する。

デジタル証明書方式の認証を行う場合、*cert\_id* に使用する証明書が保存されているファイルの識別子を指定する。

EAP-MD5 認証を行う場合、始動側は相手の証明書を検証するために *cert\_id* に自分の証明書が保存されているファイルの識別子を指定する。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

**[適用モデル]**

NVR700W

## 13.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定

---

**[書式]**

```
ipsec ike eap myname gateway_id name password
no ipsec ike eap myname gateway_id [...]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -

- *name*
  - [設定値]: 名前 (半角 256 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (半角 64 文字以内)
  - [初期値]: -

**[説明]**

EAP-MD5 認証を要求されたときに使用する名前とパスワードを設定する。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

**[適用モデル]**

NVR700W

## 13.7 EAP-MD5 によるユーザー認証の設定

---

**[書式]**

```
ipsec ike eap request gateway_id sw group_id
no ipsec ike eap request gateway_id [...]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 要求する  |
| off | 要求しない |

- [初期値]: off
- *group\_id*
  - [設定値]: 認証に使用するユーザーグループの識別番号
  - [初期値]: -

**[説明]**

IKEv2 で、EAP-MD5 認証をクライアントに要求するか否かを設定する。 *group\_id* を指定した場合には、該当のユーザーグループに含まれるユーザーを認証の対象とする。

本コマンドによる設定はルーターが応答側として動作するときのみ有効であり、始動側のセキュリティ・ゲートウェイから送信された IKE AUTH 交換に AUTH ペイロードが含まれない場合に EAP-MD5 によるユーザー認証を行う。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

**[適用モデル]**

NVR700W

## 13.8 EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定

---

**[書式]**

```
ipsec ike eap send certreq gateway_id switch
no ipsec ike eap send certreq gateway_id [switch]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: off

#### [説明]

EAP-MD5 認証方式の場合、始動側のセキュリティー・ゲートウェイから送信する IKE\_AUTH 交換に、証明書要求 (CERTREQ) ペイロードを含めるか否かを設定する。

#### [ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]  
NVR700W

## 13.9 IKE の鍵交換を始動するか否かの設定

#### [書式]

```
ipsec auto refresh [gateway_id] switch
no ipsec auto refresh [gateway_id]
```

#### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明        |
|-----|-----------|
| on  | 鍵交換を始動する  |
| off | 鍵交換を始動しない |

- [初期値]:
  - off ( 全体的な動作 )
  - on (*gateway\_id* 毎)

#### [説明]

IKE の鍵交換を始動するかどうかを設定する。他のルーターが始動する鍵交換については、このコマンドに関係なく常に受け付ける。

*gateway\_id* パラメーターを指定しない書式は、ルーターの全体的な動作を決める。この設定が off のときにはルーターは鍵交換を始動しない。

*gateway\_id* パラメーターを指定する書式は、指定したセキュリティー・ゲートウェイに対する鍵交換の始動を抑制するために用意されている。

例えば、次の設定では、1 番のセキュリティー・ゲートウェイのみが鍵交換を始動しない。

```
ipsec auto refresh on
ipsec auto refresh 1 off
```

#### [ノート]

**ipsec auto refresh off** の設定では、*gateway\_id* パラメーターを指定する書式は効力を持たない。例えば、次の設定では、1 番のセキュリティー・ゲートウェイでは鍵交換を始動しない。

```
ipsec auto refresh off ( デフォルトの設定 )
ipsec auto refresh 1 on
```

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 13.10 設定が異なる場合に鍵交換を拒否するか否かの設定

[書式]

```
ipsec ike negotiate-strictly gateway_id switch
no ipsec ike negotiate-strictly gateway_id
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- switch
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | 鍵交換を拒否する |
| off | 鍵交換を受理する |

- [初期値]: off

[説明]

IKEv1 として動作する際、設定が異なる場合に鍵交換を拒否するか否かを設定する。このコマンドの設定が off のときには、従来のファームウェアと同様に動作する。すなわち、相手の提案するパラメーターが自分の設定と異なる場合でも、そのパラメーターをサポートしていれば、それを受理する。このコマンドの設定が on のときには、同様の状況で相手の提案を拒否する。このコマンドが適用されるパラメーターと対応するコマンドは以下の通りである。

| パラメーター      | 対応するコマンド                |
|-------------|-------------------------|
| 暗号アルゴリズム    | ipsec ike encryption    |
| グループ        | ipsec ike group         |
| ハッシュアルゴリズム  | ipsec ike hash          |
| PFS         | ipsec ike pfs           |
| フェーズ 1 のモード | ipsec ike local name など |

[ノート]

本コマンドは IKEv2 としての動作には影響を与えない。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 13.11 IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定

[書式]

```
ipsec ike always-on gateway_id switch
no ipsec ike always-on
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- switch

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | 鍵交換を継続する |
| off | 鍵交換を休止する |

- [初期値]: off

#### [説明]

IKE の鍵交換に失敗したときに鍵交換を休止せずに継続できるようにする。IKE キープアライブを用いるときには、このコマンドを設定しなくても、常に鍵交換を継続する。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.12 鍵交換の再送回数と間隔の設定

#### [書式]

```
ipsec ike retry count interval [max_session]
no ipsec ike retry [count interval [max_session]]
```

#### [設定値及び初期値]

- *count*
  - [設定値]: 再送回数 (1..50)
  - [初期値]: 10
- *interval*
  - [設定値]: 再送間隔の秒数 (1..100)
  - [初期値]: 5
- *max\_session*
  - [設定値]: 同時に動作するフェーズ 1 の最大数 (1..5)
  - [初期値]: 3

#### [説明]

鍵交換の packets が相手に届かないときに実施する再送の回数と間隔を設定する。

また、*max\_session* パラメーターは、IKEv1 において同時に動作するフェーズ 1 の最大数を指定する。ルーターは、フェーズ 1 が確立せずに再送を継続する状態にあるとき、鍵の生成を急ぐ目的で、新しいフェーズ 1 を始動することがある。このパラメーターは、このような状況で、同時に動作するフェーズ 1 の数を制限するものである。なお、このパラメーターは、始動側のフェーズ 1 のみを制限するものであり、応答側のフェーズ 1 に対しては効力を持たない。

#### [ノート]

IKEv2 として動作する場合、*max\_session* パラメーターは効力を持たない。同じ相手側セキュリティー・ゲートウェイに対して始動する鍵交換セッションは、常に最大 1 セッションとなる。

相手側セキュリティー・ゲートウェイに掛かっている負荷が非常に高い場合、本コマンドの設定値を調整することで鍵交換が成功しやすくなる可能性がある。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.13 相手側のセキュリティー・ゲートウェイの名前の設定

#### [書式]

```
ipsec ike remote name gateway name [type]
```



**no ipsec ike remote name gateway [name]**

**[設定値及び初期値]**

- gateway
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- name
  - [設定値]: 名前 (256 文字以内)
  - [初期値]: -
- type : id の種類
  - [設定値]:

| 設定値                          | 説明                            |
|------------------------------|-------------------------------|
| ipv4-addr                    | ID_IPV4_ADDR                  |
| fqdn                         | ID_FQDN                       |
| user-fqdn (もしくは rfc822-addr) | ID_USER_FQDN (ID_RFC822_ADDR) |
| ipv6-addr                    | ID_IPV6_ADDR                  |
| key-id                       | ID_KEY_ID                     |
| tel                          | NGN 網電話番号 (ID_IPV6_ADDR)      |
| tel-key                      | NGN 網電話番号 (ID_KEY_ID)         |

- [初期値]: -

**[説明]**

相手側のセキュリティ・ゲートウェイの名前と ID の種類を設定する。  
 その他、動作する IKE のバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1
 

このコマンドの設定は、フェーズ 1 のアグレッシブモードで使用され、メインモードでは使用されない。  
 また、type パラメーターは相手側セキュリティ・ゲートウェイの判別時に考慮されない。
- IKEv2
 

相手側セキュリティ・ゲートウェイの判別時には name、type パラメーターの設定が共に一致している必要がある。  
 type パラメーターが 'tel' の場合、相手側 IPv6 アドレス (ID\_IPV6\_ADDR) を相手側セキュリティ・ゲートウェイの判別に使用する。  
 type パラメーターが 'tel-key' の場合、設定値を ID\_KEY\_ID として相手側セキュリティ・ゲートウェイの判別に使用する。  
 type パラメーターが 'key-id' 以外の場合、name から相手側セキュリティ・ゲートウェイの IP アドレスの特定を試み、特定できれば、そのホストに対して鍵交換を始動する。この場合、**ipsec ike remote address** コマンドの設定は不要である。  
 ただし、**ipsec ike remote address** コマンドが設定されている場合は、そちらの設定にしたがって始動時の接続先ホストが決定される。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**13.14 相手側セキュリティ・ゲートウェイの IP アドレスの設定**

**[書式]**

**ipsec ike remote address gateway\_id ip\_address**  
**no ipsec ike remote address gateway\_id [ip\_address]**

**[設定値及び初期値]**

- `gateway_id`
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- `ip_address`
  - [設定値]:

| 設定値             | 説明                                              |
|-----------------|-------------------------------------------------|
| IP アドレス、またはホスト名 | 相手側セキュリティ・ゲートウェイの IP アドレス、またはホスト名 (半角 255 文字以内) |
| any             | 自動選択                                            |

- [初期値]: -

**[説明]**

相手側セキュリティ・ゲートウェイの IP アドレスまたはホスト名を設定する。ホスト名で設定した場合には、鍵交換の始動時にホスト名から IP アドレスを DNS により検索する。

その他、動作する IKE バージョンによって異なる、本コマンドの影響、注意点については以下の通り。

## • IKEv1

応答側になる場合、本コマンドで指定したホストは相手側セキュリティ・ゲートウェイの判別に使用される。'any' が設定された場合は、相手側セキュリティ・ゲートウェイとして任意のホストから鍵交換を受け付ける。その代わりに、自分から鍵交換を始動することはできない。例えば、アグレッシブモードで固定のグローバルアドレスを持つ場合などに利用する。

## • IKEv2

このコマンドで設定したホストは、鍵交換を始動する際の接続先としてのみ使用される。'any' は自分側から鍵交換を始動しないことを明示的に示す。

応答側となる場合、本コマンドの設定による相手側セキュリティ・ゲートウェイの判別は **ipsec ike remote name** コマンド等の設定によって行われる。

**[ノート]**

ホスト名を指定する場合には、**dns server** コマンドなどで必ず DNS サーバーを設定しておくこと。IPsec メインモード接続では、相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定しない。相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定した場合の動作は保証されない。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**13.15 相手側の ID の設定****[書式]**

```
ipsec ike remote id gateway_id ip_address[/mask]
no ipsec ike remote id gateway_id [ip_address[/mask]]
```

**[設定値及び初期値]**

- `gateway_id`
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- `ip_address`
  - [設定値]: IP アドレス
  - [初期値]: -
- `mask`
  - [設定値]: ネットマスク
  - [初期値]: -

**[説明]**

IKEv1 のフェーズ 2 で用いる相手側の ID を設定する。

このコマンドが設定されていない場合は、フェーズ 2 で ID を送信しない。

*mask* パラメーターを省略した場合は、タイプ 1 の ID が送信される。また、*mask* パラメーターを指定した場合は、タイプ 4 の ID が送信される。

**[ノート]**

本コマンドは IKEv2 の動作には影響を与えない。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 13.16 自分側のセキュリティー・ゲートウェイの名前の設定

**[書式]**

**ipsec ike local name gateway\_id name [type]**

**no ipsec ike local name gateway\_id [name]**

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *name*
  - [設定値]: 名前 (256 文字以内)
  - [初期値]: -
- *type*: id の種類
  - [設定値]:

| 設定値                          | 説明                            |
|------------------------------|-------------------------------|
| ipv4-addr                    | ID_IPV4_ADDR                  |
| fqdn                         | ID_FQDN                       |
| user-fqdn (もしくは rfc822-addr) | ID_USER_FQDN (ID_RFC822_ADDR) |
| ipv6-addr                    | ID_IPV6_ADDR                  |
| key-id                       | ID_KEY_ID                     |
| tel                          | NGN 網電話番号 (ID_IPV6_ADDR)      |
| tel-key                      | NGN 網電話番号 (ID_KEY_ID)         |

- [初期値]: -

**[説明]**

自分側のセキュリティー・ゲートウェイの名前と ID の種類を設定する。

なお、IKEv1 として動作する際に *type* パラメーターが 'ipv4-addr'、'ipv6-addr'、'tel'、'tel-key' に設定されていた場合は 'key-id' を設定したときと同等の動作となる。IKEv2 かつ *type* パラメーターが 'tel' の場合、自分側 IPv6 アドレス (ID\_IPV6\_ADDR) を鍵交換に使用する。IKEv2 かつ *type* パラメーターが 'tel-key' の場合、設定値を ID\_KEY\_ID とし鍵交換に使用する。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 13.17 自分側セキュリティ・ゲートウェイの IP アドレスの設定

### [書式]

```
ipsec ike local address gateway_id ip_address
ipsec ike local address gateway_id vrrp interface vrid
ipsec ike local address gateway_id ipv6 prefix prefix on interface
ipsec ike local address gateway_id ipcp pp pp_num
no ipsec ike local address gateway_id [ip_address]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティ・ゲートウェイの識別子
  - [初期値]: -
- *ip\_address*
  - [設定値]: 自分側セキュリティ・ゲートウェイの IP アドレス
  - [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*
  - [設定値]: VRRP グループ ID (1..255)
  - [初期値]: -
- *prefix*
  - [設定値]: プレフィックス
  - [初期値]: -
- *pp\_num*
  - [設定値]: PP インターフェース番号
  - [初期値]: -

### [説明]

自分側セキュリティ・ゲートウェイの IP アドレスを設定する。

vrrp キーワードを指定する第 2 書式では、VRRP マスターとして動作している場合のみ、指定した LAN インターフェース/VRRP グループ ID の仮想 IP アドレスを自分側セキュリティ・ゲートウェイアドレスとして利用する。VRRP マスターでない場合には鍵交換は行わない。

ipv6 キーワードを指定する第 3 書式では、IPv6 のダイナミックアドレスを指定する。

ipcp キーワードを指定する第 4 書式では、IPCP アドレスを取得する PP インターフェースを指定する。

### [ノート]

本コマンドが設定されていない場合には、相手側のセキュリティ・ゲートウェイに近いインターフェースの IP アドレスを用いて IKE を起動する。

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 13.18 自分側の ID の設定

### [書式]

```
ipsec ike local id gateway_id ip_address[/mask]
no ipsec ike local id gateway_id [ip_address[/mask]]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティ・ゲートウェイの識別子
  - [初期値]: -

- *ip\_address*
  - [設定値]: IP アドレス
  - [初期値]: -
- *mask*
  - [設定値]: ネットマスク
  - [初期値]: -

**[説明]**

IKEv1 のフェーズ 2 で用いる自分側の ID を設定する。

このコマンドが設定されていない場合には、フェーズ 2 で ID を送信しない。  
*mask* パラメーターを省略した場合は、タイプ 1 の ID が送信される。  
 また、*mask* パラメーターを指定した場合は、タイプ 4 の ID が送信される。

**[ノート]**

本コマンドは IKEv2 としての動作には影響を与えない。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 13.19 IKE キープアライブ機能の設定

**[書式]**

```

ipsec ike keepalive use gateway_id switch [down=disconnect] [send-only-new-sa=send]
ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect] [send-only-new-sa=send]
ipsec ike keepalive use gateway_id switch icmp-echo ip_address [length=length] [interval count [upwait]]
[down=disconnect]
ipsec ike keepalive use gateway_id switch dpd [interval count [upwait]]
ipsec ike keepalive use gateway_id switch rfc4306 [interval count [upwait]]
no ipsec ike keepalive use gateway_id [switch ....]
    
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *switch*: キープアライブの動作
  - [設定値]:

| 設定値  | 説明                                                          |
|------|-------------------------------------------------------------|
| on   | キープアライブを使用する                                                |
| off  | キープアライブを使用しない                                               |
| auto | 対向のルーターがキープアライブを送信するときに限って送信する ( heartbeat 、 rfc4306 でのみ有効) |

- [初期値]: auto
- *ip\_address*
  - [設定値]: ping を送信する宛先の IP アドレス ( IPv4/IPv6 )
  - [初期値]: -
- *length*
  - [設定値]: ICMP echo のデータ部の長さ ( 64..1500 )
  - [初期値]: 64
- *interval*
  - [設定値]: キープアライブパケットの送信間隔秒数 ( 1..600 )
  - [初期値]: 10
- *count*

- [設定値]: キープアライブパケットが届かないときに障害とみなすまでの試行回数 ( 1..50 )
- [初期値]: 6
- *upwait*
  - [設定値]: IPsec SA が生成されてから実際にトンネルインターフェースを有効にするまでの時間 ( 0..1000000 )
  - [初期値]: 0
- *send*
  - [設定値]:

| 設定値 | 説明                                           |
|-----|----------------------------------------------|
| on  | 新旧の SA が混在する場合、新しい SA のみに対してキープアライブパケットを送信する |
| off | 新旧の SA が混在する場合、新旧 SA の両方に対してキープアライブパケットを送信する |

- [初期値]: off

### [説明]

IKE キープアライブの動作を設定する。

本コマンドは、動作する IKE のバージョンによって以下のように動作が異なる。

#### • IKEv1

キープアライブの方式としては、heartbeat、ICMP Echo、DPD ( RFC3706 ) の 3 種類から選ぶことができる。第 1 書式は自動的に heartbeat 書式となる。

heartbeat 書式を利用するには第 1、第 2 書式を使用する。 heartbeat 方式において *switch* パラメーターが *auto* に設定されている場合は、相手から heartbeat パケットを受信したときだけ heartbeat パケットを送信する。従って、双方の設定が *auto* になっているときには、IKE キープアライブは動作しない。

ICMP Echo を利用するときには第 3 書式を使用し、送信先の IP アドレスを設定する。オプションとして、ICMP Echo のデータ部の長さを指定することができる。この方式では、*switch* パラメーターが *auto* でも *on* の場合と同様に動作する。

DPD を利用するときには第 4 書式を使用する。この方式では *switch* パラメーターが *auto* でも *on* の場合と同様に動作する。

その他、IKEv1 で対応していない方式 ( 書式 ) が設定されている場合は、代替方式として heartbeat で動作する。このとき、*switch*、*count*、*interval*、*upwait* パラメーターは設定内容が反映される。

#### • IKEv2

キープアライブの方式として、RFC4306 ( IKEv2 標準 )、ICMP Echo の 2 種類から選ぶことができる。第 1 書式は自動的に RFC4306 方式となる。

*switch* パラメーターが *auto* の場合には、RFC4306 方式のキープアライブパケットを受信したときだけ応答パケットを送信する。なお、IKEv2 ではこの方式のキープアライブパケットには必ず応答しなければならないため、*switch* パラメーターが *auto* でも *off* の場合でも同様に動作する。

ICMP Echo を利用するときには第 3 書式を使用し、送信先の IP アドレスを設定する。オプションとして、ICMP Echo のデータ部の長さを指定することができる。この方式では、*switch* パラメーターが *auto* でも *on* の場合と同様に動作する。

その他、IKEv2 で対応していない方式 ( 書式 ) が設定されている場合は、代替方式として RFC4306 で動作する。このとき、*switch*、*count*、*interval*、*upwait* パラメーターは設定内容が反映される。

### [ノート]

相手先が PP インターフェースの先にある場合、*down* オプションを指定することができる。 *down* オプションを指定すると、キープアライブダウン検出時と IKE の再送回数満了時に PP インターフェースの切断を行うことができる。網側の状態などで PP インターフェースの再接続によりトンネル確立状態の改善を望める場合に利用することができる。

キープアライブの方式として heartbeat を使用する場合、*send-only-new-sa* オプションを指定することができる。 *send-only-new-sa* オプションに *on* を設定すると、鍵交換後の新旧の SA が混在するときに新しい SA のみに対してキープアライブパケットを送信するようになり、鍵交換時の負荷を軽減することができる。ただし、*send-only-new-sa* オプ

ションに対応していないファームウェアとトンネルを構築する場合は、send-only-new-sa オプションを off に設定しておかなければトンネルがダウンする。

length パラメーターで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。同じ相手に対して、複数の方法を併用することはできない。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.20 IKE キープアライブに関する SYSLOG を出力するか否かの設定

[書式]

```
ipsec ike keepalive log gateway_id log
no ipsec ike keepalive log gateway_id [log]
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- log
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

- [初期値]: on

[説明]

IKE キープアライブに関する SYSLOG を出力するか否かを設定する。この SYSLOG は DEBUG レベルの出力である。

[ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.21 IKE が用いる暗号アルゴリズムの設定

[書式]

```
ipsec ike encryption gateway_id algorithm
no ipsec ike encryption gateway_id [algorithm]
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- algorithm
  - [設定値]:

| 設定値      | 説明       |
|----------|----------|
| 3des-cbc | 3DES-CBC |
| des-cbc  | DES-CBC  |
| aes-cbc  | AES-CBC  |

| 設定値        | 説明         |
|------------|------------|
| aes256-cbc | AES256-CBC |

- [初期値]: 3des-cbc

#### [説明]

IKE が用いる暗号アルゴリズムを設定する。

始動側として働く場合に、本コマンドで設定されたアルゴリズムを提案する。応答側として働く場合は本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。

ただし、IKEv1 で `ipsec ike negotiate-strictly` コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。

#### [ノート]

IKEv2 では、`ipsec ike proposal-limitation` コマンドが on に設定されているとき、本コマンドで設定されたアルゴリズムを提案する。`ipsec ike proposal-limitation` コマンドが off に設定されているときは、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティー・ゲートウェイに選択させる。また応答側として働く場合は、提案されたものからより安全なアルゴリズムを選択する。

IKEv2 でサポート可能な暗号アルゴリズム及び応答時の選択の優先順位は以下の通り。

- AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

※IKEv2 でのみ AES192-CBC をサポートする。ただし、コマンドで AES192-CBC を選択することはできない。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [設定例]

```
# ipsec ike encryption 1 aes-cbc
```

#### [適用モデル]

NVR700W, NVR510

## 13.22 受信した IKE パケットを蓄積するキューの長さの設定

#### [書式]

```
ipsec ike queue length length
no ipsec ike queue length [length]
```

#### [設定値及び初期値]

- *length*
  - [設定値]: キュー長 (6...12)
  - [初期値]: 12

#### [説明]

受信した IKE パケットを蓄積するキューの長さを設定する。この設定は、短時間に集中して IKE パケットを受信した際のルーターの振る舞いを決定する。設定した値が大きいくほど、IKE パケットが集中したときにより多くのパケットを取りこぼさないで処理することができるが、逆に IKE パケットがルーターに滞留する時間が長くなるためキーブアライブの応答が遅れ、トンネルの障害を間違えて検出する可能性が増える。通常の運用では、この設定を変更する必要はないが、多数のトンネルを構成しており、多数の SA を同時に消す状況があるならば値を大きめに設定するとよい。

#### [ノート]

キューの長さを長くすると、一度に受信して処理できる IKE パケットの数を増やすことができる。しかし、あまり大きくすると、ルーター内部にたまった IKE パケットの処理が遅れ、対向のルーターでタイムアウトと検知されてしまう可能性が増える。そのため、このコマンドの設定を変更する時には、慎重に行う必要がある。

通常の運用では、この設定を変更する必要はない。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510



## 13.23 IKE が用いるグループの設定

### [書式]

```
ipsec ike group gateway_id group [group]
no ipsec ike group gateway_id [group [group]]
```

### [設定値及び初期値]

- *gateway\_id*: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *group*: グループ識別子
  - [設定値]:
    - modp768
    - modp1024
    - modp1536
    - modp2048
  - [初期値]: modp1024

### [説明]

IKE で用いるグループを設定する。

始動側として働く場合には、このコマンドで設定されたグループを提案する。応答側として働く場合には、このコマンドの設定に関係なく、サポート可能な任意のグループを用いることができる。

その他、動作する IKE のバージョンによって異なる本コマンドの影響、注意点については以下の通り。

- IKEv1
  - 2 種類のグループを設定した場合には、1 つ目がフェーズ 1 で、2 つ目がフェーズ 2 で提案される。グループを 1 種類しか設定しない場合は、フェーズ 1 とフェーズ 2 の両方で、設定したグループが提案される。
  - また、**ipsec ike negotiate-strictly** コマンドが on の場合は、応答側であっても設定したグループしか利用できない。
- IKEv2
  - 常に 1 つ目に設定したグループのみが使用される。2 つ目に設定したグループは無視される。
  - また、始動側として提案したグループが相手に拒否され、別のグループを要求された場合は、そのグループで再度提案する (要求されたグループがサポート可能な場合)。以後、IPsec の設定を変更するか再起動するまで、同じ相手側セキュリティ・ゲートウェイに対しては再提案したグループが優先的に使用される。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 13.24 IKE が用いるハッシュアルゴリズムの設定

### [書式]

```
ipsec ike hash gateway_id algorithm
no ipsec ike hash gateway_id [algorithm]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *algorithm*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| md5 | MD5   |
| sha | SHA-1 |

| 設定値    | 説明      |
|--------|---------|
| sha256 | SHA-256 |

- [初期値]: sha

#### [説明]

IKE が用いるハッシュアルゴリズムを設定する。

始動側として働く場合に、本コマンドで設定されたアルゴリズムを提案する。応答側として働く場合は本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。

ただし、IKEv1 で **ipsec ike negotiate-strictly** コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。

#### [ノート]

IKEv2 では、IKEv1 のハッシュアルゴリズムに相当する折衝パラメーターとして、認証アルゴリズム (Integrity Algorithm) と PRF (Pseudo-Random Function) がある。IKEv2 で **ipsec ike proposal-limitation** コマンドが on に設定されているとき、本コマンドで設定されたアルゴリズムを提案する。**ipsec ike proposal-limitation** コマンドが off に設定されているときは、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティー・ゲートウェイに選択させる。また応答側として働く場合は、提案されたものからより安全なアルゴリズムを選択する。

IKEv2 でサポート可能な認証アルゴリズム及び応答時の選択の優先順位は以下の通り。

- HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

また、IKEv2 でサポート可能な PRF、及び応答選択時の優先順位は以下の通り。

- HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.25 受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定

#### [書式]

**ipsec log illegal-spi** *switch*

**no ipsec log illegal-spi**

#### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | ログに出力する  |
| off | ログに出力しない |

- [初期値]: off

#### [説明]

IPsec で、受信したパケットの SPI 値が無効な値の場合に、その旨をログに出力するか否かを設定する。SPI 値と相手の IP アドレスがログに出力される。

無効な SPI 値を含むパケットを大量に送り付けられることによる DoS の可能性を減らすため、ログは 1 秒あたり最大 10 種類のパケットだけを記録する。実際に受信したパケットの数を知ることはできない。

#### [ノート]

鍵交換時には、鍵の生成速度の差により一方が新しい鍵を使い始めても他方ではまだその鍵が使用できない状態になっているためにこのログが一時的に出力されてしまうことがある。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.26 IKE ペイロードのタイプの設定

### [書式]

```
ipsec ike payload type gateway_id type1 [type2]
no ipsec ike payload type gateway_id [type1 ...]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *type1*: IKEv1 のメッセージのフォーマット
  - [設定値]:

| 設定値 | 説明                           |
|-----|------------------------------|
| 1   | ヤマハルーターのリリース 2 との互換性を保持する    |
| 2   | ヤマハルーターのリリース 3 に合わせる         |
| 3   | 初期ベクトル (IV) の生成方法を一部の実装に合わせる |

- [初期値]: 2
- *type2*: IKEv2 のメッセージのフォーマット
  - [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| 1   | ヤマハルーターの IKEv2 のリリース 1 との互換性を保持する |
| 2   | 鍵交換や鍵の使用方法を一部の実装に合わせる             |

- [初期値]: 2

### [説明]

IKEv1 および IKEv2 のペイロードのタイプを設定する。

IKEv1 でヤマハルーターの古いリビジョンと接続する場合には、*type1* パラメーターを 1 に設定する必要がある。

IKEv2 でヤマハルーターの以下のリビジョンと接続する場合には、*type2* パラメーターを 1 に設定する必要がある。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 13.27 IKEv1 鍵交換タイプの設定

### [書式]

```
ipsec ike backward-compatibility gateway_id type
no ipsec ike backward-compatibility gateway_id [type]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *type*: IKEv1 で使用する鍵交換のタイプ
  - [設定値]:

| 設定値 | 説明                                  |
|-----|-------------------------------------|
| 1   | ヤマハルーターのリリース 1 (過去のリリース) との互換性を保持する |
| 2   | ヤマハルーターのリリース 2 (新リリース) に合わせる        |

- [初期値]: 1

#### [説明]

IKEv1 で使用する鍵交換のタイプを設定する。

IKEv1 でヤマハルーターの古いリビジョンと接続する場合には、*type* パラメーターを 1 に設定する必要がある。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.28 IKE の情報ペイロードを送信するか否かの設定

#### [書式]

```
ipsec ike send info gateway_id info
```

```
no ipsec ike send info gateway_id [info]
```

#### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *info*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

#### [説明]

IKEv1 動作時に、情報ペイロードを送信するか否かを設定する。受信に関しては、この設定に関わらず、すべての情報ペイロードを解釈する。

#### [ノート]

このコマンドは、接続性の検証などの特別な目的で使用される。定常の運用時は on に設定する必要がある。

本コマンドは IKEv2 としての動作には影響を与えない。IKEv2 では常に、必要に応じて情報ペイロードの送受信を行う。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.29 PFS を用いるか否かの設定

#### [書式]

```
ipsec ike pfs gateway_id pfs
```

```
no ipsec ike pfs gateway_id [pfs]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *pfs*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: off

**[説明]**

IKE の始動側として働く場合に、PFS (Perfect Forward Secrecy) を用いるか否かを設定する。応答側として働く場合は、このコマンドの設定に関係なく、相手側セキュリティ・ゲートウェイの PFS の使用有無に合わせて動作する。ただし、IKEv1 として動作し、且つ **ipsec ike negotiate-strictly** コマンドが on の場合は、本コマンドの設定と相手側セキュリティ・ゲートウェイの PFS の使用有無が一致していなければならない。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 13.30 XAUTH の設定

---

**[書式]**

```
ipsec ike xauth myname gateway_id name password
no ipsec ike xauth myname gateway_id
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *name*
  - [設定値]: XAUTH で通知する名前 (32 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: XAUTH で通知するパスワード (32 文字以内)
  - [初期値]: -

**[説明]**

XAUTH の認証を要求されたときに通知する名前とパスワードを設定する。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 13.31 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の設定

---

**[書式]**

```
auth user userid username password
no auth user userid [username ...]
```

**[設定値及び初期値]**

- *userid*
  - [設定値]: ユーザー識別番号 (1..1000)
  - [初期値]: -
- *username*
  - [設定値]: ユーザー名 (256 文字以内)(\* 3 文字以上に設定してください。)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (64 文字以内)(\* 同上)
  - [初期値]: -

**[説明]**

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザー ID を設定する。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 13.32 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の属性の設定

**[書式]**

```
auth user attribute userid attribute=value [attribute=value ...]
```

```
no auth user attribute userid [attribute=value ...]
```

**[設定値及び初期値]**

- *userid*
  - [設定値]: ユーザー識別番号 (1..1000)
  - [初期値]: -
- *attribute=value*
  - [設定値]: ユーザー属性
  - [初期値]: xauth=off

**[説明]**

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザー ID の属性を設定する。  
設定できる属性は以下のとおり。

| <i>attribute</i> | <i>value</i>                      | 説明                                       |
|------------------|-----------------------------------|------------------------------------------|
| xauth            | on                                | IPsec の XAUTH 認証にこの ID を使用する             |
|                  | off                               | IPsec の XAUTH 認証にこの ID を使用しない            |
| xauth-address    | IP address[/netmask] (IPv6 アドレス可) | IPsec の接続時に、このアドレスを内部 IP アドレスとして通知する     |
| xauth-dns        | IP address (IPv6 アドレス可)           | IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する  |
| xauth-wins       | IP address (IPv6 アドレス可)           | IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する |
| xauth-filter     | フィルタセットの名前を表す文字列                  | IPsec の接続時に、このフィルターを適用する                 |

| <i>attribute</i> | <i>value</i> | 説明                              |
|------------------|--------------|---------------------------------|
| eap-md5          | on           | IKEv2 の EAP-MD5 認証にこの ID を使用する  |
|                  | off          | IKEv2 の EAP-MD5 認証にこの ID を使用しない |

同じ属性が重複して指定されている場合はコマンドエラーとなる。

#### [ノート]

本コマンドにて明示的に設定した属性値は、該当のユーザー ID が属しているユーザーグループに対して、**auth user group attribute** コマンドによって設定された属性値に優先して適用される。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.33 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの設定

#### [書式]

**auth user group** *groupid* *userid* [*userid* ...]

**no auth user group** *groupid*

#### [設定値及び初期値]

- *groupid*
  - [設定値]: ユーザーグループ識別番号 (1..1000)
  - [初期値]: -
- *userid*
  - [設定値]: ユーザー識別番号もしくはユーザー識別番号の範囲 (複数指定することが可能)
  - [初期値]: -

#### [説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザーグループを設定する。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [設定例]

```
# auth user group 1 100 101 102
# auth user group 1 200-300
# auth user group 1 100 103 105 107-110 113
```

#### [適用モデル]

NVR700W, NVR510

## 13.34 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの属性の設定

#### [書式]

**auth user group attribute** *groupid* *attribute=value* [*attribute=value* ...]

**no auth user group attribute** *groupid* [*attribute=value* ...]

#### [設定値及び初期値]

- *groupid*
  - [設定値]: ユーザー識別番号 (1..1000)
  - [初期値]: -
- *attribute=value*
  - [設定値]: ユーザー属性
  - [初期値]: xauth=off

## [説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザーグループの属性を設定する。設定できる属性は以下のとおり。

| <i>attribute</i>   | <i>value</i>            | 説明                                                |
|--------------------|-------------------------|---------------------------------------------------|
| xauth              | on                      | IPsec の XAUTH 認証にこのグループに含まれるユーザー ID を使用する         |
|                    | off                     | IPsec の XAUTH 認証にこのグループに含まれるユーザー ID を使用しない        |
| xauth-address-pool | IP アドレスの範囲 (IPv6 アドレス可) | IPsec の接続時に、このアドレスプールからアドレスを選択し、内部 IP アドレスとして通知する |
| xauth-dns          | IP address (IPv6 アドレス可) | IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する           |
| xauth-wins         | IP address (IPv6 アドレス可) | IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する          |
| xauth-filter       | フィルタセットの名前を表す文字列        | IPsec の接続時に、このフィルターを適用する                          |
| eap-md5            | on                      | IKEv2 の EAP-MD5 認証にこの ID を使用する                    |
|                    | off                     | IKEv2 の EAP-MD5 認証にこの ID を使用しない                   |

xauth-address-pool の属性値である IP アドレスの範囲は、以下のいずれかの書式にて記述する。

- IP address[/netmask]
- IP address-IP address[/netmask]

同じ属性が重複して指定されている場合はコマンドエラーとなる。

## [ノート]

本コマンドで設定した属性値は、該当のユーザーグループに含まれるすべてのユーザーに対して有効となる。

NVR510 は Rev.15.01.03 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 13.35 XAUTH によるユーザー認証の設定

## [書式]

```
ipsec ike xauth request gateway_id auth [group_id]
no ipsec ike xauth request gateway_id [auth ...]
```

## [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *group\_id*
  - [設定値]: 認証に使用するユーザーグループの識別番号
  - [初期値]: -
- *auth*
  - [設定値]:



| 設定値 | 説明    |
|-----|-------|
| on  | 要求する  |
| off | 要求しない |

- [初期値]: off

#### [説明]

IPsec の認証を行う際、Phase1 終了後に XAUTH によるユーザー認証をクライアントに要求するか否かを設定する。  
*group\_id* を指定した場合には、該当のユーザーグループに含まれるユーザーを認証の対象とする。  
*group\_id* の指定がない場合や、指定したユーザーグループに含まれるユーザー情報では認証できなかった場合、RADIUS サーバーの設定があれば RADIUS サーバーを用いた認証を追加で試みる。

#### [ノート]

本コマンドによる設定はルーターが受動側として動作する時にのみ有効であり、始動側のセキュリティー・ゲートウェイから送信された *isakmp SA* パラメーターの提案に、認証方式として XAUTHInitPreShared (65001) が含まれていた場合に、この提案を受け入れ、XAUTH によるユーザー認証を行う。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.36 内部 IP アドレスプールの設定

#### [書式]

```
ipsec ike mode-cfg address pool pool_id ip_address[/mask]  

ipsec ike mode-cfg address pool pool_id ip_address-ip_address[/mask]  

no ipsec ike mode-cfg address pool pool_id [ip_address ...]
```

#### [設定値及び初期値]

- *pool\_id*
  - [設定値]: アドレスプール ID (1..65535)
  - [初期値]: -
- *ip\_address*
  - [設定値]: IP アドレス (IPv6 アドレス可)
  - [初期値]: -
- *ip\_address-ip\_address*
  - [設定値]: IP アドレスの範囲 (IPv6 アドレス可)
  - [初期値]: -
- *mask*
  - [設定値]: ネットマスク (IPv6 アドレスの時はプレフィックス長)
  - [初期値]: -

#### [説明]

IPsec クライアントに割り当てる内部 IP アドレスのアドレスプールを設定する。  
 本コマンドにて設定したアドレスプールは、**ipsec ike mode-cfg address gateway\_id ...** コマンドにて用いられる。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.37 IKE XAUTH Mode-Cfg メソッドの設定

### [書式]

```
ipsec ike mode-cfg method gateway_id method [option]
no ipsec ike mode-cfg method gateway_id [method ...]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *method*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| set | SET メソッド |

- [初期値]: set
- *option*

- [設定値]:

| 設定値      | 説明             |
|----------|----------------|
| openswan | Openswan 互換モード |

- [初期値]: -

### [説明]

IKE XAUTH の Mode-Cfg でのアドレス割り当てメソッドを設定する。指定できるのは SET メソッドのみである。  
*option* に 'openswan' を指定した場合には Openswan 互換モードとなり、Openswan と接続できるようになる。

### [ノート]

ダイヤルアップ VPN の発呼側にヤマハルーターおよび YMS-VPN1 を利用するときに、*option* を指定していると XAUTH では接続できない。

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 13.38 IPsec クライアントに割り当てる内部 IP アドレスプールの設定

### [書式]

```
ipsec ike mode-cfg address gateway_id pool_id
no ipsec ike mode-cfg address gateway_id [pool_id]
```

### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *pool\_id*
  - [設定値]: アドレスプール ID
  - [初期値]: -

### [説明]

IPsec クライアントに内部 IP アドレスを割り当てる際に参照する、内部 IP アドレスプールを設定する。  
内部 IP アドレスの IPsec クライアントへの通知は、XAUTH 認証に使用する Config-Mode にて行われるため、XAUTH 認証を行わない場合には通知は行われない。

以下のいずれかの方法にて、認証ユーザー毎に割り当てる内部 IP アドレスが設定されている場合には、アドレスプールからではなく、個別に設定されているアドレスを通知する。

- RADIUS サーバーに登録されている場合
- 以下のコマンドを用いて設定されている場合
  - **auth user attribute** *userid* xauth-address=*address*[/*mask*]
  - **auth user group attribute** *groupid* xauth-address-pool=*address-address*[/*mask*]

アドレスプールに登録されているアドレスが枯渇した場合には、アドレスの割当を行わない。

[ノート]

VPN クライアントとして YMS-VPN1 を用いる場合、XAUTH 認証を行うためには必ず内部 IP アドレスの通知を行う設定にしなければならない。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.39 IKE のログの種類の設定

[書式]

```
ipsec ike log [gateway_id] type [type]
no ipsec ike log [gateway_id] [type]
```

[設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値          | 説明           |
|--------------|--------------|
| message-info | IKE メッセージの内容 |
| payload-info | ペイロードの処理内容   |
| key-info     | 鍵計算の処理内容     |

- [初期値]: -

[説明]

出力するログの種類を設定する。ログはすべて、debug レベルの SYSLOG で出力される。

IKEv2 に対応した機種では、*gateway\_id* パラメーターを省略することができる。*gateway\_id* パラメーターを省略した設定は、応答側として働く際、セキュリティー・ゲートウェイが特定できない時点での通信に対して適用される。

[ノート]

このコマンドが設定されていない場合には、最小限のログしか出力しない。複数の *type* パラメーターを設定することもできる。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.40 ESP を UDP でカプセル化して送受信するか否かの設定

[書式]

```
ipsec ike esp-encapsulation gateway_id encap
no ipsec ike esp-encapsulation gateway_id
```

[設定値及び初期値]

- *gateway\_id*

- [設定値]: セキュリティー・ゲートウェイの識別子
- [初期値]: -
- *encap*
- [設定値]:

| 設定値 | 説明                       |
|-----|--------------------------|
| on  | ESP を UDP でカプセル化して送信する   |
| off | ESP を UDP でカプセル化しないで送信する |

- [初期値]: off

#### [説明]

NAT などの影響で ESP が通過できない環境で IPsec の通信を確立するために、ESP を UDP でカプセル化して送受信できるようにする。このコマンドの設定は双方のルーターで一致させる必要がある。

#### [ノート]

**ipsec ike nat-traversal** コマンドとの併用はできない。

本コマンドは IKEv2 により確立された SA を伴う IPsec 通信には影響を与えない。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 13.41 折衝パラメーターを制限するか否かの設定

#### [書式]

```
ipsec ike proposal-limitation gateway_id switch
```

```
no ipsec ike proposal-limitation gateway_id [switch]
```

#### [設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | 折衝パラメーターを制限する  |
| off | 折衝パラメーターを制限しない |

- [初期値]: off

#### [説明]

IKEv2 で鍵交換を開始するとき、SA を構築するための各折衝パラメーターを、特定のコマンド設定値に限定して提案するか否かを設定する。このコマンドの設定が off のときは、サポート可能な折衝パラメーター全てを提案する。

このコマンドが適用されるパラメーターと対応するコマンドは以下の通りである。

| パラメーター      | コマンド                                  |
|-------------|---------------------------------------|
| 暗号アルゴリズム    | <b>ipsec ike encryption</b>           |
| グループ        | <b>ipsec ike group</b>                |
| ハッシュアルゴリズム  | <b>ipsec ike hash</b>                 |
| 暗号・認証アルゴリズム | <b>ipsec sa policy</b> ※ CHILD SA 作成時 |

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]  
NVR700W

### 13.42 IKE のメッセージ ID 管理の設定

[書式]

```
ipsec ike message-id-control gateway_id switch
no ipsec ike message-id-control gateway_id [switch]
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- switch
  - [設定値]:

| 設定値 | 説明                            |
|-----|-------------------------------|
| on  | リクエストメッセージの送信をメッセージ ID で管理する  |
| off | リクエストメッセージの送信をメッセージ ID で管理しない |

- [初期値]: off

[説明]

自機から IKEv2 のリクエストメッセージを送信するときのメッセージ ID 管理方法を設定する。  
on に設定しているとき、同じ IKE SA を使用して送信済みの IKE メッセージに対する全てのレスポンスメッセージを受信していない場合、新しい IKE メッセージは送信しない。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]  
NVR700W

### 13.43 CHILD SA 作成方法の設定

[書式]

```
ipsec ike child-exchange type gateway_id type
no ipsec ike child-exchange type gateway_id [type]
```

[設定値及び初期値]

- gateway\_id
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- type: IKEv2 の CHILD SA 作成方法のタイプ
  - [設定値]:

| 設定値 | 説明                              |
|-----|---------------------------------|
| 1   | ヤマハルーターの IKEv2 の従来の動作との互換性を保持する |
| 2   | CREATE_CHILD_SA 交換を一部の実装にあわせる   |

- [初期値]: 1

**[説明]**

IKEv2 の CHILD SA 作成方法を設定する。  
このコマンドに対応する機種同士で接続する場合、*type* を同じ設定にして接続する必要がある。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

**[適用モデル]**

NVR700W

## 13.44 鍵交換の始動パケットを受信するか否かの設定

---

**[書式]**

```
ipsec ike negotiation receive gateway_id switch
no ipsec ike negotiation receive gateway_id [switch]
```

**[設定値及び初期値]**

- *gateway\_id*
  - [設定値]: セキュリティ・ゲートウェイの識別子
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | 鍵交換の始動パケットを受信する  |
| off | 鍵交換の始動パケットを受信しない |

- [初期値]: on

**[説明]**

IKEv2 で、鍵交換の始動パケットを受信するか否かを設定する。  
受信しないに設定した場合は、結果として受動側としては動作せず、必ず始動側として動作するようになる。

**[ノート]**

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。  
off にする場合には、*ipsec ike remote address* または *ipsec ike remote name* を IP アドレスで設定しておく必要がある。  
NVR700W Rev.15.00.14 以降で使用可能。

**[適用モデル]**

NVR700W

## 13.45 SA 関連の設定

---

再起動されるとすべての SA がクリアされることに注意しなくてはならない。

### 13.45.1 SA の寿命の設定

---

**[書式]**

```
ipsec ike duration sa gateway_id second [kbytes] [rekey rekey] [forced-reduction=del_time]
no ipsec ike duration sa gateway_id [second [kbytes] [rekey rekey] [forced-reduction=del_time]]
```

**[設定値及び初期値]**

- *sa*
  - [設定値]:

| 設定値                      | 説明                  |
|--------------------------|---------------------|
| ipsec-sa (もしくは child-sa) | IPsec SA (CHILD SA) |
| isakmp-sa (もしくは ike-sa)  | ISAKMP SA (IKE SA)  |

- [初期値]: -
- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *second*
  - [設定値]: 秒数 (300..691200)
  - [初期値]: 28800 秒
- *kbytes*
  - [設定値]:

| 設定値             | 説明                                                           |
|-----------------|--------------------------------------------------------------|
| 100..2147483647 | キロ単位のバイト数 (NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降)   |
| 100..100000     | キロ単位のバイト数 (上記以外)                                             |
| off             | バイト寿命を設定しない (NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降) |

- [初期値]:
  - 2000000 (NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降)
  - -(上記以外)
- *rekey*: SA を更新するタイミング
  - [設定値]:

| 設定値     | 説明                                                                 |
|---------|--------------------------------------------------------------------|
| 70%-90% | パーセント                                                              |
| off     | 更新しない ( <i>sa</i> パラメーターで <i>isakmp-sa (ike-sa)</i> を指定したときのみ設定可能) |

- [初期値]: 75%
- *del\_time*
  - [設定値]: 古くなった SA の寿命を強制的に短縮する時間(1..691200)
  - [初期値]: -

**[説明]**

各 SA の寿命を設定する。

*kbytes* パラメーターを指定した場合には、*second* パラメーターで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。*kbytes* パラメーターは *sa* パラメーターとして *ipsec-sa (child-sa)* を指定したときのみ有効である。SA の更新は *kbytes* パラメーターに設定したバイト数の 75% を処理したタイミングで行われる。また、IPsec SA (CHILD SA) が更新されたとき、古くなった既存の IPsec SA (CHILD SA) の寿命が 30 秒以上である場合は、寿命が 30 秒に短縮される。

*rekey* パラメーターは SA を更新するタイミングを決定する。例えば、*second* パラメーターで 20000 を指定し、*rekey* パラメーターで 75% を指定した場合には、SA を生成してから 15000 秒経過したときに新しい SA を生成する。*rekey* パラメーターは *second* パラメーターに対する比率を表すもので、*kbytes* パラメーターの値とは関係がない。

*sa* パラメーターで *isakmp-sa (ike-sa)* を指定したときに限り、*rekey* パラメーターで 'off' を設定できる。このとき、IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作する IKE のバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1

始動側として働く場合に、このコマンドで設定した寿命値が提案される。応答側として働く場合は、このコマンドの設定に関係なく相手側から提案された寿命値に合わせる。

また、ISAKMP SA に対する *rekey* パラメーターを off に設定した場合、その効果を得るためには、次の 2 点に注意して設定する必要がある。

1. IPsec SA よりも ISAKMP SA の寿命を短く設定する。
2. ダングリング SA を許可する。すなわち、**ipsec ike restrict-dangling-sa** コマンドの設定を off にする。

NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降が始動側になる場合は、最大で 2147483647 KB のバイト寿命値を相手側へ提案可能であるが、相手側機器が NVR700W Rev.15.00.24 以降および、NVR510 Rev.15.01.25 以降、RTX830 Rev.15.02.27 以降、RTX1300、vRX Amazon EC2 版、vRX VMware ESXi 版以外の場合は 2 GB を超えるバイト寿命値を正しく認識できないため、NVR700W Rev.15.00.24 以降および、NVR510 Rev.15.01.25 以降、RTX830 Rev.15.02.27 以降、RTX1300、vRX Amazon EC2 版、vRX VMware ESXi 版以外の機種と接続する場合は必ず 2 GB 以下に設定する必要がある。

- IKEv2

IKEv2 では SA 寿命値は折衝されず、各セキュリティー・ゲートウェイが独立して管理するものとなっている。従って、確立された SA には、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティー・ゲートウェイの方が SA 更新のタイミングが早ければ、SA はその分早く更新されることになる。

forced-reduction オプションに時間を指定すると、SA を更新した際に古くなった既存の SA の寿命を強制的に設定値に変更し、消滅までの時間を早めることができる。ただし、IPsec SA (CHILD SA) で *kbytes* パラメーターにバイト寿命値を指定している場合は、*del\_time* パラメーターで 31 秒以上の値を設定していても、短縮される値は 30 秒となる。また、IKEv1 では寿命が設定値よりも短い場合は変更しない。

ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在する SA の寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

forced-reduction オプションは以下の機種およびリビジョンで使用可能。

NVR700W は Rev.15.00.24 以降。

NVR510 は Rev.15.01.25 以降。

#### [適用モデル]

NVR700W, NVR510

## 13.45.2 SA のポリシーの定義

### [書式]

```
ipsec sa policy policy_id gateway_id ah [ah_algorithm] [local-id=local-id] [remote-id=remote-id] [anti-replay-check=check]
```

```
ipsec sa policy policy_id gateway_id esp [esp_algorithm] [ah_algorithm] [anti-replay-check=check]
```

```
no ipsec sa policy policy_id [gateway_id]
```

### [設定値及び初期値]

- *policy\_id*
  - [設定値]: ポリシー ID (1..2147483647)
  - [初期値]: -
- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *ah*: 認証ヘッダ (Authentication Header) プロトコルを示すキーワード
  - [初期値]: -
- *esp*: 暗号ペイロード (Encapsulating Security Payload) プロトコルを示すキーワード
  - [初期値]: -



- *ah\_algorithm* : 認証アルゴリズム

- [設定値] :

| 設定値         | 説明            |
|-------------|---------------|
| md5-hmac    | HMAC-MD5      |
| sha-hmac    | HMAC-SHA      |
| sha256-hmac | HMAC-SHA2-256 |

- [初期値] :

- sha-hmac ( AH プロトコルの場合 )
- - ( ESP プロトコルの場合 )

- *esp\_algorithm* : 暗号アルゴリズム

- [設定値] :

| 設定値        | 説明         |
|------------|------------|
| 3des-cbc   | 3DES-CBC   |
| des-cbc    | DES-CBC    |
| aes-cbc    | AES128-CBC |
| aes256-cbc | AES256-CBC |

- [初期値] : aes-cbc

- *local-id*

- [設定値] : 自分側のプライベートネットワーク
- [初期値] : -

- *remote-id*

- [設定値] : 相手側のプライベートネットワーク
- [初期値] : -

- *check*

- [設定値] :

| 設定値 | 説明                |
|-----|-------------------|
| on  | シーケンス番号のチェックを行う   |
| off | シーケンス番号のチェックを行わない |

- [初期値] : on

**[説明]**

SA のポリシーを定義する。この定義はトンネルモードおよびトランスポートモードの設定に必要である。この定義は複数のトンネルモードおよびトランスポートモードで使用できる。

*local-id*、*remote-id* には、カプセル化したいパケットの始点／終点アドレスの範囲をネットワークアドレスで記述する。これにより、1つのセキュリティー・ゲートウェイに対して、複数の IPsec SA を生成し、IP パケットの内容に応じて SA を使い分けることができるようになる。

*check=on* の場合、受信パケット毎にシーケンス番号の重複や番号順のチェックを行い、エラーとなるパケットは破棄する。破棄する際には *debug* レベルで

```
[IPSEC] sequence difference
[IPSEC] sequence number is wrong
```

といったログが記録される。

相手側が、トンネルインターフェースでの優先/帯域制御を行っている場合、シーケンス番号の順序が入れ替わってパケットを受信することがある。その場合、実際にはエラーではないのに上のログが表示され、パケットが破棄されることがあるので、そのような場合には設定を *off* にするとよい。

IKEv2 では、*ipsec ike proposal-limitation* コマンドが *on* に設定されているとき、本コマンドの *ah\_algorithm*、および *esp\_algorithm* パラメーターで設定されたアルゴリズムを提案する。*ipsec ike proposal-limitation* コマンドが *off* に設定されているときは、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズムを同時に提案し、相手

側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は受け取った提案から以下の優先順位でアルゴリズムを選択する。

- 認証アルゴリズム

HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

- 暗号アルゴリズム

AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

※IKEv2 でのみ AES192-CBC をサポートする。ただし、コマンドで AES192-CBC を選択することはできない。また、IKEv2 では *local-id*、*remote-id* パラメーターに関しても効力を持たない。

[ノート]

双方で設定する *local-id* と *remote-id* は一致している必要がある。

NVR510 は Rev.15.01.03 以降で使用可能。

[設定例]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

[適用モデル]

NVR700W, NVR510

### 13.45.3 SA の手動更新

[書式]

**ipsec refresh sa**

[説明]

SA を手動で更新する。

[ノート]

管理されている SA をすべて削除して、IKE の状態を初期化する。

このコマンドでは、SA の削除を相手に通知しないので、通常の運用では **ipsec sa delete all** コマンドの方が望ましい。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.45.4 ダングリング SA の動作の設定

[書式]

**ipsec ike restrict-dangling-sa gateway\_id action**

**no ipsec ike restrict-dangling-sa gateway\_id [action]**

[設定値及び初期値]

- *gateway\_id*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *action*
  - [設定値]:

| 設定値  | 説明                                        |
|------|-------------------------------------------|
| auto | アグレッシブモードの始動側でのみ IKE SA と IPsec SA を同期させる |
| off  | IKE SA と IPsec SA を同期させない。                |

- [初期値]: auto

**[説明]**

このコマンドは IKEv1 のダングリング SA の動作に制限を設ける。

ダングリング SA とは、IKE SA を削除するときに対応する IPsec SA を削除せずに残したときの状態を指す。基本的にはダングリング SA を許す方針で実装しており、IKE SA と IPsec SA を独立のタイミングで削除する。

auto を設定したときには、アグレッシブモードの始動側でダングリング SA を排除し、IKE SA と IPsec SA を同期して削除する。この動作は IKE keepalive が正常に動作するために必要な処置である。

off を設定したときには、常にダングリング SA を許す動作となり、IKE SA と IPsec SA を独立なタイミングで削除する。

ダイヤルアップ VPN のクライアント側ではない場合には、このコマンドの設定に関わらず常に IKE SA と IPsec SA は独立に管理され、削除のタイミングは必ずしも同期しない。

**[ノート]**

ダングリング SA の強制削除が行われても、通常は新しい IKE SA に基づいた新しい IPsec SA が存在するので通信に支障が出ることはない。

ダイヤルアップ VPN のクライアント側では、このコマンドにより動作を変更でき、それ以外では、ダングリング SA が発生しても何もせず通信を続ける。

ダイヤルアップ VPN のクライアント側でダングリング SA を許さないのは、IKE キープアライブを正しく機能させるために必要なことである。

IKE キープアライブでは、IKE SA に基づいてキープアライブを行う。ダングリング SA が発生した場合には、その SA についてはキープアライブを行う IKE SA が存在せず、キープアライブ動作が行えない。そのため、IKE キープアライブを有効に動作させるにはダングリング SA が発生したら強制的に削除して、通信は対応する IKESA が存在する IPsec SA で行われるようにしなくてはならない。

本コマンドは IKEv2 の動作には影響を与えない。IKEv2 では仕様として、ダングリング SA の存在を禁止している。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**13.45.5 IPsec NAT トラバーサルを利用するための設定**

**[書式]**

`ipsec ike nat-traversal gateway switch [keepalive=interval] [force=force_switch] [type=type]`

`no ipsec ike nat-traversal gateway [switch ...]`

**[設定値及び初期値]**

- *gateway*
  - [設定値]: セキュリティー・ゲートウェイの識別子
  - [初期値]: -
- *switch*: 動作の有無
  - [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | NAT トラバーサルの動作を有効にする |
| off | NAT トラバーサルの動作を無効にする |

- [初期値]: off
- *interval*: NAT キープアライブの送信間隔
  - [設定値]:

| 設定値       | 説明    |
|-----------|-------|
| off       | 送信しない |
| 30-100000 | 時間[秒] |

- [初期値]: 300
- *force\_switch*
- [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| on  | 通信経路上に NAT がなくても NAT トラバーサルを使用する  |
| off | 通信経路上に NAT がなければ NAT トラバーサルを使用しない |

- [初期値]: off
- *type*
- [設定値]:

| 設定値 | 説明                                 |
|-----|------------------------------------|
| 1   | ヤマハルーターの従来動作との互換性を保持する             |
| 2   | NAT トラバーサル使用時に交換するペイロードを一部の実装に合わせる |

- [初期値]: 1

#### [説明]

NAT トラバーサルの動作を設定する。この設定があるときには、IKE で NAT トラバーサルの交渉を行う。相手が NAT トラバーサルに対応していないときや、通信経路上に NAT の処理がないときには、NAT トラバーサルを使用せず、ESP パケットを使って通信する。対向のルーターや端末でも NAT トラバーサルの設定が必要である。いずれか一方にしか設定がないときには、NAT トラバーサルを使用せず、ESP パケットを使って通信する。

*type* に対応した機種同士で接続する場合、*type* を同じ設定にして接続する必要がある。また、*type* に 2 を指定した場合、*type* に対応していない機種との接続はできない。

IKEv2 では、イニシエータとして動作する場合のみ *switch* パラメーターが影響する。このオプションは、通信経路上に NAT 処理がなくても NAT トラバーサル動作が必要な対向機器と接続する場合に使用する。なお、通常は 'off' にしておくことが望ましい。

#### [ノート]

**ipsec ike esp-encapsulation** コマンドとの併用はできない。

また、IPComp が設定されているトンネルインターフェースでは利用できない。

IKEv1 では、メインモードおよび、アグレッシブモードの ESP トンネルでのみ利用できる。AH では利用できず、トランスポートモードでも利用できない。

ただし、L2TP/IPsec と L2TPv3 を用いた L2VPN で使用される IKEv1 では、メインモードかつトランスポートモードの ESP トンネルでも利用できる。

IKEv2 では、ESP トンネルを確立する場合のみ利用できる。AH では利用できず、トランスポートモードでも利用できない。

IKEv1 メインモードでの NAT トラバーサルは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアで利用できる。

*type* オプションは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアで使用できる。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 13.45.6 SA の削除

#### [書式]

**ipsec sa delete id**

[設定値及び初期値]

- *id*
  - [設定値]:

| 設定値 | 説明      |
|-----|---------|
| 番号  | SA の ID |
| all | すべての SA |

- [初期値]: -

[説明]

指定した SA を削除する。  
SA の ID は自動的に付与され、**show ipsec sa** コマンドで確認することができる。

[ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

## 13.46 トンネルインターフェース関連の設定

### 13.46.1 IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定

[書式]

**ipsec tunnel fastpath-fragment-function follow df-bit *switch***  
**no ipsec tunnel fastpath-fragment-function follow df-bit [*switch*]**

[設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                                                           |
|-----|--------------------------------------------------------------|
| on  | ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに従ってフラグメントするかを決定する |
| off | ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに関係なくフラグメントする      |

- [初期値]: off

[説明]

ESP パケットをフラグメントする必要がある場合に、DF ビットに従ってフラグメントするか否かを設定する。**ipsec tunnel outer df-bit** コマンドによって DF ビットがセットされた ESP パケットであっても本コマンドで **off** が設定されている場合はフラグメントされる。本コマンドは、トンネルインターフェースに対して設定し、ファストパスで処理される ESP パケットのみを対象とする。

[ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 13.46.2 IPsec トンネルの外側の IPv4 パケットに対する DF ビットの制御の設定

#### [書式]

```
ipsec tunnel outer df-bit mode
no ipsec tunnel outer df-bit [mode]
```

#### [設定値及び初期値]

- *mode*
- [設定値]:

| 設定値   | 説明                              |
|-------|---------------------------------|
| copy  | 内側の IPv4 パケットの DF ビットを外側にもコピーする |
| set   | 常に 1                            |
| clear | 常に 0                            |

- [初期値]: copy

#### [説明]

IPsec トンネルの外側の IPv4 パケットで、DF ビットをどのように設定するかを制御する。

copy の場合には、内側の IPv4 パケットの DF ビットをそのまま外側にもコピーする。

set または clear の場合には、内側の IPv4 パケットの DF ビットに関わらず、外側の IPv4 パケットの DF ビットはそれぞれ 1、または 0 に設定される。

トンネルインターフェース毎のコマンドである。

#### [ノート]

トンネルインターフェースの MTU と実インターフェースの MTU の値の大小関係により、IPsec 化されたパケットをフラグメントしなくてはいけない時には、このコマンドの設定に関わらず DF ビットは 0 になる。

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 13.46.3 使用する SA のポリシーの設定

#### [書式]

```
ipsec tunnel policy_id
no ipsec tunnel [policy_id]
```

#### [設定値及び初期値]

- *policy\_id*
- [設定値]: 整数 (1..2147483647)
- [初期値]: -

#### [説明]

選択されているトンネルインターフェースで使用する SA のポリシーを設定する。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 13.46.4 IPComp によるデータ圧縮の設定

#### [書式]

```
ipsec ipcomp type type
```

**no ipsec ipcomp type** [*type*]

[設定値及び初期値]

- *type*
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| deflate | deflate 圧縮でデータを圧縮する |
| none    | データ圧縮を行わない          |

- [初期値]: none

[説明]

IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信した場合には、設定に関係なく展開する。必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側にのみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。トランスポートモードのみを使用する場合には、IPComp を使用することはできない。

[ノート]

データ圧縮には、PPP で使われる CCP や、フレームリレーで使われる FRF.9 もある。圧縮アルゴリズムとして、IPComp で使われる deflate と、CCP/FRF.9 で使われる Stac-LZS との間に基本的な違いはない。しかし、CCP/FRF.9 でのデータ圧縮は IPsec による暗号化の後に行われる。このため、暗号化でランダムになったデータを圧縮しようとすることになり、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果を得られる。また、CCP/FRF.9 とは異なり、対向のセキュリティ・ゲートウェイまでの全経路で圧縮されたままのデータが流れるため、例えば本機の出カインターフェースが LAN であってもデータ圧縮効果を期待できる。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

## 13.46.5 トンネルバックアップの設定

[書式]

```
tunnel backup none
tunnel backup interface ip_address
tunnel backup pp peer_num [switch-router=switch1]
tunnel backup tunnel tunnel_num [switch-interface=switch2]
no tunnel backup
```

[設定値及び初期値]

- none: トンネルバックアップを使用しない
  - [初期値]: none
- interface
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- ip\_address
  - [設定値]: バックアップ先のゲートウェイの IP アドレス
  - [初期値]: -
- peer\_num
  - [設定値]: バックアップ先の相手先情報番号
  - [初期値]: -
- tunnel\_num
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

- `switch1` : バックアップの受け側のルーターを 2 台に分けるか否か

[設定値] :

| 設定値 | 説明   |
|-----|------|
| on  | 分ける  |
| off | 分けない |

[初期値] : off

- `switch2` : LAN/PP インターフェースのバックアップにしたがってトンネルを作り直すか否か

[設定値] :

| 設定値 | 説明     |
|-----|--------|
| on  | 作り直す   |
| off | 作り直さない |

[初期値] : on

#### [説明]

トンネルインターフェースに障害が発生したときにバックアップとして利用するインターフェースを指定する。

`switch-router` オプションについては、以下の 2 つの条件を満たすときに `on` を設定する。

- バックアップの受け側に 2 台のルーターがあり、一方がバックアップ元の回線に接続し、もう一方がバックアップ先の回線に接続している。
- バックアップ先の回線に接続しているルーターのファームウェアがこのリビジョンよりも古い。

#### [適用モデル]

NVR700W

## 13.46.6 トンネルテンプレートの設定

#### [書式]

`tunnel template tunnel [tunnel ...]`

`no tunnel template`

#### [設定値及び初期値]

• `tunnel`

- [設定値] : トンネルインターフェース番号、または間にハイフン (-) をはさんでトンネルインターフェース番号を範囲指定したもの
- [初期値] : -

#### [説明]

`tunnel select` コマンドにて選択されたトンネルインターフェースを展開元として、当該インターフェースに設定されているコマンドの展開先となるトンネルインターフェースを設定する。

展開元のトンネルインターフェースに設定することで、展開先のトンネルインターフェースにも適用されるコマンドは以下のとおりである。

- `ipsec tunnel`
- `ipsec sa policy`
- `ipsec ike` で始まるコマンドのうち、パラメーターにセキュリティー・ゲートウェイの識別子をとるもの
- `ipsec auto refresh` (引数にセキュリティー・ゲートウェイの識別子を指定する場合)
- `tunnel encapsulation`
- `tunnel ngn arrive permit`
- `tunnel ngn bandwidth`
- `tunnel ngn disconnect time`
- `tunnel ngn radius auth`
- `l2tp` で始まるコマンド
- `tunnel enable`

上記コマンドのうち以下のコマンドについては、特定のパラメーターの値が展開元のトンネルインターフェース番号に一致する場合のみ、コマンドが展開される。その場合、当該パラメーターの値は展開先のトンネルインターフェース番号に置換される。



| コマンド                      | パラメーター             |
|---------------------------|--------------------|
| <b>ipsec tunnel</b>       | ポリシー ID            |
| <b>ipsec sa policy</b>    | ポリシー ID            |
| <b>ipsec ike</b> で始まるコマンド | セキュリティー・ゲートウェイの識別子 |
| <b>ipsec auto refresh</b> | セキュリティー・ゲートウェイの識別子 |
| <b>tunnel enable</b>      | トンネルインターフェース番号     |

**ipsec sa policy** コマンドでは、セキュリティー・ゲートウェイの識別子が展開先のトンネルインターフェース番号に置換される。

**ipsec ike remote name** コマンドでは、相手側セキュリティー・ゲートウェイの名前の末尾に展開先のトンネルインターフェース番号が付加される。

展開元のトンネルインターフェースに設定されているコマンドと同じコマンドが、展開先のトンネルインターフェースに既に設定されている場合、展開先のトンネルインターフェースに設定されているコマンドが優先される。

コマンド展開後の、ルーターの動作時に参照される設定は **show config tunnel** コマンドに **expand** キーワードを指定することで確認できる。

### [ノート]

トンネルインターフェースが選択されている時のみ使用できる。

NVR510 は Rev.15.01.03 以降で使用可能。

### [設定例]

展開先のトンネルインターフェースとして、番号の指定と範囲の指定を同時に記述することができる。

```
tunnel select 1
  tunnel template 8 10-20
tunnel select 2
  tunnel template 100 200-300 400
```

以下の 2 つの設定は同じ内容を示している。

```
tunnel select 1
  tunnel template 2
    ipsec tunnel 1
    ipsec sa policy 1 1 esp aes-cbc sha-hmac
    ipsec ike encryption 1 aes-cbc
    ipsec ike group 1 modp1024
    ipsec ike local address 1 192.168.0.1
    ipsec ike pre-shared-key 1 text himitsu1
    ipsec ike remote address 1 any
    ipsec ike remote name 1 pc
  tunnel enable 1
tunnel select 2
  ipsec ike pre-shared-key 2 text himitsu2
```

```
tunnel select 1
  ipsec tunnel 1
    ipsec sa policy 1 1 esp aes-cbc sha-hmac
    ipsec ike encryption 1 aes-cbc
    ipsec ike group 1 modp1024
    ipsec ike local address 1 192.168.0.1
    ipsec ike pre-shared-key 1 text himitsu1
    ipsec ike remote address 1 any
    ipsec ike remote name 1 pc
  tunnel enable 1
tunnel select 2
  ipsec tunnel 2
    ipsec sa policy 2 2 esp aes-cbc sha-hmac
    ipsec ike encryption 2 aes-cbc
    ipsec ike group 2 modp1024
    ipsec ike local address 2 192.168.0.1
    ipsec ike pre-shared-key 2 text himitsu2
    ipsec ike remote address 2 any
```

```
ipsec ike remote name 2 pc2
tunnel enable 2
```

## [適用モデル]

NVR700W, NVR510

## 13.47 トランスポートモード関連の設定

### 13.47.1 トランスポートモードの定義

## [書式]

```
ipsec transport id policy_id [proto [src_port_list [dst_port_list]]]
no ipsec transport id [policy_id [proto [src_port_list [dst_port_list]]]]
```

## [設定値及び初期値]

- *id*
  - [設定値]: トランスポート ID (1..2147483647)
  - [初期値]: -
- *policy\_id*
  - [設定値]: ポリシー ID (1..2147483647)
  - [初期値]: -
- *proto*
  - [設定値]: プロトコル
  - [初期値]: -
- *src\_port\_list*: UDP、TCP のソースポート番号列
  - [設定値]:
    - ポート番号を表す十進数
    - ポート番号を表すニーモニック
    - \*(すべてのポート)
  - [初期値]: -
- *dst\_port\_list*: UDP、TCP のデスティネーションポート番号列
  - [設定値]:
    - ポート番号を表す十進数
    - ポート番号を表すニーモニック
    - \*(すべてのポート)
  - [初期値]: -

## [説明]

トランスポートモードを定義する。

定義後、*proto*、*src\_port\_list*、*dst\_port\_list* パラメーターに合致する IP パケットに対してトランスポートモードでの通信を開始する。

## [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

## [設定例]

- TELNET のデータをトランスポートモードで通信

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
# ipsec transport 1 101 tcp * telnet
```

## [適用モデル]

NVR700W, NVR510

## 13.47.2 トランスポートモードのテンプレートの設定

---

### [書式]

```
ipsec transport template id1 id2 [id2 ...]  
no ipsec transport id1 [id2 ...]
```

### [設定値及び初期値]

- *id1*
  - [設定値]: 展開元のトランスポート ID
  - [初期値]: -
- *id2*
  - [設定値]: 展開先のトランスポート ID、または間にハイフン (-) をはさんでトランスポート ID を範囲指定したもの
  - [初期値]: -

### [説明]

指定した **ipsec transport** コマンドの設定の展開先となるトランスポート ID を設定する。展開先のポリシー ID は展開先のトランスポート ID と同じ値が設定される。

展開先のトランスポート ID に対して既に設定が存在する場合、展開先の設定が優先される。

本コマンドによって VPN 対地数まで **ipsec transport** コマンドの設定を展開することができる。VPN 対地数を超える範囲に展開することはできない。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [設定例]

展開先の設定としてトランスポート ID とトランスポート ID の範囲を同時に記述することができる。

```
ipsec transport 1 1 udp 1701 *  
ipsec transport template 1 10 20-30
```

以下の 2 つの設定は同じ内容を示している。

```
ipsec transport 1 1 udp 1701 *  
ipsec transport template 1 2 10-12
```

```
ipsec transport 1 1 udp 1701 *  
ipsec transport 2 2 udp 1701 *  
ipsec transport 10 10 udp 1701 *  
ipsec transport 11 11 udp 1701 *  
ipsec transport 12 12 udp 1701 *
```

### [適用モデル]

NVR700W, NVR510

## 13.48 PKI 関連の設定

---

### 13.48.1 証明書ファイルの設定

---

#### [書式]

```
pki certificate file cert_id file type [password]  
no pki certificate file cert_id [file ...]
```

#### [設定値及び初期値]

- *cert\_id*
  - [設定値]: 証明書ファイルの識別子 (1..8)

- [初期値]: -
- *file*
  - [設定値]: 外部メモリ、RTFS 領域内のファイルを絶対パスまたは相対パスで指定する
  - [初期値]: -
- *type*: ファイル形式
  - [設定値]:

| 設定値      | 説明                |
|----------|-------------------|
| pkcs12   | PKCS#12 形式のファイル   |
| x509-pem | X.509 PEM 形式のファイル |

- [初期値]: -
- *password*
  - [設定値]: ファイルを復号するためのパスワード (半角 64 文字以内)
  - [初期値]: -

#### [説明]

証明書ファイルを設定する。

*file* に相対パスを指定する場合、**set** コマンドの環境変数 *pwd* で指定したディレクトリからの相対パスを指定する。  
*type* に pkcs12 を指定した場合、ファイルを復号するための *password* を指定する必要がある。

#### [適用モデル]

NVR700W

## 13.48.2 CRL ファイルの設定

#### [書式]

```
pki crl file crl_id file
no pki crl file crl_id [file]
```

#### [設定値及び初期値]

- *crl\_id*
  - [設定値]: CRL ファイルの識別子 (1..8)
  - [初期値]: -
- *file*
  - [設定値]: 外部メモリ、RTFS 領域内のファイルを絶対パスまたは相対パスで指定する
  - [初期値]: -

#### [説明]

CRL ファイルを設定する。

*file* に相対パスを指定する場合、**set** コマンドの環境変数 *pwd* で指定したディレクトリからの相対パスを指定する。

#### [適用モデル]

NVR700W

## 第 14 章

### L2TP 機能の設定

#### L2TP/IPsec 機能

L2TP (Layer Two Tunneling Protocol) は、ネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。L2TP 自体は暗号化の仕組みを持ちませんが、IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を実現する L2TP/IPsec があります。ヤマハルーターは、L2TP/IPsec を用いたリモートアクセス VPN のサーバーとして動作します。スマートフォンなどに搭載されている L2TP クライアントからインターネット越しにヤマハルーター配下のプライベートネットワーク内の端末とのセキュアな通信を可能にします。

ヤマハルーターでサポートする L2TP/IPsec には以下の制限があります。

- L2TP 単体での機能は提供しません。L2TP/IPsec のみサポートします。
- リモートアクセス VPN のサーバーとして動作します。クライアントとしては動作しません。
- LAN 間接続 VPN には対応していません。
- L2TP パケットの最初の待ち受けは UDP のポート番号 1701 が使用されます。変更することはできません。
- IKEv1 にのみ対応しており、IKEv2 は使用できません。

#### L2TPv3 機能

L2TPv3 (Layer 2 Tunneling Protocol version 3) は、データリンク層(L2)での VPN 接続 (L2VPN)を実現するトンネリングプロトコルです。L2 フレームを IP パケットとしてカプセル化することでルーター間での L2 フレーム転送を可能にし、複数の拠点で同一セグメントのネットワークを構築することができます。L2TPv3 自体は暗号化の仕組みを持ちませんが、IPsec と併用することでデータの機密性や完全性を確保した VPN 接続を実現する L2TPv3/IPsec があります。ヤマハルーターでは、L2TPv3 を用いた L2VPN および L2TPv3/IPsec を用いた L2VPN を構築することができます。

ヤマハルーターでサポートする L2TPv3 には以下の制限があります。

- L2 フレームのカプセル化方式として、UDP パケットとしてカプセル化する方法(L2TPv3 over UDP)にのみ対応しています。IP プロトコル番号 115 を使用して IP パケットとしてカプセル化する方法(L2TPv3 over IP)には対応していません。
- L2TPv3 パケットの受信には UDP のポート番号 1701 が使用されます。変更することはできません。
- L2TPv3 によってトンネリングできる L2 フレームは、イーサフレームのみです。
- L2TPv3/IPsec では、IKEv1 のトランスポートモードのみ対応しています。

### 14.1 L2TP を動作させるか否かの設定

#### [書式]

```
l2tp service service [version [version]]
no l2tp service [service [version [version]]]
```

#### [設定値及び初期値]

- *service*

- [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| on  | L2TP を有効にする |
| off | L2TP を無効にする |

- [初期値]: off

- *version*

- [設定値]:

| 設定値    | 説明                          |
|--------|-----------------------------|
| l2tp   | L2TP/IPsec を有効にする           |
| l2tpv3 | L2TPv3, L2TPv3/IPsec を有効にする |

- [初期値]: -

**[説明]**

L2TP を動作させるか否かを設定する。

version によって動作する L2TP のバージョンを指定できる。version を指定しない場合には L2TPv2 と L2TPv3 の両方が動作する。

L2TP が有効になると UDP のポート番号 1701 を開き、L2TP コネクションの接続を待つ。

L2TP が無効になると UDP のポート番号 1701 を閉じ、接続中の L2TP コネクションはすべて切断される。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 14.2 L2TP トンネル認証に関する設定

---

**[書式]**

**l2tp tunnel auth** *switch* [*password*]

**no l2tp tunnel auth** [*switch* ...]

**[設定値及び初期値]**

- switch*

- [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| on  | L2TP トンネル認証を行う   |
| off | L2TP トンネル認証を行わない |

- [初期値]: off

- password*

- [設定値]: L2TP トンネル認証に用いるパスワード(32 文字以内)
- [初期値]: -

**[説明]**

L2TP トンネル認証を行うか否かを設定する。

password を省略した場合には機種名がパスワードとして使用される。

NVR700W の場合には "NVR700W" がパスワードとなる。大文字小文字の区別に注意すること。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 14.3 L2TP トンネルの切断タイマの設定

---

**[書式]**

**l2tp tunnel disconnect time** *time*

**no l2tp tunnel disconnect time** [*time*]

**[設定値及び初期値]**

- time*

- [設定値]:

| 設定値         | 説明 |
|-------------|----|
| 1..21474836 | 秒数 |

| 設定値 | 説明        |
|-----|-----------|
| off | タイマを設定しない |

- [初期値]: 60

#### [説明]

L2TP トンネルの切断タイマを設定する。

選択されている L2TP トンネルに対して、データパケット無入力・無送信時に、タイムアウトにより L2TP トンネルを切断する時間を設定する。

L2TP 制御メッセージ以外はすべてデータパケットとなるため、PPP キープアライブを使用する場合などは切断タイマによる L2TP トンネルの切断は行われない場合がある。

トンネルインターフェースにのみ設定可能です。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 14.4 L2TP キープアライブの設定

#### [書式]

**l2tp keepalive use switch** [*interval* [*count*]]

**no l2tp keepalive use** [*switch* ...]

#### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | L2TP キープアライブを使用する  |
| off | L2TP キープアライブを使用しない |

- [初期値]: on
- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
  - [初期値]: 10
- *count*
  - [設定値]: ダウン検出を判定する回数 (1..50)
  - [初期値]: 6

#### [説明]

L2TP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値の応じて L2TP の Hello メッセージによるキープアライブが動作する。

トンネルインターフェースにのみ設定可能です。

#### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 14.5 L2TP キープアライブのログ設定

### [書式]

```
l2tp keepalive log log
no l2tp keepalive log [log]
```

### [設定値及び初期値]

- *log*
- [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | L2TP キープアライブをログに出力する  |
| off | L2TP キープアライブをログに出力しない |

- [初期値]: off

### [説明]

L2TP キープアライブのログを出力するか否かを設定する。  
 ログはすべて、**debug** レベルの **SYSLOG** に出力される。  
 トンネルインターフェースにのみ設定可能です。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 14.6 L2TP の接続制御の syslog を出力するか否かの設定

### [書式]

```
l2tp syslog syslog
no l2tp syslog [syslog]
```

### [設定値及び初期値]

- *syslog*
- [設定値]:

| 設定値 | 説明                                     |
|-----|----------------------------------------|
| on  | L2TP の接続制御に関するログを <b>SYSLOG</b> に出力する  |
| off | L2TP の接続制御に関するログを <b>SYSLOG</b> に出力しない |

- [初期値]: off

### [説明]

L2TP の接続制御に関するログを **SYSLOG** に出力するか否かを設定する。  
 L2TP のキープアライブに関するログは出力されない。  
 ログはすべて、**debug** レベルの **SYSLOG** に出力される。  
 トンネルインターフェースにのみ設定可能です。

### [ノート]

NVR510 は Rev.15.01.03 以降で使用可能。

### [適用モデル]

NVR700W, NVR510



## 14.7 L2TPv3 の常時接続の設定

### [書式]

```
l2tp always-on sw
no l2tp always-on [sw]
```

### [設定値及び初期値]

- *sw*
- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 常時接続する  |
| off | 常時接続しない |

- [初期値]: on

### [説明]

L2TPv3 のコネクションを常時接続するか否かを設定する。  
トンネルインターフェースにのみ設定可能です。

[適用モデル]  
NVR700W

## 14.8 L2TP トンネルのホスト名の設定

### [書式]

```
l2tp hostname hostname
no l2tp hostname [name]
```

### [設定値及び初期値]

- *name*
- [設定値]: ホスト名 (32 文字以内)
- [初期値]: 機種名

### [説明]

接続相手に通知するホスト名を設定する。  
show status l2tp コマンドで出力される L2TP トンネル情報に表示される。  
本コマンドを設定しない場合には機種名がホスト名として使用される。  
トンネルインターフェースのみ設定可能です。

[適用モデル]  
NVR700W

## 14.9 L2TPv3 の Local Router ID の設定

### [書式]

```
l2tp local router-id ipv4_address
no l2tp local router-id [ipv4_address]
```

### [設定値及び初期値]

- *ipv4\_address*
- [設定値]: IPv4 アドレス
- [初期値]: 0.0.0.0

### [説明]

L2TPv3 の接続相手に通知する Router ID を設定する。  
接続相手の Remote Router ID と同じ IPv4 アドレスを設定します。

ルーターに設定されている IPv4 アドレスを使用する必要はない。  
トンネルインターフェースにのみ設定可能です。

[適用モデル]  
NVR700W

## 14.10 L2TPv3 の Remote Router ID の設定

---

### [書式]

```
l2tp remote router-id ipv4_address  
no l2tp remote router-id [ipv4_address]
```

### [設定値及び初期値]

- *ipv4\_address*
  - [設定値]: IPv4 アドレス
  - [初期値]: 0.0.0.0

### [説明]

L2TPv3 の接続相手の Router ID を設定する。  
接続相手の Local Router ID と同じ IPv4 アドレスを設定する。  
ルーターに設定されている IPv4 アドレスを使用する必要はない。  
トンネルインターフェースにのみ設定可能です。

[適用モデル]  
NVR700W

## 14.11 L2TPv3 の Remote End ID の設定

---

### [書式]

```
l2tp remote end-id end-id  
no l2tp remote end-id [end-id]
```

### [設定値及び初期値]

- *end-id*
  - [設定値]: 任意文字列(32 文字以内)
  - [初期値]: なし

### [説明]

L2TPv3 の Remote End ID を設定する。  
接続相手の Remote End ID と同じ文字列を設定する。  
トンネルインターフェースにのみ設定可能です。

[適用モデル]  
NVR700W

## 第 15 章

### PPTP 機能の設定

本機能を使用して PC と接続するためには、PC 側には Microsoft 社 Windows の「仮想プライベートネットワーク」が必要となります。

#### 15.1 共通の設定

`tunnel encapsulation`、`tunnel endpoint address`、`tunnel endpoint name`、`ppp ccp type` コマンドも合わせて参照のこと。

##### 15.1.1 PPTP サーバーを動作させるか否かの設定

###### [書式]

```
pptp service service
no ptp service [service]
```

###### [設定値及び初期値]

- `service`
- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | PPTP サーバーとして動作する  |
| off | PPTP サーバーとして動作しない |

- [初期値]: off

###### [説明]

PPTP サーバー機能を動作させるか否かを設定する。

###### [ノート]

off に設定すると PPTP サーバーで使う TCP のポート番号 1723 を閉じる。デフォルト off なので、PPTP サーバーを起動する場合には、`pptp service on` を設定する。

###### [適用モデル]

NVR700W, NVR510

##### 15.1.2 相手先情報番号にバインドされるトンネルインターフェースの設定

###### [書式]

```
pp bind interface [interface ...]
no pp bind [interface]
```

###### [設定値及び初期値]

- `interface`
- [設定値]:

| 設定値             | 説明                 |
|-----------------|--------------------|
| tunnelN         | TUNNEL インターフェース名   |
| tunnelN-tunnelM | TUNNEL インターフェースの範囲 |

- [初期値]: -

###### [説明]

選択されている相手先情報番号にバインドされるトンネルインターフェースを指定する。  
anonymous インターフェースに対してのみ、複数のトンネルインターフェースが指定できる。  
また、連続している複数のトンネルインターフェースの場合は、インターフェース範囲指定が可能である。

## [ノート]

PPTP または L2TP/IPsec は PP 毎に設定する。

**tunnel encapsulation** コマンドで **pptp** または **l2tp** を設定したトンネルインターフェースをバインドすることによって PPTP または L2TP/IPsec で通信することを可能にする。

なお、NVR510 では Rev.15.01.03 以降で L2TP/IPsec を使用可能。

## [適用モデル]

NVR700W, NVR510

### 15.1.3 PPTP の動作タイプの設定

---

## [書式]

**pptp service type** *type*

**no pptp service type** [*type*]

## [設定値及び初期値]

• *type*

- [設定値]:

| 設定値    | 説明          |
|--------|-------------|
| server | サーバーとして動作   |
| client | クライアントとして動作 |

- [初期値]: server

## [説明]

PPTP サーバーとして動作するか、PPTP クライアントとして動作するかを設定する。

## [ノート]

PPTP はサーバー、クライアント方式の接続で、ルーター間で接続する場合には必ず一方がサーバーで、もう一方がクライアントである必要がある。

## [適用モデル]

NVR700W, NVR510

### 15.1.4 PPTP ホスト名の設定

---

## [書式]

**pptp hostname** *name*

**no pptp hostname** [*name*]

## [設定値及び初期値]

• *name*

- [設定値]: ホスト名 (64 バイト以下)
- [初期値]:
  - なし (NVR700W Rev.15.00.11 以降、NVR510 Rev.15.01.10 以降)
  - 機種名 (上記以外)

## [説明]

PPTP ホスト名を設定する。

## [ノート]

コマンドで設定したユーザー定義の名前が相手先に通知される。

相手先のルーターには、**show status pp** コマンドの '接続相手先:' で表示される。

## [適用モデル]

NVR700W, NVR510

### 15.1.5 PPTP ホスト名の設定

**[書式]**

**pptp vendorname** *name*  
**no pptp vendorname** [*name*]

**[設定値及び初期値]**

- *name*
  - [設定値]: ベンダー名 (最大 64 文字/半角、32 文字/全角)
  - [初期値]: -

**[説明]**

PPTP ベンダー名を設定する。

**[ノート]**

本コマンドで設定した値が Start-Control-Connection-Request と Start-Control-Connection-Reply のベンダー名にセットされる。

本コマンドが設定されていないときはベンダー名に空文字がセットされる。

NVR700W Rev.15.00.11 以降、NVR510 Rev.15.01.10 以降のファームウェアで使用可能。  
 それ以外のファームウェアではベンダー名に"YAMAHA Corporation"がセットされる。

**[適用モデル]**

NVR700W, NVR510

### 15.1.6 PPTP パケットのウィンドウサイズの設定

**[書式]**

**pptp window size** *size*  
**no pptp window size** [*size*]

**[設定値及び初期値]**

- *size*
  - [設定値]: パケットサイズ (1..128)
  - [初期値]: 32

**[説明]**

受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を設定する。

**[適用モデル]**

NVR700W, NVR510

### 15.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定

**[書式]**

**pp auth request** *auth* [arrive-only]  
**no pp auth request** [*auth*]

**[設定値及び初期値]**

- *auth*
  - [設定値]:

| 設定値       | 説明              |
|-----------|-----------------|
| pap       | PAP             |
| chap      | CHAP            |
| mschap    | MSCHAP          |
| mschap-v2 | MSCHAP-Version2 |
| chap-pap  | CHAP と PAP 両方   |

- [初期値]: -

**[説明]**

要求する認証方式を設定します

**[ノート]**

PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常サーバー側で設定する。

**[適用モデル]**

NVR700W, NVR510

### 15.1.8 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定

**[書式]**

```
pp auth accept auth [auth]
no pp auth accept [auth auth]
```

**[設定値及び初期値]**

- *auth*
  - [設定値]:

| 設定値       | 説明              |
|-----------|-----------------|
| pap       | PAP             |
| chap      | CHAP            |
| mschap    | MSCHAP          |
| mschap-v2 | MSCHAP-Version2 |

- [初期値]: -

**[説明]**

受け入れ可能な認証方式を設定します。

**[ノート]**

PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常クライアント側で設定する。

MacOS 10.2 以降 および Windows Vista、Windows 7 をクライアントとして使用する場合は mschap-v2 を用いる。

**[適用モデル]**

NVR700W, NVR510

### 15.1.9 PPTP の接続制御の syslog を出力するか否かの設定

**[書式]**

```
pptp syslog syslog
no pptp syslog [syslog]
```

**[設定値及び初期値]**

- *syslog*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

- [初期値]: off

**[説明]**

PPTP の接続制御の syslog を出力するか否かを設定する。

キープアライブ用の Echo-Request, Echo-Reply については出力されない。

[適用モデル]  
NVR700W, NVR510

## 15.2 リモートアクセス VPN 機能

### 15.2.1 PPTP トンネルの出力切断タイマの設定

[書式]

```
pptp tunnel disconnect time time
no pptp tunnel disconnect time [time]
```

[設定値及び初期値]

- *time*
- [設定値]:

| 設定値         | 説明        |
|-------------|-----------|
| 1..21474836 | 秒数        |
| off         | タイマを設定しない |

- [初期値]: 60

[説明]

選択されている PPTP トンネルに対して、データパケット無送信の場合、タイムアウトにより PPTP トンネルを切断する時間を設定する。

[適用モデル]  
NVR700W, NVR510

### 15.2.2 PPTP キープアライブの設定

[書式]

```
pptp keepalive use use
no pptp keepalive use [use]
```

[設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on

[説明]

トンネルキープアライブを使用するか否かを選択する。

[ノート]

PPTP トンネルの端点に対して、PPTP 制御コネクション確認要求 (Echo-Request) を送出して、それに対する PPTP 制御コネクション確認要求への応答 (Echo-Reply) で相手先からの応答があるかどうかを確認する。応答がない場合には、**pptp keepalive interval** コマンドに従った切断処理を行う。

[適用モデル]  
NVR700W, NVR510

### 15.2.3 PPTP キープアライブのログ設定

[書式]

```
pptp keepalive log log
no pptp keepalive log [log]
```

[設定値及び初期値]

- *log*

- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | ログにとる   |
| off | ログにとらない |

- [初期値]: off

#### [説明]

トンネルキープアライブをログに取るかどうか選択する。

#### [適用モデル]

NVR700W, NVR510

### 15.2.4 PPTP キープアライブを出すインターバルとカウントの設定

#### [書式]

```
pptp keepalive interval interval [count]
```

```
no pptp keepalive interval [interval count]
```

#### [設定値及び初期値]

- *interval*
  - [設定値]: インターバル (1..65535)
  - [初期値]: 30
- *count*
  - [設定値]: カウント (3..100)
  - [初期値]: 6

#### [説明]

トンネルキープアライブを出すインターバルとダウン検出用のカウントを設定する。

#### [ノート]

一度 PPTP 制御コネクション確認要求 (Echo-Request) に対するリプライが返ってこないのを検出したら、その後の監視タイムは 1 秒に短縮される。

#### [適用モデル]

NVR700W, NVR510

### 15.2.5 PPTP 接続において暗号化の有無により接続を許可するか否かの設定

#### [書式]

```
ppp ccp no-encryption mode
```

```
no ppp ccp no-encryption [mode]
```

#### [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値    | 説明          |
|--------|-------------|
| reject | 暗号化なしでは接続拒否 |
| accept | 暗号化なしでも接続許可 |

- [初期値]: accept

#### [説明]

MPPE(Microsoft Point-to-Point Encryption) の暗号化がネゴシエーションされないときの動作を設定する。

#### [適用モデル]

NVR700W, NVR510



## 第 16 章

### IPIP トンネリング機能の設定

#### IPIP トンネリング機能

IPIP トンネリング (IP over IP) は、IP パケットにさらに IP ヘッダを付加してカプセル化することでネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。IPIP トンネリングには認証や暗号化の仕組みは無いため、閉域網サービスなど安全な通信が提供されている環境で利用します。

ヤマハルーターでは独自仕様の IPIP キープアライブを使用することができます。IPIP キープアライブを使用すると、以下のようなメリットがあります。

- 対向ルーターの応答を確認してからトンネルを確立することで、確実に対向ルーターにパケットを送信することができます。
- トンネル端点をホスト名で指定している場合に、ホスト名に対応する IP アドレスが変わっても、切断検知後に再度名前解決を行うことで自動的に復旧することができます。

#### 16.1 IPIP キープアライブの設定

##### [書式]

```
ipip keepalive use switch [interval [count]]
```

```
no ipip keepalive use [switch ...]
```

##### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | IPIP キープアライブを使用する  |
| off | IPIP キープアライブを使用しない |

- [初期値]: off
- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
  - [初期値]: 10
- *count*
  - [設定値]: ダウンと見なすまでのキープアライブパケット送信回数 (1..50)
  - [初期値]: 6

##### [説明]

IPIP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値に応じて独自仕様の IPIP キープアライブが動作する。

トンネルインターフェースにのみ設定可能。

キープアライブ有効時に、*count* 回連続してキープアライブの応答が確認できなければ接続性がないと見なしてトンネルをダウンする。

また、トンネル端点を名前指定している場合は、*count* 回キープアライブを送信しても応答がない場合、再度名前解決を実行する。

##### [ノート]

NVR700W の Rev.15.00.10 以降、NVR510 の Rev.15.01.09 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

## 16.2 IPIP キープアライブのログ設定

---

### [書式]

**ipip keepalive log** *log*

**no ipip keepalive log** [*log*]

### [設定値及び初期値]

- *log*

- [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | IPIP キープアライブをログに出力する  |
| off | IPIP キープアライブをログに出力しない |

- [初期値]: off

### [説明]

IPIP キープアライブのログを出力するか否かを設定する。  
ログはすべて、`debug` レベルの `SYSLOG` に出力される。  
トンネルインターフェースにのみ設定可能。

### [ノート]

NVR700W の Rev.15.00.10 以降、NVR510 の Rev.15.01.09 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 第 17 章

### クラウドサービスとの VPN 接続設定機能の設定

クラウドサービスと VPN 接続するためのヤマハルーターの設定を、かんたんに行うための機能です。本機能を利用することで、インターネットのゲートウェイにしているヤマハルーターと、クラウドサービスの仮想ネットワークとをかんたんに VPN 接続することができます。

本機能を使用するためには、事前にクラウドサービス側の設定をしておく必要があります。

接続するクラウドサービスとして選べるサービスは以下の URL を参照してください。

- [http://www.rtpro.yamaha.co.jp/RT/docs/cloud\\_vpn/](http://www.rtpro.yamaha.co.jp/RT/docs/cloud_vpn/)

#### 17.1 VPN 接続するクラウドサービスの指定

##### [書式]

```
cloud vpn service id service_name
no cloud vpn service id [service_name]
```

##### [設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *service\_name*
  - [設定値]:

| 設定値        | 説明                         |
|------------|----------------------------|
| amazon-api | API を用いた Amazon VPC との接続設定 |

- [初期値]: -

##### [説明]

VPN 接続するクラウドサービスを指定する。

##### [ノート]

NVR700W の Rev.15.00.10 以降で使用可能。

##### [適用モデル]

NVR700W

#### 17.2 クラウドサービスとの VPN 接続設定に必要なパラメーターの設定

##### [書式]

```
cloud vpn parameter id parameter [parameter [parameter]]
no cloud vpn parameter id [parameter ...]
```

##### [設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *parameter*
  - [設定値]: パラメーター (半角 256 文字以内)
  - [初期値]: -

##### [説明]

クラウドサービスとの VPN 接続設定に必要なパラメーターを設定する。

Amazon VPC との VPN 接続を行う場合、次の順番で *parameter* に指定する。これらの情報は、事前に AWS の管理画面で設定しておく必要がある。

1. アクセスキー ID

2. シークレットアクセスキー
3. VPN ID

[ノート]

NVR700W の Rev.15.00.10 以降で使用可能。

[設定例]

Amazon VPC との VPN 接続を行う場合

```
cloud vpn parameter 1 abcdefghij ABCDEFGHIJKLM vpn-01234567
```

[適用モデル]

NVR700W

## 17.3 クラウドサービスとの VPN 接続設定の名称の設定

---

[書式]

**cloud vpn name** *id name*

**no cloud vpn name** *id [name]*

[設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *name*
  - [設定値]: クラウド設定の名称 (半角 32 文字以内)
  - [初期値]: -

[説明]

クラウドサービスとの VPN 接続設定の名称を設定する。

*name* に指定した名称は、設定を取得したときに自動的に設定される **tunnel description** コマンドの文字列に反映される。

[ノート]

NVR700W の Rev.15.00.10 以降で使用可能。

[適用モデル]

NVR700W

## 17.4 クラウドサービスとの VPN 接続を設定するトンネルインターフェースの指定

---

[書式]

**cloud vpn bind** *id tunnel\_if1 [tunnel\_if2]*

**no cloud vpn bind** *id [tunnel\_if1 ...]*

[設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *tunnel\_if1, tunnel\_if2*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

[説明]

クラウドサービスとの VPN 接続を設定するトンネルインターフェースを指定する。

本コマンドを事前に設定した場合、指定したトンネルインターフェースにクラウドサービスとの VPN 接続を設定する。

Amazon VPC との VPN 接続設定を行う場合、トンネルインターフェースを 2 つ指定する必要がある。

本コマンドを設定していない状態で、クラウドサービスから設定値を取得した場合、使用していないトンネルインターフェースを検索して自動的に設定する。

[ノート]

NVR700W の Rev.15.00.10 以降で使用可能。

[適用モデル]

NVR700W

## 17.5 クラウドサービスとの VPN 接続設定に使用するオプションの設定

[書式]

```
cloud vpn option id option=value
no cloud vpn option id [option=value]
```

[設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *option=value*
  - [設定値]:

| option | value | 説明                                        |
|--------|-------|-------------------------------------------|
| region | リージョン | Amazon VPC のインスタンスを生成したリージョン (半角 32 文字以内) |

- [初期値]:
  - region=ap-northeast-1

[説明]

クラウドサービスとの VPN 接続設定に使用するオプションを設定する。

region には、Amazon VPC のインスタンスを生成したリージョンを設定する。初期値は ap-northeast-1 で、アジアパシフィック (東京) のリージョンである。Amazon VPC のリージョン名、およびリージョンについては以下の URL を参照のこと。

- [http://www.rtpro.yamaha.co.jp/RT/docs/cloud\\_vpn/amazon-vpc\\_api.html](http://www.rtpro.yamaha.co.jp/RT/docs/cloud_vpn/amazon-vpc_api.html)

[ノート]

NVR700W の Rev.15.00.10 以降で使用可能。

[適用モデル]

NVR700W

## 17.6 クラウドサービスとの VPN 接続設定の手動実行

[書式]

```
cloud vpn set go id [option]
```

[設定値及び初期値]

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -
- *option*
  - [設定値]:

| 設定値     | 説明                 |
|---------|--------------------|
| save    | 生成した CONFIG を保存する  |
| no-save | 生成した CONFIG を保存しない |

- [初期値]: -

**[説明]**

クラウドサービスとの VPN 接続設定を実行する。

クラウドサービスから取得した設定値を基に、クラウドサービスとの VPN 接続を行うための CONFIG を生成し、VPN 接続する。

*option* を省略した場合、クラウドサービスとの VPN 接続設定が完了すると、設定を保存するか否か (Y/N) の問い合わせを表示する。Y を入力すると設定を保存し、N を入力すると設定を保存しない。

Web GUI でのコマンド実行やスケジュール実行、Lua スクリプトなど、対話型の入力ができない場合、*option* は必ず指定する必要がある。

**[ノート]**

本コマンドを実行して手動で設定値を取得する場合、リトライは行わない。

NVR700W の Rev.15.00.10 以降で使用可能。

**[設定例]**

```
# cloud vpn set go 1
.....
クラウドサービスとの VPN 接続設定が完了しました。
設定を保存しますか？ (Y/N)
```

**[適用モデル]**

NVR700W

## 17.7 クラウドサービスとの VPN 接続設定の状態の表示

---

**[書式]**

**show status cloud vpn [id]**

**[設定値及び初期値]**

- *id*
  - [設定値]: クラウド設定番号 (1..3)
  - [初期値]: -

**[説明]**

クラウドサービスとの VPN 接続設定の状態を表示する。

- 設定名
- ステータス (設定取得状況)
- CONFIG の更新日時
- 設定情報の最終取得日時
- トンネルの接続状態

ID を省略すると、設定されているすべてのクラウドサービスとの VPN 接続設定の状態を表示する。

**[ノート]**

NVR700W の Rev.15.00.10 以降で使用可能。

**[表示例]**

```
# show status cloud vpn 1
クラウド設定 [1]
サービス名:          Amazon (API 方式)
設定名:              yamaha          # cloud vpn name コマンドの設定値
ステータス:          設定済み
最終取得日時:        2017/01/25 10:11:22
CONFIG の更新日時:    2017/01/24 12:00:00
TUNNEL の接続状態:
  TUNNEL [01]: 接続されています
  TUNNEL [02]: 接続されています
```

**[適用モデル]**

NVR700W

## 17.8 クラウドサービス接続時の詳細情報を SYSLOG に表示

### [書式]

**cloud vpn syslog** *sw*

**no cloud vpn syslog** [*sw*]

### [設定値及び初期値]

- *sw*

- [設定値]:

| 設定値 | 説明                              |
|-----|---------------------------------|
| on  | クラウドサービス接続時の詳細情報を SYSLOG に表示する  |
| off | クラウドサービス接続時の詳細情報を SYSLOG に表示しない |

- [初期値]: off

### [説明]

クラウドサービス接続時の詳細情報を SYSLOG に表示する。

### [ノート]

Rev.15.00.16 以降で使用可能。

### [適用モデル]

NVR700W

## 第 18 章

### SNMP の設定

SNMP (Simple Network Management Protocol) の設定を行うことにより、SNMP 管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができますようになります。このとき NVR700W, NVR510 は SNMP エージェントとなります。

NVR700W, NVR510 は SNMPv1, SNMPv2c, SNMPv3 による通信に対応しています。また MIB (Management information Base) として RFC1213 (MIB-II) とプライベート MIB に対応しています。プライベート MIB については以下の URL から参照することができます。

- YAMAHA private MIB: <http://www.rtpro.yamaha.co.jp/RT/docs/mib/>

SNMPv1 および SNMPv2c では、コミュニティと呼ばれるグループの名前を相手に通知し、同じコミュニティに属するホスト間でのみ通信します。このとき、読み出し専用 (read-only) と読み書き可能 (read-write) の 2 つのアクセスモードに対して別々にコミュニティ名を設定することができます。

このようにコミュニティ名はある種のパスワードとして機能しますが、その反面、コミュニティ名は必ず平文でネットワーク上を流れるという特性があり、セキュリティ面では脆弱と言えます。よりセキュアな通信が必要な場合は SNMPv3 の利用を推奨します。

SNMPv3 では通信内容の認証、および暗号化に対応しています。SNMPv3 はコミュニティの概念を廃し、新たに USM (User-based Security Model) と呼ばれるセキュリティモデルを利用することで、より高度なセキュリティを確保しています。

NVR700W, NVR510 の状態を通知する SNMP メッセージをトラップと呼びます。NVR700W, NVR510 では SNMP 標準トラップの他にも、一部機能で特定のイベントを通知するため独自のトラップを送信することがあります。なお、これらの独自トラップはプライベート MIB として定義されています。

トラップの送信先ホストについては、各 SNMP バージョン毎に複数のホストを設定することができます。

SNMPv1 および SNMPv2c で利用する読み出し専用と送信トラップ用のコミュニティ名は、共に初期値が "public" となっています。SNMP 管理ソフトウェア側も "public" がコミュニティ名である場合が多いため、当該バージョンの通信でセキュリティを考慮する場合は適切なコミュニティ名に変更してください。ただし、上述の通りコミュニティ名はネットワーク上を平文で流れますので、コミュニティ名にログインパスワードや管理パスワードを決して使用しないよう注意してください。

工場出荷状態では、各 SNMP バージョンにおいてアクセスが一切できない状態となっています。また、トラップの送信先ホストは設定されておらず、どこにもトラップを送信しません。

#### 18.1 SNMPv1 によるアクセスを許可するホストの設定

##### [書式]

```
snmp host host [ro_community [rw_community]]
```

```
no snmp host [host]
```

##### [設定値及び初期値]

- *host*: SNMPv1 によるアクセスを許可するホスト

- [設定値]:

| 設定値               | 説明                                          |
|-------------------|---------------------------------------------|
| <i>ip_address</i> | 1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス(範囲指定) |
| <i>lanN</i>       | LAN インターフェース名                               |
| <i>onul</i>       | ONU インターフェース名                               |
| <i>bridgeN</i>    | ブリッジインターフェース名                               |
| any               | すべてのホストからのアクセスを許可する                         |
| none              | すべてのホストからのアクセスを禁止する                         |

- [初期値]: none

- *ro\_community*

- [設定値]: 読み出し専用のコミュニティ名 (16 文字以内)



- [初期値]:-
- *rw\_community*
  - [設定値]: 読み書き可能なコミュニティ名 (16 文字以内)
  - [初期値]:-

**[説明]**

SNMPv1 によるアクセスを許可するホストを設定する。

'any' を設定した場合は任意のホストからの SNMPv1 によるアクセスを許可する。

IP アドレスや *lanN*、*onu1*、*bridgeN* でホストを指定した場合には、同時にコミュニティ名も設定できる。

*rw\_community* パラメーターを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。

*ro\_community* パラメーターも省略した場合には、**snmp community read-only** コマンド、および **snmp community read-write** コマンドの設定値が用いられる。

**[適用モデル]**

NVR700W, NVR510

## 18.2 SNMPv1 の読み出し専用のコミュニティ名の設定

---

**[書式]**

**snmp community read-only** *name*

**no snmp community read-only**

**[設定値及び初期値]**

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: public

**[説明]**

SNMPv1 によるアクセスモードが読み出し専用であるコミュニティ名を設定する。

**[適用モデル]**

NVR700W, NVR510

## 18.3 SNMPv1 の読み書き可能なコミュニティ名の設定

---

**[書式]**

**snmp community read-write** *name*

**no snmp community read-write**

**[設定値及び初期値]**

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]:-

**[説明]**

SNMPv1 によるアクセスモードが読み書き可能であるコミュニティ名を設定する。

**[適用モデル]**

NVR700W, NVR510

## 18.4 SNMPv1 トラップの送信先の設定

---

**[書式]**

**snmp trap host** *host* [*community*]

**no snmp trap host** *host*

**[設定値及び初期値]**

- *host*
  - [設定値]: SNMPv1 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
  - [初期値]:-
- *community*

- [設定値]: コミュニティ名 (16 文字以内)
- [初期値]: -

**[説明]**

SNMPv1 トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ名にはこのコマンドの *community* パラメーターが用いられるが、省略されている場合には **snmp trap community** コマンドの設定値が用いられる。

**[適用モデル]**

NVR700W, NVR510

## 18.5 SNMPv1 トラップのコミュニティ名の設定

---

**[書式]**

```
snmp trap community name
no snmp trap community
```

**[設定値及び初期値]**

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: public

**[説明]**

SNMPv1 トラップを送信する際のコミュニティ名を設定する。

**[適用モデル]**

NVR700W, NVR510

## 18.6 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定

---

**[書式]**

```
snmp trap cpu threshold switch
no snmp trap cpu threshold
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: off

**[説明]**

system cpu threshold により設定した警告を発する CPU 使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

**[ノート]**

NVR700W は Rev.15.00.16 以降で使用可能。 NVR510 は Rev.15.01.15 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 18.7 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定

---

**[書式]**

```
snmp trap memory threshold switch
no snmp trap memory threshold
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: off

#### [説明]

system memory threshold により設定した警告を発するメモリ使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

#### [ノート]

NVR700W は Rev.15.00.16 以降で使用可能。NVR510 は Rev.15.01.15 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 18.8 SNMPv2c によるアクセスを許可するホストの設定

#### [書式]

```
snmpv2c host host [ro_community [rw_community]]
```

```
no snmpv2c host [host]
```

#### [設定値及び初期値]

- *host*: SNMPv2c によるアクセスを許可するホスト
- [設定値]:

| 設定値               | 説明                                          |
|-------------------|---------------------------------------------|
| <i>ip_address</i> | 1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス(範囲指定) |
| <i>lanN</i>       | LAN インターフェース名                               |
| <i>onu1</i>       | ONU インターフェース名                               |
| <i>bridgeN</i>    | ブリッジインターフェース名                               |
| any               | すべてのホストからのアクセスを許可する                         |
| none              | すべてのホストからのアクセスを禁止する                         |

- [初期値]: none
- *ro\_community*
  - [設定値]: 読み出し専用のコミュニティ名 (16 文字以内)
  - [初期値]: -
- *rw\_community*
  - [設定値]: 読み書き可能なコミュニティ名 (16 文字以内)
  - [初期値]: -

#### [説明]

SNMPv2c によるアクセスを許可するホストを設定する。

'any' を設定した場合は任意のホストからの SNMPv2c によるアクセスを許可する。

IP アドレスや *lanN*、*onu1*、*bridgeN* でホストを指定した場合には、同時にコミュニティ名も設定できる。*rw\_community* パラメーターを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。*ro\_community* パラメーターも省略した場合には、**snmpv2c community read-only** コマンド、および **snmpv2c community read-write** コマンドの設定値が用いられる。

#### [適用モデル]

NVR700W, NVR510

## 18.9 SNMPv2c の読み出し専用のコミュニティ名の設定

#### [書式]

```
snmpv2c community read-only name
```

**no snmpv2c community read-only**

[設定値及び初期値]

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: public

[説明]

SNMPv2c によるアクセスモードが読み出し専用であるコミュニティ名を設定する。

[適用モデル]

NVR700W, NVR510

## 18.10 SNMPv2c の読み書き可能なコミュニティ名の設定

[書式]

**snmpv2c community read-write *name***

**no snmpv2c community read-write**

[設定値及び初期値]

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: -

[説明]

SNMPv2c によるアクセスモードが読み書き可能であるコミュニティ名を設定する。

[適用モデル]

NVR700W, NVR510

## 18.11 SNMPv2c トラップの送信先の設定

[書式]

**snmpv2c trap host *host* [*type* [*community*]]**

**no snmpv2c trap host *host***

[設定値及び初期値]

- *host*
  - [設定値]: SNMPv2c トラップの送信先ホストの IP アドレス (IPv4/IPv6)
  - [初期値]: -
- *type*: メッセージタイプ
  - [設定値]:

| 設定値    | 説明                |
|--------|-------------------|
| trap   | トラップを送信する         |
| inform | Inform リクエストを送信する |

- [初期値]: trap
- *community*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: -

[説明]

SNMPv2c トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ名にはこのコマンドの *community* パラメーターが用いられるが、省略されている場合には **snmpv2c trap community** コマンドの設定値が用いられる。

*type* パラメーターで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

[適用モデル]

NVR700W, NVR510

## 18.12 SNMPv2c トラップのコミュニティ名の設定

---

### [書式]

```
snmpv2c trap community name
no snmpv2c trap community
```

### [設定値及び初期値]

- *name*
  - [設定値]: コミュニティ名 (16 文字以内)
  - [初期値]: public

### [説明]

SNMPv2c トラップを送信する際のコミュニティ名を設定する。

### [適用モデル]

NVR700W, NVR510

## 18.13 SNMPv3 エンジン ID の設定

---

### [書式]

```
snmpv3 engine id engine_id
no snmpv3 engine id
```

### [設定値及び初期値]

- *engine\_id*
  - [設定値]: SNMP エンジン ID (27 文字以内)
  - [初期値]: LAN1 の MAC アドレス

### [説明]

SNMP エンジンを識別するためのユニークな ID を設定する。SNMP エンジン ID は SNMPv3 通信で相手先に通知される。

相手先に通知されるフォーマットは以下。

- *engine\_id* が初期値の場合  
「8000049e03」 + (LAN1 の MAC アドレス)
- *engine\_id* に任意の値を設定した場合  
「8000049e04」 + 設定値の ASCII 文字列

### [適用モデル]

NVR700W, NVR510

## 18.14 SNMPv3 コンテキスト名の設定

---

### [書式]

```
snmpv3 context name name
no snmpv3 context name
```

### [設定値及び初期値]

- *name*
  - [設定値]: SNMP コンテキスト名 (16 文字以内)
  - [初期値]: -

### [説明]

SNMP コンテキストを識別するための名前を設定する。SNMP コンテキスト名は SNMPv3 通信で相手先に通知される。

### [適用モデル]

NVR700W, NVR510

## 18.15 SNMPv3 USM で管理するユーザーの設定

---

### [書式]

```
snmpv3 usm user user_id name [group group_id] [auth auth_pass [priv priv_pass]]
```

```
no snmpv3 usm user user_id
```

#### [設定値及び初期値]

- *user\_id*
  - [設定値]: ユーザー番号 (1..65535)
  - [初期値]: -
- *name*
  - [設定値]: ユーザー名 (32 文字以内)
  - [初期値]: -
- *group\_id*
  - [設定値]: ユーザーグループ番号 (1..65535)
  - [初期値]: -
- *auth*: 認証アルゴリズム
  - [設定値]:

| 設定値 | 説明           |
|-----|--------------|
| md5 | HMAC-MD5-96  |
| sha | HMAC-SHA1-96 |

- [初期値]: -
- *auth\_pass*
  - [設定値]: 認証パスワード (8 文字以上、32 文字以内)
  - [初期値]: -
- *priv*: 暗号アルゴリズム
  - [設定値]:

| 設定値        | 説明         |
|------------|------------|
| des-cbc    | DES-CBC    |
| aes128-cfb | AES128-CFB |

- [初期値]: -
- *priv\_pass*
  - [設定値]: 暗号パスワード (8 文字以上、32 文字以内)
  - [初期値]: -

#### [説明]

SNMPv3 によるアクセスが可能なユーザー情報を設定する。

ユーザーグループ番号を指定した場合は VACM によるアクセス制御の対象となる。指定しない場合、そのユーザーはすべての MIB オブジェクトにアクセスできる。

SNMPv3 では通信内容の認証および暗号化が可能であり、本コマンドでユーザー名と共にアルゴリズムおよびパスワードを設定して使用する。なお、認証を行わず暗号化のみを行うことはできない。

認証や暗号化の有無、アルゴリズムおよびパスワードは、対向となる SNMP マネージャ側のユーザー設定と一致させておく必要がある。

#### [適用モデル]

NVR700W, NVR510

## 18.16 SNMPv3 によるアクセスを許可するホストの設定

#### [書式]

```
snmpv3 host host user user_id ...
```

```
snmpv3 host none
```

```
no snmpv3 host [host]
```

#### [設定値及び初期値]

- *host*: SNMPv3 によるアクセスを許可するホスト
  - [設定値]:

| 設定値               | 説明                                          |
|-------------------|---------------------------------------------|
| <i>ip_address</i> | 1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス(範囲指定) |
| <i>lanN</i>       | LAN インターフェース名                               |
| <i>onu1</i>       | ONU インターフェース名                               |
| <i>bridgeN</i>    | ブリッジインターフェース名                               |
| <i>any</i>        | すべてのホストからのアクセスを許可する                         |

- [初期値]: -
- *none*: すべてのホストからのアクセスを禁止する
  - [初期値]: *none*
- *user\_id*: ユーザー番号
  - [設定値]:
    - 1 個の数字、または間に - をはさんだ数字 (範囲指定)、およびこれらを任意に並べたもの (128 個以内)
  - [初期値]: -

#### [説明]

SNMPv3 によるアクセスを許可するホストを設定する。

*host* パラメーターに '*any*' を設定した場合は任意のホストからの SNMPv3 によるアクセスを許可する。なお、アクセスのあったホストが *host* パラメーターに合致していても、*user\_id* パラメーターで指定したユーザーに合致しなければアクセスはできない。

#### [適用モデル]

NVR700W, NVR510

## 18.17 SNMPv3 VACM で管理する MIB ビューファミリの設定

#### [書式]

```
snmpv3 vacm view view_id type oid [type oid ...]
```

```
no snmpv3 vacm view view_id
```

#### [設定値及び初期値]

- *view\_id*
  - [設定値]: ビュー番号 (1..65535)
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値            | 説明                        |
|----------------|---------------------------|
| <i>include</i> | 指定したオブジェクト ID を管理対象にする    |
| <i>exclude</i> | 指定したオブジェクト ID を管理対象から除外する |

- [初期値]: -
- *oid*
  - [設定値]: MIB オブジェクト ID (サブ ID の数は 2 個以上、128 個以下)
  - [初期値]: -

#### [説明]

VACM による管理で使用する MIB ビューファミリを設定する。MIB ビューファミリとは、アクセス権を許可する際に指定する MIB 変数の集合である。

*type* パラメーターと *oid* パラメーターの組は、指定のオブジェクト ID 以降の MIB サブツリーを管理対象とする／しないことを意味する。また複数の組を指定した際に、それぞれ指定したオブジェクト ID の中で包含関係にあるものは、より下位の階層まで指定したオブジェクト ID に対応する *type* パラメーターが優先される。128 組まで指定可能。

## [設定例]

- `inetnet` サブツリー (1.3.6.1) 以降を管理対象とする。ただし `enterprises` サブツリー (1.3.6.1.4.1) 以降は管理対象から除外する

```
# snmpv3 vacm view 1 include 1.3.6.1 exclude 1.3.6.1.4.1
```

## [適用モデル]

NVR700W, NVR510

## 18.18 SNMPv3 VACM で管理するアクセスポリシーの設定

## [書式]

```
snmpv3 vacm access group_id read read_view write write_view
```

```
no snmpv3 vacm access group_id
```

## [設定値及び初期値]

- `group_id`
  - [設定値]: グループ番号 (1..65535)
  - [初期値]: -
- `read_view`
  - [設定値]:

| 設定値                  | 説明                     |
|----------------------|------------------------|
| <code>view_id</code> | 読み出し可能なアクセス権を設定するビュー番号 |
| <code>none</code>    | 読み出し可能なビューを設定しない       |

- [初期値]: -
- `write_view`
  - [設定値]:

| 設定値                  | 説明                     |
|----------------------|------------------------|
| <code>view_id</code> | 書き込み可能なアクセス権を設定するビュー番号 |
| <code>none</code>    | 書き込み可能なビューを設定しない       |

- [初期値]: -

## [説明]

ユーザーグループに対してアクセスできる MIB ビューファミリを設定する。このコマンドで設定された MIB ビューファミリに含まれない MIB 変数へのアクセスは禁止される。

## [適用モデル]

NVR700W, NVR510

## 18.19 SNMPv3 トラップの送信先の設定

## [書式]

```
snmpv3 trap host host [type] user user_id
```

```
no snmpv3 trap host host
```

## [設定値及び初期値]

- `host`
  - [設定値]: SNMPv3 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
  - [初期値]: -
- `type`: メッセージタイプ
  - [設定値]:

| 設定値                 | 説明                |
|---------------------|-------------------|
| <code>trap</code>   | トラップを送信する         |
| <code>inform</code> | Inform リクエストを送信する |



- [初期値]: trap
- *user\_id*
  - [設定値]: ユーザー番号
  - [初期値]: -

**[説明]**

SNMPv3 トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のユーザー設定は **snmpv3 usm user** コマンドで設定したユーザー設定が用いられる。

*type* パラメーターで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

**[適用モデル]**

NVR700W, NVR510

## 18.20 SNMP 送信パケットの始点アドレスの設定

---

**[書式]**

```
snmp local address ip_address
```

```
no snmp local address
```

**[設定値及び初期値]**

- *ip\_address*
  - [設定値]: IP アドレス (IPv4/IPv6)
  - [初期値]: インターフェースに設定されているアドレスから自動選択

**[説明]**

SNMP 送信パケットの始点 IP アドレスを設定する。

**[適用モデル]**

NVR700W, NVR510

## 18.21 sysContact の設定

---

**[書式]**

```
snmp syscontact name
```

```
no snmp syscontact
```

**[設定値及び初期値]**

- *name*
  - [設定値]: sysContact として登録する名称 (255 文字以内)
  - [初期値]: -

**[説明]**

MIB 変数 sysContact を設定する。空白を含ませるためには、パラメーター全体をダブルクォート ("), もしくはシングルクォート (') で囲む。

sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。

**[設定例]**

```
# snmp syscontact "RT administrator"
```

**[適用モデル]**

NVR700W, NVR510

## 18.22 sysLocation の設定

---

**[書式]**

```
snmp syslocation name
```

```
no snmp syslocation
```

**[設定値及び初期値]**

- *name*

- [設定値]: sysLocation として登録する名称 (255 文字以内)
- [初期値]: -

#### [説明]

MIB 変数 sysLocation を設定する。空白を含ませるためには、パラメーター全体をダブルクォート ("), もしくはシングルクォート (') で囲む。

sysLocation は一般的に、機器の設置場所を記入しておく変数である。

#### [設定例]

```
# snmp syslocation "RT room"
```

#### [適用モデル]

NVR700W, NVR510

## 18.23 sysName の設定

#### [書式]

```
snmp sysname name
```

```
no snmp sysname
```

#### [設定値及び初期値]

- *name*
  - [設定値]: sysName として登録する名称 (255 文字以内)
  - [初期値]: -

#### [説明]

MIB 変数 sysName を設定する。空白を含ませるためには、パラメーター全体をダブルクォート ("), もしくはシングルクォート (') で囲む。

sysName は一般的に、機器の名称を記入しておく変数である。

#### [設定例]

```
# snmp sysname "NVR700W working with a master mode"
```

#### [適用モデル]

NVR700W, NVR510

## 18.24 SNMP 標準トラップを送信するか否かの設定

#### [書式]

```
snmp trap enable snmp trap [trap...]
```

```
snmp trap enable snmp all
```

```
no snmp trap enable snmp
```

#### [設定値及び初期値]

- *trap*: 標準トラップの種類
  - [設定値]:

| 設定値                   | 説明      |
|-----------------------|---------|
| coldstart             | 電源投入時   |
| warmstart             | 再起動時    |
| linkdown              | リンクダウン時 |
| linkup                | リンクアップ時 |
| authenticationfailure | 認証失敗時   |

- [初期値]: -
- all: 全ての標準トラップを送信する

- [初期値]: -

#### [初期設定]

```
snmp trap enable snmp all
```

#### [説明]

SNMP 標準トラップを送信するか否かを設定する。

all を設定した場合には、すべての標準トラップを送信する。個別にトラップを設定した場合には、設定されたトラップだけが送信される。

#### [ノート]

authenticationFailure トラップを送信するか否かはこのコマンドによって制御される。

coldStart トラップは、電源投入、再投入による起動後およびファームウェアリビジョンアップによる再起動後に coldStart トラップを送信する。

linkDown トラップは、**snmp trap send linkdown** コマンドによってインターフェース毎に制御できる。あるインターフェースについて、linkDown トラップが送信されるか否かは、**snmp trap send linkdown** コマンドで送信が許可されており、かつ、このコマンドでも許可されている場合に限られる。

#### [適用モデル]

NVR700W, NVR510

## 18.25 SNMP トラップの送信の遅延時間の設定

---

#### [書式]

```
snmp trap delay-timer wait
snmp trap delay-timer off
no snmp trap delay-timer [wait]
```

#### [設定値及び初期値]

- *wait*
  - [設定値]: SNMP トラップを送信するまでの遅延時間の秒数(1 .. 21474836)
  - [初期値]: off
- *off*: SNMP トラップ遅延機能無効
  - [初期値]: -

#### [説明]

SNMP トラップを送信するイベントが発生してからトラップを送信するまでの間隔を指定する。off を設定した場合、即座に SNMP トラップを送信する。設定する遅延時間は最低限保証する値であり、設定値以上遅延する場合もある。

#### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 18.26 SNMP の linkDown トラップの送信制御の設定

---

#### [書式]

```
snmp trap send linkdown interface switch
snmp trap send linkdown pp peer_num switch
snmp trap send linkdown tunnel tunnel_num switch
no snmp trap send linkdown interface
no snmp trap send linkdown pp peer_num
no snmp trap send linkdown tunnel tunnel_num
```

**[設定値及び初期値]**

- *interface*
  - [設定値]:
    - LAN インターフェース名
    - ONU インターフェース名
    - WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 送信する  |
| off | 送信しない |

- [初期値]: on

**[説明]**

指定したインターフェースの linkDown トラップを送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 18.27 PP インターフェースの情報を MIB2 の範囲で表示するか否かの設定

---

**[書式]**

```
snmp yrifppdisplayatmib2 switch
no snmp yrifppdisplayatmib2
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明                                             |
|-----|------------------------------------------------|
| on  | MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする  |
| off | MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする |

- [初期値]: off

**[説明]**

MIB 変数 yrIfPpDisplayAtMib2 の値をセットする。この MIB 変数は、PP インターフェースを MIB2 の範囲で表示するかどうかを決定する。

**[適用モデル]**

NVR700W, NVR510

## 18.28 トンネルインターフェースの情報を MIB2 の範囲で表示するか否かの設定

---

**[書式]**

```
snmp yriftunneldisplayatmib2 switch
no snmp yriftunneldisplayatmib2
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明                                                 |
|-----|----------------------------------------------------|
| on  | MIB 変数 yrIfTunnelDisplayAtMib2 を "enabled(1)" とする  |
| off | MIB 変数 yrIfTunnelDisplayAtMib2 を "disabled(2)" とする |

- [初期値] : off

#### [説明]

MIB 変数 yrIfTunnelDisplayAtMib2 の値をセットする。この MIB 変数は、トンネルインターフェースを MIB2 の範囲で表示するかどうかを決定する。

#### [適用モデル]

NVR700W, NVR510

## 18.29 スイッチのインターフェースの情報を MIB2 の範囲で表示するか否かの設定

#### [書式]

```
snmp yrifswitchdisplayatmib2 switch
```

```
no snmp yrifswitchdisplayatmib2
```

#### [設定値及び初期値]

- *switch*
- [設定値] :

| 設定値 | 説明                                                 |
|-----|----------------------------------------------------|
| on  | MIB 変数 yrIfSwitchDisplayAtMib2 を "enabled(1)" とする  |
| off | MIB 変数 yrIfSwitchDisplayAtMib2 を "disabled(2)" とする |

- [初期値] : on

#### [説明]

MIB 変数 yrIfSwitchDisplayAtMib2 の値をセットする。この MIB 変数は、スイッチのインターフェースを MIB2 の範囲で表示するかどうかを決定する。

#### [適用モデル]

NVR700W, NVR510

## 18.30 内蔵無線 WAN インターフェースの情報を MIB2 の範囲で表示するか否かの設定

#### [書式]

```
snmp yrifwwandisplayatmib2 switch
```

```
no snmp yrifwwandisplayatmib2
```

#### [設定値及び初期値]

- *switch*
- [設定値] :

| 設定値 | 説明                                               |
|-----|--------------------------------------------------|
| on  | MIB 変数 yrIfWwanDisplayAtMib2 を "enabled(1)" とする  |
| off | MIB 変数 yrIfWwanDisplayAtMib2 を "disabled(2)" とする |

- [初期値] : off

#### [説明]

MIB 変数 yrIfWwanDisplayAtMib2 の値をセットする。この MIB 変数は、内蔵無線 WAN インターフェースを MIB2 の範囲で表示するかどうかを決定する。

## [ノート]

本コマンドは Rev.15.00.22 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 18.31 PP インターフェースのアドレスの強制表示の設定

## [書式]

```
snmp display ipcp force switch
no snmp display ipcp force
```

## [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                                                   |
|-----|------------------------------------------------------|
| on  | IPCP により付与された IP アドレスを PP インターフェースのアドレスとして必ず表示する     |
| off | IPCP により付与された IP アドレスは PP インターフェースのアドレスとして必ずしも表示されない |

- [初期値]: off

## [説明]

NAT を使用しない場合や、NAT の外側アドレスとして固定の IP アドレスが指定されている場合には、IPCP で得られた IP アドレスはそのまま PP インターフェースのアドレスとして使われる。この場合、SNMP では通常のインターフェースの IP アドレスを調べる手順で IPCP としてどのようなアドレスが得られたのか調べることができる。しかし、NAT の外側アドレスとして 'ipcp' と指定している場合には、IPCP で得られた IP アドレスは NAT の外側アドレスとして使用され、インターフェースには付与されない。そのため、SNMP でインターフェースの IP アドレスを調べても、IPCP でどのようなアドレスが得られたのかを知ることができない。

本コマンドを on に設定しておく、IPCP で得られた IP アドレスが NAT の外側アドレスとして使用される場合でも、SNMP ではそのアドレスをインターフェースのアドレスとして表示する。アドレスが実際にインターフェースに付与されるわけではないので、始点 IP アドレスとして、その IP アドレスが利用されることはない。

[適用モデル]  
NVR700W, NVR510

## 18.32 LAN インターフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設定

## [書式]

```
snmp trap link-updown separate-l2switch-port interface switch
no snmp trap link-updown separate-l2switch-port interface
```

## [設定値及び初期値]

- *interface*: インターフェース (現状では 'lan1' のみ設定可能)
  - [設定値]:
    - lan1
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | トラップを送信する  |
| off | トラップを送信しない |

- [初期値]: off

**[説明]**

各ポートのリンクが up/down したときにトラップを送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**18.33 電波強度トラップを送信するか否かの設定****[書式]**

```
snmp trap mobile signal-strength switch [level]
```

```
no snmp trap mobile signal-strength [switch [level]]
```

**[設定値及び初期値]**

- *switch*

- [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | トラップを送信する  |
| off | トラップを送信しない |

- [初期値]: off

- *level*: アンテナ本数の閾値

- [設定値]:

| 設定値  | 説明     |
|------|--------|
| 0..3 | アンテナ本数 |
| 省略   | 省略時は圏外 |

- [初期値]: -

**[説明]**

モバイル端末の電波強度トラップを送信するか否かを設定する。自動/手動に関わらず、ルーターが電波強度を取得した時にトラップ送信が許可されており、電波強度のアンテナ本数が閾値以下であった場合にトラップが送信される。

**[ノート]**

トラップは `yrIfMobileStatusTrap` が送信される。

**[適用モデル]**

NVR700W, NVR510

**18.34 内蔵無線 WAN モジュールの電波強度トラップを送信するか否かの設定****[書式]**

```
snmp trap wwan-module signal-strength switch [level]
```

```
no snmp trap wwan-module signal-strength [switch [level]]
```

**[設定値及び初期値]**

- *switch*

- [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | トラップを送信する  |
| off | トラップを送信しない |

- [初期値]: off

- *level*: アンテナ本数の閾値

- [設定値]:

| 設定値  | 説明     |
|------|--------|
| 0..3 | アンテナ本数 |

| 設定値 | 説明     |
|-----|--------|
| 省略  | 省略時は圏外 |

- [初期値]:-

#### [説明]

内蔵無線 WAN モジュールの電波強度トラップを送信するか否かを設定する。自動/手動に関わらず、ルーターが電波強度を取得した時にトラップ送信が許可されており、電波強度のアンテナ本数が閾値以下であった場合にトラップが送信される。

#### [ノート]

トラップは `yrIfWwanModStatTrp` が送信される。

#### [適用モデル]

NVR700W

## 18.35 スイッチへ静的に付与するインターフェース番号の設定

#### [書式]

```
snmp ifindex switch static index index switch
no snmp ifindex switch static index index [switch]
```

#### [設定値及び初期値]

- *index*
  - [設定値]: オブジェクト ID のインデックス(100000000 .. 199999999)
  - [初期値]:-
- *switch*: MAC アドレス、あるいはポート番号の組
  - [初期値]:-

#### [説明]

スイッチのインターフェースを示すオブジェクト ID のインデックスの先頭を静的に指定する。

#### [ノート]

オブジェクト ID が重複した場合の動作は保証されない。

静的にオブジェクト ID のインデックスの先頭を指定した場合、スイッチのインターフェースを示すオブジェクト ID のインデックスは動的に割り当てられない。

`snmp yrswindex switch static index` コマンドが設定された場合、`snmp yrswindex switch static index` コマンドで指定されたスイッチのみインデックスが割り当てられる。

#### [適用モデル]

NVR700W, NVR510

## 18.36 スイッチへ静的に付与するスイッチ番号の設定

#### [書式]

```
snmp yrswindex switch static index index switch
no snmp yrswindex switch static index index [switch]
```

#### [設定値及び初期値]

- *index*
  - [設定値]: オブジェクト ID のインデックス(1 .. 2147483647)
  - [初期値]:-
- *switch*: MAC アドレス、あるいはポート番号の組
  - [初期値]:-

#### [説明]

スイッチのオブジェクト ID のインデックスを静的に指定する。



## [ノート]

静的にオブジェクト ID のインデックスを指定した場合、スイッチのオブジェクト ID のインデックスは動的に割り当てられない。

## [適用モデル]

NVR700W, NVR510

## 18.37 スイッチの状態による SNMP トラップの条件の設定

## [書式]

**snmp trap enable switch** *switch trap* [*trap...*]

**snmp trap enable switch** *switch* all

**snmp trap enable switch** *switch* none

**no snmp trap enable switch** *switch*

## [設定値及び初期値]

- *switch* : default、MAC アドレス、あるいはポート番号の組
  - [初期値] :-
- *trap* : トラップの種類
  - [設定値] :

| 設定値          | 説明       |
|--------------|----------|
| linkup       | リンクアップ時  |
| linkdown     | リンクダウン時  |
| fanlock      | ファン異常時   |
| loopdetect   | ループ検出時   |
| poesupply    | 給電開始     |
| poetermine   | 給電停止     |
| oversupply   | 給電能力オーバー |
| overtemp     | 温度異常     |
| powerfailure | 電源異常     |

- [初期値] :-
- all : 全てのトラップを送信する
  - [初期値] :-
- none : 全てのトラップを送信しない
  - [初期値] :-

## [初期設定]

snmp trap enable switch default all

## [説明]

選択されたスイッチの監視状態に応じてトラップを送信する条件を設定する。default を指定して設定した場合は、個別のスイッチについて SNMP トラップの条件の設定がない場合の動作を決定する。

all を設定した場合には、すべてのトラップを送信する。none を設定した場合には、すべてのトラップを送信しない。個別にトラップを設定した場合には、設定されたトラップだけが送信される。

リンクアップ・リンクダウントラップは標準 MIB のトラップであり、送信するには **snmp trap enable snmp** コマンドでもトラップ送信が許可されている必要がある。

ループ検出のトラップを送信するにはスイッチ側に **switch control function set loopdetect-linkdown linkdown** コマンドあるいは **switch control function set loopdetect-linkdown linkdown-recovery** コマンドが設定されている必要がある。

給電開始、給電停止、給電能力オーバー、温度異常、電源異常のトラップを設定した場合、SWX2200-8PoE 以外のスイッチではトラップは送信されない。

[適用モデル]  
NVR700W, NVR510

## 18.38 スイッチで共通の SNMP トラップの条件の設定

### [書式]

**snmp trap enable switch common trap** [trap...]

**snmp trap enable switch common all**

**snmp trap enable switch common none**

**no snmp trap enable switch common**

### [設定値及び初期値]

- *trap* : トラップの種類
  - [設定値] :

| 設定値         | 説明            |
|-------------|---------------|
| find-switch | スイッチが監視下に入った時 |
| detect-down | スイッチが監視から外れた時 |

- [初期値] : -
- all : 全てのトラップを送信する
  - [初期値] : -
- none : 全てのトラップを送信しない
  - [初期値] : -

### [初期設定]

snmp trap enable switch common all

### [説明]

スイッチの監視状態に応じてトラップを送信する条件を設定する。

[適用モデル]  
NVR700W, NVR510

## 第 19 章

### RADIUS の設定

ISDN 接続のための認証とアカウントを RADIUS サーバーを利用して管理できます。PPTP 接続のための認証とアカウントの管理はサポートされません。

#### 19.1 RADIUS による認証を使用するか否かの設定

##### [書式]

```
radius auth auth
no radius auth [auth]
```

##### [設定値及び初期値]

- *auth*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

##### [説明]

anonymous に対して何らかの認証を要求する設定の場合に、相手から受け取ったユーザーネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザーネーム (**pp auth username** コマンドで指定) の中に含まれていない場合には RADIUS サーバーに問い合わせるか否かを設定する。

##### [ノート]

RADIUS による認証と RADIUS によるアカウントは独立して使用できる。  
サポートしているアトリビュートについては、WWW サイトのドキュメント<<http://www.rtpro.yamaha.co.jp>> を参照すること。

NVR510 は Rev.15.01.03 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

#### 19.2 RADIUS によるアカウントを使用するか否かの設定

##### [書式]

```
radius account account
no radius account [account]
```

##### [設定値及び初期値]

- *account*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

##### [説明]

RADIUS によるアカウントを使用するか否かを設定する。

## [ノート]

RADIUS による認証と RADIUS によるアカウントは独立して使用できる。

サポートしているアトリビュートについては、WWW サイトのドキュメント<<http://www.rtpro.yamaha.co.jp>> を参照すること。

NVR510 は Rev.15.01.03 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 19.3 RADIUS サーバーの指定

---

## [書式]

```
radius server ip1 [ip2]
```

```
no radius server [ip1 [ip2]]
```

## [設定値及び初期値]

- *ip1*
  - [設定値]: RADIUS サーバー(正)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -
- *ip2*
  - [設定値]: RADIUS サーバー(副)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -

## [説明]

RADIUS サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

## [ノート]

RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバーは **radius auth server/radius account server** コマンドで個別に設定できる。**radius server** コマンドでの設定は、これら個別の設定が行われていない場合に有効となり、認証、アカウントいずれでも用いられる。

NVR510 は Rev.15.01.03 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 19.4 RADIUS 認証サーバーの指定

---

## [書式]

```
radius auth server ip1 [ip2]
```

```
no radius auth server [ip1 [ip2]]
```

## [設定値及び初期値]

- *ip1*
  - [設定値]: RADIUS 認証サーバー(正)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -
- *ip2*
  - [設定値]: RADIUS 認証サーバー(副)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -

## [説明]

RADIUS 認証サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

## [ノート]

このコマンドで RADIUS 認証サーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスを認証サーバーとして用いる。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 19.5 RADIUS アカウントサーバーの指定

---

### [書式]

```
radius account server ip1 [ip2]
no radius account server [ip1 [ip2]]
```

### [設定値及び初期値]

- *ip1*
  - [設定値]: RADIUS アカウントサーバー(正)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -
- *ip2*
  - [設定値]: RADIUS アカウントサーバー(副)の IP アドレス (IPv6 アドレス可)
  - [初期値]: -

### [説明]

RADIUS アカウントサーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

### [ノート]

このコマンドで RADIUS アカウントサーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスをアカウントサーバーとして用いる。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 19.6 RADIUS 認証サーバーの UDP ポートの設定

---

### [書式]

```
radius auth port port_num
no radius auth port [port_num]
```

### [設定値及び初期値]

- *port\_num*
  - [設定値]: UDP ポート番号
  - [初期値]: 1645

### [説明]

RADIUS 認証サーバーの UDP ポート番号を設定する

### [ノート]

RFC2138 ではポート番号として 1812 を使うことになっている。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 19.7 RADIUS アカウントサーバーの UDP ポートの設定

---

### [書式]

```
radius account port port_num
no radius account port [port_num]
```

**[設定値及び初期値]**

- *port\_num*
  - [設定値]: UDP ポート番号
  - [初期値]: 1646

**[説明]**

RADIUS アカウントサーバーの UDP ポート番号を設定する。

**[ノート]**

RFC2138 ではポート番号として 1813 を使うことになっている。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 19.8 RADIUS シークレットの設定

---

**[書式]**

**radius secret** *secret*

**no radius secret** [*secret*]

**[設定値及び初期値]**

- *secret*
  - [設定値]: シークレット文字列 (16 文字以内)
  - [初期値]: -

**[説明]**

RADIUS シークレットを設定する。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 19.9 RADIUS 再送信パラメーターの設定

---

**[書式]**

**radius retry** *count time*

**no radius retry** [*count time*]

**[設定値及び初期値]**

- *count*
  - [設定値]: 再送回数 (1..10)
  - [初期値]: 4
- *time*
  - [設定値]: ミリ秒 (20..10000)
  - [初期値]: 3000

**[説明]**

RADIUS パケットの再送回数とその時間間隔を設定する。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 第 20 章

### NAT 機能

NAT 機能は、ルーターが転送する IP パケットの始点/終点 IP アドレスや、TCP/UDP のポート番号を変換することにより、アドレス体系の異なる IP ネットワークを接続することができる機能です。

NAT 機能を用いると、プライベートアドレス空間とグローバルアドレス空間との間でデータを転送したり、1 つのグローバル IP アドレスに複数のホストを対応させたりすることができます。

NVR700W, NVR510 では、始点/終点 IP アドレスの変換だけを行うことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいます。

アドレス変換規則を表す記述を NAT ディスクリプターと呼び、それぞれの NAT ディスクリプターには、アドレス変換の対象とすべきアドレス空間が定義されます。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用います。前者は NAT 処理の内側 (INNER) のアドレス空間を、後者は NAT 処理の外側 (OUTER) のアドレス空間を定義するコマンドです。原則的に、これら 2 つのコマンドを対で設定することにより、変換前のアドレスと変換後のアドレスとの対応づけが定義されます。

NAT ディスクリプターはインターフェースに対して適用されます。インターフェースに接続された先のネットワークが NAT 処理の外側であり、インターフェースから本機を経由して他のインターフェースから繋がるネットワークが NAT 処理の内側になります。

NAT ディスクリプターは動作タイプ属性を持ちます。IP マスカレードやアドレスの静的割当てなどの機能を利用する場合には、該当する動作タイプを選択する必要があります。

#### 20.1 NAT 機能の動作タイプの設定

##### [書式]

```
nat descriptor backward-compatibility type
no nat descriptor backward-compatibility [type]
```

##### [設定値及び初期値]

- *type*
  - [設定値]:

| 設定値 | 説明                                               |
|-----|--------------------------------------------------|
| 1   | Rev.14 系以前の動作タイプ (ポートセービング IP マスカレード機能を無効にする)    |
| 2   | Rev.14.01 系以降の動作タイプ (ポートセービング IP マスカレード機能を有効にする) |

- [初期値]: 2

##### [説明]

NAT 機能全体の動作タイプを設定する。

Rev.14.01 系以降の機種では、ポートセービング IP マスカレード機能に対応しており、IP マスカレードにおいて同一のポート番号を使用して複数の接続先とのセッションを確立できる。本コマンドは、ポートセービング IP マスカレード機能をサポートしていない Rev.14 系以前の機種との互換性維持のために用意されており、*type* パラメーターを 1 に設定した場合の NAT 機能の動作は、Rev.14 系以前の NAT 機能の動作と同等となる。*type* パラメーターを 2 に設定して動作させた場合に問題が生じる場合は、*type* パラメーターを 1 にして NAT 機能を使用する必要がある。

##### [ノート]

本コマンドによる設定の変更を反映するには、ルーターの再起動が必要となる。

##### [適用モデル]

NVR700W, NVR510

#### 20.2 インターフェースへの NAT ディスクリプター適用の設定

##### [書式]

```
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
```

```

ip pp nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip tunnel nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
no ip interface nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip pp nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip tunnel nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *nat\_descriptor\_list*
  - [設定値]: 空白で区切られた NAT ディスクリプター番号 (1..2147483647) の並び (16 個以内)
  - [初期値]: -

#### [説明]

適用されたインターフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプターによって定義された NAT 変換を順番に処理する。

*reverse* の後ろに記述した NAT ディスクリプターでは、通常処理される IP アドレス、ポート番号とは逆向きの IP アドレス、ポート番号に対して NAT 変換を施す。

#### [ノート]

LAN インターフェースと ONU インターフェースの場合、NAT ディスクリプターの外側アドレスに対しては、同一 LAN の ARP 要求に対して応答する。

#### [適用モデル]

NVR700W, NVR510

## 20.3 NAT ディスクリプターの動作タイプの設定

#### [書式]

```

nat descriptor type nat_descriptor type [hairpin=sw]
no nat descriptor type nat_descriptor [type [hairpin=sw]]

```

#### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値            | 説明                               |
|----------------|----------------------------------|
| none           | NAT 変換機能を利用しない                   |
| nat            | 動的 NAT 変換と静的 NAT 変換を利用           |
| masquerade     | 静的 NAT 変換と IP マスカレード変換           |
| nat-masquerade | 動的 NAT 変換と静的 NAT 変換と IP マスカレード変換 |

- [初期値]: none
- *sw*
  - [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | ヘアピン NAT 機能を利用する  |
| off | ヘアピン NAT 機能を利用しない |

- [初期値]: off



**[説明]**

NAT 変換の動作タイプを指定する。

**[ノート]**

nat-masquerade は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能な場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

hairpin オプションは、NVR700W Rev.15.00.23、NVR510 Rev.15.01.23 以降のファームウェアで指定可能。また、type に none を指定したときは、hairpin オプションは指定できない。

**[適用モデル]**

NVR700W, NVR510

## 20.4 NAT 処理の外側 IP アドレスの設定

**[書式]**

```
nat descriptor address outer nat_descriptor outer_ipaddress_list
no nat descriptor address outer nat_descriptor [outer_ipaddress_list]
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *outer\_ipaddress\_list*: NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック
  - [設定値]:

| 設定値       | 説明                                                         |
|-----------|------------------------------------------------------------|
| IP アドレス   | 1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの   |
| ipcp      | PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス         |
| primary   | <b>ip interface address</b> コマンドで設定されている IP アドレス           |
| secondary | <b>ip interface secondary address</b> コマンドで設定されている IP アドレス |
| map-e     | MAP-E で自動的に生成された IP アドレス                                   |

- [初期値]: ipcp

**[説明]**

動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。

**[ノート]**

ニーモニックをリストにすることはできない。

適用されるインターフェースにより使用できるパラメーターが異なる。

| 適用インターフェース | LAN | PP | トンネル |
|------------|-----|----|------|
| ipcp       | ×   | ○  | ×    |
| primary    | ○   | ×  | ×    |
| secondary  | ○   | ×  | ×    |
| IP アドレス    | ○   | ○  | ○    |
| map-e      | ×   | ×  | ○    |

map-e キーワードは、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で指定可能。

[適用モデル]  
NVR700W, NVR510

## 20.5 NAT 処理の内側 IP アドレスの設定

### [書式]

```
nat descriptor address inner nat_descriptor inner_ipaddress_list
no nat descriptor address inner nat_descriptor [inner_ipaddress_list]
```

### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *inner\_ipaddress\_list*: NAT 対象の内側 IP アドレス範囲のリストまたはニーモニック
  - [設定値]:

| 設定値     | 説明                                                       |
|---------|----------------------------------------------------------|
| IP アドレス | 1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの |
| auto    | すべて                                                      |

- [初期値]: auto

### [説明]

NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。

[適用モデル]  
NVR700W, NVR510

## 20.6 静的 NAT エントリの設定

### [書式]

```
nat descriptor static nat_descriptor id outer_ip=inner_ip [count]
nat descriptor static nat_descriptor id outer_ip=inner_ip/netmask
no nat descriptor static nat_descriptor id [outer_ip=inner_ip [count]]
```

### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *id*
  - [設定値]: 静的 NAT エントリの識別情報 (1..2147483647)
  - [初期値]: -
- *outer\_ip*
  - [設定値]: 外側 IP アドレス (1 個)
  - [初期値]: -
- *inner\_ip*
  - [設定値]: 内側 IP アドレス (1 個)
  - [初期値]: -
- *count*
  - [設定値]:
    - 連続設定する個数
    - 省略時は 1
  - [初期値]: -
- *netmask*
  - [設定値]:
    - xxx.xxx.xxx.xxx (xxx は十進数)

- 0x に続く十六進数
- マスクビット数 (16...32)
- [初期値]:-

**[説明]**

NAT 変換で固定割り付けする IP アドレスの組み合わせを指定する。個数を同時に指定すると指定されたアドレスを始点とした範囲指定とする。

**[ノート]**

外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。  
 静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。初期値がそれぞれ *ipcp* と *auto* であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

**[適用モデル]**

NVR700W, NVR510

## 20.7 IP マスカレード使用時に **rlogin,rcp** と **ssh** を使用するか否かの設定

**[書式]**

```
nat descriptor masquerade rlogin nat_descriptor use
no nat descriptor masquerade rlogin nat_descriptor [use]
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]:-
- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

IP マスカレード使用時に **rlogin**、**rcp**、**ssh** の使用を許可するか否かを設定する。

**[ノート]**

on にすると、**rlogin**、**rcp** と **ssh** のトラフィックに対してはポート番号を変換しなくなる。  
 また on の場合に **rsh** は使用できない。

**[適用モデル]**

NVR700W, NVR510

## 20.8 静的 IP マスカレードエントリの設定

**[書式]**

```
nat descriptor masquerade static nat_descriptor id inner_ip protocol [outer_port=]inner_port
no nat descriptor masquerade static nat_descriptor id [inner_ip protocol [outer_port=]inner_port]
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]:-
- *id*
  - [設定値]: 静的 IP マスカレードエントリの識別情報 (1 以上の数値)
  - [初期値]:-

- *inner\_ip*
  - [設定値]: 内側 IP アドレス (1 個)
  - [初期値]: -
- *protocol*
  - [設定値]:

| 設定値     | 説明                               |
|---------|----------------------------------|
| esp     | ESP                              |
| tcp     | TCP プロトコル                        |
| udp     | UDP プロトコル                        |
| icmp    | ICMP プロトコル                       |
| プロトコル番号 | IANA で割り当てられている protocol numbers |

- [初期値]: -
- *outer\_port*
  - [設定値]: 固定する外側ポート番号 (ニーモニック)
  - [初期値]: -
- *inner\_port*
  - [設定値]: 固定する内側ポート番号 (ニーモニック)
  - [初期値]: -

#### [説明]

IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

#### [ノート]

*outer\_port* と *inner\_port* を指定した場合には IP マスカレード適用時にインターフェースの外側から内側へのパケットは *outer\_port* から *inner\_port* に、内側から外側へのパケットは *inner\_port* から *outer\_port* へとポート番号が変換される。

*outer\_port* を指定せず、*inner\_port* のみの場合はポート番号の変換はされない。

#### [適用モデル]

NVR700W, NVR510

## 20.9 NAT の IP アドレスマップの消去タイマの設定

#### [書式]

```

nat descriptor timer nat_descriptor time
nat descriptor timer nat_descriptor protocol=protocol [port=port_range] time
nat descriptor timer nat_descriptor tcpfin time2
no nat descriptor timer nat_descriptor [time]
no nat descriptor timer nat_descriptor protocol=protocol [port=port_range] [time]
no nat descriptor timer nat_descriptor tcpfin [time2]

```

#### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *time*
  - [設定値]: 消去タイマの秒数 (30..21474836)
  - [初期値]: 900
- *time2*
  - [設定値]: TCP/FIN 通過後の消去タイマの秒数 (1-21474836)
  - [初期値]: 60
- *protocol*
  - [設定値]: プロトコル

- [初期値]:-
- *port\_range*
  - [設定値]: ポート番号の範囲、プロトコルが TCP または UDP の場合にのみ有効
  - [初期値]:-

#### [説明]

NAT や IP マスカレードのセッション情報を保持する期間を表す NAT タイマを設定する。IP マスカレードの場合には、プロトコルやポート番号別の NAT タイマを設定することもできる。指定されていないプロトコルの場合は、第一の形式で設定した NAT タイマの値が使われる。

IP マスカレードの場合には、TCP/FIN 通過後の NAT タイマを設定することができる。TCP/FIN が通過したセッションは終了するセッションなので、このタイマを短くすることで NAT テーブルの使用量を抑えることができる。DNS の場合、このコマンドでの設定値にかかわらず、応答パケットが通過してから約 10 秒でセッション情報を削除する。

#### [適用モデル]

NVR700W, NVR510

## 20.10 IP マスカレードテーブルの TTL 処理方式の設定

#### [書式]

```
nat descriptor masquerade ttl hold type
no nat descriptor masquerade ttl hold
```

#### [設定値及び初期値]

- *type*
  - [設定値]:

| 設定値  | 説明                                              |
|------|-------------------------------------------------|
| auto | 自動認識可能なアプリケーションの接続の制御チャンネルとデータチャンネルの TTL を同期させる |
| all  | 同じホストによるすべての TCP 接続を対象                          |
| ftp  | FTP の制御チャンネルのみを対象                               |

- [初期値]: auto

#### [説明]

制御チャンネルとデータチャンネルからなるアプリケーションにおいて、データチャンネル上でのデータ転送中に、対応する制御チャンネルが消滅することによるデータ通信不良が発生しないようにするために、制御チャンネルとデータチャンネルの両 IP マスカレードテーブルの TTL を同期させる方法を設定する。

auto と設定した場合には、ルーターが自動認識可能なアプリケーションの接続に対応するテーブルの TTL を同期させる。

all と設定した場合には、同じホストによるすべての接続に対応するテーブルの TTL を同期させる。ftp と設定した場合には、FTP 接続に対応するテーブルの TTL のみを同期させる。

#### [ノート]

all と設定した場合には、多くのテーブルの TTL が同期して、多くのテーブルが残留するために、内部リソースが枯渇することがある。

auto と設定した場合に正常動作しないアプリケーションがあるときは all と設定しなければならない。

#### [適用モデル]

NVR700W, NVR510

## 20.11 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

#### [書式]

```
nat descriptor masquerade incoming nat_descriptor action [ip_address]
no nat descriptor masquerade incoming nat_descriptor
```

## [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *action*
  - [設定値]:

| 設定値     | 説明                 |             |
|---------|--------------------|-------------|
|         | TCP/0~1023 宛てのパケット | 左記以外        |
| through | 破棄して、RST を返す       | 変換せずに通す     |
| reject  | 破棄して、RST を返す       | 破棄して、何も返さない |
| discard | 破棄して、何も返さない        |             |
| forward | 指定されたホストに転送する      |             |

- [初期値]: reject
- *ip\_address*
  - [設定値]: 転送先の IP アドレス
  - [初期値]: -

## [説明]

IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。*action* が forward のときには *ip\_address* を設定する必要がある。

## [適用モデル]

NVR700W, NVR510

## 20.12 IP マスカレードで利用するポートの範囲の設定

## [書式]

```
nat descriptor masquerade port range nat_descriptor port_range1 [port_range2 [port_range3 [port_range4]]]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2 [port_range3 [port_range4]]]]
```

## [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *port\_range1*, *port\_range2*, *port\_range3*, *port\_range4*
  - [設定値]: 間に - をはさんだポート番号の範囲 (1-65534)
  - [初期値]: port\_range1=60000-64095、port\_range2=49152-59999、port\_range3=44096-49151

## [説明]

IP マスカレードで利用するポート番号の範囲を設定する。

ポート番号は、まず最初に *port\_range1* の範囲から利用される。*port\_range1* のポート番号がすべて使用中になったら、*port\_range2* の範囲のポート番号を使い始める。このように、*port\_range1* から *port\_rangeN* の範囲まで、小さい番号のポート範囲から順番にポート番号が利用される。

同一のポート番号を使用して複数の接続先とのセッションを確立できるため、本コマンドで設定したポート数を超えるセッションの確立が可能である。最大セッション数は **nat descriptor masquerade session limit total** コマンドで設定する。ただし、**nat descriptor backward-compatibility** コマンドで *type* パラメーターを 1 に変更した場合は、最大セッション数は本コマンドで設定したポート数と同等となるため、最大セッション数を変更する場合は本コマンドの設定を変更する必要がある。

## [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降では、ポート範囲を 16 個まで設定できる。  
NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降では、ポート範囲を 64 個まで設定できる。

[適用モデル]  
NVR700W, NVR510

## 20.13 FTP として認識するポート番号の設定

### [書式]

```
nat descriptor ftp port nat_descriptor port [port...]
no nat descriptor ftp port nat_descriptor [port...]
```

### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 21

### [説明]

TCP で、このコマンドにより設定されたポート番号を FTP の制御チャネルの通信だとみなして処理をする。

[適用モデル]  
NVR700W, NVR510

## 20.14 IP マスカレードで変換しないポート番号の範囲の設定

### [書式]

```
nat descriptor masquerade unconvertible port nat_descriptor if-possible
nat descriptor masquerade unconvertible port nat_descriptor protocol port
no nat descriptor masquerade unconvertible port nat_descriptor protocol [port]
```

### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *protocol*
  - [設定値]:

| 設定値 | 説明  |
|-----|-----|
| tcp | TCP |
| udp | UDP |

- [初期値]: -
- *port*
  - [設定値]: ポート番号の範囲
  - [初期値]: -

### [説明]

IP マスカレードで変換しないポート番号の範囲を設定する。

if-possible が指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

[適用モデル]  
NVR700W, NVR510

## 20.15 NAT のアドレス割当をログに記録するか否かの設定

### [書式]

```
nat descriptor log switch
no nat descriptor log
```

**[設定値及び初期値]**

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 記録する  |
| off | 記録しない |

- [初期値]: off

**[説明]**

NAT のアドレス割当をログに記録するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 20.16 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定

---

**[書式]**

**nat descriptor sip nat\_descriptor sip**

**no nat descriptor sip nat\_descriptor**

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *sip*
  - [設定値]:

| 設定値  | 説明                         |
|------|----------------------------|
| on   | 変換する                       |
| off  | 変換しない                      |
| auto | <b>sip use</b> コマンドの設定値に従う |

- [初期値]: auto

**[説明]**

静的 NAT や静的 IP マスカレードで SIP メッセージに含まれる IP アドレスを書き換えるか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 20.17 IP マスカレード変換時に DF ビットを削除するか否かの設定

---

**[書式]**

**nat descriptor masquerade remove df-bit remove**

**no nat descriptor masquerade remove df-bit [remove]**

**[設定値及び初期値]**

- *remove*
- [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | IP マスカレード変換時に DF ビットを削除する  |
| off | IP マスカレード変換時に DF ビットを削除しない |

- [初期値]: on

**[説明]**

IP マスカレード変換時に DF ビットを削除するか否かを設定する。



DF ビットは経路 MTU 探索のために用いるが、そのためには長すぎるパケットに対する ICMP エラーを正しく発信元まで返さなくてはならない。しかし、IP マスカレード処理では IP アドレスなどを書き換えてしまうため、ICMP エラーを正しく発信元に返せない場合がある。そうすると、パケットを永遠に届けることができなくなってしまう。このように、経路 MTU 探索のための ICMP エラーが正しく届かない状況を、経路 MTU ブラックホールと呼ぶ。

IP マスカレード変換時に同時に DF ビットを削除してしまうと、この経路 MTU ブラックホールを避けることができる。その代わりに、経路 MTU 探索が行われなくなるので、通信効率が下がる可能性がある。

**[適用モデル]**

NVR700W, NVR510

## 20.18 IP マスカレードで変換するホスト毎のセッション数の設定

---

**[書式]**

```
nat descriptor masquerade session limit nat_descriptor id limit
```

```
no nat descriptor masquerade session limit nat_descriptor id
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *id*
  - [設定値]: セッション数設定の識別番号 (1)
  - [初期値]: -
- *limit*
  - [設定値]: 制限値 (1..65534)
  - [初期値]: 65534

**[説明]**

ホスト毎に IP マスカレードで変換するセッションの最大数を設定する。

ホストはパケットの始点 IP アドレスで識別され、任意のホストを始点とした変換テーブルの登録数が *limit* に制限される。

**[適用モデル]**

NVR700W, NVR510

## 20.19 IP マスカレードで変換する合計セッション数の設定

---

**[書式]**

```
nat descriptor masquerade session limit total nat_descriptor limit
```

```
no nat descriptor masquerade session limit total nat_descriptor
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]: NAT ディスクリプター番号 (1..2147483647)
  - [初期値]: -
- *limit*
  - [設定値]: 制限値 (1..2147483647)
  - [初期値]: 65534

**[説明]**

ひとつの NAT ディスクリプターにおいて、IP マスカレードで変換するセッション数の最大数を設定する。 **nat descriptor masquerade session limit** コマンドとは異なり、すべてのホストのセッション数の合計が対象となる。

**[ノート]**

本コマンドの設定は、**nat descriptor backward-compatibility** コマンドで、*type* パラメーターを 2 に設定した場合のみ有効となる。

**[適用モデル]**

NVR700W, NVR510

## 第 21 章

### DNS の設定

本機は、DNS(Domain Name Service) 機能として名前解決、リカーシブサーバー機能、上位 DNS サーバーの選択機能、簡易 DNS サーバー機能 ( 静的 DNS レコードの登録 ) を持ちます。

名前解決の機能としては、**ping** や **traceroute**、**rdate**、**ntpdate**、**telnet** コマンドなどの IP アドレスパラメーターの代わりに名前を指定したり、**SYSLOG** などの表示機能において IP アドレスを名前解決したりします。

リカーシブサーバー機能は、DNS サーバーとクライアントの間に入って、DNS パケットの中継を行います。本機宛にクライアントから届いた DNS 問い合わせパケットを **dns server** 等のコマンドで設定された DNS サーバーに中継します。DNS サーバーからの回答は本機宛に届くので、それをクライアントに転送します。**dns cache max entry** コマンドで設定した件数 ( 初期値 = 256 ) のキャッシュを持ち、キャッシュにあるデータに関しては DNS サーバーに問い合わせることなく返事を返すため、DNS によるトラフィックを削減する効果があります。キャッシュは、DNS サーバーからデータを得た場合にデータに記されていた時間だけ保持されます。

DNS の機能を使用するためには、**dns server** 等のコマンドで、問い合わせ先 DNS サーバーを設定しておく必要があります。また、この設定は DHCP サーバー機能において、DHCP クライアントの設定情報にも使用されます。問い合わせ先 DNS サーバーを設定するコマンドは複数存在しますが、これらのうち複数のコマンドで問い合わせ先 DNS サーバーが設定されている場合、利用できる中で最も優先順位の高いコマンドの設定が使用されます。各コマンドによる設定の優先順位は、高い順に以下の通りです。

1. **dns server select** コマンド
2. **dns server** コマンド
3. **dns server pp** コマンド
4. **dns server pdp** コマンド
5. **dns server dhcp** コマンド

なお、これらのコマンドで問い合わせ先 DNS サーバーが全く設定されていない場合でも、DHCP サーバーから取得した DNS サーバーが存在すれば、そちらが自動的に使用されます。

#### 21.1 DNS を利用するか否かの設定

##### [書式]

```
dns service service
no dns service [service]
```

##### [設定値及び初期値]

- *service*
- [設定値]:

| 設定値       | 説明                   |
|-----------|----------------------|
| recursive | DNS リカーシブサーバーとして動作する |
| off       | サービスを停止させる           |

- [初期値]: recursive

##### [説明]

DNS リカーシブサーバーとして動作するかどうかを設定する。off を設定すると、DNS 的機能は一切動作しない。また、ポート 53/udp も閉じられる。

##### [適用モデル]

NVR700W, NVR510

#### 21.2 ルーター自身の FQDN の設定

##### [書式]

```
dns private name name
no dns private name [name]
```

##### [設定値及び初期値]

- *name*

- [設定値]: ルーターの FQDN
- [初期値]: -

**[説明]**

ルーターの DNS 名を指定する。

**[適用モデル]**

NVR700W, NVR510

## 21.3 DNS サーバーの IP アドレスの設定

**[書式]**

```
dns server ip_address [edns=sw] [nat46=tunnel_num] [ip_address [edns=sw] [nat46=tunnel_num]...]
no dns server [ip_address [edns=sw] [nat46=tunnel_num]...]
```

**[設定値及び初期値]**

- *ip\_address*
  - [設定値]: DNS サーバーの IP アドレス (空白で区切って最大 4 ヶ所まで設定可能)
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 対象の DNS サーバーへの通信を EDNS で行う |
| off | 対象の DNS サーバーへの通信を DNS で行う  |

- [初期値]: off
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

**[説明]**

DNS サーバーの IP アドレスを指定する。

この IP アドレスはルーターが DHCP サーバーとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

nat46 オプションを指定すると DNS46 機能が有効になり、この DNS サーバー宛ての A レコードの問い合わせを AAAA レコードの問い合わせに変換する。

また、DNS サーバーからの応答に含まれる AAAA レコードを、**nat46 ip address pool** コマンドの設定値を使用して A レコードに変換する。変換した A レコードは、DNS キャッシュに登録する。

*tunnel\_num* には、**tunnel translation nat46** コマンドを設定したトンネルインターフェースの番号を指定する。

**[ノート]**

DHCP サーバーから通知された DNS サーバーを使うときには、**dns server dhcp** コマンドを使う。

edns オプションは以下の機種およびリビジョンで使用可能。

NVR700W Rev.15.00.17 以降。

NVR510 Rev.15.01.16 以降。

nat46 オプションは以下の機種およびリビジョンで使用可能。

NVR700W Rev.15.00.23 以降。

NVR510 Rev.15.01.23 以降。

[適用モデル]  
NVR700W, NVR510

## 21.4 DNS ドメイン名の設定

### [書式]

```
dns domain domain_name
no dns domain [domain_name]
```

### [設定値及び初期値]

- *domain\_name*
  - [設定値]: DNS ドメインを表す文字列
  - [初期値]: -

### [説明]

ルーターが所属する DNS ドメインを設定する。

ルーターのホストとしての機能 (ping, traceroute) を使うときに名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。ルーターが DHCP サーバーとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルーターのあるネットワークおよびそれが含むサブネットワークの DHCP クライアントに対して通知する。

空文字列を設定する場合には、**dns domain .** と入力する。

[適用モデル]  
NVR700W, NVR510

## 21.5 DNS サーバーを通知してもらおう相手先情報番号の設定

### [書式]

```
dns server pp peer_num [edns=sw]
no dns server pp [peer_num [edns=sw]]
```

### [設定値及び初期値]

- *peer\_num*
  - [設定値]: DNS サーバーを通知してもらおう相手先情報番号
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 対象の DNS サーバーへの通信を EDNS で行う |
| off | 対象の DNS サーバーへの通信を DNS で行う  |

- [初期値]: off

### [説明]

DNS サーバーを通知してもらおう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の IPCPMS 拡張機能で通知された DNS サーバーに対して問い合わせを行う。

相手先に接続できなかつたり、接続できても DNS サーバーの通知がなかった場合には名前解決は行われない。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

## [ノート]

この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**ppp ipcp msextn** の設定が必要である。

DHCP サーバーから通知された DNS サーバーを使うときには、**dns server dhcp** コマンドを使う。

edns オプションは以下の機種およびリビジョンで使用可能。

NVR510 は Rev.15.01.16 以降。

NVR700W は Rev.15.00.17 以降。

## [設定例]

```
# pp select 2
pp2# ppp ipcp msextn on
pp2# dns server pp 2
```

## [適用モデル]

NVR700W, NVR510

## 21.6 DNS サーバーアドレスを取得するインターフェースの設定

## [書式]

```
dns server dhcp interface [edns=sw]
```

```
no dns server dhcp
```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 対象の DNS サーバーへの通信を EDNS で行う |
| off | 対象の DNS サーバーへの通信を DNS で行う  |

- [初期値]: off

## [説明]

DNS サーバーアドレスを取得するインターフェースを設定する。このコマンドでインターフェース名が設定されていると、DNS で名前解決を行うときに、指定したインターフェースで DHCP サーバーから取得した DNS サーバーアドレスに対して問い合わせを行う。DHCP サーバーから DNS サーバーアドレスを取得できなかった場合は名前解決を行わない。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

## [ノート]

ブリッジインターフェースは NVR700W で指定可能。

この機能は指定したインターフェースが DHCP クライアントとして動作していなければならない。

edns オプションは以下の機種およびリビジョンで使用可能。

NVR510 は Rev.15.01.16 以降。

NVR700W は Rev.15.00.17 以降。

## [適用モデル]

NVR700W, NVR510

## 21.7 DNS サーバーアドレスを取得するインターフェースの設定

### [書式]

```
dns server pdp interface [edns=sw]
```

```
no dns server pdp
```

### [設定値及び初期値]

- *interface*
  - [設定値]: WAN インターフェース名
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 対象の DNS サーバーへの通信を EDNS で行う |
| off | 対象の DNS サーバーへの通信を DNS で行う  |

- [初期値]: off

### [説明]

DNS サーバーアドレスを取得するインターフェースを設定する。

このコマンドでインターフェース名が設定されていると、DNS で名前解決を行うときに指定したインターフェースで

内蔵無線 WAN モジュールから取得した DNS サーバーアドレスに対して問い合わせを行う。

内蔵無線 WAN モジュールから DNS サーバーアドレスを取得できなかった場合は名前解決を行わない。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。

DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

### [ノート]

この機能は指定したインターフェースが内蔵無線 WAN モジュールと Bind されていなければならない。

edns オプションは Rev.15.00.17 以降で使用可能。

### [適用モデル]

NVR700W

## 21.8 DHCP/DHCPv6/IPCP MS 拡張で DNS サーバーを通知する順序の設定

### [書式]

```
dns notice order protocol server [server]
```

```
no dns notice order protocol [server [server]]
```

### [設定値及び初期値]

- *protocol*
  - [設定値]:

| 設定値    | 説明              |
|--------|-----------------|
| dhcp   | DHCP による通知      |
| dhcpv6 | DHCPv6 による通知    |
| msex   | IPCP MS 拡張による通知 |

- [初期値]: dhcp、dhcpv6 および msex

- *server*

- [設定値]:

| 設定値    | 説明                                                                                              |
|--------|-------------------------------------------------------------------------------------------------|
| none   | 一切通知しない                                                                                         |
| me     | 本機自身                                                                                            |
| server | <b>dns server</b> コマンドに設定したサーバー群、 <i>protocol</i> に <i>dhcpv6</i> を指定した場合に DHCPv6 で割り当てられたサーバー群 |

- [初期値]:
  - me server (*protocol* が *dhcp* または *msex* の場合)
  - me (*protocol* が *dhcpv6* の場合)

[説明]

DHCP や DHCPv6、IPCP MS 拡張では DNS サーバーを複数通知できるが、それをどのような順序で通知するかを設定する。

*server* に none を設定した場合、他の設定に関わらず DNS サーバーの通知を行わなくなる。

*server* に me を設定した場合、本機自身の DNS リカーシブサーバー機能を使うことを通知する。

*server* に server を設定した場合、*protocol* に *dhcp* または *msex* を指定したときは **dns server** コマンドに設定したサーバー群を通知し、*protocol* に *dhcpv6* を指定したときは、IPv6 網から DHCPv6 で通知された DNS サーバー群を通知する。

*protocol* に *dhcpv6* を指定したときは、IPv6 網と連動できない環境では、*server* の設定値にかかわらず、ルーターが IPv6 DNS サーバーアドレスを一切通知しない。

IPCP MS 拡張では通知できるサーバーの数が最大 2 に限定されているので、後ろに me が続く場合は先頭の 1 つだけと本機自身を、*server* 単独で設定されている場合には先頭の 2 つだけを通知する。

[ノート]

*dhcpv6* パラメーターは、NVR700W は、Rev.15.00.17 以降、NVR510 は、Rev.15.01.16 以降で指定可能。

[適用モデル]

NVR700W, NVR510

## 21.9 プライベートアドレスに対する問い合わせを処理するか否かの設定

[書式]

**dns private address spoof** *spoof*

**no dns private address spoof** [*spoof*]

[設定値及び初期値]

- *spoof*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 処理する  |
| off | 処理しない |

- [初期値]: off

[説明]

on の場合、DNS リカーシブサーバー機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバーに問い合わせを転送することなく、自分でその問い合わせに対し“NXDomain”、すなわち「そのようなレコードはない」というエラーを返す。

[適用モデル]

NVR700W, NVR510

## 21.10 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定

[書式]

**dns service aaaa filter** *switch*

```
no dns service aaaa filter [switch]
```

#### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | AAAA レコードの問い合わせを制限する  |
| off | AAAA レコードの問い合わせを制限しない |

- [初期値]: off

#### [説明]

DNS サーバーへの AAAA レコードの問い合わせを制限するか否かを設定する。

IPv6 での接続環境がないのに AAAA レコードが引けてしまうことで、接続に失敗するような場合は、このコマンドにより AAAA レコードの問い合わせに対して、AAAA レコードを回答しないようにする。

本機が DNS リレーサーバーになっている通信及び本機発の通信が影響を受ける。

#### [適用モデル]

NVR700W, NVR510

## 21.11 SYSLOG 表示で DNS により名前解決するか否かの設定

#### [書式]

```
dns syslog resolv resolv
```

```
no dns syslog resolv [resolv]
```

#### [設定値及び初期値]

- *resolv*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 解決する  |
| off | 解決しない |

- [初期値]: off

#### [説明]

SYSLOG 表示で DNS により名前解決するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 21.12 DNS 問い合わせの内容に応じた DNS サーバーの選択

#### [書式]

```
dns server select id server [edns=sw] [nat46=tunnel_num] [server2 [edns=sw]] [nat46=tunnel_num] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id pp peer_num [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id dhcp interface [edns=sw] [nat46=tunnel_num] [default-server [edns=sw]] [nat46=tunnel_num] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id pdp wan_interface [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id reject [type] query [original-sender]
```

```
no dns server select id
```

#### [設定値及び初期値]

- *id*
- [設定値]: DNS サーバー選択テーブルの番号
- [初期値]: -



- *server*
  - [設定値]: プライマリ DNS サーバーの IP アドレス
  - [初期値]: -
- *server2*
  - [設定値]: セカンダリ DNS サーバーの IP アドレス
  - [初期値]: -
- *type*: DNS レコードタイプ
  - [設定値]:

| 設定値   | 説明                |
|-------|-------------------|
| a     | ホストの IP アドレス      |
| aaaa  | ホストの IPv6 アドレス    |
| ptr   | IP アドレスの逆引き用のポインタ |
| mx    | メールサーバー           |
| ns    | ネームサーバー           |
| cname | 別名                |
| any   | すべてのタイプにマッチする     |
| 省略    | 省略時は a            |

- [初期値]: -
- *query*: DNS 問い合わせの内容
  - [設定値]:

| 設定値                                  | 説明                                                                                                                                                                                                                                                                   |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>type</i> が a、aaaa、mx、ns、cname の場合 | <i>query</i> はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp" であれば、rtpro.yamaha.co.jp などにマッチする。"." を指定するとすべてのドメイン名にマッチする。                                                                                                                                                  |
| <i>type</i> が ptr の場合                | <i>query</i> は IP アドレス ( <i>ip_address</i> [/ <i>masklen</i> ]) であり、 <i>masklen</i> を省略したときは IP アドレスにのみマッチし、 <i>masklen</i> を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる .in-addr.arpa ドメインで記述された FQDN は、IP アドレスへ変換された後に比較される。すべての IP アドレスにマッチする設定はできない。 |
| reject キーワードを指定した場合                  | <i>query</i> は完全一致とし、前方一致、及び後方一致には "*" を用いる。つまり、前方一致では、"NetVolante.*" であれば、NetVolante.jp、NetVolante.rtpro.yamaha.co.jp などにマッチする。また、後方一致では、"*yamaha.co.jp" と記述する。                                                                                                     |

- [初期値]: -
- *original-sender*
  - [設定値]: DNS 問い合わせの送信元の IP アドレスの範囲
  - [初期値]: -
- *connection-pp*
  - [設定値]: DNS サーバーを選択する場合、接続状態を確認する接続相手先情報番号
  - [初期値]: -
- *peer\_num*
  - [設定値]: IPCP により接続相手から通知される DNS サーバーを使う場合の接続相手先情報番号
  - [初期値]: -
- *interface*

- [設定値]: DHCP サーバーより取得する DNS サーバーを使う場合の LAN インターフェース名、ONU インターフェース名、WAN インターフェース名またはブリッジインターフェース名
- [初期値]: -
- *wan\_interface*
  - [設定値]: 内蔵無線 WAN 経由で DNS サーバーを使う場合の WAN インターフェース名
  - [初期値]: -
- *default-server*
  - [設定値]: *peer\_num* パラメーターで指定した接続相手から DNS サーバーを獲得できなかったときに使う DNS サーバーの IP アドレス
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 対象の DNS サーバーへの通信を EDNS で行う |
| off | 対象の DNS サーバーへの通信を DNS で行う  |

- [初期値]: off
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

DNS 問い合わせの解決を依頼する DNS サーバーとして、DNS 問い合わせの内容および DNS 問い合わせの送信元および回線の接続状態を確認する接続相手先情報番号と DNS サーバーとの組合せを複数登録しておき、DNS 問い合わせに応じてその組合せから適切な DNS サーバーを選択できるようにする。テーブルは小さい番号から検索され、DNS 問い合わせの内容に *query* がマッチしたら、その DNS サーバーを用いて DNS 問い合わせを解決しようとする。一度マッチしたら、それ以降のテーブルは検索しない。すべてのテーブルを検索してマッチするものがない場合には、他のコマンドで指定された DNS サーバーを用いる。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

*reject* キーワードを使用した書式の場合、*query* がマッチしたら、その DNS 問い合わせパケットを破棄し、DNS 問い合わせを解決しない。

*restrict pp* 節が指定されていると、*connection-pp* で指定した相手先がアップしているかどうかをサーバーの選択条件に追加される。相手先がアップしていないとサーバーは選択されない。相手先がアップしていて、かつ、他の条件もマッチしている場合に指定したサーバーが選択される。

*edns* オプションを省略、または *edns=off* を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。*edns=on* を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。*edns=on* で名前解決ができない場合、*edns=off* に変更すると名前解決できる場合がある。EDNS はバージョン 0 に対応。

*nat46* オプションを指定すると DNS46 機能が有効になり、この DNS サーバー宛ての A レコードの問い合わせを AAAA レコードの問い合わせに変換する。

また、DNS サーバーからの応答に含まれる AAAA レコードを、*nat46 ip address pool* コマンドの設定値を使用して A レコードに変換する。変換した A レコードは、DNS キャッシュに登録する。

*tunnel\_num* には、*tunnel translation nat46* コマンドを設定したトンネルインターフェースの番号を指定する。

#### [ノート]

第 4 書式、および、ブリッジインターフェースは NVR700W で指定可能。

*edns* オプションは以下の機種およびリビジョンで使用可能。  
NVR700W Rev.15.00.17 以降。  
NVR510 Rev.15.01.16 以降。

*nat46* オプションは以下の機種およびリビジョンで使用可能。

NVR700W Rev.15.00.23 以降。  
NVR510 Rev.15.01.23 以降。

[適用モデル]  
NVR700W, NVR510

## 21.13 静的 DNS レコードの登録

### [書式]

```
ip host fqdn value [ttl=ttl]
dns static type name value [ttl=ttl]
no ip host fqdn [value]
no dns static type name [value]
```

### [設定値及び初期値]

- *type* : 名前のタイプ
- [設定値] :

| 設定値   | 説明                |
|-------|-------------------|
| a     | ホストの IPv4 アドレス    |
| aaaa  | ホストの IPv6 アドレス    |
| ptr   | IP アドレスの逆引き用のポインタ |
| mx    | メールサーバー           |
| ns    | ネームサーバー           |
| cname | 別名                |

- [初期値] : -
- *name*、*value*
- [設定値] :

*type* パラメーターによって以下のように意味が異なる

| <i>type</i> パラメーター | <i>name</i> | <i>value</i> |
|--------------------|-------------|--------------|
| a                  | FQDN        | IPv4 アドレス    |
| aaaa               | FQDN        | IPv6 アドレス    |
| ptr                | IPv4 アドレス   | FQDN         |
| mx                 | FQDN        | FQDN         |
| ns                 | FQDN        | FQDN         |
| cname              | FQDN        | FQDN         |

- [初期値] : -
- *fqdn*
  - [設定値] : ドメイン名を含んだホスト名
  - [初期値] : -
- *ttl*
  - [設定値] : 秒数 (1~4294967295)
  - [初期値] : -

### [説明]

静的な DNS レコードを定義する。

**ip host** コマンドは、**dns static** コマンドで **a** と **ptr** を両方設定することを簡略化したものである。

### [ノート]

問い合わせに対して返される DNS レコードは以下のような特徴を持つ。

- TTL フィールドには、*tll* パラメーターの設定値がセットされる。*tll* パラメーターが省略された時には 1 がセットされる。
- Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
- MX レコードの *preference* フィールドは 0 にセットされる

## [設定例]

```
# ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

## [適用モデル]

NVR700W, NVR510

## 21.14 DNS 問い合わせパケットの始点ポート番号の設定

## [書式]

**dns srcport** *port*[-*port*]**no dns srcport** [*port*[-*port*]]

## [設定値及び初期値]

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 10000-10999

## [説明]

ルーターが送信する DNS 問い合わせパケットの始点ポート番号を設定する。

ポート番号を一つだけしか設定しなかった場合には、指定したポート番号を始点ポートとして利用する。

ポート番号を範囲で指定した場合には、DNS 問い合わせパケットを送信するたびに、範囲内のポート番号をランダムに利用する。

## [ノート]

DNS 問い合わせパケットをフィルターで扱うとき、始点番号がランダムに変化するということを考慮しておく必要がある。

## [適用モデル]

NVR700W, NVR510

## 21.15 DNS サーバーへアクセスできるホストの設定

## [書式]

**dns host** *ip\_range* [*ip\_range*...]**dns host** *any***dns host** *none***dns host** *lan***no dns host**

## [設定値及び初期値]

- *ip\_range*: DNS サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

| 設定値                                                            | 説明                       |
|----------------------------------------------------------------|--------------------------|
| 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの | 指定したホストからのアクセスを許可する      |
| lanN                                                           | LAN インターフェースからのアクセスを許可する |
| onu1                                                           | ONU インターフェースからのアクセスを許可する |
| wan1                                                           | WAN インターフェースからのアクセスを許可する |

| 設定値     | 説明                           |
|---------|------------------------------|
| bridge1 | ブリッジインターフェースからのアクセスを許可する     |
| vlanN   | VLAN インターフェースからのアクセスを許可する    |
| lanN/M  | タグ VLAN インターフェースからのアクセスを許可する |

- [初期値]: -
- *any*
  - [設定値]: すべてのホストからのアクセスを許可する
  - [初期値]: any
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: -
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: -

**[説明]**

DNS サーバー機能へのアクセスを許可するホストを設定する。

**[ノート]**

このコマンドで LAN インターフェースまたは ONU インターフェースを指定した場合には、ネットワークアドレスと limited broadcast address を除く IP アドレスからのアクセスを許可する。指定した LAN インターフェースと ONU インターフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 21.16 DNS キャッシュを使用するか否かの設定

**[書式]**

```
dns cache use switch
no dns cache use [switch]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | DNS キャッシュを利用する  |
| off | DNS キャッシュを利用しない |

- [初期値]: on

**[説明]**

DNS キャッシュを利用するか否かを設定する。

*switch* を on に設定した場合、DNS キャッシュを利用する。すなわち、ルーターが送信した DNS 問い合わせパケットに対する上位 DNS サーバーからの返答をルーター内部に保持し、次に同じ問い合わせが発生したときでも、サーバーには問い合わせず、キャッシュの内容を返す。

上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。

ルーター内部に保持する DNS エントリの数は **dns cache max entry** コマンドで設定する。

*switch* を off にした場合、DNS キャッシュは利用しない。ルーターが送信した DNS 問い合わせパケットに対する上

位 DNS サーバーからの返答はルーター内部に保持せず、同じ問い合わせがあっても毎回 DNS サーバーに問い合わせを行う。

[適用モデル]  
NVR700W, NVR510

## 21.17 DNS キャッシュの最大エントリ数の設定

[書式]

```
dns cache max entry num
no dns cache max entry [num]
```

[設定値及び初期値]

- *num*
  - [設定値]: 最大エントリ数 (1...1024)
  - [初期値]: 256

[説明]

DNS キャッシュの最大エントリ数を設定する。

設定した数だけ、ルーター内部に DNS キャッシュとして上位 DNS サーバーからの返答を保持できる。設定した数を超えた場合、返答が返ってきた順で古いものから破棄される。

上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。返答が得られてから保持時間を経過したエントリは、DNS キャッシュから削除される。

[適用モデル]  
NVR700W, NVR510

## 21.18 DNS フォールバック機能を使用するか否かの設定

[書式]

```
dns service fallback switch
no dns service fallback [switch]
```

[設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | DNS フォールバック機能を使用する  |
| off | DNS フォールバック機能を使用しない |

- [初期値]: off

[説明]

DNS フォールバック機能を使用するか否かを設定する。

DNS フォールバック機能を使用する場合は、DNS サーバーへ FQDN から IP アドレスを問い合わせるとき、AAAA レコードによるクエリーを優先する。

AAAA レコードに対応した IPv6 アドレスが無かった場合、または DNS サーバーへ問い合わせを行った機能の処理中にエラーが発生した場合、DNS サーバーに A レコードによるクエリーを行い、A レコードに対応した IPv4 アドレスがあった場合にその IP アドレスをクライアントへ返すよう切り替える。

[適用モデル]  
NVR700W, NVR510

## 第 22 章

### NAT46/DNS46 機能

NAT46/DNS46 機能とは、IPv4 パケットを IPv6 パケットに変換して転送する機能です。

本来、IP バージョンが異なるネットワークにあるホスト同士では、通信ができません。しかし、本機能を利用すると、LAN が IPv4 ネットワーク、WAN が IPv6 ネットワークという構成において、LAN にある PC から WAN にあるサーバーへのアクセスが可能になります。

既に IPv4 アドレスで構築された LAN を変更することなく、IPv6 アドレスで提供されているサービスを利用できます。

#### 22.1 NAT46 機能で使用する IPv4 アドレスプールの設定

##### [書式]

```
nat46 ip address pool ipaddress_list  
no nat46 ip address pool [ipaddress_list]
```

##### [設定値及び初期値]

- *ipaddress\_list*
  - [設定値]: 1 個の IPv4 アドレスまたは間に - をはさんだ IPv4 アドレス (範囲指定)、または、IPv4 ネットワークアドレス、および、これらを任意に並べたもの
  - [初期値]: -

##### [説明]

NAT46 機能で IPv4 アドレスを IPv6 アドレスに変換するために使用する IPv4 アドレスのプールを設定する。

DNS46 機能が AAAA レコードを A レコードに変換するとき、AAAA レコードの IPv6 アドレスを当コマンドで設定した範囲内の IPv4 アドレスに変換する。

DNS46 機能で行われた IPv4 アドレスと IPv6 アドレスとの対応づけは、以降の通信において NAT46 機能が IP ヘッダーを変換する際に使用する。

*ipaddress\_list* は 8 個まで設定可能。ただし、*ipaddress\_list* に含まれる IPv4 アドレスの合計が 254 個を超えた場合はコマンドエラーとなる。

##### [ノート]

tunnel translation コマンドで変換種別として nat46 を選択した場合だけ有効である。

NVR700W Rev.15.00.23 以降で使用可能。

NVR510 Rev.15.01.23 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

#### 22.2 NAT46 機能で使用する IPv6 プレフィックスの設定

##### [書式]

```
nat46 ipv6 prefix prefix_id  
no nat46 ipv6 prefix [prefix_id]
```

##### [設定値及び初期値]

- *prefix\_id*
  - [設定値]: プレフィックス番号 (1..4294967295)
  - [初期値]: -

##### [説明]

NAT46 機能で送信元 IPv4 アドレスを送信元 IPv6 アドレスに変換するために使用するプレフィックスを設定する。

ipv6 prefix コマンドで設定したプレフィックス番号を指定する。

**[ノート]**

本コマンドで指定する `ipv6 prefix` コマンドのプレフィックスは以下の条件を満たす必要がある。

- プレフィックス長が /96 であること
- XXXX:XXXX:XXXX:XXXX:YYXX:XXXX:0000:0000/96 : 64 ~ 71 ビット目 (YY) が 0 であること

NVR700W Rev.15.00.23 以降で使用可能。

NVR510 Rev.15.01.23 以降で使用可能。

**[設定例]**

LAN2 で受信した /64 の RA のプレフィックスから、NAT46 機能で使用する IPv6 プレフィックスを設定する。

RA で配られる プレフィックス(/64) : XXXX:XXXX:XXXX:XXXX:0000:0000:0000:0000/64

IPv4 アドレスに付与するプレフィックス : XXXX:XXXX:XXXX:XXXX:0000:0000:0000:0000/96

IPv6 アドレスに変換された IPv4 アドレス : XXXX:XXXX:XXXX:XXXX:0000:0000:YYY.YYY.YYY.YYY

```
# ipv6 prefix 1 ra-prefix@lan2::/96
# nat46 ipv6 prefix 1
```

**[適用モデル]**

NVR700W, NVR510

## 22.3 NAT46 機能で使用する宛先アドレスを静的に対応づける設定

---

**[書式]**

```
nat46 static id ipv4_address ipv6_address
```

```
no nat46 static id [ipv4_address] ipv6_address
```

**[設定値及び初期値]**

- *id*
  - [設定値]: 識別情報 ( 1..2147483647 )
  - [初期値]: -
- *ipv4\_address*
  - [設定値]: IPv4 アドレス ( 1 個 )
  - [初期値]: -
- *ipv6\_address*
  - [設定値]: IPv6 アドレス ( 1 個 )
  - [初期値]: -

**[説明]**

NAT46 機能で使用する宛先の IPv6 アドレスに対応する IPv4 アドレスを静的に設定する。

宛先にホスト名ではなく IPv4 アドレスを指定してアクセスする場合 ( DNS46 機能で名前解決させずに NAT46 機能を使用する場合 ) に設定する。

**[ノート]**

`nat46 ip address pool` コマンドで設定している IPv4 アドレスとは異なるアドレスを設定する必要がある。

NVR700W Rev.15.00.23 以降で使用可能。

NVR510 Rev.15.01.23 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 22.4 NAT46 エントリーの表示

---

**[書式]**

```
show status nat46 table [tunnel tunnel_num] [type]
```



**[設定値及び初期値]**

- *tunnel\_num* : トンネルインターフェース番号
  - [初期値] : -
- *type*
  - [設定値] :

| 設定値     | 説明                      |
|---------|-------------------------|
| static  | 静的エントリーの情報を表示する         |
| dynamic | 動的エントリーの情報を表示する         |
| all     | 静的エントリーと動的エントリーの情報を表示する |

- [初期値] : all

**[説明]**

NAT46 エントリーを表示する。TYPE を省略した場合は、静的エントリーと動的エントリーの情報を表示する。

**[ノート]**

NVR700W Rev.15.00.23 以降で使用可能。  
NVR510 Rev.15.01.23 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 第 23 章

### 優先制御／帯域制御

優先制御と帯域制御の機能は、インターフェースに入力されたパケットの順序を入れ換えて別のインターフェースに出力します。これらの機能を使用しない場合には、パケットは入力した順番に処理されます。

優先制御は、クラス分けしたキューに優先順位をつけ、まず高位のキューのパケットを出力し、そのキューが空になると次の順位のキューのパケットを出力する、という処理を行います。

帯域制御は、クラス分けしたキューをラウンドロビン方式で監視しますが、監視頻度に差を与えてキューごとに利用できる帯域に差をつけます。

帯域制御は NVR700W で使用可能です。

クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。帯域制御では 1 から 16 までのクラスが使用できます。優先制御では 1 から 4 までのクラスが使用できます。クラスは番号が大きいほど優先順位が高くなります。

パケットの処理アルゴリズムは、**queue interface type** コマンドにより、NVR700W では優先制御、帯域制御、単純 FIFO、NVR510 では優先制御、単純 FIFO の中から選択します。これはインターフェースごとに選択することができます。

#### 23.1 インターフェース速度の設定

##### [書式]

```
speed interface speed
no speed interface [speed]
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *speed*
  - [設定値]: インターフェース速度 (bit/s)
  - [初期値]: -

##### [説明]

指定したインターフェースに対して、インターフェースの速度を設定する。

**queue interface type** コマンドで **priority** および **shaping** を指定しているときのみ有効となる。

##### [ノート]

*speed* パラメーターの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。

##### [適用モデル]

NVR700W, NVR510

#### 23.2 クラス分けのためのフィルター設定

##### [書式]

```
queue class filter num class [cos=cos] ip src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num class [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip src_addr [dest_addr [protocol
[src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 src_addr [dest_addr [protocol
[src_port [dest_port]]]]
queue class filter num class1 ip dpi src_addr [dest_addr [application]]
queue class filter num class1 ipv6 dpi src_addr [dest_addr [application]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr
[application]]
```

```

queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr
[application]]
queue class filter num class1 ip dpi src_addr [dest_addr [group_num]]
queue class filter num class1 ipv6 dpi src_addr [dest_addr [group_num]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr
[group_num]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr
[group_num]]
no queue class filter num [...]
    
```

**[設定値及び初期値]**

- *num*
  - [設定値]: クラスフィルターの識別番号 (1..100)
  - [初期値]: -
- *class*
  - [設定値]: クラス (1..16)
  - [初期値]: -
- *prec*
  - [設定値]: precedence 値 (0..7)
  - [初期値]: -
- *cos*
  - [設定値]:

| 設定値        | 説明                                                         |
|------------|------------------------------------------------------------|
| 0-7        | CoS 値                                                      |
| precedence | 転送するパケットの TOS の precedence(0-7) を ToS-CoS 変換として COS 値に格納する |

- [初期値]: -
- *src\_addr*: IP パケットの始点アドレス
  - [設定値]:
    - IP アドレス
      - A.B.C.D (A~D: 0~255 もしくは\*)
        - 上記表記で A~D を\*とすると、該当する 8 ビット分についてはすべての値に対応する
      - IPv6 アドレス
      - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
      - , を区切りとして複数設定することができる。
    - FQDN
      - 任意の文字列 (半角 255 文字以内。 / : は使用できない。 , は区切り文字として使われるため、使用できない)
      - \* から始まる FQDN は \* より後ろの文字列を後方一致条件として判断する 例えば \*.example.co.jp は www.example.co.jp、mail.example.co.jp などと一致する
      - , を区切りとして複数設定することができる。
      - \* (すべての IP アドレスまたは IPv6 アドレスに対応)
  - [初期値]: -
- *dest\_addr*: IP パケットの終点アドレス
  - [設定値]:
    - *src\_addr* と同じ形式
    - 省略した場合は一個の \* と同じ
  - [初期値]: -
- *protocol*: フィルタリングするパケットの種類
  - [設定値]:
    - プロトコルを表す十進数
    - プロトコルを表すニーモニック

|      |    |
|------|----|
| icmp | 1  |
| tcp  | 6  |
| udp  | 17 |

- 上項目のカンマで区切った並び (5 個以内)
- \*(すべてのプロトコル)
- established
- 省略時は \* と同じ
- [初期値]: -
- *src\_port*: UDP、TCP のソースポート番号
- [設定値]:
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック (一部)

| ニーモニック     | ポート番号 |
|------------|-------|
| ftp        | 20,21 |
| ftpdata    | 20    |
| telnet     | 23    |
| smtp       | 25    |
| domain     | 53    |
| gopher     | 70    |
| finger     | 79    |
| www        | 80    |
| pop3       | 110   |
| sunrpc     | 111   |
| ident      | 113   |
| ntp        | 123   |
| nntp       | 119   |
| snmp       | 161   |
| syslog     | 514   |
| printer    | 515   |
| talk       | 517   |
| route      | 520   |
| uucp       | 540   |
| submission | 587   |

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- \*(すべてのポート)
- 省略時は \* と同じ。
- [初期値]: -
- *dest\_port*: UDP、TCP のディスティネーションポート番号
  - [設定値]: *src\_port* と同じ形式
  - [初期値]: -
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
  - [設定値]:
    - アプリケーションを表すニーモニック
    - "@" で始まるカテゴリーを表すニーモニック

- 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリーの混在が可能)
- 省略時は 1 つの \* と同じ
- [初期値]: -
- `group_num`: グループ ID
  - [設定値]: `dpi group set` コマンドでグループ化したアプリケーションのグループ ID
  - [初期値]: -

**[説明]**

クラス分けのためのフィルターを設定する。

`precedence` 形式の場合、転送するパケットの TOS フィールドの `precedence(0-7)` に応じてクラス (1-8) を分けて優先制御もしくはシェーピング、Dynamic Traffic Control による帯域制御を行う。 `precedence` 値からクラスへの変換は、`mapping` オプションにより指定できる。例えば、以下の例では `precedence` 値=1 をクラス 8 に、 `precedence` 値=4 をクラス 3 に変換する。

`queue class filter 1 precedence mapping=1:8,4:3 ip *`

`mapping` オプション全体を省略した場合、あるいは `mapping` オプションは指定しているものの、その中で記述しなかった `precedence` 値については以下の表のような変換が行われる。

|              |   |   |   |   |   |   |   |   |
|--------------|---|---|---|---|---|---|---|---|
| precedence 値 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| クラス          | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

`cos=cos` 指定を行うと、フィルターに合致したパケットに付加される IEEE802.1Q タグの `user_priority` フィールドには、指定した CoS 値が格納される。 `cos` に `precedence` を指定した場合、そのパケットの IP ヘッダの `precedence` 値に対応する値が `user_priority` フィールドに格納される。

パケットフィルターに該当したパケットは、指定したクラスに分類される。このコマンドで設定したフィルターを使用するかどうか、あるいはどのような順番で適用するかは、各インターフェースにおける `queue interface class filter list` コマンドで設定する。

`application`、または、`group_num` を指定した場合、DPI のアプリケーション識別結果を利用したクラス分けが行われる。アプリケーションの識別が完了したパケットは、直ちに指定のクラスに分類されるようになる。識別処理中のパケットや DPI がアクティベーション中で識別されなかったパケットは、DPI のフィルターにはマッチせず、通常の設定に従ってクラスに分類される。

**[ノート]**

第 3 書式、および、第 4 書式は NVR700W で指定可能。  
`application` パラメータ、および `group_num` パラメータは、NVR700W の Rev.15.00.17 以降で指定可能。

`src_addr` および `dest_addr` への FQDN の指定は NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.13 以降のファームウェアで指定可能。

**[設定例]**

```
# queue class filter 1 4 ip * *udp 5004-5060 *
# queue class filter 2 10 ip * 172.16.1.0/24 tcp telnet *
# queue class filter 3 precedence ip 172.16.5.0/24 * tcp * *
# queue class filter 4 precedence ip * 172.16.6.0/24 tcp * *
# queue class filter 12 4 ip dpi * * @audio_video
```

**[適用モデル]**

NVR700W, NVR510

## 23.3 キューイングアルゴリズムタイプの選択

**[書式]**

- `queue interface type type [shaping-level=level]`
- `queue pp type type`
- `no queue interface type [type]`
- `no queue pp type [type]`

**[設定値及び初期値]**

- `interface`
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名

- [初期値]: -
- *type*
- [設定値]:

| 設定値      | 説明                           |
|----------|------------------------------|
| fifo     | First In,First Out 形式のキューイング |
| priority | 優先制御キューイング                   |
| shaping  | 帯域制御                         |

- [初期値]: fifo
- *level*: 帯域速度の計算を行うレイヤー
- [設定値]:

| 設定値 | 説明     |
|-----|--------|
| 1   | レイヤー 1 |
| 2   | レイヤー 2 |

- [初期値]: 2

#### [説明]

指定したインターフェースに対して、キューイングアルゴリズムタイプを選択する。

fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルーターに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が **queue interface length** コマンドで指定した値を越えた場合、キューの最後尾、つまり最後に到着したパケットが破棄される。

priority は優先制御を行う。**queue class filter** コマンドおよび **queue interface class filter list** コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。

shaping は LAN インターフェースまたは ONU インターフェースに対する帯域制御を行う。LAN インターフェースまたは ONU インターフェースにだけ設定できる。

shaping-level オプションは TYPE パラメーターに priority および shaping を指定しているときのみ指定可能。

shaping-level に 1 を設定した場合、帯域速度の計算をプリアンブル、SFD(Start Frame Delimiter)、IFG(Inter Frame Gap)を含んだフレームサイズでおこなう。

#### [ノート]

shaping は NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 23.4 クラス分けフィルターの適用

#### [書式]

```
queue interface class filter list filter_list
queue pp class filter list filter_list
queue tunnel class filter list filter_list
no queue interface class filter list [filter_list]
no queue pp class filter list [filter_list]
no queue tunnel class filter list [filter_list]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *filter\_list*
  - [設定値]: 空白で区切られたクラスフィルターの並び
  - [初期値]: -

**[説明]**

指定した LAN インターフェース、ONU インターフェース、WAN インターフェースまたは選択されている PP、トンネルに対して、**queue class filter** コマンドで設定したフィルターを適用する順番を設定する。フィルターにマッチしなかったパケットは、**queue interface default class** コマンドで指定したデフォルトクラスに分類される。

**[ノート]**

第 3 書式は NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 23.5 クラス毎のキュー長の設定

---

**[書式]**

```
queue interface length len1 [len2...len16]
```

```
queue pp length len1 [len2...len16]
```

```
no queue interface length [len1...]
```

```
no queue pp length [len1...]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *len1..len16*
  - [設定値]: クラス 1 からクラス 16 のキュー長 (1..10000)
  - [初期値]:
    - 200 (LAN/ONU/WAN)
    - 20 (PP)

**[説明]**

インターフェースに対して、指定したクラスのキューに入れることができるパケットの個数を指定する。指定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

**[適用モデル]**

NVR700W, NVR510

## 23.6 デフォルトクラスの設定

---

**[書式]**

```
queue interface default class class
```

```
queue pp default class class
```

```
queue tunnel default class class
```

```
no queue interface default class [class]
```

```
no queue pp default class [class]
```

```
no queue tunnel default class [class]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *class*
  - [設定値]: クラス (1..16)
  - [初期値]: 2

**[説明]**

インターフェースに対して、フィルターにマッチしないパケットをどのクラスに分類するかを指定する。第 3、第 6 書式は NVR700W は Rev.15.00.22 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W, NVR510

## 23.7 クラスの属性の設定

---

### [書式]

```
queue interface class property class bandwidth=bandwidth
no queue interface class property class [bandwidth=bandwidth...]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *class*
  - [設定値]: クラス (1..16)
  - [初期値]: -
- *bandwidth*
  - [設定値]:
    - クラスに割り当てる帯域 (bit/s)
    - 数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値の後ろに '%' をつけると、回線全体の帯域に対するパーセンテージとなる。
    - 'ngn' を設定した場合はデータコネク ト拠点間接続の接続時に決めた帯域に設定される。
  - [初期値]: -

### [説明]

指定したクラスの属性を設定する。

### [ノート]

*bandwidth* パラメーターで各クラスに割り当てる帯域の合計は、回線全体の帯域を越えてはいけない。回線全体の帯域は、**speed** コマンドで設定される。'ngn' を指定した場合は、データコネク ト拠点間接続で接続時に決まる帯域に自動的に設定される。複数のデータコネク ト拠点間接続を利用する場合は、トンネルインターフェース毎にクラスを分ける必要がある。また、**tunnel ngn interface** コマンドで使用する LAN インターフェースまたは ONU インターフェースを設定する必要がある。

**queue interface type** コマンドで **shaping** が指定されている場合は、Dynamic Traffic Control による帯域制御を行うことが可能である。Dynamic Traffic Control を行うためには、*bandwidth* パラメーターに「,」（コンマ）でつないだ2つの速度を指定することで、保証帯域と上限帯域を設定する。記述順に関係なく、常に値の小さな方が保証帯域となる。なお、保証帯域の合計が回線全体の帯域を越えてはいけない。

このコマンドが設定されていないクラスには、常に 100% の帯域が割り振られている。そのため、帯域制御の設定をする場合には最低限でも対象としているクラスと、デフォルトクラスの2つに関してこのコマンドを設定しなくてはならない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。

[適用モデル]  
NVR700W

## 23.8 動的なクラス変更 (Dynamic Class Control) の設定

---

### [書式]

```
queue interface class control class [except ip_address ...] [option=value ...]
no queue interface class control class [except ip_address...]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *class*
  - [設定値]: DCC を有効にするクラス (1..16)
  - [初期値]: -



- `ip_address`
- [設定値]:

| 設定値     | 説明                                                                     |
|---------|------------------------------------------------------------------------|
| IP アドレス | サーバーなどの監視対象から除外するホストの IP アドレスを設定する (空白で区切って複数指定可能、ハイフン「-」を使用して範囲指定も可能) |

- [初期値]: -
- `option = value` 列
- [設定値]:

| option     | value              | 説明                                                               |
|------------|--------------------|------------------------------------------------------------------|
| forwarding | reject, 1..16      | 過剰送信と見なしたトラフィックの転送先のクラス                                          |
| watch      | source             | 送信元 IP アドレス単位で帯域を監視する                                            |
|            | destination        | 宛先 IP アドレス単位で帯域を監視する                                             |
| threshold  | 占有率, 秒数            | 過剰送信と見なす閾値を帯域の占有率と占有時間をカンマ「,」で結び設定する (占有率 1%..100%、秒数 10..86400) |
| time       | infinity           | 過剰送信と見なしたトラフィックを遮断する時間、または、使用するクラスを変更する時間 (秒)                    |
|            | 10..604800         |                                                                  |
| mode       | forced             | 動作モードを強制制御モードにする                                                 |
|            | adaptive           | 動作モードを適応制御モードにする                                                 |
| trigger    | winny              | Winny 検知をトリガとして制御を開始する                                           |
|            | share              | Share 検知をトリガとして制御を開始する                                           |
|            | masquerade-session | IP マスカレード変換セッション数制限をトリガとして制御を開始する                                |
| notice     | on                 | 制御されていることを通知する                                                   |
|            | off                | 制御されていることを通知しない                                                  |

- [初期値]:
  - watch=source
  - threshold=70%,30
  - time=600
  - mode=forced
  - notice=on

**[説明]**

指定したインターフェースについて、同一のホストが過剰な送信/受信を行い、帯域を逼迫していないか監視をする。監視対象のインターフェースに適用されている QoS 種別が `shaping` の場合は、`queue interface class property` コマンドで設定されたクラス帯域に対する占有率 (クラス帯域に保証値と上限値を指定している場合は保証値に対する占有率) を監視する。QoS 種別が `priority` の場合は、インターフェース帯域に対する占有率を監視する。監視時は 10 秒毎に占有率を求め、その占有率が指定秒数を越えたときに閾値超過と判定される。例えば、`threshold=70%,30` と設定した場合、帯域使用率 70% 以上である 10 秒間が連続して 3 回続いたときに閾値超過と判定される。

同一のホストから (*watch=source*)、あるいは、同一のホスト宛て (*watch=destination*) の過剰送信を検知した場合、そのトラフィックは *forwarding* パラメーターに指定されたクラスへ転送され、転送先のクラス設定に従ってパケットの送出行われる。なお、*forwarding* パラメーターに *reject* を指定した場合、当該トラフィックは遮断される。また、*forwarding* パラメーターは省略することも可能で、この場合転送制御は行われませんが、*threshold* を超過しているホストを **show status qos** コマンドから確認することができる。

*time* パラメーターは転送制御が行われる時間を示し、*infinity* を指定した場合は、無期限に対象のトラフィックの遮断、または、使用クラスの変更がなされる。

*mode* パラメーターは動作モードを指定する。*forced* を指定した場合は、*threshold* パラメーターで指定した占有時間が経過したら直ちに当該フローの制御を実行する。また、*time* パラメーターで指定した制御時間が経過したら直ちに当該フローの制御を解除する。*adaptive* を指定した場合は、*threshold* パラメーターで指定した占有時間が経過しても当該クラスの使用帯域が保証帯域の 90% 未満である間は制御を保留する。また、*time* パラメーターで指定した制御時間が経過しても当該クラスの使用帯域が保証帯域の 90% 以上である間は制御解除を保留する。制御が保留されているホストは **show status qos** コマンドで表示されず、制御が保留されている間に *threshold* の占有率を割ったらその時点で制御は解除される。

*trigger* パラメーターは制御開始のトリガとなるルーター内部のイベントを指定する。カンマ「,」で区切って併記することができる。

*notice* パラメーターは Dynamic Class Control により制御されていることをホストに通知するかどうかを指定する。*on* を指定した場合は、当該ホストが制御されてから初めていずれかの **http** サーバー(ポート番号: 80) へ Web アクセスをした時に、Web 画面上にその旨を表示して通知する。

#### [ノート]

トラフィックの転送は 1 段のみ可能である。転送先のクラスにも当コマンドが設定されている場合、2 段目の設定は無効となり、トラフィックの 2 重転送は行われぬ。

#### [適用モデル]

NVR700W

## 第 24 章

### 連携機能

#### 24.1 連携動作を行うか否かの設定

##### [書式]

**cooperation** *type* *role* *sw*

**no cooperation** *type* *role* [*sw*]

##### [設定値及び初期値]

- *type* : 連携動作タイプ

- [設定値] :

| 設定値                 | 説明     |
|---------------------|--------|
| bandwidth-measuring | 回線帯域検出 |
| load-watch          | 負荷監視通知 |

- [初期値] : -

- *role* : 連携動作での役割

- [設定値] :

| 設定値    | 説明        |
|--------|-----------|
| server | サーバー側動作   |
| client | クライアント側動作 |

- [初期値] : -

- *sw*

- [設定値] :

| 設定値 | 説明       |
|-----|----------|
| on  | 機能を有効にする |
| off | 機能を無効にする |

- [初期値] : すべての連携動作で off

##### [説明]

連携動作の機能毎の動作を設定する。

##### [適用モデル]

NVR700W, NVR510

#### 24.2 連携動作で使用するポート番号の設定

##### [書式]

**cooperation** *port* *port*

**no cooperation** *port* [*port*]

##### [設定値及び初期値]

- *port*

- [設定値] : ポート番号

- [初期値] : 59410

##### [説明]

連携動作で使用する UDP のポート番号を設定する。連携動作で送出されるパケットの送信元ポート番号にこの番号を使用する。またこのポート番号宛のパケットを受信した場合には連携動作に関わるパケットとして処理する。

##### [適用モデル]

NVR700W, NVR510

## 24.3 帯域測定で連携動作を行う相手毎の動作の設定

### [書式]

```
cooperation bandwidth-measuring remote id role address [option=value]
```

```
no cooperation bandwidth-measuring remote id [role address [option=value]]
```

### [設定値及び初期値]

- *id*
  - [設定値]: 相手先 ID 番号 (1..100)
  - [初期値]: -
- *role*: 連携動作での相手側の役割
  - [設定値]:

| 設定値    | 説明               |
|--------|------------------|
| server | 相手側がサーバー側動作を行う   |
| client | 相手側がクライアント側動作を行う |

- [初期値]: -
- *address*
  - [設定値]: 連携動作の相手側 IP アドレス、FQDN または 'any'
  - [初期値]: -
- *option*: オプション
  - [設定値]:

| 設定値            | 説明                                                                         |
|----------------|----------------------------------------------------------------------------|
| apply          | 測定結果を LAN インターフェース、ONU インターフェース、または WAN インターフェースの速度設定に反映させるか否か、'on'or'off' |
| port           | 相手側が使用する UDP のポート番号 (1-65535)                                              |
| initial-speed  | 測定開始値 (64000-100000000)[bit/s]                                             |
| interval       | 定期監視間隔 (60..2147483647)[sec]or'off'                                        |
| retry-interval | エラー終了後の再試行までの間隔 (60..2147483647)[sec]                                      |
| sensitivity    | 測定感度、'high','middle'or'low'                                                |
| syslog         | 動作をログに残すか否か、'on'or'off'                                                    |
| interface      | 測定結果を反映させる LAN インターフェース、ONU インターフェース、または WAN インターフェース                      |
| class          | 測定結果を反映させるクラス                                                              |
| limit-rate     | 設定値の最大変化割合 (1-10000)[%]                                                    |
| number         | 測定に使用するパケット数 (5..100)                                                      |
| local-address  | パケット送信時の始点 IP アドレス                                                         |

- [初期値]:
  - apply=on
  - port=59410
  - initial-speed=10000000
  - interval=3600
  - retry-interval=3600
  - sensitivity=high
  - syslog=off
  - number=30

### [説明]

帯域測定で連携動作を行う相手毎の動作を設定する。

## [ノート]

`role` パラメーターで `client` を設定する場合には、オプションは `port` と `syslog` だけが設定できる。`server` を設定する場合には全てのオプションが設定できる。

連携動作の相手側設定として `any` を指定できるのは、`role` パラメーターで `client` を設定した場合のみである。

`apply` オプションが 'on' の場合、帯域測定の結果を相手先に向かう LAN インターフェースの `speed lan` コマンドの設定値、ONU インターフェースの `speed onu1` コマンドの設定値、または WAN インターフェースの `speed wan1` コマンドの設定値に書きする。`class` オプションに値が設定されている場合には、`queue lan class property` コマンドの `bandwidth` パラメーター、または `queue wan1 class property` コマンドの `bandwidth` パラメーターに測定結果が反映される。

`initial-speed` オプションでは初期状態で測定を開始する速度を設定できる。パラメーターの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。

`retry-interval` オプションでは、帯域測定が相手先からの応答がなかったり測定値が許容範囲を越えたなど、何らかの障害で正しい測定ができなかった場合の再試行までの時間を設定できる。ただし、網への負荷等を考慮すると正常に動作できない状況でむやみに短時間間隔で試行を繰り返すべきではない。正常に測定できない原因を回避することが先決である。

`number` オプションでは、測定に使用するパケット数を設定できる。パケット間隔のゆらぎが大きい環境ではこの数を多くすることで、より安定した結果が得られる。ただし測定に使用するパケットの数が増えるため測定パケットが他のデータ通信に与える影響も大きくなる可能性がある。

`sensitivity` オプションでは、測定感度を変更することができる。パケット間隔のゆらぎが大きかったりパケットロスのある環境では、測定感度を鈍くすることで、頻繁な設定変更を抑制したり測定完了までの時間を短縮することができる。

`interface` オプションで LAN インターフェースが設定されている場合には、その LAN インターフェースの `speed lan` コマンドに測定結果が反映される。`class` オプションに値が設定されている場合には `queue lan class property` コマンドの `bandwidth` パラメーターに測定結果が反映される。ONU インターフェースが設定されている場合には、`speed onu1` コマンドに測定結果が反映される。`class` オプションに値が設定されている場合には `queue onu1 class property` コマンドの `bandwidth` パラメーターに測定結果が反映される。WAN インターフェースが設定されている場合には、`speed wan1` コマンドに測定結果が反映される。`class` オプションに値が設定されている場合には `queue wan1 class property` コマンドの `bandwidth` パラメーターに測定結果が反映される。

`class` オプションは帯域制御機能が実装されている機種でのみ利用できる。

`limit-rate` オプションは、設定値の急激な変動をある割合内に抑えたい場合に設定する。直前の測定結果と今回の測定結果に大きな差がある場合、今回の測定結果そのものではなく、この `limit-rate` に応じた値を今回の設定値として採用する。

`local-address` オプションでは、送信パケットの始点 IP アドレスを設定できる。設定がない場合、インターフェースに付与された IP アドレスを使用する

## [適用モデル]

NVR700W, NVR510

## 24.4 負荷監視通知で連携動作を行う相手毎の動作の設定

## [書式]

```
cooperation load-watch remote id role address [option=value]
```

```
no cooperation load-watch remote id [role address [option=value]]
```

## [設定値及び初期値]

- `id`
  - [設定値]: 相手先 ID 番号 (1..100)
  - [初期値]: -
- `role`: 連携動作での相手側の役割
  - [設定値]:

| 設定値    | 説明               |
|--------|------------------|
| server | 相手側がサーバー側動作を行う   |
| client | 相手側がクライアント側動作を行う |

- [初期値]: -
- `address`
  - [設定値]: 連携動作の相手側 IP アドレス、FQDN または 'any'

- [初期値]:-
- *option*: オプション
- [設定値]:

| 設定値               | 説明                                                                                 |
|-------------------|------------------------------------------------------------------------------------|
| trigger           | サーバー動作として、クライアントに通知を行う条件のトリガ定義番号 (1-65535)、'!'で区切って複数の指定が可能、相手側動作をクライアントに設定する時のみ可能 |
| control           | クライアント動作として、サーバーから通知を受けた時の制御動作定義番号 (1-65535)、相手側動作をサーバーに設定する時のみ可能                  |
| port              | 相手側が使用する UDP のポート番号 (1-65535)                                                      |
| syslog            | 動作をログに残すか否か、'on'or'off'                                                            |
| apply             | 負荷監視通知の結果を動作に反映させるかどうか、'on'or'off'                                                 |
| register          | サーバーに対する登録パケットを送るか否か、'on'or'off'                                                   |
| register-interval | クライアントからサーバーへの登録パケット送信間隔、(1..2147483647)[sec]                                      |
| register-time     | サーバーでのクライアント登録情報保持時間、(1..2147483647)[sec]                                          |
| name              | 相手側を識別する名前 (最大 16 文字)                                                              |
| local-address     | パケット送信時の始点 IP アドレス                                                                 |

- [初期値]:
  - port=59410
  - syslog=off
  - apply=on
  - register=off
  - register-interval=1200
  - register-time=3600

#### [説明]

負荷監視通知で連携動作を行う相手毎の動作を設定する。

#### [ノート]

*role* パラメーターで *client* を設定する場合のみ *trigger* オプションを利用でき、*client* を設定する場合は *trigger* オプションの設定は必須である。また、*server* を設定する場合のみ *control* オプションを利用でき、*server* を設定する場合は *control* オプションの設定は必須である。

サーバー側で *any* を指定した場合、サーバー側にクライアントの存在を通知登録するためにクライアント側では *register=on* を設定する必要がある。

*name* オプションを設定した場合、サーバーとクライアントの双方で同じ名前を設定した場合にのみ機能する。

*local-address* オプションでは、送信パケットの始点 IP アドレスを設定できる。設定がない場合、インターフェースに付与された IP アドレスを使用する。

複数のトリガを設定した場合、抑制要請の送信タイミングはそれぞれのトリガで個別に検出される。それらの送信タイミングが異なる時には抑制要請はそれぞれのタイミングで個別に送られ、送信タイミングが一致する時にはひとつの抑制要請となる。

相手先に一度抑制解除が送られた後は、次に抑制要請を送信するまで抑制解除は送信しない。

抑制要請を送信していないトリガ条件が抑制解除条件を満たしても抑制解除通知は送信しない。

抑制制御を行っている最中に相手先情報が削除されると、制御対象のインターフェースの速度はその時点の設定が保持される。

#### [適用モデル]

NVR700W, NVR510

## 24.5 負荷監視サーバーとしての動作トリガの設定

### [書式]

**cooperation load-watch trigger id point high=high [, count] low=low [, count] [option=value]**

**no cooperation load-watch trigger id [point high=high [, count] low=low [, count] [option=value]]**

### [設定値及び初期値]

- *id*
  - [設定値]: 相手先 ID 番号 (1-100)
  - [初期値]: -
- *point*: 負荷監視対象ポイント
  - [設定値]:
    - *cpu load*
      - 単位時間間隔で CPU 負荷率を監視する値は % で指定する
    - *interface receive*
      - インターフェースでの単位時間当たりの受信量を監視する。値は 1 秒あたりのビット数で指定する

|                  |                              |
|------------------|------------------------------|
| <i>interface</i> | インターフェース名 (LAN, ONU, TUNNEL) |
|------------------|------------------------------|

- *interface overflow*
  - LAN インターフェースおよび ONU インターフェースでの単位時間当たりの受信オーバーフロー数と受信バッファエラー数を監視する。値は発生回数で指定する

|                  |                                 |
|------------------|---------------------------------|
| <i>interface</i> | LAN インターフェース名、および ONU インターフェース名 |
|------------------|---------------------------------|

- *interface [class] transmit*
  - インターフェースでの単位時間当たりの送信量を監視する。値は 1 秒あたりのビット数で指定する

|                  |                                          |
|------------------|------------------------------------------|
| <i>interface</i> | インターフェース名 (LAN, ONU, TUNNEL)             |
| <i>class</i>     | クラス番号 (LAN インターフェース、および ONU インターフェースの場合) |

- [初期値]: -
- *high*
  - [初期値]: 高負荷検出閾値
- *low*
  - [設定値]: 負荷減少検出閾値
  - [初期値]: -
- *count*
  - [設定値]: 通知を送出するに至る検出回数 (1-100)、省略時は 3
  - [初期値]: -
- *option*: オプション
  - [設定値]:

| 設定値      | 説明                                 |
|----------|------------------------------------|
| interval | 監視する間隔 (1-65535)[sec]、省略時は 10[sec] |
| syslog   | 動作をログに残すか否か、'on'or'off'、省略時は 'off' |

- [初期値]: -

### [説明]

機器の負荷を検出して相手側にトラフィック抑制要請を送出する条件を設定する。監視対象ポイントの負荷を単位時間毎に監視し、*high* に設定された閾値を上回ることを *count* 回数続けて検出すると抑制要請を送出する。この状態で閾値を上回る高負荷状態が続く限り、*count* の間隔で抑制要請を送出し続ける。

同様に、*low* に設定された閾値を *count* 回数続けて下回って検出すると抑制解除を送出する。抑制解除は同じ相手に対して連続して送出不される。

*class* オプションは NVR700W (帯域制御機能が実装されている機種) でのみ利用できる。

**[ノート]**

閾値を決定する際の参考値として、**show environment** や **show status lan**、**show status onu1** で表示される情報のほか、syslog オプションによりログに表示される値も利用できる。

**[設定例]**

```
# cooperation load-watch trigger 1 cpu load high=80 low=30
```

一定間隔で CPU の負荷率を観測し、負荷率が 80% 以上であることが連続 3 回測定されたら抑制要請を送り、その後 30% 以下であることが 3 回続けて観測されたら抑制解除を送る。

```
# cooperation load-watch trigger 2 lan2 receive high=80m,5 low=50m,1
```

単位時間内での LAN2 からの受信バイト数から受信速度を求め、その値が 80[Mbit/s]以上であることが連続 5 回あれば抑制要請を送り、その後 50[Mbit/s]以下であることが 1 度でも観測されれば抑制解除を送る。

```
# cooperation load-watch trigger 3 lan2 overflow high=2,1 low=0,5
```

単位時間内での LAN2 での受信オーバーフロー数の増加を監視し、2 回検出されることが 1 度でもあれば抑制要請を送り、検出されないことが 5 回続けば抑制解除を送る。

**[適用モデル]**

NVR700W, NVR510

## 24.6 負荷監視クライアントとしての動作の設定

**[書式]**

```
cooperation load-watch control id high=high [raise=raise] low=low [lower=lower] [option=value]  
no cooperation load-watch control id [high=high [raise=raise] low=low [lower=lower] [option=value]]
```

**[設定値及び初期値]**

- *id*
  - [設定値]: 相手先 ID 番号 (1-100)
  - [初期値]: -
- *high*
  - [設定値]: bit/sec、帯域上限値
  - [初期値]: -
- *raise*
  - [設定値]:
    - %、帯域上限値に達していない限り、定時間毎にこの割合だけ帯域を増加させる
    - 省略時は 5%
  - [初期値]: -
- *low*
  - [設定値]: bit/sec、帯域下限値
  - [初期値]: -
- *lower*
  - [設定値]:
    - %、帯域下限値に達していない限り、抑制要請を受けた時に現在の帯域からこの割合だけ送出帯域を減少させる
    - 省略時は 30%
  - [初期値]: -
- *option*: オプション
  - [設定値]:

| 設定値       | 説明                                      |
|-----------|-----------------------------------------|
| interval  | 帯域を増加させる間隔 (1-65535) [sec]、省略時は 10[sec] |
| interface | 帯域を変化させる LAN インターフェース、または ONU インターフェース  |



| 設定値   | 説明          |
|-------|-------------|
| class | 帯域を変化させるクラス |

- [初期値]:-

#### [説明]

トラフィック抑制要請を受けた場合の動作を設定する。帯域は *high* に設定された帯域と *low* に設定された帯域との間で制御される。

抑制要請を受信すると、送出帯域は現状の運用帯域値の *lower* の値に応じた割合に減少する。帯域が *high* に達していない限り、*raise* の値に応じて運用帯域は増加する。

トラフィック抑制解除を受信した場合には、帯域は *high* に設定された帯域に増加する。

#### [適用モデル]

NVR700W, NVR510

## 24.7 連携動作の手動実行

#### [書式]

**cooperation bandwidth-measuring go id**

**cooperation load-watch go id type**

#### [設定値及び初期値]

- bandwidth-measuring : 回線帯域検出
  - [初期値]:-
- load-watch : 負荷監視通知
  - [初期値]:-
- id
  - [設定値]: 相手先 ID 番号 (1-100)
  - [初期値]:-
- type : パケットタイプ
  - [設定値]:

| 設定値   | 説明         |
|-------|------------|
| lower | 負荷減少検出パケット |
| raise | 高負荷検出パケット  |

- [初期値]:-

#### [説明]

手動で連携動作を実行する。

#### [ノート]

bandwidth-measuring を指定した場合、測定結果がログに表示される。インターフェース速度の設定で回線帯域検出の値を使用するように設定されている場合には、この実行結果の値も設定への反映の対象となる。

load-watch を指定した場合は、指定した相手先に対して負荷監視のトリガで送出されるパケットと同じパケットが送出される。相手の役割がクライアントである相手にのみ有効である。

#### [適用モデル]

NVR700W, NVR510

## 第 25 章

### OSPF

OSPF はインテリアゲートウェイプロトコルの一種で、グラフ理論をベースとしたリンク状態型の動的ルーティングプロトコルである。

#### 25.1 OSPF の有効設定

##### [書式]

```
ospf configure refresh
```

##### [説明]

OSPF 関係の設定を有効にする。OSPF 関係の設定を変更したら、ルーターを再起動するか、あるいはこのコマンドを実行しなくてはならない。

##### [適用モデル]

NVR700W

#### 25.2 OSPF の使用設定

##### [書式]

```
ospf use use  
no ospf use [use]
```

##### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| on  | OSPF を使用する  |
| off | OSPF を使用しない |

- [初期値]: off

##### [説明]

OSPF を使用するか否かを設定する。

##### [ノート]

以下の機能はまだサポートされていない。

- NSSA (RFC1587)
- OSPF over demand circuit (RFC1793)
- OSPF MIB

##### [適用モデル]

NVR700W

#### 25.3 OSPF による経路の優先度設定

##### [書式]

```
ospf preference preference  
no ospf preference [preference]
```

##### [設定値及び初期値]

- *preference*
- [設定値]: OSPF による経路の優先度 (1 以上の数値)
- [初期値]: 2000

**[説明]**

OSPF による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPF と RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

**[ノート]**

静的経路の優先度は 10000 で固定である。

**[適用モデル]**

NVR700W

## 25.4 OSPF のルーター ID 設定

---

**[書式]**

```
ospf router id router-id
no ospf router id [router-id]
```

**[設定値及び初期値]**

- *router\_id*
  - [設定値]: IP アドレス
  - [初期値]: -

**[説明]**

OSPF のルーター ID を指定する。

**[ノート]**

ルーター ID が本コマンドで設定されていないときは、以下のインターフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インターフェース
- LOOPBACK インターフェース
- PP インターフェース

なお、プライマリ IPv4 アドレスが付与されたインターフェースがない場合は初期値は設定されない。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか `bgp router id` コマンドのいずれか一方を設定する。Rev.15.00.03 以降のファームウェアでは、本コマンドと `bgp router id` コマンドの両方を設定することができるが、必ず同一のルーター ID を指定する必要がある。

**[適用モデル]**

NVR700W

## 25.5 OSPF で受け取った経路をルーティングテーブルに反映させるか否かの設定

---

**[書式]**

```
ospf export from ospf [filter filter_num...]
no ospf export from ospf [filter filter_num...]
```

**[設定値及び初期値]**

- *filter\_num*
  - [設定値]: `ospf export filter` コマンドのフィルター番号
  - [初期値]: すべての経路がルーティングテーブルに反映される

**[説明]**

OSPF で受け取った経路をルーティングテーブルに反映させるかどうかを設定する。指定したフィルターに一致する経路だけがルーティングテーブルに反映される。コマンドが設定されていない場合には、すべての経路がルーティングテーブルに反映される。

**[ノート]**

フィルター番号は 101 個まで設定できる。

このコマンドは OSPF のリンク状態データベースには影響を与えない。つまり、OSPF で他のルーターと情報をやり取りする動作としては、このコマンドがどのように設定されていても変化は無い。OSPF で計算した経路が、実際にパケットをルーティングするために使われるかどうかだけが変わる。

[適用モデル]  
NVR700W

## 25.6 外部プロトコルによる経路導入

[書式]

```
ospf import from protocol [filter filter_num...]
no ospf import from protocol [filter filter_num...]
```

[設定値及び初期値]

- *protocol* : OSPF の経路テーブルに導入する外部プロトコル

- [設定値]:

| 設定値    | 説明   |
|--------|------|
| static | 静的経路 |
| rip    | RIP  |
| bgp    | BGP  |

- [初期値]: -
- *filter\_num*
  - [設定値]: フィルター番号
  - [初期値]: -

[説明]

OSPF の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルーターに広告される。

*filter\_num* は **ospf import filter** コマンドで定義したフィルター番号を指定する。外部プロトコルから導入されようとする経路は指定したフィルターにより検査され、フィルターに該当すればその経路は OSPF に導入される。該当するフィルターがない経路は導入されない。また、*filter* キーワード以降を省略した場合には、すべての経路が OSPF に導入される

経路を広告する場合のパラメーターであるメトリック値、メトリックタイプ、タグは、フィルターの検査で該当した **ospf import filter** コマンドで指定されたものを使う。*filter* キーワード以降を省略した場合には、以下のパラメーターを使用する。

- metric=1
- type=2
- tag=1

[ノート]

フィルター番号は 101 個まで設定できる。

[適用モデル]  
NVR700W

## 25.7 OSPF で受け取った経路をどう扱うかのフィルターの設定

[書式]

```
ospf export filter filter_num [nr] kind ip_address/mask...
no ospf export filter filter_num [...]
```

[設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号
  - [初期値]: -
- *nr* : フィルターの解釈の方法
  - [設定値]:

| 設定値    | 説明                 |
|--------|--------------------|
| not    | フィルターに該当しない経路を導入する |
| reject | フィルターに該当した経路を導入しない |
| 省略時    | フィルターに該当した経路を導入する  |

- [初期値]: -
- *kind*: フィルター種別
- [設定値]:

| 設定値     | 説明                                        |
|---------|-------------------------------------------|
| include | 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)   |
| refines | 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含まない) |
| equal   | 指定したネットワークアドレスに一致する経路                     |

- [初期値]: -
- *ip\_address/mask*
  - [設定値]: ネットワークアドレスをあらわす IP アドレスとマスク長
  - [初期値]: -

#### [説明]

OSPF により他の OSPF ルーターから受け取った経路を経路テーブルに導入する際に適用するフィルターを定義する。このコマンドで定義したフィルターは、**ospf export from ospf** コマンドの *filter* 項で指定されてはじめて効果を持つ。

*ip\_address/mask* では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行う。

*nr* が省略されている場合には、一つでも該当するフィルターがある場合には経路が導入される。

**not** 指定時には、すべての検査でフィルターに該当しなかった場合に経路が導入される。**reject** 指定時には、一つでも該当するフィルターがある場合には経路が導入されない

*kind* では、経路の検査方法を設定する。

|         |                                                  |
|---------|--------------------------------------------------|
| include | ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる     |
| refines | ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない |
| equal   | ネットワークアドレスに一致する経路だけが該当となる                        |

#### [ノート]

**not** 指定のフィルターを **ospf export from ospf** コマンドで複数設定する場合には注意が必要である。**not** 指定のフィルターに合致するネットワークアドレスは、そのフィルターでは導入するかどうか決定しないため、次のフィルターで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が導入されることになり、フィルターの意味が無い。

```
ospf export from ospf filter 1 2
ospf export filter 1 not equal 192.168.1.0/24
ospf export filter 2 not equal 192.168.2.0/24
```

1 番のフィルターでは、192.168.1.0/24 以外の経路を導入し、2 番のフィルターで 192.168.2.0/24 以外の経路を導入している。つまり、経路 192.168.1.0/24 は 2 番のフィルターにより、経路 192.168.2.0/24 は 1 番のフィルターにより導入されるため、導入されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を導入したくない場合には以下のような設定を行う必要がある。

```
ospf export from ospf filter 1
ospf export filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは

```
ospf export from ospf filter 1 2 3
ospf export filter 1 reject equal 192.168.1.0/24
ospf export filter 2 reject equal 192.168.2.0/24
ospf export filter 3 include 0.0.0.0/0
```

[適用モデル]  
NVR700W

## 25.8 外部経路導入に適用するフィルター定義

[書式]

```
ospf import filter filter_num [nr] kind ip_address/mask... [parameter...].
no ospf import filter filter_num [[not] kind ip_address/mask... [parameter...]]
```

[設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号
  - [初期値]: -
- *nr*: フィルターの解釈の方法
  - [設定値]:

| 設定値    | 説明                 |
|--------|--------------------|
| not    | フィルターに該当しない経路を広告する |
| reject | フィルターに該当した経路を広告しない |
| 省略時    | フィルターに該当した経路を広告する  |

- [初期値]: -

- *kind*
  - [設定値]:

| 設定値     | 説明                                        |
|---------|-------------------------------------------|
| include | 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)   |
| refines | 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身は含まない) |
| equal   | 指定したネットワークアドレスに一致する経路                     |

- [初期値]: -
- *ip\_address/mask*
  - [設定値]: ネットワークアドレスをあらわす IP アドレスとマスク長
  - [初期値]: -
- *parameter*: 外部経路を広告する場合のパラメーター
  - [設定値]:

| 設定値    | 説明                   |
|--------|----------------------|
| metric | メトリック値 (0..16777215) |
| type   | メトリックタイプ (1..2)      |
| tag    | タグの値 (0..4294967295) |

- [初期値]: -

[説明]

OSPF の経路テーブルに外部経路を導入する際に適用するフィルターを定義する。このコマンドで定義したフィルターは、**ospf import from** コマンドの *filter* 項で指定されてはじめて効果を持つ。

*ip\_address/mask* では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行い、1つでも該当するものがあればそれが適用される。

*nr* が省略されている場合には、一つでも該当するフィルターがある場合には経路を広告する。**not** 指定時には、すべての検査でフィルターに該当しなかった場合に経路を広告する。**reject** 指定時には、一つでも該当するフィルターがある場合には経路を広告しない。

*kind* では、経路の検査方法を設定する。

|         |                                                  |
|---------|--------------------------------------------------|
| include | ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる     |
| refines | ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない |
| equal   | ネットワークアドレスに一致する経路だけが該当となる                        |

*kind* の前に **not** キーワードを置くと、該当/非該当の判断が反転する。例えば、**not equal** では、ネットワークアドレスに一致しない経路が該当となる

*parameter* では、該当した経路を OSPF の外部経路として広告する場合のパラメーターとして、メトリック値、メトリックタイプ、タグがそれぞれ *metric*、*type*、*tag* により指定できる。これらを省略した場合には、以下の値が採用される。

- *metric*=1
- *type*=2
- *tag*=1

#### [ノート]

**not** 指定のフィルターを **ospf import from** コマンドで複数設定する場合には注意が必要である。**not** 指定のフィルターに合致するネットワークアドレスは、そのフィルターでは導入するかどうかは決定しないため、次のフィルターで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が広告されることになり、フィルターの意味が無い。

```
ospf import from static filter 1 2
ospf import filter 1 not equal 192.168.1.0/24
ospf import filter 2 not equal 192.168.2.0/24
```

1 番のフィルターでは、192.168.1.0/24 以外の経路を広告し、2 番のフィルターで 192.168.2.0/24 以外の経路を広告している。つまり、経路 192.168.1.0/24 は 2 番のフィルターにより、経路 192.168.2.0/24 は 1 番のフィルターにより広告されるため、広告されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を広告したくない場合には以下のような設定を行う必要がある。

```
ospf import from static filter 1
ospf import filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは

```
ospf import from static filter 1 2 3
ospf import filter 1 reject equal 192.168.1.0/24
ospf import filter 2 reject equal 192.168.2.0/24
ospf import filter 3 include 0.0.0.0/0
```

#### [適用モデル]

NVR700W

## 25.9 OSPF エリア設定

### [書式]

```
ospf area area [auth=auth] [stub [cost=cost]]
no ospf area area [auth=auth] [stub [cost=cost]]
```

### [設定値及び初期値]

- *area*
- [設定値]:

| 設定値                     | 説明         |
|-------------------------|------------|
| backbone                | バックボーンエリア  |
| 1 以上の数値                 | 非バックボーンエリア |
| IP アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -
- *auth*
- [設定値]:

| 設定値  | 説明         |
|------|------------|
| text | プレーンテキスト認証 |
| md5  | MD5 認証     |

- [初期値]: 認証は行わない
- *stub*: スタブエリアであることを指定する。
- [初期値]: スタブエリアではない
- *cost*
- [設定値]: 1 以上の数値
- [初期値]: -

#### [説明]

OSPF エリアを設定する。

*cost* は 1 以上の数値で、エリア境界ルーターがエリア内に広告するデフォルト経路のコストとして使われる。*cost* を指定しないとデフォルト経路の広告は行われない。

#### [適用モデル]

NVR700W

## 25.10 エリアへの経路広告

#### [書式]

```
ospf area network area network/mask [restrict]
no ospf area network area network/mask [restrict]
```

#### [設定値及び初期値]

- *area*
- [設定値]:

| 設定値                     | 説明         |
|-------------------------|------------|
| backbone                | バックボーンエリア  |
| 1 以上の数値                 | 非バックボーンエリア |
| IP アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -
- *network*
- [設定値]: IP アドレス
- [初期値]: -
- *mask*
- [設定値]: ネットマスク長
- [初期値]: -

#### [説明]

エリア境界ルーターが他のエリアに経路を広告する場合に、このコマンドで指定したネットワークの範囲内の経路は単一のネットワーク経路として広告する。*restrict* キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

#### [適用モデル]

NVR700W



## 25.11 スタブ的接続の広告

### [書式]

```
ospf area stubhost area host [cost cost]
```

```
no ospf area stubhost area host
```

### [設定値及び初期値]

- *area*

- [設定値]:

| 設定値                     | 説明         |
|-------------------------|------------|
| backbone                | バックボーンエリア  |
| 1 以上の数値                 | 非バックボーンエリア |
| IP アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -

- *host*

- [設定値]: IP アドレス

- [初期値]: -

- *cost*

- [設定値]: 1 以上の数値

- [初期値]: -

### [説明]

指定したホストが指定したコストでスタブ的に接続されていることをエリア内に広告する。

### [適用モデル]

NVR700W

## 25.12 仮想リンク設定

### [書式]

```
ospf virtual-link router_id area [parameters...]
```

```
no ospf virtual-link router_id [area [parameters...]]
```

### [設定値及び初期値]

- *router\_id*

- [設定値]: 仮想リンクの相手のルーター ID

- [初期値]: -

- *area*

- [設定値]:

| 設定値                     | 説明         |
|-------------------------|------------|
| 1 以上の数値                 | 非バックボーンエリア |
| IP アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -

- *parameters*

- [設定値]: NAME=VALUE の列

- [初期値]:

- retransmit-interval = 5 秒
- transmit-delay = 1 秒
- hello-interval = 10 秒
- dead-interval = 40 秒
- authkey=なし
- md5key=なし
- md5-sequence-mode=second

## [説明]

仮想リンクを設定する。仮想リンクは *router\_id* で指定したルーターに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメーターが設定できる。パラメーターは NAME=VALUE の形で指定され、以下の種類がある。

| NAME                | VALUE        | 説明                                                                                                                                                                                   |
|---------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| retransmit-interval | 秒数           | LSA を連続して送る場合の再送間隔を秒単位で設定する。(1..)                                                                                                                                                    |
| transmit-delay      | 秒数           | リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。(1..)                                                                                                                                          |
| hello-interval      | 秒数           | HELLO パケットの送信間隔を秒単位で設定する。(1..)                                                                                                                                                       |
| dead-interval       | 秒数           | 相手から HELLO を受け取れない場合に、相手がダウンしたと判断するまでの時間を秒単位で設定する。(1..)                                                                                                                              |
| authkey             | 文字列          | プレーンテキスト認証の認証鍵を表す文字列を設定する。(8 文字以内)                                                                                                                                                   |
| md5key              | "(ID),(KEY)" | MD5 認証の認証鍵を表す ID と鍵文字列 KEY を設定する。ID は十進数で 0~255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。 |
| md5-sequence-mode   | "second"     | 送信時刻の秒数                                                                                                                                                                              |
|                     | "increment"  | 単調増加                                                                                                                                                                                 |

## [ノート]

## • hello-interval/dead-interval について

hello-interval と dead-interval の値は、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメーターの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

## • MD5 認証鍵について

MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。

通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルーターで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルーターで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルーターで古い鍵を削除すれば良い。

## [適用モデル]

NVR700W

## 25.13 指定インターフェースの OSPF エリア設定

## [書式]

```
ip interface ospf area area [parameters...]
```

```
ip pp ospf area area [parameters...]
```

```
ip tunnel ospf area area [parameters...]
```

```
no ip interface ospf area [area [parameters...]]
```

```
no ip pp ospf area [area [parameters...]]
```

**no ip tunnel ospf area** [*area* [*parameters...*]]

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、LOOPBACK インターフェース名
  - [初期値]: -
- *area*

- [設定値]:

| 設定値                     | 説明         |
|-------------------------|------------|
| backbone                | バックボーンエリア  |
| 1 以上の数値                 | 非バックボーンエリア |
| IP アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: インターフェースは OSPF エリアに属していない

- *parameters*

- [設定値]: NAME=VALUE の列
- [初期値]:
  - type=broadcast(LAN インターフェース、ONU インターフェース設定時)
  - type=point-to-point(PP または TUNNEL インターフェース設定時)
  - type=loopback(LOOPBACK インターフェース設定時)
  - passive=インターフェースは passive ではない
  - cost=1(LAN インターフェース、ONU インターフェース、LOOPBACK インターフェース設定時)、1562(トンネル設定時)、pp は回線速度に依存
  - priority=1
  - retransmit-interval=5 秒
  - transmit-delay=1 秒
  - hello-interval=10 秒 (type=broadcast 設定時)
  - hello-interval=10 秒 (point-to-point 設定時)
  - hello-interval=30 秒 (non-broadcast 設定時)
  - hello-interval=30 秒 (point-to-multipoint 設定時)
  - dead-interval=hello-interval の 4 倍
  - poll-interval=120 秒
  - authkey=なし
  - md5key=なし
  - md5-sequence-mode=second

**[説明]**

指定したインターフェースの属する OSPF エリアを設定する。

NAME パラメーターの type はインターフェースのネットワークがどのようなタイプであるかを設定する。

parameters では、リンクパラメーターを設定する。パラメーターは NAME=VALUE の形で指定され、以下の種類がある。

| NAME    | VALUE               | 説明                                                              |
|---------|---------------------|-----------------------------------------------------------------|
| type    | broadcast           | ブロードキャスト                                                        |
|         | point-to-point      | ポイント・ポイント                                                       |
|         | point-to-multipoint | ポイント・マルチポイント                                                    |
|         | non-broadcast       | NBMA                                                            |
| passive |                     | インターフェースに対して、OSPF パケットを送信しない。該当インターフェースに他の OSPF ルーターがない場合に設定する。 |

| NAME                | VALUE        | 説明                                                                                                                                                                                                                                                                                                                             |
|---------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cost                | コスト          | <p>インターフェースのコストを設定する。初期値は、インターフェースの種類と回線速度によって決定される。LAN インターフェースと ONU インターフェースの場合は 1、PP インターフェースの場合は、バインドされている回線の回線速度を S[kbit/s]とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。(0..65535)</p> <ul style="list-style-type: none"> <li>• COST=100000/S</li> </ul> <p>TUNNEL インターフェースの場合は、1562 がデフォルト値となる。</p> |
| priority            | 優先度          | <p>指定ルーターの選択の際の優先度を設定する。PRIORITY 値が大きいルーターが指定ルーターに選ばれる。0 を設定すると、指定ルーターに選ばれなくなる。(0..255)</p>                                                                                                                                                                                                                                    |
| retransmit-interval | 秒数           | <p>LSA を連続して送る場合の再送間隔を秒単位で設定する。(1..)</p>                                                                                                                                                                                                                                                                                       |
| transmit-delay      | 秒数           | <p>リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。(1..)</p>                                                                                                                                                                                                                                                                             |
| hello-interval      | 秒数           | <p>HELLO パケットの送信間隔を秒単位で設定する。(1..)</p>                                                                                                                                                                                                                                                                                          |
| dead-interval       | 秒数           | <p>近隣ルーターから HELLO を受け取れない場合に、近隣ルーターがダウンしたと判断するまでの時間を秒単位で設定する。(1..)</p>                                                                                                                                                                                                                                                         |
| poll-interval       | 秒数           | <p>非ブロードキャストリンクでのみ有効なパラメーターで、近隣ルーターがダウンしている場合の HELLO パケットの送信間隔を秒単位で設定する。(1..)</p>                                                                                                                                                                                                                                              |
| authkey             | 文字列          | <p>プレーンテキスト認証の認証鍵を表す文字列を設定する。(8 文字以内)</p>                                                                                                                                                                                                                                                                                      |
| md5key              | "(ID),(KEY)" | <p>MD5 認証の認証鍵を表す ID と鍵文字列 KEY を設定する。ID は十進数で 0~255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。</p>                                                                                                                                    |
| md5-sequence-mode   | "second"     | 送信時刻の秒数                                                                                                                                                                                                                                                                                                                        |
|                     | "increment"  | 単調増加                                                                                                                                                                                                                                                                                                                           |

LOOPBACK インターフェースに設定する場合は、*type* パラメーターでインターフェースタイプを、*cost* パラメーターでインターフェースのコストを指定できる。LOOPBACK インターフェースのタイプで指定できるのは、以下の 2 種類だけとなる。

| NAME | VALUE            | 広告される経路の種類                            | OSPF 的なインターフェースの扱い |          |
|------|------------------|---------------------------------------|--------------------|----------|
|      |                  |                                       | タイプ                | 状態       |
| type | loopback         | LOOPBACK インターフェースの IP アドレスのみのホスト経路    | point-to-point     | Loopback |
|      | loopback-network | LOOPBACK インターフェースの implicit なネットワーク経路 | NBMA               | DROther  |

## [ノート]

- NAME パラメーターの **type** について  
NAME パラメーターの **type** として、LAN インターフェースは **broadcast** のみが許される。PP インターフェースは、PPP を利用する場合は **point-to-point**、フレームリレーを利用する場合は **point-to-multipoint** と **non-broadcast** のいずれかが設定できる。  
フレームリレーで **non-broadcast(NBMA)** を利用する場合には、フレームリレーの各拠点間のすべての間で PVC が設定されており、FR に接続された各ルーターは他のルーターと直接通信できるような状態、すなわちフルメッシュになっていなくてはならない。また、**non-broadcast** では近隣ルーターを自動的に認識することができないため、すべての近隣ルーターを **ip pp ospf neighbor** コマンドで設定する必要がある。  
**point-to-multipoint** を利用する場合には、フレームリレーの PVC はフルメッシュである必要はなく、一部が欠けたパーシャルメッシュでも利用できる。近隣ルーターは **InArp** を利用して自動的に認識するため、**InArp** が必須となる。RT では **InArp** を使うかどうかは **fr inarp** コマンドで制御できるが、デフォルトでは **InArp** を使用する設定になっているので、**ip pp address** コマンドでインターフェースに適切な IP アドレスを与えるだけでよい。

**point-to-multipoint** と設定されたインターフェースでは、**ip pp ospf neighbor** コマンドの設定は無視される。**point-to-multipoint** の方が **non-broadcast** よりもネットワークの制約が少なく、また設定も簡単だが、その代わりに回線を通るトラフィックは大きくなる。**non-broadcast** では、**broadcast** と同じように指定ルーターが選定され、HELLO などの OSPF トラフィックは各ルーターと指定ルーターの間だけに限定されるが、**point-to-multipoint** ではすべての通信可能なルーターペアの間に **point-to-point** リンクがあるという考え方なので、OSPF トラフィックもすべての通信可能なルーターペアの間でやりとりされる。

- **passive** について  
**passive** は、インターフェースが接続しているネットワークに他の OSPF ルーターが存在しない場合に指定する。**passive** を指定しておく、インターフェースから OSPF パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インターフェースと ONU インターフェース (**type=broadcast** であるインターフェース) の場合には、インターフェースが接続しているネットワークへの経路は、**ip interface ospf area** コマンドを設定していないと他の OSPF ルーターに広告されない。そのため、OSPF を利用しないネットワークに接続する LAN インターフェースと ONU インターフェースに対しては、**passive** を付けた **ip interface ospf area** コマンドを設定しておくことでそのネットワークでは OSPF を利用しないまま、そこへの経路を他の OSPF ルーターに広告することができる。

PP インターフェースに対して **ip interface ospf area** コマンドを設定していない場合は、インターフェースが接続するネットワークへの経路は外部経路として扱われる。外部経路なので、他の OSPF ルーターに広告するには **ospf import** コマンドの設定が必要である。

- **hello-interval/dead-interval** について  
**hello-interval/dead-interval** の値は、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメーターの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

- MD5 認証鍵について  
MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。  
通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルーターで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルーターで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルーターで古い鍵を削除すれば良い。

[適用モデル]  
NVR700W

## 25.14 非ブロードキャスト型ネットワークに接続されている OSPF ルーターの指定

[書式]

```
ip interface ospf neighbor ip_address [eligible]
ip pp ospf neighbor ip_address [eligible]
ip tunnel ospf neighbor ip_address [eligible]
no ip interface ospf neighbor ip_address [eligible]
no ip pp ospf neighbor ip_address [eligible]
no ip tunnel ospf neighbor ip_address [eligible]
```

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *ip\_address*
  - [設定値]: 近隣ルーターの IP アドレス
  - [初期値]: -

[説明]

非ブロードキャスト型のネットワークに接続されている OSPF ルーターを指定する。  
eligible キーワードが指定されたルーターは指定ルーターとして適格であることを表す。

[適用モデル]  
NVR700W

## 25.15 スタブが存在する時のネットワーク経路の扱いの設定

[書式]

```
ospf merge equal cost stub merge
no ospf merge equal cost stub
```

[設定値及び初期値]

- *merge*
  - [設定値]:

| 設定値 | 説明                        |
|-----|---------------------------|
| on  | イコールコストになるスタブを他の経路とマージする  |
| off | イコールコストになるスタブを他の経路とマージしない |

- [初期値]: on

[説明]

他の経路と同じコストになるスタブをどう扱うかを設定する。  
on の場合にはスタブへの経路を他の経路とマージして、イコールコストマルチパス動作をする。これは、RFC2328 の記述に沿うものである。  
off の場合にはスタブへの経路を無視する。

[適用モデル]  
NVR700W

## 25.16 OSPF の状態遷移とパケットの送受信をログに記録するか否かの設定

[書式]

```
ospf log log [log...]
```

**no ospf log** [*log...*]

[設定値及び初期値]

- *log*
  - [設定値]:

| 設定値       | 説明            |
|-----------|---------------|
| interface | インターフェースの状態遷移 |
| neighbor  | 近隣ルーターの状態遷移   |
| packet    | 送受信したパケット     |

- [初期値]: OSPF のログは記録しない。

[説明]

指定した種類のログを INFO レベルで記録する。

[適用モデル]

NVR700W

## 25.17 インターフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定

[書式]

**ospf reric interval** *time*

**no ospf reric interval** [*time*]

[設定値及び初期値]

- *time*
  - [設定値]: 秒数 (1 以上の数値)
  - [初期値]: 1

[説明]

ルーターのインターフェースの状態が変化するとき、OSPF に外部経路を反映させる時間の間隔を設定する。

OSPF ではインターフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インターフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

[ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。  
 本コマンドの設定値は、BGP への外部経路の反映にも影響する。本コマンドと **bgp reric interval** コマンドの設定値が食い違う場合には、本コマンドの設定値が優先して適用される。  
 本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**ospf configure refresh** コマンドを実行しなくても即時反映される。

NVR700W は Rev.15.00.03 以降で使用可能。

[適用モデル]

NVR700W

## 第 26 章

### BGP

#### 26.1 BGP の起動の設定

##### [書式]

```
bgp use use
no bgp use [use]
```

##### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値  | 説明    |
|------|-------|
| on   | 起動する  |
| off. | 起動しない |

- [初期値]: off

##### [説明]

BGP を起動するか否かを設定する

##### [ノート]

いずれかのインターフェースにセカンダリアドレスを割り当てた場合、BGP を使用することはできない。

##### [適用モデル]

NVR700W

#### 26.2 経路の集約の設定

##### [書式]

```
bgp aggregate ip_address/mask filter filter_num ...
no bgp aggregate ip_address/mask [filter filter_num... ]
```

##### [設定値及び初期値]

- *ip\_address/mask*
  - [設定値]: IP アドレス/ネットマスク
  - [初期値]: -
- *filter\_num*
  - [設定値]: フィルター番号 (1..2147483647)
  - [初期値]: -

##### [説明]

BGP で広告する集約経路を設定する。フィルターの番号には、**bgp aggregate filter** コマンドで定義した番号を指定する。

##### [適用モデル]

NVR700W

#### 26.3 経路を集約するためのフィルターの設定

##### [書式]

```
bgp aggregate filter filter_num protocol [reject] kind ip_address/mask ...
no bgp aggregate filter filter_num [protocol [reject] kind ip_address/mask ...]
```

##### [設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号 (1..2147483647)
  - [初期値]: -



- *protocol*
- [設定値]:

| 設定値    | 説明        |
|--------|-----------|
| static | 静的経路      |
| rip    | RIP       |
| ospf   | OSPF      |
| bgp    | BGP       |
| all    | すべてのプロトコル |

- [初期値]: -
- *kind*

- [設定値]:

| 設定値     | 説明                                      |
|---------|-----------------------------------------|
| include | 指定したネットワークに含まれる経路 ( ネットワークアドレス自身を含む )   |
| refines | 指定したネットワークに含まれる経路 ( ネットワークアドレス自身を含まない ) |
| equal   | 指定したネットワークに一致する経路                       |

- [初期値]: -
- *ip\_address/mask*
- [設定値]: IP アドレス/ネットマスク
- [初期値]: -

**[説明]**

BGP で広告する経路を集約するためのフィルターを定義する。このコマンドで定義したフィルターは、**bgp aggregate** コマンドの *filter* 節で指定されてはじめて効果を持つ。  
*ip\_address/mask* では、ネットワークアドレスを設定する。これは複数設定でき、そのうち、一致するネットワーク長が長い設定が採用される。  
*kind* の前に *reject* キーワードを置くと、その経路は集約されない。

**[適用モデル]**  
 NVR700W

## 26.4 AS 番号の設定

**[書式]**

```
bgp autonomous-system as
no bgp autonomous-system [as]
```

**[設定値及び初期値]**

- *as*
- [設定値]: AS 番号 (1..65535)
- [初期値]: -

**[説明]**

ルーターの AS 番号を設定する。

**[ノート]**

AS 番号を設定するまで BGP は動作しない。

**[適用モデル]**  
 NVR700W

## 26.5 ルーター ID の設定

### [書式]

```
bgp router id ip_address
no bgp router id [ip_address]
```

### [設定値及び初期値]

- *ip\_address*
  - [設定値]: IP アドレス
  - [初期値]: インターフェースに付与されているプライマリアドレスから自動的に選択する。

### [説明]

ルーター ID を設定する。

### [ノート]

ルーター ID が本コマンドで設定されていないときは、以下のインターフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インターフェース
- LOOPBACK インターフェース
- PP インターフェース

なお、プライマリ IPv4 アドレスが付与されたインターフェースがない場合は初期値は設定されない。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか `ospf router id` コマンドのいずれか一方を設定する。Rev.15.00.03 以降のファームウェアでは、本コマンドと `ospf router id` コマンドの両方を設定することができるが、必ず同一のルーター ID を指定する必要がある。

### [適用モデル]

NVR700W

## 26.6 BGP による経路の優先度の設定

### [書式]

```
bgp preference preference
no bgp preference [preference]
```

### [設定値及び初期値]

- *preference*
  - [設定値]: 優先度 (1..2147483647)
  - [初期値]: 500

### [説明]

BGP による経路の優先度を設定する。優先度は 1 以上の整数で示され、数字が大きいほど優先度が高い。BGP とその他のプロトコルで得られた経路が食い違う場合には、優先度の高い経路が採用される。優先度が同じ場合には、先に採用された経路が有効になる。

### [ノート]

各プロトコルに与えられた優先度の初期値は次のとおり。

|        |       |
|--------|-------|
| スタティック | 10000 |
| RIP    | 1000  |
| OSPF   | 2000  |
| BGP    | 500   |

### [適用モデル]

NVR700W

## 26.7 BGP で受信した経路に対するフィルターの適用

### [書式]

```

bgp export remote_as filter filter_num ...
bgp export aspath seq "aspath_regexp" filter filter_num ...
no bgp export remote_as [filter filter_num ...]
no bgp export aspath seq ["aspath_regexp" [filter filter_num ...]]

```

### [設定値及び初期値]

- *remote\_as*
  - [設定値]: 相手の AS 番号 (1..65535)
  - [初期値]: -
- *seq*
  - [設定値]: AS パスを指定したときの評価順序 (1..65535)
  - [初期値]: -
- *aspath\_regexp*
  - [設定値]: 正規表現
  - [初期値]: -
- *filter\_num*
  - [設定値]: フィルター番号 (1..2147483647)
  - [初期値]: -

### [説明]

BGP で受けた経路に対してフィルターを設定する。*remote\_as* を指定してフィルターを設定した場合、接続先から受けた経路についてフィルターに該当した経路が実際のルーティングテーブルに導入され、RIP や OSPF のような他のプロトコルにも通知される。フィルターに該当しない経路はルーティングには適用されず、他のプロトコルに通知されることもない。フィルターの番号には **bgp export filter** コマンドで定義した番号を指定する。

*aspath\_regexp* を指定してフィルターを設定した場合、*remote\_as* を指定した場合と同様に、AS パスが正規表現と一致する経路についてフィルターに該当した経路が導入される。*aspath\_regexp* には **grep** コマンドで使用できる検索パターンを指定する。

*aspath\_regexp* を指定したフィルターを複数設定した場合、*seq* の小さい順に評価される。また、*aspath\_regexp* を指定したフィルターを設定した場合、*remote\_as* を指定したフィルターよりも優先して評価される。

### [ノート]

正規表現によって AS パスを表す例

- すべての AS パスと一致する

```
# bgp export aspath 10 ".*" filter 1
```

- AS 番号が 1000 または 1100 で始まる AS パスと一致する

```
# bgp export aspath 20 "^1[01]00 .*" filter 1
```

- AS 番号に 2000 を含む AS パスと一致する

```
# bgp export aspath 30 "2000" filter 1
```

- AS パスが 3000 3100 3200 であるパスと完全一致する

```
# bgp export aspath 40 "^3000 3100 3200$" filter 1
```

- AS パスに AS\_SET を含むパスと一致する

```
# bgp export aspath 50 "{.*}" filter 1
```

フィルター番号は、101 個まで設定できる。

### [適用モデル]

NVR700W

## 26.8 BGP で受信する経路に適用するフィルターの設定

### [書式]

```

bgp export filter filter_num [reject] kind ip_address/mask ... [parameter ]
no bgp export filter filter_num [[reject] kind ip_address/mask ... [parameter]]

```

### [設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号 (1..2147483647)
  - [初期値]: -
- *kind*
  - [設定値]:

| 設定値     | 説明                                    |
|---------|---------------------------------------|
| include | 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)   |
| refines | 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない) |
| equal   | 指定したネットワークに一致する経路                     |

- [初期値]: -
- *ip\_address/mask*
  - [設定値]:

| 設定値                    | 説明             |
|------------------------|----------------|
| <i>ip_address/mask</i> | IP アドレス/ネットマスク |
| all                    | すべてのネットワーク     |

- [初期値]: -
- *parameter*: TYPE=VALUE の組
  - [設定値]:

| TYPE       | VALUE  | 説明                                |
|------------|--------|-----------------------------------|
| preference | 0..255 | 同じ経路を複数の相手から受信したときに、一方を選択するための優先度 |

- [初期値]: 0

### [説明]

BGP で受信する経路に適用するフィルターを定義する。このコマンドで定義したフィルターは、**bgp export** コマンドの *filter* 節で指定されてはじめて効果を持つ。

*ip\_address/mask* では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。

*kind* の前に **reject** キーワードを置くと、その経路が拒否される。

### [ノート]

*preference* の設定は BGP 経路の間で優先順位をつけるために使用される。BGP 経路の全体の優先度は、**bgp preference** コマンドで設定する。

### [設定例]

```

# bgp export filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp export filter 2 reject equal 192.168.0.0/24

```

### [適用モデル]

NVR700W

## 26.9 BGP に導入する経路に対するフィルターの適用

### [書式]

```
bgp import remote_as protocol [from_as] filter filter_num ...
no bgp import remote_as protocol [from_as] [filter filter_num ...]
```

### [設定値及び初期値]

- *remote\_as*
  - [設定値]: 相手の AS 番号 (1..65535)
  - [初期値]: -
- *protocol*
  - [設定値]:

| 設定値       | 説明   |
|-----------|------|
| static    | 静的経路 |
| rip       | RIP  |
| ospf      | OSPF |
| bgp       | BGP  |
| aggregate | 集約経路 |

- [初期値]: -
- *from\_as*
  - [設定値]: 導入する経路を受信した AS(*protocol* で **bgp** を指定したときのみ) (1..65535)
  - [初期値]: -
- *filter\_num*
  - [設定値]: フィルター番号 (1..2147483647)
  - [初期値]: -

### [説明]

RIP や OSPF のような BGP 以外の経路を導入するときに適用するフィルターを設定する。フィルターに該当しない経路は導入されない。フィルターの番号には、**bgp import filter** コマンドで定義した番号を指定する。BGP の経路を導入するときには、その経路を受信した AS 番号を指定する必要がある。

### [ノート]

このコマンドが設定されていないときには、外部経路は導入されない。  
フィルター番号は、102 個まで設定できる。

### [適用モデル]

NVR700W

## 26.10 BGP の設定の有効化

### [書式]

```
bgp configure refresh
```

### [説明]

BGP の設定を有効にする。BGP の設定を変更したら、ルーターを再起動するか、このコマンドを実行する必要がある。

### [適用モデル]

NVR700W

## 26.11 BGP に導入する経路に適用するフィルターの設定

### [書式]

```
bgp import filter filter_num [reject] kind ip_address/mask ... [parameter ...]
no bgp import filter filter_num [[reject] kind ip_address/mask ... [parameter ...]]
```

### [設定値及び初期値]

- *filter\_num*

- [設定値]: フィルター番号 (1..2147483647)
- [初期値]: -
- *kind*
- [設定値]:

| 設定値     | 説明                                    |
|---------|---------------------------------------|
| include | 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)   |
| refines | 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない) |
| equal   | 指定したネットワークに一致する経路                     |

- [初期値]: -
- *ip\_address/mask*
- [設定値]:

| 設定値             | 説明             |
|-----------------|----------------|
| ip_address/mask | IP アドレス/ネットマスク |
| all             | すべてのネットワーク     |

- [初期値]: -
- *parameter*: TYPE=VALUE の組
- [設定値]:

| TYPE       | VALUE       | 説明                                                              |
|------------|-------------|-----------------------------------------------------------------|
| metric     | 1..16777215 | MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない) |
| preference | 0..255      | 同じ経路を複数の相手から受信したときに、一方を選択するための優先度                               |

- [初期値]:
  - preference=100

### [説明]

BGP に導入する経路に適用するフィルターを定義する。このコマンドで定義したフィルターは、**bgp import** コマンドの *filter* 節で指定されてはじめて効果を持つ。

*ip\_address/mask* では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。

*kind* の前に **reject** キーワードを置くと、その経路が拒否される。

### [設定例]

```
# bgp import filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp import filter 2 reject equal 192.168.0.0/24
```

### [適用モデル]

NVR700W

## 26.12 BGP による接続先の設定

### [書式]

```
bgp neighbor neighbor_id remote_as remote_address [parameter...]
no bgp neighbor neighbor_id [remote_as remote_address [parameter...]]
```

### [設定値及び初期値]

- *neighbor\_id*
- [設定値]: 近隣ルーターの番号 (1...2147483647)

- [初期値]: -
- *remote\_as*
  - [設定値]: 相手の AS 番号 (1..65535)
  - [初期値]: -
- *remote\_address*
  - [設定値]: 相手の IP アドレス
  - [初期値]: -
- *parameter*: TYPE=VALUE の組
  - [設定値]:

| TYPE              | VALUE            | 説明                                       |
|-------------------|------------------|------------------------------------------|
| hold-time         | off、秒数           | ダウン判定までの時間 (3..28,800 秒)                 |
| metric            | 1..21474836      | MED(Multi-Exit Discriminator) で通知するメトリック |
| passive           | on または off       | 能動的な BGP コネクションの接続を抑制するか否か               |
| gateway           | IP アドレス/インターフェース | 接続先に対するゲートウェイ                            |
| local-address     | IP アドレス          | BGP コネクションの自分のアドレス                       |
| ignore-capability | on または off       | capability を無視するか否か                      |

- [初期値]:
  - hold-time=180
  - metric は送信されない
  - passive=off
  - gateway は指定されない
  - local-address は指定されない
  - ignore-capability=off

**[説明]**

BGP コネクションを接続する近隣ルーターを定義する。

**[ノート]**

*hold-time* パラメータに設定した時間の 1/3 程度の間隔で KEEPALIVE メッセージを送信する。*hold-time* パラメータの時間だけ待っても KEEPALIVE メッセージを受信できなかったとき、コネクションがダウンしたものと判断する。

*metric* パラメータはすべての MED の初期値として働くので、**bgp import** コマンドで MED を設定したときにはそれが優先される。

*gateway* では、接続先が同一のセグメントにないときに、その接続先に対するゲートウェイ (ネクストホップ) を指定する。

本コマンドは最大で 32 個までしか設定することはできない。

**[適用モデル]**

NVR700W

## 26.13 BGP のログの設定

**[書式]**

```
bgp log log [log]
no bgp log [log ...]
```

**[設定値及び初期値]**

- *log*
  - [設定値]:

| 設定値      | 説明             |
|----------|----------------|
| neighbor | 近隣ルーターに対する状態遷移 |
| packet   | 送受信したパケット      |

- [初期値]: ログを記録しない。

#### [説明]

指定した種類のログを INFO レベルで記録する。

#### [適用モデル]

NVR700W

## 26.14 インターフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定

#### [書式]

**bgp reric interval** *time*

**no bgp reric interval** [*time*]

#### [設定値及び初期値]

- *time*
  - [設定値]: 秒数 (1 以上の数値)
  - [初期値]: 1

#### [説明]

ルーターのインターフェースの状態が変化するとき、BGP に外部経路を反映させる時間の間隔を設定する。

BGP ではインターフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インターフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

#### [ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。  
 本コマンドの設定値は、OSPF への外部経路の反映にも影響する。本コマンドと **ospf reric interval** コマンドの設定値が食い違う場合には、**ospf reric interval** コマンドの設定値が優先して適用される。  
 本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**bgp configure refresh** コマンドを実行しなくても即時反映される。

NVR700W は Rev.15.00.03 以降で使用可能。

#### [適用モデル]

NVR700W

## 26.15 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値の設定

#### [書式]

**bgp default med** *med*

**no bgp default med** [*med*]

#### [設定値及び初期値]

- *med*
  - [設定値]: MED 値 (1..2147483647)
  - [初期値]: 2147483647



## [説明]

BGP の最適経路選択で、MED 属性が付加されていない経路に対するデフォルトの MED 値を設定する。本コマンドが設定されていない場合、MED 属性が付加されていない経路は最大の MED 値(2147483647)を持つことになり、優先度は最低となる。本コマンドの設定は、MED 属性が付加されている経路には影響しない。

## [ノート]

NVR700W は Rev.15.00.22 以降で使用可能

[適用モデル]  
NVR700W

## 26.16 BGP で受信した経路に対する経路選択の優先順位の規則を設定

## [書式]

```
bgp export route selection rule rule
no bgp export route selection rule [rule]
```

## [設定値及び初期値]

- *rule*
  - [設定値]:

| 設定値       | 説明                           |
|-----------|------------------------------|
| ebgp-only | EBGP で受信した同じ宛先の経路を比較対象とする    |
| all       | 全ての BGP で受信した同じ宛先の経路を比較対象とする |

- [初期値]: ebgp-only

## [説明]

BGP で同じ宛先の経路を複数の相手から受信した際、一方を選択するための優先度による経路選択の規則を設定する。

本コマンドの設定により **bgp export filter** コマンドの *preference* で比較する経路の種別が変更される。*rule* に ebgp-only を設定した場合、EBGP で受信した経路間でのみ *preference* による比較が働く。このため、EBGP と IBGP で受信した経路間では、*preference* による比較は働かない。*rule* に all を設定した場合、全ての BGP で受信した経路間で *preference* による比較が働く。このため、EBGP と IBGP で受信した経路間でも、*preference* による比較が働く。

従来 IBGP で受信した経路は EBGP で受信した経路よりも低い優先度の経路として扱われていたが、*rule* に all を指定することで IBGP で受信した経路の優先度を EBGP で受信した経路よりも高くすることが可能になる。IBGP のみを使用した構成では、本コマンドの設定によって選択される経路が変わることはない。

同じ近隣ルーター番号をもつ近隣ルータから複数の同一宛先経路を受信する場合、本コマンドによって規則を変更した経路選択の優先度に差を設けることはできない。この場合、EBGP であれば MED を、IBGP であれば Local Preference を使用して経路の優先度を設定できる。

本コマンドに対応していないリビジョンでは、*rule* が ebgp-only のときの動作をする。

## [ノート]

本コマンドで動作を設定可能な経路選択プロセスは以下の URL を参照してください。

- [http://www.rtpro.yamaha.co.jp/RT/docs/bgp/index.html#rt\\_select](http://www.rtpro.yamaha.co.jp/RT/docs/bgp/index.html#rt_select)

EBGP と IBGP 間で同じ宛先の経路を受信する環境下で特定の経路を優先するよう制御したい場合、本コマンドを設定することで実現できる。

NVR700W は Rev.15.00.24 以降で使用可能。

[適用モデル]  
NVR700W

## 第 27 章

### IPv6

#### 27.1 共通の設定

##### 27.1.1 IPv6 パケットを扱うか否かの設定

###### [書式]

```
ipv6 routing routing
no ipv6 routing [routing]
```

###### [設定値及び初期値]

- *routing*
  - [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| on  | 処理対象として扱う   |
| off | 処理対象として扱わない |

- [初期値]: on

###### [説明]

IPv6 パケットをルーティングするか否かを設定する。本スイッチを on にしないと PP 側の IPv6 関連は一切動作しない。

off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。

###### [適用モデル]

NVR700W, NVR510

##### 27.1.2 IPv6 インターフェースのリンク MTU の設定

###### [書式]

```
ipv6 interface mtu mtu0
ipv6 pp mtu mtu1
ipv6 tunnel mtu mtu2
no ipv6 interface mtu [mtu0]
no ipv6 pp mtu [mtu1]
no ipv6 tunnel mtu [mtu2]
```

###### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *mtu0*、*mtu1*、*mtu2*
  - [設定値]: MTU の値 (1280..1500)
  - [初期値]:
    - mtu0=1500
    - mtu1=1500
    - mtu2=1280

###### [説明]

IPv6 インターフェースの MTU の値を設定する

###### [ノート]

ipv6 tunnel mtu コマンドは NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 27.1.3 TCP セッションの MSS 制限の設定

#### [書式]

```
ipv6 interface tcp mss limit mss
ipv6 pp tcp mss limit mss
ipv6 tunnel tcp mss limit mss
no ipv6 interface tcp mss limit [mss]
no ipv6 pp tcp mss limit [mss]
no ipv6 tunnel tcp mss limit [mss]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *mss*
  - [設定値]:

| 設定値       | 説明       |
|-----------|----------|
| 536..1440 | MSS の最大長 |
| auto      | 自動設定     |
| off       | 設定しない    |

- [初期値]:
  - off(Rev.15.00.07 以前、Rev.15.01.06 以前)
  - auto(Rev.15.00.10 以降、Rev.15.01.09 以降)

#### [説明]

インターフェースを通過する TCP セッションの MSS を制限する。インターフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード **auto** を指定した場合には、インターフェースの MTU、もしくは PP インターフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

#### [ノート]

PPPoE 用の PP インターフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

[適用モデル]  
NVR700W, NVR510

### 27.1.4 TCP ウィンドウ・スケール・オプションを変更する

#### [書式]

```
ipv6 interface tcp window-scale sw
ipv6 pp tcp window-scale sw
ipv6 tunnel tcp window-scale sw
no ipv6 interface tcp window-scale [...]
no ipv6 pp tcp window-scale [...]
no ipv6 tunnel tcp window-scale [...]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *sw*

- [設定値]:

| 設定値    | 説明                        |
|--------|---------------------------|
| off    | 何もしない                     |
| remove | TCP ウィンドウ・スケール・オプションを削除する |

- [初期値]: off

[説明]

インターフェースを通過する TCP パケットのウィンドウ・スケール・オプションを強制的に変更する。  
remove を指定すると、ウィンドウ・スケール・オプションが有効になっていた場合には、無効にして転送する。

[ノート]

NVR700W は Rev.15.00.03 以降、NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

### 27.1.5 タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かの設定

[書式]

**ipv6 rh0 discard** *switch*  
**no ipv6 rh0 discard**

[設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 破棄する  |
| off | 破棄しない |

- [初期値]: on

[説明]

タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かを選択する。

[適用モデル]

NVR700W, NVR510

### 27.1.6 IPv6 ファストパス機能の設定

[書式]

**ipv6 routing process** *process*  
**no ipv6 routing process**

[設定値及び初期値]

- *process*

- [設定値]:

| 設定値    | 説明                                       |
|--------|------------------------------------------|
| fast   | ファストパス機能を利用する                            |
| normal | ファストパス機能を利用せず、すべての IPv6 パケットをノーマルパスで処理する |

- [初期値]: fast

[説明]

IPv6 パケットの転送をファストパス機能で処理するか、ノーマルパス機能で処理するかを設定する。

## [ノート]

ファストパスでは使用できる機能に制限は無いが、取り扱うパケットの種類によってはファストパスで処理されず、ノーマルパスで処理されることもある。

## [適用モデル]

NVR700W, NVR510

### 27.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケット数の設定

## [書式]

```
ipv6 interface icmp-nd queue length len
no ipv6 interface icmp-nd queue length [len]
```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *len*
  - [設定値]: キュー長 (0..10000)
  - [初期値]: 200

## [説明]

ICMPv6 の Neighbor Discovery のアドレス解決が完了していないホストに対してパケットを送信しようとした時に、アドレス解決が完了するかタイムアウトにより解決できないことが確定するまで、インターフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。

## [ノート]

NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

### 27.1.8 近隣キャッシュの最大エントリー数の設定

## [書式]

```
ipv6 interface neighbor cache max entry num
no ipv6 interface neighbor cache max entry [num]
```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インタフェース名、ONU インターフェース名
  - [初期値]: -
- *num*
  - [設定値]: 最大エントリー数 (256...20480)
  - [初期値]:
    - 1024

## [説明]

インターフェースごとに近隣キャッシュの最大エントリー数を設定する。近隣キャッシュのエントリー数が、設定した最大エントリー数に達した場合は、古い近隣キャッシュを削除する。本コマンド実行時、現在の近隣キャッシュのエントリー数が最大エントリー数を超える場合は、古い近隣キャッシュを削除する。

## [ノート]

NVR700W は Rev.15.00.22 以降で使用可能。

NVR510 は Rev.15.01.21 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

## 27.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定

### [書式]

```
ipv6 reassembly hold-time sec
no ipv6 reassembly hold-time [sec]
```

### [設定値及び初期値]

- *sec*
- [設定値]:

| 設定値            | 説明                          |
|----------------|-----------------------------|
| 秒数 ( 1 .. 60 ) | フラグメントパケットを再構成するために保持しておく時間 |

- [初期値]: 60 秒

### [説明]

IPv6 のフラグメントパケットを再構成するために保持しておく時間。  
 設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。  
 コマンド実行時にすでに保持していたパケットについては変更しない。

### [ノート]

NVR700W は Rev.15.00.22 以降で使用可能。  
 NVR510 は Rev.15.01.21 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 27.1.10 IPv6 パケットの DS フィールドの書き換えの設定

### [書式]

```
ipv6 dscp supersede id dscp filter_num [filter_num_list]
no ipv6 dscp supersede id [dscp]
```

### [設定値及び初期値]

- *id*
  - [設定値]: 識別番号 (1..65535)
  - [初期値]: -
- *dscp*
  - [設定値]:
    - 書き換える DSCP 値 (0..63)
    - 以下のニーモニックが利用できる

| ニーモニック  | DSCP 値 |
|---------|--------|
| default | 0      |
| cs1     | 8      |
| cs2     | 16     |
| cs3     | 24     |
| cs4     | 32     |
| cs5     | 40     |
| cs6     | 48     |
| cs7     | 56     |
| af11    | 10     |
| af12    | 12     |

| ニーモニック | DSCP 値 |
|--------|--------|
| af13   | 14     |
| af21   | 18     |
| af22   | 20     |
| af23   | 22     |
| af31   | 26     |
| af32   | 28     |
| af33   | 30     |
| af41   | 34     |
| af42   | 36     |
| af43   | 38     |
| ef     | 46     |

- [初期値]: -
- *filter\_num*
  - [設定値]: 静的フィルターの番号 (1..21474836)
  - [初期値]: -
- *filter\_num\_list*
  - [設定値]: 静的フィルターの番号 (1..21474836) の並び
  - [初期値]: -

#### [説明]

IPv6 パケットを中継する場合に DS フィールドを指定した値に書き換える。識別番号順にリストをチェックし、*filter\_num* リストのフィルターを順次適用していく。そして、最初にマッチした IPv6 フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。

reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

#### [ノート]

NVR700W は Rev.15.00.24 以降で使用可能。

#### [適用モデル]

NVR700W

## 27.2 IPv6 アドレスの管理

### 27.2.1 インターフェースの IPv6 アドレスの設定

#### [書式]

```

ipv6 interface address ipv6_address/prefix_len [address_type]
ipv6 interface address auto
ipv6 interface address dhcp
ipv6 interface address proxy
ipv6 pp address ipv6_address/prefix_len [address_type]
ipv6 pp address auto
ipv6 pp address dhcp
ipv6 pp address proxy
ipv6 tunnel address ipv6_address/prefix_len [address_type]
ipv6 tunnel address auto
ipv6 tunnel address dhcp
ipv6 tunnel address proxy
no ipv6 interface address ipv6_address/prefix_len [address_type]

```



```
no ipv6 interface address auto
no ipv6 interface address dhcp
no ipv6 interface address proxy
no ipv6 pp address ipv6_address/prefix_len [address_type]
no ipv6 pp address auto
no ipv6 pp address dhcp
no ipv6 pp address proxy
no ipv6 tunnel address ipv6_address/prefix_len [address_type]
no ipv6 tunnel address auto
no ipv6 tunnel address dhcp
no ipv6 tunnel address proxy
```

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、LOOPBACK インターフェース名、ブリッジ インターフェース名
  - [初期値]: -
- *ipv6\_address*
  - [設定値]: IPv6 アドレス部分
  - [初期値]: -
- *prefix\_len*
  - [設定値]: IPv6 プレフィックス長
  - [初期値]: -
- *address\_type*
  - [設定値]:

| 設定値     | 説明      |
|---------|---------|
| unicast | ユニキャスト  |
| anycast | エニーキャスト |

- [初期値]: unicast
- *auto*: RA で取得したプレフィックスとインターフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
  - [初期値]: -
- *dhcp*: DHCPv6 で取得したプレフィックスとインターフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
  - [初期値]: -
- *proxy*: プロキシ
  - [設定値]:
    - *prefix\_type@prefix\_interface[interface\_id/prefix\_len]*

| 設定値         | 説明          |
|-------------|-------------|
| dhcp-prefix | DHCPv6 プロキシ |
| ra-prefix   | RA プロキシ     |

- *prefix\_interface*

| 設定値                     | 説明            |
|-------------------------|---------------|
| <i>prefix_interface</i> | 転送元のインターフェース名 |

- *interface\_id*

| 設定値                 | 説明          |
|---------------------|-------------|
| <i>interface_id</i> | インターフェース ID |

- *prefix\_len*

| 設定値               | 説明            |
|-------------------|---------------|
| <i>prefix_len</i> | IPv6 プレフィックス長 |

- [初期値]:-

#### [説明]

インターフェースに IPv6 アドレスを付与する。

#### [ノート]

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。

複数の LAN インターフェース、または ONU インターフェースでアドレスを自動で設定する機能を利用することができる。

具体的には、RA で取得したプレフィックスとインターフェース ID から IPv6 アドレスを生成する機能と、DHCPv6 で取得したプレフィックスとインターフェース ID から IPv6 アドレスを生成する機能が利用できる。

これらを設定する場合、デフォルト経路は最後に設定が完了したインターフェースに向く。

LOOPBACK インターフェースを指定した場合は、**auto**、**dhcp**、**address\_type**、**proxy** は指定できない。

**prefix\_interface** には LOOPBACK インターフェースは指定できない。

ブリッジインターフェースは NVR700W で指定可能。

#### [設定例]

- LAN2 で受信した RA のプレフィックスに::1 を付け足して IPv6 アドレスを作り、それを LAN1 に付与する

```
# ipv6 lan1 address ra-prefix@lan2::1/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスの IPv6 アドレスを付与する

```
LAN1 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX01::1/64
```

```
LAN3 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX02::1/64
```

```
# ipv6 lan1 address dhcp-prefix@lan2::1:0:0:0:1/64
```

```
# ipv6 lan3 address dhcp-prefix@lan2::2:0:0:0:1/64
```

#### [適用モデル]

NVR700W, NVR510

## 27.2.2 インターフェースのプレフィックスに基づく IPv6 アドレスの設定

#### [書式]

```
ipv6 interface prefix ipv6_prefix/prefix_len
```

```
ipv6 interface prefix proxy
```

```
ipv6 pp prefix ipv6_prefix/prefix_len
```

```
ipv6 pp prefix proxy
```

```
ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
ipv6 tunnel prefix proxy
```

```
no ipv6 interface prefix ipv6_prefix/prefix_len
```

```
no ipv6 interface prefix proxy
```

```
no ipv6 pp prefix ipv6_prefix/prefix_len
```

```
no ipv6 pp prefix proxy
```

```
no ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
no ipv6 tunnel prefix proxy
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、ブリッジインターフェース名
  - [初期値]:-
- *ipv6\_prefix*
  - [設定値]: IPv6 プレフィックスのアドレス部分
  - [初期値]:-
- *prefix\_len*
  - [設定値]: IPv6 プレフィックス長

- [初期値]:-
- *proxy*: プロキシ
- [設定値]:
  - *prefix\_type@prefix\_interface[interface\_id/prefix\_len]*

| 設定値         | 説明          |
|-------------|-------------|
| dhcp-prefix | DHCPv6 プロキシ |
| ra-prefix   | RA プロキシ     |

- *prefix\_interface*

| 設定値                     | 説明            |
|-------------------------|---------------|
| <i>prefix_interface</i> | 転送元のインターフェース名 |

- *interface\_id*

| 設定値                 | 説明          |
|---------------------|-------------|
| <i>interface_id</i> | インターフェース ID |

- *prefix\_len*

| 設定値               | 説明            |
|-------------------|---------------|
| <i>prefix_len</i> | IPv6 プレフィックス長 |

- [初期値]:-

**[説明]**

インターフェースに IPv6 アドレスを付与する。類似のコマンドに **ipv6 interface address** コマンドがあるが、このコマンドではアドレスではなくプレフィックスのみを指定する。プレフィックス以降の部分は MAC アドレスに基づいて自動的に補完する。このときに使用する MAC アドレスは、設定しようとするインターフェースに割り当てられているものが使われる。ただし、MAC アドレスを持たない PP インターフェースやトンネルインターフェースでは LAN1 インターフェースの MAC アドレスを使用する。

なお、類似の名前を持つ **ipv6 prefix** コマンドはルーター広告で通知するプレフィックスを定義するものであり、IPv6 アドレスを付与するものではない。しかしながら、通常の運用では、インターフェースに付与する IPv6 アドレスのプレフィックスとルーター広告で通知するプレフィックスは同じであるから、双方のコマンドに同じプレフィックスを設定することが多い。

**[ノート]**

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。  
*prefix\_interface* には LOOPBACK インターフェースは指定できない。  
 ブリッジインターフェースは NVR700W で指定可能。

**[設定例]**

- LAN2 で受信した RA のプレフィックスを LAN1 に付与する

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスを付与する

```
LAN1 に付与するプレフィックス : XXXX:XXXX:XXXX:XX01::/64
LAN3 に付与するプレフィックス : XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 lan1 prefix dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 lan3 prefix dhcp-prefix@lan2::2:0:0:0:1/64
```

( 注: 内部動作の関係上「dhcp-prefix@lan2::1:0:0:0:0/64」ではなく、「dhcp-prefix@lan2::1:0:0:0:1/64」と設定してください。 )

**[適用モデル]**

NVR700W, NVR510

### 27.2.3 IPv6 プレフィックスに変化があった時にログに記録するか否かの設定

#### [書式]

```

ipv6 interface prefix change log log
ipv6 pp prefix change log log
ipv6 tunnel prefix change log log
no ipv6 interface prefix change log log
no ipv6 pp prefix change log log
no ipv6 tunnel prefix change log log

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *log*
  - [設定値]:

| 設定値 | 説明                       |
|-----|--------------------------|
| on  | IPv6 プレフィックスの変化をログに記録する  |
| off | IPv6 プレフィックスの変化をログに記録しない |

- [初期値]: off

#### [説明]

IPv6 プレフィックスに変化があった時にそれをログに記録するか否かを設定する。  
ログは INFO レベルで記録される。

同じプレフィックスに対するアドレスを複数設定した場合、同じログが複数回表示される。

#### [ノート]

ブリッジインターフェースは NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

### 27.2.4 DHCPv6 の動作の設定

#### [書式]

```

ipv6 interface dhcp service type
ipv6 interface dhcp service client [ir=value]
ipv6 pp dhcp service type
ipv6 pp dhcp service client [ir=value]
ipv6 tunnel dhcp service type
ipv6 tunnel dhcp service client [ir=value]
no ipv6 interface dhcp service
no ipv6 pp dhcp service
no ipv6 tunnel dhcp service

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値 | 説明           |
|-----|--------------|
| off | DHCPv6 を使わない |

| 設定値    | 説明     |
|--------|--------|
| client | クライアント |
| server | サーバー   |

- [初期値]: off
- *value*
- [設定値]:

| 設定値 | 説明                                  |
|-----|-------------------------------------|
| on  | クライアントとして動作する時、Inform-Request を送信する |
| off | クライアントとして動作する時、Solicit を送信する        |

- [初期値]: off

#### [説明]

各インターフェースにおける DHCPv6 の動作を設定する。

#### [適用モデル]

NVR700W, NVR510

## 27.2.5 DAD (Duplicate Address Detection) の送信回数の設定

#### [書式]

```
ipv6 interface dad retry count count
```

```
ipv6 pp dad retry count count
```

```
no ipv6 interface dad retry count [count]
```

```
no ipv6 pp dad retry count [count]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *count*
  - [設定値]: 選択したインターフェースでの DAD の再送回数 (0..10)
  - [初期値]: 1

#### [説明]

インターフェースに IPv6 アドレスが設定されたときに、アドレスの重複を検出するために送信する DAD の送信回数を設定する。ただし、0 を設定した場合は、DAD を送信せずにアドレスを有効なものとして扱う。

#### [ノート]

ブリッジインターフェースは NVR700W で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 27.2.6 自動的に設定される IPv6 アドレスの最大数の設定

#### [書式]

```
ipv6 max auto address max
```

```
no ipv6 max auto address [max]
```

#### [設定値及び初期値]

- *max*
  - [設定値]: 自動的に設定される IPv6 アドレスの 1 インターフェースあたりの最大数 (1..256)
  - [初期値]: 16

**[説明]**

RA によりインターフェースに自動的に設定される IPv6 アドレスの 1 インターフェースあたりの最大数を設定する。

**[適用モデル]**

NVR700W, NVR510

## 27.2.7 始点 IPv6 アドレスを選択する規則の設定

---

**[書式]**

```
ipv6 source address selection rule rule
no ipv6 source address selection rule [rule]
```

**[設定値及び初期値]**

- *rule* : 始点 IPv6 アドレスを選択する規則
  - [設定値] :

| 設定値      | 説明           |
|----------|--------------|
| prefix   | プレフィックスの最長一致 |
| lifetime | 寿命の長い方を優先    |

- [初期値] : prefix

**[説明]**

始点 IPv6 アドレスを選択する規則を設定する。

'prefix' を設定した場合には、終点 IPv6 アドレスと始点 IPv6 アドレス候補とを比較して、先頭から一致している部分 (プレフィックス) がもっとも長いものを始点アドレスとして選択する。

'lifetime' を設定した場合には、IPv6 アドレスの寿命が長いものを優先して選択する。

**[ノート]**

通常は 'prefix' を設定しておけばよいが、アドレスリナンバリングが発生するときには、'lifetime' の設定が有効な場合がある。

**[適用モデル]**

NVR700W, NVR510

## 27.3 近隣探索

---

### 27.3.1 ルーター広告で配布するプレフィックスの定義

---

**[書式]**

```
ipv6 prefix prefix_id prefix/prefix_len [preferred_lifetime=time] [valid_lifetime=time] [l_flag=switch] [a_flag=switch]
ipv6 prefix prefix_id proxy [preferred_lifetime=time] [valid_lifetime=time] [l_flag=switch] [a_flag=switch]
no ipv6 prefix prefix_id
```

**[設定値及び初期値]**

- *prefix\_id*
  - [設定値] : プレフィックス番号
  - [初期値] : -
- *prefix*
  - [設定値] : プレフィックス
  - [初期値] : -
- *prefix\_len*
  - [設定値] : プレフィックス長
  - [初期値] : -
- *proxy* : プロキシ
  - [設定値] :

- *prefix\_type*@*prefix\_interface*[*interface\_id*/*prefix\_len*]

- *prefix\_type*

| 設定値         | 説明          |
|-------------|-------------|
| dhcp-prefix | DHCPv6 プロキシ |
| ra-prefix   | RA プロキシ     |

- *prefix\_interface*

| 設定値                     | 説明            |
|-------------------------|---------------|
| <i>prefix_interface</i> | 転送元のインターフェース名 |

- *interface\_id*

| 設定値                 | 説明          |
|---------------------|-------------|
| <i>interface_id</i> | インターフェース ID |

- *prefix\_len*

| 設定値               | 説明            |
|-------------------|---------------|
| <i>prefix_len</i> | IPv6 プレフィックス長 |

- [初期値]: -
- *preferred\_lifetime*: プレフィックスの推奨寿命 ( 0.4294967295 )
  - [初期値]: 604800
- *valid\_lifetime*: プレフィックスの有効寿命 ( 0.4294967295 )
  - [初期値]: 2592000
- *time*: 時間設定
  - [設定値]:
    - *yyyy-mm-dd*[*hh:mm*[:*ss*]]

| 設定値  | 説明                 |
|------|--------------------|
| yyyy | 年 (1980..2079)     |
| mm   | 月 (01..12)         |
| dd   | 日 (01..31)         |
| hh   | 時 (00..23)         |
| mm   | 分 (00..59)         |
| ss   | 秒 (00..59、省略時は 00) |

- [初期値]: -
- *l\_flag*: on-link フラグ
  - [初期値]: on
- *a\_flag*: autonomous address configuration フラグ
  - [初期値]: on
- *switch*
  - [設定値]:
    - on
    - off
  - [初期値]: -

**[説明]**

ルーター広告で配布するプレフィックスを定義する。実際に広告するためには、**ipv6 interface rtadv send** コマンドの設定が必要である。

*time* では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。*time* として数値 ( 0 以上 4294967295 以下 ) を設定すると、その秒数を寿命として広告する。*time* として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。有効寿命とはアドレスが無効に

なるまでの時間であり、推奨寿命とはアドレスを新たな接続での使用が不可となる時間である。また、`on-link` フラグはプレフィックスがそのデータリンクに固有である時に `on` とする。`autonomous address configuration` フラグはプレフィックスを自律アドレス設定で使うことができる場合に `on` とする。

`prefix_interface` には LOOPBACK インターフェースは指定できない。

#### [ノート]

リンクローカルのプレフィックスを設定することはできない。

ブリッジインターフェースは NVR700W で指定可能。

#### [設定例]

- LAN2 で受信した RA を LAN1 に転送する

```
# ipv6 prefix 1 ra-prefix@lan2::/64
# ipv6 lan1 rtadv send 1
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 から異なる /64 のプレフィックスをルーター広告で配布する

```
LAN1 のルーター広告で配布するプレフィックス : XXXX:XXXX:XXXX:XX01::/64
LAN3 のルーター広告で配布するプレフィックス : XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 prefix 1 dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 prefix 2 dhcp-prefix@lan2::2:0:0:0:1/64
# ipv6 lan1 rtadv send 1
# ipv6 lan3 rtadv send 2
```

( 注 : 内部動作の関係上「dhcp-prefix@lan2::1:0:0:0:0/64」ではなく、「dhcp-prefix@lan2::1:0:0:0:1/64」と設定してください。 )

#### [適用モデル]

NVR700W, NVR510

### 27.3.2 ルーター広告で配布する RDNSS オプションの定義

#### [書式]

```
ipv6 nd ra-rdnss rdns_id dns_ipv6_address [dns_ipv6_address...] [option=value]
```

```
no ipv6 nd ra-rdnss rdns_id [...]
```

#### [設定値及び初期値]

- `rdns_id`
  - [設定値]: RDNSS オプション番号 (1..21474836)
  - [初期値]: -
- `dns_ipv6_address`
  - [設定値]:

| 設定値          | 説明                                |
|--------------|-----------------------------------|
| dhcpv6       | DHCPv6 で通知された DNS サーバーの IPv6 アドレス |
| ipv6_address | 任意の DNS サーバーの IPv6 アドレス           |

- [初期値]: -
- `option=value`: NAME=VALUE の列
  - [設定値]:

| NAME     | VALUE       | 説明                                                                 |
|----------|-------------|--------------------------------------------------------------------|
| lifetime | 秒数、infinity | DNS サーバーの有効時間 (0.4294967294 秒)。infinity は DNS サーバーを無期限で使用できることを示す。 |

- [初期値]:



- lifetime = **ipv6 interface rtadv send** コマンドのルーター広告を送信する最大間隔 (max-rtr-adv-interval) の 3 倍

**[説明]**

ルーター広告で配布する RDNSS オプションを定義する。実際に広告するためには、**ipv6 interface rtadv send** コマンドの rdnss= オプションの設定が必要である。  
 dns\_ipv6\_address は最大 3 つまで指定可能。

**[ノート]**

NVR700W Rev.15.00.23 以降、NVR510 Rev.15.01.23 以降のファームウェアで使用可能。

**[適用モデル]**

NVR700W, NVR510

**27.3.3 ルーター広告の送信の制御**

**[書式]**

```

ipv6 interface rtadv send prefix_id [prefix_id...] [option=value...]
ipv6 pp rtadv send prefix_id [prefix_id...] [option=value...]
no ipv6 interface rtadv send [...]
no ipv6 pp rtadv send [...]
    
```

**[設定値及び初期値]**

- interface
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- prefix\_id
  - [設定値]: プレフィックス番号
  - [初期値]: -
- option=value : NAME=VALUE の列
  - [設定値]:

| NAME                 | VALUE           | 説明                                                                                                      |
|----------------------|-----------------|---------------------------------------------------------------------------------------------------------|
| m_flag               | on、off          | managed address configuration フラグ。ルーター広告による自動設定とは別に、DHCP6 に代表されるルーター広告以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。 |
| o_flag               | on、off          | other stateful configuration フラグ。ルーター広告以外の手段により IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。                |
| prf_flag             | high、medium、low | default router preference フラグ。ルーター広告の優先度を示す設定。                                                          |
| max-rtr-adv-interval | 秒数              | ルーター広告を送信する最大間隔 (4-1,800 秒)                                                                             |
| min-rtr-adv-interval | 秒数              | ルーター広告を送信する最小間隔 (3-1,350 秒)                                                                             |
| adv-default-lifetime | 秒数              | ルーター広告によって設定される端末のデフォルト経路の有効時間 (0-9,000 秒)                                                              |

| NAME               | VALUE                          | 説明                                                                                    |
|--------------------|--------------------------------|---------------------------------------------------------------------------------------|
| adv-reachable-time | ミリ秒数                           | ルーター広告を受信した端末が、ノード間で確認した到達性の有効時間 (0-3,600,000 ミリ秒)                                    |
| adv-retrans-time   | ミリ秒数                           | ルーター広告を再送する間隔 (0-4,294,967,295 ミリ秒)                                                   |
| adv-cur-hop-limit  | ホップ数                           | ルーター広告の限界ホップ数 (0-255)                                                                 |
| mtu                | auto、off、バイト数                  | ルーター広告に MTU オプションを含めるか否かと、含める場合の値の設定。auto の場合はインターフェースの MTU を採用する。                    |
| rdnss              | rdnss、off、dhcpv6、RDNSS オプション番号 | ルーター広告に RDNSS オプションを含めるか否かと、含める場合の値の設定。rdnss の場合は RA の RDNSS オプションで割り当てられたサーバー群を通知する。 |

• [初期値] :

- m\_flag = off
- o\_flag = off
- prf\_flag = medium
- max-rtr-adv-interval = 600
- min-rtr-adv-interval = 200
- adv-default-lifetime = 1800
- adv-reachable-time = 0
- adv-retrans-time = 0
- adv-cur-hop-limit = 64
- mtu=auto
- rdnss=rdnss

#### [説明]

インターフェースごとにルーター広告の送信を制御する。送信されるプレフィックスとして、**ipv6 prefix** コマンドで設定されたものが用いられる。また、オプションとして **m\_flag** および **o\_flag** を利用して、管理するホストがルーター広告以外の自動設定情報をどのように解釈するかを設定することができる。オプションでは、送信するルーター広告の送信間隔や、ルーター広告に含まれる情報の設定を行うこともできる。

#### [ノート]

prf\_flag= オプションは、NVR700W は Rev.15.00.23 以降、NVR510 は Rev.15.01.23 以降のファームウェアで指定可能。  
rdnss= オプションは、NVR700W は Rev.15.00.22 以降、NVR510 は Rev.15.01.21 以降のファームウェアで指定可能。  
rdnss= オプションの RDNSS オプション番号の指定は、NVR700W は Rev.15.00.23 以降、NVR510 Rev.15.01.23 以降のファームウェアで指定可能。

#### [適用モデル]

NVR700W, NVR510

### 27.3.4 ルーター要請の再送機能の設定

#### [書式]

```
ipv6 interface rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC
```

```
ipv6 pp rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC
```

```
no ipv6 interface rtsol max-retransmit [...]
```

```
no ipv6 pp rtsol max-retransmit [...]
```

#### [設定値及び初期値]

- interface
  - [設定値] : LAN インタフェース名
  - [初期値] : -
- MRT

- [設定値]: 最大再送間隔(4..3600(秒))
- [初期値]: 3600
- *MRD*
  - [設定値]: 最大再送継続時間(4..2147483647(秒)または infinity)
  - [初期値]: infinity
- *MRC*
  - [設定値]: 最大再送回数(0..2147483647 または infinity)
  - [初期値]: infinity

**[説明]**

再送間隔は初期値 4 秒から 2 倍ずつ増加していく。初期値は+10%幅、倍率は±10%幅でランダムな値を取る。  
 MRD と MRC の両方を infinity 以外に設定している場合は、MRD と MRC のどちらかの条件が満たされたら再送はストップする。  
 MRC を 0 に設定している場合は再送を行わない。

**[ノート]**

NVR700W は Rev.15.00.16 以降で使用可能。  
 NVR510 は Rev.15.01.15 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 27.4 経路制御

### 27.4.1 IPv6 の経路情報の追加

**[書式]**

**ipv6 route network gateway gateway [parameter] [gateway gateway [parameter]]**

**no ipv6 route network [gateway...]**

**[設定値及び初期値]**

- *network*
  - [設定値]:

| 設定値                | 説明      |
|--------------------|---------|
| IPv6 アドレス/プレフィックス長 | 送り先のホスト |
| default            | デフォルト経路 |

- [初期値]: -
- *gateway*: ゲートウェイ
  - [設定値]:
    - IP アドレス % スコープ識別子
    - *pp peer\_num*: PP インターフェースへの経路
      - *peer\_num*
        - 相手先情報番号
        - anonymous
    - *pp anonymous name=name*

| 設定値  | 説明             |
|------|----------------|
| name | PAP/CHAP による名前 |

- *ra interface*

| 設定値              | 説明                                                                                          |
|------------------|---------------------------------------------------------------------------------------------|
| <i>interface</i> | RA にて決定されるデフォルトゲートウェイを使う場合の、RA クライアントとして動作する LAN インタフェース名、ブリッジインタフェース名(送り先が Default の時のみ有効) |

- *dhcp interface*

| 設定値              | 説明                                                                                              |
|------------------|-------------------------------------------------------------------------------------------------|
| <i>interface</i> | DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名、ブリッジインタフェース名(送り先が Default の時のみ有効) |

- *tunnel tunnel\_num* : トンネルインタフェースへの経路
- LOOPBACK インタフェース名、NULL インタフェース名
- [初期値] :-
- *parameter* : 以下のパラメーターを空白で区切り複数設定可能
- [設定値] :

| 設定値                             | 説明                                                                                                                                                                       |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>filter number [number..]</i> | フィルター型経路の指定 <ul style="list-style-type: none"> <li>• <i>number</i> <ul style="list-style-type: none"> <li>• フィルターの番号 (1..21474836) (空白で区切り複数設定可能)</li> </ul> </li> </ul> |
| <i>metric metric</i>            | メトリックの指定 <ul style="list-style-type: none"> <li>• <i>metric</i> <ul style="list-style-type: none"> <li>• メトリック値 (1..15)</li> <li>• 省略時は 1</li> </ul> </li> </ul>         |
| <i>hide</i>                     | 出力インタフェースが LAN インタフェース、または PP インタフェース、TUNNEL インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する                                                                         |

- [初期値] :-

### [説明]

IPv6 の経路情報を追加する。スコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は **show ipv6 address** コマンドで表示される。

*gateway* のパラメーターとしてフィルター型経路を指定した場合には、記述されている順にフィルターを適用していき、適合したゲートウェイが選択される。

適合するゲートウェイが存在しない場合や、フィルター型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルター型経路が指定されていないゲートウェイが選択される。

フィルター型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。

フィルター型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。

なお LOOPBACK インタフェース、NULL インタフェースは常にアップ状態なので、*hide* オプションは指定はできるものの意味はない。

### [ノート]

*ra interface* は NVR700W Rev.15.00.24 以降、NVR510 Rev.15.01.25 以降のファームウェアで指定可能。

ブリッジインタフェースは NVR700W で指定可能。

*filter* オプションは NVR510 Rev.15.01.25 以降のファームウェアで指定可能。

### [適用モデル]

NVR700W, NVR510

## 27.4.2 IPv6 の経路情報に変化があった時にログに記録するか否かの設定

### [書式]

```
ipv6 route change log log
no ipv6 route change log [log]
```

### [設定値及び初期値]

- *log*
- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | IPv6 経路の変化をログに記録する  |
| off | IPv6 経路の変化をログに記録しない |

- [初期値]: off

### [説明]

IPv6 の経路情報に変化があった時にそれをログに記録するか否かを設定する。  
ログは INFO レベルで記録される。

### [ノート]

NVR700W Rev.15.00.23 以降、NVR510 Rev.15.01.25 以降のファームウェアで使用可能。

### [適用モデル]

NVR700W, NVR510

## 27.5 RIPng

### 27.5.1 RIPng の使用の設定

### [書式]

```
ipv6 rip use use
no ipv6 rip use
```

### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| on  | RIPng を使う   |
| off | RIPng を使わない |

- [初期値]: off

### [説明]

RIPng を使うか否かを設定する。

### [適用モデル]

NVR700W, NVR510

### 27.5.2 インターフェースにおける RIPng の送信ポリシーの設定

### [書式]

```
ipv6 interface rip send send
ipv6 pp rip send send
ipv6 tunnel rip send send
no ipv6 interface rip send
no ipv6 pp rip send
no ipv6 tunnel rip send
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *send*
  - [設定値]:

| 設定値 | 説明           |
|-----|--------------|
| on  | RIPng を送信する  |
| off | RIPng を送信しない |

- [初期値]: on

**[説明]**

RIPng の送信ポリシーを設定する。

**[適用モデル]**

NVR700W, NVR510

### 27.5.3 インターフェースにおける RIPng の受信ポリシーの設定

---

**[書式]**

```

ipv6 interface rip receive receive
ipv6 pp rip receive receive
ipv6 tunnel rip receive receive
no ipv6 interface rip receive
no ipv6 pp rip receive
no ipv6 tunnel rip receive

```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *receive*
  - [設定値]:

| 設定値 | 説明                   |
|-----|----------------------|
| on  | 受信した RIPng パケットを処理する |
| off | 受信した RIPng パケットを無視する |

- [初期値]: on

**[説明]**

RIPng の受信ポリシーを設定する。

**[適用モデル]**

NVR700W, NVR510

### 27.5.4 RIPng の加算ホップ数の設定

---

**[書式]**

```

ipv6 interface rip hop direction hop
ipv6 pp rip hop direction hop
no ipv6 interface rip hop direction
no ipv6 pp rip hop direction

```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *direction*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| in  | 受信時に加算する |
| out | 送信時に加算する |

- [初期値]: -
- *hop*
  - [設定値]: 加算ホップ数 (0..15)
  - [初期値]: 0

#### [説明]

PP インターフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。

#### [適用モデル]

NVR700W, NVR510

## 27.5.5 インターフェースにおける信頼できる RIPng ゲートウェイの設定

#### [書式]

```
ipv6 interface rip trust gateway [except] gateway [gateway...]
ipv6 pp rip trust gateway [except] gateway [gateway...]
no ipv6 interface rip trust gateway [[except] gateway [gateway...]]
no ipv6 pp rip trust gateway [[except] gateway [gateway...]]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *gateway*
  - [設定値]: IPv6 アドレス
  - [初期値]: -

#### [説明]

信頼できる RIPng ゲートウェイを設定する。

*except* キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

*except* キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

*gateway* は 10 個まで指定可能。

#### [適用モデル]

NVR700W, NVR510

## 27.5.6 RIPng で送受信する経路に対するフィルタリングの設定

#### [書式]

```
ipv6 interface rip filter direction filter_list [filter_list...]
ipv6 pp rip filter direction filter_list [filter_list...]
ipv6 tunnel rip filter direction filter_list [filter_list...]
no ipv6 interface rip filter direction
no ipv6 pp rip filter direction
no ipv6 tunnel rip filter direction
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *direction*

- [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| in  | 内向きのパケットを対象にする |
| out | 外向きのパケットを対象にする |

- [初期値]: -
- *filter\_list*
  - [設定値]: フィルター番号
  - [初期値]: -

#### [説明]

インターフェースで送受信する RIPng パケットに対して適用するフィルターを設定する。

#### [適用モデル]

NVR700W, NVR510

## 27.5.7 回線接続時の PP 側の RIPng の動作の設定

#### [書式]

```
ipv6 pp rip connect send action
no ipv6 pp rip connect send
```

#### [設定値及び初期値]

- *action*
  - [設定値]:

| 設定値      | 説明                                                              |
|----------|-----------------------------------------------------------------|
| none     | RIPng を送信しない                                                    |
| interval | <b>ipv6 pp rip connect interval</b> コマンドで設定された時間間隔で RIPng を送出する |
| update   | 経路情報が変わった時にのみ RIPng を送出する                                       |

- [初期値]: update

#### [説明]

選択されている相手について回線接続時に RIPng を送出する条件を設定する。

#### [設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

#### [適用モデル]

NVR700W, NVR510

## 27.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

#### [書式]

```
ipv6 pp rip connect interval time
no ipv6 pp rip connect interval
```

#### [設定値及び初期値]

- *time*
  - [設定値]: 秒数 (30..21474836)
  - [初期値]: 30

#### [説明]

選択されている相手について回線接続時に RIPng を送出する時間間隔を設定する。

#### [設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```



[適用モデル]  
NVR700W, NVR510

### 27.5.9 回線切断時の PP 側の RIPng の動作の設定

#### [書式]

```
ipv6 pp rip disconnect send action
no ipv6 pp rip disconnect send
```

#### [設定値及び初期値]

- *action*
- [設定値]:

| 設定値      | 説明                                                              |
|----------|-----------------------------------------------------------------|
| none     | RIPng を送信しない                                                    |
| interval | <b>ipv6 pp rip connect interval</b> コマンドで設定された時間間隔で RIPng を送出する |
| update   | 経路情報が変わった時にのみ RIPng を送信する                                       |

- [初期値]: none

#### [説明]

選択されている相手について回線切断時に RIPng を送出する条件を設定する。

#### [設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]  
NVR700W, NVR510

### 27.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

#### [書式]

```
ipv6 pp rip disconnect interval time
no ipv6 pp rip disconnect interval
```

#### [設定値及び初期値]

- *time*
- [設定値]: 秒数 (30..21474836)
- [初期値]: 3600

#### [説明]

選択されている相手について回線切断時に RIPng を送出する時間間隔を設定する。

#### [設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]  
NVR700W, NVR510

### 27.5.11 RIPng による経路を回線切断時に保持するか否かの設定

#### [書式]

```
ipv6 pp rip hold routing hold
no ipv6 pp rip hold routing
```

#### [設定値及び初期値]

- *hold*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 保持する  |
| off | 保持しない |

- [初期値]: off

#### [説明]

PP インターフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 27.5.12 RIPng による経路の優先度の設定

#### [書式]

```
ipv6 rip preference preference
no ipv6 rip preference [preference]
```

#### [設定値及び初期値]

- *preference*
  - [設定値]: RIPng による経路の優先度 (1-2147483647)
  - [初期値]: 1000

#### [説明]

RIPng による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。RIPng とスタティックなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

#### [ノート]

静的経路の優先度は 10000 で固定である。

#### [適用モデル]

NVR700W, NVR510

## 27.6 VRRPv3 の設定

### 27.6.1 インターフェース毎の VRRPv3 の設定

#### [書式]

```
ipv6 interface vrrp vrid ipv6_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
no ipv6 interface vrrp vrid [vrid...]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*
  - [設定値]: VRRPv3 グループ ID (1..255)
  - [初期値]: -
- *ipv6\_address*
  - [設定値]: 仮想ルーターの IPv6 アドレス
  - [初期値]: -
- *priority*
  - [設定値]: 優先度 (1..254)
  - [初期値]: 100
- *preempt*: プリエンプトモード
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *auth*
  - [設定値]: テキスト認証文字列 (8 文字以内)
  - [初期値]: -
- *time1*
  - [設定値]: VRRPv3 広告の送信間隔 (1..60 秒)
  - [初期値]: 1
- *time2*
  - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
  - [初期値]: 3

#### [説明]

指定した VRRPv3 グループを利用することを設定する。

同じ VRRPv3 グループに所属するルーターの間では、VRID および仮想ルーターの IPv6 アドレスを一致させておかななくてはならない。これらが食い違った場合の動作は予測できない。

*auth* パラメーターを指定しない場合には、認証なしとして動作する。

*time1* および *time2* パラメーターで、マスターが VRRPv3 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRPv3 ルーターで一致している必要がある。

#### [ノート]

*priority* および *preempt* パラメーターの設定は、仮想ルーターの IPv6 アドレスとして自分自身の LAN インターフェースに付与されているアドレスを指定している場合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。

#### [適用モデル]

NVR700W

## 27.6.2 シャットダウントリガーの設定

#### [書式]

```

ipv6 interface vrrp shutdown trigger vrid interface
ipv6 interface vrrp shutdown trigger vrid pp peer_num
ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
ipv6 interface vrrp shutdown trigger vrid route network [nexthop]
no ipv6 interface vrrp shutdown trigger vrid interface
no ipv6 interface vrrp shutdown trigger vrid pp peer_num [...]
no ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
no ipv6 interface vrrp shutdown trigger vrid route network

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*
  - [設定値]: VRRPv3 グループ ID (1..255)
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*

- [設定値]: tunnel インターフェース 番号
- [初期値]: -
- *network*
  - [設定値]:
    - IPv6 プレフィックス/プレフィックス長
    - default
  - [初期値]: -
- *nexthop*
  - [設定値]:
    - インターフェース名
    - IPv6 アドレス
  - [初期値]: -

#### [説明]

設定した VRRPv3 グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

| 形式             | 説明                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LAN インターフェース形式 | 指定した LAN インターフェースがリンクダウンするか、あるいは <b>lan keepalive</b> でダウンが検知されると、シャットダウンする。                                                                                                                                                                                                                                                                                                                       |
| pp 形式          | 指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。 <ul style="list-style-type: none"> <li>• <b>pp keepalive use</b> 設定によりダウンが検出された場合</li> </ul>                                                                                                                                                                                                                 |
| tunnel 形式      | 指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。 <ul style="list-style-type: none"> <li>• IPsec トンネルで、<b>ipsec ike keepalive use</b> 設定によりダウンが検出された場合</li> <li>• L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、<b>l2tp keepalive use</b> 設定によりダウンが検出された場合</li> <li>• PPTP トンネルで、<b>pptp keepalive use</b> 設定によりダウンが検出された場合</li> <li>• IPIP トンネルで、<b>ipip keepalive use</b> 設定によりダウンが検出された場合</li> </ul> |
| route 形式       | 指定した経路が経路テーブルに存在しないか、 <i>nexthop</i> で指定したインターフェースもしくは IPv6 アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。 <i>nexthop</i> を省略した場合には、経路がどのような先に向いていても存在する限りはシャットダウンしない。                                                                                                                                                                                                                                       |

#### [ノート]

tunnel インターフェースは Rev.15.00.14 以降のファームウェアで使用可能。

#### [適用モデル]

NVR700W

## 27.7 フィルターの設定

### 27.7.1 IPv6 フィルターの定義

#### [書式]

```
ipv6 filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len]] [protocol [src_port_list [dest_port_list]]]
no ipv6 filter filter_num [pass_reject]
```

[設定値及び初期値]

- *filter\_num*
  - [設定値]: 静的フィルター番号 (1..21474836)
  - [初期値]: -
- *pass\_reject*
  - [設定値]: フィルターのタイプ (**ip filter** コマンドに準ずる)
  - [初期値]: -
- *src\_addr*: IPv6 パケットの始点 IPv6 アドレス
  - [設定値]:
    - IPv6 アドレス
      - 静的または動的 IPv6 アドレス
      - , を区切りとして複数設定することができる。
    - FQDN
      - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
      - \* から始まる FQDN は \* より後ろの文字列を後方一致条件として判断する 例えば \*.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
      - , を区切りとして複数設定することができる。
    - map-e
      - MAP-E により付与されたグローバル IPv4 アドレスを表すキーワード
      - \* (すべての IPv6 アドレスに対応)
  - [初期値]: -
- *prefix\_len*
  - [設定値]: プレフィックス長
  - [初期値]: -
- *dest\_addr*: IPv6 パケットの終点 IPv6 アドレス
  - [設定値]:
    - *src\_addr* と同じ形式
    - 省略した場合は一個の \* と同じ
  - [初期値]: -
- *protocol*: フィルタリングするパケットの種類 (**ip filter** コマンドに準ずる)
  - [設定値]:

|         |                                                                       |
|---------|-----------------------------------------------------------------------|
| icmp-nd | 近隣探索に関するパケットの指定を示すキーワード。(TYPE が 133、134、135、136 のいずれかである ICMPv6 パケット) |
| icmp4   | ICMPv4 パケットの指定を示すキーワード                                                |
| icmp    | ICMPv6 パケットの指定を示すキーワード                                                |
| icmp6   |                                                                       |

- [初期値]: -
- *src\_port\_list*
  - [設定値]: TCP/UDP のソースポート番号、あるいは ICMPv6 タイプ (**ip filter** コマンドに準ずる)
  - [初期値]: -
- *dest\_port\_list*
  - [設定値]: TCP/UDP のデスティネーションポート番号、あるいは ICMPv6 コード
  - [初期値]: -

[説明]

IPv6 のフィルターを定義する。

[ノート]

近隣探索に関するパケットとは以下の 4 つを意味する。

- 133: Router Solicitation
- 134: Router Advertisement
- 135: Neighbor Solicitation
- 136: Neighbor Advertisement

`src_addr` および `dest_addr` は IPv6 アドレス と FQDN と `map-e` を混合することも可能。

`src_addr` および `dest_addr` への FQDN の指定は NVR700W Rev.15.00.23 以降、NVR510 Rev.15.01.23 以降で指定可能。  
`src_addr` および `dest_addr` に FQDN を指定することによって、固定 IP アドレスではないサーバーや 1 つの FQDN に対して複数の固定 IP アドレスを持つサーバーを対象にしたフィルタリングを行うことができる。FQDN を使用する場合、ルーター自身が DNS リカーシブサーバーとして動作し、ルーター配下の端末は DNS サーバーとして本機を指定する必要がある。

指定した FQDN に一致する通信が発生した場合、設定した FQDN に該当する IPv6 アドレスの情報が保持される。保持される期間は、`ip filter fqdn timer` コマンドで指定できる。

`src_addr` および `dest_addr` への `map-e` の指定は NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で指定可能。

### [設定例]

```
PP 1 で送受信される IPv6 Packet Too Big を記録する
# pp select 1
# ip pp secure filter in 1 100
# ip pp secure filter out 1 100
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

### [適用モデル]

NVR700W, NVR510

## 27.7.2 IPv6 フィルターの適用

### [書式]

```
ipv6 interface secure filter direction [filter_list...] [dynamic filter_list]
ipv6 pp secure filter direction [filter_list...] [dynamic filter_list]
ipv6 tunnel secure filter direction [filter_list...] [dynamic filter_list]
no ipv6 interface secure filter direction
no ipv6 pp secure filter direction
no ipv6 tunnel secure filter direction
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、LOOPBACK インターフェース名、NULL インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *direction*
  - [設定値]:

| 設定値 | 説明               |
|-----|------------------|
| in  | 受信したパケットのフィルタリング |
| out | 送信するパケットのフィルタリング |

- [初期値]: -
- *filter\_list*
  - [設定値]: 空白で区切られたフィルター番号の並び (静的フィルターと動的フィルターの数の合計として 129 個以内)
  - [初期値]: -
- *dynamic*: キーワード後に動的フィルターの番号を記述する
  - [初期値]: -

### [説明]

IPv6 フィルターをインターフェースに適用する。

[ノート]

LOOPBACK インターフェースと NULL インターフェースでは動的フィルターは使用できない。  
 NULL インターフェースで *direction* に 'in' は指定できない。  
 ブリッジインターフェースは NVR700W で指定可能。

[適用モデル]

NVR700W, NVR510

### 27.7.3 IPv6 動的フィルターの定義

[書式]

**ipv6 filter dynamic** *dyn\_filter\_num srcaddr[/prefix\_len] dstaddr[/prefix\_len] protocol [option ...]*

**ipv6 filter dynamic** *dyn\_filter\_num srcaddr[/prefix\_len] dstaddr[/prefix\_len] filter filter\_list [in filter\_list] [out filter\_list] [option ...]*

**no ipv6 filter dynamic** *dyn\_filter\_num [srcaddr ...]*

[設定値及び初期値]

- *dyn\_filter\_num*
  - [設定値]: 動的フィルター番号 (1..21474836)
  - [初期値]: -
- *srcaddr*: IPv6 パケットの始点 IPv6 アドレス
  - [設定値]:
    - **ipv6 filter** コマンドの *src\_addr* と同じ形式
    - 省略した場合は一個の \* と同じ
  - [初期値]: -
- *prefix\_len*
  - [設定値]: プレフィックス長
  - [初期値]: -
- *dstaddr*: IPv6 パケットの終点 IPv6 アドレス
  - [設定値]:
    - *srcaddr* と同じ形式
    - 省略した場合は一個の \* と同じ
  - [初期値]: -
- *protocol*: プロトコルのニーモニック
  - [設定値]:
    - echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/dhcps/
    - dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/
    - netbios\_ns/netbios\_dgm/netbios\_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
    - https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
    - dhcpv6c/dhcpv6s/ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
    - ping/ping6/tcp/udp
    - submission
  - [初期値]: -
- *filter\_list*
  - [設定値]: **ipv6 filter** コマンドで登録されたフィルター番号のリスト
  - [初期値]: -
- *option*
  - [設定値]:
    - syslog=*switch*

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | 接続の通信履歴を syslog に残す   |
| off | 接続の通信履歴を syslog に残さない |

- timeout=*time*

| 設定値  | 説明                           |
|------|------------------------------|
| time | データが流れなくなったときに接続情報を解放するまでの秒数 |

- [初期値]:
  - syslog=on
  - timeout=60

### [説明]

IPv6 の動的フィルターを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザーがアクセス制御のルールを記述する。キーワードの `filter`、`in`、`out` の後には、**ipv6 filter** コマンドで定義されたフィルター番号を設定する。

`filter` キーワードの後に記述されたフィルターに該当する接続 (トリガー) を検出したら、それ以降 `in` キーワードと `out` キーワードの後に記述されたフィルターに該当する接続を通過させる。`in` キーワードはトリガーの方向に対して逆方向のアクセスを制御し、`out` キーワードは動的フィルターと同じ方向のアクセスを制御する。なお、**ipv6 filter** コマンドの IP アドレスは無視される。`pass/reject` の引数も同様に無視される。ここに記載されていないアプリケーションについては、`filter` キーワードを使って定義することで扱える可能性がある。特に `snmp` のように動的にポート番号が変化しないプロトコルの扱いは容易である。

`tcp` か `udp` を設定することで扱える可能性がある。特に、`telnet` のように動的にポート番号が変化しないプロトコルは `tcp` を指定することで扱うことができる。

### [ノート]

`srcaddr` および `dstaddr` は IPv6 アドレスと FQDN と `map-e` を混合することも可能。

`srcaddr` および `dstaddr` への FQDN の指定は NVR700W Rev.15.00.23 以降、NVR510 Rev.15.01.23 以降で指定可能。

`srcaddr` および `dstaddr` への `map-e` の指定は NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で指定可能。

### [適用モデル]

NVR700W, NVR510

## 27.8 IPv6 マルチキャストパケットの転送の設定

MLDv1、MLDv2、MLD プロキシの機能を提供します。MLDv1 と MLDv2 については、ホスト側とルーター側の双方に対応し、インターフェースごとにホストとルーターの機能を使い分けることができます。MLDv1 は RFC2710、MLDv2 は `draft-vida-mldv2-07.txt` に対応します。MLD プロキシは、下流のインターフェースに存在するリスナーの情報を、上流のインターフェースに中継する機能であり、`draft-ietf-magma-igmp-proxy-04.txt` に基づいて実装しています。

特定の端末が送信するマルチキャストパケットを複製して、複数の端末に配送します。マルチキャストパケットを送信する端末をソース (`source`) と呼び、それを受信する端末をリスナー (`listener`) と呼びます。以下の説明では、マルチキャストパケットを単にパケットと書きます。

ソースが送信するパケットは原則としてすべてのリスナーに届きます。しかし、リスナーによって受信するパケットを変えたければ、リスナーをグループに分けることができます。同じグループに属する端末は同じパケットを受信し、異なるグループに属する端末は異なるパケットを受信します。それぞれのグループには識別子としてマルチキャストアドレスが割り当てられます。

パケットの IP ヘッダの終点アドレスには、グループに対応するマルチキャストアドレスが格納されます。網内のルーターは、このマルチキャストアドレスを見て、パケットの転送先のグループを確認します。網内のルーターはグループごとに編成された経路表を持っているので、その経路表にしたがってパケットを配布します。経路表は、通常、PIM-SM、PIM-DM、DVMRP などのルーティングプロトコルによって自動的に生成されます。

MLD (MulticastListenerDiscovery) の目的は、端末がマルチキャスト網に対して、端末が参加するグループを通知することです。

網内のルーターは端末に対してクエリー (`Query`) というメッセージを送信します。クエリーを受信した端末は、ルーターに対してレポート (`Report`) というメッセージを返信します。レポートの中には、端末が参加するグループのマルチキャストアドレスを格納します。レポートを受信したルーターはその情報をルーティングに反映します。

MLDv2 では、受信するパケットのソースを制限することができますが、この機能を実現するためにフィルターモー



ド (FilterMode) とソースリスト (SourceList) を使用します。フィルターモードには INCLUDE と EXCLUDE があり、INCLUDE では許可するソースを列挙し、EXCLUDE では許可しないソースを列挙します。

例えば、次の場合には、2001:x:x:x::1 と 2001:x:x:x::2 をソースとするパケットだけが転送の対象になります。

- フィルターモード : INCLUDE
- ソースリスト : { 2001:x:x:x::1, 2001:x:x:x::2 }

MLD のメッセージは原則としてルーターを超えることができません。そこで、端末とマルチキャスト網の間にルーターが介在する場合には、ルーターが MLD プロキシの機能を持つ必要があります。MLD プロキシの機能を持つルーターは、LAN 側に対してクエリを送信し、LAN 側からレポートを受信します。また、そのレポートに含まれる情報を WAN 側に転送します。

### 27.8.1 MLD の動作の設定

#### [書式]

```

ipv6 interface mld type [option ...]
ipv6 pp mld type [option ...]
ipv6 tunnel mld type [option ...]
no ipv6 interface mld [type [option ...]]
no ipv6 pp mld [type [option ...]]
no ipv6 tunnel mld [type [option ...]]
    
```

#### [設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名、ONU インターフェース名
  - [初期値] : -
- *type* : MLD の動作方式
  - [設定値] :

| 設定値    | 説明              |
|--------|-----------------|
| off    | MLD は動作しない      |
| router | MLD ルーターとして動作する |
| host   | MLD ホストとして動作する  |

- [初期値] : off
- *option* : オプション
  - [設定値] :
    - version=*version*
      - MLD のバージョン

| 設定値 | 説明                                   |
|-----|--------------------------------------|
| 1   | MLDv1                                |
| 2   | MLDv2                                |
| 1,2 | MLDv1 と MLDv2 の両方に対応する。(MLDv1 互換モード) |

- *syslog=switch*
  - 詳細な情報を syslog に出力するか否か

| 設定値 | 説明    |
|-----|-------|
| on  | 表示する  |
| off | 表示しない |

- *robust-variable=VALUE (1..10)*
  - MLD で規定される Robust Variable の値を設定する。
- *report-link-local-group=switch*
  - リンクローカルスコープのグループを処理するか否か

| 設定値 | 説明                                                                                                  |
|-----|-----------------------------------------------------------------------------------------------------|
| on  | MLD ルーターとして動作しているとき、リンクローカルスコープのグループのレポート受信を有効にする。MLD ホストとして動作しているとき、リンクローカルスコープのグループのレポート送信を有効にする。 |
| off | リンクローカルスコープのグループのレポート送受信を無効にする。                                                                     |

- [初期値]:
  - version=1,2
  - syslog=off
  - robust-variable=2
  - report-link-local-group=off

**[説明]**

インターフェースの MLD の動作を設定する。

**[ノート]**

report-link-local-group オプションは、NVR700W の Rev.15.00.03 以降、NVR510 の Rev.15.01.03 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 27.8.2 MLD の静的な設定

**[書式]**

```

ipv6 interface mld static group [filter_mode [source...]]
ipv6 pp mld static group [filter_mode [source...]]
ipv6 tunnel mld static group [filter_mode [source...]]
no ipv6 interface mld static group [filter_mode source...]
no pv6 pp mld static group [filter_mode source...]
no ipv6 tunnel mld static group [filter_mode source...]

```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *group*
  - [設定値]: グループのマルチキャストアドレス
  - [初期値]: -
- *filter\_mode*: フィルターモード
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| include | MLD の "INCLUDE" モード |
| exclude | MLD の "EXCLUDE" モード |

- [初期値]: -

• *source*

- [設定値]:

| 設定値       | 説明                         |
|-----------|----------------------------|
| IPv6 アドレス | マルチキャストパケットの送信元アドレス        |
| 省略        | 省略時はすべての送信元アドレスに対して同様に動作する |

- [初期値]: -

**[説明]**

指定したグループについて、常にリスナーが存在するものとみなす。このコマンドは、MLDをサポートするリスナーがないときに設定する。*filter\_mode* と *source* は、マルチキャストパケットの送信元を限定するものである。*filter\_mode* として *include* を指定したときには、*source* として受信したい送信元を列挙する。*source* を省略した場合は、全ての送信元からの要求を受信しない。*filter\_mode* として *exclude* を指定したときには、*source* として受信したくない送信元を列挙する。*source* を省略した場合は、全ての送信元からの要求を受信する。

**[ノート]**

このコマンドで設定されたリスナーは、**ipv6 interface mld** コマンドで *host* を設定したインターフェースで通知される。もし、このインターフェースが MLDv1 を使う場合には、*filter\_mode* や *source* の値は無視される。

**[適用モデル]**

NVR700W, NVR510

## 27.9 近隣要請

### 27.9.1 アドレス重複チェックをトリガーに近隣要請を行うか否かの設定

**[書式]**

```
ipv6 nd ns-trigger-dad on [option=value]
ipv6 nd ns-trigger-dad off
no ipv6 nd ns-trigger-dad [...]
```

**[設定値及び初期値]**

- on
  - [設定値]: 近隣要請を行う
  - [初期値]: -
- off
  - [設定値]: 近隣要請を行わない
  - [初期値]: -
- *option=value* 列: MLD の動作方式
  - [設定値]:

| <i>option</i> | <i>value</i>     | 説明                                                 |
|---------------|------------------|----------------------------------------------------|
| na-proxy      | all              | 近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告はすべてプロキシする          |
|               | discard-one-time | 近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告を一回のみ破棄し、その後はプロキシする |

- [初期値]: na-proxy=all

**[初期設定]**

```
ipv6 nd ns-trigger-dad off
```

**[説明]**

RA プロキシにおいて、下流よりアドレス重複チェックの近隣要請を受信した際に、そのグローバルアドレスを送信元とした近隣要請を上流に送信するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

## 第 28 章

### OSPFv3

#### 28.1 OSPFv3 の有効設定

**[書式]**

```
ipv6 ospf configure refresh
```

**[説明]**

OSPFv3 の設定を有効にする。OSPFv3 関係の設定を変更したら、ルーターを再起動するか、あるいはこのコマンドを実行しなくてはならない。

**[ノート]**

このコマンドを入力したとき、次のいずれかならば、OSPFv3 の設定は有効にならない。

- ルーター ID が設定されていない
- エリアが設定されていない
- いずれのインターフェースもエリアに属していない
- 仮想リンクが経由するエリアが存在しない
- 仮想リンクが経由するエリアに属するインターフェースが存在しない

すでに OSPFv3 の設定が有効であるときにこのコマンドを入力した場合、初期状態から再度設定を読み込む。よって、それまで OSPFv3 が保持していた経路情報や、他のプロトコルに配布した経路情報は一旦破棄され、初期状態から動作を開始する。

**[適用モデル]**

NVR700W

#### 28.2 OSPFv3 の使用設定

**[書式]**

```
ipv6 ospf use use
no ipv6 ospf use [use]
```

**[設定値及び初期値]**

- *use*
- [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | OSPFv3 を使用する  |
| off | OSPFv3 を使用しない |

- [初期値]: off

**[説明]**

OSPFv3 を使用するか否かを設定する。

**[適用モデル]**

NVR700W

#### 28.3 OSPFv3 のルーター ID 設定

**[書式]**

```
ipv6 ospf router id router-id
no ipv6 ospf router id [router-id]
```

**[設定値及び初期値]**

- *router\_id*
- [設定値]: IPv4 アドレス表記 (0.0.0.0 は不可)

- [初期値]:-

**[説明]**

ルーター ID を設定する。

**[ノート]**

**ipv6 ospf configure refresh** コマンドが入力されたとき、このコマンドによってルーター ID が設定されていない場合、以下の順序でインターフェースに付与されているプライマリ IPv4 アドレスを探索して最初に見つかった IPv4 アドレスをルーター ID として使用する。

- LAN インターフェース (若番順)
- ONU インターフェース
- LOOPBACK インターフェース (若番順)

プライマリ IPv4 アドレスが付与されたインターフェースがない場合は初期値は設定されない。

**[適用モデル]**

NVR700W

## 28.4 OSPFv3 エリア設定

**[書式]**

```
ipv6 ospf area area [stub [cost=cost]]
no ipv6 ospf area area [stub [cost=cost]]
```

**[設定値及び初期値]**

- *area*
  - [設定値]:

| 設定値                       | 説明         |
|---------------------------|------------|
| backbone                  | バックボーンエリア  |
| 1 以上の数値 (1...4294967295)  | 非バックボーンエリア |
| IPv4 アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]:-
- *cost*
  - [設定値]: デフォルト経路のコスト (0~16777215)
  - [初期値]: 0

**[説明]**

OSPFv3 エリアを設定する。

stub キーワードを指定した場合、そのエリアはスタブエリアであることを表わす。cost は 0 以上の数値で、エリア境界ルーターがエリア内に広告するデフォルト経路のコストとして使われる。cost を指定しないとデフォルト経路の広告は行われない。

**[適用モデル]**

NVR700W

## 28.5 エリアへの経路広告

**[書式]**

```
ipv6 ospf area network area ipv6_prefix/prefix_len [restrict]
no ipv6 ospf area network area ipv6_prefix/prefix_len [restrict]
```

**[設定値及び初期値]**

- *area*
  - [設定値]:

| 設定値                      | 説明         |
|--------------------------|------------|
| backbone                 | バックボーンエリア  |
| 1 以上の数値 (1...4294967295) | 非バックボーンエリア |

| 設定値                       | 説明         |
|---------------------------|------------|
| IPv4 アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -
- *ipv6\_prefix/prefix\_len*
  - [設定値]: IPv6 プレフィックス
  - [初期値]: サブネットの範囲は設定されていない

**[説明]**

エリア境界ルーターが他のエリアに経路を広告する場合に、このコマンドで指定したサブネットの範囲内の経路は単一のサブネット経路として広告する。**restrict** キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

**[適用モデル]**

NVR700W

## 28.6 指定インターフェースの OSPFv3 エリア設定

**[書式]**

```

ipv6 interface ospf area area [parameters ...]
ipv6 pp ospf area area [parameters...]
ipv6 tunnel ospf area area [parameters...]
no ipv6 interface ospf area [area [parameters...]]
no ipv6 pp ospf area [area [parameters...]]
no ipv6 tunnel ospf area [area [parameters...]]

```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、LOOPBACK インターフェース名
  - [初期値]: -
- *area*
  - [設定値]:

| 設定値                       | 説明         |
|---------------------------|------------|
| backbone                  | バックボーンエリア  |
| 1 以上の数値 (1...4294967295)  | 非バックボーンエリア |
| IPv4 アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: インターフェースは OSPF エリアに属していない
- *parameters*
  - [設定値]: NAME=VALUE の列
  - [初期値]:
    - **type=broadcast**(LAN インターフェース、ONU インターフェース設定時)
    - **type=point-to-point**(PP インターフェース設定時、トンネルインターフェース設定時)
    - **passive**=インターフェースは **passive** ではない
    - **cost=1**(LAN インターフェース、ONU インターフェース設定時)、**1562**(トンネル設定時)、**pp** は回線速度に依存
    - **priority=1**
    - **retransmit-interval=5** 秒
    - **transmit-delay=1** 秒
    - **hello-interval=10** 秒
    - **dead-interval=40** 秒

**[説明]**

指定したインターフェースの属する OSPFv3 エリアを設定する。NAME パラメーターの **type** はインターフェースの接続するリンクがどのようなタイプであるかを設定する。*parameters* では、リンクパラメーターを設定する。パラメーターは NAME=VALUE の形で指定され、以下の種類がある。

| NAME                | VALUE           | 説明                                                                                                                                                                                                                                    |
|---------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type                | broadcast       | ブロードキャスト型                                                                                                                                                                                                                             |
|                     | point-to-point  | ポイント・ポイント型                                                                                                                                                                                                                            |
| passive             |                 | インターフェースに対して、OSPFv3 パケットを送信しない。該当インターフェースに他の OSPFv3 ルーターがない場合に設定する。                                                                                                                                                                   |
| cost                | コスト (1...65535) | インターフェースのコストを設定する。初期値はインターフェースの種類と回線速度によって決定される。LAN インターフェースと ONU インターフェースの場合は 1、トンネルインターフェースの場合は 1562、PP インターフェースの場合は、バインドされている回線の回線速度を S[kbit/s]とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。<br>cost=100000/S |
| priority            | 優先度 (0...255)   | 指定ルーター選択の際の優先度を設定する。値が大きいルーターが指名ルーターに選ばれる。0 を指定すると指定ルーターに選ばれなくなる。                                                                                                                                                                     |
| retransmit-interval | 秒数 (1...65535)  | LSA を連続して送る場合の再送間隔を秒単位で指定する。                                                                                                                                                                                                          |
| transmit-delay      | 秒数              | リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。                                                                                                                                                                                                |
| hello-interval      | 秒数 (1...65535)  | HELLO パケットの送信間隔を秒単位で設定する                                                                                                                                                                                                              |
| dead-interval       | 秒数 (1...65535)  | 近隣ルーターから HELLO を受け取れない場合に、近隣ルーターがダウンしたと判断するまでの時間を秒単位で設定する。                                                                                                                                                                            |

## [ノート]

• NAME パラメーターの **type** について  
NAME パラメーターの **type** として、LAN インターフェースと ONU インターフェースは **broadcast** のみが設定できる。PP インターフェースで PPP を利用する場合や、トンネルインターフェースを利用する場合は、**point-to-point** のみが設定できる。

• **passive** について  
**passive** は、インターフェースが接続しているリンクに他の OSPFv3 ルーターが存在しない場合に指定する。**passive** を指定しておく、インターフェースから OSPFv3 パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インターフェースと ONU インターフェース (**type=broadcast** であるインターフェース) の場合には、インターフェースが接続しているリンクへの経路は、**ipv6 interface ospf area** コマンドを設定していないと他の OSPFv3 ルーターに広告されない。そのため、OSPFv3 を利用しないリンクに接続する LAN インターフェースと ONU インターフェースに対しては、**passive** を付けた **ipv6 interface ospf area** コマンドを設定しておくことでそのリンクでは OSPFv3 を利用しないまま、そこへの経路を他の OSPFv3 ルーターに広告することができる。

PP インターフェースに対して **ipv6 pp ospf area** コマンドを設定していない場合は、インターフェースが接続するリンクへの経路は外部経路として扱われる。外部経路なので、他の OSPFv3 ルーターに広告するには **ipv6 ospf import** コマンドの設定が必要である。

- hello-interval/dead-interval について

hello-interval/dead-interval の値は、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメーターが設定値とは異なる HELLO パケットを受信した場合には、それは無視される。

- インスタンス ID について

本機のインスタンス ID は常に 0 であり、OSPFv3 パケットを受信する場合には、同じ値を持つパケットのみを受信する。

[適用モデル]  
NVR700W

## 28.7 仮想リンク設定

### [書式]

```
ipv6 ospf virtual-link router_id area [parameters ...]
no ipv6 ospf virtual-link router_id [area [parameters...]]
```

### [設定値及び初期値]

- *router\_id*
  - [設定値]: 仮想リンクの相手のルーター ID
  - [初期値]: -
- *area*: 経由するエリア
  - [設定値]:

| 設定値                       | 説明         |
|---------------------------|------------|
| 1 以上の数値 (1...4294967295)  | 非バックボーンエリア |
| IPv4 アドレス表記 (0.0.0.0 は不可) | 非バックボーンエリア |

- [初期値]: -
- *parameters*
  - [設定値]: NAME=VALUE の列
  - [初期値]:
    - retransmit-interval=5 秒
    - transmit-delay=1 秒
    - hello-interval=10 秒
    - dead-interval=40 秒

### [説明]

仮想リンクを設定する。仮想リンクは *router\_id* で指定したルーターに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメーターが設定できる。パラメーターは NAME=VALUE の形で指定され、以下の種類がある。

| NAME                | VALUE          | 説明                                                 |
|---------------------|----------------|----------------------------------------------------|
| retransmit-interval | 秒数 (1...65535) | LSA を連続して送る場合の再送間隔を秒数で設定する。                        |
| transmit-delay      | 秒数 (1...65535) | リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。             |
| hello-interval      | 秒数 (1...65535) | HELLO パケットの送信間隔を秒単位で設定する。                          |
| dead-interval       | 秒数 (1...65535) | 相手から HELLO を受け取れない場合に、相手がダウンしたと判断するまでの時間を秒単位で設定する。 |



## [ノート]

- hello-interval/dead-interval について  
hello-interval と dead-interval の値は、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメーターの値が設定値とは異なっている HELLO パケットを受信した場合には、それは無視される。

- インスタンス ID について  
本機のインスタンス ID は常に 0 であり、OSPFv3 パケットを受信する場合には、同じ値を持つパケットのみを受信する。

- 出力インターフェースについて  
仮想リンクを設定した場合、経由するエリアへの出力インターフェースにグローバルアドレスが付与されていなければ、仮想リンクは使用できない。

[適用モデル]  
NVR700W

## 28.8 OSPFv3 による経路の優先度設定

---

## [書式]

```
ipv6 ospf preference preference
no ipv6 ospf preference [preference]
```

## [設定値及び初期値]

- *preference*
  - [設定値]: OSPFv3 による経路の優先度 (1...2147483647)
  - [初期値]: 2000

## [説明]

OSPFv3 による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPFv3 と RIPng など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

## [ノート]

静的経路の優先度は 10000 で固定である。

[適用モデル]  
NVR700W

## 28.9 OSPFv3 で受け取った経路をルーティングテーブルに反映させるか否かの設定

---

## [書式]

```
ipv6 ospf export from ospf filter filter_num ...
no ipv6 ospf export from ospf [filter filter_num...]
```

## [設定値及び初期値]

- *filter\_num*
  - [設定値]: **ipv6 ospf export filter** コマンドのフィルター番号 (1...2147483647)
  - [初期値]: すべての経路がルーティングテーブルに反映される

## [説明]

OSPFv3 で受け取った経路をルーティングテーブルに導入するかどうかを設定する。指定した順にフィルターを評価し、最初に合致したフィルターによって導入すると判断された経路だけがルーティングテーブルに導入される。導入しないと判断された経路や合致するフィルターがない経路は導入されない。

このコマンドが設定されていない場合には、すべての経路がルーティングテーブルに導入される。

## [ノート]

このコマンドは OSPFv3 のリンク状態データベースには影響を与えない。つまり、OSPFv3 で他のルーターと情報をやり取りする動作としては、このコマンドがどのように設定されていても変化はない。OSPFv3 で計算した経路が実際にパケットをルーティングするために使われるかどうかだけが変わる。

## [適用モデル]

NVR700W

## 28.10 OSPFv3 で受け取った経路をどう扱うかのフィルターの設定

## [書式]

```
ipv6 ospf export filter filter_num [nr] kind ipv6_prefix/prefix_len ...
```

```
no ipv6 ospf export filter filter_num[...]
```

## [設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号 (1...2147483647)
  - [初期値]: -
- *nr*: フィルターの解釈の方法
  - [設定値]:

| 設定値    | 説明                        |
|--------|---------------------------|
| not    | IPv6 プレフィックスに該当しない経路を導入する |
| reject | IPv6 プレフィックスに該当した経路を導入しない |

- [初期値]: -
- *kind*: IPv6 プレフィックスの解釈の方法
  - [設定値]:

| 設定値     | 説明                                             |
|---------|------------------------------------------------|
| include | 指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含む)   |
| refines | 指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含まない) |
| equal   | 指定した IPv6 プレフィックスに一致する経路                       |

- [初期値]: -
- *ipv6\_prefix/prefix\_len*
  - [設定値]: IPv6 プレフィックス
  - [初期値]: -

## [説明]

OSPFv3 により他の OSPFv3 ルーターから受け取った経路をルーティングテーブルに導入する際に適用するフィルターを定義する。このコマンドで定義したフィルターは、**ipv6 ospf export from ospf** コマンドの *filter* 項で指定されてはじめて効果を持つ。

*ipv6\_prefix/prefix\_len* では、IPv6 プレフィックスを設定する。これは複数設定でき、*kind* に指定した方法で解釈される。

|         |                                                     |
|---------|-----------------------------------------------------|
| include | IPv6 プレフィックスと一致する経路および、IPv6 プレフィックスに含まれる経路が該当       |
| refines | IPv6 プレフィックスに含まれる経路が該当するが、IPv6 プレフィックスと一致する経路は含まれない |
| equal   | IPv6 プレフィックスに一致する経路のみ該当                             |

*nr* が省略されている場合には、一つでも該当する IPv6 プレフィックスがある場合にフィルターに合致したのとし、その経路を導入する。**not** 指定時には、いずれの IPv6 プレフィックスにも該当しなかった場合にフィルターに合致したのとし、その経路を導入する。**reject** 指定時には、一つでも該当する IPv6 プレフィックスがある場合にフィルターに合致したのとし、その経路を導入しない。

[ノート]

not 指定のフィルターを **ipv6 ospf export from ospf** コマンドで複数設定する場合には注意が必要である。not 指定のフィルターに合致する IPv6 プレフィックスは、そのフィルターでは導入するかどうかが決まれないため、**ipv6 ospf export from ospf** コマンドで指定された次のフィルターで評価される。そのため、例えば、以下のような設定ではすべての経路が導入されることになりフィルターの意味がない。

```
ipv6 ospf export from ospf filter 1 2
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 not equal fec0:12ab:34cd:2::/64
```

1 番のフィルターは fec0:12ab:34cd:1::/64 以外の経路に合致し、2 番のフィルターは fec0:12ab:34cd:2::/64 以外の経路に合致する。つまり、経路 fec0:12ab:34cd:1::/64 は 1 番のフィルターに合致しないが、2 番のフィルターに合致するため導入される。一方で経路 fec0:12ab:34cd:2::/64 は 1 番のフィルターに合致するため、2 番のフィルターにかかわらず導入される。よって、導入されない経路は存在しない。

経路 fec0:12ab:34cd:1::/64 と経路 fec0:12ab:34cd:2::/64 を導入したくない場合には以下のような設定を行う必要がある

```
ipv6 ospf export from ospf filter 1
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

あるいは

```
ipv6 ospf export from ospf filter 1 2 3
ipv6 ospf export filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf export filter 3 include ::/0
```

[適用モデル]  
NVR700W

## 28.11 外部プロトコルによる経路導入

[書式]

```
ipv6 ospf import from protocol [filter filter_num ...]
no ipv6 ospf import from protocol [filter filter_num...]
```

[設定値及び初期値]

- *protocol* : OSPFv3 の経路テーブルに導入する外部プロトコル
  - [設定値] :

| 設定値    | 説明    |
|--------|-------|
| static | 静的経路  |
| rip    | RIPng |

- [初期値] :-
- *filter\_num*
  - [設定値] : **ipv6 ospf import filter** コマンドのフィルター番号 (1...2147483647)
  - [初期値] :-

[説明]

OSPFv3 の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入した経路は外部経路として他の OSPFv3 ルーターに広告される。

*filter\_num* は **ipv6 ospf import filter** コマンドで定義したフィルター番号を指定する。外部プロトコルから導入されようとする経路は指定した順にフィルターにより評価される。最初に合致したフィルターによって導入すると判断された経路は OSPFv3 に導入される。導入しないと判断された経路や合致するフィルターがない経路は導入されない。また、*filter* キーワード以降を省略した場合には、すべての経路が OSPFv3 に導入される

経路を広告する場合のパラメーターであるメトリック値、メトリックタイプは、フィルターの検査で該当した **ipv6 ospf import filter** コマンドで指定されたものを使う。*filter* キーワード以降を省略した場合には、以下のパラメーターを使用する。

- metric=1
- type=2

[適用モデル]  
NVR700W

## 28.12 外部経路導入に適用するフィルター定義

### [書式]

```
ipv6 ospf import filter filter_num [nr] kind ipv6_prefix/prefix_len ... [parameters ...]
no ipv6 ospf import filter filter_num [[nr] kind ipv6_prefix/prefix_len ... [parameters...]]
```

### [設定値及び初期値]

- *filter\_num*
  - [設定値]: フィルター番号 (1...2147483647)
  - [初期値]: -
- *nr*: フィルターの解釈の方法
  - [設定値]:

| 設定値    | 説明                        |
|--------|---------------------------|
| not    | IPv6 プレフィックスに該当しない経路を導入する |
| reject | IPv6 プレフィックスに該当する経路を導入しない |

- [初期値]: -
- *kind*: IPv6 プレフィックスの解釈の方法
  - [設定値]:

| 設定値     | 説明                                             |
|---------|------------------------------------------------|
| include | 指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含む)   |
| refines | 指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含まない) |
| equal   | 指定した IPv6 プレフィックスに一致する経路                       |

- [初期値]: -
- *ipv6\_prefix/prefix\_len*
  - [設定値]: IPv6 プレフィックス
  - [初期値]: -
- *parameters*: 外部経路を広告する場合のパラメーター
  - [設定値]:

| 設定値                    | 説明                    |
|------------------------|-----------------------|
| metric = <i>metric</i> | メトリック値 (1 ~ 16777215) |
| type = <i>type</i>     | メトリックのタイプ (1 または 2)   |

- [初期値]: -

### [説明]

OSPFv3 の経路テーブルに外部経路を導入する際に適用するフィルターを定義する。このコマンドで定義したフィルターは **ipv6 ospf import from** コマンドの *filter* 項で指定されてはじめて効果を持つ。

*ipv6\_prefix/prefix\_len* では IPv6 プレフィックスを指定する。これは複数指定でき、*kind* に指定した方法で解釈される。

|         |                                                     |
|---------|-----------------------------------------------------|
| include | IPv6 プレフィックスと一致する経路および、IPv6 プレフィックスに含まれる経路が該当       |
| refines | IPv6 プレフィックスに含まれる経路が該当するが、IPv6 プレフィックスと一致する経路は該当しない |
| equal   | IPv6 プレフィックスに一致する経路のみ該当                             |

*nr* が省略されている場合には、一つでも該当する IPv6 プレフィックスがある場合にフィルターに合致したものとし、その経路を導入する。not 指定時には、いずれの IPv6 プレフィックスにも該当しなかった場合にフィルターに

合致したものとし、その経路を導入する。reject 指定時には、一つでも該当する IPv6 プレフィックスがある場合にフィルターに合致したものとし、その経路を導入しない。

parameters では、導入する経路を OSPFv3 の外部経路として広告する場合のパラメータとして、メトリック値、メトリックタイプがそれぞれ metric、type により指定できる。これらを省略した場合には、以下の値が採用される。

- metric=1
- type=2

[ノート]

not 指定のフィルターを **ipv6 ospf import from** コマンドで複数設定する場合には注意が必要である。not 指定のフィルターに合致しない経路は、そのフィルターでは導入するかどうか決定しないため、**ipv6 ospf import from** コマンドで指定された次のフィルターで評価される。そのため、例えば以下のような設定ではすべての経路が導入されることになりフィルターの意味がない。

```
ipv6 ospf import from static filter 1 2
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 not equal fec0:12ab:34cd:2::/64
```

1 番のフィルターは fec0:12ab:34cd:1::/64 以外の経路に合致し、2 番のフィルターは fec0:12ab:34cd:2::/64 以外の経路に合致する。つまり、経路 fec0:12ab:34cd:1::/64 は 1 番のフィルターに合致しないが、2 番のフィルターに合致するため導入される。一方で経路 fec0:12ab:34cd:2::/64 は 1 番のフィルターに合致するため、2 番のフィルターにかかわらず導入される。よって、導入されない経路は存在しない。

経路 fec0:12ab:34cd:1::/64 と経路 fec0:12ab:34cd:2::/64 を導入したくない場合には以下のような設定を行う必要がある。

```
ipv6 ospf import from static filter 1
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

あるいは

```
ipv6 ospf import from static filter 1 2 3
ipv6 ospf import filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf import filter 3 include ::/0
```

[適用モデル]  
NVR700W

## 28.13 OSPFv3 のログ出力設定

[書式]

```
ipv6 ospf log log ...
no ipv6 ospf log [log...]
```

[設定値及び初期値]

- log
  - [設定値]:

| 設定値       | 説明                      |
|-----------|-------------------------|
| interface | インターフェースの状態や仮想リンクに関わるログ |
| neighbor  | 近隣ルーターの状態に関わるログ         |
| packet    | OSPFv3 パケットに関わるログ       |

- [初期値]: いずれの種類ログも出力しない

[説明]

OSPFv3 に関わるログ出力の種類を設定する。

[適用モデル]  
NVR700W

## 第 29 章

### アナログ通信機能の設定

NVR700W, NVR510 のアナログ通信機能の設定は、TEL ポートに接続した PB 電話機のキー操作でも可能ですが、ここではコンソールからのコマンドについてだけ述べます。キー操作による設定手順は活用マニュアルを参照してください。キー操作とコンソールコマンドの対応表は本ページに示します。

TEL ポートには、識別着信リストと呼ぶリストがあり、このリストに一致した着信だけを許可したり拒否したりすることができます。識別着信リストへの登録は **analog arrive restrict list** コマンド、削除は **no analog arrive restrict list** コマンドで行います。実際の許可拒否動作はポート毎に行うことができ、**analog arrive restrict** コマンドにより動作を指定します。

NVR700W, NVR510 の TEL ポートの電氣的入出力レベルは調節することができます。受話器からの音声が大きくなって耳障りな音になったり、モデムや FAX の通信がうまくいかない場合には、**analog pad send**、**analog pad receive** コマンドで送話と受話レベルを調節し、最適な状態にします。

アナログ通信機器の発着信回数は **show account analog** コマンドで知ることができます。

#### 29.1 キー操作とコンソールコマンドの対応

TEL ポート(機器) 側の設定

| 機能                  | 機能番号 | 対応するコンソールコマンド                           |
|---------------------|------|-----------------------------------------|
| TEL ポートのダイヤル番号設定    | 11   | analog local address                    |
| TEL ポートのサブアドレス設定    | 12   | analog local address                    |
| 通信機器の種類設定           | 13   | analog device type                      |
| TEL ポート使用制限の設定      | 14   | analog use                              |
| VoIP 着信制限の設定        | 15   | analog sip arrive permit                |
| VoIP 発信制限の設定        | 16   | analog sip call permit                  |
| 発信者番号通知             | 21   | analog local address notice             |
| 即時発信                | 22   | analog rapid call                       |
| ポーズを判定する時間          | 23   | analog pause timer                      |
| グローバル着信             | 31   | analog arrive global permit             |
| 識別着信                | 32   | analog arrive restrict                  |
| 識別着信の番号登録           | 33   | analog arrive restrict list             |
| サブアドレスなしの着信         | 34   | analog arrive without-subaddress permit |
| 通信機器種別指定の着信         | 35   | analog arrive another-device permit     |
| 話中着信                | 36   | analog arrive ring-while-talking permit |
| 優先着信ポート             | 37   | analog arrive priority                  |
| 着信ベル設定              | 38   | analog arrive ringer-type list          |
| ナンバー・ディスプレイ機能       | 39   | analog arrive number display            |
| ダイヤル桁の間隔設定(秒)       | 41   | analog wait dial timer                  |
| フッキング判定時間(1/10 秒)   | 42   | analog hooking timer                    |
| フッキング後の操作有効時間(秒)    | 43   | analog hooking wait timer               |
| フッキング, オンフック無効時間(秒) | 44   | analog hooking inhibit timer            |
| 擬似切断信号の設定           | 45   | analog disc-signal                      |
| サブアドレスにかかわらない着信     | 47   | analog arrive ignore-subaddress permit  |

| 機能                        | 機能番号 | 対応するコンソールコマンド                                        |
|---------------------------|------|------------------------------------------------------|
| INS キャッチホン機能(コールウェイトィング)  | 52   | analog supplementary-service                         |
| 通信中転送機能                   | 53   | analog supplementary-service                         |
| 三者通話機能                    | 54   | analog supplementary-service                         |
| 着信転送機能                    | 55   | analog supplementary-service                         |
| 着信転送先番号登録                 | 56   | analog supplementary-service call-deflection address |
| 着信転送トーキ設定                 | 57   | analog supplementary-service call-deflection talkie  |
| 着信転送起動タイミング設定             | 58   | analog supplementary-service call-deflection ringer  |
| 着信転送失敗時の動作設定              | 59   | analog supplementary-service call-deflection reject  |
| 送話 PAD の音量設定              | 61   | analog pad send                                      |
| 受話 PAD の音量設定              | 62   | analog pad receive                                   |
| LAN ポートの IP アドレスとネットマスク設定 | 71   | ip interface address                                 |
| BOD の設定                   | 73   | analog mp prior                                      |
| i・ナンバーの設定                 | 81   | analog arrive inumber-port                           |
| 着信時サービス設定                 | 82   | analog arrive incoming-signal                        |
| 発番号無し着信設定                 | 83   | analog arrive without-calling-number                 |
| ダイヤル完了ボタンの設定              | 84   | analog end-of-dialing-code                           |
| TEL ポートの再呼出時間設定           | 85   | analog re-ringing-timer                              |
| TEL ポート設定の消去              | 91   |                                                      |
| 識別着信の番号削除                 | 92   | no analog arrive restrict list                       |
| 着信ベルの番号削除                 | 93   | no analog arrive ringer-type list                    |
| 料金情報の消去                   | 94   | clear account analog                                 |
| TEL ポート設定の全消去             | 99   |                                                      |
| パスワードの設定                  | 00   | login password, administrator password               |

## 29.2 TEL ポートごとの設定

### 29.2.1 TEL ポートを使うか否かの設定

[書式]

`analog use port use`

`no analog use port`

[設定値及び初期値]

- `port`

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *use*
- [設定値]:

| 設定値         | 説明           |
|-------------|--------------|
| on          | 発着信可能として使用する |
| off         | 使用しない        |
| call-only   | 発信専用として使用    |
| arrive-only | 着信専用として使用    |

- [初期値]: on

#### [説明]

TEL ポートを公衆回線および内線の発着信に使用するか否かを設定する。

#### [ノート]

SIP に対する発着信については、**analog sip arrive permit** コマンドと **analog sip call permit** コマンドで別途設定する。

#### [適用モデル]

NVR700W, NVR510

## 29.2.2 TEL ポートのダイヤルイン番号の設定

#### [書式]

```
analog local address port dialin_num [/sub_address] [dialin_num_list]
no analog local address port
```

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *dialin\_num*
  - [設定値]: ダイヤルイン番号
  - [初期値]: -
- *sub\_address*
  - [設定値]: サブアドレス(0x21 から 0x7e の ASCII 文字列)
  - [初期値]: -
- *dialin\_num\_list*
  - [設定値]: *dialin\_num* [/sub\_address] を空白で区切った並び(最大 4 つ)
  - [初期値]: -

#### [説明]

TEL ポートのダイヤルイン番号を設定する。最大 5 つまで設定できる。

#### [ノート]

サブアドレスの指定は、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

#### [適用モデル]

NVR700W, NVR510

## 29.2.3 TEL ポートに接続する機器の設定

#### [書式]

```
analog device type port type
no analog device type port
```



## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *type*

- [設定値]:

| 設定値 | 説明        |
|-----|-----------|
| any | 通信機器の設定なし |
| tel | 電話        |
| fax | G2/G3 FAX |

- [初期値]: any

## [説明]

TEL ポートに接続する機器を指定する。

これを設定すると、*type* パラメーターが any の場合には HLC をつけずに、それ以外では指定した HLC をつけて発信する。また **analog arrive another-device permit** コマンドとの組み合わせにより、着信時に *port* パラメーターで指定したポートへは、*type* パラメーターで指定した以外の着信に応答しなくなる。

## [ノート]

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

## [適用モデル]

NVR700W, NVR510

## 29.2.4 TEL ポートの発信者番号を通知するか否かの設定

## [書式]

**analog local address notice** *port* *notice*

**no analog local address notice** *port*

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *notice*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 通知する  |
| off | 通知しない |

- [初期値]: on

## [説明]

TEL ポートに設定した発信者番号を相手に通知するか否かを設定する。

相手に通知される番号は **analog local address** コマンドで設定されたものである。

**analog local address** コマンドで複数の番号が設定されている場合は最初に設定した番号が通知される。

## [ノート]

契約時に発信者番号通知サービスを選択しない場合には、常に通知されなくなる。  
このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

## [適用モデル]

NVR700W, NVR510

## 29.2.5 相手先番号による即時発信を許可するか否かの設定

## [書式]

**analog rapid call** *port rapid*

**no analog rapid call** *port*

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *rapid*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

## [説明]

相手先番号による即時発信を許可するか否かを設定する。

ダイヤル終了後、# ボタンを押さなくても、一定時間の経過を待たずに発信を開始することを即時発信と呼ぶ。  
過去に、発信により通話状態となった相手先が即時発信の対象となる。

## [ノート]

カスケード接続機能でアナログ回線に接続して使用する場合、アナログ回線への発信には即時発信機能は動作しない。

## [適用モデル]

NVR700W, NVR510

## 29.2.6 ダイヤル完了ボタンの設定

## [書式]

**analog end-of-dialing-code** *port switch*

**no analog end-of-dialing-code** *port*

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *switch*

- [設定値]:

| 設定値 | 説明                        |
|-----|---------------------------|
| on  | '#' ボタンをダイヤル完了ボタンとして使用する  |
| off | '#' ボタンをダイヤル完了ボタンとして使用しない |

- [初期値]: on

[説明]

'#' ボタンをダイヤル完了ボタンとして使用するか否かを選択する。  
 off を指定している場合には、'#' ボタンは回線番号として網に通知される。  
 ダイヤルの先頭が'#' の場合、最初の'#' ボタンは、本コマンドの設定にかかわらず回線番号として網に通知される。  
 (# ダイヤル(短縮ダイヤルサービス)のようにダイヤルの先頭が'#' の場合)

[適用モデル]

NVR700W, NVR510

### 29.2.7 グローバル着信を許可するか否かの設定

[書式]

**analog arrive global permit port permit**

**no analog arrive global permit port**

[設定値及び初期値]

- port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- permit

- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 許可する |
| off | 拒否する |

- [初期値]: on

[説明]

グローバル着信を許可するか否かを設定する。  
 グローバル着信の場合、着信時に着番号情報要素が付かない。グローバル着信を使用するためには、ダイヤルイン契約の際に利用指定が必要。

[ノート]

このコマンドは、カスケード接続機能で ISDN 回線と PSTN 回線を使用する場合にのみ有効である。

[適用モデル]

NVR700W, NVR510

### 29.2.8 TEL ポートでの識別着信をするか否かの設定

[書式]

**analog arrive restrict port restrict**

**no analog arrive restrict port**

[設定値及び初期値]

- port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *restrict*

- [設定値]:

| 設定値    | 説明      |
|--------|---------|
| permit | 着信許可    |
| reject | 着信拒否    |
| none   | 識別着信しない |

- [初期値]: reject

#### [説明]

TEL ポートで識別着信をするか否かを設定する。

**analog arrive restrict list** コマンドで登録された識別着信リストに対しての着信動作を決定する。  
 permit の場合には、発番号が登録リストに含まれれば着信許可となり、それ以外は着信拒否となる。  
 reject の場合には、発番号が登録リストに含まれれば着信拒否となり、それ以外は着信許可となる。  
 none の場合には、すべての発番号に対して着信許可となる。

#### [ノート]

ナンバー・ディスプレイサービスの契約が必要。

カスケード接続機能でアナログ回線を使用している場合は、着信拒否に設定しても発信側には話中音は流れず、呼出状態となる。

#### [適用モデル]

NVR700W, NVR510

## 29.2.9 識別着信リストの登録

#### [書式]

**analog arrive restrict list** *port number dial\_num* [/sub\_address]

**no analog arrive restrict list** *port number*

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *number*

- [設定値]: リスト番号

- [初期値]: -

- *dial\_num*

- [設定値]: 電話番号

- [初期値]: -

- *sub\_address*

- [設定値]: サブアドレス(0x21 から 0x7e の ASCII 文字列)

- [初期値]: -

## [説明]

識別着信用の電話番号を識別着信リストへ登録する。

リスト番号とは、識別着信リストの中で管理される通し番号である。また、識別着信リストは TEL ポート毎に管理される個別のリストである。

## [ノート]

サブアドレスの指定は、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

## [適用モデル]

NVR700W, NVR510

## 29.2.10 サブアドレス無し着信を許可するか否かの設定

## [書式]

```
analog arrive without-subaddress permit port permit
```

```
no analog arrive without-subaddress permit port
```

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *permit*

- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 許可する |
| off | 拒否する |

- [初期値]: on

## [説明]

サブアドレス情報要素の無い着信を許可するか否かを設定する。

**analog local address** コマンドを使用してポート毎に異なるサブアドレスを設定しておくこと、ポートを区別して着信させることが可能になる。

ISDN 回線以外からの着信にはサブアドレス情報要素が付いてこない。

## [ノート]

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

## [適用モデル]

NVR700W, NVR510

## 29.2.11 サブアドレスにかかわらず着信を許可するか否かの設定

## [書式]

```
analog arrive ignore-subaddress permit port permit
```

```
no analog arrive ignore-subaddress permit port
```

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |

| 設定値 | 説明       |
|-----|----------|
| 2   | TEL2 ポート |

- [初期値]: -
- *permit*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: off

#### [説明]

サブアドレス情報要素にかかわらず着信を許可するか否かを設定する。**analog local address** コマンドによってサブアドレスを含むダイヤルイン番号を設定している場合は、このコマンドの設定にかかわらず、サブアドレス情報要素まで一致した場合に着信する。

#### [ノート]

ダイヤルイン番号を設定し、かつサブアドレス情報要素にかかわらず着信させるためには、ダイヤルイン番号をサブアドレスなしで設定する必要がある。

#### [適用モデル]

NVR700W, NVR510

## 29.2.12 異なる種類の通信機器からの着信を許可するか否かの設定

#### [書式]

**analog arrive another-device permit** *port permit*

**no analog arrive another-device permit** *port*

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *permit*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

#### [説明]

異なる種類の通信機器からの着信を許可するか否かを設定する。

#### [ノート]

着信時の HLC 情報要素と **analog device type** コマンドにより設定された機器を比較して、着信整合性を調べる。このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

#### [適用モデル]

NVR700W, NVR510

## 29.2.13 話中着信を許可するか否かの設定

### [書式]

```
analog arrive ring-while-talking permit port permit
```

```
no analog arrive ring-while-talking permit port
```

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *permit*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: off

### [説明]

話中着信を許可するか否かを設定する。

### [ノート]

- カスケード接続機能で ISDN 回線を使用している場合  
*permit* が on になっていないと、フレックスホンの INS キャッチホン(コールウェイティング) も擬似キャッチホン(擬似コールウェイティング) も使用できない。
- カスケード接続機能でアナログ回線を使用している場合  
*permit* を on にすると、通話中にアナログ回線への着信があった場合、着信音によって着信が確認できる。  
なお、フッキングによる通話の切り替えを行うことはできない。  
網の付加サービスによる話中着信はこの設定に関わらず動作する。  
また、**pstn supplementary-service** が on に設定されている場合は、話中着信はこの設定に関わらず動作しない。

### [適用モデル]

NVR700W, NVR510

## 29.2.14 着信ベルリストの登録

### [書式]

```
analog arrive ringer-type list port type number dial_num [/sub_address]
```

```
no analog arrive ringer-type list port type number
```

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *type*

- [設定値]: 着信時のベル音の種類(1,2)
- [初期値]: -

- *number*

- [設定値]: リスト番号
- [初期値]: -
- *dial\_num*
  - [設定値]: 相手発信者の電話番号
  - [初期値]: -
- *sub\_address*
  - [設定値]: サブアドレス(0x21 から 0x7e の ASCII 文字列)
  - [初期値]: -

**[説明]**

着信ベルリストを登録する。

**[ノート]**

*type* パラメーターで指定される着信ベル音の種類と、通常の着信時のベル音及び内線着信ベル音は異なる。サブアドレスの指定は、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。ナンバー・ディスプレイサービスの契約が必要。

**[適用モデル]**

NVR700W, NVR510

## 29.2.15 ナンバー・ディスプレイの設定

---

**[書式]**

**analog arrive number display port mode**

**no analog arrive number display port**

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *mode*

- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| off | ナンバー・ディスプレイを使用しない |
| on  | ナンバー・ディスプレイを使用する  |

- [初期値]: -

**[説明]**

指定した TEL ポートでナンバー・ディスプレイを使用可能にする。

**[ノート]**

ナンバー・ディスプレイサービスの契約が必要。

• カスケード接続機能でアナログ回線を使用時のみ  
 キャッチホン・ディスプレイサービスを契約されているアナログ回線を使用した通話中は、設定に関係なく通話中の電話機がキャッチホン・ディスプレイに対応していればキャッチホン・ディスプレイサービスが利用可能。

**[適用モデル]**

NVR700W, NVR510



## 29.2.16 指定した TEL ポートの優先着信順位を設定

### [書式]

**analog arrive priority port priority**

**no analog arrive priority port**

### [設定値及び初期値]

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *priority*
  - [設定値]: 優先順位(1..3)
  - [初期値]: 2

### [説明]

指定した TEL ポートの優先着信順位を設定する。  
*priority* は、1(優先度高) - 3(優先度低) である。

### [適用モデル]

NVR700W, NVR510

## 29.2.17 ダイヤル桁間タイマの設定

### [書式]

**analog wait dial timer port time**

**no analog wait dial timer port**

### [設定値及び初期値]

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
  - [設定値]: 秒数(1..59)
  - [初期値]: 4

### [説明]

ダイヤル桁間タイマ値を設定する。  
ダイヤル中に本タイマ値を越えてキー操作が無いと発信動作を開始する。秒数は 1 秒単位で設定できる。

### [適用モデル]

NVR700W, NVR510

## 29.2.18 フッキングを判定する時間の設定

### [書式]

**analog hooking timer port time**

**no analog hooking timer port**

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
  - [設定値]: 秒数(0.5..2)
  - [初期値]: 1

**[説明]**

フッキングとして判断する最大の時間を設定する。

この時間を越えて TEL ポートに接続された通信機器のフックスイッチを押し続けた場合はオンフックとみなして切断処理される。秒数は 0.1 秒単位で設定できる。

**[適用モデル]**

NVR700W, NVR510

## 29.2.19 フッキング後にキー操作を受け入れる時間の設定

---

**[書式]**

**analog hooking wait timer *port time***

**no analog hooking wait timer *port***

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
  - [設定値]: 秒数(1..9)
  - [初期値]: 4

**[説明]**

フッキング後にキー操作を受け入れる時間を設定する。

フレックスホン機能を利用するためのフック操作を行った後、次のフッキングまたはオンフック操作を受け入れる時間である。秒数は 1 秒単位で設定できる。

**[適用モデル]**

NVR700W, NVR510

## 29.2.20 フッキング及びオンフック検出を無効と判断する時間の設定

---

**[書式]**

**analog hooking inhibit timer *port time***

**no analog hooking inhibit timer *port***

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
  - [設定値]:
    - 秒数(1..3)
    - off ... 0 秒
  - [初期値]: off

**[説明]**

オフフック後から、フッキング及びオンフック検出を無効と判断する時間を設定する。秒数は 1 秒単位で設定できる。

**[ノート]**

オフフック後の数秒間、直流ループ断が発生するようなホームテレホン等を接続した場合に有効。通常は off でよい。

**[適用モデル]**

NVR700W, NVR510

### 29.2.21 オフフックを検出するまでの遅延時間の設定

**[書式]**

**analog off-hook mask port mask\_open mask\_ring**

**no analog off-hook mask port**

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *mask\_open*
  - [設定値]: 回路開放中におけるマスク時間。80ms 単位(1..8)
  - [初期値]: 1
- *mask\_ring*
  - [設定値]: リンギング中におけるマスク時間。100ms 単位(1..2)
  - [初期値]: 1

**[説明]**

TEL ポートの回路が閉じてからオフフックを検出するまでの時間を設定する。

**[適用モデル]**

NVR700W, NVR510

### 29.2.22 オフフック/オンフックを検出する閾値の設定

**[書式]**

**analog loop-closure threshold port lcroffhk lcronhk**

**no analog loop-closure threshold port**

**[設定値及び初期値]**

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *lcroffhk*

- [設定値]: オフフック検出閾値(0..-3)

- [初期値]: 0

- *lcronhk*

- [設定値]: オンフック検出閾値(0..-3)

- [初期値]: 0

#### [説明]

TEL ポートでオフフックおよびオンフックを検出する閾値を設定する。

TEL ポートに接続した電話機との接続性に問題がある場合、本コマンドで閾値を変更すると改善する場合があります。

#### [適用モデル]

NVR700W, NVR510

## 29.2.23 インピーダンスの設定

#### [書式]

**analog impedance port type**

**no analog impedance port**

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *type*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| 1   | タイプ 1 |
| 2   | タイプ 2 |

- [初期値]: 1

#### [説明]

TEL ポートのインピーダンスを設定する。

TEL ポートに接続した電話機との接続性に問題がある場合、本コマンドでインピーダンスを変更すると改善する場合があります。

#### [適用モデル]

NVR700W, NVR510

## 29.2.24 保留音の種類の設定

#### [書式]

**audio hold-tone type type**

**no audio hold-tone type**

**[設定値及び初期値]**

- *type*
  - [設定値]:

| 設定値    | 説明                   |
|--------|----------------------|
| melody | 保留音としてメロディーを流す       |
| beep   | 保留音としてビープ音(「プップ」)を流す |

- [初期値]: melody

**[説明]**

保留音としてメロディーを流すかビープ音を流すかを設定する。

**[ノート]**

beep に設定すると、ビープ音による保留音「プップ」が流れる。

**[適用モデル]**

NVR700W, NVR510

### 29.2.25 TEL ポートの再呼出時間設定

---

**[書式]**

**analog re-ringing-timer port time**  
**no analog re-ringing-timer port**

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
  - [設定値]: 再呼出時間の秒数(10..180)
  - [初期値]: 30

**[説明]**

指定した TEL ポートの再呼出時間を設定する。

再呼出時間とは、以下の時間を示す。

- 相手呼出状態で内線転送を行った場合の呼出時間
- 呼び返し(保留呼があることを通知するための呼出)の呼出時間

**[適用モデル]**

NVR700W, NVR510

### 29.2.26 フレックスホン機能の使用パターンの設定

---

**[書式]**

**analog supplementary-service [network] func [func...]**  
**analog supplementary-service pseudo func [func...]**  
**no analog supplementary-service**

**[設定値及び初期値]**

- *network*: 網提供のフレックスホンを示すキーワード
  - [初期値]: -
- *func*
  - [設定値]:

| 設定値               | 説明                                  |
|-------------------|-------------------------------------|
| call-waiting      | INS キャッチホン(コールウェイティング) 機能使用を示すキーワード |
| call-transfer     | 通信中転送機能使用を示すキーワード                   |
| add-on            | 三者通話機能使用を示すキーワード                    |
| call-deflection 1 | TEL1 ポートでの着信転送機能使用を示すキーワード          |
| call-deflection 2 | TEL2 ポートでの着信転送機能使用を示すキーワード          |

- [初期値]: フレックスホン機能を使用しない
- pseudo: 擬似機能使用を示すキーワード
  - [初期値]: -

**[説明]**

フレックスホン機能の使用パターンを設定する。

**[ノート]**

着信転送機能を実際に動作させるためには、着信転送先アドレスの設定(**analog supplementary-service call-deflection address** コマンド)が必要。

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

**[適用モデル]**

NVR700W, NVR510

## 29.2.27 着信転送先アドレスの設定

---

**[書式]**

**analog supplementary-service call-deflection address** *port dial\_num* [/sub\_address]

**no analog supplementary-service call-deflection address** *port*

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *dial\_num*
  - [設定値]: 電話番号
  - [初期値]: -
- *sub\_address*
  - [設定値]: サブアドレス(0x21 から 0x7e の ASCII 文字列)
  - [初期値]: -

**[説明]**

着信転送先アドレスを登録する。

**[ノート]**

網提供のフレックスホンによる着信転送では、サブアドレスの指定は無効となる。

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

**[適用モデル]**

NVR700W, NVR510

## 29.2.28 着信転送を起動するタイミングの設定

### [書式]

**analog supplementary-service call-deflection ringer port count**

**no analog supplementary-service call-deflection ringer port**

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *count*

- [設定値]:

| 設定値       | 説明                  |
|-----------|---------------------|
| 回数(1..10) | 指定回数着信ベルを鳴らした後に起動する |
| off       | 着信ベルを鳴らさずにすぐに起動開始する |

- [初期値]: off

### [説明]

着信転送を起動するタイミングを設定する。  
タイミングは3秒周期のリズムを1回とカウントする。

### [ノート]

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

### [適用モデル]

NVR700W, NVR510

## 29.2.29 着信転送トーキの設定

### [書式]

**analog supplementary-service call-deflection talkie port transfer originator**

**no analog supplementary-service call-deflection talkie port**

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *transfer*

- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 転送トーキあり |
| off | 転送トーキなし |

- [初期値]: off

- *originator*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | 転送元トーキあり |
| off | 転送先トーキなし |

- [初期値]: off

#### [説明]

着信転送におけるトーキのありなしを設定する。

#### [ノート]

転送トーキは、網提供の着信転送使用時に、発信側で聞こえる音声ガイドであり、転送元トーキは、転送先の相手に聞こえる音声ガイドのこと。

なお、擬似機能による着信転送使用時には転送トーキは無い。

フレックスホンの着信転送機能の契約が必要。

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

#### [適用モデル]

NVR700W, NVR510

### 29.2.30 着信転送が拒否された時の動作の設定

#### [書式]

**analog supplementary-service call-deflection reject port action**

**no analog supplementary-service call-deflection reject port**

#### [設定値及び初期値]

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *action*

- [設定値]:

| 設定値   | 説明                  |
|-------|---------------------|
| busy  | 着信に対し、ビジートーン(話中)を返す |
| alert | 着信に対して応答する          |

- [初期値]: alert

#### [説明]

着信転送を行う際、網からそれを拒否された場合の動作を設定する。 **busy** の場合には、着信に対しビジー(話中)を返すので、電話をかけてきた方にはビジートーンが返り、通話はできない。 **alert** の場合には、呼出を返すと同時に手元の電話機のベルを鳴らすので、ここで受話器をとれば通話できる。

#### [ノート]

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

#### [適用モデル]

NVR700W, NVR510

### 29.2.31 送話 PAD の設定

#### [書式]

**analog pad send port pad**

**no analog pad send port**



[設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *pad*

- [設定値]:

| 設定値  | 説明          |
|------|-------------|
| -3dB | -3dB PAD 挿入 |
| -6dB | -6dB PAD 挿入 |
| -9dB | -9dB PAD 挿入 |
| off  | PAD なし      |

- [初期値]: off

[説明]

送話 PAD を設定する。

[ノート]

従来機種とは *pad* パラメーターの設定範囲が異なる。

従来機種の設定を流用する場合、設定値そのままでは読み込むことのできない場合があるので注意が必要。

[適用モデル]

NVR700W, NVR510

## 29.2.32 受話 PAD の設定

[書式]

`analog pad receive port pad`

`no analog pad receive port`

[設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *pad*

- [設定値]:

| 設定値  | 説明          |
|------|-------------|
| -3dB | -3dB PAD 挿入 |
| -6dB | -6dB PAD 挿入 |
| -9dB | -9dB PAD 挿入 |
| off  | PAD なし      |

- [初期値]: off

**[説明]**

受話 PAD を設定する。

**[ノート]**

従来機種とは *pad* パラメーターの設定範囲が異なる。

従来機種の設定を流用する場合、設定値そのままでは読み込むことのできない場合があるので注意が必要。

**[適用モデル]**

NVR700W, NVR510

### 29.2.33 MP 時に電話発着信のために 1B チャンネルに落とすか否かの設定

---

**[書式]**

**analog mp prior port down**

**no analog mp prior port**

**[設定値及び初期値]**• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *down*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 落とす   |
| off | 落とさない |

- [初期値]: on

**[説明]**

MP 時に 2B チャンネルでデータ通信中、電話の発着信を行うためにデータ通信のチャンネル数を 1B に落とすか否かを設定する。

**[ノート]**

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

**[適用モデル]**

NVR700W, NVR510

### 29.2.34 TEL ポートへの切断信号の送出の設定

---

**[書式]**

**analog disc-signal port use**

**no analog disc-signal port**

**[設定値及び初期値]**• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *use*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on

**[説明]**

指定した TEL ポートへの切断信号を送出するか否かを設定する。

on に設定すると、着信による通話時、発信側が先に通信を切断した場合に、極性反転して擬似的な切断信号をその TEL ポートへ送化する。

**[ノート]**

カスケード接続機能でアナログ回線を使用した通話時はこのコマンドは無効である。

**[適用モデル]**

NVR700W, NVR510

### 29.2.35 アザーダイヤルトーンを出すか否かの設定

**[書式]**

**analog extension other-dial-tone switch**

**no analog extension other-dial-tone**

**[設定値及び初期値]**

- *switch*
- [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | アザーダイヤルトーンを出す   |
| off | アザーダイヤルトーンを出さない |

- [初期値]: on

**[説明]**

一般回線またはひかり電話回線から発呼できない場合のダイヤルトーン(アザーダイヤルトーン)を区別するか否かを設定する。off とした場合、内線を含めて発信が可能な場合は通常のダイヤルトーンが鳴る。

**[適用モデル]**

NVR700W, NVR510

### 29.2.36 着信時の着信ベル鳴動モードの設定

**[書式]**

**analog extension incoming ringer mode**

**no analog extension incoming ringer**

**[設定値及び初期値]**

- *mode*
- [設定値]:

| 設定値        | 説明                            |
|------------|-------------------------------|
| all        | 着信可能な全 TEL ポートを鳴動させる          |
| one-by-one | 着信可能な TEL ポートのうちの 1 つだけを鳴動させる |

- [初期値]: all

**[説明]**

着信時、着信可能なすべての TEL ポートを鳴動させるか、そのうちの 1 つだけを鳴動させるかを設定する。

## [ノート]

カスケード接続時には、親機の設定モードで動作することに注意。  
TEL ポートに PBX 等を接続し、複数のポートを同時に鳴動させたくない場合、one-by-one に設定する。  
優先度が同じ場合には、TEL1, TEL2 の順番で検索した最初の空きポートに着信する。

## [適用モデル]

NVR700W, NVR510

## 29.2.37 緊急番号の処理方式の設定

## [書式]

**analog extension emergency-call-dial type type**

**no analog extension emergency-call-dial type**

## [設定値及び初期値]

## • type

- [設定値]:

| 設定値            | 説明                |
|----------------|-------------------|
| special-number | 緊急番号を特別な番号として処理する |
| normal-number  | 通常の番号として処理する      |

- [初期値]: special-number

## [説明]

緊急番号の処理方式を設定する。special-number の場合、緊急番号(110、118、119 番)を特別な番号として認識し、必要桁を押した時点で一般回線に即時発信されるが、normal-number の場合は通常通りダイヤル桁間タイマが作用し、次桁以降もダイヤルすることができる。

また、normal-number の場合、110、118、119 番の発信経路を VoIP にすることが可能となる。

カスケード接続構成を取っている場合、このコマンドについては全ての機器が同一の設定である必要がある。

## [適用モデル]

NVR700W, NVR510

## 29.2.38 i・ナンバーサービスのポート番号の設定

## [書式]

**analog arrive inumber-port port inum\_port [inum\_port...]**

**no analog arrive inumber-port port**

## [設定値及び初期値]

## • port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

## • inum\_port

- [設定値]:

| 設定値  | 説明             |
|------|----------------|
| 1    | ポート番号 1 で着信する  |
| 2    | ポート番号 2 で着信する  |
| all  | すべてのポート番号で着信する |
| none | 着信しない          |

- [初期値]: i・ナンバーサービスのポート番号と同じ番号の TEL ポートが着信を受ける

**[説明]**

i・ナンバーサービスで網から送られるポート番号を TEL ポートに対応させる。対応させたポート番号が送られてきたら、その TEL ポートが着信を受ける。

all を設定したときには、どのポート番号が送られてきても着信を受ける。

none を設定したときには、どのポート番号が送られてきても着信を受けない。

**[ノート]**

このコマンドは、カスケード接続機能で ISDN 回線を使用する場合にのみ有効である。

**[適用モデル]**

NVR700W, NVR510

### 29.2.39 アナログダイヤルインと無鳴動着信機能の設定

**[書式]**

**analog arrive incoming-signal port number address type signal dial\_in-num**

**no analog arrive incoming-signal port number**

**[設定値及び初期値]**

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *number*

- [設定値]: 登録番号(1..65535)

- [初期値]: -

- *address*

- [設定値]:

| 設定値      | 説明                 |
|----------|--------------------|
| global   | グローバル着信を登録         |
| local1   | 1 番目のローカルアドレスを登録   |
| local2   | 2 番目のローカルアドレスを登録   |
| local3   | 3 番目のローカルアドレスを登録   |
| local4   | 4 番目のローカルアドレスを登録   |
| local5   | 5 番目のローカルアドレスを登録   |
| inumber1 | i・ナンバーのポート番号 1 を登録 |
| inumber2 | i・ナンバーのポート番号 2 を登録 |
| inumber3 | i・ナンバーのポート番号 3 を登録 |

- [初期値]: -

- *type*

- [設定値]:

| 設定値  | 説明        |
|------|-----------|
| tel  | HLC が電話   |
| fax  | HLC が FAX |
| none | HLC がない   |

| 設定値 | 説明  |
|-----|-----|
| all | すべて |

- [初期値]: -
- *signal*
- [設定値]:

| 設定値         | 説明        |
|-------------|-----------|
| modem       | モデムダイヤルイン |
| pb          | PB ダイヤルイン |
| no-ring-fax | 無鳴動着信     |

- [初期値]: -
- *dial\_in-num*
- [設定値]: アナログ機器に送出するダイヤルイン番号(*signal* で *modem* と *pb* を指定したときのみ有効)
- [初期値]: -

#### [説明]

指定した *port* に対して、*address* の一致する着信があったときに、*signal* に相当した着信処理を行う。アナログダイヤルインのときには、*dial\_in-num* で設定されたダイヤルイン信号を出す。*dial\_in-num* は *signal* が *modem* の場合には 20 桁以内、*pb* の場合には 4 桁以内で設定できる。

#### [ノート]

ダイヤルインサービスあるいは i・ナンバーサービスの契約が必要。

• カスケード接続機能で ISDN 回線を使用している場合  
*address* にグローバル着信を指定する場合は、ダイヤルイン契約時にグローバル着信ありを指定した場合のみ有効。  
*address* に i・ナンバーのポート番号を指定する場合は、i・ナンバーの契約が必要。  
*type* に HLC を指定した場合は、発信側が ISDN 回線ではないときは無効となる。

• カスケード接続機能でアナログ回線を使用している場合  
*address* にグローバル着信、i・ナンバーのポート番号を指定しても無効である。  
*type* に all 以外を指定しても無効である。

#### [適用モデル]

NVR700W, NVR510

### 29.2.40 PB ダイヤルインの一次応答検出タイミングの設定

#### [書式]

```
analog arrive incoming-signal timing pb port mode
no analog arrive incoming-signal timing pb port
```

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *mode*
- [設定値]:

| 設定値 | 説明                                         |
|-----|--------------------------------------------|
| 1   | 呼出信号送出前の極性反転のタイミングにおける直流ループ閉成を一次応答信号とみなさない |
| 2   | 呼出信号送出前の極性反転のタイミングにおける直流ループ閉成を一次応答信号とみなす   |

- [初期値]: 1

#### [説明]

指定した *port* に対して、PB ダイヤルインの動作を行う場合において、呼出信号送出前の極性反転のタイミングにおける直流ループ閉成に対する動作を選択する。

#### [適用モデル]

NVR700W, NVR510

## 29.2.41 発番号情報なし着信機能の設定

#### [書式]

**analog arrive without-calling-number** *port type* [*option1* [*option2* [*option3*]]]

**no analog arrive without-calling-number** *port*

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *mode*

- [設定値]:

| 設定値    | 説明             |
|--------|----------------|
| permit | 発番号情報なし着信を許可する |
| reject | 発番号情報なし着信を拒否する |

- [初期値]: permit

- *option*

- [設定値]:

| 設定値                 | 説明                      |
|---------------------|-------------------------|
| all                 | すべての着信を対象にする            |
| public-telephone    | 本設定を公衆電話からの着信に限定する      |
| rejected-by-user    | 本設定をユーザーによる通知拒否の着信に限定する |
| service-unavailable | 本設定を表示圏外からの着信に限定する      |

- [初期値]: all

#### [説明]

指定した TEL ポートの発番号情報なしの着信を、指定した非通知理由により許可するか否かを選択する。

#### [ノート]

ナンバー・ディスプレイサービスの契約が必要。

*option* 省略時は all と同じ。

#### [適用モデル]

NVR700W, NVR510

## 29.2.42 RTP 音声の受話 PAD の設定

### [書式]

```
analog pad rtp receive port pad
```

```
no analog pad rtp receive port
```

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *pad*

- [設定値]:

| 設定値  | 説明          |
|------|-------------|
| -9dB | -9dB PAD 挿入 |
| -6dB | -6dB PAD 挿入 |
| -3dB | -3dB PAD 挿入 |
| off  | PAD なし      |
| +3dB | +3dB PAD 挿入 |
| +6dB | +6dB PAD 挿入 |

- [初期値]: off

### [説明]

指定した TEL ポートの RTP 音声(カスケード接続、VoIP)に対する受話 PAD を設定する。最終的な音量は、**analog pad receive** と組み合わさった値となる。

### [ノート]

通常の音量は問題なく、RTP 音声の音量だけを調整したい場合に使用する。

音量を上げる方向に PAD を設定した場合、エコーのレベルも大きくなるため、通話に支障がでる場合がある。

従来機種とは *pad* パラメーターの設定範囲が異なる。

従来機種の設定を流用する場合、設定値そのままでは読み込むことのできない場合があるので注意が必要。

### [適用モデル]

NVR700W, NVR510

## 29.2.43 RTP 音声の送話 PAD の設定

### [書式]

```
analog pad rtp send port pad
```

```
no analog pad rtp send port
```

### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *pad*

- [設定値]:



| 設定値  | 説明          |
|------|-------------|
| -9dB | -9dB PAD 挿入 |
| -6dB | -6dB PAD 挿入 |
| -3dB | -3dB PAD 挿入 |
| off  | PAD なし      |
| +3dB | +3dB PAD 挿入 |
| +6dB | +6dB PAD 挿入 |

- [初期値]: off

**[説明]**

指定した TEL ポートの RTP 音声(カスケード接続、VoIP) に対する送話 PAD を設定する。最終的な音量は、**analog pad send** と組み合わせさせた値となる。

**[ノート]**

通常の音量は問題なく、RTP 音声の音量だけを調整したい場合に使用する。  
音量を上げる方向に PAD を設定した場合、エコーのレベルも大きくなるため、通話に支障がでる場合がある。

従来機種とは *pad* パラメーターの設定範囲が異なる。  
従来機種の設定を流用する場合、設定値そのままでは読み込むことのできない場合があるので注意が必要。

**[適用モデル]**

NVR700W, NVR510

### 29.2.44 ポーズを判定する時間の設定

**[書式]**

**analog pause timer port time**

**no analog pause timer port**

**[設定値及び初期値]**

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *time*
- [設定値]: 秒数(1..10)
- [初期値]: 2

**[説明]**

ポーズとして判断する最小の時間を設置する。

**[ノート]**

このコマンドは、カスケード接続機能でアナログ回線を使用する場合にのみ有効である。

**[適用モデル]**

NVR700W, NVR510

### 29.2.45 TEL ポートに対する電力供給の設定

**[書式]**

**analog power port sw**

**no analog power port**

**[設定値及び初期値]**

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *sw*

- [設定値]:

| 設定値 | 説明                     |
|-----|------------------------|
| on  | TEL ポートに電力を供給し、使用可能にする |
| off | 電力供給を行わず、使用不可能にする      |

- [初期値]: on

#### [説明]

TEL ポートに対して電力を供給するか否かを設定する。  
電力供給を行わない場合、その TEL ポートは機能しなくなる。  
再起動によって設定変更が有効となる。

#### [適用モデル]

NVR700W, NVR510

## 29.2.46 オフフックで発信する相手先電話番号の設定

#### [書式]

**analog off-hook call** *port number*

**no analog off-hook call** *port*

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *number*
- [設定値]: 相手先の電話番号
- [初期値]: -

#### [説明]

TEL ポートに接続された電話機をオフフックしたときに自動的に発信する相手先の電話番号を設定する。プレフィックスまで含めて設定する。

#### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で設定できる。

#### [適用モデル]

NVR700W, NVR510

## 第 30 章

### カスケード接続機能の設定

NVR700W, NVR510 では、「カスケード接続機能」により複数のルーターのうちの 1 台が他のルーターの TEL ポート及びアナログ回線または ISDN 回線のアナログ通話を一括管理することが可能です。これにより、異なるルーターに接続されているアナログ機器同士で内線通話が可能で、加えて電話回線に接続されていないルーターから、他のルーターに接続された電話回線を使用して外線通話をすることも可能です。

複数のルーターのうち、TEL ポート及びアナログ回線または ISDN 回線のアナログ通話を管理するルーターを「アナログ親機」と呼び、その他のルーターを「アナログ子機」と呼びます。ひとつのアナログ親機が管理できるルーターは、アナログ親機も含めて最大 9 台です。アナログ親機または子機に設定するには、**analog extension mode** コマンドを使います。

アナログ子機は、同一ネットワーク内にアナログ親機があるかどうか自動で検索することが可能です。これは NVR510 および NVR700W Rev.15.00.22 以前で **analog extension master** コマンド、NVR700W Rev.15.00.23 以降で **analog extension manager** コマンドにより設定します。

アナログ親機と子機には、機器番号を設定してください。機器番号を設定していない場合には、機器を指定した内線呼び出しができません(" \* \*" による一斉内線呼び出しは可能です)。

機器番号は **analog extension machine-id** コマンドで設定します。

#### 30.1 カスケード接続モードの設定

##### [書式]

```
analog extension mode mode
no analog extension mode
```

##### [設定値及び初期値]

- *mode*
- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| standalone | 単独動作モード   |
| master     | アナログ親機モード |
| manager    | アナログ親機モード |
| slave      | アナログ子機モード |
| agent      | アナログ子機モード |

- [初期値]: standalone

##### [説明]

カスケード接続モードを設定する。

##### [ノート]

複数機器で協調してアナログ通話を行う場合、同一ネットワーク上で必ず一つをアナログ親機モードとし、残りはアナログ子機モードとすること。

manager オプションと agent オプションは NVR700W Rev.15.00.23 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

#### 30.2 カスケード接続に利用する IP アドレス取得インターフェースの設定

##### [書式]

```
analog extension address refer interface
analog extension address refer pp peer_num
no analog extension address refer
no analog extension address refer pp peer_num
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、または ONU インターフェース名
  - [初期値]: lan1
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -

**[説明]**

カスケード接続に使用する IP アドレスを取得するインターフェースを設定する。

**[ノート]**

PP インターフェースで NAT を使用する場合、静的 NAT を UDP ポートの 2427-2433 および RTP による音声通話に使用される 5004 からの UDP ポートに対して設定する必要がある。またフィルター設定も、上記ポートを通す設定が必要である。

**[適用モデル]**

NVR700W, NVR510

### 30.3 アナログ親機となる機器の設定

---

**[書式]**

```
analog extension master master
no analog extension master
```

**[設定値及び初期値]**

- *master*
  - [設定値]:
    - IP アドレス
    - auto ..... 自動検索
  - [初期値]: auto

**[説明]**

アナログ子機モードにおいて、アナログ親機となる機器の IP アドレスを設定する。  
auto の場合、同一ネットワーク内のアナログ親機を自動検索する。

**[ノート]**

自動検索失敗時は、10 秒毎に再検索を行う。

NVR700W は Rev.15.00.23 以降で使用不可。  
代わりに **analog extension manager** コマンドを使用することができる。

**[適用モデル]**

NVR510

### 30.4 アナログ親機となる機器の設定

---

**[書式]**

```
analog extension manager manager
no analog extension manager
```

**[設定値及び初期値]**

- *manager*
  - [設定値]:
    - IP アドレス
    - auto ..... 自動検索

- [初期値]: auto

#### [説明]

アナログ子機モードにおいて、アナログ親機となる機器の IP アドレスを設定する。  
auto の場合、同一ネットワーク内のアナログ親機を自動検索する。

#### [ノート]

自動検索失敗時は、10 秒毎に再検索を行う。

NVR700W は Rev.15.00.23 以降で使用可能。

#### [適用モデル]

NVR700W

## 30.5 アナログ子機受け入れモードの設定

#### [書式]

**analog extension slave permit mode**

**no analog extension slave permit**

#### [設定値及び初期値]

- *mode*

- [設定値]:

| 設定値             | 説明                   |
|-----------------|----------------------|
| all             | すべて受け入れる             |
| registered-only | 機器番号を設定している機器のみ受け入れる |

- [初期値]: all

#### [説明]

アナログ親機モードにおいて、アナログ子機の受け入れモードを設定する。

#### [ノート]

受け入れ拒否された子機では、アナログ回線、ISDN 回線のアナログ発着信としての使用および TEL ポートの使用 (" \*#" をダイヤルすることによる TEL ポートからの設定を除く) が不可能となる。

本コマンドの設定が **show analog extension** コマンドで表示される「接続拒否中子機一覧」に反映されるまでに、数十秒程度時間を要する。

NVR700W は Rev.15.00.23 以降で使用不可。

代わりに **analog extension agent permit** コマンドを使用することができる。

#### [適用モデル]

NVR510

## 30.6 アナログ子機受け入れモードの設定

#### [書式]

**analog extension agent permit mode**

**no analog extension agent permit**

#### [設定値及び初期値]

- *mode*

- [設定値]:

| 設定値             | 説明                   |
|-----------------|----------------------|
| all             | すべて受け入れる             |
| registered-only | 機器番号を設定している機器のみ受け入れる |

- [初期値]: all

**[説明]**

アナログ親機モードにおいて、アナログ子機の受け入れモードを設定する。

**[ノート]**

受け入れ拒否された子機では、アナログ回線、ISDN 回線のアナログ発着信としての使用および TEL ポートの使用 ("\*#" をダイヤルすることによる TEL ポートからの設定を除く) が不可能となる。

本コマンドの設定が **show analog extension** コマンドで表示される「接続拒否中子機一覧」に反映されるまでに、数十秒程度時間を要する。

NVR700W は Rev.15.00.23 以降で使用可能。

**[適用モデル]**

NVR700W

## 30.7 アナログ子機受け入れモードの設定

---

**[書式]**

```
analog extension machine-id id mac_address
```

```
no analog extension machine-id id
```

**[設定値及び初期値]**

- *id*
  - [設定値]: 機器番号 (1..9)
  - [初期値]: -
- *mac\_address*
  - [設定値]: MAC アドレス xx:xx:xx:xx:xx:xx (xx は 16 進数)
  - [初期値]: -

**[説明]**

アナログ親機モードにおいて、アナログ親機 / 子機の機器番号を設定する。

**[ノート]**

機器番号を設定することにより、そのアナログ子機を着呼側とする機器間内線通話が可能になる。ただし、機器番号を設定していなくても外線及び一斉外線 ("\*\*") による呼び出しは可能。既に同じ *id* のアナログ子機が設定されている場合は、現在の設定が消されて新しい設定が上書きされる。同じ *mac\_address* の機器が既に設定されている場合は、エラーとなる。

**[適用モデル]**

NVR700W, NVR510

## 30.8 カスケード接続のログを記録するか否かの設定

---

**[書式]**

```
analog extension log switch
```

```
no analog extension log
```

**[設定値及び初期値]**

- *log*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | ログを出力する  |
| off | ログを出力しない |

- [初期値]: off

**[説明]**

カスケード接続のログを出力するか否かを設定する。

**[適用モデル]**  
NVR700W, NVR510

## 第 31 章

### SIP 機能の設定

#### 31.1 共通の設定

##### 31.1.1 SIP による VoIP 機能を使用するか否かの設定

[書式]

`sip use use`

`no sip use`

[設定値及び初期値]

• `use`

• [設定値]:

| 設定値 | 説明    |
|-----|-------|
| off | 使用しない |
| on  | 使用する  |

• [初期値]: off

[説明]

SIP プロトコルによる VoIP 機能を使用するか否かを設定する。

[ノート]

off の場合、設定した機器及び設定した機器をアナログ親機とするアナログ子機において SIP プロトコルによる VoIP 機能の発着信ができない。

on から off への設定の変更は再起動後有効となる。

[適用モデル]

NVR700W, NVR510

##### 31.1.2 SIP による発信時に使用する IP プロトコルの選択

[書式]

`sip ip protocol protocol`

`no sip ip protocol`

[設定値及び初期値]

• `protocol`

• [設定値]:

| 設定値 | 説明      |
|-----|---------|
| udp | UDP を使用 |
| tcp | TCP を使用 |

• [初期値]: udp

[説明]

SIP プロトコルによる VoIP の発信時、呼制御に使用する IP プロトコルを選択する。

[ノート]

着信した場合は、この設定に関わらず、受信したプロトコルで送信を行う。

[適用モデル]

NVR700W, NVR510



### 31.1.3 SIP による VoIP 機能で利用可能な音声コーデックの設定

#### [書式]

```

sip codec permit interface codec [codec ...]
sip codec permit pp peer_num codec [codec ...]
sip codec permit tunnel tunnel_num codec [codec ...]
no sip codec permit interface [codec ...]
no sip codec permit pp peer_num [codec ...]
no sip codec permit tunnel tunnel_num [codec ...]

```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェースの番号
  - [初期値]: -
- *codec*
  - [設定値]:

| 設定値   | 説明               |
|-------|------------------|
| g711u | G.711 $\mu$ -law |
| g711a | G.711 A-law      |

- [初期値]: g711u g711a

#### [説明]

SIP プロトコルによる VoIP で使用できるコーデック種別をインターフェース毎に設定する。

#### [ノート]

実際に VoIP で使用される CODEC は、このコマンドで設定された CODEC と、SIP メッセージにより通知された CODEC によって決定される。

従来機種とは *codec* パラメーターの設定が異なる。

従来機種の設定を流用する場合、設定値そのままでは読み込むことができないので注意が必要。

#### [設定例]

- pp1 で使用できる CODEC を G.711u だけに設定する

```
# sip codec permit pp 1 g711u
```

- lan2 で使用できる CODEC の設定値を初期値に戻す

```
# no sip codec permit lan2
```

#### [適用モデル]

NVR700W, NVR510

### 31.1.4 SIP のリクエスト再送タイムアウト値の設定

#### [書式]

```

sip request retransmit timer timer1 [timer2]
no sip request retransmit timer [timer1 [timer2]]

```

**[設定値及び初期値]**

- *timer1*
  - [設定値]: 通常の発信における INVITE 再送タイムアウト秒数 (4.0..32.0)
  - [初期値]: 32
- *timer2*
  - [設定値]: 迂回を伴う発信における INVITE 再送タイムアウト秒数 (4.0..32.0)
  - [初期値]: 4

**[説明]**

UDP プロトコルを用いた SIP の INVITE を送信する際の再送タイムアウト時間を設定する。最初に INVITE を送信した時点から指定した時間を経過した以降は、再送を行わない。

**[ノート]**

RFC3261 に従った動作とするためには、**sip request retransmit timer 32 32** と設定する必要がある。

**[適用モデル]**

NVR700W, NVR510

### 31.1.5 ネットボランチ電話で使用するドメイン名の設定

---

**[書式]**

**sip netvolante dial domain *name***

**no sip netvolante dial domain**

**[設定値及び初期値]**

- *name*
  - [設定値]: ネットボランチ電話番号に使用するドメイン名
  - [初期値]: tel.netvolante.jp

**[説明]**

[#][#] のプレフィックスを使用するネットボランチ電話番号への発呼での宛先アドレスに使用するドメイン名を設定する。rtpro.yamaha.co.jp に設定し、##87654321 をダイヤルした場合、sip:NetVolantePhone@87654321.rtpro.yamaha.co.jp に対して SIP の発呼を行う。

**[ノート]**

ネットボランチ DNS サービス以外の DDNS による電話番号割り当てサービスを利用する場合に設定する。

**[適用モデル]**

NVR700W, NVR510

### 31.1.6 ネットボランチ電話で SIP ユーザー名として付与する番号桁数の設定

---

**[書式]**

**sip netvolante dial figure *figure***

**no sip netvolante dial figure**

**[設定値及び初期値]**

- *figure*
  - [設定値]:

| 設定値            | 説明                                             |
|----------------|------------------------------------------------|
| ダイヤル桁数 (1..20) |                                                |
| 0              | SIP ユーザー名として付与する桁数なし。すなわち、従来通りすべてドメイン名として付与する。 |

- [初期値]: 0

**[説明]**

ネットボランチ電話番号に SIP ユーザー名として付与する桁数を、下位からの桁数で設定する。

**[ノート]**

設定例の設定を行った場合、##432187654321 をダイヤルすると、sip:4321@43218765.tel.netvolante.jp に対して SIP の発呼を行う。

**[設定例]**

SIP ユーザー名として付与する桁数を 4 桁で設定

```
# sip netvolante dial figure 4
```

**[適用モデル]**

NVR700W, NVR510

**31.1.7 特定のダイヤルに対応する SIP による発信先の設定****[書式]**

```
analog extension sip address number dial_number sip_address [name=description]
analog extension sip address number dial_number sip_address phone [name=description]
analog extension sip address number dial_number sip_address presence [name=description]
analog extension sip address number dial_number sip_address server=server_number [phone] [name=description]
no analog extension sip address number
```

**[設定値及び初期値]**

- *number*
  - [設定値]: 登録番号 (1..65535)
  - [初期値]: -
- *dial\_number*
  - [設定値]: TEL ポートからのダイヤル番号
  - [初期値]: -
- *sip\_address*
  - [設定値]: SIP で発呼する先の SIP URI
  - [初期値]: -
- *server\_number*
  - [設定値]: SIP で発呼する時に使用するサーバーの登録番号 (1..65535)
  - [初期値]: -
- *phone*: user=phone のタグを付けて発信することを示すキーワード
  - [初期値]: -
- *presence*: Windows Messenger に発信することを示すキーワード
  - [初期値]: -
- *description*
  - [設定値]: 登録名
  - [初期値]: -

**[説明]**

特定のダイヤルに対応する SIP による発信先の設定を行う。

**[ノート]**

ダイヤル番号に合致する設定を登録番号順に検索し、はじめに合致した設定が適用される。

*sip\_address* は、"sip:user\_name@domain\_name" という形式。

*server\_number* は、**sip server** コマンドで登録した SIP サーバーの登録番号を指定する。サーバーの指定がない場合あるいは登録番号で登録されたサーバーがない場合は、サーバーを使用せず、直接接続を行う。

*phone* を設定すると、宛先の URI に user=phone のタグを埋め込んで発呼する。一般回線に抜ける発呼を行う際に必要に応じて設定する。

発呼する相手が Windows Messenger の場合、*presence* を指定する。

*description* には自由な登録名が設定できる。

**[適用モデル]**

NVR700W, NVR510

### 31.1.8 SIP の session-timer 機能のタイマ値の設定

#### [書式]

**sip session timer** *time* [update=*update*] [refresher=*refresher*]

**no sip session timer**

#### [設定値及び初期値]

- *time*

- [設定値]:

| 設定値          | 説明                     |
|--------------|------------------------|
| 秒数 (60..540) |                        |
| 0            | session-timer 機能を利用しない |

- [初期値]: 0

- *update*

- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | UPDATE メソッドを使用する  |
| off | UPDATE メソッドを使用しない |

- [初期値]: off

- *refresher*

- [設定値]:

| 設定値  | 説明                          |
|------|-----------------------------|
| none | refresher パラメーターを設定しない      |
| uac  | refresher パラメーターに uac を設定する |
| uas  | refresher パラメーターに uas を設定する |

- [初期値]: uac

#### [説明]

SIP の session-timer 機能のタイマ値を設定する。

SIP の通話中に相手が停電などにより突然落ちた場合にタイマにより自動的に通話を切断する。

*update* を on に設定すれば、発信時に session-timer 機能において UPDATE メソッドを使用可能とする。

*refresher* を none に設定した時は refresher パラメーターを設定せず、uac/uas を設定した時はそれぞれのパラメーター値で発信する。

#### [適用モデル]

NVR700W, NVR510

### 31.1.9 SIP による発信時に 100rel をサポートするか否かの設定

#### [書式]

**sip 100rel** *switch*

**no sip 100rel**

#### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | 100rel をサポートする  |
| off | 100rel をサポートしない |

- [初期値]: off

**[説明]**

SIP の発信時に 100rel(RFC3262) をサポートするか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**31.1.10 送信する SIP パケットに User-Agent ヘッダを付加する設定****[書式]**

```
sip user agent sw [user-agent]
```

```
no sip user agent
```

**[設定値及び初期値]**

- *sw*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 付加する  |
| off | 付加しない |

- [初期値]: off

- *user-agent*

- [設定値]: ヘッダに記述する文字列

- [初期値]: -

**[説明]**

送信する SIP パケットに User-Agent ヘッダを付加することができる。

付加する文字列は、*user-agent* パラメーターにて設定することが可能であるが、64 文字以内で ASCII 文字のみ設定可能である。

**[適用モデル]**

NVR700W, NVR510

**31.1.11 着信可能なポートがない場合に返す SIP のレスポンスコードの設定****[書式]**

```
sip response code busy code
```

```
no sip response code busy
```

**[設定値及び初期値]**

- *code*: レスポンスコード

- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| 486 | 486 を返す |
| 503 | 503 を返す |

- [初期値]: 486

**[ノート]**

SIP 着信時に、ビジーで着信できない場合に返すレスポンスコードを設定する。

**[適用モデル]**

NVR700W, NVR510

**31.1.12 SIP による着信時の INVITE に refresher 指定がない場合の設定****[書式]**

```
sip arrive session timer refresher refresher
```

```
no sip arrive session timer refresher
```

**[設定値及び初期値]**

- *refresher*
- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| uac | refresher=uac と指定する |
| uas | refresher=uas と指定する |

- [初期値]: uac

**[説明]**

VoIP 機能の着信時において INVITE が *refresher* を指定していない場合に UAC/UAS を指定できる。

**[適用モデル]**

NVR700W, NVR510

**31.1.13 インターネット電話着信時におけるネーム・ディスプレイ情報通知設定****[書式]**

**sip arrive name-display default mode**

**no sip arrive name-display default [mode]**

**[設定値及び初期値]**

- *mode*
- [設定値]:

| 設定値 | 説明                                                                           |
|-----|------------------------------------------------------------------------------|
| off | ネーム・ディスプレイ情報として送出的る有効な情報がない場合にネーム・ディスプレイ情報を出力しない                             |
| on  | ネーム・ディスプレイ情報として送出的る有効な情報がない場合に「インターネット電話」あるいは「ネットボランチ電話」というネーム・ディスプレイ情報を通知する |

- [初期値]: off

**[説明]**

SIP プロトコルによる VoIP の着信において、ネーム・ディスプレイ情報として通知する有効な情報がない場合におけるネーム・ディスプレイの通知内容に関する設定を行う。

**[ノート]**

この設定に関わらず、ネーム・ディスプレイの設定がされていない TEL ポートにはネーム・ディスプレイ情報は通知されない。

ネーム・ディスプレイ情報として送出的る有効な情報が存在する場合、ネーム・ディスプレイの設定がされている TEL ポートには、この設定に関わらずネーム・ディスプレイの情報が通知される。

**[適用モデル]**

NVR700W, NVR510

**31.1.14 SIP による着信時に P-N-UAType ヘッダをサポートするか否かの設定****[書式]**

**sip arrive ringing p-n-uatype switch**

**no sip arrive ringing p-n-uatype**

**[設定値及び初期値]**

- *switch*
- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | P-N-UAType ヘッダを付加する |

| 設定値 | 説明                   |
|-----|----------------------|
| off | P-N-UAType ヘッダを付加しない |

- [初期値] : off

**[説明]**

SIP プロトコルによる着信時に送信する Ringing レスポンスに、P-N-UAType ヘッダを付加するか否かを設定する。

**[ノート]**

設定はすべての着信に適用される。

**[適用モデル]**

NVR700W, NVR510

### 31.1.15 着信時のセッションタイマのリクエストを設定

**[書式]**

**sip arrive session timer method *method***

**no sip arrive session timer method [*method*]**

**[設定値及び初期値]**

- *method*

- [設定値] :

| 設定値    | 説明             |
|--------|----------------|
| auto   | 自動的に判断する       |
| invite | INVITE のみを使用する |

- [初期値] : auto

**[説明]**

着信時にセッションタイマ機能で使用するリクエストを設定する。

auto に設定した場合には UPDATE, INVITE とともに使用でき、発信側またはサーバーで UPDATE に対応していれば UPDATE を使用する。

invite に設定した場合には、発信側またはサーバーで UPDATE に対応していてもこれを使用せずに動作する。

UPDATE のみを使用する設定はできない。

また、サーバー毎に設定することできないため、全ての着信でこの設定が有効となる。

発信の場合は、**sip server session timer** または **sip session timer** の *update* オプションで設定できる。

**[適用モデル]**

NVR700W, NVR510

### 31.1.16 SIP 着信時に SIP ユーザー名を検証するかどうかの設定

**[書式]**

**sip arrive address check *SW***

**no sip arrive address check**

**[設定値及び初期値]**

- *SW*

- [設定値] :

| 設定値 | 説明              |
|-----|-----------------|
| on  | SIP ユーザー名を検証する  |
| off | SIP ユーザー名を検証しない |

- [初期値] : on

**[説明]**

SIP の着信時に SIP ユーザー名が正常かどうかを検証する設定をする。

## [ノート]

この検証は **sip server** コマンドの設定がある場合に有効となる。

## [適用モデル]

NVR700W, NVR510

### 31.1.17 SIP で使用する IP アドレスの設定

---

## [書式]

**sip outer address** *ipaddress*

**no sip outer address**

## [設定値及び初期値]

- *ipaddress*

- [設定値]:

| 設定値     | 説明      |
|---------|---------|
| auto    | 自動設定    |
| IP アドレス | IP アドレス |

- [初期値]: auto

## [説明]

SIP で使用する IP アドレスを設定する。RTP/RTCP もこの値が使用される。

## [ノート]

初期設定のまま使用する事を推奨する。

## [適用モデル]

NVR700W, NVR510

### 31.1.18 SIP メッセージのログを記録するか否かの設定

---

## [書式]

**sip log** *switch*

**no sip log**

## [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | SIP メッセージのログを記録する  |
| off | SIP メッセージのログを記録しない |

- [初期値]: off

## [説明]

SIP メッセージのログを DEBUG レベルのログに記録するか否かを設定する。

## [適用モデル]

NVR700W, NVR510

## 31.2 SIP サーバー毎の設定

---

### 31.2.1 SIP サーバーの設定

---

## [書式]

**sip server** *number address type protocol sip\_uri [username [password]] [name=name]*

**no sip server** *number*



**[設定値及び初期値]**

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *address*
  - [設定値]: SIP サーバーの IP アドレス
  - [初期値]: -
- *type*
  - [設定値]:
    - register
    - no-register
  - [初期値]: -
- *protocol*
  - [設定値]:

| 設定値 | 説明        |
|-----|-----------|
| tcp | TCP プロトコル |
| udp | UDP プロトコル |

- [初期値]: -
- *sip\_uri*
  - [設定値]: SIP アドレス
  - [初期値]: -
- *username*
  - [設定値]: ユーザー名
  - [初期値]: -
- *password*
  - [設定値]: パスワード
  - [初期値]: -
- *name*
  - [設定値]: 登録名
  - [初期値]: -

**[説明]**

SIP サーバー設定を追加または削除する。

**[適用モデル]**

NVR700W, NVR510

**31.2.2 SIP サーバー毎の先頭に付加された 184/186 の扱いの設定**

**[書式]**

**sip server privacy number switch [pattern]**  
**no sip server privacy number switch [pattern]**

**[設定値及び初期値]**

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値        | 説明                                      |
|------------|-----------------------------------------|
| off        | ダイヤルされたそのままの番号で発信する                     |
| always-off | ダイヤルされた番号から 184 / 186 を取り除き、常に「通知」で発信する |

| 設定値         | 説明                                                                     |
|-------------|------------------------------------------------------------------------|
| always-on   | ダイヤルされた番号から 184 / 186 を取り除き、常に「非通知」で発信する                               |
| default-off | ダイヤルされた番号から 184 / 186 を取り除き、184 が付加されている場合には「非通知」で、それ以外の場合には「通知」で発信する。 |
| default-on  | ダイヤルされた番号から 184 / 186 を取り除き、186 が付加されている場合には「通知」で、それ以外の場合には「非通知」で発信する。 |

- [初期値] : off
- *pattern*
- [設定値] :

| 設定値         | 説明                                               |
|-------------|--------------------------------------------------|
| sip-privacy | draft-ietf-sip-privacy-01 に従って発信者番号の通知 / 非通知を行う。 |
| rfc3325     | RFC3325 に従って発信者番号の通知 / 非通知を行う。                   |
| as-is       | ダイヤルされた番号に 184 / 186 を付加して発信する。                  |

- [初期値] :-

#### [説明]

ダイヤルされた番号の先頭に付加された 184 / 186 をどのように取り扱うかを指定する。各 *pattern* パラメーターで指定した方式に従って、ダイヤルされた番号を処理する。*pattern* パラメーターを省略した場合は、draft-ietf-sip-privacy-01 に従って、ダイヤルされた番号を処理する。

#### [適用モデル]

NVR700W, NVR510

### 31.2.3 SIP サーバー毎の発信時に使用する自己 SIP ディスプレイ名の設定

#### [書式]

**sip server display name** *number displayname*

**no sip server display name** *number*

#### [設定値及び初期値]

- *number*
  - [設定値] : SIP サーバーの登録番号 (1..65535)
  - [初期値] :-
- *displayname*
  - [設定値] : ディスプレイ名
  - [初期値] :-

#### [説明]

SIP サーバー毎の発信時に使用される自己 SIP ディスプレイ名を設定する。

#### [ノート]

空白を含むディスプレイ名を設定する場合、"" で囲む必要がある。漢字を設定する場合は、シフト JIS コードで設定を行う。

#### [適用モデル]

NVR700W, NVR510

### 31.2.4 SIP サーバー毎の発信時の相手 SIP アドレスのドメイン名の設定

#### [書式]

```

sip server call remote domain number domain
no sip server call remote domain number

```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *domain*
  - [設定値]: ドメイン名
  - [初期値]: -

#### [説明]

SIP サーバー経由の発信時に、相手の SIP アドレスの host 部分を設定したドメイン名にして発信する。

ドメイン名の長さは 58 文字まで設定できる。

なお、ドメイン名として使用可能な文字は、アルファベット、数字、ハイフン、ピリオド、コロン、カッコ[]のみである。ドメイン名を設定しない場合には、**sip server** コマンドの SIP-URI の host 部分と同じドメイン名にして発信する。

#### [適用モデル]

NVR700W, NVR510

### 31.2.5 SIP サーバー毎の session-timer 機能のタイマ値の設定

#### [書式]

```

sip server session timer number time [update=update] [refresher=refresher]
no sip server session timer number

```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *time*
  - [設定値]:
    - 秒数(60..540)
    - 0 ... session-timer 機能を利用しない
  - [初期値]: -
- *update*
  - [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | UPDATE メソッドを使用する  |
| off | UPDATE メソッドを使用しない |

- [初期値]: -
- *refresher*
  - [設定値]:

| 設定値  | 説明                          |
|------|-----------------------------|
| none | refresher パラメーターを設定しない      |
| uac  | refresher パラメーターに uac を設定する |
| uas  | refresher パラメーターに uas を設定する |

- [初期値]: -

**[説明]**

SIP サーバー毎の session-timer 機能のタイマ値を設定する。

SIP の通話中に相手が停電などにより突然落ちた場合にタイマにより自動的に通話を切断する。

サーバーが session-timer に対応していれば、端末が 2 台同時に突然落ちてもサーバーでの呼の持ち切りを防ぐことができる。

*update* を on に設定すれば、発信時に session-timer 機能において UPDATE メソッドを使用可能とする。

*refresher* を none に設定した時は refresher パラメーターを設定せず、uac/uas を設定した時はそれぞれのパラメーター値で発信する。

**[適用モデル]**

NVR700W, NVR510

**31.2.6 SIP サーバー毎の発信時に 100rel をサポートするか否かの設定****[書式]**

```
sip server 100rel number switch
```

```
no sip server 100rel number
```

**[設定値及び初期値]**• *number*

- [設定値]: SIP サーバーの登録番号 (1..65535)
- [初期値]: -

• *switch*

- [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | 100rel をサポートする  |
| off | 100rel をサポートしない |

- [初期値]: off

**[説明]**

SIP サーバー経由の発信時に 100rel(RFC3262) をサポートするか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

**31.2.7 SIP サーバー毎の REGISTER リクエストの更新間隔の設定****[書式]**

```
sip server register timer server=number OK_time NG_time
```

```
no sip server register timer server=number
```

**[設定値及び初期値]**• *number*

- [設定値]: SIP サーバーの登録番号 (1..65535)
- [初期値]: -

• *OK\_time*

- [設定値]: 通常時更新間隔 (分)
- [初期値]: 30

• *NG\_time*

- [設定値]: 異常時更新間隔 (分)
- [初期値]: 5

**[説明]**

SIP サーバーに REGISTER リクエストを送信する間隔を設定する。

正常に更新されている場合には通常時更新間隔毎に更新する。サーバーからエラーが返されたり、サーバーから応

答が無い場合には、異常時更新間隔毎に更新する。また、この時の Expires ヘッダは通常時更新間隔を 2 倍して秒に直した値で送信する。しかし、サーバーから Expires の指定があった場合はその値に従って、指定された値の半分の時間で通常時の更新を行う。

[適用モデル]  
NVR700W, NVR510

### 31.2.8 SIP サーバー毎の REGISTER リクエストの Request-URI の設定

---

#### [書式]

```
sip server register request-uri number sip_address
no sip server register request-uri number
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *sip\_address*
  - [設定値]: Request-URI
  - [初期値]: -

#### [説明]

SIP サーバーに送信する REGISTER リクエストの Request-URI を設定する。  
設定しない場合は、**sip server** コマンドで設定した SIP-URI の host 部分を入れて REGISTER リクエストを送信する。

[適用モデル]  
NVR700W, NVR510

### 31.2.9 SIP サーバー毎の REGISTER リクエストの Contact ヘッダに付加する q 値の設定

---

#### [書式]

```
sip server qvalue number value
no sip server qvalue number
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *value*
  - [設定値]: q 値 (0..1.000)
  - [初期値]: 0

#### [説明]

SIP サーバーへ接続する時に送信する REGISTER リクエストの Contact ヘッダに付加する q 値を設定する。0.001 単位で設定可能。

同じアカウントで同時に複数の端末から接続が許されている SIP サーバーを利用する時に、この設定により着信する優先順位を SIP サーバーに通知することが可能となる。数値が大きい方が優先される。

*value* = 0 で q 値を付加しない設定となる。

[適用モデル]  
NVR700W, NVR510

### 31.2.10 SIP サーバー毎の着信時の発番号情報通知ルールの設定

---

#### [書式]

```
sip server arrive number display server=number rule=rule
no sip server arrive number display server=number
```

**[設定値及び初期値]**

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *rule*: ナンバー・ディスプレイ表示内容ルール
  - [設定値]:

| 設定値   | 説明                                                                                                                                                                                                                                                                                                                                         |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| as-is | DisplayName、SIP ユーザー名の順に検索、表示できる内容をそのまま表示。                                                                                                                                                                                                                                                                                                 |
| 1     | 1. SIP ユーザー名が数字であった場合、SIP ユーザー名を使用し、<br>1.1 8桁未満であればそのまま表示<br>1.2 先頭が'0'であればそのまま表示<br>1.3 先頭が'81'または'+81'であれば、その部分を'0'に置き換えて表示<br>1.4 その他の場合は先頭に'0'を付加して表示<br>2. SIP ユーザー名が数字のみでない場合、<br>2.1 DisplayName に番号非通知の理由表示が示されていればその内容を表示<br>2.2 DisplayName がすべて数字の場合、その番号を表示<br>2.3 DisplayName が数字のみでない場合、あるいは DisplayName がない場合、サービス提供不可で非表示 |
| 2     | 1. のルールにおいて、2.2 の場合にサービス提供不可で非表示とする                                                                                                                                                                                                                                                                                                        |

- [初期値]: 1

**[説明]**

SIP プロトコルによるインターネット電話着信で、自分の SIP アドレス帳に設定されていない相手からの着信、あるいは NetVolante 電話番号が通知された着信でない場合に、ナンバー・ディスプレイ等での発番号情報表示内容のルールを設定する。

**[適用モデル]**

NVR700W, NVR510

### 31.2.11 SIP サーバー経由接続時におけるアナログ付加サービス設定

**[書式]**

```

sip server analog service number rule=rule
sip server analog service number off
no sip server analog service number
  
```

**[設定値及び初期値]**

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *rule*
  - [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| 5   | アナログ付加サービスルール 5 |

- [初期値]: off

**[説明]**

SIP サーバー経由の通話時におけるアナログ付加サービスサポートを設定する。

## [ノート]

`rule=5` においてサポートする付加サービスは以下の通り。

- 被保留 / 被保留解除 (`m=sendonly`, `c=0` に対応)
- `off` の場合、アナログ付加サービスは機能しない。

## [適用モデル]

NVR700W, NVR510

### 31.2.12 SIP サーバーへの接続状態に応じて発信するか否かの設定

## [書式]

`sip server call mode number mode`

`no sip server call mode number`

## [設定値及び初期値]

- `number`
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- `mode`
  - [設定値]:
    - `normal`
    - `connect-only`
  - [初期値]: `normal`

## [説明]

SIP サーバーへの接続状態 (`show status sip server` コマンド参照) に応じて、SIP サーバーへの発信を行うか否かを設定する。

`normal` を指定すると、接続状態にかかわらず常に発信する。

`connect-only` を指定すると、接続状態が「通信中」の場合のみ発信する。

電話番号ルーティングの自動迂回機能を利用し、第 1 経路として SIP サーバーを指定している場合は、その SIP サーバーがアクセス不能の時は常にタイムアウトを待って迂回発信することになるが、発信動作モードを `connect-only` に設定することで、即座に第 2 経路へ迂回発信させることができるようになる。

また、接続状況が「通信中」であっても、一度接続に失敗 (タイムアウトするか、または 500 番台の応答コードを受信) すれば、次の発信からは即座に迂回発信するようになる。

以降は再び SIP サーバーへのアクセスが可能となり接続状況が「通信中」となるまで、SIP サーバーへの発信は行われない。

## [ノート]

SIP サーバーの登録でサーバー種類を `no-register` で登録している場合は、接続状況をあらかじめ知ることができないので、動作モードの指定によらず常に発信する動作になる。

## [適用モデル]

NVR700W, NVR510

### 31.2.13 SIP サーバーへの発信に番号以外を使えないように制限する設定

## [書式]

`sip server dial number-only server=number sw`

`no sip server dial number-only server=number`

## [設定値及び初期値]

- `number`
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- `sw`
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 制限する |

| 設定値 | 説明    |
|-----|-------|
| off | 制限しない |

- [初期値]: off

#### [説明]

SIP サーバー経由での VoIP 発信時に \* など番号以外をダイヤルして発信しようとした場合に番号が正しくないとして発信しないように制限する。

#### [適用モデル]

NVR700W, NVR510

### 31.2.14 自分自身の SIP アドレスへの発信を許可するかどうかの設定

#### [書式]

```
sip server call own permit server=number sw
```

```
no sip server call own permit server=number
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: off

#### [説明]

To, From が同じ SIP アドレスとなるような発信を許可するか否かを設定する。

この機能を利用して正常に発信ができるのは、Call-ID や tag 等の乱数値を発信側と着信側で別の値を付加して管理する SIP サーバーを利用する場合だけである。

そのため、通常は off で運用する。

#### [適用モデル]

NVR700W, NVR510

### 31.2.15 SIP サーバー毎の代表 SIP アドレスの設定

#### [書式]

```
sip server pilot address number sipaddress
```

```
no sip server pilot address number
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *sipaddress*
  - [設定値]: 代表 SIP アドレス
  - [初期値]: -

#### [説明]

SIP サーバー経由の発信時に、INVITE リクエストの P-Preferred-Identity ヘッダに設定した代表 SIP アドレスを入れて発信する。

#### [適用モデル]

NVR700W, NVR510



### 31.2.16 発信時の 5xx エラーをサーバー障害とするか否かの設定

#### [書式]

```
sip server call server error server=number sw
```

```
no sip server call server error server=number
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | サーバー障害とする  |
| off | サーバー障害としない |

- [初期値]: off

#### [説明]

on に設定した場合は、SIP サーバーを経由した発信時に initial-INVITE に対して 5xx エラーレスポンスを返された時に、サーバー障害と認識してサーバーとの接続状態を未接続とする。

より早くサーバー障害を検知することが可能となるが、SIP サーバーの仕様によっては、設定ミスや発信タイムアウト等によっても 5xx エラーレスポンスを返すことがあるので、設定する際には SIP サーバーの仕様を確認する必要がある。

#### [適用モデル]

NVR700W, NVR510

### 31.2.17 SIP サーバー毎の REGISTER リクエストの Contact ヘッダーの設定

#### [書式]

```
sip server register contact mode number mode
```

```
no sip server register contact mode number [mode]
```

#### [設定値及び初期値]

- *number*
  - [設定値]: SIP サーバーの登録番号 (1..65535)
  - [初期値]: -
- *mode*
  - [設定値]: 動作モード (1..3)
  - [初期値]: 1

#### [説明]

SIP サーバーに送信する REGISTER リクエストの Contact ヘッダーに関する動作を設定する。一部の VoIP キャリアを使う場合にのみ設定を変更する必要がある。

#### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で設定できる。

#### [適用モデル]

NVR700W, NVR510

## 31.3 TEL ポートの設定

### 31.3.1 TEL ポートからの SIP による発信の制限の設定

#### [書式]

**analog sip call permit** *port permit*

**no analog sip call permit** *port*

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *permit*

- [設定値]:

| 設定値 | 説明          |
|-----|-------------|
| off | SIP への発信を拒否 |
| on  | SIP への発信を許可 |

- [初期値]: on

#### [説明]

指定した TEL ポートの SIP 発信に対する設定を行う。

#### [適用モデル]

NVR700W, NVR510

### 31.3.2 TEL ポートからの SIP による発信で使用する自己 SIP ユーザー名の設定

#### [書式]

**analog sip call myname** *port username*

**no analog sip call myname** *port*

#### [設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- *username*

- [設定値]: ユーザー名 (sip: で始まり、@ を含まない SIP ユーザー名)

- [初期値]:

- sip:nvr700w ( NVR700W )
- sip:nvr510 ( NVR510 )

#### [説明]

SIP プロトコルによる VoIP 発信で使用する自己 SIP ユーザー名を設定する。

*username* には "sip:" の部分を除いて最大 28 文字まで設定できる。

#### [ノート]

SIP 着信時の宛先による着信制限では、このコマンドと **analog sip arrive myaddress** で設定されたアドレスに対する着信を **analog sip arrive permit** によって許可することができる。

[適用モデル]  
NVR700W, NVR510

### 31.3.3 TEL ポートからの SIP による発信で使用する自己 SIP ディ스플레이名の設定

#### [書式]

**analog sip call display name** *port displayname*  
**no analog sip call display name** *port*

#### [設定値及び初期値]

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *displayname*
  - [設定値]: ディ스플레이名
  - [初期値]: -

#### [説明]

SIP プロトコルによる VoIP 発信で使用する自己 SIP ディ스플레이名を設定する。

#### [ノート]

空白を含むディスプレイ名を設定する場合、"" で囲む必要がある。  
漢字を設定する場合は、シフト JIS コードで設定を行う。

[適用モデル]  
NVR700W, NVR510

### 31.3.4 TEL ポートにおける宛先 SIP アドレスによる着信制限の設定

#### [書式]

**analog sip arrive permit** *port mode*

#### [設定値及び初期値]

- *port*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *mode*

- [設定値]:

| 設定値    | 説明                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------|
| off    | TEL ポートへの着信をすべて拒否                                                                                  |
| myname | <b>analog sip call myname</b> 及び <b>analog sip arrive myaddress</b> で登録されているユーザー名 / アドレスに対する着信のみ許可 |
| on     | TEL ポートへの着信をすべて許可                                                                                  |

- [初期値]: on

#### [説明]

SIP プロトコルによる VoIP の宛先アドレスに対する着信制限を設定する。

## [ノート]

myname に設定されている場合の動作は以下の通りになる。

- SIP の To: フィールドのユーザー名 (@ 以前) と **analog sip call myname** の設定及び **analog sip arrive myaddress** の設定でドメイン指定のないものを比較し、一致する設定があれば着信する。
- SIP の To: フィールドの SIP URI と **analog sip arrive myaddress** の設定でドメイン指定があるものを比較し、一致する設定があれば着信する。

## [適用モデル]

NVR700W, NVR510

### 31.3.5 TEL ポートにおける SIP の着信識別で使用する自己 SIP アドレスの設定

## [書式]

**analog sip arrive myaddress** port number sip\_address

**no analog sip arrive myaddress** port number

## [設定値及び初期値]

- port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- number

- [設定値]: 登録番号 (1..65535)

- [初期値]: -

- sip\_address

- [設定値]: SIP アドレス ( sip: で始まり @ を含んだ SIP URI または sip: で始まる @ を含まない SIP ユーザー名 )

- [初期値]: -

## [説明]

SIP プロトコルによる VoIP の着信識別に使用する自己 SIP アドレスを設定する。

## [適用モデル]

NVR700W, NVR510

### 31.3.6 TEL ポートにおける SIP の着信に対するアナログダイヤルインと無鳴動着信機能の設定

## [書式]

**analog sip arrive incoming-signal** port number sip\_address signal dial\_in-num

**analog sip arrive incoming-signal** port number lastdigit signal dial\_in-digit

**no analog sip arrive incoming-signal** port number

## [設定値及び初期値]

- port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

- number

- [設定値]: 登録番号 (1..65535)

- [初期値]: -

- sip\_address

- [設定値]:

| 設定値      | 説明                                                       |
|----------|----------------------------------------------------------|
| SIP アドレス | sip: で始まり @ を含んだ SIP URI または sip: で始まる @ を含まない SIP ユーザー名 |
| default  | 一致する登録エントリが見つからない場合にはこの記述で指定された動作に従うことを示すキーワード           |

- [初期値]:-
- `lastdigit`: ダイヤルイン番号として送出手数を引数とすることを示すキーワード
  - [初期値]:-
- `signal`
  - [設定値]:

| 設定値            | 説明        |
|----------------|-----------|
| modem          | モデムダイヤルイン |
| pb             | PB ダイヤルイン |
| no-ringing-fax | 無鳴動着信     |

- [初期値]:-
- `dial_in-num`
  - [設定値]: アナログ機器に送出するダイヤルイン番号 (`signal` で `modem` または `pb` を指定したときのみ有効)
  - [初期値]:-
- `dial_in-digit`
  - [設定値]: ダイヤルイン番号として送出手数 (1..20)
  - [初期値]:-

#### [説明]

SIP プロトコルによる VoIP の着信において、指定した `port` に対して、`sip_address` の一致する着信があったときに、`signal` に相当した着信処理を行う。アナログダイヤルインのときには、`dial_in-num` で設定されたダイヤルイン信号を出す。

`sip_address` に `lastdigit` を設定すると、数字で構成された SIP ユーザー名から下位 `dial_in-digit` 桁の番号をダイヤルイン信号として出力する。`dial_in-digit` は `signal` が `modem` の場合 1-20、`pb` の場合 1-4 の範囲で設定できる。

`sip_address` に `default` を設定すると、SIP アドレスが一致する項目がなかった場合あるいは、`lastdigit` の書式が設定されている時に SIP ユーザー名が数字で構成されておらず、ダイヤルイン信号のための情報を構成できない場合の動作を指定できる。

`dial_in-num` は `signal` が `modem` の場合には 20 桁以内、`pb` の場合には 4 桁以内で設定できる。

#### [ノート]

`sip_address` に '@' が含まれない場合、着信したインターネット電話の宛先 SIP ユーザー名 ('@'以前) のみを比較して着信処理が行われる。

TEL ポートに PBX が接続されており、PB ダイヤルインサービスを使用している場合に、着 SIP ユーザー名とダイヤルイン登録の SIP ユーザー名が一致しない、あるいは `lastdigit` で SIP ユーザー名が数字の情報でないことによってダイヤルイン信号が出力されず PBX に正しく着信できないようなケースの対応として、`default` を設定することにより常にダイヤルイン信号が出力されるように動作させることができる。

#### [設定例]

- TEL1 ポートの SIP 着信サービスのデフォルト動作を PB ダイヤルイン 1234 とする場合

```
# analog sip arrive incoming-signal 1 1 default pb 1234
```

- TEL1 ポートの SIP 着信時にユーザー名の下位 4 桁を PB ダイヤルインとする場合

```
# analog sip arrive incoming-signal 1 1 lastdigit pb 4
```

#### [適用モデル]

NVR700W, NVR510

## 31.3.7 TEL ポートにおける特定のプレフィックスによる発呼経路選択の設定

## [書式]

```

analog extension dial prefix [port=port] route [prefix="dial"]
analog extension dial prefix [port=port] sip [server=server_num [phone]] [prefix="dial"]
analog extension dial prefix [port=port] ngn interface [prefix="dial"]
analog extension dial prefix [port=port] routing route-table=route_table_num server=server_num[/server_sign] [phone]
[prefix="dial"]
analog extension dial prefix [port=port] routing route-table=route_table_num ngn interface [prefix="dial"]
no analog extension dial prefix [port=port] route
no analog extension dial prefix [port=port] sip [server=server_num [phone]]
no analog extension dial prefix [port=port] ngn interface
no analog extension dial prefix [port=port] routing route-table=route_table_num server=server_num[/server_sign]
[phone]
no analog extension dial prefix [port=port] routing route-table=route_table_num ngn interface

```

## [設定値及び初期値]

• *port*

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

• *route*

- [設定値]:

| 設定値        | 説明                                   |
|------------|--------------------------------------|
| line       | アナログ回線、ISDN 回線でかけるためのプレフィックス設定       |
| netvolante | NetVolante インターネット電話でかけるためのプレフィックス設定 |

- [初期値]: -

• *route\_table\_num*

- [設定値]: 発呼経路のテーブル登録番号
- [初期値]: -

• *server\_num*

- [設定値]: ダイヤルした番号を埋め込むサーバー番号
- [初期値]: -

• *server\_sign*

- [設定値]: ダイヤルした番号を埋め込むサーバー(記号表示)
- [初期値]: -

• *phone*: 宛先の URI に user=*phone* のタグを埋め込むことを示すキーワード

- [初期値]: -

• *interface*

- [設定値]: ひかり電話回線を接続する LAN インターフェース名、または ONU インターフェース名
- [初期値]: -

• *dial*

- [設定値]:

| 設定値                                    | 説明        |
|----------------------------------------|-----------|
| 入力なし                                   | プレフィックスなし |
| "0" から "9" までの数字または "#" (2桁目のみ)、最大 4 桁 | プレフィックス   |

- [初期値]:-

#### [説明]

TEL ポートからのダイヤル時に、特定のプレフィックスによる発呼経路を設定する。プレフィックスはダブルクォーテーション(")で括弧で指定する。"#" が設定できるのは2桁目だけである。

プレフィックスが既に他の経路に設定されている場合、新しく設定した経路が有効となり、以前の経路は削除される。

*port* を設定すると、選択された TEL ポートのみに対してプレフィックスと発呼経路の関係が設定される。発呼時には、まず TEL ポートに対する設定が優先され、そのプレフィックスに対する設定が存在しない場合は TEL ポートが指定されていない設定が使用される。

*sip* を設定すると、*sip* による発呼を行う。また、これに続けて *server\_num* を設定すると、**sip server** コマンドによるサーバー設定における SIP\_URI のユーザー名部分をダイヤルした番号に置き換えて SIP の発呼を行う。

*phone* を設定すると、宛先の URI に *user=phone* のタグを埋め込んで SIP の発呼を行う。アナログ回線または ISDN 回線に抜ける発呼を行う際に必要に応じて設定する。

*routing* を設定すると、ダイヤル番号に応じて番号経路テーブルを参照して、発呼を行う。

*ngn interface* を設定した場合は、設定した LAN インターフェース、または ONU インターフェースからひかり電話により発呼を行う。

#### [ノート]

先頭からの一部が重複するプレフィックス (例えば "9#" と "9#9") は異なるものとして扱われる。また次のパターンをプレフィックスとして設定することはできない。

"1", "11", "110", "118", "119", "110x", "118x", "119x", "x#1", "x#11" (x は 0-9 の数字)

*route* パラメーターが *netvolante* の設定に対しては、プレフィックスとして "###" が固定で登録されており、この設定を削除することはできない。新規に設定されたプレフィックスは "###" の置き換えではなく、追加されるプレフィックスとして扱われる。

*port* パラメーターを省略した場合において、カスケード接続の親機子機に明示的なプレフィックスの設定が無い場合は、その設定がカスケード接続全体を代表する設定として扱われる。

発呼経路を *routing* で設定した場合には、*route\_table\_num* も合わせて設定しなければならない。またこの場合に該当する発呼経路テーブルが **analog call route-table** コマンドによって登録されていないと、さらに、**analog call route** コマンドによる発呼経路のサーバー設定がサーバー記号による記述である場合には、*server\_sign* も合わせて設定しなければならない。

全体で 10 件まで、各 TEL ポートに関してそれぞれ 10 件まで、プレフィックスを指定することが可能。

#### [適用モデル]

NVR700W, NVR510

### 31.3.8 TEL ポートでの識別着信をするか否かの設定

#### [書式]

```
analog sip arrive restrict port restrict
no analog sip arrive restrict port
```

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |

| 設定値 | 説明       |
|-----|----------|
| 2   | TEL2 ポート |

- [初期値]: -
- *restrict*
- [設定値]:

| 設定値    | 説明      |
|--------|---------|
| permit | 着信許可    |
| reject | 着信拒否    |
| none   | 識別着信しない |

- [初期値]: reject

#### [説明]

SIP の着信に対して、TEL ポートで識別着信をするか否かを設定する。

**analog sip arrive restrict list** コマンドで登録された識別着信リストに対しての着信動作を決定する。permit の場合には、発番号が登録リストに含まれれば着信許可となり、それ以外は着信拒否となる。reject の場合には、発番号が登録リストに含まれれば着信拒否となり、それ以外は着信許可となる。none の場合には、すべての発番号に対して着信許可となる。

#### [ノート]

ナンバー・ディスプレイサービスの契約が必要。

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で設定できる。

#### [適用モデル]

NVR700W, NVR510

### 31.3.9 識別着信リストの登録

#### [書式]

**analog sip arrive restrict list** *port number sip\_address*

**no analog sip arrive restrict list** *port number*

#### [設定値及び初期値]

- *port*
- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -
- *number*
- [設定値]: リスト番号
- [初期値]: -
- *sip\_address*
- [設定値]: SIP アドレス(*sip:* で始まり *@* を含んだ SIP URI または *sip:* で始まる *@* を含まない SIP ユーザー名)
- [初期値]: -

#### [説明]

SIP の識別着信用の SIP アドレスをリストへ登録する。

リスト番号とは、SIP の識別着信リストの中で管理される通し番号である。また、SIP の識別着信リストは TEL ポート毎に管理される個別のリストである。



## [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で設定できる。

## [適用モデル]

NVR700W, NVR510

### 31.3.10 発番号情報なし SIP 着信機能の設定

## [書式]

**analog sip arrive without-calling-number port type [option [option [option]]]**

**no analog sip arrive without-calling-number port**

## [設定値及び初期値]

## • port

- [設定値]:

| 設定値 | 説明       |
|-----|----------|
| 1   | TEL1 ポート |
| 2   | TEL2 ポート |

- [初期値]: -

## • type

- [設定値]:

| 設定値    | 説明                  |
|--------|---------------------|
| permit | 発番号情報なし SIP 着信を許可する |
| reject | 発番号情報なし SIP 着信を拒否する |

- [初期値]: permit

## • option

- [設定値]:

| 設定値                 | 説明                     |
|---------------------|------------------------|
| all                 | すべての着信を対象にする           |
| public-telephone    | 本設定を公衆電話からの着信に限定する     |
| rejected-by-user    | 本設定をユーザによる通知拒否の着信に限定する |
| service-unavailable | 本設定を表示圏外からの着信に限定する     |

- [初期値]: all

## [説明]

SIP 着信に対して、指定した TEL ポートの発番号情報なしの着信を、指定した非通知理由により許可するか否かを選択する。

## [ノート]

ナンバー・ディスプレイサービスの契約が必要。

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で設定できる。

## [適用モデル]

NVR700W, NVR510

## 31.4 電話番号ルーティングの設定

### 31.4.1 ダイヤル番号によって発呼経路を自動選択するテーブルの設定

#### [書式]

```
analog call route-table route_table_num [name=route_table_name] route_num_list...
no analog call route-table route_table_num
```

#### [設定値及び初期値]

- *route\_table\_num*
  - [設定値]: 経路テーブル登録番号 (1..100)
  - [初期値]: -
- *route\_table\_name*
  - [設定値]: 経路テーブル名称
  - [初期値]: -
- *route\_num\_list*
  - [設定値]: 空白で区切られた発呼経路番号の並び (100 個以内)
  - [初期値]: -

#### [説明]

**analog call route** コマンドによる発呼経路を組み合わせ、ダイヤル番号によって発呼経路を自動選択するテーブルを設定する。

発呼経路番号のリストは、評価したい順に記述する。

入力ダイヤルの条件が一致する経路が見つかった時点で経路が決定し、以降の経路情報は参照しない。

評価の際に最終的にリスト内のどの経路情報とも一致しない場合は、発信不可である。

#### [ノート]

経路テーブルの総数は最大で 8 個まで登録できる。

同じ経路番号を同一リスト内に 2 回以上記述することはできない。

#### [適用モデル]

NVR700W, NVR510

### 31.4.2 ダイヤル番号と発呼経路との関連付けの設定

#### [書式]

```
analog call route route_num in_dial [out_dial1] route1 [[out_dial2] route2]
no analog call route route_num
```

#### [設定値及び初期値]

- *route\_num*
  - [設定値]: 経路登録番号 (1..65535)
  - [初期値]: -
- *in\_dial*
  - [設定値]: 入力ダイヤル番号
  - [初期値]: -
- *out\_dial1*
  - [設定値]: 第 1 経路の出力ダイヤル番号
  - [初期値]: -
- *route1*: 第 1 経路
  - [設定値]:

| 設定値                             | 説明                    |
|---------------------------------|-----------------------|
| line                            | アナログ回線、ISDN 回線経由で発信する |
| server=SIP サーバー番号または SIP サーバー記号 | SIP サーバー経由で発信する       |
| ngn interface                   | ひかり電話で発信する            |
| prohibit                        | 発信禁止                  |

- [初期値]: -
- *out\_dial2*
  - [設定値]: 第 2 経路の出力ダイヤル番号
  - [初期値]: -
- *route2*: 第 2 経路
  - [設定値]:

| 設定値                       | 説明                    |
|---------------------------|-----------------------|
| <i>line</i>               | アナログ回線、ISDN 回線経由で発信する |
| <i>server</i> =SIP サーバー番号 | SIP サーバー経由で発信する       |
| <i>ngn interface</i>      | ひかり電話で発信する            |

- [初期値]: -
- *interface*
  - [設定値]: ひかり電話回線を接続する LAN インターフェース名、ONU インターフェース名
  - [初期値]: -

**[説明]**

ダイヤル番号によって発呼経路を自動選択して発呼する場合のダイヤル番号と発呼経路との関連付けを設定する。ダイヤル番号は、*in\_dial* に正規表現に準ずる書式で記述することで、複数のダイヤル番号を対象とする経路指定が 1 つの設定で可能である。

第 1 経路として VoIP (SIP サーバー経由あるいはひかり電話)での発信を指定する場合は、第 2 経路としてカスケード接続されたアナログ回線、ISDN 回線、または VoIP 経由の発信を指定することが可能である。その場合、最初に VoIP で発信した後に、サーバーが応答しない、または、サーバーがエラーを返すという場合には、第 2 経路へ自動的に迂回して発信を行う。

SIP サーバー経由で発信する場合は、**sip server** コマンドで設定している SIP サーバーの登録番号を指定する方法と、**analog extension dial prefix** コマンドで設定している SIP サーバー記号を指定する方法のどちらを使用することも可能である。なお、SIP サーバー記号を指定できるのは第 1 経路のみである。

SIP サーバー記号を指定する場合、例えば、発信ポートによって別々の SIP サーバーを経由する使い方の場合でも、発呼経路情報としては共通の設定を使うことができる。

出力ダイヤル番号の指定がある場合には、入力ダイヤル番号の一部に番号を追加する、一部から番号を削除する、一部の番号を置き換える、等の操作を行った後に発信を行う。

*ngn interface* を設定した場合は、設定した LAN インターフェース、または ONU インターフェースからひかり電話により発信を行う。

**[ノート]**

発呼経路情報は、全部で最大 100 件まで登録できる。

第 1 経路としてひかり電話あるいは SIP サーバー経由での発信を指定しない場合には、第 2 経路を設定することはできない。

SIP サーバー記号で指定する場合、プレフィックスの設定で該当する SIP サーバー記号の指定が存在しなければ、発信できない。

経路に *line* を指定し、アナログ回線を使用した場合、ダイヤル時のポーズは無視された上で、設定内容との比較が行われる。また、発呼経路としてアナログ回線が選択された場合の回線への発信動作においても、ダイヤル時のポーズは無視される。

入力ダイヤル番号、および、出力ダイヤル番号は、以下に示す正規表現に準じた書式で指定し、最大長はそれぞれ 19 文字である。

- \*: 任意桁の数字列を示す (この右側にはダイヤル番号を記述できない)
- x: 1..9 のどれか 1 桁の数字を示す
- [1-5]: 範囲指定を示す (この例では 1 から 5 までの 1 桁の数字)
- [789]: 表示しているいずれかの数値を示す (この例では 7,8,9 のどれか 1 桁の数字を示す)

例えば、

0x0 ... 「010」「020」.. 「090」の 9 個のいずれか

[01][0-2] ... 「00」「01」「02」「10」「11」「12」の6個のいずれかとなる。

出力ダイヤル番号は、入力ダイヤル番号の記述と呼応した形で設定しなければならない。

例えば、

入力ダイヤル番号 = A\*、出力ダイヤル番号 = \*、と指定した場合には、番号 A を入力ダイヤルの先頭から削除することを示す。

入力ダイヤル番号 = \*、出力ダイヤル番号 = A\*、と指定した場合には、番号 A を入力ダイヤルの先頭に付与することを示す。

入力ダイヤル番号 = A\*、出力ダイヤル番号 = B\*、と指定した場合には、番号 A を番号 B に置換することを示す。

184, 186 で始まるダイヤル番号の関連付けは、18[46]/184/186 で始まる入力ダイヤル番号については 184, 186 を含んだダイヤルで判断され、それ以外の入力ダイヤル番号については、ダイヤル番号から先頭の 184, 186 を除いたダイヤルで判断される。そのため、明示的に 184, 186 ダイヤル時の経路を区別したい場合を除き、184, 186 に限定した経路登録は不要である。

#### [設定例]

例えば、以下の route-table においては、0.../1840.../1860... で始まるダイヤルが 1 の経路に従い出力ダイヤル番号は入力ダイヤル番号の先頭あるいは 184, 186 直後の 0 を 00 に置き換えたもの、それ以外の 184/186 で始まるダイヤルが 2 の経路に従い 184/186 が取り除かれ、1, 2 の経路に該当しないダイヤルが 3 の経路に従い出力ダイヤル番号は入力ダイヤル番号のままとなる。

```
analog call route-table 1 1 2 3
analog call route 1 0* 00* server=1
analog call route 2 18[46]* * line
analog call route 3 * * line
```

#### [適用モデル]

NVR700W, NVR510

## 31.5 ひかり電話の設定

### 31.5.1 NGN 網に接続するインターフェースの設定

#### [書式]

**ngn type** *interface type*

**no ngn type** *interface [type]*

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース、ONU インターフェース名
  - [初期値]: -
- *type*
  - [設定値]:

| 設定値 | 説明                                 |
|-----|------------------------------------|
| off | NGN 網のサービスを使用しない                   |
| ntt | NTT 東日本または NTT 西日本が提供する NGN 網を使用する |

- [初期値]: off

#### [説明]

NGN 網に接続するインターフェースを設定する。

#### [適用モデル]

NVR700W, NVR510

### 31.5.2 NGN 網を介したリナンバリング発生時に LAN インターフェースを一時的にリンクダウンするか否かの設定

#### [書式]

```
ngn renumbering link-refresh switch
no ngn renumbering link-refresh [switch]
```

#### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明                                                     |
|-----|--------------------------------------------------------|
| on  | リナンバリング発生時、LAN インターフェースを一時的にリンクダウンする                   |
| off | リナンバリング発生時、取得したプレフィックスに変更がない場合は、LAN インターフェースをリンクダウンしない |

- [初期値]: on

#### [説明]

NGN 網を介したリナンバリングが発生した時、LAN インターフェースを一時的にリンクダウンするか否かを設定する。

LAN インターフェースを一時的にリンクダウンさせることにより、DHCPv6-PD/RA プロキシの配下のより多くの端末に対して、IPv4/IPv6 アドレスの再取得を促し、リナンバリング後も通信を継続できるようにする。

このコマンドを on に設定した場合は、NGN 網を介したリナンバリングの発生時、取得したプレフィックスに変更がないときでも LAN インターフェースを一時的にリンクダウンする。off に設定した場合は、取得したプレフィックスに変更がないときはリンクダウンしない。

#### [適用モデル]

NVR700W, NVR510

### 31.5.3 NGN 網接続情報の表示

#### [書式]

```
show status ngn
```

#### [説明]

NGN 網への接続状態を表示する。

#### [適用モデル]

NVR700W, NVR510

## 31.6 データコネク ト接続機能の設定

### 31.6.1 NGN 網を介したトンネルインターフェースの切断タイマの設定

#### [書式]

```
tunnel ngn disconnect time time
no tunnel ngn disconnect time [time]
```

#### [設定値及び初期値]

- *time*
- [設定値]:

| 設定値         | 説明        |
|-------------|-----------|
| 1..21474836 | 秒数        |
| off         | タイマを設定しない |

- [初期値]: 60

#### [説明]

NGN 網を介したトンネルインターフェースのデータ送受信がない場合の切断までの時間を設定する。off に設定した場合は切断しない。

#### [ノート]

通信中の変更は無効。

#### [適用モデル]

NVR700W, NVR510

### 31.6.2 NGN 網を介したトンネルインターフェースの帯域の設定

#### [書式]

**tunnel ngn bandwidth** *bandwidth* [arrivepermit=*sw*]

**no tunnel ngn bandwidth** [*bandwidth* arrivepermit=*sw*]

#### [設定値及び初期値]

- *bandwidth*
  - [設定値]: 帯域 (1k..1000m)
  - [初期値]: 1m
- *sw*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | 帯域の設定と一致しない着信も許可する |
| off | 帯域の設定と一致した着信のみ許可する |

- [初期値]: on

#### [説明]

NGN 網を介したトンネルインターフェースの帯域を設定した値にする。

帯域の設定が一致しない着信について、arrivepermit オプションが off の場合は着信せず、on の場合は着信する。

#### [ノート]

通信中の変更は無効である。

#### [適用モデル]

NVR700W, NVR510

### 31.6.3 NGN 網を介したトンネルインターフェースの着信許可の設定

#### [書式]

**tunnel ngn arrive permit** *permit*

**no tunnel ngn arrive permit** [*permit*]

#### [設定値及び初期値]

- *permit*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

[説明]

選択されている相手からの着信を許可するか否かを設定する。

[ノート]

**tunnel ngn arrive permit**、**tunnel ngn call permit** コマンドとも off を設定した場合は通信できない。

[適用モデル]

NVR700W, NVR510

### 31.6.4 NGN 網を介したトンネルインターフェースの発信許可の設定

[書式]

**tunnel ngn call permit** *permit*  
**no tunnel ngn call permit** [*permit*]

[設定値及び初期値]

- *permit*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

[説明]

選択されている相手への発信を許可するか否かを設定する。

[ノート]

**tunnel ngn arrive permit**、**tunnel ngn call permit** コマンドとも off を設定した場合は通信できない。

[適用モデル]

NVR700W, NVR510

### 31.6.5 NGN 網を介したトンネルインターフェースで使用する LAN インターフェースの設定

[書式]

**tunnel ngn interface** *lan*  
**no tunnel ngn interface** [*lan*]

[設定値及び初期値]

- *lan*
- [設定値]:

| 設定値           | 説明      |
|---------------|---------|
| auto          | 自動設定    |
| LAN インターフェース名 | LAN ポート |
| ONU インターフェース名 | ONU ポート |

- [初期値]: auto

[説明]

NGN 網を介したトンネルインターフェースで使用する LAN インターフェースまたは ONU インターフェースを設定する。

auto に設定した時はトンネルインターフェースで設定した電話番号を利用して、使用する LAN インターフェースまたは ONU インターフェースを決定する。

追加番号を使用する場合や HGW 配下で使用する場合に設定する。

[適用モデル]

NVR700W, NVR510

### 31.6.6 NGN 網を介したトンネルインターフェースで接続に失敗した場合に接続を試みる相手番号の設定

#### [書式]

```
tunnel ngn fallback remote_tel ...
no tunnel ngn fallback [remote_tel ...]
```

#### [設定値及び初期値]

- *remote\_tel*
  - [設定値]: 相手電話番号
  - [初期値]: -

#### [説明]

NGN 網を介したトンネルインターフェースで使用する相手番号は、**ipsec ike remote name** コマンドや **tunnel endpoint name** コマンドで設定した番号に対して発信するが、これが何らかの原因で接続できなかった場合に、設定された番号に対して発信する。

設定は最大 7 個まで可能で、接続に失敗すると設定された順番に次の番号を用いて接続を試みる。

#### [適用モデル]

NVR700W, NVR510

### 31.6.7 NGN 電話番号を RADIUS で認証するか否かの設定

#### [書式]

```
tunnel ngn radius auth use
no tunnel ngn radius auth
```

#### [設定値及び初期値]

- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 認証する  |
| off | 認証しない |

- [初期値]: off

#### [説明]

データコネクタを利用した拠点間接続において、着信を受けたときに発信元の NGN 電話番号を RADIUS で認証するか否かを設定する。

#### [ノート]

トンネルインターフェースが選択されている時のみ使用できる。

トンネルに相手の電話番号が設定されている場合は RADIUS 認証を行わない。

以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**
- **ngn radius auth password**

NVR510 は Rev.15.01.03 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

### 31.6.8 NGN 電話番号を RADIUS で認証するとき使用するパスワードの設定

#### [書式]

```
ngn radius auth password password
```



**no ngn radius auth password****[設定値及び初期値]**

- *password*
  - [設定値]: パスワード
  - [初期値]: -

**[説明]**

NGN 電話番号を RADIUS で認証するとき使用するパスワードを設定する。NGN 電話番号をユーザー名、当コマンドで設定した文字列をパスワードとして RADIUS サーバーに問い合わせを行う。

PASSWORD に使用できる文字は半角英数字および記号 (7bit ASCII Code で表示可能なもの) で、文字列の長さは 0 文字以上 64 文字以下となる。

**[ノート]**

当コマンドが設定されていない場合は、NGN 電話番号を RADIUS で認証することができない。

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**31.6.9 NGN 網への発信時に RADIUS アカウンティングを使用するか否かの設定****[書式]**

**ngn radius account caller use**

**no ngn radius account caller**

**[設定値及び初期値]**

- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

NGN 網への発信時に RADIUS アカウンティングを使用するか否かを設定する。

**[ノート]**

RADIUS アカウンティングサーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**31.6.10 NGN 網からの着信時に RADIUS アカウンティングを使用するか否かの設定****[書式]**

**ngn radius account callee use**

**no ngn radius account callee**

**[設定値及び初期値]**

- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

NGN 網からの着信時に RADIUS アカウンティングを使用するか否かを設定する。

**[ノート]**

RADIUS アカウンティングサーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 第 32 章

### トリガによるメール通知機能

この機能は、あらかじめ設定したトリガを検出してその内容をメールで通知する機能です。

**mail notify** コマンドで設定したトリガを検出すると、**mail template** コマンドで設定したメールテンプレートを基にメールを作成し、**mail server smtp** コマンドで指定したメールサーバーを使用して検出したトリガの内容を記述したメールを送信します。

SMTP 認証として、CRAM-MD5/DIGEST-MD5/PLAIN に対応しており、POP-before-SMTP にも対応しています。

#### 32.1 メール設定識別名の設定

##### [書式]

**mail server name** *id name*

**no mail server name** *id [name]*

##### [設定値及び初期値]

- *id*
  - [設定値]: メールサーバー設定 ID (1..10)
  - [初期値]: -
- *name*
  - [設定値]: 識別名
  - [初期値]: -

##### [説明]

メール設定の識別名を設定する。空白を伴う識別名の場合は、「"」で囲む必要がある。

##### [適用モデル]

NVR700W, NVR510

#### 32.2 SMTP メールサーバーの設定

##### [書式]

**mail server smtp** *id address [port=port] [smtp-auth username password [auth\_protocol]] [pop-before-smtp] [smtps]*

**no mail server smtp** *id [...]*

##### [設定値及び初期値]

- *id*
  - [設定値]: メールサーバー設定 ID (1..10)
  - [初期値]: -
- *address*
  - [設定値]: サーバーの IP アドレスまたはホスト名 (半角 1 文字以上 64 文字以内)
  - [初期値]: -
- *port*
  - [設定値]: サーバーのポート番号 (省略時は 25、または、465)
  - [初期値]: -
- *username*
  - [設定値]: 認証用ユーザー名
  - [初期値]: -
- *password*
  - [設定値]: 認証用パスワード
  - [初期値]: -
- *auth\_protocol*: SMTP-AUTH 認証プロトコル
  - [設定値]:

| 設定値        | 説明         |
|------------|------------|
| cram-md5   | CRAM-MD5   |
| digest-md5 | DIGEST-MD5 |
| plain      | PLAIN 認証   |

- [初期値]: -
- pop-before-smtp
  - [設定値]: POP before SMTP の使用
  - [初期値]: -
- smtps
  - [設定値]: SMTPS の使用
  - [初期値]: -

#### [説明]

メール送信に使用するサーバー情報を設定する。

*smtp-auth* パラメーターでは、メール送信の際の SMTP 認証のためのデータ (ユーザー名、パスワード) を指定する。SMTP サーバーで認証が必要ない場合は *smtp-auth* の設定は必要ない。

SMTP 認証でサポートしている認証プロトコルは、CRAM-MD5、DIGEST-MD5 および PLAIN 認証の 3 種類である。*smtp-auth* パラメーターでプロトコルを指定した場合にはそれを用い、プロトコルが省略された場合には SMTP サーバーとの前記の順で認証交渉を行う。

*pop-before-smtp* パラメーターを設定すると、メール送信時に POP before SMTP 動作を行う。ここで行う POP 動作は、**mail server pop** コマンドで同じ ID で設定したものを利用する。*pop-before-smtp* パラメーターが設定されているのに、対応する **mail server pop** コマンドの設定がないと、メールは送信できない。

*smtps* パラメーターが設定されている場合、SMTPS を使用してメールを送信する。*smtps* パラメーターと *pop-before-smtp* パラメーターは同時に設定できない。

*port* パラメーターを省略した場合、*smtps* パラメーターの設定によって、メールサーバーのポート番号として使用する値が変わる。*smtps* パラメーターの設定と、メールサーバーのポート番号の対応は以下のとおり。

| <i>smtps</i> パラメーター | 使用するポート番号 |
|---------------------|-----------|
| 設定しない (省略)          | 25        |
| 設定する                | 465       |

#### [ノート]

*smtps* パラメーターは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアで指定可能。

#### [適用モデル]

NVR700W, NVR510

## 32.3 POP メールサーバーの設定

#### [書式]

```
mail server pop id address [port=port] protocol username password
no mail server pop id [...]
```

#### [設定値及び初期値]

- *id*
  - [設定値]: メールサーバー設定 ID (1..10)
  - [初期値]: -
- *address*
  - [設定値]: サーバーの IP アドレスまたはホスト名
  - [初期値]: -
- *port*
  - [設定値]: サーバーのポート番号 (省略時は 110)
  - [初期値]: -
- *protocol*
  - [設定値]:

| 設定値  | 説明   |
|------|------|
| pop3 | POP3 |
| apop | APOP |

- [初期値]: -
- *username*
  - [設定値]: 認証用ユーザー名
  - [初期値]: -
- *password*
  - [設定値]: 認証用パスワード
  - [初期値]: -

#### [説明]

メール受信に使用するサーバー情報を設定する。

**mail server smtp** コマンドで *pop-before-smtp* パラメーターを設定したときに必要な設定である。

#### [適用モデル]

NVR700W, NVR510

## 32.4 メール処理のタイムアウト値の設定

#### [書式]

**mail server timeout id timeout**

**no mail server timeout id [timeout]**

#### [設定値及び初期値]

- *id*
  - [設定値]: メールサーバー設定 ID (1..10)
  - [初期値]: -
- *timeout*
  - [設定値]: タイムアウト値 (1..600 秒)
  - [初期値]: 60

#### [説明]

メールの送受信処理に対するタイムアウト値を設定する。

指定した時間以内にメールの処理が終らない時には、いったん処理を中断して、**mail template** コマンドで設定した待機時間 (デフォルトは 30 秒) の間を置いた後、メール処理を最初からやり直す。処理のやり直しは、最初のメール処理を除き、最大 3 回行われる。最大回数を超えた場合には、メール処理は失敗となる。

#### [適用モデル]

NVR700W, NVR510

## 32.5 メールを送信時に使用するテンプレートの設定

#### [書式]

**mail template template\_id mailserver\_id From:from\_address To:to\_address [Subject:subject] [Date:date] [MIME-Version:mime\_version] [Content-Type:content\_type] [notify-log=switch] [notify-wait-time=sec]**

**no mail template template\_id [...]**

#### [設定値及び初期値]

- *template\_id*
  - [設定値]: メールテンプレート ID (1..10)
  - [初期値]: -
- *mailserver\_id*
  - [設定値]: このテンプレートで使用するメールサーバー ID (1..10)
  - [初期値]: -
- *from\_address*

- [設定値]: 送信元メールアドレス
- [初期値]: -
- *to\_address*
  - [設定値]: 宛先メールアドレス
  - [初期値]: -
- *subject*
  - [設定値]: 送信時の件名
  - [初期値]: Backup Info/Route Change Info/Filter Info/Status Info/Intrusion Info
- *date*
  - [設定値]: メールのヘッダに表示する時刻
  - [初期値]: 送信時の時刻
- *mime\_version*
  - [設定値]: メールのヘッダに表示する MIME-Version
  - [初期値]: 1.0
- *content\_type*
  - [設定値]: メールのヘッダに表示する Content-Type
  - [初期値]: text/plain;charset=iso-2022-jp
- *switch*
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| on  | 通知系のメール内容に syslog の内容を含める  |
| off | 通知系のメール内容に syslog の内容を含めない |

- [初期値]: off
- *sec*
  - [設定値]: 通知系のメール送信時に、実際に送信されるまでの待機時間 (1.86400 秒)
  - [初期値]: 30

### [説明]

メール送信時に使用するメールサーバー設定 ID、送信元メールアドレス、宛先メールアドレスおよびヘッダ等を設定する。

*from\_address* に送信元メールアドレスを指定する。送信元メールアドレスは一つしか指定できない。  
*to\_address* に宛先メールアドレスを指定する。宛先メールアドレスは複数指定できる。複数指定する場合はカンマ (,) で区切り、間に空白を入れてはいけない。  
 メールアドレスは local-part@domain もしくは local-part@ipaddress の形式のみ対応している。"NAME<local-part@domain>" 等の形式には対応していない。

*subject* でメールの件名を指定する。空白を含む場合は、ダブルクォーテーション (") で Subject:subject 全体を囲む必要がある。

*date* には、RFC822 に示されるフォーマットの時刻を指定する。RFC822 のフォーマットでは必ず空白が含まれるため、ダブルクォーテーション (") で Date:date 全体を囲む必要がある。

*content-type* に指定できる type/subtype は "text/plain" のみで、パラメーターは "charset=us-ascii" および "charset=iso-2022-jp" のみ対応している。

### [ノート]

メールヘッダ情報として必須のものは、"送信元メールアドレス" と "宛先メールアドレス" になる。

### [表示例]

```
mail template 1 1 From:test@test.com To:test1@test.com,test2@test.com
  "Subject:Test Mail" notify-log=on
mail template 1 2 From:test@test.com To:test1@test.com
  "Subject:NVR700W, NVR510 test" "Date:Sun, 10 Jul 2016 10:10:10 +0900"
  MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

### [適用モデル]

NVR700W, NVR510

## 32.6 メール通知のトリガの設定

### [書式]

```
mail notify id template_id trigger backup if_b [[range_b] if_b ...]
mail notify id template_id trigger route route [route ...]
mail notify id template_id trigger route6 route6 [route6 ...]
mail notify id template_id trigger filter ethernet if_f dir_f [if_f dir_f ...]
mail notify id template_id trigger status type [type ...]
mail notify id template_id trigger intrusion if_i [range_i] dir_i [if_i [range_i] dir_i ...]
mail notify id template_id trigger lan-map
no mail notify id [...]
```

### [設定値及び初期値]

- *id*
  - [設定値]: 設定番号 (1..10)
  - [初期値]: -
- *template\_id*
  - [設定値]: テンプレート ID (1..10)
  - [初期値]: -
- *if\_b*: メール通知を行うバックアップ対象のインターフェース
  - [設定値]:

| 設定値    | 説明            |
|--------|---------------|
| pp     | PP バックアップ     |
| lanN   | LAN バックアップ    |
| tunnel | TUNNEL バックアップ |

- [初期値]: -
- *range\_b*
  - [設定値]:
    - インターフェース番号および範囲指定
    - pp,tunnel のみ (\*,xx-yy,zz etc)
  - [初期値]: -
- *route*
  - [設定値]:
    - ネットマスク付きの経路
    - default
  - [初期値]: -
- *route6*
  - [設定値]:
    - プレフィックス長付きの経路
    - default
  - [初期値]: -
- *if\_f*
  - [設定値]: メール通知を行うイーサネットフィルタの設定された LAN インターフェース
  - [初期値]: -
- *dir\_f*: フィルタ設定の方向
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| in  | 受信方向 |
| out | 送信方向 |

- [初期値]: -
- *type*: メール通知で通知する情報

- [設定値]:

| 設定値        | 説明          |
|------------|-------------|
| all        | 全ての内容       |
| interface  | インターフェースの情報 |
| routing    | ルーティングの情報   |
| vpn        | VPN の情報     |
| nat        | NAT の情報     |
| firewall   | ファイアウォールの情報 |
| config-log | 設定情報とログ     |

- [初期値]: -

- *if\_i*: 不正アクセス検知設定のインターフェース

- [設定値]:

| 設定値           | 説明              |
|---------------|-----------------|
| pp            | PP インターフェース     |
| lanN(N,M,N/M) | LAN インターフェース    |
| wan1          | WAN インターフェース    |
| tunnel        | TUNNEL インターフェース |
| *             | 全てのインターフェース     |

- [初期値]: -

- *range\_i*

- [設定値]:

- インターフェース番号および範囲指定
- lan(\*,x)
- pp,tunnel(\*,x,xx-yy,zz etc)

- [初期値]: -

- *dir\_i*: 不正アクセス検知設定の方向

- [設定値]:

| 設定値    | 説明      |
|--------|---------|
| in     | 受信方向    |
| out    | 送信方向    |
| in/out | 受信/送信方向 |

- [初期値]: -

### [説明]

メール通知の行うトリガ動作の設定を行う。バックアップ、経路変更、イーサネットフィルターのログ表示、**mail notify status exec** コマンド実行時、および不正アクセス検知時をトリガとして指定できる。

バックアップおよび経路については以下で設定されたものが対象となる。

|                     |                           |
|---------------------|---------------------------|
| PP バックアップ           | <b>pp backup</b> コマンド     |
| LAN バックアップ          | <b>lan backup</b> コマンド    |
| TUNNEL バックアップ       | <b>tunnel backup</b> コマンド |
| 経路に対するバックアップ (IPv4) | <b>ip route</b> コマンド      |
| 経路に対するバックアップ (IPv6) | <b>ipv6 route</b> コマンド    |

イーサネットフィルターについてはログ表示されるものが対象となる。

イーサネットフィルター.....

pass-log,reject-log パラメーターの定義



内部状態を通知する場合は、**mail notify status exec** コマンドを実行する必要がある。

不正アクセス検知については **ip interface intrusion detection** コマンドの設定により検出されたものが通知対象となる。

LAN マップによる異常検知については **switch control use interface** コマンドが設定された LAN インターフェースが対象となる。スナップショット機能による異常を含める場合は **lan-map snapshot use interface** コマンドを設定する必要がある。

また、一つのテンプレート ID に所属するメール通知設定はまとめて処理される。

#### [ノート]

**trigger backup** と **trigger route** は NVR700W で使用可能。

**trigger route6** は NVR700W Rev.15.00.23 以降のファームウェアで使用可能。

#### [設定例]

```
mail notify 1 1 trigger backup pp * lan2 tunnel 1-4,6
mail notify 2 1 trigger route 192.168.1.0/24 172.16.0.0/16
mail notify 3 1 trigger route6 1000::1/64
mail notify 4 1 trigger filter ethernet lan1 in
mail notify 5 1 trigger status all
mail notify 6 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
mail notify 7 1 trigger lan-map
```

#### [適用モデル]

NVR700W, NVR510

## 第 33 章

### HTTP サーバー機能

#### 33.1 共通の設定

##### 33.1.1 HTTP サーバー機能の有無の設定

[書式]

```
httpd service switch
no httpd service
```

[設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | HTTP サーバー機能を有効にする |
| off | HTTP サーバー機能を無効にする |

- [初期値]: on

[説明]

HTTP サーバーを有効にするか否かを選択する。

[適用モデル]

NVR700W, NVR510

##### 33.1.2 HTTP サーバーへアクセスできるホストの設定

[書式]

```
httpd host ip_range [ip_range...]
httpd host any
httpd host none
httpd host lan
no httpd host
```

[設定値及び初期値]

- *ip\_range*: HTTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

| 設定値                                                            | 説明                           |
|----------------------------------------------------------------|------------------------------|
| 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの | 指定したホストからのアクセスを許可する          |
| lanN                                                           | LAN インターフェースからのアクセスを許可する     |
| onu1                                                           | ONU インターフェースからのアクセスを許可する     |
| wan1                                                           | WAN インターフェースからのアクセスを許可する     |
| bridge1                                                        | ブリッジインターフェースからのアクセスを許可する     |
| vlanN                                                          | VLAN インターフェースからのアクセスを許可する    |
| lanN/M                                                         | タグ VLAN インターフェースからのアクセスを許可する |

- [初期値]: -
- *any*

- [設定値]: すべてのホストからのアクセスを許可する
- [初期値]: -
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: -
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: *lan*

**[説明]**

HTTP サーバーへのアクセスを許可するホストを設定する。

**[ノート]**

このコマンドで LAN インターフェースまたは ONU インターフェースを指定した場合には、ネットワークアドレスとリミテッドブロードキャストアドレスを除く IP アドレスからのアクセスを許可する。指定した LAN インターフェースまたは ONU インターフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

**[適用モデル]**

NVR700W, NVR510

### 33.1.3 HTTP サーバーのセッションタイムアウト時間の設定

---

**[書式]**

**httpd timeout *time***

**no httpd timeout [*time*]**

**[設定値及び初期値]**

- *time*
  - [設定値]: 秒数 (1..180)
  - [初期値]: 5

**[説明]**

HTTP サーバーのタイムアウト時間を設定する。

**[ノート]**

インターネット経由でルーターにアクセスするときに、通信タイムアウトが発生するならば、このコマンドで大きな値を設定する。

**[適用モデル]**

NVR700W, NVR510

### 33.1.4 HTTP サーバー機能の listen ポートの設定

---

**[書式]**

**httpd listen *port***

**no httpd listen**

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 80

**[説明]**

HTTP サーバーの待ち受けるポートを設定する。

**[適用モデル]**

NVR700W, NVR510

### 33.1.5 PP インターフェイスとトンネルインターフェイスの名前の設定

---

#### [書式]

**pp name** *name*  
**tunnel name** *name*  
**no pp name**  
**no tunnel name**

#### [設定値及び初期値]

- *name*
  - [設定値]: 名前 (64 文字以内)
  - [初期値]: -

#### [説明]

PP インターフェイス、またはトンネルインターフェイスの説明を設定しておく。設定内容はあくまで説明のためだけであり、動作には影響を与えない。

#### [適用モデル]

NVR700W, NVR510

## 第 34 章

### ネットボランチ DNS サービスの設定

ネットボランチ DNS とは、一種のダイナミック DNS 機能であり、ルーターの IP アドレスをヤマハが運営するネットボランチ DNS サーバーに希望の名前で登録することができます。そのため、動的 IP アドレス環境でのサーバー公開や拠点管理などに用いることができます。IP アドレスの登録、更新などの手順には独自のプロトコルを用いるため、他のダイナミック DNS サービスとの互換性はありません。

ヤマハが運営するネットボランチ DNS サーバーは現時点では無料、無保証の条件で運営されています。利用料金は必要ありませんが、ネットボランチ DNS サーバーに対して名前が登録できること、および登録した名前が引けることは保証できません。また、ネットボランチ DNS サーバーは予告無く停止することがあることに注意してください。

ネットボランチ DNS には、ホストアドレスサービスと電話番号サービスの 2 種類があります。

ネットボランチ DNS では、個々の RT シリーズ、ネットボランチシリーズルーターを MAC アドレスで識別しているため、機器の入れ換えなどをした場合には同じ名前がそのまま利用できる保証はありません。

#### 34.1 ネットボランチ DNS サービスの使用の可否

##### [書式]

```
netvolante-dns use interface switch
netvolante-dns use pp switch
no netvolante-dns use interface [switch]
no netvolante-dns use pp [switch]
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値  | 説明      |
|------|---------|
| auto | 自動更新する  |
| off  | 自動更新しない |

- [初期値]: auto

##### [説明]

ネットボランチ DNS サービスを使用するか否かを設定する。  
IP アドレスが更新された時にネットボランチ DNS サーバーに自動で IP アドレスを更新する。

##### [適用モデル]

NVR700W, NVR510

#### 34.2 ネットボランチ DNS サーバーへの手動更新

##### [書式]

```
netvolante-dns go interface
netvolante-dns go pp peer_num
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号

- [初期値]:-

**[説明]**

ネットボランチ DNS サーバーに手動で IP アドレスを更新する。

**[適用モデル]**

NVR700W, NVR510

### 34.3 ネットボランチ DNS サーバーからの削除

---

**[書式]**

```
netvolante-dns delete go interface [host]
netvolante-dns delete go pp peer_num [host]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]:-
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]:-
- *host*
  - [設定値]: ホスト名
  - [初期値]:-

**[説明]**

登録した IP アドレスをネットボランチ DNS サーバーから削除する。  
インターフェースの後にホスト名を指定することで、指定したホスト名のみを削除可能。

**[適用モデル]**

NVR700W, NVR510

### 34.4 ネットボランチ DNS サービスで使用するポート番号の設定

---

**[書式]**

```
netvolante-dns port port
no netvolante-dns port [port]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 2002

**[説明]**

ネットボランチ DNS サービスで使用するポート番号を設定する。

**[適用モデル]**

NVR700W, NVR510

### 34.5 ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得

---

**[書式]**

```
netvolante-dns get hostname list interface
netvolante-dns get hostname list pp peer_num
netvolante-dns get hostname list all
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、WAN インターフェース名
  - [初期値]:-

- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *all*: すべてのインターフェース
  - [初期値]: -

#### [説明]

ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得し、表示する。

#### [適用モデル]

NVR700W, NVR510

## 34.6 ホスト名の登録

#### [書式]

```
netvolante-dns hostname host interface [server=server_num] host [duplicate]
netvolante-dns hostname host interface [server=server_num] host ipv6 address [ipv6_address] [duplicate]
netvolante-dns hostname host interface [server=server_num] host ipv6 prefix [ipv6_prefix] [duplicate]
netvolante-dns hostname host pp [server=server_num] host [duplicate]
netvolante-dns hostname host pp [server=server_num] host ipv6 address [ipv6_address] [duplicate]
netvolante-dns hostname host pp [server=server_num] host ipv6 prefix [ipv6_prefix] [duplicate]
no netvolante-dns hostname host interface [server=server_num] [host [duplicate]]
no netvolante-dns hostname host pp [server=server_num] [host [duplicate]]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *server\_num*
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバ番号               |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -
- *host*
  - [設定値]: ホスト名 (63 文字以内)
  - [初期値]: -
- *ipv6\_address*
  - [設定値]: IPv6 アドレス
  - [初期値]: -
- *ipv6\_prefix*
  - [設定値]: IPv6 プレフィックス
  - [初期値]: -

#### [説明]

ネットボランチ DNS サービス (ホストアドレスサービス) で使用するホスト名を設定する。ネットボランチ DNS サーバーから取得されるホスト名は、『(ホスト名).(サブドメイン).netvolante.jp』という形になる。(ホスト名)はこのコマンドで設定した名前となり、(サブドメイン)はネットボランチ DNS サーバーから割り当てられる。(サブドメイン)をユーザーが指定することはできない。

このコマンドを一番最初に設定する際は、(ホスト名)部分のみを設定する。ネットボランチ DNS サーバーに対する登録・更新が成功すると、コマンドが上記の完全な FQDN の形になって保存される。

*duplicate* を付加すると、1 台のルーターで異なるインターフェースに同じ名前を登録できる。

#### [ノート]

*ipv6 address* および *ipv6 prefix* は NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で指定可能。

[適用モデル]  
NVR700W, NVR510

## 34.7 電話アドレスの設定

---

[書式]

```
netvolante-dns hostname sip name
no netvolante-dns hostname sip
```

[設定値及び初期値]

- *name*
  - [設定値]: 電話アドレス
  - [初期値]: -

[説明]

電話アドレスを設定する。

[ノート]

GUI 設定専用の識別コマンドである。

[適用モデル]  
NVR700W, NVR510

## 34.8 通信タイムアウトの設定

---

[書式]

```
netvolante-dns timeout interface time
netvolante-dns timeout pp time
no netvolante-dns timeout interface [time]
no netvolante-dns timeout pp [time]
```

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *time*
  - [設定値]: タイムアウト秒数 (1..180)
  - [初期値]: 90

[説明]

ネットボランチ DNS サーバーとの間の通信がタイムアウトするまでの時間を秒単位で設定する。

[適用モデル]  
NVR700W, NVR510

## 34.9 ホスト名を自動生成するか否かの設定

---

[書式]

```
netvolante-dns auto hostname interface [server=server_num] switch
netvolante-dns auto hostname interface [server=server_num] ipv6 address [ipv6_address]
netvolante-dns auto hostname interface [server=server_num] ipv6 prefix [ipv6_prefix]
netvolante-dns auto hostname pp [server=server_num] switch
netvolante-dns auto hostname pp [server=server_num] ipv6 address [ipv6_address]
netvolante-dns auto hostname pp [server=server_num] ipv6 prefix [ipv6_prefix]
no netvolante-dns auto hostname interface [switch]
no netvolante-dns auto hostname pp [switch]
```

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -



- *server\_num*

- [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバ番号               |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -

- *switch*

- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 自動生成する  |
| off | 自動生成しない |

- [初期値]: off

- *ipv6\_address*

- [設定値]: IPv6 アドレス

- [初期値]: -

- *ipv6\_prefix*

- [設定値]: IPv6 プレフィックス

- [初期値]: -

#### [説明]

ホスト名の自動生成機能を利用するか否かを設定する。自動生成されるホスト名は、MAC アドレス上 6 桁が "00:a0:de" のときは、『y'+(MAC アドレス下 6 桁).auto.netvolante.jp』という形になる。MAC アドレス上 6 桁が "00:a0:de" 以外のときは、『y'+(MAC アドレス全 12 桁).auto.netvolante.jp』という形になる。このコマンドを 'on' に設定して、**netvolante-dns go** コマンドを実行すると、ネットボランチ DNS サーバーから上記のホスト名が割り当てられる。割り当てられたドメイン名は、**show status netvolante-dns** コマンドで確認することができる。

#### [ノート]

MAC アドレス上 6 桁が "00:a0:de" 以外のときは Rev.15.00.03 以降の NVR700W、Rev.15.01.03 以降の NVR510 でホスト名の自動生成機能を利用可能。

ipv6 address および ipv6 prefix は NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 34.10 NetVolante インターネット電話用ホスト名の使用の可否

#### [書式]

```
netvolante-dns sip use interface [server=server_num] switch [duplicate]
netvolante-dns sip use interface [server=server_num] switch ipv6 address [ipv6_address] [duplicate]
netvolante-dns sip use interface [server=server_num] switch ipv6 prefix [ipv6_prefix] [duplicate]
netvolante-dns sip use pp [server=server_num] switch [duplicate]
netvolante-dns sip use pp [server=server_num] switch ipv6 address [ipv6_address] [duplicate]
netvolante-dns sip use pp [server=server_num] switch ipv6 prefix [ipv6_prefix] [duplicate]
no netvolante-dns sip use interface [server=server_num] [switch [duplicate]]
no netvolante-dns sip use pp [server=server_num] [switch [duplicate]]
```

#### [設定値及び初期値]

- *interface*

- [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名

- [初期値]: -

- *server\_num*

- [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバー番号              |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -
- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *ipv6\_address*
  - [設定値]: IPv6 アドレス
  - [初期値]: -
- *ipv6\_prefix*
  - [設定値]: IPv6 プレフィックス
  - [初期値]: -

#### [説明]

ネットボランチ DNS サービス（電話アドレスサービス）で使用する電話アドレスを使用するか否かを設定する。  
duplicate を付加すると、異なるインターフェースで登録済みの電話アドレスと同じアドレスを登録できるようになる。

#### [ノート]

ipv6 address および ipv6 prefix は NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 34.11 シリアル番号を使ったホスト名登録コマンドの設定

#### [書式]

```
netvolante-dns set hostname interface serial
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名あるいは "pp"
  - [初期値]: -

#### [説明]

機器のシリアル番号を使ったホスト名を利用するためのコマンドを自動設定する。  
本コマンドを実行すると、**netvolante-dns hostname host** コマンドが設定される。  
例えば機器のシリアル番号が D000ABCDE の場合、**netvolante-dns set hostname pp serial** を実行すると、**netvolante-dns hostname host pp server=1 SER-D000ABCDE** が設定される。

#### [適用モデル]

NVR700W, NVR510

## 34.12 ネットボランチ DNS サーバーの設定

#### [書式]

```
netvolante-dns server ip_address
netvolante-dns server name
no netvolante-dns server [ip_address]
```

**no netvolante-dns server** [*name*]

**[設定値及び初期値]**

- *ip\_address*
  - [設定値]: IP アドレス
  - [初期値]: -
- *name*
  - [設定値]: ドメイン名
  - [初期値]: netvolante-dns.netvolante.jp

**[説明]**

ネットボランチ DNS サーバーの IP アドレスまたはホスト名を設定する。

**[適用モデル]**

NVR700W, NVR510

### 34.13 ネットボランチ DNS サーバーアドレス更新機能の ON/OFF の設定

**[書式]**

**netvolante-dns server update address use** [server=*server\_num*] *switch*

**no netvolante-dns server update address use** [server=*server\_num*]

**[設定値及び初期値]**

- *server\_num*
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバー番号              |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -

- *switch*

- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | サーバーアドレスの更新機能を有効にする |
| off | サーバーアドレスの更新機能を停止させる |

- [初期値]: on

**[説明]**

ネットボランチ DNS サーバーからの IP アドレスの変更通知を受け取り、設定を自動更新するか否かを設定する。

**[適用モデル]**

NVR700W, NVR510

### 34.14 ネットボランチ DNS サーバーアドレス更新機能のポート番号の設定

**[書式]**

**netvolante-dns server update address port** [server=*server\_num*] *port*

**no netvolante-dns server update address port** [server=*server\_num*]

**[設定値及び初期値]**

- *server\_num*
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバー番号              |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -

- *port*
  - [設定値]: ポート番号 (1..65535)
  - [初期値]: 2002

**[説明]**

ネットボランチ DNS サーバーの IP アドレス更新通知の待ち受けポート番号を設定する。

**[適用モデル]**

NVR700W, NVR510

## 34.15 自動更新に失敗した場合のリトライ間隔と回数の設定

---

**[書式]**

```
netvolante-dns retry interval interface interval count
netvolante-dns retry interval pp interval count
no netvolante-dns retry interval interface [interval count]
no netvolante-dns retry interval pp [interval count]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *interval*
  - [設定値]:
    - auto
    - 秒数 (60-300)
  - [初期値]: auto
- *count*
  - [設定値]: 回数 (1-50)
  - [初期値]: 10

**[説明]**

ネットボランチ DNS で自動更新に失敗した場合に、再度自動更新を行う間隔と回数を設定する。

**[ノート]**

*interval* に auto を設定した時には、自動更新に失敗した場合には 30 秒から 90 秒の時間をおいて再度自動更新を行う。それにも失敗した場合には、その後、60 秒後間隔で自動更新を試みる。

自動更新に失敗してから、指定した時間までの間に手動実行をした場合は、その後の自動更新は行われない。

**[適用モデル]**

NVR700W, NVR510

## 34.16 ネットボランチ DNS 登録の定期更新間隔の設定

---

**[書式]**

```
netvolante-dns register timer [server=server_num] time
no netvolante-dns register timer [server=server_num]
```

**[設定値及び初期値]**

- *server\_num*
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバー番号              |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -
- *time*
  - [設定値]:

| 設定値                 | 説明                       |
|---------------------|--------------------------|
| 3600 ... 2147483647 | 秒数                       |
| off                 | ネットボランチ DNS 登録の定期更新を行わない |

- [初期値]: off

#### [説明]

ネットボランチ DNS 登録を定期的に更新する間隔を指定する。

#### [適用モデル]

NVR700W, NVR510

## 34.17 ネットボランチ DNS の自動登録に成功したとき設定を保存するファイルの設定

#### [書式]

```
netvolante-dns auto save [server=server_num] file
```

```
no netvolante-dns auto save [server=server_num]
```

#### [設定値及び初期値]

- *server\_num*

- [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| 1 または 2 | サーバー番号              |
| 省略      | 省略時は 1 が指定されたものとみなす |

- [初期値]: -

- *file*

- [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| off  | 設定の自動保存を行わない        |
| auto | デフォルト設定ファイルに自動保存を行う |
| 番号   | 自動保存を行うファイル名        |

- [初期値]: auto

#### [説明]

ネットボランチ DNS の自動登録に成功したとき、およびネットボランチ DNS サーバーからのアドレス通知を受け取ったとき、設定を自動保存するかどうか、および自動保存する場合は保存先のファイル名を指定する。

#### [適用モデル]

NVR700W, NVR510

## 第 35 章

### UPnP の設定

#### 35.1 UPnP を使用するか否かの設定

##### [書式]

**upnp use** *use*

**no upnp use**

##### [設定値及び初期値]

- *use*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

##### [説明]

UPnP 機能を使用するか否かを設定する。

##### [適用モデル]

NVR700W, NVR510

#### 35.2 UPnP に使用する IP アドレスを取得するインターフェースの設定

##### [書式]

**upnp external address refer** *interface*

**upnp external address refer pp** *peer\_num*

**upnp external address refer** default

**no upnp external address refer** [*interface*]

**no upnp external address refer pp** [*peer\_num*]

##### [設定値及び初期値]

- *interface*

- [設定値]:

| 設定値           | 説明                              |
|---------------|---------------------------------|
| LAN インターフェース名 | 指定した LAN インターフェースの IP アドレスを取得する |
| ONU インターフェース名 | 指定した ONU インターフェースの IP アドレスを取得する |
| WAN インターフェース名 | 指定した WAN インターフェースの IP アドレスを取得する |
| default       | デフォルトルートのインターフェース               |

- [初期値]: default

- *peer\_num*

- [設定値]:

- 相手先情報番号
- anonymous

- [初期値]: -

##### [説明]

UPnP に使用する IP アドレスを取得するインターフェースを設定する。

[適用モデル]  
NVR700W, NVR510

### 35.3 UPnP のポートマッピング用消去タイマのタイプの設定

[書式]

```
upnp port mapping timer type type
no upnp mapping timer type
```

[設定値及び初期値]

- *type*
- [設定値]:

| 設定値    | 説明           |
|--------|--------------|
| normal | ARP 情報を参照しない |
| arp    | ARP 情報を参照する  |

- [初期値]: arp

[説明]

UPnP のポートマッピングを消去するためのタイマのタイプを設定する。  
このコマンドで変更を行うと消去タイマ値は 3600 秒にセットされる。消去タイマの秒数は **upnp port mapping timer** コマンドで変更できる。

arp を指定すると **upnp port mapping timer off** の設定よりも優先する。  
arp に影響されずにポートマッピングを残す場合は normal を指定する。

[適用モデル]  
NVR700W, NVR510

### 35.4 UPnP のポートマッピングの消去タイマの設定

[書式]

```
upnp port mapping timer time
no upnp port mapping timer
```

[設定値及び初期値]

- *time*
- [設定値]:

| 設定値           | 説明    |
|---------------|-------|
| 600..21474836 | 秒数    |
| off           | 消去しない |

- [初期値]: 3600

[説明]

UPnP によって生成されたポートマッピングを消去するまでの時間を設定する。

[ノート]

**upnp port mapping timer type** コマンドで設定を行った後、このコマンドを設定する。  
off に設定した場合でも **upnp port mapping timer type arp** の設定にしてあるとポートマッピングは消去される。  
ARP がタイムアウトした状態でもポートマッピングを消去したくない場合は **upnp port mapping timertype normal** に設定するようにする。

[適用モデル]  
NVR700W, NVR510

## 35.5 UPnP の syslog を出力するか否かの設定

---

### [書式]

**upnp syslog** *syslog*

**no upnp syslog**

### [設定値及び初期値]

- *syslog*

- [設定値]:

| 設定値 | 説明                   |
|-----|----------------------|
| on  | UPnP の syslog を出力する  |
| off | UPnP の syslog を出力しない |

- [初期値]: off

### [説明]

UPnP の syslog を出力するか否かを設定する。デバッグレベルで出力される。

### [適用モデル]

NVR700W, NVR510



## 第 36 章

### スケジュール

#### 36.1 スケジュールの設定

##### [書式]

```

schedule at id [date] time * command...
schedule at id [date] time pp peer_num command...
schedule at id [date] time tunnel tunnel_num command...
schedule at id [date] time wwan wwan_num command...
schedule at id [date] time switch switch command...
schedule at id +timer * command...
schedule at id +timer pp peer_num command...
schedule at id +timer tunnel tunnel_num command...
schedule at id +timer switch switch command...
no schedule at id [[date]...]

```

##### [設定値及び初期値]

- *id*
  - [設定値]: スケジュール番号
  - [初期値]: -
- *date*: 日付 (省略可)
  - [設定値]:
    - 月/日
    - 省略時は \*/\* とみなす

| 月の設定例 | 設定内容      |
|-------|-----------|
| 1,2   | 1月と2月     |
| 2-    | 2月から12月まで |
| 2-7   | 2月から7月まで  |
| -7    | 1月から7月まで  |
| *     | 毎月        |

| 日の設定例   | 設定内容     |
|---------|----------|
| 1       | 1日のみ     |
| 1,2     | 1日と2日    |
| 2-      | 2日から月末まで |
| 2-7     | 2日から7日まで |
| -7      | 1日から7日まで |
| mon     | 月曜日のみ    |
| sat,sun | 土曜日と日曜日  |
| mon-fri | 月曜日から金曜日 |
| -fri    | 日曜日から金曜日 |
| *       | 毎日       |

- [初期値]: -
- *time*: 時刻
- [設定値]:

| 設定値           | 説明                                                |
|---------------|---------------------------------------------------|
| hh:mm[:ss]    | 時 (0..23 または *): 分 (0..59 または *): 秒 (0..59)、秒は省略可 |
| startup       | 起動時                                               |
| usb-attached  | USB デバイス認識時                                       |
| usb1-attached | USB デバイス認識時                                       |
| sd-attached   | microSD デバイス認識時                                   |
| sd1-attached  | microSD デバイス認識時                                   |

- [初期値]: -
- *timer*: *command* を実行するまでの時間 (秒、1..3600)
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェースの番号
  - [初期値]: -
- *wwan\_num*
  - [設定値]: 内蔵無線 WAN インターフェースの番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -
- *command*
  - [設定値]: 実行するコマンド (制限あり)
  - [初期値]: -

## [説明]

*time* で指定した時刻、または *timer* で指定した時間後に、*command* で指定されたコマンドを実行する。

第 2、第 3、第 4、第 5 書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号/トンネル番号/内蔵無線 WAN 番号/スイッチでの、**pp select/tunnel select/wwan select/switch select** コマンドが発行済みであるように動作する。

**schedule at** コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。

*time* は hh:mm 形式で指定されたときは秒指定なしとみなされ、hh:mm:ss 形式で指定されたときは秒指定ありとみなされる。秒数に "-" を用いた範囲指定や "\*" による全指定をすることはできない。

以下のコマンドは指定できない。

**administrator**、**administrator password**、**administrator password encrypted**、**ap select** (※)、**auth user**、**auth user group**、**bgp configure refresh**、**change wwan pin-code**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**copy exec**、**date**、**delete**、**disable wwan pin-auth**、**enable wwan pin-auth**、**exit**、**external-memory performance-test go**、**help**、**http revision-up go**、**http revision-up schedule**、**interface reset**、**ipsec transport template**、**ipv6 bgp configure refresh**、**ipv6 ospf configure refresh**、**less** で始まるコマンド、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**make directory**、**nslookup**、**ospf configure refresh**、**packetdump**、**ping**、**ping6**、**pp select** (※)、**quit**、**rename**、**rtfs format**、**rtfs garbage collect**、**save**、**schedule at**、**scp**、**show** で始まるコマンド、**ssh**、**sshd host key generate**、**sshd session**、**switch control function get FUNCTION**、**switch select** (※)、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select** (※)、**tunnel template**、**unlock wwan pin-code**、**user attribute**、**wwan select** (※)

(※) のコマンドは NVR700W Rev.15.01.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

## [ノート]

入力時、*command* パラメーターに対して TAB キーによるコマンド補完は行わぬが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。

*date* に数字と曜日を混在させて指定はできない。

**startup** を指定したスケジュールはルーター起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。

第 4 書式は NVR700W で使用できる。

第 6～9 書式は NVR510 Rev.15.01.23 以降および、NVR700W Rev.15.00.23 以降で利用できる。

## [設定例]

- ウィークデイの 8:00～17:00 だけ接続を許可する

```
# schedule at 1 */mon-fri 8:00 pp 1 pppoe auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 pppoe auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

- 毎時 0 分から 15 分間だけ接続を許可する

```
# schedule at 1 *:00 pp 1 pppoe auto connect on
# schedule at 2 *:15 pp 1 pppoe auto connect off
# schedule at 3 *:15 * disconnect 1
```

- 今度の元旦にルーティングを切替える

```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

- 毎日 12 時から 13 時の間だけ 20 秒間隔で Lua スクリプトを実行する

```
# schedule at 1 12:*:00 * lua script.lua
# schedule at 2 12:*:20 * lua script.lua
# schedule at 3 12:*:40 * lua script.lua
```

- 毎日 3 時にスイッチを再起動する

```
# schedule at 1 */* 03:00 switch 00:a0:de:01:02:03 switch control function execute restart
# schedule at 2 */* 03:00 switch lan1:4 switch control function execute restart
```

- コマンド設定時から 10 分後に再起動する

```
# schedule at 1 +600 * restart
```

## [適用モデル]

NVR700W, NVR510

## 第 37 章

### VLAN の設定

#### 37.1 VLAN ID の設定

##### [書式]

```
vlan interface/sub_interface 802.1q vid=vid [name=name]
no vlan interface/sub_interface 802.1q
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *sub\_interface*
  - [設定値]: 1-32
  - [初期値]: -
- *vid*
  - [設定値]: VLAN ID(IEEE802.1Q タグの VID フィールド格納値) (2 -4094)
  - [初期値]: -
- *name*
  - [設定値]: VLAN に付ける任意の名前 (最大 127 文字)
  - [初期値]: -

##### [説明]

LAN インターフェースで使用する VLAN の VLAN ID を設定する。  
設定された VID を格納した IEEE802.1Q タグ付きパケットを扱うことができる。  
ひとつの LAN インターフェースあたり最大 32VLAN の設定ができる。

##### [ノート]

タグ付きパケットを受信した場合、そのタグの VID が受信 LAN インターフェースに設定されていない場合はパケットを破棄する。  
同一 LAN インターフェースで LAN 分割機能との併用はできない。両者のうち先に入力されたものが有効となり、後から入力されるものはコマンドエラーになる。

##### [適用モデル]

NVR700W, NVR510

#### 37.2 スイッチングハブのポートが所属する VLAN の設定

##### [書式]

```
vlan port mapping sw_port vlan_interface
no vlan port mapping sw_port [vlan_interface]
```

##### [設定値及び初期値]

- *sw\_port*
  - [設定値]: スイッチングハブのポート (lan1.1 - lan1.N)
  - [初期値]: -
- *vlan\_interface*
  - [設定値]: VLAN インターフェース名 (vlan1 - vlanN)
  - [初期値]: -

##### [説明]

LAN 分割機能の拡張機能において、スイッチングハブの各ポートが所属する VLAN インターフェースを指定する。

ポートの名称には `lan1.N` を使用する。

同一の VLAN インターフェースに所属するポート間はスイッチとして動作する。

`lan1.N` が所属する VLAN インターフェースは `vlanN` となる。

#### [ノート]

**lan type** コマンドで `"port-based-option=divide-network"` を設定し、LAN 分割機能を有効にしなければ本コマンドは機能しない。

`"port-based-option=divide-network"` の設定が無い場合でも **vlan port mapping** は設定できるが、スイッチングハブの動作は変化しない。

#### [設定例]

```
# vlan port mapping lan1.3 vlan3
# vlan port mapping lan1.4 vlan3
```

#### [適用モデル]

NVR700W

## 第 38 章

### 生存通知機能

#### 38.1 生存通知の共有鍵の設定

##### [書式]

**heartbeat pre-shared-key** *key*

**no heartbeat pre-shared-key**

##### [設定値及び初期値]

- *key*
  - [設定値]: ASCII 文字列で表した鍵 (32 文字以内)
  - [初期値]: -

##### [説明]

生存通知を受信する側で認証を行うための共有鍵を設定する。生存通知の送信側、受信側の両方で同じ鍵が設定されている必要がある。

このコマンドが設定されていない場合、生存通知の送信および受信時のログ出力は行われない。

##### [適用モデル]

NVR700W

#### 38.2 生存通知を受信するか否かの設定

##### [書式]

**heartbeat receive** *switch* [*option=value* ...]

**no heartbeat receive** [*switch*]

##### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| on  | 生存通知パケットを受信する  |
| off | 生存通知パケットを受信しない |

- [初期値]: off
- *option=value*

- [設定値]:

| <i>option</i> | <i>value</i>          | 説明                         |
|---------------|-----------------------|----------------------------|
| log           | on                    | 受信した内容を syslog に出力する。      |
|               | off                   | 受信した内容を syslog に出力しない。     |
| monitor       | 監視時間[秒](30..21474836) | 指定した秒数の間に通知がない場合にアラートを上げる。 |
|               | off                   | 生存通知の受信がない場合でもアラートを上げない。   |

- [初期値]:
  - log=off
  - monitor=off

**[説明]**

受信した生存通知の内容を **syslog** に出力するか否かを設定する。  
**monitor** オプションで指定した監視時間内に生存通知が届かないとき、**syslog** を出力し **SNMP** トラップを送出する。

**[ノート]**

本コマンドを設定する前に、**heartbeat pre-shared-key** コマンドで、送信側ルーターとの共有鍵を設定する必要がある。

**[適用モデル]**

NVR700W

**38.3 生存通知の実行****[書式]**

```
heartbeat send dest_addr [log=switch]
```

**[設定値及び初期値]**

- *dest\_addr*
  - [設定値]: 送信先ルーターの IPv4 アドレスまたは FQDN
  - [初期値]: -
- *switch*: syslog の出力
  - [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | syslog を出力する  |
| off | syslog を出力しない |

- [初期値]: off

**[説明]**

*dest\_addr* で指定した IP アドレスに、**snmp sysname** で設定した機器の名称と IP アドレスを送り、通信できる状態であることを通知する。

**log=on** の場合、パケットを送信するときに **syslog** を出力する。

**[ノート]**

本コマンドを設定する前に、**heartbeat pre-shared-key** コマンドで、受信側ルーターとの共有鍵を設定する必要がある。

**[適用モデル]**

NVR700W

## 第 39 章

### 生存通知機能 リリース 2

生存通知機能とは、ネットワークに接続しているルーターから他拠点のルーターへ、自分の名前と IP アドレスを含めたパケットを送り、通信できる状態であることを通知する機能です。通知パケットを受信したルーターは、通知された名前と IP アドレスをログに出力し、保存します。WAN の IP アドレスが不定となる拠点のルーターから他拠点のルーターへ通信可能であることを知らせる手段として本機能を利用することができます。

#### リリースについて

前章で説明する従来の生存通知機能はリリース 1、本章で説明する生存通知機能はリリース 2 と区別します。両者の機能概念は同じですが、コマンド体系、動作には互換性がありませんので注意してください。

#### リリース 2 の特徴

- 生存通知パケットとして UDP / 8512 番ポートを使用します ( 始点 / 終点ともに )。
- 生存通知を受信したルーターでは、通知された名前によって送信元のルーターを識別します。そのため、生存通知を送信するルーター毎に固有の名前を設定する必要があります。
- 送信側ルーター、受信側ルーターで共通の暗号鍵、および認証鍵を持つことにより、通知情報の暗号化や改竄の検出が可能となります。
- 多対地通信における運用管理を容易にするため、送信 / 受信設定はそれぞれ識別子を指定することで複数設定できるようになっています。ここで、ペアとなる送信側の送信設定と受信側の受信設定は、それぞれ同じ識別子を指定する必要があります。この設定識別子を通知パケットに含めることにより、受信側は任意の通知パケットに対して使用する受信設定を一意に決定します。
- 従来、**schedule** コマンドと組み合わせることで実現していた通知の定期送信は、送信設定コマンドのみで実施できるようになります。
- 通知する IP アドレスは原則として生存通知パケットの送出インターフェースに設定されている IP アドレスとなります。ここで、当該インターフェースに NAT や IP マスカレードが設定されていれば、送出する通知パケットに NAT / IP マスカレード設定を適用した場合の IP アドレスが使用されます。ただし、**unnumbered** 接続の回線を使用して生存通知パケットを送信する場合は、IP アドレスが設定されている LAN インターフェースの中で、若番のインターフェースから優先的に IP アドレスを選択して通知します ( 通知パケットの IP ヘッダの始点アドレスと同期 )。
- 受信した生存通知の情報を **show status heartbeat2** コマンドで表示することができます。

### 39.1 通知名称の設定

#### [書式]

```
heartbeat2 myname name
no heartbeat2 myname
```

#### [設定値及び初期値]

- *name*
  - [設定値]: 生存通知で使用する名称 (1~64 文字/ASCII、1~32 文字/シフト JIS)
  - [初期値]: -

#### [説明]

生存通知で通知する本機の名前を設定する。

*name* には ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 ( 半角カタカナを除く ) も使用できる。ただし、**console character** コマンドの設定が **sjis** の場合にのみ正しく設定、表示でき、他の設定では意図した通りに処理されない場合がある。

#### [適用モデル]

NVR700W

### 39.2 通知設定の定義

#### [書式]

```
heartbeat2 transmit trans_id [crypto crypto_key] auth auth_key dest_addr ...
no heartbeat2 transmit trans_id
```

#### [設定値及び初期値]

- *trans\_id*



- [設定値]: 通知設定の識別子 (1..65535)
- [初期値]: -
- *crypto\_key*
  - [設定値]: ASCII 文字列で表した暗号鍵 (1~32 文字)
  - [初期値]: -
- *auth\_key*
  - [設定値]: ASCII 文字列で表した認証鍵 (1~32 文字)
  - [初期値]: -
- *dest\_addr*
  - [設定値]: 送信先ルーターの IPv4 アドレス、または FQDN( 空白で区切って 4 つまで指定可能)
  - [初期値]: -

**[説明]**

生存通知の定期的な送信設定を定義する。本コマンドで設定した *auth\_key* を元に、通知パケットには認証情報が付与される。また、*crypto\_key* を指定した場合は更に通知内容が暗号化される。

対応する受信側の設定として **heartbeat2 receive** コマンドを設定する際には、*recy\_id* が本コマンドの *trans\_id* と一致していなければならない。また同様に、*crypto\_key*、*auth\_key* も一致させる必要がある。

本コマンドは送信に最低限必要なパラメーターを *trans\_id* に紐付けて定義するためのものである。実際に送信処理を有効にするには **heartbeat2 transmit enable** コマンドを設定する必要がある。

なお、複数の通知設定による送信負荷を分散させるため、通知設定が有効になってから最初に通知パケットを送信するまでの時間は、通知設定/宛先毎にランダムとなる (ただし 30 秒以内)。

**[適用モデル]**

NVR700W

### 39.3 通知設定の有効化

---

**[書式]**

```
heartbeat2 transmit enable [one-shot] trans_id_list
no heartbeat2 transmit enable
```

**[設定値及び初期値]**

- *trans\_id\_list*: 有効にしたい通知設定の識別子のリスト
  - [設定値]:
    - 1 個の数字、または間に - をはさんだ数字 ( 範囲指定)、およびこれらを任意に並べたもの (128 個以内)
  - [初期値]: -

**[説明]**

定義した通知設定から実際に有効にしたいものを指定する。  
識別子のリストは空白で区切って 128 個まで指定することができる。

'one-shot' キーワードを指定した場合は、*trans\_id\_list* で指定された各設定の通知処理を 1 回だけ実行する。なお、この形式で入力したコマンドは保存できない。

**[適用モデル]**

NVR700W

### 39.4 通知間隔の設定

---

**[書式]**

```
heartbeat2 transmit interval time
heartbeat2 transmit interval trans_id time
no heartbeat2 transmit interval [time]
no heartbeat2 transmit interval trans_id time
```

**[設定値及び初期値]**

- *trans\_id*
  - [設定値]: 通知設定の識別子

- [初期値]: -
- *time*
  - [設定値]: 通知間隔秒数 (30..65535)
  - [初期値]: 30

**[説明]**

*trans\_id* に対応する通知設定の送信間隔を指定する。  
*trans\_id* を省略した場合は全ての通知設定が適用対象となる。  
 ただし、*trans\_id* を個別に指定した設定の方が優先して適用される。

**[適用モデル]**  
 NVR700W

## 39.5 通知を送信した際にログを記録するか否かの設定

---

**[書式]**

```
heartbeat2 transmit log [trans_id] sw
no heartbeat2 transmit log [trans_id]
```

**[設定値及び初期値]**

- *trans\_id*
  - [設定値]: 通知設定の識別子
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | 送信した内容を syslog に出力する  |
| off | 送信した内容を syslog に出力しない |

- [初期値]: off

**[説明]**

*trans\_id* に対応する通知設定のログ出力に関する設定を行う。*sw* を 'on' にした場合、生存通知を送信する際に INFO レベルの syslog を出力する。

*trans\_id* を省略した場合は全ての通知設定が適用対象となる。ただし、*trans\_id* を個別に指定した設定の方が優先して適用される。

**[適用モデル]**  
 NVR700W

## 39.6 受信設定の定義

---

**[書式]**

```
heartbeat2 receive recv_id [crypto crypto_key] auth auth_key
no heartbeat2 receive recv_id
```

**[設定値及び初期値]**

- *recv\_id*
  - [設定値]: 受信設定の識別子
  - [初期値]: -
- *crypto\_key*
  - [設定値]: ASCII 文字列で表した暗号鍵 (1~32 文字)
  - [初期値]: -
- *auth\_key*
  - [設定値]: ASCII 文字列で表した認証鍵 (1~32 文字)
  - [初期値]: -

**[説明]**

生存通知の受信設定を定義する。受信処理を行う際は、通知パケットに含まれる送信側の設定識別子 (*trans\_id*) を元に、同じ *recv\_id* を持つ本コマンドの設定を使用して復号化、認証チェックが行われる。

対応する送信側の設定として **heartbeat2 transmit** コマンドを設定する際には、*trans\_id* が本コマンドの *recv\_id* と一致していなければならない。また同様に、*crypto\_key*、*auth\_key* も一致させる必要がある。

本コマンドは受信に最低限必要なパラメーターを *recv\_id* に紐付けて定義するためのものである。実際に受信処理を有効にするには **heartbeat2 receive enable** コマンドを設定する必要がある。

**[適用モデル]**

NVR700W

## 39.7 受信設定の有効化

---

**[書式]**

**heartbeat2 receive enable** *recv\_id\_list*

**no heartbeat2 receive enable**

**[設定値及び初期値]**

- *recv\_id\_list* : 有効にしたい受信設定の識別子のリスト
  - [設定値]:
    - 1 個の数字、または間に - をはさんだ数字 ( 範囲指定 )、およびこれらを任意に並べたもの (128 個以内)
  - [初期値]: -

**[説明]**

定義した受信設定から実際に有効にしたいものを指定する。  
識別子のリストは空白で区切って 128 個まで指定することができる。

**[適用モデル]**

NVR700W

## 39.8 受信間隔の監視設定

---

**[書式]**

**heartbeat2 receive monitor** *time*

**heartbeat2 receive monitor** *recv\_id time*

**no heartbeat2 receive monitor** [*time*]

**no heartbeat2 receive monitor** *recv\_id time*

**[設定値及び初期値]**

- *recv\_id*
  - [設定値]: 受信設定の識別子
  - [初期値]: -
- *time* : 監視時間
  - [設定値]:

| 設定値          | 説明         |
|--------------|------------|
| 30..21474836 | 秒数         |
| off          | 受信間隔を監視しない |

- [初期値]: off

**[説明]**

*recv\_id* に対応する受信設定における受信間隔の監視設定を行う。監視が有効な場合は、指定した時間内に生存通知が届かないとき INFO レベルの syslog を出力して SNMP トラップを送出する。

*recv\_id* を省略した場合は全ての受信設定が適用対象となる。ただし、*recv\_id* を個別に指定した設定の方が優先して適用される。

**[適用モデル]**

NVR700W

## 39.9 通知を受信した際にログを記録するか否かの設定

### [書式]

```
heartbeat2 receive log [recv_id] sw
no heartbeat2 receive log [recv_id]
```

### [設定値及び初期値]

- *recv\_id*
  - [設定値]: 受信設定の識別子
  - [初期値]: -
- *sw*
  - [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | 受信した内容を syslog に出力する  |
| off | 受信した内容を syslog に出力しない |

- [初期値]: off

### [説明]

*recv\_id* に対応する受信設定のログ出力に関する設定を行う。*sw* を 'on' にした場合、生存通知を送信する際に INFO レベルの syslog を出力する。

*recv\_id* を省略した場合は全ての受信設定が適用対象となる。ただし、*recv\_id* を個別に指定した設定の方が優先して適用される。

### [適用モデル]

NVR700W

## 39.10 同時に保持できる生存情報の最大数の設定

### [書式]

```
heartbeat2 receive record limit num
no heartbeat2 receive record limit
```

### [設定値及び初期値]

- *num*
  - [設定値]: 生存情報の最大保持数 ( 64..1000 )
  - [初期値]: 64

### [説明]

受信した生存情報を同時に保持できる最大数を設定する。生存情報数が最大に達した状態では新規の情報を取り込むことができない。そのような場合は **clear heartbeat2** コマンドで不要な情報を削除する必要がある。

### [適用モデル]

NVR700W

## 39.11 生存通知の状態のクリア

### [書式]

```
clear heartbeat2
clear heartbeat2 id recv_id
clear heartbeat2 name string
```

### [設定値及び初期値]

- *recv\_id*
  - [設定値]: 受信設定の識別子
  - [初期値]: -
- *string*
  - [設定値]: 文字列 (1~64 文字/ASCII、1~32 文字/シフト JIS)
  - [初期値]: -

**[説明]**

受信した生存通知の情報をクリアする。

第 1 書式では保持している全ての情報をクリアする。

第 2 書式では指定の受信設定により受信した情報のみクリアする。

第 3 書式では指定の文字列が通知名称に含まれる情報のみクリアする。

*string* には ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 ( 半角カタカナを除く ) も使用できる。ただし、**console character** コマンドの設定が sjis の場合にのみ正しく動作し、他の設定では誤動作する可能性がある。

**[適用モデル]**

NVR700W

## 第 40 章

### SNTP サーバー機能

SNTP は、ネットワークを利用してコンピュータやネットワーク機器の時刻を同期させるためのプロトコルです。SNTP サーバー機能ではクライアントからの時刻の問い合わせに対してルーターの内蔵クロックの値を返します。SNTP サーバー機能は SNTP バージョン 4 を実装しています。また、下位互換として SNTP バージョン 1~3 のリクエストにも対応しています。

SNTP サーバー機能を利用して正確な時刻を得るために、定期的に **ntpdate** コマンドを実行して、他の NTP サーバーにルーターの時刻を合わせておくことを推奨します。

#### 40.1 SNTP サーバー機能を有効にするか否かの設定

##### [書式]

```
sntp service switch
no sntp service
```

##### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | SNTP サーバー機能を有効にする |
| off | SNTP サーバー機能を無効にする |

- [初期値]: on

##### [説明]

SNTP サーバー機能を有効にするか否かを設定します。

##### [適用モデル]

NVR700W, NVR510

#### 40.2 SNTP サーバーへのアクセスを許可するホストの設定

##### [書式]

```
sntp host ip_range [ip_range...]
sntp host any
sntp host none
sntp host lan
no sntp host
```

##### [設定値及び初期値]

- *ip\_range*: SNTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

| 設定値                                                            | 説明                        |
|----------------------------------------------------------------|---------------------------|
| 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの | 指定したホストからのアクセスを許可する       |
| lanN                                                           | LAN インターフェースからのアクセスを許可する  |
| onu1                                                           | ONU インターフェースからのアクセスを許可する  |
| wan1                                                           | WAN インターフェースからのアクセスを許可する  |
| bridge1                                                        | ブリッジインターフェースからのアクセスを許可する  |
| vlanN                                                          | VLAN インターフェースからのアクセスを許可する |

| 設定値    | 説明                           |
|--------|------------------------------|
| lanN/M | タグ VLAN インターフェースからのアクセスを許可する |

- [初期値]: -
- *any*
  - [設定値]: すべてのホストからのアクセスを許可する
  - [初期値]: -
- *none*
  - [設定値]: すべてのホストからのアクセスを禁止する
  - [初期値]: -
- *lan*
  - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
  - [初期値]: lan

#### [説明]

SNTP サーバーへのアクセスを許可するホストを設定する。

#### [ノート]

このコマンドで LAN インターフェースまたは ONU インターフェースを指定した場合には、ネットワークアドレスとディレクテッドブロードキャストアドレスを除く IPv4 アドレスからのアクセスを許可する。指定した LAN インターフェースまたは ONU インターフェースにプライマリアドレスもセカンダリアドレスも設定していなければアクセスを許可しない。

ブリッジインターフェースと VLAN インターフェースは NVR700W で指定可能。

WAN インターフェースは NVR700W の Rev.15.00.03 以降、NVR510 の Rev.15.01.03 以降で指定可能。

ブリッジインターフェースは NVR700W の Rev.15.00.03 以降で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 第 41 章

### 外部メモリ機能

本機能は、ルーター本体へ外部メモリ (USB メモリ、microSD カード) を接続することにより、ルーターと外部メモリ間で各種データの操作を行います。

本機能により、以下の動作が可能となります。

- コマンド設定、あるいは実行コマンドによる動作
  - 外部メモリへ SYSLOG メッセージを出力する。
  - 外部メモリへ設定ファイルをコピーする。
  - 外部メモリから設定ファイルをコピーする。
  - 外部メモリからファームウェアファイルをコピーする。
- ルーター本体の外部メモリボタンおよび DOWNLOAD ボタンの操作による動作
  - 外部メモリボタンと DOWNLOAD ボタンを同時に 3 秒以上押し続け、外部メモリから設定ファイルおよびファームウェアファイルをコピーする。
- 外部メモリからの起動
- バッチファイル実行機能

#### バッチファイル実行機能

外部メモリの中に、コマンドを羅列したファイル (バッチファイルと呼びます) を入れておき、そのファイルに記述されたコマンドを実行する機能です。

設定によって DOWNLOAD ボタンを押して実行させることができます。コンソールでの **execute batch** コマンドによって実行することもできます。

コマンドの実行結果やログは、ファイルとして外部メモリに書き出します。

本機能を用いると、PC がない環境でも PING での疎通確認などを行うことができます。例えばルーターの設置作業時に、必要な装置や作業手順を大幅に減らすことができます。実行結果や設定内容、ルーターの状態などは、外部メモリにファイルとして書き出されます。書き出されたファイルは、外部メモリを取り出して携帯電話で確認することができます。作業ログとして利用することもできます。

本機能に関する技術情報は以下に示す URL で公開されています。

<http://www.rtpro.yamaha.co.jp>

#### 41.1 USB ホスト機能を使うか否かの設定

##### [書式]

**usbhost use switch**

**no usbhost use**

##### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明              |
|-----|-----------------|
| on  | USB ホスト機能を使用する  |
| off | USB ホスト機能を使用しない |

- [初期値]: on

##### [説明]

USB ホスト機能を使用するか否かを設定する。

このコマンドが **off** に設定されているときは USB メモリをルーターに接続しても認識されない。

また、過電流により USB ホスト機能に障害が発生した場合、USB メモリが接続されていない状態で本コマンドを再設定すると復旧させることができる。



[適用モデル]  
NVR700W, NVR510

## 41.2 USB バスで過電流保護機能が働くまでの時間の設定

[書式]

**usbhost overcurrent duration** *duration*  
**no usbhost overcurrent duration**

[設定値及び初期値]

- *duration*
  - [設定値]: 時間 (5..100、1 単位が 10 ミリ秒)
  - [初期値]: 5 (50 ミリ秒)

[説明]

過電流保護機能が働くまでの時間を設定する。ここで設定した時間、連続して過電流が検出されたら、過電流保護機能が働く。

[適用モデル]  
NVR700W, NVR510

## 41.3 microSD カードスロットを使うか否かの設定

[書式]

**sd use** *switch*  
**no sd use** [*switch*]

[設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| on  | microSD カードスロットを使用する  |
| off | microSD カードスロットを使用しない |

- [初期値]: on

[説明]

microSD カードスロットを使用するか否かを設定する。このコマンドが off に設定されているときは microSD カードをカードスロットに差し込んでも認識されない。

[適用モデル]  
NVR700W, NVR510

## 41.4 外部メモリ用キャッシュメモリの動作モードの設定

[書式]

**external-memory cache mode** *mode*  
**no external-memory cache mode** [*mode*]

[設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値           | 説明          |
|---------------|-------------|
| write-through | ライトスルーモード   |
| copy-back1    | コピーバックモード 1 |
| copy-back2    | コピーバックモード 2 |

- [初期値]: copy-back1

**[説明]**

外部メモリ用キャッシュメモリの動作モードを設定する。ライトスルーモード、コピーバックモード1、及びコピーバックモード2の3種類の動作モードをサポートしており、各モードによってFAT、DIR、FILEの各キャッシュ上のデータを外部メモリへ書き出すタイミングが異なる。

各動作モードについて、以下に説明する。

`write-through` を指定した場合、FAT、DIR、FILE に割り当てられていたキャッシュは、ライトスルーモードで動作し、常に外部メモリへ書き出される。最も安全性が高い。

`copy-back1` を指定した場合、FAT と DIR キャッシュはコピーバックモードで動作し、FILE キャッシュは、ライトスルーモードで動作する。ライトスルーモードより高速に動作させることができる。

`copy-back2` を指定した場合、FAT、DIR、FILE キャッシュがコピーバックモードで動作する。この設定では、外部メモリへの書き出しが抑制されるので、最も高速に動作する。しかし、外部メモリへ書き出しが完了していない状態が続く為、予期しない電源断が発生すると外部メモリのファイルシステムがダメージを受ける可能性が高くなる。

FAT : File Allocation Table の略

DIR : Directory Entry の略

**[ノート]**

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

**[適用モデル]**

NVR700W, NVR510

## 41.5 ファイルアクセス高速化用キャッシュメモリのサイズの設定

**[書式]**

`external-memory accelerator cache size interface size`

`no external-memory accelerator cache size interface [size]`

**[設定値及び初期値]**

- `interface`

- [設定値]:

| 設定値  | 説明              |
|------|-----------------|
| usb1 | USB ポート         |
| sd1  | microSD カードスロット |

- [初期値]: -

- `size`

- [設定値]:

| 設定値 | 説明                                |
|-----|-----------------------------------|
| 1-5 | キャッシュメモリのサイズ (数値が大きいほどメモリサイズが大きい) |
| off | ファイルアクセス高速化機構を使用しない               |

- [初期値]: 1

**[説明]**

ファイルアクセスを高速化するために使用するキャッシュメモリのサイズを設定する。

`size` に数値を指定した場合は、ファイルアクセスを高速化するための機構が働き、特にディレクトリ数やファイル数の多い構成での外部メモリへのアクセス性能が向上する。アクセス性能が向上しない場合は、`size` を大きくすることで向上することがある。ただし、`size` が大きいほど、外部メモリを接続してから使用可能になるまでの時間が長くなることがある。

`size` に `off` を指定した場合は、ファイルアクセスを高速化するためのキャッシュメモリは確保されない。

なお、すべてのインターフェースに対して `size` に最大値を設定した状態で、同時にすべてのインターフェースに外部メモリを接続して使用すると、システム全体の性能に影響を与える可能性があるため、本コマンドを設定してファイルアクセスを高速化するインターフェースは一つに限定することを推奨する。

## [ノート]

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

また、本コマンドで、*size* を大きくしてもアクセス性能が向上しない場合は、下記に示す操作を行うことで、改善されることがある。

- 可能であれば、外部メモリ内のディレクトリやファイルを減らす
- 外部メモリ内の総ディレクトリ数を 2,000 個以内となるように調整する
- 頻繁にアクセスするディレクトリ内の総ファイル数 (ディレクトリ含む) を 20,000 個以内となるように調整する
- ファイル名やディレクトリ名をなるべく短くする (32 文字以内を推奨)

## [適用モデル]

NVR700W, NVR510

## 41.6 外部メモリに保存する統計情報のファイル名のプレフィックスの設定

## [書式]

**external-memory statistics filename prefix *prefix* [*crypto password*] [**max-filename**=*filename*] [**interval**=*minute*]**

**no external-memory statistics filename prefix [*prefix* [*crypto password*] [**max-filename**=*filename*] [**interval**=*minute*]]**

## [設定値及び初期値]

- *prefix*: ファイル名のプレフィックス (半角英数字のみ)

- [設定値]:

| 設定値                   | 説明            |
|-----------------------|---------------|
| usb1: <i>filename</i> | ファイル名のプレフィックス |
| sd1: <i>filename</i>  | ファイル名のプレフィックス |

- [初期値]: -
- *crypto*: 統計情報ファイルを暗号化して保存する場合の暗号アルゴリズムの選択

- [設定値]:

| 設定値    | 説明            |
|--------|---------------|
| aes128 | AES128 で暗号化する |
| aes256 | AES256 で暗号化する |

- [初期値]: -
- *password*
  - [設定値]: ASCII 文字列で表したパスワード (半角 8 文字以上 32 文字以内)
  - [初期値]: -
- *filename*: 外部メモリーに保存する統計情報のファイル数の上限

- [設定値]:

| 設定値                | 説明                          |
|--------------------|-----------------------------|
| 100 ... 2147483647 | 外部メモリーに保存する統計情報のファイル数の上限    |
| infinity           | 外部メモリーに保存する統計情報のファイル数を制限しない |

- [初期値]: infinity
- *minute*: 統計情報を外部メモリーに書き出す間隔

- [設定値]:

| 設定値       | 説明                     |
|-----------|------------------------|
| 2 ... 120 | 統計情報を外部メモリーに書き出す間隔 (分) |

- [初期値]: 12

**[説明]**

統計情報を書き出すファイル名のプレフィックス ( 接頭語 ) を設定する。  
 実際のファイル名は、このプレフィックスをもとにして自動的に決まる。  
 例えば、*prefix* を「yamaha」と設定した場合、LAN2 インターフェースのトラフィック量を書き出すファイル名は、「yamaha\_traffic\_lan2\_20080708.csv」のようになる。

*crypt*、および、*password* を指定した場合、統計情報は暗号化してから外部ストレージに書き込まれる。暗号化する場合、自動的にファイル名に .rtfg 拡張子が追加される。

**[ノート]**

上限を超えた場合、各種別・インターフェースの統計情報のファイルで最も古いファイルを削除して新しいファイルを作成する。

アプリケーションのトラフィック情報に関しては、*crypto* パラメータの有無にかかわらず、暗号化されない実際のファイル名は、*prefix* の後に種別や日付を表す文字列が加わる。

ファイル名の書式は以下に従う。 *prefix\_type[id]\_yyyymm[dd].ext*

- *prefix*
  - 本コマンドにより設定される任意の文字列
- *type*
  - 統計情報の種類

|             |                   |
|-------------|-------------------|
| cpu         | CPU 使用率           |
| memory      | メモリ使用率            |
| flow        | ファストパスのフロー数       |
| route       | 経路数               |
| nat         | NAT テーブルのエントリー数   |
| filter      | 動的フィルターのセッション数    |
| traffic     | インターフェース別のトラフィック量 |
| application | アプリケーションのトラフィック情報 |

- *id*
  - *id* の意味は統計情報の種類によって異なる
    - インターフェース別のトラフィック量.....インターフェースを表す
    - これ以外の統計情報では *id* は省略される
- *yyyy*
  - 西暦 (4 桁)
- *mm*
  - 月 (2 桁)
- *dd*
  - 日 (2 桁)
- *ext*
  - 拡張子

|      |            |
|------|------------|
| csv  | CSV        |
| rtfg | 暗号化されたファイル |

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。  
 アプリケーションのトラフィック情報は、暗号化して保存することはできない。

*prefix* に指定可能な文字数は"usb1:"などのプレフィックスを含めずに半角 15 文字以内。

`max-filenum` オプションで制限するファイル数は、すべての種別・インターフェースの統計情報を書き出したファイルの合計数となる。

アプリケーションのトラフィック情報に関しては、`interval` の設定によらず 1 分ごとに統計情報が書き出される。

NVR700W は Rev.15.00.16 以降で使用可能。

NVR510 は Rev.15.01.15 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 41.7 外部メモリに保存する SYSLOG ファイル名の指定

### [書式]

`external-memory syslog filename name [crypto password] [limit=size] [backup=num] [interval=interval] [line=line]`

`no external-memory syslog filename [name]`

### [設定値及び初期値]

- `name` : SYSLOG ファイル名

- [設定値] :

| 設定値                        | 説明                                        |
|----------------------------|-------------------------------------------|
| <code>usb1:filename</code> | USB メモリ内のファイル名 (.bak 拡張子を含む名前は指定できない)     |
| <code>sd1:filename</code>  | microSD カード内のファイル名 (.bak 拡張子を含む名前は指定できない) |

- [初期値] :-

- `crypto` : SYSLOG を暗号化して保存する場合の暗号アルゴリズムの選択

- [設定値] :

| 設定値                 | 説明            |
|---------------------|---------------|
| <code>aes128</code> | AES128 で暗号化する |
| <code>aes256</code> | AES256 で暗号化する |

- [初期値] :-

- `password`

- [設定値] : ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

- [初期値] :-

- `size`

- [設定値] : SYSLOG ファイルの上限サイズ (1 - 1024 単位:MB)

- [初期値] : 10

- `num`

- [設定値] : バックアップファイルの上限数 (1 - 100)

- [初期値] : 10

- `interval`

- [設定値] : SYSLOG を外部メモリに書き出す間隔 (2 - 86400 単位:秒)

- [初期値] : 2

- `line`

- [設定値] : SYSLOG を外部メモリに書き出す行数 (1000 - 10000 単位:行)

- [初期値] : 1000

### [説明]

外部メモリに保存する SYSLOG ファイル名を設定する。

`name` に .bak 拡張子を含むファイル名は指定できない。また、暗号化しない場合、`name` に .rtfg 拡張子を含むファイル名は指定できない。

*crypto* および、*password* を指定した場合、SYSLOG は暗号化してから外部メモリに書き込まれる。暗号化する場合、*name* に *.rtfg* 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に *.rtfg* 拡張子が追加される。

SYSLOG ファイルが上限サイズに達すると、SYSLOG ファイルのバックアップが行われる。バックアップファイル名は、*name* で指定されたファイル名の後にバックアップを行った日時を表す *\_yyyymmdd\_hhmmss* 形式の文字列を付加したものとなる。

- *yyyy* ... 西暦 (4 桁)
- *mm* ... 月 (2 桁)
- *dd* ... 日 (2 桁)
- *hh* ... 時 (2 桁)
- *mm* ... 分 (2 桁)
- *ss* ... 秒 (2 桁)

バックアップファイル数が *num* で指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。

*interval* で指定した時間が経過した場合、もしくは *line* で指定した行数だけ SYSLOG が出力された場合に、外部メモリに SYSLOG を書き出す。

本コマンドが設定されていないときは SYSLOG は外部メモリに書き込まれない。

#### [ノート]

以下の変更を行う場合、*name* を変更しなければならない。

- SYSLOG を暗号化しないで保存するから、暗号化して保存するに変更する場合
- SYSLOG を暗号化して保存するから、暗号化しないで保存するに変更する場合
- 暗号アルゴリズムまたは、パスワードを変更する場合

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

*name* は半角 99 文字以内。

#### [適用モデル]

NVR700W, NVR510

## 41.8 外部メモリボタンと DOWNLOAD ボタンの同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定

#### [書式]

**operation external-memory download permit *switch***

**no operation external-memory download permit [*switch*]**

#### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

#### [説明]

外部メモリボタンと DOWNLOAD ボタンの同時押下による、設定ファイルとファームウェアファイルのコピー操作を許可するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 41.9 外部メモリ内のファイルからの起動を許可するか否かの設定

### [書式]

```
external-memory boot permit switch
no external-memory boot permit [switch]
```

### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

### [説明]

外部メモリ内のファイルからの起動を許可するか否かを設定する。この設定を OFF に設定すると外部メモリ内のファイルからの起動はできなくなる。

起動時に読み込む設定ファイルとファームウェアファイルの名前はそれぞれ、**external-memory config filename** コマンドと **external-memory exec filename** コマンドで設定できる。

### [適用モデル]

NVR700W, NVR510

## 41.10 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する

### [書式]

```
external-memory boot timeout time
no external-memory boot timeout [time]
```

### [設定値及び初期値]

- *time*
- [設定値]: タイムアウト秒数 (1..30)
- [初期値]: 1

### [説明]

ルーター起動時に外部メモリを検出するまでのタイムアウト時間を設定する。

**external-memory boot permit on** コマンドによって、外部メモリ内のファイルからの起動を許可するに設定されている場合に有効である。

接続認識が遅いデバイスの場合、タイムアウト時間を大きくすることで認識されるようになることがある。

### [ノート]

外部メモリ性能測定コマンドで、**boot device attach** で表示される時間を目安にして設定するとよい。

### [適用モデル]

NVR700W, NVR510

## 41.11 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定

### [書式]

```
external-memory exec filename from [to]
external-memory exec filename off
no external-memory exec filename [from] [to]
no external-memory exec filename [off]
```

### [設定値及び初期値]

- *from*: 外部メモリとファームウェアファイル名
- [設定値]:

| 設定値           | 説明                                                                  |
|---------------|---------------------------------------------------------------------|
| usb1:filename | USB メモリ内のファームウェアファイル名 ( <i>filename</i> は半角 99 文字以内)                |
| sd1:filename  | microSD カード内のファームウェアファイル名 ( <i>filename</i> は半角 99 文字以内)            |
| *:filename    | USB メモリおよび microSD カード内のファームウェアファイル名 ( <i>filename</i> は半角 99 文字以内) |

- [初期値]:
  - \*:nvr700w.bin(NVR700W)
  - \*:nvr510.bin(NVR510)
- *to*: コピー先ファイル名
- [設定値]:

| 設定値                      | 説明                                      |
|--------------------------|-----------------------------------------|
| 0~1 (NVR700W)、0 (NVR510) | 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号 (省略時は 0) |

- [初期値]: 0

### [説明]

外部メモリを差して起動した時、あるいは外部メモリボタンと **DOWNLOAD** ボタンを同時に押下した時に読み込まれる、外部メモリ上のファームウェアファイル名を指定する。

外部メモリボタンと **DOWNLOAD** ボタンを同時に押下した時は、ファームウェアファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM のファームウェアファイル番号も指定できる。

外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリから検索される。

ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

*filename* は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

off に指定した場合、ファームウェアファイルの検索と読み込みを行わない。

### [ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

### [設定例]

- microSD カード内から "nvr700w.bin" を検索し、ファームウェアファイルとして読み込む

```
# external-memory exec filename sd1:nvr700w.bin
```

- microSD カード内のディレクトリ "test" から "nvr700w.bin" を検索し、ファームウェアファイルとして読み込む

```
# external-memory exec filename sd1:/test/nvr700w.bin
```

### [適用モデル]

NVR700W, NVR510

## 41.12 起動時、あるいは外部メモリボタンと **DOWNLOAD** ボタン同時押下により読み込まれる、設定ファイル名の指定

### [書式]

```
external-memory config filename from[from] [to] [password]
```



**external-memory config filename off**

**no external-memory config filename** [*from*] [*to*] [*password*]

**no external-memory config filename** [off]

#### [設定値及び初期値]

- *from* : 外部メモリと設定ファイル名

- [設定値] :

| 設定値                   | 説明                                                             |
|-----------------------|----------------------------------------------------------------|
| usb1: <i>filename</i> | USB メモリ内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)                |
| sd1: <i>filename</i>  | microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)            |
| *: <i>filename</i>    | USB メモリおよび microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内) |

- [初期値] : \*:config.rtf、\*:config.txt

- *to* : コピー先ファイル名

- [設定値] :

| 設定値 | 説明                             |
|-----|--------------------------------|
| 0~4 | 内蔵フラッシュ ROM の設定ファイル番号 (省略時は 0) |

- [初期値] : 0

- *password*

- [設定値] : 復号パスワード (ASCII 文字列で半角 8 文字以上、32 文字以内)

- [初期値] : -

#### [説明]

外部メモリを差して起動した時、あるいは外部メモリボタンと **DOWNLOAD** ボタンを同時に押下した時に読み込まれる、外部メモリ上の設定ファイル名を指定する。

また外部メモリボタンと **DOWNLOAD** ボタンを同時に押下した時は、設定ファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM の設定ファイル番号も指定できる。

外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリから検索される。

ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

*filename* は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

パスワードを指定して暗号化されている設定ファイルを復号して読み込む場合は、*password* に暗号化したときのパスワードを設定する。

off に指定した場合、設定ファイルの検索と読み込みを行わない。

#### [ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

#### [設定例]

- microSD カード内から "config.txt" を検索し、設定ファイルとして読み込む

```
# external-memory config filename sd1:config.txt
```

- microSD カード内のディレクトリ "test" から "config.txt" を検索し、設定ファイルとして読み込む

```
# external-memory config filename sd1:/test/config.txt
```

[適用モデル]

NVR700W, NVR510

## 41.13 ファイル検索時のタイムアウトを設定する

[書式]

```
external-memory auto-search time time
```

```
no external-memory auto-search time [time]
```

[設定値及び初期値]

- *time*
  - [設定値]:
    - 秒数 (1..600)
  - [初期値]: 300

[説明]

外部メモリに格納されているファイルを検索する時のタイムアウト時間を設定する。

[適用モデル]

NVR700W, NVR510

## 41.14 バッチファイルを実行する

[書式]

```
execute batch
```

[説明]

外部メモリのバッチファイルを実行する。実行されるバッチファイル名は **external-memory batch filename** コマンドで指定する。

[ノート]

実行中のバッチファイルを中断したい場合は Ctrl+C を入力する。

[適用モデル]

NVR700W, NVR510

## 41.15 バッチファイルと実行結果ファイルの設定

[書式]

```
external-memory batch filename batchfile [logfile]
```

```
no external-memory batch filename [batchfile [logfile]]
```

[設定値及び初期値]

- *batchfile*: バッチファイル名 (*logfile* を指定した場合は、半角 99 文字以内。 *logfile* を省略した場合は、拡張子を除いて半角 91 文字以内。)
- [設定値]:

| 設定値                   | 説明                               |
|-----------------------|----------------------------------|
| usb1: <i>filename</i> | USB メモリ内のバッチファイル名                |
| sd1: <i>filename</i>  | microSD カード内のバッチファイル名            |
| *: <i>filename</i>    | USB メモリおよび microSD カード内のバッチファイル名 |

- [初期値]: \*:command.txt
- *logfile*
- [設定値]:

| 設定値             | 説明                     |
|-----------------|------------------------|
| <i>filename</i> | 実行結果ファイル名 (半角 99 文字以内) |

- [初期値] : `command-log.txt`

#### [説明]

外部メモリ内のバッチファイル名と実行結果ファイル名を指定する。

外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリから検索される。

ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

*filename* は絶対パスを使ってファイルを指定するかファイル名のみを指定する。バッチファイルの *filename* にファイル名のみを指定した場合は外部メモリ内から自動検索する。複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

*logfile* を省略した場合、" バッチファイル名 -log.txt" という名前で実行結果ファイルが作成される。

#### [設定例]

- microSD カードのファイルから "command\_test.txt" をバッチファイルとして検索する。

```
# external-memory batch filename sd1:command_test.txt
```

- microSD カードのディレクトリ "test" から "command\_test.txt" を読み込む。

```
# external-memory batch filename sd1:/test/command_test.txt
```

#### [適用モデル]

NVR700W, NVR510

## 41.16 外部メモリ性能測定コマンド

#### [書式]

```
external-memory performance-test go interface
```

#### [設定値及び初期値]

- *interface*
- [設定値] :

| 設定値  | 説明               |
|------|------------------|
| usb1 | USB インターフェース     |
| sd1  | microSD インターフェース |

- [初期値] : -

#### [説明]

外部メモリ機能の使用に耐えうる性能を持つメモリであるか否かを確認する。

外部メモリの認識に要する時間やデータの読み書き速度を確認し、一連のテスト終了後、使用に耐えうる性能を持つと判断されれば、

- OK:succeeded

そうでないものは

- NG:failed

と表示する。

#### [ノート]

外部メモリはフォーマット直後の状態のものを対象とする。

本機能は他の機能を使用していない状態で実行する必要がある。

本コマンド実行中は **syslog debug on**、**no syslog host** が設定される。そのため、**syslog debug off** にしていても DEBUG タイプの SYSLOG が出力されることがある。また、**syslog host** コマンドを設定していても SYSLOG サーバーにログが転送されない。

boot device attach テストで、NG 判定と表示された場合は、**external-memory boot timeout** コマンドでタイムアウト時間を表示された値よりも大きくすることで、OK 判定になることがある。

ただし、ルーター起動時に外部メモリからの起動の対象メモリとして扱わない場合には特に変更する必要は無い。

device attach テストで、NG 判定と表示された場合は、USB ボタンを押下して、一旦デバイスを取り外して接続し直してから再度テストを実行することで、OK 判定になることがある。

ヤマハルーターの外部メモリ機能を利用する際に外部メモリに求められる最低限の性能を確認するものであり、本機能の結果はその外部メモリの全ての動作を保証するものではない。

外部メモリ機能を使用する際は、**show status external-memory** コマンドで外部メモリへの書き込みエラーなどが発生していないことを定期的に確認することを推奨する。

#### [適用モデル]

NVR700W, NVR510

## 41.17 DOWNLOAD ボタンを押した時に実行する機能の設定

### [書式]

**operation button function download** *function* [*script\_file* [*args* ...]]

**no operation button function download** [*function* [*script\_file* [*args* ...]]]

### [設定値及び初期値]

- *function* : DOWNLOAD ボタンを押した時に実行する機能

- [設定値]:

| 設定値                    | 説明               |
|------------------------|------------------|
| http revision-up       | HTTP リビジョンアップ    |
| execute batch          | バッチファイルの実行       |
| mobile signal-strength | 携帯端末の電波の受信レベルの取得 |
| execute lua            | Lua スクリプトの実行     |

- [初期値]: http revision-up
- *script\_file*
  - [設定値]: スクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
  - [初期値]: -
- *args*
  - [設定値]: *script\_file* に渡す可変個引数
  - [初期値]: -

### [説明]

DOWNLOAD ボタンを押した時に実行する機能を設定する。

*function* に execute lua を設定した場合、*script\_file* を必ず指定する必要がある。*script\_file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は set コマンドで変更可能であり、初期値は "/" である。

### [ノート]

Lua スクリプトを実行させる場合、環境変数 LUA\_INIT が設定されていれば *script\_file* よりも先に LUA\_INIT のスクリプトが実行される。

#### [適用モデル]

NVR700W, NVR510

## 41.18 DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定

### [書式]

**operation execute batch permit** *permit*

**no operation execute batch permit** [*permit*]

### [設定値及び初期値]

- *permit*
  - [設定値]:

| 設定値 | 説明                              |
|-----|---------------------------------|
| on  | DOWNLOAD ボタンによるバッチファイルの実行を許可する  |
| off | DOWNLOAD ボタンによるバッチファイルの実行を許可しない |

- [初期値]: off

#### [説明]

DOWNLOAD ボタンによりバッチファイルの実行機能を使用するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 41.19 シグネチャーを保存する外部メモリのディレクトリの設定

#### [書式]

```
external-memory dpi signature directory path
no external-memory dpi signature directory [path]
```

#### [設定値及び初期値]

- *path*
  - [設定値]: ディレクトリのパス(半角 99 文字以内)
  - [初期値]: -

#### [説明]

シグネチャーを保存する外部メモリのディレクトリを指定する。

DPI が有効になったとき、本コマンドが設定されており、かつ本コマンドで指定されている外部メモリ上のディレクトリにシグネチャーが存在する場合には、ネットワーク経由のシグネチャーのダウンロードは行わず、外部メモリ上のシグネチャーを使用する。

シグネチャーをダウンロードしたとき、*path* に指定した外部メモリ上のディレクトリが存在しなければ、ディレクトリを自動生成して、シグネチャーを保存する。*path* に指定したディレクトリを含む外部メモリが接続されていない場合、その間にダウンロードしたシグネチャーは保存できない。その後外部メモリが接続された場合には、次のシグネチャー更新時にダウンロードしたシグネチャーが保存される。

次の更新を待たずに外部メモリにシグネチャーをダウンロードしたい場合には、**dpi signature download go** コマンドを **force** オプションを付けて実行すると、シグネチャーの更新がなくとも直ちにダウンロード、および外部メモリへの保存が可能となる。*path* で指定したディレクトリに以前保存したシグネチャーが存在する場合には、新たにダウンロードしたシグネチャーを既存のシグネチャーに上書きして保存する。

#### [ノート]

シグネチャーは "rt\_dpi\_(機種名).ysig" というファイル名で保存される。例えば、NVR700W の場合には、"rt\_dpi\_nvr700w.ysig" となる。*path* に RTFS 上のディレクトリを指定することはできない。

NVR700W は Rev.15.00.17 以降で使用可能。

#### [設定例]

- microSD カードの dpi/signature ディレクトリにシグネチャーを保存する。

```
# external-memory dpi signature directory sd:/dpi/signature
```

#### [適用モデル]

NVR700W

## 第 42 章

### 内蔵無線 WAN 機能

本機能は LTE などの携帯通信網を使ってインターネットに接続するための機能です。

本機能を利用することで、固定回線がない場所でも携帯端末を接続することなくルーター本体のみでインターネット接続が可能になります。

本機能は発信のみに対応し、着信での利用はできません。

内蔵無線 WAN 機能のスペックは以下になります。

|        |                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| 対応キャリア | NTT ドコモ、及び NTT ドコモ回線を使用する MVNO (仮想回線業者)<br>KDDI、及び KDDI 回線を使用する MVNO (仮想回線業者) ※1<br>SoftBank、及び SoftBank 回線を使用する MVNO (仮想回線業者) ※1 |
| 通信方式   | 3G / LTE                                                                                                                          |
| 通信方式選択 | 自動/3G 固定/LTE 固定                                                                                                                   |
| バンド    | LTE Band 1 / 3 / 8(※1) / 11(※1) / 18(※1) / 19 / 21<br>3G Band 1 / 6 / 8(※1) / 9(※1) / 11(※1) / 19                                 |
| 通信速度   | LTE 最大 DL:150Mbps / UL:50Mbps<br>3G 最大 DL:14Mbps / UL:5Mbps                                                                       |

※1 ルーターファームウェアを Rev.15.00.10 以降にし、内蔵無線 WAN モジュールファームウェアを更新することにより対応可能になります。

#### 高額な課金について

データ通信 (パケット通信) の契約が従量制である場合、あるいはデータ通信が定額制の契約の対象外である場合、長時間通信したり大量のデータをやりとりすると高額な料金が発生します。

ご使用にあたっては、通信料金について十分ご注意ください。

通信時間や通信量を、接続毎あるいは累積で監視して警告を出したり接続を制限する機能もあります。必要に応じてご利用ください。

#### 42.1 内蔵無線 WAN モジュールを使用するか否かの設定

##### [書式]

```
wwan-module use use
```

```
no wwan-module use [use]
```

##### [設定値及び初期値]

- use

- [設定値]:

| 設定値 | 説明                   |
|-----|----------------------|
| on  | 内蔵無線 WAN モジュールを使用する  |
| off | 内蔵無線 WAN モジュールを使用しない |

- [初期値]: off

##### [説明]

内蔵無線 WAN モジュールを使うか否かを設定する。on に設定されている時は内蔵無線 WAN モジュールに電源が供給され機能が有効になる。

## [ノート]

本コマンドで内蔵無線 WAN モジュールへの電源供給を設定してから実際にモジュールが使用できる状態になるまで、最大で数十秒掛かる場合があります。

## [適用モデル]

NVR700W

## 42.2 内蔵無線 WAN モジュールの無線通信機能を使うか否かの設定

## [書式]

```
wwan-module radio-power switch
no wwan-module radio-power [switch]
```

## [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                          |
|-----|-----------------------------|
| on  | 内蔵無線 WAN モジュールの無線通信機能を有効にする |
| off | 内蔵無線 WAN モジュールの無線通信機能を無効にする |

- [初期値]: on

## [説明]

内蔵無線 WAN モジュールで無線通信機能を有効にするか否かを設定する。off に設定されている時、内蔵無線 WAN モジュールは電波を出さない。  
本コマンドは **wwan-module use** コマンドにより内蔵無線 WAN モジュールに電源が供給されている場合に有効となる。

## [適用モデル]

NVR700W

## 42.3 電波の受信レベル取得機能の設定

## [書式]

```
wwan-module signal-strength switch [option=value]
no wwan-module signal-strength [...]
```

## [設定値及び初期値]

- *switch*: 電波の受信レベルの取得を許可するか否か
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on
- *option=value*: 取得時のオプション
  - [設定値]:
    - syslog
      - 取得結果を INFO レベルで SYSLOG に出力するか否か

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

| 設定値   | 説明                    |
|-------|-----------------------|
| trans | 圏内、圏外の遷移が発生したときだけ出力する |

- interval
  - 定期的に電波の受信レベルを取得する間隔及び回数
    - 間隔

| 設定値     | 説明        |
|---------|-----------|
| 1..3600 | 秒数        |
| off     | 定期的に取得しない |

- 回数

| 設定値      | 説明  |
|----------|-----|
| 1..1000  | 回数  |
| infinity | 無期限 |

- [初期値]:
  - syslog=on
  - interval=off

#### [説明]

電波の受信レベルを取得する際の諸設定を行う。

**wwan-module signal-strength go** コマンドによる取得では、本コマンドの設定が適用される。

また、interval オプションでは、秒数及び回数をカンマで区切って指定することができる。

interval オプションで秒数及び回数を指定した場合は本コマンド設定後、指定回数に応じて定期的に取得する。

定期的に取得した結果は **show status wwan-module signal-strength** コマンドで確認できる。

なお、データ通信の開始直前と終了直後は本コマンドの設定に関係なく取得される。定期的に電波の受信レベルを取得する場合、SYSLOG オプションに trans を指定していると、電波レベルが圏外から圏内、または圏内から圏外へと遷移したときだけ SYSLOG に出力する。on を指定した場合には、取得した受信レベルを毎回 SYSLOG に出力し、それに加えて、電波レベルが圏外、圏内への遷移が発生したときも出力する。

#### [適用モデル]

NVR700W

## 42.4 電波の受信レベルの取得

#### [書式]

**wwan-module signal-strength go**

#### [説明]

内蔵無線 WAN モジュールの電波の受信レベルを取得する。

#### [適用モデル]

NVR700W

## 42.5 内蔵無線 WAN モジュールに対する詳細な SYSLOG を出力するか否かの設定

#### [書式]

**wwan-module syslog switch**

**no wwan-module syslog [switch]**

#### [設定値及び初期値]

- switch
  - [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | 詳細な SYSLOG を出力する  |
| off | 詳細な SYSLOG を出力しない |

- [初期値]: off



## [説明]

内蔵無線 WAN モジュールに対して発行した AT コマンドを SYSLOG に出力する否かを設定する。併せて **syslog debug on** の設定が必要となる。

## [適用モデル]

NVR700W

## 42.6 内蔵無線 WAN インターフェースの選択

## [書式]

**wwan select num**

**no wwan select**

## [設定値及び初期値]

## • num

- [設定値]:

| 設定値  | 説明                        |
|------|---------------------------|
| 1-30 | 内蔵無線 WAN インターフェース番号       |
| none | 内蔵無線 WAN インターフェース番号を選択しない |

- [初期値]:-

## [説明]

内蔵無線 WAN インターフェースの設定や表示をグループ化する際のインターフェース番号を設定する。以降プロンプトには、**console prompt** コマンドで設定した文字列と番号が続けて表示される。none を指定すると、プロンプトに番号を表示しない。

## [ノート]

この操作コマンドは一般ユーザーでも実行できる。

**no wwan select** コマンドは **wwan select none** コマンドと同じ動作をする。

## [適用モデル]

NVR700W

## 42.7 内蔵無線 WAN インターフェースの使用許可の設定

## [書式]

**wwan enable num**

**no wwan enable num**

## [設定値及び初期値]

## • num

- [設定値]:

| 設定値  | 説明                    |
|------|-----------------------|
| 1-30 | 内蔵無線 WAN インターフェース番号   |
| all  | すべての内蔵無線 WAN インターフェース |

- [初期値]:-

## [説明]

内蔵無線 WAN インターフェースを使用できる状態にする。工場出荷時、すべての内蔵無線 WAN インターフェースは disable 状態なので、使用する場合は必ずこのコマンドで **enable** 状態にしなければならない。

[ノート]

必ず、1. **wwan disable**、2. **disconnect**、3. **wwan** の設定変更、4. **wwan enable**、5. **connect** の手順を踏んで設定を変更する。  
**wwan enable** コマンドを実行すると内部情報の初期化が行われる。

[適用モデル]

NVR700W

## 42.8 内蔵無線 WAN インターフェースの使用不許可の設定

[書式]

**wwan disable num**

[設定値及び初期値]

• *num*

• [設定値]:

| 設定値  | 説明                    |
|------|-----------------------|
| 1-30 | 内蔵無線 WAN インターフェース番号   |
| all  | すべての内蔵無線 WAN インターフェース |

• [初期値]: -

[説明]

内蔵無線 WAN インターフェースを使用できない状態にする。

[適用モデル]

NVR700W

## 42.9 内蔵無線 WAN の常時接続の設定

[書式]

**wwan always-on switch [time]****no wwan always-on**

[設定値及び初期値]

• *switch*

• [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 常時接続する  |
| off | 常時接続しない |

• [初期値]: off

• *time*

• [設定値]: 再接続を要求するまでの秒数 (60..21474836)

• [初期値]: 60

[説明]

内蔵無線 WAN インターフェースについて、常時接続するか否かを設定する。また、常時接続での通信終了時に再接続を要求するまでの時間間隔を指定する。

常時接続に設定されている場合には、起動時に接続を実施し、通信終了時には再接続を行う。接続失敗時あるいは通信の異常終了時には *time* に設定された時間間隔を待った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。*switch* が on に設定されている場合には、*time* の設定が有効となる。*time* が設定されていない場合、*time* は 60 になる。

[適用モデル]

NVR700W

## 42.10 内蔵無線 WAN の発信先アクセスポイントの設定

### [書式]

```
wwan access-point name apn
no wwan access-point name [apn]
```

### [設定値及び初期値]

- *apn*
  - [設定値]: パケット通信に対応したアクセスポイント名 (Access Point Name)
  - [初期値]: -

### [説明]

内蔵無線 WAN インターフェースで使用するアクセスポイント名 (Access Point Name) を設定する。

### [設定例]

```
wwan access-point name mopera.net (mopera U の場合 )
```

### [適用モデル]

NVR700W

## 42.11 内蔵無線 WAN の接続時の認証タイプの設定

### [書式]

```
wwan auth accept [accept]
no wwan auth accept [accept]
```

### [設定値及び初期値]

- *accept*
  - [設定値]:

| 設定値  | 説明              |
|------|-----------------|
| pap  | PAP による認証を指定する  |
| chap | CHAP による認証を指定する |
| none | 認証プロトコルを使わない    |

- [初期値]: none

### [説明]

内蔵無線 WAN インターフェースにおいて、携帯電話通信網への接続時に使用する認証タイプを設定する。

### [適用モデル]

NVR700W

## 42.12 内蔵無線 WAN でのユーザー名とパスワードの設定

### [書式]

```
wwan auth myname myname password
no wwan auth myname [myname password]
```

### [設定値及び初期値]

- *myname*
  - [設定値]: ユーザー名 (64 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (64 文字以内)
  - [初期値]: -

## [説明]

内蔵無線 WAN インターフェースにおいて、携帯電話通信網への接続時に使用するユーザー名とパスワードを設定する。

## [適用モデル]

NVR700W

## 42.13 内蔵無線 WAN からの自動発信設定

## [書式]

**wwan auto connect** *auto*

**no wwan auto connect** [*auto*]

## [設定値及び初期値]

- *auto*

- [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | 内蔵無線 WAN から自動発信する  |
| off | 内蔵無線 WAN から自動発信しない |

- [初期値]: off

## [説明]

内蔵無線 WAN インターフェースにおいて、自動接続するか否かを設定する。

## [適用モデル]

NVR700W

## 42.14 入力がないときに内蔵無線 WAN を切断するタイマの設定

## [書式]

**wwan disconnect input time** *time*

**no wwan disconnect input time** [*time*]

## [設定値及び初期値]

- *time*

- [設定値]:

| 設定値        | 説明          |
|------------|-------------|
| 1-21474836 | 切断までの時間 (秒) |
| off        | タイマを設定しない   |

- [初期値]: 120

## [説明]

内蔵無線 WAN インターフェースにおいて、データ受信がない場合の切断までの時間を設定する。

## [適用モデル]

NVR700W

## 42.15 出力がないときに内蔵無線 WAN を切断するタイマの設定

## [書式]

**wwan disconnect output time** *time*

**no wwan disconnect output time** [*time*]

## [設定値及び初期値]

- *time*

- [設定値]:

| 設定値        | 説明          |
|------------|-------------|
| 1-21474836 | 切断までの時間 (秒) |
| off        | タイマを設定しない   |

- [初期値]: 120

#### [説明]

内蔵無線 WAN インターフェースにおいて、データ送信がない場合の切断までの時間を設定する。

#### [適用モデル]

NVR700W

## 42.16 内蔵無線 WAN を切断するタイマの設定

#### [書式]

**wwan disconnect time** *time*

**no wwan disconnect time** [*time*]

#### [設定値及び初期値]

- *time*

- [設定値]:

| 設定値        | 説明          |
|------------|-------------|
| 1-21474836 | 切断までの時間 (秒) |
| off        | タイマを設定しない   |

- [初期値]: 60

#### [説明]

内蔵無線 WAN インターフェースにおいて、データ送受信がない場合の切断までの時間を設定する。

#### [適用モデル]

NVR700W

## 42.17 内蔵無線 WAN での接続毎パケット通信量制限の設定

#### [書式]

**wwan access limit connection length** *length* [*alert=alert*]

**no wwan access limit connection length** [*length*]

#### [設定値及び初期値]

- *length*

- [設定値]:

| 設定値          | 説明                      |
|--------------|-------------------------|
| 1-2147483647 | 送受信するパケットデータ長の上限值 (バイト) |
| off          | 制限しない                   |

- [初期値]: off

- *alert*

- [設定値]: 警告値 (パケットデータ長あるいは[%]指定)

- [初期値]: -

#### [説明]

内蔵無線 WAN インターフェースにおいて、1 回の接続で送受信するパケットのデータ長の上限值を設定する。上限に達した場合は通信を強制的に切断する。

*alert* を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

*length*、*alert* パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。

## [ノート]

内蔵無線 WAN モジュールのパケット通信は 128 バイトごとに課金されるが、ルーターと内蔵無線 WAN モジュール間で送受信されるデータが 128 バイト単位である保証はない。例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

したがって、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

[適用モデル]  
NVR700W

## 42.18 内蔵無線 WAN での接続毎パケット通信時間制限の設定

## [書式]

```
wwan access limit connection time time [alert=alert]
```

```
no wwan access limit connection time [time]
```

## [設定値及び初期値]

• *time*

- [設定値]:

| 設定値          | 説明           |
|--------------|--------------|
| 1-2147483647 | 通信時間の上限値 (秒) |
| off          | タイマを設定しない    |

- [初期値]: off

• *alert*

- [設定値]: 警告値 (秒数あるいは[%]指定)
- [初期値]: -

## [説明]

内蔵無線 WAN インターフェースにおいて、1 回の接続の通信時間の上限値を設定する。上限に達した場合は通信を強制的に切断する。

本コマンドは **wwan disconnect time** コマンドとは独立して動作する。

*alert* を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[適用モデル]  
NVR700W

## 42.19 内蔵無線 WAN での通信制限の累積期間の設定

## [書式]

```
wwan access limit duration duration
```

```
no wwan access limit duration [duration]
```

## [設定値及び初期値]

• *duration*

- [設定値]:

| 設定値       | 説明              |
|-----------|-----------------|
| 1-2592000 | 通信制限の累積対象期間 (秒) |
| off       | 過去の全期間を対象とする    |

- [初期値]: off

## [説明]

内蔵無線 WAN インターフェースにおいて累積通信時間や累積データ長に基づく通信制限を行う場合に、本コマンドにより累積期間を設定する。

[適用モデル]  
NVR700W

## 42.20 内蔵無線 WAN でのパケット通信量制限の設定

### [書式]

**wwan access limit length** *length* [*alert*=*alert*[,*alert\_cancel*]]

**no wwan access limit length** [*length*]

### [設定値及び初期値]

#### • *length*

- [設定値]:

| 設定値          | 説明                        |
|--------------|---------------------------|
| 1-2147483647 | 送受信する累積パケットデータ長の上限值 (バイト) |
| off          | 制限しない                     |

- [初期値]: 50M

#### • *alert*

- [設定値]: 警告値 (データ長あるいは[%]指定)

- [初期値]: -

#### • *alert\_cancel*

- [設定値]: 警告解除値 (データ長あるいは[%]指定)

- [初期値]: -

### [説明]

内蔵無線 WAN インターフェースにおいて、送受信するパケットの累積データ長の上限值を設定する。

上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。

*length*、*alert* および *alert\_cancel* パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。

累積値は、

- **clear wwan access limitation** コマンドの発行
- **wwan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status wwan** コマンドで、現在までの累積パケットデータ長を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wwan access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が 0 になるまで警告を解除しない。

### [ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。内蔵無線 WAN モジュールのパケット通信は 128 バイトごとに課金されるが、ルーターと内蔵無線 WAN モジュール間で送受信されるデータが 128 バイト単位である保証はない。

例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

したがって、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

off を設定したときは警告が表示される。

[適用モデル]  
NVR700W

## 42.21 内蔵無線 WAN でのパケット通信時間制限の設定

### [書式]

**wwan access limit time** *time* [alert=*alert*[,*alert\_cancel*]] [unit=*unit*]

**no wwan access limit time** [*time*]

### [設定値及び初期値]

- *time*

- [設定値]:

| 設定値          | 説明             |
|--------------|----------------|
| 1-2147483647 | 累積通信時間の上限値 (秒) |
| off          | タイマを設定しない      |

- [初期値]: 3600

- *alert*

- [設定値]: 警告値 (秒数あるいは[%]指定)

- [初期値]: -

- *alert\_cancel*

- [設定値]: 警告解除値 (秒数あるいは[%]指定)

- [初期値]: -

- *unit*

- [設定値]: 単位 (second または minute)

- [初期値]: second

### [説明]

内蔵無線 WAN インターフェースにおいて、累積時間の上限値を設定する。上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。本コマンドは **wwan disconnect time** コマンドとは独立して動作する。

累積値は、

- **clear wwan access limitation** コマンドの発行
- **wwan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status wwan** コマンドで、現在までの累積通信時間を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wwan access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

累積通信時間が警告値に達している間は再接続できない。警告解除値を下回ると再接続できる。

警告解除値を指定しない場合は、期間累積の接続時間が 0 になるまで警告を解除しない。

*unit* で minute を指定すると、接続時間を分単位で算出する。秒単位は切り上げられる。

### [ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

**wwan access limit duration** が設定されている場合、*unit=minute* を指定しても、期間内累積時間は、秒単位で加算される。

off を設定したときは警告が表示される。

### [適用モデル]

NVR700W

## 42.22 内蔵無線 WAN で使用する通信方式とバンドの設定

### [書式]

**wwan radio access technology** *rat* [3g=3g\_*band*[,*3g\_band*...]] [lte=lte\_*band*[,*lte\_band*...]]



**no wwan radio access technology [rat]****[設定値及び初期値]**• *rat*

- [設定値]:

| 設定値  | 説明                    |
|------|-----------------------|
| auto | 通信方式を 3G/LTE の自動選択に設定 |
| 3g   | 通信方式を 3G に固定          |
| lte  | 通信方式を LTE に固定         |

- [初期値]: auto

• *3g\_band*

- [設定値]:

| 設定値    | 説明        |
|--------|-----------|
| 1,6,19 | 3G のバンド番号 |

- [初期値]: 1,6,19

• *lte\_band*

- [設定値]:

| 設定値       | 説明         |
|-----------|------------|
| 1,3,19,21 | LTE のバンド番号 |

- [初期値]: 1,3,19,21

**[説明]**

内蔵無線 WAN で使用する通信方式(RAT)とバンドを設定する。バンドは設定したいバンド番号をコンマ区切りで指定する。通信方式のみ指定した場合、バンド設定には指定した通信方式のバンド番号の初期値が設定される。通信方式を auto にし、かつバンド設定も行う場合、3G\_BAND, LTE\_BAND のそれぞれに少なくとも 1 つ以上のバンドを指定しなければならない。

**[ノート]**

本コマンドで設定を変更する場合、網に接続していない状態で変更することを推奨する。網に接続した状態で設定を変更した場合、網と切断されることがある。

通信方式を 3G に固定した場合、通信事業者によっては接続できない場合がある。

本コマンドは Rev.15.00.03 以降のファームウェアで使用可能。

**[適用モデル]**

NVR700W

**42.23 内蔵無線 WAN に入力する PIN コードの設定****[書式]**

**wwan pin code** *pin*

**no wwan pin code** [*pin*]

**[設定値及び初期値]**• *pin*

- [設定値]: PIN コード
- [初期値]: -

**[説明]**

内蔵無線 WAN で使用する SIM カードに PIN コードが必要な場合に本コマンドで設定する。PIN コード認証を行うか否かは **enable wwan pin-auth**, **disable wwan pin-auth** コマンドで設定する。

## [ノート]

SIM カードに登録された PIN コードと本コマンドの設定が一致せず 3 回連続して失敗すると、自動的に PIN ロック状態になる。

PIN ロックの解除は **unlock wwan pin-code** コマンドで可能。

## [適用モデル]

NVR700W

## 42.24 内蔵無線 WAN の PIN 認証を有効にする

---

## [書式]

**enable wwan pin-auth**

## [説明]

SIM カードの PIN コード認証を有効にする。PIN コード認証を有効にする時に、PIN コードの入力が必要となる。PIN コード認証を有効にした場合は、**wwan pin code** コマンドを設定する必要がある。設定しない場合は次回の PIN コード認証でエラーとなる。

## [ノート]

PIN コードの入力を 3 回連続で間違えると、自動的に PIN ロック状態になる。

PIN ロックの解除は **unlock wwan pin-code** コマンドで可能。

## [設定例]

PIN コード "0000" の場合

```
#enable wwan pin-auth
pin code:0000
PIN コード認証を有効にしました
```

## [適用モデル]

NVR700W

## 42.25 内蔵無線 WAN の PIN 認証を無効にする

---

## [書式]

**disable wwan pin-auth**

## [説明]

SIM カードの PIN コード認証を無効にする。PIN コード認証を無効にする時に、PIN コードの入力が必要となる。

PIN コード認証を無効にした場合は、**wwan pin code** コマンドの設定は不要になる。

## [ノート]

PIN コードの入力を 3 回連続で間違えると、自動的に PIN ロック状態になる。

PIN ロックの解除は **unlock wwan pin-code** コマンドで可能。

## [設定例]

PIN コード "0000" の場合

```
#disable wwan pin-auth
pin code:0000
PIN コード認証を無効にしました
```

## [適用モデル]

NVR700W

## 42.26 内蔵無線 WAN モジュールで使用する PIN コードの変更

---

### [書式]

```
change wwan pin-code
```

### [説明]

SIM カードに設定されている PIN コードを変更する。PIN コードを変更する時に、旧 PIN コードと新 PIN コードの入力が必要となる。

PIN コードを変更した場合は、**wwan pin code** コマンドに反映する必要がある。反映しない場合は次回の PIN コード認証でエラーとなる。

### [ノート]

PIN コードを変更する場合は、PIN コード認証が有効状態の SIM のみ変更可能。

PIN コードの入力を 3 回連続で間違えると、自動的に PIN ロック状態になる。

PIN ロックの解除は **unlock wwan pin-code** コマンドで可能。

### [設定例]

旧 PIN コード "0000" を新 PIN コード "1234" に変更する場合

```
#change wwan pin-code
Old pin code:0000
New pin code:1234
SIM カード上の PIN コードを New pin code に変更しても良いですか? (Y/N)Y
PIN コードを変更しました
```

### [適用モデル]

NVR700W

## 42.27 内蔵無線 WAN モジュールの PIN ロック解除コードの入力

---

### [書式]

```
unlock wwan pin-code
```

### [説明]

PIN ロック状態を解除する。PIN ロック状態を解除する時に、PIN ロック解除コードと新 PIN コードの入力が必要となる。

入力した新 PIN コードは、**wwan pin code** コマンドに反映する必要がある。反映しない場合は次回の PIN コード認証でエラーとなる。

### [ノート]

PIN ロック解除コードの入力を 10 回連続で間違えると、完全にロック状態になる。

完全ロック状態になった場合は、使用できなくなるため注意が必要である。

### [設定例]

PIN ロック解除コード "12345678"、新 PIN コード "0000" の場合

```
#unlock wwan pin-code
Pin unlock code:12345678
New pin code:0000
SIM カード上の PIN コードを New pin code に変更しても良いですか? (Y/N)Y
PIN ロック解除に成功しました
```

### [適用モデル]

NVR700W

## 42.28 指定した相手に対して発信制限を解除する

---

### [書式]

```
clear wwan access limitation [num]
```

## [設定値及び初期値]

- *num*

- [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| 1～30 | 内蔵無線 WAN インターフェース番号 |
| 省略   | 省略時は現在選択している番号      |

- [初期値]: -

## [説明]

**wwan access limit** コマンドによって発信制限がかかったインターフェースに対し、制限を解除して再び発信できるようにする。  
なお、電源の再投入でも発信制限は解除される。

## [適用モデル]

NVR700W

## 42.29 定期実行で取得した電波の受信レベルの表示

## [書式]

```
show status wwan-module signal-strength [reverse]
```

## [設定値及び初期値]

- *reverse* : 取得時刻の新しいものから順に結果を表示する

- [初期値]: -

## [説明]

**wwan-module signal-strength** コマンドの設定で定期的に電波の受信レベルを取得した場合、取得結果を最大 256 件表示する。256 件を超えた場合は古い情報から削除される。  
このコマンドでは、通常は取得時刻の古いものから順に結果を表示するが、*reverse* を指定することで新しいものから表示させることができる。

## [適用モデル]

NVR700W

## 42.30 外部メモリから内蔵無線 WAN モジュールのファームウェアを更新する

## [書式]

```
update wwan-module firmware firmware
```

## [設定値及び初期値]

- *firmware*

- [設定値]:

| 設定値                  | 説明                                                 |
|----------------------|----------------------------------------------------|
| <i>usb1:filename</i> | USB メモリ内の内蔵無線 WAN モジュールファームウェアファイル名                |
| <i>sd1:filename</i>  | microSD カード内の内蔵無線 WAN モジュールファームウェアファイル名            |
| <i>*:filename</i>    | USB メモリおよび microSD カード内の内蔵無線 WAN モジュールファームウェアファイル名 |

- [初期値]: -

## [説明]

外部メモリから内蔵無線 WAN モジュールのファームウェアを更新する。外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。  
*filename* は絶対パスを使ってファイルを指定するかファイル名のみを指定する。*filename* にファイル名のみを指定

した場合は外部メモリ内から自動検索する。複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。コマンド実行後、ルーターは再起動する。

#### [ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

本コマンドは Rev.15.00.10 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 42.31 HTTP を利用した内蔵無線 WAN モジュールファームウェアのチェックおよび更新の実行

#### [書式]

**http wwan-module-up go**

#### [説明]

WEB サーバーに置いている内蔵無線 WAN モジュールファームウェアと現在動作中の内蔵無線 WAN モジュールファームウェアの対応キャリア及びバージョンをチェックし、書き換え可能であればファームウェアのバージョンアップを行う。書き換え可能なバージョンのファームウェアが存在すると、「更新しますか? (Y/N)」という確認を求めてくるので、更新する場合は "Y" を、更新しない場合は "N" を入力する必要がある。 **http wwan-module-up permit** コマンドで HTTP を利用した更新が許可されていない時は、ファームウェアの書き換えは行わない。なお、WEB サーバーに置いてあるファームウェアが以下の条件の時は、ファームウェアの書き換えは行わない。

- 現在使用中のファームウェアと同一キャリア、同一バージョンの時。

#### [ノート]

本コマンドは Rev.15.00.10 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 42.32 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新用 URL の設定

#### [書式]

**http wwan-module-up url url**

**no http wwan-module-up url [url]**

#### [設定値及び初期値]

- *url*
  - [設定値]: ファームウェアが置いてある URL を設定する
  - [初期値]: [http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan\\_nvr700w\\_mc.fly](http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan_nvr700w_mc.fly) (マルチキャリア向けファームウェア)

#### [説明]

内蔵無線 WAN モジュールファームウェアが置いてある URL を設定する。入力形式は“http://サーバーの IP アドレスあるいはホスト名/パス名”という形式となる。サーバーのポート番号が 80 以外の場合は、“http://サーバーの IP アドレスあるいはホスト名:ポート番号/パス名”という形式で、URL の中に指定する必要がある。

#### [ノート]

NTT ドコモ向けの内蔵無線 WAN モジュールファームウェアに更新する際は以下の URL を指定する。

- [http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan\\_nvr700w\\_dc.fly](http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan_nvr700w_dc.fly) (NTT ドコモ 及び その MVNO 事業者向けファームウェア)

NTT ドコモ、KDDI、SoftBank の全てのキャリアに対応した内蔵無線 WAN モジュールファームウェアに更新する際は以下の URL を指定する。

- [http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan\\_nvr700w\\_mc.fly](http://www.rtpro.yamaha.co.jp/firmware/wwan-module/wwan_nvr700w_mc.fly) (マルチキャリア向けファームウェア)  
本コマンドは Rev.15.00.10 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 42.33 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新を許可するか否かの設定

[書式]

```
http wwan-module-up permit permit
no http wwan-module-up permit [permit]
```

[設定値及び初期値]

- *permit*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

[説明]

HTTP を利用した内蔵無線 WAN モジュールファームウェア更新を許可するか否かを設定する。

[ノート]

このコマンドの設定は、コマンドによる直接の更新、Web GUI からの更新に影響する。

本コマンドは Rev.15.00.10 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 42.34 HTTP を利用した内蔵無線 WAN モジュールファームウェア更新のタイムアウトの設定

[書式]

```
http wwan-module-up timeout time
no http wwan-module-up timeout [time]
```

[設定値及び初期値]

- *time*
  - [設定値]: タイムアウトするまでの秒数 (1..180)
  - [初期値]: 30

[説明]

HTTP を利用した内蔵無線 WAN モジュールファームウェア更新のタイムアウト時間を設定する。

[ノート]

本コマンドは Rev.15.00.10 以降のファームウェアで使用可能。

[適用モデル]  
NVR700W

## 第 43 章

### モバイルインターネット接続機能

携帯端末をルーター本体に接続し、携帯端末から発信してインターネット接続する機能です。固定回線がなくても本機能に対応した携帯端末があればインターネット接続をすることができます。本機能は発信のみに対応し、着信での利用はできません。

現時点で対応する携帯端末は USB で接続するものだけとなります。この場合、携帯端末を PP(USB モデム)として制御、又は WAN(ネットワークアダプタ)として制御することになります。本機能をご利用になるには以下の機材等が必要になります。

- 対応ルーター
- 対応携帯端末
- 対応携帯端末のデータ通信に必要なプロバイダー契約 (mopera U 等)

本機能ではパケット通信量およびパケット通信時間の制限が初期値として設定されています。これら上限値に達した場合、通信を強制的に切断し、その後発信できなくなります。発信を許可するためには **clear mobile access limitation** コマンドを発行するか、ルーター本体を再起動します。これらの上限値は、PP(USB モデム)として制御する場合には **mobile access limit length** および **mobile access limit time** コマンドで、WAN(ネットワークアダプタ)として制御する場合には **wan access limit time** および **wan access limit length** コマンドで変更することができます。

#### 43.1 携帯端末を使用するか否かの設定

##### [書式]

**mobile use interface use** [first-connect-wait-time=time]

**no mobile use interface** [use]

##### [設定値及び初期値]

- *interface*
- [設定値]:

| 設定値  | 説明                       |
|------|--------------------------|
| usb1 | USB ポートをモバイルインターネット接続に使用 |

- [初期値]: -
- *use*

- [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | 携帯端末を使用する  |
| off | 携帯端末を使用しない |

- [初期値]: off
- *time*

- [設定値]:

| 設定値   | 説明               |
|-------|------------------|
| 0-300 | 携帯端末アタッチ後の発信抑制秒数 |

- [初期値]: 0

##### [説明]

指定のバスに接続された携帯端末をインターネット接続に使用するか否かを設定する。

first-connect-wait-time オプションは、携帯端末のアタッチ後の発信抑制時間を設定し、網への接続を抑制する。

**mobile auto connect** コマンドや、**wan1 auto connect** コマンド、**pp always-on** コマンド、**wan1 always-on** コマンドで

on が設定されている場合の 網への接続要求も、このコマンドで設定された発信抑制秒数のあいだは、発信が抑制される。

**[適用モデル]**

NVR700W, NVR510

## 43.2 携帯端末に入力する PIN コードの設定

**[書式]**

**mobile pin code interface pin**

**no mobile pin code interface [pin]**

**[設定値及び初期値]**

- *interface*

- [設定値]:

| 設定値  | 説明       |
|------|----------|
| usb1 | USB1 ポート |

- [初期値]: -

- *pin*

- [設定値]: PIN コード

- [初期値]: -

**[説明]**

USB インターフェースに接続する携帯端末の使用に PIN コードを必要とする場合に、用いる PIN コードを設定する。携帯端末が PIN コードを必要としない場合には、本コマンドの設定に関係なく携帯端末を使用することができる。

**[ノート]**

PIN コードを利用する場合は、予め携帯端末の接続ユーティリティ等を使用して SIM カードに PIN コードを登録する必要がある。ルーターでは SIM カードに PIN コードを登録することはできない。

SIM カードに登録された PIN コードと本コマンドの設定が一致せず、3 回連続して失敗すると、携帯端末は自動的にロック (PIN ロック) される。PIN ロックがかかるとルーターでは解除できない。携帯端末の接続ユーティリティにて PIN ロック解除コードを入力する必要がある。

**[適用モデル]**

NVR700W, NVR510

## 43.3 モバイルインターネット接続機能の発信方式の設定

**[書式]**

**mobile call type type**

**no mobile call type [type]**

**[設定値及び初期値]**

- *type*

- [設定値]:

| 設定値 | 説明     |
|-----|--------|
| 1   | 発信方式 1 |
| 2   | 発信方式 2 |

- [初期値]: 1

**[説明]**

モバイルインターネット接続機能で、発信動作を行うときの方式を設定する。

**[ノート]**

モバイルインターネット接続機能で接続失敗する場合、本コマンドの設定値を変更することにより接続できるようになる可能性がある。



NVR700W は Rev.15.00.16 以降で使用可能。  
NVR510 は Rev.15.01.15 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 43.4 携帯端末または内蔵無線 WAN モジュールに直接コマンドを発行する

### [書式]

```
execute at-command interface command
```

### [設定値及び初期値]

- *interface*
  - [設定値]:
    - usb1
    - wwan-module
  - [初期値]: -
- *command*
  - [設定値]:
    - AT コマンド
  - [初期値]: -

### [説明]

指定したインターフェースに接続された携帯端末または、内蔵無線 WAN モジュールに対して、AT コマンドを直接発行する。

以下のコマンドも同様に AT コマンドを発行するので、本コマンドと併用するときは注意が必要である。

**usbhost modem initialize**

### [ノート]

特別な理由がない限り本コマンドを使用する必要はない。  
wwan-module 指定は NVR700W で指定可能。

### [設定例]

```
execute at-command usb1 AT+CGDCONT=<1>,"IP","mopera.net"
ダブルクォート (") を指定するときは\" のように\"を付加する必要がある。
```

[適用モデル]  
NVR700W, NVR510

## 43.5 指定した相手に対して発信制限を解除する

### [書式]

```
clear mobile access limitation [interface]
clear mobile access limitation pp [peer_num]
```

### [設定値及び初期値]

- *interface*
    - [設定値]:
- | 設定値  | 説明           |
|------|--------------|
| usb1 | USB ポート      |
| wan1 | WAN インターフェース |
- [初期値]: -
  - *peer\_num*
    - [設定値]:

| 設定値   | 説明              |
|-------|-----------------|
| 1..30 | 相手先情報番号         |
| 省略    | 省略時は現在選択している相手先 |

- [初期値]:-

#### [説明]

**mobile access limit** コマンドによって発信制限がかかったインターフェースに対し、制限を解除して再び発信できるようにする。

なお、電源の再投入でも発信制限は解除される。

#### [適用モデル]

NVR700W, NVR510

## 43.6 PP で使用するインターフェースの設定

#### [書式]

**pp bind interface**

**no pp bind [interface]**

#### [設定値及び初期値]

- *interface*

- [設定値]:

| 設定値  | 説明         |
|------|------------|
| usb1 | usb1 を使用する |

- [初期値]:-

#### [説明]

選択されている相手について使用するインターフェースを設定する。

#### [適用モデル]

NVR700W, NVR510

## 43.7 携帯端末からの自動発信設定

#### [書式]

**mobile auto connect auto**

**no mobile auto connect [auto]**

#### [設定値及び初期値]

- *auto*

- [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | 携帯端末から自動発信する  |
| off | 携帯端末から自動発信しない |

- [初期値]: off

#### [説明]

選択されている相手について自動接続するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

## 43.8 携帯端末を切断するタイマの設定

#### [書式]

**mobile disconnect time time**

**no mobile disconnect time** [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 60

[説明]

選択されている相手について PP 側の送受信がない場合の切断までの時間を設定する。

[適用モデル]

NVR700W, NVR510

## 43.9 携帯端末を入力がないときに切断するタイマの設定

[書式]

**mobile disconnect input time** *time*

**no mobile disconnect input time** [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 120

[説明]

選択されている相手について PP 側からデータ受信がない場合の切断までの時間を設定する。

[適用モデル]

NVR700W, NVR510

## 43.10 携帯端末を出力がないときに切断するタイマの設定

[書式]

**mobile disconnect output time** *time*

**no mobile disconnect output time** [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 120

[説明]

選択されている相手について PP 側へのデータ送信がない場合の切断までの時間を設定する。

[適用モデル]

NVR700W, NVR510

## 43.11 発信先アクセスポイントの設定

### [書式]

**mobile access-point name** *apn* *cid=cid* [*pdp=type*]

**no mobile access-point name** [*apn cid=cid*]

### [設定値及び初期値]

- *apn*
  - [設定値]: パケット通信に対応したアクセスポイント名 (Access Point Name)
  - [初期値]: -
- *cid*
  - [設定値]:

| 設定値  | 説明     |
|------|--------|
| 1-10 | CID 番号 |

- [初期値]: -
- *type*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| ppp | PDP type を PPP とする |
| ip  | PDP type を IP とする  |

- [初期値]: -

### [説明]

選択されている相手についてアクセスポイント名 (APN) と CID 番号、PDP タイプの割り当てを設定する。なお *pdp=type* を省略すると、通常は *ip* となる。

### [設定例]

```
mobile access-point name mopera.net cid=3 (mopera U の場合 )
```

### [適用モデル]

NVR700W, NVR510

## 43.12 携帯端末に指示する発信先の設定

### [書式]

**mobile dial number** *dial\_string*

**no mobile dial number** [*dial\_string*]

### [設定値及び初期値]

- *dial\_string*
  - [設定値]: 発信先を指定する文字列
  - [初期値]: -

### [説明]

選択されている相手について、携帯端末に ATD に続いて発行する発信先を設定する。

### [ノート]

設定がない場合、**mobile access-point name** コマンドで設定された *cid* 番号 [CID] を使って「ATD\*99\*\*\*[CID]#」を発行する。

### [適用モデル]

NVR700W, NVR510

## 43.13 パケット通信量制限の設定

### [書式]

**mobile access limit length** *length* [*alert=alert* [, *alert\_cancel*]]

**no mobile access limit length** [*length*]

[設定値及び初期値]

- *length*
  - [設定値]:

| 設定値          | 説明                       |
|--------------|--------------------------|
| 1-2147483647 | バイト数、送受信する累積パケットデータ長の上限值 |
| off          | 制限しない                    |

- [初期値]: 50M
- *alert*
  - [設定値]: 警告値、データ長あるいは[%]指定
  - [初期値]: -
- *alert\_cancel*
  - [設定値]: 警告解除値、データ長あるいは[%]指定
  - [初期値]: -

[説明]

選択されている相手について、送受信するパケットの累積データ長の上限值を設定する。

上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。

*length*、*alert* および *alert\_cancel* パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **mobile access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status pp** コマンドで、現在までの累積パケットデータ長を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **mobile access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が 0 になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。

例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

off を設定したときは警告が表示される。

[適用モデル]

NVR700W, NVR510

## 43.14 パケット通信時間制限の設定

[書式]

**mobile access limit time** *time* [*alert*=*alert*[,*alert\_cancel*]] [*unit*=*unit*]

**no mobile access limit time** [*time*]

[設定値及び初期値]

- *time*

- [設定値]:

| 設定値          | 説明         |
|--------------|------------|
| 1-2147483647 | 累積通信秒数の上限値 |
| off          | タイマを設定しない  |

- [初期値]: 3600
- *alert*
  - [設定値]: 警告値、秒数あるいは[%]指定
  - [初期値]: -
- *alert\_cancel*
  - [設定値]: 警告解除値、秒数あるいは[%]指定
  - [初期値]: -
- *unit*
  - [設定値]: 単位、second 又は minute
  - [初期値]: second

#### [説明]

選択されている相手について、累積通信時間の上限値を設定する。  
上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。  
本コマンドは **mobile disconnect time** コマンドとは独立して動作する。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **mobile access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status pp** コマンドで、現在までの累積通信時間を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **mobile access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

累積通信時間が警告値に達している間は再接続できない。警告解除値を下回ると再接続できる。

警告解除値を指定しない場合は、期間累積の接続時間が 0 になるまで警告を解除しない。

*unit* で minute を指定すると、接続時間を分単位で算出する。秒単位は切り上げられる。

#### [ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

**mobile access limit duration** が設定されている場合、*unit=minute* を指定しても、期間内累積時間は、秒単位で加算される。

off を設定したときは警告が表示される。

#### [適用モデル]

NVR700W, NVR510

## 43.15 同じ発信先に対して連続して認証に失敗できる回数の設定

#### [書式]

**mobile call prohibit auth-error count** *count*

**no mobile call prohibit auth-error count** [*count*]

#### [設定値及び初期値]

- *count*
  - [設定値]:

| 設定値        | 説明             |
|------------|----------------|
| 1-21474836 | 連続して認証に失敗できる回数 |
| off        | 発信制限をかけない      |

- [初期値]: 5

**[説明]**

選択された相手に対して連続して認証に失敗できる回数を指定する。ここで設定した回数だけ連続して認証に失敗した場合、その後は、その発信先に発信しない。

なお、以下のコマンドを実行すると、再び発信が可能となる。

**pp auth accept / pp auth request / pp auth myname / pp auth username / no pp auth accept / no pp auth request / no pp auth myname / no pp auth username**

また、電源の再投入でも発信制限は解除される。

**[適用モデル]**

NVR700W, NVR510

### 43.16 LCP の Async Control Character Map オプション使用の設定

**[書式]**

**ppp lcp accm *accm***  
**no ppp lcp accm [*accm*]**

**[設定値及び初期値]**

- *accm*
- [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 用いる  |
| off | 用いない |

- [初期値]: off

**[説明]**

選択された相手に対して[PPP,LCP]の Async-Control-Character-Map オプションを用いるか否かを設定する。これを設定することで通信量を減らせることがある。本設定はモバイルインターネット接続機能でのみ有効である。

**[ノート]**

on を設定しても相手に拒否された場合は用いない。また、Async-Control-Character-Map の値は、自分から送出する場合も相手から受信する場合も 0x00000000 のみが用いられる。

**[適用モデル]**

NVR700W, NVR510

### 43.17 発信者番号通知 (186) を付加するかどうかの設定

**[書式]**

**mobile display caller id *switch***  
**no mobile display caller id [*switch*]**

**[設定値及び初期値]**

- *switch*
- [設定値]:

| 設定値 | 説明                          |
|-----|-----------------------------|
| on  | 発信者番号を通知する (186 を付加して発信する)  |
| off | 発信者番号を通知しない (186 を付加せず発信する) |

- [初期値]: off

#### [説明]

選択された相手に対して、発信時に 186 を付けて発信者番号を通知するかどうかを設定する。

#### [適用モデル]

NVR700W, NVR510

## 43.18 詳細な SYSLOG を出力するか否かの設定

#### [書式]

**mobile syslog switch**

**no mobile syslog** [*switch*]

#### [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値 | 説明                |
|-----|-------------------|
| on  | 詳細な SYSLOG を出力する  |
| off | 詳細な SYSLOG を出力しない |

- [初期値]: off

#### [説明]

携帯端末に対して発行した AT コマンドを SYSLOG として詳細に出力するかどうかを指定する。モバイルインターネット接続として発信動作に入ってからのもので記録され、発信動作前のもは記録されない。FOMA リモートセットアップ時も記録されない。併せて **syslog debug on** の設定が必要となる。

#### [適用モデル]

NVR700W, NVR510

## 43.19 接続毎パケット通信量制限の設定

#### [書式]

**mobile access limit connection length length** [*alert=alert*]

**no mobile access limit connection length** [*length*]

#### [設定値及び初期値]

- *length*
  - [設定値]:

| 設定値          | 説明                     |
|--------------|------------------------|
| 1-2147483647 | バイト数、送受信するパケットデータ長の上限值 |
| off          | 制限しない                  |

- [初期値]: off
- *alert*
  - [設定値]: 警告値、データ長あるいは[%]指定
  - [初期値]: -

#### [説明]

選択されている相手について、1 回の接続で送受信するパケットのデータ長の上限值を設定する。上限に達した場合は通信を強制的に切断する。

*alert* を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

*length*、*alert* パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。



## [ノート]

携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。

例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

## [適用モデル]

NVR700W, NVR510

## 43.20 接続毎パケット通信時間制限の設定

## [書式]

**mobile access limit connection time** *time* [alert=*alert*]

**no mobile access limit connection time** [*time*]

## [設定値及び初期値]

- *time*

- [設定値]:

| 設定値          | 説明          |
|--------------|-------------|
| 1-2147483647 | 秒数、通信秒数の上限値 |
| off          | タイマを設定しない   |

- [初期値]: off

- *alert*

- [設定値]: 警告値、秒数あるいは[%]指定
- [初期値]: -

## [説明]

選択されている相手について、1 回の接続の通信時間の上限値を設定する。

上限に達した場合は通信を強制的に切断する。

本コマンドは **mobile disconnect time** コマンドとは独立して動作する。

*alert* を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

## [適用モデル]

NVR700W, NVR510

## 43.21 通信制限の累積期間の設定

## [書式]

**mobile access limit duration** *duration*

**no mobile access limit duration** [*duration*]

## [設定値及び初期値]

- *duration*

- [設定値]:

| 設定値       | 説明                 |
|-----------|--------------------|
| 1-2592000 | 秒数、通信制限の累積対象の過去の期間 |
| off       | 過去の全期間を対象とする       |

- [初期値]: off

## [説明]

選択されている相手について、通信制限を行う場合に累積対象となる過去の期間を設定する。

[適用モデル]  
NVR700W, NVR510

## 43.22 携帯端末でパケット着信機能を使用するか否かの設定

### [書式]

**mobile arrive use interface use**  
**no mobile arrive use interface [use]**

### [設定値及び初期値]

#### • interface

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| usb1 | USB1 インターフェース |

- [初期値]: -

#### • use

- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | 携帯端末でパケット着信機能を使用する  |
| off | 携帯端末でパケット着信機能を使用しない |

- [初期値]: -

### [説明]

指定したインターフェースに接続された携帯端末でモバイルインターネット接続のパケット着信機能を使用するか否かを設定する。

### [ノート]

パケット着信機能に対応している携帯端末を使用する場合は、本コマンドを **on** か **off** に必ず設定してください。本コマンドが設定されていない場合は、アタッチされた時点における携帯端末本体のパケット着信機能の設定値が使用されます。

パケット着信機能の詳細は携帯端末の取扱説明書などを参照のこと。

また、パケット着信機能を使用することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/>

[適用モデル]  
NVR700W, NVR510

## 43.23 モバイルインターネット機能の着信許可の設定

### [書式]

**mobile arrive permit arrive**  
**no mobile arrive permit [arrive]**

### [設定値及び初期値]

#### • arrive

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: off

[説明]

モバイルインターネット機能で、相手からの着信を許可するか否かを設定する。  
on に設定すると、相手からのパケット着信を受けたときに自動接続されるようになる。

[適用モデル]

NVR700W, NVR510

### 43.24 電波の受信レベルの取得

[書式]

**mobile signal-strength go**

[説明]

電波の受信レベルを取得する。

[適用モデル]

NVR700W, NVR510

### 43.25 電波の受信レベル取得機能の設定

[書式]

**mobile signal-strength switch** [option=value]

**no mobile signal-strength** [...]

[設定値及び初期値]

- switch : 電波の受信レベルの取得を許可するか否か

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 許可する  |
| off | 許可しない |

- [初期値]: on

- option=value : 取得時のオプション

- [設定値]:

- interface

- 電波の受信レベルを取得するインターフェース

| 設定値  | 説明      |
|------|---------|
| usb1 | USB ポート |

- syslog

- 取得結果を INFO レベルで SYSLOG に出力するか否か

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

- interval

- 定期的に電波の受信レベルを取得する間隔及び回数

- 間隔

| 設定値     | 説明        |
|---------|-----------|
| 1..3600 | 秒数        |
| off     | 定期的に取得しない |

- 回数

| 設定値      | 説明  |
|----------|-----|
| 1..1000  | 回数  |
| infinity | 無期限 |

- [初期値]:
  - interface=usb1
  - syslog=on
  - interval=off

#### [説明]

電波の受信レベルを取得する際の諸設定を行う。

**mobile signal-strength go** コマンドや DOWNLOAD ボタンの押下による取得では、本コマンドの設定が適用される。また、interval オプションでは、秒数及び回数をカンマで区切って指定することができる。

interval オプションで秒数及び回数を指定した場合は本コマンド設定後、指定回数に応じて定期的に取得する。

定期的に取得した結果は **show status mobile signal-strength** コマンドで確認できる。

なお、データ通信の開始直前と終了直後は本コマンドの設定に関係なく取得される。

#### [ノート]

一部の携帯端末では、「網に接続しているとき」あるいは「網から切断されているとき」のみ電波の受信レベルが取得できるものがある。

#### [適用モデル]

NVR700W, NVR510

## 43.26 定期実行で取得した電波の受信レベルの表示

#### [書式]

```
show status mobile signal-strength [reverse]
```

#### [設定値及び初期値]

- reverse : 取得時刻の新しいものから順に結果を表示する
  - [初期値]: -

#### [説明]

**mobile signal-strength** コマンドの設定で定期的に電波の受信レベルを取得した場合、取得結果を最大 256 件表示する。256 件を超えた場合は古い情報から削除される。

このコマンドでは、通常は取得時刻の古いものから順に結果を表示するが、

reverse を指定することで新しいものから表示させることができる。

#### [ノート]

携帯端末が接続されている状態で USB ボタンを 2 秒以上押し続け、端末とルーターの接続を解除すると、この履歴はクリアされる。

#### [適用モデル]

NVR700W, NVR510

## 43.27 USB ポートに接続した機器の初期化に使う AT コマンドの設定

#### [書式]

```
usbhost modem initialize interface command [command_list]
```

```
no usbhost modem initialize interface
```

#### [設定値及び初期値]

- interface : インターフェース名
  - [設定値]:
    - usb1
  - [初期値]: -
- command
  - [設定値]: AT コマンド文字列 (最大 64 文字)

- [初期値]:-
- *command\_list*
  - [設定値]: AT コマンド文字列を空白で区切った並び
  - [初期値]:-

**[説明]**

USB ポートに接続した機器を初期化するための AT コマンドを設定する。  
 USB ポートに機器が接続されている状態で起動したときには起動時に、機器が接続されていない状態で起動したときには機器を接続したときに、本コマンドで指定した AT コマンドが機器に設定される。  
 コマンドは AT(アテンションコード) を付加した AT コマンド文字列で指定する。  
 なお、1つの AT コマンド文字列に複数のコマンドを指定することも可能である。

**[ノート]**

FOMA を使ったりリモートセットアップを行う場合は、この初期化設定は不要です。

**[適用モデル]**

NVR700W, NVR510

### 43.28 USB ポートに接続した機器のフロー制御を行うか否かの設定

**[書式]**

**usbhost modem flow control interface sw**  
**no usbhost modem flow control interface**

**[設定値及び初期値]**

- *interface*: インターフェース名
  - [設定値]:
    - usb1
  - [初期値]:-
- *sw*
  - [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | フロー制御を行う   |
| off | フロー制御を行わない |

- [初期値]: off

**[説明]**

USB ポートに接続した機器のフロー制御を行うかどうかを設定する。  
 接続した機器を用いたリモートセットアップ通信時に通信が意図せず切断されてしまう場合に off に設定すると効果がある場合がある。

**[適用モデル]**

NVR700W, NVR510

### 43.29 携帯端末のファームウェア更新

**[書式]**

**mobile firmware update go interface**

**[設定値及び初期値]**

- *interface*
  - [設定値]:

| 設定値  | 説明            |
|------|---------------|
| usb1 | USB1 インターフェース |

- [初期値]:-

**[説明]**

指定したインターフェースに接続された携帯端末のファームウェアを更新する。

**[ノート]**

ソフトウェア更新機能の詳細は携帯端末の取扱説明書などを参照のこと。

また、本コマンドによりファームウェアを更新することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/>

**[適用モデル]**

NVR700W, NVR510

### 43.30 携帯端末のネットワーク事業者モードの設定

---

**[書式]**

**mobile carrier mode interface mode**

**no mobile carrier mode interface [mode]**

**[設定値及び初期値]**

- *interface*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| usb1 | USB1 インターフェース |

- [初期値]: -

- *mode*

- [設定値]:

| 設定値 | 説明             |
|-----|----------------|
| 0   | 工場出荷時の設定       |
| 1   | ネットワーク事業者モード 1 |
| 2   | ネットワーク事業者モード 2 |
| 3   | ネットワーク事業者モード 3 |

- [初期値]: -

**[説明]**

指定したインターフェースに接続された携帯端末のネットワーク事業者モードを設定する。

**[ノート]**

ネットワーク事業者モードを設定することが可能な携帯端末を使用する場合は、本コマンドを設定する必要がある。本コマンドが設定されていない場合は、アタッチされた時点における携帯端末本体のネットワーク事業者モードの設定値が使用される。

すでにアタッチされている携帯端末に対してこのコマンドの設定が変更された場合、次に携帯端末がアタッチされた時点から新しい設定が反映される。

また、本コマンドによりネットワーク事業者モードを設定することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/>

NVR700W は Rev.15.00.10 以降、NVR510 は Rev.15.01.09 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 43.31 自分の名前とパスワードの設定

---

**[書式]**

**wan auth myname myname password**

**no wan auth myname [myname password]**

**[設定値及び初期値]**• *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]:-

• *myname*

- [設定値]: 名前 (64 文字以内)

- [初期値]:-

• *password*

- [設定値]: パスワード (64 文字以内)

- [初期値]:-

**[説明]**

モバイルインターネットで、接続時に送信する自分の名前とパスワードを設定する。

**[適用モデル]**

NVR700W, NVR510

## 43.32 WAN で使用するインターフェースの設定

**[書式]**

*wan bind interface*

*wan bind wwan num*

**no wan bind** [*interface*]

**[設定値及び初期値]**• *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]:-

• *interface*

- [設定値]:

| 設定値  | 説明      |
|------|---------|
| usb1 | USB ポート |

- [初期値]:-

• *num*

- [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| 1~30 | 内蔵無線 WAN インターフェース番号 |

- [初期値]:-

**[説明]**

指定した WAN インターフェースについて実際に使用するインターフェースを設定する。

**[ノート]**

第 2 書式は NVR700W で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 43.33 携帯端末からの自動発信設定

#### [書式]

```
wan auto connect auto
```

```
no wan auto connect [auto]
```

#### [設定値及び初期値]

- *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- *auto*

- [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | 携帯端末から自動発信する  |
| off | 携帯端末から自動発信しない |

- [初期値]: off

#### [説明]

指定した WAN インターフェースについて自動接続するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

### 43.34 携帯端末を切断するタイマの設定

#### [書式]

```
wan disconnect time time
```

```
no wan disconnect time [time]
```

#### [設定値及び初期値]

- *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- *time*

- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 60

#### [説明]

指定した WAN インターフェースについて、送受信がない場合の切断までの時間を設定する。

#### [適用モデル]

NVR700W, NVR510

### 43.35 携帯端末を入力がないときに切断するタイマの設定

#### [書式]

```
wan disconnect input time time
```



**no wan disconnect input time** [*time*]

[設定値及び初期値]

• *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

• *time*

- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 120

[説明]

指定した WAN インターフェースについて、データ受信がない場合の切断までの時間を設定する。

[適用モデル]

NVR700W, NVR510

### 43.36 携帯端末を出力がないときに切断するタイマの設定

[書式]

*wan disconnect output time time*

**no wan disconnect output time** [*time*]

[設定値及び初期値]

• *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

• *time*

- [設定値]:

| 設定値        | 説明        |
|------------|-----------|
| 1-21474836 | 秒数        |
| off        | タイマを設定しない |

- [初期値]: 120

[説明]

指定した WAN インターフェースについて、データ送信がない場合の切断までの時間を設定する。

[適用モデル]

NVR700W, NVR510

### 43.37 常時接続の設定

[書式]

*wan always-on switch* [*time*]

**no wan always-on**

[設定値及び初期値]

• *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -
- *switch*

- [設定値]:

| 設定値 | 説明      |
|-----|---------|
| on  | 常時接続する  |
| off | 常時接続しない |

- [初期値]: off
- *time*
  - [設定値]: 再接続を要求するまでの秒数 (60..21474836)
  - [初期値]: -

#### [説明]

指定した WAN インターフェースについて、常時接続するか否かを設定する。また、常時接続での通信終了時に再接続を要求するまでの時間間隔を指定する。

常時接続に設定されている場合には、起動時に接続を起動し、通信終了時には再接続を起動する。接続失敗時あるいは通信の異常終了時には *time* に設定された時間間隔を待った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。*switch* が on に設定されている場合には、*time* の設定が有効となる。*time* が設定されていない場合には *time* は 60 になる。

#### [適用モデル]

NVR700W, NVR510

## 43.38 発信先アクセスポイントの設定

#### [書式]

*wan access-point name apn*

**no** *wan access-point name [apn]*

#### [設定値及び初期値]

- *wan*
  - [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -
- *apn*
  - [設定値]: モバイルインターネット通信に対応したアクセスポイント名 (Access Point Name)
  - [初期値]: -

#### [説明]

指定した WAN インターフェースについてアクセスポイント名 (APN) の割り当てを設定する。

#### [適用モデル]

NVR700W, NVR510

## 43.39 パケット通信量制限の設定

#### [書式]

*wan access limit length length [alert=alert[,alert\_cancel]]*

**no** *wan access limit length [length]*

#### [設定値及び初期値]

- *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

*length*

- [設定値]:

| 設定値          | 説明                       |
|--------------|--------------------------|
| 1-2147483647 | バイト数、送受信する累積パケットデータ長の上限值 |
| off          | 制限しない                    |

- [初期値]: 50M

*alert*

- [設定値]: 警告値、データ長あるいは[%]指定

- [初期値]: -

*alert\_cancel*

- [設定値]: 警告解除値、データ長あるいは[%]指定

- [初期値]: -

[説明]

指定した WAN インターフェースについて、送受信するパケットの累積データ長の上限值を設定する。上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。

*length*、*alert* および *alert\_cancel* パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **wan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status wan1** コマンドで、現在までの累積パケットデータ長を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wan access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が 0 になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。

例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

off を設定したときは警告が表示される。

[適用モデル]

NVR700W, NVR510

## 43.40 パケット通信時間制限の設定

[書式]

**wan access limit time** *time* [*alert*=*alert*[,*alert\_cancel*]] [*unit*=*unit*]

**no wan access limit time** [*time*]

#### [設定値及び初期値]

- *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- *time*

- [設定値]:

| 設定値          | 説明         |
|--------------|------------|
| 1-2147483647 | 累積通信秒数の上限値 |
| off          | タイマを設定しない  |

- [初期値]: 3600

- *alert*

- [設定値]: 警告値、秒数あるいは[%]指定

- [初期値]: -

- *alert\_cancel*

- [設定値]: 警告解除値、秒数あるいは[%]指定

- [初期値]: -

- *unit*

- [設定値]: 単位、second 又は minute

- [初期値]: second

#### [説明]

指定した WAN インターフェースについて、累積通信時間の上限値を設定する。上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。本コマンドは **wan disconnect time** コマンドとは独立して動作する。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **wan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

**show status wan1** コマンドで、現在までの累積通信時間を確認できる。

*alert* で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wan access limit duration** コマンドで累積期間を設定している場合には、*alert\_cancel* で指定した警告解除値を下回った時にログに表示することができる。

累積通信時間が警告値に達している間は再接続できない。警告解除値を下回ると再接続できる。

警告解除値を指定しない場合は、期間累積の接続時間が 0 になるまで警告を解除しない。

*unit* で minute を指定すると、接続時間を分単位で算出する。秒単位は切り上げられる。

#### [ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

**wan access limit duration** が設定されている場合、*unit=minute* を指定しても、期間内累積時間は、秒単位で加算される。off を設定したときは警告が表示される。

#### [適用モデル]

NVR700W, NVR510

## 43.41 接続毎パケット通信量制限の設定

### [書式]

`wan access limit connection length length [alert=alert]`

`no wan access limit connection length [length]`

### [設定値及び初期値]

- `wan`

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- `length`

- [設定値]:

| 設定値          | 説明                     |
|--------------|------------------------|
| 1-2147483647 | バイト数、送受信するパケットデータ長の上限值 |
| off          | 制限しない                  |

- [初期値]: off

- `alert`

- [設定値]: 警告値、データ長あるいは[%]指定

- [初期値]: -

### [説明]

指定した WAN インターフェースについて、1 回の接続で送受信するパケットのデータ長の上限值を設定する。上限に達した場合は通信を強制的に切断する。

`alert` を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

`length`、`alert` パラメーターの後ろに 'k' または、'M'、'G' をつけると、それぞれ k byte または M byte、G byte として扱われる。

### [ノート]

携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。

例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。

また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることもある。

従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

### [適用モデル]

NVR700W, NVR510

## 43.42 接続毎パケット通信時間制限の設定

### [書式]

`wan access limit connection time time [alert=alert]`

`no wan access limit connection time [time]`

### [設定値及び初期値]

- `wan`

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- *time*

- [設定値]:

| 設定値          | 説明          |
|--------------|-------------|
| 1-2147483647 | 秒数、通信秒数の上限値 |
| off          | タイマを設定しない   |

- [初期値]: off

- *alert*

- [設定値]: 警告値、秒数あるいは[%]指定
- [初期値]: -

## [説明]

指定した WAN インターフェースについて、1 回の接続の通信時間の上限値を設定する。上限に達した場合は通信を強制的に切断する。本コマンドは **wan disconnect time** コマンドとは独立して動作する。*alert* を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

## [適用モデル]

NVR700W, NVR510

### 43.43 通信制限の累積期間の設定

## [書式]

*wan access limit duration duration*

**no wan access limit duration** [*duration*]

## [設定値及び初期値]

- *wan*

- [設定値]:

| 設定値  | 説明            |
|------|---------------|
| wan1 | WAN インターフェース名 |

- [初期値]: -

- *duration*

- [設定値]:

| 設定値       | 説明                 |
|-----------|--------------------|
| 1-2592000 | 秒数、通信制限の累積対象の過去の期間 |
| off       | 過去の全期間を対象とする       |

- [初期値]: off

## [説明]

指定した WAN インターフェースについて、通信制限を行う場合に累積対象となる過去の期間を設定する。

## [適用モデル]

NVR700W, NVR510

## 第 44 章

### ブリッジインターフェース (ブリッジ機能)

ブリッジインターフェースは複数のインターフェースを 1 つの仮想インターフェースに收容し、收容したインターフェース間でブリッジングを行う機能です。

收容された各インターフェースが接続する物理的なセグメントは 1 つのセグメントとして扱います。

#### 注意事項

- 本機能におけるブリッジ処理はワイヤレートを保証するものではありません。
- QoS 機能には対応していません。そのため、QoS 機能を利用した Dynamic Traffic Control 機能を利用することはできません。
- スパニングツリープロトコルには対応していません。
- BPDU フレームは透過します。
- IEEE802.1Q タグ付きパケットは透過します。

#### 44.1 ブリッジインターフェースに收容する実インターフェースを設定する

##### [書式]

```
bridge member bridge_interface interface interface [...]
```

```
no bridge member bridge_interface [interface ...]
```

##### [設定値及び初期値]

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -
- *interface*
  - [設定値]:

| 設定値     | 説明               |
|---------|------------------|
| lanN    | LAN インターフェース名    |
| lanN.M  | LAN 分割 インターフェース名 |
| vlanN   | VLAN インターフェース名   |
| onu1    | ONU インターフェース名    |
| tunnelN | TUNNEL インターフェース名 |

- [初期値]: -

##### [説明]

仮想インターフェースであるブリッジインターフェースに收容する実インターフェースを指定する。

收容したインターフェース間でブリッジ動作が行われる。

トンネルインターフェースを收容した場合、L2TPv3 トンネルが確立しているトンネルインターフェースでのみブリッジ動作が行われる。

##### [ノート]

- 收容する LAN インターフェース、および ONU インターフェースについて  
收容した実インターフェースに IPv4,IPv6 アドレスを付与してはならない。  
收容した実インターフェースの IPv6 リンクローカルアドレスは削除される。  
收容する LAN インターフェースや ONU インターフェースの MTU はすべて同一の値でなければならない。  
いずれかのブリッジインターフェースに收容した実インターフェースは、他のブリッジインターフェースに收容することはできない。  
收容するインターフェースがスイッチングハブを持つインターフェースである場合、スイッチングハブのポート間で完結する通信は本機能によるブリッジ動作ではなく、スイッチングハブ LSI 内部で処理される。

- ・ 収容するトンネルインターフェースについて

収容するトンネルインターフェースの MTU は無効となり、トンネルインターフェースでフラグメントは行われず、カプセル化されたパケットの送信インターフェースの MTU に従ってフラグメントが発生する。いずれかのブリッジインターフェースに収容したインターフェースは、他のブリッジインターフェースに収容することはできない。

- ・ ブリッジインターフェースについて

ブリッジインターフェースのリンク状態は収容した LAN インターフェースや ONU インターフェースのリンク状態に応じて変化する。

いずれかの収容したインターフェースがアップ状態だった場合、ブリッジインターフェースはアップ状態になる。

すべてのインターフェースがダウン状態だった場合、ブリッジインターフェースもダウン状態になる。

ブリッジインターフェースの MAC アドレスは、収容した LAN インターフェースや ONU インターフェースのうち、インターフェース番号がもっとも小さいインターフェースのアドレスを使用する。

**[適用モデル]**

NVR700W

## 44.2 自動的なラーニングを行うか否かの設定

**[書式]**

**bridge learning** *bridge\_interface* *switch*

**no bridge learning** *bridge\_interface* [*switch*]

**[設定値及び初期値]**

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -
- *switch*
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| on  | ラーニングする  |
| off | ラーニングしない |

- [初期値]: on

**[説明]**

ブリッジ機能で自動的な MAC アドレスのラーニングを行うか否かを設定する。

*bridge\_interface* には対象となるブリッジインターフェース名を指定する。

ラーニングを行う場合、ブリッジインターフェースに収容したインターフェースでパケットを受信すると、そのパケットの始点 MAC アドレスと受信インターフェースを学習してラーニングテーブルに登録する。

学習した情報はブリッジ処理が行われるときに参照され、パケットが不要なインターフェースに出力されることを抑制する。

**[ノート]**

学習時にラーニングテーブルが上限に達していた場合、もっとも古いエントリを削除した上で登録される。

ブリッジ処理においてラーニングテーブルを参照したとき、一致するエントリが存在しなかった場合、受信インターフェースを除くすべての収容インターフェースにパケットが出力される。これはリピーターと同様の動作である。

**[適用モデル]**

NVR700W

## 44.3 ブリッジがラーニングした情報の消去タイマの設定

**[書式]**

**bridge learning** *bridge\_interface* **timer** *time*



**no bridge learning bridge\_interface timer [time]**

**[設定値及び初期値]**

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -
- *time*
  - [設定値]:

| 設定値       | 説明        |
|-----------|-----------|
| 30..32767 | 秒数        |
| off       | タイマを設定しない |

- [初期値]: 300

**[説明]**

ブリッジが自動的にラーニングした情報の寿命を設定する。

*bridge\_interface* には対象となるブリッジインターフェース名を指定する。

指定した時間内に、ある始点 MAC アドレスからパケットを受信しなかった場合はその MAC アドレスに関する学習した情報を消去する。

off を指定した場合には、学習した情報が自動的に消去されることはなくなる。

**[適用モデル]**

NVR700W

## 44.4 静的なラーニング情報の設定

**[書式]**

**bridge learning bridge\_interface static mac\_address interface**  
**no bridge learning bridge\_interface static mac\_address [interface]**

**[設定値及び初期値]**

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -
- *mac\_address*
  - [設定値]: MAC アドレス
  - [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -

**[説明]**

ブリッジが参照する静的な登録情報を設定する。

*bridge\_interface* には対象となるブリッジインターフェース名を指定する。

*mac\_address* に指定した MAC アドレスが宛先であるパケットは、*interface* で指定したインターフェースに出力されるようになる。

*interface* には *bridge\_interface* に收容された LAN インターフェース、または ONU インターフェースを指定する。

**[ノート]**

静的に登録した情報は自動的に学習した情報よりも優先して参照される。

*interface* で指定した LAN インターフェースや ONU インターフェースが *bridge\_interface* に收容されていない場合、登録した情報は無視される。

**[適用モデル]**

NVR700W

## 第 45 章

### Lua スクリプト機能

Lua 言語で記述されたスクリプトを実行する機能です。Lua スクリプトにヤマハルーター専用 API を埋め込むことで、ルーターの状態に応じて、ルーターの設定変更やアクションをプログラミングすることが可能になります。

#### 45.1 Lua スクリプト機能を有効にするか否かの設定

##### [書式]

```
lua use switch
no lua use [switch]
```

##### [設定値及び初期値]

- *switch*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 有効にする |
| off | 無効にする |

- [初期値]: on

##### [説明]

Lua スクリプト機能を有効にするか否かを設定をする。

Lua スクリプトの走行中に当コマンドで Lua スクリプト機能を無効にした場合、走行中のすべての Lua スクリプトは強制終了される。

##### [適用モデル]

NVR700W, NVR510

#### 45.2 Lua スクリプトの実行

##### [書式]

```
lua [-e stat] [-l module] [-v] [--] [script_file [args ...]]
```

##### [設定値及び初期値]

- *stat*
  - [設定値]: スクリプト文字列
  - [初期値]: -
- *module*
  - [設定値]: ロード (require する) モジュール名
  - [初期値]: -
- *script\_file*
  - [設定値]: スクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
  - [初期値]: -
- *args*
  - [設定値]: *script\_file* に渡す可変個引数
  - [初期値]: -

##### [説明]

Lua スクリプトを実行する。

基本的な文法は Lua 標準の **lua** コマンドと同じであるが、標準入力 (stdin) をスクリプトの入力対象とする **-i/-** オプションと、パラメーターなしの実行には対応していない。**-v** オプションはバージョン情報を出力する。**--** オプションは記述したポイントでオプション処理を終了することを表し、*script\_file* や *args* に "-" で始まるファイル名および文字列を指定できるようになる。なお、**-e/-l/-v** の各オプションは繰り返して複数個指定できるが *script\_file* よりも後に

指定することはできない。 *script\_file* は1つしか指定できず、 *script\_file* を記述したポイント以降のパラメータはすべて無視される。このとき、エラーメッセージは出力されない。

*script\_file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

#### [ノート]

環境変数 LUA\_INIT が設定されている場合は、そのスクリプトが最初に実行される。

*script\_file* にバイトコードファイルを指定する場合、ルーター上で生成したバイトコードだけが実行可能であり、Lua をインストールした PC 等で生成したバイトコードは実行できない。

#### [適用モデル]

NVR700W, NVR510

## 45.3 Lua コンパイラの実行

#### [書式]

```
luac [-l] [-o output_file] [-p] [-s] [-v] [--] script_file [script_file ..]
```

#### [設定値及び初期値]

- *output\_file*
  - [設定値]: バイトコードの出力先のファイル名を絶対パスもしくは相対パスで指定する
  - [初期値]: luac.out (相対パス)
- *script\_file*
  - [設定値]: コンパイル対象のスクリプトファイル名を絶対パスもしくは相対パスで指定する
  - [初期値]: -

#### [説明]

Lua コンパイラを実行し、バイトコードを生成する。

基本的な文法は Lua 標準の **luac** コマンドと同じであるが、- オプションは指定できない。-l オプションは生成したバイトコードをリスト表示する。-p オプションは構文解析のみを行う。-s オプションはコメント等のデバッグ情報を取り除く。-v オプションはバージョン情報を出力する。-- オプションは記述したポイントでオプション処理を終了することを表し、*script\_file* に "-" で始まるファイル名を指定できるようになる。なお、*script\_file* を複数指定して、一つのバイトコードファイルにまとめることもできる。

*script\_file/output\_file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

#### [適用モデル]

NVR700W, NVR510

## 45.4 Lua スクリプトの走行状態の表示

#### [書式]

```
show status lua [info]
```

#### [設定値及び初期値]

- *info*: 表示する情報の種類
  - [設定値]:

| 設定値     | 説明                 |
|---------|--------------------|
| running | 走行中のスクリプトに関する情報    |
| history | 過去に走行したスクリプトに関する情報 |
| 省略      | すべての情報を表示する        |

- [初期値]: -

#### [説明]

現在の Lua スクリプトの走行状態や過去の走行履歴を表示する。この情報は **lua use** コマンドで Lua スクリプト機能を無効にするとクリアされる。

- Lua のバージョン情報
- 走行中のスクリプト[**running**]
- Lua タスク番号
- 走行状態

|             |                               |
|-------------|-------------------------------|
| RUN         | 走行中                           |
| SLEEP       | スリープ中                         |
| WATCH       | SYSLOG 監視中 (Lua タスクはスリープしている) |
| COMMUNICATE | 通信中                           |
| TERMINATE   | 強制終了中                         |

- トリガ
  - **lua** コマンド
  - **luac** コマンド
  - スケジュール
  - DOWNLOAD ボタン
- コマンドライン
- スクリプトファイル名
- 監視文字列 (SYSLOG 監視中のとき)
- 開始日時/走行時間
- 過去に走行したスクリプト[**history**] (最新 10 種類まで新しい順に表示)
  - トリガ
    - **lua** コマンド
    - **luac** コマンド
    - スケジュール
    - DOWNLOAD ボタン
  - コマンドライン
  - スクリプトファイル名
  - 走行回数/エラー発生回数/エラー履歴 (最新 5 回分まで新しい順に表示)
  - 前回の開始日時/終了時間/走行結果

#### [適用モデル]

NVR700W, NVR510

## 45.5 Lua スクリプトの強制終了

### [書式]

```
terminate lua task_id
```

```
terminate lua file script_file
```

### [設定値及び初期値]

- *task\_id*: 強制終了する Lua タスクの番号
- [設定値]:

| 設定値   | 説明             |
|-------|----------------|
| all   | すべての Lua タスク番号 |
| 1..10 | Lua タスクの番号     |

- [初期値]: -
- *script\_file*
  - [設定値]: 強制終了するスクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
  - [初期値]: -

### [説明]

指定した Lua タスク、または、Lua スクリプトを強制終了する。

第1書式では、*task\_id*で指定された Lua タスクを強制終了する。Lua タスクの番号や実行しているスクリプトについては **show status lua** コマンドで確認できる。

第2書式では、*script\_file*で指定されたパスとファイル名が完全に一致するスクリプトを実行しているすべての Lua タスクを強制終了する。*script\_file*に相対パスを指定した場合、環境変数 PWD を基点とする絶対パスに置換された後で対象の Lua タスクの検索が行われる。

**lua** コマンドの **-e** オプションを使用して、スクリプトファイルを使用せずに実行されているような Lua スクリプトを強制終了させる場合は、第1書式を使用する。

**[適用モデル]**

NVR700W, NVR510

## 45.6 Lua スクリプト機能に関連するアラーム音を鳴らすか否かの設定

**[書式]**

**alarm lua switch**

**no alarm lua** [*switch*]

**[設定値及び初期値]**

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 鳴らす   |
| off | 鳴らさない |

- [初期値]: on

**[説明]**

Lua スクリプト機能に関連するアラーム音を鳴らすか否かを選択する。

本コマンドでは、DOWNLOAD ボタンによる Lua スクリプトの実行に関するアラーム音を鳴らすか否かの設定ができる。ハードウェアライブラリでの制御によるアラーム音を鳴らすか否かは、**alarm entire** コマンドの設定に従う。

**[適用モデル]**

NVR700W, NVR510

## 第 46 章

### カスタム GUI

カスタム GUI とは、ルーターの設定を行うための GUI (WWW ブラウザに対応するユーザーインターフェース) をユーザーが独自に設計し組み込むことができる機能です。ルーターにはホストから HTTP で設定を転送するためのインターフェースが用意されており、ユーザーは JavaScript を使用して GUI を作成します。

NVR700W, NVR510 には WWW ブラウザ設定支援機能が搭載されていますが、ユーザーごとに設定画面を変更することはできません。本機能では、カスタム GUI を複数組み込み、ログインするユーザーによって画面を切り替えることが可能です。

#### 46.1 カスタム GUI を使用するか否かの設定

##### [書式]

```
httpd custom-gui use use
no httpd custom-gui use [use]
```

##### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

##### [説明]

カスタム GUI を使用するか否かを設定する。

##### [適用モデル]

NVR700W, NVR510

#### 46.2 カスタム GUI を使用するユーザーの設定

##### [書式]

```
httpd custom-gui user [user] directory=path [index=name]
no httpd custom-gui user [user...]
```

##### [設定値及び初期値]

- *user*
  - [設定値]: ユーザー名
  - [初期値]: -
- *path*
  - [設定値]: 基点となるディレクトリの絶対パスまたは相対パス
  - [初期値]: -
- *name*
  - [設定値]: スラッシュ '/' 止めの URL でアクセスした場合に出力するファイル名
  - [初期値]: index.html

##### [説明]

カスタム GUI を使用するユーザーを設定する。http://(ルーターの IP アドレス)/にアクセスし、本コマンドで登録されているユーザー名でログインすると http://(ルーターの IP アドレス)/custom/user/にリダイレクトされる。

*user* を省略した場合には無名ユーザーに対する設定となる。この場合の URL は http://(ルーターの IP アドレス)/custom/anonymous.user/となる。

*path* には基点となるディレクトリを絶対パス、もしくは相対パスで指定する。相対パスで指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は set コマンドで変更可能であり、初期値は "/" である。

*name* にはブラウザから '/' 止めの URL でアクセスした場合に表示するファイル名を指定する。

**[ノート]**

本コマンドを設定する場合、無名ユーザー以外は事前に **login user** コマンドでユーザーを登録しておく必要がある。登録されていないユーザーに対して本コマンドを設定するとエラーになる。

NVR700W, NVR510 の外部メモリにおいて自動検索機能は使用できない。また、*name* にスラッシュ '/' を含む文字列を指定することはできない。

本コマンドが設定されているユーザーは、ルーターに内蔵されている通常の GUI にアクセスすることができない。

**[適用モデル]**

NVR700W, NVR510

**46.3 カスタム GUI の API を使用するか否かの設定****[書式]**

```
httpd custom-gui api use use
no httpd custom-gui api use [use]
```

**[設定値及び初期値]**

- *use*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

API 用の URL "http://( ルーターの IP アドレス )/custom/api" に対する POST リクエストを受け付けるか否かを設定する。

**[ノート]**

API 用の URL を使用するには、本コマンドに加えて **httpd custom-gui use on** が設定されている必要がある。

本コマンドを on にしても **httpd custom-gui api password** コマンドを設定しなければ API 用の URL を使用することはできない。

**[適用モデル]**

NVR700W, NVR510

**46.4 カスタム GUI の API にアクセスするためのパスワードの設定****[書式]**

```
httpd custom-gui api password password
no httpd custom-gui api password [password]
```

**[設定値及び初期値]**

- *password*
- [設定値]: パスワード
- [初期値]: -

**[説明]**

API 用の URL へ POST リクエストを送信する際のパスワードを設定する。32 文字以内で半角英数字を使用することができる。

例えば、本コマンドでパスワードとして *doremi* を設定した場合、URL は http://( ルーターの IP アドレス )/custom/api?password=doremi となる。

**[適用モデル]**

NVR700W, NVR510

## 第 47 章

### 診断

#### 47.1 ポートの開閉状態の診断

##### [書式]

```
diagnose config port map interface protocol [src_addr [src_port]] dst_addr
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: 受信側の LAN、PP インターフェース名
  - [初期値]: -
- *protocol*
  - [設定値]: 診断対象のパケット種別 (カンマで区切って複数指定可能)
  - [設定値]:
    - プロトコルを表す十進数 (0..255)
    - プロトコルを表すニーモニック

| 設定値  | 説明               |
|------|------------------|
| tcp  | TCP パケット         |
| udp  | UDP パケット         |
| icmp | ICMP パケット        |
| gre  | PPTP の gre パケット  |
| esp  | IPsec の esp パケット |
| ah   | IPsec の ah パケット  |

- [初期値]: -
- *src\_addr*
  - [設定値]: 入力パケットの送信元 IP アドレス
  - [初期値]: -
- *src\_port*
  - [設定値]: 入力パケットの送信元ポート番号
  - [初期値]: -
- *dst\_addr*
  - [設定値]: 診断対象の宛先 IP アドレス (カンマで区切って複数指定可能)
  - [初期値]: -

##### [説明]

*interface* パラメーターで指定されたインターフェースから受信するパケットがルーターを通過することが可能か診断をする。

tcp、udp パケットでは、*dst\_addr* パラメーターで指定された宛先 IP アドレスのウェルノウンポートに対して、ルーターを通過することのできるポートが存在した場合、その内容を表示する。tcp、udp 以外のパケットについては、ポートに関する設定は無視され、*dst\_addr* までパケットが到達可能であった場合にその内容を表示する。

*src\_addr*、及び、*src\_port* が省略された場合、送信元 IP アドレスと送信元ポート番号は、フィルターの設定内容から必要と思われる組み合わせをルーターが自動的にサンプリングする。

##### [ノート]

本コマンドはルーターの内部だけで擬似的にパケットの転送処理を行うことにより実現しているため、*dst\_addr* に指定されるホストに対して診断対象のパケットを送信することはない。そのため、ホスト側では閉じられているポートでもルーターを通過することが可能である場合は、そのポートは開いていると判断される。これは、*dst\_addr* にルーター自身の IP アドレスが指定された場合も同様であり、ルーター自身のポートの開閉状態を診断するわけではない。

なお、本コマンドではイーサネットフィルターは考慮されない。



[適用モデル]  
NVR700W, NVR510

## 47.2 ポートへ到達可能なアクセス範囲の診断

### [書式]

```
diagnose config port access interface [protocol] dst_addr dst_port
```

### [設定値及び初期値]

- *interface*
  - [設定値]: 受信側の LAN、ONU、PP インターフェース名
  - [初期値]: -
- *protocol*: 診断対象のパケット種別 (カンマで区切って複数指定可能、省略時は全種別)
  - [設定値]:

| 設定値 | 説明       |
|-----|----------|
| tcp | TCP パケット |
| udp | UDP パケット |

- [初期値]: -
- *dst\_addr*
  - [設定値]: 診断対象の宛先 IP アドレス
  - [初期値]: -
- *src\_port*
  - [設定値]: 診断対象の宛先ポート番号
  - [初期値]: -

### [説明]

*dst\_addr/dst\_port* パラメーターで指定されたホストのポート番号へ、*protocol* パラメーターで指定されたパケットが到達可能な送信元 IP アドレスと送信元ポート番号の範囲を表示する。

### [ノート]

本コマンドはルーターの内部だけで擬似的にパケットの転送処理を行うことにより実現しているため、*dst\_addr* に指定されるホストに対して診断対象のパケットを送信することはない。そのため、ホスト側では閉じられているポートでもルーターを通過することが可能である場合は、そのポートへ到達可能と判断される。これは、*dst\_addr* にルーター自身の IP アドレスが指定された場合も同様であり、ルーター自身のポートの開閉状態には依存しない。

なお、本コマンドではイーサネットフィルタは考慮されない。

[適用モデル]  
NVR700W, NVR510

## 47.3 ポートの開閉状態の診断で検出可能な通過パケットの最大数の設定

### [書式]

```
diagnosis config port max-detect num
```

### [設定値及び初期値]

- *num*
  - [設定値]: 検出可能な通過パケットの最大数 (100..1000000)
  - [初期値]: 2000

### [説明]

ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断で検出が可能な通過パケットの最大数を設定する。この数値を超えて通過パケットを検出した場合、診断が中断される。

### [ノート]

ポートの開閉状態の診断結果では、通過可能な送信元アドレス空間と送信元ポート番号空間を可能な限り集約して表示している。しかし、集約前の通過数が本設定値を超えた時点で診断が中断されるため、診断結果で表示される通過数が、実際には本設定値を下回る場合でも診断が中断されることがある。

[適用モデル]  
NVR700W, NVR510

## 47.4 ポートの開閉状態の診断結果の履歴数の設定

---

### [書式]

**diagnosis config port history-num** *num*

### [設定値及び初期値]

- *num*
  - [設定値]: 診断結果として保存する履歴数 (1..10)
  - [初期値]: 3

### [説明]

ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断の診断結果として保存する履歴数を設定する。

### [ノート]

本コマンドを実行したときに設定値を上回る履歴が既に保存されていた場合、設定値を超える履歴は消去される。

### [適用モデル]

NVR700W, NVR510

## 47.5 ポートの開閉状態の診断結果の表示

---

### [書式]

**show diagnosis config port map**

### [説明]

ポートの開閉状態の診断結果を表示する。

### [適用モデル]

NVR700W, NVR510

## 47.6 ポートへ到達可能なアクセス範囲の診断結果の表示

---

### [書式]

**show diagnosis config port access**

### [説明]

ポートへ到達可能なアクセス範囲の診断結果を表示する。

### [適用モデル]

NVR700W, NVR510

## 47.7 ポートの開閉状態の診断結果の消去

---

### [書式]

**clear diagnosis config port**

### [説明]

ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断の診断結果をすべて消去する。

### [適用モデル]

NVR700W, NVR510

## 第 48 章

### 統計

#### 48.1 統計機能を有効にするか否かの設定

##### [書式]

```
statistics type sw
no statistics type [sw]
```

##### [設定値及び初期値]

- *type* : 内部リソースの種別
  - [設定値]:

| 設定値         | 説明                |
|-------------|-------------------|
| cpu         | CPU 利用率           |
| memory      | メモリ使用率            |
| traffic     | インターフェース別のトラフィック量 |
| flow        | ファストパスフロー数        |
| nat         | NAT テーブルのエントリー数   |
| route       | 経路数               |
| filter      | 動的フィルターのセッション数    |
| application | アプリケーションのトラフィック情報 |

- [初期値]: -
- *sw*
- [設定値]:

| 設定値 | 説明         |
|-----|------------|
| on  | 統計機能を有効にする |
| off | 統計機能を無効にする |

- [初期値]: off

##### [説明]

各種統計機能を有効にするか否かを設定する。

##### [ノート]

off にするとそれ以前の統計情報はクリアされる。

*type* パラメータの *application* キーワードは NVR700W の Rev.15.00.17 以降で使用可能。

NVR700W は Rev.15.00.16 以降で使用可能

NVR510 は Rev.15.01.15 以降で使用可能

##### [適用モデル]

NVR700W, NVR510

## 第 49 章

### DPI

Deep Packet Inspection (以下 DPI) は、IP ネットワーク上を流れるトラフィックを高度に検査することにより、そのパケットがどのアプリケーションのものであるかを識別することができる技術です。

ヤマハルーターでは、DPI の識別結果を以下のように利用することができます。

- 経路の選択
- フィルタリング
- QoS
- トラフィックの可視化

DPI は有償サービスにより提供される機能です。ご利用いただくには、別途ライセンス製品を購入していただく必要があります。

本機能に関する技術情報は以下に示す URL で公開しています。

<http://www.rtpro.yamaha.co.jp/RT/docs/dpi/>

#### 49.1 DPI を使用するか否かの設定

##### [書式]

```
dpi use switch [reject]
```

```
no dpi use [switch [reject]]
```

##### [設定値及び初期値]

- *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *reject*: 未識別のパケットを破棄するか否か

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 破棄する  |
| off | 破棄しない |

- [初期値]: off

##### [説明]

DPI を使用するか否かを設定する。

DPI のアクティベーション中でアプリケーションの識別ができない場合のパケットは、*reject* パラメーターの設定に従い通過、または破棄される。

##### [ノート]

NVR700W の Rev.15.00.22 以前のファームウェアで、アプリケーション識別を行うためには、すべてのパケットをノーマルパスで処理する必要がある。IPv4 の環境では、**ip routing process** コマンドを、IPv6 の環境では **ipv6 routing process** コマンドを **normal** に設定する必要がある。

NVR700W は Rev.15.00.17 以降で使用可能。

##### [適用モデル]

NVR700W

## 49.2 IPv4 の DPI フィルターの設定

### [書式]

```
ip dpi filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [application]]
ip dpi filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [group_num]]
no ip dpi filter filter_num [pass_reject ...]
```

### [設定値及び初期値]

- *filter\_num*
  - [設定値]: DPI のフィルター番号 (1..2147483647)
  - [初期値]: -

- *pass\_reject*
  - [設定値]:

| 設定値          | 説明                  |
|--------------|---------------------|
| pass         | 一致すれば通す(ログに記録しない)   |
| pass-log     | 一致すれば通す(ログに記録する)    |
| pass-nolog   | 一致すれば通す(ログに記録しない)   |
| reject       | 一致すれば破棄する(ログに記録しない) |
| reject-log   | 一致すれば破棄する(ログに記録する)  |
| reject-nolog | 一致すれば破棄する(ログに記録しない) |

- [初期値]: -
- *src\_addr*: IP パケットの始点アドレス
  - [設定値]:
    - IPv4 アドレス
      - A.B.C.D (A ~ D: 0 ~ 255 もしくは \*)
        - 上記表記で A ~ D を \* とすると、該当する 8 ビット分についてはすべての値に対応する
      - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する
      - カンマ区切りで複数設定することができる
    - FQDN
      - 任意の文字列 (半角 255 文字以内。/, : は使用できない。 , は区切り文字として使われるため、使用できない)
      - \* から始まる FQDN は \* より後ろの文字列を後方一致条件として判断する。たとえば \*.example.co.jp は www.example.co.jp、mail.example.co.jp などと一致する
      - , を区切りとして複数設定することができる。IP アドレスと混在することも可能
      - \* (すべてのアドレスに対応)
  - [初期値]: -
- *dest\_addr*: IP パケットの終点アドレス
  - [設定値]:
    - *src\_addr* と同じ形式
    - 省略した場合は 1 個の \* と同じ
  - [初期値]: -
- *mask*: ネットワークアドレスのビットマスク
  - [設定値]:
    - A.B.C.D (A ~ D: 0 ~ 255)
    - 0x に続く十六進数
    - マスクビット数
    - 省略時は 0xffffffff と同じ
  - [初期値]: -
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
  - [設定値]:

- アプリケーションを表すニーモニック
- "@" で始まるカテゴリをあらわすニーモニック
- 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリの混在が可能)
- 省略時は 1 つの \* と同じ
- [初期値]:-
- `group_num`: グループ ID
  - [設定値]: **dpi group set** コマンドでグループ化したアプリケーションのグループ ID
  - [初期値]:-

**[説明]**

DPI で使用する IPv4 のフィルターを設定する。本コマンドで設定されたフィルターは **ip interface dpi filter** コマンドと組み合わせて利用することで、特定アプリケーションのパケットのフィルタリングをすることができる。また、フィルター型ルーティングと利用することで、特定アプリケーションのパケットの経路選択を行うことができる。アプリケーションを表すニーモニックには、**show dpi application** コマンドで表示されるものを使用する。またカテゴリを表すニーモニックには、**show dpi category** コマンドで表示されるものを使用する。

**[ノート]**

アプリケーションの識別が完了していないパケットは、フィルターの設定によらず必ず通過する。また、DPI のアクティベーション中でアプリケーションの識別結果が得られない場合には、すべてのパケットは **dpi use** コマンドの `reject` の設定に従う。

NVR700W は Rev.15.00.17 以降で使用可能。

**[設定例]**

- Web アクセスとメールの使用のみ許可する

```
# ip dpi filter 1 pass * * @web,@email,@webmail
# ip dpi filter 100 reject * *
# ip lan2 dpi filter out 1 100
```

- Office365 のパケットは PP1 インターフェース経由で、その他は TUNNEL1 経由で送信する

```
# dpi group set 100 name=o365 word_online sharepoint_online powerpoint_online
outlook office_docs office365 ms_sway ms_planner ms_onenote lync_online
excel_online
# ip dpi filter 1 pass * * 100
# ip route default gateway pp 1 dpi 1 gateway tunnel 1
```

**[適用モデル]**

NVR700W

## 49.3 IPv6 の DPI フィルタの設定

**[書式]**

```
ipv6 dpi filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len][application]]
ipv6 dpi filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len][group]]
no ipv6 dpi filter filter_num [pass_reject ...]
```

**[設定値及び初期値]**

- `filter_num`
  - [設定値]: DPI のフィルタ番号 (1..2147483647)
  - [初期値]:-
- `pass_reject`
  - [設定値]:

| 設定値        | 説明                  |
|------------|---------------------|
| pass       | 一致すれば通す(ログに記録しない)   |
| pass-log   | 一致すれば通す(ログに記録する)    |
| pass-nolog | 一致すれば通す(ログに記録しない)   |
| reject     | 一致すれば破棄する(ログに記録しない) |

| 設定値          | 説明                  |
|--------------|---------------------|
| reject-log   | 一致すれば破棄する(ログに記録する)  |
| reject-nolog | 一致すれば破棄する(ログに記録しない) |

- [初期値]:-
- *src\_addr*: IPv6 パケットの始点アドレス
  - [設定値]:
    - IPv6 アドレス
      - 間に - を挟む、- を前につける、または - を後ろにつける範囲の指定ができる
      - カンマ区切りで複数設定することができる
    - \*(すべてのアドレスに対応)
  - [初期値]:-
- *dest\_addr*: IPv6 パケットの終点アドレス
  - [設定値]:
    - *src\_addr* と同じ形式
    - 省略した場合は 1 個の \* と同じ
  - [初期値]:-
- *prefix\_len*
  - [設定値]: プレフィックス長
  - [初期値]:-
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
  - [設定値]:
    - アプリケーションを表すニーモニック
    - "@" で始まるカテゴリーをあらわすニーモニック
    - 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリーの混在が可能)
    - 省略時は 1 つの \* と同じ
  - [初期値]:-
- *group\_num*: グループ ID
  - [設定値]: **dpi group set** コマンドでグループ化したアプリケーションのグループ ID
  - [初期値]:-

#### [説明]

DPI で使用する IPv6 フィルタを設定する。本コマンドで設定されたフィルタは **ipv6 interface dpi filter** コマンドと組み合わせて利用することで、特定アプリケーションのパケットのフィルタリングをすることができる。

アプリケーションを表すニーモニックには、**show dpi application** コマンドで表示されるものを使用する。またカテゴリーを表すニーモニックには、**show dpi category** コマンドで表示されるものを使用する。

#### [ノート]

アプリケーションの識別が完了していないパケットは、フィルタの設定によらず必ず通過する。また、DPI のアクティベーション中でアプリケーションの識別結果が得られない場合には、すべてのパケットは **dpi use** コマンドの *reject* の設定に従う。

NVR700W は Rev.15.00.17 以降で使用可能。

#### [設定例]

IPv6 による FTP サーバーへのアクセスは禁止する

```
# ipv6 dpi filter 1 reject * * ftp,ftp_data
# ipv6 dpi filter 100 pass * *
# ipv6 lan2 dpi filter out 1 100
```

#### [適用モデル]

NVR700W

## 49.4 DPI のフィルターのインターフェースへの適用

### [書式]

```
ip interface dpi filter direction filter_list...
ipv6 interface dpi filter direction filter_list...
ip pp dpi filter direction filter_list...
ipv6 pp dpi filter direction filter_list...
ip tunnel dpi filter direction filter_list...
ipv6 tunnel dpi filter direction filter_list...
no ip interface dpi filter direction [filter_list...]
no ipv6 interface dpi filter direction [filter_list...]
no ip pp dpi filter direction [filter_list...]
no ipv6 pp dpi filter direction [filter_list...]
no ip tunnel dpi filter direction [filter_list...]
no ipv6 tunnel dpi filter direction [filter_list...]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インタフェース名、WAN インタフェース名、LOOPBACK インタフェース名、NULL インタフェース名、ブリッジインタフェース名
  - [初期値]: -
- *direction*

- [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| in  | 受信したパケットに対するフィルタリング |
| out | 送信したパケットに対するフィルタリング |

- [初期値]: -
- *filter\_list*
  - [設定値]: 空白で区切られた静的フィルタ番号の並び (最大 128 個以内)
  - [初期値]: -

### [説明]

**ip dpi filter** コマンド、および **ipv6 dpi filter** コマンドによるフィルターを組み合わせ、インターフェースで送受信するパケットの種類を制限する。

送信/受信のそれぞれの方向に対して、適用するフィルター列をフィルター番号で指定する。指定された番号のフィルターが順番に適用され、パケットにマッチするフィルターが見つければそのフィルターにより通過/破棄が決定する。それ以降のフィルターは調べられない。すべてのフィルターにマッチしないパケットは破棄される。

### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

### [設定例]

- 192.168.200.0/24 のネットワークに属する端末で、指定のファイル共有ソフトと、ゲームカテゴリーに属するアプリケーションを禁止する

```
# dpi group set 1000 name=file-sharing winmx winny share bittorrent
# ip dpi filter 1 reject 192.168.200.0/24 * 1000
# ip dpi filter 2 reject 192.168.200.0/24 * @game
# ip dpi filter 100 pass * *
# pp select 1
# ip pp dpi filter out 1 2 100
```

### [適用モデル]

NVR700W



## 49.5 DPI のアプリケーショングループの作成

### [書式]

```
dpi group set group_num [name=name] application_list...
no dpi group set group_num [[name=name] application_list...]
```

### [設定値及び初期値]

- *group\_num*
  - [設定値]: グループ ID (1..2147483647)
  - [初期値]: -
- *name*
  - [設定値]: グループ名 (最大 32 文字以内)
  - [初期値]: -
- *application\_list*
  - [設定値]: アプリケーション、およびカテゴリーの並び(空白区切り、最大 128 個以内)
  - [初期値]: -

### [説明]

DPI のアプリケーションのグループを作成する。本コマンドで作成したグループは、以下の各コマンドで `group` キーワードに続いて指定することができる。

- **ip dpi filter**
- **ipv6 dpi filter**
- **queue class filter**

*application\_list* には、アプリケーションやカテゴリーを表すニーモニックを並べて指定する。

*name* は、半角英数字、"-"(ハイフン)、および"\_"(アンダースコア)で、最大 32 文字以内で指定する。グループはルーターの揮発性メモリが許す限り作成することができる。

### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

### [設定例]

- 音楽ストリーミングアプリケーションを禁止する

```
# dpi group set 1000 name=music-streaming spotify google_play_music apple_music
amazon_music
# ip dpi filter 1 reject 1000
# ip dpi filter 100 pass * *
# ip lan2 dpi filter out 1 100
```

### [適用モデル]

NVR700W

## 49.6 シグネチャーのダウンロードの手動実行

### [書式]

```
dpi signature download go [no-confirm [prompt]] [force]
```

### [設定値及び初期値]

- `no-confirm`: 更新可能なシグネチャーが存在するときに、シグネチャーの更新を行うか否かを確認しない
  - [初期値]: -
- `prompt`: コマンド実行後、すぐにプロンプトを表示させ、他のコマンドを実行できるようにする
  - [初期値]: -
- `force`: 新しいシグネチャーの有無のチェックを行わず、強制的にシグネチャーをダウンロードする
  - [初期値]: -

### [説明]

DPI のシグネチャーのダウンロードや更新の手動実行をする。

シグネチャーのダウンロードに一度も成功していない状態で本コマンドを実行すると、配布サーバーからシグネチャーのダウンロードを試みる。ダウンロードに成功した場合、シグネチャーが DPI エンジンにロードされて DPI が使用可能な状態になる。

シグネチャーがダウンロードされている状態で本コマンドを実行した場合、配布サーバーに対して新しいシグネチャーの有無のチェックをして、更新可能なシグネチャーが存在すれば「更新しますか?(Y/N)」の確認を求める。「Y」を入力するとダウンロード、およびロードを行う。「N」を入力すると、更新を中止する。更新可能なシグネチャーがなければ、「新しいシグネチャーはありません。」と表示する。

`no-confirm` を指定すると、更新可能なシグネチャーが存在する場合に更新を行うか否かの確認を行わない。`prompt` を指定すると、コマンド実行直後にプロンプトが表示され、続けて他のコマンドを実行することができるようになる。

`force` を指定した場合には、新しいシグネチャーの有無のチェックを行わず、強制的にシグネチャーをダウンロードする。外部メモリにシグネチャーを保存したい場合に有効である。

新しいシグネチャーの有無のチェックやダウンロードに失敗した場合でも、リトライはしない。

本コマンドは、`dpi use` コマンドが `off` に設定されている場合には実行できない。

#### [ノート]

シグネチャーのダウンロードや更新は自動で行われるため、通常は本コマンドを実行する必要はない。自動でのダウンロードに失敗したときなどに、直ちにリトライした場合に使用する。

NVR700W は Rev.15.00.17 以降で使用可能。

#### [適用モデル]

NVR700W

## 49.7 シグネチャーのダウンロード先 URL の設定

---

#### [書式]

`dpi signature download url url`

`no dpi signature download url [url]`

#### [設定値及び初期値]

- `url`
  - [設定値]: シグネチャーを配布している URL を設定する
  - [初期値]:
    - `http://www.rtpro.yamaha.co.jp/signature/v1.1/rt_dpi_(機種名).ysig` ( NVR700W Rev.15.00.24 以降 )
    - `http://www.rtpro.yamaha.co.jp/signature/rt_dpi_(機種名).ysig` ( 上記以外 )

#### [説明]

個別に用意した Web サーバーを用いてシグネチャーを配布する場合に、シグネチャーが置かれている URL を 255 文字以内の半角英数字および半角記号で指定する。ヤマハの配信サーバーからシグネチャーをダウンロードして使用する場合には、本コマンドを設定する必要はない。

シグネチャーのダウンロードには、HTTP または HTTPS を使用できる。入力形式は以下の通りで、Web サーバーのアドレスは FQDN 形式のホスト名、もしくは IPv4 または IPv6 アドレスを指定する。

- `http[s]://(Web サーバーのアドレス):(ポート番号)/(パス名)`

ポート番号は HTTP の場合 80 番以外、HTTPS の場合 433 番以外を使用するとき指定する。

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

#### [適用モデル]

NVR700W

## 49.8 アプリケーションの識別に関するログを出力するか否かの設定

---

#### [書式]

`dpi log switch`

`no dpi log [switch]`

**[設定値及び初期値]**• *switch*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

- [初期値]: off

**[説明]**

DPI のアプリケーションの識別に関するログを出力するか否かの設定をする。

本コマンドを on に設定すると、アプリケーションの識別結果や識別処理に関するエラー情報を NOTICE レベルのログに出力する。

**[ノート]**

NVR700W は Rev.15.00.17 以降で使用可能。

**[適用モデル]**

NVR700W

## 49.9 DPI の統計情報の表示

**[書式]**

**show dpi statistics** [all]

**show dpi statistics** application *application* [detail]

**show dpi statistics** category *category*

**show dpi statistics** address *ip\_address*

**[設定値及び初期値]**• *application*

- [設定値]: アプリケーションを表すニーモニック
- [初期値]: -

• *category*

- [設定値]: "@"で始まるカテゴリーを表すニーモニック
- [初期値]: -

• *ip\_address*

- [設定値]: 端末の IPv4 または IPv6 アドレス
- [初期値]: -

**[説明]**

DPI の統計情報を表示する。

**show dpi statistics** コマンドをオプション無しで実行した場合、ルーターを通過するトラフィック全体に対して送信オクテット数と受信オクテット数の合計が上位 11 位以内のアプリケーションの送受信オクテット数と、全体に占める割合の高いものから表示する。all を指定した場合には、11 位以下の"other"にまとめられたアプリケーションの一覧を表示する

application に続いて *application* を指定した場合には、指定のアプリケーションに関する統計情報のみを表示する。*application* には **show dpi application** コマンドで表示されるアプリケーションのニーモニックを指定する。detail を指定した場合、端末ごとの情報も表示する。

category に続いて *category* を指定した場合には、指定のカテゴリーに属するアプリケーションに関する統計情報のみを表示する。*category* には "@" で始まる **show dpi category** コマンドで表示されるカテゴリーのニーモニックを指定する。カテゴリー内のアプリケーションは、アプリケーションのニーモニックを基準に、0-9、a-z の準に表示する。

address に続いて *ip\_address* に端末の IPv4 アドレスまたは IPv6 アドレスを指定した場合には、指定した端末の統計情報を表示する。

**[ノート]**

統計情報を記録できる端末の台数には上限がある。機種別の上限の台数は以下の通り。

| 機種      | 上限の台数 (台) |
|---------|-----------|
| NVR700W | 512       |

ルーターの揮発性メモリに記録されている統計情報は、以下の条件でクリアされる。

- ルーターの電源断
- ルーターの再起動
- **dpi use** コマンドを off に設定する、または削除する
- **clear dpi statistics** コマンドの実行

NVR700W は Rev.15.00.17 以降で使用可能。

#### [表示例]

```
# show dpi statistics
アプリケーション 送受信オクテット数 割合
-----+-----+-----
office365          18,754,987 25%
lync                15,854,347 21%
google_map         11,115,753 14%
facebook           9,835,354 11%
windows_update     6,354,682 8%
twitter            5,854,965 6%
dns                 5,032,886 5%
ftp                 4,258,369 4%
icmp                3,125,784 3%
imap                1,411,955 1%
other               1,923,854 2%
-----+-----+-----
合計                83,522,936 100%
```

```
# show dpi statistics application office365 detail
[office365]
```

```
                オクテット数
端末            送信            受信
-----+-----+-----
Total          88,258            131,564
 192.168.0.15  11,254            10,223
 192.168.0.68  48,256            58,825
      :
      :
```

```
# show dpi statistics category @game
[@game]
```

```
                オクテット数
アプリケーション 送信            受信
-----+-----+-----
akinator          456                1,675
all_slots_casino  11,254            10,223
      :
      :
```

```
# show dpi statistics address 192.168.0.15
[192.168.0.15]
```

```
                オクテット数
アプリケーション 送信            受信
-----+-----+-----
lync                32,645            1,556,998
office365           546                665,320
      :
      :
```

#### [適用モデル]

NVR700W

## 49.10 DPI の統計情報のクリア

### [書式]

```
clear dpi statistics
```

### [説明]

ルーターの揮発性メモリに保存された DPI の統計情報をクリアする。  
本コマンドを実行しても、外部メモリに記録された統計情報が削除されることはない。

### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

### [適用モデル]

NVR700W

## 49.11 識別結果のキャッシュの表示

### [書式]

```
show dpi cache
```

### [説明]

アプリケーションの識別結果のキャッシュを IPv4/IPv6 アドレスに分けて、0-9、a-z の順に表示する。TTL は分'秒'のフォーマットで表示する。

### [ノート]

NVR700W は Rev.15.00.22 以降で使用可能。

### [表示例]

```
# show dpi cache
エントリー数: 6
アプリケーション名      宛先 IP アドレス      ポート  TTL
-----+-----+-----+-----+
microsoft                203.0.113.254          443    58'41"
ntp                      203.0.113.110          123    51'38"
office365                203.0.113.31           443     6'25"
microsoft                2001:0db8:09ec:a541:20f7:3ba8:2808:bfd5 443    52'34"
ntp                      2001:0db8:e201:bc01:2951:c821:ba11:bbdd 123    12'56"
pokemon_go              2001:0db8:02c1:1bbb:5489:cde9:0001:ac19 443     2'12"
```

### [適用モデル]

NVR700W

## 49.12 識別結果のキャッシュのクリア

### [書式]

```
clear dpi cache
```

### [説明]

アプリケーションの識別結果のキャッシュをクリアする。

### [ノート]

NVR700W は Rev.15.00.22 以降で使用可能。

### [適用モデル]

NVR700W

## 49.13 アプリケーションを表すニーモニック一覧の表示

### [書式]

```
show dpi application [category]
```

**show dpi application detail** [*category*]

#### [設定値及び初期値]

- *category*
  - [設定値]: "@"で始まるカテゴリーを表すニーモニック
  - [初期値]: -
- *detail*: ニーモニックに加えて、アプリケーションの詳細情報を表示する
  - [初期値]: -

#### [説明]

**ip dpi filter** コマンド、**ipv6 dpi filter** コマンド、および、**queue class filter** コマンドで指定可能なアプリケーションを表すニーモニック一覧を 0-9、a-z の順に表示する。

*category* を指定した場合には、該当カテゴリーに属するアプリケーションを表すニーモニックのみを表示する。*category* には、**show dpi category** コマンドで表示される "@" で始まるニーモニックを指定する。*detail* キーワードを指定した場合には、アプリケーションの詳細情報を表示する。

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

#### [表示例]

```
# show dpi application
01net          050plus          0zz0          10050net
10086cn        104com           1111tw        1141a
115com         118114cn         11st          123people
1337x          139mail          15min         163com
17173com       17u              20min         24h
24ora          24sata           24ur          2ch
2shared        3366_com         360buy        360cn
3gpp_li        3pc              4399com       4chan
4shared        4tube           51_com        51_com_bbs
51_com_music  51_com_posting  51job         51la
---つづく---
```

```
# show dpi application detail @game
ニーモニック      説明
-----+-----
akinator          Akinator the Genie
all_slots_casino  All Slots Casino
angry_birds       Angry Birds
aniping           Anipang
battlenet         battlenet
bf1               Battlefield 1
bf4               Battlefield 4
bitstrips         BitStrips
candy_crush_saga  Candy Crush Saga
champion_football Champion Football
---つづく---
```

#### [適用モデル]

NVR700W

## 49.14 カテゴリーを表すニーモニック一覧の表示

#### [書式]

**show dpi category**  
**show dpi category detail**

#### [設定値及び初期値]

- *detail*: ニーモニックに加えて、カテゴリーの詳細情報を表示する
  - [初期値]: -

[説明]

**ip dpi filter** コマンド、**ipv6 dpi filter** コマンド、および、**queue class filter** コマンドで指定可能なカテゴリを表すニーモニック一覧を 0-9、a-z の順に、先頭に "@" を付加して表示する。

*detail* キーワードを指定した場合には、ニーモニックに加えてカテゴリの詳細情報を表示する。

[ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

[表示例]

```
# show dpi category
@antivirus          @app_service        @audio_video        @authentication
@behavioral         @compression        @database           @encrypted
@erp                @file_server        @file_transfer      @forum
@game              @instant_messaging @mail               @microsoft_office
@middleware         @network_management @network_service    @peer_to_peer
@printer           @routing            @security_service   @standard
@telephony         @terminal          @thin_client        @tunneling
@wap               @web                @webmail
```

```
# show dpi category detail
ニーモニック      詳細
-----+-----
@antivirus        Antivirus update
@app_service       Background service
@audio_video       Application/Protocol used to transport audio or video content
@authentication    Protocol used for authentication purposes
@behavioral        Protocol classified by non-deterministic criteria based on
statistical analysis of packet form and session behavior.
@compression       Compression layers
@database          Protocol used for database remote queries
@encrypted         Encryption protocol
@erp              Enterprise Resource Planning application
@file_server       File transfer protocol
---つづく---
```

[適用モデル]  
NVR700W

## 49.15 DPI の動作状態、およびシグネチャーの状態の表示

[書式]

**show status dpi**

[説明]

DPI の動作状態、およびシグネチャーの情報を表示する。

- DPI の状態

| 表示                       | 説明                                  |
|--------------------------|-------------------------------------|
| 無効                       | DPI の設定は無効である                       |
| ライセンス認証中                 | ライセンス認証中である                         |
| シグネチャーのダウンロード中           | シグネチャーをダウンロードしている                   |
| シグネチャーの読み込み中             | シグネチャーを読み込んでいる                      |
| 正常動作中                    | DPI は正常に動作している                      |
| 停止処理中                    | DPI の停止処理をしている                      |
| ライセンス認証失敗                | ライセンス認証に失敗して停止している、ライセンス認証の成功を待っている |
| シグネチャーのダウンロード失敗 (リトライ待ち) | シグネチャーのダウンロードに失敗し、リトライを待っている        |

| 表示         | 説明                                |
|------------|-----------------------------------|
| 異常停止中 (理由) | エラーが発生し、DPI は停止している(括弧内には異常理由を表示) |

- シグネチャ情報
  - バージョン：シグネチャのバージョン情報
  - ダウンロード日時：現在使用中のシグネチャをダウンロードした日時
    - 外部メモリのシグネチャを使用している場合には"外部メモリのシグネチャを使用中"と表示する
  - 最終更新チェック日時：最後にシグネチャの更新チェックを行った日時
  - 保存先：ダウンロードしたシグネチャの外部メモリ上の保存先
    - 保存しない場合には "-" を表示する

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

#### [表示例]

```
# show status dpi
現在の状態
  正常動作中
シグネチャの情報
  バージョン           Ver. 1.0.6
  最終ダウンロード日時  外部メモリのシグネチャを使用中
  最終更新チェック日時  2019/10/13 09:14:25
  保存先                usb1:/signature/rt_dpi_nvr700w.ysig
```

#### [適用モデル]

NVR700W



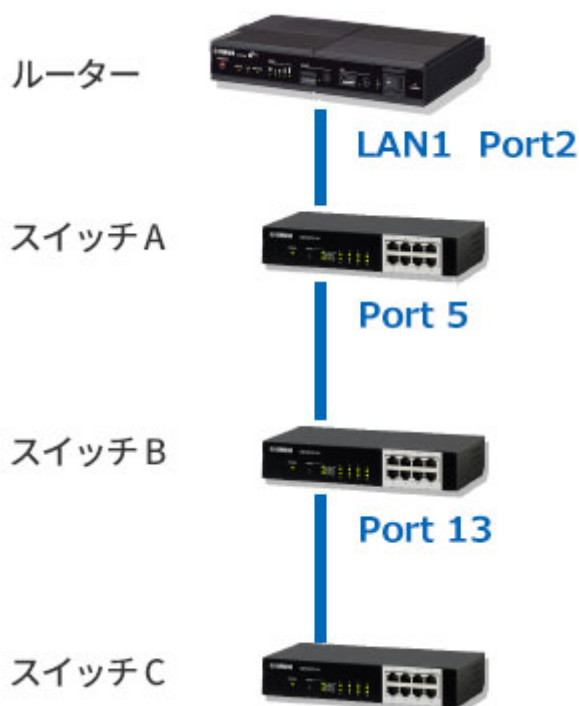
## 第 50 章

### L2MS

L2MS とは、ヤマハネットワーク機器 (スイッチ、無線 LAN アクセスポイント、ルーター) をルーターから制御するための機能です。L2MS では制御を行う機器をマネージャー、マネージャーから制御される機器をエージェントと呼びます。エージェントの制御を行うためには、共通の設定の他に、それぞれの機器に対応する制御コマンドを参照してください。

当機能の各コマンドでスイッチまたはアクセスポイントを指定する場合、MAC アドレスによる指定と経路による指定の 2 つの方法があります。

経路による指定方法では、ルーターを基点として途中にある各スイッチのポート番号を順に記述します。



上図のような構成でスイッチ C を指定する場合の表記は "lan1:2-5-13" となります。

- 最初にルーターの LAN インターフェースを指定します。
- LAN インターフェースがスイッチングハブである場合、ポート番号を指定します。LAN インターフェース名とポート番号の間はコロン ":" で区切ります。
- LAN インターフェースがスイッチングハブでない場合、ポート番号の指定は不要です。
- ルーターとスイッチ C の間にある各スイッチのポート番号をルーターに近い方から順に指定します。各ポート番号はハイフン "-" で区切ります。

L2MS によって制御できる機器の種類や対応ファームウェアバージョンの詳細については、以下に示す、L2MS の技術資料をご覧ください。

<http://www.rtpro.yamaha.co.jp/RT/docs/swctl/>

## 50.1 共通の設定

### 50.1.1 L2MS の動作モードの設定

[書式]

```
switch control mode mode
no switch control mode [mode]
```

[設定値及び初期値]

- mode
  - [設定値]:

| 設定値     | 説明                  |
|---------|---------------------|
| manager | L2MS のマネージャーとして動作する |
| agent   | L2MS のエージェントとして動作する |
| off     | L2MS を使用しない         |

- [初期値] : manager

#### [説明]

L2MS の動作モードを設定する。*mode* が **manager** である場合は L2MS のマネージャーとして動作する。*mode* が **agent** である場合は L2MS のエージェントとして動作する。

#### [ノート]

本コマンドを設定できるのは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアである。本コマンドが設定できないファームウェアは L2MS のマネージャーとして動作する。

manager オプションと agent オプションは NVR700W Rev.15.00.23 以降、NVR510 Rev.15.01.23 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 50.1.2 L2MS を使用するか否かの設定

#### [書式]

**switch control use interface use** [terminal=*terminal*]

**no switch control use interface** [*use* [terminal=*terminal*]]

#### [設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名、ブリッジインターフェース名
  - [初期値] : -
- *use*
  - [設定値] :

| 設定値 | 説明          |
|-----|-------------|
| on  | L2MS を使用する  |
| off | L2MS を使用しない |

- [初期値] : off
- *terminal*
  - [設定値] :

| 設定値 | 説明           |
|-----|--------------|
| on  | 端末情報の取得を行う   |
| off | 端末情報の取得を行わない |

- [初期値] : off

#### [説明]

L2MS を使用するか否かをインターフェースごとに設定する。*use* が **on** であるインターフェースで L2MS を使用する。L2MS は **switch control use** コマンドの設定にしたがって動作する。L2MS のマネージャーとして動作している場合は、L2MS に対応したエージェントを制御するための通信を行う。また、*terminal* オプションが **on** に設定されたインターフェースでは端末情報の取得も行う。L2MS を使用しないインターフェースでは *use* を **off** に設定することで不要なパケットの送出を抑えることができる。L2MS のエージェントとして動作している場合は、マネージャーからの探索パケットに対して応答パケットを返す。

#### [ノート]

**switch control mode** コマンドで *mode* に **off** が設定されている場合、本コマンドの設定は反映されない。

LAN 分割機能が有効になっているインターフェースでは本コマンドを設定することができない。

**bridge member** コマンドで LAN インターフェースが収容されていない場合、本コマンドのブリッジインターフェースへの設定は反映されない。また、ブリッジインターフェースとブリッジインターフェースに収容されている LAN

インターフェースで *use* に *on* を設定している場合、ブリッジインターフェースへの設定のみ反映される。ブリッジインターフェースで本コマンドを設定できるのは、NVR700W Rev.15.00.10 以降のファームウェアである。

*use* が *off* に設定されたインターフェースでは *terminal* オプションが *on* であっても端末情報の取得は行わない。また、L2MS のエージェントとして動作している場合、*terminal* オプションの設定は L2MS の動作に反映されない。

**[適用モデル]**

NVR700W, NVR510

### 50.1.3 エージェントの監視時間間隔の設定

**[書式]**

**switch control watch interval *time* [*count*]**

**no switch control watch interval**

**[設定値及び初期値]**

- *time*
  - [設定値]: 秒数 (2 .. 10)
  - [初期値]: 3
- *count*
  - [設定値]: 回数 (2 .. 10)
  - [初期値]: 3

**[説明]**

エージェントを探索するパケットの送信時間間隔、およびエージェントからの応答パケットを受信せずダウンしたと判断するまでの探索パケット送信回数を設定する。

*time* を大きな値に設定した場合、探索パケットの送信頻度は減るが、エージェントを接続してからマネージャーが認識するまでの時間が長くなる。*time* を小さな値に設定した場合はその逆となり、探索パケットの送信頻度は増えるが、エージェントを接続してからマネージャーが認識するまでの時間が短くなる。

探索パケットを *count* で設定した回数送信してもエージェントから応答パケットを受信しない場合、当該のエージェントはダウンしたと判断する。

**[ノート]**

**switch control mode** コマンドで *mode* に *manager* が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

エージェントを接続しているイーサネットケーブルを抜いた場合は、当コマンドの設定よりも早いタイミングでエージェントがダウンしたと判断することがある。

**[適用モデル]**

NVR700W, NVR510

### 50.1.4 端末情報の監視時間間隔の設定

**[書式]**

**lan-map terminal watch interval *time1* [*time2*]**

**no lan-map terminal watch interval [*time1* [*time2*]]**

**[設定値及び初期値]**

- *time1*
  - [設定値]: マネージャー/エージェント配下の端末情報を取得する間隔 (秒) (1800 .. 86400)
  - [初期値]: 1800
- *time2*
  - [設定値]: 端末の接続/切断を即時通知できないエージェント配下の端末情報を取得する間隔 (秒) (10 .. 86400)
  - [初期値]: 60

**[説明]**

LAN マップで管理しているネットワークの端末情報の定期取得を行う間隔を設定する。

マネージャーは、各エージェントからの端末の接続/切断の即時通知を契機に取得する端末情報と、指定の間隔で各エージェントに対して行う定期取得処理を契機に取得する端末情報を基に LAN マップの端末情報を更新している。ただし、端末の接続/切断を即時通知できるエージェントと、端末の接続/切断を即時通知できないエージェントがあり、それぞれで定期取得処理の実行間隔と目的が以下のように異なる。

- 定期取得 1

マネージャー、および端末の接続/切断を即時通知できるエージェントを対象機器として、*time1* に設定した時間が経過する度に端末情報を取得する。定期取得 1 は端末情報の補正を目的としている。端末の接続/切断を即時通知できるエージェント配下の端末の接続/切断は、*time1* の経過を待たずに LAN マップに即時に反映される。しかし、端末からの通信がなく、エージェントの MAC アドレステーブルに端末が登録されていなかった場合やパケットロスにより端末情報を受信できなかった場合、端末の接続は LAN マップに即時に反映されない。このような場合は、*time1* が経過する度に行う定期取得により、端末情報が取得できたときに LAN マップに反映される。

- 定期取得 2

端末の接続/切断を即時通知できないエージェントを対象機器として、*time2* に設定した時間が経過する度に端末情報を取得する。端末の接続/切断を即時通知できないエージェント配下の端末の接続/切断は、LAN マップに即時に反映されず、*time2* の間隔で反映される。

#### [ノート]

端末の接続/切断を即時通知できないエージェントは以下の無線 AP である。

- WLX202
- WLX302
- WLX313
- WLX402 (Rev.17.00.09 より前のファームウェア)

他のエージェントは端末の接続/切断の即時通知が可能である。

**switch control mode** コマンドで *mode* に *manager* が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

**switch control use** コマンドで *terminal* オプションに *on* が設定されていない場合、本コマンドの設定に関わらず、端末情報の補正、および更新は行わない。

#### [適用モデル]

NVR700W, NVR510

## 50.1.5 スナップショット機能を使用するか否かの設定

#### [書式]

```
lan-map snapshot use interface use [terminal=terminal]
no lan-map snapshot use interface [use [terminal=terminal]]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *terminal*
  - [設定値]:

| 設定値        | 説明               |
|------------|------------------|
| on         | 端末情報を含める         |
| off        | 端末情報を含めない        |
| wired-only | 有線接続された端末情報のみ含める |

- [初期値]: off

#### [説明]

LAN マップのスナップショット機能を使用するか否かをインターフェースごとに設定する。*terminal* オプションが *on* に設定されたインターフェースでは、端末情報がスナップショット機能の対象に含まれるようになる。*terminal*

オプションが `wired-only` に設定されたインターフェースでは、有線接続された端末情報のみがスナップショット機能の対象に含まれるようになる。無線接続された端末情報はスナップショット機能の対象には含まれない。

#### [ノート]

**switch control mode** コマンドで `mode` に `manager` が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

**switch control use** コマンドで `terminal` オプションが `on` に設定されていない場合、本コマンドの設定に関わらず、端末情報はスナップショット機能の対象に含まれない。

ブリッジインターフェースを指定できるのは、NVR700W Rev.15.00.10 以降のファームウェアである。

#### [適用モデル]

NVR700W, NVR510

## 50.1.6 スナップショットファイルを作成する

#### [書式]

```
take lan-map snapshot interface [update]
```

#### [設定値及び初期値]

- `interface`
  - [設定値]: LAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- `update`: ネットワークの接続状態を更新した後、スナップショットファイルを作成する
  - [初期値]: -

#### [説明]

LAN マップのスナップショット機能でベースとなるスナップショットファイルを作成する。`update` オプションが含まれない場合、現在マネージャーが保持しているネットワークの状態をスナップショットファイルとして保存する。`update` オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新した後、スナップショットファイルとして保存する。

#### [ノート]

**switch control mode** コマンドで `mode` に `manager` が設定されている場合、本コマンドを使用できる。

スナップショットファイルの作成を開始すると、以下の SYSLOG が出力される。

```
[LANMAP] SnapShot(LAN1): Take snapshot files: Start.
```

スナップショットファイルの作成が完了すると、以下の SYSLOG が出力される。

```
[LANMAP] SnapShot(LAN1): Take snapshot files: Complete.
```

`update` オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新するが、ネットワークの構成によっては更新が完了するまでに時間がかかる場合がある。

ブリッジインターフェースを指定できるのは、NVR700W Rev.15.00.10 以降のファームウェアである。

#### [適用モデル]

NVR700W, NVR510

## 50.1.7 LAN マップの SYSLOG 出力の設定

#### [書式]

```
lan-map log sw
```

```
no lan-map log [sw]
```

#### [設定値及び初期値]

- `sw`
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 出力する  |
| off | 出力しない |

- [初期値]: off

## [説明]

LAN マップに関する SYSLOG 出力の設定をする。

## [適用モデル]

NVR700W, NVR510

## 50.1.8 LAN マップで使用する機器名の設定

---

## [書式]

**lan-map sysname** *name*

**no lan-map sysname** [*name*]

## [設定値及び初期値]

- *name*
  - [設定値]: 機器名 (半角 1 文字以上、32 文字以下)
  - [初期値]: (製品名称)\_(シリアル番号)

## [説明]

LAN マップで表示する機器名を設定をする。 *name* に使用できる文字は、半角英数字、ハイフン (-)、アンダーバー ( \_)、および半角スペース ( )。半角スペースを含ませるためには、 *name* 全体をダブルクォーテーション (" )、またはシングルクォーテーション ( ' )で囲む。

## [ノート]

本コマンドを設定できるのは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアである。

## [適用モデル]

NVR700W, NVR510

## 50.2 スイッチの制御

---

### 50.2.1 スイッチの選択

---

## [書式]

**switch select** *switch*

**no switch select**

## [設定値及び初期値]

- *switch*
  - [設定値]:

| 設定値  | 説明             |
|------|----------------|
| スイッチ | MAC アドレスもしくは経路 |
| none | スイッチを選択しない     |

- [初期値]: -

## [説明]

対象とするスイッチを選択する。以降プロンプトには console prompt で設定した文字列と選択したスイッチが続けて表示される。

**switch select none** または **no switch select** を実行すると、プロンプトにスイッチを表示しなくなる。

## [適用モデル]

NVR700W, NVR510

### 50.2.2 スイッチが持つ機能の設定

---

## [書式]

**switch control function set** *function* [*index ...*] *value*

**no switch control function set** *function* [*index ...*]

## [設定値及び初期値]

- *function*
  - [設定値]: 機能の名前

- [初期値]:-
- *index*
  - [設定値]: インデックス
  - [初期値]:-
- *value*
  - [設定値]: 設定値
  - [初期値]:-

**[説明]**

スイッチが持つ機能について設定を行う。設定したい機能の名前とその機能に対する設定値をパラメーターとして指定する。複数の設定対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。ただし、実行後に同期処理が開始された場合は中断できない。

**[ノート]**

本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

**[適用モデル]**

NVR700W, NVR510

### 50.2.3 スイッチが持つ機能の設定内容や動作状態の取得

---

**[書式]**

```
switch control function get function [index ...] [switch]
```

**[設定値及び初期値]**

- *function*
  - [設定値]: 機能の名前
  - [初期値]:-
- *index*
  - [設定値]: インデックス
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

スイッチが持つ機能の設定内容や動作状態を取得する。取得したい機能の名前をパラメーターとして指定する。複数の取得対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。

**[ノート]**

*switch* を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

**[適用モデル]**

NVR700W, NVR510

### 50.2.4 スイッチに対して特定の動作を実行

---

**[書式]**

```
switch control function execute function [index ...] [switch]
```

**[設定値及び初期値]**

- *function*
  - [設定値]: 機能の名前
  - [初期値]:-
- *index*
  - [設定値]: インデックス

- [初期値]:-
- *switch*: スイッチ
- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]:-

**[説明]**

スイッチに対して特定の動作を実行させる。実行したい動作に対応する機能の名前をパラメーターとして指定する。複数の実行対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。

**[ノート]**

*switch* を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

**[適用モデル]**

NVR700W, NVR510

## 50.2.5 スイッチの設定の削除

---

**[書式]**

**switch control function default [both] [switch]**

**[設定値及び初期値]**

- *both*: 対象のスイッチに対して適用可能な設定をすべて削除する
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

選択したスイッチに対するルーター上の設定を削除する。同時に、ルーターがスイッチを制御している場合は同期処理を行う。

*both* オプションを指定しない場合、スイッチに対して適用可能な他の設定が存在すれば、その設定でスイッチを同期する。例えば、MAC アドレス指定と経路指定の設定が存在する状態で、MAC アドレス指定の設定を選択して本コマンドを実行した場合、MAC アドレス指定の設定が削除された後、スイッチは経路指定の設定で同期される。

*both* オプションを指定する場合、スイッチに対して適用可能な他の設定が存在すれば、その設定も同時に削除する。上記の例では、MAC アドレス指定と経路指定の両方の設定が削除される。

すなわち、スイッチを確実に初期化したい場合は *both* オプションを指定する。

**[ノート]**

*switch* を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

**[適用モデル]**

NVR700W, NVR510

## 50.2.6 スイッチのファームウェアの更新

---

**[書式]**

**switch control firmware upload go file [switch]**

**[設定値及び初期値]**

- *file*
  - [設定値]: ファームウェアのファイルへの相対パスまたは絶対パス
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス



- 経路
- [初期値]:-

#### [説明]

スイッチのファームウェアを更新する。ファームウェアのファイルはフラッシュ ROM や外部メモリへ事前に保存しておき、*file* にパスを指定する。ファームウェアの書き換えに成功すると、スイッチは自動的に再起動する。

コマンド実行中に Ctrl-C 押下で中断することができる。

*file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

#### [ノート]

*switch* を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

#### [適用モデル]

NVR700W, NVR510

## 50.2.7 LAN ケーブル二重化機能の設定

---

#### [書式]

```
switch control route backup route port
no switch control route backup route
```

#### [設定値及び初期値]

- *route*
  - [設定値]: メイン経路
  - [初期値]: -
- *port*
  - [設定値]: バックアップ経路として使用するポート番号
  - [初期値]: -

#### [説明]

LAN ケーブル二重化機能を動作させるメイン経路とバックアップ経路を設定する。

*route* で指定した経路をメイン経路、*port* に接続される先の経路をバックアップ経路として、LAN ケーブル二重化機能が動作する。

#### [ノート]

以下のポートを *port* に設定することはできない

- *route* でメイン経路として指定したポート
- 既に LAN ケーブル二重化機能が設定されているポート

ルーターのスイッチングハブに対して本コマンドを設定した場合、設定した LAN インターフェースで **switch control use** コマンドが on に設定されているときのみ、LAN ケーブル二重化機能が動作する。

スイッチに対して本コマンドを設定した場合、当該ポートが一時的にリンクダウンする。

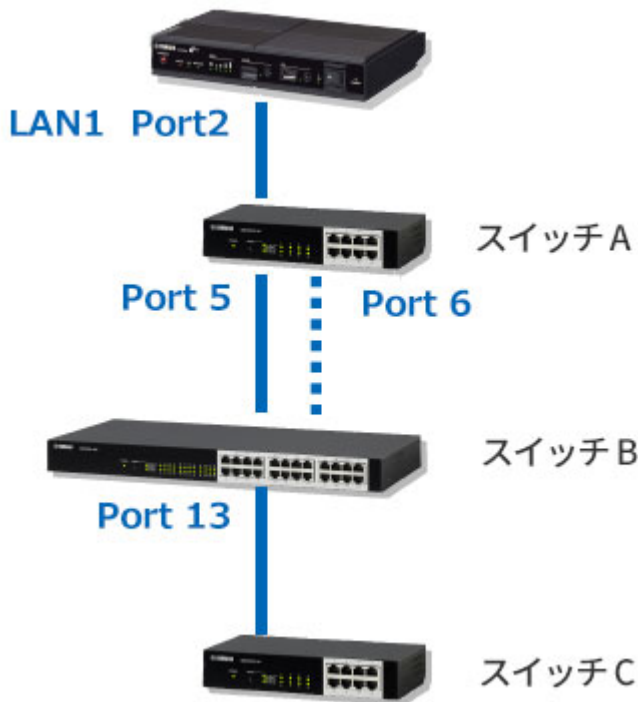
LAN ケーブル二重化機能の動作状態は **show status switch control route backup** コマンドで確認できる。

スイッチに本機能が実装されていない場合はコマンドエラーとなる。

#### [設定例]

下図のようにスイッチ A のポート 5 をメイン経路、ポート 6 をバックアップ経路とする場合の設定

```
switch control route backup lan1:2-5 6
```



[適用モデル]  
NVR700W, NVR510

## 50.2.8 スイッチの設定ファイルを格納するディレクトリの指定

---

### [書式]

```
switch config directory path
no switch config directory [path]
```

### [設定値及び初期値]

- *path*
  - [設定値]: 相対パスまたは絶対パス (半角 256 文字以下、全角 128 文字以下)
  - [初期値]: /sw\_config

### [説明]

スイッチの設定ファイル(config)を格納するディレクトリを指定する。  
相対パスを指定した場合、環境変数 PWD を起点としたパスと解釈される。  
PWD は **set** コマンドで変更可能であり、初期値は "/" である。  
*path* が RTFS 領域となる場合には、*path* にマルチバイト文字を使用することはできない。

### [ノート]

NVR700W は Rev.15.00.14 以降で使用可能。  
NVR510 は Rev.15.01.13 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 50.2.9 スイッチの設定を保存するファイル名の指定

---

### [書式]

```
switch config filename name
no switch config filename [name]
```

### [設定値及び初期値]

- *name*
  - [設定値]: config ファイル名 (半角 99 文字以下、全角 49 文字以下)
  - [初期値]: -

**[説明]**

スイッチの設定を保存するファイル名を指定する。

このコマンドが省略された場合は、**switch select** で指定された文字列に **.conf** を付けたものをファイル名とする。

ただし:(コロン)は\_(アンダースコア)に置き換えられる。

複数の **switch select** コマンドで同じファイル名を指定することができる。

**switch config directory** コマンドで指定したディレクトリが RTFS 領域である場合は、ファイル名にマルチバイト文字を使用することはできない。

本コマンドを実行する前に **switch select** コマンドでスイッチを指定しておく必要がある。

**[ノート]**

NVR700W は Rev.15.00.14 以降で使用可能。

NVR510 は Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.2.10 スイッチの設定の取得****[書式]**

```
switch control config get [switch]
```

```
switch control config get [[interface] all]
```

**[設定値及び初期値]**• *switch*

- [設定値]:

| 設定値            | 説明         |
|----------------|------------|
| MAC アドレスもしくは経路 | 選択したスイッチのみ |
| all            | 全てのスイッチ    |

- [初期値]:-

• *interface*

- [設定値]: LAN インターフェース名、ブリッジインターフェース名
- [初期値]:-

**[説明]**

スイッチの設定ファイルを取得して保存する。

*switch* パラメータに MAC アドレスもしくは経路を指定した場合は、指定したスイッチの設定ファイルを取得する。

**all** を指定すると、マネージャーが認識している全てのスイッチの設定ファイルを取得する。

*interface* パラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。

*interface* パラメータを省略した場合は、**all** を指定した時と同様になる。

**[ノート]**

スイッチの設定ファイルの名前には、**switch config filename** コマンドで指定したファイル名を使用する。

スイッチの設定ファイルは **switch config directory** コマンドで指定したディレクトリに保存される。

**schedule at** コマンドで指定することができる。

NVR700W は Rev.15.00.14 以降で使用可能。

NVR510 は Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.2.11 スイッチの設定の復元****[書式]**

```
switch control config set [switch]
```

```
switch control config set [[interface] all]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:

| 設定値            | 説明         |
|----------------|------------|
| MAC アドレスもしくは経路 | 選択したスイッチのみ |
| all            | 全てのスイッチ    |

- [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -

**[説明]**

マネージャーに保存されているスイッチの設定ファイルを使用して、スイッチの設定を復元する。  
*switch* パラメータに MAC アドレスもしくは経路を指定した場合は、指定したスイッチの設定を復元する。  
 all を指定すると、マネージャーが認識している全てのスイッチの設定を復元する。  
*interface* パラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。  
*interface* パラメータを省略した場合は、all を指定した時と同様になる。

**[ノート]**

復元に使用するスイッチの設定ファイルには、**switch config filename** コマンドで指定した設定ファイルを使用する。  
 スwitchの設定ファイルは **switch config directory** コマンドで指定したディレクトリに保存されている必要がある。  
**schedule at** コマンドで指定することができる。  
 NVR700W は Rev.15.00.14 以降で使用可能。  
 NVR510 は Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.2.12 スwitchのゼロコンフィグ機能を使用するか否かの設定****[書式]**

**switch control config-auto-set use use**  
**no switch control config-auto-set use [use]**

**[設定値及び初期値]**

- *use*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

**[説明]**

Switchのゼロコンフィグ機能を使用するか否かを設定する。  
 Switchのゼロコンフィグ機能が有効かつ、L2MS エージェントのヤマハSwitchの設定（コンフィグ）が保存されている場合、工場出荷状態の L2MS エージェントがネットワークに接続されたときに、保存されている設定（コンフィグ）を自動で設定する。

**[ノート]**

NVR510 Rev.15.01.25 以降で使用可能。

**[適用モデル]**

NVR510

## 50.3 スイッチの機能

---

### 50.3.1 システム

---

#### 50.3.1.1 BootROM バージョンの取得

##### [書式]

**switch control function get boot-rom-version** [*switch*]

##### [設定値及び初期値]

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

##### [説明]

BootROM バージョンを取得する。

##### [適用モデル]

NVR700W, NVR510

#### 50.3.1.2 ファームウェアリビジョンの取得

##### [書式]

**switch control function get firmware-revision** [*switch*]

##### [設定値及び初期値]

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

##### [説明]

ファームウェアリビジョンを取得する。

##### [適用モデル]

NVR700W, NVR510

#### 50.3.1.3 シリアル番号の取得

##### [書式]

**switch control function get serial-number** [*switch*]

##### [設定値及び初期値]

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

##### [説明]

シリアル番号を取得する。

##### [適用モデル]

NVR700W, NVR510

#### 50.3.1.4 製品名称の取得

##### [書式]

**switch control function get model-name** [*switch*]

**[設定値及び初期値]**

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

製品名称を取得する。

**[適用モデル]**

NVR700W, NVR510

**50.3.1.5 MAC アドレスの取得****[書式]**

```
switch control function get system-macaddress [switch]
```

**[設定値及び初期値]**

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

MAC アドレスを取得する。

**[適用モデル]**

NVR700W, NVR510

**50.3.1.6 機器の名前の設定****[書式]**

```
switch control function set system-name name
no switch control function set system-name
switch control function get system-name [switch]
```

**[設定値及び初期値]**

- *name*
  - [設定値]: 機器の名前 (1 文字以上、64 文字以下)
  - [初期値]: (製品名称)\_(シリアル番号)
- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

機器の名前を設定する。*name* に使用できる文字は、半角英数字およびハイフン (-)、アンダーバー (\_)。

**[適用モデル]**

NVR700W, NVR510

**50.3.1.7 省電力機能を使用するか否かの設定****[書式]**

```
switch control function set energy-saving mode
no switch control function set energy-saving
switch control function get energy-saving [switch]
```

**[設定値及び初期値]**

- *mode*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *switch*: スイッチ

- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]: -

#### [説明]

LAN ポートの省電力機能を使用するか否かを設定する。

#### [ノート]

本機能の設定を変更すると、全てのポートが一時的にリンクダウンする。

#### [適用モデル]

NVR700W, NVR510

### 50.3.1.8 LED の輝度の調整

#### [書式]

```
switch control function set led-brightness mode
no switch control function set led-brightness
switch control function get led-brightness [switch]
```

#### [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値     | 説明  |
|---------|-----|
| normal  | 明るい |
| economy | 暗い  |

- [初期値]: normal
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

#### [説明]

LED の輝度を調整する。

#### [適用モデル]

NVR700W, NVR510

### 50.3.1.9 LED の表示モードの取得

#### [書式]

```
switch control function get status-led-mode [switch]
```

#### [設定値及び初期値]

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

## [説明]

LAN ポートごとの LED の現在の表示モードを取得する。

| 表示モード    | 説明                                                                                                                                                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| link/act | 各ポートのリンク状態を表示する。<br><ul style="list-style-type: none"> <li>緑色で点灯: リンク確立状態</li> <li>緑色で点滅: データ転送中</li> <li>消灯: リンク喪失状態</li> </ul>                    |
| speed    | 各ポートの接続速度を表示する。<br><ul style="list-style-type: none"> <li>緑色で点灯: 1000BASE-T で接続</li> <li>橙色で点灯: 100BASE-TX で接続</li> <li>消灯: 10BASE-T で接続</li> </ul> |
| duplex   | 各ポートの接続状態 (全二重/半二重) を表示する。<br><ul style="list-style-type: none"> <li>緑色で点灯: 全二重で接続</li> <li>橙色で点灯: 半二重で接続</li> </ul>                                |
| status   | 機器の状態を表示。<br><ul style="list-style-type: none"> <li>橙色で点灯: ループを検出</li> </ul> SWX2200-24G でファンの故障を検知した場合は、モード LED 下側が橙色で点滅する。                        |

## [適用モデル]

NVR700W, NVR510

## 50.3.1.10 ファンの状態の取得

## [書式]

**switch control function get status-fan** [*switch*]

## [設定値及び初期値]

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

## [説明]

ファンの状態を取得する。

| 状態     | 説明 |
|--------|----|
| normal | 正常 |
| lock   | 異常 |

## [ノート]

SWX2200-24G、SWX2200-8PoE でのみ使用可能。

## [適用モデル]

NVR700W, NVR510

## 50.3.1.11 ファンの回転数の取得

## [書式]

**switch control function get status-fan-rpm** *FAN* [*switch*]

## [設定値及び初期値]

- *FAN*
  - [設定値]: ファン番号
  - [初期値]: -
- *switch*: スイッチ



- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]:-

**[説明]**

ファンの回転数を取得する。

**[ノート]**

SWX2200-8PoE でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.1.12 再起動****[書式]**

**switch control function execute restart** [*switch*]

**[設定値及び初期値]**

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

機器を再起動する。

**[適用モデル]**

NVR700W, NVR510

**50.3.1.13 起動してからの時間の取得****[書式]**

**switch control function get system-uptime** [*switch*]

**[設定値及び初期値]**

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

起動してからの時間を取得する。

**[適用モデル]**

NVR700W, NVR510

**50.3.2 ポート**

---

**50.3.2.1 リンクアグリゲーションのタイプの取得****[書式]**

**switch control function get lag-type** [*switch*]

**[設定値及び初期値]**

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

リンクアグリゲーションのタイプを取得する。

| 状態         | 説明                                       |
|------------|------------------------------------------|
| Not bundle | リンクアグリゲーションが設定されていない                     |
| Type-A     | グループ#1: ポート 21, 22                       |
| Type-B     | グループ#1: ポート 21, 22    グループ#2: ポート 23, 24 |
| Type-C     | グループ#1: ポート 21, 22, 23, 24               |

**[ノート]**

SWX2100-24G でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.2 ポートの通信速度および動作モードの設定****[書式]**

```
switch control function set port-speed port speed
no switch control function set port-speed port
switch control function get port-speed port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *speed*: 通信速度および動作モード
  - [設定値]:

| 設定値      | 説明             |
|----------|----------------|
| auto     | 速度自動判別         |
| 1000-fdx | 1000BASE-T 全二重 |
| 100-fdx  | 100BASE-TX 全二重 |
| 100-hdx  | 100BASE-TX 半二重 |
| 10-fdx   | 10BASE-T 全二重   |
| 10-hdx   | 10BASE-T 半二重   |

- [初期値]: auto
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

ポートの通信速度および動作モードを設定する。

**[ノート]**

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.3 ポートを使用するか否かの設定****[書式]**

```
switch control function set port-use port mode
no switch control function set port-use port
```

**switch control function get port-use port [switch]****[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

ポートを使用するか否かを設定する。本機能を off に設定すると、当該ポートに LAN ケーブルを接続してもリンクアップしなくなる。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.4 オートクロスオーバー機能を使用するか否かの設定****[書式]**

```
switch control function set port-auto-crossover port mode
no switch control function set port-auto-crossover port
switch control function get port-auto-crossover port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

オートクロスオーバー機能を使用するか否かを設定する。

オートクロスオーバー機能とは、LAN ケーブルがストレートケーブルかクロスケーブルかを自動的に判定して接続する機能である。本機能を on に設定すると、ケーブルのタイプがどのようなものであるかを気にする必要がなくなる。

**[ノート]**

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]  
NVR700W, NVR510

### 50.3.2.5 速度ダウンシフト機能を使用するか否かの設定

#### [書式]

```
switch control function set port-speed-downshift port mode
no switch control function set port-speed-downshift port
switch control function get port-speed-downshift port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

#### [説明]

速度ダウンシフト機能を使用するか否かを設定する。

速度ダウンシフト機能とは、例えば 1000BASE-T で使用できない LAN ケーブルを接続された時に速度を落としてリンクを試みる機能である。

#### [ノート]

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]  
NVR700W, NVR510

### 50.3.2.6 フロー制御を使用するか否かの設定

#### [書式]

```
switch control function set port-flow-control port mode
no switch control function set port-flow-control port
switch control function get port-flow-control port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:

- MAC アドレス
- 経路
- [初期値]:-

**[説明]**

フロー制御を使用するか否かを設定する。

本機能を on に設定すると、受信側と送信側の両方でフロー制御が有効になる。全二重でリンクアップしている場合は IEEE802.3x、半二重の場合はバックプレッシャ方式による制御がそれぞれ行われる。

**[ノート]**

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.7 L2MS パケットを遮断するか否かの設定****[書式]**

```
switch control function set port-blocking-control-packet port mode
no switch control function set port-blocking-control-packet port
switch control function get port-blocking-control-packet port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *mode*
  - [設定値]:

| 設定値 | 説明           |
|-----|--------------|
| on  | 制御パケットを遮断する  |
| off | 制御パケットを遮断しない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

L2MS パケットを遮断するか否かを設定する。本機能を on に設定すると、当該ポートでスイッチを制御するための通信が行われなくなる。

**[ノート]**

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.8 L2MS パケット以外のデータパケットを遮断するか否かの設定****[書式]**

```
switch control function set port-blocking-data-packet port mode
no switch control function set port-blocking-data-packet port
switch control function get port-blocking-data-packet port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *mode*

- [設定値]:

| 設定値 | 説明            |
|-----|---------------|
| on  | データパケットを遮断する  |
| off | データパケットを遮断しない |

- [初期値]: off
- *switch*: スイッチ

- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]: -

#### [説明]

L2MS パケット以外のデータパケットを遮断するか否かを設定する。本機能を on に設定すると、当該ポートでスイッチを制御するための通信以外のデータ通信が行われなくなる。

#### [ノート]

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

#### [適用モデル]

NVR700W, NVR510

### 50.3.2.9 コンボポートの使用状況の取得

#### [書式]

```
switch control function get status-combo-port port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

#### [説明]

ポートが SFP と Ethernet のどちらで使用されているかを取得する。

| 状態       | 説明                |
|----------|-------------------|
| disable  | ポートが使用されていない      |
| sfp      | SFP ポートとして使用されている |
| ethernet | イーサポートとして使用されている  |

#### [ノート]

SWX2100-24G でのみ使用可能。

#### [適用モデル]

NVR700W, NVR510

### 50.3.2.10 ポートの受光レベルの取得

#### [書式]

```
switch control function get status-port-sfp-rx-power port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

SFP ポートの受光レベルを取得する。

| 状態     | 説明                |
|--------|-------------------|
| normal | 正常                |
| low    | 受光レベルが下限閾値を下回っている |
| high   | 受光レベルが上限閾値を超えている  |

**[ノート]**

SWX2100-24G でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.2.11 ポートのリンク状態の取得**

**[書式]**

**switch control function get status-port-speed *port* [*switch*]**

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

ポートの現在のリンク状態を取得する。

| 状態       | 説明             |
|----------|----------------|
| 1000-fdx | 1000BASE-T 全二重 |
| 100-fdx  | 100BASE-TX 全二重 |
| 100-hdx  | 100BASE-TX 半二重 |
| 10-fdx   | 10BASE-T 全二重   |
| 10-hdx   | 10BASE-T 半二重   |
| down     | リンクダウン         |

**[適用モデル]**

NVR700W, NVR510

**50.3.3 MAC アドレステーブル**

ヤマハスイッチの MAC アドレステーブルの大きさは以下の通りです。

| 機種                      | 最大エントリ数 |
|-------------------------|---------|
| SWX2200-24G             | 8192    |
| SWX2200-8G、SWX2200-8PoE |         |

## 50.3.3.1 MAC アドレスエイジング機能を使用するか否かの設定

## [書式]

```
switch control function set macaddress-aging mode
no switch control function set macaddress-aging
switch control function get macaddress-aging [switch]
```

## [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

## [説明]

MAC アドレスエイジング機能を使用するか否かを設定する。

MAC アドレスエイジング機能とは、スイッチが持つ MAC アドレステーブル内のエントリを一定時間で消去していく機能である。本機能を off に設定すると、一度スイッチが学習した MAC アドレスは自動的に消去されない。

消去する時間間隔は **macaddress-aging-timer** で設定する。

## [適用モデル]

NVR700W, NVR510

## 50.3.3.2 MAC アドレスエイジングの時間間隔の設定

## [書式]

```
switch control function set macaddress-aging-timer time
no switch control function set macaddress-aging-timer
switch control function get macaddress-aging-timer [switch]
```

## [設定値及び初期値]

- *time*
  - [設定値]: 秒数 (10 .. 64800)
  - [初期値]: 300

## [説明]

MAC アドレスエイジング機能において、スイッチが学習した MAC アドレスを消去する時間間隔を設定する。

スイッチが MAC アドレスを学習してからエントリを消去するまでの時間は、最短で本機能で設定した秒数、最長でその 2 倍の秒数となる。例えば設定値が 300 秒だった場合、最短 300 秒、最長 600 秒となる。

なお、一度学習した MAC アドレスからのフレームを再度受信した場合、当該エントリが消去されるまでの時間はリセットされる。

## [適用モデル]

NVR700W, NVR510

## 50.3.3.3 MAC アドレスをキーにした MAC アドレステーブルの検索

## [書式]

```
switch control function get status-macaddress-addr mac_address [switch]
```

## [設定値及び初期値]

- *mac\_address*
  - [設定値]: MAC アドレス
  - [初期値]: -



- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

MAC アドレスをキーにして MAC アドレステーブルを検索し、当該 MAC アドレスを学習したポート番号を取得する。同一の MAC アドレスを異なる VLAN で学習している場合は、ポート番号が複数表示されることがある。

**[適用モデル]**

NVR700W, NVR510

**50.3.3.4 ポート番号をキーにした MAC アドレステーブルの検索****[書式]**

```
switch control function get status-macaddress-port port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

ポート番号をキーにして MAC アドレステーブルを検索し、当該ポートで学習した MAC アドレスを取得する。同一の MAC アドレスを異なる VLAN で学習している場合は、複数のポートで同一の MAC アドレスが表示される場合がある。

**[適用モデル]**

NVR700W, NVR510

**50.3.3.5 MAC アドレステーブルのエントリの消去****[書式]**

```
switch control function execute clear-macaddress-table [switch]
```

**[設定値及び初期値]**

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

MAC アドレステーブルの全エントリを消去する。

**[適用モデル]**

NVR700W, NVR510

**50.3.4 VLAN**

ヤマハスイッチでポート VLAN / タグ VLAN の設定を行う場合、コマンドでは VLAN ID を直接入力せず、VLAN 登録番号を指定します。VLAN 登録番号と VLAN ID の紐付けは **vlan-id** で行います。例えば以下のような設定を行った場合、ポート 2 の VLAN ID は 4 になります。

```
switch control function set vlan-id 10 4
switch control function set vlan-access 2 10
```

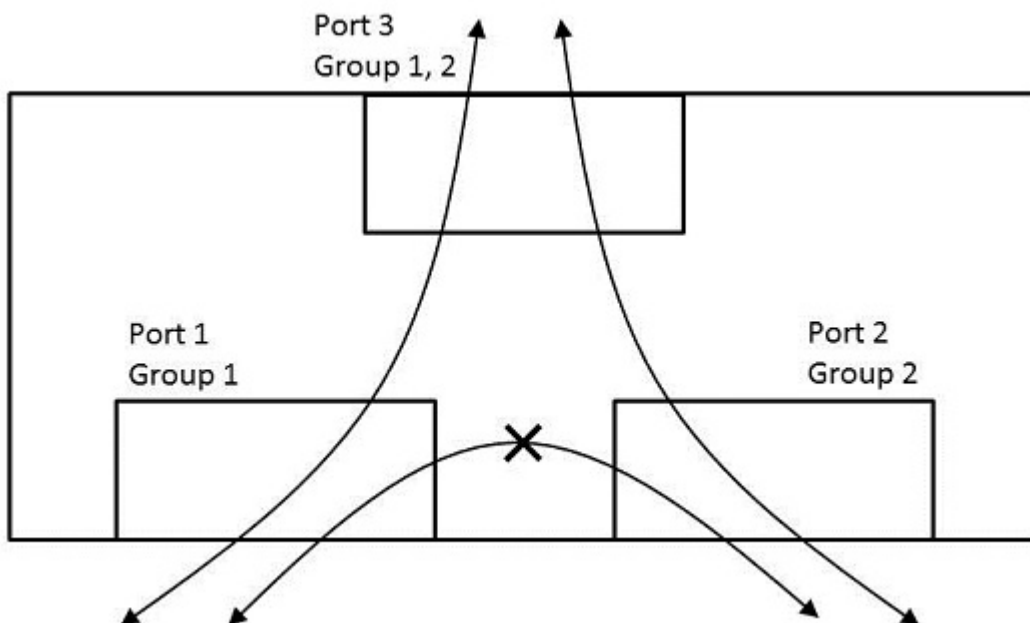
スイッチで受信したパケットは、VLAN タグの有無に関わらずいずれかの VLAN ID に分類され、その情報に基づいて転送処理が行われます。ポートの VLAN 動作モードは **vlan-port-mode** で設定します。

| vlan-port-mode | 受信時の動作                                                                                                                                        | 送信時の動作                                                                                                                                                                                |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access         | VLAN タグ無しのパケットのみ受信します。VLAN ID の分類は <b>vlan-access</b> の設定に基づいて行われます。                                                                          | 受信時に、送信するポートの VLAN ID ( <b>vlan-access</b> ) に分類されたパケットを VLAN タグ無しで送信します。                                                                                                             |
| trunk          | VLAN タグ付きのパケットのみ受信します。ただし、VLAN タグ中の VLAN ID にポートが参加している必要があります。ポートが参加する VLAN ID は <b>vlan-trunk</b> で設定します。VLAN ID の分類は VLAN タグの情報に基づいて行われます。 | 受信時に、送信するポートが参加する VLAN ID ( <b>vlan-trunk</b> ) に分類されたパケットを VLAN タグ付きで送信します。                                                                                                          |
| hybrid         | VLAN タグ付き、VLAN タグ無し、両方のパケットを受信します。VLAN タグ無しのパケットを受信した場合は、アクセスポートと同様の動作をします。VLAN タグ付きのパケットを受信した場合は、トランクポートと同様の動作をします。                          | 受信時に、送信するポートの VLAN ID ( <b>vlan-access</b> ) に分類されたパケットを VLAN タグ無しで送信します。また、受信時に、送信するポートが参加する VLAN ID ( <b>vlan-trunk</b> ) に分類されたパケットを VLAN タグ付きで送信します。どちらにも該当する場合は、VLAN タグ無しで送信します。 |

マルチプル VLAN は、1つのスイッチにおいてポートをグループに分けて、グループ間の通信を禁止する機能です。

**vlan-multiple-use** で機能を有効にした後、**vlan-multiple** でポートが所属するグループ番号を指定します。1つのポートを複数のグループに所属させることができます。あるポートで受信したパケットは、当該ポートと同じグループ番号に所属する他のポートから送信されます。

例として、以下のような設定を行った場合を考えます。



```
switch control function set vlan-multiple-use on
switch control function set vlan-multiple 1 1 join
switch control function set vlan-multiple 2 2 join
switch control function set vlan-multiple 3 1 join
switch control function set vlan-multiple 3 2 join
```

- ポート 1 で受信したパケットはポート 3 からのみ送信されます。
- ポート 2 で受信したパケットはポート 3 からのみ送信されます。
- ポート 3 で受信したパケットはポート 1 とポート 2 から送信されます。

マルチプル VLAN はネットワークを分割するものではないので、異なるグループ間でも同一のネットワークアドレスが割り振られます。

ポート VLAN / タグ VLAN とマルチプル VLAN を併用する場合、マルチプル VLAN において同一のグループに所属するポート間であっても、ポート VLAN / タグ VLAN において同一の VLAN に所属していない場合は通信することができません。

#### 50.3.4.1 VLAN ID の設定

##### [書式]

```
switch control function set vlan-id vlan_register_num vid
no switch control function set vlan-id vlan_register_num
switch control function get vlan-id vlan_register_num [switch]
```

##### [設定値及び初期値]

- *vlan\_register\_num*
  - [設定値]: VLAN 登録番号 (1 .. 256)
  - [初期値]: -
- *vid*
  - [設定値]: VLAN ID (1 .. 4094)
  - [初期値]: VLAN 登録番号と同じ値
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

##### [説明]

VLAN 登録番号に対して VLAN ID を設定する。

##### [適用モデル]

NVR700W, NVR510

#### 50.3.4.2 ポートの VLAN 動作モードの設定

##### [書式]

```
switch control function set vlan-port-mode port mode
no switch control function set vlan-port-mode port
switch control function get vlan-port-mode port [switch]
```

##### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*: VLAN 動作モード
  - [設定値]:

| 設定値    | 説明        |
|--------|-----------|
| access | アクセスポート   |
| trunk  | トランクポート   |
| hybrid | ハイブリッドポート |

- [初期値]: access
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

##### [説明]

ポートの VLAN 動作モードを設定する。

[適用モデル]  
NVR700W, NVR510

#### 50.3.4.3 アクセスポートの設定

[書式]

```
switch control function set vlan-access port vlan_register_num
no switch control function set vlan-access port
switch control function get vlan-access port [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *vlan\_register\_num*
  - [設定値]: VLAN 登録番号 (1 .. 256)
  - [初期値]: 1
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

[説明]

**vlan-port-mode** が access または hybrid であるポートについて、ポートの VLAN ID を設定する。VLAN ID は VLAN 登録番号を用いて指定する。

[ノート]

**vlan-port-mode** が trunk であるポートにおいて、本機能の設定を変更しても動作に影響はない。

[適用モデル]  
NVR700W, NVR510

#### 50.3.4.4 トランクポートの設定

[書式]

```
switch control function set vlan-trunk port vlan_register_num mode
no switch control function set vlan-trunk port vlan_register_num
switch control function get vlan-trunk port vlan_register_num [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *vlan\_register\_num*
  - [設定値]: VLAN 登録番号 (1 .. 256)
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値   | 説明    |
|-------|-------|
| join  | 参加する  |
| leave | 参加しない |

- [初期値]: leave
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路

- [初期値]:-

#### [説明]

**vlan-port-mode** が trunk もしくは hybrid であるポートにおいて、参加する VLAN ID を設定する。VLAN ID は VLAN 登録番号を用いて指定する。

#### [ノート]

**vlan-port-mode** が access であるポートにおいて、本機能の設定を変更しても動作に影響はない。

#### [適用モデル]

NVR700W, NVR510

### 50.3.4.5 マルチプル VLAN を使用するか否かの設定

#### [書式]

```
switch control function set vlan-multiple-use mode
no switch control function set vlan-multiple-use
switch control function get vlan-multiple-use [switch]
```

#### [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

#### [説明]

マルチプル VLAN を使用するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

### 50.3.4.6 マルチプル VLAN のグループ設定

#### [書式]

```
switch control function set vlan-multiple port group_num mode
no switch control function set vlan-multiple port group_num
switch control function get vlan-multiple port group_num [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *group\_num*: グループ番号
  - [設定値]:

| 機種                      | 範囲      |
|-------------------------|---------|
| SWX2200-24G             | 1 .. 24 |
| SWX2200-8G、SWX2200-8PoE | 1 .. 8  |

- [初期値]:-
- *mode*
  - [設定値]:

| 設定値   | 説明    |
|-------|-------|
| join  | 参加する  |
| leave | 参加しない |

- [初期値]: leave
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

#### [説明]

ポートが所属するマルチプル VLAN のグループ番号を設定する。

#### [ノート]

**vlan-multiple-use** が off の場合、本機能の設定を変更しても動作に影響はない。

#### [適用モデル]

NVR700W, NVR510

## 50.3.5 QoS

DSCP リマーキングは、IP ヘッダの DS フィールド中の 6 ビットの DSCP 値を書き換える機能です。書き換える値は、パケットを受信したポートのクラス (**qos-dscp-remark-class**) と送信するポートの書き換え方式 (**qos-dscp-remark-type**) により決定されます。具体的には以下ようになります。

| qos-dscp-remark-type | qos-dscp-remark-class | DSCP 値 | PHB            |
|----------------------|-----------------------|--------|----------------|
| af                   | class1                | 001100 | AF12           |
|                      | class2                | 010100 | AF22           |
|                      | class3                | 011100 | AF32           |
|                      | class4                | 100100 | AF42           |
| cs                   | class1                | 000000 | default        |
|                      | class2                | 001000 | Class Selector |
|                      | class3                | 010000 |                |
|                      | class4                | 011000 |                |

### 50.3.5.1 DSCP リマーキングの書き換え方式の設定

#### [書式]

```
switch control function set qos-dscp-remark-type port type
no switch control function set qos-dscp-remark-type port
switch control function get qos-dscp-remark-type port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *type*: 書き換え方式
  - [設定値]:

| 設定値 | 説明                               |
|-----|----------------------------------|
| off | 書き換えを行わない                        |
| af  | AF (Assured Forwarding) で書き換えを行う |
| cs  | CS (Class Selector) で書き換えを行う     |

- [初期値]: off

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

スイッチから送信する IP パケットの DSCP 値を書き換える際の方式を設定する。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.2 受信パケットのクラス分けの設定**

**[書式]**

```
switch control function set qos-dscp-remark-class port class
no switch control function set qos-dscp-remark-class port
switch control function get qos-dscp-remark-class port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *class*
  - [設定値]:

| 設定値    | 説明          |
|--------|-------------|
| off    | 分類しない       |
| class1 | クラス 1 に分類する |
| class2 | クラス 2 に分類する |
| class3 | クラス 3 に分類する |
| class4 | クラス 4 に分類する |

- [初期値]: off
- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

DSCP リマーキングにおいて、スイッチが受信したパケットのクラス分けを行う。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.3 帯域制限を行う際の速度単位の設定**

**[書式]**

```
switch control function set qos-speed-unit unit
no switch control function set qos-speed-unit
switch control function get qos-speed-unit [switch]
```

**[設定値及び初期値]**

- *unit* : 速度単位
  - [設定値]:
    - 128k
    - 1m
    - 10m

- 32m
- [初期値]: 32m
- *switch*: スイッチ
- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]: -

**[説明]**

受信トラフィックのポリシングおよび送信トラフィックのシェーピングを行う際の速度単位を設定する。

**[ノート]**

SWX2200-24G でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.4 受信トラフィックのポリシングを行うか否かの設定****[書式]**

```
switch control function set qos-policing-use port mode
no switch control function set qos-policing-use port
switch control function get qos-policing-use port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 行う   |
| off | 行わない |

- [初期値]: off
- *switch*: スイッチ
- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]: -

**[説明]**

受信トラフィックのポリシングを行うか否かを設定する。

**[ノート]**

SWX2200-24G でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.5 受信トラフィックの帯域幅の設定****[書式]**

```
switch control function set qos-policing-speed port level
no switch control function set qos-policing-speed port
switch control function get qos-policing-speed port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -



- *level*
  - [設定値]: 帯域幅 (1 .. 31)
  - [初期値]: 1
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

受信トラフィックのポリシングを行う際の帯域幅を設定する。**qos-speed-unit** の設定値に *level* を掛けた値が実際の帯域幅となる。

**[ノート]**

SWX2200-24G でのみ使用可能。

**qos-policing-use** が off の場合、本機能の設定を変更しても動作に影響はない。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.6 送信トラフィックのシェーピングを行うか否かの設定**

**[書式]**

```
switch control function set qos-shaping-use port mode
no switch control function set qos-shaping-use port
switch control function get qos-shaping-use port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *mode*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| on  | 行う   |
| off | 行わない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

送信トラフィックのシェーピングを行うか否かを設定する。

**[ノート]**

SWX2200-24G でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.5.7 送信トラフィックの帯域幅の設定**

**[書式]**

```
switch control function set qos-shaping-speed port level
no switch control function set qos-shaping-speed port
switch control function get qos-shaping-speed port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *level*
  - [設定値]: 帯域幅 (1 .. 31)
  - [初期値]: 1
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

送信トラフィックのシェーピングを行う際の帯域幅を設定する。**qos-speed-unit** の設定値に *level* を掛けた値が実際の帯域幅となる。

**[ノート]**

SWX2200-24G でのみ使用可能。

**qos-shaping-use** が off の場合、本機能の設定を変更しても動作に影響はない。

**[適用モデル]**

NVR700W, NVR510

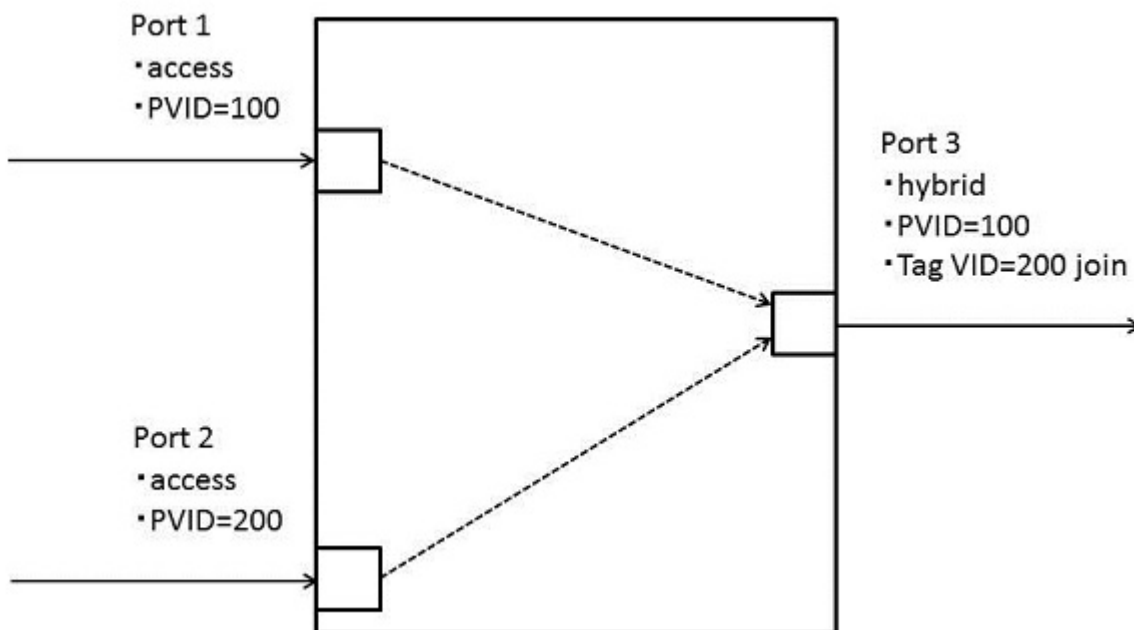
**50.3.6 ミラーリング**

ミラーリングは、特定ポートでの通信を他のポートで観測できる機能です。

ミラーリングとポートブロッキング機能(**port-blocking-control-packet** および **port-blocking-data-packet**)は併用できません。

ミラーリングとポート VLAN / タグ VLAN、マルチプル VLAN を併用する場合、ミラーリングを行うポート (**mirroring-src-rx** および **mirroring-src-tx**) とミラーリング packets を送出するポート (**mirroring-dest**) が同一の VLAN、グループ番号に所属するようにしてください。

ミラーリング packets と元の packets で VLAN タグの有無に違いが生じることがあります。ミラーリング packets に VLAN タグが付くか否かは、ミラーリング packets を送出するポートの VLAN 動作モードに依存します。例えば以下の設定があるとします。



- ポート 1 はアクセスポートで VLAN ID=100
- ポート 2 はアクセスポートで VLAN ID=200
- ポート 3 はハイブリッドポートで、アクセスポートの VLAN ID=100、タグ VLAN で VLAN ID=200 に参加。
- ポート 1 とポート 2 で受信した packets をポート 3 でミラーリングする。

```
switch control function set vlan-port-mode 3 hybrid
switch control function set vlan-access 1 100
switch control function set vlan-access 2 200
switch control function set vlan-access 3 100
switch control function set vlan-trunk 3 200 join
switch control function set mirroring-use on
switch control function set mirroring-dest 3
switch control function set mirroring-src-rx 1 on
switch control function set mirroring-src-rx 2 on
```

- ポート 1 で受信したパケットをポート 3 でミラーリングする場合、パケットに VLAN タグは付加されません。
- ポート 2 で受信したパケットをポート 3 でミラーリングする場合、パケットに VLAN ID=200 の VLAN タグが付加されます。

### 50.3.6.1 ミラーリング機能を使用するか否かの設定

#### [書式]

```
switch control function set mirroring-use mode
no switch control function set mirroring-use
switch control function get mirroring-use [switch]
```

#### [設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

#### [説明]

ミラーリング機能を使用するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

### 50.3.6.2 ミラーリングパケットを送出するポートの設定

#### [書式]

```
switch control function set mirroring-dest port
no switch control function set mirroring-dest
switch control function get mirroring-dest [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ミラーリングパケットを送出するポート番号
  - [初期値]:

| 機種                      | ポート番号 |
|-------------------------|-------|
| SWX2200-24G             | 24    |
| SWX2200-8G、SWX2200-8PoE | 8     |

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路

- [初期値]:-

#### [説明]

ミラーリングパケットを送出するポートを設定する。

#### [ノート]

**mirroring-use** が off の場合、本機能の設定を変更しても動作に影響はない。

#### [適用モデル]

NVR700W, NVR510

### 50.3.6.3 受信したパケットをミラーリングするか否かの設定

#### [書式]

```
switch control function set mirroring-src-rx port mode
no switch control function set mirroring-src-rx port
switch control function get mirroring-src-rx port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *mode*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | 受信したパケットをミラーリングする  |
| off | 受信したパケットをミラーリングしない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

#### [説明]

受信したパケットをミラーリングするか否かを設定する。

#### [ノート]

**mirroring-dest** に設定しているポートにおいて当機能を on にしても、ミラーリングは行われない。

**mirroring-use** が off の場合、本機能の設定を変更しても動作に影響はない。

#### [適用モデル]

NVR700W, NVR510

### 50.3.6.4 送信するパケットをミラーリングするか否かの設定

#### [書式]

```
switch control function set mirroring-src-tx port mode
no switch control function set mirroring-src-tx port
switch control function get mirroring-src-tx port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *mode*
  - [設定値]:

| 設定値 | 説明                 |
|-----|--------------------|
| on  | 送信するパケットをミラーリングする  |
| off | 送信するパケットをミラーリングしない |

- [初期値]: off
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

送信するパケットをミラーリングするか否かを設定する。

**[ノート]**

**mirroring-dest** に設定しているポートにおいて当機能を on にしても、ミラーリングは行われぬ。

**mirroring-use** が off の場合、本機能の設定を変更しても動作に影響はない。

**[適用モデル]**

NVR700W, NVR510

### 50.3.7 カウンタ

ポートごとにフレームカウンタとオクテットカウンタがあり、それぞれ受信と送信で個別にカウントすることができます。フレームカウンタでは同時に複数の種類のパケットをカウントすることができます。

フレームカウンタを使用する場合、事前に **counter-frame-rx-type** または **counter-frame-tx-type** でカウントするパケットの種類を設定します。カウンタの値は **status-counter-frame-rx** または **status-counter-frame-tx** で取得します。

オクテットカウンタの値は **status-counter-octet-rx** または **status-counter-octet-tx** で取得します。

フレームカウンタでカウントするパケットの種類のうち class-0~class-3 は DSCP リマーカーキングによるクラス分け (**qos-dscp-remark-class**) に対応しています。対応関係は以下の通りです。

| DSCP によるクラス分け | 送信キューまたは受信キューのクラス |
|---------------|-------------------|
| class1        | class-0           |
| class2        | class-1           |
| class3        | class-2           |
| class4        | class-3           |
| クラス分け無し (off) |                   |

スイッチで受信したパケットを送信するとき、受信キューと送信キューのクラスは常に同一となります。

#### 50.3.7.1 受信フレームカウンタでカウントするフレームの種類の設定

**[書式]**

```
switch control function set counter-frame-rx-type port counter type
no switch control function set counter-frame-rx-type port counter
switch control function get counter-frame-rx-type port counter [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *counter*: カウンタ番号
  - [設定値]:

| 機種                      | 範囲     |
|-------------------------|--------|
| SWX2200-24G             | 1 .. 5 |
| SWX2200-8G、SWX2200-8PoE | 1 .. 3 |

- [初期値]:-
- *type*: カウントするパケットの種類
- [設定値]:

| 設定値                             | 説明                                                                                                 |
|---------------------------------|----------------------------------------------------------------------------------------------------|
| packets                         | 全てのパケット                                                                                            |
| broadcast-and-multicast-packets | ブロードキャストパケットとマルチキャストパケット                                                                           |
| total-error-packets             | CRC エラー、アライメントエラー、フレームサイズエラーを含むパケット                                                                |
| broadcast-packets               | ブロードキャストパケット                                                                                       |
| multicast-packets               | マルチキャストパケット                                                                                        |
| packets-64-octets               | 64 オクテットのパケット                                                                                      |
| packets-65-to-127-octets        | 65～127 オクテットのパケット                                                                                  |
| packets-128-to-255-octets       | 128～255 オクテットのパケット                                                                                 |
| packets-256-to-511-octets       | 256～511 オクテットのパケット                                                                                 |
| packets-512-to-1023-octets      | 512～1023 オクテットのパケット                                                                                |
| packets-1024-to-1526-octets     | 1024～1526 オクテットのパケット                                                                               |
| pause                           | PAUSE パケット                                                                                         |
| fifo-drops                      | 受信バッファのオーバーフローで破棄されたパケット                                                                           |
| total-good-packets              | 正常に受信したパケット                                                                                        |
| class-0                         | 受信キュー class-0 に振り分けられたパケット                                                                         |
| class-1                         | 受信キュー class-1 に振り分けられたパケット                                                                         |
| class-2                         | 受信キュー class-2 に振り分けられたパケット                                                                         |
| class-3                         | 受信キュー class-3 に振り分けられたパケット                                                                         |
| backward-drops                  | バッファが輻輳しているために破棄されたパケット                                                                            |
| classifier-drops                | 送信元もしくは送信先 MAC アドレスが 00:00:00:00:00:00 のパケット、アクセスポートで受信した VLAN タグ付きパケット、トランクポートで受信した VLAN タグ無しパケット |
| crc-align-errors                | CRC エラー、アライメントエラー、物理層でのエラーを検出したパケット                                                                |
| under-size-packets              | 64 バイト未満で CRC は正常であるパケット                                                                           |
| over-size-packets               | 1519 バイト以上 (VLAN タグ無し) もしくは 1523 バイト以上 (VLAN タグ付き) で CRC は正常であるパケット                                |
| fragments                       | 64 バイト未満で CRC が異常であるパケット                                                                           |
| jabbers                         | 1519 バイト以上 (VLAN タグ無し) もしくは 1523 バイト以上 (VLAN タグ付き) で CRC が異常であるパケット                                |
| control-packets                 | イーサネットタイプが 0x8808 であるパケット                                                                          |

- [初期値]:

| 機種                      | カウンタ番号 | 種類                  |
|-------------------------|--------|---------------------|
| SWX2200-24G             | 1      | packets             |
|                         | 2      | total-good-packets  |
|                         | 3      | total-error-packets |
|                         | 4      | fifo-drops          |
|                         | 5      | crc-align-errors    |
| SWX2200-8G、SWX2200-8PoE | 1      | packets             |
|                         | 2      | total-good-packets  |
|                         | 3      | total-error-packets |

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

受信フレームカウンタでカウントするフレームの種類を設定する。カウンタの値は **status-counter-frame-rx** で取得する。

**[ノート]**

本機能の設定を変更すると、当該ポートにおけるすべてのカウンタ (送信、受信、フレーム、オクテット) がリセットされる。

**[適用モデル]**

NVR700W, NVR510

**50.3.7.2 送信フレームカウンタでカウントするフレームの種類の設定**

**[書式]**

```
switch control function set counter-frame-tx-type port counter type
no switch control function set counter-frame-tx-type port counter
switch control function get counter-frame-tx-type port counter [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *counter* : カウンタ番号
  - [設定値]:

| 機種                      | 範囲     |
|-------------------------|--------|
| SWX2200-24G             | 1 .. 5 |
| SWX2200-8G、SWX2200-8PoE | 1 .. 3 |

- [初期値]: -
- *type* : カウントするパケットの種類
  - [設定値]:

| 設定値                             | 説明                         |
|---------------------------------|----------------------------|
| packets                         | 全てのパケット                    |
| broadcast-and-multicast-packets | ブロードキャストパケットとマルチキャストパケット   |
| total-error-packets             | パケットの送信時にエラーが発生して送信を中断した回数 |

| 設定値                         | 説明                                                                              |
|-----------------------------|---------------------------------------------------------------------------------|
| broadcast-packets           | ブロードキャストパケット                                                                    |
| multicast-packets           | マルチキャストパケット                                                                     |
| packets-64-octets           | 64 オクテットのパケット                                                                   |
| packets-65-to-127-octets    | 65～127 オクテットのパケット                                                               |
| packets-128-to-255-octets   | 128～255 オクテットのパケット                                                              |
| packets-256-to-511-octets   | 256～511 オクテットのパケット                                                              |
| packets-512-to-1023-octets  | 512～1023 オクテットのパケット                                                             |
| packets-1024-to-1526-octets | 1024～1526 オクテットのパケット                                                            |
| pause                       | PAUSE パケット                                                                      |
| fifo-drops                  | 送信バッファのオーバーフローで破棄されたパケット                                                        |
| total-good-packets          | 正常に送信されたパケット                                                                    |
| class-0                     | 送信キュー class-0 から送信されたパケット                                                       |
| class-1                     | 送信キュー class-1 から送信されたパケット                                                       |
| class-2                     | 送信キュー class-2 から送信されたパケット                                                       |
| class-3                     | 送信キュー class-3 から送信されたパケット                                                       |
| drops                       | コリジョンの多発、レイトコリジョン、送信バッファへの長時間滞留のいずれかの理由により破棄されたパケット                             |
| collisions                  | コリジョンが発生した回数                                                                    |
| cfi-drop                    | CFI ビットが 1 であるために破棄したパケット (CFI ビットが 1 であるパケットを受信し、当該パケットをタグ無しで送信しようとした場合は破棄される) |

- [初期値]:

| 機種                      | カウンタ番号 | 種類                  |
|-------------------------|--------|---------------------|
| SWX2200-24G             | 1      | packets             |
|                         | 2      | total-good-packets  |
|                         | 3      | total-error-packets |
|                         | 4      | fifo-drops          |
|                         | 5      | collisions          |
| SWX2200-8G、SWX2200-8PoE | 1      | packets             |
|                         | 2      | total-good-packets  |
|                         | 3      | total-error-packets |

- *switch*: スイッチ

- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]: -

#### [説明]

送信フレームカウンタでカウントするフレームの種類を設定する。カウンタの値は **status-counter-frame-tx** で取得する。



## [ノート]

本機能の設定を変更すると、当該ポートにおけるすべてのカウンタ (送信、受信、フレーム、オクテット) がリセットされる。

## [適用モデル]

NVR700W, NVR510

## 50.3.7.3 受信フレームカウンタの値の取得

## [書式]

```
switch control function get status-counter-frame-rx port counter [switch]
```

## [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *counter*: カウンタ番号
  - [設定値]:

| 機種                      | 範囲     |
|-------------------------|--------|
| SWX2200-24G             | 1 .. 5 |
| SWX2200-8G、SWX2200-8PoE | 1 .. 3 |

- [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

## [説明]

受信フレームカウンタの値を取得する。

## [適用モデル]

NVR700W, NVR510

## 50.3.7.4 送信フレームカウンタの値の取得

## [書式]

```
switch control function get status-counter-frame-tx port counter [switch]
```

## [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *counter*: カウンタ番号
  - [設定値]:

| 機種                      | 範囲     |
|-------------------------|--------|
| SWX2200-24G             | 1 .. 5 |
| SWX2200-8G、SWX2200-8PoE | 1 .. 3 |

- [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

## [説明]

送信フレームカウンタの値を取得する。

**[適用モデル]**

NVR700W, NVR510

**50.3.7.5 受信オクテットカウンタの値の取得****[書式]****switch control function get status-counter-octet-rx port [switch]****[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

受信オクテットカウンタの値を取得する。当カウンタは **counter-frame-rx-type** の設定によらず、受信したすべてのパケットについてオクテット数をカウントする。

**[適用モデル]**

NVR700W, NVR510

**50.3.7.6 送信オクテットカウンタの値の取得****[書式]****switch control function get status-counter-octet-tx port [switch]****[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

送信オクテットカウンタの値を取得する。当カウンタは **counter-frame-tx-type** の設定によらず、送信したすべてのパケットについてオクテット数をカウントする。

**[適用モデル]**

NVR700W, NVR510

**50.3.7.7 カウンタのクリア****[書式]****switch control function execute clear-counter [switch]****[設定値及び初期値]**

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

全てのカウンタ (全ポート、送信、受信、フレーム、オクテット) をクリアする。

[適用モデル]  
NVR700W, NVR510

### 50.3.8 ループ検出

ヤマハスイッチは、MAC アドレスの移動を監視する方法と L2MS パケットを監視する方法の 2 種類の方法でネットワークのループを検出します。

MAC アドレスの移動とは、同一の MAC アドレスが異なるポートにおいて学習されることです。スイッチは、1 秒あたりの MAC アドレス移動回数を監視しています。移動回数が **loopdetect-count** で指定した閾値を超えている状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断します。

L2MS パケットを監視する方法では、スイッチ自身が送信した制御パケットを受信した回数を監視しています。自身が送信した制御パケットを受信した回数が **loopdetect-count** で指定した閾値を越えている状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断します。

どちらの方法で検出した場合でも、ループが発生したポートでは LED が橙色で点灯します。

ループ検出機能を使用するポートでは、**loopdetect-port-use** を on に設定します。

ループ発生後の動作は **loopdetect-linkdown** で設定します。**loopdetect-linkdown** が linkdown または linkdown-recovery の場合、ループが発生しているポートのうち番号の大きいものから順に、ループが停止するまでリンクダウンしていきます。ループ発生時にもルーターと通信できるようにしておくため、アップリンクポートはポート 1 を使用することが推奨されます。

なお、ループの発生によってリンクダウンしたポートの LED は橙色で点滅します。

#### 50.3.8.1 1 秒あたりのループが発生したと判断する閾値の設定

[書式]

```
switch control function set loopdetect-count count
no switch control function set loopdetect-count count
switch control function get loopdetect-count [switch]
```

[設定値及び初期値]

- *count*
  - [設定値]: 1 秒あたりのループが発生したと判断する閾値 (3 .. 65535)
  - [初期値]: 3
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

[説明]

1 秒あたりのループが発生したと判断する閾値を設定する。MAC アドレス移動回数またはスイッチ自身が送信した制御パケットを受信した回数が本機能で設定した閾値を越えた状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断する。

[適用モデル]  
NVR700W, NVR510

#### 50.3.8.2 ループが発生したと判断するまでの時間の設定

[書式]

```
switch control function set loopdetect-time time
no switch control function set loopdetect-time
switch control function get loopdetect-time [switch]
```

[設定値及び初期値]

- *time*
  - [設定値]: 秒数 (2 .. 60)
  - [初期値]: 3
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス

- 経路
- [初期値]:-

**[説明]**

1 秒あたりの MAC アドレス移動回数またはスイッチ自身が送信した制御パケットを受信した回数が **loopdetect-count** で設定した閾値以上である状態が継続し、ループが発生したと判断するまでの時間を設定する。

**[適用モデル]**

NVR700W, NVR510

**50.3.8.3 ループ発生時の動作の設定****[書式]**

```
switch control function set loopdetect-linkdown action
no switch control function set loopdetect-linkdown
switch control function get loopdetect-linkdown [switch]
```

**[設定値及び初期値]**

- *action*
- [設定値]:

| 設定値               | 説明                                  |
|-------------------|-------------------------------------|
| none              | 何も行わない                              |
| linkdown          | ループが発生したポートをリンクダウンする                |
| linkdown-recovery | ループが発生したポートをリンクダウンした後、一定時間経過後に復帰させる |

- [初期値]: none
- *switch*: スイッチ
- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]:-

**[説明]**

ループ発生時の動作を設定する。

*action* が linkdown または linkdown-recovery の場合、ループが発生しているポートのうち番号の大きいものから順に、ループが停止するまでリンクダウンしていく。リンクダウンしたポートを復帰させるには **reset-loopdetect** を実行するか、MODE ボタンを押下する。

*action* が linkdown-recovery の場合、ポートをリンクダウンしてから **loopdetect-recovery-timer** で設定した時間経過後に自動的に復帰させる。

**[ノート]**

**loopdetect-port-use** が off に設定されているポートでは、実際にループが発生してもそのことを検出しないため、当機能で設定された動作は行わない。

**[適用モデル]**

NVR700W, NVR510

**50.3.8.4 ポートをリンクダウンしてから復帰させるまでの時間の設定****[書式]**

```
switch control function set loopdetect-recovery-timer time
no switch control function set loopdetect-recovery-timer
switch control function get loopdetect-recovery-timer [switch]
```

**[設定値及び初期値]**

- *time*
- [設定値]: 秒数 (1 .. 86400)
- [初期値]: 300
- *switch*: スイッチ

- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]:-

[説明]

**loopdetect-linkdown** の設定が linkdown-recovery の場合に、リンクダウンしてから復帰させるまでの時間を設定する。

[適用モデル]

NVR700W, NVR510

50.3.8.5 ループ検出機能を使用するか否かの設定

[書式]

```
switch control function set loopdetect-port-use port mode
no switch control function set loopdetect-port-use port
switch control function get loopdetect-port-use port [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *mode*
  - [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

[説明]

ループ検出機能を使用するか否かを設定する。当機能が on に設定されているポートと off に設定されているポートでループが発生した場合は、on に設定されているポートでループを検出する。off に設定されているポートのみでループが発生した場合は、検出しない。

[適用モデル]

NVR700W, NVR510

50.3.8.6 L2MS パケットを用いたループ検出を行うか否かの設定

[書式]

```
switch control function set loopdetect-use-control-packet mode
no switch control function set loopdetect-use-control-packet
switch control function get loopdetect-use-control-packet [switch]
```

[設定値及び初期値]

- *mode*
  - [設定値]:

| 設定値 | 説明                  |
|-----|---------------------|
| on  | 制御パケットによるループ検出を行う   |
| off | 制御パケットによるループ検出を行わない |

- [初期値]: on
- *switch*: スイッチ

- [設定値]:
  - MAC アドレス
  - 経路
- [初期値]:-

**[説明]**

L2MS パケットを用いたループ検出を行うか否かを設定する。本機能を on に設定すると、スイッチ自身が送信した制御パケットを受信した場合にループが発生したと判断する。

**[ノート]**

スイッチ配下のハブやスイッチにて輻輳等が発生し、制御パケットが転送されない場合は、ループを検出できないことがある

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

**[適用モデル]**

NVR700W, NVR510

**50.3.8.7 ループ検出機能に関するポートの状態の取得****[書式]**

```
switch control function get status-loopdetect-port port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

ループ検出機能に関するポートの状態を取得する。

| 状態         | 説明                  |
|------------|---------------------|
| normal     | 正常                  |
| loopdetect | ループが発生している          |
| linkdown   | ループが発生したため、リンクダウンした |

**[適用モデル]**

NVR700W, NVR510

**50.3.8.8 リンクダウンしている状態から復帰するまでの残り時間の取得****[書式]**

```
switch control function get status-loopdetect-recovery-timer port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

ループ発生によってリンクダウンしている状態から復帰するまでの残り時間を取得する。

[適用モデル]  
NVR700W, NVR510

### 50.3.8.9 ループ発生によってリンクダウンしているポートの復帰

[書式]

```
switch control function execute reset-loopdetect [switch]
```

[設定値及び初期値]

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

[説明]

ループ発生によってリンクダウンしている全てのポートを復帰させる。

[適用モデル]  
NVR700W, NVR510

## 50.3.9 PoE 給電

### 50.3.9.1 各ポートで給電可能なクラスの上限の設定

[書式]

```
switch control function set poe-class port class
no switch control function set poe-class port class
switch control function get poe-class port [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *class*
  - [設定値]:

| 設定値    | 説明                |
|--------|-------------------|
| none   | 給電しない             |
| class3 | 15.4W までの機器まで給電する |
| class4 | 30W までの機器まで給電する   |

- [初期値]:
  - class4(1、3、5、7ポート)
  - class3(2、4、6、8ポート)
- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

[説明]

各ポート毎に給電する上限を設定する。スイッチの上段ポート(1、3、5、7ポート)は、クラス 4(30W)を上限に設定できる。下段ポート(2、4、6、8ポート)はクラス 3(15.4W)が上限となる。給電は上下のポートを対として、上段のポートにクラス 4(30W)の機器を接続すると、その直下に位置するポートへの給電を停止する。

[ノート]

SWX2200-8PoE でのみ使用可能。

設定したクラス以上の機器を接続した場合、実際に使用する電力が設定したクラス以下であっても給電は行われな

[適用モデル]  
NVR700W, NVR510

### 50.3.9.2 各ポートの給電状態の取得

[書式]

```
switch control function get status-poe-state port [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

[説明]

| 状態                                                                        | 説明                                                    | 備考                 |
|---------------------------------------------------------------------------|-------------------------------------------------------|--------------------|
| none                                                                      | 給電していない                                               | -                  |
| terminate                                                                 | 給電停止                                                  | -                  |
| supply-class0, supply-class1, supply-class2, supply-class3, supply-class4 | 給電中(給電中のクラス)                                          | -                  |
| overcurrent                                                               | 過電流による給電停止                                            | -                  |
| class-failure                                                             | 電力クラス設定より大きなクラスを認識したことによる給電停止                         | SWX2200-8PoE でのみ発生 |
| over-supply                                                               | 供給電力が最大給電能力を超えたことによる給電停止                              | -                  |
| over-temperature                                                          | 内部温度が 60°C を超えたことによる給電停止                              | SWX2200-8PoE でのみ発生 |
| fan-lock                                                                  | ファン停止による給電停止                                          | SWX2200-8PoE でのみ発生 |
| forced-terminate                                                          | Class3(15.4W)を給電していたポートに Class4(30W)給電が給電されたことによる給電停止 | SWX2200-8PoE でのみ発生 |
| power-failure                                                             | 電源故障による給電停止                                           | -                  |

[ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE でのみ使用可能。

[適用モデル]  
NVR700W, NVR510

### 50.3.9.3 各ポートに接続された機器のクラスの取得

[書式]

```
switch control function get status-poe-detect-class port [switch]
```

[設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路



- [初期値]:-

#### [説明]

ポートに接続された機器のクラスを取得する。

#### [ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE でのみ使用可能。

#### [適用モデル]

NVR700W, NVR510

### 50.3.9.4 スイッチの内部温度の取得

#### [書式]

```
switch control function get status-poe-temperature [switch]
```

#### [設定値及び初期値]

- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

#### [説明]

スイッチの内部温度を取得する。

#### [ノート]

SWX2200-8PoE でのみ使用可能。

#### [適用モデル]

NVR700W, NVR510

### 50.3.9.5 各ポートの消費電力の取得

#### [書式]

```
switch control function get status-poe-supply port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

#### [説明]

各ポートの現在の消費電力を取得する。

#### [ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE でのみ使用可能。

#### [適用モデル]

NVR700W, NVR510

### 50.3.9.6 各ポートの詳細な供給電力の取得

#### [書式]

```
switch control function get status-poe-supply-detail port [switch]
```

#### [設定値及び初期値]

- *port*
  - [設定値]: ポート番号
  - [初期値]:-

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

各ポートの詳細な現在の供給電力を取得する。

**[ノート]**

SWX2100-10PoE、SWX2100-5PoE で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.9.7 スイッチの総供給電力の取得****[書式]**

```
switch control function get status-poe-supply-total [switch]
```

**[設定値及び初期値]**

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

スイッチの総供給電力を取得する。単位は W (ワット)。

**[ノート]**

SWX2100-10PoE、SWX2100-5PoE で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.9.8 給電復帰****[書式]**

```
switch control function execute restart-poe-supply [switch]
```

**[設定値及び初期値]**

- *switch* : スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]:-

**[説明]**

給電を復帰させる。なお、何らかの異常により給電を停止している場合には、電源異常による給電停止の場合は、本コマンドでの給電復帰はできない。

**[ノート]**

SWX2200-8PoE でのみ使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.9.9 各ポートへの給電を開始****[書式]**

```
switch control function execute start-poe-supply port [switch]
```

**[設定値及び初期値]**

- *port*

- [設定値]: ポート番号
- [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

各ポートへの給電を開始する。

**[ノート]**

SWX2100-10PoE、SWX2100-5PoE で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.3.9.10 各ポートへの給電を停止****[書式]**

```
switch control function execute stop-poe-supply port [switch]
```

**[設定値及び初期値]**

- *port*
  - [設定値]: ポート番号
  - [初期値]: -
- *switch*: スイッチ
  - [設定値]:
    - MAC アドレス
    - 経路
  - [初期値]: -

**[説明]**

各ポートへの給電を停止する。

**[ノート]**

SWX2100-10PoE、SWX2100-5PoE で使用可能。

**[適用モデル]**

NVR700W, NVR510

**50.4 アクセスポイントの制御****50.4.1 アクセスポイントの選択****[書式]**

```
ap select ap
no ap select
```

**[設定値及び初期値]**

- *ap*
  - [設定値]:
 

| 設定値            | 説明             |
|----------------|----------------|
| MAC アドレスもしくは経路 | アクセスポイントを選択する  |
| none           | アクセスポイントを選択しない |
  - [初期値]: -

**[説明]**

対象とするアクセスポイントを選択する。以降プロンプトには **console prompt** で設定した文字列と *ap* パラメータにより選択したアクセスポイントが続けて表示される。

**ap select none** または **no ap select** を実行すると、プロンプトにアクセスポイントが表示されなくなる。

[適用モデル]

NVR700W, NVR510

#### 50.4.2 アクセスポイントの設定ファイルを格納するディレクトリの指定

---

[書式]

**ap config directory** *path*

**no ap config directory** [*path*]

[設定値及び初期値]

- *path*

- [設定値]: 相対パスまたは絶対パス (半角 256 文字以下、全角 128 文字以下 (NVR700W Rev.15.00.14 以降、および、NVR510 Rev.15.01.13 以降))
- [初期値]: /ap\_config

[説明]

アクセスポイントの設定ファイル(config)を格納するディレクトリを指定する。

相対パスを指定した場合、環境変数 PWD を起点としたパスと解釈される。

PWD は **set** コマンドで変更可能であり、初期値は "/" である。

NVR700W Rev.15.00.14 以降、および、NVR510 Rev.15.01.13 以降では、*path* が RTFS 領域となる場合には、*path* にマルチバイト文字を使用することはできない。

[適用モデル]

NVR700W, NVR510

#### 50.4.3 アクセスポイントの設定を保存するファイル名の指定

---

[書式]

**ap config filename** *name*

**no ap config filename** [*name*]

[設定値及び初期値]

- *name*

- [設定値]: config ファイル名 (半角 99 文字以下、全角 49 文字以下 (NVR700W Rev.15.00.14 以降、および、NVR510 Rev.15.01.13 以降))
- [初期値]: -

[説明]

アクセスポイントの設定を保存するファイル名を指定する。

このコマンドが省略された場合は、**ap select** で指定された文字列に .conf を付けたものをファイル名とする。

ただし:(コロン)は\_(アンダースコア)に置き換えられる。

複数の **ap select** コマンドで同じファイル名を指定することができる。

NVR700W Rev.15.00.14 以降、および、NVR510 Rev.15.01.13 以降では、**ap config directory** コマンドで指定したディレクトリが RTFS 領域である場合は、ファイル名にマルチバイト文字を使用することはできない。

本コマンドを実行する前に **ap select** コマンドでスイッチを指定しておく必要がある。

[適用モデル]

NVR700W, NVR510

#### 50.4.4 アクセスポイントの設定のバックアップ実行

---

[書式]

**ap control config get** [*ap*]

**ap control config get** [[*interface*] all]

[設定値及び初期値]

- *ap*

- [設定値]:

| 設定値            | 説明             |
|----------------|----------------|
| MAC アドレスもしくは経路 | 選択したアクセスポイントのみ |
| all            | 全てのアクセスポイント    |

- [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -

#### [説明]

アクセスポイントの設定のバックアップ動作を実行する。

*ap* パラメーターを使用した場合は、対象となるアクセスポイントのみバックアップを行う。  
*all* を指定すると、ヤマハルーターが認識している全てのアクセスポイントのコンフィグを保存する。  
 LAN インターフェースを指定すると、LAN インターフェースにつながっているアクセスポイントだけを対象とする。  
 パラメーターを省略した場合は、*all* を指定した時と同様になる。

#### [ノート]

**schedule at** コマンドで指定することができる。

#### [適用モデル]

NVR700W, NVR510

### 50.4.5 アクセスポイントの設定の復元実行

#### [書式]

```
ap control config set [ap]  
ap control config set [[interface] all]
```

#### [設定値及び初期値]

- *ap*
  - [設定値]:

| 設定値            | 説明             |
|----------------|----------------|
| MAC アドレスもしくは経路 | 選択したアクセスポイントのみ |
| all            | 全てのアクセスポイント    |

- [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -

#### [説明]

アクセスポイントの設定の復元動作を実行する。

*ap* パラメーターを使用した場合は、対象となるアクセスポイントのみ復元を行う。  
*all* を指定すると、ヤマハルーターが認識している全てのアクセスポイントのコンフィグを復元する。  
 LAN インターフェースを指定すると、LAN インターフェースにつながっているアクセスポイントだけを対象とする。  
 パラメーターを省略した場合は、*all* を指定した時と同様になる。

#### [ノート]

**schedule at** コマンドで指定することができる。

#### [適用モデル]

NVR700W, NVR510

### 50.4.6 アクセスポイントの設定の削除

#### [書式]

**ap control config delete** [*ap*]

#### [設定値及び初期値]

- *ap*
- [設定値]:

| 設定値            | 説明             |
|----------------|----------------|
| MAC アドレスもしくは経路 | 選択したアクセスポイントのみ |
| all            | 全てのアクセスポイント    |

- [初期値]:-

#### [説明]

アクセスポイントの設定の削除を実行する。

*ap* パラメーターを使用した場合は、対象となるアクセスポイントのみ削除を行う。

*ap* パラメーターを省略した場合は、全てのアクセスポイントの削除を行う。

#### [ノート]

**schedule at** コマンドで指定することができる。

#### [適用モデル]

NVR700W, NVR510

### 50.4.7 アクセスポイント設定のゼロコンフィグ機能を使用するか否かの設定

#### [書式]

**ap control config-auto-set use** *use*

**no ap control config-auto-set use** [*use*]

#### [設定値及び初期値]

- *use*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on

#### [説明]

アクセスポイント設定のゼロコンフィグ機能を使用するか否かを設定する。

#### [適用モデル]

NVR700W, NVR510

### 50.4.8 アクセスポイントの HTTP リビジョンアップ機能の実行

#### [書式]

**ap control firmware update go** [*ap*]

#### [設定値及び初期値]

- *ap*
- [設定値]:

| 設定値            | 説明             |
|----------------|----------------|
| MAC アドレスもしくは経路 | 選択したアクセスポイントのみ |
| all            | 全てのアクセスポイント    |

- [初期値]:-

**[説明]**

アクセスポイントに対してファームウェアの更新を要求する。

ap パラメーターを省略した場合は、全てのアクセスポイントに対して本コマンドを実行する。

**[ノート]**

**schedule at** コマンドで指定することができる。

**[適用モデル]**

NVR700W, NVR510

## 50.4.9 アクセスポイント制御用の HTTP プロキシの使用

---

**[書式]**

```
ap control http proxy use use
```

```
no ap control http proxy use [use]
```

**[設定値及び初期値]**

- *use*

- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: on

**[説明]**

アクセスポイント制御用の HTTP プロキシ機能を使用するか否かを設定する。

use を on に設定した場合、ルーター経由でアクセスポイントの GUI にアクセスすることができる。

**[ノート]**

L2MS においてルーターの管理下におかれているアクセスポイントに対してのみ、HTTP プロキシ機能を利用することができる。

また、アクセスポイントに IP アドレスが割り当てられている必要がある。

アクセスポイント毎に認証情報を入力する必要がなく、ルーターを経由することで、遠隔拠点から VPN や静的 IP マスカレードなどを使わずともアクセスポイントの設定ができる。

**[適用モデル]**

NVR700W, NVR510

## 50.4.10 アクセスポイント制御用の HTTP プロキシのタイムアウト時間の設定

---

**[書式]**

```
ap control http proxy timeout time
```

```
no ap control http proxy timeout [time]
```

**[設定値及び初期値]**

- *time*

- [設定値]: タイムアウトの秒数
- [初期値]: 60

**[説明]**

アクセスポイント制御用の HTTP プロキシ機能のタイムアウト時間を設定する。

プロキシ経由でアクセスポイントの GUI にアクセスする際、アクセスポイントから指定時間以内に応答がなければタイムアウトになる。

**[適用モデル]**

NVR700W, NVR510

## 50.5 ルーターの制御

---

## 50.5.1 HTTP プロキシ経由での Web GUI へのアクセスを許可するか否かの設定

### [書式]

```
httpd proxy-access l2ms permit permit
no httpd proxy-access l2ms permit [permit]
```

### [設定値及び初期値]

- *permit*
- [設定値]:

| 設定値 | 説明                                 |
|-----|------------------------------------|
| on  | HTTP プロキシ経由での Web GUI へのアクセスを許可する  |
| off | HTTP プロキシ経由での Web GUI へのアクセスを許可しない |

- [初期値]: off

### [説明]

HTTP プロキシ経由での Web GUI へのアクセスを許可するか否かを設定する。*permit* が on である場合は、マネージャーの Web GUI から本機の Web GUI を表示するときに HTTP プロキシ経由でアクセスする。

### [ノート]

**switch control mode** コマンドで *mode* に *agent* が設定されていない場合、本コマンドの設定は反映されない。

本コマンドを設定できるのは、NVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.09 以降のファームウェアである。

### [適用モデル]

NVR700W, NVR510



## 第 51 章

### YNO エージェント

YNO エージェントは、ヤマハネットワーク機器を「Yamaha Network Organizer (YNO)」で遠隔管理するための機能です。YNO エージェント機能を有効にしたヤマハネットワーク機器はインターネット経由で YNO マネージャーへ接続し、必要に応じて以下の処理を実施します。

- ヤマハネットワーク機器動作状態の YNO マネージャーへの通知
- CONFIG の送信・適用・保存
- ファームウェアの更新
- コマンドの実行
- GUI Forwarder によるヤマハネットワーク機器 GUI の表示
- ゼロコンフィグによる CONFIG の自動適用

本機能に関する技術情報は以下に示す URL で公開されています。  
<http://www.rtpo.yamaha.co.jp/RT/docs/yno/agent/>

#### 51.1 YNO エージェント機能を使用するか否かの設定

##### [書式]

```
yno use sw
no yno use sw
```

##### [設定値及び初期値]

- *sw*
- [設定値]:

| 設定値 | 説明    |
|-----|-------|
| on  | 使用する  |
| off | 使用しない |

- [初期値]: off

##### [説明]

YNO エージェント機能を使用するか否かを設定する。

##### [ノート]

NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降で使用可能。

##### [適用モデル]

NVR700W, NVR510

#### 51.2 YNO マネージャー接続用のアクセスコードの設定

##### [書式]

```
yno access code operator_id access_code
no yno access code [operator_id [access_code]]
```

##### [設定値及び初期値]

- *operator\_id*
  - [設定値]: オペレーター ID (半角 4 文字以上 かつ 半角 64 文字以内)
  - [初期値]: -
- *access\_code*
  - [設定値]: アクセスコード (半角 8 文字以上 かつ 半角 64 文字以内)
  - [初期値]: -

**[説明]**

YNO エージェント機能が YNO マネージャーへ接続する際に使用するアクセスコードを設定する。

ヤマハネットワーク機器は `operator_id` で指定したオペレーターの管理対象となる。同一オペレーターが管理するすべてのヤマハネットワーク機器には、同一のオペレーター ID およびアクセスコードを設定する必要がある。

`yno zero-config id` コマンドが設定されているときは、本コマンドは設定できない。

**[ノート]**

YNO マネージャーでアクセスコードを変更すると、管理対象のヤマハネットワーク機器で新しいアクセスコードを含んだ本コマンドが自動で実行・保存される。

NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 51.3 YNO エージェント機能に関する追加の SYSLOG を出力するか否かの設定

**[書式]**

`yno log type [type...]`

`no yno log [type...]`

**[設定値及び初期値]**

- `type`
- [設定値]:

| 設定値         | 説明                                              |
|-------------|-------------------------------------------------|
| action-read | ヤマハネットワーク機器の動作状態や CONFIG の読み出しに関する SYSLOG を出力する |
| inform      | YNO マネージャーとの定期通信に関する SYSLOG を出力する               |

- [初期値]: -

**[説明]**

YNO エージェント機能に関する追加の SYSLOG を出力するか否かを設定する。

**[ノート]**

NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 51.4 YNO マネージャーに表示される自身の機器説明の設定

**[書式]**

`description yno description`

`no description yno [description]`

**[設定値及び初期値]**

- `description`
- [設定値]: 説明の文字列 (最大 32 文字/半角、16 文字/全角)
- [初期値]: 空文字列

**[説明]**

YNO マネージャーに表示されるヤマハネットワーク機器の説明を設定する。

**[ノート]**

NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 51.5 YNO で使用する HTTPS プロキシサーバーの設定

---

### [書式]

```
yno https-proxy proxy_server port
no yno https-proxy [proxy_server [port]]
```

### [設定値及び初期値]

- *proxy\_server*
  - [設定値]: HTTPS プロキシサーバーのホスト名、もしくは IP アドレス
  - [初期値]: -
- *port*
  - [設定値]: HTTPS プロキシサーバーのポート番号 (1..65535)
  - [初期値]: -

### [説明]

YNO で使用する HTTPS プロキシサーバーを設定する。

*proxy\_server* には、HTTPS プロキシサーバーの FQDN 形式のホスト名、または IP アドレスを 255 文字以内の半角英数字および半角記号で指定する。

*port* には、HTTPS プロキシサーバーのポート番号を指定する。

### [ノート]

ユーザー認証が必要な HTTPS プロキシサーバーを使用することはできない。

NVR700W は Rev.15.00.14 以降、NVR510 は Rev.15.01.13 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 51.6 GUI Forwarder 接続のタイムアウト時間の設定

---

### [書式]

```
yno gui-forwarder timeout time
no yno gui-forwarder timeout [time]
```

### [設定値及び初期値]

- *time*
  - [設定値]: 秒数 (3..60)
  - [初期値]:
    - 30 (NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降)
    - 5 (上記以外)

### [説明]

GUI Forwarder 接続のタイムアウト時間を設定する。

本コマンドで設定した時間以内に GUI Forwarder サーバーからの応答がなかった場合、GUI Forwarder セッションを切断する。

### [ノート]

NVR700W は Rev.15.00.14 以降、NVR510 は Rev.15.01.13 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

## 51.7 YNO のゼロコンフィグの設定

---

### [書式]

```
yno zero-config id text operator_id place_id [password]
```

```
no yno zero-config id [text [operator_id [place_id [password]]]]
```

#### [設定値及び初期値]

- *operator\_id*
  - [設定値]: オペレーター ID (半角 4 文字以上 かつ 半角 64 文字以内)
  - [初期値]: -
- *place\_id*
  - [設定値]: プレース ID (半角 64 文字以内)
  - [初期値]: -
- *password*
  - [設定値]: パスワード (半角 64 文字以内 省略可)
  - [初期値]: -

#### [説明]

YNO エージェント機能のゼロコンフィグで使用するプレース ID やパスワードを設定する。本コマンドが設定されると自動で YNO マネージャーへの接続を試み、接続確立後にゼロコンフィグが作動する。

**yno access code** コマンドが設定されているときは、本コマンドは設定できない。

#### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510

## 51.8 YNO エージェント機能の動作状態の表示

#### [書式]

```
show status yno
```

#### [説明]

YNO エージェント機能の動作状態を表示する。ファームウェアのリビジョンにより表示内容が異なる。

- [新型式]
  - CWMP の動作状態

| 表示                  | 説明                                                  |
|---------------------|-----------------------------------------------------|
| 未接続(設定未完了)          | YNO エージェント機能が無効、または設定が不足している                        |
| 未接続(起動処理中)          | YNO エージェント機能が有効になり、初期化および ACS への接続中                 |
| 未接続(終了処理中)          | YNO エージェント機能が無効になり、ACS と切断処理中                       |
| 正常([セッション確立日時])     | ACS との接続に成功した(括弧内にはセッションの確立日時を表示)                   |
| 異常([理由])            | ACS との接続に失敗した(括弧内には異常理由を表示)                         |
| ゼロコンフィグ処理中 ([異常理由]) | ACS との接続に成功し、ゼロコンフィグが動作中(処理中に異常が発生した場合は括弧内に異常理由を表示) |

- XMPP の動作状態

| 表示  | 説明                |
|-----|-------------------|
| 未接続 | XMPP サーバーに接続していない |
| 接続  | XMPP を使用できる       |
| 異常  | XMPP を使用できない      |

- GFW の動作状態

| 表示  | 説明               |
|-----|------------------|
| 未接続 | GFW サーバーに接続していない |
| 接続  | GFW を使用できる       |
| 異常  | GFW を使用できない      |

- LAS の動作状態 (LAS 対応ファームウェアのみ)

| 表示  | 説明               |
|-----|------------------|
| 未接続 | LAS サーバーに接続していない |
| 接続  | LAS を使用できる       |
| 異常  | LAS を使用できない      |

- ヤマハネットワーク機器を管理しているオペレーターの ID

[旧型式]

- YNO エージェント機能の動作状態

| 現在の状態 | 説明                                        |
|-------|-------------------------------------------|
| 設定未完了 | YNO エージェント機能が無効、または設定が不足している              |
| 起動処理中 | YNO エージェント機能が有効になり、初期化および YNO マネージャーへの接続中 |
| 終了処理中 | YNO エージェント機能が無効になり、YNO マネージャーと切断処理中       |
| 正常動作中 | YNO マネージャーへの接続に成功した                       |
| 異常発生  | YNO マネージャーへの接続に失敗した                       |

- ヤマハネットワーク機器を管理しているオペレーターの ID
- YNO マネージャーへのセッション確立日時
- XMPP プロトコルを使用できるか否か
- GUI Forwarder を使用できるか否か (GUI Forwarder 接続対応ファームウェアのみ)

[ノート]

以下の機種及びファームウェアでは新型式の内容が、その他では旧型式の内容が表示される。

| 機種      | リビジョン           |
|---------|-----------------|
| NVR700W | Rev.15.00.14 以降 |
| NVR510  | Rev.15.01.13 以降 |

NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降で使用可能。

[表示例]

- [新形式]

```
> show status yno
CWMP:          正常 (2018/03/14 14:30:21)
XMPP:          正常
GFW:          正常
LAS:          正常
オペレーター ID:  dummy_id

> show status yno
CWMP:          異常 (ACS への接続に失敗しました)
XMPP:          未接続
GFW:          未接続
```

```

LAS:                未接続
オペレーター ID:   dummy_id

```

- [旧形式]

```

> show status yno
現在の状態:        正常動作中
オペレーター ID:   dummy_id
セッション確立日時: 2016/12/18 11:46:03
XMPP 接続:         有効
GFW 接続:         有効

```

[適用モデル]  
NVR700W, NVR510

## 51.9 LAS (Log Analysis Service)

---

### 51.9.1 SYSLOG 送信キューの長さの設定

---

[書式]

```

yno las syslog queue length length
no yno las syslog queue length

```

[設定値及び初期値]

- *length*
  - [設定値]: 長さ (1000..10000)
  - [初期値]: 10000

[説明]

SYSLOG 送信キュー長の最大値を設定する。現在の送信キュー長より小さい値を設定しても、すでに送信キューに蓄積されている SYSLOG は破棄されることなく、順次 LAS サーバーに送信される。

[ノート]

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 51.9.2 LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間の設定

---

[書式]

```

yno las request timeout seconds
no yno las request timeout

```

[設定値及び初期値]

- *seconds*
  - [設定値]: 秒数 (10..60)
  - [初期値]: 30

[説明]

LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間を設定する。

[ノート]

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で使用可能。

[適用モデル]  
NVR700W, NVR510

### 51.9.3 LAS クライアントがリクエストの送信を再試行する回数の設定

**[書式]**

**yno las request retry *count***  
**no yno las request retry**

**[設定値及び初期値]**

- *count*
  - [設定値]: 回数 (0..5)
  - [初期値]: 3

**[説明]**

LAS クライアントがリクエストの送信を再試行する回数を設定する。

**[ノート]**

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 51.9.4 LAS サーバーとのコネクションに対するキープアライブの設定

**[書式]**

**yno las connection keepalive *interval* [timeout=*sw*]**  
**no yno las connection keepalive**

**[設定値及び初期値]**

- *interval*
  - [設定値]:

| 設定値     | 説明                |
|---------|-------------------|
| off     | キープアライブをしない       |
| 30..300 | キープアライブの時間間隔 (秒数) |

- [初期値]: 60
- *sw*

- [設定値]:

| 設定値 | 説明                            |
|-----|-------------------------------|
| on  | LAS サーバーから応答がない場合にコネクションを切断する |
| off | LAS サーバーから応答がなくてもコネクションを切断しない |

- [初期値]: off

**[説明]**

YNO マネージャーでリアルタイム表示をしている間、LAS クライアントは LAS サーバーとの間でコネクションを確立した状態となる。コネクションが確立されている間は、*interval* に設定された時間間隔で LAS クライアントからキープアライブパケットが送信される。*sw* が on に設定されている場合、キープアライブパケットが送信されてから *interval* で設定された時間までに LAS サーバーから応答がないと、LAS クライアントはコネクションを一旦切断し、再接続を試みる。

**[ノート]**

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 51.9.5 LAS の動作状態の表示

---

### [書式]

```
show status yno las
```

### [説明]

LAS の動作状態を表示する。

### [ノート]

NVR700W Rev.15.00.22 以降、NVR510 Rev.15.01.21 以降で使用可能。

### [表示例]

```
> show status yno las
機能                : 有効
ログ送信結果        : 成功
SYSLOG 送信速度     : 100 行 / 60 秒
SYSLOG 送信キュー長 : 26
```

### [適用モデル]

NVR700W, NVR510

## 51.10 XMPP サーバーとのキープアライブの時間間隔の設定

---

### [書式]

```
yno xmpp connection keepalive interval
no yno xmpp connection keepalive [interval]
```

### [設定値及び初期値]

- *interval*
  - [設定値]: キープアライブパケットを送出する時間間隔 (30..300 秒)
  - [初期値]: 300

### [説明]

XMPP サーバーとのキープアライブ通信を実施する時間間隔を設定する。

### [ノート]

本コマンドを実行した場合、YNO マネージャーとの通信が一時的にできなくなる可能性があります。その場合、次の XMPP サーバーとのキープアライブ通信の実施時に XMPP 接続が再接続され、自動的に復旧されます。

NVR700W は Rev.15.00.23 以降で使用可能。

NVR510 は Rev.15.01.23 以降で使用可能。

### [適用モデル]

NVR700W, NVR510



## 第 52 章

### ダッシュボード

#### 52.1 ダッシュボードのデータを蓄積するか否かの設定

##### [書式]

```
dashboard accumulate type sw
no dashboard accumulate type [sw]
```

##### [設定値及び初期値]

- *type* : ガジェットの種類別
  - [設定値] :

| 設定値     | 説明        |
|---------|-----------|
| traffic | トラフィック情報  |
| nat     | NATセッション数 |

- [初期値] : -
- *sw*

- [設定値] :

| 設定値 | 説明        |
|-----|-----------|
| on  | データを蓄積する  |
| off | データを蓄積しない |

- [初期値] : off

##### [説明]

Web GUI のダッシュボードのガジェットで使用するデータを蓄積するか否かを設定する。なお、ダッシュボードで *type* で示されるガジェットを追加すると自動的に本コマンドの設定が on となる。

##### [ノート]

NVR700W は Rev.15.00.16 以降で使用不可。  
 NVR510 は Rev.15.01.15 以降で使用不可。  
 代わりに **statistics** コマンドを使用することができる。

##### [適用モデル]

NVR700W, NVR510

## 第 53 章

### 操作

#### 53.1 相手先情報番号の選択

##### [書式]

```
pp select peer_num
```

```
no pp select
```

##### [設定値及び初期値]

- *peer\_num*

- [設定値]:

| 設定値       | 説明                 |
|-----------|--------------------|
| 番号        | 相手先情報番号            |
| none      | 相手を選択しない           |
| anonymous | ISDN 番号が不明である相手の設定 |

- [初期値]: -

##### [説明]

設定や表示の対象となる相手先情報番号を選択する。以降プロンプトには、**console prompt** コマンドで設定した文字列と相手先情報番号が続けて表示される。

none を指定すると、プロンプトに相手先情報番号を表示しない。

##### [ノート]

この操作コマンドは一般ユーザーでも実行できる。

**no pp select** コマンドは **pp select none** コマンドと同じ動作をする。

##### [適用モデル]

NVR700W, NVR510

#### 53.2 トンネルインターフェース番号の選択

##### [書式]

```
tunnel select tunnel_num
```

```
no tunnel select
```

##### [設定値及び初期値]

- *tunnel\_num*

- [設定値]:

| 設定値  | 説明                 |
|------|--------------------|
| 番号   | トンネルインターフェース番号     |
| none | トンネルインターフェースを選択しない |

- [初期値]: -

##### [説明]

トンネルモードの設定や表示の対象となるトンネルインターフェース番号を選択する。

##### [ノート]

本コマンドの操作は、一般ユーザーでも実行できる。

プロンプトが **tunnel** の場合は、**pp** 関係のコマンドは入力できない。

**no tunnel select** コマンドは **tunnel select none** コマンドと同じ動作をする。  
 選択できるトンネルインターフェース番号のモデルによる違いは「[IPsec の設定](#)」を参照

[適用モデル]  
 NVR700W, NVR510

## 53.3 設定に関する操作

### 53.3.1 管理ユーザーへの移行

[書式]  
**administrator**

[説明]

このコマンドを発行してからでないと、ルーターの設定は変更できない。また操作コマンドも実行できない。パラメーターはなく、コマンド入力後にプロンプトに応じて改めて管理パスワードを入力する。入力されるパスワードは画面には表示されない。

[適用モデル]  
 NVR700W, NVR510

### 53.3.2 終了

[書式]  
**quit**  
**quit save**  
**exit**  
**exit save**

[設定値及び初期値]

- **save** : 管理ユーザーから抜ける際に指定すると、設定内容を不揮発性メモリに保存して終了
  - [初期値] :-

[説明]

ルーターへのログインを終了、または管理ユーザーから抜ける。  
 設定を変更して保存せずに管理ユーザーから抜けようとする、新しい設定内容を不揮発性メモリに保存するか否かを問い合わせる。不揮発性メモリに保存されれば、再起動を経ても同じ設定での起動が可能となる。

[適用モデル]  
 NVR700W, NVR510

### 53.3.3 設定内容の保存

[書式]  
**save** [*filename* [*comment*]]

[設定値及び初期値]

- *filename* : 設定を保存するファイル名
  - [設定値] :

| 設定値                   | 説明                                                  |
|-----------------------|-----------------------------------------------------|
| 0~4                   | 内蔵フラッシュ ROM の設定ファイル番号                               |
| usb1: <i>filename</i> | USB メモリ内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)     |
| sd1: <i>filename</i>  | microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内) |

- [初期値] :-
- *comment*

- [設定値]: 設定ファイルのコメント (半角 200 文字以内)
- [初期値]: -

#### [説明]

現在の設定内容を不揮発性メモリに保存する。  
ファイル指定を省略すると、起動時に使用した設定ファイルに保存する。

#### [適用モデル]

NVR700W, NVR510

### 53.3.4 設定ファイルの複製

#### [書式]

```
copy config from to
copy config from to crypto [password]
copy config from to [password]
```

#### [設定値及び初期値]

- *from*: コピー元ファイル名
- [設定値]:

| 設定値                   | 説明                                                               |
|-----------------------|------------------------------------------------------------------|
| 0~4.2                 | 内蔵フラッシュ ROM の設定ファイル番号                                            |
| usb1: <i>filename</i> | USB ストレージ内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)                |
| sd1: <i>filename</i>  | microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)              |
| *: <i>filename</i>    | USB ストレージおよび microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内) |
| emfs: <i>filename</i> | EMFS 内の設定ファイル名                                                   |

- [初期値]: -
- *to*: コピー先ファイル名
- [設定値]:

| 設定値                   | 説明                                                  |
|-----------------------|-----------------------------------------------------|
| 0~4                   | 内蔵フラッシュ ROM の設定ファイル番号                               |
| usb1: <i>filename</i> | USB ストレージ内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内)   |
| sd1: <i>filename</i>  | microSD カード内の設定ファイル名 ( <i>filename</i> は半角 99 文字以内) |

- [初期値]: -
- *crypto*: 設定ファイルを暗号化して保存する場合の暗号アルゴリズムの選択
- [設定値]:

| 設定値    | 説明             |
|--------|----------------|
| aes128 | AES128 で暗号化する。 |
| aes256 | AES256 で暗号化する。 |

- [初期値]: -
- *password*
- [設定値]: ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)
- [初期値]: -

**[説明]**

保存されている設定ファイルを複製する。  
 コピー元、コピー先の両方に外部メモリのファイルを指定することはできない。  
 FILENAME には "/" (ルート) からの絶対パスを指定することもできる。

**cold start** 直後は設定ファイルが存在しないので内蔵フラッシュ ROM から外部メモリへ設定ファイルのコピーはできない。

この場合、一度 **save** コマンドで設定を保存してから実行する必要がある。  
 内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB ストレージから検索される。

*filename* は絶対パスを使ってファイルを指定するかファイル名のみを指定する。*filename* にファイル名のみを指定した場合は外部メモリ内から自動検索する。  
 複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。  
 コピー先に外部メモリを指定する場合、*filename* に絶対パスを使ってファイルを指定する。

外部メモリを対象として暗号化機能を利用することができる。

CRYPTO を指定した場合、設定ファイルを暗号化してから外部メモリにコピーする。暗号化してコピーする場合、ファイル名には .rtfg 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に .rtfg 拡張子を追加する。

パスワードを省略して暗号化することができる。

**[ノート]**

外部メモリ上の暗号化された設定ファイルを復号しないで内蔵フラッシュ ROM にコピーすることはできない。  
 第 2 書式は、内蔵フラッシュ ROM の設定ファイルを外部メモリへ暗号化してコピーする場合にのみ利用できる。  
 第 3 書式は、外部メモリ内の暗号化された設定ファイルを復号化して内蔵フラッシュ ROM 内にコピーする場合にのみ利用できる。復号するときの暗号アルゴリズムは自動的に判別するので、復号時には暗号アルゴリズムを指定する必要はない。

外部メモリ内のファイルを指定できるのは、外部メモリインターフェースを持つ機種に限られる。  
 内蔵フラッシュ ROM の設定ファイル番号をコピー先ファイルとした場合、元のコピー先ファイルはこのコマンドの実行後は退避ファイルとなる。

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。  
 検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

EMFS 内のファイルは NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

**53.3.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー****[書式]**

**copy exec from to**

**[設定値及び初期値]**

- *from* : コピー元ファイル名
- [設定値]:

| 設定値           | 説明                                                          |
|---------------|-------------------------------------------------------------|
| 番号            | 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号、0 のみ指定可 (NVR700W で指定可能)      |
| usb1:filename | USB メモリ内のファームウェアファイル名 (filename は半角 99 文字以内)                |
| sd1:filename  | microSD カード内のファームウェアファイル名 (filename は半角 99 文字以内)            |
| *:filename    | USB メモリおよび microSD カード内のファームウェアファイル名 (filename は半角 99 文字以内) |

- [初期値]: -
- to: コピー先ファイル名
- [設定値]:

| 設定値 | 説明                                                                     |
|-----|------------------------------------------------------------------------|
| 番号  | 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号。(NVR700W では 0、1 が指定可、NVR510 では 0 のみ指定可) |

- [初期値]: -

#### [説明]

実行形式ファームウェアファイルを内蔵フラッシュ ROM にコピーする。  
内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "\*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリから検索される。

filename は絶対パスを使ってファイルを指定するかファイル名のみを指定する。

filename にファイル名のみを指定した場合は外部メモリ内から自動検索する。

複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

#### [ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

#### [適用モデル]

NVR700W, NVR510

### 53.3.6 設定ファイルの削除

#### [書式]

**delete config filename**

#### [設定値及び初期値]

- filename: 削除するファイル名
- [設定値]:

| 設定値   | 説明                     |
|-------|------------------------|
| all   | 内蔵フラッシュ ROM の全ての設定ファイル |
| 0~4.2 | 内蔵フラッシュ ROM の設定ファイル番号  |

- [初期値]: -

**[説明]**

保存されている設定ファイルを削除する。

**[適用モデル]**

NVR700W, NVR510

### 53.3.7 実行形式ファームウェアファイルの削除

---

**[書式]**

**delete exec filename**

**[設定値及び初期値]**

- *filename* : 削除するファイル名
  - [設定値]:

| 設定値 | 説明                           |
|-----|------------------------------|
| 番号  | 実行形式ファームウェアファイル番号 (1 のみ指定可能) |

- [初期値]: -

**[説明]**

保存されている実行形式ファームウェアファイルを削除する。

**[適用モデル]**

NVR700W

### 53.3.8 デフォルト設定ファイルの設定

---

**[書式]**

**set-default-config filename**

**[設定値及び初期値]**

- *filename* : 設定ファイル番号
  - [設定値]: 0~4.2
  - [初期値]: -

**[説明]**

起動時に使用する設定ファイルを設定する。

**[適用モデル]**

NVR700W, NVR510

### 53.3.9 デフォルトファームウェアファイルの設定

---

**[書式]**

**set-default-exec filename**

**[設定値及び初期値]**

- *filename*
  - [設定値]: 実行形式ファームウェアファイル番号 (0..1)
  - [初期値]: -

**[説明]**

起動時に使用するファームウェアファイルを設定する。

**[適用モデル]**

NVR700W

### 53.3.10 シリアルポートのボーレートの設定

---

**[書式]**

**set-serial-baudrate rate**

**[設定値及び初期値]**

- *rate*
  - [設定値]: ボーレート (9600 / 19200 / 38400 / 57600 / 115200)
  - [初期値]: 9600

**[説明]**

シリアルポートのボーレートを設定する。

**[適用モデル]**

NVR700W, NVR510

**53.3.11 設定の初期化**

---

**[書式]**

**cold start**

**[説明]**

工場出荷時の設定に戻し、再起動する。  
コマンド実行時に管理パスワードを入力する必要がある。

**[ノート]**

内蔵フラッシュ ROM の設定ファイルがすべて削除されることに注意。

**[適用モデル]**

NVR700W, NVR510

**53.3.12 遠隔地のルーターからの設定に対する制限**

---

**[書式]**

**remote setup accept *tel\_num* [*tel\_num\_list*]**

**remote setup accept any**

**remote setup accept none**

**no remote setup accept**

**[設定値及び初期値]**

- *tel\_num*
  - [設定値]: 電話番号
  - [初期値]: -
- *tel\_num\_list*
  - [設定値]: 電話番号を空白で区切った並び
  - [初期値]: -
- any: すべての遠隔地のルーターからの設定を許可することを示すキーワード
  - [初期値]: any
- none: すべての遠隔地のルーターからの設定を拒否することを示すキーワード
  - [初期値]: -

**[説明]**

自分のルーターの設定を許可する相手先を設定する。

**[適用モデル]**

NVR700W, NVR510

**53.4 動的情報のクリア操作**

---

**53.4.1 アカウントのクリア**

---

**[書式]**

**clear account**

**clear account pp [*peer\_num*]**

**clear account sip**



**clear account ngn data**  
**clear account ngn tel**  
**clear account mobile**  
**clear account wwan** [*num*]

[設定値及び初期値]

- *peer\_num*

- [設定値]:

| 設定値       | 説明                 |
|-----------|--------------------|
| 番号        | 相手先情報番号            |
| anonymous | anonymous インターフェース |
| 省略        | 省略時は現在選択している相手先    |

- [初期値]: -

- *num*

- [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| 1~30 | 内蔵無線 WAN インターフェース番号 |
| 省略   | 省略時は現在選択している番号      |

- [初期値]: -

[説明]

指定したインターフェース (第 1 書式ではすべての合計) に関するアカウント情報および通信履歴をクリアする。

[ノート]

通信履歴とは **show history** コマンドで表示される内容を指す。

**clear account** を実行すると、**show account analog** コマンドで表示されるような通話のアカウント情報および通信履歴についてもクリアされる。ただし、アナログ親機時に子機の情報まではクリアしない。

第 7 書式は NVR700W で使用可能。

[適用モデル]

NVR700W, NVR510

### 53.4.2 TEL ポートに関するアカウントのクリア

[書式]

**clear account analog** [*port*]  
**clear account analog total**

[設定値及び初期値]

- *port*

- [設定値]:

| 設定値 | 説明                        |
|-----|---------------------------|
| 1   | TEL1 ポート                  |
| 2   | TEL2 ポート                  |
| 省略  | 省略時はすべての TEL ポートについてクリアする |

- [初期値]: -

- *total*

- [設定値]: 電話回線を示すキーワード

- [初期値]: -

**[説明]**

TEL ポートに関するアカウントをクリアする。  
*port* パラメーターを省略した場合には、すべての TEL ポートのアカウントがクリアされる。

**[適用モデル]**

NVR700W, NVR510

### 53.4.3 ARP テーブルのクリア

---

**[書式]**

**clear arp**

**[説明]**

ARP テーブルをクリアする。

**[適用モデル]**

NVR700W, NVR510

### 53.4.4 IP の動的経路情報のクリア

---

**[書式]**

**clear ip dynamic routing**

**[説明]**

動的に設定された IP の経路情報をクリアする。

**[適用モデル]**

NVR700W, NVR510

### 53.4.5 ブリッジのラーニング情報のクリア

---

**[書式]**

**clear bridge learning *bridge\_interface***

**[設定値及び初期値]**

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -

**[説明]**

動的に受け取ったブリッジのラーニング情報をすべて消去する。

**[ノート]**

静的に設定した登録情報は消去されない。

**[適用モデル]**

NVR700W

### 53.4.6 ログのクリア

---

**[書式]**

**clear log [saved]**

**[設定値及び初期値]**

- saved
  - [設定値]: リポート直前のログをクリアする
  - [初期値]: -

**[説明]**

ログをクリアする。

**[適用モデル]**

NVR700W, NVR510

### 53.4.7 DNS キャッシュのクリア

#### [書式]

```
clear dns cache
```

#### [説明]

DNS リカーシブサーバーで持っているキャッシュをクリアする。

#### [適用モデル]

NVR700W, NVR510

### 53.4.8 インターフェースのカウンタ情報のクリア

#### [書式]

```
clear status interface
```

```
clear status pp peer_num
```

```
clear status tunnel tunnel_num
```

```
clear status wwan num
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -
- *num*
  - [設定値]: 内蔵無線 WAN インターフェース番号
  - [初期値]: -

#### [説明]

指定したインターフェースのカウンタ情報をクリアする。

#### [ノート]

モバイルインターネット機能で使用されるインターフェースの累積受信、累積送信、累計エラーは、発信制限に関する操作が行われないようにするためにクリアしない。これらの累積のカウンタ情報は、**clear mobile access limitation** コマンドを使用することでクリアできる。

#### [適用モデル]

NVR700W, NVR510

### 53.4.9 NAT アドレステーブルのクリア

#### [書式]

```
clear nat descriptor dynamic nat_descriptor
```

#### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]:

| 設定値           | 説明                  |
|---------------|---------------------|
| 1..2147483647 | NAT ディスクリプター番号      |
| all           | すべての NAT ディスクリプター番号 |

- [初期値]: -

#### [説明]

NAT アドレステーブルをクリアする。

## [ノート]

通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。

## [適用モデル]

NVR700W, NVR510

### 53.4.10 インターフェースの NAT アドレステーブルのクリア

---

## [書式]

```
clear nat descriptor interface dynamic interface
clear nat descriptor interface dynamic pp [peer_num]
clear nat descriptor interface dynamic tunnel [tunnel_num]
```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
    - 省略時は現在選択している相手先
  - [初期値]: -
- *tunnel\_num*
  - [設定値]:
    - トンネルインターフェース番号
    - 省略時は現在選択されているトンネルインターフェース
  - [初期値]: -

## [説明]

インターフェースに適用されている NAT アドレステーブルをクリアする。

## [適用モデル]

NVR700W, NVR510

### 53.4.11 IP マスカレードで管理しているセッションの統計情報のクリア

---

## [書式]

```
clear nat descriptor masquerade session statistics [nat_descriptor]
```

## [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]:
    - NAT ディスクリプター番号 (1..2147483647)
    - *nat\_descriptor* 省略時はすべての NAT ディスクリプタについて統計情報のクリアを行う。
  - [初期値]: -

## [説明]

IP マスカレードで管理しているセッションの統計情報をクリアする。

## [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

## [適用モデル]

NVR700W, NVR510

### 53.4.12 PPPoE パススルー機能がラーニングした情報のクリア

---

## [書式]

```
clear pppoe pass-through learning
```

**[説明]**

PPPoE パススルー機能がラーニングした情報を消去する。

**[ノート]**

本コマンドを実行しても PPPoE のセッションが切れることはない。NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

**53.4.13 IPv6 の動的経路情報の消去**

---

**[書式]**

```
clear ipv6 dynamic routing
```

**[説明]**

経路制御プロトコルが得た IPv6 の経路情報を消去する。

**[適用モデル]**

NVR700W, NVR510

**53.4.14 近隣キャッシュの消去**

---

**[書式]**

```
clear ipv6 neighbor cache [interface]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インタフェース名、ONU インターフェース名
  - [初期値]: -

**[説明]**

近隣キャッシュを消去する。

*interface* を指定した場合、そのインタフェース経由で得られた近隣キャッシュのみ消去する。

**[ノート]**

*interface* は、NVR700W は Rev.15.00.22 以降、NVR510 は Rev.15.01.21 以降のファームウェアで指定可能。

**[適用モデル]**

NVR700W, NVR510

**53.4.15 起動情報の履歴を削除する**

---

**[書式]**

```
clear boot list
```

**[説明]**

起動情報の履歴を削除する。

**[適用モデル]**

NVR700W, NVR510

**53.4.16 外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除**

---

**[書式]**

```
clear external-memory syslog
```

**[説明]**

外部メモリに保存された現在書き込み中の SYSLOG ファイル内のログのクリアとすべての SYSLOG のバックアップファイルの削除を行う。

削除の対象となる SYSLOG のバックアップファイルは、**external-memory syslog filename** コマンドで指定されたパス内に存在するファイルが対象となる。

なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインターフェースに外部メモリが接続されている場合にのみ動作する。

[適用モデル]

NVR700W, NVR510

## 53.5 ファイル、ディレクトリの操作

---

### 53.5.1 ディレクトリの作成

---

[書式]

**make directory path**

[設定値及び初期値]

- *path*
  - [設定値]: 相対パスまたは絶対パス
  - [初期値]: -

[説明]

指定した名前のディレクトリを作成する。

*path* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[適用モデル]

NVR700W, NVR510

### 53.5.2 ファイルまたはディレクトリの削除

---

[書式]

**delete path**

[設定値及び初期値]

- *path*
  - [設定値]: 相対パスまたは絶対パス
  - [初期値]: -

[説明]

指定したファイルまたはディレクトリを削除する。

ディレクトリが空でない場合は配下のファイルとディレクトリも同時に削除される。

*path* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

*path* に相対パスで "config" または "exec" を指定した場合、本コマンドではなく、**delete config** コマンドまたは **delete exec** コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

[適用モデル]

NVR700W, NVR510

### 53.5.3 ファイルまたはディレクトリの複製

---

[書式]

**copy from to**

[設定値及び初期値]

- *from*
  - [設定値]: コピー元のファイル名またはディレクトリ名
  - [初期値]: -
- *to*
  - [設定値]: コピー先のファイル名またはディレクトリ名
  - [初期値]: -

**[説明]**

ファイルまたはディレクトリを複製する。*from* がディレクトリの場合は、配下のすべてのファイルとディレクトリが再帰的に複製される。

*from* と *to* は、それぞれ相対パスまたは絶対パスで指定する。

*from* がファイルの場合の動作は以下の通りとなる。

*to* と同名のファイルが存在する場合は *to* のデータが *from* のデータで上書きされる。

*to* と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のファイルが作成される。

*to* と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

*from* がディレクトリの場合の動作は以下の通りとなる。

*to* と同名のファイルが存在する場合は複製を実行できない。

*to* と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のディレクトリが作成される。

*to* と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

*from*、*to* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

**[ノート]**

*from* に相対パスで "config" または "exec" を指定した場合、本コマンドではなく、**copy config** コマンドまたは **copy exec** コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

本コマンドでは、必要に応じた親ディレクトリ作成が行われないため、*to* のパス中に存在しないディレクトリが含まれているとエラーになる。

**[適用モデル]**

NVR700W, NVR510

**53.5.4 ファイル名またはディレクトリ名の変更**

---

**[書式]**

```
rename path name
```

**[設定値及び初期値]**

- *path*
  - [設定値]: 変更対象のファイルまたはディレクトリの相対パスまたは絶対パス
  - [初期値]: -
- *name*
  - [設定値]: 変更後の名前
  - [初期値]: -

**[説明]**

指定したファイルまたはディレクトリの名前を変更する。

*path* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

**[適用モデル]**

NVR700W, NVR510

**53.6 その他の操作**

---

**53.6.1 相手先の使用許可の設定**

---

**[書式]**

```
pp enable peer_num [peer_num ...]
no pp enable peer_num
```

**[設定値及び初期値]**

- *peer\_num*
  - [設定値]:

| 設定値       | 説明                     |
|-----------|------------------------|
| 番号        | 相手先情報番号                |
| 番号 1-番号 2 | 番号 1 から番号 2 までの相手先情報番号 |
| 番号 1-     | 番号 1 以上のすべての相手先情報番号    |
| -番号 1     | 番号 1 以下のすべての相手先情報番号    |
| anonymous | anonymous インターフェース     |
| all       | すべての相手先情報番号            |

- [初期値] :-

#### [説明]

相手先を使用できる状態にする。工場出荷時、すべての相手先は **disable** 状態なので、使用する場合は必ずこのコマンドで **enable** 状態にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。複数指定は、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

#### [ノート]

必ず、1. **pp disable**、2. **disconnect**、3. **pp** の設定変更、4. **pp enable**、5. **connect** の手順を踏んで設定を変更する。**pp enable** コマンドを実行すると内部情報の初期化が行われる。**pp** の設定変更の有無に関わらず、**pp** が接続中に **pp enable** を実行すると、内部情報の初期化により、**pp** に紐付けられている **tunnel** 等が切断される場合がある。

#### [適用モデル]

NVR700W, NVR510

## 53.6.2 相手先の使用不許可の設定

#### [書式]

```
pp disable peer_num [peer_num ...]
```

#### [設定値及び初期値]

- *peer\_num*
- [設定値] :

| 設定値       | 説明                     |
|-----------|------------------------|
| 番号        | 相手先情報番号                |
| 番号 1-番号 2 | 番号 1 から番号 2 までの相手先情報番号 |
| 番号 1-     | 番号 1 以上のすべての相手先情報番号    |
| -番号 1     | 番号 1 以下のすべての相手先情報番号    |
| anonymous | anonymous インターフェース     |
| all       | すべての相手先情報番号            |

- [初期値] :-

#### [説明]

相手先を使用できない状態にする。

相手先の設定を行う場合は **disable** 状態であることが望ましい。

複数指定した場合には、その全てで使用できない状態になる。複数指定は、NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

#### [適用モデル]

NVR700W, NVR510



### 53.6.3 再起動

---

#### [書式]

**restart** [*binary* [*config*]]

**restart** [*config*]

#### [設定値及び初期値]

- *binary*
  - [設定値]: 実行形式ファームウェアファイル番号 (0~1)
  - [初期値]: -
- *config*
  - [設定値]: 内蔵フラッシュ ROM の設定ファイル番号 (0~4.2)
  - [初期値]: -

#### [説明]

ルーターを再起動する。

起動時の設定ファイルと実行形式ファームウェアファイルを指定できる。

*binary* は、デフォルトファームウェアファイルに設定される。

*config* は、デフォルト設定ファイルに設定される。

#### [ノート]

第 1 書式は、NVR700W のみ指定可能。

#### [適用モデル]

NVR700W, NVR510

### 53.6.4 インターフェースの再起動

---

#### [書式]

**interface reset** *interface* [*interface* ...]

#### [設定値及び初期値]

- *interface*
  - [設定値]:
    - LAN インターフェース名
    - ONU インターフェース名
    - WAN インターフェース名
    - USB インターフェース名
    - SD インターフェース名
  - [初期値]: -

#### [説明]

指定したインターフェースを再起動する。

LAN インターフェースと ONU インターフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。

USB と SD インターフェースでは、ポートの給電が OFF,ON され、USB デバイスや microSD カードの再アタッチが行われる。

#### [ノート]

lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インターフェースが同時にリセットされる。

**pp bind** コマンド、経路情報などすべての設定を整えた後に実行する。対象とするインターフェースがバインドされているすべての相手先情報番号の通信を停止した状態で実行すること。

#### [適用モデル]

NVR700W, NVR510

### 53.6.5 内蔵無線 WAN モジュールの再起動

#### [書式]

```
interface reset wwan-module
```

#### [説明]

内蔵無線 WAN モジュールをリセットする。

#### [適用モデル]

NVR700W

### 53.6.6 発信

#### [書式]

```
connect interface
```

```
connect peer_num
```

```
connect pp peer_num
```

```
connect tunnel tunnel_num
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 発信相手の相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
  - [初期値]: -

#### [説明]

手動で発信する。

#### [ノート]

**connect tunnel** コマンドは、データコネクトを使用した拠点間接続以外のトンネルには使用できない。

#### [適用モデル]

NVR700W, NVR510

### 53.6.7 切断

#### [書式]

```
disconnect interface
```

```
disconnect peer_num
```

```
disconnect pp peer_num
```

```
disconnect tunnel tunnel_num
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:

| 設定値           | 説明             |
|---------------|----------------|
| 番号            | 切断する相手先情報番号    |
| all           | すべての相手先情報番号    |
| anonymous     | anonymous のすべて |
| anonymous1 .. | 指定した anonymous |

- [初期値]: -
- *tunnel\_num*
  - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
  - [初期値]: -

**[説明]**

手動で切断する。

**[ノート]**

**disconnect tunnel** コマンドは、データコネクトを使用した拠点間接続以外のトンネルには使用できない。

**[適用モデル]**

NVR700W, NVR510

## 53.6.8 ping

---

**[書式]**

```
ping [-s datalen] [-c count] [-sa ip_address] [-w wait] host
```

**[設定値及び初期値]**

- *datalen*: データ長 (1..65535 バイト)
  - [初期値]: 64
- *count*
  - [設定値]: 実行回数 (1..21474836)
  - [初期値]: Ctrl+c キーが入力されるまで繰り返す
- *ip\_address*
  - [設定値]: 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - [初期値]: ルーターのインターフェースに付与されたアドレスの中から選択する
- *wait*: パケット送信間隔秒数 (0.1 .. 3600.0)
  - [初期値]: 1
- *host*
  - [設定値]:
    - ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
    - ping をかけるホストの名称
  - [初期値]: -

**[説明]**

ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。

*count* パラメーターを省略すると、Ctrl+c キーを入力するまで実行を継続する。

-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

**[適用モデル]**

NVR700W, NVR510

## 53.6.9 ping6 の実行

---

**[書式]**

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination
```

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination %scope_id
```

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination interface
```

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination pp peer_num
```

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination tunnel tunnel_num
```

```
ping6 destination [count]
```

```
ping6 destination %scope_id [count]
ping6 destination interface [count]
ping6 destination pp peer_num [count]
ping6 destination tunnel tunnel_num [count]
```

#### [設定値及び初期値]

- *datalen*
  - [設定値]: データ長 (1..65535 バイト)
  - [初期値]: 64
- *count*
  - [設定値]: 実行回数 (1..21474836)
  - [初期値]: Ctrl+c キーが入力されるまで繰り返す
- *ipv6\_address*
  - [設定値]: 始点 IPv6 アドレス
  - [初期値]: ルーターのインターフェースに付与されたアドレスの中から選択する
- *wait*: パケット送信間隔秒数 (0.1 .. 3600.0)
  - [初期値]: 1
- *destination*
  - [設定値]: 送信する宛先の IPv6 アドレス、または名前
  - [初期値]: -
- *scope\_id*
  - [設定値]: スコープ識別子
  - [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

指定した宛先に対して ICMPv6 Echo Request を送信する。

スコープ識別子は、**show ipv6 address** コマンドで表示できる。

*count* パラメーターを省略すると、Ctrl+c キーを入力するまで実行を継続する。

-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

#### [適用モデル]

NVR700W, NVR510

## 53.6.10 traceroute

---

#### [書式]

```
traceroute host [noresolv] [-sa source]
```

#### [設定値及び初期値]

- *host*
  - [設定値]:
    - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx)
    - traceroute をかけるホストの名称
  - [初期値]: -
- *noresolv*: DNS による解決を行わないことを示すキーワード

- [初期値]: -
- *source*
  - [設定値]: 始点 IP アドレス
  - [初期値]: -

**[説明]**

指定したホストまでの経路を調べて表示する。

**[適用モデル]**

NVR700W, NVR510

### 53.6.11 traceroute6 の実行

---

**[書式]**

```
traceroute6 destination [noresolv] [-sa source]
```

**[設定値及び初期値]**

- *destination*
  - [設定値]: 送信する宛先の IPv6 アドレス、または名前
  - [初期値]: -
- *noresolv*
  - [設定値]: DNS による解決を行わないことを示すキーワード
  - [初期値]: -
- *source*
  - [設定値]: 始点 IP アドレス
  - [初期値]: -

**[説明]**

指定した宛先までの経路を調べて表示する。

*noresolv* オプションおよび *-sa* オプションは NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

### 53.6.12 nslookup

---

**[書式]**

```
nslookup host
```

**[設定値及び初期値]**

- *host*
  - [設定値]:
    - IP アドレス
    - IPv6 アドレス
    - ホスト名
  - [初期値]: -

**[説明]**

DNS による名前解決を行う。

**[ノート]**

AAAA レコードと IPv6 アドレスの PTR レコードは、以下の機種およびリビジョンで使用可能。

- NVR700W Rev.15.00.16 以降

- NVR510 Rev.15.01.15 以降

**[適用モデル]**

NVR700W, NVR510

### 53.6.13 SIP サーバーに対し手動で接続

---

**[書式]**

**sip server connect number**

**[設定値及び初期値]**

- *number*
  - [設定値]: 登録番号( 1..65535)
  - [初期値]: -

**[説明]**

SIP サーバーに対し手動で接続(サインイン)する。

基本的には自動的に SIP サーバーに接続するので、本コマンドは手動で切断した時や接続されていない状態を確認した時に、接続する場合に使用する。

**[適用モデル]**

NVR700W, NVR510

### 53.6.14 SIP サーバーに対し手動で切断

---

**[書式]**

**sip server disconnect number**

**[設定値及び初期値]**

- *number*
  - [設定値]: 登録番号( 1..65535)
  - [初期値]: -

**[説明]**

SIP サーバーに対し手動で切断 (サインアウト) する。

切断後、ルーターを再起動するか手動で接続しない限り SIP サーバーに接続しない。

**[適用モデル]**

NVR700W, NVR510

### 53.6.15 IPv4 動的フィルターの接続管理情報の削除

---

**[書式]**

**disconnect ip connection session\_id [channel\_id]**

**[設定値及び初期値]**

- *session\_id*
  - [設定値]: セッションの識別子
  - [初期値]: -
- *channel\_id*
  - [設定値]: チャンネルの識別子
  - [初期値]: -

**[説明]**

指定したセッションに属する特定のチャンネルを削除する。チャンネルを指定しないときには、そのセッションに属するすべてのチャンネルを削除する。

**[適用モデル]**

NVR700W, NVR510

### 53.6.16 IPv6 動的フィルターの接続管理情報の削除

---

**[書式]**

**disconnect ipv6 connection session\_id [channel\_id]**

**[設定値及び初期値]**

- *session\_id*
  - [設定値]: セッションの識別子
  - [初期値]: -
- *channel\_id*
  - [設定値]: チャネルの識別子
  - [初期値]: -

**[説明]**

指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

**[適用モデル]**

NVR700W, NVR510

**53.6.17 TELNET クライアント****[書式]**

```
telnet host [port [mode [negotiation [abort]]]]
```

**[設定値及び初期値]**

- *host*
  - [設定値]: TELNET をかける相手の IP アドレス、ホスト名、または NGN 網電話番号
  - [初期値]: -
- *port*: 使用するポート番号
  - [設定値]:
    - 十進数
    - ポート番号のニーモニック
    - 省略時は 23 (TELNET)
  - [初期値]: 23
- *mode*: TELNET 通信 (送信) の動作モード
  - [設定値]:

| 設定値       | 説明                                           |
|-----------|----------------------------------------------|
| character | 文字単位で通信する                                    |
| line      | 行単位で通信する                                     |
| auto      | <i>port</i> パラメーターの設定値により character/line を選択 |
| 省略        | 省略時は auto                                    |

- [初期値]: auto
- *negotiation*: TELNET オプションのネゴシエーションの選択
  - [設定値]:

| 設定値  | 説明                                   |
|------|--------------------------------------|
| on   | ネゴシエーションする                           |
| off  | ネゴシエーションしない                          |
| auto | <i>port</i> パラメーターの設定値により on/off を選択 |
| 省略   | 省略時は auto                            |

- [初期値]: auto
- *abort*: TELNET クライアントを強制的に終了させるためのアボートキー
  - [設定値]:
    - 十進数の ASCII コード
    - 省略時は 29(^)
  - [初期値]: 29

**[説明]**

TELNET クライアントを実行する。

**[ノート]**

ホスト名による接続は A レコード (IPv4) のみ対応している。

character モードは、通常の TELNET サーバーなどへの接続のための透過的な通信を行う。

line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について

**1. TELNET 通信の動作モードの自動選択**

port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

**2. TELNET オプションのネゴシエーションの自動選択**

port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

**[適用モデル]**

NVR700W, NVR510

**53.6.18 スイッチングハブ MAC アドレステーブルの消去**

---

**[書式]**

```
clear switching-hub macaddress [interface]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -

**[説明]**

スイッチングハブ LSI 内部に保持している動的 MAC アドレステーブルを消去する。

**[ノート]**

**lan type** コマンドの *macaddress-aging* パラメーターが off の場合にこのコマンドを実行してもテーブルエントリ情報は消去されず、次に *macaddress-aging* パラメーターが on にされた時点で消去される。

**[適用モデル]**

NVR700W, NVR510

**53.6.19 Magic Packet の送信**

---

**[書式]**

```
wol send [-i interval] [-c count] interface mac_address [ip_address [udp port]]
```

```
wol send [-i interval] [-c count] interface mac_address ethernet type
```

**[設定値及び初期値]**

- *interval*
  - [設定値]: パケットの送信間隔 (秒)
  - [初期値]: 1
- *count*
  - [設定値]: パケットの送信回数
  - [初期値]: 4
- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *mac\_address*
  - [設定値]: MAC アドレス
  - [初期値]: -
- *ip\_address*



- [設定値]: IPv4 アドレス
- [初期値]: -
- *port*
  - [設定値]: UDP ポート番号
  - [初期値]: -
- *type*
  - [設定値]: イーサネットタイプフィールドの値 (1501..65535)
  - [初期値]: -

#### [説明]

指定した LAN インターフェースに Magic Packet を送信する。

第 1 書式では、IPv4 UDP パケットとして UDP ペイロードに Magic Packet データシーケンスを格納したパケットを送信する。終点 IP アドレスと、終点 UDP ポート番号を指定できるが、省略した場合には、終点 IP アドレスとしてはインターフェースのディレクティッドブロードキャストアドレスが、終点ポート番号には 9(discard) が使われる。また、終点 IP アドレスを指定した場合にはユニキャストでパケットを送信する。その場合、通常のルーティングや ARP の手順は踏まず、終点 MAC アドレスはコマンドで指定したものになる。終点 IP アドレスを省略した場合にはブロードキャストでパケットを送信する。

第 2 書式では、Ethernet ヘッダの直後から Magic Packet のデータシーケンスが始まるパケットを送信する。

どちらの形式でも、*-i*、*-c* オプションで Magic Packet の送信間隔および回数を指定できる。パケットの送信中でも、*^C* キーでコマンドを中断できる。

#### [ノート]

ヤマハルーター自身が直結している LAN インターフェース以外には Magic Packet を送信できない。

#### [適用モデル]

NVR700W, NVR510

## 53.6.20 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行

#### [書式]

```
http revision-up go [no-confirm [prompt]]
```

#### [設定値及び初期値]

- *no-confirm*: 書き換え可能なリビジョンのファームウェアが存在するときに、ファームウェアの更新を行うかどうかを確認しない
  - [初期値]: -
- *prompt*: コマンド実行後、すぐにプロンプトを表示させ、他のコマンドを実行できるようにする
  - [初期値]: -

#### [説明]

WEB サーバーに置いているファームウェアと現在実行中のファームウェアのリビジョンをチェックし、書き換え可能であればファームウェアのリビジョンアップを行う。書き換え可能なリビジョンのファームウェアが存在すると、「更新しますか? (Y/N)」という確認を求めてくるので、更新する場合は "Y" を、更新しない場合は "N" を入力する必要がある。

"no-confirm" オプションを指定すると、更新の確認をせずにファームウェアの書き換えを行う。さらに、"prompt" オプションを指定すると、コマンド実行直後にプロンプトが表示され、続けて他のコマンドを実行することができるようになる。ただし、ファームウェアを内蔵フラッシュ ROM に書き込んでいる間は他の操作ができなくなる。

**http revision-up permit** コマンドで HTTP リビジョンアップを許可されていない時は、ファームウェアの書き換えは行わない。

**http revision-down permit** コマンドでリビジョンダウンが許可されている場合は、WEB サーバーにおいてあるファームウェアが現在のファームウェアよりも古いリビジョンであってもファームウェアの書き換えを行う。

なお、WEB サーバーにおいてあるファームウェアが現在のファームウェアと同一リビジョンの場合には、ファームウェアの書き換えは行わない。

#### [適用モデル]

NVR700W, NVR510

### 53.6.21 URL フィルターの統計情報のクリア

---

#### [書式]

```
clear url filter
clear url filter [interface]
clear url filter pp [peer_num]
clear url filter tunnel [tunnel_num]
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

URL フィルターの統計情報を消去する。インターフェースが指定されない場合は、すべてのインターフェースの情報を消去する。

#### [適用モデル]

NVR700W

### 53.6.22 メール通知の実行

---

#### [書式]

```
mail notify status exec id
```

#### [設定値及び初期値]

- *id*
  - [設定値]: 設定番号 (1..10)
  - [初期値]: -

#### [説明]

状態情報をメールで送信する。

#### [適用モデル]

NVR700W, NVR510

### 53.6.23 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ)

---

#### [書式]

```
rotate external-memory syslog
```

#### [説明]

外部メモリに保存された SYSLOG ファイルのローテート (バックアップ) を行う。  
 現在書き込み中の SYSLOG ファイルをバックアップファイルに退避し、新たに書き込み用の SYSLOG ファイルを作成する。既に同名のバックアップファイルが存在する場合には実行されない。  
 また、バックアップファイルを作成する際、バックアップファイル数が **external-memory syslog filename** コマンドで指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。  
 バックアップファイル名の書式については、**external-memory syslog filename** コマンドを参照のこと。  
 なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインターフェースに外部メモリが接続されている場合のみ動作する。

## [ノート]

`schedule at` コマンドで定期的に本コマンドを実行するようにしておくと、日毎、週毎、あるいは月毎の SYSLOG のバックアップファイルを自動で作成することが可能になる。

## [設定例]

```
schedule at 1 */* 00:00 * rotate external-memory syslog # 毎日バックアップを実行する
schedule at 1 */mon 00:00 * rotate external-memory syslog # 毎週月曜日にバックアップを実行する
schedule at 1 */1 00:00 * rotate external-memory syslog # 毎月 1 日にバックアップを実行する
```

## [適用モデル]

NVR700W, NVR510

### 53.6.24 ライセンス認証の実行

---

## [書式]

`license authentication go`

## [説明]

LMS サーバーに対してライセンス認証を行う。実行中に Ctrl-C 押下で中断することができる。

## [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

## [適用モデル]

NVR700W

### 53.6.25 ライセンス認証のリトライの間隔と回数の設定

---

## [書式]

`license authentication retry interval interval count`

`no license authentication retry interval [interval count]`

## [設定値及び初期値]

- *interval*
  - [設定値]: ライセンス認証をリトライするまでの間隔 (秒) (1 .. 3600)
  - [初期値]: 30
- *count*
  - [設定値]: ライセンス認証をリトライする回数 (1 - 10)
  - [初期値]: 5

## [説明]

ライセンス認証に失敗したときのリトライ間隔と回数を設定する。

ライセンス認証に失敗したとき、*interval* に設定した間隔でライセンス認証のリトライを行う。*count* に設定した回数連続でライセンス認証に失敗した場合はリトライを停止する。

本コマンドの設定に関わらず、`license authentication go` コマンドによる手動認証に失敗した場合は、ライセンス認証のリトライは行わない。

## [ノート]

ライセンス認証のリトライ待ちであるとき、`license authentication go` コマンドによる手動認証を行った場合は、ライセンス認証のリトライは停止する。

NVR700W は Rev.15.00.17 以降で使用可能。

## [適用モデル]

NVR700W

### 53.6.26 設定の一括更新

---

## [書式]

`load [config-type] config [difference] [silent | interactive] [no-configure-refresh] [no-key-generate] [rollback-timer=timer]`

**[設定値及び初期値]**

- *config-type* : 引数 *config* の種類を表す

- [設定値] :

| 設定値    | 説明                                   |
|--------|--------------------------------------|
| config | config 番号                            |
| file   | RTFS, EMFS, 外部メモリーに保存されているファイルのファイル名 |

- [初期値] : -

- *config*

- [設定値] : config 番号、またはファイル名

- [初期値] : -

- *timer*

- [設定値] : 復元タイマーの値 ( 120 .. 21474836 )

- [初期値] : -

**[説明]**

指定された設定ファイルへ設定を復元・更新する。

*config-type* を省略した書き方をした場合、*config* は以下の順で解釈される。

- 保存されている *config* 番号に一致する場合はその設定
- 存在するファイル名と一致する場合はそのファイル

更新方法には、置換と差分の 2 種類がある。

- 置換 : 現在の設定内容をいったんすべて消去し、設定ファイルの設定内容に置き換える。
- 差分 : 現在の設定内容を設定ファイルの設定内容に変更する、最小限のコマンドを実行する。

デフォルト動作は置換更新であり、*difference* オプションを指定することで差分更新となる。

デフォルトでは、設定を置き換えるために実行するコマンドがコンソールに表示される。*silent* オプションを指定すると、コマンドの表示はせずに設定を書き換える。*interactive* オプションを指定すると、コマンドを一つずつ実行するかどうか確認しながら設定を更新できる。*interactive* オプションは、対話的ではないインターフェース ( Web GUI 設定中のコマンド入力など ) からは利用できない。*silent* オプションと *interactive* オプションを同時に指定することはできない。

**load** コマンドで設定を置き換えた場合、必要に応じて '**ospf configure refresh**'、'**bgp configure refresh**' あるいは '**ipv6 ospf configure refresh**' コマンドが追加で実行される。*no-configure-refresh* オプションを指定すると、この動作を抑止することができる。

更新前後の設定ファイルに **sshd host key generate** コマンドが設定されていた場合、*no-key-generate* オプションを指定するとホスト鍵の再生成は実行されず、更新前のホスト鍵の設定を引き継ぐことができる。

*rollback-timer* オプションで復元タイマーが設定できる。以下の場合に、自動的に設定が **load** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

復元タイマーを停止するには以下のいずれかの操作が必要である。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- *rollback-timer* オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。*rollback-timer* オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

*rollback-timer* オプションを省略した場合には、復元タイマーは動作しない。

**[ノート]**

暗号化された設定ファイルには対応していない。

[適用モデル]  
NVR700W, NVR510

### 53.6.27 ロールバックタイマーの起動

---

[書式]

**rollback timer** *timer*

[設定値及び初期値]

- *timer*
  - [設定値]: 復元タイマーの値 (秒、1..21474836)
  - [初期値]: -

[説明]

復元タイマーのみを設定する。以下の場合に、自動的に設定が **rollback timer** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

以下の場合に、復元タイマーは停止する。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- **rollback-timer** オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。**rollback-timer** オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

[ノート]

このコマンドは、手動で設定を変更するときのセーフネットとして利用することができる。

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

[適用モデル]  
NVR700W, NVR510

### 53.6.28 設定の確認

---

[書式]

**confirm**

[説明]

**load** コマンドあるいは **rollback timer** コマンドで起動した復元タイマーを停止し、設定変更の内容を確定させる。

[ノート]

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

[適用モデル]  
NVR700W, NVR510

### 53.6.29 ファイルをマクロとして実行する

---

[書式]

**call** [-v] [-x] *filename* [*parameter..*]

[設定値及び初期値]

- *filename*
  - [設定値]: ファイル名
  - [初期値]: -
- *parameter*
  - [設定値]: マクロ引数

- [初期値]:-

**[説明]**

*filename* で指定したファイルをマクロとして実行する。

マクロには引数を渡すことができる。引数が、NAME=VALUE の形をしている場合、マクロ内では変数 NAME として VALUE を参照できる。他の形の引数は位置引数として、指定された順番に、\$1、\$2 等でアクセスできる。\$0 はファイル名、\$\* はすべての位置引数を空白で結合した文字列となる。引数はすべてマクロ内でのみ利用可能な変数である。

-v オプションを指定すると、マクロを実行するときに実行する各行について、変数とエイリアスの展開前の内容を表示しながら実行する。

-x オプションは、変数とエイリアスを展開した後の行を表示しながらマクロを実行する。

**[ノート]**

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

### 53.6.30 echo

---

**[書式]**

**echo** [*string*]

**[設定値及び初期値]**

- *string*
  - [設定値]: 表示したい文字列
  - [初期値]:-

**[説明]**

指定された文字列を表示する。

**[ノート]**

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 第 54 章

### 設定の表示

#### 54.1 機器設定の表示

**[書式]**

```
show environment [detail]
```

**[設定値及び初期値]**

- detail
  - [設定値]: 全体の平均 CPU 使用率に加えて、各コア毎の CPU 使用率を表示する
  - [初期値]: -

**[説明]**

以下の項目が表示される。

- システムのリビジョン
- MAC アドレス
- CPU、メモリの使用量 (%)
- パケットバッファの使用量 (%)
- 動作しているファームウェアと設定ファイル
- 起動時に使用されるファームウェアと設定ファイル
- シリアルボーレート
- ファンの状態

**[適用モデル]**

NVR700W, NVR510

#### 54.2 すべての設定内容の表示

**[書式]**

```
show config
show config filename
less config
less config filename
```

**[設定値及び初期値]**

- *filename*: 設定ファイル名
  - [設定値]: 0..4.2
  - [初期値]: -

**[説明]**

設定されたすべての設定内容を表示する。  
ファイルを指定した場合には、ログインパスワードと管理パスワードを問い合わせられる。

**[適用モデル]**

NVR700W, NVR510

#### 54.3 指定した AP の設定内容の表示

**[書式]**

```
show config ap [ap]
less config ap [ap]
```

**[設定値及び初期値]**

- *ap*
  - [設定値]:

- MAC アドレスもしくは経路
- 省略時は、選択されている AP について表示する
- [初期値]:-

**[説明]**

**show config**、**less config** コマンドの表示の中から、指定した AP に関するものだけを表示する。

**[適用モデル]**

NVR700W, NVR510

## 54.4 指定した PP の設定内容の表示

---

**[書式]**

```
show config pp [peer_num]
show config pp [peer_num-peer_num]
less config pp [peer_num]
less config pp [peer_num-peer_num]
```

**[設定値及び初期値]**

- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
    - 省略時、選択されている相手について表示する
  - [初期値]:-

**[説明]**

**show config**、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

相手先情報番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲の相手先情報番号に関するものを表示する。

**[適用モデル]**

NVR700W, NVR510

## 54.5 指定したスイッチの設定内容の表示

---

**[書式]**

```
show config switch [switch]
less config switch [switch]
```

**[設定値及び初期値]**

- *switch*
  - [設定値]:
    - MAC アドレスもしくは経路
    - 省略時は、選択されているスイッチについて表示する
  - [初期値]:-

**[説明]**

**show config**、**less config** コマンドの表示の中から、指定したスイッチに関するものだけを表示する。

**[適用モデル]**

NVR700W, NVR510

## 54.6 指定したトンネルの設定内容の表示

---

**[書式]**

```
show config tunnel [tunnel_num] [expand]
show config tunnel [tunnel_num-tunnel_num] [expand]
less config tunnel [tunnel_num] [expand]
less config tunnel [tunnel_num-tunnel_num] [expand]
```



**[設定値及び初期値]**

- `tunnel_num`
  - [設定値]:
    - トンネル番号
    - 省略時は、選択されているトンネルについて表示する
  - [初期値]: -

**[説明]**

**show config**、**less config** コマンドの表示の中から、指定したトンネル番号に関するものだけを表示する。

トンネル番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲のトンネル番号に関するものを表示する。

**expand** キーワードを指定すると、**tunnel template** コマンドにて指定したトンネルテンプレートが適用された後の、実際にルーターの動作時に参照される設定を表示する。

**[ノート]**

NVR510 は Rev.15.01.03 以降で **expand** パラメーターを指定可能。

**[適用モデル]**

NVR700W, NVR510

## 54.7 指定した WWAN の設定内容の表示

---

**[書式]**

```
show config wwan [wwan_num]
show config wwan [wwan_num-wwan_num]
less config wwan [wwan_num]
less config wwan [wwan_num-wwan_num]
```

**[設定値及び初期値]**

- `wwan_num`
  - [設定値]:
    - 相手先情報番号
    - 省略時、選択されている相手について表示する
  - [初期値]: -

**[説明]**

**show config**、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

相手先情報番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲の相手先情報番号に関するものを表示する。

**[ノート]**

Rev.15.00.10 以降で使用可能。

**[適用モデル]**

NVR700W

## 54.8 設定の差分の表示

---

**[書式]**

```
show config difference [[config-type1] config1] [config-type2] config2
```

**[設定値及び初期値]**

- `config-type1/2`: 引数 `config1`, `config2` の種類を表す
  - [設定値]:

| 設定値    | 説明                                   |
|--------|--------------------------------------|
| config | config 番号                            |
| file   | RTFS, EMFS, 外部メモリーに保存されているファイルのファイル名 |

- [初期値]: -

- *config1/2*
  - [設定値]:' '( 現在動作中の設定 )、config 番号、またはファイル名のいずれか
  - [初期値]:-

**[説明]**

*config1* と *config2* の差分を、*config1* を *config2* へ変換するためのコマンド列という形で表示する。

*config1* にあり、*config2* にないコマンドは **no** 形式で表示され、*config1* になく、*config2* にあるコマンドは通常形式で表示される。*config1*、*config2* とともに、**show config** コマンドでの表示に沿った形でインデント ( 段付け ) されていないわけではない。

*config1* を省略した場合は、' '( 現在動作中の設定 ) が指定されたものとする。

*config-type1/2* を省略した場合、*config1/2* は以下の順で解釈される。

- 保存されている config 番号に一致する場合は、その設定
- 存在するファイル名と一致する場合は、そのファイル

**[ノート]**

*config1/2* に config 番号を指定した場合で、保存されている設定に **login password**、**login password encrypted**、**administrator password**、**administrator password encrypted** コマンドが含まれている場合には、動作前にそれらのパスワードを入力する必要がある。

このコマンドは、管理者モードでのみ動作する。

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 54.9 設定ファイルの一覧

---

**[書式]**

```
show config list
less config list
```

**[説明]**

内蔵フラッシュ ROM に保存されている設定ファイルのファイル名、日時、コメントの一覧を表示する。起動中の設定ファイルに '\*' が表示される。

**[適用モデル]**

NVR700W, NVR510

### 54.10 アナログ親機に登録された各 TEL ポート設定内容の表示

---

**[書式]**

```
show config analog extension
```

**[説明]**

カスケード接続機能でアナログ親機に登録された、各 TEL ポートの設定内容を表示する。

**[ノート]**

各 TEL ポートの設定内容は、カスケード接続機能によってアナログ親機に登録される。本コマンドでは、カスケード接続機能によってアナログ親機に登録された各 TEL ポート設定の内容を表示する。

**[適用モデル]**

NVR700W, NVR510

### 54.11 ファイル情報の一覧の表示

---

**[書式]**

```
show file list location [all] [file-only]
less file list location [all] [file-only]
```

**[設定値及び初期値]**

- *location* : 表示するファイルのある位置

- [設定値]:

| 設定値         | 説明                             |
|-------------|--------------------------------|
| internal    | 内蔵フラッシュ ROM                    |
| 相対パスまたは絶対パス | 内蔵フラッシュ ROM の RTFS 領域、および外部メモリ |

- [初期値]: -
- *all*
  - [設定値]: 配下の全ディレクトリを対象にする
  - [初期値]: -
- *file-only*
  - [初期値]: ファイル名のみを表示する

**[説明]**

指定した場所に格納されているファイルの情報の一覧を表示する。

*all*、*file-only* オプションは、*location* に外部メモリを指定したときのみ有効となる。

内蔵フラッシュ ROM の RTFS 領域や外部メモリに保存されているファイルやディレクトリの一覧を表示する場合には、対象となるディレクトリを相対パスまたは絶対パスで *location* に指定する。

*location* に相対パスを指定した場合、環境変数 *PWD* を基点としたパスと解釈される。

*PWD* は *set* コマンドで変更可能であり、初期値は "/" である。

起動中の設定ファイルに '\*' が表示される。

**[適用モデル]**

NVR700W, NVR510

## 54.12 インターフェースに付与されている IPv6 アドレスの表示

**[書式]**

```
show ipv6 address [interface]
```

```
show ipv6 address pp [peer_num]
```

```
show ipv6 address tunnel [tunnel_num]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース、LOOPBACK インターフェース名、NULL インターフェース、ブリッジインターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - *anonymous*
    - 省略時、選択されている相手について表示する
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

**[説明]**

各インターフェースに付与されている IPv6 アドレスを表示する。

インターフェースを指定しない場合は、すべてのインターフェースについて情報を表示する。

[適用モデル]  
NVR700W, NVR510

### 54.13 SSH サーバー公開鍵の表示

---

[書式]

**show sshd public key** [fingerprint]

[設定値及び初期値]

- fingerprint: 鍵指紋を表示することを示すキーワード
  - [初期値]:-

[説明]

SSH サーバーの公開鍵を表示する。  
fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

[適用モデル]  
NVR700W, NVR510

### 54.14 指定したインターフェースのフィルター内容の表示

---

[書式]

**show ip secure filter interface** [dir]  
**show ip secure filter pp** [peer\_num] [dir]  
**show ip secure filter tunnel** [tunnel\_num] [dir]

[設定値及び初期値]

- *interface*
  - [設定値]: フィルターの適用されたインターフェース名
  - [初期値]:-
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]:-
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]:-
- *dir*
  - [設定値]: フィルターの適用された方向、'in' または 'out'
  - [初期値]:-

[説明]

指定したインターフェースに適用されているフィルター定義の内容を表示する。

[適用モデル]  
NVR700W, NVR510

### 54.15 指定したインターフェースの IPv6 フィルター内容の表示

---

[書式]

**show ipv6 secure filter interface** [dir]  
**show ipv6 secure filter pp** [peer\_num] [dir]  
**show ipv6 secure filter tunnel** [tunnel\_num] [dir]

[設定値及び初期値]

- *interface*
  - [設定値]: フィルターの適用されたインターフェース名
  - [初期値]:-
- *peer\_num*
  - [設定値]: 相手先情報番号

- [初期値]:-
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]:-
- *dir*
  - [設定値]: フィルターの適用された方向、'in' または 'out'
  - [初期値]:-

**[説明]**

指定したインターフェースに適用されている IPv6 フィルター定義の内容を表示する。

**[ノート]**

NVR700W Rev.15.00.16 以降、NVR510 Rev.15.01.15 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 54.16 ファームウェアファイルの一覧

---

**[書式]**

**show exec list**

**less exec list**

**[説明]**

内蔵フラッシュ ROM に保存されている実行形式ファームウェアファイルの情報を表示する。起動中の実行形式ファームウェアファイルには '\*' 印が表示される。実行形式ファームウェアファイルが保存されている外部メモリが接続されている場合には、そのファームウェアファイルの情報も表示される。

**[適用モデル]**

NVR700W, NVR510

## 54.17 環境変数の表示

---

**[書式]**

**show set [name]**

**[設定値及び初期値]**

- name
  - [設定値]: 環境変数名
  - [初期値]:-

**[説明]**

指定した環境変数の値を表示する。

*name* を省略した場合には、設定されている環境変数をすべて表示する。

**[ノート]**

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

## 54.18 エイリアスの表示

---

**[書式]**

**show alias [name]**

**[設定値及び初期値]**

- name
  - [設定値]: エイリアス名

- [初期値]:-

#### [説明]

指定したエイリアスの値を表示する。

*name* を省略した場合には、設定されているエイリアスをすべて表示する。

#### [ノート]

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 54.19 マクロの表示

---

#### [書式]

**show macro** [*name*]

#### [設定値及び初期値]

- name
  - [設定値]: マクロ名
  - [初期値]:-

#### [説明]

指定したマクロの値を表示する。

*name* を省略した場合には、設定されているマクロをすべて表示する。

#### [ノート]

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

#### [適用モデル]

NVR700W, NVR510

## 第 55 章

### 状態の表示

#### 55.1 ARP テーブルの表示

##### [書式]

```
show arp [interface[/sub_interface]]
```

##### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *sub\_interface*
  - [設定値]: 1-32
  - [初期値]: -

##### [説明]

ARP テーブルを表示する。インターフェース名を指定した場合、そのインターフェース経由で得られた ARP テーブル情報だけを表示する。

##### [適用モデル]

NVR700W, NVR510

#### 55.2 インターフェースの状態の表示

##### [書式]

```
show status interface
```

```
show status wwan [num]
```

##### [設定値及び初期値]

- *interface*
  - [設定値]:
    - LAN インターフェース名
    - ONU インターフェース名
    - WAN インターフェース名
    - ブリッジインターフェース名
  - [初期値]: -
- *num*
  - [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| 1～30 | 内蔵無線 WAN インターフェース番号 |
| 省略   | 省略時は現在選択している番号      |

- [初期値]: -

##### [説明]

インターフェースの状態を表示する。

##### [ノート]

**show status wwan**、および、ブリッジインターフェースは NVR700W で指定可能。

##### [適用モデル]

NVR700W, NVR510

## 55.3 各相手先の状態の表示

---

### [書式]

**show status pp** [*peer\_num*]

### [設定値及び初期値]

- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
    - 省略時、選択されている相手について表示する
  - [初期値]:-

### [説明]

各相手先の接続中または最後に接続された場合の状態を表示する。

- 現在接続されているか否か
- 直前の呼の状態
- 接続(切断)した日時
- 回線の種類
- 通信時間
- 切断理由
- 通信料金
- 相手とこちらの PP 側 IP アドレス
- 正常に送信したパケットの数
- 送信エラーの数と内訳
- 正常に受信したパケットの数
- 受信エラーの数と内訳
- PPP の状態
- CCP の状態
- その他

### [適用モデル]

NVR700W, NVR510

## 55.4 IP の経路情報テーブルの表示

---

### [書式]

**show ip route** [*destination*]

**show ip route detail**

**show ip route summary**

### [設定値及び初期値]

- *destination*
  - [設定値]:
    - 相手先 IP アドレス
    - 省略時、経路情報テーブル全体を表示する
  - [初期値]:-
- **detail**: 現在有効な IPv4 経路に加えて、動的経路制御プロトコルによって得られた経路により隠されている静的経路も表示する
  - [初期値]:-
- **summary**: IPv4 の経路数をプロトコル毎に合計して表示する
  - [初期値]:-

### [説明]

IP の経路情報テーブルまたは相手先 IP アドレスへのゲートウェイを表示する。ネットマスクは設定時の表現に関わらず連続するビット数で表現される。



**[ノート]**

動的経路制御プロトコルで得られた経路については、プロトコルに応じて付加情報を表示する。表示する付加情報は以下ようになる。

RIP: メトリック値

**[適用モデル]**

NVR700W, NVR510

## 55.5 RIP で得られた経路情報の表示

---

**[書式]**

**show ip rip table**

**[説明]**

RIP で得られた経路情報を表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.6 IPv6 の経路情報の表示

---

**[書式]**

**show ipv6 route**

**show ipv6 route detail**

**show ipv6 route summary**

**[設定値及び初期値]**

- detail : 現在有効な IPv6 経路に加えて、動的経路制御プロトコルによって得られた経路により隠されている静的経路も表示する
  - [初期値] : -
- summary : IPv6 の経路数をプロトコル毎に合計して表示する
  - [初期値] : -

**[説明]**

IPv6 の経路情報を表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.7 IPv6 の RIP テーブルの表示

---

**[書式]**

**show ipv6 rip table**

**[説明]**

IPv6 の RIP テーブルを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.8 近隣キャッシュの表示

---

**[書式]**

**show ipv6 neighbor cache [interface]**

**show ipv6 neighbor cache [interface] summary**

**[設定値及び初期値]**

- interface
  - [設定値] : LAN インタフェース名、ONU インターフェース名
  - [初期値] : -

**[説明]**

近隣キャッシュの状態を表示する。

*interface* を指定した場合、そのインターフェース経由で得られた近隣キャッシュの状態のみ表示する。

*summary* を指定した場合、近隣キャッシュのエントリー数のみ表示する。

**[ノート]**

*interface*、*summary* は、NVR700W は Rev.15.00.22 以降、NVR510 は Rev.15.01.21 以降のファームウェアで指定可能。

**[適用モデル]**

NVR700W, NVR510

## 55.9 ブリッジのラーニング情報の表示

---

**[書式]**

```
show bridge learning bridge_interface
```

**[設定値及び初期値]**

- *bridge\_interface*
  - [設定値]: ブリッジインターフェース名
  - [初期値]: -

**[説明]**

ブリッジの MAC アドレスのラーニング情報を表示する。

**[適用モデル]**

NVR700W

## 55.10 IPsec の SA の表示

---

**[書式]**

```
show ipsec sa [id]
```

```
show ipsec sa gateway [gateway_id] [detail]
```

**[設定値及び初期値]**

- *id*
  - [設定値]:
    - SA の識別子
    - 省略時はすべての SA について表示する
  - [初期値]: -
- *gateway\_id*
  - [設定値]:
    - セキュリティー・ゲートウェイの識別子
    - 省略時はすべてのセキュリティ・ゲートウェイの SA のサマリを表示する。
  - [初期値]: -
- *detail*: SA の詳細な情報を表示する。
  - [初期値]: -

**[説明]**

IPsec の SA の状態を表示する。

*id* で与えられた識別子を持つ SA の情報を表示する。

**[ノート]**

該当の SA の生成時に XAUTH 認証を行った場合、認証に使用したユーザー名

- RADIUS 認証を行ったか否か
- 通知した内部 IP アドレス
- 追加した経路情報
- 適用したフィルターの情報

を同時に表示する。

NVR510 は Rev.15.01.03 以降で使用可能。

[適用モデル]

NVR700W, NVR510

## 55.11 証明書の情報の表示

---

[書式]

**show pki certificate summary** [*cert\_id*]

[設定値及び初期値]

- *cert\_id*
  - [設定値]: 証明書ファイルの識別子(1..8)
  - [初期値]: -

[説明]

証明書の情報を表示する。

表示される情報は以下の通り

- Subject
- SubjectAltName
- 使用可能期間 (Not Before, Not After)
- 証明書のタイプ (CA 証明書 / 機器証明書)

*cert\_id* を指定した場合、指定したファイル識別子の証明書の情報だけを表示する。

[適用モデル]

NVR700W

## 55.12 CRL ファイルの情報の表示

---

[書式]

**show pki crl** [*crl\_id*]

[設定値及び初期値]

- *crl\_id*
  - [設定値]: CRL ファイルの識別子(1..8)
  - [初期値]: -

[説明]

CRL ファイルの情報を表示する。

表示される情報は以下の通り

- バージョン
- 発行者
- 更新日時
- 次の更新日時

[適用モデル]

NVR700W

## 55.13 VRRP の情報の表示

---

[書式]

**show status vrrp** [*interface* [*vrid*]]

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *vrid*

- [設定値]: VRRP グループ ID(1..255)
- [初期値]: -

**[説明]**

VRRP の情報を表示する。

**[適用モデル]**

NVR700W

## 55.14 動的 NAT ディスクリプターのアдресマップの表示

---

**[書式]**

```
show nat descriptor address [nat_descriptor] [detail]
```

**[設定値及び初期値]**

- *nat\_descriptor*
- [設定値]:

| 設定値           | 説明                  |
|---------------|---------------------|
| 1..2147483647 | NAT ディスクリプター番号      |
| all           | すべての NAT ディスクリプター番号 |

- [初期値]: -
- detail: 動的 IP マスカレードの全エントリを表示
- [初期値]: -

**[説明]**

動的な NAT ディスクリプターのアдресマップを表示する。

*nat\_descriptor* を省略した場合はすべての NAT ディスクリプター番号について表示する。

**[ノート]**

IP マスカレードで大量にポートを使用している場合は、detail オプションを指定すると全エントリの表示に時間がかかり通信に影響を及ぼすことがあるため、IP マスカレードで使用中のポートの個数を確認したいときは、detail オプションを指定しないようにするか、**show nat descriptor masquerade port summary** コマンドを使うことを推奨する。

**[適用モデル]**

NVR700W, NVR510

## 55.15 動作中の NAT ディスクリプターの適用リストの表示

---

**[書式]**

```
show nat descriptor interface bind interface
```

```
show nat descriptor interface bind pp
```

```
show nat descriptor interface bind tunnel
```

**[設定値及び初期値]**

- *interface*
- [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
- [初期値]: -

**[説明]**

NAT ディスクリプターと適用インターフェースのリストを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.16 LAN インターフェースの NAT ディスクリプターのアдресマップの表示

---

**[書式]**

```
show nat descriptor interface address interface
```

```
show nat descriptor interface address pp peer_num
show nat descriptor interface address tunnel tunnel_num
```

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

インターフェースに適用されている NAT ディスクリプターのアドレスマップを表示する。

#### [適用モデル]

NVR700W, NVR510

## 55.17 IP マスカレードで使用しているポート番号の個数の表示

---

#### [書式]

```
show nat descriptor masquerade port [nat_descriptor] summary
```

#### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]:
    - NAT ディスクリプター番号 (1..2147483647)
    - *nat\_descriptor* 省略時はすべての NAT ディスクリプターについて表示する。
  - [初期値]: -

#### [説明]

動的 IP マスカレードで使用しているポート番号の個数を表示する。静的 IP マスカレードで確保されているポート番号の個数は含まれない。

#### [ノート]

**nat descriptor backward-compatibility** コマンドで、*type* パラメーターを 2 に設定した場合は本コマンドは使用できない。

代わりに、**show nat descriptor masquerade session summary** コマンドで、管理しているセッション数を表示することができる。

#### [適用モデル]

NVR700W, NVR510

## 55.18 IP マスカレードで使用しているセッション数の表示

---

#### [書式]

```
show nat descriptor masquerade session [nat_descriptor] summary
```

#### [設定値及び初期値]

- *nat\_descriptor*
  - [設定値]:
    - NAT ディスクリプター番号 (1..2147483647)
    - *nat\_descriptor* 省略時はすべての NAT ディスクリプターについて表示する。
  - [初期値]: -

**[説明]**

IP マスカレードで管理しているセッション数およびセッション数のピーク値を表示する。セッション数のピーク値は NAT ディスクリプターの設定変更やルーターの再起動によってクリアされ、**clear nat descriptor dynamic** コマンドによるセッションの削除ではクリアされない。

**[ノート]**

本コマンドは、**nat descriptor backward-compatibility** コマンドで、*type* パラメーターを 2 に設定した場合のみ使用可能である。

**[適用モデル]**

NVR700W, NVR510

## 55.19 IP マスカレードで管理しているセッションの統計情報の表示

---

**[書式]**

```
show nat descriptor masquerade session statistics [nat_descriptor]
```

**[設定値及び初期値]**

- *nat\_descriptor*
  - [設定値]:
    - NAT ディスクリプター番号 (1..2147483647)
    - *nat\_descriptor* 省略時はすべての NAT ディスクリプターについて表示する。
  - [初期値]:-

**[説明]**

IP マスカレードで管理しているセッションの統計情報として始点 IP アドレスで識別されるホスト毎にセッション数、ピーク値、制限された回数と時刻を表示する。セッション数の制限値は、**nat descriptor masquerade session limit** コマンドの設定値に従う。

**[ノート]**

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 55.20 L2TP の状態の表示

---

**[書式]**

```
show status l2tp [tunnel tunnel_num]
```

**[設定値及び初期値]**

- *tunnel\_num*
  - [設定値]: トンネル番号
  - [初期値]:-

**[説明]**

L2TP の状態を表示します。

**[ノート]**

NVR510 は Rev.15.01.03 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 55.21 PPTP の状態の表示

---

**[書式]**

```
show status pptp
```

**[説明]**

PPTP の状態や GRE の統計情報などを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.22 IPIP トンネリングの状態の表示

---

**[書式]**

**show status ipip** [*tunnel tunnel\_num*]

**[設定値及び初期値]**

- *tunnel\_num*
  - [設定値]: トンネル番号
  - [初期値]: -

**[説明]**

IPIP トンネリングの状態を表示する。

**[ノート]**

NVR700W の Rev.15.00.10 以降、NVR510 の Rev.15.01.09 以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 55.23 OSPF 情報の表示

---

**[書式]**

**show status ospf** *info*

**[設定値及び初期値]**

- *info*: 表示する情報の種類
  - [設定値]:

| 設定値          | 説明           |
|--------------|--------------|
| database     | OSPF のデータベース |
| neighbor     | 近隣ルーター       |
| interface    | 各インターフェースの状態 |
| virtual-link | バーチャルリンクの状態  |

- [初期値]: -

**[説明]**

OSPF の各種情報を表示する。

**[適用モデル]**

NVR700W

## 55.24 BGP の状態の表示

---

**[書式]**

**show status bgp neighbor** [*ip-address*]  
**show status bgp neighbor** *ip-address route-type*

**[設定値及び初期値]**

- *ip-address*
  - [設定値]: 隣接ルーターの IP アドレス
  - [初期値]: -
- *route-type*: 経路情報の表示
  - [設定値]:

| 設定値               | 説明                          |
|-------------------|-----------------------------|
| advertised-routes | 隣接ルーターに広告している経路を表示する        |
| received-routes   | 隣接ルーターから受信した経路を表示する         |
| routes            | 隣接ルーターから受信した経路のうち有効なものを表示する |

- [初期値]:-

#### [説明]

BGP の隣接ルーターに関する情報を表示する。

*ip-address* を指定した場合には特定の隣接ルーターの情報を表示する。*ip-address* を省略した場合には、すべての隣接ルーターの情報を表示する。

*route-type* を指定した場合には、隣接ルーターとの間でやり取りしている経路の情報を表示する。*advertised-routes* を指定した時には、隣接ルーターに対して広告している経路を表示する。*received-routes* を指定した時には、隣接ルーターから受信した経路をすべて表示する。*routes* を指定した時には、隣接ルーターから受信した経路のうち、**bgp export filter** などを受け入れられた経路だけを表示する。

#### [適用モデル]

NVR700W

## 55.25 DHCP サーバーの状態の表示

#### [書式]

```
show status dhcp [summary] [scope_n]
```

#### [設定値及び初期値]

- *summary* : 各 DHCP スコープの IP アドレス割り当て状況の概要を表示する
  - [初期値]:-
- *scope\_n*
  - [設定値]: スコープ番号 (1-65535)
  - [初期値]:-

#### [説明]

各 DHCP スコープのリース状況を表示する。以下の項目が表示される。

- DHCP スコープのリース状態
- DHCP スコープ番号
- ネットワークアドレス
- 割り当て中 IP アドレス
- 割り当て中クライアント MAC アドレス
- リース残時間
- 予約済 (未使用) IP アドレス
- DHCP スコープの全 IP アドレス数
- 除外 IP アドレス数
- 割り当て中 IP アドレス数
- 利用可能アドレス数 (うち予約済 IP アドレス数)

#### [適用モデル]

NVR700W, NVR510

## 55.26 DHCP クライアントの状態の表示

#### [書式]

```
show status dhcpc
```

#### [説明]

DHCP クライアントの状態を表示する。

- クライアントの状態
  - インターフェース



- IP アドレス ( 取得できないときはその状態 )
- DHCP サーバー
- リース残時間
- クライアント ID
- ホスト名 ( 設定時 )
- 共通情報
  - DNS サーバー
  - ゲートウェイ

## [適用モデル]

NVR700W, NVR510

## 55.27 DHCPv6 の状態の表示

---

## [書式]

```
show status ipv6 dhcp
```

## [説明]

DHCPv6 に関する状態を表示する。

## [適用モデル]

NVR700W, NVR510

## 55.28 バックアップ状態の表示

---

## [書式]

```
show status backup
```

## [説明]

バックアップ設定されたインターフェースについて、バックアップの状態を表示する。

## [適用モデル]

NVR700W

## 55.29 動的フィルタによって管理されている接続の表示

---

## [書式]

```
show ip connection
show ip connection [interface [direction] [ip_address]]
show ip connection pp [peer_num [direction] [ip_address]]
show ip connection tunnel [tunnel_num [direction] [ip_address]]
show ip connection summary
show ip connection detail [interface [direction]]
show ip connection detail pp [peer_num [direction]]
show ip connection detail tunnel [tunnel_num [direction]]
```

## [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -
- *direction*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| in  | 入力方向 |
| out | 出力方向 |

- [初期値]: -
- *ip\_address*
  - [設定値]: IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
  - [初期値]: -
- *summary*: インターフェース/方向単位の管理コネクション数、および全体の合計を表示する
  - [初期値]: -
- *detail*: 動的フィルターによって管理されているすべてのコネクションを表示する
  - [初期値]: -

**[説明]**

指定したインターフェースについて、動的なフィルターによって管理されているコネクションを表示する。インターフェースを指定しないときには、すべてのインターフェースの情報を表示する。

*detail* を指定しない場合は管理されているコネクションを送信元 IP アドレスごとに集約して表示する。ただし、*ip\_address* が指定された場合には *detail* を指定した場合の情報のうちソースアドレスが *ip\_address* に一致するものを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.30 IPv6 の動的フィルターによって管理されているコネクションの表示

**[書式]**

```
show ipv6 connection
show ipv6 connection interface [direction] [ipv6_address]
show ipv6 connection pp [peer_num [direction] [ipv6_address]]
show ipv6 connection tunnel [tunnel_num [direction] [ipv6_address]]
show ipv6 connection summary
show ipv6 connection detail interface [direction]
show ipv6 connection detail pp [peer_num [direction]]
show ipv6 connection detail tunnel [tunnel_num [direction]]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -
- *direction*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| in  | 入力方向 |
| out | 出力方向 |

- [初期値]: -
- *ipv6\_address*
  - [設定値]: IPv6 アドレス部分
  - [初期値]: -
- *summary*: インターフェース/方向単位の管理コネクション数、および全体の合計を表示する

- [初期値]:-
- **detail**: 動的フィルターによって管理されているすべてのコネクションを表示する
  - [初期値]:-

**[説明]**

指定したインターフェースについて、動的なフィルターによって管理されているコネクションを表示する。インターフェースを指定しないときには、すべてのインターフェースの情報を表示する。

**detail** を指定しない場合は管理されているコネクションを送信元 IP アドレスごとに集約して表示する。ただし、*ipv6\_address* が指定された場合には **detail** を指定した場合の情報のうちソースアドレスが *ipv6\_address* に一致するものを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.31 ネットワーク監視機能の状態の表示

**[書式]**

**show status ip keepalive**

**[説明]**

ネットワーク監視機能の状態を表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.32 侵入情報の履歴の表示

**[書式]**

**show ip intrusion detection**  
**show ip intrusion detection interface [direction]**  
**show ip intrusion detection pp [peer\_num [direction]]**  
**show ip intrusion detection tunnel [tunnel\_num [direction]]**

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]:-
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]:-
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]:-
- *direction*
  - [設定値]:

| 設定値 | 説明   |
|-----|------|
| in  | 入力方向 |
| out | 出力方向 |

- [初期値]:-

**[説明]**

最近の侵入情報を表示する。各インターフェースの各方向ごとに最大 50 件まで表示できる。

**[適用モデル]**

NVR700W, NVR510

## 55.33 相手先ごとの接続時間情報の表示

### [書式]

```
show pp connect time [peer_num]
```

### [設定値及び初期値]

- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - anonymous
    - 省略時、選択されている相手について表示
  - [初期値]:-

### [説明]

選択されている相手の接続時間情報を表示する。

### [適用モデル]

NVR700W, NVR510

## 55.34 PPPoE パススルー機能がラーニングした情報の表示

### [書式]

```
show pppoe pass-through learning
```

### [説明]

PPPoE パススルー機能がラーニングした情報を表示する。

### [ノート]

NVR700W Rev.15.00.14 以降、NVR510 Rev.15.01.13 以降で使用可能。

### [適用モデル]

NVR700W, NVR510

## 55.35 ネットボランチ DNS サービスに関する設定の表示

### [書式]

```
show status netvolante-dns interface
show status netvolante-dns pp [peer_num]
```

### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]:-
- *peer\_num*
  - [設定値]:
    - 相手先情報番号
    - 省略時、選択されている相手について表示
  - [初期値]:-

### [説明]

ダイナミック DNS に関する設定を表示する。

表示内容

|                  |                            |
|------------------|----------------------------|
| ネットボランチ DNS サービス | AUTO/OFF                   |
| インターフェース         | INTERFACE                  |
| ホストアドレス          | aaa.bbb.netvolante.jp      |
| 電話アドレス           | aaaaaaaa.tel.netvolante.jp |
| IP アドレス          | aaa.bbb.ccc.ddd            |

|        |                     |
|--------|---------------------|
| 最新更新日時 | 2001/01/25 15:00:00 |
| タイムアウト | 90 秒                |

[適用モデル]  
NVR700W, NVR510

## 55.36 スイッチングハブ MAC アドレステーブルの表示

[書式]

```
show status switching-hub macaddress [interface [port]] [mac_address]
```

[設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]: -
- *port*
  - [設定値]: ポート番号 (1..4)
  - [初期値]: -
- *mac\_address*
  - [設定値]: MAC アドレス
  - [初期値]: -

[説明]

スイッチングハブ LSI 内部に保持しているポート毎の動的 MAC アドレステーブルを表示する。ポート番号を指定するとそのポートに関する情報のみが表示される。LAN インターフェース名にはスイッチングハブを持つインターフェースだけが指定可能である。

[適用モデル]  
NVR700W, NVR510

## 55.37 UPnP に関するステータス情報の表示

[書式]

```
show status upnp
```

[説明]

UPnP に関するステータス情報を表示する。

[適用モデル]  
NVR700W, NVR510

## 55.38 トンネルインターフェースの状態の表示

[書式]

```
show status tunnel [tunnel_num]
```

```
show status tunnel [state]
```

```
show status tunnel [name=name]
```

[設定値及び初期値]

- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -
- *state*: 接続状態
  - [設定値]:

| 設定値 | 説明                         |
|-----|----------------------------|
| up  | 接続されているトンネルインターフェース一覧を表示する |

| 設定値  | 説明                          |
|------|-----------------------------|
| down | 接続されていないトンネルインターフェース一覧を表示する |

- [初期値]:-
- *name*
  - [設定値]: 接続相手の名前
  - [初期値]:-

**[説明]**

トンネルインターフェースの状態を表示する。

第2書式はPPTPトンネルには対応していない。PPTPの対応機種では、PPTPトンネルは接続されていないトンネルインターフェースとして判定される。また、L2TP/IPsec機能およびL2TPv3/IPsec機能の対応機種では、L2TPトンネルはIPsecトンネルの状態に応じて接続状態が判定される。

第3書式では、マルチポイントトンネルインターフェースで接続している相手の中から *name* に指定した文字列を含む名前が付与されている接続相手の情報を抽出して表示する。なお、接続相手の名前は相手側の **tunnel multipoint local name** コマンドで設定する。

**[ノート]**

第3書式は、NVR700W Rev.15.00.10以降で使用可能。

**[適用モデル]**

NVR700W, NVR510

## 55.39 VLAN インターフェースの状態の表示

---

**[書式]**

```
show status vlan [interface/sub_interface]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名
  - [初期値]:-
- *sub\_interface*
  - [設定値]: 1-32
  - [初期値]:-

**[説明]**

VLAN インターフェースの情報を表示する。VLAN インターフェース名を指定した場合はそのインターフェースの情報だけを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.40 トリガによるメール通知機能の状態の表示

---

**[書式]**

```
show status mail service [template_id] [debug]
```

**[設定値及び初期値]**

- *template\_id*
  - [設定値]: テンプレート ID (1..10)
  - [初期値]:-
- *debug*: デバッグ用の内部情報を表示させる
  - [初期値]:-

**[説明]**

トリガによるメール通知機能の内部状態を表示する。  
 テンプレート ID を指定しない場合はすべてのテンプレート ID についての状態を表示する。

**[適用モデル]**

NVR700W, NVR510

**55.41 MLD のグループ管理情報の表示****[書式]**

```
show status ipv6 mld
```

**[説明]**

MLD で管理されている情報を一覧表示する。  
 MLD プロキシが動作している場合は、このコマンドで転送先を確認することができる。

**[適用モデル]**

NVR700W, NVR510

**55.42 IPv6 マルチキャストの経路情報の表示****[書式]**

```
show ipv6 mroute fib
```

**[説明]**

IPv6 マルチキャストパケットの転送経路を表示する。  
 このコマンドでは、転送経路ごとに以下の内容を一覧表示する。

| 項目名          | 説明                                             |
|--------------|------------------------------------------------|
| Inbound IF   | 入力インターフェース                                     |
| Source       | マルチキャストパケットのソースアドレス                            |
| Group        | マルチキャストパケットのグループアドレス                           |
| Outbound IFs | 出力インターフェース。複数のインターフェースに出力される場合は、"," 区切りで表示される。 |

**[適用モデル]**

NVR700W, NVR510

**55.43 ログインしているユーザー情報の表示****[書式]**

```
show status user
```

**[説明]**

ルーターにログインしているユーザーの情報を表示する。以下の項目が表示される。

- ユーザー名
- 接続種別
- ログインした日時
- アイドル時間
- 接続相手の IP アドレス

また、ユーザーの状態に応じてユーザー名の前に以下の記号が表示される。

| 記号         | 状態           |
|------------|--------------|
| アスタリスク (*) | 自分自身のユーザー情報  |
| プラス (+)    | 管理者モードになっている |

| 記号         | 状態               |
|------------|------------------|
| アットマーク (@) | RADIUS 認証でログインした |

[ノート]

NVR510 は Rev.15.01.03 以降でアットマークの表示が可能。

[適用モデル]

NVR700W, NVR510

## 55.44 ログインしたユーザーのログイン履歴の表示

[書式]

**show status user history**

[説明]

ルーターにログインしたユーザーのログイン履歴を最大で 50 件まで表示する。以下の項目が表示される。

- ユーザー名
- 接続種別
- ログインした日時
- アイドル時間
- 接続相手の IP アドレス

[適用モデル]

NVR700W, NVR510

## 55.45 パケットバッファの状態の表示

[書式]

**show status packet-buffer [group]**

[設定値及び初期値]

- *group*: 表示するパケットバッファのグループを指定する
  - [設定値]:

| 設定値                                  | 説明               |
|--------------------------------------|------------------|
| グループ名 ( small, middle, large, huge ) | 指定したグループの状態を表示する |
| 省略                                   | すべてのグループの状態を表示する |

- [初期値]: -

[説明]

パケットバッファの状態を表示する。表示する項目は以下の通り:

- グループ名
- 格納できるパケットサイズ
- 管理パラメーター
- 現在、割り当て中のパケットバッファ数
- 現在、フリーリストにつながれているパケットバッファ数
- 現在、確保しているチャンク数
- パケットバッファの割り当て要求を受けた回数
- パケットバッファの割り当てに成功した回数
- パケットバッファの割り当てに失敗した回数
- パケットバッファが解放された回数
- チャンクを確保した回数
- チャンクを確保しようとして失敗した回数
- チャンクを解放した回数



[表示例]

```
# show status packet-buffer large
large group: 2048 bytes length
  parameters: max-buffer=10000 max-free=2812 min-free=62
              buffer-in-chunk=625 init-chunk=4
1476 buffers in free list
1024 buffers are allocated, req/succ/fail/rel = 1024/1024/0/0
4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

[適用モデル]

NVR700W, NVR510

## 55.46 QoS ステータスの表示

[書式]

**show status qos info** [*interface* [*class*]]

[設定値及び初期値]

- *info*: 表示する情報の種類
- [設定値]:

| 設定値       | 説明                   |
|-----------|----------------------|
| bandwidth | 使用帯域                 |
| length    | キューイングしているパケット数      |
| all       | 使用帯域とキューイングしているパケット数 |

- [初期値]: -
- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *class*
  - [設定値]: クラス (1..16)
  - [初期値]: -

[説明]

インターフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。

- インターフェース名
- キューイングアルゴリズム
- インターフェース速度
- クラス数
- 各クラスの設定帯域、使用帯域、使用帯域のピーク値と記録日時
- 設定帯域の合計
- 各クラスのエンキュー成功回数/失敗回数、デキュー回数、保持しているパケット数、パケット数のピーク値と記録日時

[適用モデル]

NVR700W, NVR510

## 55.47 連携動作の状態の表示

[書式]

**show status cooperation type** [*id*]

[設定値及び初期値]

- *type*: 連携動作タイプ
- [設定値]:

| 設定値                 | 説明     |
|---------------------|--------|
| bandwidth-measuring | 回線帯域検出 |

| 設定値        | 説明     |
|------------|--------|
| load-watch | 負荷監視通知 |

- [初期値]: -
- *id*
  - [設定値]: 相手先 ID 番号 (1-100)
  - [初期値]: -

**[説明]**

連携動作の情報を表示する。

回線帯域検出の場合、以下の項目が表示される。

- 相手先情報
- 状態表示
  - 回数
  - 測定時刻
  - 測定結果 (クライアント動作のみ)
  - 現状 (クライアント動作のみ)
  - 設定変更履歴 (クライアント動作のみ)
  - 次の測定までの残り時間 (クライアント動作のみ)

負荷監視通知の場合、以下の項目が表示される。

- 相手先情報
- 状態表示
  - 抑制要請回数
  - 抑制解除回数
  - 履歴

**[適用モデル]**

NVR700W

## 55.48 OSPFv3 情報の表示

---

**[書式]**

```
show ipv6 ospf info
```

**[設定値及び初期値]**

- *info*
  - [設定値]:

| 設定値          | 説明             |
|--------------|----------------|
| database     | OSPFv3 のデータベース |
| neighbor     | 近隣ルーター         |
| interface    | 各インターフェースの状態   |
| virtual-link | 仮想リンクの状態       |

- [初期値]: -

**[説明]**

OSPFv3 の状態を表示する。

**[適用モデル]**

NVR700W

## 55.49 URL フィルターの情報の表示

---

**[書式]**

```
show url filter
```

```
show url filter interface
```

```
show url filter pp [peer_num]
```

**show url filter tunnel** [*tunnel\_num*]

#### [設定値及び初期値]

- *interface*
  - [設定値]: LAN インターフェース名、ONU インターフェース名、WAN インターフェース名
  - [初期値]: -
- *peer\_num*
  - [設定値]: 相手先情報番号
  - [初期値]: -
- *tunnel\_num*
  - [設定値]: トンネルインターフェース番号
  - [初期値]: -

#### [説明]

インターフェースに適用されている URL フィルターの中で、どのフィルターに何回マッチしたかの統計情報を表示する。

インターフェースが指定されない場合は、すべてのインターフェースの情報を表示する。

表示される内容は以下の通り。

- フィルター番号
- 始点 IP アドレス
- HTTP コネクションとフィルターが一致した回数

#### [ノート]

**url filter** コマンドで、キーワード、IP アドレスの両方に "\*" を設定したフィルターがインターフェースに適用されている場合、HTTP コネクションがこのフィルターとマッチした回数は表示されない。

#### [適用モデル]

NVR700W

## 55.50 生存通知の状態の表示

---

#### [書式]

**show status heartbeat**

#### [説明]

受信した生存通知の情報を表示する。

表示する内容は以下の通り。

- 通知された名前
- 通知された IP アドレス
- 最後に生存通知を受信した時刻
- 受信間隔 ( 秒 )

#### [適用モデル]

NVR700W

## 55.51 生存通知の状態の表示

---

#### [書式]

**show status heartbeat2**

**show status heartbeat2 id** *recv\_id*

**show status heartbeat2 name** *string*

#### [設定値及び初期値]

- *recv\_id*
  - [設定値]: 受信設定の識別子

- [初期値]: -
- *string*
  - [設定値]: 文字列 (1~64 文字/ASCII、1~32 文字/シフト JIS)
  - [初期値]: -

**[説明]**

受信した生存通知の情報を表示する。

第 1 書式では保持している全ての情報を表示する。

第 2 書式では指定の受信設定により受信した情報のみ表示する。

第 3 書式では指定の文字列が通知名称に含まれる情報のみ表示する。

*string* には ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 (半角カタカナを除く) も使用できる。ただし、**console character** コマンドの設定が *sjis* の場合にのみ正しく動作し、他の設定では誤動作する可能性がある。

**[適用モデル]**

NVR700W

## 55.52 リモートセットアップ機能に関する接続情報の表示

---

**[書式]**

**show status remote setup**

**[説明]**

リモートセットアップ機能に関する接続情報を表示する。

現在の通信状態や通信時に発生したエラーの累計、送受信した総フレーム数、発着信の回数、最新の接続情報などを表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.53 技術情報の表示

---

**[書式]**

**show techinfo**

**[説明]**

技術サポートに必要な情報を一度に出力する。

他の **show** コマンドとは異なり、**show techinfo** コマンドの出力は **console columns/lines** コマンドの設定を無視して一度に出力される。一画面ごとに出力が停止するページ動作は行わない。そのため、ターミナルソフトのログ機能を用いて、出力を PC のファイルとして保存することが望ましい。

また、**console character** コマンドの設定も無視され、常に英語モードで出力される。

一画面ごとに内容を確認しながら出力したいときには、以下のように **less** コマンドを併用するとよい。ただし、**less** コマンドは画面制御シーケンスを多数出力するため、ログを記録しながら **less** コマンドを使用すると、ログファイルがわかりにくくなる。

**show techinfo | less**

**[ノート]**

ルーターに対して PC で動作する TFTP クライアントからアクセスし、ファイル名 'techinfo' を GET すると、**show techinfo** コマンドの出力と同じものが得られる。

Windows の TFTP.EXE を使用した例:

```
C:\>tftp 192.168.0.1 get techinfo techinfo.txt
```

**[適用モデル]**

NVR700W, NVR510

## 55.54 USB ホスト機能の動作状態を表示

### [書式]

```
show status usbhost
show status usbhost modem
```

### [説明]

USB ホスト機能の動作状態を表示する。

modem を指定した場合、USB ポートに接続した機器に関する接続情報を表示する。現在の通信状態や通信時に発生したエラーの累計、送受信した総 byte 数、発着信の回数、最新の接続情報などを表示する。

### [適用モデル]

NVR700W, NVR510

## 55.55 microSD スロットの動作状態を表示

### [書式]

```
show status sd
```

### [説明]

microSD スロットの動作状態を表示する。

### [適用モデル]

NVR700W, NVR510

## 55.56 内蔵無線 WAN モジュールの動作状態を表示

### [書式]

```
show status wwan-module [info...] [detail]
```

### [設定値及び初期値]

- *info*
  - [設定値]:

| 設定値         | 説明                           |
|-------------|------------------------------|
| module-info | 内蔵無線 WAN モジュールの内部情報を表示する     |
| radio-info  | 内蔵無線 WAN モジュールのネットワーク状態を表示する |
| pdp-info    | 内蔵無線 WAN モジュールの接続情報を表示する     |

- [初期値]: -
- *detail*
  - [設定値]:

| 設定値    | 説明                               |
|--------|----------------------------------|
| detail | 内蔵無線 WAN モジュールの動作状態を詳細情報も含めて表示する |

- [初期値]: -

### [説明]

内蔵無線 WAN モジュールの動作状態を表示する。

*info* を省略した場合は、全ての情報を表示する。

### [ノート]

detail は Rev.15.00.03 以降のファームウェアで使用可能。

### [適用モデル]

NVR700W

## 55.57 外部メモリの動作状態を表示

---

### [書式]

```
show status external-memory
```

### [説明]

外部ストレージの動作状態を表示する。

- USB / microSD ホストコントローラの状態
- USB / microSD バスへの給電状態
- 接続中の USB / microSD デバイス ( デバイス名 / ベンダー名 / 最大転送速度 / 記憶容量 )
- SYSLOG 設定

### [ノート]

USB ポートに携帯端末が接続されている場合は、「外部メモリが接続されていません」と表示される。携帯端末の状態は **show status usbhost modem** で確認する。

### [適用モデル]

NVR700W, NVR510

## 55.58 RTFS の状態の表示

---

### [書式]

```
show status rtfs
```

### [説明]

内蔵フラッシュ ROM の RTFS 領域の状態を表示する。表示する内容は次の通り。

- 容量
- 空き容量
- 作成可能エントリ数
- ファイル数
- ディレクトリ数

実行例は以下の通り。

```
# show status rtfs
容量                : 3145728 バイト
空き容量           : 3145728 バイト
作成可能エントリ数: 1000
ファイル数         : 0
ディレクトリ数     : 0
#
```

### [適用モデル]

NVR700W, NVR510

## 55.59 ルーターへのサインイン状態の表示

---

### [書式]

```
show status sip presence
```

### [説明]

メッセージャーなど SIP ユーザーのルーターへのサインイン状態を表示する。

### [適用モデル]

NVR700W, NVR510

## 55.60 SIP サーバーとの接続状態の表示

---

### [書式]

```
show status sip server [server_num]
```

**[設定値及び初期値]**

- *server\_num*
  - [設定値]: SIP サーバーの登録番号(1..65535)
  - [初期値]:-

**[説明]**

SIP サーバーとの接続状態を表示する。

|       |      |             |
|-------|------|-------------|
| 接続状態  | 未接続  | 接続されていません   |
|       | 通信中  | 接続されています    |
|       | 接続中  | 接続しようとしています |
|       | 切断中  | 切断しようとしています |
| 切断コード | 0    | エラー無し       |
|       | 3018 | サーバーレスポンス無し |
|       | 3004 | サーバーの名前解決失敗 |
|       | 3002 | 経路不明        |
|       | 3000 | 認証失敗        |
|       | 3200 | その他のエラー     |

**[適用モデル]**

NVR700W, NVR510

## 55.61 アナログ関係の状態の表示

**[書式]**

**show status analog** [*port*]

**[設定値及び初期値]**

- *port*
  - [設定値]:

| 設定値 | 説明                    |
|-----|-----------------------|
| 1   | TEL1 ポート              |
| 2   | TEL2 ポート              |
| 省略  | 省略時はすべての TEL ポートを表示する |

- [初期値]:-

**[説明]**

アナログ関係の状態を表示する。

**[適用モデル]**

NVR700W, NVR510

## 55.62 カスケード接続の状態表示

**[書式]**

**show status analog extension**

**[説明]**

カスケード接続に関する状態の表示を行う。

以下の内容を表示

- カスケード接続のモード(全モード)
- IP アドレス取得インターフェース(親機または子機)
- 子機情報および子機受け入れモード(親機)

- 親機との接続情報(子機)

[適用モデル]

NVR700W, NVR510

## 55.63 起動情報を表示する

---

[書式]

**show status boot** [*num*]

[設定値及び初期値]

- num* : 履歴番号
  - [設定値]:

| 設定値  | 説明             |
|------|----------------|
| 0..4 | 指定した番号の履歴を表示する |
| 省略   | 省略時は 0         |

- [初期値]:-

[説明]

起動の情報を表示する。

**show status boot list** コマンドで表示される履歴番号を指定すると、その履歴の詳細が表示される。  
*num* を省略した場合は、履歴番号=0 の履歴が表示される。

[適用モデル]

NVR700W, NVR510

## 55.64 起動情報の履歴の詳細を表示する

---

[書式]

**show status boot all**

[説明]

起動情報の履歴の詳細を最大で 5 件まで表示する。

**cold start** コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

NVR700W, NVR510

## 55.65 起動情報の履歴の一覧を表示する

---

[書式]

**show status boot list**

[説明]

起動情報の履歴を最大で 5 件まで表示する。

**cold start** コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

NVR700W, NVR510

## 55.66 エージェント一覧の表示

---

[書式]

**show status switch control** [*interface*]

[設定値及び初期値]

- interface*



- [設定値]: LAN インターフェース名、ブリッジインターフェース名
- [初期値]: -

### [説明]

エージェントの一覧を表示する。*interface* を省略した場合は、すべてのインターフェースについて情報を表示する。

L2MS の動作状態に応じて、以下の情報を表示する。

- L2MS のマネージャーとして動作している場合
  - MAC アドレス
  - 機種名
  - 機器名
  - マネージャーからの経路
  - アップリンクポート
  - エージェントを操作するときに指定する経路
  - 現在使用している設定内容
- L2MS のエージェントとして動作している場合
  - マネージャーの MAC アドレス

### [ノート]

ブリッジインターフェースを指定できるのは、NVR700W Rev.15.00.10 以降のファームウェアである。

### [表示例]

```
> show status switch control
LAN1
[00:a0:de:01:02:03]
機種名      : SWX2200-24G
機器名      : SWX2200-24G_0123456
経路        : lan1:1
アップリンク : 1
設定用経路  : lan1:1
設定        : switch select lan1:1
---
LAN2
スイッチ制御機能が有効になっていません
---
BRIDGE1
スイッチ制御機能が有効になっていません

> show status switch control
LAN1
[00:a0:de:01:02:03]
Model name   : SWX2200-24G
System name  : SWX2200-24G_0123456
Route        : lan1:1
Uplink       : 1
Route for Config: lan1:1
Config       : switch select lan1:1
---
LAN2
Switch control function is not available.
---
BRIDGE1
Switch control function is not available.

> show status switch control
LAN1
マネージャー: 00:a0:de:01:02:03
---
LAN2
スイッチ制御機能が有効になっていません
---
BRIDGE1
スイッチ制御機能が有効になっていません

> show status switch control
```

```

LAN1
Manager: 00:a0:de:01:02:03
----
LAN2
Switch control function is not available.
----
BRIDGE1
Switch control function is not available.

```

**[適用モデル]**  
NVR700W, NVR510

## 55.67 LAN ケーブル二重化機能の動作状態を表示

### [書式]

**show status switch control route backup route**

### [設定値及び初期値]

- *route*
  - [設定値]: 経路
  - [初期値]: -

### [説明]

LAN ケーブル二重化機能の動作状態を表示する。

| 状態             | 説明                          |
|----------------|-----------------------------|
| none           | LAN ケーブル二重化機能が動作していない       |
| active         | 通信が可能な経路として動作している           |
| force-linkdown | LAN ケーブル二重化機能によってリンクダウンしている |
| blocking       | LAN ケーブル二重化機能によって通信が遮断されている |

### [ノート]

メイン経路がリンクアップしている場合、メイン経路は **active** で動作し、通信可能である。また、バックアップ経路は **force-linkdown** で動作し、ケーブルが接続されてもリンクアップしない。

メイン経路がリンクダウンしている場合、バックアップ経路は **active** で動作し、通信可能である。また、メイン経路は **blocking** で動作し、リンクアップした場合にループが発生しないよう、通信が遮断される。

スイッチに本機能が実装されていない場合はコマンドエラーとなる。

**[適用モデル]**  
NVR700W, NVR510

## 55.68 DNS キャッシュの表示

### [書式]

**show dns cache**

### [説明]

DNS キャッシュの内容を表示する。

**[適用モデル]**  
NVR700W, NVR510

## 55.69 ライセンス情報の表示

### [書式]

**show status license**

### [説明]

LMS クライアントが取得したライセンス情報を表示する。表示する項目は以下の通り。

|    |             |
|----|-------------|
| 品番 | ライセンス製品の品番。 |
|----|-------------|

|      |                          |
|------|--------------------------|
| 状態   | ライセンスの状態。                |
| 有効期限 | ライセンスの有効期限。"年/月/日"形式で示す。 |

ライセンスの状態には以下の種類がある。

|                                      |                                                                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 有効 (Active)                          | ライセンスが有効期限内であり、当該品番に対応するアプリケーションを使用できる状態。                                                                                                                                                                                          |
| 更新猶予期間 (Renew grace period)          | 有効期限を過ぎている状態。この状態より一定期間経過すると対応するアプリケーションを使用できなくなるため、ライセンスの購入手続きが必要となる。                                                                                                                                                             |
| 認証猶予期間 (Authentication grace period) | 一時的にライセンス認証が猶予されている状態。ヤマハネットワーク機器が有効なライセンス情報を保持している状態で再起動し、その後 LMS サーバーと通信できない場合にこの状態となる。対応するアプリケーションを使用することはできるが、ディアクティベートまでの時間が経過するまでにライセンス認証を行う必要がある。ディアクティベートまでの時間は <b>show status license authentication</b> コマンドで確認することができる。 |

#### [ノート]

ライセンスを保持していない場合、あるいは LMS サーバーからライセンス情報を取得していない場合、当コマンドを実行しても情報は表示されない。

NVR700W は Rev.15.00.17 以降で使用可能。

#### [適用モデル]

NVR700W

## 55.70 ライセンス認証の状態の表示

#### [書式]

**show status license authentication**

#### [説明]

ライセンス認証の状態を表示する。表示する項目は以下の通り。

|                                               |                                                                              |
|-----------------------------------------------|------------------------------------------------------------------------------|
| 最終更新日時 (Last updated)                         | 最後にライセンス認証に成功した日時。"年/月/日 時:分:秒"形式で示す。                                        |
| ディアクティベートまでの定期認証回数 (Counts to deactivation)   | アプリケーションがディアクティベートされるまでの残り定期認証回数。                                            |
| 次の定期認証までの時間 (Time to periodic authentication) | 次の定期認証までの時間。"時:分:秒"形式で示す。                                                    |
| ディアクティベートまでの時間 (Time to deactivation)         | ディアクティベートされるまでの時間。"時:分:秒"形式で示す。この時間内はアプリケーションを使用できるが、経過するまでにライセンス認証を行う必要がある。 |

#### [ノート]

NVR700W は Rev.15.00.17 以降で使用可能。

#### [適用モデル]

NVR700W

## 55.71 STATUS LED の情報の表示

#### [書式]

**show status status-led [history]**

#### [設定値及び初期値]

- history : STATUS LED の状態変化の履歴を表示
  - [初期値] :-

**[説明]**

STATUS LED の情報を表示する。

点灯していた場合は、点灯の原因となったキープアライブが設定されているインターフェースの一覧が表示される。  
history オプションを指定した場合は状態変化の履歴も表示される。

**[適用モデル]**

NVR700W, NVR510

**55.72 LAN マップの状態を表示する****[書式]**

```
show lan-map interface [detail]
```

**[設定値及び初期値]**

- *interface*
  - [設定値]: LAN インターフェース名、ブリッジインターフェース名
  - [初期値]: -
- *detail*: LAN マップで管理しているエージェントの情報に加えて、端末情報の詳細を表示する
  - [初期値]: -

**[説明]**

現在の LAN マップの状態を表示する。

- ファームウェアに取り込んでいる OUI の情報 (*detail* オプションを指定したときのみ)
- マネージャーの情報
  - リンクアップポート
  - マネージャー直下の端末情報
- エージェントの情報
  - 機種名
  - 機器名
  - 経路
  - リンクアップポート
    - アップリンクポート
    - ダウンリンクポート
  - エージェントの状態

| 状態     | 説明       |
|--------|----------|
| Idle   | 通常状態     |
| Search | 検索要求を実行中 |

- 検出時刻
- 直近の検索要求が完了するまでに費やした時間
- エージェント配下の端末情報
- 消失したエージェントの情報
  - 機種名
  - 機器名
  - 検出時刻
  - 消失時刻
  - エージェント配下の端末情報
- 端末情報の詳細 (*detail* オプションを指定したときのみ)
  - IP アドレス
  - 検出時刻
  - 消失時刻
  - 種類
  - メーカー名
  - 機種名

- 機器名
- OS
- コメント
- スナップショット機能で警告の対象とするか否か

### [ノート]

**switch control mode** コマンドで *mode* に **manager** が設定されている場合、本コマンドを使用できる。  
ブリッジインターフェースを指定できるのは、NVR700W Rev.15.00.10 以降のファームウェアである。

### [表示例]

```
# show lan-map lan1 detail
[OUI]
Generated           : Sat, 04 Mar 2017 04:31:14 -0400

[マネージャー]
リンクアップ       : lan1:1
端末数             : 0

[エージェント]
[00:a0:de:2a:dc:02]
機種名             : SWX2200-24G
機器名             : SWX1
経路               : lan1:1
リンクアップ       : 1 11
  アップリンク     : 1
  ダウンリンク     : なし
状態               : Idle
検出時刻           : 2017/05/24 11:28:59
検索時間           : 1 sec (867 msec)
端末数             : 1
  [ポート 1]
  [ポート 2]
  [ポート 3]
  [ポート 4]
  [ポート 5]
  [ポート 6]
  [ポート 7]
  [ポート 8]
  [ポート 9]
  [ポート 10]
  [ポート 11]
    [12:34:56:78:90:ab]
    IP アドレス     : 192.168.0.10
    検出時刻       : 2017/05/24 11:29:04
    種類           : Desktop PC
    メーカー       : Maker1
    機種名         : Model1
    機器名         : Host1
    OS             : OS1
    コメント       : comment1
    スナップショット : on
  [ポート 12]
  [ポート 13]
  [ポート 14]
  [ポート 15]
  [ポート 16]
  [ポート 17]
  [ポート 18]
  [ポート 19]
  [ポート 20]
  [ポート 21]
  [ポート 22]
  [ポート 23]
  [ポート 24]
```

```
[消失エージェント]  
[00:a0:de:7e:53:82]  
機種名          : SWX2200-24G  
機器名          : SWX2  
検出時刻        : 2017/05/24 11:29:32  
消失時刻        : 2017/05/24 12:18:50  
端末数          : 0
```

[適用モデル]  
NVR700W, NVR510

## 55.73 コピーライトの表示

---

### [書式]

**show copyright** [*detail*]

### [設定値及び初期値]

- *detail*
  - [設定値]: 条文を含めたソフトウェアの著作権情報を表示する
  - [初期値]: -

### [説明]

ソフトウェアの著作権情報を表示する。  
detail を指定することで、条文を含めたソフトウェアの著作権情報を表示することができる。

[適用モデル]  
NVR700W, NVR510

## 55.74 音声通話の接続状態の表示

---

### [書式]

**show status voice call**

### [説明]

すべての音声通話の接続状態を表示する。

[適用モデル]  
NVR700W, NVR510

## 55.75 小型 ONU の状態の表示

---

### [書式]

**show onu-module info** [*interface*]

### [設定値及び初期値]

- *interface*
  - [設定値]: ONU インターフェース名
  - [初期値]: -

### [説明]

ONU インターフェースに接続された小型 ONU の情報を表示する。  
インターフェースを指定しない場合には、すべての ONU インターフェースに接続された小型 ONU の情報を表示する。

### [ノート]

ONU インターフェース名は、NVR700W Rev.15.00.07 以降、NVR510 Rev.15.01.06 以降のファームウェアで指定することができる。

[適用モデル]  
NVR700W, NVR510

## 第 56 章

### ログイン

#### 56.1 ログの表示

##### [書式]

**show log** [saved] [reverse]

**show log** external-memory [backup [*fileid*]]

**less log** [saved] [reverse]

##### [設定値及び初期値]

- saved
  - [設定値]: リブート直前のログを表示する
  - [初期値]: -
- reverse
  - [設定値]: ログを逆順に表示する
  - [初期値]: -
- external-memory
  - [設定値]: **external-memory syslog filename** コマンドで設定しているファイルの中身を表示する
  - [初期値]: -
- backup
  - [設定値]: SYSLOG バックアップファイルの中身を表示する、もしくは、SYSLOG バックアップファイルの一覧を表示する
  - [初期値]: -
- *fileid*: ファイルの中身を表示させたい SYSLOG バックアップファイルのファイル名に付加されている日時データを指定する
  - [設定値]: `yyyymmdd_hhmmss`
  - [初期値]: -

##### [説明]

ルーターの動作状況を記録したログを表示する。

ログを最大 10,000 件保持することができる。最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**syslog host** コマンドでログを SYSLOG サーバーに転送して、そちらで保存する必要がある。

意図しないリブートが発生したときは、'saved' を指定することでリブート直前のログを表示することができる。

このコマンドでは、通常は発生時刻の古いものからログを順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

**external-memory** を指定した場合は、外部メモリ内のログファイルを表示する。

**external-memory backup** を指定した場合は、SYSLOG バックアップファイルの一覧を古いものから順に表示する。バックアップファイルの中身は、表示されたファイル名の日時データ (`yyyymmdd_hhmmss` 形式で表される文字列の 15 桁) を *fileid* に指定すると表示させることができる。

##### [ノート]

**clear log** コマンドを実行するとログは消去される。

**external-memory** を指定した場合は以下の制限がある。

- 外部メモリ内の暗号化したログファイルは表示できない
- リダイレクトを指定できない

**external-memory** を指定して、**external-memory syslog filename** コマンドが設定されていない場合は実行エラーとなる。

##### [適用モデル]

NVR700W, NVR510



## 56.2 アカウントの表示

### [書式]

**show account**

### [説明]

すべてのアカウントの発着信回数を表示する。

### [適用モデル]

NVR700W, NVR510

## 56.3 PP アカウントの表示

### [書式]

**show account pp** [*peer\_num*]

### [設定値及び初期値]

#### • *peer\_num*

- [設定値]:

| 設定値       | 説明                 |
|-----------|--------------------|
| 番号        | 相手先情報番号            |
| anonymous | anonymous インターフェース |
| 省略        | 省略時は現在選択している相手先    |

- [初期値]: -

### [説明]

指定した PP インターフェースに関するアカウントを表示する。

### [適用モデル]

NVR700W, NVR510

## 56.4 アナログ関係のアカウントの表示

### [書式]

**show account analog** [*port*]

**show account analog** extension

### [設定値及び初期値]

#### • *port*

- [設定値]:

| 設定値 | 説明                   |
|-----|----------------------|
| 1   | TEL1 ポート             |
| 2   | TEL2 ポート             |
| 省略  | 省略時は TEL ポートの合計を表示する |

- [初期値]: -

#### • extension

- [設定値]: カスケード接続を示すキーワード
- [初期値]: -

### [説明]

TEL ポートの発着信回数を表示する。

### [適用モデル]

NVR700W, NVR510

## 56.5 SIP のアカウントの表示

---

### [書式]

**show account sip**

### [説明]

SIP の発着信回数を表示する。

### [適用モデル]

NVR700W, NVR510

## 56.6 ひかり電話のアカウントの表示

---

### [書式]

**show account ngn tel**

### [説明]

ひかり電話の発着信回数を表示する。

### [適用モデル]

NVR700W, NVR510

## 56.7 データコネクタのアカウントの表示

---

### [書式]

**show account ngn data**

### [説明]

データコネクタの発着信回数や課金情報を表示する。

### [ノート]

課金情報は接続時間と設定した帯域幅から計算しているため、最終的に請求される料金とは異なる場合がある。

### [適用モデル]

NVR700W, NVR510

## 56.8 モバイル回線のアカウントの表示

---

### [書式]

**show account mobile**

### [説明]

モバイル回線の発着信回数を表示する。

### [適用モデル]

NVR700W, NVR510

## 56.9 内蔵無線 WAN のアカウントの表示

---

### [書式]

**show account wwan [num]**

### [設定値及び初期値]

#### • num

- [設定値]:

| 設定値  | 説明                  |
|------|---------------------|
| 1~30 | 内蔵無線 WAN インターフェース番号 |
| 省略   | 省略時は現在選択している番号      |

- [初期値]: -

**[説明]**

内蔵無線 WAN の発着信回数を表示する。

**[適用モデル]**

NVR700W

## 56.10 通信履歴の表示

---

**[書式]**

```
show history [reverse]
```

**[設定値及び初期値]**

- *reverse*
  - [設定値]: 履歴を逆順に表示する
  - [初期値]: -

**[説明]**

通信履歴を最大 100 件分表示する。履歴が最大数を越えた場合には、発生時刻の古いものから消去されていく。このコマンドでは、通常は時刻の古いものから順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

**[適用モデル]**

NVR700W, NVR510

## 56.11 コマンド履歴の表示

---

**[書式]**

```
show command history [num]
```

**[設定値及び初期値]**

- *num*
  - [設定値]: ヒストリー番号 (1..21474836)
  - [初期値]: -

**[説明]**

コマンド履歴を表示する。

*num* を指定した場合は、指定した番号のコマンドから直前のコマンドまで表示する。*num* を省略した場合には、新しいものからさかのぼって最大 20 個のコマンドを表示する。

**[ノート]**

NVR700W Rev.15.00.14 以降、および NVR510 Rev.15.01.13 以降で指定可能。

**[適用モデル]**

NVR700W, NVR510

# 索引

## 記号

> 36  
>> 36

## A

administrator 667  
 administrator password 39  
 administrator password encrypted 39  
 administrator radius auth 41  
 alarm batch 88  
 alarm connection analog 86  
 alarm connection data 86  
 alarm entire 86  
 alarm http revision-up 89  
 alarm intrusion 87  
 alarm lua 581  
 alarm sd 88  
 alarm startup 89  
 alarm usbhost 87  
 alarm wwan 88  
 alias 48  
 analog arrive another-device permit 422  
 analog arrive global permit 419  
 analog arrive ignore-subaddress permit 421  
 analog arrive incoming-signal 437  
 analog arrive incoming-signal timing pb 438  
 analog arrive innumber-port 436  
 analog arrive number display 424  
 analog arrive priority 424  
 analog arrive restrict 419  
 analog arrive restrict list 420  
 analog arrive ring-while-talking permit 422  
 analog arrive ringer-type list 423  
 analog arrive without-calling-number 439  
 analog arrive without-subaddress permit 421  
 analog call route 474  
 analog call route-table 473  
 analog device type 416  
 analog disc-signal 434  
 analog end-of-dialing-code 418  
 analog extension address refer 443  
 analog extension agent permit 445  
 analog extension dial prefix 469  
 analog extension emergency-call-dial type 436  
 analog extension incoming ringer 435  
 analog extension log 446  
 analog extension machine-id 446  
 analog extension manager 444  
 analog extension master 444  
 analog extension mode 443  
 analog extension other-dial-tone 435  
 analog extension sip address 451  
 analog extension slave permit 445  
 analog hooking inhibit timer 426  
 analog hooking timer 425  
 analog hooking wait timer 426  
 analog impedance 428  
 analog local address 416  
 analog local address notice 417  
 analog loop-closure threshold 427  
 analog mp prior 434  
 analog off-hook call 442  
 analog off-hook mask 427  
 analog pad receive 433  
 analog pad rtp receive 439  
 analog pad rtp send 440

analog pad send 432  
 analog pause timer 441  
 analog power 441  
 analog rapid call 418  
 analog re-ringing-timer 429  
 analog sip arrive incoming-signal 468  
 analog sip arrive myaddress 468  
 analog sip arrive permit 467  
 analog sip arrive restrict 471  
 analog sip arrive restrict list 472  
 analog sip arrive without-calling-number 473  
 analog sip call display name 467  
 analog sip call myname 466  
 analog sip call permit 465  
 analog supplementary-service 429  
 analog supplementary-service call-deflection address 430  
 analog supplementary-service call-deflection reject 432  
 analog supplementary-service call-deflection ringer 430  
 analog supplementary-service call-deflection talkie 431  
 analog use 415  
 analog wait dial timer 425  
 ap config directory 652  
 ap config filename 652  
 ap control config delete 653  
 ap control config get 652  
 ap control config set 653  
 ap control config-auto-set use 654  
 ap control firmware update go 654  
 ap control http proxy timeout 655  
 ap control http proxy use 655  
 ap select 651  
 audio echo-canceller 89  
 audio echo-canceller disabler 91  
 audio echo-canceller nlp threshold 91  
 audio hold-tone type 428  
 audio jitter-buffer 92  
 audio rtp port 93  
 audio rtp segsize 93  
 auth user 237  
 auth user attribute 238  
 auth user group 239  
 auth user group attribute 239

## B

bgp aggregate 360  
 bgp aggregate filter 360  
 bgp autonomous-system 361  
 bgp configure refresh 365  
 bgp default med 368  
 bgp export 362  
 bgp export aspath 362  
 bgp export filter 363  
 bgp export route selection rule 369  
 bgp import 364  
 bgp import filter 365  
 bgp log 367  
 bgp neighbor 366  
 bgp preference 362  
 bgp reric interval 368  
 bgp router id 361  
 bgp use 360  
 bridge learning 576  
 bridge learning bridge\_interface static 577  
 bridge learning bridge\_interface timer 576  
 bridge member 575

## C

call 693  
 change wwan pin-code 546  
 clear account 672  
 clear account analog 673  
 clear account mobile 672  
 clear account ngn data 672  
 clear account ngn tel 672  
 clear account pp 672  
 clear account pstm 672  
 clear account sip 672  
 clear account wwan 672  
 clear arp 674  
 clear boot list 677  
 clear bridge learning 674  
 clear diagnosis config port 586  
 clear dns cache 674  
 clear dpi cache 597  
 clear dpi statistics 596  
 clear external-memory syslog 677  
 clear heartbeat 516  
 clear heartbeat2 id 516  
 clear heartbeat2 name 516  
 clear ip dynamic routing 674  
 clear ipv6 dynamic routing 677  
 clear ipv6 neighbor cache 677  
 clear log 674  
 clear mobile access limitation 553  
 clear mobile access limitation pp 553  
 clear nat descriptor dynamic 675  
 clear nat descriptor interface dynamic 676  
 clear nat descriptor interface dynamic pp 676  
 clear nat descriptor interface dynamic tunnel 676  
 clear nat descriptor masquerade session statistics 676  
 clear pppoe pass-through learning 676  
 clear status 675  
 clear status pp 675  
 clear status tunnel 675  
 clear status wwan 675  
 clear switching-hub macaddress 688  
 clear url filter 689  
 clear url filter pp 689  
 clear url filter tunnel 689  
 clear wwan access limitation 547  
 cloud vpn bind 276  
 cloud vpn name 276  
 cloud vpn option 277  
 cloud vpn parameter 275  
 cloud vpn service 275  
 cloud vpn set go 277  
 cloud vpn syslog 278  
 cold start 672  
 confirm 693  
 connect 682  
 connect pp 682  
 connect tunnel 682  
 console character 54  
 console columns 54  
 console info 55  
 console lines 55  
 console prompt 53  
 cooperation 339  
 cooperation bandwidth-measuring remote 340  
 cooperation load-watch control 344  
 cooperation load-watch remote 341  
 cooperation load-watch trigger 343  
 cooperation port 339  
 cooperation type go 345  
 copy 678  
 copy config 668  
 copy exec 669

## D

dashboard accumulate 665  
 date 51  
 delete 678  
 delete config 670  
 delete exec 671  
 description 70  
 description yno 658  
 dhcp client client-identifier 194  
 dhcp client client-identifier pool 194  
 dhcp client client-identifier pp 194  
 dhcp client hostname 193  
 dhcp client hostname pool 193  
 dhcp client hostname pp 193  
 dhcp client option 195  
 dhcp client option pool 195  
 dhcp client option pp 195  
 dhcp client release linkdown 196  
 dhcp convert lease to bind 188  
 dhcp duplicate check 183  
 dhcp manual lease 190  
 dhcp manual release 190  
 dhcp relay select 191  
 dhcp relay server 191  
 dhcp relay srcport 191  
 dhcp relay threshold 192  
 dhcp scope 184  
 dhcp scope bind 185  
 dhcp scope lease type 187  
 dhcp scope option 189  
 dhcp server rfc2131 compliant 182  
 dhcp service 181  
 diagnose config port access 585  
 diagnose config port map 584  
 diagnosis config port history-num 586  
 diagnosis config port max-detect 585  
 disable wwan pin-auth 546  
 disconnect 682  
 disconnect ip connection 686  
 disconnect ipv6 connection 686  
 disconnect pp 682  
 disconnect tunnel 682  
 disconnect user 44  
 dns cache max entry 326  
 dns cache use 325  
 dns domain 316  
 dns host 324  
 dns notice order 318  
 dns private address spoof 319  
 dns private name 314  
 dns server 315  
 dns server dhcp 317  
 dns server pdp 318  
 dns server pp 316  
 dns server select 320  
 dns service 314  
 dns service aaaa filter 319  
 dns service fallback 326  
 dns srcport 324  
 dns static 323  
 dns syslog resolv 320  
 dpi group set 592  
 dpi log 594  
 dpi signature download go 593  
 dpi signature download url 594  
 dpi use 588

## E

echo 694  
 embedded file 50

enable wwan pin-auth 546  
 ethernet filter 154  
 ethernet interface filter 156  
 execute at-command 553  
 execute batch 530  
 exit 667  
 external-memory accelerator cache size 522  
 external-memory auto-search time 530  
 external-memory batch filename 530  
 external-memory boot permit 526  
 external-memory boot timeout 527  
 external-memory cache mode 521  
 external-memory config filename 528  
 external-memory dpi signature directory 533  
 external-memory exec filename 527  
 external-memory performance-test go 531  
 external-memory statistics filename prefix 523  
 external-memory syslog filename 525

## G

grep 34

## H

heartbeat pre-shared-key 510  
 heartbeat receive 510  
 heartbeat send 511  
 heartbeat2 myname 512  
 heartbeat2 receive 514  
 heartbeat2 receive enable 515  
 heartbeat2 receive log 516  
 heartbeat2 receive monitor 515  
 heartbeat2 receive record limit 516  
 heartbeat2 transmit 512  
 heartbeat2 transmit enable 513  
 heartbeat2 transmit interval 513  
 heartbeat2 transmit log 514  
 help 38  
 http revision-down permit 76  
 http revision-up go 689  
 http revision-up permit 75  
 http revision-up proxy 75  
 http revision-up schedule 77  
 http revision-up timeout 76  
 http revision-up url 75  
 http wwan-module-up go 549  
 http wwan-module-up permit 550  
 http wwan-module-up timeout 550  
 http wwan-module-up url 549  
 httpd custom-gui api password 583  
 httpd custom-gui api use 583  
 httpd custom-gui use 582  
 httpd custom-gui user 582  
 httpd host 490  
 httpd listen 491  
 httpd proxy-access l2ms permit 655  
 httpd service 490  
 httpd timeout 491

## I

import sshd authorized-keys 84  
 interface reset 681  
 interface reset wwan-module 681  
 ip arp timer 121  
 ip dpi filter 589  
 ip dscp supersede 127  
 ip filter 106  
 ip filter directed-broadcast 110  
 ip filter dynamic 111

ip filter dynamic timer 112  
 ip filter fqdn timer 113  
 ip filter set 109  
 ip filter source-route 110  
 ip flow limit 126  
 ip flow timer 126  
 ip forward filter 152  
 ip fragment remove df-bit 119  
 ip host 323  
 ip icmp echo-reply send 198  
 ip icmp echo-reply send-only-linkup 198  
 ip icmp error-decrypted-ipsec send 201  
 ip icmp log 202  
 ip icmp mask-reply send 198  
 ip icmp parameter-problem send 199  
 ip icmp redirect receive 199  
 ip icmp redirect send 199  
 ip icmp time-exceeded send 200  
 ip icmp timestamp-reply send 200  
 ip icmp unreachable send 201  
 ip implicit-route preference 125  
 ip interface address 98  
 ip interface arp log 123  
 ip interface arp queue length 122  
 ip interface arp static 122  
 ip interface dhcp auto default-route-add 104  
 ip interface dhcp auto interface-route-add 104  
 ip interface dhcp lease time 193  
 ip interface dhcp retry 194  
 ip interface dhcp service 192  
 ip interface dpi filter 591  
 ip interface forward filter 153  
 ip interface intrusion detection 114  
 ip interface intrusion detection notice-interval 115  
 ip interface intrusion detection repeat-control 115  
 ip interface intrusion detection report 116  
 ip interface mtu 100  
 ip interface nat descriptor 303  
 ip interface ospf area 354  
 ip interface ospf neighbor 358  
 ip interface pdp auto default-route-add 105  
 ip interface pdp auto interface-route-add 105  
 ip interface proxyarp 121  
 ip interface proxyarp vrrp 121  
 ip interface rebound 101  
 ip interface rip auth key 137  
 ip interface rip auth key text 137  
 ip interface rip auth type 136  
 ip interface rip filter 135  
 ip interface rip force-to-advertise 140  
 ip interface rip hop 136  
 ip interface rip receive 134  
 ip interface rip send 134  
 ip interface rip trust gateway 133  
 ip interface secondary address 99  
 ip interface secure filter 118  
 ip interface secure filter name 118  
 ip interface tcp mss limit 116  
 ip interface tcp window-scale 117  
 ip interface vrrp 142  
 ip interface vrrp shutdown trigger 143  
 ip interface wol relay 74  
 ip keepalive 123  
 ip local forward filter 153  
 ip pp address 98  
 ip pp dpi filter 591  
 ip pp forward filter 153  
 ip pp intrusion detection 114  
 ip pp intrusion detection notice-interval 115  
 ip pp intrusion detection repeat-control 115  
 ip pp intrusion detection report 116  
 ip pp mtu 100

ip pp nat descriptor 303  
 ip pp ospf area 354  
 ip pp ospf neighbor 358  
 ip pp rebound 101  
 ip pp remote address 128  
 ip pp remote address pool 129  
 ip pp rip auth key 137  
 ip pp rip auth key text 137  
 ip pp rip auth type 136  
 ip pp rip backup interface 140  
 ip pp rip connect interval 139  
 ip pp rip connect send 138  
 ip pp rip disconnect interval 140  
 ip pp rip disconnect send 139  
 ip pp rip filter 135  
 ip pp rip force-to-advertise 140  
 ip pp rip hold routing 138  
 ip pp rip hop 136  
 ip pp rip receive 134  
 ip pp rip send 134  
 ip pp rip trust gateway 133  
 ip pp secure filter 118  
 ip pp secure filter name 118  
 ip pp tcp mss limit 116  
 ip pp tcp window-scale 117  
 ip reassembly hold-time 127  
 ip route 101  
 ip route change log 118  
 ip routing 98  
 ip routing process 63  
 ip simple-service 101  
 ip stealth 202  
 ip tos supersede 120  
 ip tunnel address 211  
 ip tunnel dpi filter 591  
 ip tunnel forward filter 153  
 ip tunnel intrusion detection 114  
 ip tunnel intrusion detection notice-interval 115  
 ip tunnel intrusion detection repeat-control 115  
 ip tunnel intrusion detection report 116  
 ip tunnel mtu 100  
 ip tunnel nat descriptor 303  
 ip tunnel ospf area 354  
 ip tunnel ospf neighbor 358  
 ip tunnel rebound 101  
 ip tunnel remote address 211  
 ip tunnel rip auth key 137  
 ip tunnel rip auth key text 137  
 ip tunnel rip auth type 136  
 ip tunnel rip filter 135  
 ip tunnel rip force-to-advertise 140  
 ip tunnel rip hop 136  
 ip tunnel rip receive 134  
 ip tunnel rip send 134  
 ip tunnel rip trust gateway 133  
 ip tunnel secure filter 118  
 ip tunnel secure filter name 118  
 ip tunnel tcp mss limit 116  
 ip tunnel tcp window-scale 117  
 ipip keepalive log 273  
 ipip keepalive use 273  
 ipsec auto refresh 222  
 ipsec ike always-on 223  
 ipsec ike auth method 218  
 ipsec ike backward-compatibility 235  
 ipsec ike child-exchange type 245  
 ipsec ike duration 246  
 ipsec ike eap myname 220  
 ipsec ike eap request 221  
 ipsec ike eap send certreq 221  
 ipsec ike encryption 231  
 ipsec ike esp-encapsulation 243  
 ipsec ike group 232  
 ipsec ike hash 233  
 ipsec ike keepalive log 231  
 ipsec ike keepalive use 229  
 ipsec ike local address 227  
 ipsec ike local id 228  
 ipsec ike local name 227  
 ipsec ike log 243  
 ipsec ike message-id-control 245  
 ipsec ike mode-cfg address 242  
 ipsec ike mode-cfg address pool 241  
 ipsec ike mode-cfg method 241  
 ipsec ike nat-traversal 251  
 ipsec ike negotiate-strictly 223  
 ipsec ike negotiation receive 246  
 ipsec ike payload type 235  
 ipsec ike pfs 236  
 ipsec ike pki file 220  
 ipsec ike pre-shared-key 219  
 ipsec ike proposal-limitation 244  
 ipsec ike queue length 232  
 ipsec ike remote address 225  
 ipsec ike remote id 226  
 ipsec ike remote name 224  
 ipsec ike restrict-dangling-sa 250  
 ipsec ike retry 224  
 ipsec ike send info 236  
 ipsec ike version 218  
 ipsec ike xauth myname 237  
 ipsec ike xauth request 240  
 ipsec ipcomp type 254  
 ipsec log illegal-spi 234  
 ipsec refresh sa 250  
 ipsec sa delete 252  
 ipsec sa policy 248  
 ipsec transport 258  
 ipsec transport template 258  
 ipsec tunnel 254  
 ipsec tunnel fastpath-fragment-function follow df-bit 253  
 ipsec tunnel outer df-bit 253  
 ipsec use 218  
 ipv6 dpi filter 590  
 ipv6 dscp supersede 375  
 ipv6 filter 396  
 ipv6 filter dynamic 399  
 ipv6 icmp echo-reply send 203  
 ipv6 icmp echo-reply send-only-linkup 203  
 ipv6 icmp error-decrypted-ipsec send 206  
 ipv6 icmp log 206  
 ipv6 icmp packet-too-big send 206  
 ipv6 icmp parameter-problem send 204  
 ipv6 icmp redirect receive 204  
 ipv6 icmp redirect send 204  
 ipv6 icmp time-exceeded send 205  
 ipv6 icmp unreachable send 205  
 ipv6 interface address 376  
 ipv6 interface dad retry count 381  
 ipv6 interface dhcp service 380  
 ipv6 interface dpi filter 591  
 ipv6 interface icmp-nd queue length 374  
 ipv6 interface mld 401  
 ipv6 interface mld static 402  
 ipv6 interface mtu 371  
 ipv6 interface neighbor cache max entry 374  
 ipv6 interface ospf area 406  
 ipv6 interface prefix 378  
 ipv6 interface prefix change log 379  
 ipv6 interface rip filter 391  
 ipv6 interface rip hop 390  
 ipv6 interface rip receive 390  
 ipv6 interface rip send 389  
 ipv6 interface rip trust gateway 391

ipv6 interface rtadv send 385  
 ipv6 interface rtsol max-retransmit 386  
 ipv6 interface secure filter 398  
 ipv6 interface tcp mss limit 372  
 ipv6 interface tcp window-scale 372  
 ipv6 interface vrrp 394  
 ipv6 interface vrrp shutdown trigger 395  
 ipv6 max auto address 381  
 ipv6 nd ns-trigger-dad 403  
 ipv6 nd ra-rdcss 384  
 ipv6 ospf area 405  
 ipv6 ospf area network 405  
 ipv6 ospf configure refresh 404  
 ipv6 ospf export 410  
 ipv6 ospf export from ospf 409  
 ipv6 ospf import 412  
 ipv6 ospf import from 411  
 ipv6 ospf log 413  
 ipv6 ospf preference 409  
 ipv6 ospf router id 404  
 ipv6 ospf use 404  
 ipv6 ospf virtual-link 408  
 ipv6 pp address 376  
 ipv6 pp dad retry count 381  
 ipv6 pp dhcp service 380  
 ipv6 pp dpi filter 591  
 ipv6 pp mld 401  
 ipv6 pp mld static 402  
 ipv6 pp mtu 371  
 ipv6 pp ospf area 406  
 ipv6 pp prefix 378  
 ipv6 pp prefix change log 379  
 ipv6 pp rip connect interval 392  
 ipv6 pp rip connect send 392  
 ipv6 pp rip disconnect interval 393  
 ipv6 pp rip disconnect send 393  
 ipv6 pp rip filter 391  
 ipv6 pp rip hold routing 393  
 ipv6 pp rip hop 390  
 ipv6 pp rip receive 390  
 ipv6 pp rip send 389  
 ipv6 pp rip trust gateway 391  
 ipv6 pp rtadv send 385  
 ipv6 pp rtsol max-retransmit 386  
 ipv6 pp secure filter 398  
 ipv6 pp tcp mss limit 372  
 ipv6 pp tcp window-scale 372  
 ipv6 prefix 382  
 ipv6 reassembly hold-time 375  
 ipv6 rh0 discard 373  
 ipv6 rip preference 394  
 ipv6 rip use 389  
 ipv6 route 387  
 ipv6 route change log 389  
 ipv6 routing 371  
 ipv6 routing process 373  
 ipv6 source address selection rule 382  
 ipv6 stealth 207  
 ipv6 tunnel address 376  
 ipv6 tunnel dhcp service 380  
 ipv6 tunnel dpi filter 591  
 ipv6 tunnel mld 401  
 ipv6 tunnel mld static 402  
 ipv6 tunnel mtu 371  
 ipv6 tunnel ospf area 406  
 ipv6 tunnel prefix 378  
 ipv6 tunnel prefix change log 379  
 ipv6 tunnel rip filter 391  
 ipv6 tunnel rip receive 390  
 ipv6 tunnel rip send 389  
 ipv6 tunnel secure filter 398  
 ipv6 tunnel tcp mss limit 372

ipv6 tunnel tcp window-scale 372

## L

l2tp always-on 264  
 l2tp hostname 265  
 l2tp keepalive log 263  
 l2tp keepalive use 263  
 l2tp local router-id 265  
 l2tp remote end-id 266  
 l2tp remote router-id 266  
 l2tp service 261  
 l2tp syslog 264  
 l2tp tunnel auth 262  
 l2tp tunnel disconnect time 262  
 lan backup 146  
 lan backup recovery time 147  
 lan keepalive interval 148  
 lan keepalive log 149  
 lan keepalive use 147  
 lan linkup send-wait-time 64  
 lan port-mirroring 65  
 lan shutdown 64  
 lan type 65  
 lan-map log 605  
 lan-map snapshot use 604  
 lan-map sysname 606  
 lan-map terminal watch interval 603  
 less 36  
 less config 695  
 less config ap 695  
 less config list 698  
 less config pp 696  
 less config switch 696  
 less config tunnel 696  
 less config wwan 697  
 less exec list 701  
 less file list 698  
 less log 736  
 license authentication go 691  
 license authentication retry interval 691  
 load 691  
 login password 39  
 login password encrypted 39  
 login radius use 40  
 login timer 44  
 login user 40  
 lua 578  
 lua use 578  
 luac 579

## M

macro 49  
 mail notify 487  
 mail notify status exec 690  
 mail server name 483  
 mail server pop 484  
 mail server smtp 483  
 mail server timeout 485  
 mail template 485  
 make directory 678  
 mobile access limit connection length 560  
 mobile access limit connection time 561  
 mobile access limit duration 561  
 mobile access limit length 556  
 mobile access limit time 557  
 mobile access-point name 555  
 mobile arrive permit 562  
 mobile arrive use 562  
 mobile auto connect 554  
 mobile call prohibit auth-error count 558



mobile call type 552  
 mobile carrier mode 566  
 mobile dial number 556  
 mobile disconnect input time 555  
 mobile disconnect output time 555  
 mobile disconnect time 554  
 mobile display caller id 559  
 mobile firmware update go 565  
 mobile pin code 552  
 mobile signal-strength 563  
 mobile signal-strength go 563  
 mobile syslog 560  
 mobile use 551

## N

nat descriptor address inner 306  
 nat descriptor address outer 305  
 nat descriptor backward-compatibility 303  
 nat descriptor ftp port 311  
 nat descriptor log 311  
 nat descriptor masquerade incoming 309  
 nat descriptor masquerade port range 310  
 nat descriptor masquerade remove df-bit 312  
 nat descriptor masquerade rlogin 307  
 nat descriptor masquerade session limit 313  
 nat descriptor masquerade session limit total 313  
 nat descriptor masquerade static 307  
 nat descriptor masquerade ttl hold 309  
 nat descriptor masquerade unconvertible port 311  
 nat descriptor sip 312  
 nat descriptor static 306  
 nat descriptor timer 308  
 nat descriptor type 304  
 nat46 ip address pool 327  
 nat46 ipv6 prefix 327  
 nat46 static 328  
 netvolante-dns auto hostname 496  
 netvolante-dns auto hostname pp 496  
 netvolante-dns auto save 501  
 netvolante-dns delete go 494  
 netvolante-dns delete go pp 494  
 netvolante-dns get hostname list 494  
 netvolante-dns get hostname list pp 494  
 netvolante-dns go 493  
 netvolante-dns go pp 493  
 netvolante-dns hostname host 495  
 netvolante-dns hostname host pp 495  
 netvolante-dns hostname sip 496  
 netvolante-dns port 494  
 netvolante-dns register timer 500  
 netvolante-dns retry interval 500  
 netvolante-dns retry interval pp 500  
 netvolante-dns server 498  
 netvolante-dns server update address port 499  
 netvolante-dns server update address use 499  
 netvolante-dns set hostname 498  
 netvolante-dns sip use 497  
 netvolante-dns sip use pp 497  
 netvolante-dns timeout 496  
 netvolante-dns timeout pp 496  
 netvolante-dns use 493  
 netvolante-dns use pp 493  
 ngn radius account callee 481  
 ngn radius account caller 481  
 ngn radius auth password 480  
 ngn renumbering link-refresh 476  
 ngn type 476  
 nslookup 685  
 ntp backward-compatibility 53  
 ntp local address 53  
 ntpdate 52

## O

onu backup 149  
 onu backup recovery time 150  
 onu keepalive interval 151  
 onu keepalive log 151  
 onu keepalive use 150  
 onu linkup send-wait-time 72  
 onu shutdown 71  
 onu type 70  
 operation button function download 532  
 operation execute batch permit 532  
 operation external-memory download permit 526  
 operation http revision-up permit 76  
 ospf area 351  
 ospf area network 352  
 ospf area stubhost 353  
 ospf configure refresh 346  
 ospf export filter 348  
 ospf export from ospf 347  
 ospf import filter 350  
 ospf import from 348  
 ospf log 358  
 ospf merge equal cost stub 358  
 ospf preference 346  
 ospf reric interval 359  
 ospf router id 347  
 ospf use 346  
 ospf virtual-link 353

## P

packetdump 61  
 packetdump pp 61  
 password reenter 45  
 ping 683  
 ping6 683  
 pki certificate file 259  
 pki crl file 260  
 pp always-on 164  
 pp auth accept 162, 270  
 pp auth multi connect prohibit 164  
 pp auth myname 163  
 pp auth request 163, 269  
 pp auth username 162  
 pp backup 145  
 pp backup pp 145  
 pp backup recovery time 146  
 pp backup tunnel 145  
 pp bind 267, 554  
 pp disable 680  
 pp enable 679  
 pp keepalive interval 130  
 pp keepalive log 132  
 pp keepalive use 131  
 pp name 491  
 pp select 666  
 ppp ccp maxconfigure 174  
 ppp ccp maxfailure 175  
 ppp ccp maxterminate 174  
 ppp ccp no-encryption 272  
 ppp ccp restart 174  
 ppp ccp type 173  
 ppp chap maxchallenge 169  
 ppp chap restart 169  
 ppp ipcp ipaddress 170  
 ppp ipcp maxconfigure 171  
 ppp ipcp maxfailure 171  
 ppp ipcp maxterminate 171  
 ppp ipcp msexp 172  
 ppp ipcp remote address check 172  
 ppp ipcp restart 170

ppp ipcp vjc 170  
 ppp ipv6cp use 175  
 ppp lcp accm 559  
 ppp lcp acfc 165  
 ppp lcp magicnumber 166  
 ppp lcp maxconfigure 167  
 ppp lcp maxfailure 168  
 ppp lcp maxterminate 167  
 ppp lcp mru 166  
 ppp lcp pfc 166  
 ppp lcp restart 167  
 ppp lcp silent 168  
 ppp msccp maxretry 173  
 ppp msccp restart 172  
 ppp pap maxauthreq 169  
 ppp pap restart 168  
 pppoe access concentrator 176  
 pppoe auto connect 176  
 pppoe auto disconnect 176  
 pppoe call prohibit auth-error count 179  
 pppoe disconnect time 178  
 pppoe invalid-session forced close 179  
 pppoe padi maxretry 177  
 pppoe padi restart 177  
 pppoe padr maxretry 177  
 pppoe padr restart 177  
 pppoe pass-through member 180  
 pppoe service-name 178  
 pppoe tcp mss limit 178  
 pppoe use 175  
 pptp hostname 268  
 pptp keepalive interval 272  
 pptp keepalive log 271  
 pptp keepalive use 271  
 pptp service 267  
 pptp service type 268  
 pptp syslog 270  
 pptp tunnel disconnect time 271  
 pptp vendorname 268  
 pptp window size 269

## Q

queue class filter 330  
 queue interface class control 336  
 queue interface class filter list 334  
 queue interface class property 336  
 queue interface default class 335  
 queue interface length 335  
 queue interface type 333  
 queue pp class filter list 334  
 queue pp class property 336  
 queue pp default class 335  
 queue pp length 335  
 queue pp type 333  
 queue tunnel class filter list 334  
 queue tunnel default class 335  
 quit 667

## R

radius account 299  
 radius account port 301  
 radius account server 301  
 radius auth 299  
 radius auth port 301  
 radius auth server 300  
 radius retry 302  
 radius secret 302  
 radius server 300  
 rdate 52  
 remote setup accept 672

rename 679  
 restart 680  
 rip advertise mode 137  
 rip filter rule 141  
 rip preference 133  
 rip timer 142  
 rip use 132  
 rollback timer 693  
 rotate external-memory syslog 690  
 rtf format 97  
 rtf garbage-collect 97

## S

save 667  
 schedule at 505  
 scp 93  
 sd use 521  
 security class 45  
 set 48  
 set-default-config 671  
 set-default-exec 671  
 set-serial-baudrate 671  
 sftpd host 73  
 show account 736  
 show account analog 737  
 show account mobile 738  
 show account ngn data 738  
 show account ngn tel 738  
 show account pp 737  
 show account sip 737  
 show account wwan 738  
 show alias 701  
 show arp 703  
 show bridge learning 706  
 show command 38  
 show command history 739  
 show config 695  
 show config analog extension 698  
 show config ap 695  
 show config difference 697  
 show config list 698  
 show config pp 696  
 show config switch 696  
 show config tunnel 696  
 show config wwan 697  
 show copyright 734  
 show diagnosis config port access 586  
 show diagnosis config port map 586  
 show dns cache 730  
 show dpi application 597  
 show dpi cache 597  
 show dpi category 598  
 show dpi statistics 595  
 show environment 695  
 show exec list 701  
 show file list 698  
 show history 739  
 show ip connection 713  
 show ip connection pp 713  
 show ip connection tunnel 713  
 show ip intrusion detection 715  
 show ip intrusion detection pp 715  
 show ip intrusion detection tunnel 715  
 show ip rip table 705  
 show ip route 704  
 show ip secure filter 700  
 show ip secure filter pp 700  
 show ip secure filter tunnel 700  
 show ipsec sa 706  
 show ipsec sa gateway 706  
 show ipv6 address 699

show ipv6 address pp 699  
 show ipv6 address tunnel 699  
 show ipv6 connection 714  
 show ipv6 connection pp 714  
 show ipv6 connection tunnel 714  
 show ipv6 mroute fib 719  
 show ipv6 neighbor cache 705  
 show ipv6 ospf 722  
 show ipv6 rip table 705  
 show ipv6 route 705  
 show ipv6 secure filter 700  
 show ipv6 secure filter pp 700  
 show ipv6 secure filter tunnel 700  
 show lan-map 732  
 show log 736  
 show macro 702  
 show nat descriptor address 708  
 show nat descriptor interface address 708  
 show nat descriptor interface address pp 708  
 show nat descriptor interface address tunnel 708  
 show nat descriptor interface bind 708  
 show nat descriptor interface bind pp 708  
 show nat descriptor interface bind tunnel 708  
 show nat descriptor masquerade port summary 709  
 show nat descriptor masquerade session statistics 710  
 show nat descriptor masquerade session summary 709  
 show onu-module info 734  
 show pki certificate summary 707  
 show pki crl 707  
 show pp connect time 715  
 show pppoe pass-through learning 716  
 show set 701  
 show sshd authorized-keys 85  
 show sshd host key 80  
 show sshd public key 700  
 show status 703  
 show status analog 727  
 show status analog extension 727  
 show status backup 713  
 show status bgp neighbor 711  
 show status boot 728  
 show status boot all 728  
 show status boot list 728  
 show status cloud vpn 278  
 show status cooperation 721  
 show status dhcp 712  
 show status dhcpc 712  
 show status dpi 599  
 show status ethernet filter 156  
 show status external-memory 726  
 show status heartbeat 723  
 show status heartbeat2 723  
 show status heartbeat2 id 723  
 show status heartbeat2 name 723  
 show status ip keepalive 715  
 show status ipip 711  
 show status ipv6 dhcp 713  
 show status ipv6 mld 719  
 show status l2tp 710  
 show status license 730  
 show status license authentication 731  
 show status lua 579  
 show status mail service 718  
 show status mobile signal-strength 564  
 show status nat46 table 328  
 show status netvolante-dns 716  
 show status netvolante-dns pp 716  
 show status ngn 477  
 show status ospf 711  
 show status packet-buffer 720  
 show status pp 703  
 show status pptp 710  
 show status qos 721  
 show status remote setup 724  
 show status rtfS 726  
 show status sd 725  
 show status sip presence 726  
 show status sip server 726  
 show status status-led 731  
 show status switch control 728  
 show status switch control route backup 730  
 show status switching-hub macaddress 717  
 show status tunnel 717  
 show status upnp 717  
 show status usbhost 724  
 show status user 719  
 show status user history 720  
 show status vlan 718  
 show status voice call 734  
 show status vrrp 707  
 show status wwan-module 725  
 show status wwan-module signal-strength 548  
 show status yno 660  
 show status yno las 663  
 show techinfo 724  
 show url filter 722  
 show url filter pp 722  
 show url filter tunnel 722  
 sip 100rel 452  
 sip arrive address check 455  
 sip arrive name-display default 454  
 sip arrive ringing p-n-uatype 454  
 sip arrive session timer method 455  
 sip arrive session timer refresher 453  
 sip codec permit 448  
 sip ip protocol 448  
 sip log 456  
 sip netvolante dial domain 450  
 sip netvolante dial figure 450  
 sip outer address 456  
 sip request retransmit timer 449  
 sip response code busy 453  
 sip server 456  
 sip server 100rel 460  
 sip server analog service 462  
 sip server arrive number display 461  
 sip server call mode 463  
 sip server call own permit 464  
 sip server call remote domain 458  
 sip server call server error 464  
 sip server connect 685  
 sip server dial number-only 463  
 sip server disconnect 686  
 sip server display name 458  
 sip server pilot address 464  
 sip server privacy 457  
 sip server qvalue 461  
 sip server register contact mode 465  
 sip server register request-uri 461  
 sip server register timer 460  
 sip server session timer 459  
 sip session timer 451  
 sip use 448  
 sip user agent 453  
 snmp community read-only 281  
 snmp community read-write 281  
 snmp display ipcp force 294  
 snmp host 280  
 snmp ifindex switch static index 296  
 snmp local address 289  
 snmp syscontact 289  
 snmp syslocation 289  
 snmp sysname 290  
 snmp trap community 282

- snmp trap cpu threshold 282
- snmp trap delay-timer 291
- snmp trap enable snmp 290
- snmp trap enable switch 297
- snmp trap enable switch common 298
- snmp trap host 281
- snmp trap link-updown separate-l2switch-port 294
- snmp trap memory threshold 282
- snmp trap mobile signal-strength 295
- snmp trap send linkdown 291
- snmp trap send linkdown pp 291
- snmp trap send linkdown tunnel 291
- snmp trap wwan-module signal-strength 295
- snmp yrifppdisplayatmib2 292
- snmp yrifswitchdisplayatmib2 293
- snmp yrifunneldisplayatmib2 292
- snmp yrifwvdisplayatmib2 293
- snmp yrsindex switch static index 296
- snmpv2c community read-only 283
- snmpv2c community read-write 284
- snmpv2c host 283
- snmpv2c trap community 284
- snmpv2c trap host 284
- snmpv3 context name 285
- snmpv3 engine id 285
- snmpv3 host 286
- snmpv3 trap host 288
- snmpv3 usm user 285
- snmpv3 vacm access 288
- snmpv3 vacm view 287
- sntpd host 518
- sntpd service 518
- speed 330
- ssh 94
- ssh encrypt algorithm 95
- ssh known hosts 96
- sshd auth method 83
- sshd authorized-keys filename 83
- sshd client alive 82
- sshd encrypt algorithm 81
- sshd hide openssh version 82
- sshd host 79
- sshd host key generate 80
- sshd listen 78
- sshd service 78
- sshd session 80
- statistics 587
- switch config directory 610
- switch config filename 610
- switch control config get 611
- switch control config set 611
- switch control config-auto-set use 612
- switch control firmware upload go 608
- switch control function default 608
- switch control function execute 607
- switch control function execute clear-counter 642
- switch control function execute clear-macaddress-table 625
- switch control function execute reset-loopdetect 647
- switch control function execute restart 617
- switch control function execute restart-poe-supply 650
- switch control function execute start-poe-supply 650
- switch control function execute stop-poe-supply 651
- switch control function get 607
- switch control function get boot-rom-version 613
- switch control function get counter-frame-rx-type 637
- switch control function get counter-frame-tx-type 639
- switch control function get energy-saving 614
- switch control function get firmware-revision 613
- switch control function get lag-type 617
- switch control function get led-brightness 615
- switch control function get loopdetect-count 643
- switch control function get loopdetect-linkdown 644
- switch control function get loopdetect-port-use 645
- switch control function get loopdetect-recovery-timer 644
- switch control function get loopdetect-time 643
- switch control function get loopdetect-use-control-packet 645
- switch control function get macaddress-aging 623
- switch control function get macaddress-aging-timer 624
- switch control function get mirroring-dest 635
- switch control function get mirroring-src-rx 636
- switch control function get mirroring-src-tx 636
- switch control function get mirroring-use 635
- switch control function get model-name 613
- switch control function get poe-class 647
- switch control function get port-auto-crossover 619
- switch control function get port-blocking-control-packet 621
- switch control function get port-blocking-data-packet 621
- switch control function get port-flow-control 620
- switch control function get port-speed 618
- switch control function get port-speed-downshift 620
- switch control function get port-use 618
- switch control function get qos-dscp-remark-class 631
- switch control function get qos-dscp-remark-type 630
- switch control function get qos-policing-speed 632
- switch control function get qos-policing-use 632
- switch control function get qos-shaping-speed 633
- switch control function get qos-shaping-use 633
- switch control function get qos-speed-unit 631
- switch control function get serial-number 613
- switch control function get status-combo-port 622
- switch control function get status-counter-frame-rx 641
- switch control function get status-counter-frame-tx 641
- switch control function get status-counter-octet-rx 642
- switch control function get status-counter-octet-tx 642
- switch control function get status-fan 616
- switch control function get status-fan-rpm 616
- switch control function get status-led-mode 615
- switch control function get status-loopdetect-port 646
- switch control function get status-loopdetect-recovery-timer 646
- switch control function get status-macaddress-addr 624
- switch control function get status-macaddress-port 625
- switch control function get status-poe-detect-class 648
- switch control function get status-poe-state 648
- switch control function get status-poe-supply 649
- switch control function get status-poe-supply-detail 649
- switch control function get status-poe-supply-total 650
- switch control function get status-poe-temperature 649
- switch control function get status-port-sfp-rx-power 622
- switch control function get status-port-speed 623
- switch control function get system-macaddress 614
- switch control function get system-name 614
- switch control function get system-uptime 617
- switch control function get vlan-access 628
- switch control function get vlan-id 627
- switch control function get vlan-multiple 629
- switch control function get vlan-multiple-use 629
- switch control function get vlan-port-mode 627
- switch control function get vlan-trunk 628
- switch control function set 606
- switch control function set counter-frame-rx-type 637
- switch control function set counter-frame-tx-type 639
- switch control function set energy-saving 614
- switch control function set led-brightness 615
- switch control function set loopdetect-count 643
- switch control function set loopdetect-linkdown 644
- switch control function set loopdetect-port-use 645
- switch control function set loopdetect-recovery-timer 644
- switch control function set loopdetect-time 643
- switch control function set loopdetect-use-control-packet 645
- switch control function set macaddress-aging 623
- switch control function set macaddress-aging-timer 624
- switch control function set mirroring-dest 635
- switch control function set mirroring-src-rx 636
- switch control function set mirroring-src-tx 636

switch control function set mirroring-use 635  
 switch control function set poe-class 647  
 switch control function set port-auto-crossover 619  
 switch control function set port-blocking-control-packet 621  
 switch control function set port-blocking-data-packet 621  
 switch control function set port-flow-control 620  
 switch control function set port-speed 618  
 switch control function set port-speed-downshift 620  
 switch control function set port-use 618  
 switch control function set qos-dscp-remark-class 631  
 switch control function set qos-dscp-remark-type 630  
 switch control function set qos-policing-speed 632  
 switch control function set qos-policing-use 632  
 switch control function set qos-shaping-speed 633  
 switch control function set qos-shaping-use 633  
 switch control function set qos-speed-unit 631  
 switch control function set system-name 614  
 switch control function set vlan-access 628  
 switch control function set vlan-id 627  
 switch control function set vlan-multiple 629  
 switch control function set vlan-multiple-use 629  
 switch control function set vlan-port-mode 627  
 switch control function set vlan-trunk 628  
 switch control mode 601  
 switch control route backup 609  
 switch control use 602  
 switch control watch interval 603  
 switch select 606  
 syslog debug 57  
 syslog execute command 58  
 syslog facility 56  
 syslog host 55  
 syslog info 57  
 syslog local address 57  
 syslog notice 56  
 syslog srport 58  
 system cpu threshold 46  
 system memory threshold 47  
 system packet-buffer 47

## T

take lan-map snapshot 605  
 tcp log 58  
 tcp session limit 117  
 telnet 687  
 telnetd host 62  
 telnetd listen 62  
 telnetd service 61  
 telnetd session 63  
 terminate lua 580  
 terminate lua file 580  
 tftp host 72  
 time 51  
 timezone 51  
 traceroute 684  
 traceroute6 685  
 tunnel backup 255  
 tunnel backup pp 255  
 tunnel backup tunnel 255  
 tunnel disable 209  
 tunnel enable 209  
 tunnel encapsulation 210  
 tunnel endpoint address 213  
 tunnel endpoint local address 212  
 tunnel endpoint name 213  
 tunnel endpoint remote address 212  
 tunnel map-e type 215  
 tunnel multipoint local name 214  
 tunnel multipoint server 214  
 tunnel name 491  
 tunnel ngn arrive permit 478

tunnel ngn bandwidth 478  
 tunnel ngn call permit 479  
 tunnel ngn disconnect time 477  
 tunnel ngn fallback 479  
 tunnel ngn interface 479  
 tunnel ngn radius auth 480  
 tunnel select 666  
 tunnel template 256  
 tunnel translation 215  
 tunnel type 210

## U

unlock wwan pin-code 547  
 update wwan-module firmware 548  
 upnp external address refer 502  
 upnp external address refer pp 502  
 upnp port mapping timer 503  
 upnp port mapping timer type 503  
 upnp syslog 503  
 upnp use 502  
 url filter 158  
 url filter log 161  
 url filter port 159  
 url filter reject 160  
 url filter use 159  
 url interface filter 159  
 url pp filter 159  
 url tunnel filter 159  
 usbhost modem flow control 565  
 usbhost modem initialize 564  
 usbhost overcurrent duration 521  
 usbhost use 520  
 user attribute 41

## V

vlan interface 802.1q 508  
 vlan port mapping 508

## W

wan access limit connection length 572  
 wan access limit connection time 573  
 wan access limit duration 574  
 wan access limit length 570  
 wan access limit time 571  
 wan access-point name 570  
 wan always-on 569  
 wan auth myname 566  
 wan auto connect 567  
 wan bind 567  
 wan disconnect input time 568  
 wan disconnect output time 569  
 wan disconnect time 568  
 wins server 171  
 wol send 688  
 wwan access limit connection length 541  
 wwan access limit connection time 542  
 wwan access limit duration 542  
 wwan access limit length 543  
 wwan access limit time 543  
 wwan access-point name 538  
 wwan always-on 538  
 wwan auth accept 539  
 wwan auth myname 539  
 wwan auto connect 540  
 wwan disable 538  
 wwan disconnect input time 540  
 wwan disconnect output time 540  
 wwan disconnect time 541

- [wwan enable 537](#)
- [wwan pin code 545](#)
- [wwan radio access technology 544](#)
- [wwan select 537](#)
- [wwan-module radio-power 535](#)
- [wwan-module signal-strength 535](#)
- [wwan-module signal-strength go 536](#)
- [wwan-module syslog 536](#)
- [wwan-module use 534](#)

## Y

- [yno access code 657](#)
- [yno gui-forwarder timeout 659](#)
- [yno https-proxy 659](#)
- [yno las connection keepalive 663](#)
- [yno las request retry 662](#)
- [yno las request timeout 662](#)
- [yno las syslog queue length 662](#)
- [yno log 658](#)
- [yno use 657](#)
- [yno xmpp connection keepalive 664](#)
- [yno zero-config id 659](#)

**ヤマハネットワーク製品お客様相談センター**

TEL: 03-5651-1330

**ご相談受付時間**

9:00～12:00、13:00～17:00

(土・日・祝日、年末年始は休業とさせていただきます)

**お問い合わせページ**

<https://network.yamaha.com/support/> から  
サポートページにお進みください。