

NVR500

ブロードバンドVoIPルーター

Rev.11.00.43



コマンドリファレンス

ヤマハNVR500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、

正しく設置や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.....	21
第 1 章：コマンドリファレンスの見方.....	22
1.1 対応するプログラムのリビジョン.....	22
1.2 コマンドリファレンスの見方.....	22
1.3 インタフェース名について.....	22
1.4 no で始まるコマンドの入力形式について.....	22
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.....	23
1.6 工場出荷設定値について.....	23
第 2 章：コマンドの使い方.....	24
2.1 コンソールについて.....	24
2.1.1 コンソールによる設定手順.....	24
2.1.2 CONSOLE ポートからの設定.....	25
2.1.3 TELNET による設定.....	28
2.1.4 リモートセットアップ.....	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.....	30
2.3 TFTP について.....	31
2.3.1 TFTP による設定手順.....	31
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.....	32
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.....	35
2.5.3 外部メモリへのリダイレクト機能.....	36
第 3 章：ヘルプ.....	38
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
第 4 章：機器の設定.....	39
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 一般ユーザ名とログインパスワードの設定.....	39
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.....	40
4.8 ユーザーの属性を設定.....	41
4.9 他のユーザの接続の強制切断.....	43
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.....	44
4.12 セキュリティクラスの設定.....	44
4.13 パケットバッファのパラメータを変更する.....	45
4.14 LED の輝度を調整する.....	46
4.15 環境変数の設定.....	47
4.16 タイムゾーンの設定.....	47
4.17 現在の日付けの設定.....	47

4.18 現在の時刻の設定.....	48
4.19 リモートホストによる時計の設定.....	48
4.20 NTP による時計の設定.....	48
4.21 NTP パケットを送信するときの始点 IP アドレスの設定.....	49
4.22 Stratum 0 の NTP サーバーとの時刻同期を許可する設定.....	49
4.23 コンソールのプロンプト表示の設定.....	50
4.24 コンソールの言語とコードの設定.....	50
4.25 コンソールの表示文字数の設定.....	50
4.26 コンソールの表示行数の設定.....	51
4.27 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.....	51
4.28 SYSLOG を受けるホストの IP アドレスの設定.....	51
4.29 SYSLOG ファシリティの設定.....	52
4.30 NOTICE タイプの SYSLOG を出力するか否かの設定.....	52
4.31 INFO タイプの SYSLOG 出力の設定.....	52
4.32 DEBUG タイプの SYSLOG を出力するか否かの設定.....	53
4.33 SYSLOG を送信する時の始点 IP アドレスの設定.....	53
4.34 SYSLOG パケットの始点ポート番号の設定.....	53
4.35 SYSLOG に実行コマンドを出力するか否かの設定.....	53
4.36 TCP のコネクションレベルの <code>syslog</code> を出力するか否かの設定.....	54
4.37 インタ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.....	56
4.38 TELNET サーバー機能の ON/OFF の設定.....	57
4.39 TELNET サーバー機能の <code>listen</code> ポートの設定.....	57
4.40 TELNET サーバーへアクセスできるホストの IP アドレスの設定.....	57
4.41 TELNET サーバーへ同時に接続できるユーザ数の設定.....	58
4.42 ファストパス機能の設定.....	58
4.43 LAN インタフェースの動作設定.....	58
4.44 HUB IC での受信オーバーフロー数を取得するか否かの設定.....	59
4.45 LAN インタフェースのリンクアップ後の送信抑制時間の設定.....	59
4.46 LAN インタフェースの動作タイプの設定.....	60
4.47 インタフェースまたはシステムの説明の設定.....	62
4.48 TFTP によりアクセスできるホストの IP アドレスの設定.....	62
4.49 SFTP サーバーへアクセスできるホストの IP アドレスの設定.....	63
4.50 Magic Packet を LAN に中継するか否かの設定.....	63
4.51 HTTP リビジョンアップ実行を許可するか否かの設定.....	64
4.52 HTTP リビジョンアップ用 URL の設定.....	64
4.53 HTTP リビジョンアップ用 Proxy サーバーの設定.....	65
4.54 HTTP リビジョンアップ処理のタイムアウトの設定.....	65
4.55 リビジョンダウンを許可するか否かの設定.....	65
4.56 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.....	66
4.57 リビジョンアップ実行のスケジュール.....	66
4.58 SSH サーバー機能の ON/OFF の設定.....	67
4.59 SSH サーバー機能の <code>listen</code> ポートの設定.....	67
4.60 SSH サーバーへアクセスできるホストの IP アドレスの設定.....	67
4.61 SSH サーバーへ同時に接続できるユーザ数の設定.....	68
4.62 SSH サーバーホスト鍵の設定.....	68
4.63 SSH サーバーで利用可能な暗号アルゴリズムの設定.....	69
4.64 SSH クライアントの生存確認.....	69
4.65 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.....	70
4.66 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.....	70
4.67 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.....	71
4.68 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.....	71
4.69 攻撃を検知した時にアラーム音を鳴らすか否かの設定.....	71
4.70 MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かの設定.....	72
4.71 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.....	72
4.72 microSD 機能に関連するアラームを鳴らすか否かの設定.....	72
4.73 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.....	73
4.74 起動時のアラーム音を鳴らすか否かの設定.....	73
4.75 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.....	73
4.76 エコーキャンセラ制御方法の設定.....	74
4.77 エコーキャンセラの NLP 閾値の設定.....	75
4.78 エコーキャンセラを無効にする音の設定.....	76

4.79 ジッタバッファ制御方法の設定	76
4.80 RTP パケットのパケット長を設定	77
4.81 RTP/RTCP で使用するポート番号の設定	78
4.82 SCP クライアント	78
4.83 SSH クライアント	79
4.84 SSH クライアントで利用可能な暗号アルゴリズムの設定	79
4.85 SSH サーバーの公開鍵情報を保存するファイルの設定	80

第 5 章 : ヤマハルーター用ファイルシステム RTFS.....81

5.1 RTFS のフォーマット	81
5.2 RTFS のガベージコレクト	81

第 6 章 : ISDN 関連の設定.....82

6.1 共通の設定	82
6.1.1 BRI インタフェースの使用制限の設定	82
6.1.2 BRI 回線の種類の指定	82
6.1.3 自分の ISDN 番号の設定	83
6.1.4 PP で使用するインタフェースの設定	83
6.1.5 課金額による発信制限の設定	83
6.1.6 PIAFS の着信を許可するか否かの設定	84
6.1.7 PIAFS 接続時の起動側の指定	84
6.1.8 PIAFS の発信方式の設定	85
6.2 相手側の設定	86
6.2.1 常時接続の設定	86
6.2.2 相手 ISDN 番号の設定	86
6.2.3 自動接続の設定	87
6.2.4 自動切断の設定	87
6.2.5 相手への発信順序の設定	88
6.2.6 着信許可の設定	88
6.2.7 発信許可の設定	89
6.2.8 再発信抑制タイマの設定	89
6.2.9 エラー切断後の再発信禁止タイマの設定	89
6.2.10 相手にコールバック要求を行うか否かの設定	90
6.2.11 相手からのコールバック要求に応じるか否かの設定	90
6.2.12 コールバック要求タイプの設定	90
6.2.13 コールバック受け入れタイプの設定	91
6.2.14 MS コールバックでユーザからの番号指定を許可するか否かの設定	91
6.2.15 コールバックタイマの設定	91
6.2.16 コールバック待機タイマの設定	92
6.2.17 ISDN 回線を切断するタイマ方式の指定	92
6.2.18 切断タイマの設定 (ノーマル)	92
6.2.19 切断タイマの設定 (ファスト)	93
6.2.20 切断タイマの設定 (強制)	93
6.2.21 入力切断タイマの設定 (ノーマル)	94
6.2.22 出力切断タイマの設定 (ノーマル)	94
6.2.23 課金単位時間方式での課金単位時間と監視時間の設定	95
6.2.24 同じ相手に対して連続して認証に失敗できる回数	96
6.2.25 MP が失敗できる最大回数の設定	96
6.2.26 相手先毎の累積接続時間による発信制限の設定	97
6.2.27 相手先毎の累積接続回数による発信制限の設定	97
6.2.28 i・ナンバーサービスのポート番号の設定	97

第 7 章 : IP の設定.....99

7.1 インタフェース共通の設定	99
7.1.1 IP パケットを扱うか否かの設定	99
7.1.2 IP アドレスの設定	99
7.1.3 セカンダリ IP アドレスの設定	100
7.1.4 インタフェースの MTU の設定	100

7.1.5 同一インタ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
7.1.6 echo,discard,time サービスを動作させるか否かの設定	101
7.1.7 IP の静的経路情報の設定	102
7.1.8 IP パケットのフィルタの設定	104
7.1.9 フィルタセットの定義	106
7.1.10 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	107
7.1.11 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	107
7.1.12 動的フィルタの定義	108
7.1.13 動的フィルタのタイムアウトの設定	109
7.1.14 侵入検知機能の動作の設定	110
7.1.15 1 秒間に侵入検知情報を通知する頻度の設定	111
7.1.16 重複する侵入検知情報の通知抑制の設定	111
7.1.17 侵入検知情報の最大表示件数の設定	112
7.1.18 TCP セッションの MSS 制限の設定	112
7.1.19 TCP ウィンドウ・スケール・オプションを変更する	113
7.1.20 ルーターが端点となる TCP のセッション数の設定	113
7.1.21 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	114
7.1.22 フィルタリングによるセキュリティーの設定	114
7.1.23 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	115
7.1.24 代理 ARP の設定	116
7.1.25 ARP エントリの寿命の設定	116
7.1.26 静的 ARP エントリの設定	116
7.1.27 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	117
7.1.28 ARP エントリの変化をログに残すか否かの設定	117
7.1.29 ネットワーク監視機能の設定	117
7.1.30 フローテーブルの各エントリの寿命を設定する	119
7.2 PP 側の設定	119
7.2.1 PP 側 IP アドレスの設定	119
7.2.2 リモート IP アドレスプールの設定	120
7.2.3 PP 経由のキープアライブの時間間隔の設定	121
7.2.4 PP 経由のキープアライブを使用するか否かの設定	121
7.2.5 PP 経由のキープアライブのログをとるか否かの設定	122
7.2.6 専用線ダウン検出時の動作の設定	123
7.3 RIP の設定	123
7.3.1 RIP を使用するか否かの設定	123
7.3.2 RIP に関して信用できるゲートウェイの設定	123
7.3.3 RIP による経路の優先度の設定	124
7.3.4 RIP パケットの送信に関する設定	124
7.3.5 RIP パケットの受信に関する設定	125
7.3.6 RIP のフィルタリングの設定	126
7.3.7 RIP で加算するホップ数の設定	126
7.3.8 RIP2 での認証の設定	127
7.3.9 RIP2 での認証キーの設定	127
7.3.10 回線切断時の経路保持の設定	128
7.3.11 回線接続時の PP 側の RIP の動作の設定	128
7.3.12 回線接続時の PP 側の RIP 送出の時間間隔の設定	128
7.3.13 回線切断時の PP 側の RIP の動作の設定	129
7.3.14 回線切断時の PP 側の RIP 送出の時間間隔の設定	129
7.3.15 RIP で強制的に経路を広告する	130
7.3.16 RIP2 でのフィルタの比較方法	130
7.3.17 RIP のタイマーを調整する	131

第 8 章 : イーサネットフィルタの設定.....132

8.1 フィルタ定義の設定	132
8.2 インタフェースへの適用の設定	134

第 9 章 : PPP の設定.....135

9.1 相手の名前とパスワードの設定	135
9.2 受け入れる認証タイプの設定	136

9.3 要求する認証タイプの設定.....	136
9.4 自分の名前とパスワードの設定.....	137
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.....	137
9.6 LCP 関連の設定.....	137
9.6.1 Address and Control Field Compression オプション使用の設定.....	137
9.6.2 Magic Number オプション使用の設定.....	138
9.6.3 Maximum Receive Unit オプション使用の設定.....	138
9.6.4 Protocol Field Compression オプション使用の設定.....	139
9.6.5 lcp-restart パラメータの設定.....	139
9.6.6 lcp-max-terminate パラメータの設定.....	139
9.6.7 lcp-max-configure パラメータの設定.....	139
9.6.8 lcp-max-failure パラメータの設定.....	140
9.6.9 Configure-Request をすぐに送信するか否かの設定.....	140
9.7 PAP 関連の設定.....	140
9.7.1 pap-restart パラメータの設定.....	140
9.7.2 pap-max-authreq パラメータの設定.....	141
9.8 CHAP 関連の設定.....	141
9.8.1 chap-restart パラメータの設定.....	141
9.8.2 chap-max-challenge パラメータの設定.....	141
9.9 IPCP 関連の設定.....	141
9.9.1 Van Jacobson Compressed TCP/IP 使用の設定.....	141
9.9.2 PP 側 IP アドレスのネゴシエーションの設定.....	142
9.9.3 ipcp-restart パラメータの設定.....	142
9.9.4 ipcp-max-terminate パラメータの設定.....	142
9.9.5 ipcp-max-configure パラメータの設定.....	142
9.9.6 ipcp-max-failure パラメータの設定.....	143
9.9.7 WINS サーバーの IP アドレスの設定.....	143
9.9.8 IPCP の MS 拡張オプションを使うか否かの設定.....	143
9.9.9 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.....	144
9.10 MSCBCP 関連の設定.....	144
9.10.1 mscbcpc-restart パラメータの設定.....	144
9.10.2 mscbcpc-maxretry パラメータの設定.....	144
9.11 CCP 関連の設定.....	144
9.11.1 全パケットの圧縮タイプの設定.....	145
9.11.2 ccp-restart パラメータの設定.....	145
9.11.3 ccp-max-terminate パラメータの設定.....	145
9.11.4 ccp-max-configure パラメータの設定.....	146
9.11.5 ccp-max-failure パラメータの設定.....	146
9.12 IPV6CP 関連の設定.....	146
9.12.1 IPV6CP を使用するか否かの設定.....	146
9.13 MP 関連の設定.....	147
9.13.1 MP を使用するか否かの設定.....	147
9.13.2 MP の制御方法の設定.....	147
9.13.3 MP のための負荷閾値の設定.....	147
9.13.4 MP の最大リンク数の設定.....	148
9.13.5 MP の最小リンク数の設定.....	148
9.13.6 MP のための負荷計測間隔の設定.....	148
9.13.7 MP のパケットを分割するか否かの設定.....	148
9.14 PPPoE 関連の設定.....	149
9.14.1 PPPoE で使用する LAN インタフェースの指定.....	149
9.14.2 アクセスコンセントレータ名の設定.....	149
9.14.3 セッションの自動接続の設定.....	149
9.14.4 セッションの自動切断の設定.....	150
9.14.5 PADI パケットの最大再送回数の設定.....	150
9.14.6 PADI パケットの再送時間の設定.....	150
9.14.7 PADR パケットの最大再送回数の設定.....	150
9.14.8 PADR パケットの再送時間の設定.....	151
9.14.9 PPPoE セッションの切断タイマの設定.....	151
9.14.10 サービス名の指定.....	151
9.14.11 TCP パケットの MSS の制限の有無とサイズの指定.....	152
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.....	152

9.14.13 認証失敗の最大回数を設定する.....	152
第 10 章 : DHCP の設定.....	154
10.1 DHCP サーバー・リレーエージェント機能.....	154
10.1.1 DHCP の動作の設定.....	154
10.1.2 RFC2131 対応動作の設定.....	155
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.....	156
10.1.4 DHCP スコープの定義.....	156
10.1.5 DHCP 予約アドレスの設定.....	158
10.1.6 DHCP アドレス割り当て動作の設定.....	159
10.1.7 DHCP 割り当て情報を元にした予約設定の生成.....	160
10.1.8 DHCP オプションの設定.....	161
10.1.9 DHCP リース情報の手動追加.....	162
10.1.10 DHCP リース情報の手動削除.....	163
10.1.11 DHCP サーバーの指定の設定.....	163
10.1.12 DHCP サーバーの選択方法の設定.....	163
10.1.13 DHCP BOOTREQUEST パケットの中継基準の設定.....	164
10.1.14 インターフェース毎の DHCP の動作の設定.....	164
10.2 DHCP クライアント機能.....	165
10.2.1 DHCP クライアントのホスト名の設定.....	165
10.2.2 DNS サーバーアドレスを取得するインタフェースの設定.....	165
10.2.3 要求する IP アドレスリース期間の設定.....	166
10.2.4 IP アドレス取得要求の再送回数と間隔の設定.....	166
10.2.5 DHCP クライアント ID オプションの設定.....	167
10.2.6 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.....	167
10.2.7 リンクダウンした時に情報を解放するか否かの設定.....	168
第 11 章 : ICMP の設定.....	170
11.1 IPv4 の設定.....	170
11.1.1 ICMP Echo Reply を送信するか否かの設定.....	170
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.....	170
11.1.3 ICMP Mask Reply を送信するか否かの設定.....	170
11.1.4 ICMP Parameter Problem を送信するか否かの設定.....	171
11.1.5 ICMP Redirect を送信するか否かの設定.....	171
11.1.6 ICMP Redirect 受信時の処理の設定.....	171
11.1.7 ICMP Time Exceeded を送信するか否かの設定.....	172
11.1.8 ICMP Timestamp Reply を送信するか否かの設定.....	172
11.1.9 ICMP Destination Unreachable を送信するか否かの設定.....	173
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.....	173
11.1.11 受信した ICMP のログを記録するか否かの設定.....	174
11.1.12 ステルス機能の設定.....	174
11.2 IPv6 の設定.....	174
11.2.1 ICMP Echo Reply を送信するか否かの設定.....	174
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.....	175
11.2.3 ICMP Parameter Problem を送信するか否かの設定.....	175
11.2.4 ICMP Redirect を送信するか否かの設定.....	175
11.2.5 ICMP Redirect 受信時の処理の設定.....	176
11.2.6 ICMP Time Exceeded を送信するか否かの設定.....	176
11.2.7 ICMP Destination Unreachable を送信するか否かの設定.....	177
11.2.8 受信した ICMP のログを記録するか否かの設定.....	177
11.2.9 ICMP Packet-Too-Big を送信するか否かの設定.....	178
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.....	178
11.2.11 ステルス機能の設定.....	178
第 12 章 : トンネリング.....	180
12.1 トンネルインターフェースの使用許可の設定.....	180
12.2 トンネルインターフェースの使用不許可の設定.....	180
12.3 トンネルインターフェースの種別の設定.....	181

12.4 トンネルインタフェースの IPv4 アドレスの設定	181
12.5 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	181
12.6 トンネルインターフェースの端点 IP アドレスの設定	182
12.7 トンネルの端点の名前の設定	182

第 13 章 : IPsec の設定.....184

13.1 IPsec の動作の設定	184
13.2 事前共有鍵の登録	185
13.3 IKE の鍵交換を始動するか否かの設定	185
13.4 設定が異なる場合に鍵交換を拒否するか否かの設定	186
13.5 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	187
13.6 鍵交換の再送回数と間隔の設定	187
13.7 相手側のセキュリティ・ゲートウェイの名前の設定	188
13.8 相手側セキュリティ・ゲートウェイの IP アドレスの設定	188
13.9 相手側の ID の設定	189
13.10 自分側のセキュリティ・ゲートウェイの名前の設定	190
13.11 自分側セキュリティ・ゲートウェイの IP アドレスの設定	190
13.12 自分側の ID の設定	191
13.13 IKE キープアライブ機能の設定	191
13.14 IKE キープアライブに関する SYSLOG を出力するか否かの設定	193
13.15 IKE が用いる暗号アルゴリズムの設定	193
13.16 受信した IKE パケットを蓄積するキューの長さの設定	194
13.17 IKE が用いるグループの設定	194
13.18 IKE が用いるハッシュアルゴリズムの設定	195
13.19 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	195
13.20 IKE ペイロードのタイプの設定	196
13.21 IKEv1 鍵交換タイプの設定	196
13.22 IKE の情報ペイロードを送信するか否かの設定	197
13.23 PFS を用いるか否かの設定	197
13.24 XAUTH の設定	198
13.25 XAUTH 認証に使用するユーザ ID の設定	198
13.26 XAUTH 認証に使用するユーザ ID の属性の設定	199
13.27 XAUTH 認証に使用するユーザグループの設定	199
13.28 XAUTH 認証に使用するユーザグループの属性の設定	200
13.29 XAUTH によるユーザ認証の設定	201
13.30 内部 IP アドレスプールの設定	201
13.31 IKE XAUTH Mode-Cfg メソッドの設定	202
13.32 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	202
13.33 IKE のログの種類の設定	203
13.34 ESP を UDP でカプセル化して送受信するか否かの設定	203
13.35 SA 関連の設定	204
13.35.1 SA の寿命の設定	204
13.35.2 SA のポリシーの定義	205
13.35.3 SA の手動更新	206
13.35.4 ダングリング SA の動作の設定	207
13.35.5 IPsec NAT トラバーサルを利用するための設定	208
13.35.6 SA の削除	208
13.36 トンネルインタフェース関連の設定	209
13.36.1 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	209
13.36.2 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	209
13.36.3 使用する SA のポリシーの設定	210
13.36.4 IPComp によるデータ圧縮の設定	210
13.36.5 トンネルテンプレートの設定	211
13.37 トランスポートモード関連の設定	212
13.37.1 トランスポートモードの定義	212
13.37.2 トランスポートモードのテンプレートの設定	213

第 14 章 : L2TP 機能の設定.....215

14.1 L2TP/IPsec を動作させるか否かの設定	215
------------------------------	-----

14.2 L2TP トンネル認証に関する設定.....	215
14.3 L2TP トンネルの切断タイマの設定.....	216
14.4 L2TP キープアライブの設定.....	216
14.5 L2TP キープアライブのログ設定.....	217
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.....	217
第 15 章 : PPTP 機能の設定.....	219
15.1 共通の設定.....	219
15.1.1 PPTP サーバーを動作させるか否かの設定.....	219
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フェースの設定.....	219
15.1.3 PPTP の動作タイプの設定.....	220
15.1.4 PPTP ホスト名の設定.....	220
15.1.5 PPTP ホスト名の設定.....	220
15.1.6 PPTP パケットのウィンドウサイズの設定.....	221
15.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定.....	221
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.....	221
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.....	222
15.2 リモートアクセス VPN 機能.....	222
15.2.1 PPTP トンネルの出力切断タイマの設定.....	222
15.2.2 PPTP キープアライブの設定.....	223
15.2.3 PPTP キープアライブのログ設定.....	223
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.....	223
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.....	224
第 16 章 : データコネクト接続機能の設定.....	225
16.1 NGN 網を介したトンネルインタフェースの切断タイマの設定.....	225
16.2 NGN 網を介したトンネルインタフェースの帯域の設定.....	225
16.3 NGN 網を介したトンネルインタフェースの着信許可の設定.....	226
16.4 NGN 網を介したトンネルインタフェースの発信許可の設定.....	226
16.5 NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定.....	226
16.6 NGN 網を介したトンネルインタ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.....	227
16.7 NGN 電話番号を RADIUS で認証するか否かの設定.....	227
16.8 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.....	228
16.9 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.....	228
16.10 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.....	229
16.11 NGN 網を介したリナンバリング発生時に LAN インタフェースを一時的にリンクダウンするか否かの設定.....	229
第 17 章 : SNMP の設定.....	231
17.1 SNMPv1 によるアクセスを許可するホストの設定.....	231
17.2 SNMPv1 の読み出し専用のコミュニティ名の設定.....	232
17.3 SNMPv1 の読み書き可能なコミュニティ名の設定.....	232
17.4 SNMPv1 トラップの送信先の設定.....	232
17.5 SNMPv1 トラップのコミュニティ名の設定.....	232
17.6 SNMPv2c によるアクセスを許可するホストの設定.....	233
17.7 SNMPv2c の読み出し専用のコミュニティ名の設定.....	233
17.8 SNMPv2c の読み書き可能なコミュニティ名の設定.....	234
17.9 SNMPv2c トラップの送信先の設定.....	234
17.10 SNMPv2c トラップのコミュニティ名の設定.....	234
17.11 SNMP エンジン ID の設定.....	235
17.12 SNMP コンテキスト名の設定.....	235
17.13 USM で管理するユーザの設定.....	235
17.14 SNMPv3 によるアクセスを許可するホストの設定.....	236
17.15 VACM で管理する MIB ビューファミリの設定.....	237
17.16 VACM で管理するアクセスポリシーの設定.....	237
17.17 SNMPv3 トラップの送信先の設定.....	238
17.18 SNMP 送信パケットの始点アドレスの設定.....	238
17.19 sysContact の設定.....	239

17.20 sysLocation の設定.....	239
17.21 sysName の設定.....	239
17.22 SNMP 標準トラップを送信するか否かの設定.....	240
17.23 SNMP の linkDown トラップの送信制御の設定.....	240
17.24 PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定.....	241
17.25 トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定.....	241
17.26 スイッチのインタフェースの情報を MIB2 の範囲で表示するか否かの設定.....	242
17.27 PP インタフェースのアドレスの強制表示の設定.....	242
17.28 LAN インタ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.....	242
17.29 電波強度トラップを送信するか否かの設定.....	243
17.30 スイッチへ静的に付与するインタフェース番号の設定.....	243
17.31 スイッチへ静的に付与するスイッチ番号の設定.....	244
17.32 スイッチの状態による SNMP トラップの条件の設定.....	244
17.33 スイッチで共通の SNMP トラップの条件の設定.....	245
第 18 章 : RADIUS の設定.....	247
18.1 RADIUS による認証を使用するか否かの設定.....	247
18.2 RADIUS によるアカウントを使用するか否かの設定.....	247
18.3 RADIUS サーバーの指定.....	248
18.4 RADIUS 認証サーバーの指定.....	248
18.5 RADIUS アカウントサーバーの指定.....	248
18.6 RADIUS 認証サーバーの UDP ポートの設定.....	249
18.7 RADIUS アカウントサーバーの UDP ポートの設定.....	249
18.8 RADIUS シークレットの設定.....	249
18.9 RADIUS 再送信パラメータの設定.....	250
第 19 章 : NAT 機能.....	251
19.1 インタフェースへの NAT ディスクリプタ適用の設定.....	251
19.2 NAT ディスクリプタの動作タイプの設定.....	251
19.3 NAT 処理の外側 IP アドレスの設定.....	252
19.4 NAT 処理の内側 IP アドレスの設定.....	253
19.5 静的 NAT エントリの設定.....	253
19.6 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.....	254
19.7 静的 IP マスカレードエントリの設定.....	254
19.8 NAT の IP アドレスマップの消去タイマの設定.....	255
19.9 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.....	256
19.10 IP マスカレードで利用するポートの範囲の設定.....	256
19.11 FTP として認識するポート番号の設定.....	257
19.12 IP マスカレードで変換しないポート番号の範囲の設定.....	257
19.13 NAT のアドレス割当をログに記録するか否かの設定.....	257
19.14 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.....	258
19.15 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.....	258
19.16 IP マスカレードで変換するセッション数の設定.....	258
第 20 章 : DNS の設定.....	260
20.1 DNS を利用するか否かの設定.....	260
20.2 ルーター自身の FQDN の設定.....	260
20.3 DNS サーバーの IP アドレスの設定.....	260
20.4 DNS ドメイン名の設定.....	261
20.5 DNS サーバーを通知してもらう相手先情報番号の設定.....	261
20.6 DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定.....	262
20.7 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.....	262
20.8 SYSLOG 表示で DNS により名前解決するか否かの設定.....	262
20.9 DNS 問い合わせの内容に応じた DNS サーバーの選択.....	263
20.10 静的 DNS レコードの登録.....	264
20.11 DNS 問い合わせパケットの始点ポート番号の設定.....	266
20.12 DNS サーバーへアクセスできるホストの IP アドレス設定.....	266
20.13 DNS キャッシュを使用するか否かの設定.....	266

20.14 DNS キャッシュの最大エントリ数の設定.....	267
20.15 DNS フォールバック機能を使用するか否かの設定.....	267
第 21 章 : 優先制御.....	269
21.1 インタフェース速度の設定.....	269
21.2 クラス分けのためのフィルタ設定.....	269
21.3 キューイングアルゴリズムタイプの選択.....	271
21.4 MP インタリーブの設定.....	272
21.5 クラス分けフィルタの適用.....	273
21.6 クラス毎のキュー長の設定.....	273
21.7 デフォルトクラスの設定.....	274
第 22 章 : 連携機能.....	275
22.1 連携動作を行うか否かの設定.....	275
22.2 連携動作で使用するポート番号の設定.....	275
22.3 帯域測定で連携動作を行う相手毎の動作の設定.....	275
22.4 負荷監視通知で連携動作を行う相手毎の動作の設定.....	277
22.5 負荷監視サーバーとしての動作トリガの設定.....	278
22.6 負荷監視クライアントとしての動作の設定.....	280
22.7 連携動作の手動実行.....	280
第 23 章 : IPv6.....	282
23.1 共通の設定.....	282
23.1.1 IPv6 パケットを扱うか否かの設定.....	282
23.1.2 IPv6 インタフェースのリンク MTU の設定.....	282
23.1.3 TCP セッションの MSS 制限の設定.....	282
23.1.4 TCP ウィンドウ・スケール・オプションを変更する.....	283
23.1.5 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.....	283
23.1.6 IPv6 ファストパス機能の設定.....	284
23.2 IPv6 アドレスの管理.....	284
23.2.1 インタフェースの IPv6 アドレスの設定.....	284
23.2.2 インタフェースのプレフィックスに基づく IPv6 アドレスの設定.....	286
23.2.3 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.....	287
23.2.4 DHCPv6 の動作の設定.....	288
23.2.5 DAD(Duplicate Address Detection) の送信回数設定.....	289
23.2.6 自動的に設定される IPv6 アドレスの最大数の設定.....	289
23.2.7 始点 IPv6 アドレスを選択する規則の設定.....	289
23.3 近隣探索.....	290
23.3.1 ルーター広告で配布するプレフィックスの定義.....	290
23.3.2 ルーター広告の送信の制御.....	292
23.4 経路制御.....	293
23.4.1 IPv6 の経路情報の追加.....	293
23.5 RIPng.....	294
23.5.1 RIPng の使用の設定.....	294
23.5.2 インタフェースにおける RIPng の送信ポリシーの設定.....	294
23.5.3 インタフェースにおける RIPng の受信ポリシーの設定.....	295
23.5.4 RIPng の加算ホップ数の設定.....	295
23.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定.....	296
23.5.6 RIPng で送受信する経路に対するフィルタリングの設定.....	296
23.5.7 回線接続時の PP 側の RIPng の動作の設定.....	297
23.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定.....	297
23.5.9 回線切断時の PP 側の RIPng の動作の設定.....	297
23.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定.....	298
23.5.11 RIPng による経路を回線切断時に保持するか否かの設定.....	298
23.5.12 RIPng による経路の優先度の設定.....	298
23.6 フィルタの設定.....	299
23.6.1 IPv6 フィルタの定義.....	299
23.6.2 IPv6 フィルタの適用.....	300

23.6.3 IPv6 動的フィルタの定義.....	300
23.7 IPv6 マルチキャストパケットの転送の設定.....	302
23.7.1 MLD の動作の設定.....	302
23.7.2 MLD の静的な設定.....	304
23.8 近隣要請.....	304
23.8.1 アドレス重複チェックをトリガに近隣要請を行うか否かの設定.....	304

第 24 章 : アナログ通信機能の設定.....306

24.1 キー操作とコンソールコマンドの対応.....	306
24.2 TEL ポートごとの設定.....	307
24.2.1 TEL ポートを使うか否かの設定.....	308
24.2.2 TEL ポートのダイヤルイン番号の設定.....	308
24.2.3 TEL ポートに接続する機器の設定.....	309
24.2.4 TEL ポートの発信者番号を通知するか否かの設定.....	309
24.2.5 相手先番号による即時発信を許可するか否かの設定.....	310
24.2.6 ダイヤル完了ボタンの設定.....	310
24.2.7 グローバル着信を許可するか否かの設定.....	311
24.2.8 TEL ポートでの識別着信をするか否かの設定.....	311
24.2.9 識別着信リストの登録.....	312
24.2.10 サブアドレス無し着信を許可するか否かの設定.....	313
24.2.11 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.....	313
24.2.12 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.....	314
24.2.13 話中着信を許可するか否かの設定.....	314
24.2.14 着信ベルリストの登録.....	315
24.2.15 ナンバー・ディスプレイの設定.....	316
24.2.16 指定した TEL ポートの優先着信順位を設定.....	316
24.2.17 ダイヤル桁間タイマの設定.....	317
24.2.18 フッキングを判定する時間の設定.....	317
24.2.19 フッキング後にキー操作を受け入れる時間の設定.....	317
24.2.20 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.....	318
24.2.21 オフフックを検出するまでの遅延時間の設定.....	318
24.2.22 オフフック/オンフックを検出する閾値の設定.....	319
24.2.23 インピーダンスの設定.....	319
24.2.24 保留音の種類の設定.....	320
24.2.25 TEL ポートの再呼出時間設定.....	320
24.2.26 フレックスホン機能の使用パターンの設定.....	321
24.2.27 着信転送先アドレスの設定.....	321
24.2.28 着信転送を起動するタイミングの設定.....	322
24.2.29 着信転送トーカーの設定.....	322
24.2.30 着信転送が拒否された時の動作の設定.....	323
24.2.31 送話 PAD の設定.....	324
24.2.32 受話 PAD の設定.....	324
24.2.33 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.....	325
24.2.34 TEL ポートへの切断信号の送付の設定.....	325
24.2.35 DTMF 検出レベルの設定.....	326
24.2.36 アザーダイヤルトーンを出すか否かの設定.....	327
24.2.37 着信時の着信ベル鳴動モードの設定.....	327
24.2.38 緊急番号の処理方式の設定.....	327
24.2.39 i・ナンバーサービスのポート番号の設定.....	328
24.2.40 アナログダイヤルインと無鳴動着信機能の設定.....	328
24.2.41 PB ダイヤルインの一次応答検出タイミングの設定.....	330
24.2.42 発番号情報なし着信機能の設定.....	330
24.2.43 RTP 音声の受話 PAD の設定.....	331
24.2.44 RTP 音声の送話 PAD の設定.....	332
24.2.45 ポーズを判定する時間の設定.....	332
24.2.46 TEL ポートに対する電力供給の設定.....	333
24.3 アナログ回線の設定.....	333
24.3.1 ダイヤルの種別を選択.....	333
24.3.2 フッキング時間の設定.....	334
24.3.3 アナログ回線のモデム信号を検出するまでの時間を設定する.....	334

24.3.4 ナンバー・ディスプレイ(ダイヤルイン)の着信の識別設定.....	334
24.3.5 アナログ回線に対する受話 PAD の設定.....	334
24.3.6 アナログ回線に対する送話 PAD の設定.....	335
24.3.7 アナログ回線に対するポーズ時間の設定.....	335
24.3.8 付加サービス機能の設定.....	336
24.3.9 アナログ回線を使用するか否かの設定.....	336
24.3.10 アナログ回線で検出する呼出信号の周波数範囲の設定.....	336
24.3.11 鳴動時間により呼出信号の種別を判定する閾値の設定.....	337

第 25 章 : カスケード接続機能の設定.....338

25.1 カスケード接続モードの設定.....	338
25.2 カスケード接続に利用する IP アドレス取得インタフェースの設定.....	338
25.3 アナログ親機となる機器の設定.....	339
25.4 アナログ子機受け入れモードの設定.....	339
25.5 アナログ子機受け入れモードの設定.....	340
25.6 カスケード接続のログを記録するか否かの設定.....	340

第 26 章 : VoIP 機能の設定.....341

26.1 共通の設定.....	341
26.1.1 SIP による VoIP 機能を使用するか否かの設定.....	341
26.1.2 SIP による発信時に使用する IP プロトコルの選択.....	341
26.1.3 SIP による VoIP 機能で利用可能な音声コーデックの設定.....	341
26.1.4 SIP のリクエスト再送タイムアウト値の設定.....	342
26.1.5 ネットボランチ電話で使用するドメイン名の設定.....	343
26.1.6 ネットボランチ電話で SIP ユーザ名として付与する番号桁数の設定.....	343
26.1.7 特定のダイヤルに対応する SIP による発信先の設定.....	343
26.1.8 SIP の session-timer 機能のタイマ値の設定.....	344
26.1.9 SIP による発信時に 100rel をサポートするか否かの設定.....	345
26.1.10 送信する SIP パケットに User-Agent ヘッダを付加する設定.....	345
26.1.11 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.....	346
26.1.12 SIP による着信時の INVITE に refresher 指定がない場合の設定.....	346
26.1.13 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.....	346
26.1.14 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.....	347
26.1.15 着信時のセッションタイマーのリクエストを設定.....	347
26.1.16 SIP 着信時に user 名を検証するかどうかの設定.....	348
26.1.17 SIP で使用する IP アドレスの設定.....	348
26.1.18 SIP メッセージのログを記録するか否かの設定.....	348
26.2 SIP サーバー毎の設定.....	349
26.2.1 SIP サーバーの設定.....	349
26.2.2 SIP サーバー毎の先頭に付加された 184/186 の扱いの設定.....	349
26.2.3 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.....	350
26.2.4 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.....	351
26.2.5 SIP サーバー毎の session-timer 機能のタイマ値の設定.....	351
26.2.6 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.....	352
26.2.7 SIP サーバー毎の REGISTER リクエストの更新間隔の設定.....	352
26.2.8 SIP サーバー毎の REGISTER リクエストの Request-URI の設定.....	352
26.2.9 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.....	353
26.2.10 SIP サーバー毎の着信時の発番号情報通知ルールの設定.....	353
26.2.11 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.....	354
26.2.12 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.....	354
26.2.13 SIP サーバへの発信に番号以外を使えないように制限する設定.....	355
26.2.14 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.....	355
26.2.15 SIP サーバー毎の代表 SIP アドレスの設定.....	356
26.2.16 発信時の 5xx エラーをサーバー障害とするか否かの設定.....	356
26.3 TEL ポートの設定.....	357
26.3.1 TEL ポートからの SIP による発信の制限の設定.....	357
26.3.2 TEL ポートからの SIP による発信で使用する自己 SIP ユーザ名の設定.....	357
26.3.3 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.....	357
26.3.4 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.....	358

26.3.5 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	359
26.3.6 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	359
26.3.7 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	360
26.4 電話番号ルーティングの設定	362
26.4.1 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	362
26.4.2 ダイヤル番号と発呼経路との関連付けの設定	363
26.5 ひかり電話の設定	364
26.5.1 NGN 網に接続するインタフェースの設定	364
26.5.2 NGN 網接続情報の表示	365
第 27 章 : トリガによるメール通知機能	366
27.1 メール設定識別名の設定	366
27.2 SMTP メールサーバーの設定	366
27.3 POP メールサーバーの設定	367
27.4 メール処理のタイムアウト値の設定	367
27.5 メールの送信時に使用するテンプレートの設定	368
27.6 メール通知のトリガの設定	369
第 28 章 : HTTP サーバー機能	372
28.1 共通の設定	372
28.1.1 HTTP サーバー機能の有無の設定	372
28.1.2 HTTP サーバーへアクセスできるホストの IP アドレス設定	372
28.1.3 HTTP サーバーのセッションタイムアウト時間の設定	373
28.1.4 HTTP サーバー機能の listen ポートの設定	373
28.1.5 PP インタフェースとトンネルインタフェースの名前の設定	373
28.2 かんたん設定ページ用の設定	373
28.2.1 プロバイダ接続タイプの設定	374
28.2.2 プロバイダ情報の PP との関連付けと名前の設定	374
28.2.3 プロバイダ接続設定	375
28.2.4 プロバイダの DNS サーバーのアドレス設定	375
28.2.5 LAN インタフェースの DNS サーバーのアドレスの設定	376
28.2.6 DNS サーバーを通知してくれる相手の相手先情報番号の設定	376
28.2.7 フィルタ型ルーティングの形式の設定	376
28.2.8 LAN 側のプロバイダ名称の設定	377
28.2.9 プロバイダに対する昼間課金単位時間の設定	377
28.2.10 プロバイダに対する昼間課金単位時間方式での単位時間と監視時間の設定	378
28.2.11 プロバイダに対する夜間課金単位時間の設定	378
28.2.12 プロバイダに対する夜間課金単位時間方式での単位時間と監視時間の設定	379
28.2.13 プロバイダに対する自動切断タイマ無効時間の設定	379
28.2.14 プロバイダに対する夜間料金時間の設定	380
28.2.15 NTP サーバーの設定	380
28.2.16 プロバイダの NTP サーバーのアドレス設定	381
28.2.17 MP 使用時間帯の設定	381
28.2.18 かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定	381
28.2.19 かんたん設定ページで IPv6 接続を行うか否かの設定	382
28.2.20 電話アドレスの設定	382
28.2.21 プロバイダ情報とトンネルとの関連付け	382
28.2.22 LAN インタフェースのプロバイダ情報とトンネルとの関連付け	383
第 29 章 : ネットボランチ DNS サービスの設定	384
29.1 ネットボランチ DNS サービスの使用の可否	384
29.2 ネットボランチ DNS サーバーへの手動更新	384
29.3 ネットボランチ DNS サーバーからの削除	385
29.4 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	385
29.5 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	385
29.6 ホスト名の登録	386
29.7 通信タイムアウトの設定	386
29.8 ホスト名を自動生成するか否かの設定	387

29.9 NetVolante インターネット電話用ホスト名の使用の可否.....	387
29.10 シリアル番号を使ったホスト名登録コマンドの設定.....	388
29.11 ネットボランチ DNS サーバーの設定.....	388
29.12 ネットボランチ DNS サーバアドレス更新機能の ON/OFF の設定.....	388
29.13 ネットボランチ DNS サーバアドレス更新機能のポート番号の設定.....	389
29.14 自動更新に失敗した場合のリトライ間隔と回数設定.....	389
29.15 ネットボランチ DNS 登録の定期更新間隔の設定.....	390
29.16 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.....	390
第 30 章 : UPnP の設定.....	392
30.1 UPnP を使用するかどうかの設定.....	392
30.2 UPnP に使用する IP アドレスを取得するインタフェースの設定.....	392
30.3 UPnP のポートマッピング用消去タイマのタイプの設定.....	392
30.4 UPnP のポートマッピングの消去タイマの設定.....	393
30.5 UPnP の syslog を出力するかどうかの設定.....	393
第 31 章 : スケジュール.....	395
31.1 スケジュールの設定.....	395
第 32 章 : VLAN の設定.....	398
32.1 VLAN ID の設定.....	398
第 33 章 : SNTP サーバー機能.....	399
33.1 SNTP サーバー機能を有効にするかどうかの設定.....	399
33.2 SNTP サーバーへのアクセスを許可するホストの設定.....	399
第 34 章 : 外部メモリ機能.....	401
34.1 USB ホスト機能を使うかどうかの設定.....	401
34.2 USB バスで過電流保護機能が働くまでの時間の設定.....	402
34.3 microSD カードスロットを使うかどうかの設定.....	402
34.4 外部メモリ用キャッシュメモリの動作モードの設定.....	402
34.5 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.....	403
34.6 外部メモリに保存する SYSLOG ファイル名の指定.....	404
34.7 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どうかの設定.....	406
34.8 外部メモリ内のファイルからの起動を許可するかどうかの設定.....	406
34.9 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.....	406
34.10 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.....	407
34.11 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、設定フ ァイル名の指定.....	408
34.12 ファイル検索時のタイムアウトを設定する.....	409
34.13 バッチファイルを実行する.....	409
34.14 バッチファイルと実行結果ファイルの設定.....	410
34.15 外部メモリ性能測定コマンド.....	410
34.16 DOWNLOAD ボタンを押した時に実行する機能の設定.....	411
34.17 DOWNLOAD ボタンによるバッチファイルの実行を許可するかどうかの設定.....	412
第 35 章 : モバイルインターネット接続機能.....	413
35.1 携帯端末を使用するかどうかの設定.....	413
35.2 携帯端末に入力する PIN コードの設定.....	414
35.3 携帯端末に直接コマンドを発行する.....	414
35.4 指定した相手に対して発信制限を解除する.....	415
35.5 PP で使用するインタフェースの設定.....	415
35.6 携帯端末からの自動発信設定.....	416

35.7 携帯端末を切断するタイマの設定.....	416
35.8 携帯端末を入力がないときに切断するタイマの設定.....	416
35.9 携帯端末を出力がないときに切断するタイマの設定.....	417
35.10 発信先アクセスポイントの設定.....	417
35.11 携帯端末に指示する発信先の設定.....	417
35.12 パケット通信量制限の設定.....	418
35.13 パケット通信時間制限の設定.....	419
35.14 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.....	420
35.15 LCP の Async Control Character Map オプション使用の設定.....	420
35.16 発信者番号通知 (186) を付加するかどうかの設定.....	420
35.17 詳細な SYSLOG を出力するか否かの設定.....	421
35.18 接続毎パケット通信量制限の設定.....	421
35.19 接続毎パケット通信時間制限の設定.....	422
35.20 通信制限の累積期間の設定.....	422
35.21 携帯端末でパケット着信機能を使用するか否かの設定.....	423
35.22 モバイルインターネット機能の着信許可の設定.....	423
35.23 電波の受信レベルの取得.....	424
35.24 電波の受信レベル取得機能の設定.....	424
35.25 定期実行で取得した電波の受信レベルの表示.....	425
35.26 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.....	425
35.27 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.....	426
35.28 携帯端末のファームウェア更新.....	426
35.29 携帯端末のネットワーク事業者モードの設定.....	427
35.30 自分の名前とパスワードの設定.....	428
35.31 WAN で使用するインタフェースの設定.....	428
35.32 携帯端末からの自動発信設定.....	429
35.33 携帯端末を切断するタイマの設定.....	429
35.34 携帯端末を入力がないときに切断するタイマの設定.....	430
35.35 携帯端末を出力がないときに切断するタイマの設定.....	430
35.36 常時接続の設定.....	430
35.37 発信先アクセスポイントの設定.....	431
35.38 パケット通信量制限の設定.....	432
35.39 パケット通信時間制限の設定.....	433
35.40 接続毎パケット通信量制限の設定.....	434
35.41 接続毎パケット通信時間制限の設定.....	434
35.42 通信制限の累積期間の設定.....	435
第 36 章 : Lua スクリプト機能.....	436
36.1 Lua スクリプト機能を有効にするか否かの設定.....	436
36.2 Lua スクリプトの実行.....	436
36.3 Lua コンパイラの実行.....	437
36.4 Lua スクリプトの走行状態の表示.....	437
36.5 Lua スクリプトの強制終了.....	438
36.6 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.....	439
第 37 章 : カスタム GUI.....	440
37.1 カスタム GUI を使用するか否かの設定.....	440
37.2 カスタム GUI を使用するユーザの設定.....	440
37.3 カスタム GUI の API を使用するか否かの設定.....	441
37.4 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.....	441
第 38 章 : ONFS.....	442
38.1 ONFS ファイルシステム.....	442
38.1.1 ONFS で使用する外部ストレージを接続するインタフェースの設定.....	442
38.1.2 ONFS で使用する外部ストレージの初期設定 / ONFS の再起動.....	442
38.1.3 ONFS の動作状態の表示.....	443
38.2 ONFS ファイル共有.....	444
38.2.1 ファイル共有機能の設定.....	444

38.2.2	ファイル共有機能を使用できるホストの IP アドレス設定	445
38.2.3	ファイル共有機能を利用するユーザーの設定	445
38.2.4	ファイル共有機能を利用するグループの設定	446
38.2.5	ファイル共有機能のアクセス制御を有効にするか否かの設定	447
38.2.6	ファイル共有機能の ACL の設定	447
38.2.7	ファイル共有機能の ACL の消去	449
38.2.8	ファイル共有機能の ACL の表示	449
38.3	ONFS ミラーリング	450
38.3.1	ONFS ミラーリング機能の使用設定	450
38.3.2	ONFS ミラーリング機能の自拠点設定	450
38.3.3	ONFS ミラーリンググループに参加するためのコンタクトノード設定	451
38.3.4	ONFS ミラーリンググループへの参加認証に使用する事前共有鍵の設定	452
38.3.5	ONFS ミラーリングのファイル同期機能を手動実行	452

第 39 章 : スイッチ制御機能.....453

39.1	共通の設定	453
39.1.1	スイッチ制御機能を使用するか否かの設定	453
39.1.2	スイッチの監視時間間隔の設定	454
39.2	スイッチの制御	454
39.2.1	スイッチの選択	454
39.2.2	スイッチが持つ機能の設定	455
39.2.3	スイッチが持つ機能の設定内容や動作状態の取得	455
39.2.4	スイッチに対して特定の動作を実行	455
39.2.5	スイッチの設定の削除	456
39.2.6	スイッチのファームウェアの更新	456
39.2.7	LAN ケーブル二重化機能の設定	457
39.3	スイッチの機能	458
39.3.1	システム	458
39.3.2	ポート	462
39.3.3	MAC アドレステーブル	468
39.3.4	VLAN	470
39.3.5	QoS	474
39.3.6	ミラーリング	478
39.3.7	カウンタ	481
39.3.8	ループ検出	486
39.3.9	PoE 給電	490
39.4	アクセスポイントの制御	494
39.4.1	アクセスポイントの選択	494
39.4.2	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	494
39.4.3	アクセスポイントの設定を保存するファイル名の指定	495
39.4.4	アクセスポイントの設定のバックアップ実行	495
39.4.5	アクセスポイントの設定の復元実行	496
39.4.6	アクセスポイントの設定の削除	496
39.4.7	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	496
39.4.8	アクセスポイントの HTTP リビジョンアップ機能の実行	497
39.4.9	アクセスポイント制御用の HTTP プロキシの使用	497
39.4.10	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	498

第 40 章 : 操作.....499

40.1	相手先情報番号の選択	499
40.2	トンネルインタフェース番号の選択	499
40.3	設定に関する操作	499
40.3.1	管理ユーザへの移行	500
40.3.2	終了	500
40.3.3	設定内容の保存	500
40.3.4	設定ファイルの複製	501
40.3.5	ファームウェアファイルを内蔵フラッシュ ROM にコピー	502
40.3.6	設定ファイルの削除	503
40.3.7	設定の初期化	504

40.3.8 遠隔地のルーターの設定.....	504
40.3.9 遠隔地のルーターからの設定に対する制限.....	504
40.4 動的情報のクリア操作.....	505
40.4.1 アカウントのクリア.....	505
40.4.2 TEL ポートに関するアカウントのクリア.....	505
40.4.3 ARP テーブルのクリア.....	506
40.4.4 IP の動的経路情報のクリア.....	506
40.4.5 ログのクリア.....	506
40.4.6 DNS キャッシュのクリア.....	506
40.4.7 インタフェースのカウンター情報のクリア.....	506
40.4.8 NAT アドレステーブルのクリア.....	507
40.4.9 インタフェースの NAT アドレステーブルのクリア.....	507
40.4.10 IPv6 の動的経路情報の消去.....	508
40.4.11 近隣キャッシュの消去.....	508
40.4.12 起動情報の履歴を削除する.....	508
40.4.13 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.....	508
40.5 ファイル、ディレクトリの操作.....	508
40.5.1 ディレクトリの作成.....	508
40.5.2 ファイルまたはディレクトリの削除.....	509
40.5.3 ファイルまたはディレクトリの複製.....	509
40.5.4 ファイル名またはディレクトリ名の変更.....	510
40.6 その他の操作.....	510
40.6.1 相手先の使用許可の設定.....	510
40.6.2 相手先の使用不許可の設定.....	510
40.6.3 再起動.....	511
40.6.4 インタフェースの再起動.....	511
40.6.5 PP インタフェースの再起動.....	512
40.6.6 発信.....	512
40.6.7 切断.....	513
40.6.8 ping.....	513
40.6.9 ping6 の実行.....	514
40.6.10 traceroute.....	515
40.6.11 traceroute6 の実行.....	515
40.6.12 nslookup.....	516
40.6.13 SIP サーバーに対し手動で接続.....	516
40.6.14 SIP サーバーに対し手動で切断.....	516
40.6.15 IPv4 動的フィルタのコネクション管理情報の削除.....	516
40.6.16 IPv6 動的フィルタのコネクション管理情報の削除.....	517
40.6.17 TELNET クライアント.....	517
40.6.18 スイッチングハブ MAC アドレステーブルの消去.....	518
40.6.19 Magic Packet の送信.....	518
40.6.20 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.....	519
40.6.21 メール通知の実行.....	520
40.6.22 累積課金情報のメール通知の実行.....	520
40.6.23 SSL 公開鍵の生成.....	520
40.6.24 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).....	520

第 41 章 : 設定の表示.....522

41.1 機器設定の表示.....	522
41.2 すべての設定内容の表示.....	522
41.3 指定した AP の設定内容の表示.....	522
41.4 指定した PP の設定内容の表示.....	522
41.5 指定したスイッチの設定内容の表示.....	523
41.6 指定したトンネルの設定内容の表示.....	523
41.7 設定ファイルの一覧.....	523
41.8 アナログ親機に登録された各 TEL ポート設定内容の表示.....	524
41.9 ファイル情報の一覧の表示.....	524
41.10 インタフェースに付与されている IPv6 アドレスの表示.....	524
41.11 SSH サーバー公開鍵の表示.....	525
41.12 SSL サーバー公開鍵の表示.....	526

41.13 指定したインタフェースのフィルタ内容の表示.....	526
41.14 ファームウェアファイルの一覧.....	526
第 42 章 : 状態の表示.....	527
42.1 ARP テーブルの表示.....	527
42.2 インタフェースの状態の表示.....	527
42.3 各相手先の状態の表示.....	527
42.4 IP の経路情報テーブルの表示.....	528
42.5 RIP で得られた経路情報の表示.....	528
42.6 IPv6 の経路情報の表示.....	528
42.7 IPv6 の RIP テーブルの表示.....	529
42.8 近隣キャッシュの表示.....	529
42.9 IPsec の SA の表示.....	529
42.10 動的 NAT ディスクリプタのアドレスマップの表示.....	530
42.11 動作中の NAT ディスクリプタの適用リストの表示.....	530
42.12 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示.....	530
42.13 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.....	531
42.14 L2TP の状態の表示.....	531
42.15 PPTP の状態の表示.....	531
42.16 DHCP サーバーの状態の表示.....	531
42.17 DHCP クライアントの状態の表示.....	532
42.18 DHCPv6 の状態の表示.....	532
42.19 動的フィルタによって管理されている接続の表示.....	532
42.20 IPv6 の動的フィルタによって管理されている接続の表示.....	533
42.21 ネットワーク監視機能の状態の表示.....	534
42.22 侵入情報の履歴の表示.....	534
42.23 相手先ごとの接続時間情報の表示.....	534
42.24 ネットボランチ DNS サービスに関する設定の表示.....	535
42.25 スイッチングハブ MAC アドレステーブルの表示.....	535
42.26 UPnP に関するステータス情報の表示.....	535
42.27 トンネルインタフェースの状態の表示.....	536
42.28 VLAN インタフェースの状態の表示.....	536
42.29 トリガによるメール通知機能の状態の表示.....	536
42.30 MLD のグループ管理情報の表示.....	537
42.31 IPv6 マルチキャストの経路情報の表示.....	537
42.32 ログインしているユーザ情報の表示.....	537
42.33 パケットバッファの状態の表示.....	538
42.34 QoS ステータスの表示.....	539
42.35 連携動作の状態の表示.....	539
42.36 リモートセットアップ機能に関する接続情報の表示.....	540
42.37 技術情報の表示.....	540
42.38 USB ホスト機能の動作状態を表示.....	540
42.39 microSD スロットの動作状態を表示.....	541
42.40 外部メモリの動作状態を表示.....	541
42.41 RTFS の状態の表示.....	541
42.42 ルーターへのサインイン状態の表示.....	542
42.43 SIP サーバーとの接続状態の表示.....	542
42.44 アナログ関係の状態の表示.....	542
42.45 音声通話の接続状態の表示.....	543
42.46 音声の処理状態の表示.....	543
42.47 カスケード接続の状態表示.....	543
42.48 起動情報を表示する.....	543
42.49 起動情報の履歴の詳細を表示する.....	543
42.50 起動情報の履歴の一覧を表示する.....	543
42.51 ルーターが制御しているスイッチ一覧の表示.....	544
42.52 LAN ケーブル二重化機能の動作状態を表示.....	545
42.53 DNS キャッシュの表示.....	545
42.54 WAN LED の情報の表示.....	545
42.55 上面スイッチの状態の表示.....	545
42.56 コピーライトの表示.....	546

第 43 章 : ログイング	547
43.1 ログの表示.....	547
43.2 アカウントの表示.....	547
43.3 アナログ関係のアカウントの表示.....	548
43.4 アナログ回線のアカウントの表示.....	549
43.5 SIP のアカウントの表示.....	549
43.6 ひかり電話のアカウントの表示.....	549
43.7 データコネクタのアカウントの表示.....	549
43.8 モバイル回線のアカウントの表示.....	549
43.9 通信履歴の表示.....	549
索引	550

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ます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、NVR500 のファームウェア、Rev.11.00.43 に対応しています。
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 (Bold face) で示します。
	パラメータ部分は斜体 (<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フェースを指定するためにインタフェース名を利用します。インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、"lan"、"bri" があります。

例

インタフェースの種類	インタフェース名
LAN、WAN	lan1, lan2
BRI	bri1

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

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

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多い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が記載されていることがあります。これらは、パラメータ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 line
analog extension dial prefix sip prefix="9#"
```

Rev.11.00.38 以降では **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

NVR500 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、必要なコマンド一式を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。必要なコマンド一式を記述したファイルを設定ファイル (Config) と呼び、TFTP により NVR500 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。

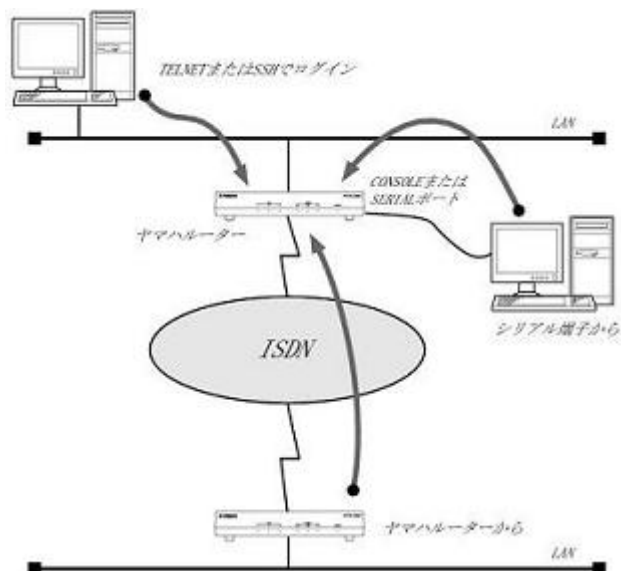
2.1 コンソールについて

各種の設定を行うためには、NVR500 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、ISDN 回線や専用線を介して別のヤマハルーターからログインする方法の3つがあります。

NVR500 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
ISDN 回線や専用線を介して別のヤマハルーターからログイン

NVR500 へは、それぞれに対して1ユーザ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になれるのは同時に1ユーザだけです。例えば、シリアル端末でアクセスしているユーザが管理ユーザとして設定を行っている場合には、別のユーザが一般ユーザとしてアクセスすることはできても管理ユーザになって設定を行うことはできません。

TELNET または SSH による同時アクセスが最大8ユーザまで可能です。また複数のユーザが同時に管理ユーザになることができ、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、各ユーザは現在アクセスしている全ユーザのアクセス状況を確認することができ、管理ユーザならば他のユーザ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 NVR500 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ある一定時間無き時には、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。

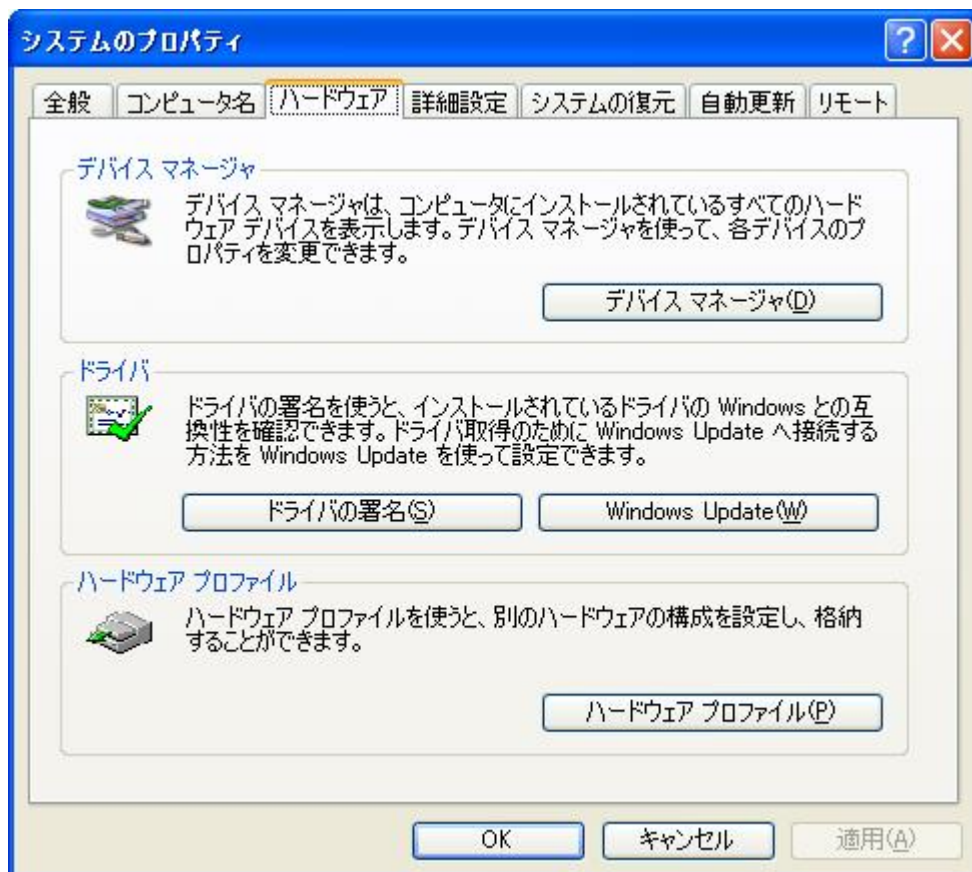
 **注意:** ご購入直後の起動や `cold start` 後にはログインパスワードも管理パスワードも設定されていません。セキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。

- NVR500 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

ここでは、Windows XP の『ハイパーターミナル』を使用する場合を例に説明します。シリアルケーブルの接続は事前にすませておきます。

1. [スタート]メニューから[マイコンピュータ]を選び、「システムのタスク」欄にある「システム情報を表示する」を選びます。「システムのプロパティ」ウィンドウが開いたら、[ハードウェア]タブを押します。



2. [デバイスマネージャ]をクリックします。

「ポート (COM と LPT)」アイコンをダブルクリックして開き、「通信ポート」の「COMx」という表現部分を調べます。通常は「COM1」の場合が多いでしょう。この COM ポート番号は、手順 5 で必要になるために覚えておきます。



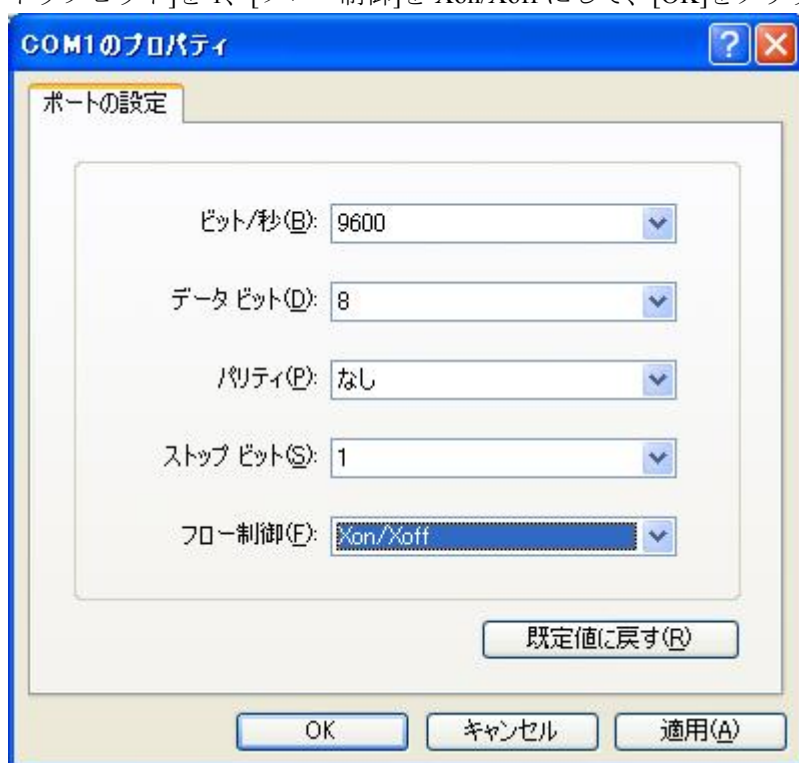
3. 「デバイスマネージャ」ウィンドウを閉じます。
4. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[通信]-[ハイパーターミナル]を選びます。「接続の設定」ウィンドウが開いたら、名前欄に適切な名前を入力して[OK]をクリックします。



5. 「接続方法」欄から、手順 2 で調べた COM ポートを選択して[OK]をクリックします。



6. 「COMx のプロパティ」ウィンドウが開いたら、[ビット/秒]を 9600、[データビット]を 8、[パリティ]をなし、[ストップビット]を 1、[フロー制御]を Xon/Xoff にして、[OK]をクリックします。



7. 「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。

※TELNET 複数セッション機能対応機種で設定した名前ありユーザ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、ユーザ名の入力待ち状態となります。ここで、設定したユーザ名を入力して Enter キーを押し、続いてユーザ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。

以下の例は、NVR500 にログインした場合の表示です。

```

test - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)

Password:
NVR500 BootROM Ver. 0.08
NVR500 FlashROM Table Ver. 0.03

NVR500 Rev.11.00.00 (build 15) (Fri Jul 16 11:28:38 2010)
Copyright (c) 1994-2010 Yamaha Corporation. All Rights Reserved.
Copyright (c) 1995-2004 Jean-loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIK
U.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2004 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights r
eserved.
Copyright (c) 1995 Iatu Ylonen , Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (C) 1994-2008 Lua.org, PUC-Rio.
00:a0:de:00:00:01, 00:a0:de:00:00:02
Memory 64Mbytes, 2LAN, 1BRI
> _

```

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。

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

9. 「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。

10. コンソールコマンドを入力して、設定を行います

11. 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。

12. 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。

13. 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。

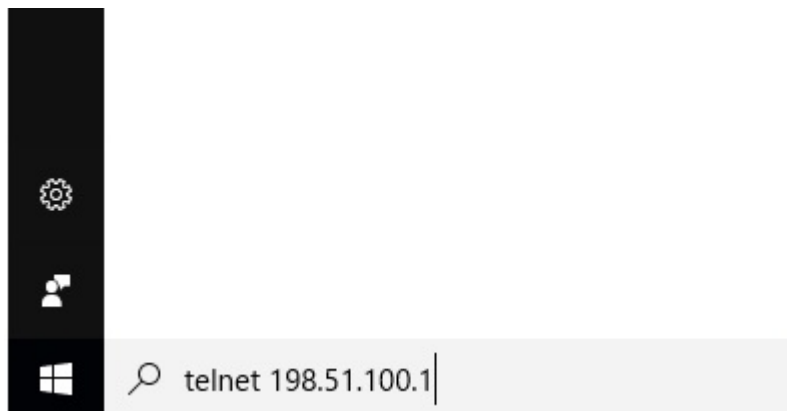
2.1.3 TELNET による設定

ここでは、Windows の TELNET を使用する場合を例に説明します。NVR500 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。

```

Telnet 198.51.100.1
Password:
NVR500 BootROM Ver. 1.02
NVR500 FlashROM Table Ver. 1.00

NVR500 Rev.11.00.42 (Tue Jul 21 11:28:20 2020)
Copyright (c) 1994-2020 Yamaha Corporation. All Rights Reserved.
To display the software copyright statement, use 'show copyright' command.
00:a0:de:00:00:00, 00:a0:de:00:00:01
Memory 64Mbytes, 2LAN, 1BRI

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
>

```

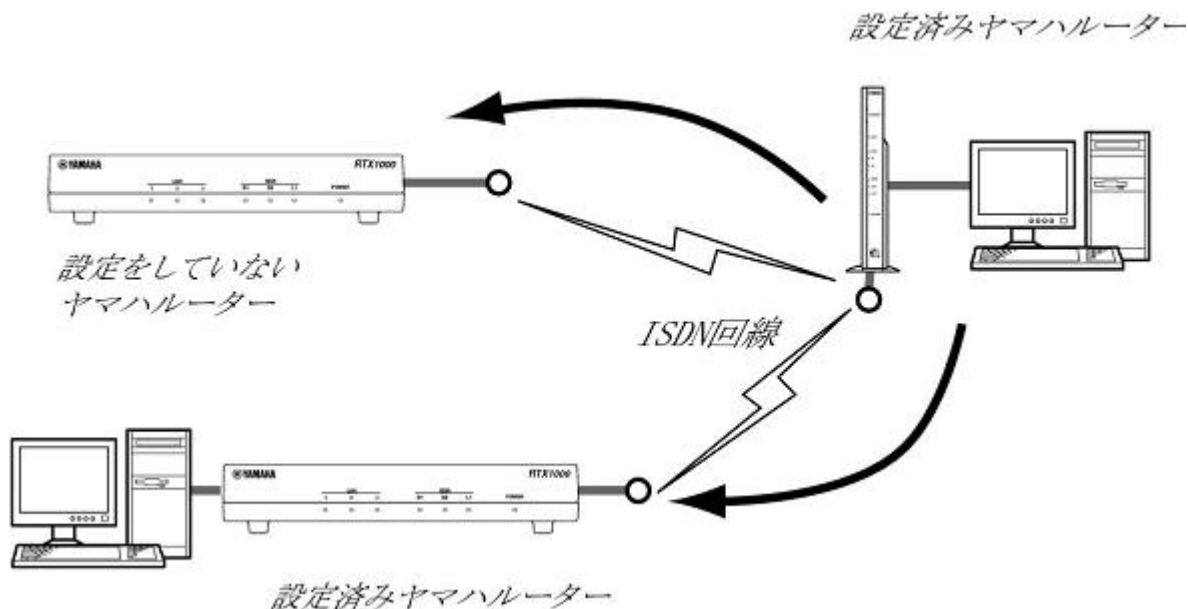
注:

- **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。

2.1.4 リモートセットアップ

すでにヤマハルーターをお使いの場合は、離れた場所の NVR500 でも ISDN 回線や専用線経由で設定できます。これを「リモートセットアップ」といいます。パスワードが設定された NVR500 であれば、リモートセットアップで設定することが可能です。ISDN 回線や専用線経由で相手の NVR500 に直接接続するので、プロバイダに契約していなくても、インターネット接続できない状態でも設定できます。



リモートセットアップを拒否するように設定できるため、拒否に設定しておけば、不特定の相手からの侵入を防げます。

リモートセットアップはコンソールから行います。コンソールを使う方法は、前節の「CONSOLE ポートからの設定」または「TELNET による設定」を参照してください。リモートセットアップのコマンドは **remote setup** です。相手の NVR500 へのログインが完了すると、コンソールコマンドで設定できるようになります。



注意：

- ヤマハルーター以外のルーターからリモートセットアップすることはできません。
- FTTH や CATV、ADSL などの WAN ポート経由で、リモートセットアップすることはできません。

2.2 SSH サーバーについて

NVR500 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

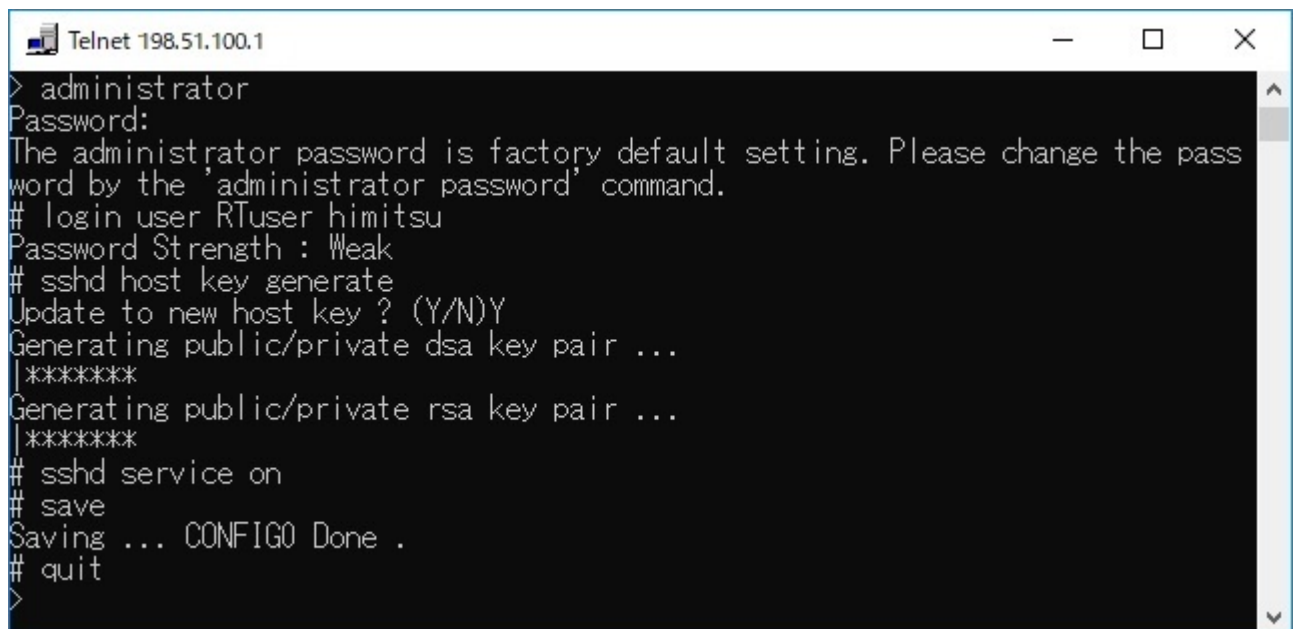
SSH サーバー機能では以下の機能をサポートしていないことに注意してください。

- 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)
- 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
- scp (Rev.11.00.23 以降では使用可能)

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を登録します。SSH ではログイン時のユーザ名の入力が必要となるため、事前に必ず名前ありユーザ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

NVR500 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、NVR500 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。

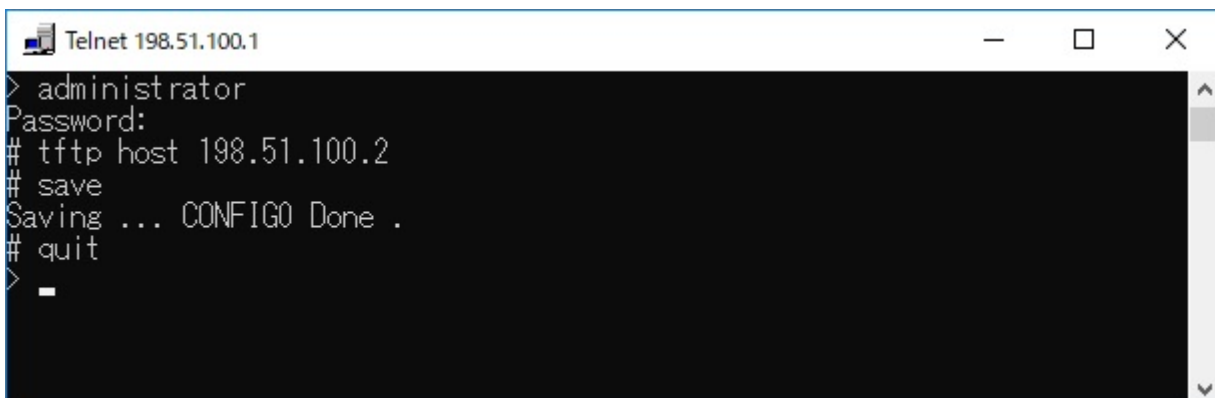


注意：

- 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。
- TFTP により設定ファイルを読み込む場合において **line type** コマンドの設定変更を行う場合は、設定の最後に **restart** コマンドが必要なことに注意してください。

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、NVR500 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。NVR500 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、NVR500 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。

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. **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

```

CAL 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。NVR500 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、NVR500 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. **tftp 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、

tftp -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。


```

C:\>cd YAMAHA
C:\YAMAHA>tftp 198.51.100.1 put NEWconfig.txt config/himitsu
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>

```

2.4 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	
{n} b	{n} 画面後ろに戻す
{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	

キーボード操作	説明・備考
{n} k	{n}行後ろに戻る
{n} Ctrl-K	
{n} y	
{n} Ctrl-Y	
{n} Ctrl-P	
{n} d	{n}半画面先に進める
{n} Ctrl-D	
{n} u	{n}半画面後ろに戻る
{n} Ctrl-U	
{n} g	{n}行目へ移動
	{n}省略時は先頭行
{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
```

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。数値プレフィクスはオプションで省略できる。数値プレフィ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 grep 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 grep コマンドと同じものである。
n	最後に入力された /、あるいは ? 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 /、あるいは ? と同じ検索パターンで逆方向に検索する。

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 ポート 1 に接続された USB メモリ内のファイル (filename は半角 99 文字以内)
usb2:filename	USB ポート 2 に接続された USB メモリ内のファイル (filename は半角 99 文字以内)
sd1:filename	microSD カード内のファイル (filename は半角 99 文字以内)

- [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)
```

[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。

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

[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
```

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。

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。

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]

一般ユーザ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)。

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。

4.3 管理パスワードの設定

[書式]

administrator password

[説明]

管理ユーザ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)。

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。

4.5 一般ユーザ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]

一般ユーザ名とパスワードを設定する。

登録できるユーザは最大 32 人。

ユーザ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。

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**

Rev.11.00.36 以降で使用可能。

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**

Rev.11.00.36 以降で使用可能。

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
*	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	administrator 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。

設定値	説明
off	administrator 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。

- 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。
インタフェース名	指定したインタ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 : ログインタイマーの指定

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	ログインタイマーを設定しない。

- [初期値] :

- administrator=on
- connection=serial,telnet,remote,ssh,sftp,http
- 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。

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。

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、タイム値は 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、すべてのユーザの接続を禁止する、またはすべてのユーザが管理ユーザ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。

user に *radius を指定できるのは Rev.11.00.36 以降である。

4.9 他のユーザの接続の強制切断

[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を指定する。

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

パラメータを省略した場合は、指定したパラメータ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を切断する。

```
# disconnect user /telnet
```

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。

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、TELENT 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。

4.12 セキュリティクラスの設定

[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 telnet コマンドが使用できる
off	telnet 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 ssh コマンドが使用できる
off	ssh コマンドは使用できない

- [初期値]: off

[説明]

セキュリティクラスを設定する。

[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が接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ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。

SSH クライアント機能が実装されていないモデルでは、*ssh* キーワードは使用できない

4.13 パケットバッファのパラメータを変更する

[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] :
NVR500

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	500	187	12	125	1
middle	1332	499	33	333	1
large	2000	562	12	125	4
huge	20	0	0	1	0

[説明]

パケットバッファの管理パラメータを変更する。

パラメータに指定できる値は、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、パラメータには 1 以上の整数を指定できる。同時に、各パラメータ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=1000 max-free=500
# system packet-buffer large min-free=100
```

4.14 LED の輝度を調整する**[書式]**

```
system led brightness mode
no system led brightness [mode]
```

[設定値及び初期値]

- *mode*
 - [設定値] :

設定値	説明
0	明るい
1	暗い

- [初期値]: 0

[説明]

LED の輝度を調整する。

[ノート]

輝度を調整できるのはフロントパネル側のみであり、リアパネル側の LED は調整できない。

4.15 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。

4.16 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。

4.17 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。

4.18 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。

4.19 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。

4.20 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、`rdate` 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。

`ntp_server` に IPv6 アドレスを指定できるのは Rev.11.00.16 以降である。

4.21 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、出力インタフェースの IP アドレスを利用する。

4.22 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。

4.23 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。

4.24 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
ascii	英語で表示する、文字コードは ASCII
sjis	日本語で表示する、文字コードはシフト JIS
euc	日本語で表示する、文字コードは EUC

- [初期値]: 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でも実行できる。

4.25 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 (80..200)
 - [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でも実行できる。

4.26 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でも実行できる。

4.27 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。

4.28 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。

4.29 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。

4.30 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。

4.31 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* パラメータが on の場合にのみ行われる。

4.32 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。

4.33 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、出力インタフェースの IP アドレスを利用する。

4.34 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。

4.35 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。

4.36 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
off	TCP コネクションの syslog を出力しない

• [初期値]: off

• *src_addr*: 始点 IP アドレス

• [設定値]:

- 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
 - *(すべての IP アドレス)

• [初期値]: -

• *dst_addr*: 終点 IP 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

ニーマモニック	ポート番号
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。

Rev.11.00.23 以降で `src_port_list` または `dst_port_list` に `submission` を指定可能。

[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 )
```

4.37 インタ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、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。

4.38 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。

4.39 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。

4.40 TELNET サーバーへアクセスできるホストの IP アドレスの設定

[書式]

```
telnetd host ip_range [ip_range...]
no telnetd host
```

[設定値及び初期値]

- `ip_range`: TELNET サーバーへアクセスを許可するホストの 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
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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する

設定値	説明
none	すべてのホストからのアクセスを禁止する
lan	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
LAN インタフェース名	指定したインタフェースへの接続のみ許可する

- [初期値]: any

[説明]

TELNET サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]

ニーモニックをリストにすることはできない。
設定後の新しい TELNET 接続から適用される。

lan キーワードは Rev.11.00.38 以降で指定可能。

4.41 TELNET サーバーへ同時に接続できるユーザ数の設定

[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が接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ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。

4.42 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。

4.43 LAN インタ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。

4.44 HUB IC での受信オーバーフロー数を取得するか否かの設定

[書式]

```
lan count-hub-overflow switch [interval]
no lan count-hub-overflow [switch [interval]]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	HUB IC での受信オーバーフロー数を定期的に取得する
off	HUB IC での受信オーバーフロー数を定期的に取得しない

- [初期値]: on
- *interval*
 - [設定値]: 受信オーバーフロー数を取得する時間間隔 [秒] (1..65535)
 - [初期値]: 120

[説明]

HUB IC での受信オーバーフロー数を定期的に取得するか否かを設定する。

[ノート]

interval に大きな値を設定するか、*switch* に off を設定することで HUB IC へのアクセスによる負荷を軽減することができる。

本コマンドの設定にかかわらず **show status lan** コマンド実行時に HUB IC での受信オーバーフロー数は取得される。

4.45 LAN インタ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。

4.46 LAN インタ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
```

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

```
lan type interface_without_swhub option=value
```

```
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 インタフェース名
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *speed*: LAN 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..3551)
off	MAC アドレスエージング機能を無効にする

- 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

- [初期値]:
 - mtu=1500
 - auto-crossover=on
 - macaddress-aging=300
 - speed-downshift=on

[説明]

指定した LAN インタ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。

○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 インタフェースでのみ利用できる。

スイッチングハブが持つ 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 1024 個のエントリを格納できる。

○速度ダウンシフト機能

例えば 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。

[ノート]

本コマンドの実行後、LAN インタ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。

[設定例]

スイッチングハブを持つ LAN インタフェースで、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
```

4.47 インタ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 インタフェース名、WAN インタフェース名、'pp'、'tunnel' 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' を指示したときにはそれぞれ、**pp select** あるいは **tunnel select** で選択したインタ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、インタフェースに対する設定内容はインタフェースに対する **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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

4.48 TFTP によりアクセスできるホストの IP アドレスの設定

[書式]

tftp host *host*

no tftp host [*host*]

[設定値及び初期値]

- *host*
- [設定値]:

設定値	説明
IP アドレス	TFTP によりアクセスできるホストの IP アドレス (IPv6 アドレス可)
any	すべてのホストから TFTP によりアクセスできる
none	すべてのホストから TFTP によりアクセスできない

- [初期値]: none

[説明]

TFTP によりアクセスできるホストの IPv4 または IPv6 アドレスを設定する。

[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。

4.49 SFTP サーバーへアクセスできるホストの IP アドレスの設定

[書式]

sftpd host *ip_range* [*ip_range* ...]

no sftpd host [*ip_range*...]

[設定値及び初期値]

- *ip_range*: SFTP サーバーへアクセスを許可するホストの 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
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	指定されたホストからのアクセスを許可する
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
LAN インタフェース名	SFTP サーバーへアクセスを許可する LAN インタフェース名

- [初期値]: none

[説明]

SFTP サーバーへアクセスできるホストの IP アドレスを設定する。

[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ければならない。ニーモニックをリストにすることはできない。設定後の新しい SFTP 接続から適用される。

4.50 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パケットは、**ip filter directed-broadcast** コマンドの設定に基づき処理される。

4.51 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、かんたん設定ページによるリビジョンアップ、DOWNLOAD ボタンによるリビジョンアップに影響する。

4.52 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/nvr500.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。

4.53 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。

4.54 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。

4.55 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。

4.56 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。

4.57 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
no http revision-up schedule [period time1 time2]
```

[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 <i>day</i> は曜日を表す文字列で、以下のいずれか sun,mon,tue,wed,thu,fri,sat
monthly <i>date</i>	毎月 <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、指定した日がある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 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。

[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
```

4.58 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。

4.59 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。

4.60 SSH サーバーへアクセスできるホストの IP アドレスの設定

[書式]

```
sshd host ip_range [ip_range ...]
```

```
no sshd host [ip_range...]
```

[設定値及び初期値]

- *ip_range* : SSH サーバーへアクセスを許可するホストの 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
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	指定されたホストからのアクセスを許可する
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
LAN インタフェース名	SSH サーバーへアクセスを許可する LAN インタフェース名

- [初期値]: any

[説明]

SSH サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]

ニーモニックをリストにすることはできない。
設定後の新しい SSH 接続から適用される。

4.61 SSH サーバーへ同時に接続できるユーザ数の設定

[書式]

```
sshd session num
```

```
no sshd 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が接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ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。

4.62 SSH サーバーホスト鍵の設定

[書式]

```
sshd host key generate [bit=bit]
```

```
no sshd 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]: 1024

[説明]

SSH サーバーのホスト鍵を設定する。
bit パラメータによって、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、**sshd 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。

[ノート]

bit キーワードは、Rev.11.00.35 以降で使用可能。

4.63 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
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

- [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。

4.64 SSH クライアントの生存確認

[書式]

```
ssh client alive switch [interval [count]]
```

```
no ssh 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。

4.65 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]

```
ssh hide openssh version use
```

```
no ssh 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置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。

Rev.11.00.28 以降で使用可能。

4.66 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。

4.67 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。

4.68 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。

4.69 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。

4.70 MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かの設定**[書式]**

alarm mp *switch*

no alarm mp

[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]

MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かを選択する。

4.71 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。

4.72 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。

4.73 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。

4.74 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。

4.75 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。

4.76 エコーキャンセラ制御方法の設定

[書式]

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

no audio echo-canceller port=*port* [route=*route* mode [*length* [nlp=*nlp*] [cng=*cng*]]]

[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
BRI インタフェース名	ISDN ポート
pstn	LINE ポート

- [初期値]: -

- *route*

- [設定値]:

設定値	説明
BRI インタフェース名	ISDN ポート
pstn	LINE 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 OFF

- [初期値]: TEL ポートおよび LINE ポートにおいては auto、ISDN ポートにおいては off

- *length*: エコーキャンセラテール長

- [設定値]:

設定値	説明
16	16 ミリ秒
32	32 ミリ秒
48	48 ミリ秒
64	64 ミリ秒

- [初期値]: TEL ポートにおいては 16、LINE ポートにおいては 64

- *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

[説明]

ポート毎のエコーキャンセラ制御方法を設定する。

mode パラメータを *auto* に指定した場合、通常はエコーキャンセラ機能が 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機能が OFF で動作する。

port パラメータに TEL ポートを指定して、*route* パラメータを *bril* または *pstn*、*mode* パラメータを *off* と指定すると、TEL ポートから ISDN ポートまたは LINE ポートを経由する通話におけるエコーキャンセラ機能を OFF にできる。

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。

[ノート]

route パラメータの指定は、同一機器内の ISDN ポートまたは LINE ポートを使用して通話する場合にのみ有効であり、カスケード接続時に他の機器の ISDN 回線を使用して通話している場合有効とはならない。この場合、エコーキャンセラの動作は *route* のパラメータがない設定に従う。

nlp のパラメータを省略した場合、*nlp=on* で設定される。

cng のパラメータを省略した場合、*cng=on* で設定される。

従来機種とは *length* パラメータ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を OFF とする
audio echo-canceller port=tell off
- TEL1 ポートの *bril* 経由の通話についてエコーキャンセラをオフとする
audio echo-canceller port=tell route=bril off
- TEL1 ポートのエコーキャンセラの設定値をデフォルト値に戻す
no audio echo-canceller port=tell

4.77 エコーキャンセラの 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]:

設定値	説明
high	強め
normal	標準
low	弱め

- [初期値]: normal
- *port*

- [設定値]:

設定値	説明
tel1	TEL1 ポート
tel2	TEL2 ポート
BRI インタフェース名	ISDN ポート
pstn	LINE ポート

- [初期値]: -

[説明]

エコーキャンセラの NLP(NonLinear Processing) の効き具合を設定する。

[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の NLP 閾値を低めに設定する。

```
audio echo-canceller nlp threshold port=tel1 low
```

4.78 エコーキャンセラ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無効
with-phase-reversal	位相反転ありの 2100Hz 検出でエコーキャンセラ無効

- [初期値]: 2100hz

[説明]

エコーキャンセラ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。

4.79 ジッタバッファ制御方法の設定

[書式]

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

[設定値及び初期値]• *port*

- [設定値]:

設定値	説明
tell	TEL1 ポート
tel2	TEL2 ポート
BRI インタフェース名	ISDN ポート
pstn	LINE 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(0..200: ミリ秒単位)
- [初期値]: 200

[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ない、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。

[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
```
- BRI1 インタ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=bril
```

4.80 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 / 40 / 50 / 60)
- [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 G.711/G.729a に関わらず一律に設定される。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なう場合、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。

[設定例]

- RTP のパケット長を 40msec に設定する

```
# audio rtp segsize 40
```

4.81 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。

4.82 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。

ルータの設定ファイル (*config0*) やファームウェア (*exec*、*exec0*) を指定する場合には、*file* に "*config0*" 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:nvr500.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
```

[ノート]

Rev.11.00.23 以降で使用可能

4.83 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]
```

[ノート]

Rev.11.00.23 以降では使用可能。

4.84 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
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

- [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。

Rev.11.00.23 以降で使用可能。

4.85 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。

[ノート]

Rev.11.00.23 以降で使用可能。

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。

5.2 RTFS のガベージコレクト

[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。

ガベージコレクト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]

ガベージコレクト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。

第 6 章

ISDN 関連の設定

6.1 共通の設定

6.1.1 BRI インタフェースの使用制限の設定

[書式]

```
isdn use interface use
```

```
no isdn use interface
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *use*
 - [設定値]:

設定値	説明
off	発着信禁止
on	発着信可
call-only	発信専用(着信規制)
arrive-only	着信専用(発信規制)

- [初期値]: on

[説明]

BRI インタフェースの発着信を制限する。

6.1.2 BRI 回線の種類の指定

[書式]

```
line type interface line [channels]
```

```
no line type interface line [channels]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *line*
 - [設定値]:

設定値	説明
isdn, isdn-ntt	ISDN 回線交換
l64	デジタル専用線、64kbit/s
l128	デジタル専用線、128kbit/s

- [初期値]: isdn
- *channels*: *line* パラメータが *isdn*、*isdn-ntt* の場合のみ指定可
- [設定値]:

設定値	説明
1b	B チャンネルは 1 チャンネルだけ使用
2b	B チャンネルは 2 チャンネルとも使用する

- [初期値]: 2b

[説明]

BRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する **interface reset** コマンドの発行により反映される。

[ノート]

別の通信機器の発着信のために 1B チャンネルを確保したい場合は *channels* パラメータを 1b に設定する。

6.1.3 自分の ISDN 番号の設定

[書式]

```
isdn local address interface isdn_num[/sub_address]
isdn local address interface /sub_address
noisdn local address interface
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *isdn_num*
 - [設定値]: ISDN 番号
 - [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
 - [初期値]: -

[説明]

自分の ISDN 番号とサブアドレスを設定する。ISDN 番号、サブアドレスとも完全に設定して運用することが推奨される。また、ISDN 番号は市外局番も含めて設定する。

[ノート]

他機種との相互接続のために、ISDN サブアドレスに英文字や記号を使わず数字だけにしなければならないことがある

6.1.4 PP で使用するインタフェースの設定

[書式]

```
pp bind interface
no pp bind [interface]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -

[説明]

選択されている相手先に対して実際に使用するインタフェースを設定する。

6.1.5 課金額による発信制限の設定

[書式]

```
account threshold [interface] yen
account threshold pp yen
no account threshold interface [yen]
no account threshold [yen]
no account threshold pp [yen]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名

- [初期値]: -
- *yen*
- [設定値]:

設定値	説明
円 (1..2147483647)	課金額
off	発信制限機能を使わない

- [初期値]: off

[説明]

網から通知される課金の合計 (これは **show account** コマンドで表示される) の累計が指定した金額に達したらそれ以上の発信を行わないようにする。

account threshold コマンドではルーター全体の合計金額を設定し、**interface** パラメータを指定した場合には、それぞれのインタフェースでの合計金額、**account threshold pp** コマンドでは選択している相手先に対する発信での合計金額で制御を行う。

課金が網から通知されるのは通信切断時なので、長時間の接続の途中で切断することはできず、制限はできない。この場合に対処するには、**isdn forced disconnect time** コマンドで通信中でも時間を監視して強制的に回線を切るような設定しておく方法がある。また、課金合計は **clear account** コマンドで 0 にリセットでき、**schedule at** コマンドで定期的に **clear account** を実行するようしておくこと、毎月一定額以内に課金を抑えるといったことが自動で可能になる。

[ノート]

課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。

6.1.6 PIAFS の着信を許可するか否かの設定

[書式]

```
isdn piafs arrive arrive
no isdn piafs arrive [arrive]
```

[設定値及び初期値]

- *arrive*
- [設定値]:

設定値	説明
on	許可する
off	拒否する

- [初期値]: on

[説明]

PIAFS の着信を許可するか否かを設定する。着信が許可されている場合には、すべての PIAFS の方式が着信できる。

[ノート]

PHS 端末側で発信者番号を通知するようになっている必要がある。

6.1.7 PIAFS 接続時の起動側の指定

[書式]

```
isdn piafs control switch
no isdn piafs control
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
call	自分が発信側の場合に PIAFS の起動側となる
both	自分が発着信いずれの場合でも PIAFS の起動側となる
arrive	自分が着信側の場合に PIAFS の起動側となる

- [初期値]: call

[説明]

PIAFS を制御する側を選択する。

[ノート]

本コマンドの設定と、発信/着信の組み合わせにより、起動側となるか被起動側となるかが以下のように決定される。

<i>switch</i> パラメータの設定	call	both	arrive
発信時	起動時	起動側	被起動側
着信時	被起動側	起動側	起動側

[設定例]

```
# pp select 2
# isdn piafs control call
# pp enable 2
```

6.1.8 PIAFS の発信方式の設定

[書式]

```
isdn piafs call speed [64kmode]
no isdn piafs call [speed [64kmode]]
```

[設定値及び初期値]

- *speed*
- [設定値]:

設定値	説明
off	発信を同期 PPP とする
32k	発信を PIAFS 32k とする
64k	発信を PIAFS 64k とする

- [初期値]: off
- *64kmode*

- [設定値]:

設定値	説明
guarantee	PIAFS 64k の発信ではギャランティー方式を使用する
best-effort	PIAFS 64k の発信ではベストエフォート方式を使用する

- [初期値]: -

[説明]

PIAFS モードの発信を可能にするか否かを設定する。

また、PIAFS モードの速度を選択する。

speed が off に設定されている場合には発信は同期 PPP になり、32k に設定されている場合には発信は PIAFS 32k に、64k に設定されている場合には発信は PIAFS 64k になる。

speed が 64k に設定されている場合には、*64kmode* の設定が有効になる。

64kmode が設定されていない、または *guarantee* に設定されている場合には、発信はギャランティー方式の PIAFS 64k

になる。

64kmode が best-effort に設定されている場合には、発信はベストエフォート方式になる。

[ノート]

PIAFS 64k では特別なサブアドレスが用いられるため、ユーザがコマンドで設定した発サブアドレスは無視される。

6.2 相手側の設定

6.2.1 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**

• ISDN 接続

• **pp bind** BRI インタフェース名

• **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 として専用線が使用される時、あるいは anonymous が選択された時には無効である。

6.2.2 相手 ISDN 番号の設定

[書式]

isdn remote address call_arrive isdn_num [/sub_address] [isdn_num_list]

isdn remote address call_arrive isdn_num [isdn_num_list]

no isdn remote address call_arrive [isdn_num [/sub_address] [isdn_num_list]]

[設定値及び初期値]

- *call_arrive*
 - [設定値]:

設定値	説明
call	発着信用
arrive	着信専用

- [初期値]: -
- *isdn_num*
 - [設定値]: ISDN 番号
 - [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
 - [初期値]: -
- *isdn_num_list*
 - [設定値]: ISDN 番号だけまたは ISDN 番号とサブアドレスの組を空白で区切った並び
 - [初期値]: -

[説明]

選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。

選択されている相手が *anonymous* の場合は無意味である。

複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。

MP のように相手先に対して複数チャンネルで接続しようとする際に発信する順番は、**isdn remote call order** コマンドで設定する。

6.2.3 自動接続の設定

[書式]

isdn auto connect auto

no isdn auto connect [auto]

[設定値及び初期値]

- *auto*
 - [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ついて自動接続するか否かを設定する。

6.2.4 自動切断の設定

[書式]

isdn auto disconnect auto

no isdn auto disconnect [auto]

[設定値及び初期値]

- *auto*
 - [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ついて自動切断するか否かを設定する。
各種切断タイムの設定を変更せずに、自動切断を無効にしたい場合に使用する。

[ノート]

schedule at コマンドと併用して、テレホーダイ時間中に自動切断しないようにしたい場合等に有効。
anonymous に対して使用する事はできない。

6.2.5 相手への発信順序の設定

[書式]

isdn remote call order *order*
no isdn remote call order [*order*]

[設定値及び初期値]

- *order*
- [設定値]:

設定値	説明
round	ラウンドロビン方式
serial	順次サーチ方式

- [初期値]: serial

[説明]

isdn remote address call コマンドで複数の ISDN 番号が設定されている場合に意味を持つ。MP を使用する場合などのように、相手先に対して同時に複数のチャンネルで接続しようとする際に、どのような順番で ISDN 番号を選択するかを設定する。

round を指定した場合は、**isdn remote address call** コマンドで最初に設定した ISDN 番号で発信した次の発信時に、このコマンドで次に設定された ISDN 番号を使う。このように順次ずれていき、最後に設定された番号で発信した次には、最初に設定された ISDN 番号を使い、これを繰り返す。

serial を指定した場合は、発信時には必ず最初に設定された ISDN 番号を使い、何らかの理由で接続できなかった場合は次に設定された ISDN 番号で発信し直す。

なお round、serial いずれの設定の場合でも、どことも接続されていない状態や相手先とすべてのチャンネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

[ノート]

MP を使用する場合は、round にした方が効率がよい。

6.2.6 着信許可の設定

[書式]

isdn arrive permit *arrive*
no isdn 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

設定値	説明
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]

isdn arrive permit、**isdn call permit** コマンドとも off を設定した場合、ISDN 回線経由では通信できない。

6.2.7 発信許可の設定

[書式]

```
isdn call permit permit
no isdn 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]

isdn arrive permit、**isdn call permit** コマンドとも off を設定した場合、ISDN 回線経由では通信できない。

6.2.8 再発信抑制タイマの設定

[書式]

```
isdn call block time time
no isdn call block time [time]
```

[設定値及び初期値]

- *time*
- [設定値]: 秒数 (0..15.0)
- [初期値]: 0

[説明]

選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call prohibit time コマンドによるタイマはエラーで切断された場合だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点が異なる。

[ノート]

切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。

isdn forced disconnect time コマンドと併用するとよい。

6.2.9 エラー切断後の再発信禁止タイマの設定

[書式]

```
isdn call prohibit time time
no isdn call prohibit time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (60..21474836.0)
 - [初期値]: 60

[説明]

選択されている相手に発信しようとして失敗した場合に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点異なる。

6.2.10 相手にコールバック要求を行うか否かの設定**[書式]**

```
isdn callback request callback_request
no isdn callback request [callback_request]
```

[設定値及び初期値]

- *callback_request*
 - [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]

選択されている相手に対してコールバック要求を行うか否かを設定する。

[ノート]

コールバックは、**backup** コマンドによる ISDN インタフェースへのバックアップとの併用はできません。バックアップと併用する場合は、ネットワークバックアップを使ってください。

6.2.11 相手からのコールバック要求に応じるか否かの設定**[書式]**

```
isdn callback permit callback_permit
no isdn callback permit [callback_permit]
```

[設定値及び初期値]

- *callback_permit*
 - [設定値]:

設定値	説明
on	応じる
off	応じない

- [初期値]: off

[説明]

選択されている相手からのコールバック要求に対してコールバックするか否かを設定する。

6.2.12 コールバック要求タイプの設定**[書式]**

```
isdn callback request type type
no isdn callback request type [type]
```

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
yamaha	ヤマハ方式
mscbcpc	MS コールバック

- [初期値]: yamaha

[説明]

コールバックを要求する場合のコールバック方式を設定する。

6.2.13 コールバック受け入れタイプの設定

[書式]

```
isdn callback permit type type1 [type2]
no isdn callback permit type [type1 [type2]]
```

[設定値及び初期値]

- type1,type2

- [設定値]:

設定値	説明
yamaha	ヤマハ方式
mscbcpc	MS コールバック

- [初期値]:

- type1=yamaha
- type2=mscbcpc

[説明]

受け入れることのできるコールバック方式を設定する。

6.2.14 MS コールバックでユーザからの番号指定を許可するか否かの設定

[書式]

```
isdn callback mscbcpc user-specify specify
no no isdn callback mscbcpc user-specify [specify]
```

[設定値及び初期値]

- specify

- [設定値]:

設定値	説明
on	許可する
off	拒否する

- [初期値]: off

[説明]

サーバー側として動作する場合にはコールバックするために利用可能な電話番号が一つでもあればそれに対してのみコールバックする。しかし、anonymous への着信で、発信者番号通知がなく、コールバックのためにつかえる電話番号が全く存在しない場合に、コールバック要求側(ユーザ)からの番号指定によりコールバックするかどうかを設定する。

[ノート]

設定が off でコールバックできない場合には、コールバックせずにそのまま接続する。

6.2.15 コールバックタイマの設定

[書式]

```
isdn callback response time type time
no isdn callback response time [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1b	1B でコールバックする

- [初期値]: -
- *time*
 - [設定値]: 秒数 (0..15.0)
 - [初期値]: 0

[説明]

選択されている相手からのコールバック要求を受け付けてから、実際に相手に発信するまでの時間を設定する。秒数は 0.1 秒単位で設定できる。

6.2.16 コールバック待機タイマの設定**[書式]**

```
isdn callback wait time time
no isdn callback wait time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..60.0)
 - [初期値]: 60

[説明]

選択されている相手にコールバックを要求し、それが受け入れられていったん回線が切断されてから、このタイマがタイムアウトするまで相手からのコールバックによる着信を受け取れなかった場合には接続失敗とする。秒数は 0.1 秒単位で設定できる。

6.2.17 ISDN 回線を切断するタイマ方式の指定**[書式]**

```
isdn disconnect policy type
no isdn disconnect policy [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1	単純トラフィック監視方式
2	課金単位時間方式

- [初期値]: 1

[説明]

単純トラフィック監視方式は従来型の方式であり、**isdn disconnect time**、**isdn disconnect input time**、**isdn disconnect output time** の 3 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。

課金単位時間方式では、課金単位時間と監視時間を **isdn disconnect interval time** コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。

[設定例]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

6.2.18 切断タイマの設定 (ノーマル)

[書式]

isdn disconnect time *time*

no isdn disconnect time [*time*]

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
1..21474836.0	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 側のデータ送受信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

[ノート]

本コマンドを off に設定した場合には、**isdn disconnect input time** コマンドおよび **isdn disconnect output time** コマンドの設定にかかわらず切断されなくなる。

本コマンドの設定値を NORMAL 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、**isdn disconnect output time** コマンドの設定値を OUT 秒とする。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

6.2.19 切断タイマの設定 (ファスト)

[書式]

isdn fast disconnect time *time*

no isdn fast disconnect time [*time*]

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: 20

[説明]

ある宛先について、パケットがルーティングされ、そこへ発信しようとしたが、ISDN 回線が他の接続先により塞がっていて発信できない場合に、ISDN 回線を塞いでいる相手先についてこのタイマが動作を始める。このタイマで指定した時間の間、パケットが全く流れなかったらその相手先を切断して、発信待ちの宛先を接続する。秒数は 0.1 秒単位で設定できる。

なお、**isdn auto connect** コマンドが off の場合はこのタイマは無視される。

[ノート]

同じ ISDN 回線に接続されている他の機器が Bch を使用している場合には、本コマンドは機能しないことがある。また、本機の PP Anonymous の接続がすべての Bch を使用している場合には、新たな PP Anonymous の接続を起動しても、本コマンドは機能しない。

6.2.20 切断タイマの設定 (強制)

[書式]

```
isdn forced disconnect time time
no isdn forced disconnect time [time]
```

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	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接続する最大時間を設定する。秒数は 0.1 秒単位で設定できる。パケットをやりととりしていても、このコマンドで設定した時間が経過すれば強制的に回線を切断する。ダイヤルアップ接続でインターネット側からの無効なパケット (ping アタック等) が原因で回線が自動切断できない場合に有効。 **isdn call block time** コマンドと併用するとよい。

6.2.21 入力切断タイマの設定 (ノーマル)

[書式]

```
isdn disconnect input time time
no isdn disconnect input time [time]
```

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	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。秒数は 0.1 秒単位で設定できる。

[ノート]

例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。

isdn disconnect time コマンドを off に設定した場合には、本コマンドおよび **isdn disconnect output time** コマンドの設定にかかわらず切断されなくなる。

isdn disconnect time コマンドの設定値を NORMAL 秒、本コマンドの設定値を IN 秒、**isdn disconnect output time** コマンドの設定値を OUT 秒とする。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

6.2.22 出力切断タイマの設定 (ノーマル)

[書式]

```
isdn disconnect output time time
no isdn disconnect output time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836.0	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。秒数は 0.1 秒単位で設定できる。

[ノート]

例えば、接続先を経由して外部から不正な UDP パケットを受信し続けるような場合、本タイマを設定しておくことにより回線を切断することができる。

isdn disconnect time コマンドを off に設定した場合には、**isdn disconnect input time** コマンドおよび本コマンドの設定にかかわらず切断されなくなる。

isdn disconnect time コマンドの設定値を NORMAL 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、本コマンドの設定値を OUT 秒とする。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

6.2.23 課金単位時間方式での課金単位時間と監視時間の設定**[書式]**

isdn disconnect interval time *unit watch spare*

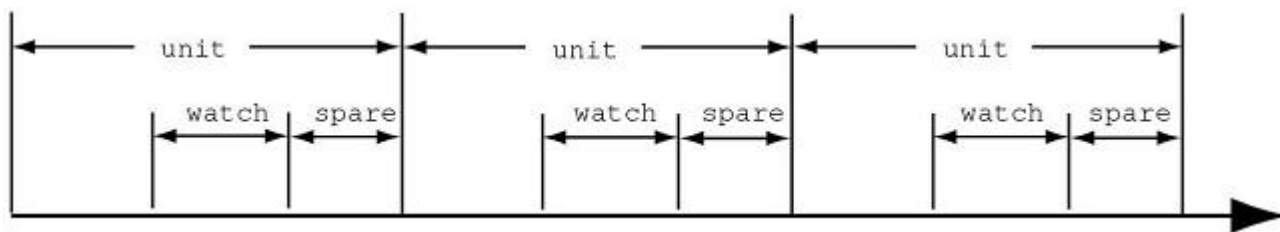
no isdn disconnect interval time [*unit watch spare*]

[設定値及び初期値]

- *unit*: 課金単位時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 180
- *watch*: 監視時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 6
- *spare*: 切断余裕時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 2

[説明]

課金単位時間方式で使われる、課金単位時間と監視時間を設定する。秒数は 0.1 秒単位で設定できる。それぞれの意味は下図参照。



watch で示した間だけトラフィックを監視し、この間にパケットが流れなければ回線を切断する。*spare* は切断処理に時間がかかりすぎて、実際の切断が単位時間を越えないように余裕を持たせるために使う。

回線を接続している時間が *unit* の倍数になるので、単純トラフィック監視方式よりも通信料金を減らす効果が期待できる。

[ノート]

外部へパケットを送信していない状態でも、外部からパケットを受信し続けていると、本コマンドの設定通りに切断されないことがある。

[設定例]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

6.2.24 同じ相手に対して連続して認証に失敗できる回数の設定

[書式]

isdn call prohibit auth-error count *count*

no isdn call prohibit auth-error 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]

連続して認証に失敗できる回数を設定する。ここで設定した回数だけ連続して認証に失敗したときには、その後は、同じ相手に対して発呼しない。

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

6.2.25 MP が失敗できる最大回数の設定

[書式]

isdn call prohibit mp-error count *times*

no isdn call prohibit mp-error count

[設定値及び初期値]

• *times*

- [設定値]:

設定値	説明
1..21474836	失敗できる最大回数
off	発信制限をかけない

- [初期値]: 5

[説明]

選択されている相手に対し、MP が失敗できる最大回数を設定する。
 最大回数を越えた場合、**ppp mp use**、**ppp mp minlink**、**ppp mp maxlink** コマンドで設定を直さないと同じ相手に MP で発呼できない。

6.2.26 相手先毎の累積接続時間による発信制限の設定**[書式]**

```
pp connect time threshold time
no pp connect time threshold
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数(1..21474836)
 - [初期値]: -

[説明]

選択された相手先に対する累計接続時間の閾値を設定する。
 なお、発信時の接続時間の累計を累積接続時間として使用する。

[ノート]

累積接続時間は本機の通信時間算出方式により計算された通信時間の累計のため、プロバイダ独自の通信時間算出方法により計算された累積接続時間とは異なることがある。

6.2.27 相手先毎の累積接続回数による発信制限の設定**[書式]**

```
pp connect count threshold count
no pp connect count threshold
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数(1..21474836)
 - [初期値]: -

[説明]

選択された相手先に対する累計接続回数の閾値を設定する。
 なお、発信時の接続回数の累計を累積接続回数として使用する。
 累積接続回数は **clear account** コマンドにより 0 に設定される。

6.2.28 i・ナンバーサービスのポート番号の設定**[書式]**

```
isdn arrive inumber-port interface inum_port [inum_port...]
no isdn arrive inumber-port interface
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *inum_port*: i・ナンバーサービスのポート番号
 - [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

設定値	説明
3	ポート番号 3 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] : all

[説明]

ルーターで着信する i・ナンバーサービスのポート番号を選択する。

第 7 章

IP の設定

7.1 インタフェース共通の設定

7.1.1 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。

7.1.2 IP アドレスの設定

[書式]

```
ip interface address ip_address/mask [broadcast broadcast_ip]
ip interface address dhcp
ip pp address ip_address[/mask]
ip loopback address ip_address[/mask]
no ip interface address [ip_address/mask [broadcast broadcast_ip]]
no ip pp address [ip_address[/mask]]
no ip loopback address [ip_address[/mask]]
```

[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
 - [初期値]: -
- *loopback*
 - [設定値]: LOOPBACK インタフェース名
 - [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]: -
- *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]:-

[説明]

インタフェースの 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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

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。

7.1.3 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。

7.1.4 インタフェースの 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 インタフェース名、WAN インタフェース名
 - [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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.5 同一インタ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 インタフェースの場合)
 - on (その他のインタフェースの場合)

[説明]

同一インタ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。

7.1.6 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。

7.1.7 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 インタフェース名、WAN インタフェース名

- 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*: 以下のパラメータを空白で区切り複数設定可能
- [設定値]:

設定値	説明
filter <i>number</i> [<i>number..</i>]	フィルタ型経路の指定 <ul style="list-style-type: none"> • <i>number</i> <ul style="list-style-type: none"> • フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
metric <i>metric</i>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
hide	出力インタフェースが LAN インタフェース、または WAN インタフェース、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、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"> • <i>weight</i> <ul style="list-style-type: none"> • 経路への重み (1..2147483647) • 省略時は 1

- [初期値] :-

[説明]

IP の静的経路を設定する。

gateway のパラメータとしてフィルタ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]

既に存在する経路を上書きすることができる。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

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
```

- マルチホーミングによる負荷分散を行う。デフォルトゲートウェイとして 2 経路持ち、PP1 には専用線 128k で、PP2 には専用線 64k で接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。

※ NAT 機能と専用線キーブアライブの併用が必要となる。

```
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
```

7.1.8 IP パケットのフィルタの設定

[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]: 静的フィルタ番号 (1..21474836)
 - [初期値]: -
- pass_reject*
 - [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-nolog	一致すれば破棄する (ログに記録しない)
reject, reject-log	一致すれば破棄する (ログに記録する)
restrict, 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)
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)

- [初期値]: -
- src_addr*: IP パケットの始点 IP アドレス
 - [設定値]:
 - 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
 - * (すべての IP アドレスに対応)
 - 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。
 - [初期値]: -
- dest_addr*: IP パケットの終点 IP 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 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

ニーマニック	ポート番号
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を設定する。本コマンドで設定されたフィルタは **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ない。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と比較される。

Rev.11.00.23 以降で *src_port_list* または *dest_port_list* に submission を指定可能。

[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 * *
```

7.1.9 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
out	出力方向のフィルタ

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたフィルタ番号の並び (1000 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 のフィルタをそれぞれ定義し、**ip interface secure filter** コマンドによりインタフェースに適用される。

7.1.10 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。

7.1.11 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、ディレクティ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、ディレクティ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でパケットを検査し、PASS フィルタ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つたパケットのみが、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。

7.1.12 動的フィルタの定義**[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 [dyn_filter_num...]
```

[設定値及び初期値]

- *dyn_filter_num*
 - [設定値]: 動的フィルタ番号 (1..21474836)
 - [初期値]: -
- *srcaddr*: IP パケットの始点 IP アドレス
 - [設定値]:
 - **ip 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]: -
- *dstaddr*: IP パケットの終点 IP 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]: -
- *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)
 - [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
 - 以下のニーモニックは設定できますが、動的フィルタ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

[説明]

動的フィルタを定義する。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に該当する接続 (トリガ) 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に該当する接続を通過させる。in キーワードはトリガ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。

[設定例]

```
# ip filter 10 pass * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

7.1.13 動的フィルタ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
tcp-syn-timeout	SYN を受けてから設定された時間内に接続が確立しなければセッションを切断する
tcp-fin-timeout	FIN を受けてから設定された時間が経てば接続を強制的に解放する
tcp-idle-time	設定された時間内に TCP 接続のデータが流れなければ接続を切断する
udp-idle-time	設定された時間内に UDP 接続のデータが流れなければ接続を切断する
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接続を切断する

- [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。

7.1.14 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 インタフェース名、WAN インタフェース名
 - [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	インタフェースの内向き
out	インタフェースの外向き

- [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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.15 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.16 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 インタフェース名、WAN インタフェース名

- [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.17 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.18 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 インタフェース名、WAN インタフェース名
 - [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.11.00.35 以前)

- auto(Rev.11.00.36 以降)

[説明]

インタ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、インタフェースの MTU、もしくは PP インタ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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

7.1.19 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 インタフェース名、WAN インタフェース名
 - [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]

Rev.11.00.35 以降で使用可能。

7.1.20 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
none	制限しない

- [初期値]: 1000

[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。

7.1.21 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。

7.1.22 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、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

- [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の組み合わせで、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 での検査は行われず。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。

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。
WAN インターフェースは Rev.11.00.16 以降で指定可能。

7.1.23 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 ip filter 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、経路の途中で ICMP パケットをフィルタ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ありません。

7.1.24 代理 ARP の設定

[書式]

```
ip interface proxyarp proxyarp
no ip interface proxyarp [proxyarp]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [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

[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 インタフェースの実 MAC アドレスとなる。

7.1.25 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。

Rev.11.00.20 以降では、*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。

7.1.26 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。

7.1.27 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 インタフェース名
 - [初期値]: -
- *len*
 - [設定値]: キュー長 (0..10000)
 - [初期値]: 40

[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。

7.1.28 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]

- *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。

7.1.29 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)
dhcp interface	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 インタフェース名または WAN インタフェース名

- [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

- [初期値]:
 - log=off
 - upwait=5
 - downwait=5
 - length=64

[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、NVR500 のフロントパネルの WAN LED が黄色に点灯する。

[ノート]

length パラメータで指定するのは 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。WAN インタフェースは Rev.11.00.16 以降で指定可能。

[設定例]

```
# ip keepalive 1 icmp-echo 5 5 192.168.100.101
# ip keepalive 2 icmp-echo 5 5 172.16.112.1
```

7.1.30 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。

7.2 PP 側の設定

7.2.1 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] : -
- *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。

dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが 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。

7.2.2 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
NVR500	11.00.06 ~	13

7.2.3 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* パラメータとは同時には指定できない
 - [初期値]: -

[説明]

PP インタ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来ている間は *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* パラメータの値に変更される。*count* パラメータ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。

7.2.4 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] :

<i>option</i>	<i>value</i>	説明
<code>upwait</code>	ミリ秒	アップ検知のための許容応答時間 (1..10000)
<code>downwait</code>	ミリ秒	ダウン検知のための許容応答時間 (1..10000)
<code>disconnect</code>	秒	無応答切断時間 (1..21474836)
<code>length</code>	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。

他のパラメータがデフォルト値の場合、`disconnect` パラメータは 70 秒程度に設定しておく、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。

7.2.5 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。

7.2.6 専用線ダウン検出時の動作の設定

[書式]

```
leased keepalive down action
no leased keepalive down [action]
```

[設定値及び初期値]

- *action*
- [設定値]:

設定値	説明
silent	何もしない
reset	ルーターを再起動する

- [初期値]: silent

[説明]

キープアライブによって専用線ダウンを検出した場合のルーターの動作を設定する。

7.3 RIP の設定

7.3.1 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。

7.3.2 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。

7.3.3 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

`invalid-route-reactivate` オプションは Rev.11.00.23 以降で指定可能。

7.3.4 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 (トンネルインタフェースの場合)
- on (その他のインタフェースの場合)

- *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。

7.3.5 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` (トンネルインタフェースの場合)
- `on` (その他のインタフェースの場合)
- `version`
 - [設定値]: 受信する RIP のバージョン (1,2)
 - [初期値]: 1 2 (トンネルインタフェース以外の場合)

[説明]

指定したインタフェースに対し、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。

7.3.6 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番号の並び (100 個以内)
 - [初期値]: -

[説明]

インタ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。

7.3.7 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。

7.3.8 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。

7.3.9 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
```

7.3.10 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。

7.3.11 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	ip pp rip connect interval 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
```


7.3.12 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
```

7.3.13 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	ip pp rip disconnect interval 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
```

7.3.14 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
```

7.3.15 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
```

7.3.16 RIP2 でのフィルタの比較方法**[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 エントリへ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	
	RIP2	

7.3.17 RIP のタイマーを調整する

[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 のタイマー値を設定する。

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* タイマーと *invalid* タイマーの値に影響するが、*holddown* タイマー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、各タイマーは以下ようになる。

<i>update</i>	T
<i>invalid</i>	T×6
<i>holddown</i>	rip timer コマンドの設定値 (デフォルト 120 秒)

PP インタ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。

第 8 章

イーサネットフィルタの設定

8.1 フィルタ定義の設定

[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]: 静的フィルタの番号 (1-100)
 - [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を設定する。本コマンドで設定されたフィルタは、**ethernet lan filter** コマンドで用いられる。

通常型のフィルタでは、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を適用する。

dhcp-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。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に合致するとみなす。

dhcp-not-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。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 型のフィルタで対象とする DHCP スコープは、*scope* パラメータで指定する。

scope パラメータとしては 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、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 パラメータを省略した場合には、フィルタが適用されるインタ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なわれる。

[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。

8.2 インタ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番号の並び (100 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]

LAN インタフェース名に指定できるのは物理的な LAN だけであり、VLAN インタフェースは指定できない。

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] [isdn1] [clid [isdn2...]] [mscbcp] [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]: 自分側のユーザ名
 - [初期値]: -
- *mypass*
 - [設定値]: 自分側のパスワード
 - [初期値]: -
- *isdn1*
 - [設定値]: 相手の ISDN アドレス
 - [初期値]: -
- *clid*: 発番号認証を利用することを示すキーワード
 - [初期値]: -
- *isdn2*
 - [設定値]: 発番号認証に用いられる ISDN アドレス
 - [初期値]: -
- *mscbcp*: MS コールバックを許可することを示すキーワード
 - [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。オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。名前に '*' を与えた場合にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。

clid キーワードは発番号認証を利用することを指示する。このキーワードがない場合は発番号認証は行われない。発番号認証は *isdn2* があれば *isdn2* を用い、または *isdn2* がなければ *isdn1* を用い、一致したら認証は成功したとみなす。

isdn2 は複数設定することができる。複数設定する場合は、まず先頭の ISDN アドレスで認証が行われ、認証に失敗すると次の ISDN アドレスが使われる。

mshcbp キーワードは MS コールバックを許可することを指示する。このユーザからの着信に対しては、同時に **isdn callback permit on** としてあれば MS コールバックの動作を行う。

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
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い場合は、認証を拒否する。

PP 毎のコマンドである。

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。

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。

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。

9.6 LCP 関連の設定

9.6.1 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。また、このオプションを相手から要求された場合には、このコマンドの設定に関わらず常にアクセプトする。

9.6.2 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。

9.6.3 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* パラメータの設定は常に 1792 として動作する。

9.6.4 Protocol Field Compression オプション使用の設定**[書式]**

```
ppp lcp pfc pfc
no ppp lcp pfc [pfc]
```

[設定値及び初期値]

- *pfc*
- [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。また、このオプションを相手から要求された場合には、このコマンドの設定に関わらず常にアクセプトする。

9.6.5 lcp-restart パラメータの設定**[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。

9.6.6 lcp-max-terminate パラメータの設定**[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。

9.6.7 lcp-max-configure パラメータの設定

[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。

9.6.8 lcp-max-failure パラメータの設定

[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。

9.6.9 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。

9.7 PAP 関連の設定

9.7.1 pap-restart パラメータの設定

[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。

9.7.2 pap-max-authreq パラメータの設定

[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。

9.8 CHAP 関連の設定

9.8.1 chap-restart パラメータの設定

[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。

9.8.2 chap-max-challenge パラメータの設定

[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。

9.9 IPCP 関連の設定

9.9.1 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。

9.9.2 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。

9.9.3 ipcp-restart パラメータの設定

[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。

9.9.4 ipcp-max-terminate パラメータの設定

[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。

9.9.5 ipcp-max-configure パラメータの設定

[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。

9.9.6 ipcp-max-failure パラメータの設定

[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。

9.9.7 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。

9.9.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式]

```
ppp ipcp msexp msexp
no ppp ipcp msexp [msexp]
```

[設定値及び初期値]

- *msexp*
 - [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。

9.9.9 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 経路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。

9.10 MSCBCP 関連の設定**9.10.1 mscbcpr-restart パラメータの設定****[書式]**

```
ppp mscbcpr restart time
no ppp mscbcpr 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。

9.10.2 mscbcpr-maxretry パラメータの設定**[書式]**

```
ppp mscbcpr maxretry count
no ppp mscbcpr 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。

9.11 CCP 関連の設定

9.11.1 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。

9.11.2 ccp-restart パラメータの設定

[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。

9.11.3 ccp-max-terminate パラメータの設定

[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。

9.11.4 ccp-max-configure パラメータの設定

[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。

9.11.5 ccp-max-failure パラメータの設定

[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。

9.12 IPV6CP 関連の設定

9.12.1 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。

9.13 MP 関連の設定**9.13.1 MP を使用するか否かの設定****[書式]**

```
ppp mp use use
no ppp mp 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]

選択されている相手について MP を使用するか否かを選択する。

on に設定していても、LCP の段階で相手とのネゴシエーションが成立しなければ MP を使わずに通信する。

9.13.2 MP の制御方法の設定**[書式]**

```
ppp mp control type
no ppp mp control [type]
```

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
arrive	自分が 1B 目の着信側の場合に MP を制御する
both	自分が 1B 目の発信着信いずれの場合でも MP を制御する
call	自分が 1B 目の発信側の場合に MP を制御する

- [初期値]: call

[説明]

選択されている相手について MP を制御して 2B 目の発信/切断を行う場合を設定する。通常は初期値のように自分が 1B 目の発信側の場合だけ制御するようしておく。

9.13.3 MP のための負荷閾値の設定**[書式]**

```
ppp mp load threshold call_load call_count disc_load disc_count
no ppp mp load threshold [call_load call_count disc_load disc_count]
```

[設定値及び初期値]

- *call_load*
 - [設定値]: 発信負荷閾値 %(1..100)
 - [初期値]: 70
- *call_count*
 - [設定値]: 回数 (1..100)

- [初期値]: 1
- *disc_load*
 - [設定値]: 切断負荷閾値 %(0..50)
 - [初期値]: 30
- *disc_count*
 - [設定値]: 回数 (1..100)
 - [初期値]: 2

[説明]

選択されている相手について[PPP,MP]の 2B 目を発信したり切断したりする場合のデータ転送負荷の閾値を設定する。

負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call_load* を超える負荷が *call_count* 回繰り返されたら 2B 目の発信を行う。逆に *disc_load* を下回る負荷が *disc_count* 回繰り返されたら 2B 目を切断する。

9.13.4 MP の最大リンク数の設定

[書式]

```
ppp mp maxlink number
no ppp mp maxlink [number]
```

[設定値及び初期値]

- *number*
 - [設定値]: リンク数
 - [初期値]: 2

[説明]

選択されている相手について[PPP,MP]の最大リンク数を設定する。リンク数の最大値は、使用モデルで使用できる ISDN Bch の数までとなる。

9.13.5 MP の最小リンク数の設定

[書式]

```
ppp mp minlink number
no ppp mp minlink [number]
```

[設定値及び初期値]

- *number*
 - [設定値]: リンク数
 - [初期値]: 1

[説明]

選択されている相手について[PPP,MP]の最小リンク数を設定する。

9.13.6 MP のための負荷計測間隔の設定

[書式]

```
ppp mp timer time
no ppp mp timer [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..21474836)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,MP]のための負荷計測間隔を設定する。

単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行われる。

9.13.7 MP のパケットを分割するか否かの設定

[書式]

```
ppp mp divide divide
no ppp mp divide [divide]
```

[設定値及び初期値]

- *divide*
- [設定値]:

設定値	説明
on	分割する
off	分割しない

- [初期値]: on

[説明]

選択されている相手について[PPP, MP]に対して、MP パケットの送信時にパケットを分割するか否かを設定する。分割するとうまく接続できない相手に対してだけ off にする。分割しないように設定した場合、特に TCP の転送効率に悪影響が出る可能性がある。64 バイト以下のパケットは本コマンドの設定に関わらず分割されない。

9.14 PPPoE 関連の設定

9.14.1 PPPoE で使用する LAN インタフェースの指定

[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 LAN インタフェースを指定する。設定がない場合は、PPPoE は使われない。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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

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通知します。

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。

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で指定する。これらのパラメータ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。 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。

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。

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..2147483647	分
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]

ひとつのネットワークについて複数の DHCP スコープを設定することはできない。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。

Rev.11.00.35 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`

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
no dhcp scope bind scope_num 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
 - [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` の指定は、同時に接続できる B チャンネルの数に限られる。また、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** 機能が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。

Rev.11.00.35 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 scope_num ip_address ethernet 00:a0:de:01:23:45
B. # dhcp scope bind scope_num ip_address text client01
C. # dhcp scope bind scope_num ip_address 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind scope_num ip_address 00:a0:de:01:23:45
```

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。

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。

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	show status dhcp summary 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

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(Rev.11.00.20 以降)
 - 1..49,64..76,85..87,128..254(Rev.11.00.20 以前)
 - 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]

Rev.11.00.35 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**

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。

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。

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]

DHCPBOOTREQUEST 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。

10.1.12 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。

10.1.13 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。

10.1.14 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り、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]

Rev.11.00.28 以降で使用可能。

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 インタフェース名、WAN インタフェース名
 - [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 インタフェースは Rev.11.00.16 以降で指定可能。

WAN インタフェースを設定した時には、*secondary* は指定できない。

10.2.2 DNS サーバーアドレスを取得するインタフェースの設定

[書式]

```
dns server dhcp interface
no dns server dhcp
```

[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
 - [初期値]: -

[説明]

DNS サーバーアドレスを取得するインタフェースを設定する。このコマンドでインタ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。

dns server コマンドで DNS サーバーが明示的に指定されているか、**dns server select**、**dns server pp** コマンドの設定により問い合わせをする DNS サーバーが決められた場合には、その設定が優先される。

[ノート]

この機能は指定したインタフェースが DHCP クライアントとして動作していなければならない。
WAN インタフェースは Rev.11.00.16 以降で指定可能。

10.2.3 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 インタフェース名、WAN インタフェース名
 - [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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

10.2.4 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 インタフェース名、WAN インタフェース名
 - [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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

10.2.5 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 インタフェース名、WAN インタフェース名
 - [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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

10.2.6 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 インタフェース名、WAN インタフェース名
 - [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 インタフェースは Rev.11.00.16 以降で指定可能。
 WAN インタフェースを設定した時には、*secondary* は指定できない。

[設定例]

1. 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。)
```

10.2.7 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

設定値	説明
off	インタ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ーが働き、*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]

タイマー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。タイマーの満了前にリンクアップした場合にはタイマーはクリアされ、情報を解放しない。タイマーの満了前に情報のリース期間が満了した場合には、タイマーはクリアされ、情報は解放される。以下のコマンド実行時には、動作中のタイマーはクリアされる。

ip interface address, ip pp remote address, ip pp remote address pool, dhcp client release linkdown

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。

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。

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。

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。

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。

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

設定値	説明
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。

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。

[ノート]

Rev.11.00.25 以降のファームウェアで rebound オプションを指定可能。

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。

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。

[ノート]

Rev.11.00.25 以降のファームウェアで rebound オプションを指定可能。

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いて、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、traceroute に対して反応がなくなるなどの現象になる。

Rev.11.00.36 以降で使用可能。

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。

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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

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。

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。

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。

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。

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。

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。

[ノート]

Rev.11.00.25 以降のファームウェアで rebound オプションを指定可能。

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。

[ノート]

Rev.11.00.25 以降のファームウェアで rebound オプションを指定可能。

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。

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。

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-decrypted-ipsec send switch
no ipv6 icmp error-decrypted-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。

Rev.11.00.36 以降で使用可能。

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。

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 Rev.11.00.36 以降で使用可能。

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 Rev.11.00.36 以降で使用可能。

12.3 トンネルインタ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
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
ipudp	IPUDP トンネル

- [初期値]: ipip

[説明]

トンネルインタ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。

PPTP 機能を実装していないモデルでは、**pptp** キーワードは使用できない。

Rev.11.00.36 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。

データコネクタ接続機能を実装していないモデルでは、**ipudp** キーワードは使用できない。

12.4 トンネルインタフェースの 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]

トンネルインタフェースの IPv4 アドレスとネットマスクを設定する。

12.5 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。

12.6 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*、*ipip* の場合である。

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。

12.7 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 pptp、ipudp の場合である。

pptp 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。

第 13 章

IPsec の設定

暗号化により IP 通信に対するセキュリティを保証する 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・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が指定可能なパラメータ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・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・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、トンネルインタフェースという仮想的なインタフェースを定義し、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フェースはトンネルインタ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		トンネルインタフェース番号による設定
<ul style="list-style-type: none"> • pp enable • pp disable • pp select 	<==>	<ul style="list-style-type: none"> • tunnel enable • tunnel disable • tunnel select

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 に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・ゲートウェイの識別子とトンネルインタフェース番号はモデルにより異なり、以下の表のようになります。

モデル	セキュリティ・ゲートウェイの識別子	トンネルインタフェース番号
NVR500	1-4	1-4

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]

Rev.11.00.36 以降で使用可能。

13.2 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・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]

Rev.11.00.36 以降で使用可能。

[設定例]

```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 4 0xCDEEEDC0CDEDCD
```

13.3 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・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 パラメータを指定する書式は、指定したセキュリティ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
```

Rev.11.00.36 以降で使用可能。

13.4 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・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が自分の設定と異なる場合でも、そのパラメータ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と対応するコマンドは以下の通りである。

パラメータ	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。

Rev.11.00.36 以降で使用可能。

13.5 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・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]

Rev.11.00.36 以降で使用可能。

13.6 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]

鍵交換のパケット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]

相手側セキュリティ・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。

Rev.11.00.36 以降で使用可能。

13.7 相手側のセキュリティ・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・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。

本コマンドの影響、注意点については以下の通り。

- 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。

[ノート]

Rev.11.00.36 以降で使用可能。

13.8 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・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。

本コマンドの影響、注意点については以下の通り。

- 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。

[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。

Rev.11.00.36 以降で使用可能。

13.9 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・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。

Rev.11.00.36 以降で使用可能。

13.10 自分側のセキュリティ・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・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
fqdn	ID_FQDN
user-fqdn	ID_USER_FQDN
key-id	ID_KEY_ID

- [初期値]: -

[説明]

自分側のセキュリティ・ゲートウェイの名前と ID の種類を設定する。

[ノート]

Rev.11.00.36 以降で使用可能。

13.11 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フェースの IP アドレスを用いて IKE を起動する。

Rev.11.00.36 以降で使用可能。

13.12 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。

Rev.11.00.36 以降で使用可能。

13.13 IKE キープアライブ機能の設定

[書式]

```
ipsec ike keepalive use gateway_id switch [down=disconnect]
ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect]
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・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、以下のように動作が異なる。

- 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* パラメータは設定内容が反映される。

[ノート]

相手先が PP インタ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。

`length` パラメータで指定するのは 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。

Rev.11.00.36 以降で使用可能。

13.14 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・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]

Rev.11.00.36 以降で使用可能。

13.15 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・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
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]

Rev.11.00.36 以降で使用可能。

[設定例]

```
# ipsec ike encryption 1 aes-cbc
```

13.16 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 (4..8)
 - [初期値]: 8

[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。

Rev.11.00.36 以降で使用可能。

13.17 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・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。

本コマンドの影響、注意点については以下の通り。

- 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。
- **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。

[ノート]

Rev.11.00.36 以降で使用可能。

13.18 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・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
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]

Rev.11.00.36 以降で使用可能。

13.19 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。

Rev.11.00.36 以降で使用可能。

13.20 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・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 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* パラメータを 1 に設定する必要がある。

機種	リビジョン
RTX3000	Rev.9.00.56 以前
RTX1200	Rev.10.01.45 以前
RTX810	Rev.11.01.06 以前
FWX120	Rev.11.03.02

[ノート]

Rev.11.00.36 以降で使用可能。

13.21 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・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 パラメータを 1 に設定する必要がある。

[ノート]

Rev.11.00.36 以降で使用可能。

13.22 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・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。

Rev.11.00.36 以降で使用可能。

13.23 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・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]

Rev.11.00.36 以降で使用可能。

13.24 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・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]

Rev.11.00.36 以降で使用可能。

13.25 XAUTH 認証に使用するユーザ 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]: ユーザ識別番号 (1..1000)
 - [初期値]: -
- *username*
 - [設定値]: ユーザ名 (256 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]

IKEv1 の XAUTH 認証に使用するユーザ ID を設定する。

[ノート]

username と *password* は 3 文字以上に設定してください。

Rev.11.00.36 以降で使用可能。

13.26 XAUTH 認証に使用するユーザ 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]: ユーザ識別番号 (1..1000)
 - [初期値]: -
- *attribute=value*
 - [設定値]: ユーザ属性
 - [初期値]: xauth=off

[説明]

IKEv1 の XAUTH 認証に使用するユーザ 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、このフィルタを適用する

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 ID が属しているユーザグループに対して、**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。

Rev.11.00.36 以降で使用可能。

13.27 XAUTH 認証に使用するユーザグループの設定

[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]: ユーザグループ識別番号 (1..1000)
 - [初期値]: -
- *userid*
 - [設定値]: ユーザ識別番号もしくはユーザ識別番号の範囲 (複数指定することが可能)
 - [初期値]: -

[説明]

IKEv1 の XAUTH 認証に使用するユーザグループを設定する。

[ノート]

Rev.11.00.36 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
```

13.28 XAUTH 認証に使用するユーザ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]: ユーザグループ識別番号 (1..1000)
 - [初期値]: -
- *attribute=value*
 - [設定値]: ユーザグループ属性
 - [初期値]: xauth=off

[説明]

IKEv1 の XAUTH 認証に使用するユーザ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 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 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、このフィルタを適用する

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、該当のユーザグループに含まれるすべてのユーザに対して有効となる。

Rev.11.00.36 以降で使用可能。

13.29 XAUTH によるユーザ認証の設定

[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、該当のユーザグループに含まれるユーザを認証の対象とする。

group_id の指定がない場合や、指定したユーザグループに含まれるユーザ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 isakmp SA パラメータの提案に、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 によるユーザ認証を行う。

Rev.11.00.36 以降で使用可能。

13.30 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]

Rev.11.00.36 以降で使用可能。

13.31 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、*option* を指定していると XAUTH では接続できない。

Rev.11.00.36 以降で使用可能。

13.32 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。

Rev.11.00.36 以降で使用可能。

13.33 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・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。

[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* パラメータを設定することもできる。

Rev.11.00.36 以降で使用可能。

13.34 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・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。

Rev.11.00.36 以降で使用可能。

13.35 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。

13.35.1 SA の寿命の設定

[書式]

ipsec ike duration *sa gateway_id second [kbytes] [rekey rekey]*

no ipsec ike duration *sa gateway_id [second [kbytes] [rekey rekey]]*

[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・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]: キロ単位のバイト数 (100..100000)
 - [初期値]: -
- *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> パラメータで <i>isakmp-sa (ike-sa)</i> を指定したときのみ設定可能)

- [初期値]: 75%

[説明]

各 SA の寿命を設定する。

kbytes パラメータを指定した場合には、*second* パラメータ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* パラメータは SA パラメータとして *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。

rekey パラメータは SA を更新するタイミングを決定する。例えば、*second* パラメータで 20000 を指定し、*rekey* パラメータで 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* パラメータは *second* パラメータに対する比率を表すもので、*kbytes* パラメータの値とは関係がない。

sa パラメータで *isakmp-sa(ike-sa)* を指定したときに限り、*rekey* パラメータで '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。

本コマンドの影響、注意点については以下の通り。

- 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。

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]

Rev.11.00.36 以降で使用可能。

13.35.2 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・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-1
sha256-hmac	HMAC-SHA-2-256

- [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・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。

- 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

[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。

ah_algorithm、および *esp_algorithm* パラメータは省略可能。

Rev.11.00.36 以降で使用可能。

[設定例]

```
# ipsec sa policy 1 1 esp aes-cbc sha-hmac
```

13.35.3 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。

Rev.11.00.36 以降で使用可能。

13.35.4 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・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。

RT シリーズでは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。

Rev.11.00.36 以降で使用可能。

13.35.5 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

[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。

[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。

Rev.11.00.36 以降で使用可能。

13.35.6 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]

Rev.11.00.36 以降で使用可能。

13.36 トンネルインタフェース関連の設定

13.36.1 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]

Rev.11.00.36 以降で使用可能。

13.36.2 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。

トンネルインタフェース毎のコマンドである。

[ノート]

トンネルインタフェースの MTU と実インタフェースの 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ならない時には、このコマンドの設定に関わらず DF ビットは 0 になる。

Rev.11.00.36 以降で使用可能。

13.36.3 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フェースで使用する SA のポリシーを設定する。

[ノート]

Rev.11.00.36 以降で使用可能。

13.36.4 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 による暗号化の後の行われる。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、一定の効果が得られる。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フェースが LAN であってもデータ圧縮効果を期待できる。

Rev.11.00.36 以降で使用可能。

13.36.5 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フェースを展開元として、当該インタ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フェースを設定する。

展開元のトンネルインタフェースに設定することで、展開先のトンネルインタ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。なお、末尾に (*1) または (*2) が付加されているコマンドについては [ノート] を参照のこと。

- **ipsec tunnel**
- **ipsec sa policy**
- **ipsec ike** で始まるコマンドのうち、パラメータにセキュリティ・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・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、特定のパラメータの値が展開元のトンネルインタ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、当該パラメータの値は展開先のトンネルインタフェース番号に置換される。

コマンド	パラメータ
ipsec tunnel	ポリシー ID
ipsec sa policy	ポリシー ID
ipsec ike で始まるコマンド	セキュリティ・ゲートウェイの識別子
ipsec auto refresh	セキュリティ・ゲートウェイの識別子
tunnel enable	トンネルインタフェース番号

ipsec sa policy コマンドでは、セキュリティ・ゲートウェイの識別子が展開先のトンネルインタ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・ゲートウェイの名前の末尾に展開先のトンネルインタフェース番号が付加される。

展開元のトンネルインタ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]

トンネルインタフェースが選択されている時のみ使用できる。

Rev.11.00.36 以降で使用可能。

[設定例]

展開先のトンネルインタフェースとして、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 2 3-4
```

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
```

13.37 トランスポートモード関連の設定

13.37.1 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]

Rev.11.00.36 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
```

13.37.2 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]

Rev.11.00.36 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 *
```

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。

14.1 L2TP/IPsec 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/IPsec を有効にする
off	L2TP/IPsec を無効にする

- [初期値]: off

[説明]

L2TP を動作させるか否かを設定する。

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]

Rev.11.00.36 以降で使用可能。

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。
NVR500 の場合には "NVR500" 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]

Rev.11.00.36 以降で使用可能。

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
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]

Rev.11.00.36 以降で使用可能。

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]

Rev.11.00.36 以降で使用可能。

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]

Rev.11.00.36 以降で使用可能。

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

[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 のコネクション制御に関するログを SYSLOG に出力する
off	L2TP のコネクション制御に関するログを SYSLOG 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]

Rev.11.00.36 以降で使用可能。

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。

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 インタフェース名
tunnelN-tunnelM	TUNNEL インタフェースの範囲

- [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フェースを指定する。

第 2 書式は `anonymous` インタフェースを使って多数の接続先を登録するために複数連続したトンネルインタフェースをバインドする場合に用いる。

`anonymous` インタフェースに対しては第 1 書式・第 2 書式ともに指定可能であり、同時に続けて併記することも可能だが、`anonymous` インタフェース以外が選択されている場合は、複数のトンネルインタフェースを指定するとエラーとなる。

[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。

L2TP/IPsec は Rev.11.00.36 以降で使用可能。

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。

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 (Rev.11.00.38 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。

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。

Rev.11.00.38 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。

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。

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。

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。

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

[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 のコネクション制御の 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。

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。

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。

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を選択する。

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、その後の監視タイマは 1 秒に短縮される。

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。

第 16 章

データコネクタ接続機能の設定

データコネクタを利用して拠点間接続を行うにはトンネルインタフェースを利用します。トンネリングの章を参照してください。

また、NGN 網へ接続するためには、**sip use**、**ngn type**、**show status ngn** コマンドを利用します。これらの項目も合わせて参照してください。

16.1 NGN 網を介したトンネルインタ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。

16.2 NGN 網を介したトンネルインタ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]:

設定値	説明
64k	64kbit/s
512k	512kbit/s
1m	1Mbit/s
1k..1000m	帯域

- [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。
`arrivepermit` オプションは、Rev.11.00.16 以降で使用可能である。
`bandwidth` パラメータは、Rev.11.00.35 以降のファームウェアで任意の数値を設定可能である。

16.3 NGN 網を介したトンネルインタ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。

16.4 NGN 網を介したトンネルインタ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。

16.5 NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定

[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 インタフェース名	LAN ポート

- [初期値]: auto

[説明]

NGN 網を介したトンネルインタフェースで使用する LAN インタフェースを設定する。
 auto に設定した時はトンネルインタ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。

16.6 NGN 網を介したトンネルインタ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フェースで使用する相手番号は、**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。

[ノート]

Rev.11.00.20 以降で使用可能。

16.7 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 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]

トンネルインタフェースが選択されている時にのみ使用できる。

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**

Rev.11.00.36 以降で使用可能。

16.8 NGN 電話番号を RADIUS で認証するときに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 で認証するときに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。

Rev.11.00.36 以降で使用可能。

16.9 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**

Rev.11.00.36 以降で使用可能。

16.10 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**

Rev.11.00.36 以降で使用可能。

16.11 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。

[ノート]

Rev.11.00.35 以降で使用可能。

第 17 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。このとき NVR500 は SNMP エージェントとなります。

NVR500 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。

NVR500 の状態を通知する SNMP メッセージをトラップと呼びます。NVR500 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。

17.1 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>any</i>	すべてのホストからのアクセスを許可する
<i>none</i>	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 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。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN を指定できるのは Rev.11.00.25 以降である。

17.2 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。

17.3 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。

17.4 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。

17.5 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。

17.6 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
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* 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。

[ノート]

HOST パラメーターに IP アドレスの範囲や *lanN* を指定できるのは Rev.11.00.25 以降である。

17.7 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。

17.8 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。

17.9 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。

17.10 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。

17.11 SNMP 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

17.12 SNMP 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。

17.13 USM で管理するユーザの設定

[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]: ユーザ番号 (1..65535)
 - [初期値]: -
- *name*
 - [設定値]: ユーザ名 (32 文字以内)
 - [初期値]: -
- *group_id*
 - [設定値]: ユーザグループ番号 (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	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情報を設定する。

ユーザ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設定と一致させておく必要がある。

17.14 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
any	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* パラメータに合致していても、*user_id* パラメータで指定したユーザに合致しなければアクセスはできない。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN を指定できるのは Rev.11.00.25 以降である。

17.15 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
include	指定したオブジェクト ID を管理対象にする
exclude	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 オブジェクトの集合である。

type パラメータと *oid* パラメータの組は、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
```

17.16 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
<i>view_id</i>	読み出し可能なアクセス権を設定するビュー番号
none	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
<i>view_id</i>	書き込み可能なアクセス権を設定するビュー番号
none	書き込み可能なビューを設定しない

- [初期値]: -

[説明]

ユーザ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 オブジェクトへのアクセスは禁止される。

17.17 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
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
- *user_id*
 - [設定値]: ユーザ番号
 - [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設定は **snmpv3 usm user** コマンドで設定したユーザ設定が用いられる。

type パラメータで '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。

17.18 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。

17.19 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"
```

17.20 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"
```

17.21 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 "NVR500 working with a master mode"
```

17.22 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 トラップについては、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 トラップについては、**snmp trap send linkdown** コマンドによってインタフェース毎に制御できる。あるインタフェースについて、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。

17.23 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 インタフェース名
- WAN インタフェース名
- BRI インタフェース名

- [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]

指定したインタフェースの linkDown トラップを送信するか否かを設定する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

17.24 PP インタフェースの情報を 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 インタフェースを MIB2 の範囲で表示するかどうかを決定する。

17.25 トンネルインタフェースの情報を 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、トンネルインタフェースを MIB2 の範囲で表示するかどうかを決定する。

17.26 スイッチのインタフェースの情報を 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 <code>yrIfSwitchDisplayAtMib2</code> を "enabled(1)" とする
off	MIB 変数 <code>yrIfSwitchDisplayAtMib2</code> 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、スイッチのインタフェースを MIB2 の範囲で表示するかどうかを決定する。

17.27 PP インタ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事ができる。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、インタフェースには付与されない。そのため、SNMP でインタフェースの 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。

17.28 LAN インタ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。

17.29 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。

Rev.11.00.16 以降で使用可能。

17.30 スイッチへ静的に付与するインタ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。

17.31 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。

17.32 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
poeterminate	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 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。

[ノート]

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は Rev.11.00.23 以降で設定可能。

17.33 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

246 | コマンドリファレンス | SNMP の設定

- [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。

第 18 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。

18.1 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ネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザネーム (**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。

Rev.11.00.36 以降で使用可能。

18.2 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。

Rev.11.00.36 以降で使用可能。

18.3 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。

Rev.11.00.36 以降で使用可能。

18.4 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。

Rev.11.00.36 以降で使用可能。

18.5 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。

Rev.11.00.36 以降で使用可能。

18.6 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。

Rev.11.00.36 以降で使用可能。

18.7 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。

Rev.11.00.36 以降で使用可能。

18.8 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。

Rev.11.00.36 以降で使用可能。

18.9 RADIUS 再送信パラメータの設定

[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。

Rev.11.00.36 以降で使用可能。

第 19 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。

NVR500 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 ディスクリプタと呼び、それぞれの NAT ディスクリプタには、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 ディスクリプタはインタフェースに対して適用されます。インタ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、インタフェースから本機を経由して他のインタ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。

19.1 インタフェースへの NAT ディスクリプタ適用の設定

[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 インタフェース名、WAN インタフェース名
 - [初期値]: -
- *nat_descriptor_list*
 - [設定値]: 空白で区切られた NAT ディスクリプタ番号 (1..2147483647) の並び (16 個以内)
 - [初期値]: -

[説明]

適用されたインタ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 インタフェースの場合、NAT ディスクリプタ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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

19.2 NAT ディスクリプタの動作タイプの設定

[書式]

```
nat descriptor type nat_descriptor type
```

no nat descriptor type nat_descriptor [type]

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (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

[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 個利用可能の場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

19.3 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	ip interface address コマンドで設定されている IP アドレス
secondary	ip interface secondary address コマンドで設定されている 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。
適用されるインタフェースにより使用できるパラメータが異なる。

適用インタフェース	LAN	PP	トンネル
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP アドレス	○	○	○

19.4 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。

19.5 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。

ネットマスクによる範囲指定は、Rev.11.00.23 以降のファームウェアで使用可能である。

19.6 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。

19.7 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。

19.8 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。ただし、HTTP 通信の場合、このコマンドでの設定値にかかわらず約 5 秒でセッション情報を削除する。

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。

19.9 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。

19.10 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_range
```

```
no nat descriptor masquerade port range nat_descriptor [port_range]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]:-
- *port_range*
 - [設定値]: 間に - をはさんだポート番号の範囲 (1024-65534)
 - [初期値]: 60000-64095

[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。

19.11 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。

19.12 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。

19.13 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します。

19.14 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	sip use 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。

19.15 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 探索が行われないことになるので、通信効率が下がる可能性がある。

19.16 IP マスカレードで変換する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..4096)
 - [初期値]: 4096

[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。

第 20 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** 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** コマンド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。

20.1 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。

20.2 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。

20.3 DNS サーバーの IP アドレスの設定

[書式]

```
dns server ip_address [ip_address...]
no dns server [ip_address...]
```

[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]:-

[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。

[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。

20.4 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。

20.5 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
no dns server pp [peer_num]
```

[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]:-

[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。

dns server コマンドで DNS サーバーが明示的に指定されている場合には、そちらの設定が優先される。**dns server** コマンドに指定したサーバーから返事がない場合には、相手先への接続と DNS サーバーの通知取得が行われる。

[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 on** 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。

[設定例]

```
# pp select 2
```

```
pp2# ppp ipcp msextn on
pp2# dns server pp 2
```

20.6 DHCP/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
msextn	IPCP MS 拡張による通知

- [初期値]: dhcp および msextn

- server*

- [設定値]:

設定値	説明
none	一切通知しない
me	本機自身
server	dns server コマンドに設定したサーバー群

- [初期値]: me server

[説明]

DHCP や IPCPMS 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。none を設定すれば、他の設定に関わらず DNS サーバーの通知を行わなくなる。me は本機自身の DNS リカーシブサーバー機能を使うことを通知する。server では、**dns server** コマンドに設定したサーバー群を通知することになる。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。

20.7 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。

20.8 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。

20.9 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 [server2] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id pp peer_num [default-server] [type] query [original-sender] [restrict pp connection-pp]
```

```
dns server select id dhcp interface [default-server] [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 インタフェース名または WAN インタフェース名
 - [初期値]: -
- *default-server*
 - [設定値]: *peer_num* パラメータ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]: -

[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、**dns server** コマンドで指定された DNS サーバーを用いる。

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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

20.10 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 パラメータによって以下のように意味が異なる

<i>type</i> パラメータ	<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、*ttl* パラメータの設定値がセットされる。*ttl* パラメータ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
```

20.11 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で扱うとき、始点番号がランダムに変化することを考慮しておく必要がある。

20.12 DNS サーバーへアクセスできるホストの IP アドレス設定

[書式]

```
dns host ip_range [ip_range [...]]
no dns host
```

[設定値及び初期値]

- *ip_range*: DNS サーバーへアクセスを許可するホストの 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
any	すべてのホストからのアクセスを許可する
lan	すべての LAN ポート側ネットワーク内ならば許可する
lanN	ひとつの任意の LAN ポート側ネットワーク内ならば許可する (N はインタフェース番号)
none	すべてのホストからのアクセスを禁止する

- [初期値]: any

[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。

20.13 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。

20.14 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。

20.15 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。

第 21 章

優先制御

優先制御の機能は、インタ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。

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。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、優先制御、単純 FIFO の中から選択します。これはインタフェースごとに選択することができます。

21.1 インタ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 インタフェース名、WAN インタフェース名
 - [初期値]: -
- *speed*
 - [設定値]: インタフェース速度 (bit/s)
 - [初期値]: -

[説明]

指定したインタフェースに対して、インタフェースの速度を設定する。

queue interface type コマンドで **priority** の設定が必要。

[ノート]

speed パラメータの後ろに '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。WAN インタフェースは Rev.11.00.16 以降で指定可能。

21.2 クラス分けのためのフィルタ設定

[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]]]]
no queue class filter num [...]
```

[設定値及び初期値]

- *num*
 - [設定値]: クラスフィルタの識別番号 (1..100)
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..16)
 - [初期値]: -
- *cos*
 - [設定値]:

設定値	説明
0-7	CoS 値

設定値	説明
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 IP アドレス
- [設定値]:
 - 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
 - *(すべての IP アドレスまたは IPv6 アドレスに対応)
 - 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。
- [初期値]: -
- *dest_addr*: IP パケットの終点 IP 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

ニーモニック	ポート番号
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]: -

[説明]

クラス分けのためのフィルタを設定する。

`cos=cos` 指定を行うと、フィルタ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、各インタフェースにおける `queue interface class filter list` コマンドで設定する。

[ノート]

`cos` パラメータは Rev.11.00.16 以降で指定可能。

Rev.11.00.23 以降で `src_port` または `dest_port` に `submission` を指定可能。

Rev.11.00.23 以降で IPv6 アドレスの指定が可能。

[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 *
```

21.3 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 インタフェース名、WAN インタフェース名
 - [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

- [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-level オプションは *TYPE* パラメーターに *priority* 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、帯域速度の計算をブリアンブル、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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。
shaping-level オプションは Rev.11.00.28 以降で指定可能。

21.4 MP インタリーブの設定

[書式]

```
ppp mp interleave [delay] switch
no ppp mp interleave [[delay] switch]
```

[設定値及び初期値]

- *delay*
 - [設定値]: 遅延 (ミリ秒)
 - [初期値]: 30
- *switch*
 - [設定値]:

設定値	説明
on	MP インタリーブを使用する
off	MP インタリーブを使用しない

- [初期値]: off

[説明]

MP インタリーブを使用するかどうかを設定する。*delay* では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、*delay* の値と回線速度により決定される。

[ノート]

delay で設定した遅延が保証されるわけではない。
データの受信側でも同じ設定をしておかないと、効果が発揮されない。

同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。

```
ppp ccp type none
```

[設定例]

```
# queue class filter 1 4 ip VOIP-GATEWAY * * * *
# queue class filter 2 3 ip * * icmp * *
# queue class filter 3 1 ip * * * * *
# pp select 1
pp1# pp bind bri2.1
pp1# queue pp type priority
pp1# queue class filter list 1 2 3
pp1# isdn remote address call 03-123-4567
pp1# ppp mp use on
pp1# ppp mp interleave on
pp1# ppp mp maxlink 1
pp1# ppp ccp type none
pp1# pp enable 1
```

21.5 クラス分けフィルタの適用

[書式]

```
queue interface class filter list filter_list
queue pp class filter list filter_list
no queue interface class filter list [filter_list]
no queue pp class filter list [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
 - [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたクラスフィルタの並び
 - [初期値]: -

[説明]

指定した LAN インタフェース、WAN インタフェースまたは選択されている PP インタフェースに対して、**queue class filter** コマンドで設定したフィルタを適用する順番を設定する。フィルタ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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

21.6 クラス毎のキュー長の設定

[書式]

```
queue interface length len1 [len2...len4]
queue pp length len1 [len2...len4]
no queue interface length [len1...]
no queue pp length [len1...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *len1..len4*
 - [設定値]: クラス 1 からクラス 4 のキュー長 (1..10000)
 - [初期値]:
 - 40 (LAN)

- 20 (PP)

[説明]

インタフェースに対して、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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

21.7 デフォルトクラスの設定

[書式]

```
queue interface default class class
queue pp default class class
no queue interface default class [class]
no queue pp default class [class]
```

[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
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..16)
 - [初期値]: 2

[説明]

インタフェースに対して、フィルタ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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

第 22 章

連携機能

22.1 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。

22.2 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。

22.3 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 インタフェースまたは WAN インタ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 インタフェースまたは WAN インタフェース
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 インタフェースの **speed lan** コマンドの設定値、または WAN インタフェースの **speed wan1** コマンドの設定値に上書きする。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、または **queue wan1 class property** コマンドの **bandwidth** パラメータ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 インタフェースが設定されている場合には、その LAN インタフェースの **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** パラメータに測定結果が反映される。WAN インタ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、インタフェースに付与された IP アドレスを使用する

WAN インタフェースは Rev.11.00.16 以降で指定可能。

22.4 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、制御対象のインタフェースの速度はその時点の設定が保持される。

22.5 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>	インタフェース名 (LAN,TUNNEL)
------------------	-----------------------

- *interface overflow*
 - LAN インタ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 インタフェース名
------------------	--------------

- *interface [class] transmit*
 - インタ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>	インタフェース名 (LAN,TUNNEL)
<i>class</i>	クラス番号 (LAN インタフェースの場合)

- [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	説明
<i>interval</i>	監視する間隔 (1-65535)[sec]、省略時は 10[sec]
<i>syslog</i>	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** 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。

22.6 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 インタフェース
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。

22.7 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。

第 23 章

IPv6

23.1 共通の設定

23.1.1 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。

23.1.2 IPv6 インタフェースのリンク MTU の設定

[書式]

```
ipv6 interface mtu mtu
ipv6 pp mtu mtu
no ipv6 interface mtu [mtu]
no ipv6 pp mtu [mtu]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mtu*
 - [設定値]: MTU の値 (1280..1500)
 - [初期値]: 1500

[説明]

IPv6 インタフェースの MTU の値を設定する

23.1.3 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.11.00.35 以前)
 - auto(Rev.11.00.36 以降)

[説明]

インタ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、インタフェースの MTU、もしくは PP インタ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。

23.1.4 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]

Rev.11.00.35 以降で使用可能。

23.1.5 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。

23.1.6 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]

本コマンドで fast を設定した場合、IPv6 マルチキャストパケットもファストパス機能で処理される。

23.2 IPv6 アドレスの管理

23.2.1 インタフェースの 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 インタフェース名、LOOPBACK インタフェース名
 - [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]*
 - *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>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース 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フェースに向く。

LOOPBACK インタフェースを指定した場合は、*auto*、*dhcp*、*address_type*、*proxy* は指定できない。

address_type を指定できるのは Rev.11.00.16 以降である。

[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
```

23.2.2 インタ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]`

- `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
<code>prefix_interface</code>	転送元のインタフェース名

- `interface_id`

設定値	説明
<code>interface_id</code>	インタフェース ID

- `prefix_len`

設定値	説明
<code>prefix_len</code>	IPv6 プレフィックス長

- [初期値]:-

[説明]

インタフェースに 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 インタフェースやトンネルインタフェースでは LAN1 インタフェースの 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 インタフェースは指定できない。

[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。)

23.2.3 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]

Rev.11.00.20 以降で使用可能。

23.2.4 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 インタフェース名
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
off	DHCPv6 を使わない
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]

各インタフェースにおける DHCPv6 の動作を設定する。

[ノート]

value パラメータは Rev.11.00.16 以降で指定可能。

23.2.5 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 インタフェース名
 - [初期値]: -
- *count*
 - [設定値]: 選択したインタフェースでの DAD の再送回数 (0..10)
 - [初期値]: 1

[説明]

インタフェースに 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。

23.2.6 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 によりインタフェースに自動的に設定される IPv6 アドレスの 1 インタフェースあたりの最大数を設定する。

23.2.7 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*: LAN インタフェース名
 - [設定値]:

設定値	説明
prefix	プレフィックスの最長一致

設定値	説明
lifetime	寿命の長いほうを優先

- [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 アドレスと候補を選択して、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' を設定しておけばいいが、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。

23.3 近隣探索

23.3.1 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>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース 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
- [設定値]:

設定値	説明
0..4294967295	Rev.11.00.16 以降
60..15552000	上記以外

- [初期値]: 604800
- valid_lifetime: プレフィックスの有効寿命
- [設定値]:

設定値	説明
0..4294967295	Rev.11.00.16 以降
60..15552000	上記以外

- [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 (Rev.11.00.16 以降では 0 以上 4294967295 以下、それ以外のリビジョンでは 60 以上 15552000 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。

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。

[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。)

23.3.2 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、DHCPv6 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。
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 の場合はインタフェースの MTU を採用する。

- [初期値]:
 - m_flag = off
 - o_flag = off
 - 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

[説明]

インタ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]

adv-retrans-time オプションと adv-cur-hop-limit オプションは、Rev.11.00.16 以降で指定できる

23.4 経路制御

23.4.1 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

- `dhcp interface`

設定値	説明
interface	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

- `tunnel tunnel_num` : トンネルインタフェースへの経路

- [初期値] :-

- `parameter` : 以下のパラメータを空白で区切り複数設定可能

- [設定値] :

設定値	説明
metric <i>metric</i>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
hide	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。LAN インタフェースが複数ある機種では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。LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

23.5 RIPng

23.5.1 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。

23.5.2 インタフェースにおける 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。

23.5.3 インタフェースにおける 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。

23.5.4 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]

- *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。

23.5.5 インタ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。

23.5.6 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]: フィルタ番号
 - [初期値]:-

[説明]

インタ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を設定する。

23.5.7 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	ipv6 pp rip connect interval 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
```

23.5.8 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
```

23.5.9 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	ipv6 pp rip connect interval 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
```

23.5.10 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
```

23.5.11 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。

23.5.12 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。

23.6 フィルタの設定

23.6.1 IPv6 フィルタの定義

[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]: 静的フィルタ番号 (1..21474836)
 - [初期値]: -
- *pass_reject*
 - [設定値]: フィルタのタイプ (**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
 - * (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
 - 省略した場合は一つの * 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 のフィルタを定義する。

[ノート]

近隣探索に関係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

[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 * *
```

23.6.2 IPv6 フィルタの適用

[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 インタフェース名、LOOPBACK インタフェース名、NULL 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番号の並び (静的フィルタと動的フィルタの数の合計として 128 個以内)
 - [初期値]:-
- *dynamic*: キーワード後に動的フィルタの番号を記述する
 - [初期値]:-

[説明]

IPv6 フィルタをインタフェースに適用する。

[ノート]

LOOPBACK インタフェースと NULL インタフェースでは動的フィルタは使用できない。
NULL インタフェースで *direction* に 'in' は指定できない。

23.6.3 IPv6 動的フィルタの定義

[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/
 - dhcpcv6c/dhcpcv6s/ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
 - ping/ping6/tcp/udp
 - [初期値]: -
- *filter_list*
 - [設定値]: **ipv6 filter** コマンドで登録されたフィルタ番号のリスト
 - [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に該当するコネクション (トリガ) 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。

23.7 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、下流のインタフェースに存在するリスナーの情報を、上流のインタ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 (Multicast Listener Discovery) 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モード (`FilterMode`) とソースリスト (`SourceList`) を使用します。フィルタモードには `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。

23.7.1 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、Rev.11.00.35 以降で指定可能。

23.7.2 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* を設定したインタフェースで通知される。もし、このインタフェースが MLDv1 を使う場合には、*filter_mode* や *source* の値は無視される。

23.8 近隣要請

23.8.1 アドレス重複チェックをトリガ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。

第 24 章

アナログ通信機能の設定

NVR500 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** コマンドで行ないます。実際の許可拒否動作はポート毎に行なうことができ、**analog arrive restrict** コマンドにより動作を指定します。

NVR500 の TEL ポートの電気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すぎ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。

24.1 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
DTMF 検出レベルの設定	63	analog dtmf level
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

LINE ポート(回線)側の設定

機能	機能番号	対応するコンソールコマンド
ダイヤルの種別選択	201	pstn dial type
ナンバー・ディスプレイ着信識別	203	pstn number display
付加サービス機能設定	204	pstn supplementary-service
回線側のポーズ時間設定(秒)	205	pstn pause timer
フッキング時間設定(1/10 秒)	206	pstn hooking timer
送話 PAD の音量設定	207	pstn pad send
受話 PAD の音量設定	208	pstn pad receive
LINE ポート使用制限の設定	209	pstn use

24.2 TEL ポートごとの設定

24.2.1 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。

24.2.2 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、ISDN 回線を使用する場合にのみ有効である。

24.2.3 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* パラメータで指定したポートへは、*type* パラメータ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、ISDN 回線を使用する場合にのみ有効である。

24.2.4 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、ISDN 回線を使用する場合にのみ有効である。

24.2.5 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]

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。

24.2.6 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)

24.2.7 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、ISDN 回線と PSTN 回線を使用する場合にのみ有効である。

24.2.8 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。

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。

24.2.9 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、ISDN 回線を使用する場合にのみ有効である。

24.2.10 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、ISDN 回線を使用する場合にのみ有効である。

24.2.11 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
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。

24.2.12 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、ISDN 回線を使用する場合にのみ有効である。

24.2.13 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]

- 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。
- 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なうことはできない。
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。

24.2.14 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、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。

24.2.15 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
name-display	ネーム・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。
 name-display に設定すると、ネーム・ディスプレイが使用可能になる。

[ノート]

ナンバー・ディスプレイサービスの契約が必要。
 ネーム・ディスプレイを使用する場合は、ネーム・ディスプレイサービスの契約も必要。

- 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。

24.2.16 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。

24.2.17 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。

24.2.18 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。

24.2.19 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。

24.2.20 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。

24.2.21 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]: 8
- *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]: 2

[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。

24.2.22 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る。

[ノート]

Rev.11.00.31 以降で使用可能。

24.2.23 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

設定値	説明
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。

[ノート]

Rev.11.00.31 以降で使用可能。

24.2.24 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。

24.2.25 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

24.2.26 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、ISDN 回線を使用する場合にのみ有効である。

24.2.27 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、ISDN 回線を使用する場合にのみ有効である。

24.2.28 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、ISDN 回線を使用する場合にのみ有効である。

24.2.29 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

設定値	説明
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、ISDN 回線を使用する場合にのみ有効である。

24.2.30 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]

着信転送を行なう際、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、ISDN 回線を使用する場合にのみ有効である。

24.2.31 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
-12dB	-12dB PAD 挿入
-15dB	-15dB PAD 挿入
-18dB	-18dB PAD 挿入
-21dB	-21dB PAD 挿入
off	PAD なし

- [初期値]: off

[説明]

送話 PAD を設定する。

24.2.32 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

設定値	説明
-6dB	-6dB PAD 挿入
-9dB	-9dB PAD 挿入
-12dB	-12dB PAD 挿入
-15dB	-15dB PAD 挿入
-18dB	-18dB PAD 挿入
-21dB	-21dB PAD 挿入
off	PAD なし

- [初期値]: off

[説明]

受話 PAD を設定する。

24.2.33 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、電話の発着信を行な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、ISDN 回線を使用する場合にのみ有効である。

24.2.34 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

設定値	説明
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]

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。

24.2.35 DTMF 検出レベルの設定

[書式]

`analog dtmf level port level`

`no analog dtmf level 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] :-
- *level*

- [設定値] :

設定値	説明
off	off
-3dB	-3dB
-6dB	-6dB
-9dB	-9dB
-12dB	-12dB
-15dB	-15dB
-18dB	-18dB
-21dB	-21dB

- [初期値] : off

[説明]

TEL ポートの DTMF 信号検出レベルを設定する。

[ノート]

従来機種とは *level* パラメータ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。

24.2.36 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。

24.2.37 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。

24.2.38 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。

24.2.39 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
3	ポート番号 3 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、ISDN 回線を使用する場合にのみ有効である。

24.2.40 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
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なう。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。

- 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。

- ・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。

24.2.41 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なう場合において、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。

24.2.42 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。

24.2.43 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。

24.2.44 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。

24.2.45 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、アナログ回線を使用する場合にのみ有効である。

24.2.46 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。

24.3 アナログ回線の設定

本節のコマンドはアナログ回線を使用する場合にのみ有効である。

24.3.1 ダイヤルの種別を選択

[書式]

```
pstn dial type type
no pstn dial type
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
10pps	パルス(10pps)
20pps	パルス(20pps)
pb	PB

- [初期値]: 20pps

[説明]

アナログ回線に対するダイヤルの種別を選択する。

24.3.2 フックング時間の設定**[書式]**

pstn hooking timer *time*
no pstn hooking timer

[設定値及び初期値]

- *time*
 - [設定値]: 秒数(0.3..1)
 - [初期値]: 0.5

[説明]

アナログ回線に対してフックング操作を行う場合のフックング時間を設定する。

24.3.3 アナログ回線のモデム信号を検出するまでの時間を設定する**[書式]**

pstn modem signal timer *time*
no pstn modem signal timer

[設定値及び初期値]

- *time*
 - [設定値]: 秒数(0.1..3)
 - [初期値]: 1.5

[説明]

アナログ回線のモデム信号を検出するまでの時間を設定する。

ナンバー・ディスプレイが表示されない場合や、モデム・ダイヤルインが正しく動作しない場合は、このコマンドを調整する必要がある。

秒数は 0.1 秒単位で設定できる。

24.3.4 ナンバー・ディスプレイ(ダイヤルイン)の着信の識別設定**[書式]**

pstn number display *sw*
no pstn number display

[設定値及び初期値]

- *sw*
 - [設定値]:

設定値	説明
auto	ナンバー・ディスプレイ(ダイヤルイン)の着信を自動判別する
off	ナンバー・ディスプレイ(ダイヤルイン)の着信を判別しない

- [初期値]: auto

[説明]

アナログ回線に対するナンバー・ディスプレイ(ダイヤルイン)の着信に対する動作を設定する。

[ノート]

auto に設定すると、ナンバー・ディスプレイの他、ダイヤルインに対する着信を自動的に判別する。

off に設定すると、上記の着信においても、通常の着信と同様な動作を行なう。

24.3.5 アナログ回線に対する受話 PAD の設定

[書式]

pstn pad receive *pad*
no pstn pad receive

[設定値及び初期値]

- *pad*
- [設定値]:

設定値	説明
-3dB	-3dB PAD 挿入
-6dB	-6dB PAD 挿入
-9dB	-9dB PAD 挿入
-12dB	-12dB PAD 挿入
-15dB	-15dB PAD 挿入
-18dB	-18dB PAD 挿入
-21dB	-21dB PAD 挿入
off	PAD なし

- [初期値]: off

[説明]

アナログ回線に対する受話 PAD を設定する。

24.3.6 アナログ回線に対する送話 PAD の設定

[書式]

pstn pad send *pad*
no pstn pad send

[設定値及び初期値]

- *pad*
- [設定値]:

設定値	説明
-3dB	-3dB PAD 挿入
-6dB	-6dB PAD 挿入
-9dB	-9dB PAD 挿入
-12dB	-12dB PAD 挿入
-15dB	-15dB PAD 挿入
-18dB	-18dB PAD 挿入
-21dB	-21dB PAD 挿入
off	PAD なし

- [初期値]: off

[説明]

アナログ回線に対する送話 PAD を設定する。

24.3.7 アナログ回線に対するポーズ時間の設定

[書式]

pstn pause timer *time*
no pstn pause timer

[設定値及び初期値]

- *time*
 - [設定値]: 秒数(1..10)
 - [初期値]: 2

[説明]

アナログ回線に対してポーズ操作を行なう場合のポーズ時間を設定する。

24.3.8 付加サービス機能の設定**[書式]**

pstn supplementary-service *sw*
no pstn supplementary-service

[設定値及び初期値]

- *sw*
 - [設定値]:

設定値	説明
on	付加サービスを契約している回線
off	付加サービスを契約していない回線

- [初期値]: off

[説明]

アナログ回線に対して付加サービス(キャッチホン/ボイスワープ/トリオホン)を契約しているかどうかを設定する。

24.3.9 アナログ回線を使用するか否かの設定**[書式]**

pstn use *sw*
no pstn use

[設定値及び初期値]

- *sw*
 - [設定値]:

設定値	説明
on	アナログ回線を使用する
off	アナログ回線を使用しない

- [初期値]: on

[説明]

アナログ回線を使用するか否かを設定する。

24.3.10 アナログ回線で検出する呼出信号の周波数範囲の設定**[書式]**

pstn ringing signal frequency *MIN MAX*
no pstn ringing signal frequency

[設定値及び初期値]

- *MIN*
 - [設定値]: 周波数の下限(10..15)
 - [初期値]: 15
- *MAX*
 - [設定値]: 周波数の上限(20..40)
 - [初期値]: 30

[説明]

アナログ回線で検出する呼出信号の周波数範囲を設定する。
設定値は再起動後に有効になる。

24.3.11 鳴動時間により呼出信号の種別を判定する閾値の設定

[書式]

pstn ringing signal threshold *T1 T2 T3 T4*
no pstn ringing signal threshold

[設定値及び初期値]

- *T1*
 - [設定値]: 呼出信号を SIR と判定する鳴動時間の閾値[msec] (200..2000)
 - [初期値]: 200
- *T2*
 - [設定値]: 呼出信号を CAR と判定する鳴動時間の閾値[msec] (200..2000)
 - [初期値]: 400
- *T3*
 - [設定値]: 呼出信号を IR と判定する鳴動時間の閾値[msec] (200..2000)
 - [初期値]: 700
- *T4*
 - [設定値]: 呼出信号を CR と判定する鳴動時間の閾値[msec] (200..2000)
 - [初期値]: 1500

[説明]

鳴動時間により呼出信号の種別を判定する閾値を設定する。
設定値は再起動後に有効になる。

第 25 章

カスケード接続機能の設定

NVR500 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 NVR500 Rev.11.00.43 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。

25.1 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
manager	アナログ親機モード
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なう場合、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 NVR500 Rev.11.00.43 以降で使用可能。

25.2 カスケード接続に利用する IP アドレス取得インタフェースの設定

[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フェースを設定する。

[ノート]

PP インタフェースで 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。またフィルタ設定も、上記ポートを通す設定が必要である。

25.3 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。

NVR500 は Rev.11.00.43 以降で使用可能。

25.4 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。

NVR500 は Rev.11.00.43 以降で使用可能。

25.5 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内線 ("**") 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。

25.6 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。

第 26 章

VoIP 機能の設定

26.1 共通の設定

26.1.1 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。

26.1.2 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なう。

26.1.3 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 インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェースの番号
 - [初期値]: -
- *codec*
 - [設定値]:

設定値	説明
g711u	G.711 μ -law
g711a	G.711 A-law
g729	G.729a

- [初期値]: g711u g711a g729

[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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

[設定例]

- pp1 で使用できる CODEC を G.729a だけに設定する

```
# sip codec permit pp 1 g729
```

- lan2 で使用できる CODEC の設定値を初期値に戻す

```
# no sip codec permit lan2
```

26.1.4 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、再送を行なわない。

[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。

26.1.5 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 の発呼を行なう。

[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。

26.1.6 ネットボランチ電話で SIP ユーザ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 の発呼を行なう。

[設定例]

SIP ユーザ名として付与する桁数を 4 桁で設定

```
# sip netvolante dial figure 4
```

26.1.7 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なう。

[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、直接接続を行なう。

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な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。

26.1.8 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]:
- [初期値]: 0
- *update*
 - [設定値]:

設定値	説明
秒数 (60..540)	
0	session-timer 機能を利用しない

設定値	説明
on	UPDATE メソッドを使用する

設定値	説明
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 パラメータを設定しない
uac	refresher パラメータに uac を設定する
uas	refresher パラメータに 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 パラメータを設定せず、uac/uas を設定した時はそれぞれのパラメータ値で発信する。

26.1.9 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。

26.1.10 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。

26.1.11 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。

26.1.12 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。

26.1.13 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す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

設定値	説明
on	ネーム・ディスプレイ情報として送出す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す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。

26.1.14 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
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。

26.1.15 着信時のセッションタイマー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ー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。

26.1.16 SIP 着信時に user 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	user 名を検証する
off	user 名を検証しない

- [初期値]: on

[説明]

SIP の着信時に user 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 設定がある場合に有効となる。

26.1.17 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。

26.1.18 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

設定値	説明
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。

26.2 SIP サーバー毎の設定

26.2.1 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。

26.2.2 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
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 / 非通知を行なう。
rfc3325	RFC3325 に従って発信者番号の通知 / 非通知を行なう。
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。

26.2.3 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 コードで設定を行なう。

26.2.4 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。

26.2.5 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 パラメータを設定しない
uac	refresher パラメータに uac を設定する
uas	refresher パラメータに 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 パラメータを設定せず、uac/uas を設定した時はそれぞれのパラメータ値で発信する。

26.2.6 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。

26.2.7 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なう。

26.2.8 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。

26.2.9 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。

26.2.10 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 ユーザ名の順に検索、表示できる内容をそのまま表示。

設定値	説明
1	1. SIP ユーザ名が数字であった場合、SIP ユーザ名を使用し、 1.1 8桁未満であればそのまま表示 1.2 先頭が'0'であればそのまま表示 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 1.4 その他の場合は先頭に'0'を付加して表示 2. SIP ユーザ名が数字のみでない場合、 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 2.2 DisplayName がすべて数字の場合、その番号を表示 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。

26.2.11 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。

26.2.12 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な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。

26.2.13 SIP サーバ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
off	制限しない

- [初期値]: off

[説明]

SIP サーバ経由での 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。

26.2.14 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。

26.2.15 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。

26.2.16 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

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。

26.3 TEL ポートの設定

26.3.1 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なう。

26.3.2 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]: ユーザ名 (sip: で始まり、@ を含まない SIP ユーザ名)
- [初期値]: sip:nvr500

[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。

26.3.3 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 コードで設定を行なう。

26.3.4 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	analog sip call myname 及び analog sip arrive myaddress で登録されているユーザ名 / 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。

26.3.5 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。

26.3.6 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する桁数 (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なう。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 ユーザ名とダイヤルイン登録の SIP ユーザ名が一致しない、あるいは *lastdigit* で SIP ユーザ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
```

26.3.7 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 lan_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 lan_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 lan_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 *lan_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]: -

- *lan_interface*

- [設定値]: ひかり電話回線を接続する LAN インタフェース名

- [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 のユーザ名部分をダイヤルした番号に置き換えて SIP の発呼を行なう。

phone を設定すると、宛先の URI に user=phone のタグを埋め込んで SIP の発呼を行なう。アナログ回線または ISDN 回線に抜ける発呼を行な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、発呼を行なう。

ngn lan_interface を設定した場合は、設定した LAN インタ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ければならない。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。

26.4 電話番号ルーティングの設定

26.4.1 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とその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。

26.4.2 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 lan_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
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	SIP サーバー経由で発信する
ngn lan_interface	ひかり電話で発信する

- [初期値]: -
- *lan_interface*
 - [設定値]: ひかり電話回線を接続する LAN インタフェース名
 - [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 経路としてアナログ回線、ISDN 回線、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 lan_interface` を設定した場合は、設定した LAN インタ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
```

26.5.1 NGN 網に接続するインタフェースの設定

[書式]

ngn type interface type

no ngn type interface [type]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース
 - [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フェースを設定する。

26.5.2 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。

第 27 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。

27.1 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。

27.2 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]*

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)
 - [初期値]: -
- *username*
 - [設定値]: 認証用ユーザ名
 - [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

設定値	説明
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]: -

[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` パラメータでは、メール送信の際の SMTP 認証のためのデータ (ユーザ名、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。

27.3 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` パラメータを設定したときに必要な設定である。

27.4 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。

27.5 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 mailserv_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]: -
- *mailserv_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]: Filter Info/Status Info/Intrusion Info/Account Info
- *date*
 - [設定値]: メールへ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]: メールへのヘッダに表示する MIME-Version
 - [初期値]: 1.0
- *content_type*
 - [設定値]: メールへ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:NVR500 test" "Date:Sun, 10 Oct 2010 10:10:10 +0900"
  MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

27.6 メール通知のトリガの設定

[書式]

```
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 account
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_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	インタフェースの情報
routing	ルーティングの情報
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フェース
- [設定値]:

設定値	説明
pp	PP インタフェース
lanN(N,M)	LAN インタフェース
wan1	WAN インタフェース
tunnel	TUNNEL インタフェース
*	全てのインタフェース

- [初期値]: -
- *range_i*
 - [設定値]:
 - インタ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。イーサネットフィルタのログ表示、**mail notify status exec** コマンド実行時、不正アクセス検知時、および **mail notify account exec** コマンド実行時をトリガとして指定できる。

イーサネットフィルタ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..... **pass-log,reject-log** パラメータの定義

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。

累積課金情報を通知する場合は、**mail notify account exec** コマンドを実行する必要がある。

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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

[設定例]

```
mail notify 1 1 trigger filter ethernet lan1 in
mail notify 2 1 trigger status all
mail notify 3 1 trigger intrusion lan1 in/out pp * in tunnel 1-3 out
mail notify 4 1 trigger account
```

第 28 章

HTTP サーバー機能

28.1 共通の設定

28.1.1 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。

28.1.2 HTTP サーバーへアクセスできるホストの IP アドレス設定

[書式]

```
httpd host ip_range
no httpd host
```

[設定値及び初期値]

- *ip_range*: HTTP サーバーへ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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
lan	すべての LAN 側ネットワーク内ならば許可する
lanN	HTTP サーバーへアクセスを許可する LAN インタフェース名
wan1	WAN1 側ネットワーク内ならば許可する
none	すべてのホストからのアクセスを禁止する

- [初期値]: 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。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

28.1.3 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、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。

28.1.4 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。

28.1.5 PP インタフェースとトンネルインタフェースの名前の設定

[書式]

```
pp name type:name
tunnel name name
no pp name
no tunnel name
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
PRV/1..10	プロバイダ型の識別 (1..10)
RAS	リモートアクセスサーバー型の識別
WAN	LAN 間接続の識別

- [初期値]: -
- *name*
 - [設定値]: ユーザが設定したプロバイダの名称 (半角 64 文字以内)
 - [初期値]: -

[説明]

かんたん設定用の識別コマンド。かんたん設定で、プロバイダ名称やトンネル接続名称等で入力した名称がここに設定される。

28.2 かんたん設定ページ用の設定

本節のコマンドは、NVR500 のかんたん設定ページでプロバイダ接続を登録する際に使用され、「設定の確定」ボタンをクリックすることで自動的に設定されるものです。本節のコマンドを手動で設定することは、かんたん設定ページで登録した内容を変更することになるため、各コマンドの機能や動作を十分に理解した上で行ってください。

かんたん設定ページからはプロバイダの情報は最大 10 個まで登録でき、既に設定されている相手先情報番号のいずれかに **provider set** コマンドを使用して対応させます。

解除する場合には **no provider set** コマンドを使用します。

設定されたプロバイダを選択するには、**provider select** コマンドを使用します。本コマンドによりプロバイダを変更すると、プロバイダごとに異なる DNS やデフォルトルートの設定など、そのプロバイダに接続するために必要な事項を自動的に設定変更します。

プロバイダ設定の状況はかんたん設定ページで調べるか、**show config** コマンドで調べます。

28.2.1 プロバイダ接続タイプの設定

[書式]

provider type *provider_type*

no provider type [*provider_type*]

[設定値及び初期値]

- *provider_type*

- [設定値]:

設定値	説明
isdn-terminal	PPPoE 型の端末接続
isdn-network	PPPoE 型のネットワーク接続
leased-network	専用線のネットワーク接続
leased-wan	専用線の LAN 間接続
none	設定なし

- [初期値]: none

[説明]

プロバイダの接続タイプを設定する。

28.2.2 プロバイダ情報の PP との関連付けと名前の設定

[書式]

provider set *peer_num* [*name*]

provider set *interface* [*name*]

no provider set *peer_num* [*name*]

no provider set *interface* [*name*]

[設定値及び初期値]

- *peer_num*

- [設定値]: 相手先情報番号
- [初期値]: -

- *interface*

- [設定値]: WAN インタフェース名
- [初期値]: -

- *name*

- [設定値]: 名前 (半角 32 文字以内)
- [初期値]: -

[説明]

プロバイダ切り替えを利用するために設定する。

結び付けられた相手先情報番号やインタフェース名はプロバイダとして扱われる。何も設定されていない相手先情報番号やインタフェース名に対しては無効である。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

28.2.3 プロバイダ接続設定

[書式]

```
provider select peer_num
provider select interface
no provider select peer_num
no provider select interface
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *interface*
 - [設定値]: WAN インタフェース名
 - [初期値]: -

[説明]

接続するプロバイダ情報を選択し、利用可能にセットアップする。

本コマンドが実行されると、各種プロバイダ設定コマンドに記録された情報に基づき、デフォルトルート、DNS サーバー、スケジュール等の変更が行われる。

また、かんたん設定のプロバイダ接続設定において、接続先の変更や手動接続を行った場合にも、本コマンドが実行され接続先が切り替えられる。

本コマンドの上書き対象コマンドは以下の通り。

すべてのプロバイダ情報: **pp disable**

選択されたプロバイダ情報: **pp enable**、**ip route**、**dns server** および **schedule at**

[ノート]

provider set コマンドに設定されていない相手先情報番号に対しては無効。

WAN インタフェースは Rev.11.00.16 以降で指定可能。

28.2.4 プロバイダの DNS サーバーのアドレス設定

[書式]

```
provider dns server peer_num ip_address [ip_address..]
no provider dns server peer_num [ip_address..]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *ip_address*
 - [設定値]: DNS サーバーの IP アドレス (最大 4 つ)
 - [初期値]: -

[説明]

プロバイダごとの情報として DNS サーバーのアドレスを設定する。

プロバイダが選択された場合に、このアドレスが **dns server** コマンドに上書きされる。

[ノート]

provider set コマンドに設定されていない相手先情報番号に対しては無効。
 削除時、**dns server** コマンドの内容はクリアされない。クリアされるのは **provider dns server** コマンドで設定された内容だけである。

28.2.5 LAN インタフェースの DNS サーバーのアドレスの設定

[書式]

```
provider interface dns server ip_address [ip_address..]
no provider interface dns server [ip_address [ip_address]]
```

[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
 - [初期値]: -
- *ip_address*
 - [設定値]: DNS サーバーの IP アドレス (最大 2 つ)
 - [初期値]: -

[説明]

かんたん設定ページでプロバイダ情報として LAN インタフェースや WAN インタフェース側 DNS サーバーの IP アドレスを設定する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

28.2.6 DNS サーバーを通知してくれる相手の相手先情報番号の設定

[書式]

```
provider dns server pp peer_num dns_peer_num
no provider dns server pp peer_num [dns_peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号 (1..30)
 - [初期値]: -
- *dns_peer_num*
 - [設定値]: DNS 通知相手先情報番号 (1..30)
 - [初期値]: -

[説明]

プロバイダ情報として DNS サーバーを通知してくれる相手先情報番号を設定する。

28.2.7 フィルタ型ルーティングの形式の設定

[書式]

```
provider filter routing type
no provider filter routing [type]
```

[設定値及び初期値]

- *type*: フィルタ型ルーティングの形式
 - [設定値]:

設定値	説明
off	かんたん設定で手動接続をした場合に、自動接続先が自動的に切り替わる
connection	かんたん設定で手動接続をした場合に、自動接続している間だけ有効なデフォルト経路が選択される。手動接続先が切断されると自動接続先に接続される

設定値	説明
mail	メールとそれ以外のプロトコルの種別を区別し、プロバイダを切り替える
host	ホスト (IP アドレス) を区別してプロバイダを切り替える。最大同時に 2 つのホストに接続
voip	VoIP とそれ以外のプロトコルの種別を区別して、プロバイダを切り替える

- [初期値]: off

[説明]

かんたん設定専用の識別コマンド。かんたん設定ページで選択中のフィルタ型ルーティングの形式を設定する。

[ノート]

コンソールなどから設定した場合の動作は保証されない。

28.2.8 LAN 側のプロバイダ名称の設定

[書式]

```
provider interface name [protocol] type:name
no provider interface name [protocol] [type:name]
```

[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
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
ipv4	IPv4 アドレスを用いたプロバイダ設定の名称
ipv6	IPv6 アドレスを用いたプロバイダ設定の名称

- [初期値]: -
- *type*
 - [設定値]: プロバイダ情報の識別情報 ("PRV" など)
 - [初期値]: -
- *name*
 - [設定値]: ユーザが設定したプロバイダの名称など
 - [初期値]: -

[説明]

かんたん設定専用の識別コマンド。かんたん設定ページでプロバイダ名称等で入力した名称が設定される。

protocol は省略可能。

省略した場合は、IPv4 アドレスを用いたプロバイダ設定の名称とする。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

protocol パラメータは Rev.11.00.16 以降で指定可能。

28.2.9 プロバイダに対する昼間課金単位時間の設定

[書式]

```
provider isdn disconnect daytime peer_num unit
no provider isdn disconnect daytime peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *unit*: 昼間料金適用時の課金単位時間
 - [設定値]:

設定値	説明
1..21474836	秒数
off	設定しない

- [初期値]: 60

[説明]

選択したプロバイダとの接続で、昼間料金適用時の課金単位時間を設定する。 *unit* パラメータは 0.1 秒単位で設定できる。

選択したプロバイダとの接続で、**isdn disconnect policy 1** の場合の切断に関するタイマ値を設定する。夜間料金適用をスケジュールで切り替える場合、**isdn disconnect time** コマンドで設定された単位時間は無視される。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.10 プロバイダに対する昼間課金単位時間方式での単位時間と監視時間の設定**[書式]**

```
provider isdn disconnect interval daytime peer_num unit watch spare
no provider isdn disconnect interval daytime peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *unit*
 - [設定値]: 課金単位秒数(1..21474836)
 - [初期値]: 180
- *watch*
 - [設定値]: 監視秒数(1..21474836)
 - [初期値]: 6
- *spare*
 - [設定値]: 切断余裕秒数(1..21474836)
 - [初期値]: 2

[説明]

選択したプロバイダとの接続で、**is dn disconnect policy 2** の場合の切断に関するタイマ値を設定する。夜間料金時間帯での値は、**provider isdn disconnect interval nighttime** コマンドで設定する。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.11 プロバイダに対する夜間課金単位時間の設定**[書式]**

```
provider isdn disconnect nighttime peer_num unit
no provider isdn disconnect nighttime peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号

- [初期値]: -
- *unit*: 昼間料金適用時の課金単位時間
- [設定値]:

設定値	説明
1..21474836	秒数
off	設定しない

- [初期値]: 60

[説明]

選択したプロバイダとの接続で、夜間料金適用時の課金単位時間を設定する。

unit パラメータは 0.1 秒単位で設定できる。

選択したプロバイダとの接続で、**isdn disconnect policy 1** の場合の切断に関するタイマ値を設定する。昼間料金適用時の課金単位時間は、**provider isdn disconnect daytime** コマンドで設定する。この昼間料金適用時の課金単位時間の設定値と異なる場合に、**provider isdn account nighttime** の設定値とともに、プロバイダが選択された場合にスケジュールに組み込まれる。この場合、**isdn disconnect time** で設定された単位時間は無視される。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.12 プロバイダに対する夜間課金単位時間方式での単位時間と監視時間の設定

[書式]

```
provider isdn disconnect interval nighttime peer_num unit watch spare
no provider isdn disconnect interval nighttime peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *unit*
 - [設定値]: 課金単位秒数(1..21474836)
 - [初期値]: 180
- *watch*
 - [設定値]: 監視秒数(1..21474836)
 - [初期値]: 6
- *spare*
 - [設定値]: 切断余裕秒数(1..21474836)
 - [初期値]: 2

[説明]

選択したプロバイダとの接続で、**is dn disconnect policy 2** に設定した場合の夜間料金時間帯での切断に関するタイマ値を設定する。昼間のタイマ値は、**provider isdn disconnect interval daytime** コマンドで設定する。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.13 プロバイダに対する自動切断タイマ無効時間の設定

[書式]

```
provider isdn auto disconnect off peer_num from to
no provider isdn auto disconnect off peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *from*

- [設定値]: 時: 分 開始時刻 (0:0..23:59)
- [初期値]: -
- *to*
 - [設定値]: 時: 分 終了時刻 (0:0..23:59)
 - [初期値]: -

[説明]

選択したプロバイダとの接続時、自動切断タイマを無効にする時間を設定する。

相手先情報番号の設定で **isdn disconnect policy** が課金単位時間方式である場合に有効。プロバイダが選択された場合にスケジュールに組み込まれる。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.14 プロバイダに対する夜間料金時間の設定

[書式]

```
provider isdn account nighttime peer_num from to
no provider isdn account nighttime peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *from*
 - [設定値]: 時: 分 開始時刻 (0:0..23:59)
 - [初期値]: -
- *to*
 - [設定値]: 時: 分 終了時刻 (0:0..23:59)
 - [初期値]: -

[説明]

選択したプロバイダとの接続で、夜間料金が適用される時間を設定する。

provider isdn disconnect nighttime コマンドで設定された夜間課金単位時間と、**provider isdn disconnect daytime** コマンドで設定された課金単位時間が異なる場合に有効。プロバイダが選択された場合にスケジュールに組み込まれる。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.15 NTP サーバーの設定

[書式]

```
provider ntpdate server_name
no provider ntpdate [server_name]
```

[設定値及び初期値]

- *server_name*
 - [設定値]: NTP サーバー名 (IP アドレスまたは FQDN)
 - [初期値]: -

[説明]

かんたん設定専用の識別コマンド。

NTP サーバーを 1 箇所設定する。**provider ntp server** コマンドでは接続先ごとの IP アドレス情報を設定し、本コマンドでは 1 箇所の IP アドレスまたは FQDN を設定する。

[ノート]

コンソールなどから手動設定した場合の動作は保証されない。

28.2.16 プロバイダの NTP サーバーのアドレス設定

[書式]

```
provider ntp server peer_num ip_address
no provider ntp server peer_num [ip_address]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *ip_address*
 - [設定値]: NTP サーバーの IP アドレス
 - [初期値]: -

[説明]

プロバイダごとの情報として NTP サーバーのアドレスを設定する。本コマンドで IP アドレスが設定されていると、プロバイダが選択されている場合に定期的に時刻を問い合わせる。プロバイダが選択された場合にスケジュールに組み込まれる。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.17 MP 使用時間帯の設定

[書式]

```
provider ppp mp use on peer_num from to
no provider ppp mp use on peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *from*
 - [設定値]: 時:分 開始時刻 (0:0..23:59)
 - [初期値]: -
- *to*
 - [設定値]: 時:分 終了時刻 (0:0..23:59)
 - [初期値]: -

[説明]

選択したプロバイダとの接続で、MP を使用する時間を設定する。プロバイダが選択された場合にスケジュールに組み込まれる。

[ノート]

provider set コマンドが実行されていない相手先情報番号に対しては無効。

28.2.18 かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定

[書式]

```
provider auto connect forced disable switch
no provider auto connect forced disable [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動接続しない
off	自動接続する

- [初期値]: off

[説明]

かんたん設定ページの切断ボタンを押した後、自動接続を禁止するか否かを設定する。

[ノート]

on に設定してある場合、かんたん設定ページの手動切断ボタンを押した後に **pp disable** コマンドを、接続ボタンを押した後に **pp enable** コマンドを自動設定する。

そのため、切断ボタンを押した後は、自動接続をしなくなる。また、**connect** コマンドからは接続できなくなる。接続するには、手動接続ボタンを押すか、ルーターを再起動する必要がある。

28.2.19 かんたん設定ページで IPv6 接続を行うか否かの設定

[書式]

```
provider ipv6 connect pp peer_num connect
no provider ipv6 connect pp peer_num [connect]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *connect*
 - [設定値]:

設定値	説明
on	接続する
off	接続しない

- [初期値]: off

[説明]

かんたん設定ページでプロバイダ情報として IPv6 接続を有効にするか否かを設定する。

[ノート]

かんたん設定ページで IPv6 接続設定をした時に自動的に on になる。

28.2.20 電話アドレスの設定

[書式]

```
provider netvolante-dns hostname sip name
no provider 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]

かんたん設定専用の識別コマンドである。

28.2.21 プロバイダ情報とトンネルとの関連付け

[書式]

```
provider pp bind pp_num tunnel_num...  
no provider pp bind pp_num [tunnel_num...]
```

[設定値及び初期値]

- *pp_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

プロバイダ情報とトンネルとの関連付けを設定します。

28.2.22 LAN インタフェースのプロバイダ情報とトンネルとの関連付け

[書式]

```
provider interface bind tunnel_num...  
no provider interface bind [tunnel_num...]
```

[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
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

LAN インタフェースや WAN インタフェースのプロバイダ情報とトンネルとの関連付けを設定します。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

第 29 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。

29.1 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.2 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.3 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.4 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。

29.5 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.6 ホスト名の登録

[書式]

```
netvolante-dns hostname host interface host [duplicate]
netvolante-dns hostname host pp host [duplicate]
no netvolante-dns hostname host interface [host [duplicate]]
no netvolante-dns hostname host pp [host [duplicate]]
```

[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
 - [初期値]: -
- *host*
 - [設定値]: ホスト名 (63 文字以内)
 - [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 サーバーに対しての登録・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フェースに同じ名前を登録できる。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.7 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 インタフェース名、WAN インタフェース名
 - [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.8 ホスト名を自動生成するか否かの設定

[書式]

```
netvolante-dns auto hostname interface switch
netvolante-dns auto hostname pp switch
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 インタフェース名、WAN インタフェース名
 - [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

[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" 以外の場合は、『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" 以外の場合は Rev.11.00.35 以降でホスト名の自動生成機能を利用可能。
WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.9 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 pp [server=server_num] switch [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 インタフェース名、WAN インタフェース名
 - [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	使用する
off	使用しない

- [初期値]: off

[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。

29.10 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 インタフェース名、WAN インタ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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.11 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。

29.12 ネットボランチ DNS サーバ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	サーバアドレスの更新機能を有効にする
off	サーバ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。

29.13 ネットボランチ DNS サーバ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。

29.14 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 インタフェース名、WAN インタフェース名

- [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。WAN インタフェースは Rev.11.00.16 以降で指定可能。

29.15 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。

29.16 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。

第 30 章

UPnP の設定

30.1 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。

30.2 UPnP に使用する IP アドレスを取得するインタフェースの設定

[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 インタフェース名	指定した LAN インタフェースの IP アドレスを取得する
WAN インタフェース名	指定した WAN インタフェースの 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フェースを設定する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

30.3 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。

30.4 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。

30.5 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。

第 31 章

スケジュール

31.1 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* 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

設定値	説明
usb-attached	USB デバイス認識時
usb1-attached	USB ポート 1 デバイス認識時
usb2-attached	USB ポート 2 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]: -
- *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 で指定した時刻に *command* で指定されたコマンドを実行する。

第 2、第 3、第 4 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/スイッチでの、**pp select/tunnel 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**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**copy exec**、**date**、**delete**、**exit**、**external-memory performance-test go**、**help**、**http revision-up go**、**http revision-up schedule**、**interface reset**、**less** で始まるコマンド、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**make directory**、**nslookup**、**packetdump**、**ping**、**ping6**、**pp select**、**quit**、**remote setup**、**rename**、**rtfs format**、**rtfs garbage collect**、**save**、**schedule at**、**show** で始まるコマンド、**sshd host key generate**、**sshd session**、**switch control function get FUNCTION**、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select**、**user attribute**

[ノート]

入力時、*command* パラメータに対して TAB キーによるコマンド補完は行われないが、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。

[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 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn 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 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn 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
```

第 32 章

VLAN の設定

32.1 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 インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-8
 - [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 インタフェースあたり最大 8VLAN 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。

Rev.11.00.16 以降で使用可能。

第 33 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。

33.1 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。

33.2 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 host
no sntp host
```

[設定値及び初期値]

- *host*: SNTP サーバーへ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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
lan	すべての LAN 側ネットワーク内ならば許可する
lanN	SNTP サーバーへのアクセスを許可する LAN インタフェース名
none	すべてのホストからのアクセスを禁止する

- [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。

第 34 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、USB 接続のハードディスクドライブ) 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>

34.1 USB ホスト機能を使うか否かの設定

[書式]

usbhost use [*port*] *switch*

no usbhost use [*port*]

[設定値及び初期値]

- *port* : USB ポート番号
 - [設定値] :

設定値	説明
1	USB ポート 1
2	USB ポート 2
省略	省略時はすべてのポート番号

- [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。

34.2 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 [*port*] *duration*

no usbhost overcurrent duration [*port*]

[設定値及び初期値]

- *port*: USB ポート番号
- [設定値]:

設定値	説明
1	USB ポート 1
2	USB ポート 2

- [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。

34.3 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。

34.4 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。

Rev.11.00.13 以降で使用可能。

34.5 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 1
usb2	USB ポート 2
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可能性がある。

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)

Rev.11.00.13 以降で使用可能。

34.6 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 storage_if:name [crypto password] [limit=size] [backup=num]
no external-memory syslog filename [storage_if:name]
```

[設定値及び初期値]

- *storage_if*
- [設定値]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2
sd1	microSD カードスロット

- [初期値]: -
- *name*
- [設定値]: SYSLOG ファイル名 (暗号化する場合でファイル名に拡張子を指定しないときは、半角 78 文字以内、それ以外の場合では、半角 83 文字以内)
- [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
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]: -
- *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

[説明]

外部メモリに保存する SYSLOG ファイル名を設定する。ファイル名はストレージインタフェースを示す *storage_if* とファイル名を示す *name* をコロン「:」で結んだ形式で指定する。*name* には "/" (ルート) からの絶対パスを指定することもできる。

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。

storage_if に指定した外部ストレージインタフェースが ONFS で使用されている (*onfs bind* コマンドで選択されている)、かつ、*name* にパスの指定がなくファイル名のみが指定されている場合、SYSLOG ファイルは ONFS 機能により作成された *system* フォルダ配下に保存される。

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。

Rev.11.00.07 以前では、*name* は半角 64 文字以内。オプションの *size* や *num* の指定はできない。各パラメータは固定となっており、それぞれ、*size* は、1,024(MB)、*num* は、1 として動作する。また、バックアップファイル名は以下の規則に従って決定される。

name に拡張子が含まれている場合

- 暗号化しないで保存する ... 拡張子を .bak に置き換える
- 暗号化して保存する ... 拡張子の前に *_bak* を追加する

name に拡張子が含まれていない場合bak という拡張子を追加する

34.7 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。

34.8 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。

34.9 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。

34.10 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: <i>filename</i>	USB ポート 1 に接続された 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)
usb2: <i>filename</i>	USB ポート 2 に接続された 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)
usb*: <i>filename</i>	USB ポート 1 および USB ポート 2 に接続された 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: <i>filename</i>	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)
*: <i>filename</i>	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] : */nvr500.bin
- *to* : コピー先ファイル名
 - [設定値]:

設定値	説明
0	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は 0 である。

from に "usb*:" を指定した場合、指定するファイルの検索はまず USB ポート 1 に接続された USB メモリから行われ、指定したファイルがなければ USB ポート 2 に接続された USB メモリが検索される。

from 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 ポート 1 に接続された USB メモリ、USB ポート 2 に接続された USB メモリの順に検索される。

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。

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

[設定例]

- microSD カード内から "nvr500.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:nvr500.bin
```

- microSD カード内のディレクトリ "test" から "nvr500.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/nvr500.bin
```

34.11 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、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 ポート 1 に接続された USB メモリ内の設定ファイル名 (<i>filename</i> は半角 99 文字以内)
usb2: <i>filename</i>	USB ポート 2 に接続された USB メモリ内の設定ファイル名 (<i>filename</i> は半角 99 文字以内)
usb*: <i>filename</i>	USB ポート 1 および USB ポート 2 に接続された 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	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]: 復号化のパスワード (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。

from に "usb*:" を指定した場合、指定するファイルの検索はまず USB ポート 1 に接続された USB メモリから行われ、指定したファイルがなければ USB ポート 2 に接続された USB メモリが検索される。

from 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 ポート 1 に接続された USB メモリ、USB ポート 2 に接続された USB メモリの順に検索される。

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化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。

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

[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
```

34.12 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。

34.13 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。

34.14 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
<i>usb1:filename</i>	USB ポート 1 に接続された USB メモリ内のバッチファイル名
<i>usb2:filename</i>	USB ポート 2 に接続された USB メモリ内のバッチファイル名
<i>usb*:filename</i>	USB ポート 1 および USB ポート 2 に接続された USB メモリ内のバッチファイル名
<i>sd1: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。

batchfile に "usb*" を指定した場合、指定するファイルの検索はまず USB ポート 1 に接続された USB メモリから行われ、指定したファイルがなければ USB ポート 2 に接続された USB メモリが検索される。

batchfile 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 ポート 1 に接続された USB メモリ、USB ポート 2 に接続された USB メモリの順に検索される。

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。

[ノート]

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

[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
```

34.15 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 ポート 1 に接続された USB メモリの性能測定をする
usb2	USB ポート 2 に接続された USB メモリの性能測定をする
sd1	microSD カードの性能測定をする

- [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]

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。

34.16 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。

34.17 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。

第 35 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。

35.1 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 1 をモバイルインターネット接続に使用
usb2	USB ポート 2 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。

[ノート]

first-connect-wait-time オプションは、Rev.11.00.25 以降で指定可能。

35.2 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 インタフェース
usb2	USB2 インタフェース

• [初期値]:-

• *pin*

• [設定値]: PIN コード

• [初期値]:-

[説明]

USB インタ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。

Rev.11.00.16 以降で使用可能。

35.3 携帯端末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]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2

• [初期値]:-

• *command*

• [設定値]:

• AT コマンド

• [初期値]:-

[説明]

指定したインタフェースに接続された携帯端末に対して、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。

[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。
```

35.4 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 1
usb2	USB ポート 2
wan1	WAN インタフェース

- [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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

35.5 PP で使用するインタフェースの設定

[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	USB ポート 1 を使用する
usb2	USB ポート 2 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フェースを設定する。

35.6 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。

35.7 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。

35.8 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

設定値	説明
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。

35.9 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。

35.10 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 )
```

35.11 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。

35.12 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]: 200000
- *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。

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 packets 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。

35.13 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。

35.14 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。

35.15 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。

35.16 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。

35.17 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が記録され、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。

35.18 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。

[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。

35.19 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。

35.20 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
1-604800	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。

35.21 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
usb2	USB2 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/>

Rev.11.00.35 以降で使用可能。

35.22 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]

- *use*

- [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。

[ノート]

mobile arrive use コマンドによって、携帯端末の設定が、"パケット着信機能を使用する"となっている場合に有効である。

Rev.11.00.35 以降で使用可能。

35.23 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。

35.24 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フェース

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2
usb*	全 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

設定値	説明
infinity	無期限

- [初期値]:
 - interface=usb*
 - 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。

GUI への表示、**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。

interface に usb* を指定すると、USB ポート 1 → USB ポート 2 の順で電波の受信レベルを取得する。

interval の設定は全 USB ポートで共通となる。

[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。

35.25 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 [*interface*] [*reverse*]

[設定値及び初期値]

- *interface*
 - [設定値]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2

- [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。

interface を指定した場合は、指定した USB インタフェースの履歴だけ表示される。interface を省略した場合、USB ポート 1、USB ポート 2 の順に表示される。

[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。interface を切り替えると、対象外となる USB インタフェースの履歴もクリアされる。

35.26 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*: インタフェース名

- [設定値]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2

- [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。

35.27 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*: インタフェース名

- [設定値]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2

- [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。

35.28 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
usb2	USB2 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/>

Rev.11.00.35 以降で使用可能。

35.29 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
usb2	USB2 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/>

Rev.11.00.36 以降で使用可能。

35.30 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.31 WAN で使用するインタフェースの設定

[書式]

`wan bind interface`

`no wan bind [interface]`

[設定値及び初期値]

- `wan`

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

- `interface`

- [設定値]:

設定値	説明
usb1	USB ポート 1
usb2	USB ポート 2

- [初期値]: -

[説明]

指定した WAN インタフェースについて実際に使用するインタフェースを設定する。

[ノート]

Rev.11.00.16 以降で使用可能。

35.32 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 インタフェースについて自動接続するか否かを設定する。

[ノート]

Rev.11.00.16 以降で使用可能。

35.33 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.34 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.35 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.36 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.37 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.38 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]: 200000

- *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。

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。

off を設定したときは警告が表示される。

Rev.11.00.16 以降で使用可能。

35.39 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。

Rev.11.00.16 以降で使用可能。

35.40 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。

[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。

Rev.11.00.16 以降で使用可能。

35.41 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。

[ノート]

Rev.11.00.16 以降で使用可能。

35.42 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 インタフェース名

- [初期値]: -
- *duration*

- [設定値]:

設定値	説明
1-604800	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。

[ノート]

Rev.11.00.16 以降で使用可能。

第 36 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。

36.1 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。

36.2 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。

36.3 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。

36.4 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

36.5 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。

36.6 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。

第 37 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インタフェース) をユーザ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フェースが用意されており、ユーザは JavaScript を使用して GUI を作成します。

NVR500 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によって画面を切り替えることが可能です。

37.1 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。

37.2 カスタム GUI を使用するユーザの設定

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

NVR500 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。

37.3 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。

37.4 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。

第 38 章

ONFS

ルーターの外部ストレージインタフェースに USB-HDD、microSD カードなどのストレージを接続することで、ルーターがファイルサーバーになります。本機能には複数のルーター間でストレージの内容をミラーリングする機能もあるため、ファイルサーバーの冗長化構成を組むことができます。各拠点に設置されたルーターでミラーリング機能を有効にしておけば、どの拠点からも WAN にアクセスすることなく常に最新の状態のファイルを共有することが可能になります。また、ある拠点の HDD が故障しても他の拠点の HDD にファイルがミラーリングされていれば、故障した拠点の HDD を新しいものに交換して簡単な操作を行うだけでファイルを復元させることができるため、バックアップ機能も兼ね備えています。

本機能のことを ONFS (Overlay Network File Server) と呼びます。

38.1 ONFS ファイルシステム

38.1.1 ONFS で使用する外部ストレージを接続するインタフェースの設定

[書式]

```
onfs bind storage_if
no onfs bind [storage_if]
```

[設定値及び初期値]

- *storage_if*
- [設定値]:

設定値	説明
usb1	USB ポート 1 に接続する
usb2	USB ポート 2 に接続する
sd1	microSD カードスロットに接続する

- [初期値]: 設定されていない

[説明]

ONFS 用のストレージを接続するインタフェースを設定する。本コマンドが設定されていないときは ONFS は一切機能しない。また、本コマンドで指定したインタフェース以外の外部ストレージインタフェースに接続されたストレージにおいても ONFS は機能せず、そのストレージは通常の外部メモリとして扱われる。

[ノート]

複数のストレージで同時に ONFS を有効にすることはできない。

38.1.2 ONFS で使用する外部ストレージの初期設定 / ONFS の再起動

[書式]

```
onfs reset [password [new_password]]
```

[設定値及び初期値]

- *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]: -
- *new_password*
 - [設定値]: ASCII 文字列で表した変更後のパスワード (半角 8 文字以上 32 文字以内)
 - [初期値]: -

[説明]

外部ストレージに ONFS の初期設定を行って ONFS を作動させたり、ONFS の再起動を行う。本コマンドの実行前に `onfs bind` コマンドを設定し、指定した外部ストレージインタフェースにストレージを接続しておく必要がある。本コマンドを実行するとルート直下に `system / local / sync` の 3 つのフォルダーが生成される。

ONFS の設定が済んでいないストレージに対して初めて本コマンドが実行された場合、*password* パラメータはストレージの認証パスワードに設定され、*system* フォルダのユーザー認証用パスワードに適用される。

既に ONFS の設定が済んでいるストレージに対して本コマンドが実行された場合、*password* パラメータがストレージに適用されているパスワードと一致したときだけ本コマンドの実行が成功する。このとき、必要なフォルダが存在しなければ再生成されるが、既存のフォルダ内のファイルやアクセス権の設定が消去されることはない。

new_password パラメータは、ストレージに適用されているパスワードを変更する場合のみ指定する。

パラメータをすべて省略した場合は、対話形式で必要なパラメータの入力が求められる。

既に本コマンドを実行済みのストレージとルーターの組み合わせであれば、ストレージを取り外した後の再接続時やルーターの再起動時に本コマンドを再実行する必要はない。ストレージもしくはルーターを交換する場合など、ストレージとルーターの組み合わせが変わる場合は本コマンドを再実行しなければ ONFS は機能しない。ルーターを工場出荷状態に戻したり、ストレージを再フォーマットした場合も本コマンドを再実行する必要がある。

[設定例]

- 初期設定を行う

```
# onfs reset PASSWORD123
リセット処理を実行しました
```

- 対話形式で初期設定を行う

```
# onfs reset
パスワードを入力してください: PASSWORD123 (入力文字は実際には表示されない)
パスワードを入力してください(確認): PASSWORD123 (再入力)
リセット処理を実行しました
```

- 初期設定が済んでいるストレージのパスワードを対話形式で変更する

```
# onfs reset
パスワードを入力してください: PASSWORD123 (入力文字は実際には表示されない)
パスワードを入力してください(確認): PASSWORD123 (再入力)
パスワードを変更しますか? (Y/N) : Y
新しいパスワードを入力してください: PASSWORD456 (入力文字は実際には表示されない)
新しいパスワードを入力してください(確認): PASSWORD456 (再入力)
リセット処理を実行しました
```

38.1.3 ONFS の動作状態の表示

[書式]

```
show status onfs [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
fs	ファイルシステムに関する情報
sharing	ファイル共有機能に関する情報
mirroring	ミラーリング機能に関する情報
省略	すべての情報を表示する

- [初期値]: -

[説明]

ONFS の動作状態を表示する。

- ファイルシステムの稼動状態
 - ストレージの接続インターフェース
 - ストレージの空き容量 / 全容量
- ファイル共有機能の稼動状態
 - 稼動時間
 - Microsoft ネットワークの設定
 - ログオン中のユーザー

- ログオン履歴
- ミラーリング機能の稼動状態
 - ミラーリンググループ内のルーター情報
 - ファイル転送の進捗状況
 - ファイル操作履歴
 - ファイル転送履歴

38.2 ONFS ファイル共有

38.2.1 ファイル共有機能の設定

[書式]

onfs sharing service *switch* [*option=value ...*]

no onfs sharing service [*switch ...*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	ファイル共有機能を使用する
off	ファイル共有機能を使用しない

- [初期値]: on
- *option = value* 列

- [設定値]:

<i>option</i>	<i>value</i>	説明
name	コンピューター名	Microsoft ネットワークで使用するコンピューター名 (半角 15 文字以内)
description	コンピューターの説明	Microsoft ネットワークで使用するコンピューターの説明 (半角 48 文字以内)
workgroup	ワークグループ名	Microsoft ネットワークで使用するワークグループ名 (半角 15 文字以内)
wins	WINS サーバーアドレス	Microsoft ネットワークの WINS サーバーの IP アドレス

- [初期値]:
 - name = 機種名-XXXXXX(X : LAN1 の MAC アドレス下位 3 バイト)
 - description = "Yamaha Router"
 - workgroup = WORKGROUP
 - wins 設定なし

[説明]

ファイル共有機能の設定をする。

オプションでは Microsoft ネットワークに関するルーターのネットワーク設定を変更することができる。

name オプションと workgroup オプションで指定する名前の命名規則は次の通りである。

- 使用可能な文字
 - 半角英数字
 - 「" * + , ; < = > ? \ | 空白」以外の半角記号
- 15 文字以内

- 英字の大文字 / 小文字の区別はせず、すべて大文字として扱われる

また、**set** コマンドで環境変数 **HOSTNAME** (大文字) を設定することで、その名前をコンピューター名に使用することもできる。環境変数 **HOSTNAME** は本コマンドの **name** オプションの設定よりも優先される。

description オプションで設定したコンピューターの説明は、コンピューターのプロパティ画面に表示され、Windows エクスプローラーの詳細表示画面のコメント欄には表示されない。なお、Windows Vista 以降の Windows OS からはコンピューターの説明は参照できない。

[ノート]

onfs bind コマンドで指定した外部ストレージインタフェースに接続されているストレージ内の **system / local / sync** フォルダがファイル共有機能の対象フォルダとなる。

38.2.2 ファイル共有機能を使用できるホストの IP アドレス設定

[書式]

onfs sharing host *host*

no onfs sharing host [*host*]

[設定値及び初期値]

- *host*
- [設定値]:

設定値	説明
使用を許可するホストの IP アドレス (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可能)	指定したホストからの使用を許可する
any	すべてのホストからの使用を許可する
none	すべてのホストからの使用を禁止する
LAN インタフェース名	指定した LAN インタフェースからの使用を許可する (空白で区切って複数指定可能)

- [初期値]: lan1

[説明]

ファイル共有機能の使用を許可するホストを設定する。

[ノート]

本コマンドで LAN インタフェースを指定する場合は、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 アドレスからの使用を許可する。ただし、指定した LAN インタ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、すべてのホストからの使用が許可されない。

38.2.3 ファイル共有機能を利用するユーザーの設定

[書式]

onfs sharing user *id user_name* [*password*]

no onfs sharing user *id* [*user_name* ...]

[設定値及び初期値]

- *id*
 - [設定値]: ユーザーの識別番号 (1..20)
 - [初期値]: -
- *user_name*
 - [設定値]: ユーザー名 (半角 20 文字以内 または 全角 10 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: ASCII 文字列で表したパスワード (半角 64 文字以内)
 - [初期値]: -

[説明]

ファイル共有機能のアクセス制御を使用する場合に、アクセス権の設定対象となるすべてのユーザーを本コマンドで設定する。最大 20 ユーザーの設定が可能である。

user_name の命名規則は次の通りである。

- 使用可能な文字
 - 半角英数字
 - 「/[]" : ; | < > + = , ? *」以外の半角記号
 - 全角文字
- 半角 20 文字以内 または 全角 10 文字以内
- 半角英字の大文字 / 小文字の区別はしない
- 半角スペースは使用可能であるが、半角スペースのみで構成することはできない

`system` フォルダへのアクセス権を持つ `"rtadmin"` というユーザー名も本コマンドで設定することが可能であるが、パスワードを変更することはできないため、`"rtadmin"` を設定する場合は *password* の指定はできない。`"rtadmin"` も他のユーザーと同様に `set-acl` コマンドでアクセス権を設定することが可能である。

ユーザー名 / パスワードは、当該ユーザーが通常利用している Windows アカウントのユーザー名 / パスワードと同一の設定をすることを推奨する。Windows アカウントとは異なる設定をする場合、アクセスするルーターに対するログオン情報を事前に Windows に登録しておく必要がある。Windows エクスプローラーで共有フォルダへアクセスしたときに認証ダイアログが表示された場合は、本コマンドで設定したユーザー名とパスワードを入力する。

[ノート]

Rev.11.00.13 以降で使用可能。

38.2.4 ファイル共有機能を利用するグループの設定

[書式]

```
onfs sharing group id group_name user_list
no onfs sharing group id [group_name ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: グループの識別番号 (1..10)
 - [初期値]: -
- *group_name*
 - [設定値]: グループ名 (半角 20 文字以内)
 - [初期値]: -
- *user_list*
 - [設定値]: グループに所属するユーザーの識別番号を空白で区切って並べる
 - [初期値]: -

[説明]

ファイル共有機能のアクセス制御を使用する場合に、アクセス権の設定対象となるすべてのグループを本コマンドで設定する。最大 10 グループの設定が可能である。

group_name の命名規則は次の通りである。

- 使用可能な文字
 - 半角英数字
 - 「/[]" : ; | < > + = , ? *」以外の半角記号
- 半角 20 文字以内
- 半角英字の大文字 / 小文字の区別はしない
- 半角スペースは使用可能であるが、半角スペースのみで構成することはできない

user_list には `onfs sharing user` コマンドで設定されている識別番号を指定する。グループ単位でアクセス制限のかけられているファイル / フォルダには、当該グループに所属し、かつ、`onfs sharing user` コマンドで設定されているユーザー情報に一致するユーザーがアクセス可能となる。

[ノート]

Rev.11.00.13 以降で使用可能。

38.2.5 ファイル共有機能のアクセス制御を有効にするか否かの設定

[書式]

onfs sharing acl *switch*

no onfs sharing acl [*switch*]

[設定値及び初期値]

• *switch*

- [設定値]:

設定値	説明
on	アクセス制御を有効にする
off	アクセス制御を無効にする

- [初期値]: off

[説明]

ファイル共有機能のアクセス制御を有効にするか否かを設定する。アクセス制御を有効にすると、**set-acl** コマンドで設定された ACL に従ったアクセス制御が行われる。

[ノート]

Rev.11.00.13 以降で使用可能。

38.2.6 ファイル共有機能の ACL の設定

[書式]

set-acl *storage_if:path acl* [*acl* ...]

[設定値及び初期値]

• *storage_if*

- [設定値]:

設定値	説明
usb1	USB1 ポート
usb2	USB2 ポート
sd1	microSD1 カードスロット

- [初期値]: -

• *path*

- [設定値]: ACL を設定するファイルまたはフォルダーを "/" (ルート) からの絶対パスで指定する

- [初期値]: -

- *acl*: 3つの項目をコロン「:」で区切り指定する (1つ目の項目の *user/group/other* はそれぞれ *u/g/o* と省略することが可能)

- [設定値]:

- *user:username:permission*

- ユーザー単位のアクセス権

- *group:groupname:permission*

- グループ単位のアクセス権

- *other::permission*

- その他のユーザーに対するアクセス権

設定値	説明
<i>username</i>	onfs sharing user コマンドで設定したユーザー名

設定値	説明
<i>groupname</i>	onfs sharing group コマンドで設定したグループ名
<i>permission</i>	アクセス種別 <ul style="list-style-type: none"> • w <ul style="list-style-type: none"> • 読み込みと書き込みを許可 • r <ul style="list-style-type: none"> • 読み込みのみを許可 • - <ul style="list-style-type: none"> • すべてのアクセスを拒否

- [初期値]:-

[説明]

共有フォルダー内のファイルまたはフォルダーごとの ACL (アクセス制御リスト) を設定する。指定した *path* が共有フォルダー `local/sync` 自身および `local/sync` 配下のファイル/フォルダーを指し、接続されている外部ストレージ内にその存在を確認できた場合に ACL の設定が成功する。ただし、ACL は "/" (ルート) を基点として 10 階層目よりも深い階層にあるファイル/フォルダーには設定できない。なお、*path* で指定したファイル/フォルダーに既に ACL が設定されている場合は、既存の ACL を消去せずに新しい設定が追記・上書きされる。また、ACL が設定されているファイル/フォルダーをファイル共有機能を経由して削除/移動した場合、対応する ACL も自動的に消去/移動される。

ACL には次の 3 つの指定形式があり、同時に複数の ACL 句を指定することが可能である。

- `user:username:permission`
 - ユーザー単位でアクセス権を設定する。
- `group:groupname:permission`
 - グループ単位でアクセス権を設定する。
- `other::permission`
 - ユーザー単位/グループ単位のアクセス権の制御対象とならないユーザーに対するアクセス権を設定する。

ユーザー単位あるいはグループ単位のアクセス権が設定されたファイル/フォルダーは、自動的にその他のユーザーのアクセスが拒否されるように設定される。したがって、"`other::-`" という ACL 句は必ずしも設定する必要はない。

複数の ACL 句でアクセス権の設定が重複するユーザーが存在する場合、次の規則に基づきアクセス権が決定される。

1. ユーザー単位のアクセス権がグループ単位のアクセス権よりも優先される。
2. 複数のグループに所属するユーザーが存在し、その複数のグループで異なるアクセス権が設定されている場合、当該ユーザーのアクセス権は最も強いものが適用される。

アクセス対象のファイル/フォルダーに ACL が存在しなかった場合は、上位階層へさかのぼり、最初に見つかった ACL のアクセス権が適用される。なお、最上位である共有フォルダー `local/sync` までさかのぼっても ACL が見つからなかった場合は、すべてのアクセスが許可される。

`storage_if:path` の部分は相対パスを指定することが可能である。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]

Rev.11.00.13 以降で使用可能。

[設定例]

- ファイル `usb1:/local/himitsu.txt` に対して、ユーザー `"taro"` のみに読み込みと書き込みを許可する


```
# set-acl usb1:/local/himitsu.txt user:taro:w
アクセス権を設定しました
```
- フォルダー `usb1:/sync/report` に対して、グループ `"staff"` には読み込みのみを許可し、ユーザー `"tencho"` には読み込みと書き込みを許可する


```
# set-acl usb1:/sync/report g:staff:r u:tencho:w
アクセス権を設定しました
```


- フォルダ "usb1:/local/read-only" に対して、すべてのユーザーに読み込みのみを許可する

```
# set PWD=usb1:/local      (相対パスの基点を設定)
# set-acl read-only o::r
アクセス権を設定しました
```

38.2.7 ファイル共有機能の ACL の消去

[書式]

```
clear acl storage_if:path [all]
```

[設定値及び初期値]

- *storage_if*
 - [設定値]:

設定値	説明
usb1	USB1 ポート
usb2	USB2 ポート
sd1	microSD1 カードスロット

- [初期値]: -
- *path*
 - [設定値]: ACL を消去するファイルまたはフォルダを "/" (ルート) からの絶対パスで指定する
 - [初期値]: -

[説明]

共有フォルダ内のファイルまたはフォルダごとの ACL (アクセス制御リスト) を消去する。

all を指定した場合は、*path* 配下にあるすべてのファイル/フォルダ (*path* が指すフォルダも含む) に対して設定されている ACL を消去する。この場合、*path* に "/" (ルート) を指定すればファイル共有機能で使用している ACL を一度に全消去することができる。

all を指定しない場合は、*path* が指すファイル/フォルダに設定されている ACL のみを消去する。この場合、*path* には "/" (ルート) などの共有フォルダ外のパスを指定することはできない。

storage_if:path の部分は相対パスを指定することが可能である。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]

Rev.11.00.13 以降で使用可能。

38.2.8 ファイル共有機能の ACL の表示

[書式]

```
show acl storage_if:path [all]
```

[設定値及び初期値]

- *storage_if*
 - [設定値]:

設定値	説明
usb1	USB1 ポート
usb2	USB2 ポート
sd1	microSD1 カードスロット

- [初期値]: -
- *path*
 - [設定値]: 表示対象のファイルまたはフォルダを "/" (ルート) からの絶対パスで指定する
 - [初期値]: -

[説明]

共有フォルダー内のファイルまたはフォルダーごとの ACL (アクセス制御リスト) を表示する。

`all` を指定した場合は、`path` 配下にあるすべてのファイル/フォルダー (`path` が指すフォルダーも含む) に対して設定されている ACL を表示する。この場合、`path` に "/" (ルート) を指定すればファイル共有機能で使用しているすべての ACL を表示させることができる。

`all` を指定しない場合は、`path` が指すファイル/フォルダーに設定されている ACL のみを表示する。この場合、`path` には "/" (ルート) などの共有フォルダー外のパスを指定することはできない。

`storage_if:path` の部分は相対パスを指定することが可能である。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]

Rev.11.00.13 以降で使用可能。

38.3 ONFS ミラーリング

38.3.1 ONFS ミラーリング機能の使用設定

[書式]

`onfs mirroring use switch`

`no onfs mirroring use`

[設定値及び初期値]

- `switch`
- [設定値]:

設定値	説明
on	ONFS ミラーリング機能を使用する
off	ONFS ミラーリング機能を使用しない

- [初期値]: off

[説明]

ONFS ミラーリング機能を使用するか否かを設定する。

38.3.2 ONFS ミラーリング機能の自拠点設定

[書式]

`onfs mirroring id name address [option=value ...]`

`no onfs mirroring id`

[設定値及び初期値]

- `name`
 - [設定値]: 機器の名前(半角 32 文字以内)
 - [初期値]: -
- `address`
 - [設定値]: IP アドレスまたはホスト名 (FQDN)
 - [初期値]: -
- `option = value 列`
 - [設定値]:

option	value	説明
control-port	1..65535	ミラーリング機能制御メッセージを待ち受けるポート番号
data-port	1..65535	ミラーリング機能でデータを待ち受けるポート番号

<i>option</i>	<i>value</i>	説明
preference	1..200	代表ノードになる優先度を設定する
retry	1..10	ミラーリングに失敗した場合のリトライ回数
	off	リトライしない
retry-interval	20..300	ミラーリングに失敗した場合に再試行するまでの待ち時間[sec]
update-interval	3600..86400	定期更新の間隔[sec]
	off	定期更新を行わない

- [初期値]:

```
control-port = 49501
data-port = 49502
preference = 100
retry = 3
retry-interval = 60
update-interval = 10800
```

[説明]

ONFS ミラーリンググループに参加する際の自分の登録情報を設定する。

name (名前)は、各拠点のルーターを識別するためにつける名前。ひとつのミラーリンググループ内で重複する名前が発見された場合は、後から参加しようとしているルーターの参加要求は拒否される。

name に「\:*\? "<>|」の文字を使用することはできない。

アドレスはインターネットに接続される WAN 側の IP アドレスを指定する。WAN アドレスが不定の場合はネットボランチ DNS に登録し、そのホスト名 (FQDN) を指定する。

ポート番号は制御メッセージ用のポート番号と、データ転送用のポート番号を指定する。

優先度 (*preference*) は、代表ノードに選出される優先度を指定する。ミラーリンググループ内で最大値をもつルーターが代表ノードとなる。ひとつのミラーリンググループ内に同値の優先度をもつルーターが存在する場合は、*name* のアルファベット順により決定される。

ミラーリングに失敗した場合に、*retry-interval* オプションの時間だけ待って、*retry* オプションの回数だけ再試行される。

update-interval では、外部ストレージのミラーリング対象フォルダー内のデータが最新のものであるかどうかを定期的にチェックする間隔を指定する。代表ノードのミラーリング対象フォルダーの内容との差分があれば、ファイル同期機能によって差分取得が行なわれる。最初の差分取得は、ミラーリンググループに参加してから *update-interval* 時間経過した後に行われる。

38.3.3 ONFS ミラーリンググループに参加するためのコンタクトノード設定

[書式]

```
onfs mirroring contact node id address [port]
no onfs mirroring contact node id
```

[設定値及び初期値]

- *id*: 識別番号
 - [設定値]: 1..3
 - [初期値]: -
- *address*
 - [設定値]: コンタクトノードのアドレスまたはホスト名 (FQDN)

- [初期値]:-
- *port*: コンタクトノードの制御メッセージ待ち受けポート番号
 - [設定値]: 1..65535
 - [初期値]:-

[説明]

ONFS ミラーリンググループを構成するルーターの相手先アドレスまたはホスト名 (FQDN) を指定する。

38.3.4 ONFS ミラーリンググループへの参加認証に使用する事前共有鍵の設定

[書式]

```
onfs mirroring pre-shared-key binary_key
onfs mirroring pre-shared-key text
no onfs mirroring pre-shared-key
```

[設定値及び初期値]

- *binary_key*
 - [設定値]: 鍵となる 0x ではじまる 16 進数列 (32 バイト以内)
 - [初期値]: 事前共有鍵は設定されていない
- *text*
 - [設定値]: ASCII 文字列で表した鍵 (32 文字以内)
 - [初期値]: 事前共有鍵は設定されていない

[説明]

ONFS ミラーリンググループに参加するための事前共有鍵を登録する。ミラーリンググループに参加する全拠点で、共通の事前共有鍵が設定されている必要がある。

[設定例]

```
onfs mirroring pre-shared-key text himitsu
onfs mirroring pre-shared-key 0xCDEEEDC0CDEDCD
```

38.3.5 ONFS ミラーリングのファイル同期機能を手動実行

[書式]

```
onfs mirroring go
```

[説明]

ONFS ミラーリングのファイル同期機能を手動で実行し、代表ノードと自拠点のミラーリング対象フォルダー内容の差分を取得する。

[ノート]

実行するルーターがミラーリンググループの代表ノードの場合には、差分取得は行われません。

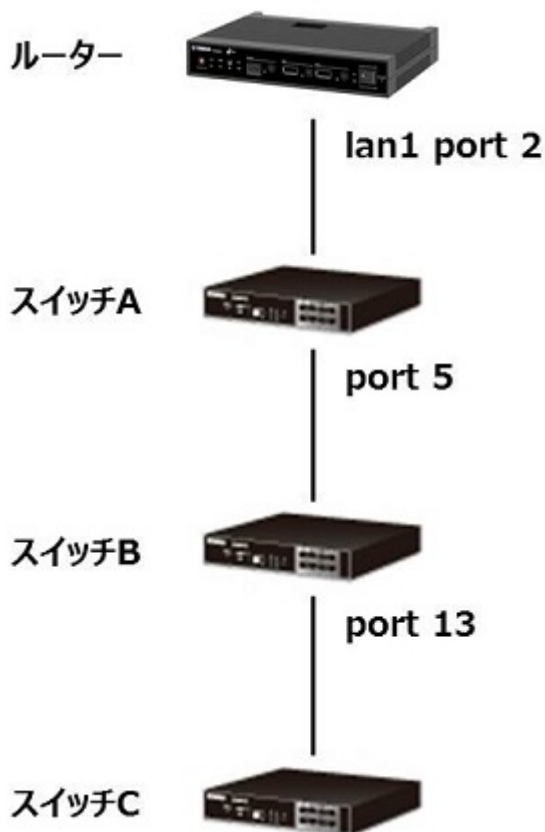
第 39 章

スイッチ制御機能

スイッチ制御機能とは、ヤマハのスイッチと無線 LAN アクセスポイントをルーターから制御するための機能です。スイッチやアクセスポイ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 インタフェースを指定します。
- LAN インタ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。

39.1 共通の設定

39.1.1 スイッチ制御機能を使用するか否かの設定

[書式]

```
switch control use interface use
```

```
no switch control use interface
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [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

[説明]

スイッチ制御機能を使用するか否かを LAN インタフェースごとに設定する。本コマンドが on に設定されたインタフェースでは、スイッチ制御機能に対応したスイッチを制御するための通信が行われる。スイッチ制御機能に対応したスイッチを配下に接続しないインタフェースにおいては本コマンドを 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。

[ノート]

interface には物理的な LAN インタフェース (lanN) のみを指定することができる。LAN 分割機能またはポート分離機能が有効になっているインタフェースでは本コマンドを設定することができない。

39.1.2 スイッチ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]

スイッチを探索するパケットの送信時間間隔、およびスイッチ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、スイッチを接続してからルータ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、スイッチを接続してからルータ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スイッチから応答パケットを受信しない場合、当該スイッチはダウンしたと判断する。

[ノート]

スイッチ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スイッチがダウンしたと判断することがある。

39.2 スイッチの制御

39.2.1 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。

39.2.2 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。

39.2.3 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。

39.2.4 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。

39.2.5 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。

39.2.6 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。

39.2.7 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。

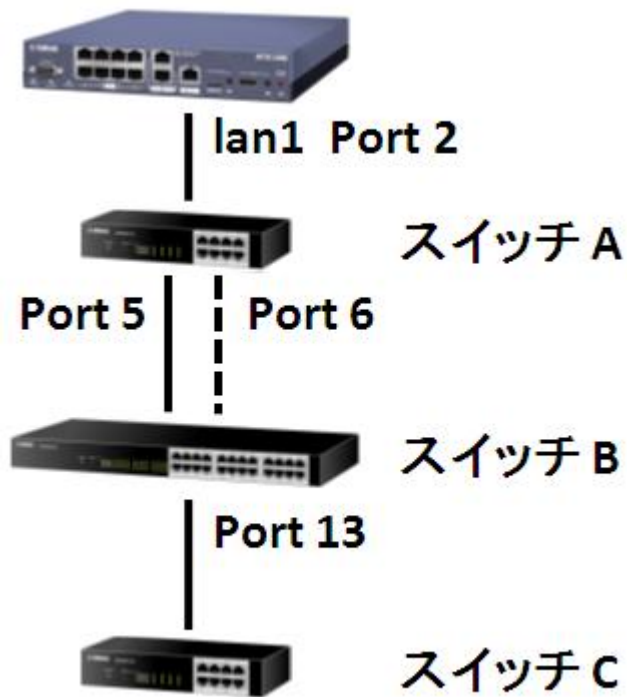
スイッチに本機能が実装されていない場合はコマンドエラーとなる。

Rev.11.00.23 以降で使用可能。

[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
```



39.3 スイッチの機能

39.3.1 システム

39.3.1.1 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。

39.3.1.2 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。

39.3.1.3 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。

39.3.1.4 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。

39.3.1.5 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。

39.3.1.6 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 (_)

39.3.1.7 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。

39.3.1.8 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。

39.3.1.9 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。 <ul style="list-style-type: none"> • 緑色で点灯: リンク確立状態 • 緑色で点滅: データ転送中 • 消灯: リンク喪失状態
speed	各ポートの接続速度を表示する。 <ul style="list-style-type: none"> • 緑色で点灯: 1000BASE-T で接続 • 橙色で点灯: 100BASE-TX で接続 • 消灯: 10BASE-T で接続
duplex	各ポートの接続状態 (全二重/半二重) を表示する。 <ul style="list-style-type: none"> • 緑色で点灯: 全二重で接続 • 橙色で点灯: 半二重で接続
status	機器の状態を表示。 <ul style="list-style-type: none"> • 橙色で点灯: ループを検出 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。

39.3.1.10 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。

39.3.1.11 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。

39.3.1.12 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。

39.3.1.13 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。

39.3.2 ポート**39.3.2.1 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

状態	説明
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。

39.3.2.2 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。

39.3.2.3 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

設定値	説明
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。

39.3.2.4 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。

39.3.2.5 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。

39.3.2.6 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。

39.3.2.7 スイッチ制御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]

スイッチ制御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。
Rev.11.00.23 以降で使用可能。

39.3.2.8 スイッチ制御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]

スイッチ制御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。
Rev.11.00.23 以降で使用可能。

39.3.2.9 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。

39.3.2.10 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。

39.3.2.11 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

39.3.3 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	

39.3.3.1 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。

39.3.3.2 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。

39.3.3.3 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。

39.3.3.4 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。

39.3.3.5 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。

39.3.4 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
```

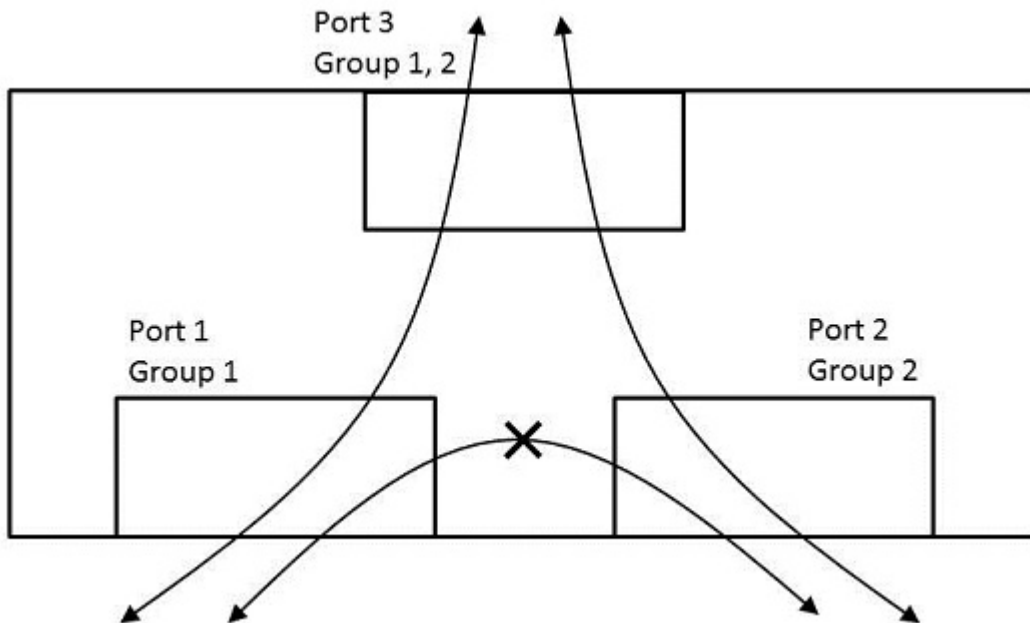
スイッチで受信したパケットは、VLAN タグの有無に関わらずいずれかの VLAN ID に分類され、その情報に基づいて転送処理が行われます。ポートの VLAN 動作モードは **vlan-port-mode** で設定します。

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 vlan-access 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 (vlan-access) 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 vlan-trunk 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 (vlan-trunk) 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 (vlan-access) 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 (vlan-trunk) 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。

39.3.4.1 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。

39.3.4.2 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。

39.3.4.3 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。

39.3.4.4 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。

39.3.4.5 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。

39.3.4.6 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。

39.3.5 QoS

DSCP リマージングは、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	

39.3.5.1 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。

39.3.5.2 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。

39.3.5.3 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。

39.3.5.4 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。

39.3.5.5 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。

39.3.5.6 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。

39.3.5.7 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。

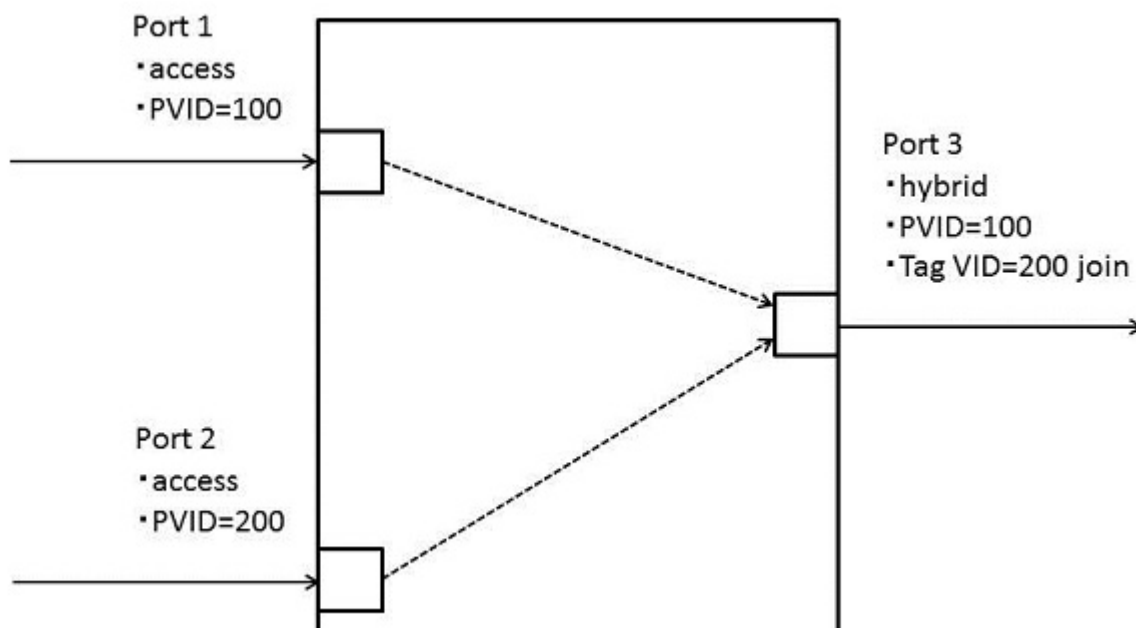
39.3.6 ミラーリング

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 で受信したパケットをポート 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。

39.3.6.1 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。

39.3.6.2 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。

39.3.6.3 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。

39.3.6.4 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。

39.3.7 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 リマール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。

39.3.7.1 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

設定値	説明
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

機種	カウンタ番号	種類
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。

39.3.7.2 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
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

設定値	説明
packets-1024-to-1526-octets	1024～1526 オクテットの packets
pause	PAUSE packets
fifo-drops	送信バッファのオーバーフローで破棄された packets
total-good-packets	正常に送信された packets
class-0	送信キュー class-0 から送信された packets
class-1	送信キュー class-1 から送信された packets
class-2	送信キュー class-2 から送信された packets
class-3	送信キュー class-3 から送信された packets
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 packets
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 packets (CFI ビットが 1 である packets を受信し、当該 packets 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。

39.3.7.3 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。

39.3.7.4 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。

39.3.7.5 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。

39.3.7.6 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。

39.3.7.7 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。

39.3.8 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スイッチ制御パケットを監視する方法の 2 種類の 방법으로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。

スイッチ制御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。

39.3.8.1 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。

39.3.8.2 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。

39.3.8.3 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。

39.3.8.4 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。

39.3.8.5 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。

39.3.8.6 スイッチ制御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]

スイッチ制御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。

Rev.11.00.23 以降で使用可能。

39.3.8.7 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

状態	説明
linkdown	ループが発生したため、リンクダウンした

39.3.8.8 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。

39.3.8.9 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。

39.3.9 PoE 給電

39.3.9.1 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い。

39.3.9.2 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 で使用可能。

39.3.9.3 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 で使用可能。

39.3.9.4 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。

39.3.9.5 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 で使用可能。

39.3.9.6 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。

39.3.9.7 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。

39.3.9.8 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。

39.3.9.9 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。

39.3.9.10 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。

39.4 アクセスポイントの制御

39.4.1 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。

39.4.2 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
 - [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。

39.4.3 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
 - [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 が付いたものが使用される。
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。

39.4.4 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 インタフェースを指定すると、LAN インタ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。

39.4.5 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 インタフェースを指定すると、LAN インタ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。

39.4.6 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。

39.4.7 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。

39.4.8 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。

39.4.9 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]

スイッチ制御機能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なくてもアクセスポイントの設定ができる。

39.4.10 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。

第 40 章

操作

40.1 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。

40.2 トンネルインタ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	トンネルインタフェース番号
none	トンネルインタ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。

40.3 設定に関する操作

40.3.1 管理ユーザへの移行

[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。

40.3.2 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。

40.3.3 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	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB ポート 1 に接続された USB メモリ内の設定ファイル名 (<i>filename</i> は半角 99 文字以内)
usb2: <i>filename</i>	USB ポート 2 に接続された 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。

[ノート]

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

40.3.4 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	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB ポート 1 に接続された 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)
usb2: <i>filename</i>	USB ポート 2 に接続された 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)
usb*: <i>filename</i>	USB ポート 1 および USB ポート 2 に接続された 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)

- [初期値]: -

- to* : コピー先ファイル名

- [設定値]:

設定値	説明
0	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB ポート 1 に接続された 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)
usb2: <i>filename</i>	USB ポート 2 に接続された 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 ポートに接続された 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。

from に "usb*:" を指定した場合、指定するファイルの検索はまず USB ポート 1 に接続された USB ストレージから行われ、指定したファイルがなければ USB ポート 2 に接続された USB ストレージが検索される。
from 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 ポート 1 に接続された USB ストレージ、USB ポート 2 に接続された USB ストレージの順に検索される。

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。

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

40.3.5 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
usb1:filename	USB ポート 1 に接続された 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)
usb2:filename	USB ポート 2 に接続された 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)
usb*:filename	USB ポート 1 および USB ポート 2 に接続された 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]: -
- *to*: コピー先ファイル名
- [設定値]:

設定値	説明
0	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

- [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。

from に "usb*:" を指定した場合、指定するファイルの検索はまず USB ポート 1 に接続された USB メモリから行われ、指定したファイルがなければ USB ポート 2 に接続された USB メモリが検索される。

from 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 ポート 1 に接続された USB メモリ、USB ポート 2 に接続された USB メモリの順に検索される。

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。

Rev.11.00.07 以前では、*filename* は半角 64 文字以内。

40.3.6 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]: 0 (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。

40.3.7 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。

40.3.8 遠隔地のルーターの設定

[書式]

remote setup interface [*number* [/sub_address]] [*type*]

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *number*
 - [設定値]: ISDN 番号
 - [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
 - [初期値]: -
- *type*: リモートセットアップの方式
 - [設定値]:

設定値	説明
retransmission	データの欠落に対応できる方式

- [初期値]: -

[説明]

指定したインタフェースを利用して、遠隔地のルーターの設定をする。
インタフェースには、ISDN、専用線いずれの場合でも設定できる。
FOMA に対してリモートセットアップを行う場合のみ、**retransmission** の指定が必要である。
retransmission を指定した場合は、データの欠落を復旧できる仕組みのリモートセットアップを行い、今までのリモートセットアップ機能とは互換性がない。

[ノート]

専用線の場合は、*number*、*sub_address* パラメータは不要。

40.3.9 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。

40.4 動的情報のクリア操作

40.4.1 アカウントのクリア

[書式]

```
clear account
clear account interface
clear account pp [peer_num]
clear account pstn
clear account sip
clear account ngn data
clear account ngn tel
clear account mobile
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [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]: -

[説明]

指定したインタフェース (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。

mobile の指定は Rev.11.00.16 以降で指定可能。

40.4.2 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

設定値	説明
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。

40.4.3 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。

40.4.4 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。

40.4.5 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。

[ノート]

saved オプションは Rev.11.00.35 以降で指定可能。

40.4.6 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。

40.4.7 インタフェースのカウンター情報のクリア

[書式]

```
clear status interface
```

```
clear status pp peer_num
```

```
clear status tunnel tunnel_num
```

[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
- [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

指定したインタフェースのカウンター情報をクリアする。

[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。

40.4.8 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 ディスクリプタ番号
all	すべての NAT ディスクリプタ番号

- [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。

40.4.9 インタフェースの 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 インタフェース名, WAN インタフェース名
 - [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フェース

- [初期値]:-

[説明]

インタ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。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

40.4.10 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。

40.4.11 近隣キャッシュの消去

[書式]

```
clear ipv6 neighbor cache
```

[説明]

近隣キャッシュを消去する。

40.4.12 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。

40.4.13 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。

[ノート]

Rev.11.00.13 以降で使用可能。

40.5 ファイル、ディレクトリの操作

40.5.1 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。

40.5.2 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。

40.5.3 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。

40.5.4 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/ディレクトリを示す相対パスまたは絶対パス
 - [初期値]: -
- *name*
 - [設定値]: 新しいファイル名/ディレクトリ名または新しいパスを示す相対パスまたは絶対パス
 - [初期値]: -

[説明]

指定したファイル/ディレクトリの名前、または、パスを変更する。

path / *name* 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。なお、*name* に "/" が一つも含まれていない場合は、相対パスの指定ではなく、名前の指定と判断される。

40.6 その他の操作

40.6.1 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 Rev.11.00.36 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。

40.6.2 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 Rev.11.00.36 以降で使用可能。

40.6.3 再起動

[書式]

```
restart
```

```
restart config_name
```

[設定値及び初期値]

- *config_name*: 設定ファイル名
 - [設定値]: 0
 - [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を指定できる。

40.6.4 インタフェースの再起動

[書式]

```
interface reset interface [interface ...]
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - LAN インタフェース名
 - WAN インタフェース名
 - BRI インタフェース名
 - USB インタフェース名
 - SD インタフェース名
 - [初期値]: -

[説明]

指定したインタフェースを再起動する。

LAN インタフェースでは、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。

BRI インタフェースでは、回線種別を **line type** コマンドで変更した場合には、本コマンドでインタフェースを再起動する必要がある。

BRI インタフェースで、MP を使用している場合には、**interface reset pp** コマンドを使用する。

USB と SD インタフェースでは、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]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

USB と SD インタフェースは Rev.11.00.28 以降で指定可能。

NVR500 では、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 インタフェースが同時にリセットされる。

line type コマンド、**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、また回線種別を変更する場合には回線を抜いた状態で実行すること。

40.6.5 PP インタフェースの再起動

[書式]

```
interface reset pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]:-

[説明]

選択した相手先番号にバインドされているインタフェースをリセットする。MP を使用しているインタフェースに対して使用する。

40.6.6 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
 - [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。
 データコネクト接続機能を実装していないモデルでは、**connect pp** コマンド、**connect tunnel** コマンドは使用できない。
 WAN インタフェースは Rev.11.00.16 以降で指定可能。

40.6.7 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
 - [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。
 データコネクト接続機能を実装していないモデルでは、**disconnect pp** コマンド、**disconnect tunnel** コマンドは使用できない。
 WAN インタフェースは Rev.11.00.16 以降で指定可能。

40.6.8 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
 - [設定値]:

設定値	説明
1..65535 バイト	Rev.11.00.16 以降
64..65535 バイト	上記以外

- [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
 - [設定値]:

設定値	説明
0.1 .. 3600.0	Rev.11.00.28 以降
0.1 .. 99.9	上記以外

- [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。

40.6.9 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
 - [設定値]:

設定値	説明
0.1 .. 3600.0	Rev.11.00.28 以降
0.1 .. 99.9	上記以外

- [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。

第 1 ~ 第 5 書式は、Rev.11.00.16 以降のリビジョンで指定できる。それ以外のリビジョンでは、第 6 ~ 第 10 書式で指定する。

count パラメータを省略すると、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。

[ノート]

-s オプション、-c オプション、-sa オプション、-w オプションは Rev.11.00.16 以降で使用可能。

40.6.10 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。

40.6.11 traceroute6 の実行

[書式]

traceroute6 *destination*

[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]: -

[説明]

指定した宛先までの経路を調べて表示する。

40.6.12 nslookup

[書式]

nslookup *host*

[設定値及び初期値]

- *host*
 - [設定値]:
 - IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - ホスト名
 - [初期値]: -

[説明]

DNS による名前解決を行う。

[ノート]

IPv4 のみ対応。

40.6.13 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。

40.6.14 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。

40.6.15 IPv4 動的フィルタのコネクション管理情報の削除

[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。

40.6.16 IPv6 動的フィルタのコネクション管理情報の削除

[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。

40.6.17 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。

40.6.18 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* パラメータが on にされた時点で消去される。

40.6.19 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 インタフェース以外には Magic Packet を送信できない。

40.6.20 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]

[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]: -

[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。

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。

40.6.21 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。

40.6.22 累積課金情報のメール通知の実行

[書式]

mail notify account 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]

累積課金情報のメールを通知する。

40.6.23 SSL 公開鍵の生成

[書式]

ssl public key generate [SEED]
no ssl public key generate

[設定値及び初期値]

- *SEED*
 - [設定値]: 公開鍵の基になる数(0..4294967295)
 - [初期値]: -

[説明]

SSL の公開鍵を生成する。
SEED を省略した場合はランダムな値が自動的に設定される。

[ノート]

既に公開鍵が生成されている状態で本コマンドを実行した場合、ユーザに対して公開鍵を更新するか否かを確認する。

公開鍵の生成には、機種によって 10 秒から 1 分程度の時間を要し、その間は応答が返ってこない。
TFTP で設定を取得した場合は、**ssl public key generate SEED KEY1 KEY2** という形式で保存される。KEY1 と KEY2 は、それぞれ RSA 秘密鍵と DSA 秘密鍵を機器固有の方式で暗号化した文字列である。そのため、保存した設定を他の機器に適用した場合は、KEY1 および KEY2 は同一の文字とはならない。

40.6.24 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。

Rev.11.00.13 以降で使用可能。

[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
```

第 41 章

設定の表示

41.1 機器設定の表示

[書式]

show environment

[説明]

以下の項目が表示される。

- システムのレビジョン
- MAC アドレス
- CPU、メモリの使用量 (%)
- 動作しているファームウェアファイルと起動時に使用した設定ファイルの名前
- 起動時刻、現在の時刻、起動してから現在までの経過時間
- セキュリティクラス

41.2 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
 - [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合わせられる。

41.3 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。

[ノート]

Rev.11.00.28 以降で使用可能。

41.4 指定した PP の設定内容の表示

[書式]

```
show config pp [peer_num]
```

```
less config 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]

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。

41.5 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。

[ノート]

Rev.11.00.28 以降で使用可能。

41.6 指定したトンネルの設定内容の表示

[書式]

```
show config tunnel [tunnel_num] [expand]
```

```
less config tunnel [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。

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]

Rev.11.00.36 以降で expand パラメーターを指定可能。

41.7 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。

41.8 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。

41.9 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
usb1:[DIR]	USB ポート 1 に接続された USB メモリ
usb2:[DIR]	USB ポート 2 に接続された USB メモリ
sd1:[DIR]	microSD カード
相対パスまたは絶対パス	ファイルの格納場所のパス

- [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。

起動中の設定ファイルに '*' が表示される。

41.10 インタ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 インタフェース名、LOOPBACK インタフェース名、NULL インタフェース
 - [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]: トンネルインタフェース番号
 - [初期値]: -

[説明]

各インタフェースに付与されている IPv6 アドレスを表示する。
 インタフェースを指定しない場合は、すべてのインタフェースについて情報を表示する。

41.11 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。

[ノート]

fingerprint キーワードは、Rev.11.00.35 以降で使用可能。

[表示例]

```
> show sshd public key
ssh-dss XXXXXXXXXXXX1kc3MAAAEBAPTb9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXg
sXJoCq1PlsLRGH0OzxVYbOouPCUV/jPFcatgOIii8eJNzUqSB1e6MOftGjmESrdYiafyIUhps+YWqd
T1Io0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKwklChbatWnT/Z7RcmEVEou0q1Oyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok81L5qFhChmGOGtqJTKZsqb5VnVpZ8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWzcZwGa6LxTGMczAjDy5uD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXXXX
ssh-rsa XXXXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3KnB7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwFMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk561AU23CW/i21o//5GZTzkFKyEJUWauHWEW9g1F5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvryr3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYcjmUwH6Ek/cst+Pctgnt0XV5B1079uRUmCACs2pDX5EWrbwPXXXXXXXXXX==

> show sshd public key fingerprint
```

```
ssh-dss 2048 XX:XX:77:c5:f9:48:fd:62:85:fb:27:a8:0a:c1:XX:XX
ssh-rsa 2048 XX:XX:58:89:e2:0b:ec:d9:6b:49:11:d2:a3:9d:XX:XX
```

41.12 SSL サーバー公開鍵の表示

[書式]

```
show ssl public key
```

[説明]

SSL サーバーの公開鍵を表示する。

41.13 指定したインタフェースのフィルタ内容の表示

[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]: フィルタの適用されたインタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *dir*
 - [設定値]: フィルタの適用された方向、'in' または 'out'
 - [初期値]: -

[説明]

指定したインタフェースに適用されているフィルタ定義の内容を表示する。

41.14 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。

[ノート]

Rev.11.00.25 以降で使用可能。

第 42 章

状態の表示

42.1 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 インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-8
 - [初期値]: -

[説明]

ARP テーブルを表示する。インタフェース名を指定した場合、そのインタ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。

[ノート]

sub_interface パラメータは Rev.11.00.16 以降で指定可能。

42.2 インタフェースの状態の表示

[書式]

```
show status interface
```

[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
 - BRI インタフェース名
 - [初期値]: -

[説明]

インタフェースの状態を表示する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.3 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

42.4 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

42.5 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。

42.6 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。

42.7 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。

42.8 近隣キャッシュの表示

[書式]

show ipv6 neighbor cache

[説明]

近隣キャッシュの状態を表示する。

42.9 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・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

- 適用したフィルタの情報
を同時に表示する。
Rev.11.00.36 以降で使用可能。

42.10 動的 NAT ディスクリプタのアドレスマップの表示

[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 ディスクリプタ番号
all	すべての NAT ディスクリプタ番号

- [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 ディスクリプタのアドレスマップを表示する。
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。

42.11 動作中の NAT ディスクリプタ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 インタフェース名、WAN インタフェース名
 - [初期値]: -

[説明]

NAT ディスクリプタと適用インタフェースのリストを表示する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.12 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示

[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 インタフェース名、WAN インタフェース名
- [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.13 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。

42.14 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]

Rev.11.00.36 以降で使用可能。

42.15 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。

42.16 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)

42.17 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

42.18 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。

42.19 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]]  

show ip connection pp [peer_num [direction]]  

show ip connection tunnel [tunnel_num [direction]]  

show ip connection summary
```

[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
 - [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]: -
- *summary*: インタフェース/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]: -

[説明]

指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.20 IPv6 の動的フィルタ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]
show ipv6 connection pp [peer_num [direction]]
show ipv6 connection tunnel [tunnel_num [direction]]
show ipv6 connection summary
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [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]: -
- *summary*: インタフェース/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]: -

[説明]

指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

42.21 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。

42.22 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 インタフェース名、WAN インタフェース名
 - [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。各インタフェースの各方向ごとに最大 50 件まで表示できる。

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.23 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。

42.24 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 インタフェース名、WAN インタフェース名
 - [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

[ノート]

WAN インタフェースは Rev.11.00.16 以降で指定可能。

42.25 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 インタフェース名にはスイッチングハブを持つインタフェースだけが指定可能である。

42.26 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。

42.27 トンネルインタフェースの状態の表示

[書式]

```
show status tunnel [tunnel_num]
```

```
show status tunnel [state]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [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フェース一覧を表示する
down	接続されていないトンネルインタフェース一覧を表示する

- [初期値]: -

[説明]

トンネルインタ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ため、PPTP トンネルは接続されていないトンネルインタフェースとして判定される。また、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。

[ノート]

第 2 書式は Rev.11.00.36 以降で使用可能。

42.28 VLAN インタ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 インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-8
 - [初期値]: -

[説明]

VLAN インタフェースの情報を表示する。VLAN インタフェース名を指定した場合はそのインタフェースの情報だけを表示する。

[ノート]

Rev.11.00.16 以降で使用可能。

42.29 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。

42.30 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。

42.31 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	出力インタフェース。複数のインタフェースに出力される場合は、";" 区切りで表示される。

42.32 ログインしているユーザ情報の表示

[書式]

```
show status user
```

[説明]

ルーターにログインしているユーザの情報を表示する。以下の項目が表示される。

- ユーザ名
- 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、ユーザの状態に応じてユーザ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
アットマーク (@)	RADIUS 認証でログインした

[ノート]

RADIUS 認証でログインしたユーザーが表示されるのは Rev.11.00.36 以降である。

[表示例]

```
> show status user
(*: 自分自身のユーザー情報, +: 管理者モード, @: RADIUS での認証)
ユーザー名      接続種別      ログイン      アイドル      IP アドレス
-----
user-local      serial        09/16 10:21   0:00:17
@user-radius2   remote       09/16 10:22   0:00:36
*+@user-radius1 telnet1      09/16 10:22   0:00:00      192.168.0.100

> show status user
(*: current user, +: administrator mode, @: authenticated via RADIUS)
username      connection login time      idle      IP address
-----
user-local      serial        09/16 10:21   0:02:08
@user-radius2   remote       09/16 10:22   0:02:27
*+@user-radius1 telnet1      09/16 10:22   0:00:00      192.168.0.100
```

42.33 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
- 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=2000 max-free=562 min-free=12
            buffers-in-chunk=125 initial-chunk=4
244 buffers in free list
256 buffers are allocated, req/succ/fail/rel = 265/265/0/9
4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

42.34 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 インタフェース名 (省略時、全ての LAN インタフェースについて表示する)
 - [初期値] :-
- *class*
 - [設定値] : クラス (1..16)
 - [初期値] :-

[説明]

インタフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。

- LAN インタフェース名
- キューイングアルゴリズム
- インタフェース速度
- 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

42.35 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
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

42.36 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。

42.37 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
```

42.38 USB ホスト機能の動作状態を表示

[書式]

```
show status usbhost [port]
```

```
show status usbhost modem [port]
```

[設定値及び初期値]

- *port* : USB ポート番号

- [設定値]:

設定値	説明
1	USB ポート 1
2	USB ポート 2
省略	省略時はすべてのポート番号

- [初期値]:-

[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。

42.39 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。

42.40 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。

42.41 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           : 524288 バイト
空き容量       : 517449 バイト
```

```
作成可能エントリ数 : 995
ファイル数          : 2
ディレクトリ数     : 3
#
```

42.42 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 ユーザのルーターへのサインイン状態を表示する。

42.43 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

42.44 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。

42.45 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。

42.46 音声の処理状態の表示

[書式]

show status voice process

[説明]

音声の処理状態を表示する。

42.47 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なう。

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)

42.48 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。

42.49 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。

42.50 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。

42.51 ルーターが制御しているスイッチ一覧の表示

[書式]

```
show status switch control interface
```

[設定値及び初期値]

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

[説明]

ルーターが制御しているスイッチの一覧を表示する。インタフェースを指定しない場合は、すべてのインタフェースについて情報を表示する。

- MAC アドレス
- 機種名
- 機器名
- ルーターからの経路
- アップリンクポート
- スイッチ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

[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
---
LAN3
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.
---
LAN3
Switch control function is not available.
```


42.52 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。

Rev.11.00.23 以降で使用可能。

42.53 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。

[ノート]

Rev.11.00.20 以降で使用可能。

42.54 WAN LED の情報の表示

[書式]

```
show status status-led [history]
```

[設定値及び初期値]

- history : WAN LED の状態変化の履歴を表示
 - [初期値]: -

[説明]

WAN 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。

[ノート]

Rev.11.00.28 以降で使用可能。

42.55 上面スイッチの状態の表示

[書式]

show status isdn switch

[説明]

上面スイッチの状態を表示する。

[ノート]

Rev.11.00.28 以降で使用可能。

42.56 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。

[ノート]

本コマンドは Rev.11.00.35 以降で使用可能。

第 43 章

ログイン

43.1 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 3000 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中身を表示する。Rev.11.00.13 以降では、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。また、バックアップファイルの中身を表示するには、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。

saved パラメータは Rev.11.00.16 以降で使用可能。

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。

43.2 アカウントの表示

[書式]

```
show account
show account interface
show account pp [peer_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [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]: -

[説明]

以下の項目を表示

- 発信回数
- 着信回数
- ISDN 料金の総計

[ノート]

電源 OFF や再起動により、それまでの課金情報がクリアされる。

課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

43.3 アナログ関係のアカウントの表示

[書式]

```
show account analog [port]
show account analog total
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]: -
- *total*
 - [設定値]: 電話回線を示すキーワード
 - [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と課金合計を表示する。

[ノート]

- ISDN 回線を使用している場合

課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合があります。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

- アナログ回線を使用している場合

アナログ回線では料金情報は通知されないため、アカウントとしても集計されない。

43.4 アナログ回線のアカウントの表示

[書式]

```
show account pstn
```

[説明]

アナログ回線の発着信回数を表示する。

43.5 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。

43.6 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。

43.7 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を表示する。

43.8 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。

[ノート]

Rev.11.00.16 以降で使用可能。

43.9 通信履歴の表示

[書式]

```
show history
```

[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。

履歴は、ルーターの電源を切ると消去される。

索引

記号

> 36
>> 36

A

account threshold 83
 account threshold pp 83
 administrator 500
 administrator password 39
 administrator password encrypted 39
 administrator radius auth 40
 alarm batch 73
 alarm connection analog 71
 alarm connection data 71
 alarm entire 70
 alarm http revision-up 73
 alarm intrusion 71
 alarm lua 439
 alarm mp 72
 alarm sd 72
 alarm startup 73
 alarm usbhost 72
 analog arrive another-device permit 314
 analog arrive global permit 311
 analog arrive ignore-subaddress permit 313
 analog arrive incoming-signal 328
 analog arrive incoming-signal timing pb 330
 analog arrive innumber-port 328
 analog arrive number display 316
 analog arrive priority 316
 analog arrive restrict 311
 analog arrive restrict list 312
 analog arrive ring-while-talking permit 314
 analog arrive ringer-type list 315
 analog arrive without-calling-number 330
 analog arrive without-subaddress permit 313
 analog call route 363
 analog call route-table 362
 analog device type 309
 analog disc-signal 325
 analog dtmf level 326
 analog end-of-dialing-code 310
 analog extension address refer 338
 analog extension agent permit 339
 analog extension dial prefix 360
 analog extension emergency-call-dial type 327
 analog extension incoming ringer 327
 analog extension log 340
 analog extension machine-id 340
 analog extension manager 339
 analog extension mode 338
 analog extension other-dial-tone 327
 analog extension sip address 343
 analog hooking inhibit timer 318
 analog hooking timer 317
 analog hooking wait timer 317
 analog impedance 319
 analog local address 308
 analog local address notice 309
 analog loop-closure threshold 319
 analog mp prior 325
 analog off-hook mask 318
 analog pad receive 324
 analog pad rtp receive 331
 analog pad rtp send 332
 analog pad send 324

analog pause timer 332
 analog power 333
 analog rapid call 310
 analog re-ringing-timer 320
 analog sip arrive incoming-signal 359
 analog sip arrive myaddress 359
 analog sip arrive permit 358
 analog sip call display name 357
 analog sip call myname 357
 analog sip call permit 357
 analog supplementary-service 321
 analog supplementary-service call-deflection address 321
 analog supplementary-service call-deflection reject 323
 analog supplementary-service call-deflection ringer 322
 analog supplementary-service call-deflection talkie 322
 analog use 308
 analog wait dial timer 317
 ap config directory 494
 ap config filename 495
 ap control config delete 496
 ap control config get 495
 ap control config set 496
 ap control config-auto-set use 496
 ap control firmware update go 497
 ap control http proxy timeout 498
 ap control http proxy use 497
 ap select 494
 audio echo-canceller 74
 audio echo-canceller disabler 76
 audio echo-canceller nlp threshold 75
 audio hold-tone type 320
 audio jitter-buffer 76
 audio rtp port 78
 audio rtp segsize 77
 auth user 198
 auth user attribute 199
 auth user group 199
 auth user group attribute 200

C

clear account 505
 clear account analog 505
 clear account mobile 505
 clear account ngn data 505
 clear account ngn tel 505
 clear account pp 505
 clear account pstn 505
 clear account sip 505
 clear acl 449
 clear arp 506
 clear boot list 508
 clear dns cache 506
 clear external-memory syslog 508
 clear ip dynamic routing 506
 clear ipv6 dynamic routing 508
 clear ipv6 neighbor cache 508
 clear log 506
 clear mobile access limitation 415
 clear mobile access limitation pp 415
 clear nat descriptor dynamic 507
 clear nat descriptor interface dynamic 507
 clear nat descriptor interface dynamic pp 507
 clear nat descriptor interface dynamic tunnel 507
 clear status 506
 clear switching-hub macaddress 518
 cold start 504
 connect 512

connect pp 512
 connect tunnel 512
 console character 50
 console columns 50
 console info 51
 console lines 51
 console prompt 50
 cooperation 275
 cooperation bandwidth-measuring remote 275
 cooperation load-watch control 280
 cooperation load-watch remote 277
 cooperation load-watch trigger 278
 cooperation port 275
 cooperation type go 280
 copy 509
 copy config 501
 copy exec 502

D

date 47
 delete 509
 delete config 503
 description 62
 dhcp client client-identifier 167
 dhcp client client-identifier pool 167
 dhcp client client-identifier pp 167
 dhcp client hostname 165
 dhcp client hostname pool 165
 dhcp client hostname pp 165
 dhcp client option 167
 dhcp client option pool 167
 dhcp client option pp 167
 dhcp client release linkdown 168
 dhcp convert lease to bind 160
 dhcp duplicate check 156
 dhcp manual lease 162
 dhcp manual release 163
 dhcp relay select 163
 dhcp relay server 163
 dhcp relay threshold 164
 dhcp scope 156
 dhcp scope bind 158
 dhcp scope lease type 159
 dhcp scope option 161
 dhcp server rfc2131 compliant 155
 dhcp service 154
 disconnect 513
 disconnect ip connection 516
 disconnect ipv6 connection 517
 disconnect pp 513
 disconnect tunnel 513
 disconnect user 43
 dns cache max entry 267
 dns cache use 266
 dns domain 261
 dns host 266
 dns notice order 262
 dns private address spoof 262
 dns private name 260
 dns server 260
 dns server dhcp 165
 dns server pp 261
 dns server select 263
 dns service 260
 dns service fallback 267
 dns srport 266
 dns static 264
 dns syslog resolv 262

E

ethernet filter 132
 ethernet interface filter 134
 execute at-command 414
 execute batch 409
 exit 500
 external-memory accelerator cache size 403
 external-memory auto-search time 409
 external-memory batch filename 410
 external-memory boot permit 406
 external-memory boot timeout 406
 external-memory cache mode 402
 external-memory config filename 408
 external-memory exec filename 407
 external-memory performance-test go 410
 external-memory syslog filename 404

G

grep 34

H

help 38
 http revision-down permit 65
 http revision-up go 519
 http revision-up permit 64
 http revision-up proxy 65
 http revision-up schedule 66
 http revision-up timeout 65
 http revision-up url 64
 httpd custom-gui api password 441
 httpd custom-gui api use 441
 httpd custom-gui use 440
 httpd custom-gui user 440
 httpd host 372
 httpd listen 373
 httpd service 372
 httpd timeout 373

I

interface reset 511
 interface reset pp 512
 ip arp timer 116
 ip filter 104
 ip filter directed-broadcast 107
 ip filter dynamic 108
 ip filter dynamic timer 109
 ip filter set 106
 ip filter source-route 107
 ip flow timer 119
 ip fragment remove df-bit 115
 ip host 264
 ip icmp echo-reply send 170
 ip icmp echo-reply send-only-linkup 170
 ip icmp error-decrypted-ipsec send 173
 ip icmp log 174
 ip icmp mask-reply send 170
 ip icmp parameter-problem send 171
 ip icmp redirect receive 171
 ip icmp redirect send 171
 ip icmp time-exceeded send 172
 ip icmp timestamp-reply send 172
 ip icmp unreachable send 173
 ip interface address 99
 ip interface arp log 117
 ip interface arp queue length 117
 ip interface arp static 116
 ip interface dhcp lease time 166

- ip interface dhcp retry [166](#)
- ip interface dhcp service [164](#)
- ip interface intrusion detection [110](#)
- ip interface intrusion detection notice-interval [111](#)
- ip interface intrusion detection repeat-control [111](#)
- ip interface intrusion detection report [112](#)
- ip interface mtu [100](#)
- ip interface nat descriptor [251](#)
- ip interface proxyarp [116](#)
- ip interface rebound [101](#)
- ip interface rip auth key [127](#)
- ip interface rip auth key text [127](#)
- ip interface rip auth type [127](#)
- ip interface rip filter [126](#)
- ip interface rip force-to-advertise [130](#)
- ip interface rip hop [126](#)
- ip interface rip receive [125](#)
- ip interface rip send [124](#)
- ip interface rip trust gateway [123](#)
- ip interface secondary address [100](#)
- ip interface secure filter [114](#)
- ip interface secure filter name [114](#)
- ip interface tcp mss limit [112](#)
- ip interface tcp window-scale [113](#)
- ip interface wol relay [63](#)
- ip keepalive [117](#)
- ip pp address [99](#)
- ip pp intrusion detection [110](#)
- ip pp intrusion detection notice-interval [111](#)
- ip pp intrusion detection repeat-control [111](#)
- ip pp intrusion detection report [112](#)
- ip pp mtu [100](#)
- ip pp nat descriptor [251](#)
- ip pp rebound [101](#)
- ip pp remote address [119](#)
- ip pp remote address pool [120](#)
- ip pp rip auth key [127](#)
- ip pp rip auth key text [127](#)
- ip pp rip auth type [127](#)
- ip pp rip connect interval [128](#)
- ip pp rip connect send [128](#)
- ip pp rip disconnect interval [129](#)
- ip pp rip disconnect send [129](#)
- ip pp rip filter [126](#)
- ip pp rip force-to-advertise [130](#)
- ip pp rip hold routing [128](#)
- ip pp rip hop [126](#)
- ip pp rip receive [125](#)
- ip pp rip send [124](#)
- ip pp rip trust gateway [123](#)
- ip pp secure filter [114](#)
- ip pp secure filter name [114](#)
- ip pp tcp mss limit [112](#)
- ip pp tcp window-scale [113](#)
- ip route [102](#)
- ip route change log [114](#)
- ip routing [99](#)
- ip routing process [58](#)
- ip simple-service [101](#)
- ip stealth [174](#)
- ip tunnel address [181](#)
- ip tunnel intrusion detection [110](#)
- ip tunnel intrusion detection notice-interval [111](#)
- ip tunnel intrusion detection repeat-control [111](#)
- ip tunnel intrusion detection report [112](#)
- ip tunnel mtu [100](#)
- ip tunnel nat descriptor [251](#)
- ip tunnel rebound [101](#)
- ip tunnel remote address [181](#)
- ip tunnel rip auth key [127](#)
- ip tunnel rip auth key text [127](#)
- ip tunnel rip auth type [127](#)
- ip tunnel rip filter [126](#)
- ip tunnel rip force-to-advertise [130](#)
- ip tunnel rip hop [126](#)
- ip tunnel rip receive [125](#)
- ip tunnel rip send [124](#)
- ip tunnel rip trust gateway [123](#)
- ip tunnel secure filter [114](#)
- ip tunnel secure filter name [114](#)
- ip tunnel tcp mss limit [112](#)
- ip tunnel tcp window-scale [113](#)
- ipsec auto refresh [185](#)
- ipsec ike always-on [187](#)
- ipsec ike backward-compatibility [196](#)
- ipsec ike duration [204](#)
- ipsec ike encryption [193](#)
- ipsec ike esp-encapsulation [203](#)
- ipsec ike group [194](#)
- ipsec ike hash [195](#)
- ipsec ike keepalive log [193](#)
- ipsec ike keepalive use [191](#)
- ipsec ike local address [190](#)
- ipsec ike local id [191](#)
- ipsec ike local name [190](#)
- ipsec ike log [203](#)
- ipsec ike mode-cfg address [202](#)
- ipsec ike mode-cfg address pool [201](#)
- ipsec ike mode-cfg method [202](#)
- ipsec ike nat-traversal [208](#)
- ipsec ike negotiate-strictly [186](#)
- ipsec ike payload type [196](#)
- ipsec ike pfs [197](#)
- ipsec ike pre-shared-key [185](#)
- ipsec ike queue length [194](#)
- ipsec ike remote address [188](#)
- ipsec ike remote id [189](#)
- ipsec ike remote name [188](#)
- ipsec ike restrict-dangling-sa [207](#)
- ipsec ike retry [187](#)
- ipsec ike send info [197](#)
- ipsec ike xauth myname [198](#)
- ipsec ike xauth request [201](#)
- ipsec ipcomp type [210](#)
- ipsec log illegal-spi [195](#)
- ipsec refresh sa [206](#)
- ipsec sa delete [208](#)
- ipsec sa policy [205](#)
- ipsec transport [212](#)
- ipsec transport template [213](#)
- ipsec tunnel [210](#)
- ipsec tunnel fastpath-fragment-function follow df-bit [209](#)
- ipsec tunnel outer df-bit [209](#)
- ipsec use [184](#)
- ipv6 filter [299](#)
- ipv6 filter dynamic [300](#)
- ipv6 icmp echo-reply send [174](#)
- ipv6 icmp echo-reply send-only-linkup [175](#)
- ipv6 icmp error-decrypted-ipsec send [178](#)
- ipv6 icmp log [177](#)
- ipv6 icmp packet-too-big send [178](#)
- ipv6 icmp parameter-problem send [175](#)
- ipv6 icmp redirect receive [176](#)
- ipv6 icmp redirect send [175](#)
- ipv6 icmp time-exceeded send [176](#)
- ipv6 icmp unreachable send [177](#)
- ipv6 interface address [284](#)
- ipv6 interface dad retry count [289](#)
- ipv6 interface dhcp service [288](#)
- ipv6 interface mld [302](#)
- ipv6 interface mld static [304](#)
- ipv6 interface mtu [282](#)
- ipv6 interface prefix [286](#)
- ipv6 interface prefix change log [287](#)

- ipv6 interface rip filter 296
- ipv6 interface rip hop 295
- ipv6 interface rip receive 295
- ipv6 interface rip send 294
- ipv6 interface rip trust gateway 296
- ipv6 interface rtadv send 292
- ipv6 interface secure filter 300
- ipv6 interface tcp mss limit 282
- ipv6 interface tcp window-scale 283
- ipv6 max auto address 289
- ipv6 nd ns-trigger-dad 304
- ipv6 pp address 284
- ipv6 pp dad retry count 289
- ipv6 pp dhcp service 288
- ipv6 pp mld 302
- ipv6 pp mld static 304
- ipv6 pp mtu 282
- ipv6 pp prefix 286
- ipv6 pp prefix change log 287
- ipv6 pp rip connect interval 297
- ipv6 pp rip connect send 297
- ipv6 pp rip disconnect interval 298
- ipv6 pp rip disconnect send 297
- ipv6 pp rip filter 296
- ipv6 pp rip hold routing 298
- ipv6 pp rip hop 295
- ipv6 pp rip receive 295
- ipv6 pp rip send 294
- ipv6 pp rip trust gateway 296
- ipv6 pp rtadv send 292
- ipv6 pp secure filter 300
- ipv6 pp tcp mss limit 282
- ipv6 pp tcp window-scale 283
- ipv6 prefix 290
- ipv6 rh0 discard 283
- ipv6 rip preference 298
- ipv6 rip use 294
- ipv6 route 293
- ipv6 routing 282
- ipv6 routing process 284
- ipv6 source address selection rule 289
- ipv6 stealth 178
- ipv6 tunnel address 284
- ipv6 tunnel dhcp service 288
- ipv6 tunnel mld 302
- ipv6 tunnel mld static 304
- ipv6 tunnel prefix 286
- ipv6 tunnel prefix change log 287
- ipv6 tunnel rip filter 296
- ipv6 tunnel rip receive 295
- ipv6 tunnel rip send 294
- ipv6 tunnel secure filter 300
- ipv6 tunnel tcp mss limit 282
- ipv6 tunnel tcp window-scale 283
- isdn arrive inumber-port 97
- isdn arrive permit 88
- isdn auto connect 87
- isdn auto disconnect 87
- isdn call block time 89
- isdn call permit 89
- isdn call prohibit auth-error count 96
- isdn call prohibit mp-error count 96
- isdn call prohibit time 89
- isdn callback mscbc user-specify 91
- isdn callback permit 90
- isdn callback permit type 91
- isdn callback request 90
- isdn callback request type 90
- isdn callback response time 91
- isdn callback wait time 92
- isdn disconnect input time 94
- isdn disconnect interval time 95

- isdn disconnect output time 94
- isdn disconnect policy 92
- isdn disconnect time 92
- isdn fast disconnect time 93
- isdn forced disconnect time 93
- isdn local address 83
- isdn piafs arrive 84
- isdn piafs call 85
- isdn piafs control 84
- isdn remote address 86
- isdn remote call order 88
- isdn use 82

L

- l2tp keepalive log 217
- l2tp keepalive use 216
- l2tp service 215
- l2tp syslog 217
- l2tp tunnel auth 215
- l2tp tunnel disconnect time 216
- lan count-hub-overflow 59
- lan linkup send-wait-time 59
- lan shutdown 58
- lan type 60
- leased keepalive down 123
- less 35
- less config 522
- less config ap 522
- less config list 523
- less config pp 522
- less config switch 523
- less config tunnel 523
- less exec list 526
- less file list 524
- less log 547
- line type 82
- login password 39
- login password encrypted 39
- login radius use 40
- login timer 44
- login user 39
- lua 436
- lua use 436
- luac 437

M

- mail notify 369
- mail notify account exec 520
- mail notify status exec 520
- mail server name 366
- mail server pop 367
- mail server smtp 366
- mail server timeout 367
- mail template 368
- make directory 508
- mobile access limit connection length 421
- mobile access limit connection time 422
- mobile access limit duration 422
- mobile access limit length 418
- mobile access limit time 419
- mobile access-point name 417
- mobile arrive permit 423
- mobile arrive use 423
- mobile auto connect 416
- mobile call prohibit auth-error count 420
- mobile carrier mode 427
- mobile dial number 417
- mobile disconnect input time 416
- mobile disconnect output time 417
- mobile disconnect time 416

mobile display caller id 420
 mobile firmware update go 426
 mobile pin code 414
 mobile signal-strength 424
 mobile signal-strength go 424
 mobile syslog 421
 mobile use 413

N

nat descriptor address inner 253
 nat descriptor address outer 252
 nat descriptor ftp port 257
 nat descriptor log 257
 nat descriptor masquerade incoming 256
 nat descriptor masquerade port range 256
 nat descriptor masquerade remove df-bit 258
 nat descriptor masquerade rlogin 254
 nat descriptor masquerade session limit 258
 nat descriptor masquerade static 254
 nat descriptor masquerade unconvertible port 257
 nat descriptor sip 258
 nat descriptor static 253
 nat descriptor timer 255
 nat descriptor type 251
 netvolante-dns auto hostname 387
 netvolante-dns auto hostname pp 387
 netvolante-dns auto save 390
 netvolante-dns delete go 385
 netvolante-dns delete go pp 385
 netvolante-dns get hostname list 385
 netvolante-dns get hostname list pp 385
 netvolante-dns go 384
 netvolante-dns go pp 384
 netvolante-dns hostname host 386
 netvolante-dns hostname host pp 386
 netvolante-dns port 385
 netvolante-dns register timer 390
 netvolante-dns retry interval 389
 netvolante-dns retry interval pp 389
 netvolante-dns server 388
 netvolante-dns server update address port 389
 netvolante-dns server update address use 388
 netvolante-dns set hostname 388
 netvolante-dns sip use 387
 netvolante-dns sip use pp 387
 netvolante-dns timeout 386
 netvolante-dns timeout pp 386
 netvolante-dns use 384
 netvolante-dns use pp 384
 ngn radius account callee 229
 ngn radius account caller 228
 ngn radius auth password 228
 ngn renumbering link-refresh 229
 ngn type 364
 nslookup 516
 ntp backward-compatibility 49
 ntp local address 49
 ntpdate 48

O

onfs bind 442
 onfs mirroring contact node 451
 onfs mirroring go 452
 onfs mirroring id 450
 onfs mirroring pre-shared-key 452
 onfs mirroring use 450
 onfs reset 442
 onfs sharing acl 447
 onfs sharing group 446
 onfs sharing host 445

onfs sharing service 444
 onfs sharing user 445
 operation button function download 411
 operation execute batch permit 412
 operation external-memory download permit 406
 operation http revision-up permit 66

P

packetdump 56
 packetdump pp 56
 password reenter 44
 ping 513
 ping6 514
 pp always-on 86
 pp auth accept 136, 221
 pp auth multi connect prohibit 137
 pp auth myname 137
 pp auth request 136, 221
 pp auth username 135
 pp bind 83, 219, 415
 pp connect count threshold 97
 pp connect time threshold 97
 pp disable 510
 pp enable 510
 pp keepalive interval 121
 pp keepalive log 122
 pp keepalive use 121
 pp name 373
 pp select 499
 ppp ccp maxconfigure 146
 ppp ccp maxfailure 146
 ppp ccp maxterminate 145
 ppp ccp no-encryption 224
 ppp ccp restart 145
 ppp ccp type 145
 ppp chap maxchallenge 141
 ppp chap restart 141
 ppp ipcp ipaddress 142
 ppp ipcp maxconfigure 142
 ppp ipcp maxfailure 143
 ppp ipcp maxterminate 142
 ppp ipcp msexit 143
 ppp ipcp remote address check 144
 ppp ipcp restart 142
 ppp ipcp vjc 141
 ppp ipv6cp use 146
 ppp lcp accm 420
 ppp lcp acfc 137
 ppp lcp magicnumber 138
 ppp lcp maxconfigure 139
 ppp lcp maxfailure 140
 ppp lcp maxterminate 139
 ppp lcp mru 138
 ppp lcp pfc 139
 ppp lcp restart 139
 ppp lcp silent 140
 ppp mp control 147
 ppp mp divide 148
 ppp mp interleave 272
 ppp mp load threshold 147
 ppp mp maxlink 148
 ppp mp minlink 148
 ppp mp timer 148
 ppp mp use 147
 ppp msbcpc maxretry 144
 ppp msbcpc restart 144
 ppp pap maxauthreq 141
 ppp pap restart 140
 pppoe access concentrator 149
 pppoe auto connect 149
 pppoe auto disconnect 150

pppoe call prohibit auth-error count 152
 pppoe disconnect time 151
 pppoe invalid-session forced close 152
 pppoe padi maxretry 150
 pppoe padi restart 150
 pppoe padr maxretry 150
 pppoe padr restart 151
 pppoe service-name 151
 pppoe tcp mss limit 152
 pppoe use 149
 pptp hostname 220
 pptp keepalive interval 223
 pptp keepalive log 223
 pptp keepalive use 223
 pptp service 219
 pptp service type 220
 pptp syslog 222
 pptp tunnel disconnect time 222
 pptp vendorname 220
 pptp window size 221
 provider auto connect forced disable 381
 provider dns server 375
 provider dns server pp 376
 provider filter routing 376
 provider interface bind 383
 provider interface dns server 376
 provider interface name 377
 provider ipv6 connect pp 382
 provider isdn account nighttime 380
 provider isdn auto disconnect off 379
 provider isdn disconnect daytime 377
 provider isdn disconnect interval daytime 378
 provider isdn disconnect interval nighttime 379
 provider isdn disconnect nighttime 378
 provider netvolante-dns hostname sip 382
 provider ntp server 381
 provider ntpdate 380
 provider pp bind 382
 provider ppp mp use on 381
 provider select 375
 provider set 374
 provider type 374
 pstn dial type 333
 pstn hooking timer 334
 pstn modem signal timer 334
 pstn number display 334
 pstn pad receive 334
 pstn pad send 335
 pstn pause timer 335
 pstn ringing signal frequency 336
 pstn ringing signal threshold 337
 pstn supplementary-service 336
 pstn use 336

Q

queue class filter 269
 queue interface class filter list 273
 queue interface default class 274
 queue interface length 273
 queue interface type 271
 queue pp class filter list 273
 queue pp default class 274
 queue pp length 273
 queue pp type 271
 quit 500

R

radius account 247
 radius account port 249
 radius account server 248

radius auth 247
 radius auth port 249
 radius auth server 248
 radius retry 250
 radius secret 249
 radius server 248
 rdate 48
 remote setup 504
 remote setup accept 504
 rename 510
 restart 511
 rip filter rule 130
 rip preference 124
 rip timer 131
 rip use 123
 rotate external-memory syslog 520
 rtf format 81
 rtf garbage-collect 81

S

save 500
 schedule at 395
 scp 78
 sd use 402
 security class 44
 set 47
 set-acl 447
 sftpd host 63
 show account 547
 show account analog 548
 show account mobile 549
 show account ngn data 549
 show account ngn tel 549
 show account pp 547
 show account pstn 549
 show account sip 549
 show acl 449
 show arp 527
 show command 38
 show config 522
 show config analog extension 524
 show config ap 522
 show config list 523
 show config pp 522
 show config switch 523
 show config tunnel 523
 show copyright 546
 show dns cache 545
 show environment 522
 show exec list 526
 show file list 524
 show history 549
 show ip connection 532
 show ip connection pp 532
 show ip connection tunnel 532
 show ip intrusion detection 534
 show ip intrusion detection pp 534
 show ip intrusion detection tunnel 534
 show ip rip table 528
 show ip route 528
 show ip secure filter 526
 show ip secure filter pp 526
 show ip secure filter tunnel 526
 show ipsec sa 529
 show ipsec sa gateway 529
 show ipv6 address 524
 show ipv6 address pp 524
 show ipv6 address tunnel 524
 show ipv6 connection 533
 show ipv6 connection pp 533
 show ipv6 connection tunnel 533

show ipv6 mroute fib 537
show ipv6 neighbor cache 529
show ipv6 rip table 529
show ipv6 route 528
show log 547
show nat descriptor address 530
show nat descriptor interface address 530
show nat descriptor interface address pp 530
show nat descriptor interface address tunnel 530
show nat descriptor interface bind 530
show nat descriptor interface bind pp 530
show nat descriptor interface bind tunnel 530
show nat descriptor masquerade port summary 531
show pp connect time 534
show sshd public key 525
show ssl public key 526
show status 527
show status analog 542
show status analog extension 543
show status boot 543
show status boot all 543
show status boot list 543
show status cooperation 539
show status dhcp 531
show status dhcpc 532
show status external-memory 541
show status ip keepalive 534
show status ipv6 dhcp 532
show status ipv6 mld 537
show status isdn switch 545
show status l2tp 531
show status lua 437
show status mail service 536
show status mobile signal-strength 425
show status netvolante-dns 535
show status netvolante-dns pp 535
show status ngn 365
show status onfs 443
show status packet-buffer 538
show status pp 527
show status pptp 531
show status qos 539
show status remote setup 540
show status rtfs 541
show status sd 541
show status sip presence 542
show status sip server 542
show status status-led 545
show status switch control 544
show status switch control route backup 545
show status switching-hub macaddress 535
show status tunnel 536
show status upnp 535
show status usbhost 540
show status user 537
show status vlan 536
show status voice call 543
show status voice process 543
show techinfo 540
sip 100rel 345
sip arrive address check 348
sip arrive name-display default 346
sip arrive ringing p-n-uatype 347
sip arrive session timer method 347
sip arrive session timer refresher 346
sip codec permit 341
sip ip protocol 341
sip log 348
sip netvolante dial domain 343
sip netvolante dial figure 343
sip outer address 348
sip request retransmit timer 342
sip response code busy 346
sip server 349
sip server 100rel 352
sip server analog service 354
sip server arrive number display 353
sip server call mode 354
sip server call own permit 355
sip server call remote domain 351
sip server call server error 356
sip server connect 516
sip server dial number-only 355
sip server disconnect 516
sip server display name 350
sip server pilot address 356
sip server privacy 349
sip server qvalue 353
sip server register request-uri 352
sip server register timer 352
sip server session timer 351
sip session timer 344
sip use 341
sip user agent 345
snmp community read-only 232
snmp community read-write 232
snmp display ipcp force 242
snmp host 231
snmp ifindex switch static index 243
snmp local address 238
snmp syscontact 239
snmp syslocation 239
snmp sysname 239
snmp trap community 232
snmp trap enable snmp 240
snmp trap enable switch 244
snmp trap enable switch common 245
snmp trap host 232
snmp trap link-updown separate-l2switch-port 242
snmp trap mobile signal-strength 243
snmp trap send linkdown 240
snmp trap send linkdown pp 240
snmp trap send linkdown tunnel 240
snmp yrifppdisplayatmib2 241
snmp yrifswitchdisplayatmib2 242
snmp yriftunneldisplayatmib2 241
snmp yrswindex switch static index 244
snmpv2c community read-only 233
snmpv2c community read-write 234
snmpv2c host 233
snmpv2c trap community 234
snmpv2c trap host 234
snmpv3 context name 235
snmpv3 engine id 235
snmpv3 host 236
snmpv3 trap host 238
snmpv3 usm user 235
snmpv3 vacm access 237
snmpv3 vacm view 237
sntpd host 399
sntpd service 399
speed 269
ssh 79
ssh encrypt algorithm 79
ssh known hosts 80
sshd client alive 69
sshd encrypt algorithm 69
sshd hide openssl version 70
sshd host 67
sshd host key generate 68
sshd listen 67
sshd service 67
sshd session 68
ssl public key generate 520

switch control firmware upload go 456
switch control function default 456
switch control function execute 455
switch control function execute clear-counter 486
switch control function execute clear-macaddress-table 469
switch control function execute reset-loopdetect 490
switch control function execute restart 462
switch control function execute restart-poe-supply 493
switch control function execute start-poe-supply 493
switch control function execute stop-poe-supply 494
switch control function get 455
switch control function get boot-rom-version 458
switch control function get counter-frame-rx-type 481
switch control function get counter-frame-tx-type 483
switch control function get energy-saving 459
switch control function get firmware-revision 458
switch control function get lag-type 462
switch control function get led-brightness 460
switch control function get loopdetect-count 486
switch control function get loopdetect-linkdown 487
switch control function get loopdetect-port-use 488
switch control function get loopdetect-recovery-timer 488
switch control function get loopdetect-time 487
switch control function get loopdetect-use-control-packet 489
switch control function get macaddress-aging 468
switch control function get macaddress-aging-timer 468
switch control function get mirroring-dest 479
switch control function get mirroring-src-rx 480
switch control function get mirroring-src-tx 480
switch control function get mirroring-use 479
switch control function get model-name 459
switch control function get poe-class 490
switch control function get port-auto-crossover 464
switch control function get port-blocking-control-packet 465
switch control function get port-blocking-data-packet 466
switch control function get port-flow-control 465
switch control function get port-speed 463
switch control function get port-speed-downshift 464
switch control function get port-use 463
switch control function get qos-dscp-remark-class 475
switch control function get qos-dscp-remark-type 474
switch control function get qos-policing-speed 477
switch control function get qos-policing-use 476
switch control function get qos-shaping-speed 477
switch control function get qos-shaping-use 477
switch control function get qos-speed-unit 476
switch control function get serial-number 458
switch control function get status-combo-port 466
switch control function get status-counter-frame-rx 484
switch control function get status-counter-frame-tx 485
switch control function get status-counter-octet-rx 485
switch control function get status-counter-octet-tx 486
switch control function get status-fan 461
switch control function get status-fan-rpm 461
switch control function get status-led-mode 460
switch control function get status-loopdetect-port 489
switch control function get status-loopdetect-recovery-timer 490
switch control function get status-macaddress-addr 469
switch control function get status-macaddress-port 469
switch control function get status-poe-detect-class 491
switch control function get status-poe-state 491
switch control function get status-poe-supply 492
switch control function get status-poe-supply-detail 492
switch control function get status-poe-supply-total 493
switch control function get status-poe-temperature 492
switch control function get status-port-sfp-rx-power 467
switch control function get status-port-speed 467
switch control function get system-macaddress 459
switch control function get system-name 459
switch control function get system-uptime 462
switch control function get vlan-access 472
switch control function get vlan-id 471

switch control function get vlan-multiple 473
switch control function get vlan-multiple-use 473
switch control function get vlan-port-mode 471
switch control function get vlan-trunk 472
switch control function set 455
switch control function set counter-frame-rx-type 481
switch control function set counter-frame-tx-type 483
switch control function set energy-saving 459
switch control function set led-brightness 460
switch control function set loopdetect-count 486
switch control function set loopdetect-linkdown 487
switch control function set loopdetect-port-use 488
switch control function set loopdetect-recovery-timer 488
switch control function set loopdetect-time 487
switch control function set loopdetect-use-control-packet 489
switch control function set macaddress-aging 468
switch control function set macaddress-aging-timer 468
switch control function set mirroring-dest 479
switch control function set mirroring-src-rx 480
switch control function set mirroring-src-tx 480
switch control function set mirroring-use 479
switch control function set poe-class 490
switch control function set port-auto-crossover 464
switch control function set port-blocking-control-packet 465
switch control function set port-blocking-data-packet 466
switch control function set port-flow-control 465
switch control function set port-speed 463
switch control function set port-speed-downshift 464
switch control function set port-use 463
switch control function set qos-dscp-remark-class 475
switch control function set qos-dscp-remark-type 474
switch control function set qos-policing-speed 477
switch control function set qos-policing-use 476
switch control function set qos-shaping-speed 477
switch control function set qos-shaping-use 477
switch control function set qos-speed-unit 476
switch control function set system-name 459
switch control function set vlan-access 472
switch control function set vlan-id 471
switch control function set vlan-multiple 473
switch control function set vlan-multiple-use 473
switch control function set vlan-port-mode 471
switch control function set vlan-trunk 472
switch control route backup 457
switch control use 453
switch control watch interval 454
switch select 454
syslog debug 53
syslog execute command 53
syslog facility 52
syslog host 51
syslog info 52
syslog local address 53
syslog notice 52
syslog sreport 53
system led brightness 46
system packet-buffer 45

T

tcp log 54
tcp session limit 113
telnet 517
telnetd host 57
telnetd listen 57
telnetd service 57
telnetd session 58
terminate lua 438
terminate lua file 438
tftp host 62
time 48
timezone 47

- [traceroute](#) [515](#)
- [traceroute6](#) [515](#)
- [tunnel disable](#) [180](#)
- [tunnel enable](#) [180](#)
- [tunnel encapsulation](#) [181](#)
- [tunnel endpoint address](#) [182](#)
- [tunnel endpoint name](#) [182](#)
- [tunnel name](#) [373](#)
- [tunnel ngn arrive permit](#) [226](#)
- [tunnel ngn bandwidth](#) [225](#)
- [tunnel ngn call permit](#) [226](#)
- [tunnel ngn disconnect time](#) [225](#)
- [tunnel ngn fallback](#) [227](#)
- [tunnel ngn interface](#) [226](#)
- [tunnel ngn radius auth](#) [227](#)
- [tunnel select](#) [499](#)
- [tunnel template](#) [211](#)

U

- [upnp external address refer](#) [392](#)
- [upnp external address refer pp](#) [392](#)
- [upnp port mapping timer](#) [393](#)
- [upnp port mapping timer type](#) [392](#)
- [upnp syslog](#) [393](#)
- [upnp use](#) [392](#)
- [usbhost modem flow control](#) [426](#)
- [usbhost modem initialize](#) [425](#)
- [usbhost overcurrent duration](#) [402](#)
- [usbhost use](#) [401](#)
- [user attribute](#) [41](#)

V

- [vlan interface 802.1q](#) [398](#)

W

- [wan access limit connection length](#) [434](#)
- [wan access limit connection time](#) [434](#)
- [wan access limit duration](#) [435](#)
- [wan access limit length](#) [432](#)
- [wan access limit time](#) [433](#)
- [wan access-point name](#) [431](#)
- [wan always-on](#) [430](#)
- [wan auth myname](#) [428](#)
- [wan auto connect](#) [429](#)
- [wan bind](#) [428](#)
- [wan disconnect input time](#) [430](#)
- [wan disconnect output time](#) [430](#)
- [wan disconnect time](#) [429](#)
- [wins server](#) [143](#)
- [wol send](#) [518](#)

●ネットボランティア・コールセンター
TEL 03-5715-0350

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
<http://NetVolante.jp/>