YAMAHA

ヤマハルーター Web GUI

RTX1300 Rev.23.00.03

操作マニュアル

ヤマハルーターをお買い上げいただきありがとうございます。
Web GUIを使用する場合は、本書を参考にしてください。

JA

2022年7月 第1.0版

マニュアルのご案内

本書では、ウェブブラウザーを使用して本製品の設定や管理を行う方を対象として、本製品の Web GUI の使用方法を説明します。

弊社ではヤマハルーターの機能を十分に活用していただくために、さまざまなマニュアルを用意しています。
最新版のマニュアルは下記のヤマハネットワーク周辺機器技術情報ページに掲載してあります。
目的に合わせて適切なマニュアルをお読みください。

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

本製品をご使用中にトラブルが発生した場合は、以下の情報を参照して、問題を解決してください。
- 「コマンドリファレンス」（ウェブサイト）を参照して、設定コマンドの使用方法を確認してください。
- ヤマハネットワーク機器ホームページの設定例を参照して、設定を見直してください。
  https://network.yamaha.com/setting/
- ヤマハネットワーク機器技術情報ページで、障害の切り分け方法や設定事例集を参照して、設定を見直してください。
  http://www.rtpro.yamaha.co.jp/RT/docs/
- 設定を見直してもトラブルが解決しない場合は、「19.7 サポート窓口のご案内」（467 ページ）を参照して、弊社のサポート窓口までご連絡ください。

- **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。**
- **本書では、発行時点の最新仕様で説明をしております。本書の最新版につきましては、下記のウェブサイトからダウンロードしてお読みいただけますよう、お願いいたします。**
  http://www.rtpro.yamaha.co.jp/RT/manual.html
- **本製品を使用した結果により発生した情報の消失などの損失については、弊社ではいかなる責任も負いかねます。保証は本製品の物損の範囲に限ります。あらかじめご了承ください。**

本書の表記について

表記の意味
本書では、本製品を安全にお使いいただくため、以下のように表記します。

- **注意**
  製品の故障、損傷や誤動作、データの損失を防ぐためにお守りいただく内容です。
- **重要**
  製品を正しく操作、運用するために、必ず知っておいていただきたい内容です。
- **メモ**
  操作や運用に関連した情報です。参考にお読みください。

Web GUI の画面について
本書では、本書制作時点での Web GUI の画面を記載しています。実際の画面とは異なる場合があります。

例示用の IP アドレス / ドメイン名
本書では、グローバル IP アドレスやドメイン名を例示するとき、文書作成用途として RFC6890 / RFC6761 で予約されている IP アドレスとドメイン名の中から、以下に示す IP アドレス / ドメイン名を使用します。

IP アドレスの範囲：203.0.113.0/24
ドメイン名：example.net

これらの IP アドレス / ドメイン名は通信で使用することはできません。実際に設定するときは、ご利用環境に合わせたものをお使いください。

LAN ケーブル /LAN ポートについて
本製品には、LAN/SFP+ コンボポートが搭載されています。
ご利用の状況に応じて、文章中の記述を以下のように読み替えてください。
・ LAN ケーブル：以下のいずれか
　・SFP+/SFP モジュールと光ファイバーケーブル
　・ダイレクトアタッチケーブル
・ LAN ポート：SFP+ スロット

略称について
本書ではそれぞれの製品について、以下のように略称で記載しています。
・ Microsoft® Windows®：Windows
・ Microsoft® Windows® 8.1：Windows 8.1
・ Microsoft® Windows® 10：Windows 10
・ Microsoft® Windows® 11：Windows 11
・ 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T/5GBASE-T/10GBASE-T ケーブル：LAN ケーブル

商標について
・ Microsoft、Windows、Microsoft Edge は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
・ Google Chrome は、Google Inc. の登録商標です。
・ Mozilla、Firefox は、米国 Mozilla Foundation の米国およびその他の国における登録商標または商標です。
・ Apple、macOS、iPadOS、Safari は、米国および他の国々で登録された Apple Inc. の商標です。
・ JavaScript は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標または商標です。
・ フレッツは、東日本電信電話株式会社および西日本電信電話株式会社の登録商標です。
・「v6 プラス」は、日本ネットワークイネイブラー株式会社の登録商標です。
・ OCN バーチャルコネクトは、エヌ・ティ・ティ・コミュニケーションズ株式会社の登録商標です。
・ その他、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。

サービスについて
・ ひかり電話、データコネクトは、東日本電信電話株式会社および西日本電信電話株式会社が提供しているサービスの名称です。

目次

第 1 章　はじめに 10
1.1　Web GUI でできること 10
1.1.1　ダッシュボード 10
1.1.2　LAN マップ 10
1.1.3　かんたん設定 11
1.1.4　詳細設定 12
1.1.5　管理 12
1.1.6　CONFIG 13
1.1.7　SYSLOG 13
1.1.8　TECHINFO 14
1.1.9　ヘルプ 15
1.2　対応機器 / リビジョン 15
1.3　利用環境 15
1.3.1　推奨ウェブブラウザー 15
1.3.2　JavaScript の設定 15
1.4　ユーザーのアクセス権 16
1.5　一般ユーザーと管理ユーザー 16
1.5.1　一般ユーザーと管理ユーザーのできることの違いや画面表示の違いなど 16
1.5.2　一般ユーザーと管理ユーザーの切り換え方法 16
1.6　コマンド入力と併用する際の注意 17

第 2 章　Web GUI へログインする 18

第 3 章　基本設定を行う 20
3.1　日付と時刻を設定する 20
3.2　管理パスワードを設定する 22
3.3　LAN1 の IP アドレスを設定する 25

第 4 章　IPv4 アドレスでインターネットに接続する 28
4.1　ブロードバンド回線でインターネットに接続する 28
4.1.1　接続方法を確認する 29
4.1.2　「PPPoE 接続」の場合 31
4.1.3　「DHCP 接続」の場合 35
4.2　USB 接続型データ通信端末でインターネットに接続する 39

第 5 章　IPv6 アドレスでインターネットに接続する 46
5.1　フレッツ光（IPv6 IPoE）でインターネットに常時接続する 46
5.2　フレッツ光（IPv6 PPPoE）でインターネットに常時接続する 52

第 6 章　IPv4 over IPv6 トンネルでインターネットに接続する 58

第 7 章　ネットボランチ DNS サービスを利用する 65
7.1　ネットボランチ DNS サービスとは？ 65
7.2　ネットボランチ DNS サービスで取得できるホスト名 66
7.3　ネットボランチ DNS ホスト名を取得する 66
7.4　ネットボランチ DNS ホスト名の登録を解除する 69

第 8 章　拠点間を VPN で接続する 70
8.1　VPN の設定をする前に 71
8.2　IPsec で接続する 71
8.3　PPTP で接続する 78
8.4　IPIP で接続する 83
8.5　データコネクトで接続する 88

第 9 章　外部から VPN 経由で LAN へアクセスする 94
9.1　LAN 内のサーバーまたはパソコンの設定をする 95
9.2　L2TP/IPsec でリモートアクセスする 95
9.2.1　本製品の設定（L2TP/IPsec）をする 95
9.2.2　接続ユーザーを追加する 99
9.2.3　YMS-VPN8 の設定をする 101
9.2.4　YMS-VPN8 から本製品へリモートアクセスする 103
9.3　PPTP でリモートアクセスする 104
9.3.1　本製品の設定（PPTP）をする 104
9.3.2　接続ユーザーを追加する 108
9.3.3　Windows 8.1 でリモートアクセスする 110
9.3.4　Windows 10 / Windows 11 でリモートアクセスする 114

第 10 章 クラウドサービスと VPN で接続する 118

第 11 章 ダッシュボードを利用する 119
11.1 ダッシュボードとは？ 119
11.2 Live 画面の基本操作 120
11.2.1 ガジェットの追加または削除をする 120
11.2.2 ガジェットを移動する 121
11.2.3 ガジェットの画面を分離する 122
11.2.4 ガジェットを最小化する 123
11.2.5 ガジェットの位置情報を保存する 123
11.2.6 ガジェットを自動更新する 123
11.2.7 警告の内容を確認する 124
11.2.8 警告の履歴を表示する 126
11.3 Live 画面の各ガジェットの説明 127
11.3.1 システム情報 127
11.3.2 リソース情報 128
11.3.3 インターフェース情報 129
11.3.4 トラフィック情報（LAN/PP/TUNNEL） 131
11.3.5 プロバイダー接続状態 132
11.3.6 VPN 接続状態（拠点間） 133
11.3.7 VPN 接続状態（リモートアクセス） 133
11.3.8 YNO エージェント動作状態 133
11.3.9 NAT セッション数 134
11.3.10 ファストパスフロー数 134
11.3.11 動的フィルターセッション数 135
11.3.12 不正アクセス検知履歴 135
11.3.13 UTX セキュリティー 136
11.3.14 URL のキーワードチェック統計 136
11.3.15 SYSLOG 137
11.4 History 画面の基本操作 138
11.4.1 統計情報の記録を開始する 138

11.4.2 グラフの表示期間を変更する 141
11.4.3 ガジェットの追加または削除をする 143
11.4.4 ガジェットを移動する 144
11.4.5 ガジェットの表示内容を保存する 145
11.5 History 画面の各ガジェットの説明 145
11.5.1 CPU 使用率 146
11.5.2 メモリ使用率 146
11.5.3 トラフィック情報（LAN/PP/TUNNEL） 146
11.5.4 トラフィック情報（アプリケーション） 147
11.5.5 NAT セッション数 148
11.5.6 ファストパスフロー数 148
11.5.7 動的フィルターセッション数 148

第 12 章 LAN マップを利用する 149
12.1 LAN マップとは？ 149
12.2 LAN マップの画面構成 149
12.2.1 マップページ 150
12.2.2 タグ VLAN ページ 151
12.2.3 マルチプル VLAN ページ 152
12.3 LAN マップを有効にする 153
12.4 エージェントの状態を確認する 155
12.5 ネットワークの異常を監視する 157
12.5.1 エージェントの動作状況と異常を監視する 158
12.5.2 ネットワークの接続状態を監視する 158
12.5.3 ネットワークの異常をメールで通知する 160
12.6 機器を検索する 161
12.7 ヤマハスイッチを設定する 163
12.7.1 スイッチの設定・保守ダイアログを表示する 164
12.7.2 ヤマハスイッチの機器名を変更する 166
12.7.3 省電力機能を設定する 167
12.7.4 ループ検出機能を設定する 168
12.7.5 ポートミラーリング機能を設定する 170
12.7.6 フレームカウンタをリセットする 172
12.7.7 ファームウェアを更新する 173
12.7.8 ヤマハスイッチを再起動する 175
12.7.9 ヤマハスイッチを初期化する 176
12.7.10 ポートの設定ダイアログを表示する 177
12.7.11 ポートの基本機能を設定する 180
12.7.12 QoS 機能を設定する 182
12.7.13 フレームカウンタを設定する 183
12.7.14 LAN ケーブル二重化機能を設定する 184
12.7.15 スイッチの指定方法を選択する 187
12.8 ヤマハ無線 AP の設定を行う 190
12.8.1 IP アドレスを変更する 190
12.8.2 無線 AP の指定方法を選択する 193
12.8.3 設定（CONFIG）を保存する 196
12.8.4 設定（CONFIG）を復元する 198
12.8.5 無線 AP の設定画面を表示する 201
12.9 エージェントルーターの設定を行う 202
12.10 ヤマハ UTM アプライアンスの設定を行う 204
12.11 タグ VLAN を設定する 206

12.11.1 タグ VLAN ページを表示する 206
12.11.2 タグ VLAN グループを作成する 208
12.11.3 タグ VLAN グループに参加させる 209
12.11.4 タグ VLAN グループを削除する 211
12.11.5 タグ VLAN 間フィルターを設定する 212
12.12 マルチプル VLAN を設定する 213
12.12.1 マルチプル VLAN ページを表示する 214
12.12.2 マルチプル VLAN グループを設定する 215
12.12.3 マルチプル VLAN グループの参加ポートを確認する 217
12.13 接続機器の一覧を見る 218
12.13.1 端末一覧画面を表示する 218
12.13.2 端末の情報を編集する 219
12.13.3 端末情報 DB 画面を表示する 221
12.13.4 端末情報 DB に端末情報を新規登録する 222
12.13.5 端末情報 DB に登録されている端末情報を編集する 224
12.13.6 端末情報 DB ファイルをパソコンへエクスポートする 225
12.13.7 端末情報 DB ファイルをパソコンからインポートする 227
12.13.8 エージェント一覧画面を表示する 228
12.13.9 エージェントの機器名を変更する 230
12.13.10 一覧マップで表示する 231
12.13.11 一覧マップを印刷する 233

第 13 章 セキュリティーを強化する 235

13.1 不正アクセスとは？ 235
13.1.1 グローバル IP アドレスが割り当てられている場合 236
13.1.2 パスワードを設定していない場合 236
13.2 不正アクセスに対抗する 236
13.2.1 インターネット側から内部の LAN への侵入 236
13.2.2 OS やサーバーソフトウェアのセキュリティーホールからの侵入 236
13.2.3 電子メールの添付ファイルからの侵入 237
13.3 不正アクセス検知を有効にする 237
13.3.1 不正アクセス検知を設定する 237
13.3.2 不正アクセス検知履歴の並び替え / 検索 / 削除をする 240
13.4 IP フィルターを設定する 242
13.4.1 本製品のフィルターの特徴 243
13.4.2 フィルター設定の基本 243
13.4.3 PING を許可する相手を限定する 244
13.4.4 遠隔からの PING をすべて破棄する 247
13.4.5 特定の端末だけ Web アクセスを許可する 252
13.5 URL フィルターを設定する 257
13.5.1 特定のキーワードを含む URL へのアクセスを禁止する 257
13.5.2 端末ごとにアクセスを許可する URL を変更する 264
13.5.3 アクセスを禁止するキーワードの例外条件を設定する 271
13.5.4 監視するポート番号を増やす 284
13.5.5 拒否リストの統計情報の並び替え / 検索 / 削除をする 286
13.6 本製品へのアクセスを管理する 288
13.6.1 本製品へのアクセスを制限する 289
13.6.2 ログインを許可するユーザーを登録する 296
13.6.3 ユーザーごとにアクセス方法を制限する 298
13.6.4 ユーザーのパスワードを変更する 301

第 14 章 詳細設定を行う 305
14.1 プロバイダーの詳細設定を行う 305
14.1.1 WAN 回線の MTU を設定する 305
14.1.2 宛先ネットワークを設定する 308
14.1.3 自動切断の設定を行う 310
14.1.4 発信制限をかける 312
14.1.5 キープアライブ設定を変更する 315
14.2 LAN のアドレスを設定する 318
14.2.1 プライマリー IP アドレスを設定する 318
14.2.2 セカンダリー IP アドレスを設定する 320
14.2.3 固定ではなく DHCP で設定する 323
14.3 ポートの動作モードを設定する 325
14.4 フレキシブル LAN/WAN ポートを設定する 327
14.5 グローバル IP アドレスを複数の端末でシェアする 330
14.6 外部にサーバーを公開する 335
14.6.1 ポートを開放する 336
14.6.2 サーバーの公開先を限定する 339
14.7 複数のプロバイダーを使用する 343
14.7.1 複数のプロバイダーを設定する 343
14.7.2 端末ごとにプロバイダーを使い分ける 344
14.7.3 バックアップ回線を用意する 354
14.7.4 マルチホーミングによる負荷分散を行う 359
14.8 DNS サーバーを設定する 365
14.8.1 DNS サーバー機能の基本設定を行う 365
14.8.2 中継先 DNS サーバーを設定する 367
14.8.3 中継先 DNS サーバーを問い合わせ内容に応じて設定する 372
14.8.4 特定の DNS 問い合わせパケットを中継せず破棄する 375
14.9 DNS サーバー機能にアクセスできるホストの設定を変更する 377
14.10 DHCP で端末に IP アドレスを割り当てる 380
14.11 異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる 384
14.12 メール通知機能を使う 386
14.12.1 メールサーバーを設定する 386
14.12.2 メール通知を設定する 388
14.12.3 本製品の内部状態をメールで通知する 391

第 15 章 本製品を管理する 393
15.1 本製品の日時を合わせる 393
15.1.1 日付と時刻を設定する 393
15.1.2 NTP サーバーと今すぐ同期する 395
15.2 ブザーを設定する 395
15.3 DOWNLOAD ボタンに機能を割り当てる 397
15.3.1 ネットワーク経由でファームウェアを更新する 397
15.3.2 USB 接続型データ通信端末の電波受信レベルを取得する 400
15.4 SYSLOG を外部メモリーへ保存する 402
15.5 外部メモリー内のファイルを用いて起動する 405
15.6 外部メモリー内のファイルをインポートする 408
15.7 コマンドを実行する 411
15.8 ファームウェアを更新する 414
15.8.1 外部メモリーを使用してファームウェアを更新する 414
15.8.2 パソコンからファームウェアを更新する 417

15.8.3 ヤマハのウェブサイトからネットワーク経由でファームウェアを更新する 420
15.8.4 社内サーバーからネットワーク経由でファームウェアを更新する 423
15.9 設定（CONFIG）を管理する 426
15.9.1 設定（CONFIG）をパソコンにエクスポートする 427
15.9.2 設定（CONFIG）をパソコンからインポートする 429
15.9.3 設定（CONFIG）を外部メモリーにエクスポートする 432
15.9.4 設定（CONFIG）を外部メモリーからインポートする 434
15.10 SYSLOG を管理する 437
15.10.1 SYSLOG に出力する種別を変更する 437
15.10.2 SYSLOG をサーバーへ送信する 440
15.11 本製品を再起動する 442
15.12 本製品を工場出荷時の状態へ戻す 444

第 16 章 アプリケーション制御（DPI）を利用する 447
16.1 アプリケーション制御とは？ 447
16.2 アプリケーション制御を有効にする 448

第 17 章 YNO（統合管理サービス）を利用する 453
17.1 YNO とは？ 453
17.2 YNO エージェント機能を有効にする 453

第 18 章 独自の GUI を作成する（カスタム GUI） 456

第 19 章 困ったときは 457
19.1 Web GUI で設定できない 457
19.2 インターネットに接続できない 458
19.3 VPN 通信できない 459
19.4 LAN マップに関する問題 462
19.4.1 LAN マップが使用できない 462
19.4.2 エージェントが正しく表示されない 462
19.4.3 端末が正しく表示されない 464
19.4.4 スナップショット機能が動作しない 464
19.4.5 タグ VLAN 間の通信を制限できない 465
19.4.6 ウェブブラウザーが操作できない 466
19.4.7 エージェントの Web GUI にアクセスできない 466
19.5 その他の問題 466
19.6 パスワードを忘れてしまった場合は 467
19.7 サポート窓口のご案内 467

第 20 章 付録 468
20.1 パソコンの IP アドレスを変更する 468
20.1.1 Windows 8.1 の場合 468
20.1.2 Windows 10 / Windows 11 の場合 469
20.2 本製品を譲渡 / 廃棄する際のご注意 470

第 1 章　はじめに

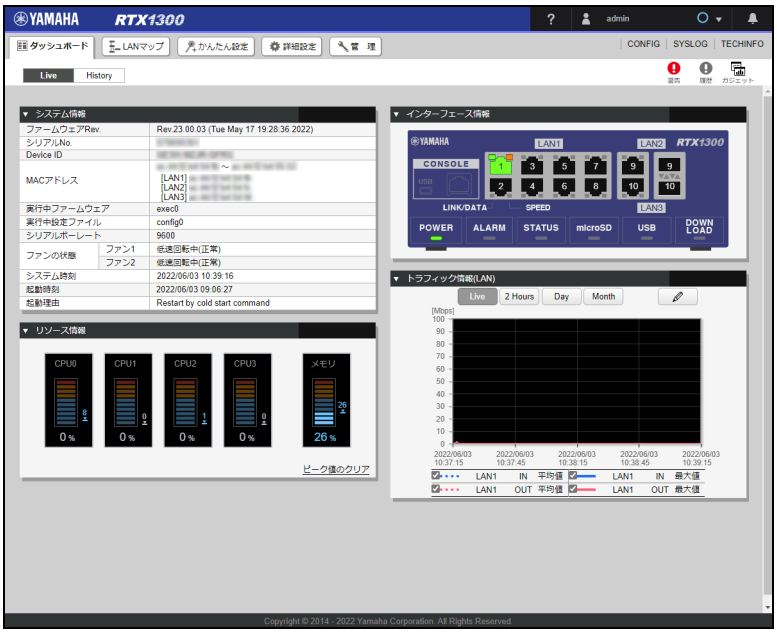
本章では、Web GUI の概要とお使いいただくために必要な事項を説明します。

1.1　Web GUI でできること

本製品は Web GUI を搭載しており、パソコンのウェブブラウザーを使って基本的な設定を行うことができます。また、設定だけでなく管理に便利な画面も搭載しています。Web GUI の画面構成について次節から説明します。

1.1.1 ダッシュボード

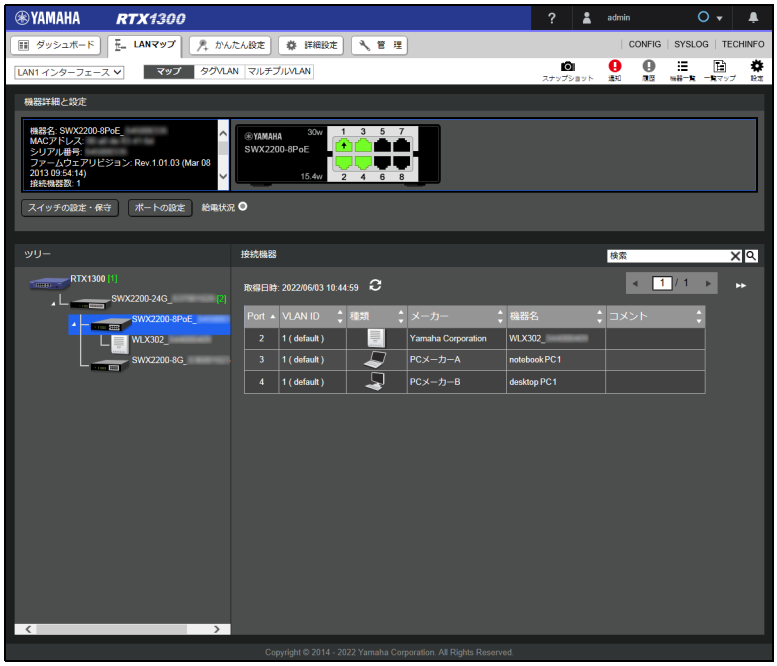
ダッシュボードページでは、各種システム情報やステータス情報を可視化、監視することができます。監視対象の各種パラメータが閾値以上の値になると警告メッセージが表示されるため、障害発生時の原因解析やトラブルシュートにも利用できます。



1.1.2 LAN マップ

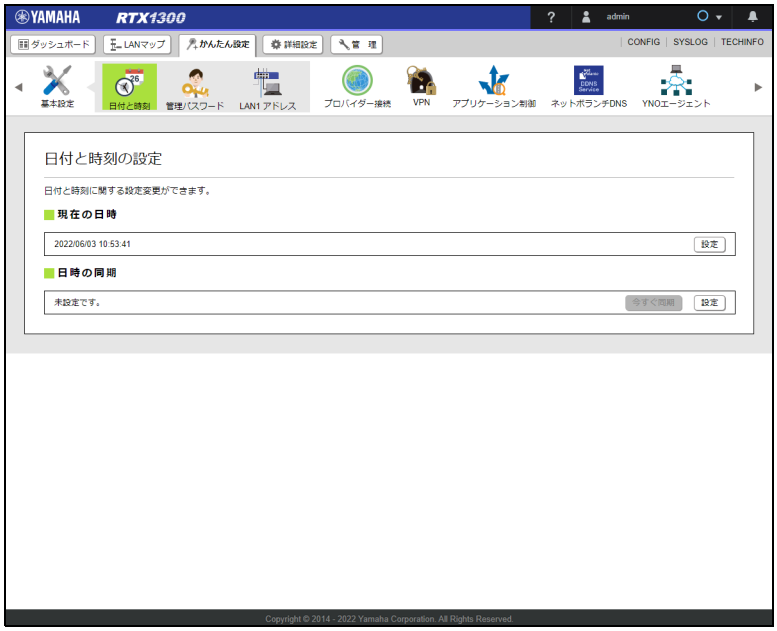
LAN マップページでは、LAN に接続されているヤマハネットワーク機器や通信端末の情報が表示され、LAN のネットワーク構成を確認することができます。また、ヤマハネットワーク機器の設定や VLAN の設定などを行うことができます。

ネットワークの異常も一目で把握することができるため、障害発生時の原因解析やトラブルシュートにも利用できます。



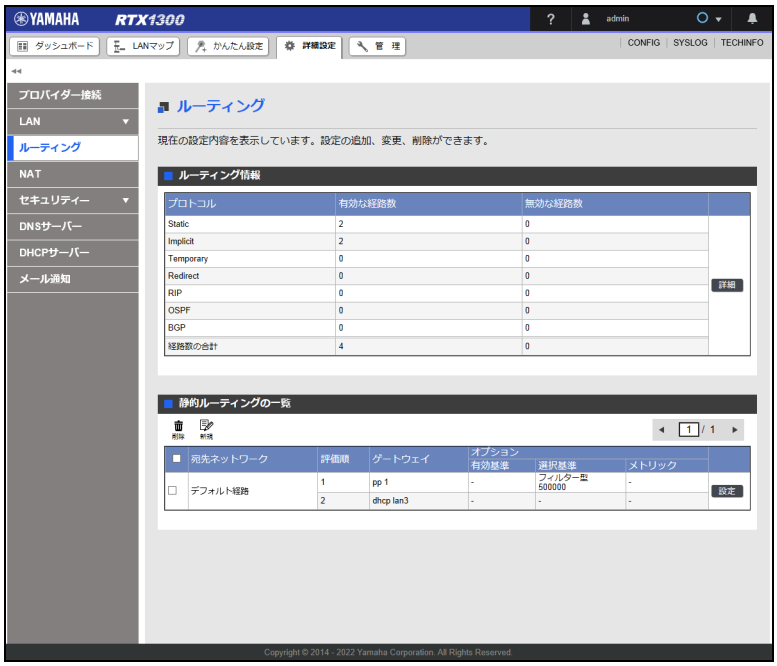
1.1.3 かんたん設定

かんたん設定ページでは、本製品の日付や時刻、管理パスワードなどのルーター本体に関する設定に加えて、インターネットに接続するための設定や VPN の設定、ネットボランチ DNS の設定を行うことができます。ウィザード形式で設定できるため、専門知識がなくてもかんたんに設定することができます。



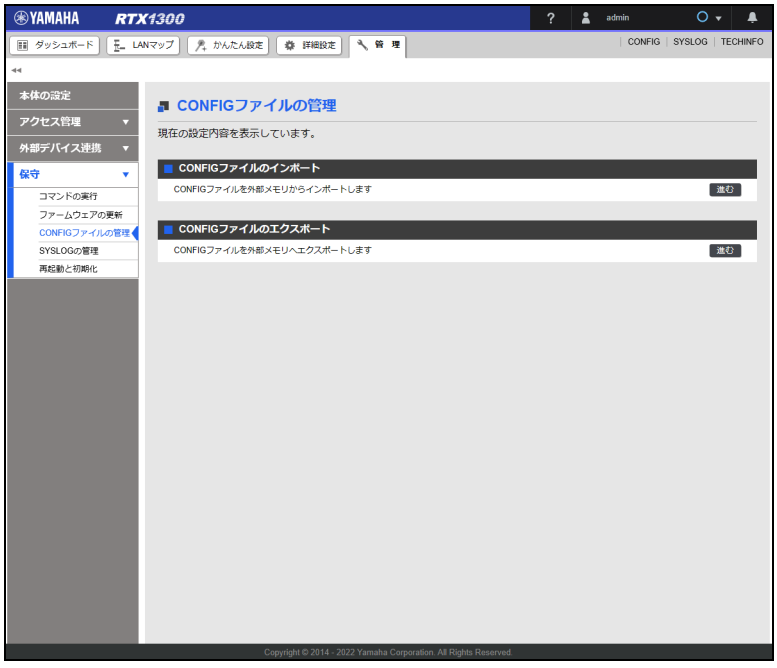
1.1.4 詳細設定

詳細設定ページでは、本製品の NAT や IP フィルターなどの、ネットワークに関する詳細な設定を行うことができます。



1.1.5 管理

管理ページでは、本製品のファームウェアの更新や CONFIG ファイルの管理、本体にアクセスするユーザーやパスワードの設定を行うことができます。

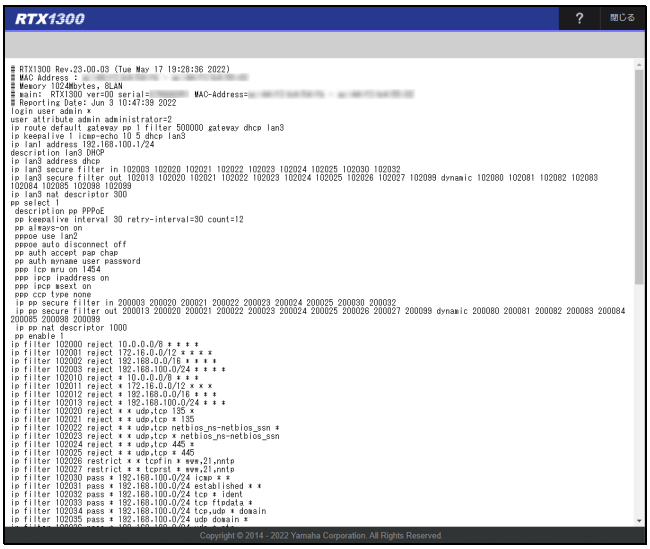


1.1.6 CONFIG

CONFIG ページでは、本製品の設定（CONFIG）をウェブブラウザーで表示したり、テキストファイルとして取得したりできます。

本製品は CONFIG に従って動作しています。CONFIG は複数のコマンドで構成されており、Web GUI から設定した内容もすべてコマンド形式で CONFIG に保存されます。

CONFIG ページをウェブブラウザーで表示するには、画面右上の「CONFIG」ボタンをクリックし、「ブラウザで表示」を選択します。



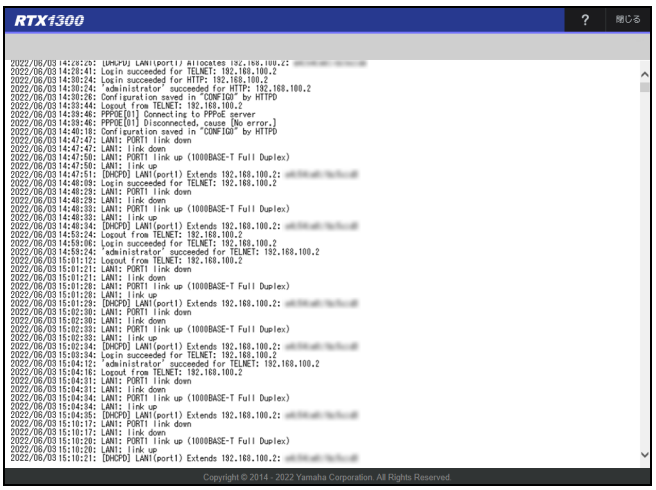
メモ

テキストファイルで取得するには、画面右上の「CONFIG」ボタンをクリックし、「テキストファイルで取得」を選択します。取得したテキストファイルは UTF-8 でエンコードされています。

1.1.7 SYSLOG

SYSLOG ページでは、本製品の内部ログ（show log コマンドの実行結果）をウェブブラウザーで表示したり、テキストファイルとして取得したりできます。

SYSLOG ページをウェブブラウザーで表示するには、画面右上の「SYSLOG」ボタンをクリックし、「ブラウザで表示」を選択します。



メモ

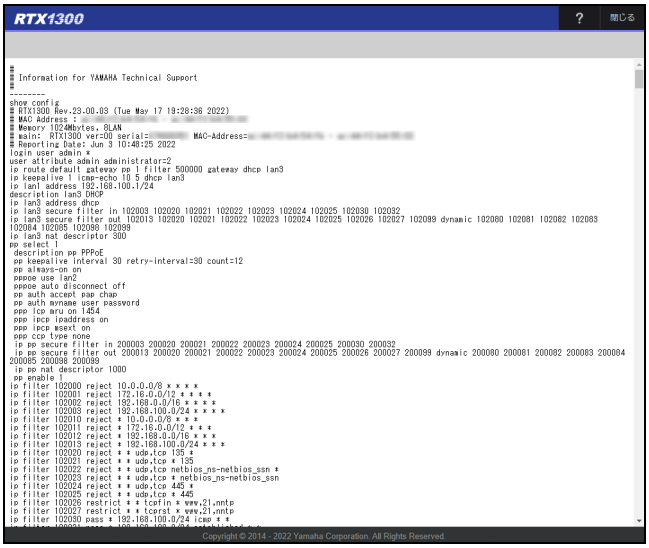
テキストファイルで取得するには、画面右上の「SYSLOG」ボタンをクリックし、「テキストファイルで取得」を選択します。取得したテキストファイルは UTF-8 でエンコードされています。

1.1.8 TECHINFO

TECHINFO ページでは、現在の本製品の設定や動作状態をウェブブラウザーで表示したり、テキストファイルとして取得したりできます。

お問い合わせ時に本製品の状態を把握するために、設定や動作状態を確認させていただくことがあります。

TECHINFO ページをウェブブラウザーで表示するには、画面右上の「TECHINFO」ボタンをクリックし、「ブラウザで表示」を選択します。



メモ

テキストファイルで取得するには、画面右上の「TECHINFO」ボタンをクリックし、「テキストファイルで取得」を選択します。取得したテキストファイルは UTF-8 でエンコードされています。

1.1.9 ヘルプ

ヘルプページでは、Web GUI の各設定画面の設定項目について、詳しい説明が記載されています。
ヘルプページを表示するには、画面右上の「?」ボタンをクリックしてください。

1.2 対応機器 / リビジョン

本書は下記のヤマハネットワーク機器に対応しています。

対応機器	リビジョン
RTX1300	Rev.23.00.01

1.3 利用環境

Web GUI を利用するための環境について説明します。

1.3.1 推奨ウェブブラウザー

推奨ウェブブラウザーについては、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/FAQ/gui/browser.html

メモ

・ ウェブブラウザーの「戻る」、「進む」ボタンは使用しないでください。使用すると意図しない動作につながることがあります。
・ Web GUI の文字エンコードは UTF-8 です。

1.3.2 JavaScript の設定

Web GUI では JavaScript を利用しています。お使いのウェブブラウザーで JavaScript が無効になっていると、Web GUI が利用できない場合があります。JavaScript が無効になっている場合は、各ウェブブラウザーの設定手順にしたがって JavaScript を有効にしてからご利用ください。

1.4 ユーザーのアクセス権

Web GUI にログインするユーザーは、一般ユーザーと管理ユーザーの 2 つに分類されます。これをアクセスレベルと呼びます。
アクセスレベルの違いは、以下のとおりです。

アクセスレベル	説明
一般ユーザー	本製品の設定内容や通信ログを参照できます。設定の変更はできません。
管理ユーザー	本製品の設定を行えます。また、設定内容や通信ログを参照できます。

メモ
- ユーザーに設定された権限によって一般ユーザーまたは管理ユーザーでログインします。
- 管理パスワードの設定は、「3.2 管理パスワードを設定する」（22 ページ）をご覧ください。
- ユーザー登録の設定は、「13.6.2 ログインを許可するユーザーを登録する」（296 ページ）をご覧ください。

1.5 一般ユーザーと管理ユーザー

本節では、一般ユーザー、管理ユーザーのログイン仕様について説明します。

1.5.1 一般ユーザーと管理ユーザーのできることの違いや画面表示の違いなど

一般ユーザーとしてログインした場合：
本製品の設定内容や動作状態を確認できます。ただし、本製品の設定変更や初期化、再起動、ファームウェアの更新などの操作は行えません。これらの操作に関連するボタンはすべてグレーアウトされ、クリックすることができないようになっています。

管理ユーザーとしてログインした場合：
Web GUI のすべての操作が可能となります。本製品の設定内容や動作状態の確認だけでなく、本製品の設定変更や初期化、再起動、ファームウェアの更新など、すべての操作を行うことができます。

1.5.2 一般ユーザーと管理ユーザーの切り換え方法

現在ログインしているアクセス権を切り替えるには、一度ログアウトした後に、切り替えたいアクセス権でログインしなおす必要があります。一般ユーザーから管理ユーザーに切り替える手順を例に説明します。

1. **画面右上に表示されているユーザー名をクリックします。**
2. **表示された「ログアウト」ボタンをクリックし、ログアウトします。**
3. **ウェブブラウザーをいったん終了し、再度ウェブブラウザーを起動します。**
4. **本製品の Web GUI にアクセスし、ユーザー名とパスワードを入力する画面で、管理ユーザーの権限を持ったユーザーのユーザー名とパスワードを入力します。**

メモ
- 現在ログインしているユーザー名は、常に画面右上に表示されています。
- アクセス権の情報は、画面右上のユーザー名をクリックすると表示されます。

1.6 コマンド入力と併用する際の注意

本製品は Web GUI による設定だけでなく、コマンドコンソール画面で直接コマンドを入力して設定することもできます。コマンド入力による設定では、Web GUI よりも多様な設定ができたり、Web GUI ではサポートしていない機能の設定を行ったりすることができます。ただし、コマンド入力による設定の後で Web GUI から設定を変更すると、入力したコマンドが消えたり、コマンドの一部が書き換わったりすることがあります。コマンド入力と Web GUI を併用する際は、必ず画面右上の「CONFIG」ボタンから CONFIG を閲覧し、入力したコマンドが書き換わっていないことを確認してください。

メモ

Web GUI にもコマンドコンソール画面があり、そこからコマンド入力を行った場合も同様です。Web GUI のコマンドコンソール画面を表示するには、「管理」タブ ―「保守」―「コマンドの実行」を順に選択してください。また、コマンドの詳細については「コマンドリファレンス」（ウェブサイト）をご覧ください。

第 2 章　Web GUI へログインする

本章では、Web GUI へのログイン方法を説明します。Web GUI にログインするには、本製品に接続するためのパソコンとウェブブラウザーが必要です。

1. **本製品の LAN1 ポートとパソコンを LAN ケーブルで接続する。**
2. **パソコンでウェブブラウザーを起動する。**
3. **アドレスバーに「http://(本製品に設定した IP アドレス)/」と半角英数字で入力してから、Enter キーを押す。**

   ユーザー名とパスワードを入力する画面が表示されます。

メモ

工場出荷状態では本製品の LAN1 ポートの IP アドレスは「192.168.100.1」に設定されているため、アドレスバーに「http://192.168.100.1/」と入力します。

4. **設定したユーザー名とパスワードを「ユーザー名」、「パスワード」に入力し、「OK」ボタンをクリックする。**

管理ユーザーとしてログインする場合は、管理ユーザーの権限を持ったユーザーのユーザー名とパスワード、一般ユーザーとしてログインする場合は、一般ユーザーの権限を持ったユーザーのユーザー名とパスワードを入力してください。

メモ

- 工場出荷状態では、初期管理ユーザー（ユーザー名「admin」、パスワード「admin」）が設定されています。ユーザー名とパスワードに「admin」を入力してください。
- 管理者権限を持つユーザーの設定がない状態で本製品を起動した場合は、初期管理ユーザーが追加されます。
- ユーザーのアクセス権については、「1.4 ユーザーのアクセス権」（16 ページ）をご覧ください。

工場出荷状態の本製品の Web GUI にログインする場合

5. 新しいパスワードを入力して、「保存」ボタンをクリックする。

メモ

初期管理ユーザーのパスワード「admin」を変更するまで、Web GUI にログインすることはできません。

6. ダッシュボードページ上に「データ蓄積の設定」ダイアログが表示された場合は、「OK」ボタンをクリックする。

メモ

工場出荷状態からの初回ログイン時のみ「データ蓄積の設定」ダイアログが表示されます。

パスワードについて

- パスワードは必ず半角の英数字で入力してください。全角文字は使用できません。また大文字 / 小文字の違いも区別します。
- 誤ったユーザー名 / パスワードがウェブブラウザーに記憶されていると、ユーザー名とパスワードを入力する画面が表示されないことがあります。ウェブブラウザーをいったん終了させてから、もう一度 Web GUI にアクセスしてください。なお、自動ログイン用のユーザー情報を登録している場合は削除してください。
- 設定したパスワードは忘れないようにしてください。万が一パスワードを忘れてしまった場合は、本製品の設定を行った管理者に、正しいパスワードをお問い合わせください。

ログアウトのしかた

画面右上のユーザー名をクリックすると表示される「ログアウト」ボタンをクリックしてください。また、他のユーザーでログインしなおす場合は、ログアウト後にウェブブラウザーをいったん終了させてから再度、本章の手順に従ってログインしてください。

自動ログアウト機能について

Web GUI の安全な利用のため、一定の時間操作が確認できなかった場合、自動ログアウト機能が作動します。自動ログアウト機能の作動前および作動後には、それぞれ以下のダイアログが表示されます。

- 「もうすぐ自動ログアウト」ダイアログ
  自動ログアウト機能の作動前になると「もうすぐ自動ログアウト」ダイアログが表示されます。
  Web GUI を引き続き利用する場合は「OK」ボタンを押して、自動ログアウトまでの時間を延長してください。
- 「自動ログアウト」ダイアログ
  自動ログアウト機能の作動後には、「自動ログアウト」ダイアログが表示されます。
  同一ユーザーで再度 Web GUI にログインする場合は、「OK」ボタンを押した後、画面右上の「ログイン」ボタンを押して、ログインしなおしてください。他のユーザーでログインする場合は、ウェブブラウザーをいったん終了させてから、もう一度 Web GUI にアクセスしてください。ログイン操作の詳細は「Web GUI へログインする」（18 ページ）をご覧ください。

第 3 章　基本設定を行う

本章では、本製品の基本設定について説明します。

・ 日付と時刻を設定する …20 ページ
・ 管理パスワードを設定する …22 ページ
・ LAN1 の IP アドレスを設定する …25 ページ

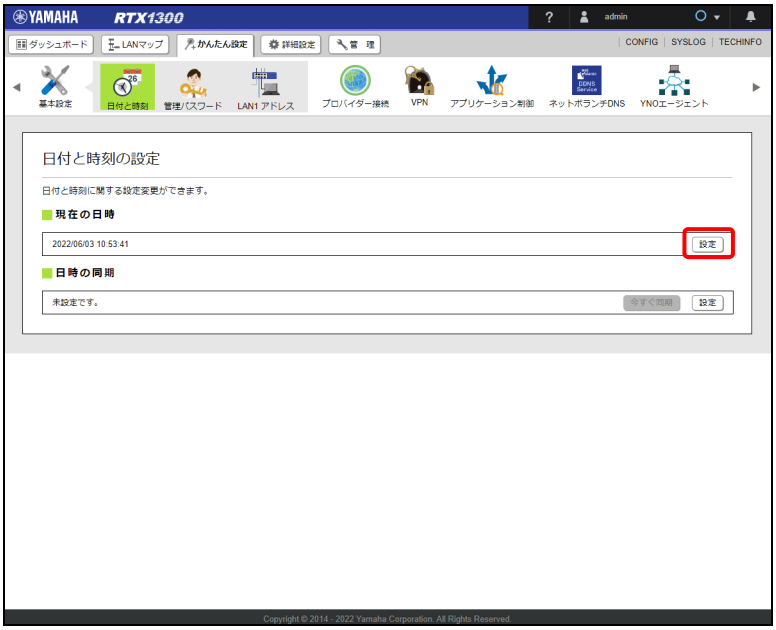
3.1　日付と時刻を設定する

本製品の日付と時刻を合わせます。

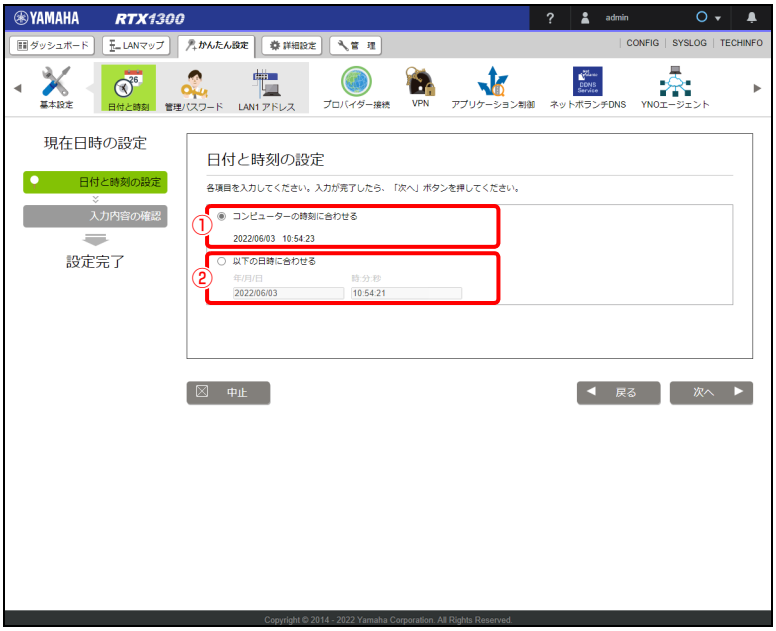
メモ

「日時の同期」については、「15.1 本製品の日時を合わせる」（393 ページ）をご覧ください。

1. **「かんたん設定」タブ ―「基本設定」―「日付と時刻」ボタンを順に選択する。**
   「日付と時刻の設定」画面が表示されます。
2. **「現在の日時」項目の「設定」ボタンをクリックする。**



3. **日時を設定する。**



① コンピューターの時刻に合わせる：
現在お使いのコンピューターに設定されている時刻と、同じ時刻を設定します。

② 以下の日時に合わせる：
設定する日時を入力します。

- 「年 / 月 / 日」：日付を YYYY/MM/DD 形式で入力します。「年 / 月 / 日」欄にフォーカスを合わせるとカレンダーが表示され、カレンダーから日付を選択することもできます。
- 「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にフォーカスを合わせると時刻のリストが表示され、リストから時刻を選択することもできます。

4. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**

設定が変更され、「日付と時刻の設定」画面が表示されます。

3.2　管理パスワードを設定する

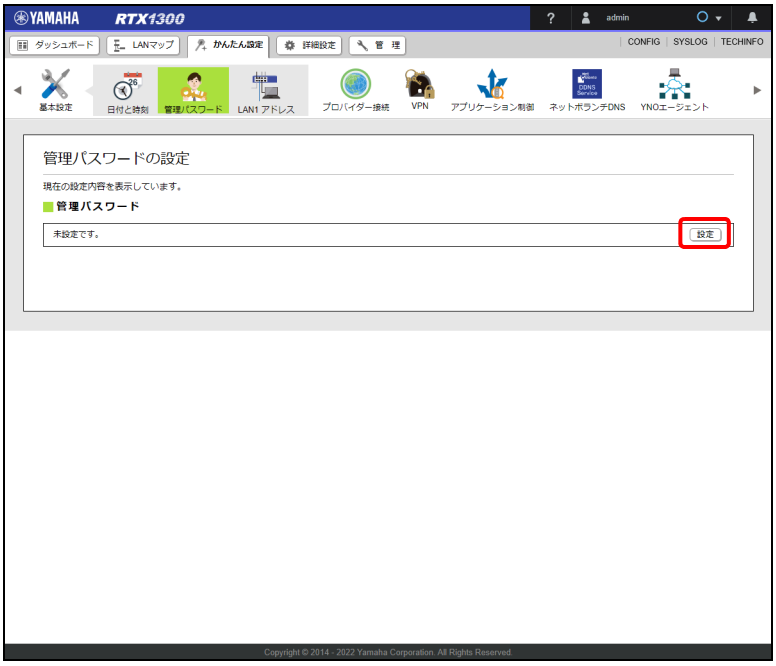
本製品の管理パスワードを変更することができます。工場出荷状態では本製品の管理パスワードは設定されていません。セキュリティー対策を行う上でも、パスワードを設定することをおすすめします。

メモ

- 管理パスワードを設定すると、第三者がシリアルコンソール画面から本製品の設定を変更することが困難になります。
- 各ユーザーのパスワードの設定方法については、「13.6 本製品へのアクセスを管理する」（288 ページ）をご覧ください。

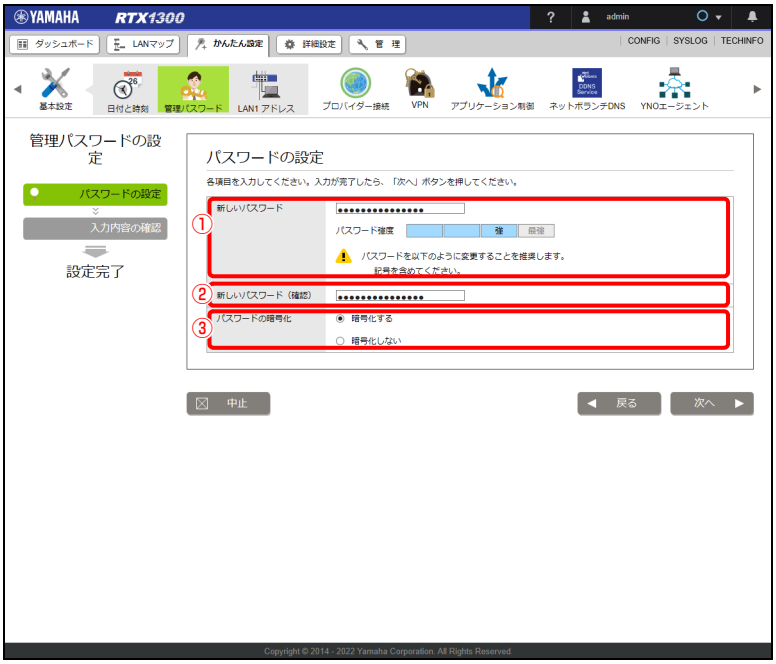
1. **「かんたん設定」タブ ―「基本設定」―「管理パスワード」ボタンを順に選択する。**
「管理パスワードの設定」画面が表示されます。

2.「管理パスワード」項目の「設定」ボタンをクリックする。



「パスワードの設定」画面が表示されます。

3. 管理パスワードを設定する。



① 新しいパスワード：
新しい管理パスワードを入力します。入力したパスワードは、●で表示されます。

② 新しいパスワード（確認）：
新しい管理パスワードを再入力します。入力したパスワードは、●で表示されます。

③ パスワードの暗号化：
管理パスワードを暗号化して保存するか選択します。暗号化せずに保存すると、パスワードは平文で保存されます。 すでに設定済みのパスワードに対して、暗号化の有無のみを変更したい場合は、設定済みのパスワードを再入力してください。

4. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**

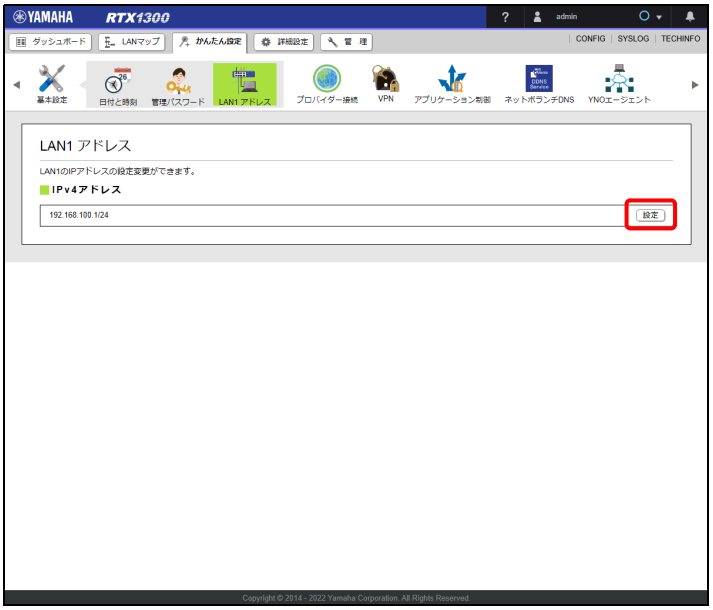
設定が変更され、「管理パスワードの設定」画面が表示されます。

3.3 LAN1 の IP アドレスを設定する

本製品の LAN1 の IP アドレスを変更することができます。すでに異なるネットワークアドレスが設定されているネットワークに設置する場合は、そのネットワークアドレスに応じた IP アドレスとネットマスクを本製品に設定してください。また、本製品には、LAN 内にすでに設置されている他の機器の IP アドレスと重複しない IP アドレスを設定してください。

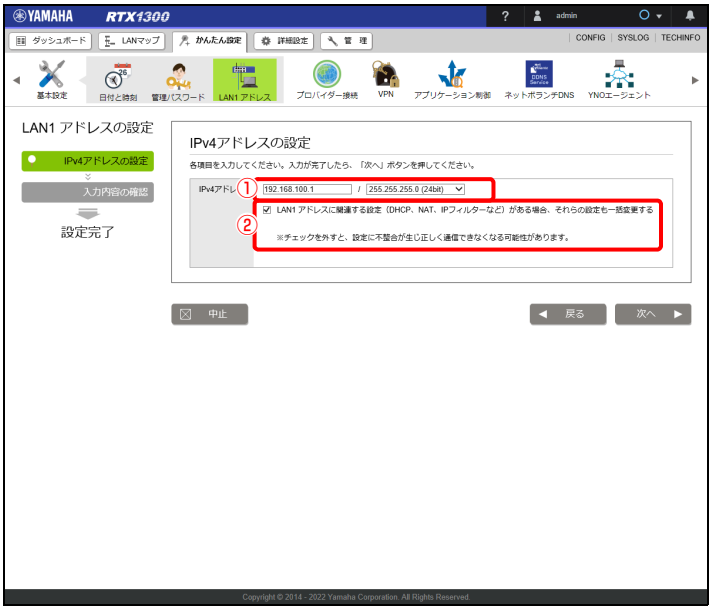
1. **「かんたん設定」タブ ―「基本設定」―「LAN1 アドレス」ボタンを順に選択する。**
   「LAN1 アドレス」画面が表示されます。

2. **「IPv4 アドレス」項目の「設定」ボタンをクリックする。**



「IPv4 アドレスの設定」画面が表示されます。

3. **LAN1 の IP アドレスを設定する。**



① アドレス入力欄：
新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0 (2bit)」から「255.255.255.252 (30bit)」までの中から選択します。

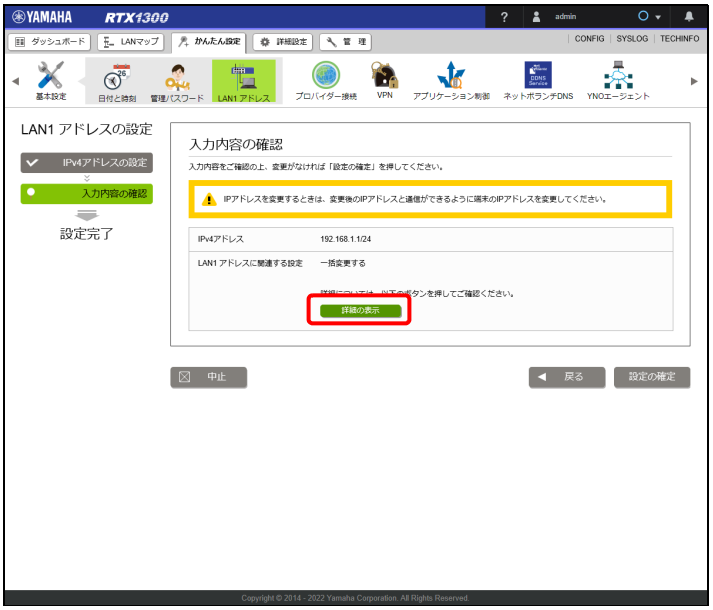
② LAN1 アドレスに関連する設定（DHCP、NAT、IP フィルターなど）がある場合、それらの設定も一括変更する：
選択すると、LAN1 インターフェースの IP アドレスの設定変更に合わせて、各種設定の IP アドレスの設定が自動的に変更されます。対象となる設定は以下のとおりです。

- DHCP で払い出す IP アドレス
- 静的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- 動的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的 NAT（内側アドレス）
- NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）
- NAT ディスクリプター静的 IP マスカレード（内側アドレス）
- IP キープアライブ（始点 IP アドレス）
- トンネルインターフェース端点 IP アドレス（ローカル IP アドレス）
- IPsec 自分側 IP アドレス

選択しないときは、LAN1 インターフェースの IP アドレスのみ変更されます。

注意
選択しないで設定した場合、設定の不整合により通信できなくなる可能性があります。

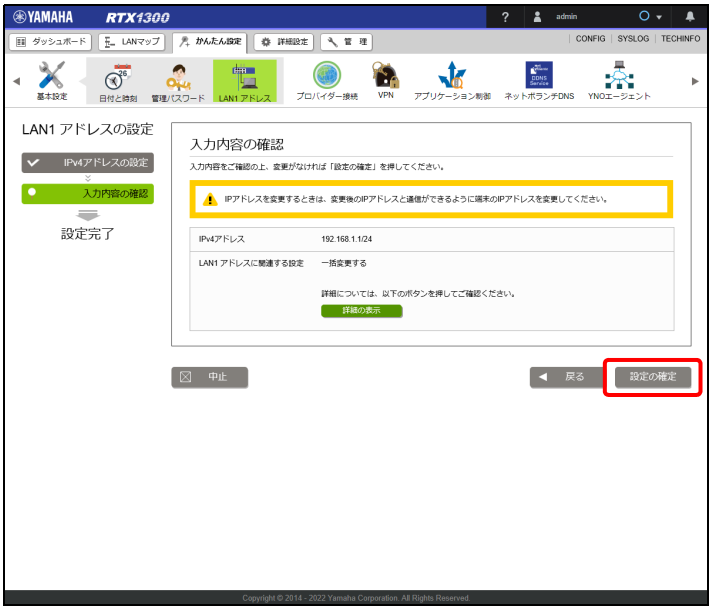
4.「次へ」ボタンをクリックする。
「入力内容の確認」画面が表示されます。表示画面の「詳細の表示」ボタンを押して詳細画面（「LAN1 アドレスに関連する設定の一括変更の詳細」画面）を表示させることで、一括変更で「変更される設定」と「変更されない設定」が確認できます。



メモ

- 「LAN1 アドレスに関連する設定の一括変更の詳細」画面を表示しておくと、設定の確定により通信ができなくなってしまった場合にも、設定を参照することができます。
- 「変更されない設定」に表示された内容は、設定の確定後に [詳細設定] またはコマンド入力での設定変更が必要となる場合がありますので、必要に応じて書き残すなどしてください。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN1 アドレスの変更」画面が表示されます。「LAN1 アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

注意

LAN 1 インターフェースの IP アドレスを変更する場合は、LAN1 インターフェースのネットワークアドレスに合わせてパソコンなどの接続機器の IP アドレスも変更してください。

第 4 章　IPv4 アドレスでインターネットに接続する

本章では、IPv4 アドレスでインターネットに接続する方法について説明します。本製品に接続するインターネット回線に合わせて、必要な接続方法を選んでください。

・ ブロードバンド回線でインターネットに接続する …28 ページ
・ USB 接続型データ通信端末でインターネットに接続する …39 ページ
・ IPv4 over IPv6 トンネルでインターネットに接続する …58 ページ

4.1　ブロードバンド回線でインターネットに接続する

ブロードバンド回線（PPPoE 接続または DHCP 接続）を使用してインターネットに接続します。
インターネット接続に使用するプロバイダーの設定資料を用意してください。

注意

- **プロバイダー契約を解除または変更したときは、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。**
- **インターネットに常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分注意したうえ、お使いください。詳しくは「第 13 章 セキュリティーを強化する」（235 ページ）をご覧ください。**

プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

- ユーザー ID（認証 ID、アカウント名）
- パスワード（認証パスワード、初期パスワード）
- IP アドレス
- ネットマスク
- ネームサーバーアドレス
- デフォルト・ゲートウェイ・アドレス

メモ

ネームサーバーアドレスはプロバイダーによって、DNS サーバーアドレスやネームサーバー IP アドレス、DNS サーバー IP アドレスなど呼び名が異なることがあります。

4.1.1 接続方法を確認する

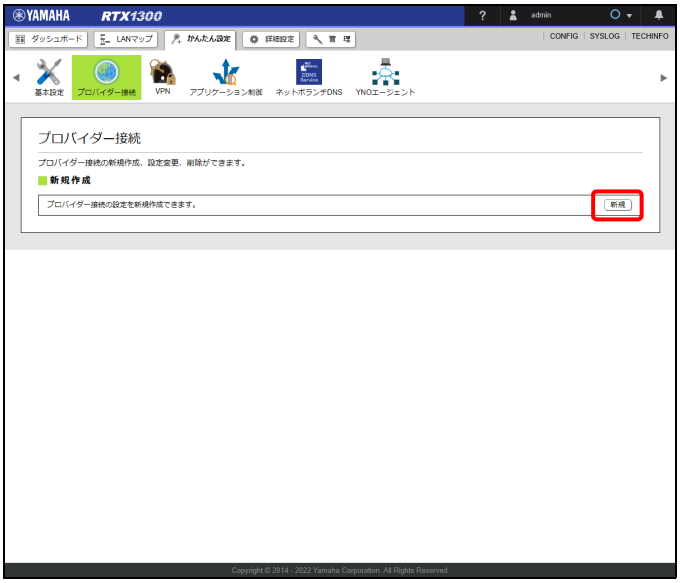
1. LAN ケーブルで ONU やモデムと本製品の LAN ポート（LAN2 または LAN3）を接続する。

メモ

・ 本項ではプロバイダーから提供されたケーブルモデムや ADSL モデムをモデムと呼びます。
・ フレキシブル LAN/WAN ポートを設定している場合、設定に応じて文章中の「LAN2 または LAN3」を適切なインターフェース名に読み替えてください。

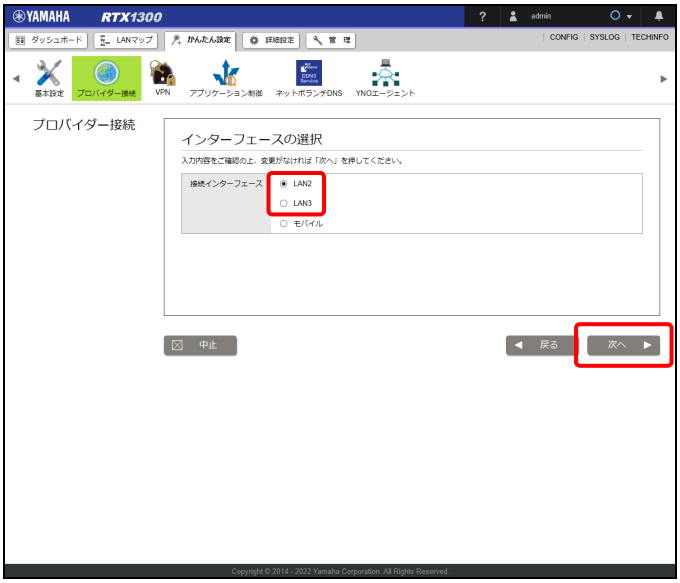
2. **「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。**
「プロバイダー接続」画面が表示されます。

3. **「新規」ボタンをクリックする。**



「インターフェースの選択」画面が表示されます。

4. **ブロードバンド回線を接続した LAN インターフェース（LAN2 または LAN3）を選択し、「次へ」ボタンをクリックする。**

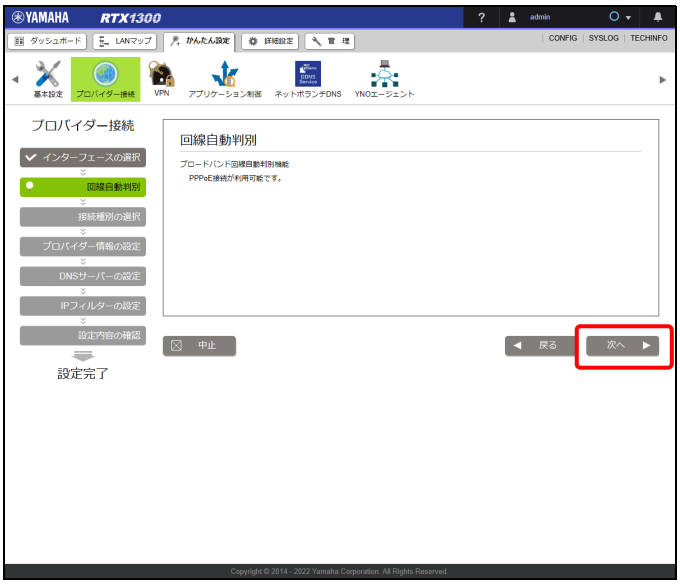


本製品のブロードバンド回線自動判別機能が動作して、「回線自動判別」画面が表示されます。
「回線自動判別」画面には、接続した回線に合わせた接続方法が表示されます。

メモ

選択したポートに回線が接続されていない場合、ブロードバンド回線自動判別機能は動作しません。

5. **自動判別された接続方法を確認し、「次へ」ボタンをクリックする。**

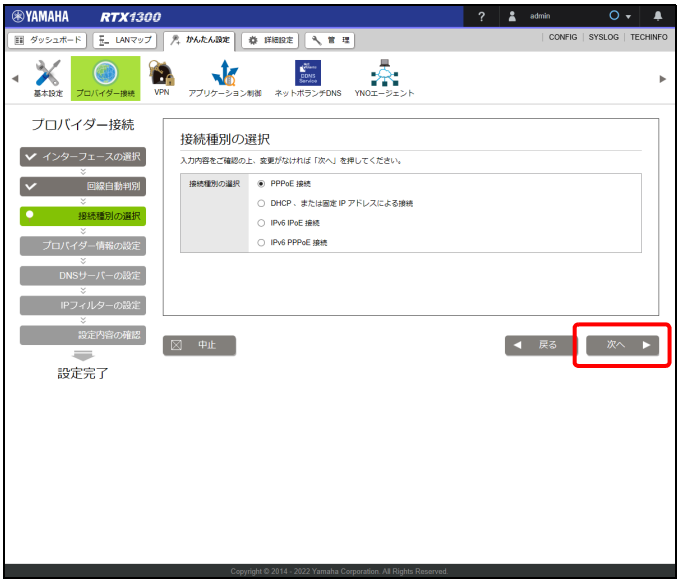


「接続種別の選択」画面が表示されます。

「ブロードバンド回線の自動判別に失敗しました。」が表示された場合

「接続種別の選択」画面で、接続回線に合わせ手動で「PPPoE 接続」または「DHCP 接続」を選択してください。
どちらかわからない場合は、プロバイダーとの契約書を確認するかプロバイダーにお問い合わせください。

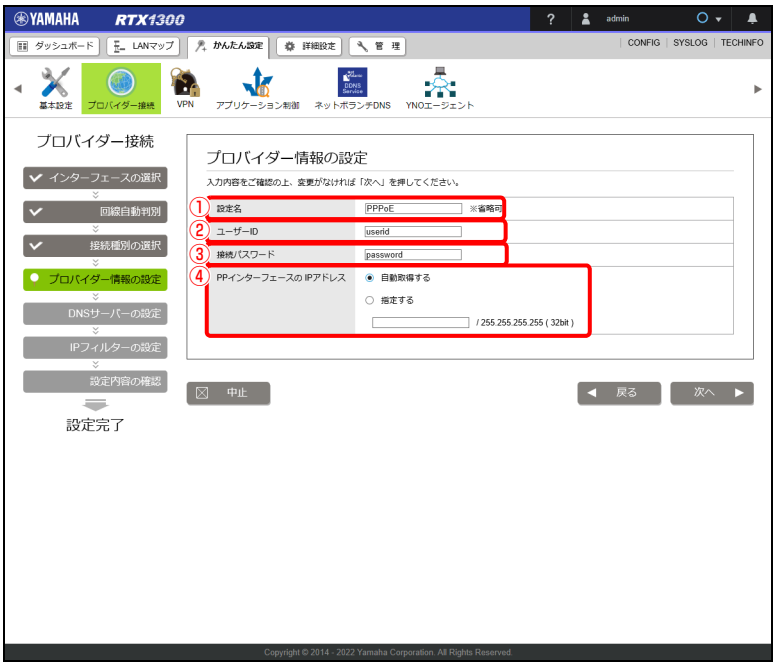
6. **「次へ」ボタンをクリックする。**



接続回線に合わせた「プロバイダー情報の設定」画面が表示されます。
以下の設定は接続回線によって異なりますので、選んだ接続回線の説明をご覧ください。
・「PPPoE 接続」の場合 …31 ページ
・「DHCP 接続」の場合 …35 ページ

4.1.2「PPPoE 接続」の場合

1. **プロバイダー情報を設定する。**



① 設定名：
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

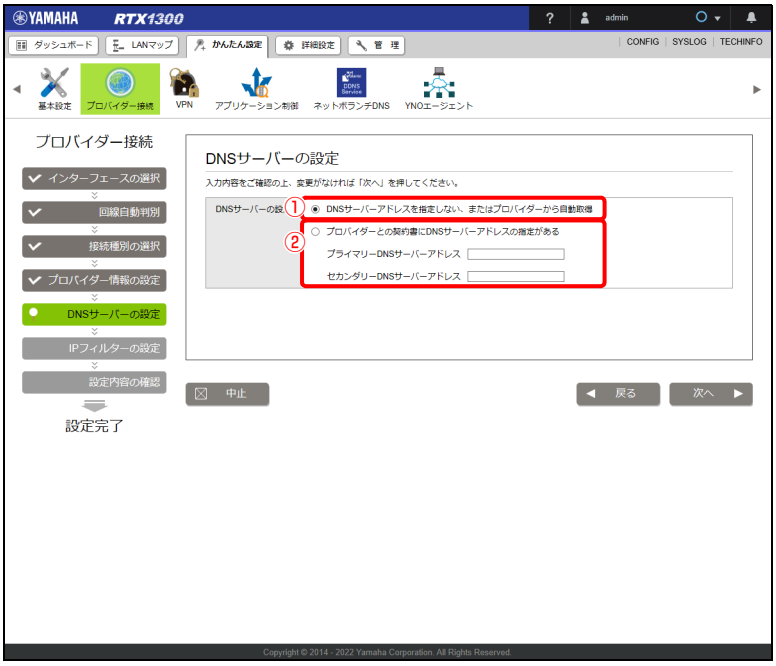
② ユーザー ID：
プロバイダーから指定されたユーザー ID を入力します。

③ 接続パスワード：
プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

④ PP インターフェースの IP アドレス：
PP インターフェースの IP アドレスを設定します。
プロバイダーから PP インターフェースの IP アドレスが指定されていない場合は「自動取得する」を選択します。

2. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

3. DNS サーバーアドレスを設定する。



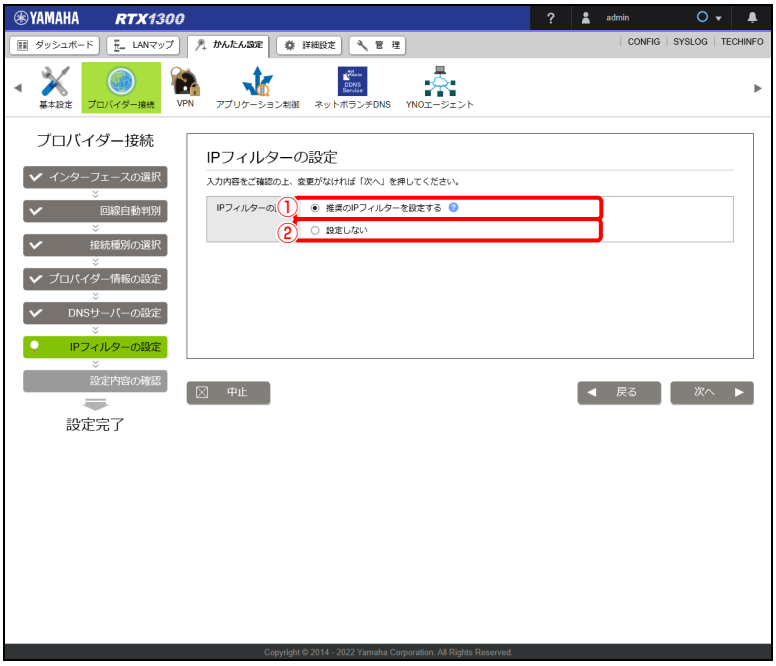
① DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：
プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② プロバイダーとの契約書に DNS サーバーアドレスの指定がある：
プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

- プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット（.）で入力します。
- セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが２つある場合に入力します（1 つだけ指定されている場合は、この欄は空欄にしてください）。

4. 「次へ」ボタンをクリックする。
「IP フィルターの設定」画面が表示されます。

5. IP フィルターを設定する。



① 推奨の IP フィルターを設定する：
以下のようなフィルタリングを実行する IP フィルターが設定されます。
- LAN 側から開始するセッションは双方向で通信を許可する。
- ICMP 以外の WAN 側から開始するセッションを遮断する。
- LAN 側と同じネットワークアドレスに偽装した通信を遮断する。
- Windows ファイル共有の通信を遮断する。

メモ

「詳細設定」タブ―「セキュリティー」―「IP フィルター」から、パケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないように設定できます。詳しくは「13.4 IP フィルターを設定する」（242 ページ）をご覧ください。

②設定しない：
IP フィルターの設定は行われません。すでに設定されている IP フィルターはすべて削除されます。

注意

プロバイダー接続の設定変更時は、「IP フィルターを現在の設定から変更しない」という選択肢も表示されます。IP フィルターの設定を独自にカスタマイズしていて変更したくない場合などは、「IP フィルターを現在の設定から変更しない」を選択してください。

6. 「次へ」ボタンをクリックする。
「設定内容の確認」画面が表示されます。

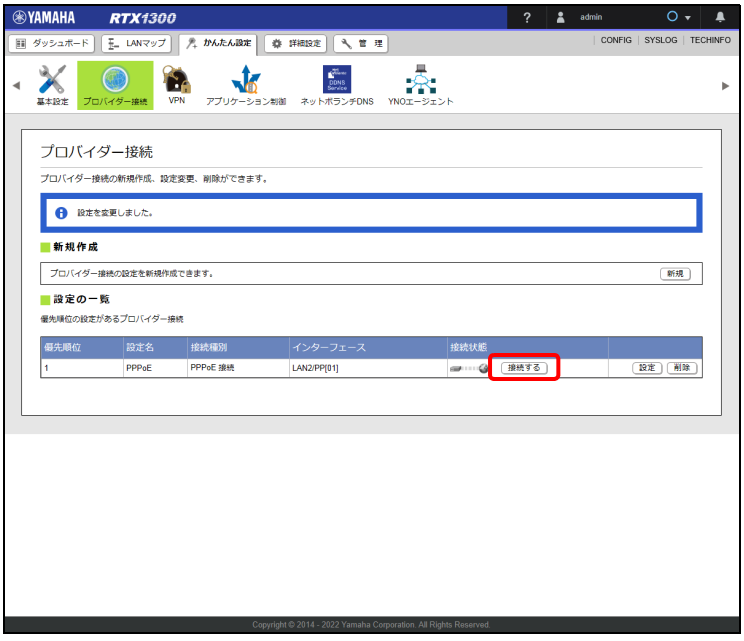
7. 内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

重要

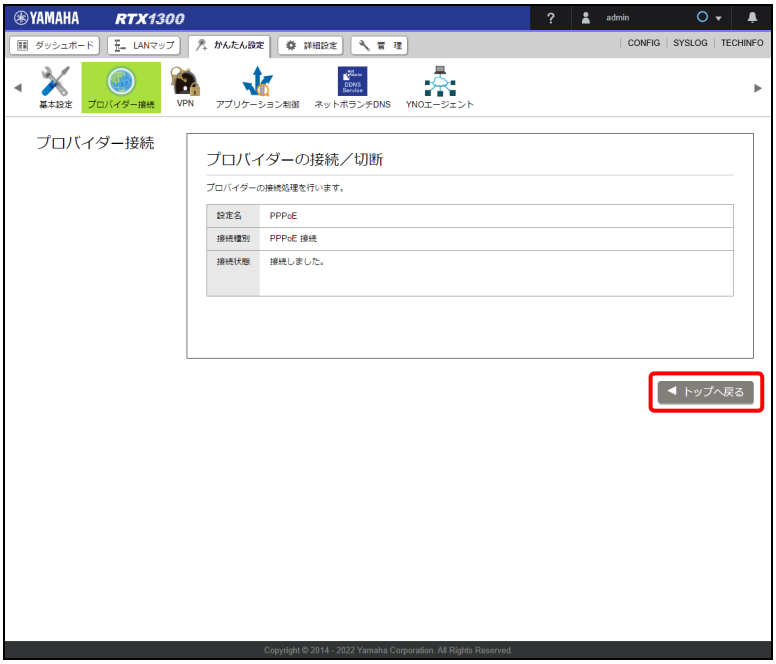
プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。

8. 「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

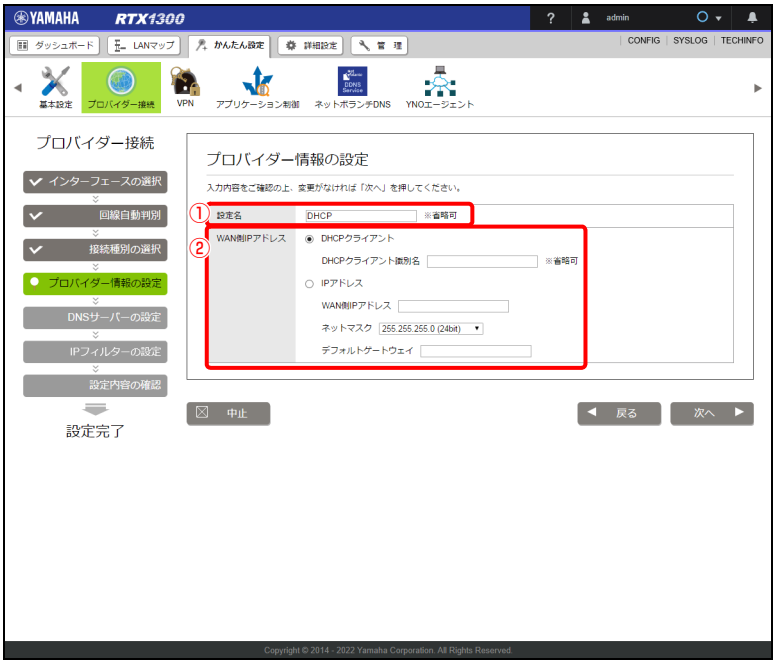
9.「トップへ戻る」ボタンをクリックする。



「接続状態」の表示が  に切り替わります。

4.1.3「DHCP 接続」の場合

1. **プロバイダー情報を設定する。**

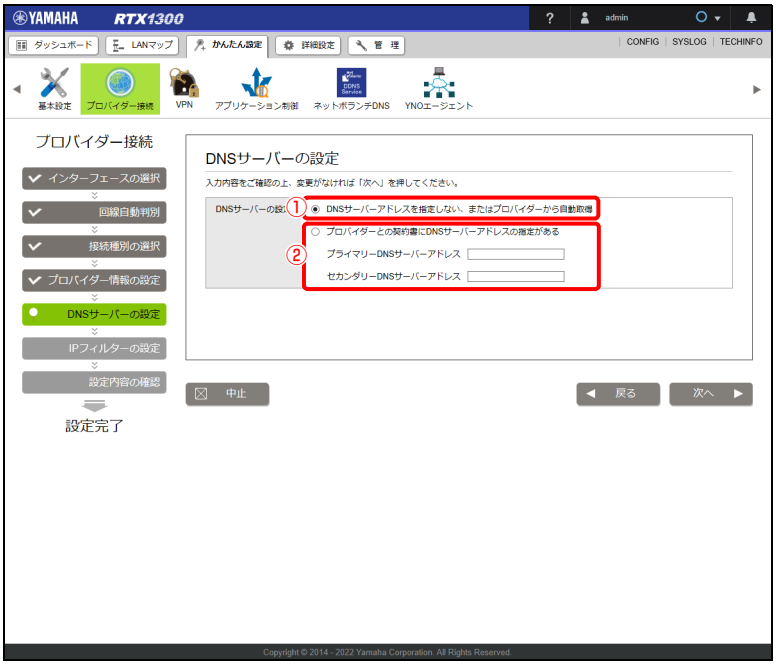


① 設定名：
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② **WAN 側 IP アドレス：**
プロバイダーから指定された IP アドレスを設定します。
・ DHCP クライアント：プロバイダーから IP アドレスが指定されていない場合に選択します。DHCP クライアント識別名に任意の名前を入力します。
・ IP アドレス：プロバイダーから IP アドレスが指定されている場合に選択し、WAN 側 IP アドレス、ネットマスク、デフォルトゲートウェイを入力します。

2. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

3. **DNS サーバーアドレスを設定する。**

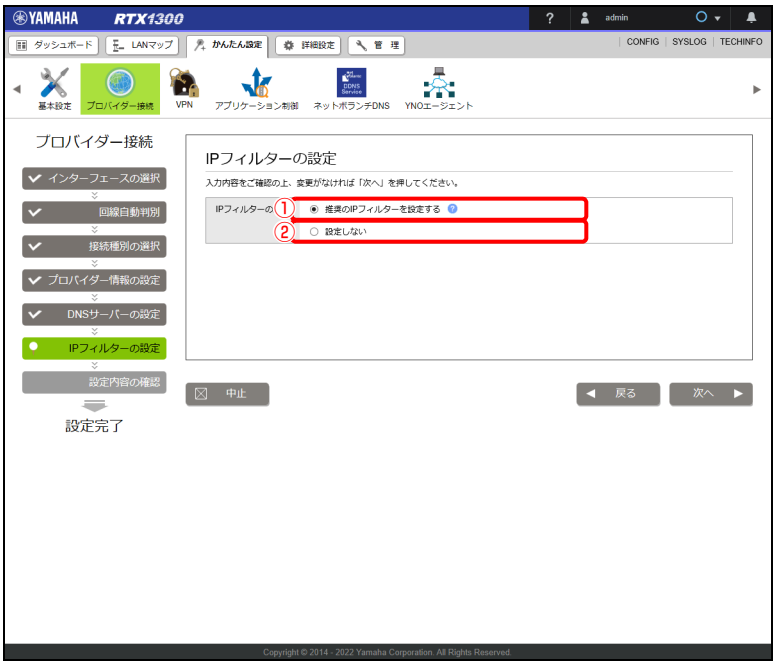


① **DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：**
プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② **プロバイダーとの契約書に DNS サーバーアドレスの指定がある：**
プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。
・ プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット（.）で入力します。
・ セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが 2 つある場合に入力します（1 つだけ指定されている場合は、この欄は空欄にしてください）。

4. **「次へ」ボタンをクリックする。**
「IP フィルターの設定」画面が表示されます。

5. IP フィルターを設定する。



① 推奨の IP フィルターを設定する：
以下のようなフィルタリングを実行する IP フィルターが設定されます。
・ LAN 側から開始するセッションは双方向で通信を許可する。
・ ICMP 以外の WAN 側から開始するセッションを遮断する。
・ LAN 側と同じネットワークアドレスに偽装した通信を遮断する。
・ Windows ファイル共有の通信を遮断する。

メモ

「詳細設定」タブ―「セキュリティー」―「IP フィルター」から、パケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないように設定できます。詳しくは「13.4 IP フィルターを設定する」（242 ページ）をご覧ください。

②設定しない：
IP フィルターの設定は行われません。すでに設定されている IP フィルターはすべて削除されます。

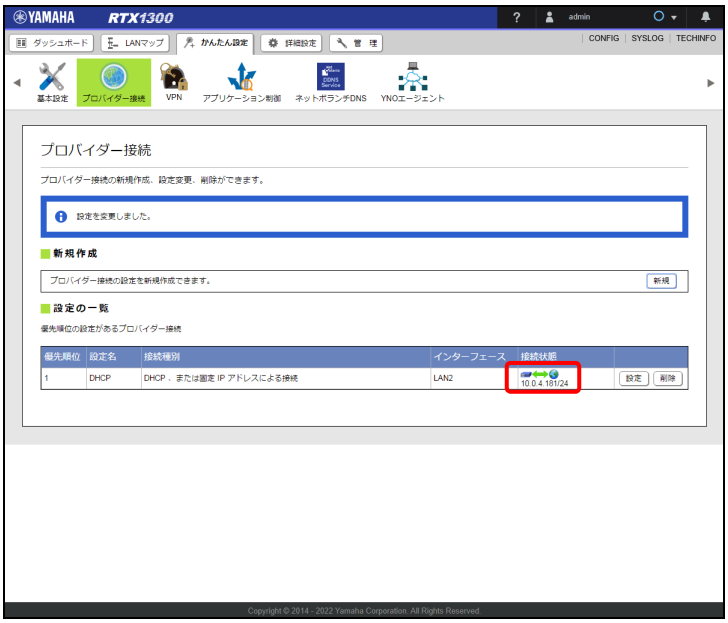
注意

プロバイダー接続の設定変更時は、「IP フィルターを現在の設定から変更しない」という選択肢も表示されます。IP フィルターの設定を独自にカスタマイズしていて変更したくない場合などは「IP フィルターを現在の設定から変更しない」を選択してください。

6. 「次へ」ボタンをクリックする。
「設定内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が に切り替わります。



重要

- プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。
- DHCP 接続のプロバイダーが設定された場合、Web GUI へのアクセスも LAN1 に制限されます。Web GUI へアクセスするインターフェースまたは IP アドレスを変更する場合は、「13.6.1 本製品へのアクセスを制限する」（289 ページ）をご覧ください。

4.2 USB 接続型データ通信端末でインターネットに接続する

3G/4G 携帯電話通信網に対応した USB 接続型データ通信端末を本製品の USB ポートに接続してインターネットに接続します。
インターネット接続に使用するプロバイダーの設定資料を用意してください。

注意

- プロバイダー契約を解除または変更したときは、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- データ通信（パケット通信）の契約が従量制である場合、あるいはデータ通信が定額制の契約の対象外である場合、長時間通信したり大量のデータをやりとりしたりすると高額な料金が発生します。使用にあたっては、通信料金について十分注意してください。
- インターネットに常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分注意したうえ、お使いください。詳しくは「第 13 章 セキュリティーを強化する」（235 ページ）をご覧ください。

メモ

- 通信端末は、利用する携帯端末の取扱説明書に指定されている使い方や、環境条件のもとでお使いください。
- 本機能は 64k データ通信には対応しておりません。

プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

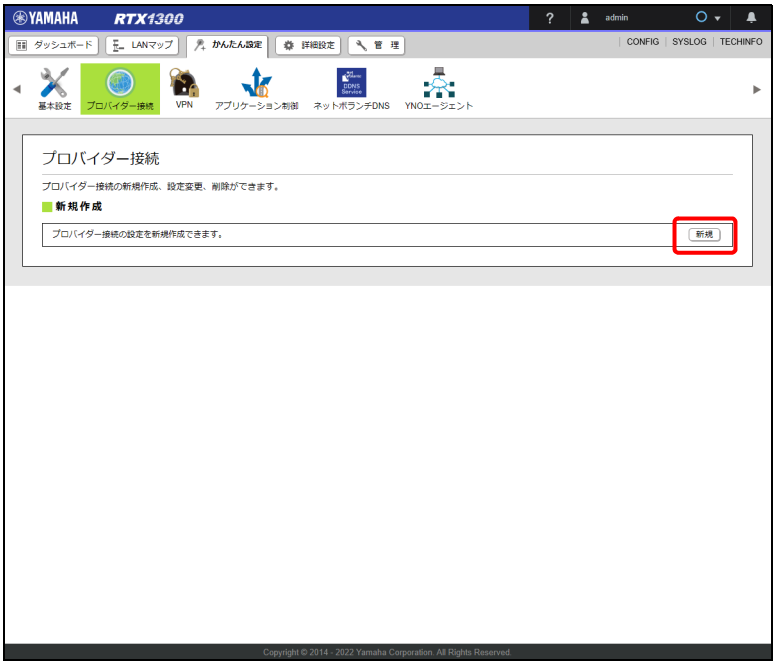
- ユーザー ID（認証 ID、アカウント名）
- パスワード（認証パスワード、初期パスワード）
- IP アドレス
- ネットマスク
- ネームサーバーアドレス
- デフォルト・ゲートウェイ・アドレス
- アクセスポイント名
- CID（Context Identifier）

メモ

ネームサーバーアドレスはプロバイダーによって、DNS サーバーアドレスやネームサーバー IP アドレス、DNS サーバー IP アドレスなど呼び名が異なることがあります。

1. **本製品の USB ポートに、USB 接続型データ通信端末を接続する。**
2. **「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。**
   「プロバイダー接続」画面が表示されます。

3.「新規」ボタンをクリックする。

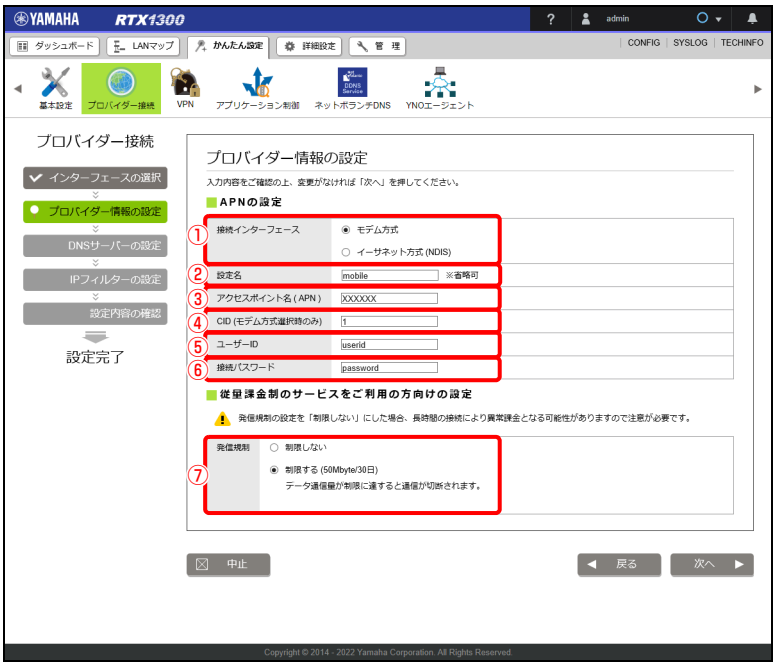


「インターフェースの選択」画面が表示されます。

4.「モバイル」を選択し、「次へ」ボタンをクリックする。

「プロバイダー情報の設定」画面が表示されます。

5. **プロバイダー情報を設定する。**



① 接続インターフェース：
「モデム方式」または「イーサーネット方式（NDIS）」を選択します。

メモ

モデム方式 / イーサネット方式のどちらを選択するかは、利用する USB 接続型データ通信端末によって異なります。
USB 接続型データ通信端末ごとに選択すべき接続インターフェースについて詳しくは、下記の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html

② 設定名：
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

③ アクセスポイント名（APN）：
キャリアまたはプロバイダーから指定された、アクセスポイント名を入力します。

④ CID（モデム方式選択時のみ）：
接続インターフェースで「モデム方式」を選択時に、キャリアまたはプロバイダーから指定された、CID 番号（Context Identifier）を入力します。

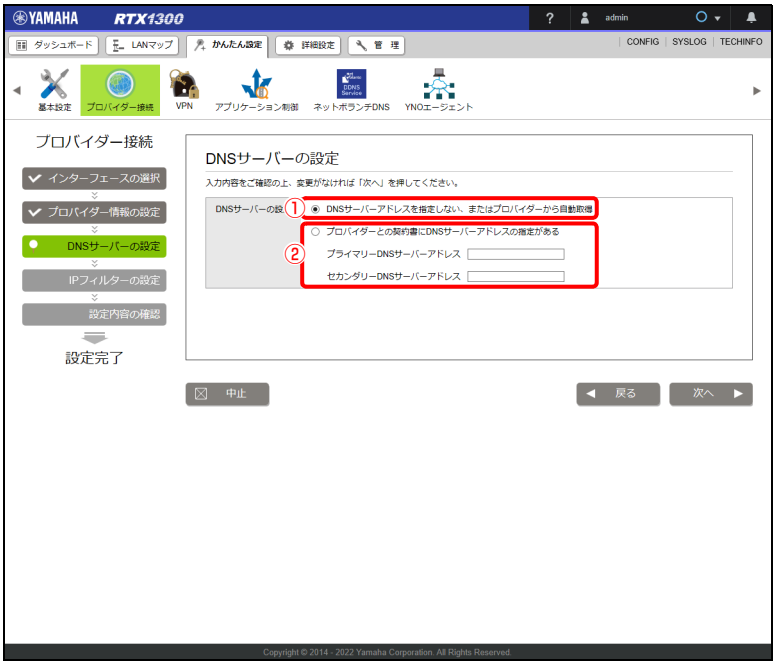
⑤ ユーザー ID：
キャリアまたはプロバイダーから指定されたユーザー ID を入力します。

⑥ 接続パスワード：
キャリアまたはプロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

⑦ 発信規制：
累積送受信データ量、累積接続時間による発信規制を行うか否かを設定します。
従量課金制サービスを利用する方のための設定です。

6. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

7. DNS サーバーアドレスを設定する。



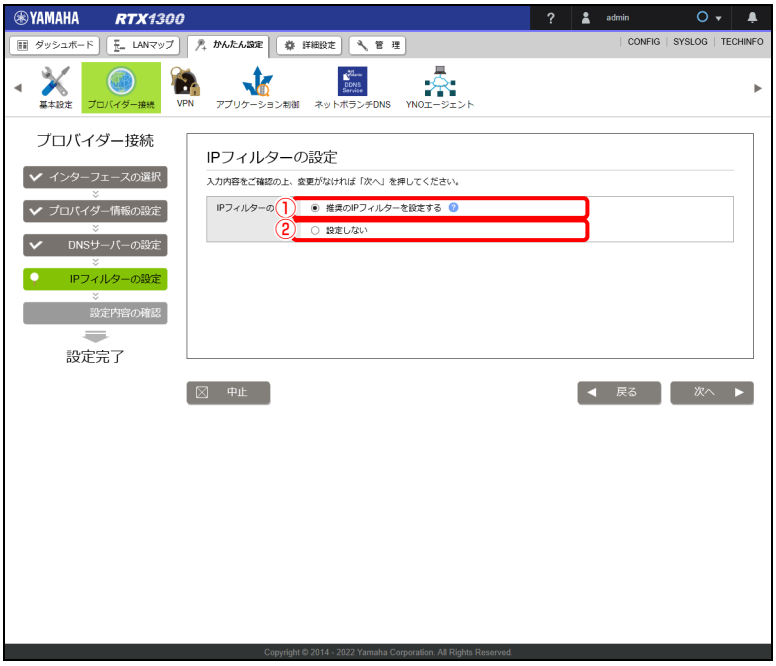
① DNS サーバーアドレスを指定しない、またはプロバイダーから自動取得：
プロバイダーから DNS サーバーアドレスが指定されていない場合に選択します。

② プロバイダーとの契約書に DNS サーバーアドレスの指定がある：
プロバイダーから DNS サーバーアドレスが指定されている場合に選択し、以下の設定を行います。

- プライマリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスを半角数字とドット（.）で入力します。
- セカンダリー DNS サーバーアドレス：プロバイダーから指定されている DNS サーバーアドレスが 2 つある場合に入力します（1 つだけ指定されている場合は、この欄は空欄にしてください）。

8. 「次へ」ボタンをクリックする。
「IP フィルターの設定」画面が表示されます。

9. IP フィルターを設定する。



① 推奨の IP フィルターを設定する：
以下のようなフィルタリングを実行する IP フィルターが設定されます。
- LAN 側から開始するセッションは双方向で通信を許可する。
- ICMP 以外の WAN 側から開始するセッションを遮断する。
- LAN 側と同じネットワークアドレスに偽装した通信を遮断する。
- Windows ファイル共有の通信を遮断する。

メモ

「詳細設定」タブ―「セキュリティー」―「IP フィルター」から、パケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないように設定できます。詳しくは「13.4 IP フィルターを設定する」（242 ページ）をご覧ください。

②設定しない：
IP フィルターの設定は行われません。すでに設定されている IP フィルターはすべて削除されます。

注意

プロバイダー接続の設定変更時は、「IP フィルターを現在の設定から変更しない」という選択肢も表示されます。IP フィルターの設定を独自にカスタマイズしていて変更したくない場合などは「IP フィルターを現在の設定から変更しない」を選択してください。

10.「次へ」ボタンをクリックする。
「設定内容の確認」画面が表示されます。

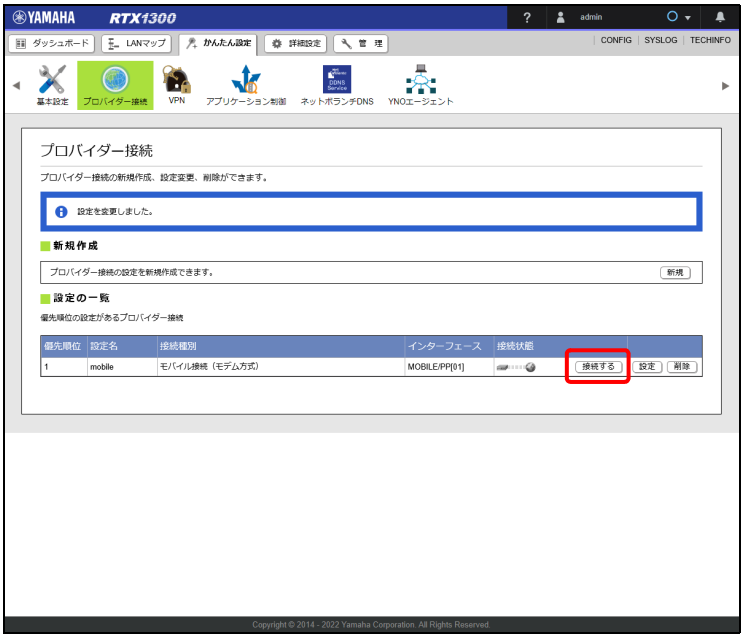
11.内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

重要

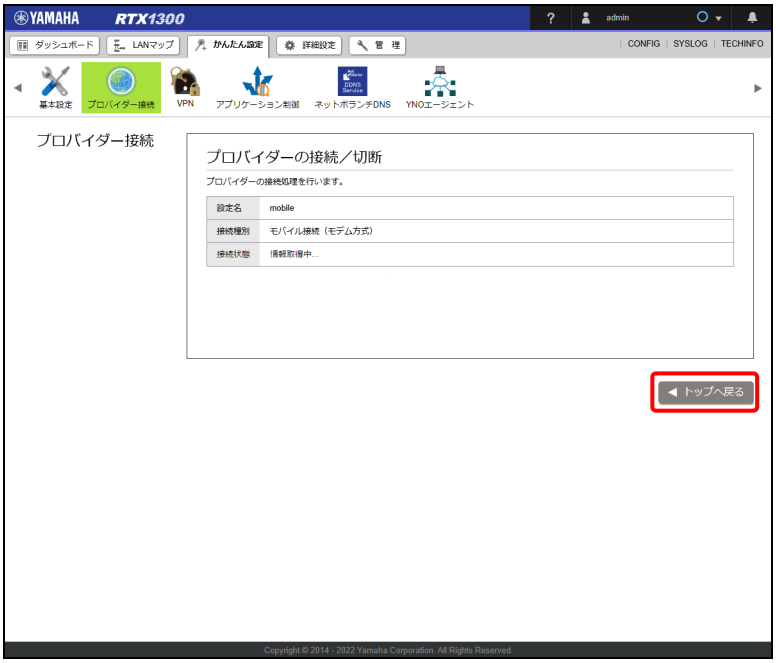
プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。

12.「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

13.「トップへ戻る」ボタンをクリックする。



「接続状態」の表示が に切り替わります。

第 5 章　IPv6 アドレスでインターネットに接続する

本章では、IPv6 アドレスでインターネットに接続する方法について説明します。本製品に接続するインターネット回線に合わせて、必要な接続方法を選んでください。

・ フレッツ光（IPv6 IPoE）でインターネットに常時接続する …46 ページ
・ フレッツ光（IPv6 PPPoE）でインターネットに常時接続する …52 ページ
・ IPv4 over IPv6 トンネルでインターネットに接続する …58 ページ

5.1　フレッツ光（IPv6 IPoE）でインターネットに常時接続する

フレッツ光（IPv6 IPoE）を使用してインターネットに接続します。
インターネット接続に使用するプロバイダーの設定資料を用意してください。

注意

・ プロバイダー契約を解除または変更したときは、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
・ インターネットに常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分注意したうえ、お使いください。詳しくは「第 13 章 セキュリティーを強化する」（235 ページ）をご覧ください。

メモ

フレッツ光ネクストにおけるインターネット（IPv6 IPoE）接続を用いてインターネット（IPv6）サービスを利用するためには、IPv6 IPoE 接続に対応したプロバイダーとの契約とフレッツ・v6 オプションへのお申し込みが必要となります。

プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です。
・ ひかり電話の契約の有無

1. LAN ケーブルで ONU やモデムと本製品の LAN ポート（LAN2 または LAN3）を接続する。

重要

ホームゲートウェイ配下に本製品を設置する場合は「ホームゲートウェイ配下に本製品を設置するためのヒント」（51 ページ）をご覧ください。

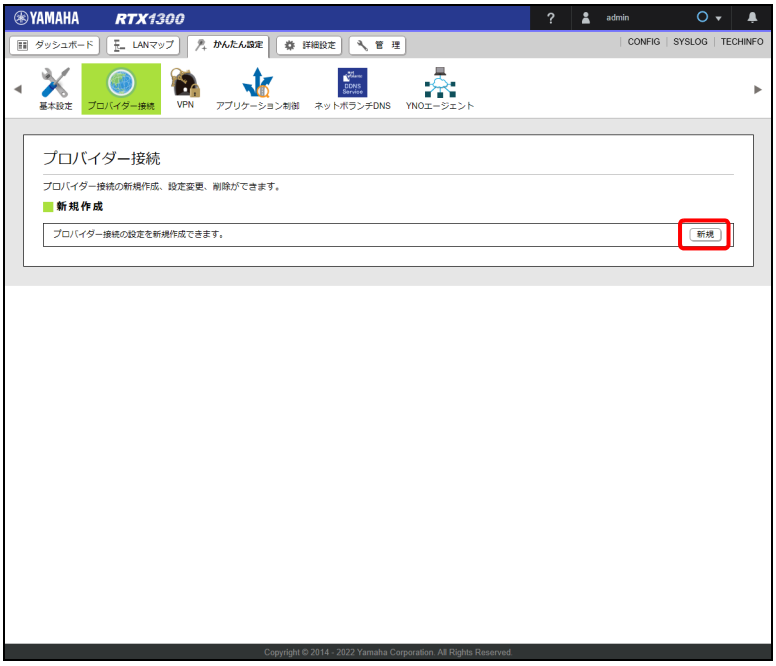
メモ

・ 本節ではプロバイダーから提供されたケーブルモデムや ADSL モデムをモデムと呼びます。
・ フレキシブル LAN/WAN ポートを設定している場合、設定に応じて文章中の「LAN2 または LAN3」を適切なインターフェース名に読み替えてください。

2.「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。

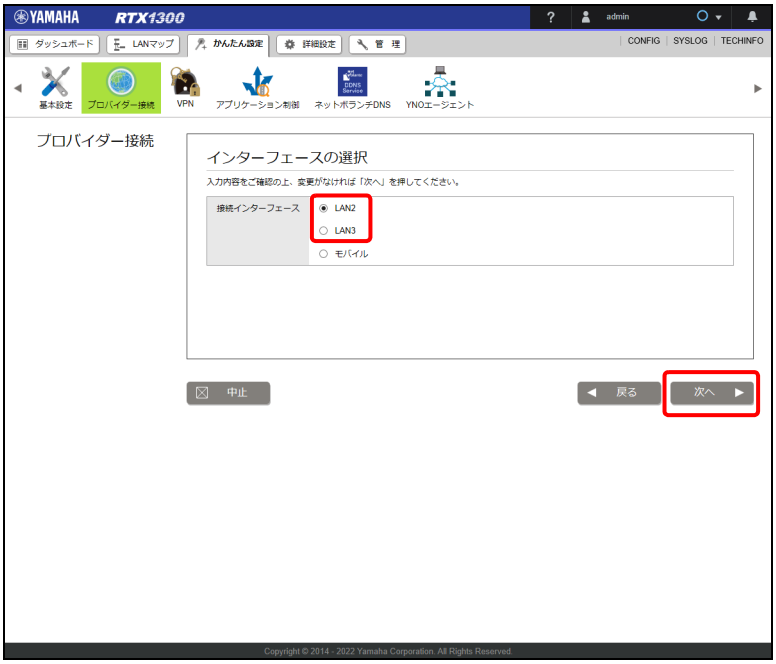
「プロバイダー接続」画面が表示されます。

3. 「新規」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

4. フレッツ光回線を接続した LAN ポート（LAN2 または LAN3）を選択し、「次へ」ボタンをクリックする。

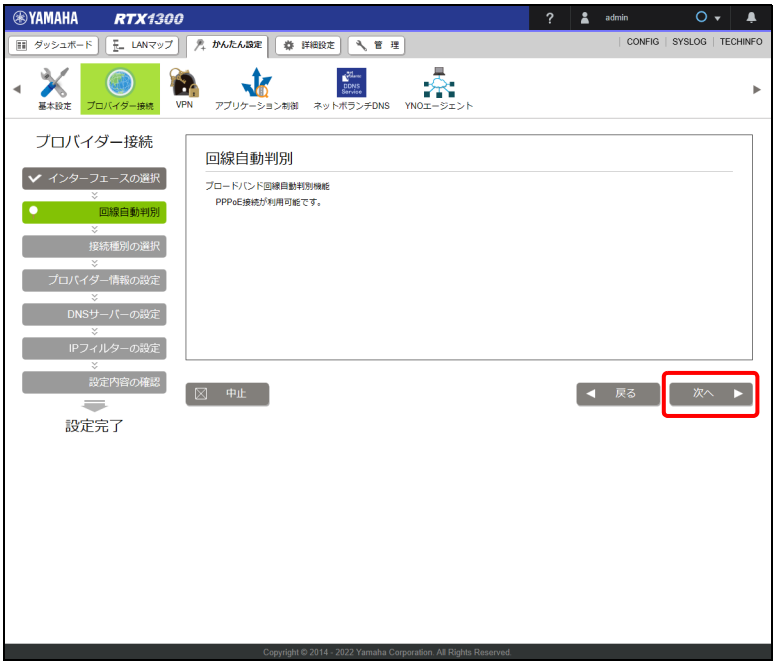


「回線自動判別」画面が表示されます。

重要

IPv6 回線の自動判別は行えないため、手順 5 の「回線自動判別」画面では適切な種別が表示されません。手順 6 の「接続種別の選択」画面で、必ず手動で接続種別を選択し直してください。

5.「次へ」ボタンをクリックする。



「接続種別の選択」画面が表示されます。

6.「IPv6 IPoE 接続」を選択し、「次へ」ボタンをクリックする。

「プロバイダー情報の設定」画面が表示されます。

7. **プロバイダー情報を設定する。**

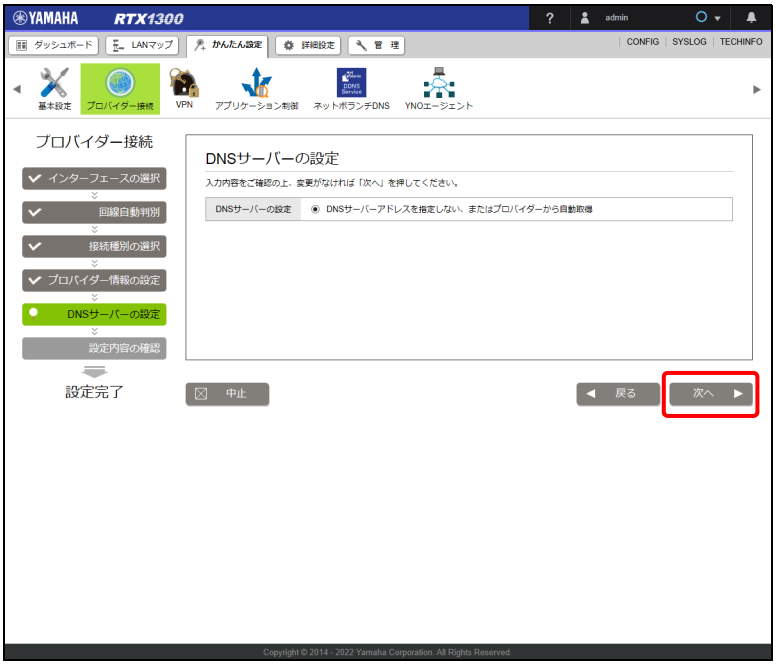
① **設定名：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② **ひかり電話の契約：**
フレッツ光ネクスト回線の契約の「ひかり電話の契約の有無」に合わせて選択します。

③ **IPv4 over IPv6 トンネルの設定：**
「使用しない」を選択してください。
IPv4 over IPv6 トンネルを使用する場合は「第 6 章 IPv4 over IPv6 トンネルでインターネットに接続する」（58 ページ）をご覧ください。

8. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

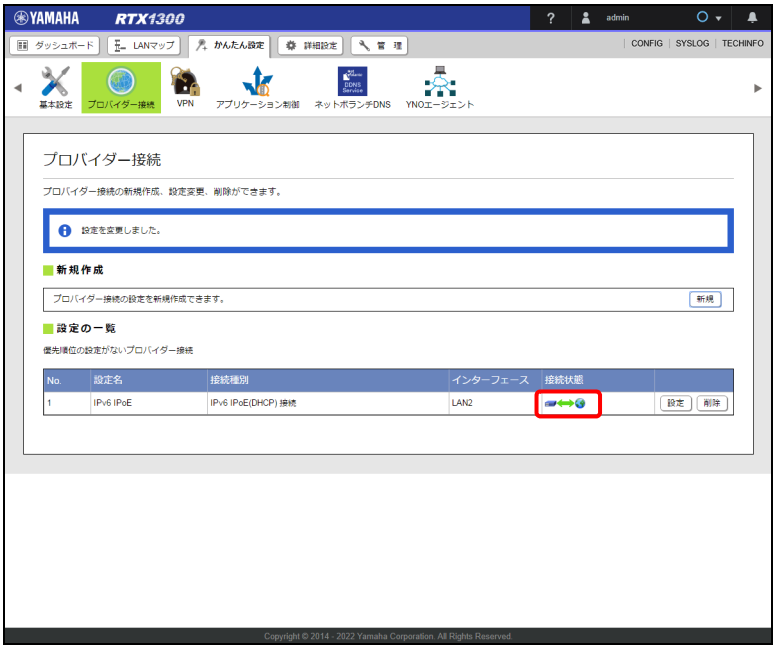
9.「次へ」ボタンをクリックする。



「設定内容の確認」画面が表示されます。

10.内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が に切り替わります。



重要

プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。

ホームゲートウェイ配下に本製品を設置するためのヒント

- Web GUI の「ひかり電話の契約」項目で「契約している」を選択した場合、本製品は DHCPv6-PD で IPv6 プレフィックスを受信するようになりますが、RA で IPv6 プレフィックスを受信する必要があるため、手順 7 の②では、ひかり電話契約の有無に関わらず「契約していない」を選択してください。
- ホームゲートウェイを本製品へ DHCPv6-PD ではなく RA で IPv6 プレフィックスを広告するように設定する必要があります。設定方法についてはホームゲートウェイのマニュアルをご覧ください。

5.2 フレッツ光（IPv6 PPPoE）でインターネットに常時接続する

フレッツ光（IPv6 PPPoE）を使用してインターネットに接続します。
インターネット接続に使用するプロバイダーの設定資料を用意してください。

注意

- プロバイダー契約を解除または変更したときは、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- インターネットに常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分注意したうえ、お使いください。詳しくは「第 13 章 セキュリティーを強化する」（235 ページ）をご覧ください。

重要

- フレッツ光ネクストにおけるインターネット（IPv6 PPPoE）接続を用いてインターネット（IPv6）サービスを利用するためには、IPv6 PPPoE 接続に対応したプロバイダーとの契約が必要となります。
- ヤマハルーターでは、フレッツ光ネクストにおけるインターネット（IPv6 PPPoE）接続を用いたインターネット（IPv6）サービスは、ひかり電話やひかり TV などの一部のサービスと同時に利用できません。

プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です。

- ユーザー ID（認証 ID、アカウント名）
- パスワード（認証パスワード、初期パスワード）

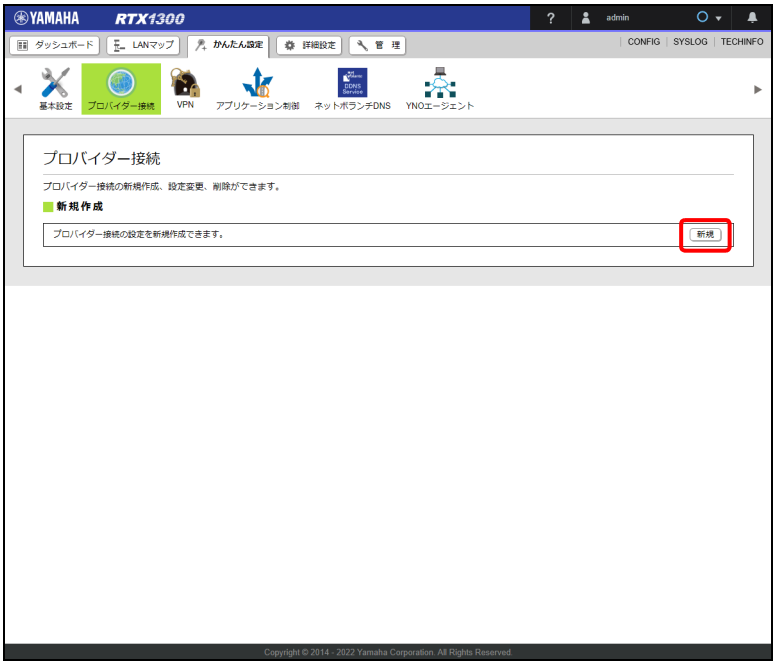
1. モデムと本製品の LAN ポート（LAN2 または LAN3）を、LAN ケーブルで接続する。

メモ

- 本節ではプロバイダーから提供されたケーブルモデムや ADSL モデム、ONU などの機器をモデムと呼びます。
- フレキシブル LAN/WAN ポートを設定している場合、設定に応じて文章中の「LAN2 または LAN3」を適切なインターフェース名に読み替えてください。

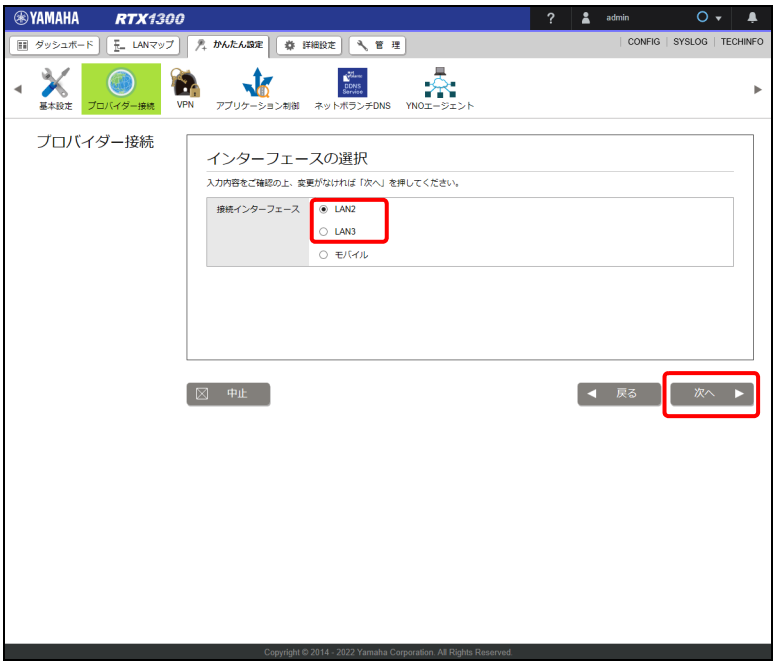
2.「かんたん設定」タブを選択し、「プロバイダー接続」ボタンをクリックする。
「プロバイダー接続」画面が表示されます。

3. 「新規」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

4. フレッツ光回線を接続した LAN インターフェース（LAN2 または LAN3）を選択し、「次へ」ボタンをクリックする。

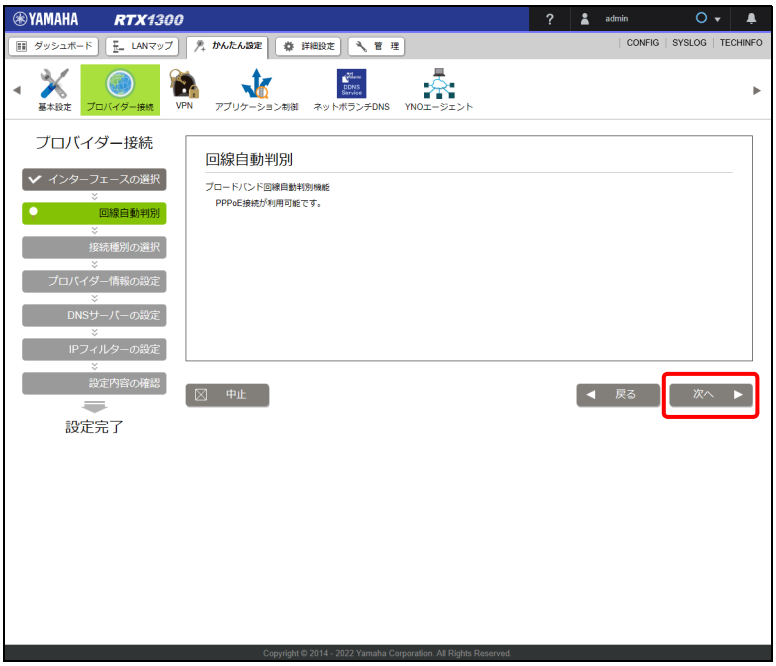


「回線自動判別」画面が表示されます。

重要

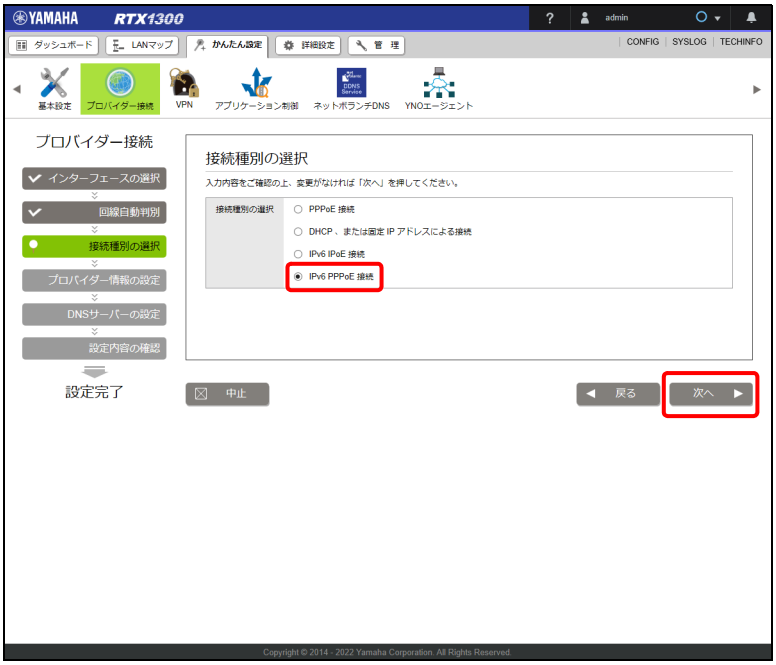
IPv6 回線の自動判別は行えないため、手順５の「回線自動判別」画面では適切な種別が表示されません。手順６の「接続種別の選択」画面で、必ず手動で接続種別を選択し直してください。

5.「次へ」ボタンをクリックする。



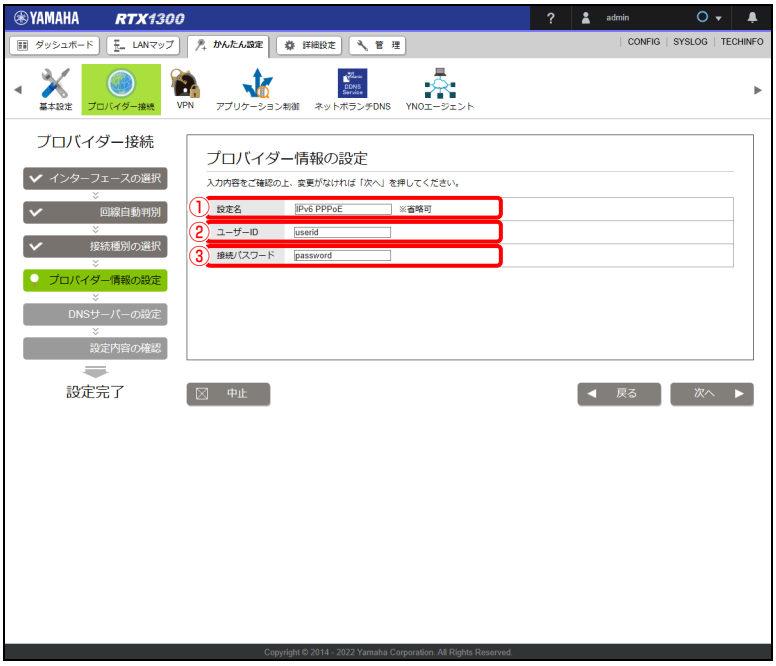
「接続種別の選択」画面が表示されます。

6.「IPv6 PPPoE 接続」を選択し、「次へ」ボタンをクリックする。



「プロバイダー情報の設定」画面が表示されます。

7. **プロバイダー情報を設定する。**



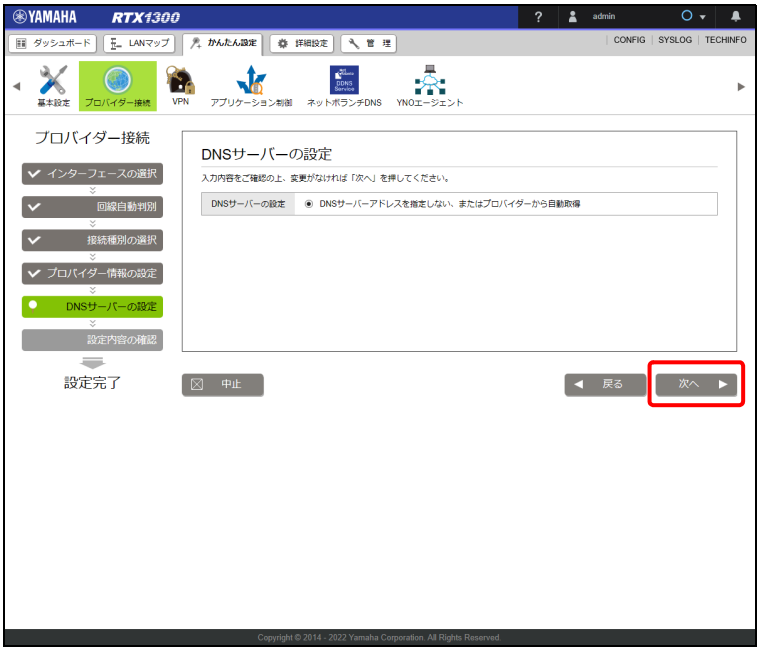
① **設定名：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② **ユーザー ID：**
プロバイダーから指定されたユーザー ID を入力します。

③ **接続パスワード：**
プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

8. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

9.「次へ」ボタンをクリックする。



「設定内容の確認」画面が表示されます。

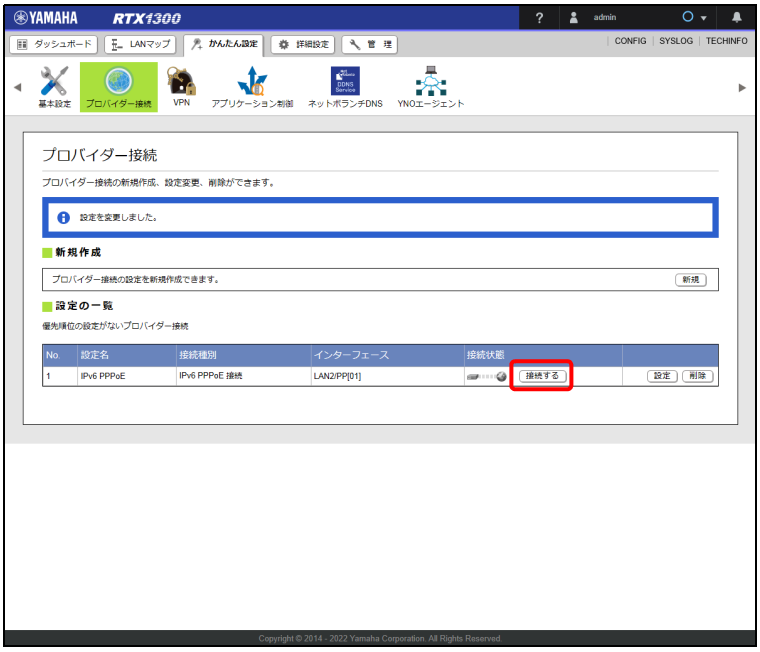
10.内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。

重要

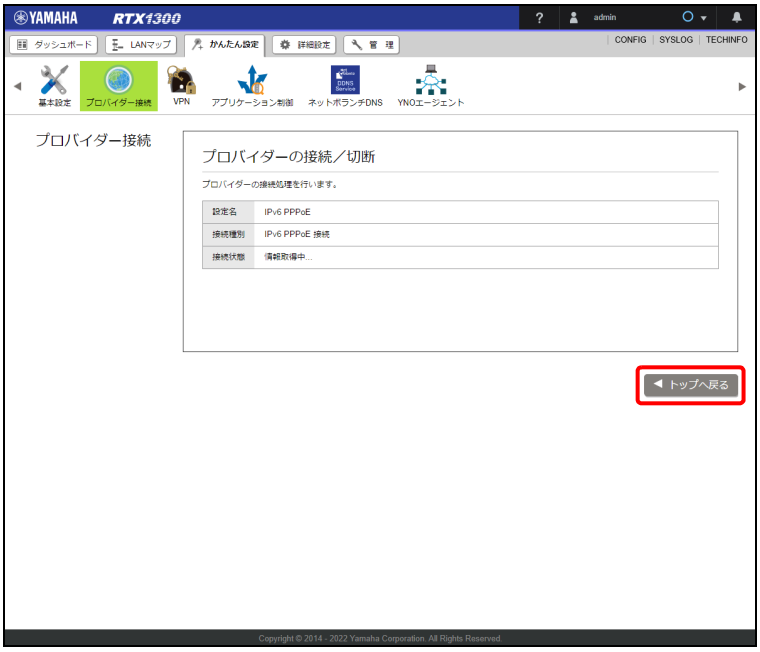
プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。

11.「設定の一覧」項目の中から設定したプロバイダー接続の「接続する」ボタンをクリックする。



プロバイダーへの接続処理が開始され、「プロバイダーの接続 / 切断」画面が表示されます。

12.「トップへ戻る」ボタンをクリックする。



「接続状態」の表示が  に切り替わります。

第 6 章　IPv4 over IPv6 トンネルでインターネットに接続する

本章では、日本ネットワークイネイブラー株式会社が提供する「v6 プラス」、または NTT コミュニケーションズ株式会社が提供する「OCN バーチャルコネクトサービス」を利用して IPv4 インターネットに接続する方法について説明します。事前に各サービスの契約が必要となります。また、インターネット接続に使用するプロバイダーの設定資料を用意してください。

重要

ホームゲートウェイ配下に本製品を設置する場合は「 ホームゲートウェイ配下に本製品を設置するためのヒント」（64 ページ）をご覧ください。

注意

- プロバイダー契約を解除または変更したときは、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダーから意図しない料金を請求される場合があります。
- インターネットに常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分ご注意の上、お使いください。詳しくは「第 13 章 セキュリティーを強化する」（235 ページ）をご覧ください。

メモ

- Web GUI で設定できるサービスは「v6 プラス」と「OCN バーチャルコネクトサービス（シェアードアドレス契約、および固定 IP1 契約）」のみです。他のサービスはコマンドコンソール画面で設定できます。
  設定方法について詳しくは、以下の URL をご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/
- フレッツ光ネクストにおけるインターネット（IPv6 IPoE）接続を用いてインターネット（IPv6）サービスをご利用いただくためには、IPv6 IPoE 接続に対応したプロバイダーとの契約とフレッツ・v6 オプションへのお申し込みが必要となります。

プロバイダーの設定資料

接続先を設定してインターネットに接続するには、プロバイダーから通知される以下の情報が必要です。

- ひかり電話の契約の有無

1. **「かんたん設定」―「プロバイダー接続」で IPv6 IPoE 接続をする場合のプロバイダー情報を設定する。**
   事前に「5.1 フレッツ光（IPv6 IPoE）でインターネットに常時接続する」（46 ページ）を参照し、IPv6 IPoE 接続の設定を行ってください。

2. **プロバイダー情報を設定する。**

① **設定名：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② **ひかり電話の契約：**
フレッツ光ネクスト回線の契約の「ひかり電話の契約の有無」に合わせて選択します。

③ **IPv4 over IPv6 トンネルの設定：**
「使用する」を選択します。
・ 契約したサービス（「v6 プラス」または「OCN バーチャルコネクトサービス」）を選択します。

3. **「次へ」ボタンをクリックする。**
「IPv4 over IPv6 トンネルの設定」画面が表示されます。

4. **IPv4 over IPv6 トンネルの設定で選択したサービスの契約内容を設定します。**
「v6 プラス」と「OCN バーチャルコネクトサービス」で設定内容が変わります。

v6 プラス

①「v6 プラス」（IPv6 IPoE + IPv4 over IPv6）動的 IP サービス：
プロバイダーと動的 IP サービスの契約をしている場合に選択します。

②「v6 プラス」固定 IP サービス：
プロバイダーと固定 IP サービスの契約をしている場合に選択します。

- アップデートサーバーの URL：プロバイダーから指定されたアップデートサーバーの URL を入力します。
- ユーザー名：プロバイダーから指定されたユーザー ID を入力します。
- パスワード：プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。
- インターフェース ID：プロバイダーから指定されたインターフェース ID を入力します。
- IPv6 アドレス：プロバイダーから指定された BR の IPv6 アドレスを入力します。
- IPv4 アドレス：プロバイダーから指定された固定の IPv4 アドレスを入力します。

「OCN バーチャルコネクトサービス」

① **OCN バーチャルコネクトサービスシェアードアドレス契約：**
プロバイダーとシェアードアドレス契約をしている場合に選択します。

② **OCN バーチャルコネクトサービス固定 IP1 契約：**
プロバイダーと固定 IP1 契約をしている場合に選択します。

- アドレス解決システム URL：プロバイダーから指定されたアドレス解決システム URL を入力します。
- 認証用 ID：プロバイダーから指定された認証用 ID を入力します。
- 認証用パスワード：プロバイダーから指定されたパスワード（または自分で変更したパスワード）を入力します。

5. **「次へ」ボタンをクリックする。**
「DNS サーバーの設定」画面が表示されます。

6. **「次へ」ボタンをクリックする。**

「IP フィルターの設定」画面が表示されます。

7. IP フィルターを設定する。

① 推奨の IP フィルターを設定する：
以下のようなフィルタリングを実行する IP フィルターが設定されます。
- LAN 側から開始するセッションは双方向で通信を許可する。
- ICMP 以外の WAN 側から開始するセッションを遮断する。
- LAN 側と同じネットワークアドレスに偽装した通信を遮断する。
- Windows ファイル共有の通信を遮断する。

メモ

「詳細設定」タブ ―「セキュリティー」―「IP フィルター」から、パケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないように設定できます。詳しくは「13.4 IP フィルターを設定する」（242 ページ）をご覧ください。

② 設定しない：
IP フィルターの設定は行われません。すでに設定されている IP フィルターはすべて削除されます。

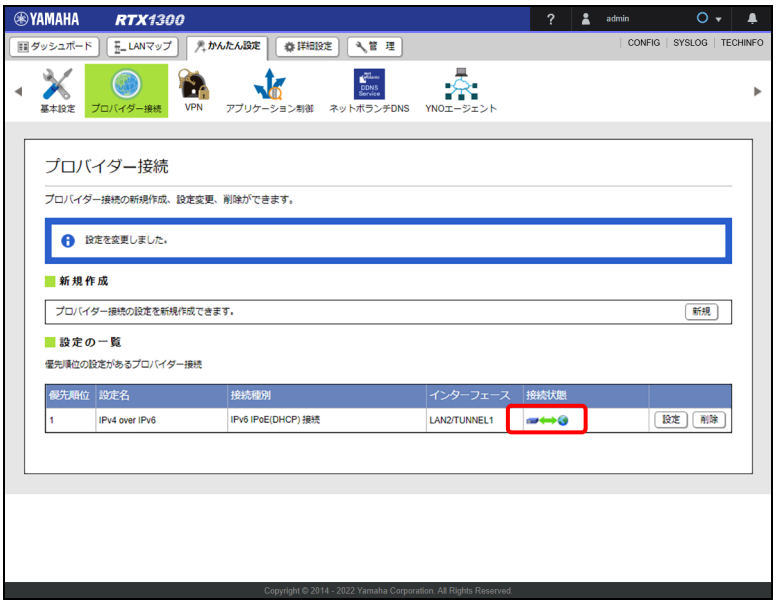
注意

プロバイダー接続の設定変更時は、「IP フィルターを現在の設定から変更しない」という選択肢も表示されます。IP フィルターの設定を独自にカスタマイズしていて変更したくない場合などは、「IP フィルターを現在の設定から変更しない」を選択してください。

8. 「次へ」ボタンをクリックする。
「設定内容の確認」画面が表示されます。

9. 内容を確認し、「設定の確定」ボタンをクリックする。

プロバイダー情報が設定され、「プロバイダー接続」画面が表示されます。自動でインターネットに接続され、「接続状態」の表示が  に切り替わります。



重要

プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。本製品の DNS サーバー機能にアクセスできるホストを変更する場合は、「14.9 DNS サーバー機能にアクセスできるホストの設定を変更する」（377 ページ）をご覧ください。

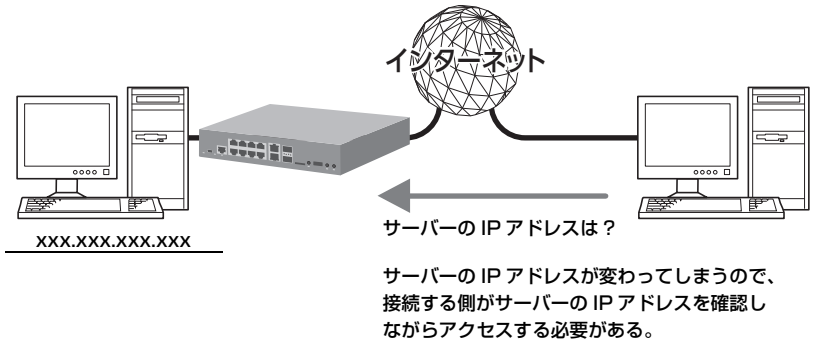
ホームゲートウェイ配下に本製品を設置するためのヒント

- Web GUI の「ひかり電話の契約」項目で「契約している」を選択した場合、本製品は DHCPv6-PD で IPv6 プレフィックスを受信するようになりますが、RA で IPv6 プレフィックスを受信する必要があるため、手順 2 の②では、ひかり電話契約の有無に関わらず「契約していない」を選択してください。
- ホームゲートウェイを本製品へ DHCPv6-PD ではなく RA で IPv6 プレフィックスを広告するように設定する必要があります。設定方法についてはホームゲートウェイのマニュアルをご覧ください。
- ホームゲートウェイを設置している場合、ホームゲートウェイで IPv4 over IPv6 トンネリングの設定を無効にしてください。

第 7 章　ネットボランチ DNS サービスを利用する

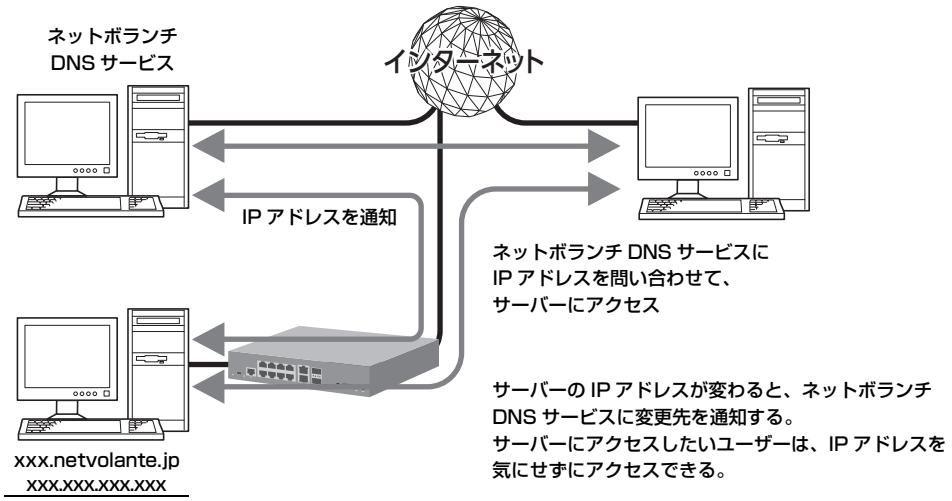
7.1　ネットボランチ DNS サービスとは？

サーバーを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、サーバーのグローバル IP アドレスがわかっている必要があります。
しかし、インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更される場合があります。そのため、固定グローバル IP アドレスサービスの契約をしていない環境では、サーバーを構築して公開することは困難です。



ネットボランチ DNS サービスを利用すると

グローバル IP アドレスが変更されるたびに IP アドレスがネットボランチ DNS サービスへ通知されるため、ネットボランチ DNS サービスで取得できた固定のホスト名でアクセスできるようになります。
したがって、固定グローバル IP アドレスサービスの契約をしていない環境でも自宅サーバーで独自ドメインを使った各種サーバーを運用したり、IPsec や PPTP を利用して VPN を構築して、外部とデータをやり取りしたりできるようになります。



7.2　ネットボランチ DNS サービスで取得できるホスト名

ネットボランチ DNS サービスを利用すると、「(ユーザーの希望ホスト名) .xxx.netvolante.jp」という形式のホスト名を取得できます。「xxx」の部分は、ネットボランチ DNS サーバーが任意に自動で割り当てます。グローバル IP アドレスが変更されるたびに設定を変更する必要がなくなり、便利です。

メモ

- ホストアドレスはルーター 1 台につき 1 つしか取得できません。
- 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ネットボランチ DNS サービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミック DNS サーバーに登録することはできません。
- ネットボランチ DNS サービスは、プロバイダーからグローバル IP アドレスが割り当てられている環境でのみ利用できます。グローバル IP アドレスとは、下記（プライベート IP アドレス）以外の IP アドレスです。
  - 10.0.0.0 ～ 10.255.255.255
  - 172.16.0.0 ～ 172.31.255.255
  - 192.168.0.0 ～ 192.168.255.255
- ご利用中のプロバイダーによっては、ホスト名の登録／更新内容がネットボランチ DNS サービスにすぐに反映されないことがあります。あらかじめご了承ください。

7.3　ネットボランチ DNS ホスト名を取得する

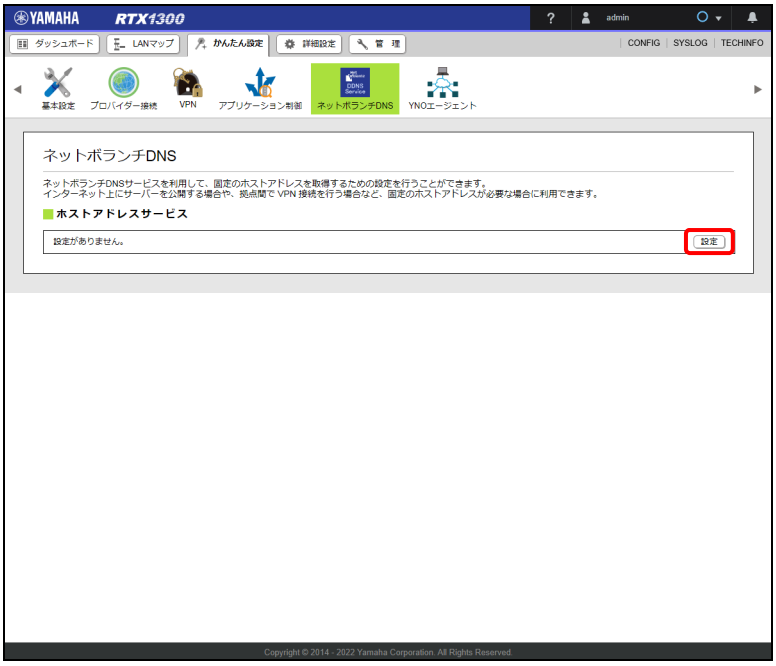
ネットボランチ DNS サービスを利用するには、ホストアドレスを登録します。
本節では「かんたん設定」を使用して LAN2 インターフェースに DHCP 接続型のプロバイダーが設定されている状態（「4.1.3 「DHCP 接続」の場合」（35 ページ）の設定が完了している状態）から設定するという前提で説明します。

メモ

ホストアドレスはルーター 1 台につき 1 つしか取得できません。

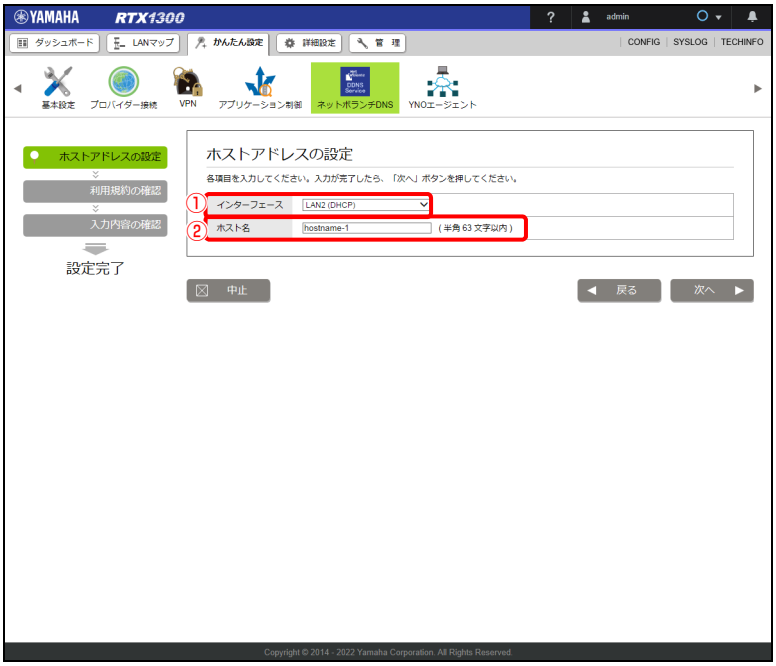
1.「かんたん設定」タブ ―「ネットボランチ DNS」ボタンを順に選択する。
「ネットボランチ DNS」画面が表示されます。

2.「ホストアドレスサービス」項目の「設定」ボタンをクリックする。



「ホストアドレスの設定」画面が表示されます。

3. ホストアドレスを設定する。

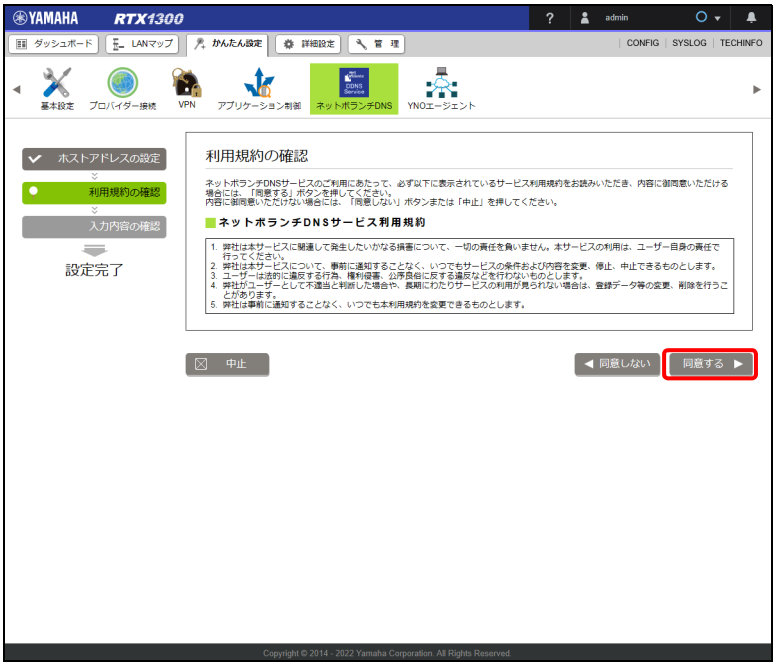


① **インターフェース：**
ホストアドレスを登録する対象のインターフェースを選択します。

② **ホスト名：**
希望のホスト名（63 文字以内）を半角英数字と '-' で入力します。

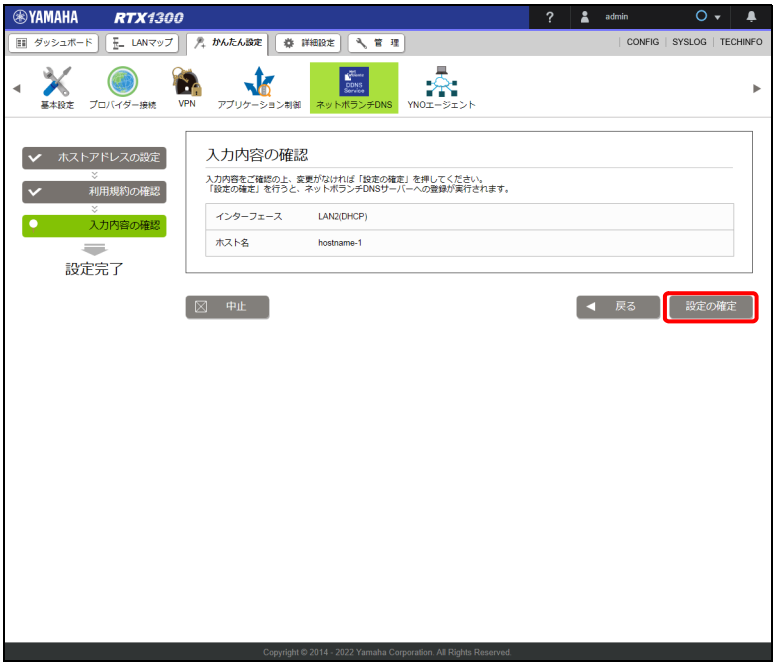
4. 「次へ」ボタンをクリックする。
「利用規約の確認」画面が表示されます。

5. 利用規約の内容をよく確認し、「同意する」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



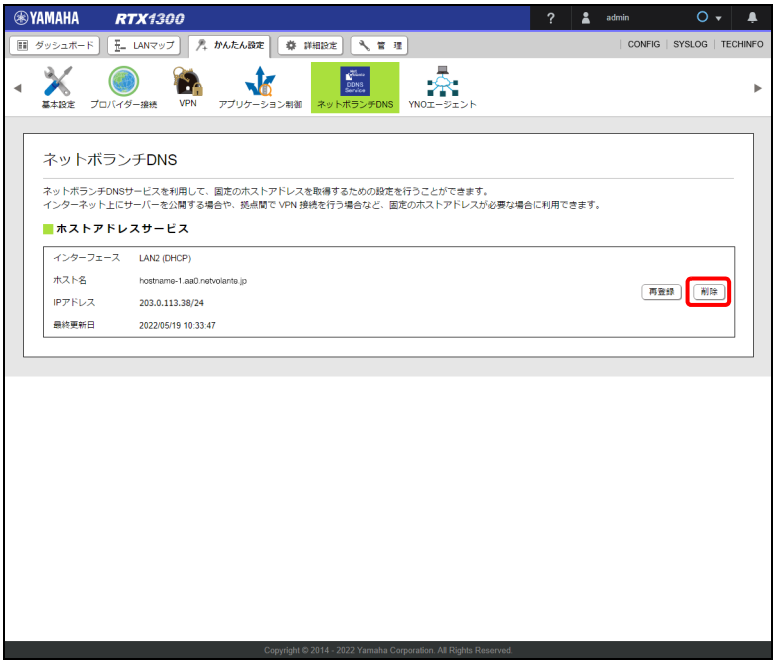
7.4 ネットボランチ DNS ホスト名の登録を解除する

ネットボランチ DNS サービスを効率良く運用するために、譲渡 / 廃棄前に不要となったネットボランチ DNS ホスト名の登録解除にご協力ください。
本節では「かんたん設定」を使用して LAN2 インターフェースに DHCP 接続型のプロバイダーが設定されている状態（「4.1.3 「DHCP 接続」の場合」（35 ページ）の設定が完了している状態）、およびネットボランチ DNS サービスのホストアドレスが、「hostname-1.aa0.netvolante.jp」で登録されている場合を例に説明します。ネットボランチ DNS ホスト名の取得について詳しくは、「7.3 ネットボランチ DNS ホスト名を取得する」（66 ページ）をご覧ください。

ネットボランチ DNS ホスト名の登録解除は、以下の手順に従ってください。

1. **「かんたん設定」タブ ―「ネットボランチ DNS」ボタンを順に選択する。**
   「ネットボランチ DNS」画面が表示されます。

2. **「ホストアドレスサービス」項目の「削除」ボタンをクリックする。**



ネットボランチ DNS ホスト名の登録が削除されます。

第 8 章　拠点間を VPN で接続する

本章では、仮想プライベートネットワーク（VPN）を構築して、拠点間の LAN 同士を接続する方法について説明します。通常のインターネット回線をそのまま利用して VPN を構築できるため、専用線を導入する場合と比較して、低コストで VPN を実現できます。
拠点間を VPN で接続するには、少なくとも一方の拠点にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。グローバル IP アドレスとは、下記（プライベート IP アドレス）以外の IP アドレスです。
— 10.0.0.0 ～ 10.255.255.255
— 172.16.0.0 ～ 172.31.255.255
— 192.168.0.0 ～ 192.168.255.255

VPN の設定をする前に …71 ページ
IPsec で接続する …71 ページ
PPTP で接続する …78 ページ
IPIP で接続する …83 ページ
データコネクトで接続する …88 ページ

重要

- VPN の設定はインターネットに接続した状態で行う必要があるため、VPN を利用した拠点間接続の設定の前にインターネット接続の設定が必要です。
- VPN を利用した拠点間接続を行うには、少なくとも一方の拠点に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要です。

メモ

- Windows でファイル共有をする場合は、NetBIOS over TCP/IP プロトコルを使用するか、または WINS サーバーを用意する必要があります。
- macOS でファイル共有をする場合は、ファイル環境設定の「共有」で「ファイル共有」をオンにします。
- 接続種別が「データコネクト」の場合、インターネット接続の設定をしなくても、拠点間接続を使用することができます。

ネットボランチ DNS ホスト名とは

ネットボランチ DNS サービスにより取得できる固定のホスト名です。ネットボランチ DNS ホスト名は、本製品のグローバル IP アドレスと結びつけられます。
インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更されることがあります。グローバル IP アドレスが変更されると IP アドレスがネットボランチ DNS サーバーへ通知され、ネットボランチ DNS ホスト名に結びつけられた IP アドレスが更新されます。
ネットボランチ DNS ホスト名の取得について詳しくは「第 7 章 ネットボランチ DNS サービスを利用する」（65 ページ）をご覧ください。

8.1 VPN の設定をする前に

LAN 同士を接続する場合には、それぞれの LAN のネットワークアドレスが重複しないように、異なるアドレスを設定しておく必要があります。あらかじめ、本製品の LAN のネットワークアドレスを変更してください。詳しくは「3.3 LAN1 の IP アドレスを設定する」（25 ページ）をご覧ください。

8.2 IPsec で接続する

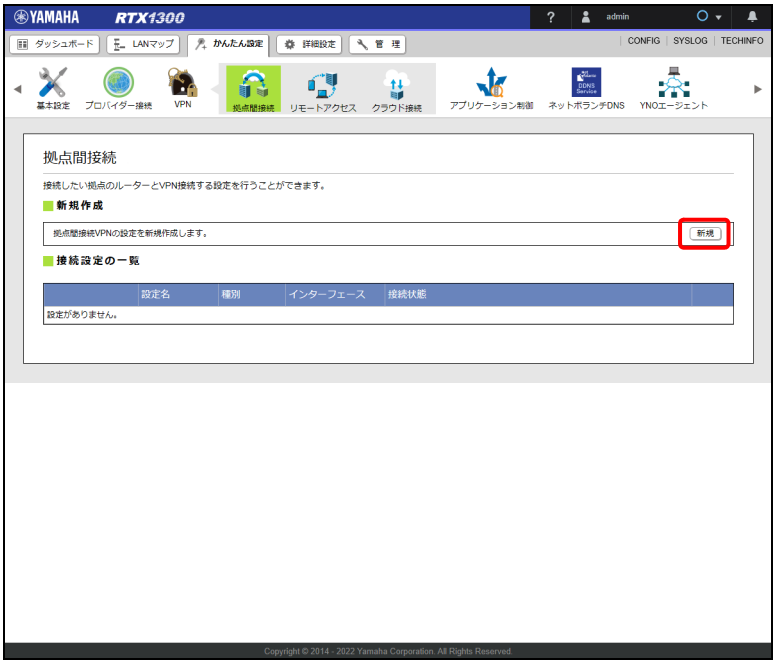
IPsec で拠点間を接続するために必要な設定と接続方法を説明します。IPsec で拠点間を接続するには、どちらかの拠点に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要になります。

メモ

本製品の IPsec の仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

1. **「かんたん設定」タブ ―「VPN」―「拠点間接続」ボタンを順に選択する。**
   「拠点間接続」画面が表示されます。

2. **「新規作成」項目の「新規」ボタンをクリックする。**



「接続種別の選択」画面が表示されます。

3. 「IPsec」を選択し、「次へ」ボタンをクリックする。

「IPsec に関する設定」画面が表示されます。

4. **IPsec の接続情報を設定する。**

注意

認証鍵（pre-shared key）はパスワードに相当する重要な情報です。英大文字および英小文字、数字、記号を組み合わせた分かりにくく長い値を設定し、十分に注意して管理してください。

重要

IPsec 接続をするには、双方の拠点で同じ認証鍵（pre-shared key）を設定する必要があります。

自分側と接続先の両方とも固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合

① ネットワーク環境：
「自分側と接続先の両方とも固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

② 自分側の設定：
本製品の設定を行います。
- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

③ 接続先の情報：
接続先の情報を入力します。
- 接続先のホスト名または IP アドレス：ネットボランチ DNS ホスト名または接続先の IP アドレスを入力します。

④ 接続先と合わせる設定：
接続先と同じ値を設定します。
- 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

自分側のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合

① **ネットワーク環境：**
「自分側のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

② **自分側の設定：**
本製品の設定を行います。
- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

③ **接続先の情報：**
接続先の情報を入力します。
- 接続先の ID：接続先の「自分側の設定」項目の「自分側の ID」に設定された ID を入力します。

④ **接続先と合わせる設定：**
接続先と同じ値を設定します。
- 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

接続先のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている場合

① ネットワーク環境：
「接続先のみ固定のグローバルアドレスまたはネットボランチ DNS ホスト名を持っている」を選択します。

② 自分側の設定：
本製品の設定を行います。

- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。
- 自分側の ID：他の拠点と重複しない ID（名前）を半角英数字で入力します。

③ 接続先の情報：
接続先の情報を入力します。

- 接続先のホスト名または IP アドレス：ネットボランチ DNS ホスト名または接続先の IP アドレスを入力します。

④ 接続先と合わせる設定：
接続先と同じ値を設定します。

- 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

5.「次へ」ボタンをクリックする。
「経路に関する設定」画面が表示されます。

6. **接続先の LAN 側のネットワークアドレスを設定する。**

① 経路を設定しない：
経路を設定しない場合に選択します。
本項目を選択した場合、本設定では通信をすることができません。別途、経路を設定する必要があります。本ページで再設定、または「詳細設定」タブ ―「ルーティング」をご覧ください。

メモ
「フィルターによる振り分け（フィルター型ルーティング）」、「重みに応じた負荷分散」、「バックアップ動作」などで運用したい場合、本設定を確定後、「詳細設定」タブ ―「ルーティング」をご覧ください。

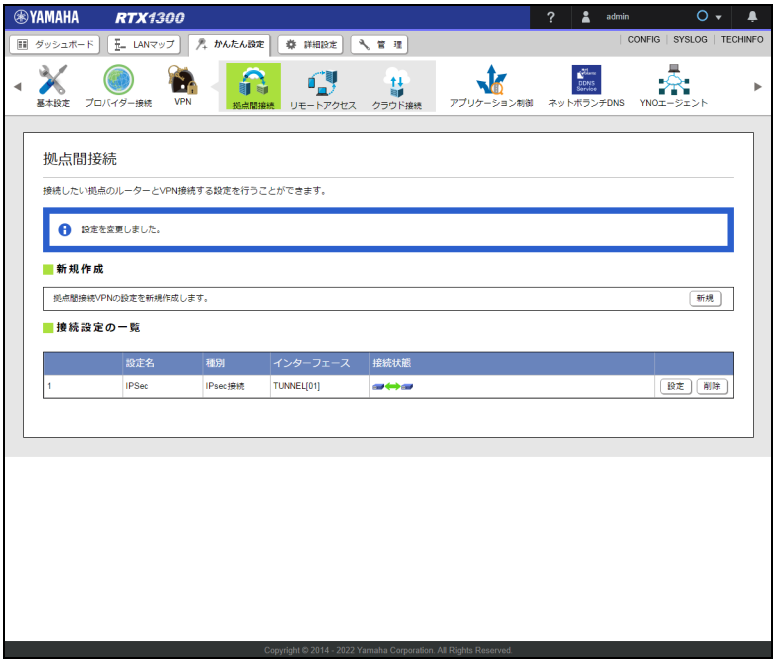
② 接続先の LAN 側のアドレス：
LAN 側のアドレスを指定する場合に選択します。
接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。
IP アドレスを追加する場合は、下部の「 ＋ 」ボタンを押してください。IP アドレスを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

③ デフォルト経路：
デフォルト経路を設定する場合に選択します。

7. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

8. 内容を確認し、「設定の確定」ボタンをクリックする。

設定が反映され、「拠点間接続」画面が表示されます。



双方の拠点で認証が成功すると、自動的に IPsec で拠点間が接続されます（特に操作は必要ありません）。
IPsec 接続が完了すると、「拠点間接続」画面の「接続状態」の表示が  に切り替わります。

自動的に IPsec で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。
・ 接続先の IP アドレス / ネットボランチ DNS のホスト名 /ID が間違っている
・ 接続先と認証鍵（pre-shared key）/ 認証アルゴリズム / 暗号アルゴリズムの設定が一致していない

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、「ユーザーガイド」（ウェブサイト）をご覧ください。

8.3　PPTP で接続する

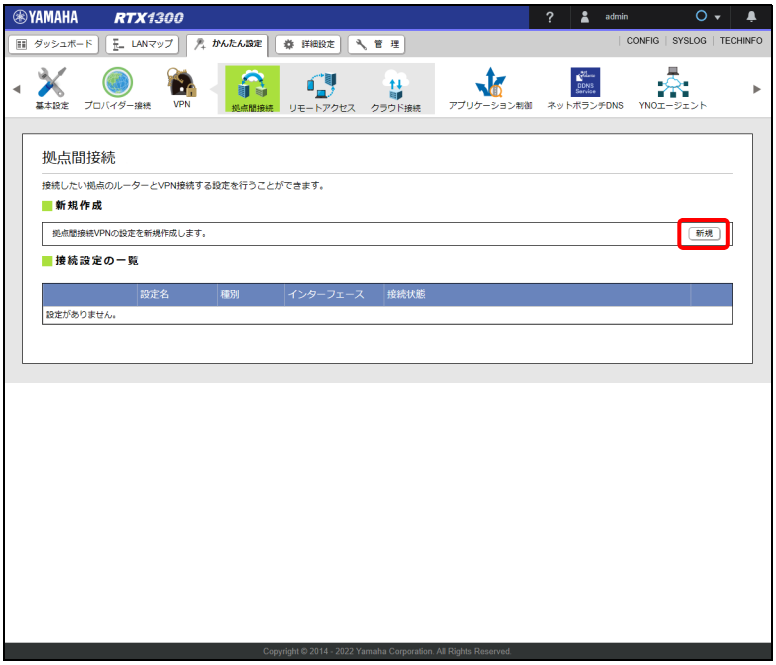
PPTP で拠点間を接続するために必要な設定と接続方法を説明します。PPTP で拠点間を接続するには、双方の拠点に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要になります。
本製品を PPTP サーバー /PPTP クライアントとして動作させるために必要な設定を行います。

メモ

本製品の PPTP の仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

1. **「かんたん設定」タブ ―「VPN」―「拠点間接続」ボタンを順に選択する。**
   「拠点間接続」画面が表示されます。

2. **「新規作成」項目の「新規」ボタンをクリックする。**

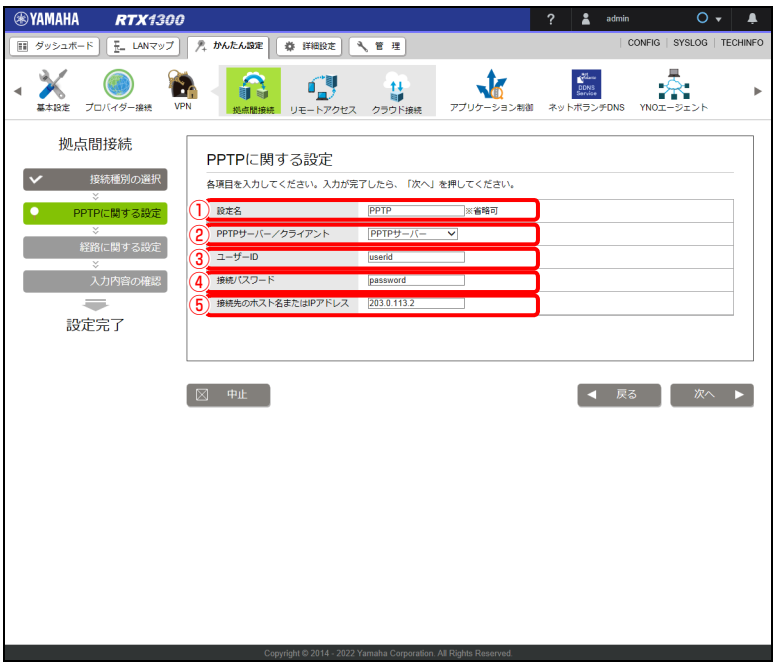


「接続種別の選択」画面が表示されます。

3. 「PPTP」を選択し、「次へ」ボタンをクリックする。

「PPTP に関する設定」画面が表示されます。

4. PPTP の接続情報を設定する。



① 設定名：
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② PPTP サーバー／クライアント：
自分側を VPN 接続のサーバー側にするかクライアント側にするかを選択します。

③ **ユーザー ID：**
VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。双方の拠点で同じユーザー ID を設定してください。

④ **接続パスワード：**
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。双方の拠点で同じパスワードを設定してください。

⑤ **接続先のホスト名または IP アドレス：**
接続先のネットボランチ DNS ホスト名または IP アドレスを入力します。

重要

接続する側を PPTP クライアント、接続される側を PPTP サーバーとして設定してください。

5. **「次へ」ボタンをクリックする。**
「経路に関する設定」画面が表示されます。

6. **接続先の LAN 側のネットワークアドレスを設定する。**

① **経路を設定しない：**
経路を設定しない場合に選択します。
本項目を選択した場合、本設定では通信をすることができません。別途、経路を設定する必要があります。本ページで再設定、または「詳細設定」タブ ―「ルーティング」をご覧ください。

メモ

「フィルターによる振り分け（フィルター型ルーティング）」、「重みに応じた負荷分散」、「バックアップ動作」などで運用したい場合、本設定を確定後、「詳細設定」タブ ―「ルーティング」をご覧ください。

② **接続先の LAN 側のアドレス：**
LAN 側のアドレスを指定する場合に選択します。

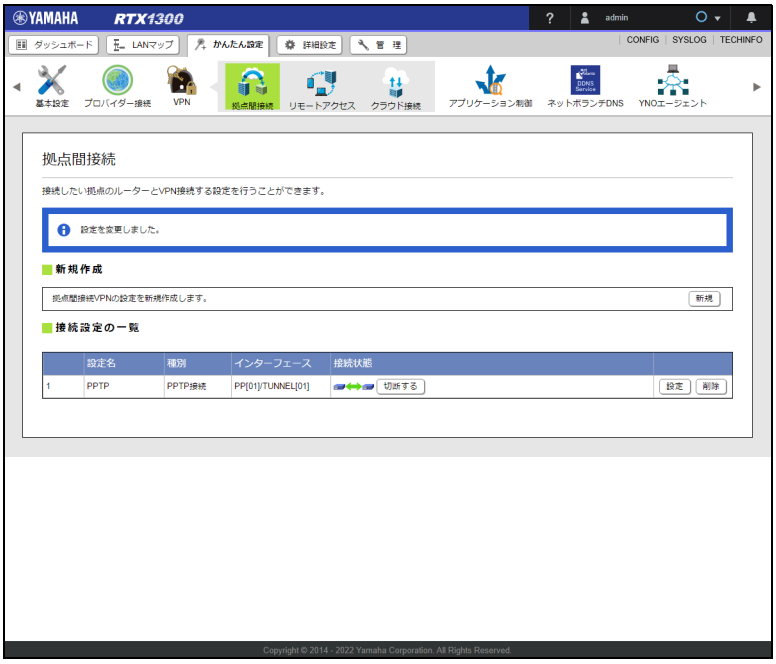
接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。
IP アドレスを追加する場合は、下部の「 ＋ 」ボタンを押してください。IP アドレスを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

③ デフォルト経路：
デフォルト経路を設定する場合に選択します。

7. 「次へ」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

8. 内容を確認し、「設定の確定」ボタンをクリックする。

設定が反映され、「拠点間接続」画面が表示されます。



双方の拠点で認証が成功すると、自動的に PPTP で拠点間が接続されます（特に操作は必要ありません）。PPTP 接続が完了すると、「拠点間接続」画面の「接続状態」の表示が  に切り替わります。「拠点間接続」画面の「接続する」または「切断する」ボタンをクリックすると、手動で拠点間接続を接続または切断できます。

自動的に PPTP で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。

- 接続先の IP アドレス / ネットボランチ DNS ホスト名が間違っている
- 接続先とユーザー ID/ 接続パスワードの設定が一致していない

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、「ユーザーガイド」（ウェブサイト）をご覧ください。

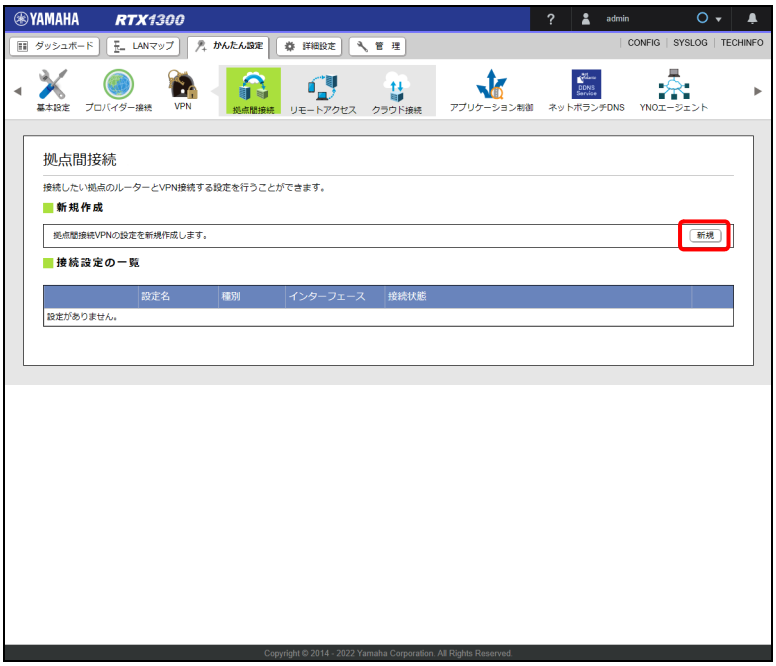
8.4 IPIP で接続する

IPIP で拠点間を接続するために必要な設定と接続方法を説明します。データは暗号化されないため、フレッツ網など機密性の高い閉域網が必要になります。

メモ

本製品の IPIP の仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

1. **「かんたん設定」タブ ―「VPN」―「拠点間接続」ボタンを順に選択する。**
   「拠点間接続」画面が表示されます。
2. **「新規作成」項目の「新規」ボタンをクリックする。**



「接続種別の選択」画面が表示されます。

3.「IPIP」を選択し、「次へ」ボタンをクリックする。

「IPIP に関する設定」画面が表示されます。

4. IPIP の接続情報を設定する。

① **設定名：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

② **接続先のホスト名または IP アドレス：**
接続先のホスト名、または IP アドレスを入力します。

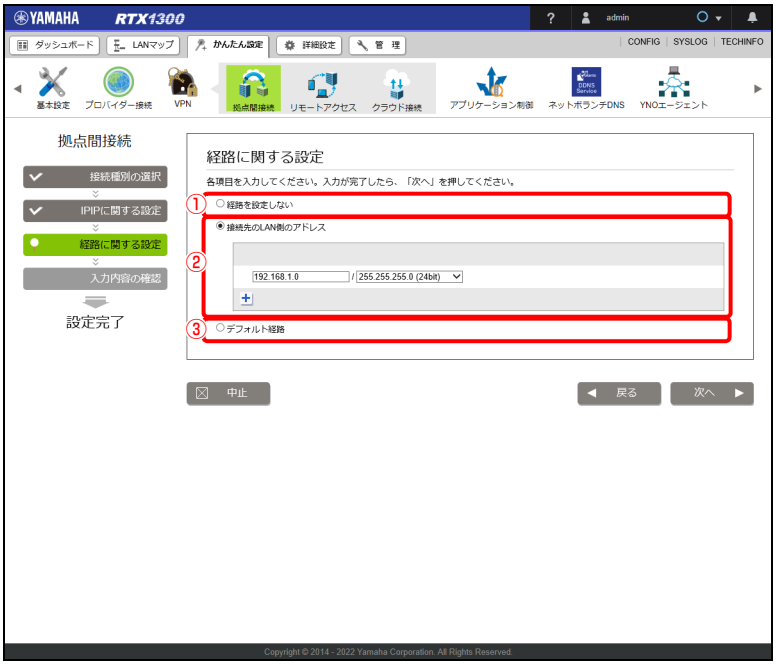
③ IPIP トンネルを使用するインターフェースの指定：
IPIP トンネルを使用するインターフェースを指定する場合は、「指定する」を選択し、使用するインターフェースを選択します。選択されたインターフェースに対して、IPIP トンネルによる通信に必要な IP フィルターと静的マスカレードの設定が追加されます。

注意
IPIP トンネルを使用するインターフェースを設定すると、本画面で IP フィルターと静的マスカレードの設定を変更することができなくなります。IP フィルターと静的マスカレードの設定を変更する場合は、「詳細設定」タブ ― 「セキュリティー」 ― 「IP フィルター」および「NAT」から行ってください。また、「かんたん設定」タブ ― 「VPN」 ― 「拠点間接続」のトップページから IPIP トンネルの設定をすべて削除すると、自動設定された IP フィルターと静的マスカレードの設定も一緒に削除されます。

④ IPIP キープアライブ：
IPIP キープアライブを使用するか否かを選択します。
「使用する」に設定すると、接続先から IPIP キープアライブの応答が返ってきた場合にのみトンネルを確立します。IPIP キープアライブ機能は、IPIP キープアライブが設定可能なヤマハルーター間でのみ使用できます。

5. 「次へ」ボタンをクリックする。
「経路に関する設定」画面が表示されます。

6. 接続先の LAN 側のネットワークアドレスを設定する。



① 経路を設定しない：
経路を設定しない場合に選択します。
本項目を選択した場合、本設定では通信をすることができません。別途、経路を設定する必要があります。本ページで再設定、または「詳細設定」タブ ― 「ルーティング」をご覧ください。

メモ

「フィルターによる振り分け（フィルター型ルーティング）」、「重みに応じた負荷分散」、「バックアップ動作」などで運用したい場合、本設定を確定後、「詳細設定」タブ ―「ルーティング」をご覧ください。

② 接続先の LAN 側のアドレス：

LAN 側のアドレスを指定する場合に選択します。

接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。

IP アドレスを追加する場合は、下部の「 ＋ 」ボタンを押してください。IP アドレスを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

③ デフォルト経路：

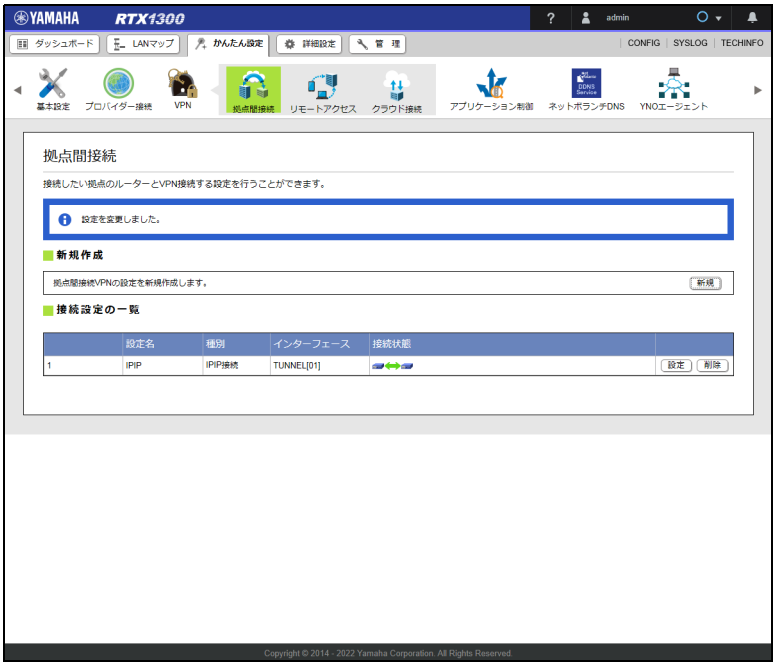
デフォルト経路を設定する場合に選択します。

7. **「次へ」ボタンをクリックする。**

「入力内容の確認」画面が表示されます。

8. **内容を確認し、「設定の確定」ボタンをクリックする。**

設定が反映され、「拠点間接続」画面が表示されます。



双方の拠点で認証が成功すると、自動的に IPIP で拠点間が接続されます（特に操作は必要ありません）。IPIP 接続が完了すると、「拠点間接続」画面の「接続状態」の表示が  に切り替わります。

自動的に IPIP で拠点間が接続されない場合は下記の可能性があります。設定を見直してください。

・ 接続先の IP アドレスが間違っている

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から ping コマンドを実行し、接続先の IP アドレスに到達できるか確認してください。到達できない場合は、双方の拠点でインターネット接続ができるか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、「ユーザーガイド」（ウェブサイト）をご覧ください。

8.5　データコネクトで接続する

フレッツ光のひかり電話の基本サービスであるデータコネクトを利用して拠点間を接続するために必要な設定と接続方法を説明します。

注意

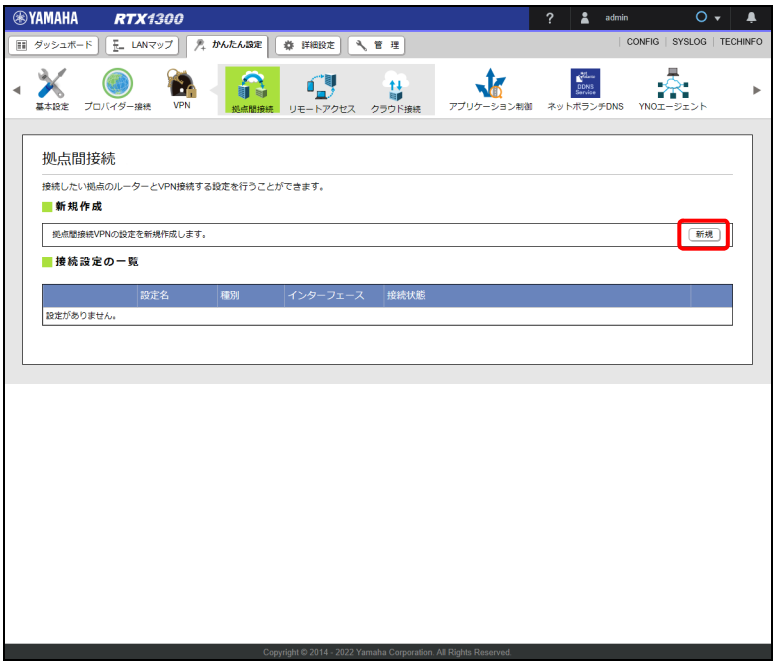
- データコネクトを用いて VPN を構築することにより、外部のネットワークとの帯域確保型データ通信が可能になります。この接続を使用する場合、フレッツ光のひかり電話およびナンバーディスプレイサービスが契約されている必要があります。
- データコネクトは利用帯域と接続時間によって課金額が決定される従量課金制のサービスです。長時間の接続や利用帯域を広く設定する場合には十分ご注意ください。

メモ

本製品のデータコネクトの仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

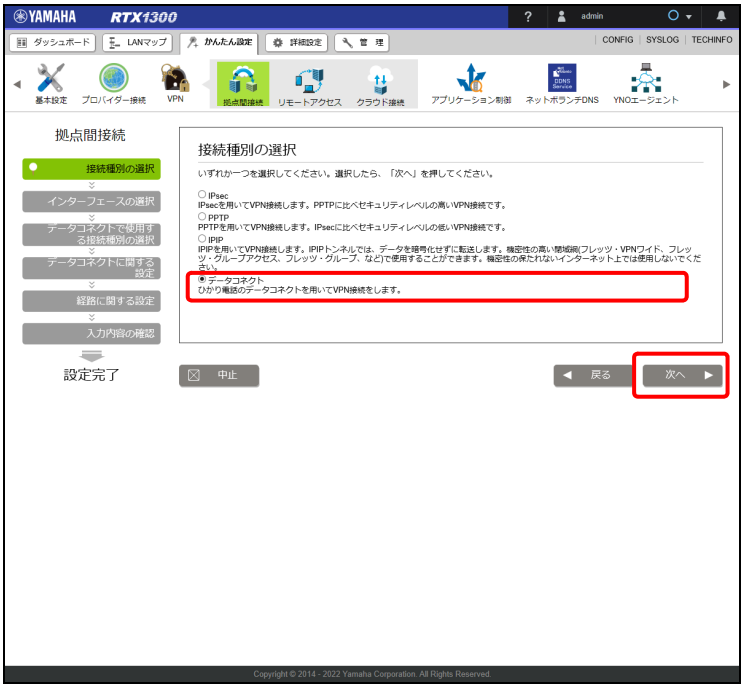
1. **「かんたん設定」タブ ―「VPN」―「拠点間接続」ボタンを順に選択する。**
   「拠点間接続」画面が表示されます。

2. **「新規作成」項目の「新規」ボタンをクリックする。**



「接続種別の選択」画面が表示されます。

3. 「データコネクト」を選択し、「次へ」ボタンをクリックする。



「インターフェースの選択」画面が表示されます。

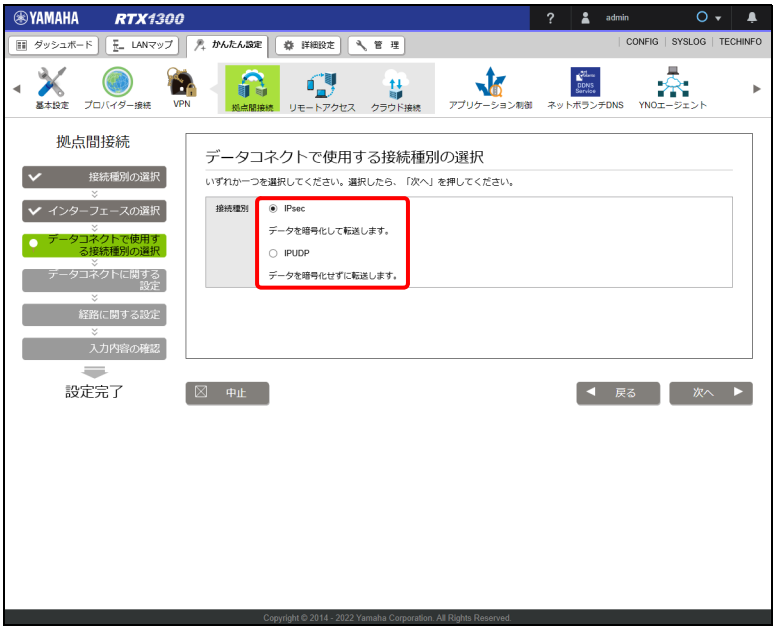
4. 使用するインターフェースを選択し、「次へ」ボタンをクリックする。

「データコネクトで使用する接続種別の選択」画面が表示されます。

重要

- IPv6 IPoE(DHCP) 接続を使用しているインターフェースがある場合、そのインターフェース以外は選択できません。
- DHCP または固定 IP アドレスを使用しているインターフェースがある場合、そのインターフェースは選択できません。

5. **接続種別の選択を設定する。**



① **接続種別：**
使用する接続種別を選択します。接続先と同じ接続種別を設定してください。
・ データを暗号化して転送する場合は「IPsec」を選択し、データを暗号化せずに転送する場合は「IPUDP」を選択します。

6. **「次へ」ボタンをクリックする。**
「データコネクト（IPsec）に関する設定」画面が表示されます。

7. **データコネクトの接続情報を設定する。**

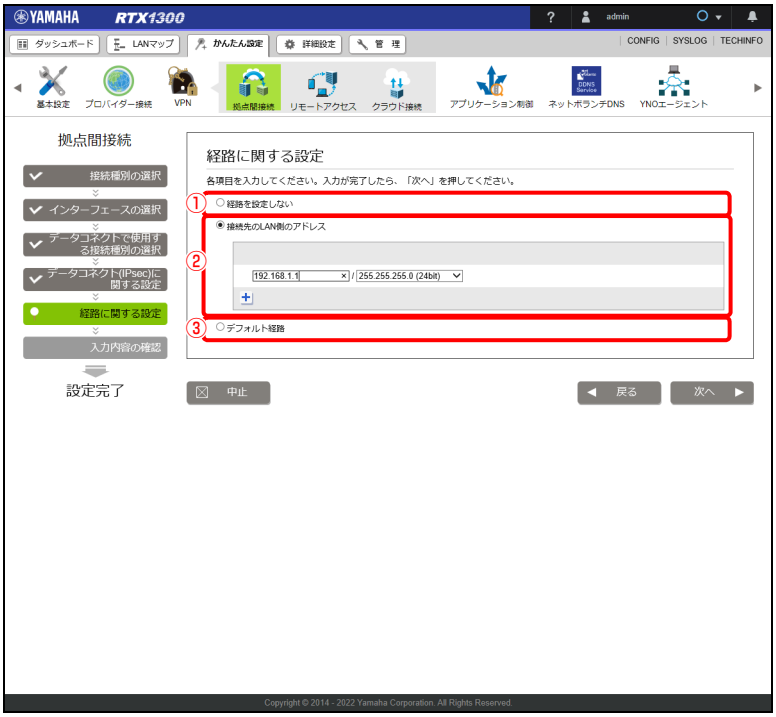
① **自分側の設定：**
本製品の設定を行います。
- 設定名：任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。
- 自分側のひかり電話番号：自分側のひかり電話番号を入力します。
- 使用する帯域：データコネクトで使用する帯域を選択します。

② **接続先の情報：**
接続先のひかり電話番号を入力します。

③ **接続先と合わせる設定：**
接続先と同じ値を設定します。
※ データコネクトで使用する「接続種別の選択」で「IPsec」を選択した場合にのみ表示されます。
- 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
- 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
- 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

8. **「次へ」ボタンをクリックする。**
「経路に関する設定」画面が表示されます。

9. **接続先の LAN 側のネットワークアドレスを設定する。**



① **経路を設定しない：**
経路を設定しない場合に選択します。
本項目を選択した場合、本設定では通信をすることができません。別途、経路を設定する必要があります。本ページで再設定、または「詳細設定」タブ ― 「ルーティング」をご覧ください。

メモ

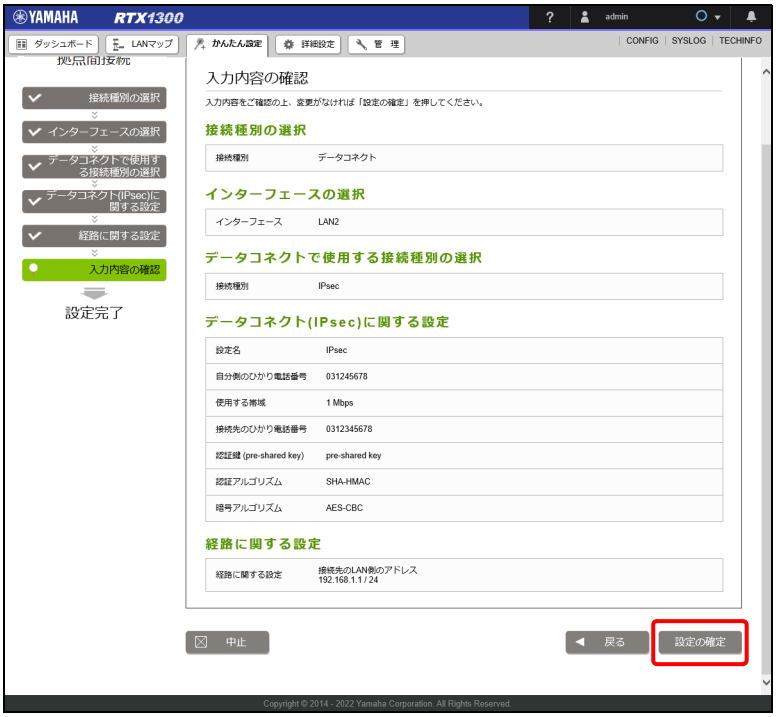
「フィルターによる振り分け（フィルター型ルーティング）」、「重みに応じた負荷分散」、「バックアップ動作」などで運用したい場合、本設定を確定後、「詳細設定」タブ ― 「ルーティング」をご覧ください。

② **接続先の LAN 側のアドレス：**
LAN 側のアドレスを指定する場合に選択します。
接続先の LAN 側のネットワークアドレスを入力します。双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。
IP アドレスを追加する場合は、下部の「 ＋ 」ボタンを押してください。IP アドレスを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

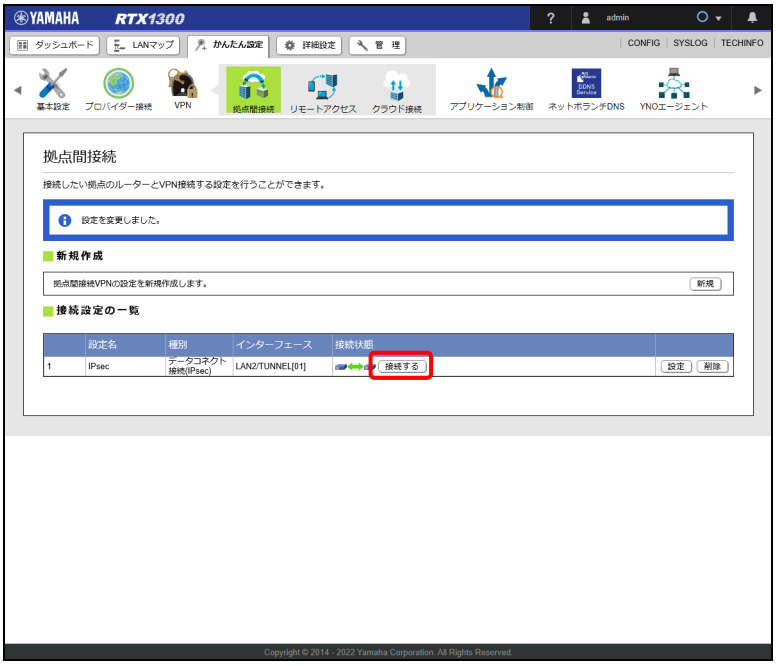
③ **デフォルト経路：**
デフォルト経路を設定する場合に選択します。

10.「次へ」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

11.内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「拠点間接続」画面が表示されます。



データコネクト接続を設定した後に「接続する」ボタンをクリック、または接続先の LAN 側アドレスに向かって通信を発生させることで接続が開始されます。
「拠点間接続」画面の「接続状態」の表示が  に切り替わることを確認してください。

重要

データコネクト接続は、自動的に通信を開始しません。「接続する」ボタンをクリックしてください。
「接続する」ボタンを押した時点で課金が開始されます。

メモ

「接続する」ボタンをクリック後、一定時間（初期値：60 秒）通信が無いと、データコネクト接続を自動的に切断します。

設定を見直しても接続されない場合は、ルーターのシリアルコンソール画面または TELNET コンソール画面から show status ngn コマンドを実行し、起動 OK と表示されるか確認してください。起動 OK 以外が表示される場合は、ケーブルが正しく繋がれているか確認してください。シリアルコンソール画面または TELNET コンソール画面へのログイン方法について詳しくは、「ユーザーガイド」（ウェブサイト）をご覧ください。

第 9 章　外部から VPN 経由で LAN へアクセスする

本章では、仮想プライベートネットワーク（VPN）を構築して、外出先から LAN へリモートアクセスする方法について説明します。
外部の端末から VPN 経由で本製品にリモートアクセスするには、本製品にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。グローバル IP アドレスとは、下記（プライベート IP アドレス）以外の IP アドレスです。
— 10.0.0.0 ～ 10.255.255.255
— 172.16.0.0 ～ 172.31.255.255
— 192.168.0.0 ～ 192.168.255.255

LAN 内のサーバーまたはパソコンの設定をする …95 ページ
L2TP/IPsec でリモートアクセスする …95 ページ
PPTP でリモートアクセスする …104 ページ

注意

リモートアクセスを利用するときは、データを保全するために十分なセキュリティー設定を行ってください。セキュリティー設定が不十分な場合は、LAN に接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などにあう可能性があります。

重要

- VPN の設定はインターネットに接続した状態で行う必要があるため、VPN を利用したリモートアクセスの設定の前にインターネット接続の設定が必要です。
- 外部の端末から VPN 経由で本製品にリモートアクセスするには、本製品にプロバイダーからグローバル IP アドレスが割り当てられている必要があります。

メモ

- Windows でファイル共有をする場合は、NetBIOS over TCP/IP プロトコルを使用するか、または WINS サーバーを用意する必要があります。
- macOS でファイル共有をする場合は、ファイル環境設定の「共有」で「ファイル共有」をオンにします。

ネットボランチ DNS ホスト名とは

ネットボランチ DNS サービスにより取得できる固定のホスト名です。ネットボランチ DNS ホスト名は、本製品のグローバル IP アドレスと結びつけられます。
インターネットに常時接続している場合でも、割り当てられるグローバル IP アドレスは再接続時または一定時間経過時に変更されることがあります。グローバル IP アドレスが変更されると IP アドレスがネットボランチ DNS サーバーへ通知され、ネットボランチ DNS ホスト名に結びつけられた IP アドレスが更新されます。
ネットボランチ DNS ホスト名の取得について詳しくは「第 7 章 ネットボランチ DNS サービスを利用する」（65 ページ）をご覧ください。

9.1 LAN 内のサーバーまたはパソコンの設定をする

リモートアクセスするには、LAN 内のサーバーやパソコンに TCP/IP プロトコルでアクセスできるようにするための設定が必要です。

ファイルサーバーソフトの設定を変更する
公開するサーバーまたはパソコンにファイルサーバーソフトやネットワーク共有を設定して、公開するフォルダーやユーザー ID、パスワードを設定します。

9.2 L2TP/IPsec でリモートアクセスする

パソコンやスマートフォンなどから L2TP/IPsec を利用してリモートアクセスを行うことができます。
本節では YMS-VPN8 をインストールしたパソコンからアクセスする場合を例に説明します。

接続先のルーター側の設定：9.2.1 本製品の設定（L2TP/IPsec）をする（95 ページ）
接続元のパソコン側の設定：9.2.3 YMS-VPN8 の設定をする（101 ページ）

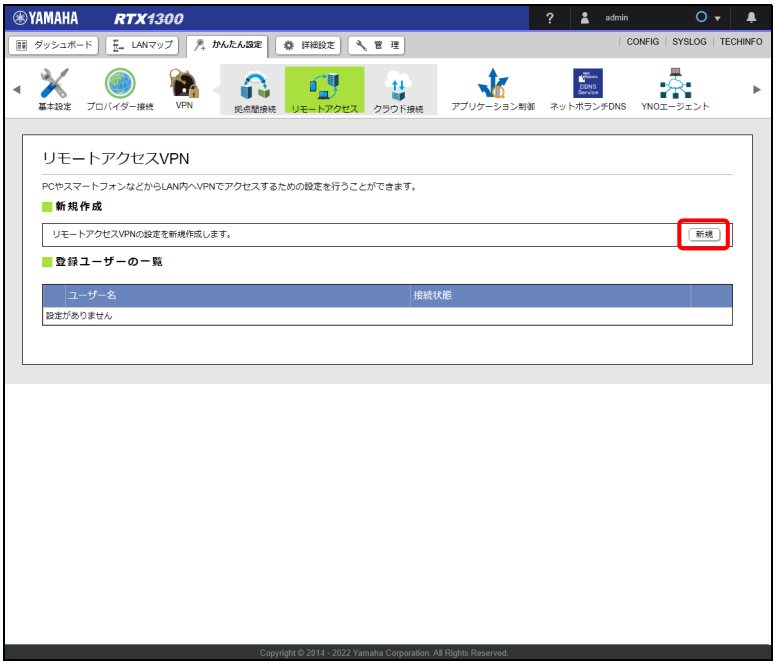
メモ
- YMS-VPN8 について詳しくは、YMS-VPN8 の取扱説明書をご覧ください。
- スマートフォンなど他のクライアントの設定方法はヤマハネットワーク周辺機器技術情報ページをご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/l2tp_ipsec/

9.2.1 本製品の設定（L2TP/IPsec）をする

重要
本製品の WAN 側または PP 側に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要です。

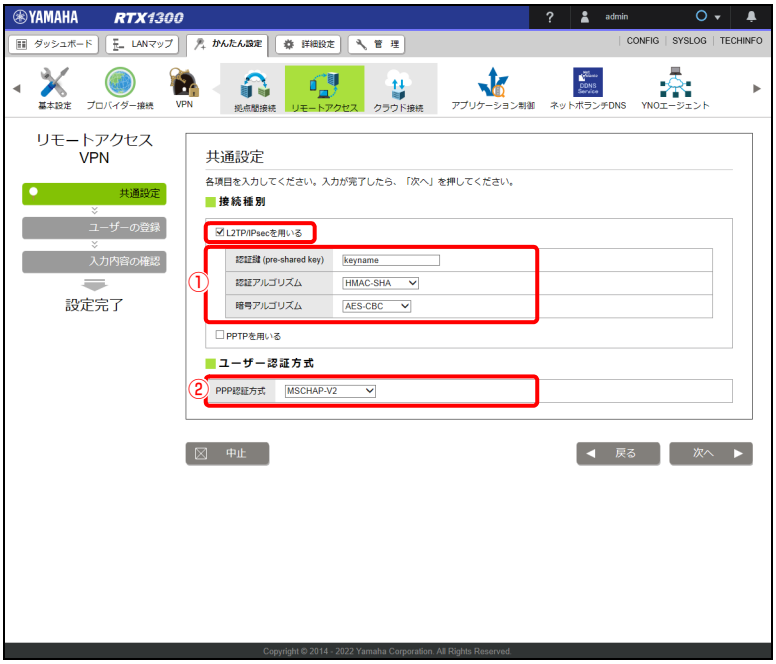
1. **「かんたん設定」タブ ― 「VPN」 ― 「リモートアクセス」ボタンを順に選択する。**
   「リモートアクセス VPN」画面が表示されます。

2.「新規作成」項目の「新規」ボタンをクリックする。



「共通設定」画面が表示されます。

3.「L2TP/IPsec を用いる」にチェックを入れ、VPN の接続情報を設定する。



① 接続種別：

・ 認証鍵（pre-shared key）：データの暗号化に使用する事前共有鍵を入力します。
・ 認証アルゴリズム：認証に使用するアルゴリズムを設定します。
・ 暗号アルゴリズム：暗号化に使用するアルゴリズムを設定します。

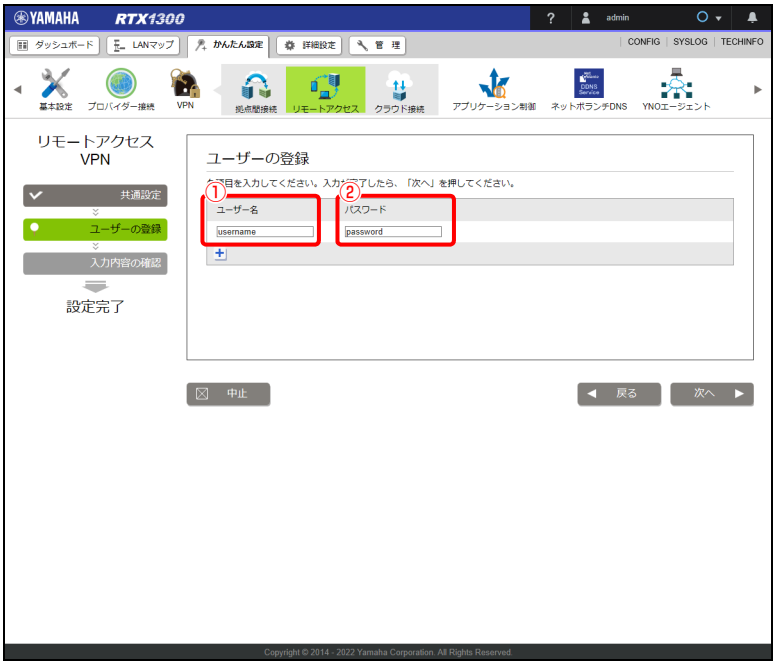
② **ユーザー認証方式：**

・ PPP 認証方式：VPN 接続を行うユーザーの認証方式を設定します。

4. **「次へ」ボタンをクリックする。**

「ユーザーの登録」画面が表示されます。

5. **リモートアクセスするユーザー情報を設定する。**



① **ユーザー名：**

VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

② **パスワード：**

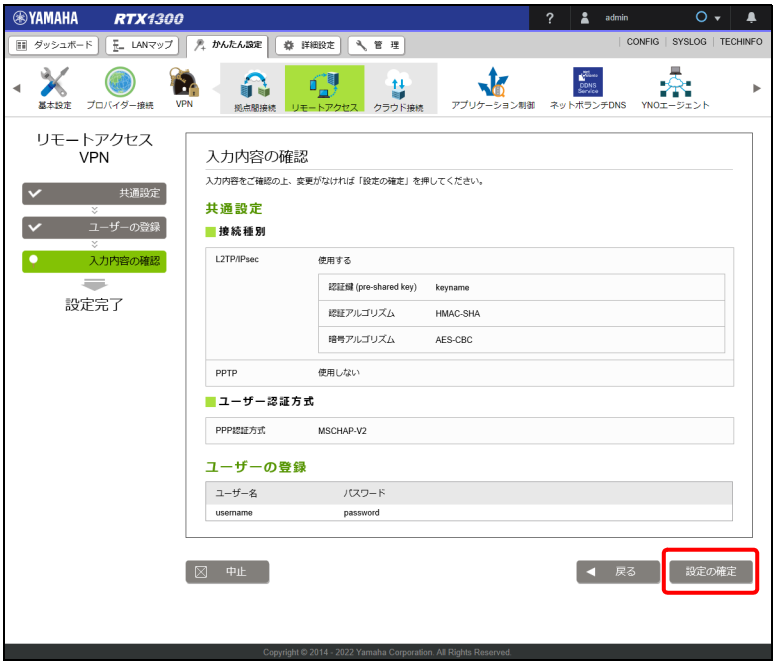
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

ユーザーを複数登録する場合は、「＋」ボタンをクリックしてください。

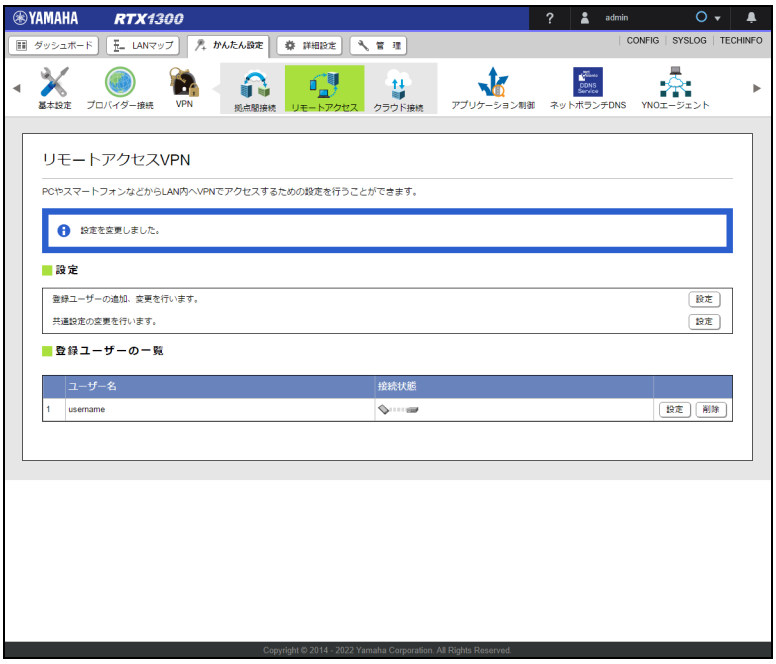
6. **「次へ」ボタンをクリックする。**

「入力内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。

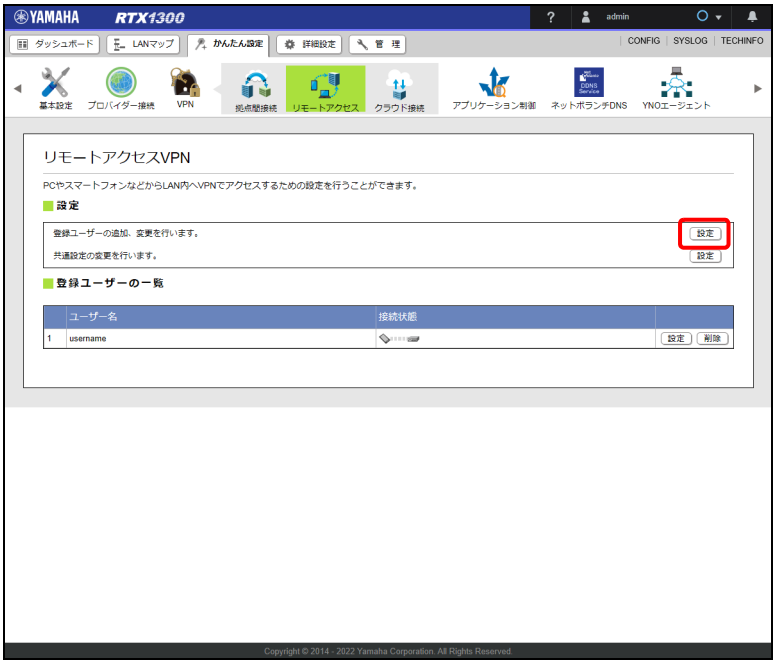


設定が反映され、「リモートアクセス VPN」画面が表示されます。



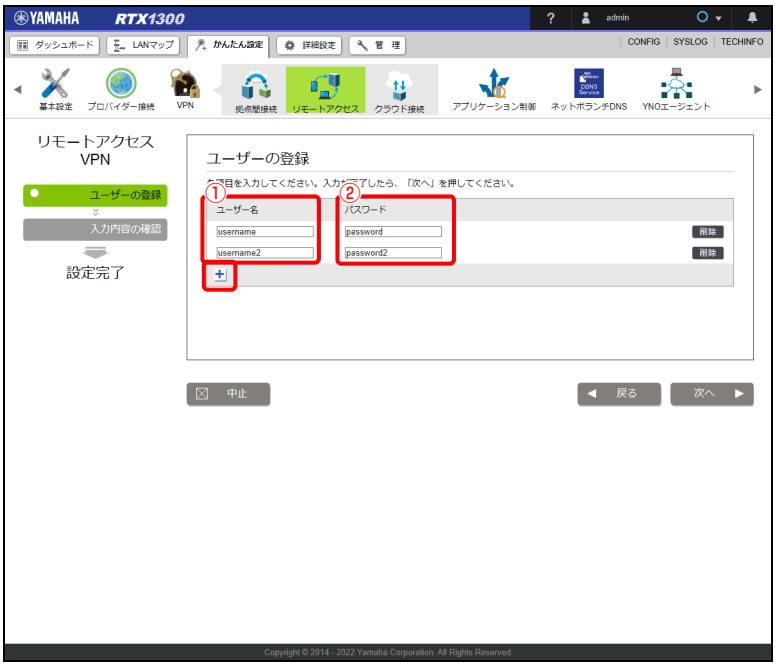
9.2.2 接続ユーザーを追加する

1. 「リモートアクセス VPN」画面で、「登録ユーザーの追加、変更を行います。」欄の「設定」ボタンをクリックする。



「ユーザーの登録」画面が表示されます。

2. 「＋」ボタンをクリックし、リモートアクセスするユーザー情報を設定する。

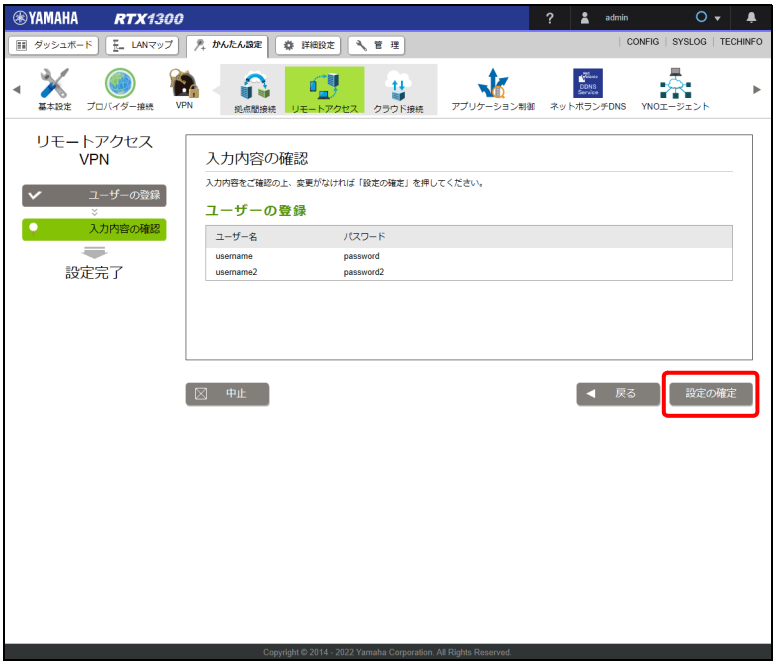


① **ユーザー名：**
VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

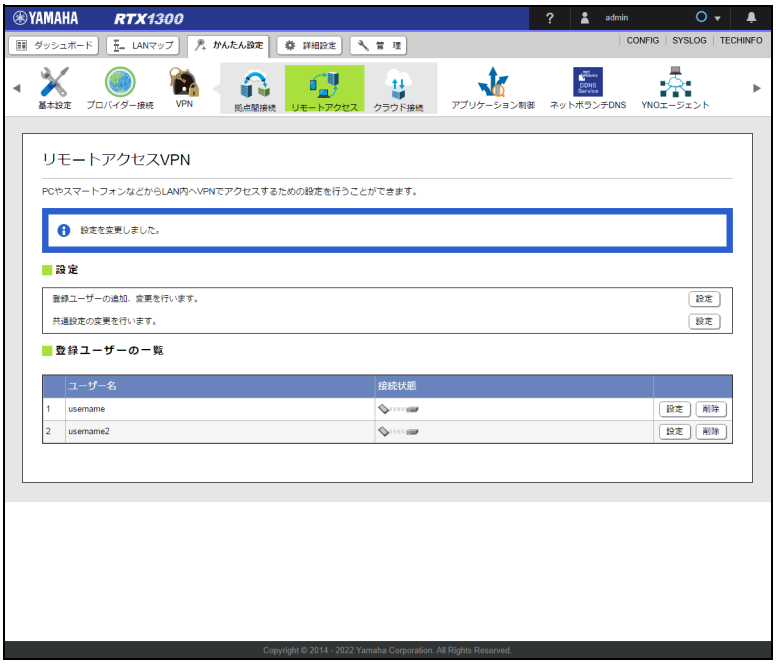
② **パスワード：**
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

3. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

4. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「リモートアクセス VPN」画面が表示されます。



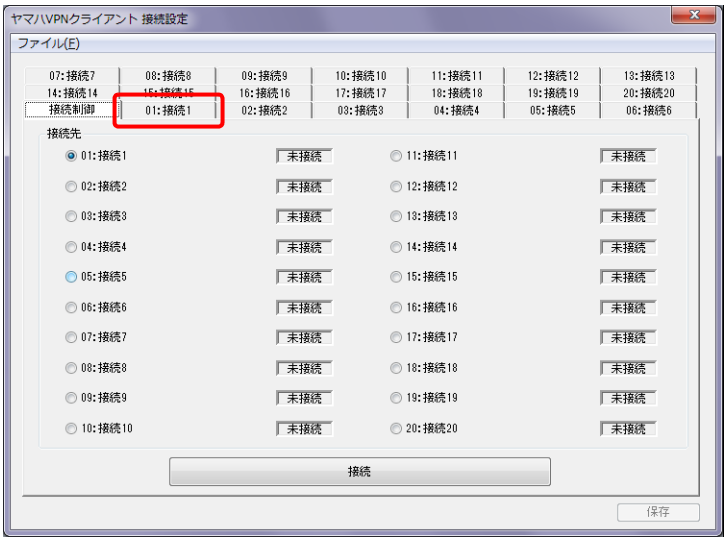
9.2.3 YMS-VPN8 の設定をする

1. **「スタート」メニューから「すべてのプログラム」—「YMS-VPN8」—「接続設定」を順に選択する。**
   YMS-VPN8 が起動して、「接続設定」画面が表示されます。

メモ

YMS-VPN8 が Windows のタスクトレイに常駐している場合は、「スタート」メニューから起動しても YMS-VPN8 の「接続設定」画面が表示されません。その場合は Windows のタスクトレイから YMS-VPN8 を起動してください。

2. **設定が登録されていないタブをクリックする。**

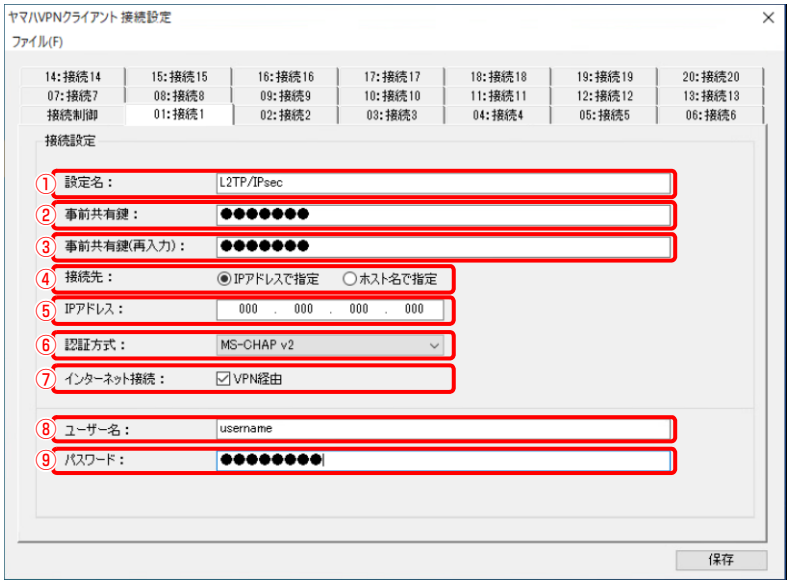


メモ

- 接続先は 20 件まで登録できます。
- すでに登録した接続先の内容を変更したい場合は、変更したい接続先のタブをクリックします。

接続先の登録画面が表示されます。

3. **VPN の接続情報を設定する。**



① 設定名：
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。
設定を保存すると、入力した設定名はタブに反映されます（タブ内に設定名が表示しきれない場合は、一部省略して表示されます）。

② 事前共有鍵：
「9.2.1 本製品の設定（L2TP/IPsec）をする」で設定した認証鍵（pre-shared key）を入力します。
入力した事前共有鍵は文字が「●」で表示されます。

③ 事前共有鍵（再入力）：
「事前共有鍵」欄と同一の事前共有鍵を入力します。
入力した事前共有鍵は文字が「●」で表示されます。

④ 接続先：
「IP アドレスで指定」または「ホスト名で指定」のどちらかを選択します。

⑤ IP アドレス：
「接続先」欄で「IP アドレスで指定」を選んだ場合は、本製品の WAN 側または PP 側の IP アドレスを入力します。
「ホスト名で指定」を選んだ場合は、「ホスト名」欄に本製品のネットボランチ DNS ホスト名を入力します。

⑥ 認証方式：
「9.2.1 本製品の設定（L2TP/IPsec）をする」で設定した PPP 認証方式を選択します。

⑦ インターネット接続：
VPN 接続先以外への通信を VPN 経由で行うかどうかを指定します。VPN 経由で通信を行う場合はチェックボックスにチェックを入れます。

⑧ ユーザー名：
「9.2.1 本製品の設定（L2TP/IPsec）をする」で設定したユーザー名を入力します。

⑨ パスワード：
「9.2.1 本製品の設定（L2TP/IPsec）をする」で設定したパスワードを入力します。

4. **「保存」ボタンをクリックする。**
設定内容が保存されます。

注意

「保存」ボタンをクリックせずに他のタブで操作を続行した場合、設定内容が失われてしまいます。
設定が終わったら、必ず「保存」ボタンをクリックしてください。

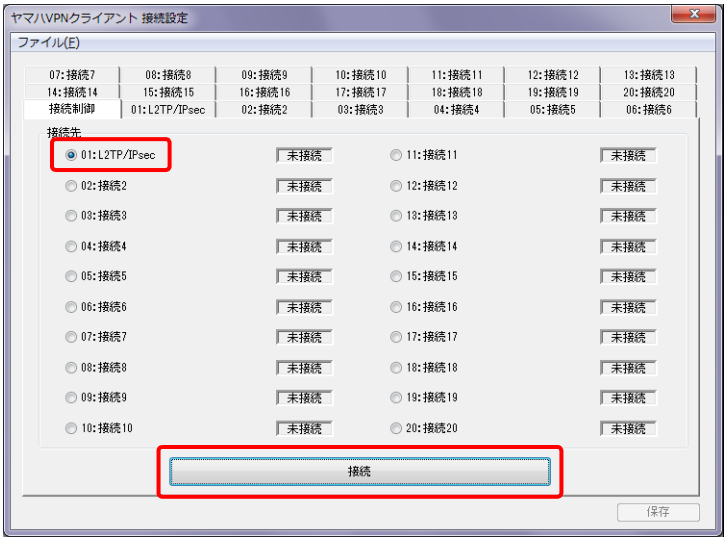
9.2.4 YMS-VPN8 から本製品へリモートアクセスする

1. **「スタート」メニューから「すべてのプログラム」—「YMS-VPN8」—「接続設定」を順に選択する。**
   YMS-VPN8 が起動して、「接続設定」画面が表示されます。

メモ

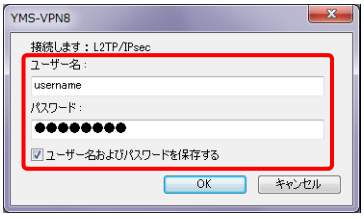
YMS-VPN8 が Windows のタスクトレイに常駐している場合は、「スタート」メニューから起動しても YMS-VPN8 の「接続設定」画面が表示されません。その場合は Windows のタスクトレイから YMS-VPN8 を起動してください。

2. **「接続制御」タブをクリックする。**
3. **設定した接続先を選び、「接続」ボタンをクリックする。**



接続時にユーザー名とパスワードの入力画面が表示されます。

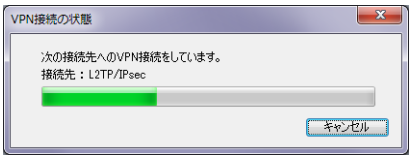
4. **「9.2.1 本製品の設定（L2TP/IPsec）をする」で設定したユーザー名とパスワードを入力する。**



メモ

ユーザー名とパスワードは接続設定で入力した設定を初期値として表示します。
接続設定でユーザー名とパスワードを事前に設定しておくことで、VPN 接続時は「OK」ボタンをクリックするだけで接続できます。

5. **「OK」ボタンをクリックする。**
   接続中は、「VPN 接続の状態」画面が表示されます。



   選んだ接続先に VPN 接続を開始します。

リモートアクセスを切断する場合は
「接続設定」画面の「接続制御」タブで、「切断」ボタンをクリックします。

9.3　PPTP でリモートアクセスする

パソコンやスマートフォンなどから PPTP を利用してリモートアクセスを行うことができます。
本節では Windows OS に標準搭載されている PPTP 接続機能を利用してアクセスする場合を例に説明します。

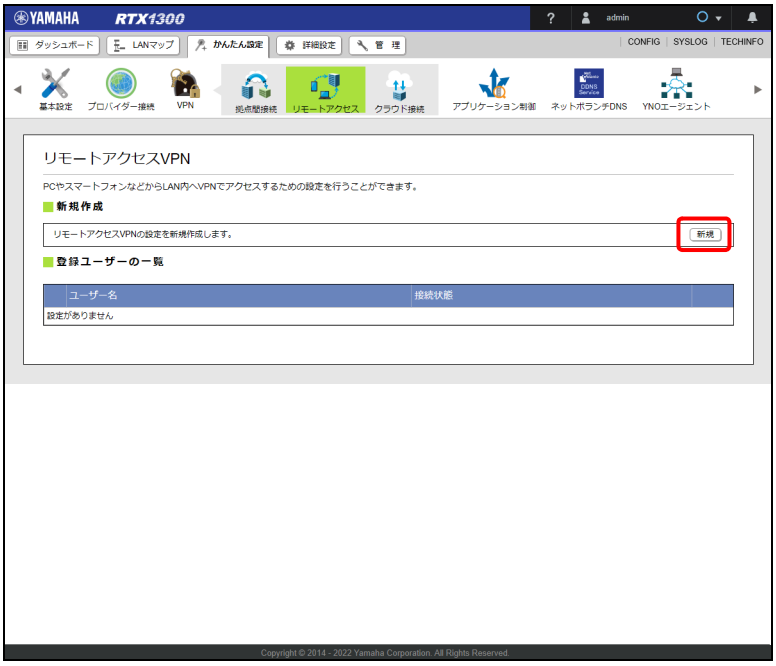
接続先のルーター側の設定：9.3.1 本製品の設定（PPTP）をする …104 ページ
接続元のパソコン側の設定：9.3.3 Windows 8.1 でリモートアクセスする …110 ページ
9.3.4 Windows 10 / Windows 11 でリモートアクセスする …114 ページ

9.3.1　本製品の設定（PPTP）をする

重要
本製品の WAN 側または PP 側に固定グローバル IP アドレスまたはネットボランチ DNS ホスト名が必要です。

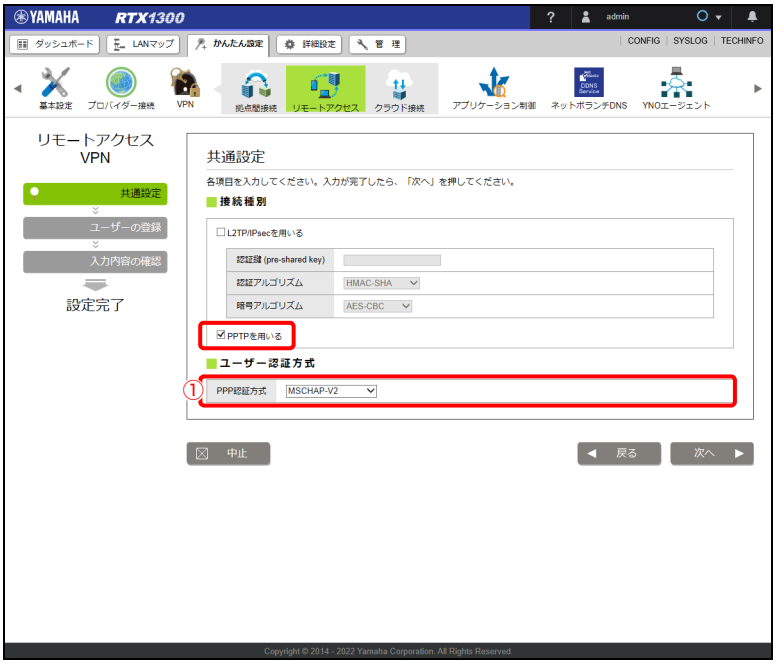
1. **「かんたん設定」タブ ―「VPN」―「リモートアクセス」ボタンを順に選択する。**
   「リモートアクセス VPN」画面が表示されます。

2.「新規作成」項目の「新規」ボタンをクリックする。



「共通設定」画面が表示されます。

3.「PPTP を用いる」にチェックを入れ、VPN の接続情報を設定する。



① ユーザー認証方式：

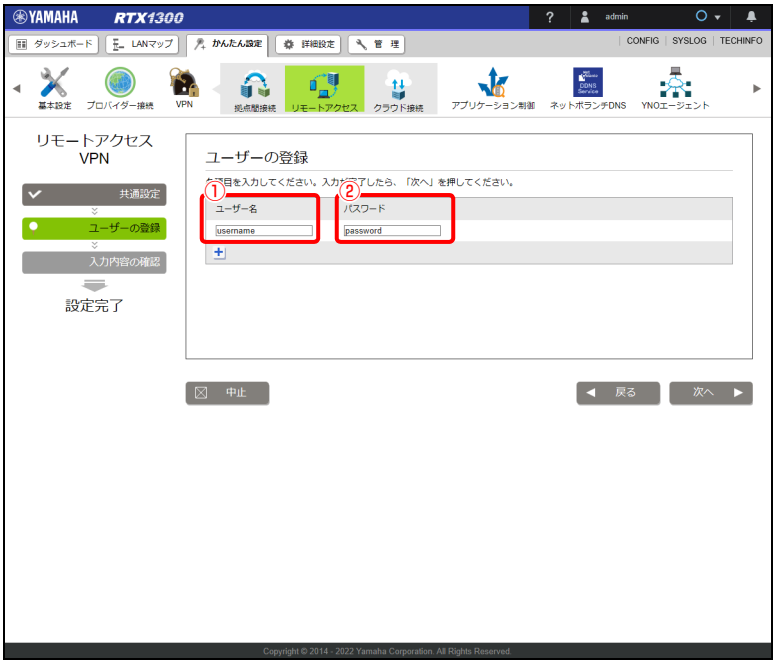
PPP 認証方式：VPN 接続を行うユーザーの認証方式を設定します。

重要

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1（MS-CHAP）はサポートされていません。Windows Vista 以降の Windows OS からリモートアクセスする場合は、「MS-CHAP-V2」を選択してください。

4. **「次へ」ボタンをクリックする。**
「ユーザーの登録」画面が表示されます。

5. **リモートアクセスするユーザー情報を設定する。**



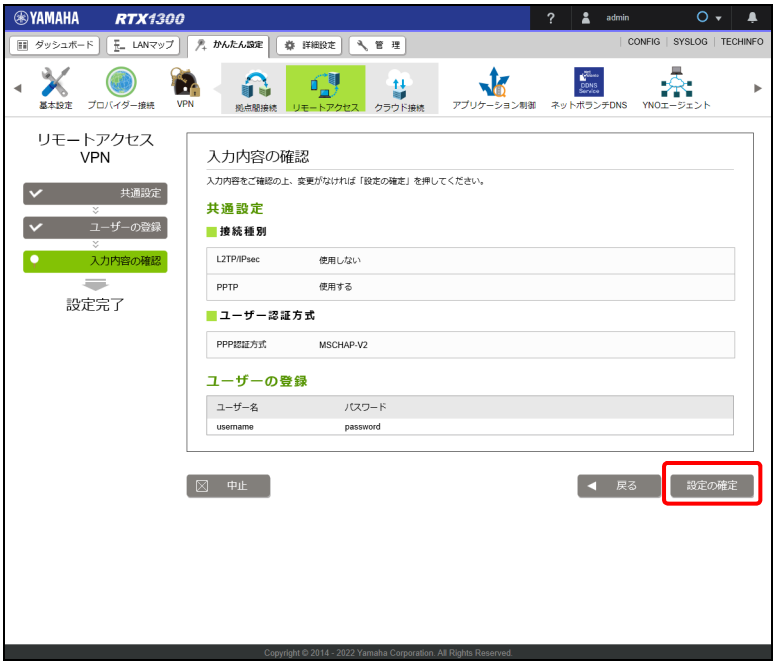
① ユーザー名：
VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

② パスワード：
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

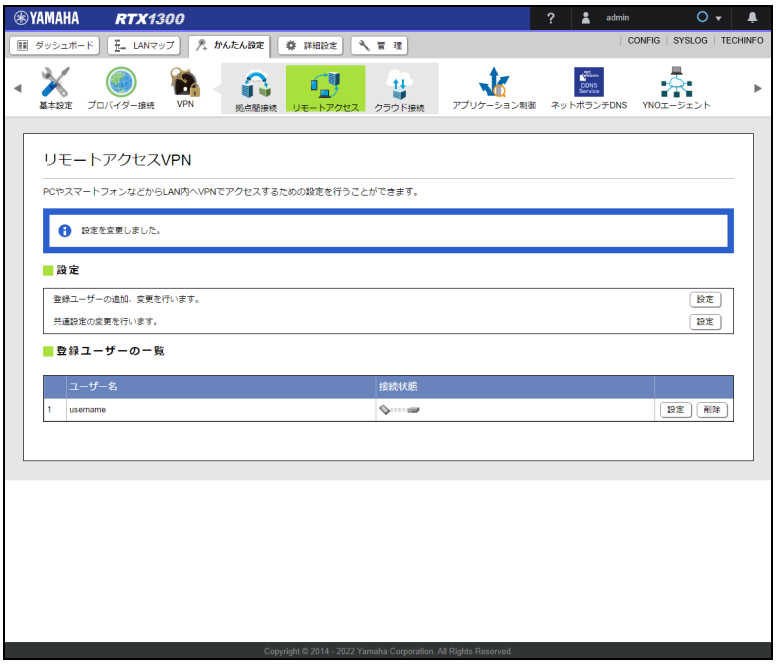
ユーザーを複数登録する場合は、「＋」ボタンをクリックしてください。

6. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。

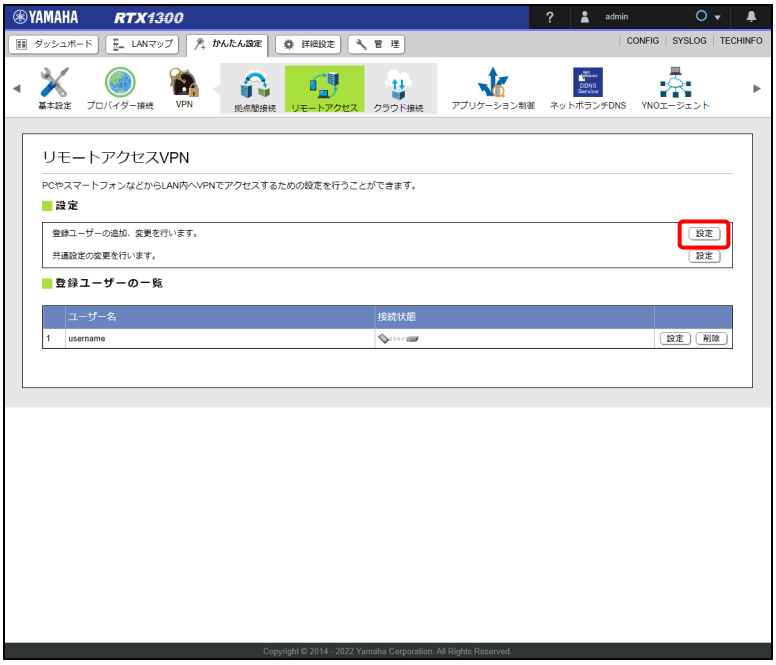


設定が反映され、「リモートアクセス VPN」画面が表示されます。



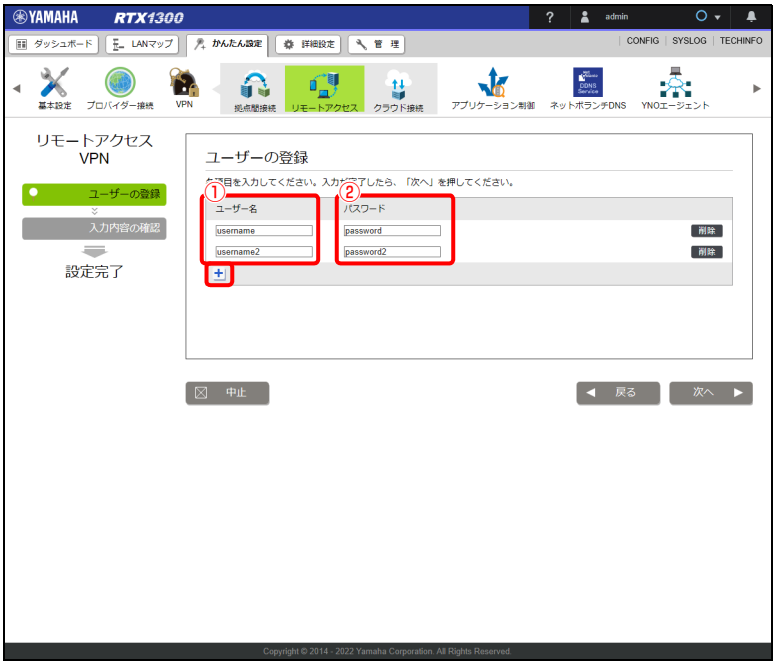
9.3.2 接続ユーザーを追加する

1. 「リモートアクセス VPN」画面で、「登録ユーザーの追加、変更を行います。」欄の「設定」ボタンをクリックする。



「ユーザーの登録」画面が表示されます。

2. 「 ＋ 」ボタンをクリックし、リモートアクセスするユーザー情報を設定する。

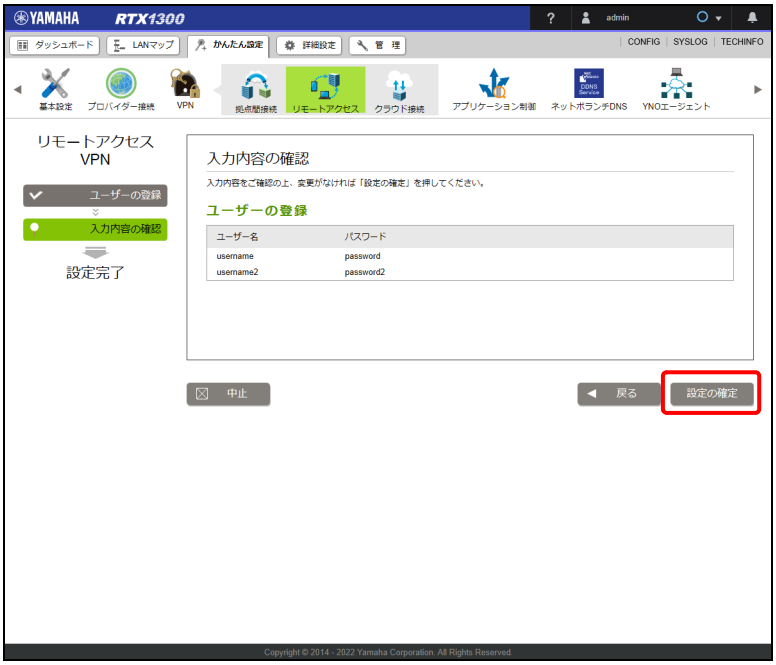


① ユーザー名：
VPN 接続を行う際のユーザー認証で使用するユーザー ID を入力します。

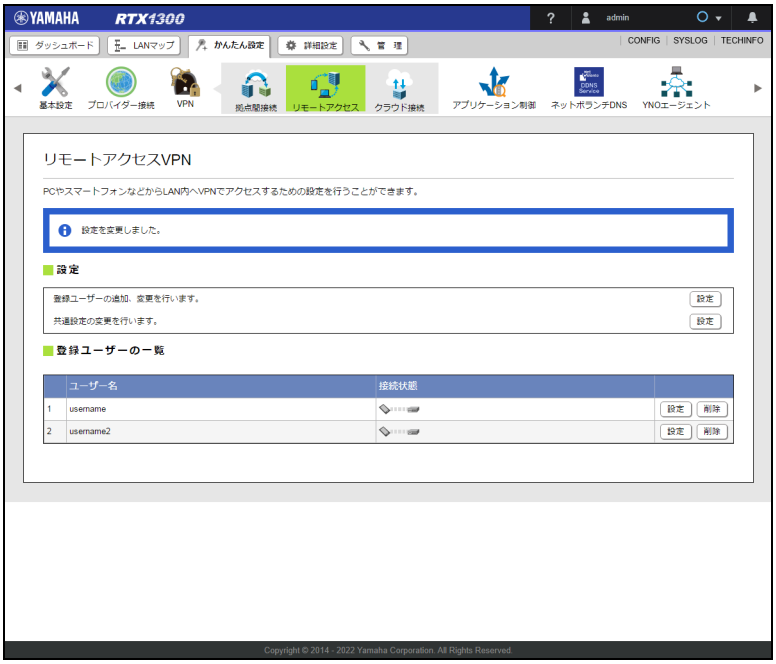
② **パスワード：**
VPN 接続を行う際のユーザー認証で使用するパスワードを入力します。

3. **「次へ」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

4. **内容を確認し、「設定の確定」ボタンをクリックする。**



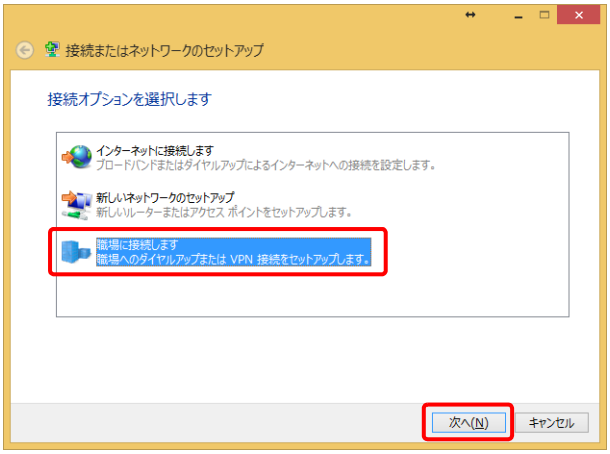
設定が反映され、「リモートアクセス VPN」画面が表示されます。



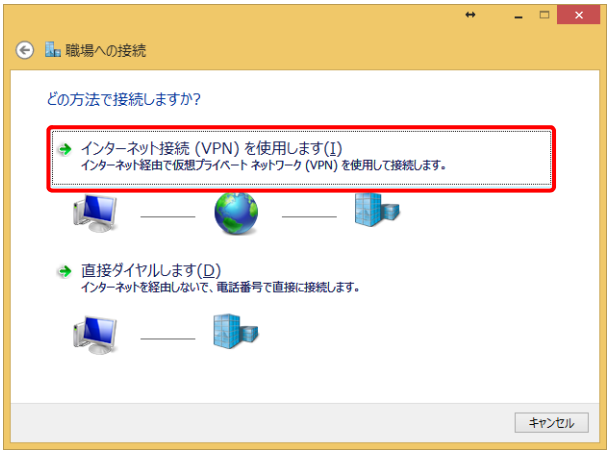
9.3.3 Windows 8.1 でリモートアクセスする

VPN の接続設定をする

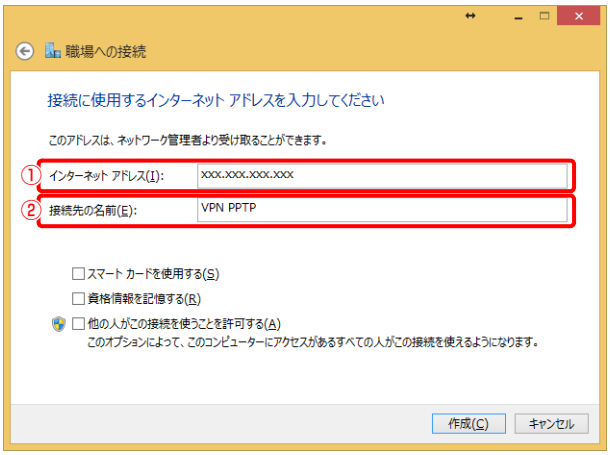
1. 「デスクトップ」画面で、マウスカーソルを右上隅または右下隅に移動する。
2. チャームから「設定」―「コントロールパネル」―「ネットワークの状態とタスクの表示」の順に選択する。
   「ネットワークと共有センター」画面が表示されます。
3. 「新しい接続またはネットワークのセットアップ」をクリックする。
4. 「職場に接続します」を選択し、「次へ」ボタンをクリックする。



5. 「インターネット接続（VPN）を使用します」をクリックする。



6. VPN の接続情報を設定する。



① **インターネットアドレス：**
本製品のネットボランチ DNS ホスト名、もしくは、WAN 側または PP 側の IP アドレスを入力します。

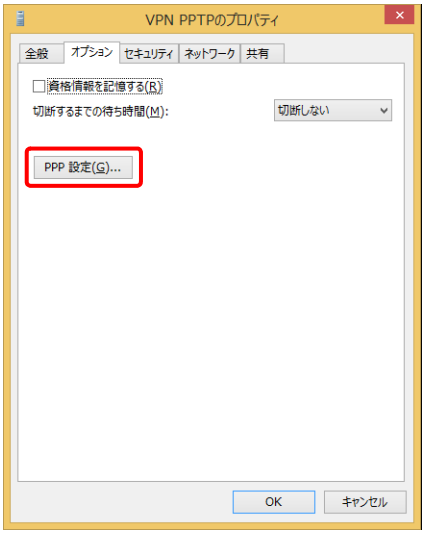
② **接続先の名前：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

7. 「作成」ボタンをクリックする。
設定内容が保存されます。

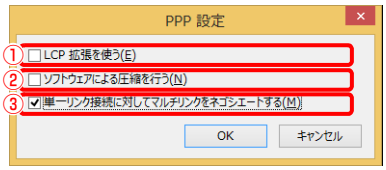
8. 「ネットワークと共有センター」画面で「アダプターの設定の変更」をクリックする。

9. 作成した VPN の接続設定を右クリックし、「プロパティ」を選択する。

10.「オプション」タブを選択し、「PPP 設定」ボタンをクリックする。



11.PPP 設定を変更する。



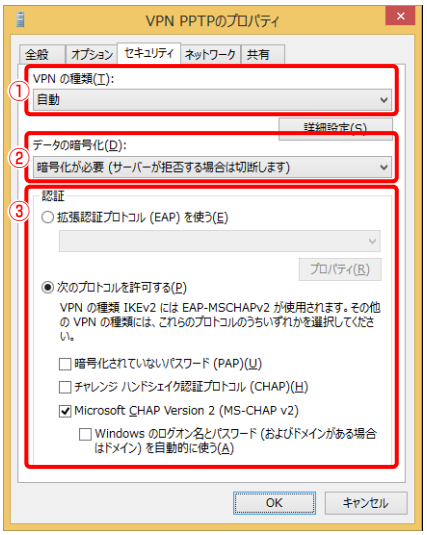
① **LCP 拡張を使う：**
チェックボックスのチェックを外します。

② **ソフトウェアによる圧縮を行う：**
チェックボックスのチェックを外します。

③ **単一リンク接続に対してマルチリンクをネゴシエートする：**
チェックボックスにチェックを付けます。

12.「OK」ボタンをクリックし、「セキュリティ」タブを選択する。

13.セキュリティー設定を変更する。



① **VPN の種類：**
「自動」を選択します。

② **データの暗号化：**
「暗号化が必要（サーバーが拒否する場合は切断します）」を選択します。

③ **認証：**
「次のプロトコルを許可する」を選択し、以下のように設定します。
- 暗号化されていないパスワード（PAP）：チェックボックスのチェックを外す。
- チャレンジハンドシェイク認証プロトコル（CHAP）：チェックボックスのチェックを外す。
- Microsoft CHAP Version 2（MS-CHAPv2）：チェックボックスにチェックを入れる。
- Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う：チェックボックスのチェックを外す。

重要

Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1（MS-CHAP）はサポートされていません。「9.3.1 本製品の設定（PPTP）をする」の手順 4 で「MSCHAP-V2」を選択してください。

14.「OK」ボタンをクリックする。

本製品へリモートアクセスする

1. マウスカーソルを右上隅または右下隅に移動する。
2. チャームから「設定」―「ネットワーク」の順に選択する。
3. 作成した VPN の接続設定を選択し、「接続」ボタンをクリックする。

4. 「9.3.1 本製品の設定（PPTP）をする」で設定したユーザー名とパスワードを入力し、「OK」ボタンをクリックする。
   本製品への VPN 接続を開始します。

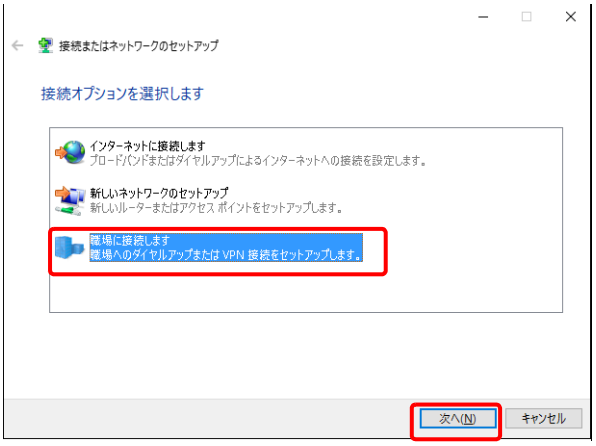
リモートアクセスを切断する場合は

「切断」ボタンをクリックします。

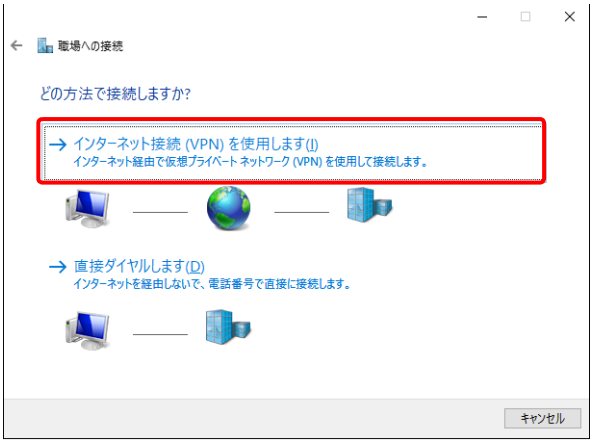
9.3.4 Windows 10 / Windows 11 でリモートアクセスする

VPN の接続設定をする

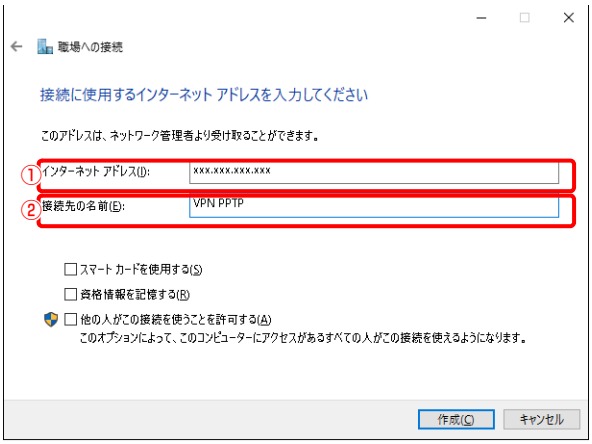
1. **「スタート」メニューから「コントロールパネル」を選択する。**
2. **画面右上の「表示方法」を「大きいアイコン」に変更する。**
   「すべてのコントロールパネル項目」画面が表示されます。
3. **「ネットワークと共有センター」をクリックする。**
   「ネットワークと共有センター」画面が表示されます。
4. **「新しい接続またはネットワークのセットアップ」をクリックする。**
5. **「職場に接続します」を選択し、「次へ」ボタンをクリックする。**



6. **「インターネット接続（VPN）を使用します」をクリックする。**



7. VPN の接続情報を設定する。



① **インターネットアドレス：**
本製品のネットボランチ DNS ホスト名、もしくは、WAN 側または PP 側の IP アドレスを入力します。

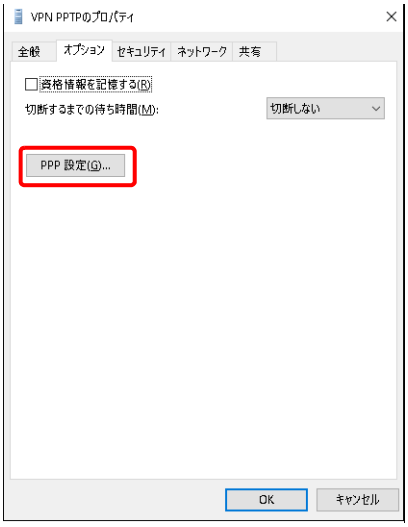
② **接続先の名前：**
任意の名前を入力します。接続先がわかるような名前にしておくと、設定の修正や削除をする場合に便利です。

8. 「作成」ボタンをクリックする。
設定内容が保存されます。

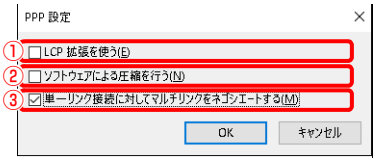
9. 「ネットワークと共有センター」画面で「アダプターの設定の変更」をクリックする。

10. 作成した VPN の接続設定を右クリックし、「プロパティ」を選択する。

11. 「オプション」タブを選択し、「PPP 設定」ボタンをクリックする。



12.PPP 設定を変更する。



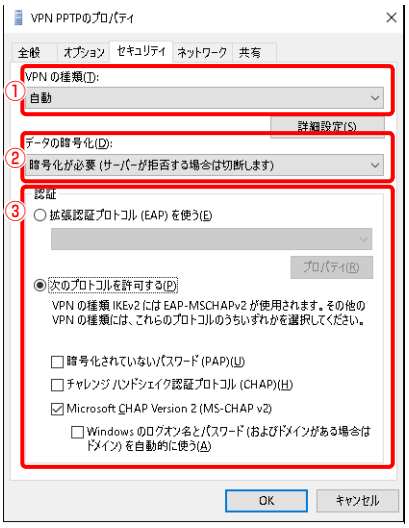
① **LCP 拡張を使う：**
チェックボックスのチェックを外します。

② **ソフトウェアによる圧縮を行う：**
チェックボックスのチェックを外します。

③ **単一リンク接続に対してマルチリンクをネゴシエートする：**
チェックボックスにチェックを付けます。

13.「OK」ボタンをクリックし、「セキュリティ」タブを選択する。

14.セキュリティー設定を変更する。



① **VPN の種類：**
「自動」を選択します。

② **データの暗号化：**
「暗号化が必要（サーバーが拒否する場合は切断します）」を選択します。

③ **認証：**
「次のプロトコルを許可する」を選択し、以下のように設定します。
- 暗号化されていないパスワード（PAP）：チェックボックスのチェックを外す。
- チャレンジハンドシェイク認証プロトコル（CHAP）：チェックボックスのチェックを外す。
- Microsoft CHAP Version 2（MS-CHAPv2）：チェックボックスにチェックを入れる。
- Windows のログオン名とパスワード（およびドメインがある場合はドメイン）を自動的に使う：チェックボックスのチェックを外す。

重要

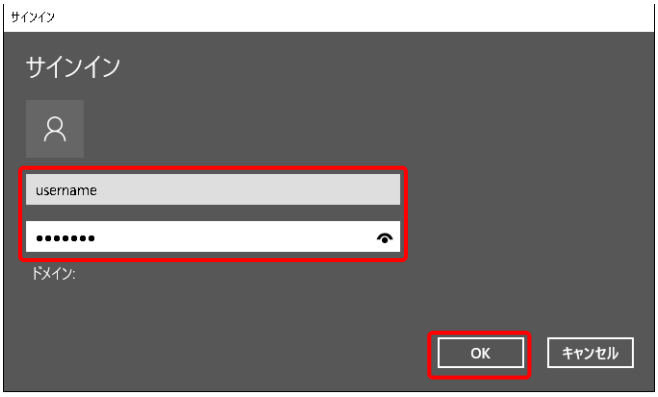
Windows Vista 以降の Windows OS では、Microsoft CHAP Version 1（MS-CHAP）はサポートされていません。「9.3.1 本製品の設定（PPTP）をする」の手順 4 で「MSCHAP-V2」を選択してください。

15.「OK」ボタンをクリックする。

本製品へリモートアクセスする

1. 「スタート」メニューから「設定」―「ネットワークとインターネット」―「VPN」の順に選択する。
2. 作成した VPN の接続設定を選択し、「接続」ボタンをクリックする。

3. 「9.3.1 本製品の設定（PPTP）をする」で設定したユーザー名とパスワードを入力し、「OK」ボタンをクリックする。
   本製品への VPN 接続を開始します。



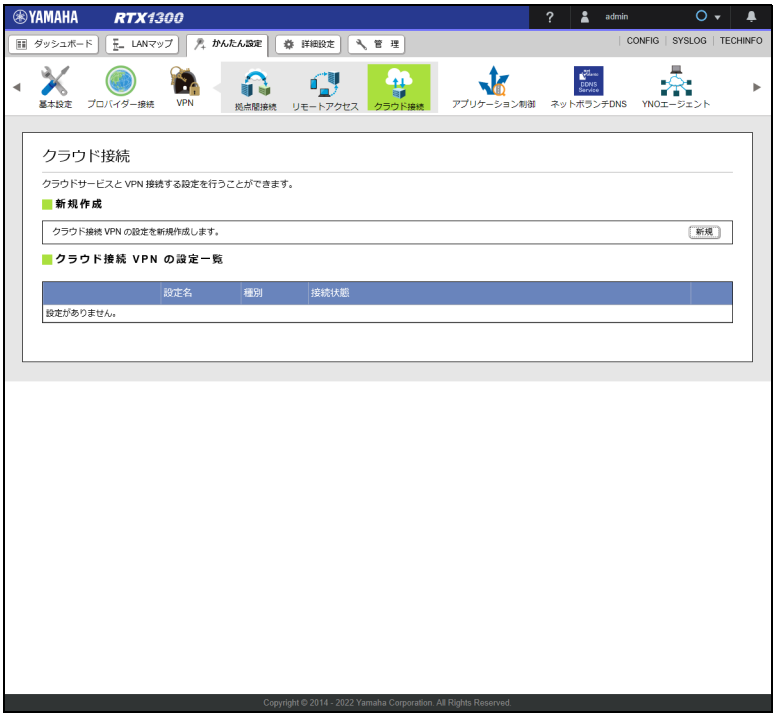
リモートアクセスを切断する場合は

「切断」ボタンをクリックします。

第 10 章 クラウドサービスと VPN で接続する

本製品にはクラウドサービスとの VPN 接続を簡単に行える機能が搭載されています。

Web GUI では「かんたん設定」タブ ―「VPN」―「クラウド接続」を選択して表示される画面で設定を行います。



設定方法について詳しくは、以下の URL をご覧ください。

クラウドサービスとの VPN 接続設定機能
http://www.rtpro.yamaha.co.jp/RT/docs/cloud_vpn/index.html

第 11 章 ダッシュボードを利用する

本章では、ダッシュボードの利用方法について説明します。

・ ダッシュボードとは？ …119 ページ
・ Live 画面の基本操作 …120 ページ
・ Live 画面の各ガジェットの説明 …127 ページ
・ History 画面の基本操作 …138 ページ
・ History 画面の各ガジェットの説明 …145 ページ

11.1 ダッシュボードとは？

各種システム情報やステータス情報を可視化、監視するページのことを「ダッシュボード」と呼びます。ダッシュボード機能とは、さまざまなガジェットを利用してシステムの状態や運用管理、トラブルシューティングに有用な情報を、ウェブブラウザー上でよりグラフィカルに表示する機能のことです。
ダッシュボードに表示される一つ一つのウィンドウのことを「ガジェット」と呼びます。各ガジェットの情報は定期的に自動更新されます。
ガジェットは環境に応じて取捨選択して画面上に自由に配置できます。
各ガジェットのパラメーターがある閾値を超えたら警告文が表示されるため、システムの監視も可能です。
ダッシュボードは「Live」および「History」の 2 種類の画面に分かれます。
Live 画面では、本製品の現在の情報を閲覧できます。表示内容は、所定時間ごとに自動的に更新されます。
History 画面では、統計機能によって本製品に蓄積された過去の情報を閲覧できます。

工場出荷状態では、それぞれの画面は以下のガジェットを表示します。

Live
・ システム情報
・ リソース情報
・ インターフェース情報
・ トラフィック情報（LAN）

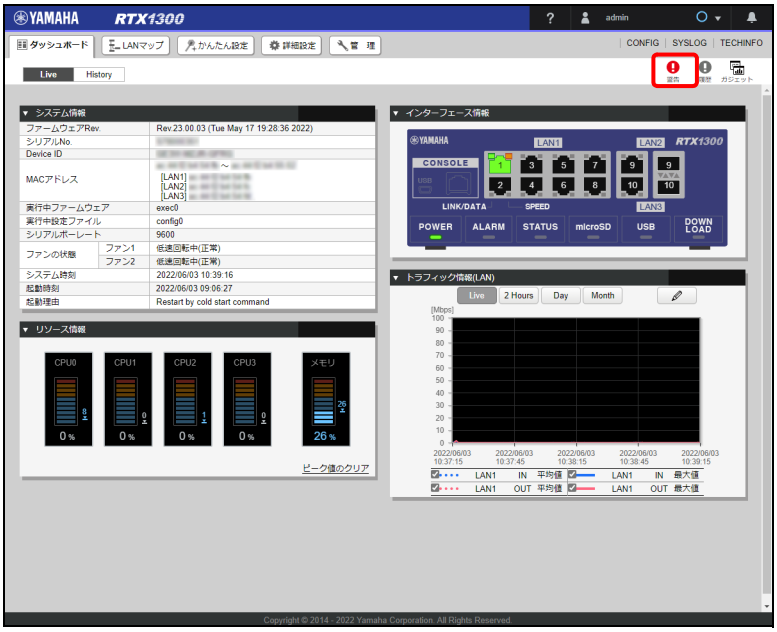
History
・ CPU 使用率

11.2 Live 画面の基本操作

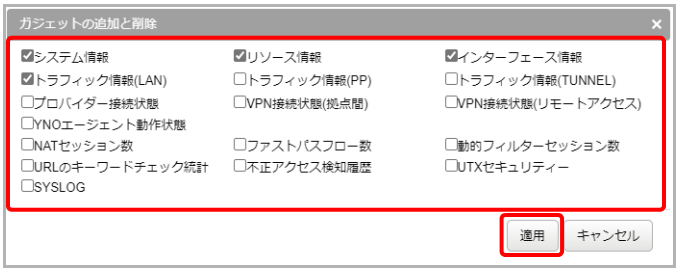
11.2.1 ガジェットの追加または削除をする

ガジェットを追加する

1. 「ガジェット」ボタンをクリックする。



2. ガジェットの一覧から追加するガジェットのチェックボックスにチェックを入れ、「適用」ボタンをクリックする。



ガジェットは常にダッシュボードページの一番左上に追加されます。

ガジェットを削除する

ガジェットを削除する場合は、ガジェットの一覧から削除したいガジェットのチェックボックスのチェックを外し、「適用」ボタンをクリックしてください。または、削除したいガジェットのタイトルバーにマウスカーソルを重ね「 」ボタンをクリックしても削除することができます。

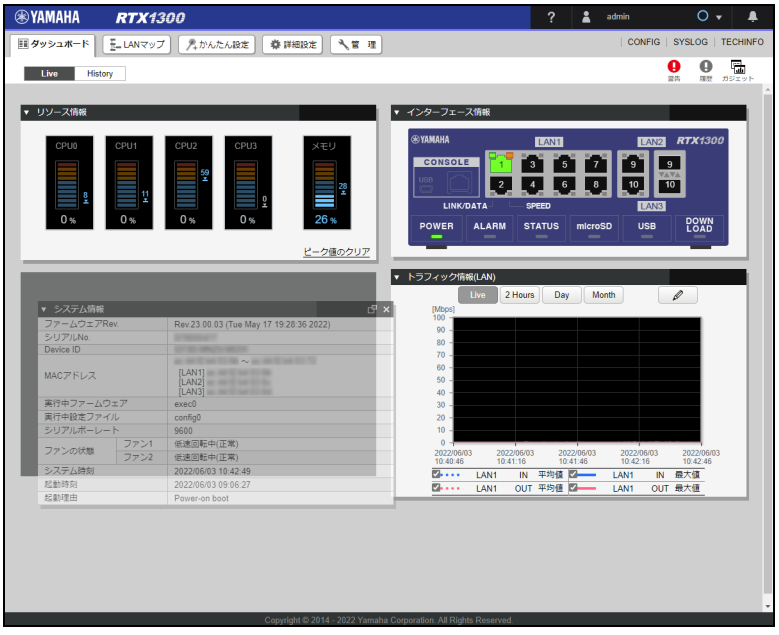
メモ

ガジェットを削除すると、該当ガジェットに対する警告表示もクリアされます。

11.2.2 ガジェットを移動する

1. **移動させたいガジェットのタイトルバーにマウスカーソルを重ねる。**
   マウスカーソルが移動マーク「 」に切り替わります。

2. **ガジェットをドラッグ & ドロップで、任意の位置に移動する。**



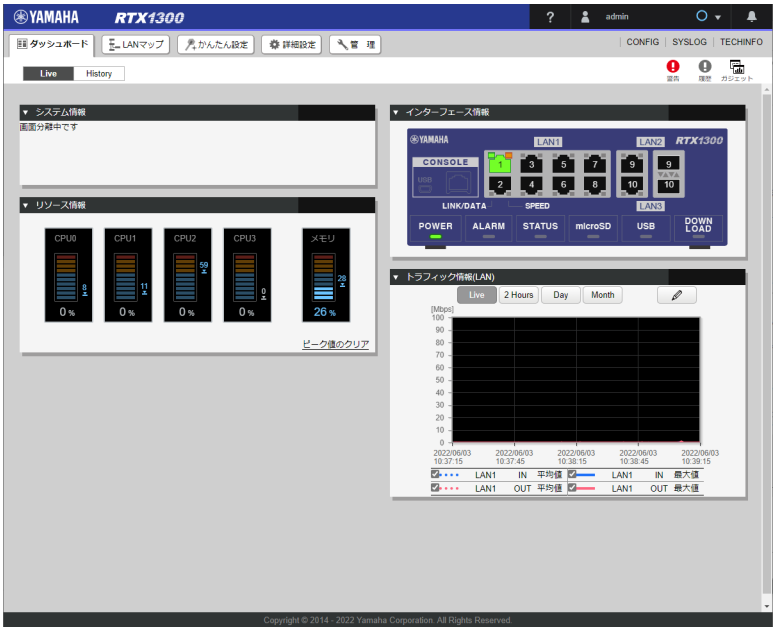
メモ

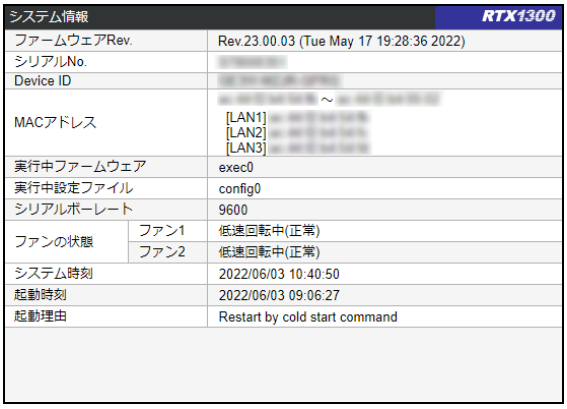
ガジェットの移動先候補は灰色で表示されます。

11.2.3 ガジェットの画面を分離する

1. **分離させたいガジェットのタイトルバーにマウスカーソルを重ねる。**
   ガジェットのタイトルバーに「 」が表示されます。

2. **「 」ボタンをクリックする。**
   ガジェットが別ウィンドウに分離されます。また、ダッシュボードでは「画面分離中です」と表示されます。





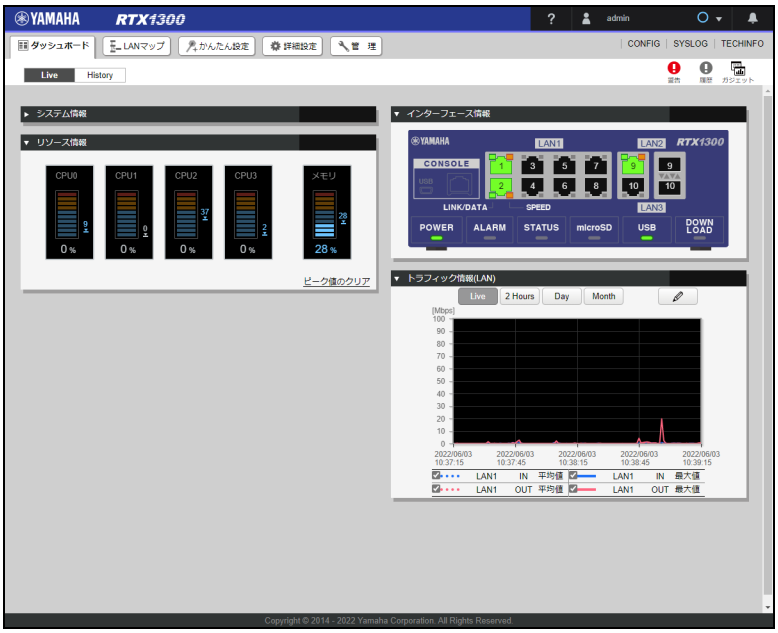
システム情報		RTX1300
ファームウェアRev.		Rev.23.00.03 (Tue May 17 19:28:36 2022)
シリアルNo.		
Device ID		
MACアドレス		[LAN1] [LAN2] [LAN3]
実行中ファームウェア		exec0
実行中設定ファイル		config0
シリアルボーレート		9600
ファンの状態	ファン1	低速回転中(正常)
	ファン2	低速回転中(正常)
システム時刻		2022/06/03 10:40:50
起動時刻		2022/06/03 09:06:27
起動理由		Restart by cold start command

ガジェット分離中の動作

- 分離元のガジェットには「 」と「 」は表示されません。
- 分離中のガジェットを閉じると、ダッシュボードページの元の場所に戻ります。
- ダッシュボードページの表示を更新すると、分離しているガジェットはすべてダッシュボードページに戻ります。
- ダッシュボードページを閉じると、分離しているすべてのガジェットも閉じられます。
- 分離したガジェットは、URL を直接ウェブブラウザーに指定して表示することができます。
  例：システム情報ガジェットは「http://(LAN1 アドレス)/dashboard/system.html」

11.2.4 ガジェットを最小化する

1. **最小化させたいガジェットの「 ▼ 」ボタンをクリックする。**
   ガジェットが最小化表示になります。また、アイコン表示が「 ▶ 」に切り替わります。
   「 ▶ 」ボタンをクリックすると、ガジェットは元の大きさに戻ります。



11.2.5 ガジェットの位置情報を保存する

ガジェットの表示内容（「ガジェットの追加と削除」ダイアログで選択したガジェットの種類とその位置情報）は下記の操作を行ったときに RTFS にファイルとして自動的に保存されます。RTFS とは、本製品の不揮発性メモリーに構築されるファイルシステムのことです。

- ガジェットを追加、削除したとき
- ガジェットを移動したとき
- ガジェットを最小化 / 元に戻したとき

注意

- 一般ユーザーでログインして操作した場合、または RTFS の空き容量が足りない場合はガジェットの表示内容は保存されません。
- 工場出荷状態に戻したり RTFS をフォーマットしたりすると、ガジェットの表示内容は初期化されます。

メモ

- トラフィック情報のガジェットについては、表示するインターフェース情報、方向（IN/OUT）、グラフの種別（平均値 / 最大値）の設定を変更したときも保存されます。
- 電源を再投入した後でもこれらの情報は保存されています。

11.2.6 ガジェットを自動更新する

すべてのガジェットは定期的に自動更新されます。
更新間隔はガジェットによって異なります。

11.2.7 警告の内容を確認する

メモ

・ 警告内容の一覧と警告履歴の一覧を同時に開くことはできません。
・ ダッシュボードに表示している各ガジェットで、異常状態または高負荷を検知すると「 」が点滅します。その際、該当ガジェットにも「 」アイコンが点滅しながら表示されます。

1. 「 」ボタンをクリックする。
   現在の警告内容が一覧で表示されます。

警告一覧には現在検出している警告内容が新しい順に表示されます。
・ 異常を検出した日時
・ 異常を検出したガジェット
・ 検出した内容

警告は、以下の条件を満たすと表示されなくなります。
・ 異常状態から復旧する（使用率やセッション数が閾値を下回った、など）
・ 状態をクリアする（設定を変更した、カウンタをクリアした、など）
・ 警告一覧の「解除」ボタンをクリックする

メモ

・「解除」ボタンをクリックして表示を消しても、異常状態が解消されたわけではありません。
・ すべての警告表示が消えると「 」の点滅は止まり、警告一覧の表示も消えます。

再度「 」ボタンをクリックすると警告内容の一覧が閉じます。

警告の対象となる状態

ガジェット	トリガー	
システム情報	起動理由でリブートを検出したとき ファンの異常を検出したとき	
リソース情報	リソースの閾値監視コマンド設定時	CPU 使用率が CPU の閾値監視コマンド（system cpu threshold）の上限の閾値以上になったとき
		メモリ使用率がメモリの閾値監視コマンド（system memory threshold）の上限の閾値以上になったとき
	リソースの閾値監視コマンド未設定時	CPU 使用率が 80%以上になったとき
		メモリ使用率が 80%以上になったとき
インターフェース情報	STATUS LED が点灯したとき ALARM LED を検出したとき LAN インターフェースでエラー（*）を検出したとき （*）以下を LAN のエラーと判定します - 送信アンダーフロー - 送信オーバーフロー - Late collision - Loss of carrier - 再送エラー - 受信フレーミングエラー - 受信オーバーフロー - 受信 CRC エラー USB ポートで過電流が検出されたとき	
トラフィック情報（LAN）	LAN インターフェースのトラフィック量がリンク速度の 80%以上になったとき	
プロバイダー接続状態	エラーにより切断されたプロバイダーを検出したとき	
VPN 接続状態 （拠点間 / リモートアクセス）	エラーにより切断された VPN を検出したとき	
YNO エージェント動作状態	オペレーター ID が存在しないとき アクセスコードが一致しないとき ACS への接続に失敗したとき ACS でアクセスコードが設定されていないとき ライセンスの有効期限が切れているとき ライセンス数が不足しているとき XMPP を使用できないとき GFW を使用できないとき LAS を使用できないとき	
NAT セッション数	NAT のセッション数が最大同時セッション数の 80% 以上になったとき	
ファストパスフロー数	ファストパスのフロー数が最大同時フロー数の 80% 以上になったとき	
動的フィルターセッション数	動的フィルターのセッション数が最大同時セッション数の 80% 以上になったとき	
不正アクセス検知履歴	不正アクセスを検知したとき	
UTX セキュリティー	配下に接続されたヤマハ UTM アプライアンスで以下のセキュリティーインシデントを検出したとき ・アンチボット ・アンチウイルス ・IPS	

11.2.8 警告の履歴を表示する

メモ

警告履歴の一覧と警告内容の一覧を同時に開くことはできません。

1. 「 」ボタンをクリックする。
   警告履歴が一覧で表示されます。警告履歴は新しい順に最大で 30 件表示されます。

メモ

- 警告履歴は太字で表示されますが、警告一覧で「解除」ボタンをクリックすることにより解除された警告内容は細字で表示されます。
- 解除されていない未確認の警告履歴がある場合は、 のように警告履歴の数が表示されます。この数字が表示されているときは、警告履歴の一覧で発生していた警告内容を確認してください。

再度「 」ボタンをクリックすると警告履歴の一覧は閉じられます。

警告履歴の操作

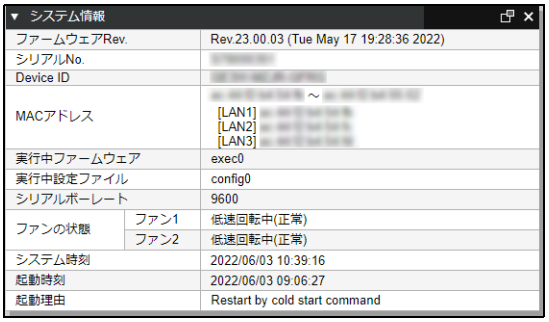
- 各履歴の「確認」ボタンをクリックすると、確認済みの履歴として細字に切り替わり、「確認」の表示が消えます。
- 「全て確認済」ボタンをクリックすると、すべての履歴が確認済みの状態になります。
- 「全て削除」ボタンをクリックすると、すべての履歴が削除されます。

11.3 Live 画面の各ガジェットの説明

ダッシュボードに対応しているガジェットは以下のとおりです。

・ システム情報 …127 ページ
・ リソース情報 …128 ページ
・ インターフェース情報 …129 ページ
・ トラフィック情報（LAN/PP/TUNNEL）…131 ページ
・ プロバイダー接続状態 …132 ページ
・ VPN 接続状態（拠点間）…133 ページ
・ VPN 接続状態（リモートアクセス）…133 ページ
・ YNO エージェント動作状態 …133 ページ
・ NAT セッション数 …134 ページ
・ ファストパスフロー数 …134 ページ
・ 動的フィルターセッション数 …135 ページ
・ 不正アクセス検知履歴 …135 ページ
・ UTX セキュリティー …136 ページ
・ URL のキーワードチェック統計 …136 ページ
・ SYSLOG…137 ページ

11.3.1 システム情報



メモ

工場出荷状態ではダッシュボードの左上の位置に表示されます。

以下の情報が表示されます。

ファームウェア Rev.

・ ファームウェアのリビジョンが表示されます。

シリアル No.

・ 機器のシリアル番号が表示されます（筐体底面のシールにも記載されています）。

Device ID

・ 機器に割り当てられている Device ID が表示されます（筐体底面のシールにも記載されています）。

MAC アドレス

・ LAN1 ～ LAN8 の MAC アドレスが表示されます（筐体底面のシールにも記載されています）。

実行中ファームウェア

・ 不揮発性メモリー内のファームウェアから起動している場合は「execN (N: 0-1)」、外部メモリー内に保存されているファームウェアから起動している場合は「usb1:/rtx1300.bin」のように表示されます。

実行中設定ファイル

・ 不揮発性メモリー内の設定ファイルから起動している場合は「configN (N: 0-4.2)」、外部メモリー内に保存されている設定ファイルから起動している場合は「usb1:/config.txt」のように表示されます。

シリアルボーレート

・ CONSOLE ポートのデータ転送速度が表示されます。

ファンの状態

・ ファン 1、ファン 2 の状態が表示されます。ファンが正常に動作、または停止しているか確認できます。

メモ

ファンの異常を検出した場合は、背景が赤色に変わり ❗ が表示されます。ネットワーク管理者に相談してください。

システム時刻

・ 現在の機器の日時が表示されます。

メモ

日時が合っていない場合は、「3.1 日付と時刻を設定する」を参照して日時を合わせてください。

起動時刻

・ 本製品の起動した日時が表示されます。

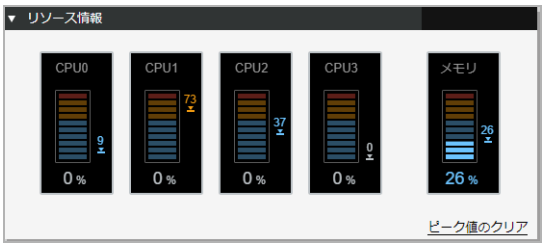
起動理由

・ 起動した理由が表示されます（電源 OFF 状態からの起動、restart コマンド、リビジョンアップなどが表示されます）。

メモ

起動理由でリブートを検出した場合は、背景が赤色に変わり ❗ が表示されます。ネットワーク管理者に確認してください。
また、警告一覧の「解除」ボタンをクリックして、警告表示を解除してください。

11.3.2 リソース情報

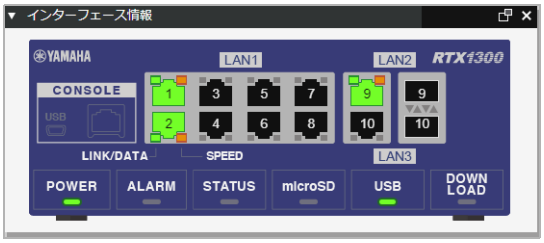


CPU0 ～ CPU3 の使用率とメモリ使用率について、現在の値とピーク値が表示されます。メーターの下側の数字は現在の使用率、右側はピーク値を示します。

メモ

- CPU 使用率が 80% 以上、または CPU 使用率の閾値が設定されている場合は閾値以上になると が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。
- メモリ使用率が 80% 以上、またはメモリ使用率の閾値が設定されている場合は閾値以上になると が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。
- 工場出荷状態ではダッシュボードの左下の位置に表示されます。
  CPU 使用率とメモリ使用率について、現在値とピーク値が表示されます。メーターの右側の数字は現在の使用率、左側はピーク値を示します。
- 「ピーク値のクリア」ボタンをクリックすると、それまでのピーク値をクリアすることができます。また。本製品を再起動してもピーク値はクリアされます。
- それぞれのメーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されます。

11.3.3 インターフェース情報



メモ

工場出荷状態ではダッシュボードの右上の位置に表示されます。

本体の LED の状態が表示されます。

LED

POWER

- 電源が入っていると緑色に点灯します。

ALARM

- ハードウェアに異常が発生すると赤色に点灯します。
- 点灯すると警告表示されます。マウスカーソルを重ねると点灯の原因を確認できます。

STATUS

- 常時接続の設定をしている接続先の機器との通信が途絶えたり、キープアライブで通信断を検出したりすると橙色に点灯します。
- 点灯すると警告表示されます。マウスカーソルを重ねると障害を検出しているキープアライブの設定やインターフェースを確認できます。
  ケーブル抜けや回線の状態、アカウント情報の確認などを行ってください。キープアライブの到達性が回復したり、回線が接続状態になったりすると警告表示は消えます。

microSD

- microSD スロットに microSD が接続されていると緑色に点灯します。
- マウスカーソルを重ねると給電状態や接続されているデバイス情報が表示されます。

USB

- USB ポートに USB メモリー、または USB 接続型データ通信端末が接続されていると緑色に点灯します。
- マウスカーソルを重ねると給電状態や接続されているデバイス情報が表示されます。
- 過電流を検出すると緑色で点滅し、警告表示されます。マウスカーソルを重ねると過電流の検出回数が表示されます。また、USB ポートに挿しているデバイスを抜き、USB ボタンを押すと警告表示も消すことができます。
- USB LED の点灯パターン
  - 点灯：USB メモリー、またはモバイル端末が接続中
  - 点滅：過電流を検出

DOWNLOAD

- DOWNLOAD ボタンによる機能の実行中に緑色に点灯または点滅します。

LAN ポート /SFP+ ポート

コネクタ部

- リンクアップしているポートは緑色に点灯します。
- マウスカーソルを重ねると、動作モードが表示されます。SFP+ ポートがリンクアップしているときは、発光レベルと受光レベルが併記されます。フレキシブル LAN の設定を変更している場合、パケット送受信数やエラーパケット数が併記されます。

ポート周辺

- フレキシブル LAN の設定を変更している場合、ポートが属している LAN インターフェースごとにポート周辺が色分けして表示されます。

LINK/DATA LED

- リンクアップしているポートは緑色に点灯します。

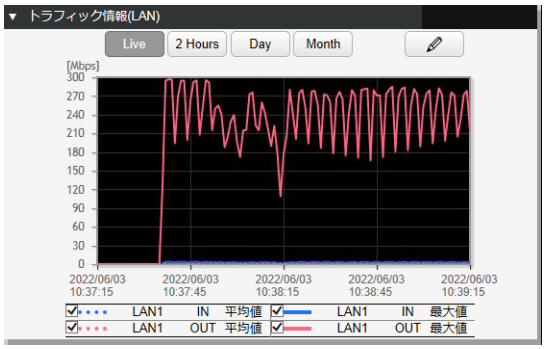
SPEED LED

- LAN ポートの場合
  - 接続速度が 2.5GBASE-T、5GBASE-T、10GBASE-T のとき緑色に点灯します。
  - 接続速度が 1000BASE-T のとき橙色に点灯します。
  - 接続速度が 10BASE-T、100BASE-TX のとき消灯します。
- SFP+ ポートの場合
  - 接続速度が 10GBASE-SR、10GBASE-LR のとき緑色に点灯します。
  - 接続速度が 1000BASE-SX、1000BASE-LX のとき橙色に点灯します。

ラベル

- マウスカーソルを重ねると LAN ポート /SFP+ ポートのパケット送受信数やエラーパケット数が表示されます。
- エラーパケットを検出すると警告表示されます。clear status lanN コマンドを実行するとパケットの送受信数やエラーカウンタがリセットされ、警告表示も消すことができます。
- フレキシブル LAN の設定を変更すると非表示になります。

11.3.4 トラフィック情報（LAN/PP/TUNNEL）



メモ

工場出荷状態では、トラフィック情報（LAN）がダッシュボードの右下の位置に表示されます。

使用中のインターフェース（LAN/PP/TUNNEL）ごとに対して「IN 平均値」、「IN 最大値」、「OUT 平均値」、「OUT 最大値」の変動を示すグラフが表示されます。
グラフは最大で 8 本まで表示でき、グラフの線には [青、サーモンピンク、黄、緑、灰、スカイブルー、ピンク、紫] の 8 色が使用されます。この色は、グラフを描画するタイミングでインターフェースの若い順に割り当てられます。

IN：該当インターフェースが受信するトラフィック
OUT：該当インターフェースから送信されるトラフィック

メモ

- 同一インターフェースかつ同一方向のグラフは、平均値は破線、最大値は実線で表示されます。
- 使用中の LAN/PP/TUNNEL インターフェースのトラフィックのみ表示されます。
- トラフィック情報は、LAN 分割やタグ VLAN インターフェースには対応していません。

グラフの縦軸の上限はトラフィック量に応じて 100[Mbps] 単位で最大 10[Gbps] まで増えていきます。また、グラフの横軸の日時は以下の周期で更新されます。

- Live：30 秒
- 2 Hours：30 分
- Day：6 時間
- Month：約 1 週間

グラフの線上にマウスカーソルを重ねると、インターフェース情報や日時、トラフィック量が表示されます。
グラフの下には現在表示されているグラフの線の色・スタイル、インターフェースの一覧（凡例）が表示されます。

凡例の使い方

凡例のチェックが入っている項目のみ表示されます。チェックを外すとグラフに表示されなくなります。
複数の線が重なっていたり、特定のインターフェースを監視したりする場合などに表示を切り替えてください。

メモ

- LAN は、LAN インターフェースごとにその時点でリンクアップしているポートのうち最も速いリンク速度の 80%を閾値とし、閾値を超えた場合 ❗ が表示されます。警告一覧や警告履歴からトラフィックが高くなっていた日時を確認し、その時間帯の各種セッション数を確認してください。

・現在監視の対象になっているインターフェースが存在しない場合は、「監視対象のインターフェースが選択されていません」と表示されます。
・画面を更新すると、すべての凡例にチェックが入り、描画期間が Live に切り替わります。

「 」により別ウィンドウでガジェットを表示させた場合

・監視対象のインターフェースや方向の設定は分離前の設定が反映されます。ただし、すべての凡例にチェックが入り、描画期間が Live に切り替わります。
・分離したウィンドウ内で選択したインターフェースや方向の設定は、分離画面を閉じるとダッシュボードページのガジェットにも反映されます。

分離したウィンドウの URL を直接入力してガジェットを表示させた場合

監視対象のインターフェースや方向の設定は直接表示専用の設定が適用されるため、ダッシュボードページの設定とは異なります。ただし、すべての凡例にチェックが入り、描画期間が Live に切り替わります。

グラフの描画期間を変更する

「Live」、「2 Hours」、「Day」、「Month」ボタンをクリックし、描画期間を変更します。
・Live：過去 2 分間
・2 Hours：過去 2 時間
・Day：過去 1 日間
・Month：過去 1ヵ月間

グラフに描画するインターフェースを選択する

「 」ボタンをクリックします。一覧から表示するインターフェースのチェックボックスにチェックを入れ、「適用」ボタンをクリックすると設定が反映されます。

メモ

・使用していないインターフェースのチェックボックスは表示されません。
・現在使用中のインターフェースが存在しない場合は、「有効なインターフェースが見つかりません」と表示されます。

11.3.5 プロバイダー接続状態

プロバイダー接続の一覧とそれぞれの接続状態が表示されます。
通信中（Up）、未接続（Down）、エラー切断（Error）、総数（All）がカウントされます。また、「Up」、「Down」、「Error」、「All」ボタンをクリックすると、各状態のプロバイダー接続のみを表示することができます。
設定名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、そのプロバイダー接続の状態が表示されます。

メモ

・エラー切断を検出すると背景が赤色に変わり、 が表示されます。状態欄にマウスカーソルを重ね、切断された日時や切断理由を確認してください。
・プロバイダーが一つも登録されていないときは「プロバイダーの設定がありません」と表示されます。

11.3.6 VPN 接続状態（拠点間）

VPN 接続（拠点間）の一覧とそれぞれの接続状態が表示されます。
通信中（Up）、未接続（Down）、エラー切断（Error）、総数（All）がカウントされます。また、「Up」、「Down」、「Error」、「All」ボタンをクリックすると、各状態の VPN 接続のみを表示することができます。
設定名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、その VPN 接続の状態が表示されます。

メモ

- エラー切断を検出すると背景が赤色に変わり、❗が表示されます。状態欄にマウスカーソルを重ね、切断された日時や切断理由を確認してください。
- VPN 接続が一つも登録されていないときは「VPN の設定がありません」と表示されます。

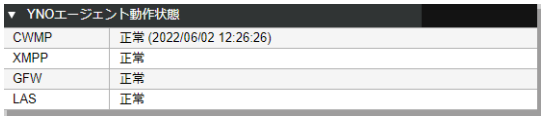
11.3.7 VPN 接続状態（リモートアクセス）

VPN 接続（リモートアクセス）の一覧とそれぞれの接続状態が表示されます。
通信中（Up）、未接続（Down）、総数（All）がカウントされます。また、「Up」、「Down」、「All」ボタンをクリックすると、各状態の VPN 接続のみを表示することができます。
ユーザー名、接続種別、インターフェース、接続状態が表示されます。状態欄にマウスカーソルを重ねると、その VPN 接続の状態が表示されます。

メモ

VPN 接続が一つも登録されていないときは「VPN の設定がありません」と表示されます。

11.3.8 YNO エージェント動作状態



YNO エージェント機能で使用する各サーバーとの接続状態が表示されます。

接続状態の詳細については、Web GUI のヘルプページをご覧ください。

CWMP：ACS との接続状態
XMPP：XMPP との接続状態
GFW：GFW との接続状態
LAS：LAS との接続状態

メモ

- YNO を利用するには YNO エージェント機能を有効にする必要があります。「17.2 YNO エージェント機能を有効にする」（453 ページ）を参照して YNO エージェント機能を有効にしてください。
- 接続状態の異常を検知すると、「 ! 」が表示されます。警告一覧や警告履歴から異常の詳細を確認し、設定を見直してください。
- 「CWMP」の接続状態には、本製品が YNO マネージャーと正常に接続されている場合、接続状態と共に接続が確立した日時が表示されます。

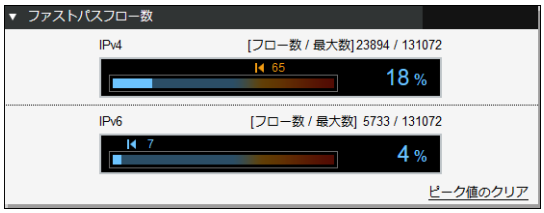
11.3.9 NAT セッション数

NAT のセッション数が表示されます。
メーターの右側の数字は現在の使用率を示し、上部はピークの使用率を示します。
メーターの左上部にディスクリプタ ID、右上部に現在の接続数と最大数が表示されます。
メーターは現在の接続数が最も多いディスクリプタ ID の NAT セッション数を表示します。

メモ

- セッション数が最大同時セッション数の 80% 以上になると ! が表示されます。ピーク値を記録した日時やセッションを大量に使用していたホストの IP アドレスを確認してください。
- 「ピーク値のクリア」ボタンをクリックすると、すべてのディスクリプタ ID のピーク値をクリアすることができます。また、本製品を再起動してもピーク値はクリアされます。
- メーターにマウスカーソルを重ねると、ピーク値 / ピーク時のセッション数上位 5 件のホストの IP アドレスとホストごとのセッション数 / ピーク値を記録した日時が表示されます。

11.3.10 ファストパスフロー数

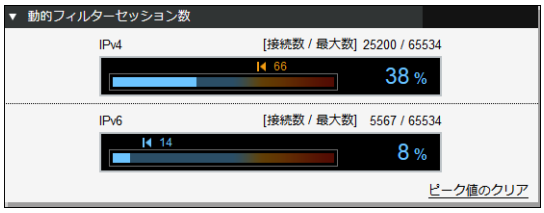


ファストパスのフロー数が表示されます。
メーターの右側の数字は現在の使用率を示し、上部はピークの使用率を示します。
メーターの上部に現在のフロー数と最大数が表示されます。

メモ

- フロー数が最大同時フロー数の 80% 以上になると ! が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。
- 「ピーク値のクリア」ボタンをクリックすると、IPv4/IPv6 のピーク値をクリアすることができます。また、本製品を再起動してもピーク値はクリアされます。
- メーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されます。

11.3.11 動的フィルターセッション数

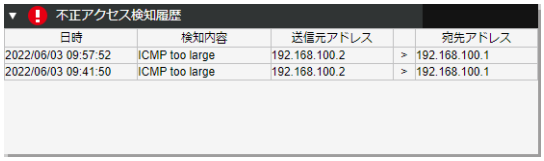


動的フィルターで管理しているセッション数が表示されます。
メーターの右側の数字は現在の使用率を示し、上部はピークの使用率を示します。
メーターの上部に現在の接続数と最大数が表示されます。

メモ

- セッション数が最大同時セッション数の 80% 以上になると ! が表示されます。ピーク値を記録した日時を確認し、他のガジェットからその時間帯のトラフィックや各種セッション数を確認してください。
- 「ピーク値のクリア」ボタンをクリックすると、IPv4/IPv6 のピーク値をクリアすることができます。また、本製品を再起動してもピーク値はクリアされます。
- メーターにマウスカーソルを重ねると、ピーク値とピーク値を記録した日時が表示されます。

11.3.12 不正アクセス検知履歴



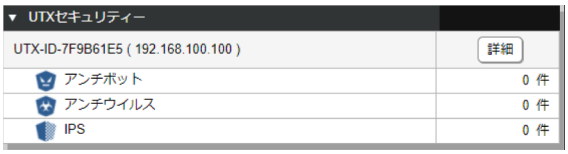
不正アクセスの検知履歴が最新のものから 10 件分表示されます。

検知した日時、検知した内容、送信元アドレス、宛先アドレスが表示されます。必要に応じて、送信元 IP アドレスからのアクセスを拒否するフィルターを設定してください。
すべてのインターフェースに対する検知結果が時系列にまとめて表示され、一番上が最新の履歴になります。

メモ

- 不正アクセス検知機能を有効に設定しておく必要があります。
- 不正アクセスを検知すると ! が表示されます。ネットワーク管理者に確認してください。
- 1 件も検知されていないときは「不正アクセスは検知していません」と表示されます。
- 不正アクセス検知機能の設定を再設定すると履歴はクリアされます。

11.3.13 UTX セキュリティー



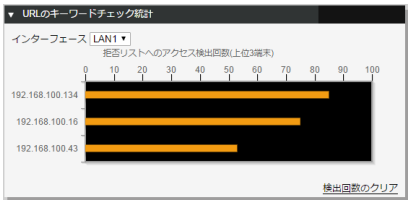
ヤマハ UTM アプライアンスで検出されたセキュリティーインシデント件数が表示されます。

アンチボット、アンチウイルス、IPS がカウントされます。
「詳細」ボタンをクリックするとヤマハ UTM アプライアンスの Web GUI を表示することができます。

メモ

- セキュリティーインシデントを検出するには LAN マップを有効にする必要があります。
- 「12.3 LAN マップを有効にする」（153 ページ）を参照して LAN マップを有効にしてください。
- エラーを検出すると、 が表示されます。警告一覧や警告履歴から異常の詳細を確認してください。

11.3.14 URL のキーワードチェック統計



拒否リストに登録されたキーワードを含む URL にアクセスした上位 3 端末の統計情報を示すグラフが表示されます。

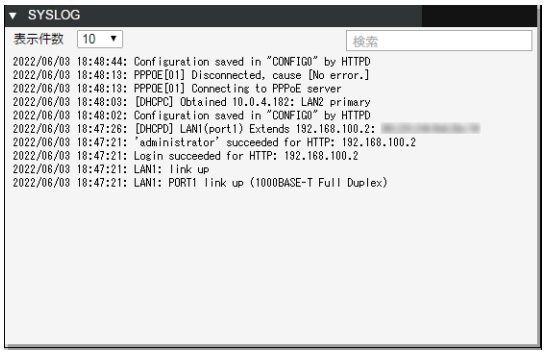
表示するインターフェースをプルダウンメニューから変更することができます。選択したインターフェースに登録された拒否リストの統計情報がグラフとして表示されます。

グラフにマウスカーソルを重ねると、上位 5 件の検出したキーワードが表示されます。

メモ

- URL フィルターのキーワードチェックを有効に設定しておく必要があります。
- 設定がない時は「設定されていません」と表示されます。
- 「検出回数のクリア」ボタンをクリック、または機器を再起動すると「グラフ」、「実行したインターフェースの検出回数」、「拒否リストの統計情報」がクリアされます。
- 1 件も検知されていない時は「検知履歴はありません」と表示されます。

11.3.15 SYSLOG



SYSLOG が最新のものから表示件数分表示されます。一番上が最新のログになります。
表示する件数（10 件、50 件、100 件）をプルダウンメニューから変更することができます（初期値：10 件）。
検索ボックスに検索したい文字列を入力すると、入力した文字列を含んだログのみを表示させることができます。なお、大文字、小文字は区別されます。

11.4 History 画面の基本操作

11.4.1 統計情報の記録を開始する

本製品に情報を蓄積するために統計機能を有効にする必要があります。統計機能では各種情報を外部メモリーに保存するため、外部メモリーを用意してください。

注意

本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータが破損することがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。

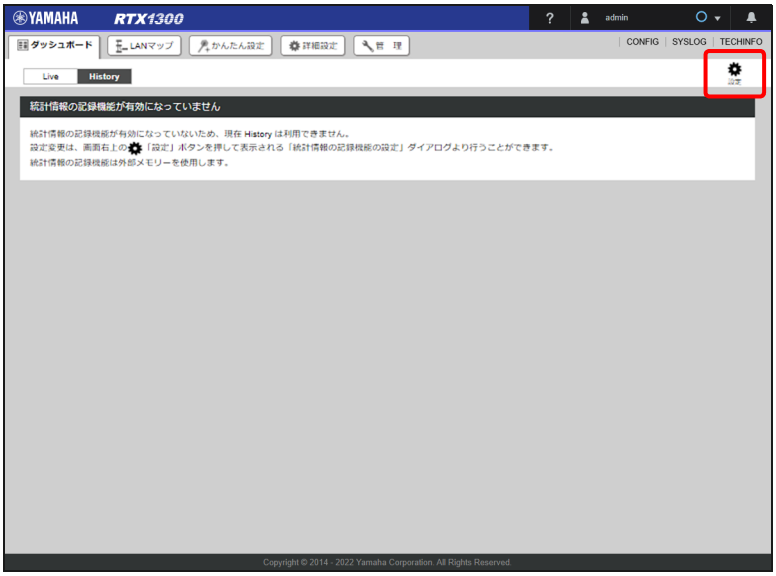
重要

- USB 延長ケーブルを介して接続した場合は、正常に動作しないことがあります。USB メモリーは本製品の USB ポートに直接挿入してご使用ください。
- FAT または FAT32 形式でフォーマットされていない外部メモリーは、本製品では使用できません。
- USB ハブを介して、複数の USB メモリーなどの外部メモリーを本製品に接続することはできません。

メモ

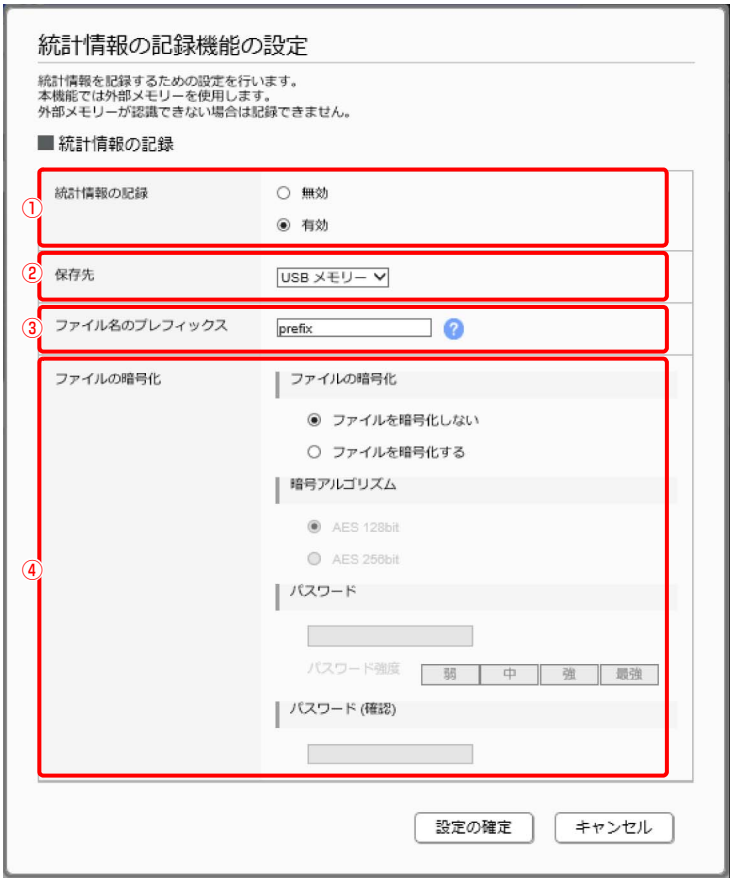
- 外部メモリーを挿していない場合は、統計機能を有効化できません。
- 正しい日時が設定されていない場合は統計情報が正しく保存されないため、日時が合っていない場合は、「3.1 日付と時刻を設定する」（20 ページ）を参照して日時を合わせてください。

1. **外部メモリーを本製品の USB ポートまたは microSD スロットに挿し込む。**
   外部メモリーを認識するとブザーが鳴り、本製品の USB インジケーターまたは microSD インジケーターが点灯します。
2. **「History」ボタンをクリックする。**
   「History」画面が表示されます。
3. **右上の「⚙」ボタンをクリックする。**



「統計情報の記録機能の設定」ダイアログが表示されます。

4. **統計情報の記録機能を設定する。**



① 統計情報の記録：
有効を選択することで統計情報が記録されます。

② 保存先：
統計情報の記録を保存する外部メモリーを選択します。

③ ファイル名のプレフィックス：
統計情報を記録するファイル名のプレフィックスを設定します。半角英数字、全角文字、および、一部の記号が使用でき、設定可能な文字数は、半角で 15 文字以内です。
以下の半角記号を使用することができます。
-!#$%&'()=-^\`@{[+;],
実際のファイル名はここで設定するプレフィックスや、統計情報の種類などを元に、以下のフォーマットで生成されます。

■ プレフィックス _ 種別 [_ インターフェース]_ 年月日 . 拡張子

●プレフィックス
本項目で設定する文字列です。

●種別
統計情報の種別です。
種別には以下の内容があります。

種別	説明
cpu	CPU 使用率
memory	メモリ使用率
traffic	トラフィック情報
nat	NAT セッション数
flow	ファストパスフロー数
filter	動的フィルターセッション数
application	アプリケーション制御

●インターフェース
対象のインターフェースです。トラフィック情報以外では省略されます。

●年月日
対象の年月日です。西暦 4 桁、月 2 桁、日 2 桁の 8 桁からなります。

●拡張子
暗号化するか否かによって以下の拡張子に分かれます。

拡張子	説明
csv	暗号化しないファイル
rtfg	暗号化するファイル

④ ファイルの暗号化：
統計情報ファイルを暗号化するか否かを設定します。統計情報ファイルを暗号化して保存する場合は、「ファイルを暗号化する」を選択してから暗号化アルゴリズムを選択し、任意のパスワードを入力します。

注意

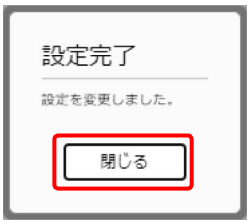
統計情報の記録が有効になっているとき、ファイル名のプレフィックスを変更せずに、ファイルの暗号化の有無を変更することはできません。

メモ

- 暗号化した統計情報ファイルは、Windows アプリケーションの「RT-FileGuard」で復号できます。「RT-FileGuard」は、http://www.rtpro.yamaha.co.jp/RT/utility/ からダウンロードできます。
- パスワードは、長さ 8 ～ 32 文字の半角英数字と半角記号が使用できます。英字の大文字と小文字は区別されます。
  以下の半角記号を使用することができます。
  !"#$%&'()=~|-^\`{@[+*};:]<>?_,./\

5. **入力内容を確認し、「設定の確定」ボタンをクリックする。**
   設定が反映され、「設定完了」ダイアログが表示されます。

6. **「閉じる」ボタンをクリックする。**

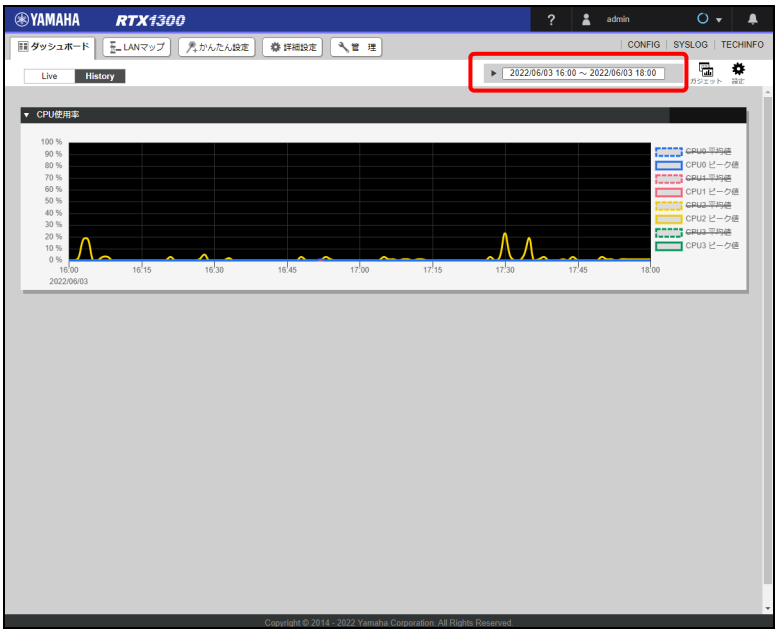


「History」画面が表示され、統計情報の記録が開始されます。

11.4.2 グラフの表示期間を変更する

ガジェットのグラフを表示する期間を設定します。

1. **「▶」ボタンをクリックする。**

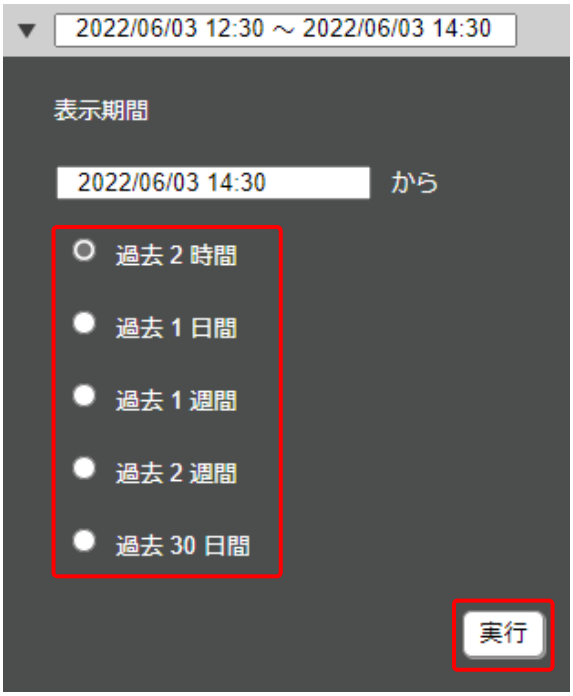


「表示期間」ダイアログが表示されます。

2. **グラフの始点となる日時を設定します。**

ダイアログを開いたときは、30 分単位の時刻で本製品の現在時刻に一番近い過去の時刻が選択されています。日時の設定欄をクリックするとカレンダーと時刻のリストが表示され、グラフの始点となる日付と時刻を変更することができます。

3. **表示する期間を設定する。**



表示したい期間を「過去 2 時間」、「過去 1 日間」、「過去 1 週間」、「過去 2 週間」、「過去 30 日間」の中から選択します。

メモ

表示期間を変更すると、表示中のすべてのグラフの表示期間が変更されます。

注意

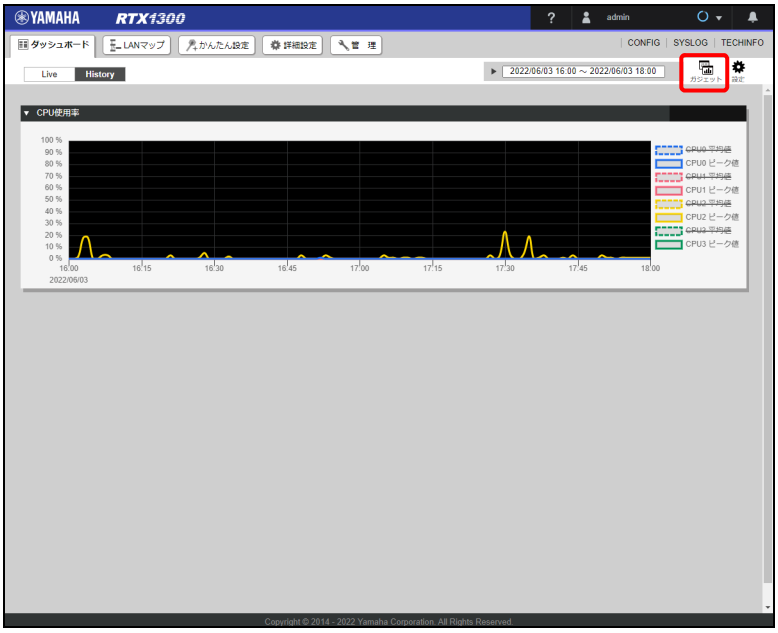
表示期間の設定は保存されません。そのため、「History」画面から別の画面へ遷移した後、再度「History」画面を開くと表示期間が初期状態の「過去 2 時間」に戻ります。

4. **「実行」ボタンをクリックする。**
   カレンダーで選択した日時から、選択した期間のグラフが表示されます。

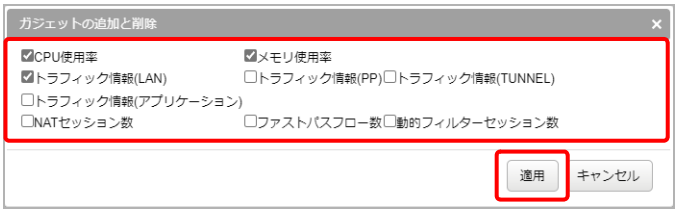
11.4.3 ガジェットの追加または削除をする

ガジェットを追加する

1. **「ガジェット」ボタンをクリックする。**

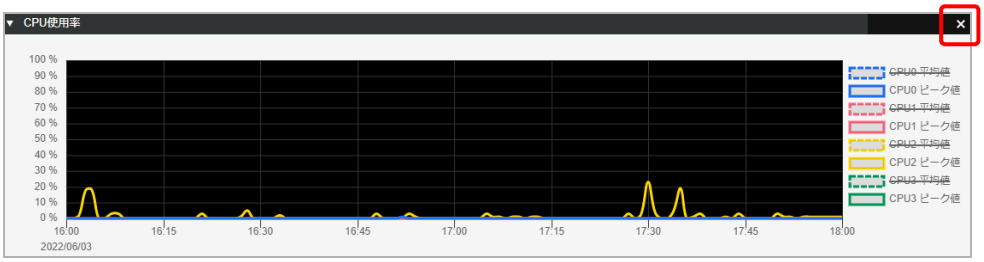


2. **「ガジェットの追加と削除」ダイアログで追加したいガジェットのチェックボックスにチェックを入れ、「適用」ボタンをクリックする。**



ガジェットを削除する

ガジェットを削除する場合は、「ガジェットの追加と削除」ダイアログで削除したいガジェットのチェックボックスのチェックを外し、「適用」ボタンをクリックしてください。または、削除したいガジェットのタイトルバーにマウスカーソルを重ね「」ボタンをクリックしても削除することができます。



11.4.4 ガジェットを移動する

1. **移動したいガジェットのタイトルバーにマウスカーソルを重ねる。**
   マウスカーソルが移動マーク「」に切り替わります。
2. **ガジェットをドラッグ & ドロップにより任意の位置に移動する。**

メモ

ガジェットの移動先候補は灰色で表示されます。

11.4.5 ガジェットの表示内容を保存する

ガジェットの表示内容（「ガジェットの追加と削除」ダイアログで選択したガジェットの種類とその位置情報）は以下の操作を行ったときに RTFS にファイルとして自動的に保存されます。RTFS とは、ヤマハルーターの不揮発性メモリーに構築されるファイルシステムのことです。

- ガジェットの追加、削除
- ガジェットの移動
- ガジェットの最小化、元に戻す

注意

- 一般ユーザーでログインして操作した場合、または RTFS の空き容量が足りない場合はガジェットの表示内容は保存されません。
- 工場出荷状態に戻したり RTFS をフォーマットしたりすると、ガジェットの表示内容は初期化されます。

メモ

本製品を再起動しても、ガジェットの表示内容は保存されています。

11.5 History 画面の各ガジェットの説明

History 画面に対応しているガジェットは以下の通りです。

- CPU 使用率 …146 ページ
- メモリ使用率 …146 ページ
- トラフィック情報（LAN/PP/TUNNEL）…146 ページ
- トラフィック情報（アプリケーション）…147 ページ
- NAT セッション数 …148 ページ
- ファストパスフロー数 …148 ページ
- 動的フィルターセッション数 …148 ページ

メモ

工場出荷状態では History 画面には CPU 使用率のガジェットのみ表示されています。

注意

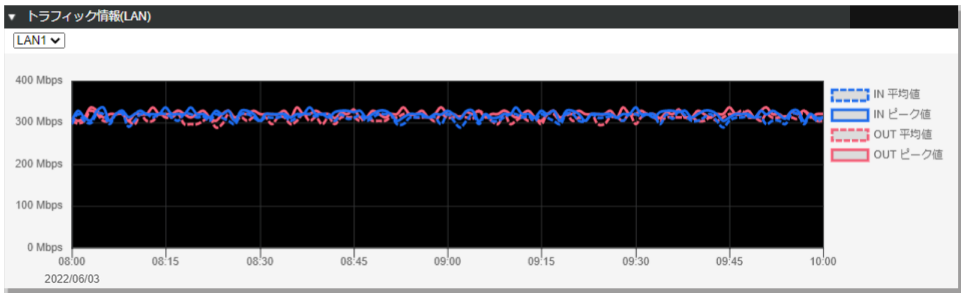
ガジェットに「統計情報の記録が有効になっていません。」と表示される場合は、「11.4.1 統計情報の記録を開始する」（138 ページ）を参照し、「統計情報の記録」を有効にしてください。

グラフの表示対象の切り替え

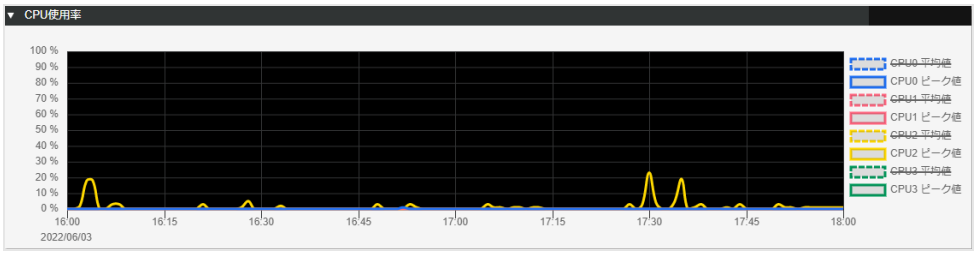
- 初期表示では平均値は破線、ピーク値は実線で表示されています。
- ガジェット右上にある凡例の各項目を押すと、その項目のグラフの表示 / 非表示を切り替えることができます。複数のグラフの線が重なっていたり、特定のインターフェースを監視したりする場合などに表示を切り替えてください。

グラフの平均値、ピーク値の詳細表示

グラフの線上にマウスカーソルを重ねると、その時刻の詳細情報（平均値、ピーク値）が表示されます。

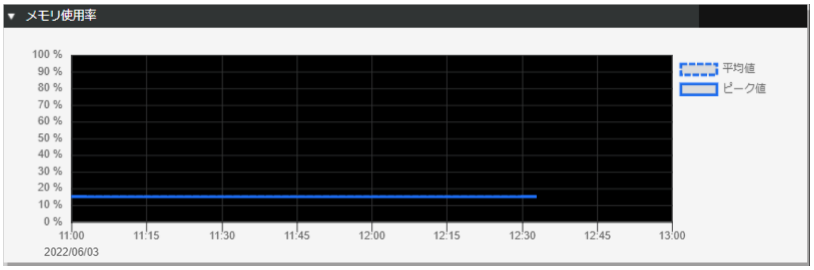


11.5.1 CPU 使用率



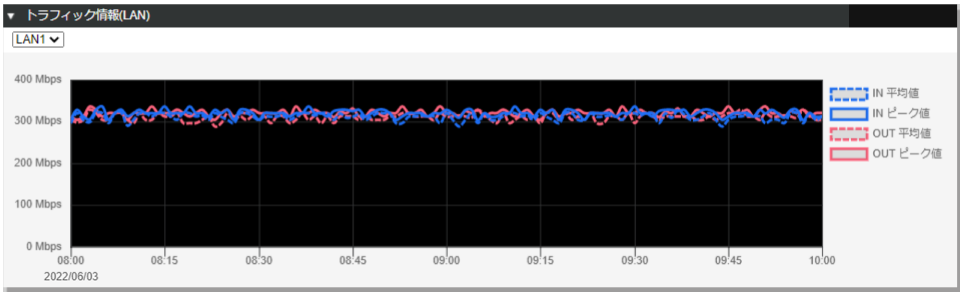
CPU 使用率の時間による変動を示すグラフが表示されます。

11.5.2 メモリ使用率



メモリ使用率の時間による変動を示すグラフが表示されます。

11.5.3 トラフィック情報（LAN/PP/TUNNEL）



各インターフェースの「IN 平均値」、「IN ピーク値」、「OUT 平均値」、「OUT ピーク値」の時間による変動を示すグラフが表示されます。

IN：該当インターフェースで受信するトラフィック
OUT：該当インターフェースから送信するトラフィック

メモ

- 使用中の LAN/PP/TUNNEL インターフェースのトラフィックのみ表示されます。
- トラフィック情報は、タグ VLAN インターフェースには対応していません。
- アプリケーション別のトラフィック情報については、「11.5.4 トラフィック情報（アプリケーション）」（147 ページ）をご覧ください。

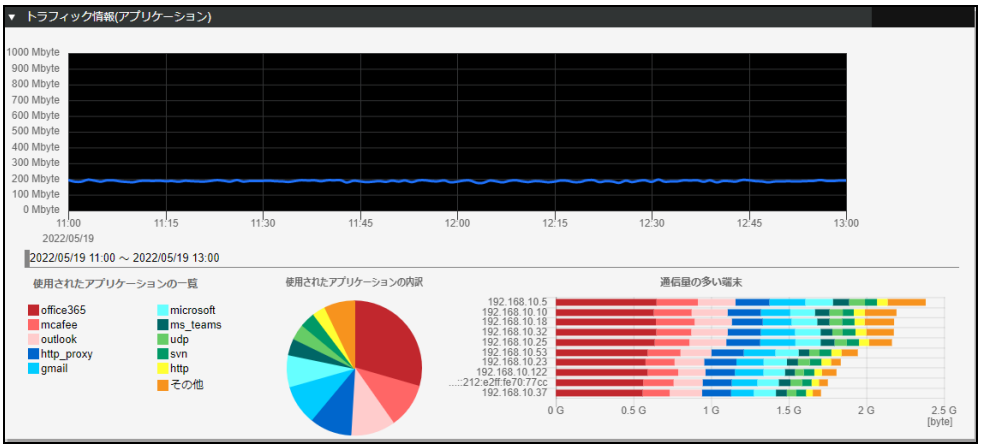
グラフの縦軸の上限はトラフィック量に応じて変動します。

グラフに表示するインターフェースを選択する

プルダウンメニューから、グラフに表示するインターフェースを選択することができます。

メモ
使用していないインターフェースはプルダウンメニューに表示されません。

11.5.4 トラフィック情報（アプリケーション）



各アプリケーションを使用した時間による変動と内訳を示すグラフが表示されます。

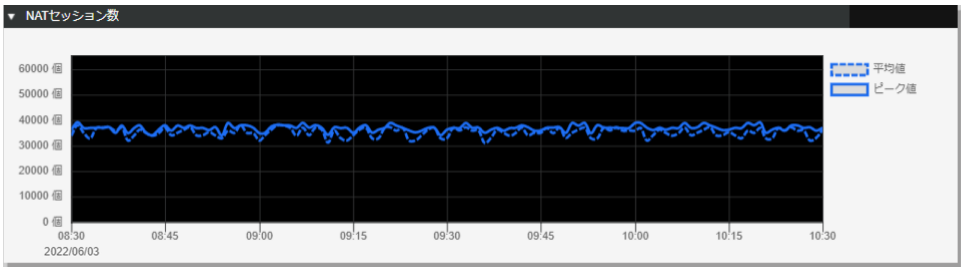
メモ
- アプリケーション別のトラフィック情報を表示するには、アプリケーション制御機能を有効にする必要があります。アプリケーション制御機能を有効にする方法は「第 16 章 アプリケーション制御（DPI）を利用する」（447 ページ）をご覧ください。
- 表示されるアプリケーションは「使用されたアプリケーションの一覧」の凡例に対応しています。

累計トラフィック量（上）
- すべての累計のトラフィック量を示すグラフが表示されます。
- グラフの線上にマウスカーソルを重ねると、日時やトラフィック量が表示されます。
- グラフの線上をクリックすると、下部にその時刻の内訳が表示されます。
  「2 時間分の表示に戻す」ボタンをクリックすると、グラフの表示が 2 時間分の累計に戻ります。
  グラフの表示期間に応じてボタンに表示される期間が変化します。

使用されたアプリケーションの内訳
- 期間中に使用されていたアプリケーションの内訳が表示されます。
- 円グラフ中にマウスカーソルを重ねると、アプリケーション名やトラフィック量、そのアプリケーションで通信量が多かった上位 3 つの端末の IP アドレスと通信量が表示されます。
- 円グラフ中の各アプリケーションをクリックすると、右の棒グラフのアプリケーションが変更されます。

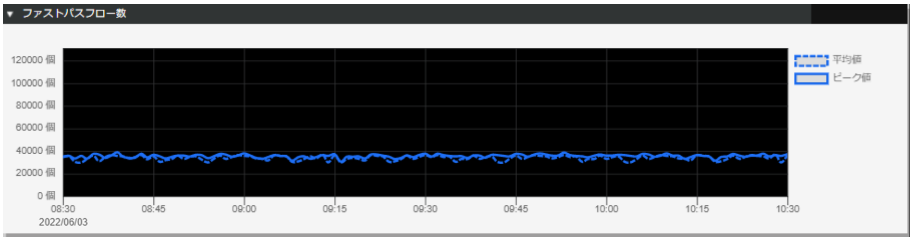
通信量の多い端末
- 期間中の通信量が多い端末が表示されます。
- 各列にマウスカーソルを重ねると、端末の IP アドレスとアプリケーションごとの通信量が表示されます。

11.5.5 NAT セッション数



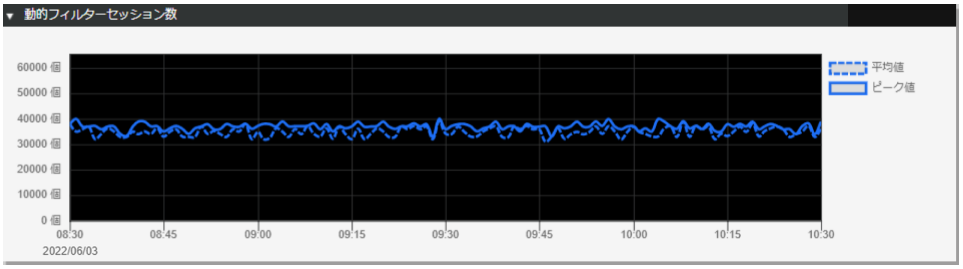
NAT セッション数の時間による変動を示すグラフが表示されます。

11.5.6 ファストパスフロー数



ファストパスフロー数の時間による変動を示すグラフが表示されます。

11.5.7 動的フィルターセッション数



動的フィルターセッション数の時間による変動を示すグラフが表示されます。

第 12 章 LAN マップを利用する

本章では、LAN マップの利用方法について説明します。
本章では、LAN マップを制御するヤマハルーターを「マネージャー」、マネージャーが制御しているヤマハネットワーク機器（ヤマハスイッチ、ヤマハ無線 AP、ヤマハルーター、ヤマハ UTM アプライアンス）の総称を「エージェント」と呼びます。また、エージェントとして動作しているヤマハスイッチを「エージェントスイッチ」、ヤマハ無線 AP を「エージェント AP」、ヤマハルーターを「エージェントルーター」、ヤマハ UTM アプライアンスを「エージェント UTM」と呼びます。

・ LAN マップとは？ …149 ページ
・ LAN マップの画面構成 …149 ページ
・ LAN マップを有効にする …153 ページ
・ エージェントの状態を確認する …155 ページ
・ ネットワークの異常を監視する …157 ページ
・ 機器を検索する …161 ページ
・ ヤマハスイッチを設定する …163 ページ
・ ヤマハ無線 AP の設定を行う …190 ページ
・ エージェントルーターの設定を行う …202 ページ
・ ヤマハ UTM アプライアンスの設定を行う …204 ページ
・ タグ VLAN を設定する …206 ページ
・ マルチプル VLAN を設定する …213 ページ
・ 接続機器の一覧を見る …218 ページ

12.1 LAN マップとは？

LAN マップでは、LAN 内に存在するエージェントと、その配下のパソコンやプリンター、ネットワークカメラ、POS 端末、スマートデバイスなどの通信端末の配置図をウェブブラウザー上に表示します。また、「LAN マップ」画面でエージェントの設定を変更したり、ネットワークの異常を一目で把握したりすることもできるため、ネットワーク管理者の作業負荷を軽減します。

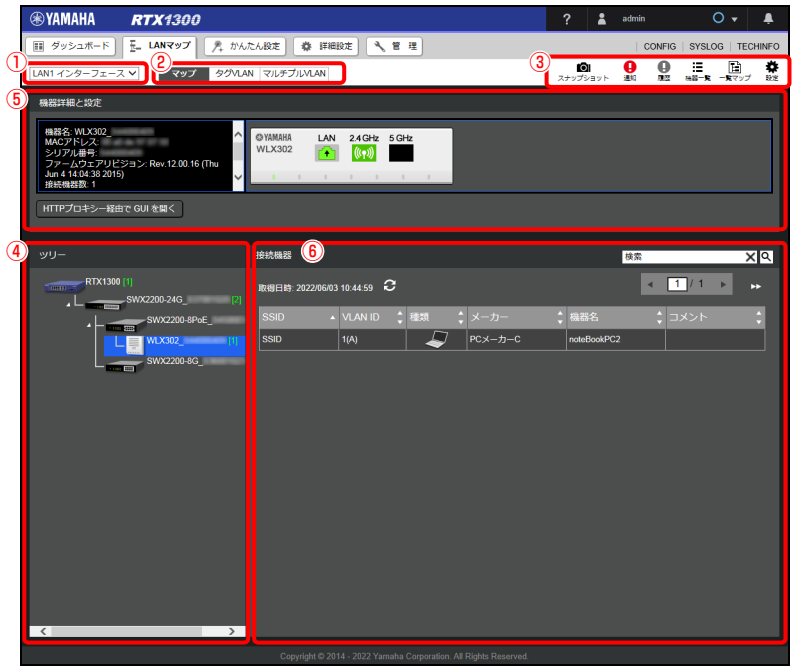
12.2 LAN マップの画面構成

LAN マップは主に以下の画面で構成されており、画面上部の表示選択スイッチにより画面を切り替えることができます。

- マップページ …150 ページ
- タグ VLAN ページ …151 ページ
- マルチプル VLAN ページ …152 ページ

12.2.1 マップページ

ネットワークの状態が可視化されます。機器の接続状況を確認したり、エージェントの設定を変更したりすることができます。



① インターフェース選択プルダウンメニュー
LAN マップを表示したいインターフェースを選択します。LAN マップが有効になっていないインターフェースは選択できません。LAN マップを有効にする方法は、「12.3 LAN マップを有効にする」（153 ページ）をご覧ください。

② 表示選択スイッチ
LAN マップで表示したいページを選択します。

③ 各種ボタン
LAN マップの設定内容や通知メッセージなどを確認したり、スナップショットを保存したりするためのボタンが配置されています。

④ ツリービュー
マネージャーを起点としたエージェントのトポロジーが表示されます。他社製ネットワーク機器は表示されません。「ツリービュー」で「機器」アイコンをクリックすると、「機器詳細と設定ビュー」と「接続機器ビュー」に機器の情報が表示されます。

⑤ 機器詳細と設定ビュー
「ツリービュー」で選択したマネージャー、およびエージェントの詳細情報と機器の詳細画像が表示されます。

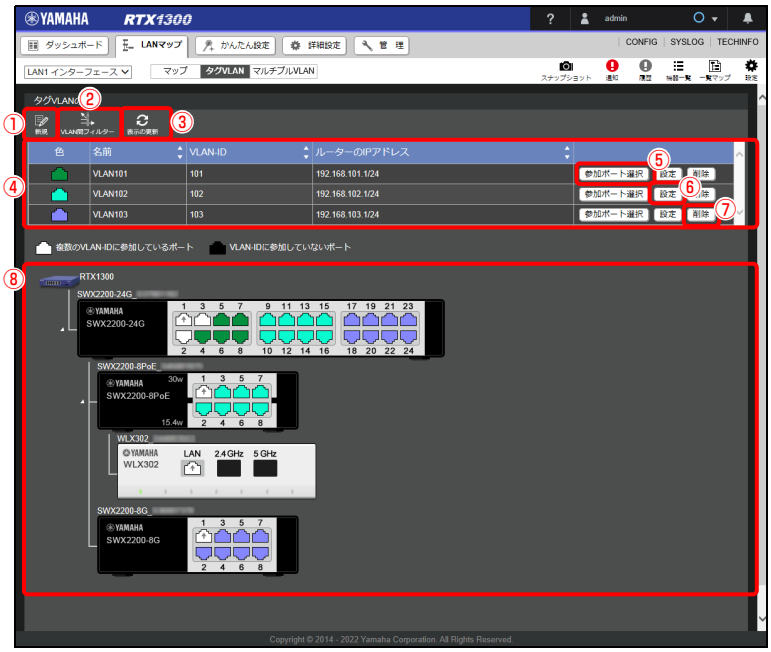
⑥ 接続機器ビュー
「ツリービュー」で選択したマネージャー、およびエージェントに接続されている機器が表示されます。端末管理が有効になっていない場合、端末の情報は表示されません。端末管理を有効にする方法は、「12.3 LAN マップを有効にする」（153 ページ）をご覧ください。

12.2.2 タグ VLAN ページ

VLAN を作成してエージェントのポートをグループ分けすることができます。また、VLAN ごとに IP アドレスを付加したり、すべての VLAN 間の通信を遮断したりすることができます。

メモ

タグ VLAN の設定の対応機器については、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/tag_vlan.html



①「新規」ボタン
VLAN グループを新たに作成します。ポートを VLAN グループに参加させるには、事前に VLAN グループを作成しておく必要があります。

②「VLAN 間フィルター」ボタン
すべての VLAN 間の通信について、全開放または全遮断を行います。新たに作成した VLAN と既存 VLAN 間の通信は開放されています。必要があれば全遮断を行ってください。

③「表示の更新」ボタン
トポロジー情報と VLAN 設定情報を取得し、タグ VLAN グループ一覧とトポロジーを再描画します。

④ タグ VLAN グループ一覧
登録されている VLAN グループの一覧が表示されます。VLAN グループごとにポートの色が割り当てられます。

⑤「参加ポート選択」ボタン
ポートをタグ VLAN グループに参加させることができます。ボタンを押した後、トポロジー内にあるエージェントのポートを選択する必要があります。

⑥「設定」ボタン
該当のタグ VLAN グループの設定を変更します。名前、ルーターの IP アドレスを変更することができます。

⑦「削除」ボタン
該当のタグ VLAN グループを削除します。

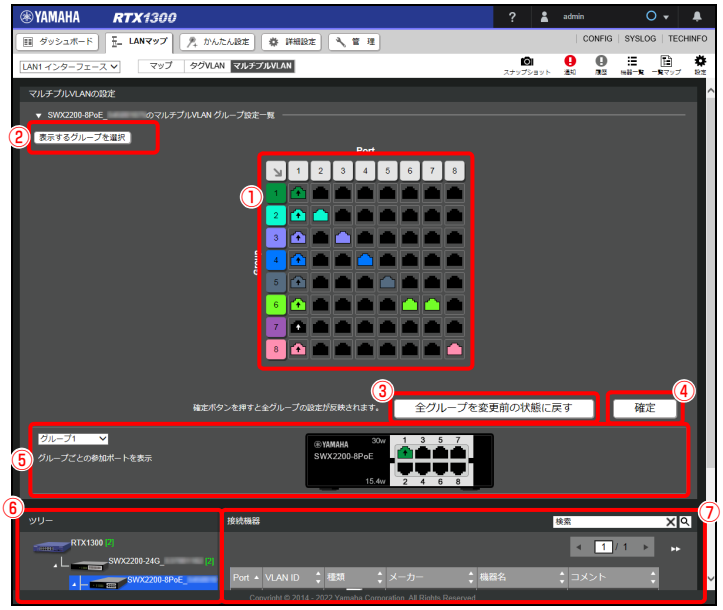
⑧ トポロジー
マネージャーを起点としたエージェントのトポロジーが表示されます。エージェントのポートの色を確認することによって、どの VLAN グループに参加しているかわかります。

12.2.3 マルチプル VLAN ページ

ひとつのスイッチのポートを複数のグループに分けて、グループ間の通信を遮断することができます。ポートを複数のグループに分けるだけでなく、ひとつのポートを複数のグループに参加させることもできます。たとえば、サーバーやルーターなど全グループと通信を行う必要がある端末が接続されるポートは、すべてのグループに重複して参加させます。なお、マルチプル VLAN ではグループが異なっても同じネットワークアドレスが使用されます。

メモ

マルチプル VLAN の設定の対応機器については、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/multiple_vlan.html



① マルチプル VLAN グループ設定一覧
マルチプル VLAN のグループごとの参加ポートの状態を、表の形式で表示します。表の横方向はスイッチのポート、縦方向はマルチプル VLAN グループを表し、表内の各ポートアイコン（ など）をクリックすることで各グループに参加させるポートを選択することができます。

②「表示するグループを選択」ボタン
「マルチプル VLAN グループ設定一覧」の表に表示するグループを選択することができます。

③「全グループを変更前の状態に戻す」ボタン
各マルチプル VLAN グループに参加させるポートの編集内容を変更前の状態に戻します。

④「確定」ボタン
各マルチプル VLAN グループに参加させるポートの編集内容を設定に反映します。

⑤ 現在のマルチプル VLAN 設定内容
設定済みのマルチプル VLAN グループごとの設定内容を表示します。左側のプルダウンメニューで選択したグループに対する各ポートの参加状態を右側のスイッチ画像内に表示します。

⑥ ツリービュー
マップページで表示されるものと同一です。マルチプル VLAN に対応しているエージェントを選択した場合は「マルチプル VLAN の設定ビュー」にマルチプル VLAN の設定が表示されます。

⑦ 接続機器ビュー
マップページで表示されるものと同一です。スイッチのどのポートにどのような機器が接続されているかが確認できるため、マルチプル VLAN グループ設定時の参考にすることができます。

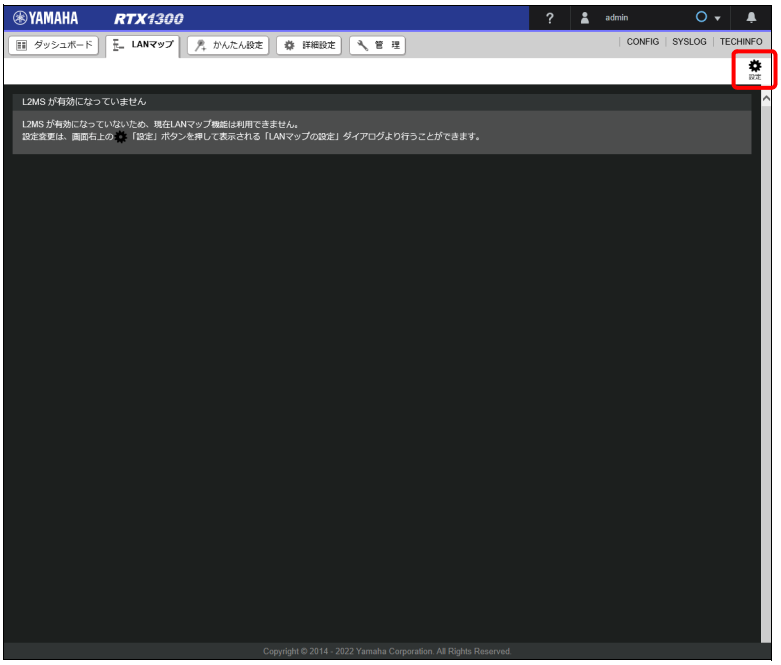
12.3 LAN マップを有効にする

LAN マップを使用するための設定方法を説明します。端末の検索を行う間隔を変更したり、スナップショット機能の設定を行ったりすることができます。

メモ

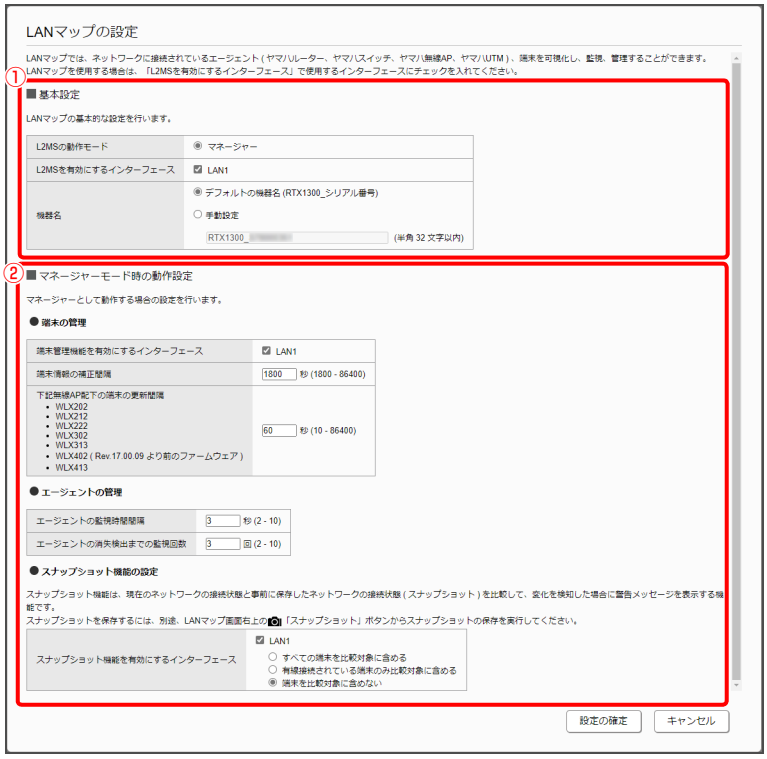
LAN 分割機能が設定されているインターフェースでは、LAN マップは使用できません。

1.「設定」ボタンをクリックする。



「LAN マップの設定」ダイアログが表示されます。

2.「L2MS を有効にするインターフェース」で、LAN マップを使用したいインターフェースを選択する。



① 基本設定：

LAN マップの基本的な設定を行います。

- L2MS の動作モード：動作モードを選択します。
- L2MS を有効にするインターフェース：有効にするインターフェースにチェックを入れます。
- 機器名：LAN マップ上で機器名として表示される名称を設定します。

② マネージャーモード時の動作設定：

マネージャーとして動作する場合の設定を行います。

- 端末の管理：基本設定で「L2MS を有効にするインターフェース」にチェックを入れたインターフェースが表示されるので、端末管理機能を有効にするインターフェースにチェックを入れ、端末情報の補正間隔と無線 AP 配下の端末の更新間隔を設定します。
- エージェントの管理：エージェントの監視時間間隔とエージェントの消失検出までの監視回数を設定します。
- スナップショット機能の設定：基本設定で「L2MS を有効にするインターフェース」にチェックを入れたインターフェースが表示されるので、スナップショット機能を有効にするインターフェースにチェックを入れ、対象とする端末の種類をインターフェースごとに以下から選択します。
  - すべての端末を比較対象に含める：無線接続端末と有線接続端末の両方を比較対象とします。
  - 有線接続されている端末のみ比較対象に含める：有線接続端末のみを比較対象とします。
  - 端末を比較対象に含めない：無線接続端末と有線接続端末のどちらもスナップショットの比較対象としません。

メモ

スナップショット機能は、現在のネットワークの接続状態と事前に保存したネットワークの接続状態（スナップショット）を比較して、変化を検知した場合に警告メッセージを表示する機能です。

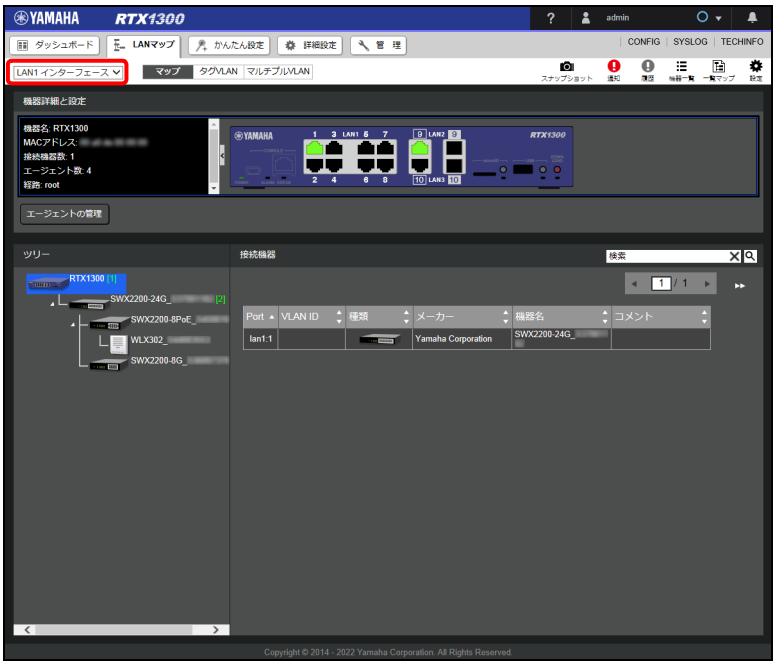
3.**「設定の確定」ボタンをクリックする。**

設定が反映され、「LAN マップ」画面が表示されます。

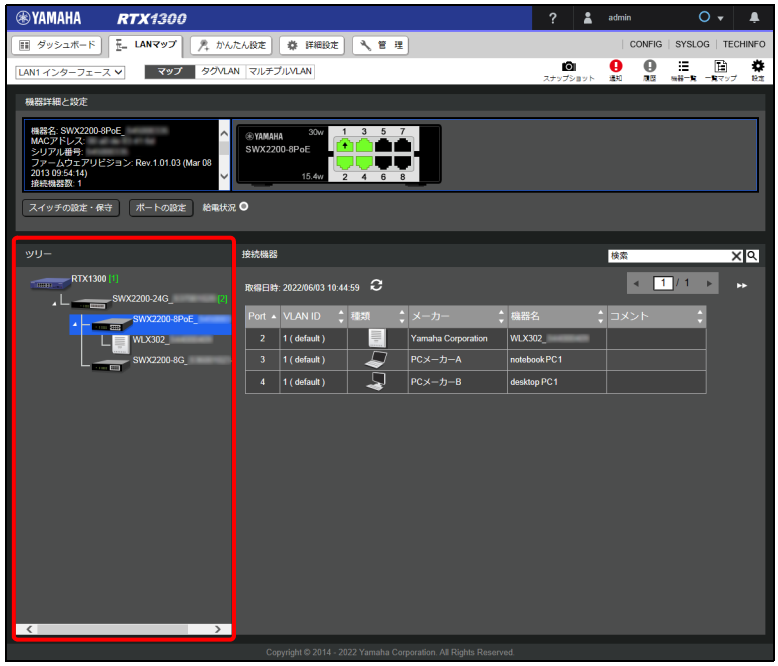
12.4 エージェントの状態を確認する

マネージャーに接続した、エージェントや端末の接続状況の確認方法を説明します。

1. **確認したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。**



2. **ツリービューで確認したい機器を選択する。**



機器詳細と設定ビューに機器の画像が表示され、ポートアイコンからリンク状態を確認することができます。また、ポートをクリックするとポートの詳細情報を確認することができます。

ポートアイコンはリンク状態によって以下のように表示されます。

LAN ポートの場合

アイコン	説明
	ポートスピード 10GBASE-T
	ポートスピード 5GBASE-T
	ポートスピード 2.5GBASE-T
	ポートスピード 1000BASE-T
	ポートスピード 100BASE-TX
	ポートスピード 10BASE-T
	異常発生
	リンクダウン

SFP ポートの場合

アイコン	説明
	ポートスピード 10GbE
	ポートスピード 1GbE
	異常発生
	リンクダウン
	スタックポート

メモ

ポートアイコンに上向き矢印が付いているポートはアップリンクポートを表しています。

PoE 対応スイッチを選択した場合

機器詳細と設定ビューの「給電状況」ボタンをクリックすると、PoE 給電状況を確認することができます。ポートアイコンは給電状況によって下記のように表示されます。

アイコン	説明
	PoE 給電中（給電 Class0 ～ 3）
	PoE 給電中（給電 Class4）
	PoE 給電は行わない
	給電停止（異常発生）
	給電停止

メモ

上記のアイコンは、SWX2200-8PoE を例としています。SWX2100-10PoE、および SWX2100-5PoE ではポートアイコンの色が異なります。
ポートアイコンについて詳しくは、下記の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/map.html#SLAVE

無線 AP を選択した場合

機器詳細と設定ビューに表示された無線 AP の画像内にある  をクリックすると、無線通信状況を確認することができます。  は無線通信が有効になっている場合に、使用している周波数帯域（2.4GHz 帯、5GHz 帯）ごとに表示されます。

12.5 ネットワークの異常を監視する

ネットワークの異常を監視する方法を説明します。エージェントの動作状況の変化や異常を検知すると、通知エリアおよび履歴エリアにメッセージが表示されます。

通知エリア

現在のネットワークに対するメッセージが表示されます。通知エリアは新しいメッセージが追加されると自動的に表示され、「  」ボタンをクリックすることでも表示することができます。また、メッセージが表示されている状態で「  」ボタンをクリックすると通知エリアを閉じることができます。

メモ

検知された状態が解消されるとメッセージの表示が消えます。その場合でもメッセージは履歴エリアに残ります。

履歴エリア

通知メッセージの履歴が表示されます。履歴は最大で 1000 件まで保存され、最大件数を超える場合は古いメッセージから削除されます。履歴エリアは「  」ボタンをクリックすることで表示することができます。なお、通知エリアに表示されたメッセージが前回のメッセージから変化していない場合は履歴には追加されません。

12.5.1 エージェントの動作状況と異常を監視する

ヤマハスイッチの下記の動作や異常を検知すると、通知エリアおよび履歴エリアにメッセージが表示されます。両エリアに表示されるメッセージと片方のみに表示されるメッセージがあります。

検知項目	通知エリア	履歴エリア
ヤマハスイッチのファンが停止した	○	○
ヤマハスイッチのポートでループが発生した	○	○
ヤマハスイッチのポートの給電が停止した	×	○
ヤマハスイッチのポートで給電を開始した（給電 Class ごと）	×	○
ヤマハスイッチの給電が異常停止した	○	○
ヤマハスイッチの電源に異常が発生した	○	○
ヤマハスイッチの供給電力が最大供給電力を超えた	○	○
ヤマハスイッチがバックアップ経路で接続された	○	○
ヤマハスイッチがメイン経路で接続された	×	○
ヤマハスイッチのポートの SFP 受光レベルが下限閾値を下回った	○	○
ヤマハスイッチのポートの SFP 受光レベルが上限閾値を超えた	○	○
ヤマハスイッチのポートの SFP 受光レベルが正常に戻った	×	○

12.5.2 ネットワークの接続状態を監視する

スナップショット機能を使用してネットワークの接続状態を監視できます。スナップショット機能は、現在のネットワークの接続状態と事前に保存したネットワークの接続状態（スナップショット）を比較して、変化を検知した場合に警告メッセージを表示する機能です。事前に「12.3 LAN マップを有効にする」（153 ページ）を参照し、スナップショット機能を有効にしてください。スナップショット機能が有効になっている状態で、以下の操作を行ってはじめてスナップショット機能が動作し始めます。

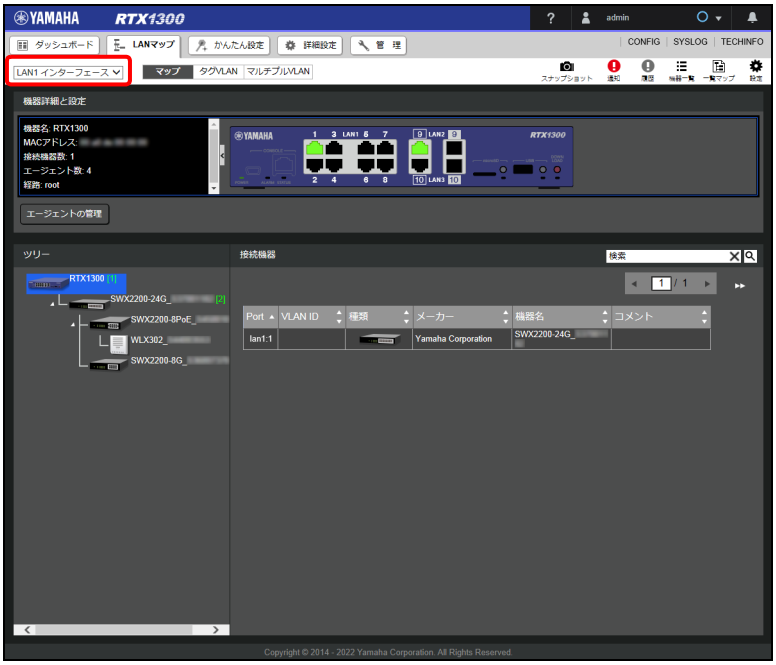
メモ

ベースとなるネットワークの接続状態（エージェントや端末の配置）が変わった場合は、その都度本操作を行ってスナップショットを保存し直してください。

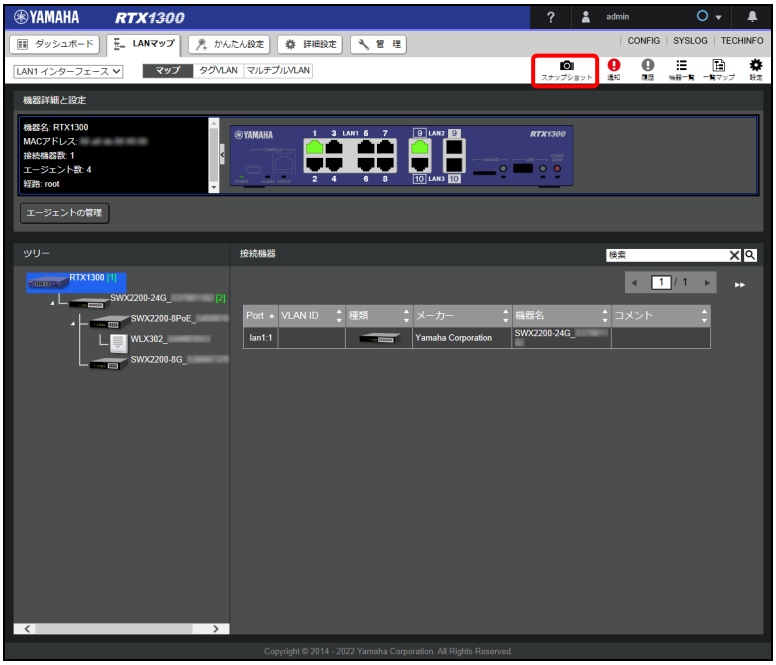
ネットワークの接続状態を保存する

現在のネットワークの接続状態を保存します。

1. 監視したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



2. 「 スナップショット 」ボタンをクリックする。



「スナップショットの保存」ダイアログが表示されます。

3.「実行」ボタンをクリックする。

重要

エージェントの経路情報の反映が完了していない場合がありますので、現在の経路をご確認の上、スナップショットを保存してください。

メモ

「保存前にネットワークの接続状態を更新する」にチェックを入れた場合は、ネットワークの接続状態の情報を更新した後に保存します。ただし、ネットワークの構成によっては保存が完了するまでに 20 ～ 30 分程かかる場合があります。その間も他の操作は行えます。

変化を検知した場合

保存したネットワークの接続状態からの変化を検知すると、通知エリアおよび履歴エリアに下記のメッセージが表示されます。両エリアに表示されるメッセージと片方のみに表示されるメッセージがあります。

検知項目	通知エリア	履歴エリア
スナップショットに登録されていない機器が接続されている	○	○
機器の接続ポートがスナップショットと異なっている	○	○
スナップショットに登録されている機器が接続されていない	○	○
異常が検出されていた機器がスナップショットと一致した	×	○

12.5.3 ネットワークの異常をメールで通知する

ネットワークの異常を検知すると、登録した宛先にメールでお知らせします。

通知内容	通知方法
LAN マップの異常検知	LAN マップの異常を検知した場合、メールで通知します。
内部状態 インターフェース情報 経路情報 VPN 接続状態 NAT ファイアウォール 設定内容・ログ	内部状態については、自動で通知されません。「メール通知」画面の「いますぐ通知」の「進む」ボタンをクリックして、表示されるダイアログの「実行」ボタンをクリックすると、ヤマハルーターの内部状態を登録した宛先へ通知します。

メモ

メール通知の設定について詳しくは、「14.12 メール通知機能を使う」（386 ページ）をご覧ください。

12.6 機器を検索する

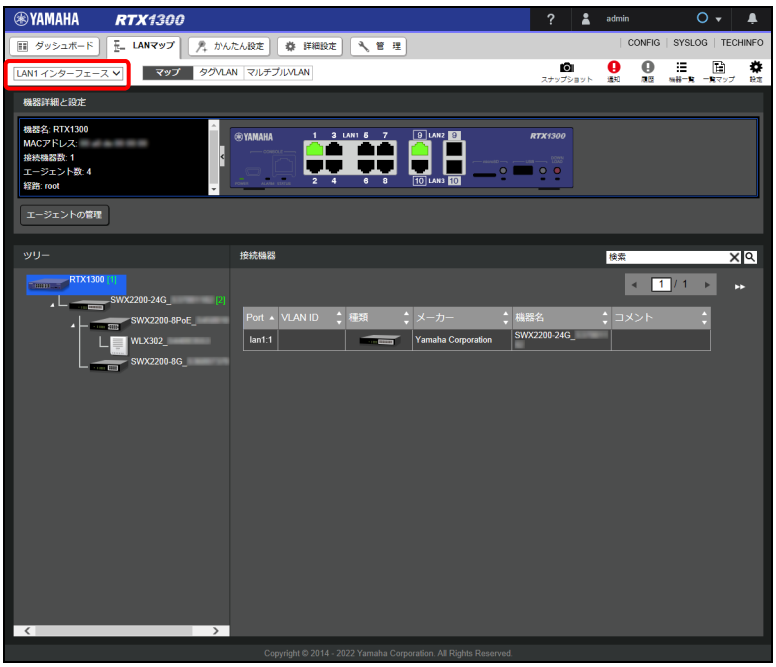
ネットワークに存在する機器を任意のキーワードで検索することができます。
機器検索はキーワードと以下の機器情報を比較することで行われます。

- 経路
- SSID
- VLAN ID
- メーカー
- 機器名
- コメント
- MAC アドレス
- IP アドレス
- 機種名
- OS
- 周波数

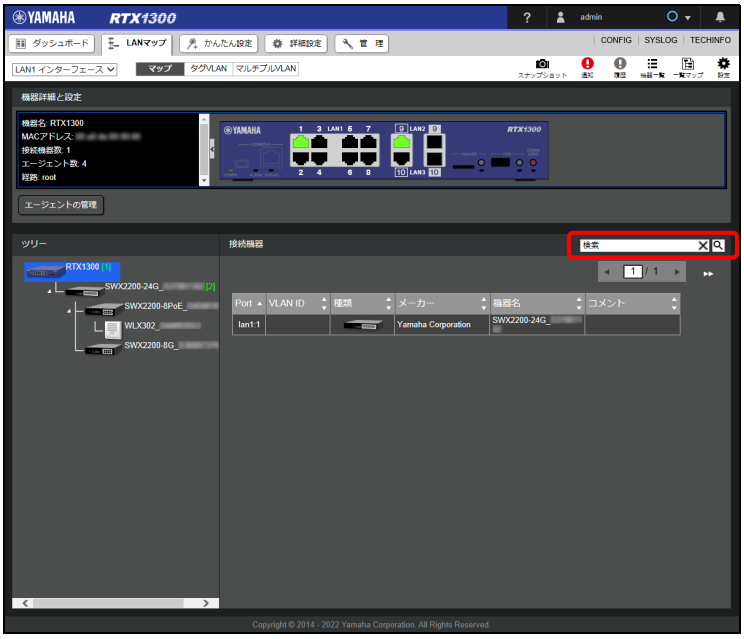
メモ

キーワードの大文字 / 小文字は区別されません。

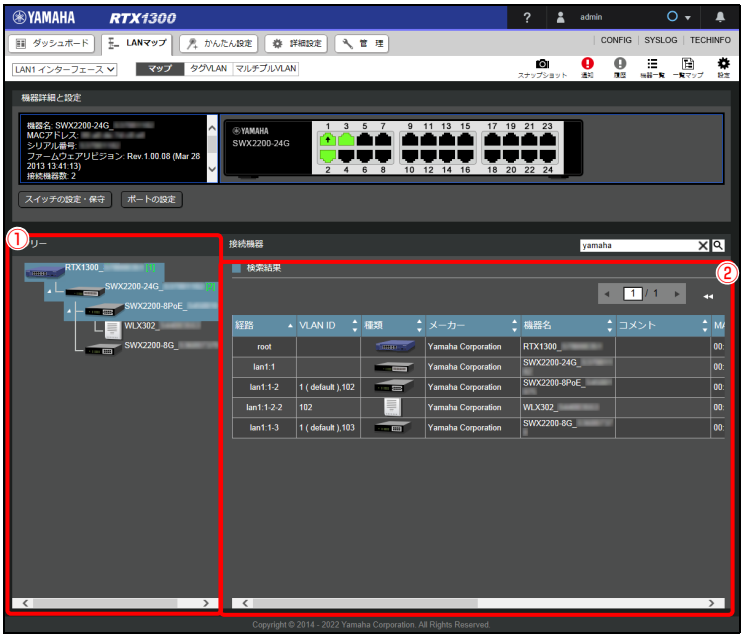
1. **機器を検索したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。**



2. 接続機器ビューの検索ボックスに任意のキーワードを入力し、「 🔍 」ボタンをクリックする。



検索結果が表示されます。



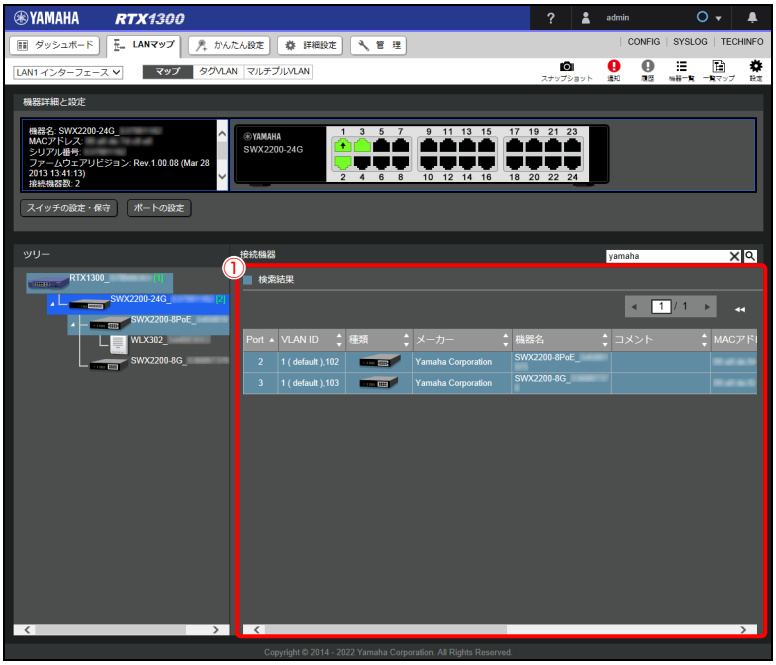
① **ツリービュー：**
検索でヒットした機器が接続されている機器アイコンがブルーグレーでハイライト表示されます。
マネージャー、およびエージェントを選択すると「接続機器ビュー」に接続機器の一覧が表示されます。

② **検索結果：**
検索でヒットした機器の一覧が表示されます。

メモ

検索結果の表示を解除するには、「 ✕ 」ボタンをクリックしてください。

3. 検索でヒットした機器が接続されているエージェントをツリービューで選択する。



① **接続機器ビュー：**
検索でヒットした機器アイコンがブルーグレーでハイライト表示されます。異常検知による赤のハイライトと重なった場合は、ブルーグレーが優先されます。

メモ
検索結果の表示を解除するには、「✕」ボタンをクリックしてください。

12.7 ヤマハスイッチを設定する

ヤマハスイッチの設定には、スイッチの Web GUI を使う方法と LAN マップ上のダイアログを使う方法があります。

スイッチの Web GUI を使う方法

LAN マップで「HTTP プロキシー経由で GUI を開く」ボタンをクリックします。スイッチの Web GUI が別ウィンドウで表示され、設定を変更することができます。
スイッチの Web GUI の使用方法については、各スイッチの技術資料をご確認ください。

LAN マップ上のダイアログを使う方法

LAN マップ上のダイアログを使う設定方法については、「12.7.1 スイッチの設定・保守ダイアログを表示する」から「12.7.15 スイッチの指定方法を選択する」をご覧ください。SWX2200 シリーズの画面を例にして説明します。

メモ
ヤマハスイッチの機種ごとに対応している設定方法が異なります。詳細は以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/swctl/l2ms_gui_comparison.html#FUNCTION_LIST2

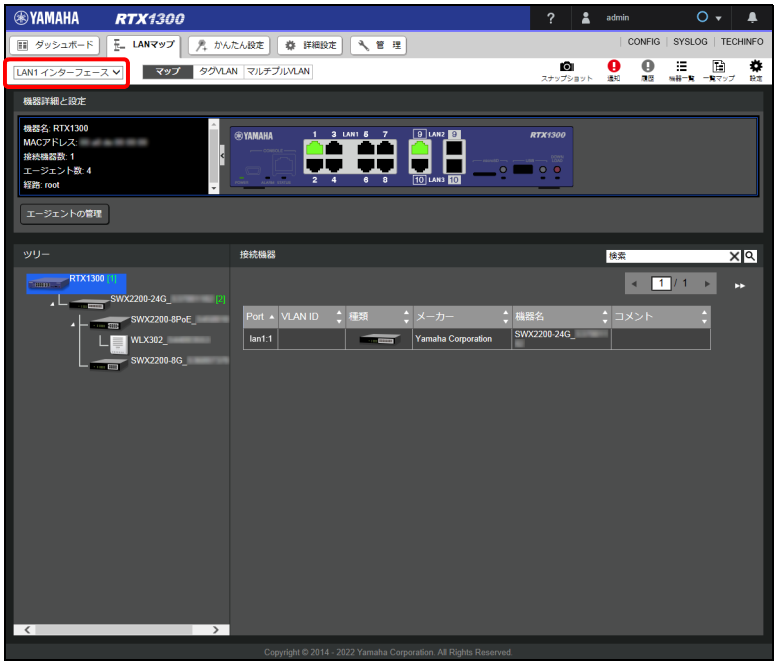
12.7.1 スイッチの設定・保守ダイアログを表示する

設定変更や保守機能を実行するヤマハスイッチの「スイッチの設定・保守」ダイアログを表示します。

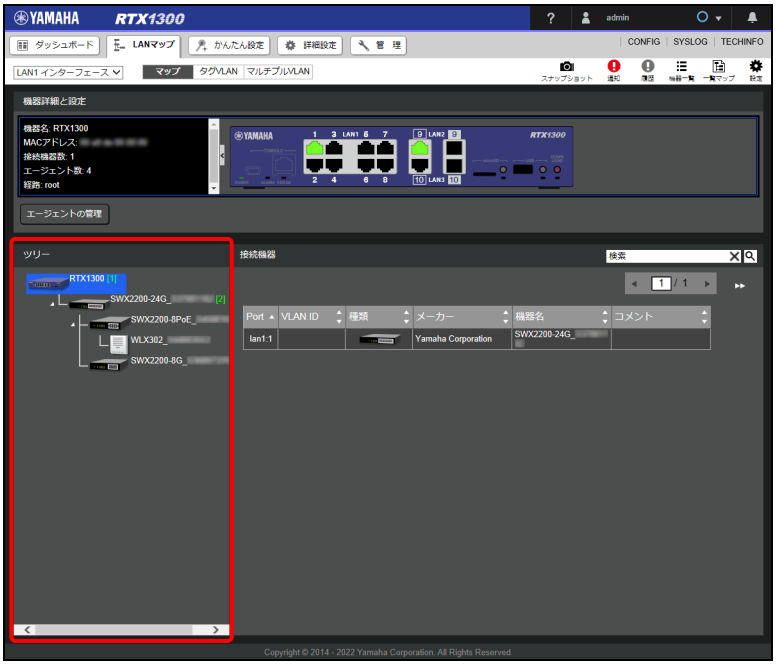
メモ

ヤマハスイッチの種類によって、設定・保守ダイアログの設定内容や表示が異なります。詳細は以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/map.html#SWITCH

1. **設定・保守したいヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

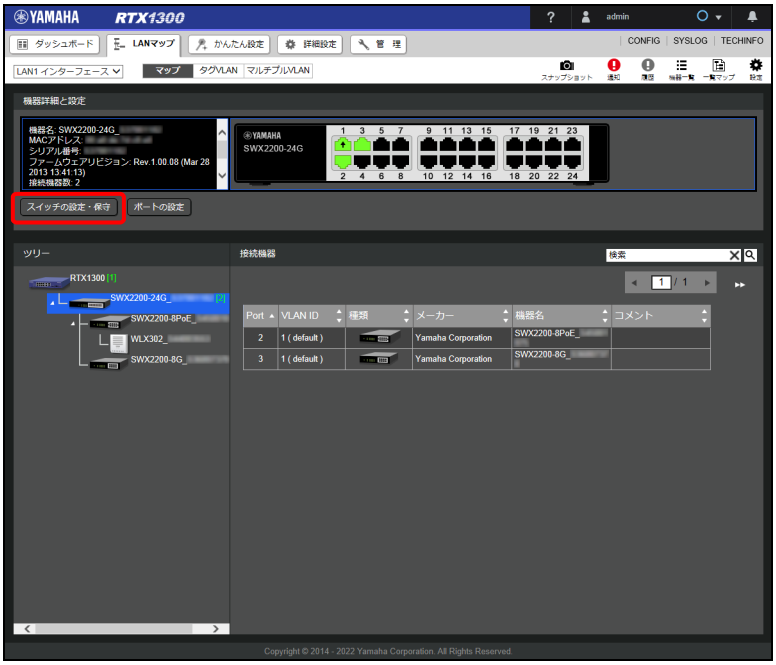


2. ツリービューでヤマハスイッチを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「スイッチの設定・保守」ボタンをクリックする。



「スイッチの設定・保守」ダイアログが表示されます。

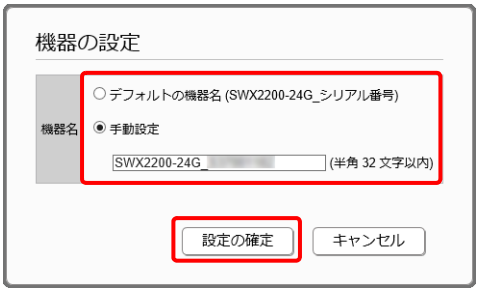
12.7.2 ヤマハスイッチの機器名を変更する

ヤマハスイッチの機器名を変更することができます。工場出荷時は、“機種名_シリアル番号”という形式で機器名が付与されています。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「機器名」項目の「設定」ボタンをクリックする。**

「機器の設定」ダイアログが表示されます。

3. **デフォルトの機種名または手動設定を選択（手動設定の場合は任意の名称を入力）し、「設定の確定」ボタンをクリックする。**



設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

12.7.3 省電力機能を設定する

省電力機能の設定を変更することができます。ヤマハスイッチには待機時の消費電力をカットする省電力機能が搭載され、動作モードをエコノミーモードに切り替えることで電力を節約することができます。

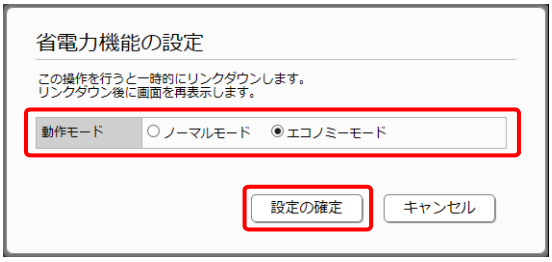
エコノミーモード時の動作

- リンクダウンしているポートの待機電力の低減
- ケーブル長検出による電力供給量の自動調節
- インジケーターの明るさ調整

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「省電力機能」項目の「設定」ボタンをクリックする。**

「省電力機能の設定」ダイアログが表示されます。

3. **動作モードでエコノミーモードを選択し、「設定の確定」ボタンをクリックする。**



設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

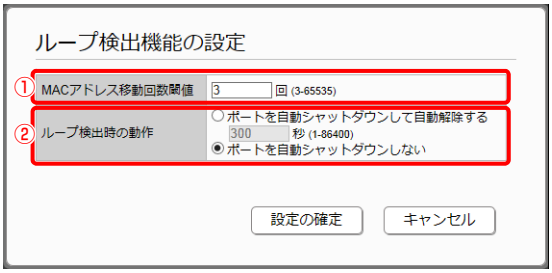
12.7.4 ループ検出機能を設定する

ループ検出機能の設定を変更することができます。ループ検出機能を有効にすると、誤ってループ状態が構成されブロードキャスト / マルチキャスト・ストームが発生した場合に自動的にループが発生したポートを一定時間シャットダウンすることができます。この動作により、ネットワーク全体が利用できなくなる状態を防ぐことができます。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「ループ検出機能の設定」項目の「設定」ボタンをクリックする。**

「ループ検出機能の設定」ダイアログが表示されます。

3. **ループ検出機能を設定する。**



① MAC アドレス移動回数閾値：
MAC アドレスのラーニング元ポートの移動回数の閾値を設定します。一定時間内にこの閾値に達するとループが発生したと判断されます。

② ループ検出時の動作：
ループ検出時にポートを一定時間シャットダウンする場合は、「ポートを自動シャットダウンして自動解除する」を選択します。また、シャットダウンを解除する時間も設定します。

メモ

「12.7.11 ポートの基本機能を設定する」（180 ページ）で、ループ検出機能を「使用する」に設定しているポートが対象となります。工場出荷状態ではすべてのポートで「使用する」が設定されています。

4. **「設定の確定」ボタンをクリックする。**
設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

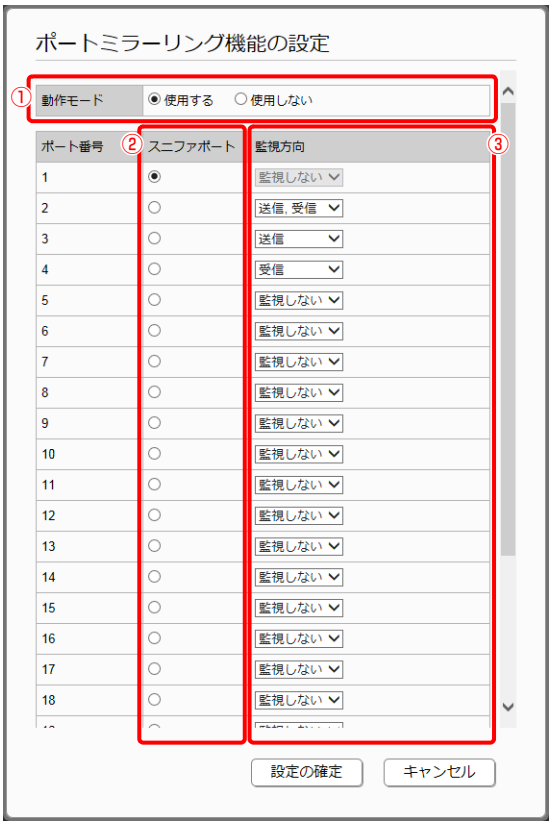
12.7.5 ポートミラーリング機能を設定する

ポートミラーリング機能の設定を変更することができます。ポートミラーリング機能を有効にすると、任意のポートのトラフィックを、指定したポートにコピーすることが可能になります。コピーされたパケットを採取することで通信状況を解析できます。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「ポートミラーリング機能」項目の「設定」ボタンをクリックする。**

「ポートミラーリング機能の設定」ダイアログが表示されます。

3. **ポートミラーリング機能を設定する。**



① 動作モード：
ポートミラーリング機能を使用するか否かを設定します。

② スニファポート：
コピー先のポートを設定します。

③ 監視方向：
各ポートのトラフィックの監視したい方向（コピーしたい方向）を設定します。

4. **「設定の確定」ボタンをクリックする。**
設定が反映され、「スイッチの設定・保守」ダイアログに戻ります。

12.7.6 フレームカウンタをリセットする

「マップページ」の機器詳細と設定ビューで、機器画像内のポートを選択するとポートの情報が表示されます。その際に表示されるフレームカウンタ（統計情報）の値をリセットすることができます。

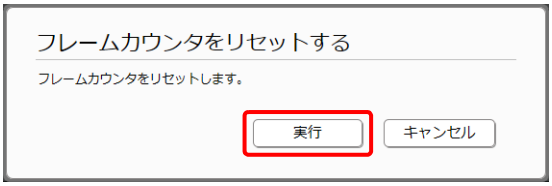
メモ

フレームカウンタの設定について詳しくは、「12.7.13 フレームカウンタを設定する」（183 ページ）をご覧ください。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「フレームカウンタをリセットする」欄の「進む」ボタンをクリックする。**

「フレームカウンタをリセットする」ダイアログが表示されます。

3. **「実行」ボタンをクリックする。**



フレームカウンタがリセットされ、「スイッチの設定・保守」ダイアログに戻ります。

12.7.7 ファームウェアを更新する

ヤマハスイッチのファームウェアを更新することができます。ヤマハスイッチでは外部メモリー（USB メモリーまたは microSD カード）に保存したファームウェアをマネージャーに読み込ませて更新します。

注意

- ファームウェアの更新を始めたら、完了してヤマハスイッチが再起動するまで他の操作は絶対しないでください。万一、中断したときはヤマハスイッチが使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- ファームウェアの更新が完了すると、ヤマハスイッチは自動的に再起動されるため、すべての通信が切断されます。
- ファームウェアの更新中は、絶対にケーブルを抜かないでください。ヤマハスイッチが使えなくなり、持ち込み修理が必要となる場合があります。
- FAT または FAT32 形式でフォーマットされていない外部メモリーは、マネージャーで使用できません。
- マネージャーの USB インジケーターまたは microSD インジケーターが点灯／点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損することがあります。USB ボタンまたは microSD ボタンを 2 秒間押し続けて、USB インジケーターまたは microSD インジケーターが消灯していることを確認してから外部メモリーを取り外してください。

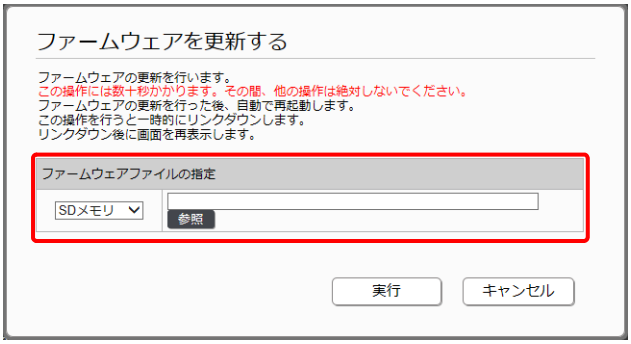
メモ

USB ハブを介して、複数の USB メモリーなどの外部メモリーをマネージャーに接続することはできません。

1. **ヤマハスイッチのファームウェアを保存した外部メモリーを用意する。**
2. **外部メモリーをマネージャーの USB ポートまたは microSD スロットに挿し込む。**
3. **「スイッチの設定・保守」ダイアログを表示する。**
4. **「ファームウェアを更新する」欄の「進む」ボタンをクリックする。**

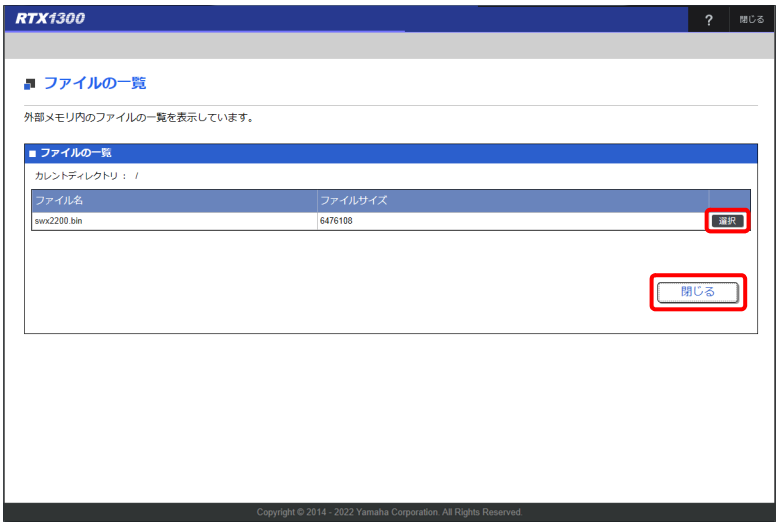
「ファームウェアを更新する」ダイアログが表示されます。

5. 外部メモリーの種類を選択し、「参照」ボタンをクリックする。

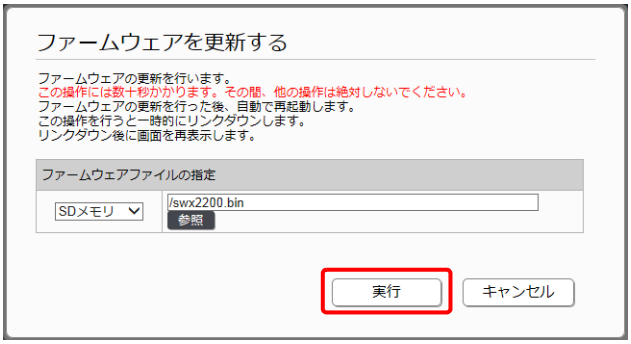


「ファイルの一覧」画面が表示されます。

6. 更新に使用するファームウェアファイルを選択し、「閉じる」ボタンをクリックする。



7. 「実行」ボタンをクリックする。



ファームウェアの更新が開始されます。ファームウェアの更新が終了すると、ヤマハスイッチは自動的に再起動します。

12.7.8 ヤマハスイッチを再起動する

ヤマハスイッチを再起動することができます。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「再起動を行う」欄の「進む」ボタンをクリックする。**

「再起動を行う」ダイアログが表示されます。

3. **「実行」ボタンをクリックする。**

ヤマハスイッチが再起動されます。

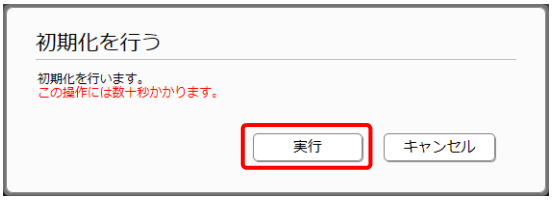
12.7.9 ヤマハスイッチを初期化する

ヤマハスイッチの設定内容を工場出荷状態に戻すことができます。

1. **「スイッチの設定・保守」ダイアログを表示する。**
2. **「初期化を行う」欄の「進む」ボタンをクリックする。**

「初期化を行う」ダイアログが表示されます。

3. **「実行」ボタンをクリックする。**



ヤマハスイッチが初期化されます。

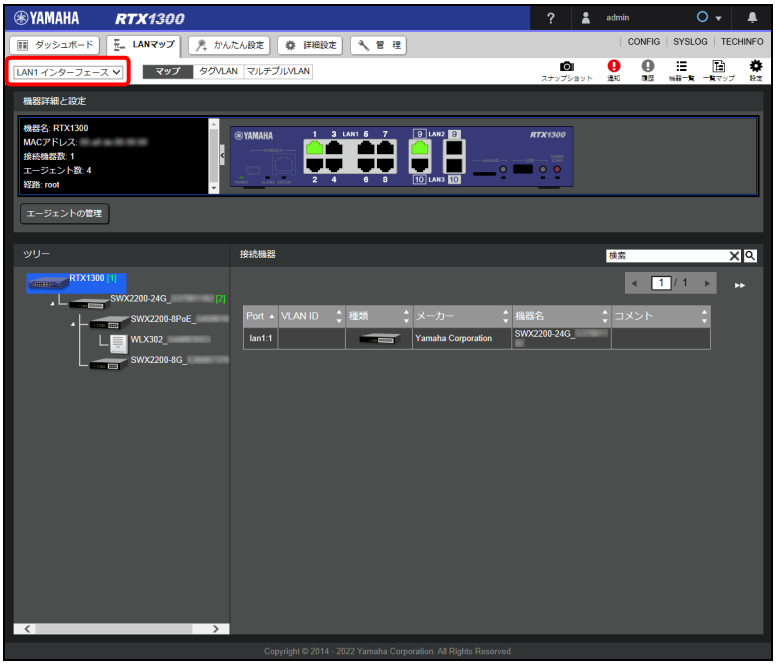
12.7.10 ポートの設定ダイアログを表示する

ヤマハスイッチのポートごとに設定するための「ポートの設定」ダイアログを表示します。

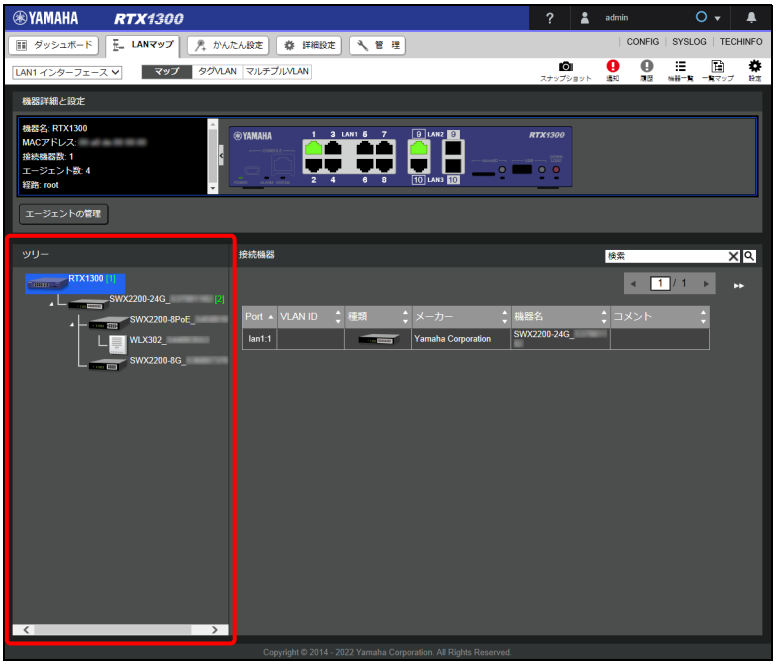
メモ

ポートの設定は対応しているスイッチをお使いの場合に設定できます。対応しているスイッチについて詳しくは下記の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/map.html#PORT

1. **ポートの設定を行いたいヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

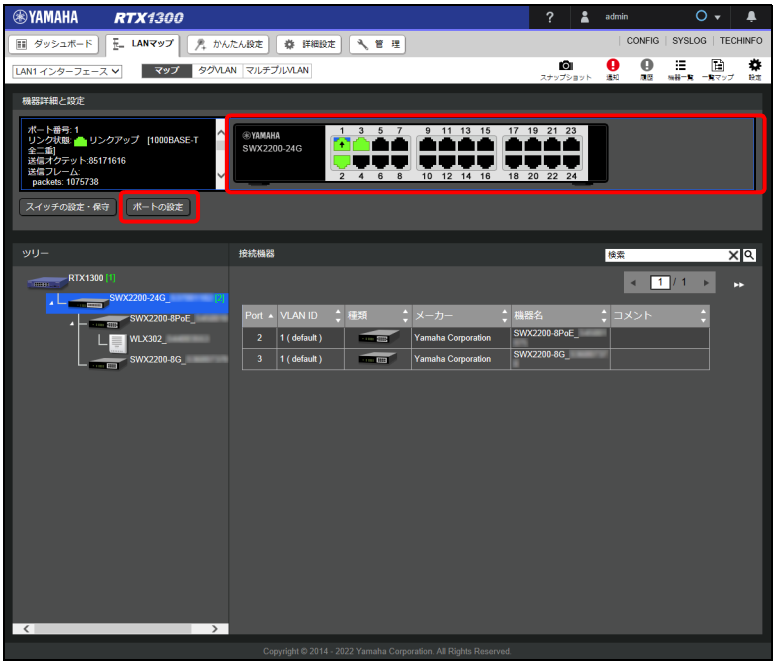


2. ツリービューでヤマハスイッチを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューで設定するポートを選択し、「ポートの設定」ボタンをクリックする。



「ポートの設定」ダイアログが表示されます。

12.7.11 ポートの基本機能を設定する

SWX2200 シリーズでは、ポートごとに以下の設定ができます。SWX2200 シリーズ以外のスイッチでの設定項目については、以下の URL をご覧ください。

http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/map.html#PORT

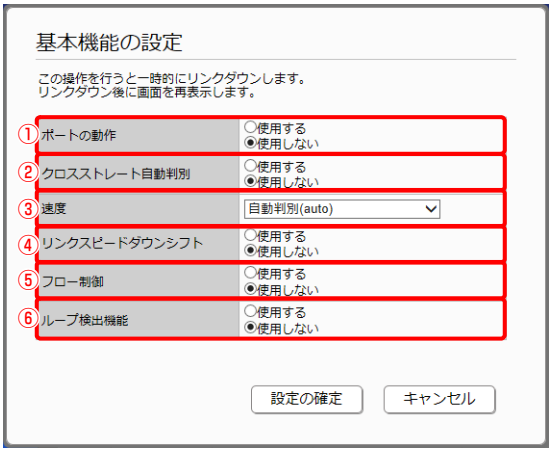
- ポートの動作
- クロスストレート自動判別
- 速度
- リンクスピードダウンシフト
- フロー制御
- ループ検出機能

1.「ポートの設定」ダイアログを表示する。

2.「基本機能」項目の「設定」ボタンをクリックする。

「基本機能の設定」ダイアログが表示されます。

3. **ポートの基本機能を設定する。**



① **ポートの動作：**
ポートを使用するか否かを設定します。

② **クロスストレート自動判別：**
LAN ケーブルの種類の自動判別機能を使用するか否かを設定します。

③ **速度：**
ポートの速度を選択します。

④ **リンクスピードダウンシフト：**
速度ダウンシフト機能を使用するか否かを設定します。

⑤ **フロー制御：**
フロー制御機能を使用するか否かを設定します。

⑥ **ループ検出機能：**
ループ検出機能を使用するか否かを設定します。

4. **「設定の確定」ボタンをクリックする。**
設定が反映され、「ポートの設定」ダイアログが表示されます。

12.7.12 QoS 機能を設定する

QoS 機能の設定を変更することができます。ポートごとにポートを経由するパケットに DSCP 値を付加することで優先度を指定します。また、ポートごとに送信帯域や受信帯域を指定できます。

1. **「ポートの設定」ダイアログを表示する。**
2. **「QoS」項目の「設定」ボタンをクリックする。**

「QoS 機能の設定」ダイアログが表示されます。

3. **QoS 機能を設定する。**

① **DSCP リマーキング：**
DSCP 値に設定する優先度を選択します。

② **送信シェービング：**
送信帯域を選択します。

③ **受信ポリシング：**
受信帯域を選択します。

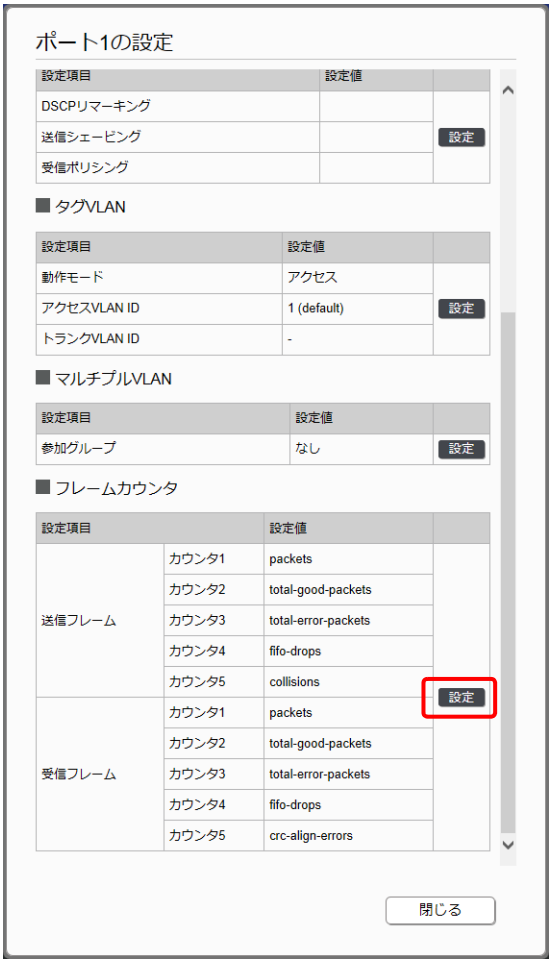
メモ
送信シェービングと受信ポリシングは、SWX2200-24G のみで設定できます。

4. **「設定の確定」ボタンをクリックする。**
設定が反映され、「ポートの設定」ダイアログが表示されます。

12.7.13 フレームカウンタを設定する

フレームカウンタの設定を変更することができます。「マップページ」の機器詳細と設定ビューで、機器画像内のポートを選択するとポートの情報が表示されます。その際に表示されるフレームカウンタ（統計情報）にどの情報を表示するかを設定することができます。

1. **「ポートの設定」ダイアログを表示する。**
2. **「フレームカウンタ」項目の「設定」ボタンをクリックする。**



「フレームカウンタの設定」ダイアログが表示されます。

3. フレームカウンタの表示情報を設定する。

① **送信フレーム：**
カウンタ 1 ～ 5 のそれぞれで表示する種別を設定します。

② **受信フレーム：**
カウンタ 1 ～ 5 のそれぞれで表示する種別を設定します。

メモ
SWX2200-24G のみカウンタが 5 個設定できます。SWX2200-8G および SWX2200-8PoE は 3 個まで設定できます。

4. 「設定の確定」ボタンをクリックする。
設定が反映され、「ポートの設定」ダイアログが表示されます。

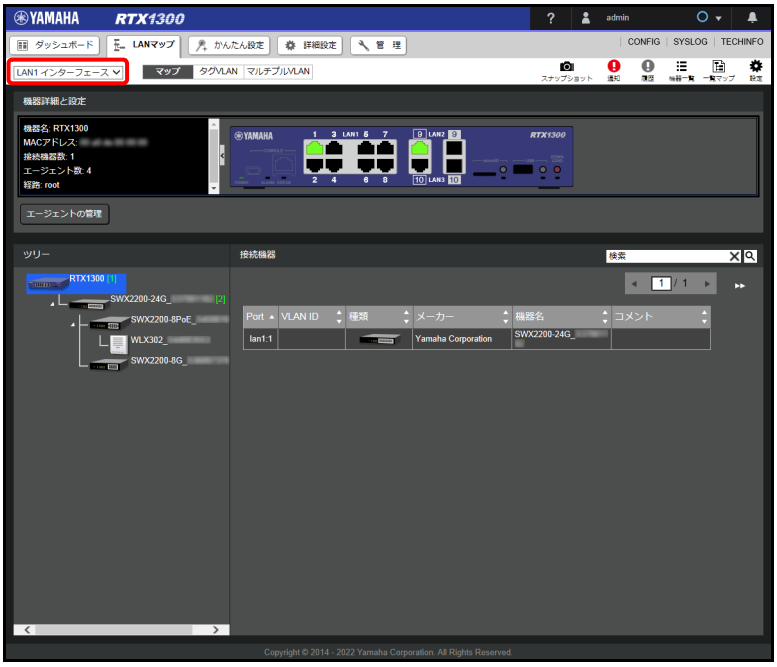
12.7.14 LAN ケーブル二重化機能を設定する

LAN ケーブル二重化機能を設定することができます。マネージャーとヤマハスイッチの間で LAN ケーブルを二重化し、ネットワークの信頼性を向上させる機能です。二重化することで、主ケーブルの断線や抜けによって接続が切れてしまったときに、自動的にバックアップケーブルがリンクアップして、ネットワークを継続して利用することができます。
本機能では主ケーブルが接続されている機器間のことをメイン経路、バックアップケーブルが接続されている機器間のことをバックアップ経路と呼びます。

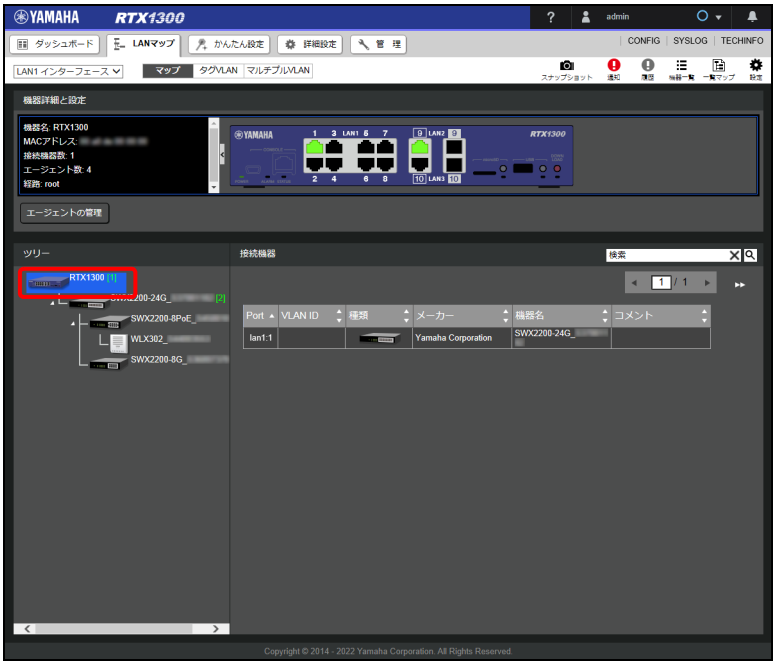
重要
本機能の設定前にバックアップ経路にケーブルを接続するとループが発生してしまうことがあります。
ケーブルの接続は、本機能の設定後に行ってください。

メモ
LAN ケーブル二重化機能の設定は、設定対象の機器がマネージャー、あるいは SWX2200 のダウンリンクポートに接続されている場合のみ設定できます。

1. 対象のヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

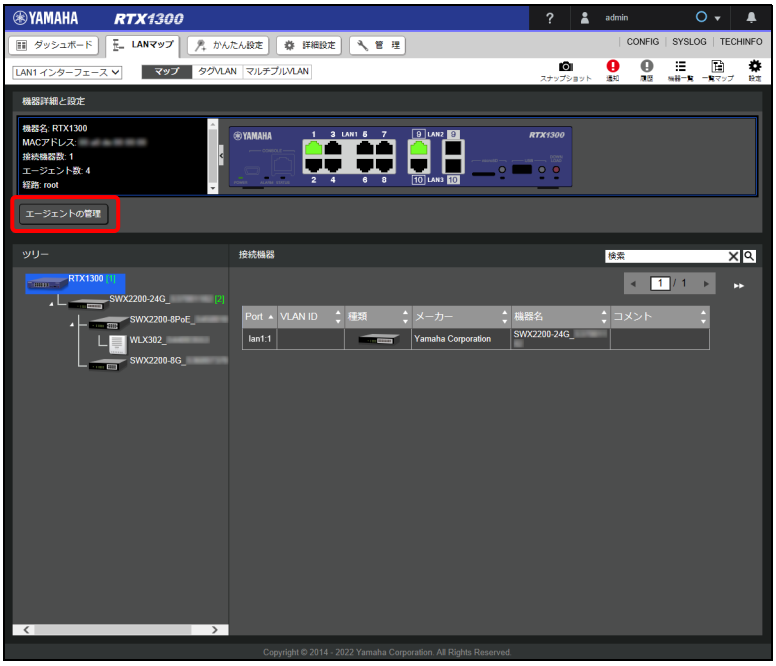


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。

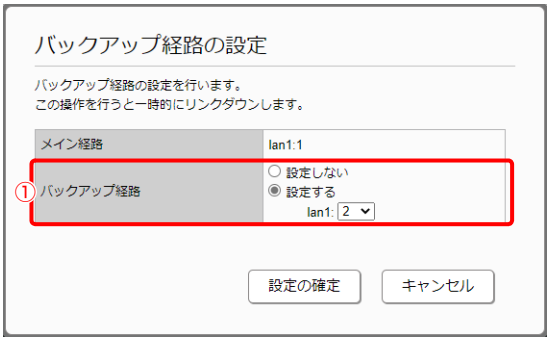


「エージェントの管理」ダイアログが表示されます。

4. 「スイッチの管理」項目の「バックアップ経路」欄の「設定」ボタンをクリックする。

「バックアップ経路の設定」ダイアログが表示されます。

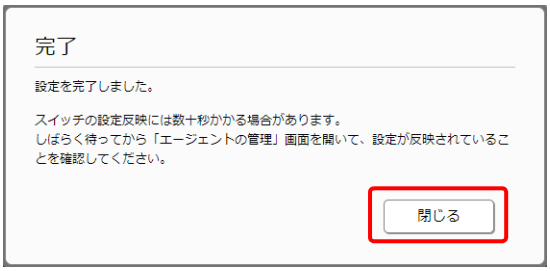
5. **バックアップ経路を設定する。**



① バックアップ経路：
バックアップ経路を設定するか否かを設定します。「設定する」を選択した場合は、バックアップ経路に設定するポートを選択します。

6. **「設定の確定」ボタンをクリックする。**
「完了」ダイアログが表示されます。

7. **「閉じる」ボタンをクリックする。**



「エージェントの管理」ダイアログが表示されます。また、設定の反映には数十秒かかる場合があります。

12.7.15 スイッチの指定方法を選択する

ヤマハスイッチの設定はマネージャーで保存・復元することができますが、その際にスイッチを経路で指定して管理するのか、MAC アドレスで指定して管理するのかをスイッチごとに選択することができます。経路指定で管理しているスイッチは、故障した場合でも新しいスイッチにリプレースするだけでリプレース前のスイッチと同じ設定を復元することができます。

経路での管理

スイッチを経路と紐付けて管理します。故障などの理由でスイッチをリプレースした場合でも、同じ経路上に設置した新しいスイッチに対して、リプレース前の旧スイッチと同じ設定を復元することができます。

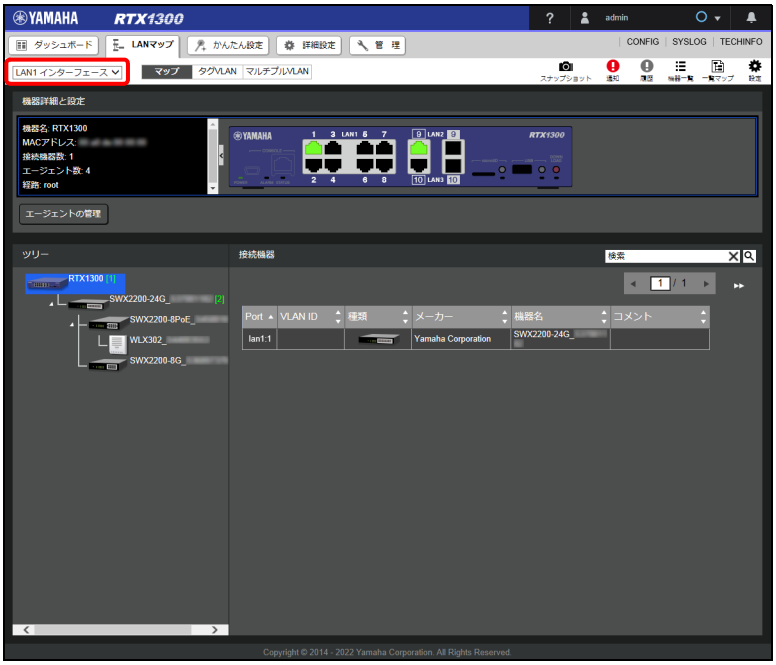
MAC アドレスでの管理

スイッチを MAC アドレスと紐付けて管理します。スイッチの設置場所（経路）を変更しても、スイッチの設定は変更されません。

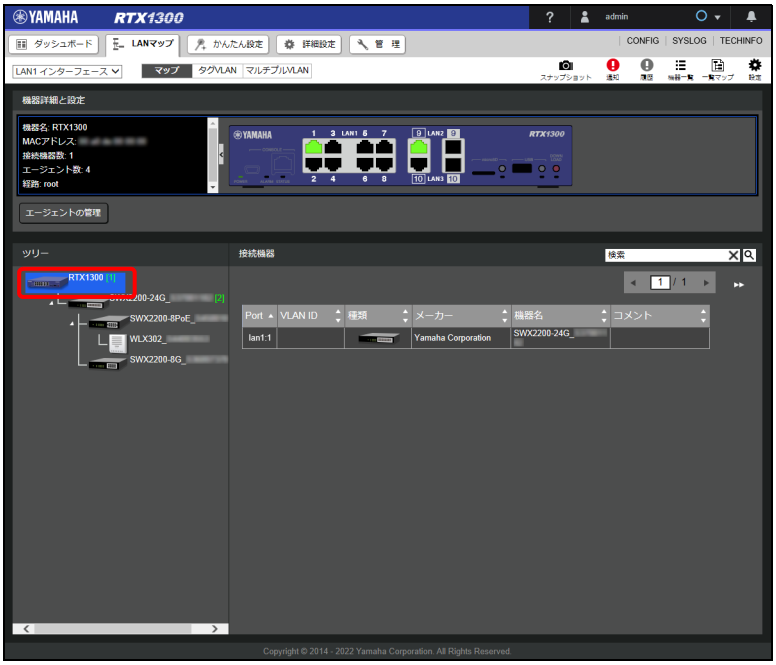
メモ

- スイッチの指定方法の選択は、SWX2200 シリーズまたは CONFIG の保存と復元に対応したスイッチのみ設定することができます。詳細は以下の URL をご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/swctl/operation.html#config_getset
- 工場出荷状態では MAC アドレスで指定されています。
- エージェントの経路情報の反映が完了していない場合がありますので、現在の経路をご確認の上、設定してください。

1. 対象のヤマハスイッチが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

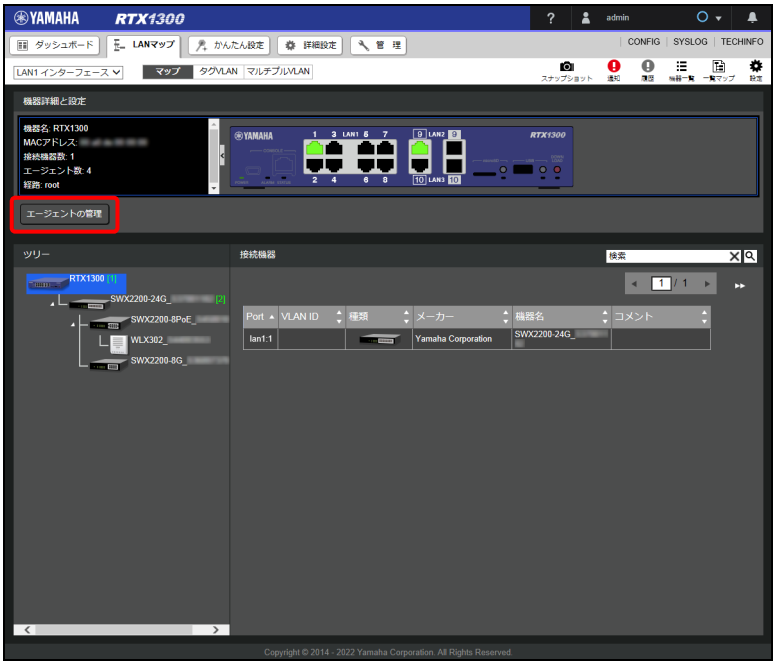


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。

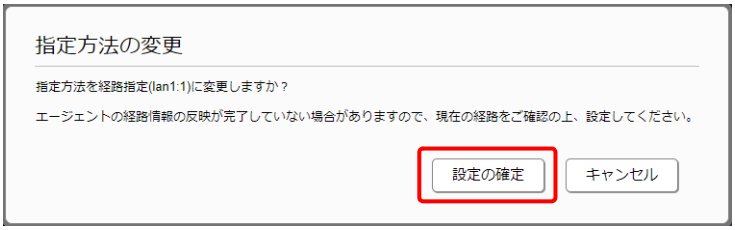


「エージェントの管理」ダイアログが表示されます。

4. 「スイッチの管理」項目の「スイッチの指定方法」欄の「設定」ボタンをクリックする。

「指定方法の変更」ダイアログが表示されます。

5. 「設定の確定」ボタンをクリックする。



「設定の確定」ボタンをクリックするたびに、「スイッチの指定方法」欄の「経路指定」と「MAC アドレス指定」が交互に切り替わります。

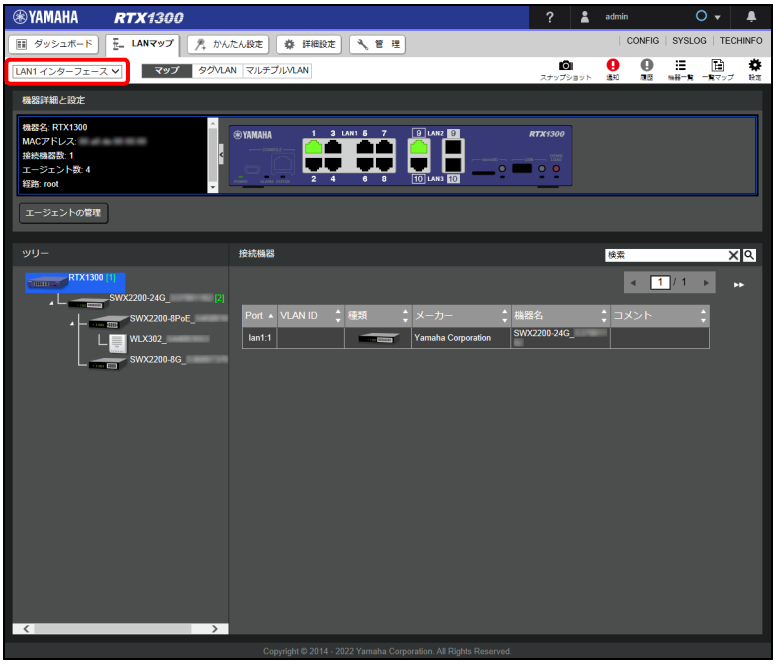
12.8 ヤマハ無線 AP の設定を行う

ヤマハ無線 AP の設定方法を説明します。

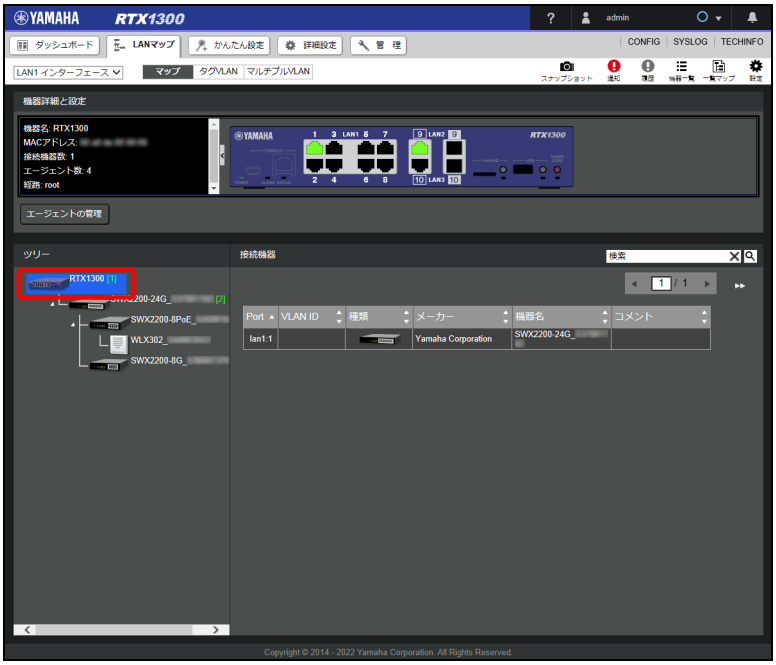
12.8.1 IP アドレスを変更する

ヤマハ無線 AP の IP アドレスを変更することができます。

1. 設定したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

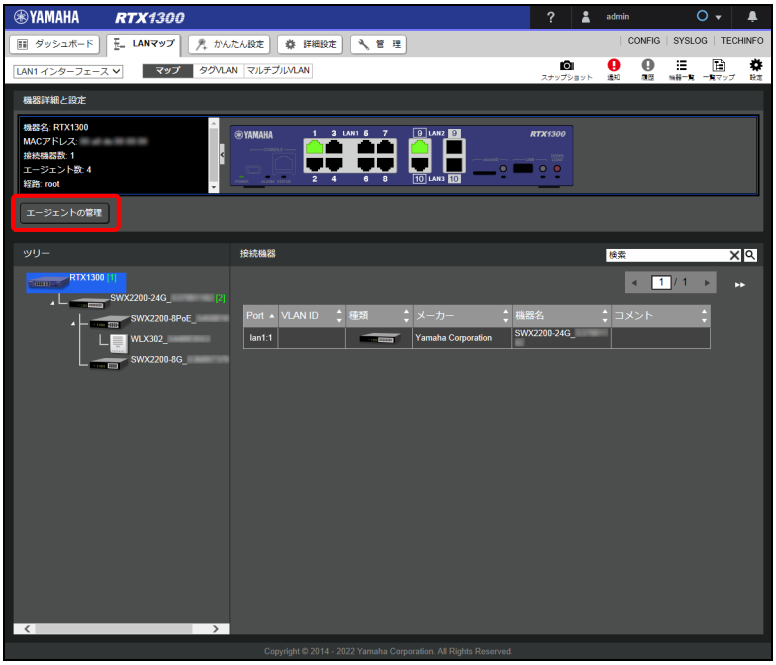


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。

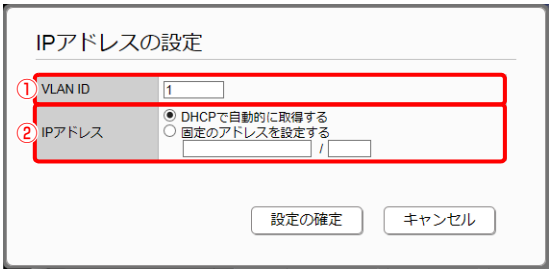


「エージェントの管理」ダイアログが表示されます。

4. 「無線 AP の管理」項目の「IP アドレス」欄の「設定」ボタンをクリックする。

「IP アドレスの設定」ダイアログが表示されます。

5. IP アドレスを設定する。



① **VLAN ID：**
VLAN ID を入力します。

② **IP アドレス：**
IP アドレスを DHCP から取得するか、固定 IP アドレスを設定するかを設定します。
・ DHCP で自動的に取得する：DHCP から IP アドレスを取得する場合に選択します。
・ 固定のアドレスを設定する：固定の IP アドレスを設定する場合に選択し、IP アドレスを入力します。

6. 「設定の確定」ボタンをクリックする。
IP アドレスが変更され、「エージェントの管理」ダイアログが表示されます。

12.8.2 無線 AP の指定方法を選択する

ヤマハ無線 AP の設定（CONFIG）は手動でマネージャー内に保存することができますが、その際に無線 AP を経路で指定して管理するのか、MAC アドレスで指定して管理するのかを無線 AP ごとに選択することができます。マネージャー内に無線 AP の設定（CONFIG）を保存しておけば、無線 AP をリプレースする際に、リプレース前の旧無線 AP と同じ設定（CONFIG）を簡単な操作で復元させることができます。

経路での管理

無線 AP を経路と紐付けて管理します。故障などの理由で無線 AP をリプレースした場合でも、同じ経路上に設置した新しい無線 AP に対して、リプレース前の旧無線 AP と同じ設定（CONFIG）を簡単な操作で復元させることができます。

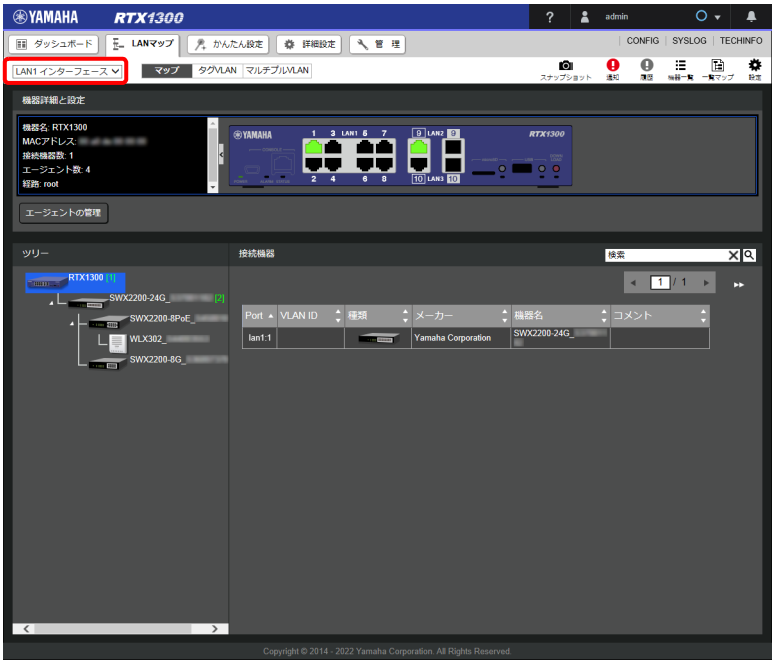
MAC アドレスでの管理

無線 AP を MAC アドレスと紐付けて管理します。マネージャーに保存されている設定（CONFIG）ファイルは対象の無線 AP（MAC アドレスが同一の無線 AP）のみにしか復元できません。

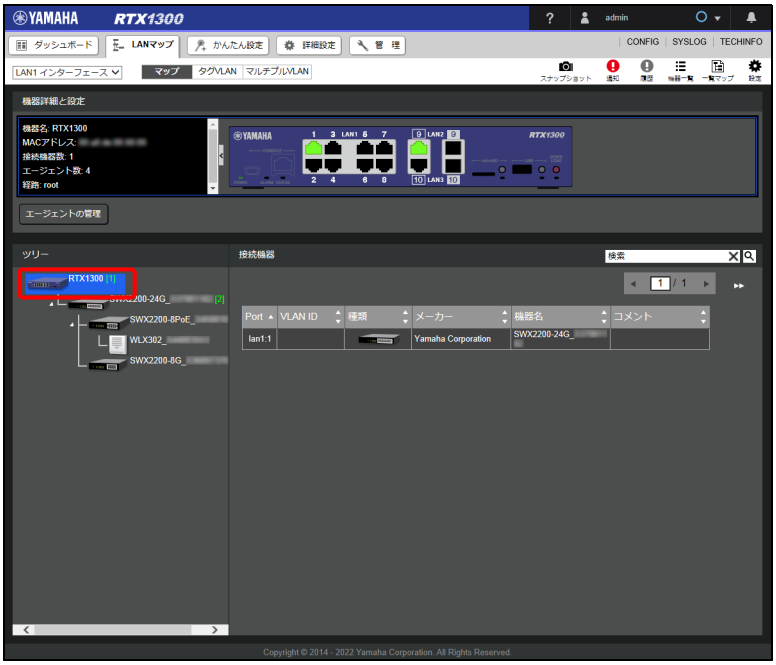
メモ

工場出荷状態では MAC アドレスで指定されています。

1. **設定したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

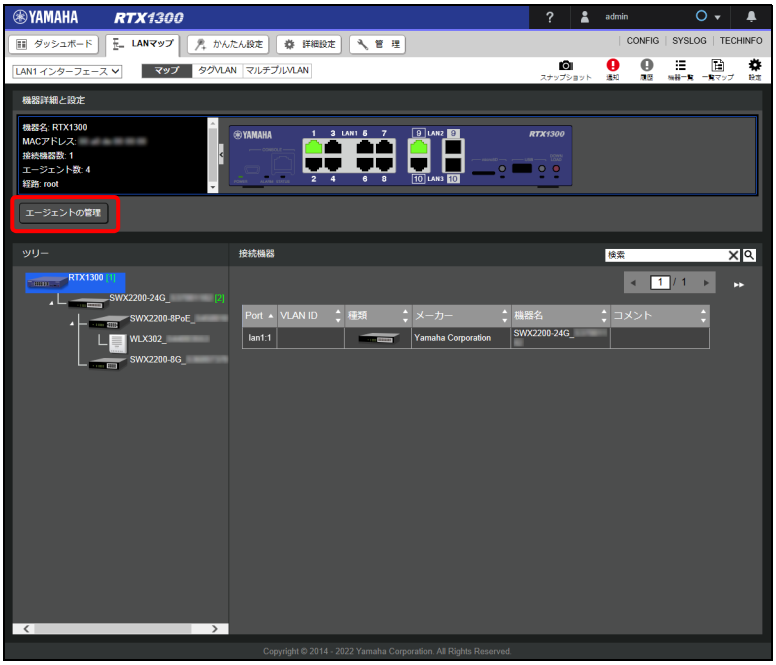


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。

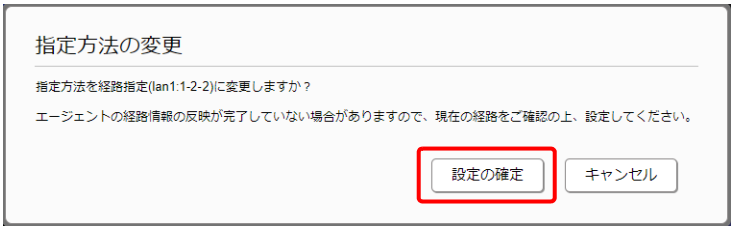


「エージェントの管理」ダイアログが表示されます。

4. 「無線 AP の管理」項目の「無線 AP の指定方法」欄の「設定」ボタンをクリックする。

「指定方法の変更」ダイアログが表示されます。

5. 「設定の確定」ボタンをクリックする。



「設定の確定」ボタンをクリックするたびに、「経路指定」と「MAC アドレス指定」が交互に切り替わります。

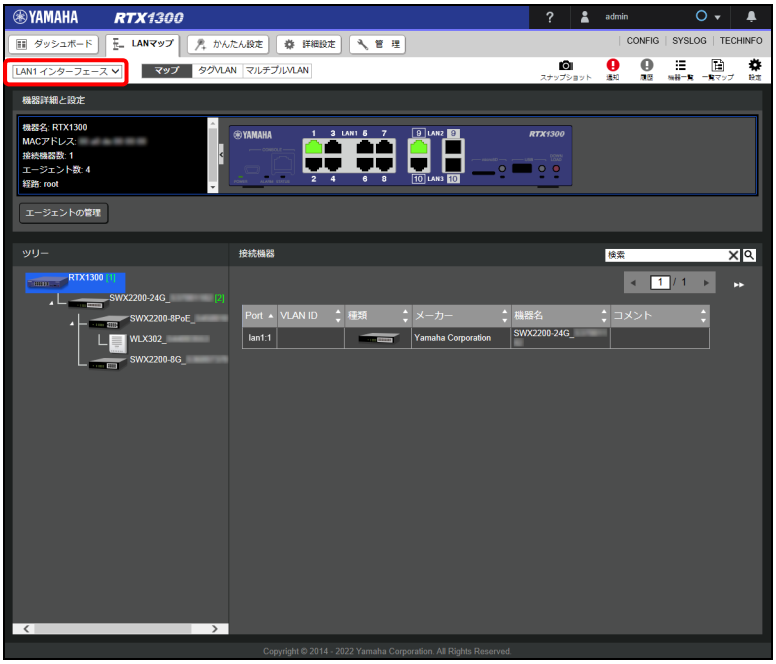
12.8.3 設定（CONFIG）を保存する

ヤマハ無線 AP の設定（CONFIG）をマネージャー内に保存します。

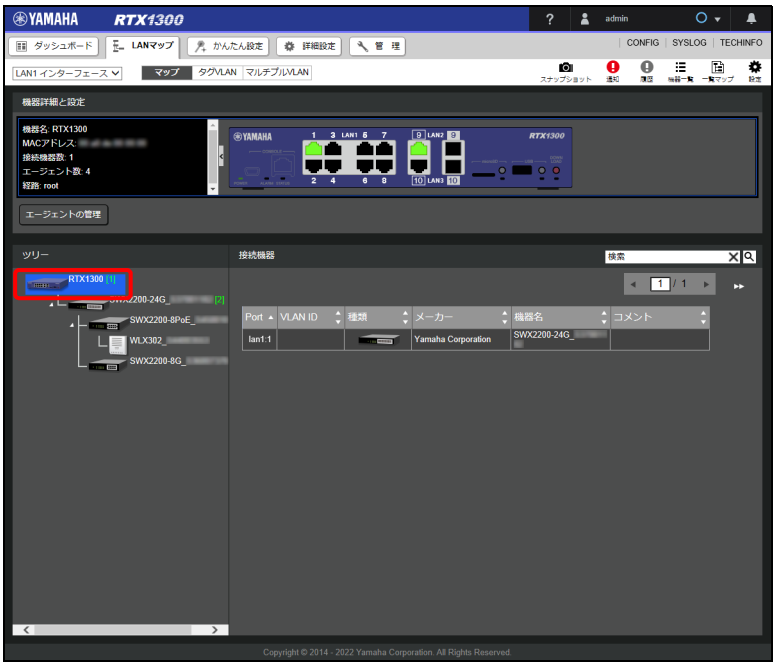
メモ

ヤマハ無線 AP はヤマハスイッチと異なり、自動ではマネージャー内に設定が保存されません。

1. 設定（CONFIG）を保存したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

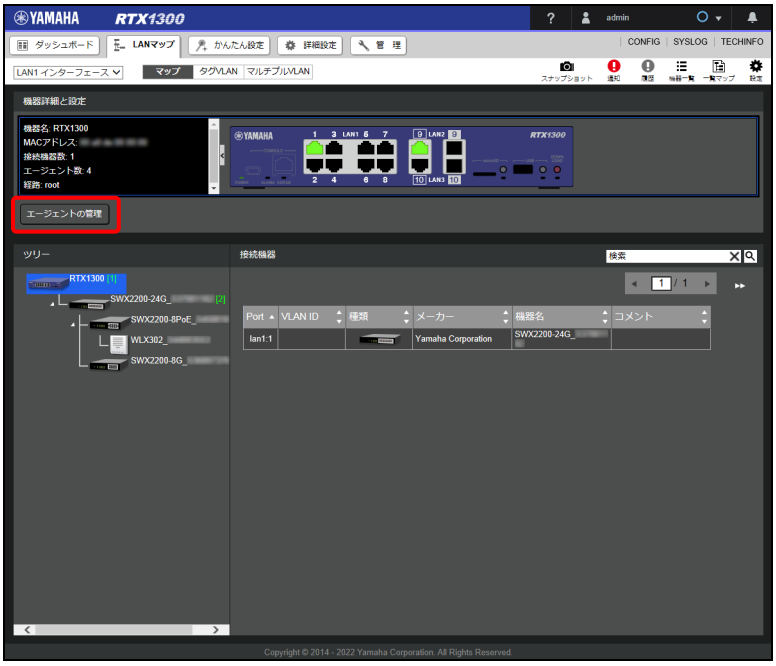


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。



「エージェントの管理」ダイアログが表示されます。

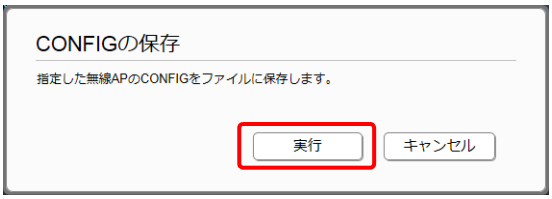
4. 「無線 AP の管理」項目の「CONFIG」欄の「保存」ボタンをクリックする。

「CONFIG の保存」ダイアログが表示されます。

メモ

ネットワーク内のすべてのヤマハ無線 AP の設定（CONFIG）を保存するときは、「無線 AP の CONFIG の一括操作」欄の「保存」ボタンをクリックします。

5. **「実行」ボタンをクリックする。**



設定（CONFIG）が保存され、「エージェントの管理」ダイアログが表示されます。

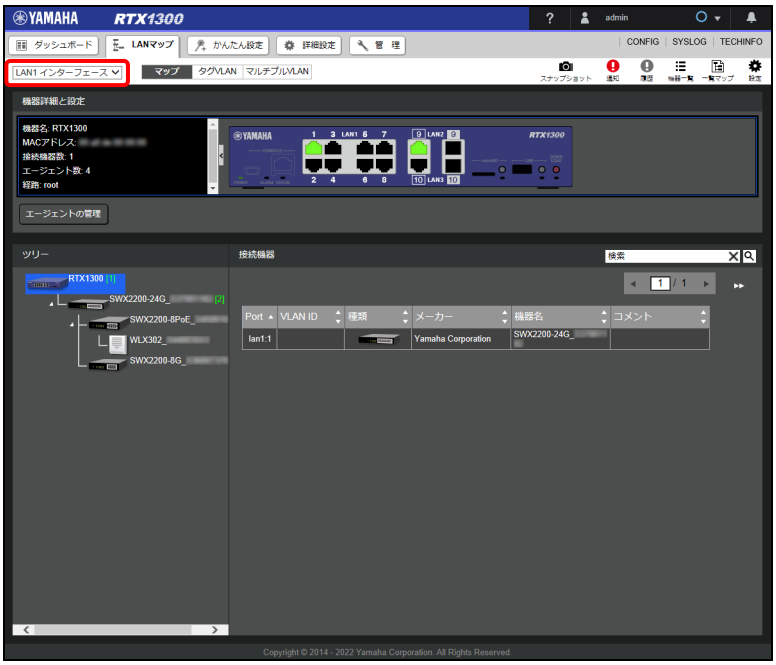
12.8.4 設定（CONFIG）を復元する

マネージャー内に保存した設定（CONFIG）から、ヤマハ無線 AP の設定を復元します。

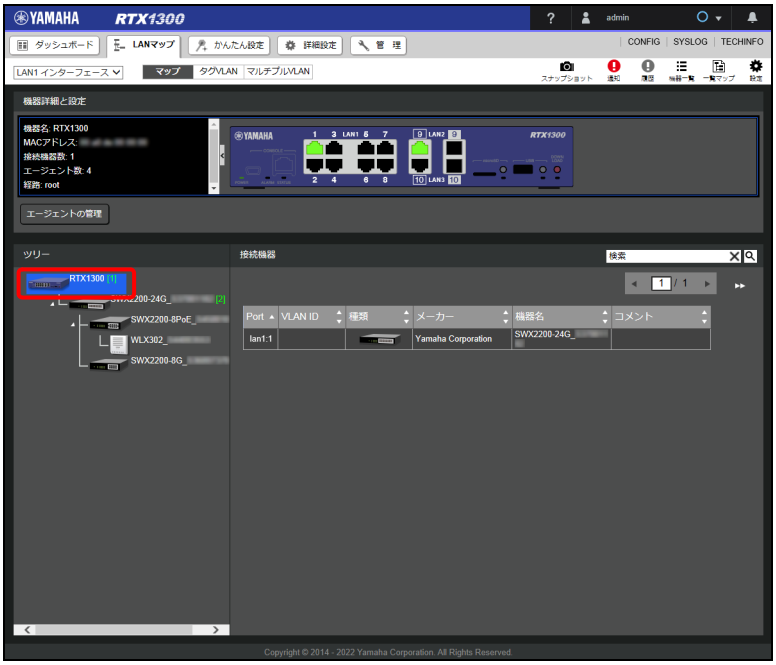
メモ

- マネージャー内に設定（CONFIG）が保存されていない場合は、復元することはできません。
- ヤマハ無線 AP の設定の復元は、「12.8.2 無線 AP の指定方法を選択する」（193 ページ）で指定したヤマハ無線 AP に対して実行されます。
- 「12.8.2 無線 AP の指定方法を選択する」（193 ページ）で指定したヤマハ無線 AP の設定（CONFIG）がマネージャー内に保存されている場合、対象のヤマハ無線 AP が工場出荷状態であれば設定（CONFIG）が自動的に復元されます。工場出荷状態でない場合は、本項の復元操作を行う必要があります。

1. **設定（CONFIG）を復元したいヤマハ無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

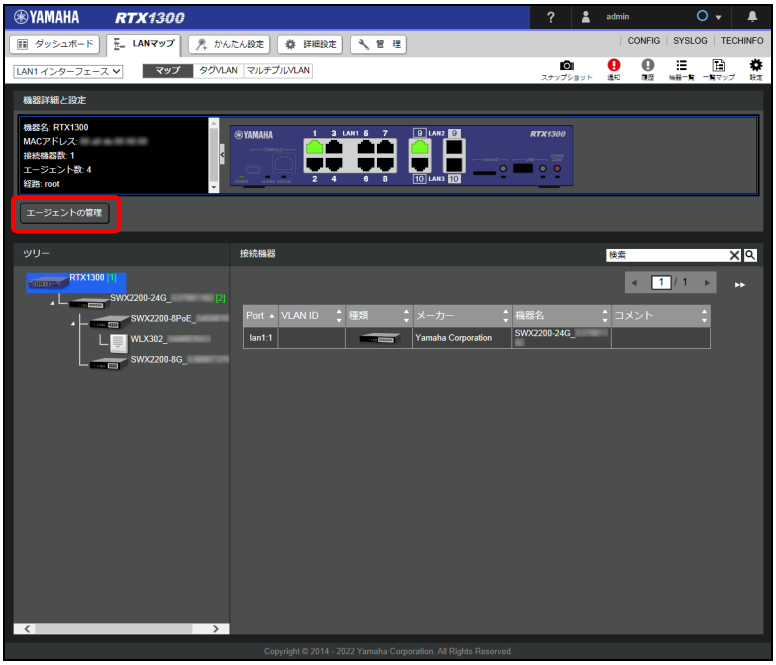


2. ツリービューでマネージャーを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「エージェントの管理」ボタンをクリックする。



「エージェントの管理」ダイアログが表示されます。

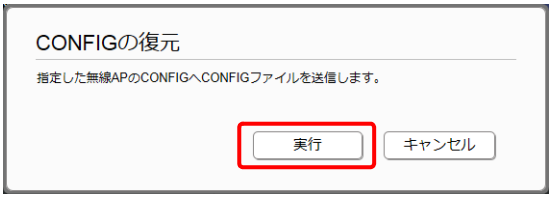
4. 「無線 AP の管理」項目の「CONFIG」欄の「復元」ボタンをクリックする。

「CONFIG の復元」ダイアログが表示されます。

メモ

ネットワーク内のすべてのヤマハ無線 AP の設定（CONFIG）を復元するときは、「無線 AP の CONFIG の一括操作」欄の「復元」ボタンをクリックします。

5. 「実行」ボタンをクリックする。

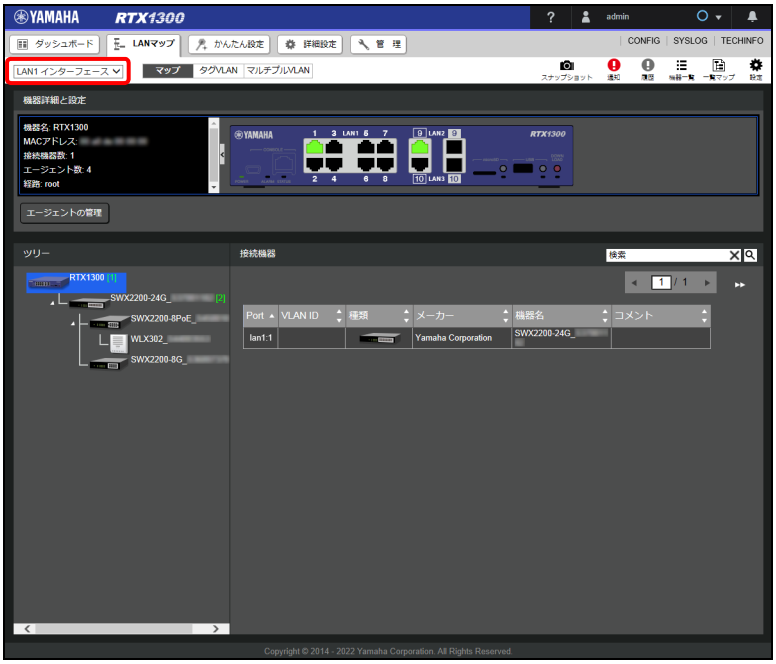


設定（CONFIG）が復元され、「エージェントの管理」ダイアログが表示されます。

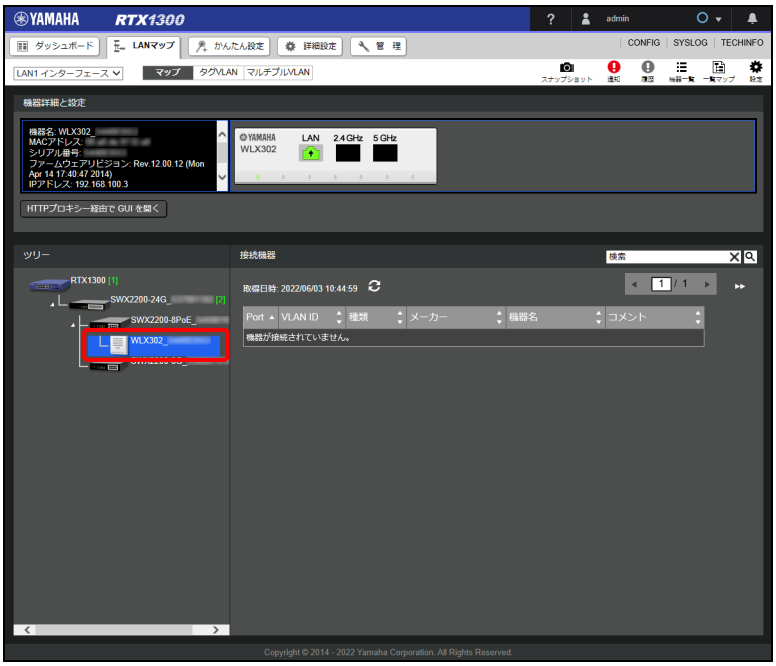
12.8.5 無線 AP の設定画面を表示する

ヤマハ無線 AP の詳細設定を変更するために、ヤマハ無線 AP の Web GUI を表示します。ヤマハ無線 AP の Web GUI の使い方について詳しくは、ヤマハ無線 AP の操作マニュアル（ウェブサイト）をご覧ください。

1. **設定したい無線 AP が接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

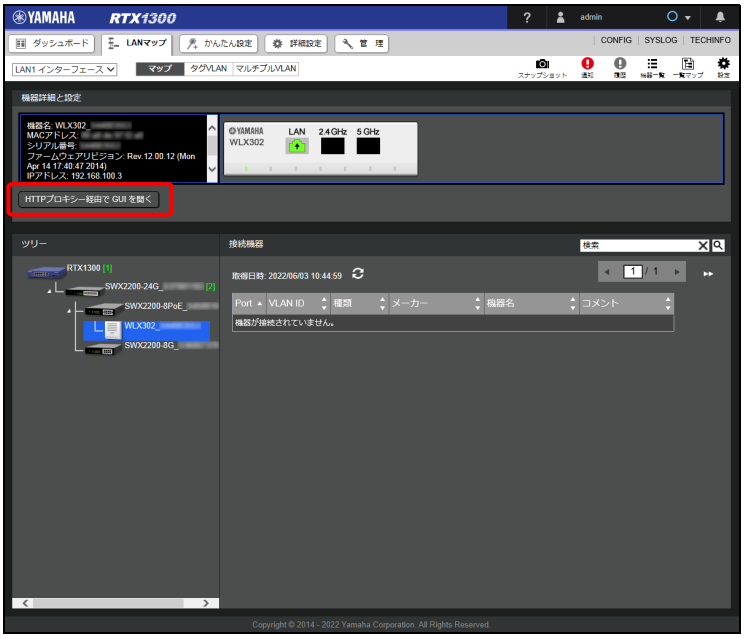


2. **ツリービューで無線 AP を選択する。**



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「HTTP プロキシー経由で GUI を開く」ボタンをクリックする。

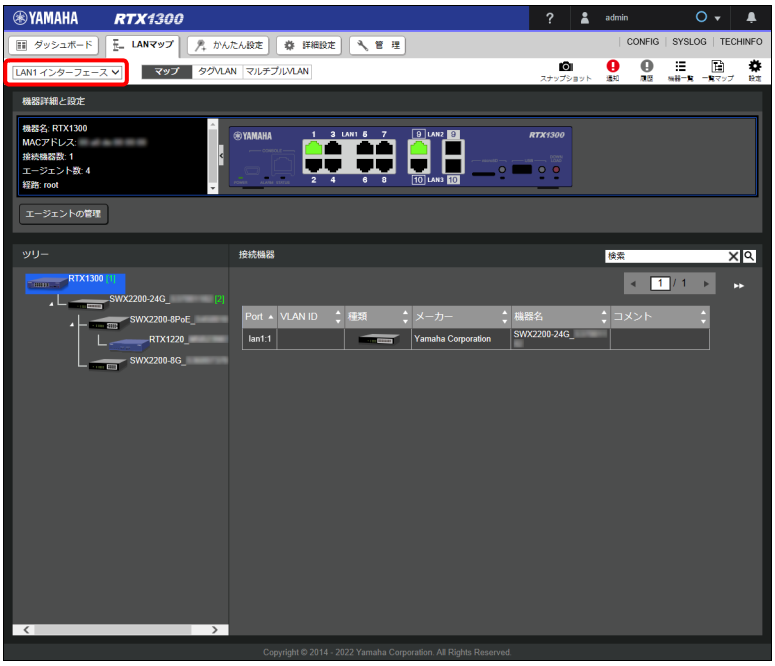


無線 AP 機器の Web GUI が表示されます。

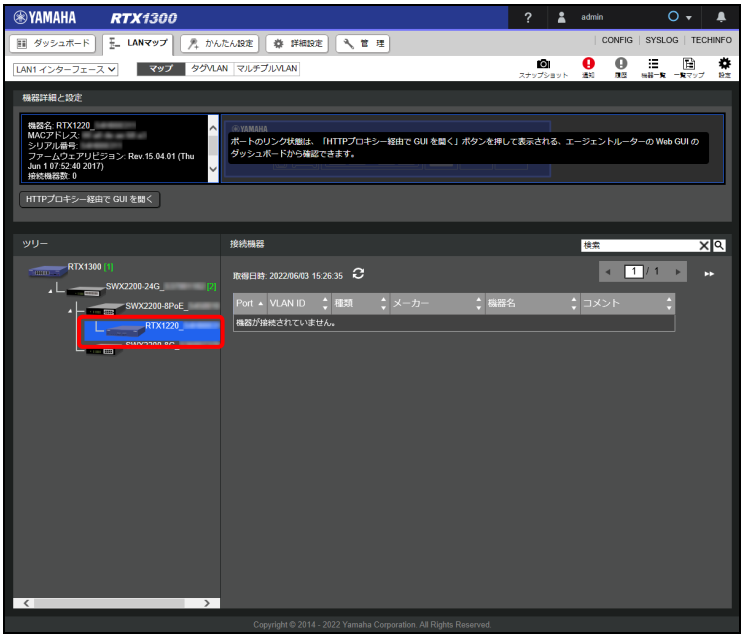
12.9 エージェントルーターの設定を行う

エージェントルーターの詳細設定を変更するために、エージェントルーターの Web GUI を表示します。エージェントルーターの Web GUI の使い方について詳しくは、エージェントルーターの Web GUI 操作マニュアル（ウェブサイト）をご覧ください。

1. 設定したいエージェントルーターが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。

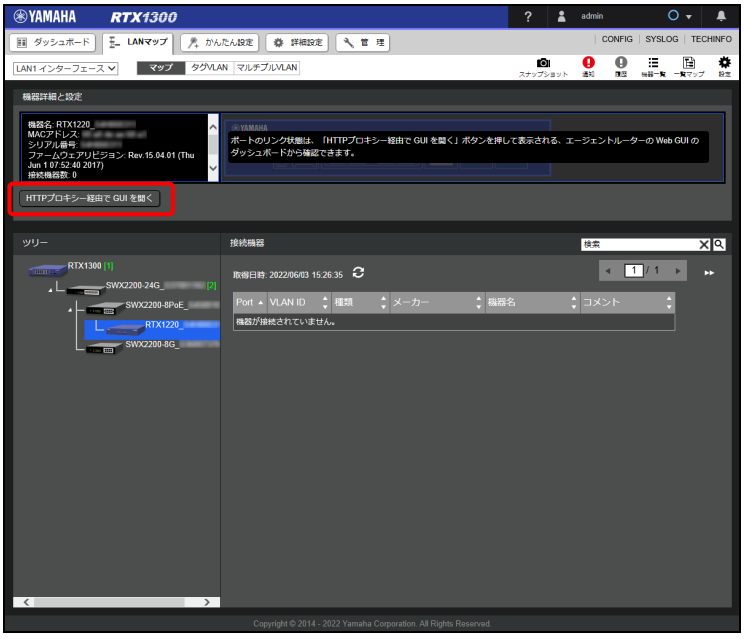


2. ツリービューでエージェントルーターを選択する。



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「HTTP プロキシー経由で GUI を開く」ボタンをクリックする。



エージェントルーター機器の Web GUI が表示されます。

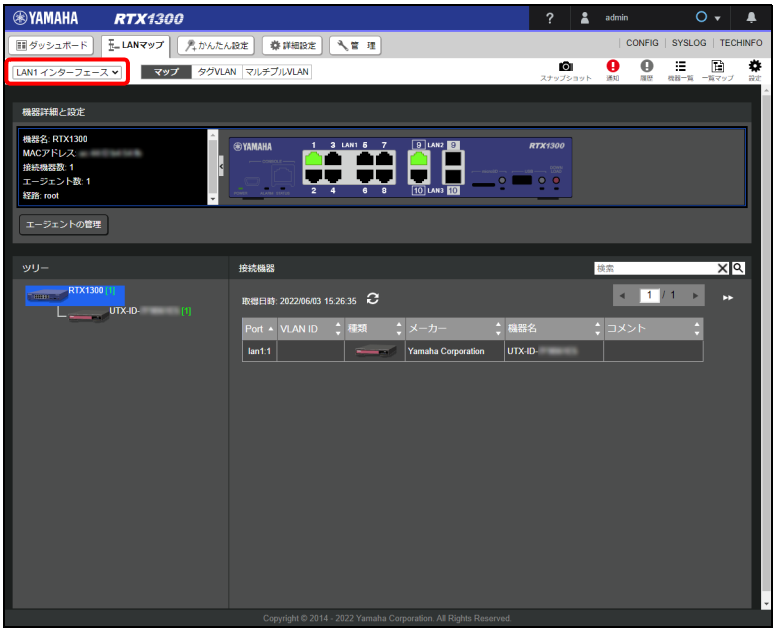
メモ

- L2MS のエージェントとして動作しているルーターの設定で、マネージャーの HTTP プロキシー経由で GUI アクセスを許可しないに設定している場合、「GUI を開く」ボタンが表示されます。
- パソコンからエージェントルーターに直接アクセスするためには、マネージャーおよびエージェントルーターのフィルターや NAT 等の設定変更が必要になる場合があります。

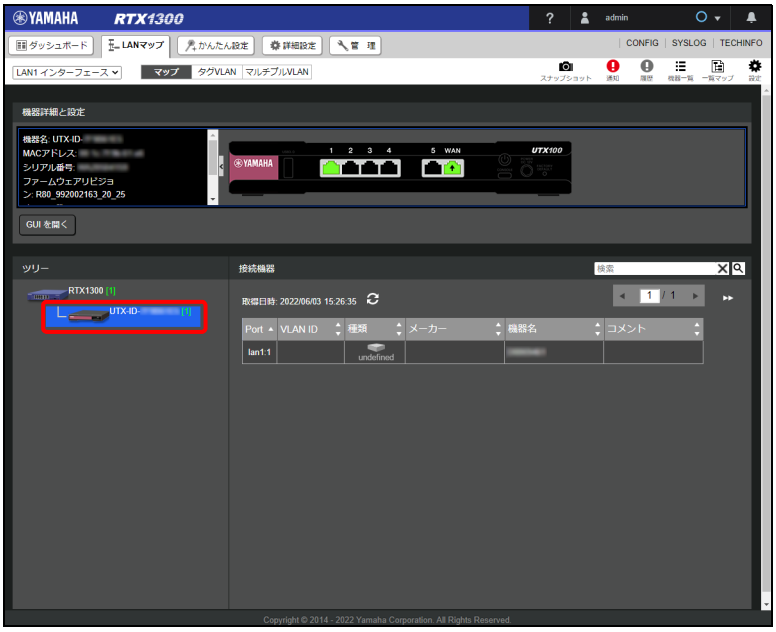
12.10 ヤマハ UTM アプライアンスの設定を行う

ヤマハ UTM アプライアンスの詳細設定を変更するために、ヤマハ UTM アプライアンスの Web GUI を表示します。ヤマハ UTM アプライアンスの Web GUI の使い方について詳しくは、ヤマハ UTM アプライアンスのユーザーガイド（ウェブサイト）をご覧ください。

1. **設定したいヤマハ UTM アプライアンスが接続されたインターフェースを、インターフェース選択プルダウンメニューから選択する。**

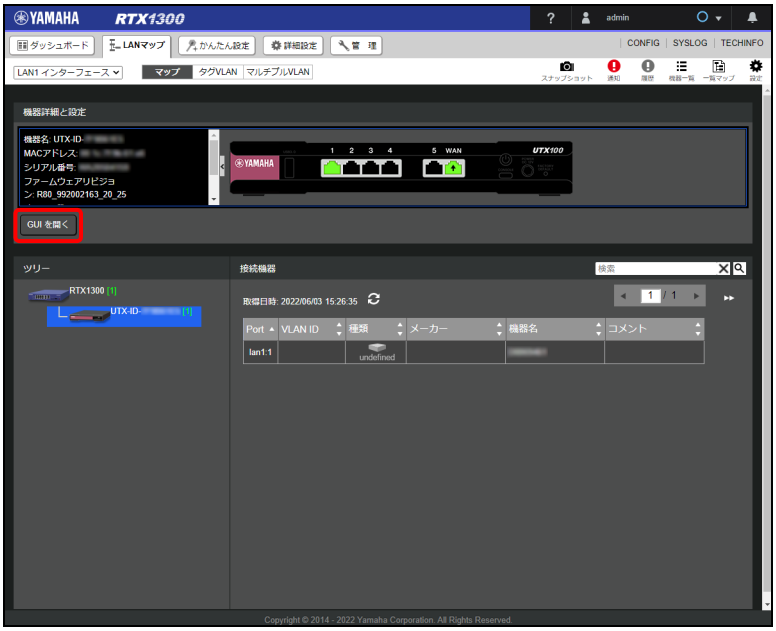


2. **ツリービューでヤマハ UTM アプライアンスを選択する。**



機器詳細と設定ビューと接続機器ビューの表示が切り替わります。

3. 機器詳細と設定ビューの「GUI を開く」ボタンをクリックする。



ヤマハ UTM アプライアンスの Web GUI が表示されます。

12.11 タグ VLAN を設定する

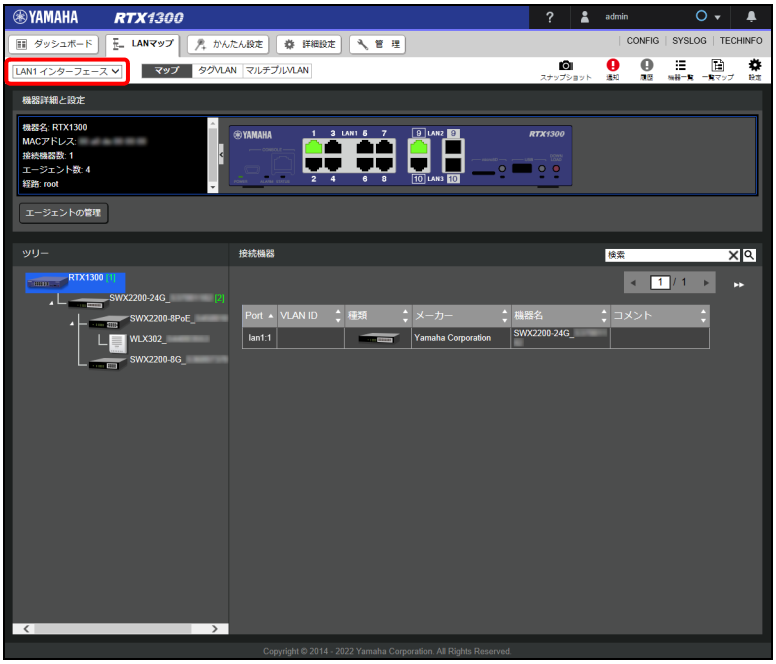
タグ VLAN の設定方法を説明します。タグ VLAN 機能とは、ヤマハスイッチのポートやヤマハ無線 AP の SSID をグループ分けし、グループごとにユニークな VLAN ID タグと IP アドレスを付与することで、物理的な配置に依存することなく、仮想的な LAN を形成する機能のことです。VLAN 間の通信はマネージャーを経由して行われます。

メモ

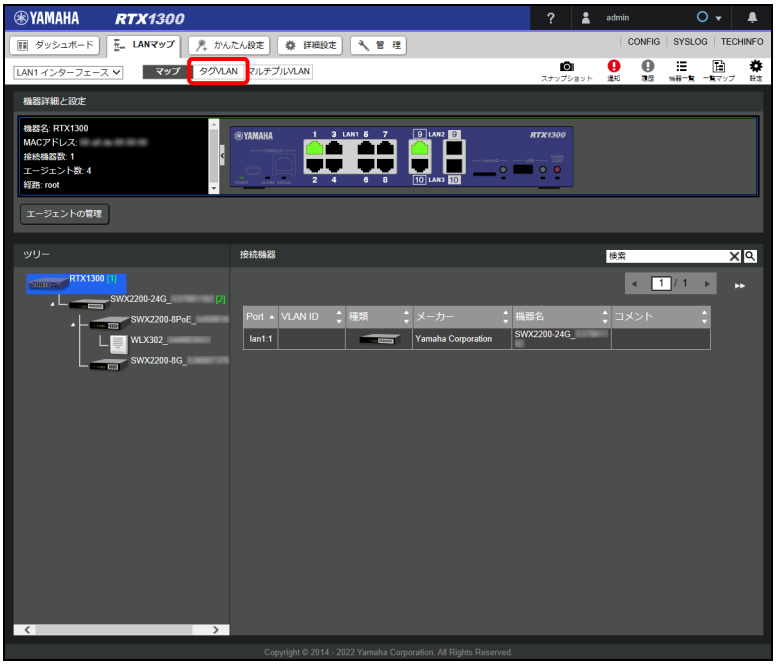
タグ VLAN の設定の対応機器については、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/tag_vlan.html

12.11.1 タグ VLAN ページを表示する

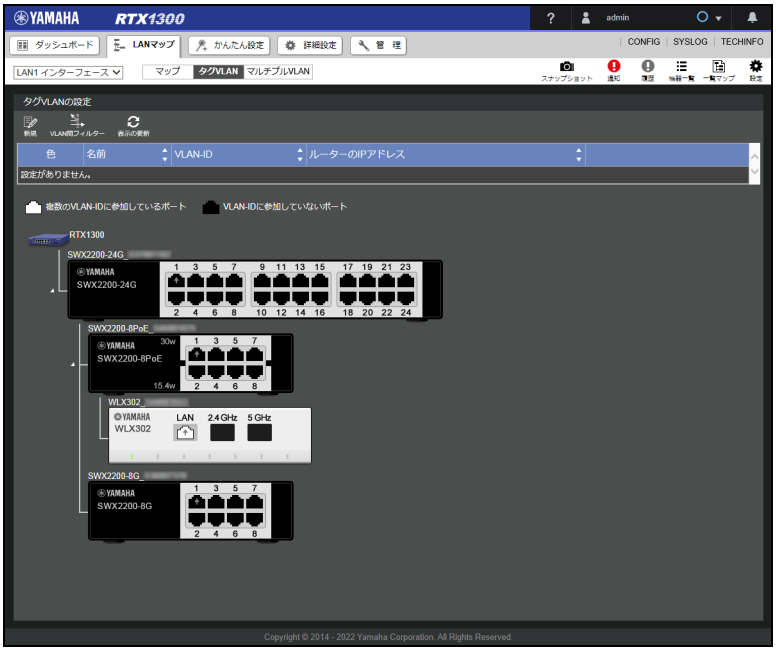
1. **設定したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。**



2. 表示選択スイッチで「タグ VLAN」を選択する。



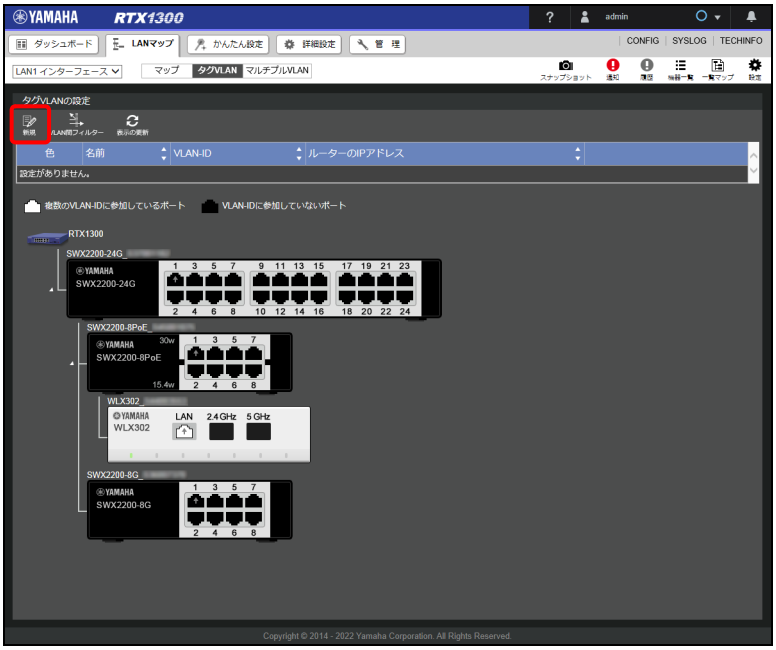
「タグ VLAN ページ」が表示されます。



12.11.2 タグ VLAN グループを作成する

タグ VLAN のグループを作成します。

1. **「タグ VLAN ページ」を表示する。**
2. **「 」ボタンをクリックする。**



「VLAN グループの作成」ダイアログが表示されます。

3. **タグ VLAN のグループ情報を入力する。**

① VLAN ID：
VLAN の ID を入力します。

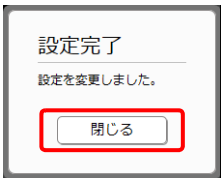
② 名前：
任意の名前を入力します。区別しやすい名前を付けておくと、設定の修正や削除をする場合に便利です。

③ ルーターの IP アドレス：
VLAN で使用する IP アドレスを入力します。

④ DHCP サーバー機能：
VLAN 配下の端末に DHCP で IP アドレスを払い出す場合は、「使用する」を選択して IP アドレスを入力します。DHCP サーバー機能を使用しない場合は、「使用しない」を選択します。

4. **「確定」ボタンをクリックする。**
タグ VLAN のグループが登録され、「設定完了」ダイアログが表示されます。

5. 「閉じる」ボタンをクリックする。



「タグ VLAN ページ」が表示されます。

12.11.3 タグ VLAN グループに参加させる

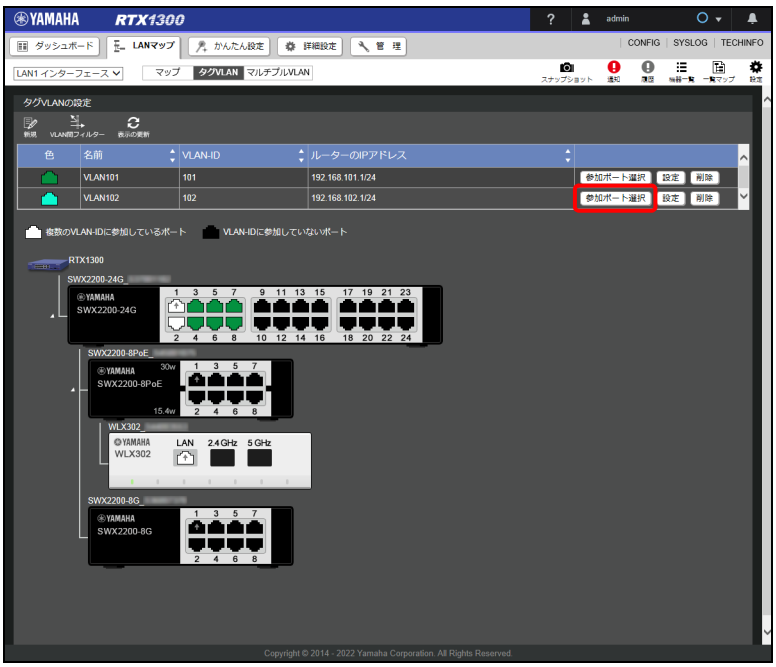
作成したタグ VLAN のグループごとに、参加させるポートを設定します。

メモ

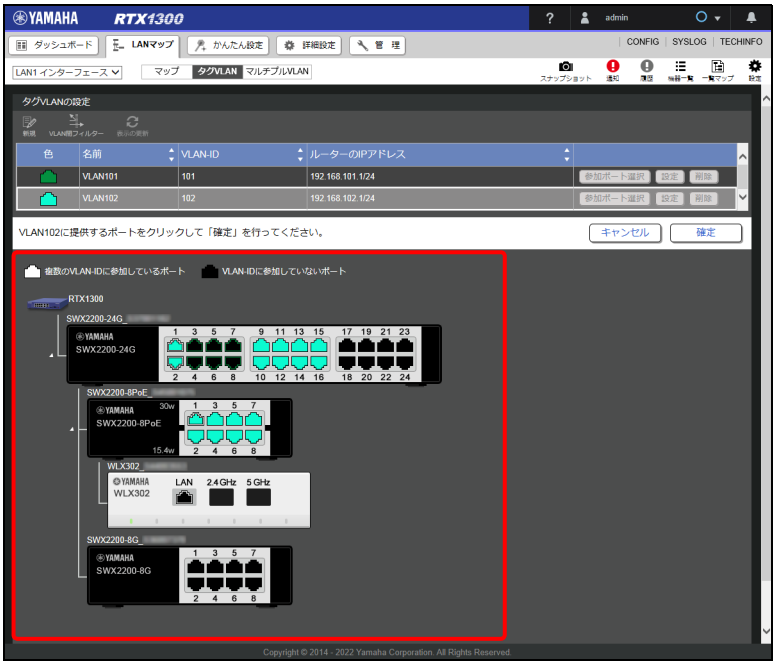
ヤマハ無線 AP の SSID も VLAN グループに参加させたい場合は、ヤマハ無線 AP の Web GUI で SSID ごとに VLAN ID を設定してください。また、「タグ VLAN ページ」でヤマハ無線 AP の LAN ポートも VLAN グループに参加させてください。ヤマハ無線 AP の Web GUI の使い方について詳しくは、ヤマハ無線 AP の操作マニュアル（ウェブサイト）をご覧ください。

1. 「タグ VLAN ページ」を表示する。

2. 設定したいタグ VLAN グループの「参加ポート選択」ボタンをクリックする。



3. 機器アイコンからタグ VLAN グループに参加させたいポートを選択する。



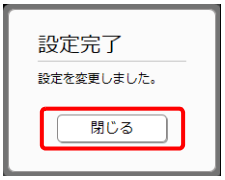
ポートを選択するとポートの色が変わり、指定の VLAN グループに参加させることができます。また、選択したポートを再選択すると参加をキャンセルすることができます。

メモ

ポートを VLAN グループに参加させた場合、マネージャーから対象のエージェントまでをつなぐポート（アップリンク / ダウンリンク）も自動で選択されます。

4. 「確定」ボタンをクリックする。
   設定が反映され、「設定完了」ダイアログが表示されます。

5. 「閉じる」ボタンをクリックする。

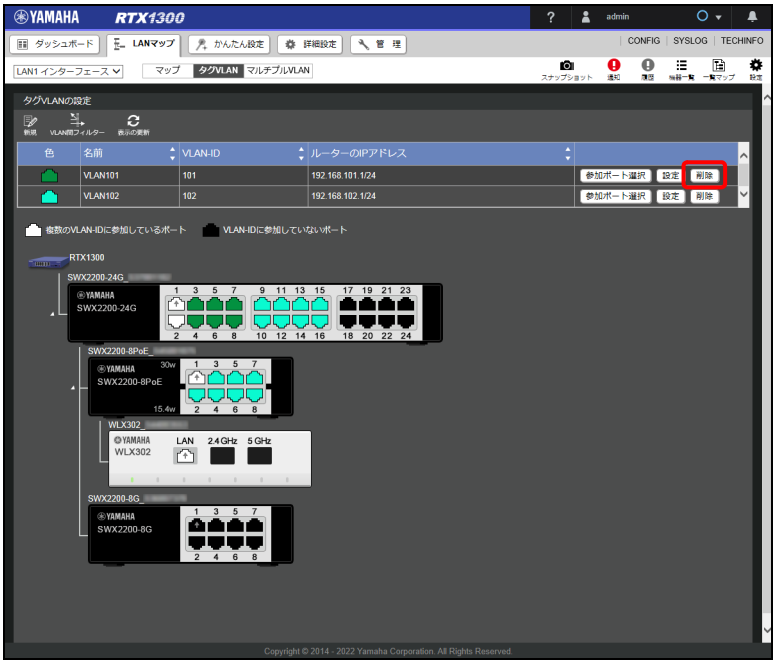


「タグ VLAN ページ」が表示されます。

12.11.4 タグ VLAN グループを削除する

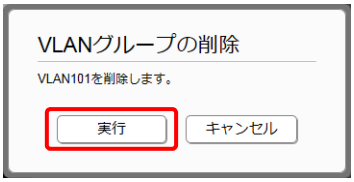
作成したタグ VLAN グループを削除します。

1. **「タグ VLAN ページ」を表示する。**
2. **削除したいタグ VLAN グループの「削除」ボタンをクリックする。**



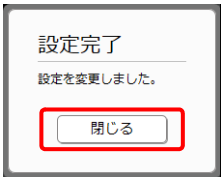
「VLAN グループの削除」ダイアログが表示されます。

3. **「実行」ボタンをクリックする。**



タグ VLAN グループが削除され、「設定完了」ダイアログが表示されます。

4. **「閉じる」ボタンをクリックする。**



「タグ VLAN ページ」が表示されます。

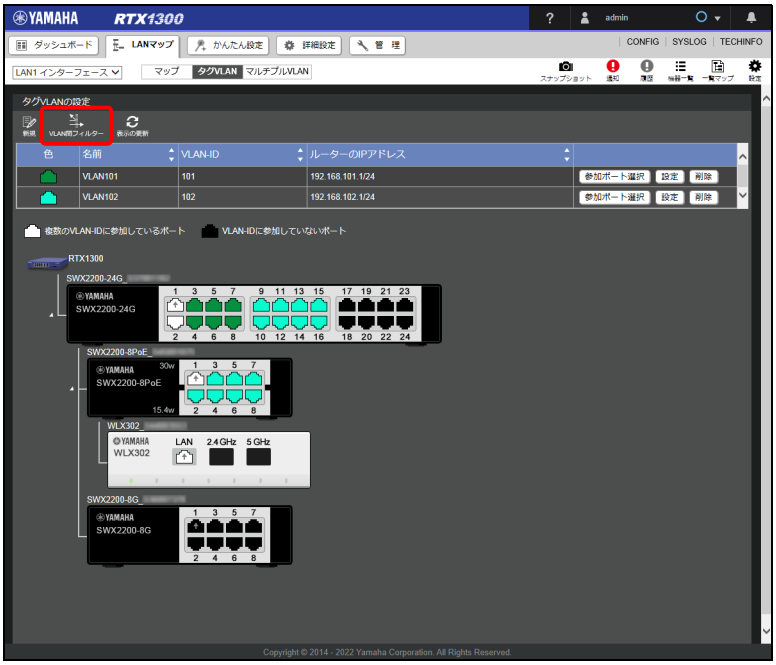
12.11.5 タグ VLAN 間フィルターを設定する

VLAN 間の通信を開放するか遮断するかを設定します。VLAN 間フィルターの設定操作を行わない場合は、VLAN 間の通信が常に全開放された状態になります。

メモ

タグ VLAN グループが 2 個以上作成されていなければ VLAN 間フィルターの設定はできません。

1. **「タグ VLAN ページ」を表示する。**
2. **「 VLAN間フィルター 」ボタンをクリックする。**



「VLAN 間フィルター」ダイアログが表示されます。

3. **タグ VLAN グループ間のフィルターを設定する。**

① 全遮断：

VLAN 間の通信をすべて遮断します。全遮断を選択した場合は、すべての VLAN 間の通信を遮断する IP フィルターが登録されます。

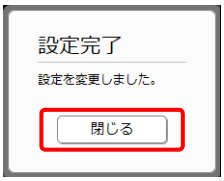
重要

VLAN グループを追加した場合は、改めて全遮断のフィルター設定操作を行ってください。新規作成した VLAN グループは、既存の VLAN グループとの通信が開放されているためです。
VLAN グループで使用する IP アドレスを変更した場合も、改めて全遮断のフィルター設定操作を行ってください。

② **全開放：**
VLAN 間の通信をすべて開放します。全開放を選択した場合は、全遮断した際に追加した IP フィルターがすべて削除されます。

4. **「確定」ボタンをクリックする。**
設定が反映され、「設定完了」ダイアログが表示されます。

5. **「閉じる」ボタンをクリックする。**



「タグ VLAN ページ」が表示されます。

メモ

全遮断の設定を行った後で VLAN グループを削除すると、削除した VLAN グループに関連する IP フィルターの設定が残ったままになりますが、全開放の設定を行えば IP フィルターの設定は削除されます。ただし、VLAN グループが 2 個以上作成されていなければ VLAN 間フィルターの設定は変更できないため、VLAN グループを削除する場合は、先に VLAN 間フィルターの全開放の設定を行っておくことで IP フィルターの設定を削除することができます。

12.12 マルチプル VLAN を設定する

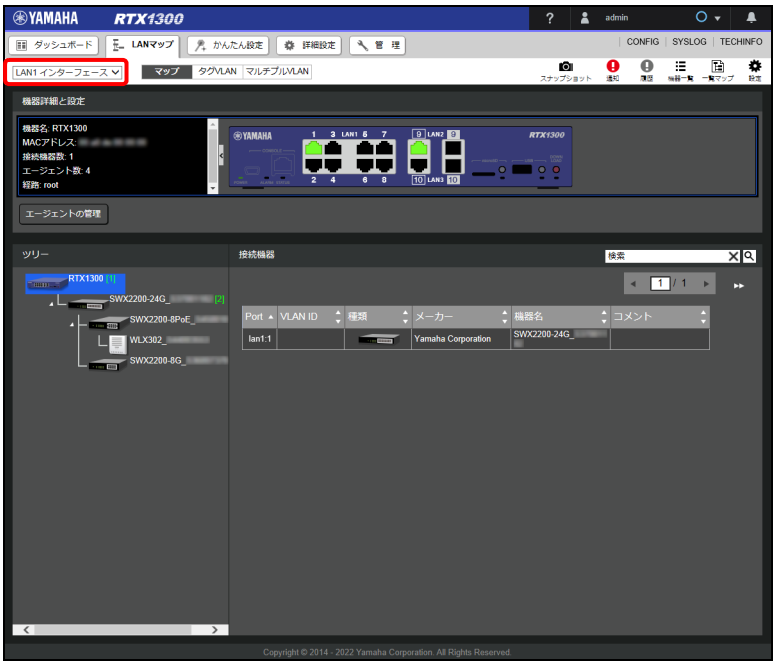
マルチプル VLAN の設定方法を説明します。マルチプル VLAN 機能とは、ヤマハスイッチのポートをグループ分けし、グループ間の通信を遮断する機能のことです。マルチプル VLAN 機能はヤマハスイッチのみに設定することができます。

メモ

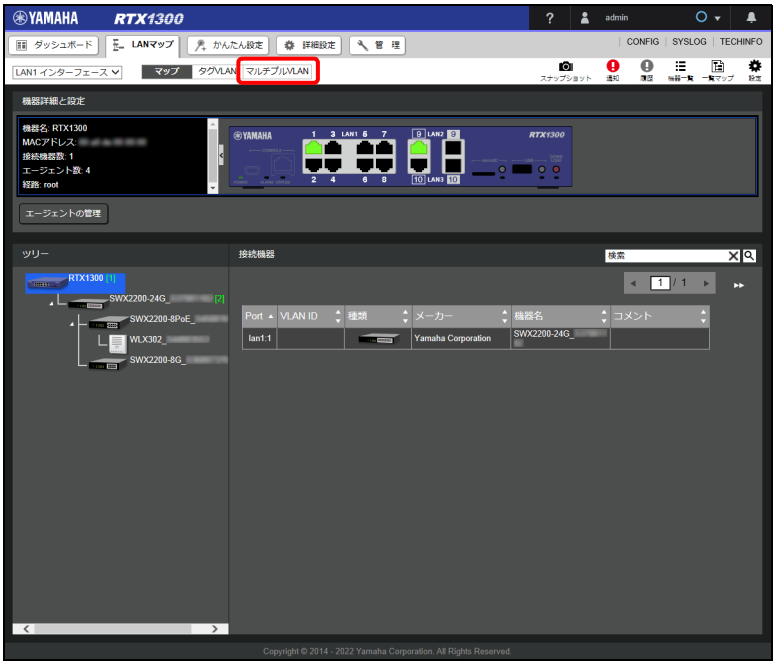
- マルチプル VLAN は対応しているスイッチをお使いの場合に設定できます。設定できるスイッチについて詳しくは下記の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/multiple_vlan.html
- サーバーやルーターなど全グループと通信する必要がある機器が接続されるポートについては、すべてのグループに参加させることで、すべてのグループとの通信を可能にすることができます。
- マルチプル VLAN 機能では、グループが異なっても同じネットワークアドレスが使用されます。

12.12.1 マルチプル VLAN ページを表示する

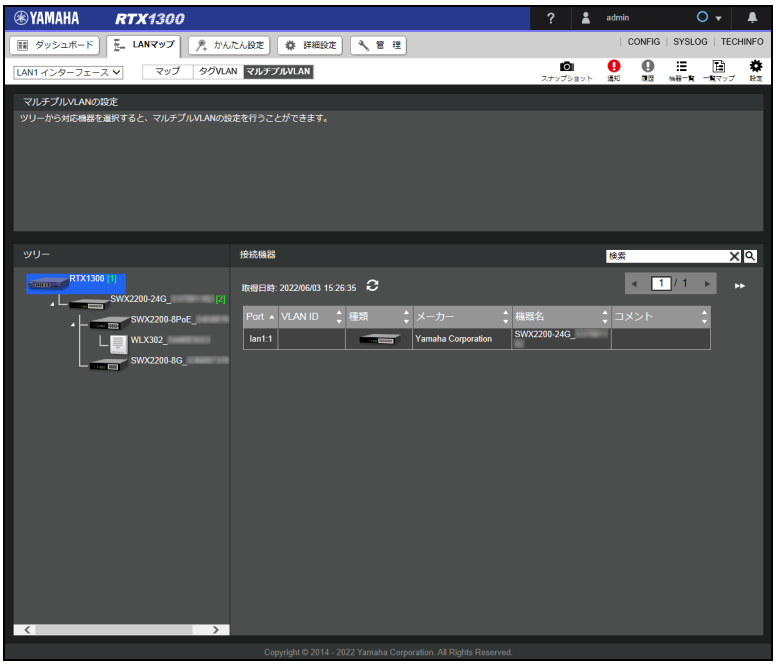
1. 設定したいネットワークのインターフェースを、インターフェース選択プルダウンメニューから選択する。



2. 表示選択スイッチで「マルチプル VLAN」を選択する。



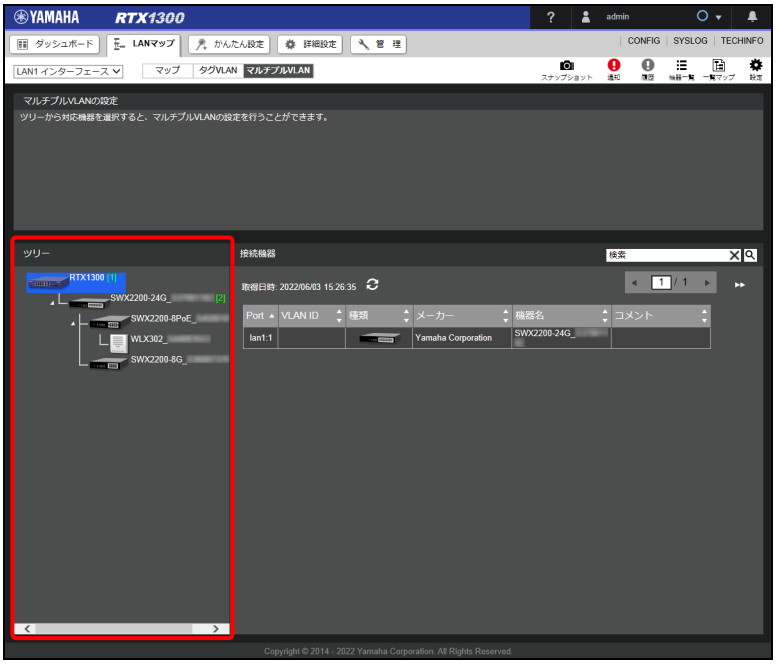
「マルチプル VLAN ページ」が表示されます。



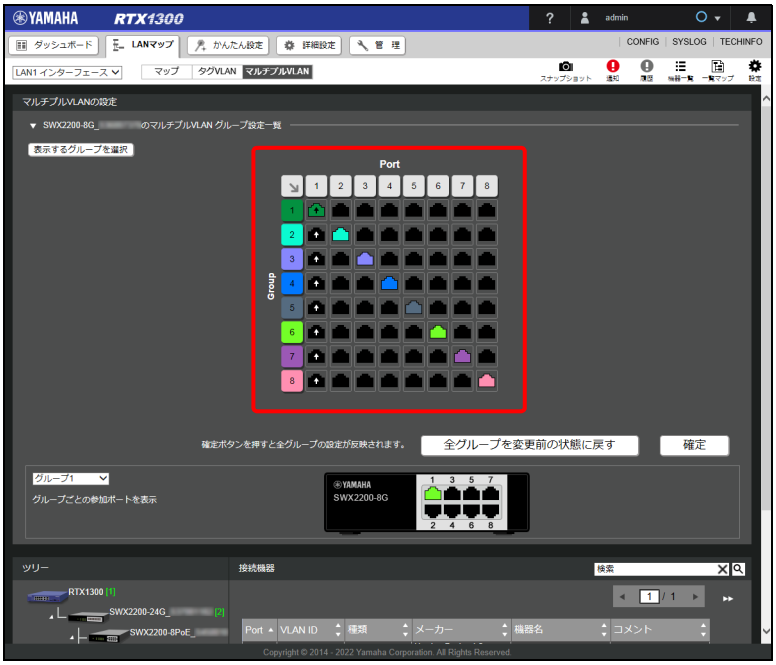
12.12.2 マルチプル VLAN グループを設定する

マルチプル VLAN のグループごとに、参加させるポートを設定します。

1. **「マルチプル VLAN ページ」を表示する。**
2. **ツリービューで確認したいヤマハスイッチのアイコンを選択する。**



3. マルチプル VLAN の設定ビューで、グループごとに参加ポートを選択する。



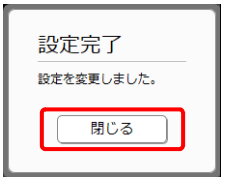
ポートを選択するとポートの色が変わり、指定のマルチプル VLAN グループに参加させることができます。また、選択したポートを再選択すると参加をキャンセルすることができます。

メモ

- ポートの番号をクリックすると、Port 列のすべてのグループのポートを選択できます。
- グループの番号をクリックすると、Group 行のすべてのポートを選択できます。
- 「 ↘ 」ボタンをクリックすると、左上から斜線上にポートを選択できます。
- 「表示するグループを選択」ボタンをクリックすると、マルチプル VLAN の設定ビューに表示したいグループを設定することができます。表示したいグループのみにチェックを入れ「確定」ボタンをクリックすると、選択したマルチプル VLAN のグループのみが表示されます。
- 「全グループを変更前の状態に戻す」ボタンをクリックすると、マルチプル VLAN に参加するポートを変更前の状態に戻すことができます。

4. 「確定」ボタンをクリックする。
マルチプル VLAN グループへの参加ポートが登録され、「設定完了」ダイアログが表示されます。

5. 「閉じる」ボタンをクリックする。

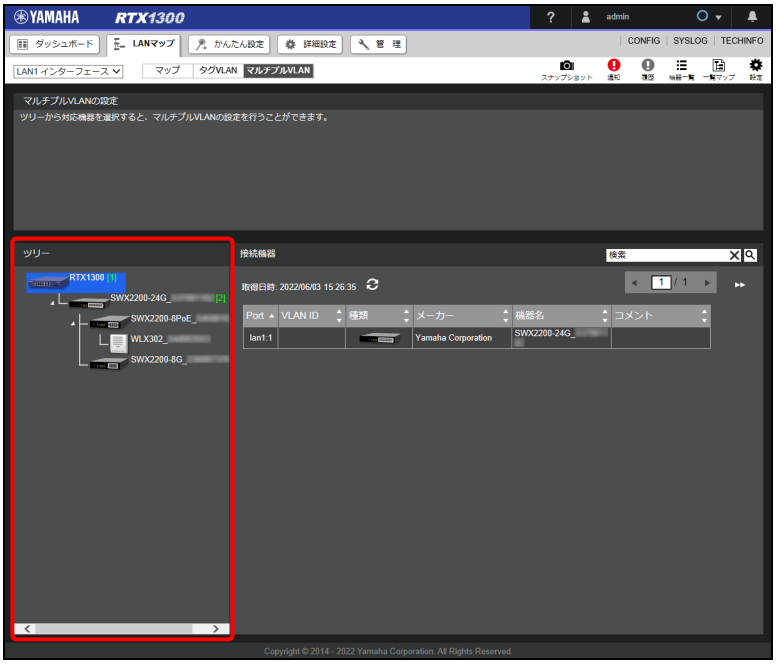


「マルチプル VLAN ページ」が表示されます。

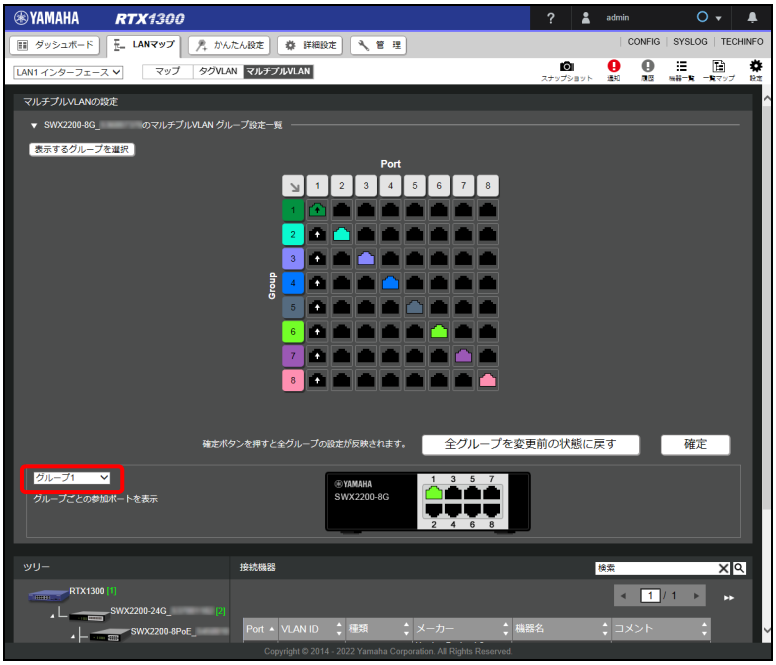
12.12.3 マルチプル VLAN グループの参加ポートを確認する

マルチプル VLAN のグループごとの参加ポートをスイッチ画像上で確認することができます。

1. 「マルチプル VLAN ページ」を表示する。
2. ツリービューで確認したいヤマハスイッチのアイコンを選択する。



3. 「グループごとの参加ポートを表示」項目のプルダウンメニューから、表示させたいグループを選択する。



右側のスイッチ画像で、選択したグループに参加しているポートがグループに対応した色に切り替わります。

12.13 接続機器の一覧を見る

LAN マップで管理している機器の一覧を表示することができます。端末情報の編集を行ったり、端末情報 DB をエクスポートしたりすることができます。端末情報 DB とは、端末ごとの詳細情報を記載した CSV 形式のファイルのことで、RTFS に自動的に保存されます。RTFS とは、本製品の不揮発性メモリーに構築されるファイルシステムのことです。端末情報 DB は Web GUI 上での編集に加え、エクスポートしてパソコン上で編集することもできます。端末の検索を行ったとき、端末情報 DB に登録された端末であれば端末情報が自動的に反映されます。端末ごとの情報を事前に設定しておくことができるため、検出された端末の管理が簡単になります。

また、「 一覧マップ 」ボタンをクリックすると、ネットワークに接続された機器全体を一覧マップで表示することができます。一覧マップについては、「12.13.10 一覧マップで表示する」（231 ページ）をご覧ください。

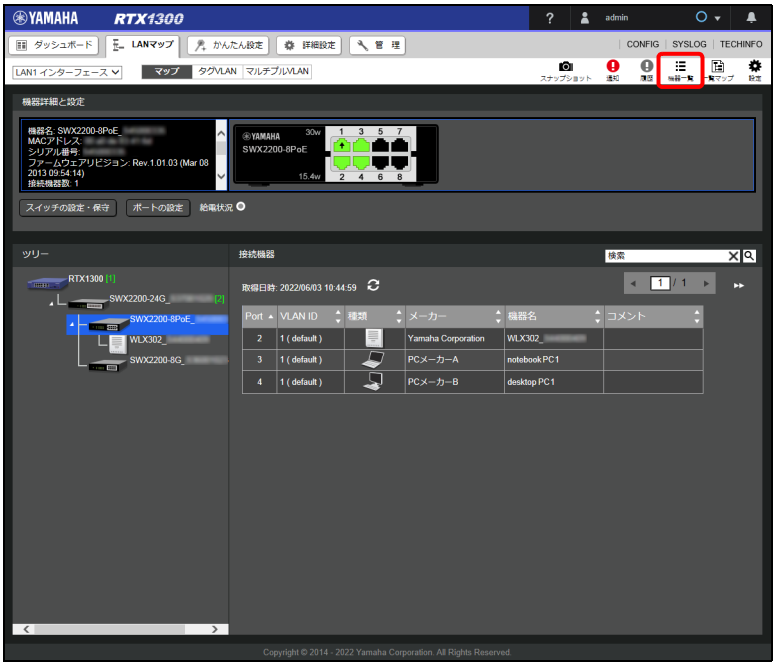
注意

- RTFS の空き容量が足りない場合、端末情報 DB は保存されません。
- 工場出荷状態に戻したり RTFS をフォーマットしたりすると、端末情報 DB の情報も初期化されます。

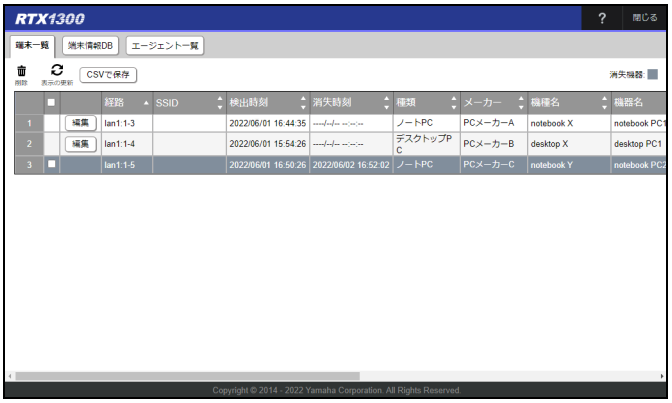
12.13.1 端末一覧画面を表示する

LAN マップで管理している端末を一覧表示します。「端末一覧」画面では、存在を確認できている端末だけでなく、存在を確認できなくなった端末も消失端末として表示され、消失した時刻が確認できます。LAN に接続されている端末であっても、無通信状態が長く続くと消失扱いになる場合があります。なお、消失扱いになった端末でも、存在が確認できた時点で消失扱いではなくなります。

1. **「 機器一覧 」ボタンをクリックする。**



「端末一覧」画面が表示され、LAN マップで管理している端末の情報が確認できます。



項目ごとの「 」ボタンをクリックすることでリストを並び替えることができます。初期表示では経路順にソートされています。なお、消失している端末はグレーにハイライトされて表示されます。

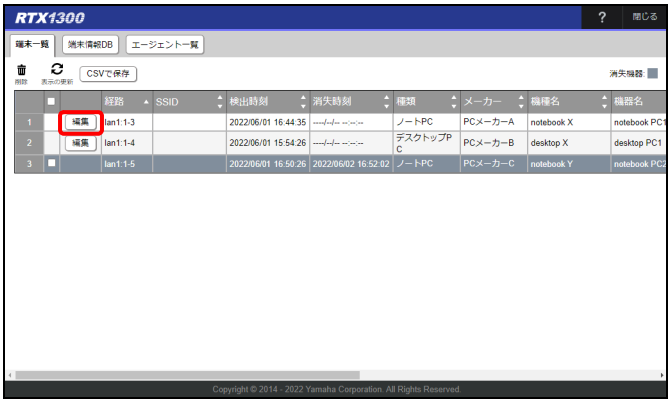
メモ

- 「 削除 」ボタンをクリックすると、選択した端末の情報が端末一覧から削除されます。消失端末の情報のみ削除することができます。実際に LAN から切断している端末で、情報が不要になった場合に削除します。
- 「 表示の更新 」ボタンをクリックすると、「端末一覧」画面の表示が、マネージャーが保持している最新の情報に更新されます。
- 「CSV で保存」ボタンをクリックすると、端末一覧情報を CSV ファイル形式で保存することができます。

12.13.2 端末の情報を編集する

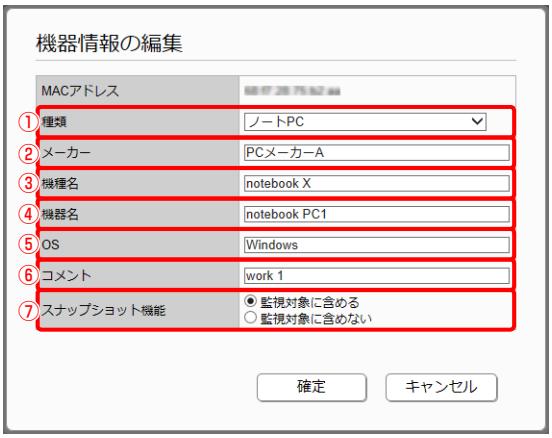
LAN マップで管理している端末の情報を編集することができます。編集した情報は自動的に端末情報 DB にも登録されます。

1. **「端末一覧」画面で編集したい端末の「編集」ボタンをクリックする。**



「機器情報の編集」ダイアログが表示されます。

2. **端末の情報を編集する。**



① **種類：**
プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

② **メーカー：**
メーカー名を入力します。

③ **機種名：**
機種名を入力します。

④ **機器名：**
機器名を入力します。

⑤ **OS：**
OS 名を入力します。

⑥ **コメント：**
任意のコメントを入力します。

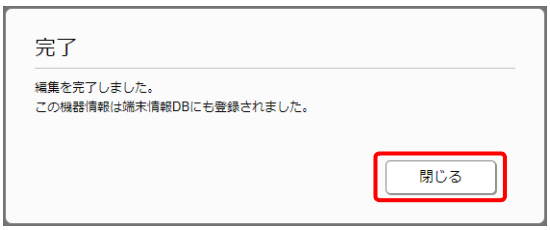
⑦ **スナップショット機能：**
スナップショット機能の監視対象に含める / 含めないを選択します。

メモ

端末情報 DB に登録済みの端末情報の編集は、「端末情報 DB」画面でも行えます。

3. **「確定」ボタンをクリックする。**
端末の情報が変更され、「完了」ダイアログが表示されます。

4. **「閉じる」ボタンをクリックする。**



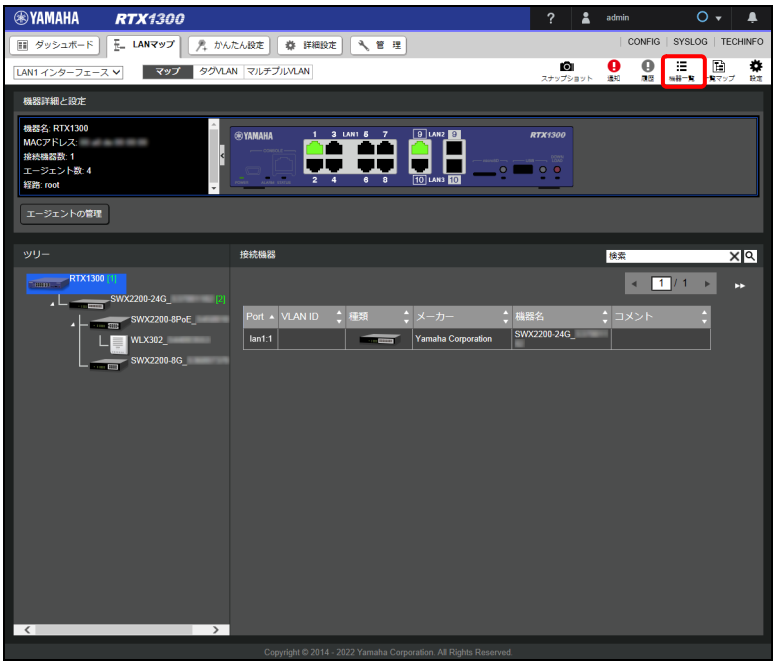
「端末一覧」画面が表示されます。

12.13.3 端末情報 DB 画面を表示する

端末情報の基準となる情報を端末情報 DB と呼びます。LAN マップで検出された端末と MAC アドレスが一致する端末情報が端末情報 DB に登録されていれば、端末情報 DB の情報が接続機器ビューや「端末一覧」画面に表示されるようになります。

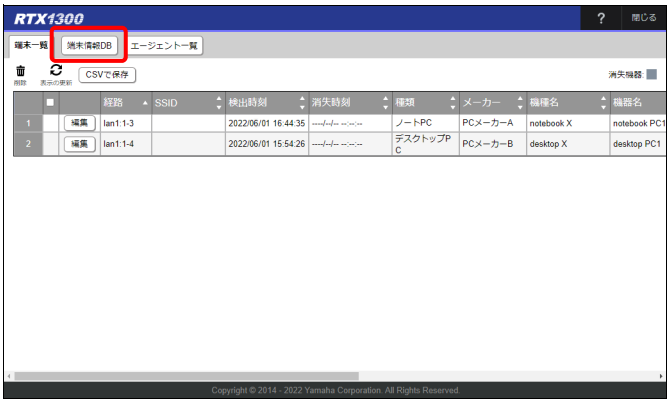
「端末情報 DB」画面では端末情報 DB に登録されている端末情報を一覧表示します。端末情報 DB の情報を新規に登録したり、登録済みの情報を編集したりすることができます。

1. 「 機器一覧 」ボタンをクリックする。

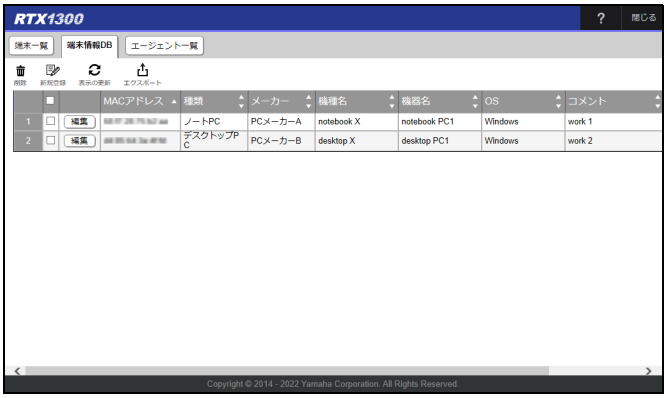


「端末一覧」画面が表示されます。

2. 「端末情報 DB」タブをクリックする。



「端末情報 DB」画面が表示され、端末情報 DB に登録されている端末情報が確認できます。



項目ごとの「 」ボタンをクリックすることでリストを並び替えることができます。初期表示では MAC アドレス順にソートされています。

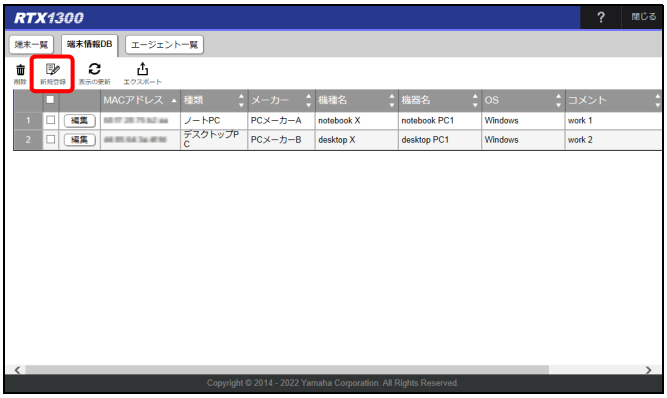
メモ

- 「 削除 」ボタンをクリックすると、選択した端末の情報が端末情報 DB から削除されます。
- 「 表示の更新 」ボタンをクリックすると、「端末情報 DB」画面の表示が更新されます。
- 「 エクスポート 」ボタンをクリックすると、端末情報 DB の情報を CSV ファイル形式で保存することができます。

12.13.4 端末情報 DB に端末情報を新規登録する

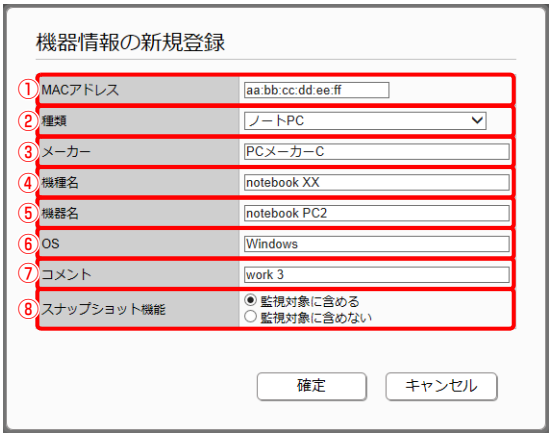
端末の情報を端末情報 DB に新規登録することができます。

1. **「端末情報 DB」画面で「 新規登録 」ボタンをクリックする。**



「機器情報の新規登録」ダイアログが表示されます。

2. **端末の情報を登録する。**



① **MAC アドレス：**
MAC アドレスを「aa:bb:cc:dd:ee:ff」の形式で入力します。

② **種類：**
プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

③ **メーカー：**
メーカー名を入力します。

④ **機種名：**
機種名を入力します。

⑤ **機器名：**
機器名を入力します。

⑥ **OS：**
OS 名を入力します。

⑦ **コメント：**
任意のコメントを入力します。

⑧ **スナップショット機能：**
スナップショット機能の監視対象に含める / 含めないを選択します。

3. **「確定」ボタンをクリックする。**
端末の情報が登録され、「完了」ダイアログが表示されます。

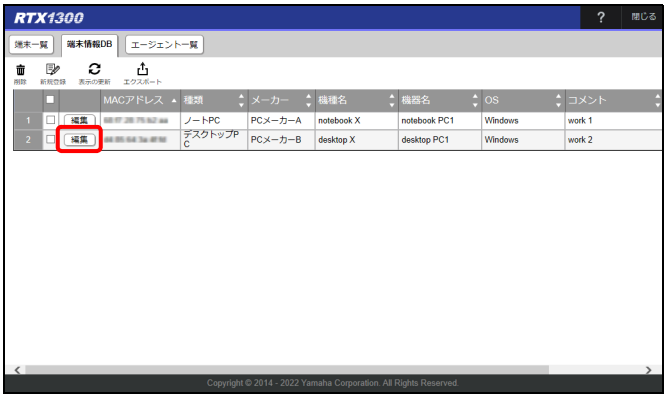
4. **「閉じる」ボタンをクリックする。**

「端末情報 DB」画面が表示されます。

12.13.5 端末情報 DB に登録されている端末情報を編集する

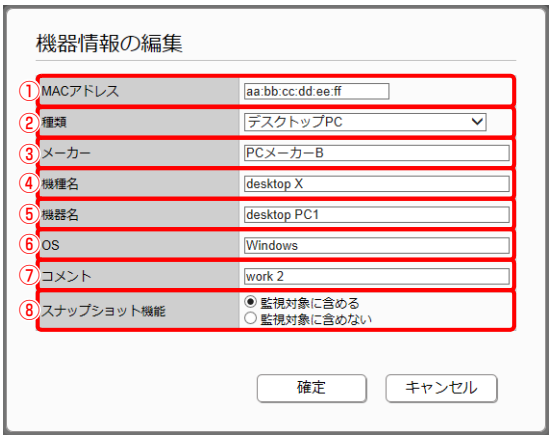
端末情報 DB に登録されている端末の情報を編集することができます。

1. **「端末情報 DB」画面で編集したい端末の「編集」ボタンをクリックする。**



「機器情報の編集」ダイアログが表示されます。

2. **端末の情報を編集する。**



① MAC アドレス：
MAC アドレスを「aa:bb:cc:dd:ee:ff」の形式で入力します。

② 種類：
プルダウンメニューから端末の種類を選択します。選択した種類に合わせて接続機器ビューの端末アイコンが切り替わります。

③ メーカー：
メーカー名を入力します。

④ 機種名：
機種名を入力します。

⑤ 機器名：
機器名を入力します。

⑥ OS：
OS 名を入力します。

⑦ コメント：
任意のコメントを入力します。

⑧ **スナップショット機能：**
スナップショット機能の監視対象に含める / 含めないを選択します。

3. **「確定」ボタンをクリックする。**
端末の情報が登録され、「完了」ダイアログが表示されます。

4. **「閉じる」ボタンをクリックする。**

「端末情報 DB」画面が表示されます。

12.13.6 端末情報 DB ファイルをパソコンへエクスポートする

端末情報 DB はファイル形式で RTFS に保存されており、ルーター間で移行することができます。ネットワーク全体で使用する端末の情報を一つの端末情報 DB ファイルにまとめておき、各ルーターでその端末情報 DB を共有したり、ルーターをリプレースする際に新しいルーターへ端末情報 DB ファイルを移行して端末情報を引き継いだり、といった使い方ができます。
本項では、TFTP を使用して端末情報 DB ファイルをパソコンへエクスポートする方法について説明します。

注意

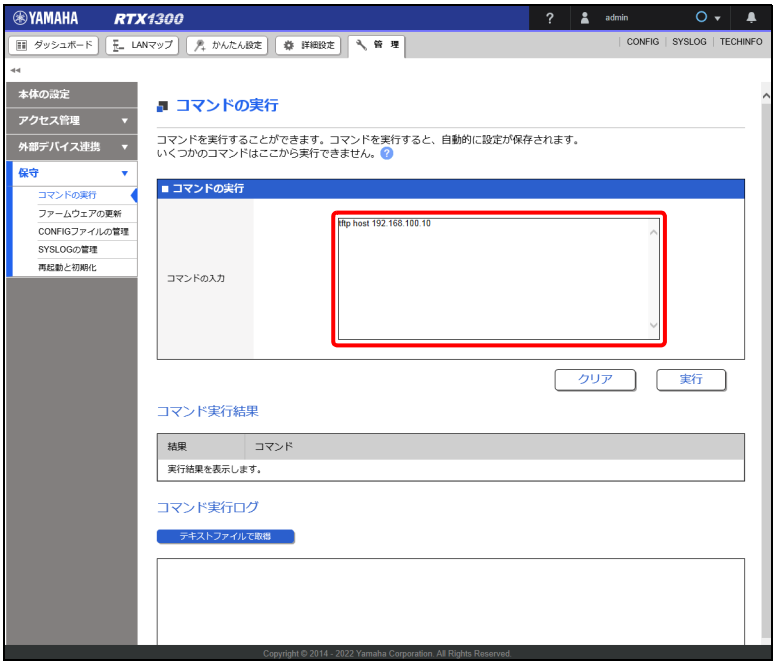
工場出荷状態に戻したり、RTFS をフォーマットしたりすると、端末情報 DB ファイルも消去されてしまうため、定期的にバックアップしておくことをおすすめいたします。

1. **「管理」タブ ―「保守」―「コマンドの実行」を順に選択する。**
「コマンドの実行」画面が表示されます。

メモ

「端末情報 DB」画面の「エクスポート」ボタンからエクスポートすることもできます。

2. 「コマンドの実行」項目にコマンドを入力する。
   tftp host コマンドでエクスポート先のパソコンの IP アドレスを設定します。



コマンドの入力例

- エクスポート先のパソコンの IP アドレス：192.168.100.10

```
tftp host 192.168.100.10
```

3. 「実行」ボタンをクリックする。

4. パソコンのコマンドプロンプトを起動して、tftp コマンドを実行する。
   - 使用するコマンドの形式は、OS に依存します。
   - tftp コマンドのパラメーターに、ヤマハルーターの IP アドレスを指定します。
   - 転送モードは「アスキー」または「文字」にします。
   - ヤマハルーターに管理パスワードが設定されている場合は、ファイル名に続けて管理パスワードを指定します。

コマンドの入力例

- ヤマハルーターの IP アドレス：192.168.100.1
- ヤマハルーターの管理パスワード：adM123
- 端末情報 DB ファイルのファイルパス（固定）：/lanmap/devinfo_master.csv

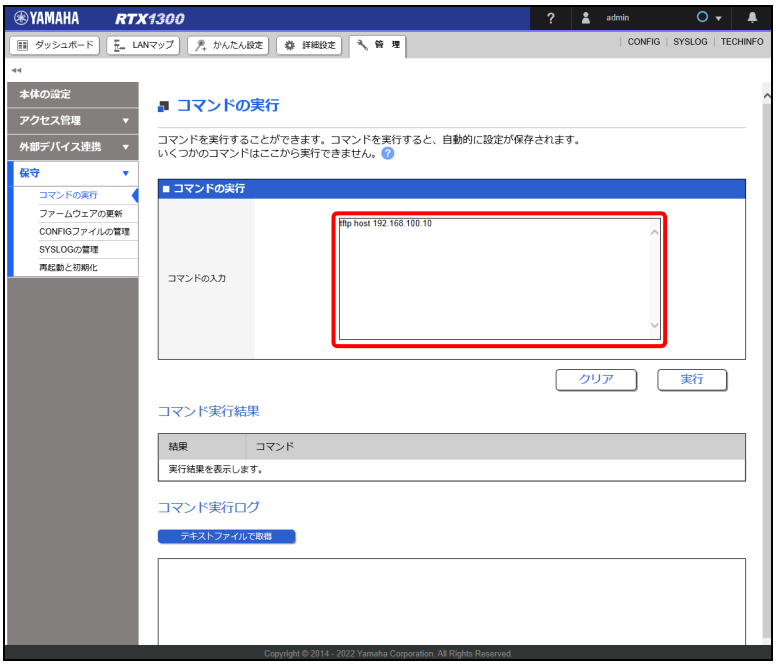
```
C:¥>tftp 192.168.100.1 get /lanmap/devinfo_master.csv/adM123
devinfo_master.csv
転送を正常に完了しました： 1 秒間に xxxx バイト、xxxx バイト / 秒

C:¥>
```

12.13.7 端末情報 DB ファイルをパソコンからインポートする

本項では、TFTP を使用して端末情報 DB ファイルをパソコンからインポートする方法について説明します。リプレースの際に端末情報 DB ファイルを新しいルーターへ移行する場合などは、パソコンを新しいルーターに接続して本操作を行ってください。

1. **「管理」タブ ―「保守」―「コマンドの実行」を順に選択する。**
   「コマンドの実行」画面が表示されます。

2. **「コマンドの実行」項目にコマンドを入力する。**
   tftp host コマンドでインポート元のパソコンの IP アドレスを設定します。



コマンドの入力例

- インポート元のパソコンの IP アドレス：192.168.100.10

```
tftp host 192.168.100.10
```

3. **「実行」ボタンをクリックする。**

4. **パソコンのコマンドプロンプトを起動して、tftp コマンドを実行する。**
   - 使用するコマンドの形式は、OS に依存します。
   - tftp コマンドのパラメーターに、ヤマハルーターの IP アドレスを指定します。
   - 転送モードは「アスキー」または「文字」にします。
   - ヤマハルーターに管理パスワードが設定されている場合は、ファイル名に続けて管理パスワードを指定します。
   - 端末情報 DB ファイルが保存されているディレクトリに移動します。

コマンドの入力例

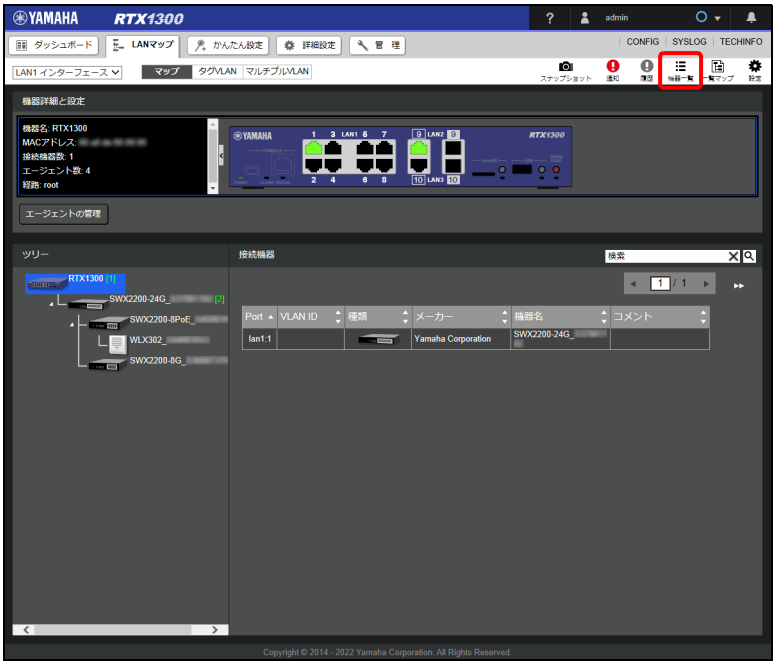
- ヤマハルーターの IP アドレス：192.168.100.1
- ヤマハルーターの管理パスワード：adM123
- 端末情報 DB ファイルのファイルパス（固定）：/lanmap/devinfo_master.csv

```
C:¥>tftp 192.168.100.1 put devinfo_master.csv /lanmap/
devinfo_master.csv/adM123
転送を正常に完了しました： 1 秒間に xxxx バイト、xxxx バイト / 秒

C:¥>
```

12.13.8 エージェント一覧画面を表示する

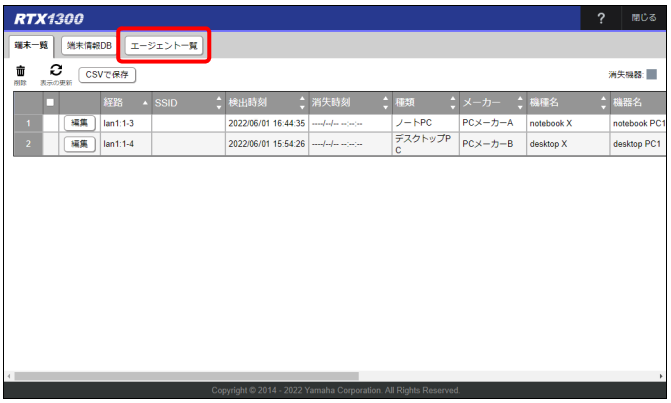
LAN マップで管理しているエージェントを一覧表示します。「エージェント一覧」画面では、存在を確認できているエージェントだけでなく、存在を確認できなくなったエージェントも消失機器として表示され、消失した時刻が確認できます。LAN に接続されているエージェントであっても、応答がない状態が続くと消失扱いになる場合があります。なお、消失扱いになったエージェントでも、存在が確認できた時点で消失扱いではなくなります。

1. 「 」ボタンをクリックする。

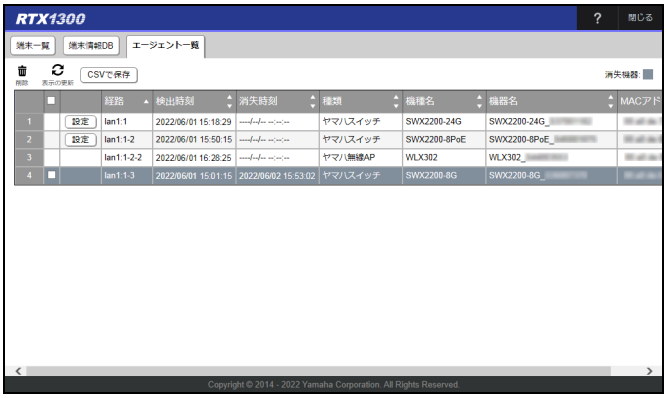


「端末一覧」画面が表示されます。

2.「エージェント一覧」タブをクリックする。



「エージェント一覧」画面が表示され、LAN マップで管理しているエージェントの情報が確認できます。



項目ごとの「 」ボタンをクリックすることでリストを並び替えることができます。初期表示では経路順にソートされています。なお、消失しているエージェントはグレーにハイライトされて表示されます。

メモ

- 「削除」ボタンをクリックすると、選択したエージェントの情報がエージェント一覧から削除されます。消失しているエージェントの情報のみ削除することができます。実際に LAN から切断しているエージェントで、情報が不要になった場合に削除します。
- 「表示の更新」ボタンをクリックすると、「エージェント一覧」画面の表示が、マネージャーが保持している最新の情報に更新されます。
- 「CSV で保存」ボタンをクリックすると、エージェント一覧情報を CSV ファイル形式で保存することができます。

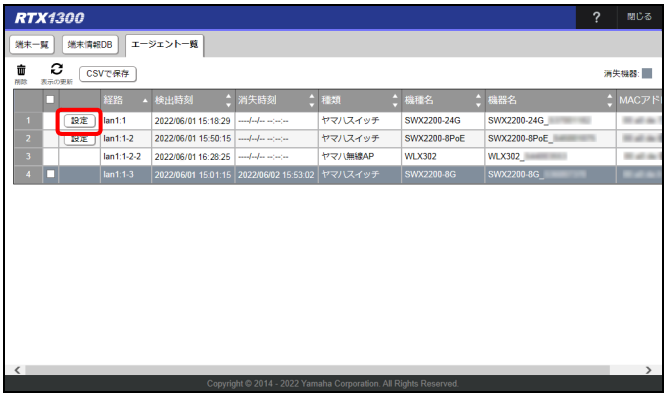
12.13.9 エージェントの機器名を変更する

LAN マップで管理しているエージェントの機器名を変更することができます。工場出荷時は、“機種名 _ シリアル番号” という形式で機器名が付与されています。

メモ

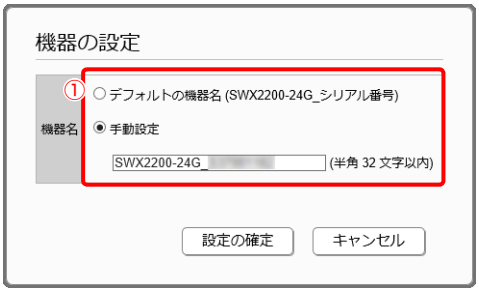
- ヤマハスイッチの機器名は対応しているスイッチのみ「エージェント一覧」画面で変更できます。設定できるスイッチについて詳しくは下記の URL をご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/lanmap/device_list.html#SLAVE
- 無線 AP の機器名は「エージェント一覧」画面では変更することができません。無線 AP の機器名は無線 AP の Web GUI で変更することができます。Web GUI で、「管理機能」メニューの「基本設定」を開きます。「本製品の情報」の「名称」を任意の名称に変更し、「設定」ボタンをクリックすると、無線 AP の機器名を変更できます。無線 AP の Web GUI の開き方は「12.8.5 無線 AP の設定画面を表示する」（201 ページ）をご覧ください。
- エージェントルーターの機器名は、「エージェント一覧」画面で変更できます。

1. **「エージェント一覧」画面で機器名を変更したいエージェントの「設定」ボタンをクリックする。**



「機器の設定」ダイアログが表示されます。

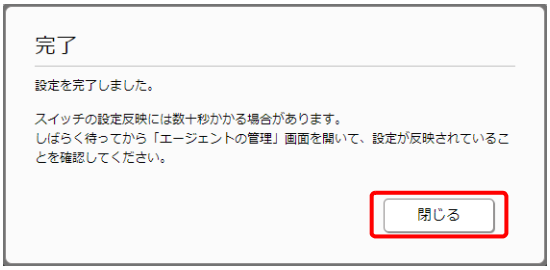
2. **エージェントの機器名を変更する。**



① 機器名：
機器名を入力します。
「デフォルトの機器名」を選択した場合は、各機器ごとに決められたデフォルトの機器名が設定されます。通常は、機種名およびシリアル番号からなる文字列となります。「手動設定」を選択した場合は、直後の入力ボックスに入力した機器名が設定されます。

3. **「設定の確定」ボタンをクリックする。**
機器名が変更され、「完了」ダイアログが表示されます。

4. 「閉じる」ボタンをクリックする。



「エージェント一覧」画面が表示されます。

12.13.10 一覧マップで表示する

ネットワークに接続されている機器全体を 1 つのトポロジーで表示します。トポロジーの表示範囲や機器情報の表示を切り替えることができ、自分が見やすいようにカスタマイズできます。さらに、印刷機能を使って表示している一覧マップを印刷でき、ネットワーク運用管理業務のさまざまな場面で活用することができます。

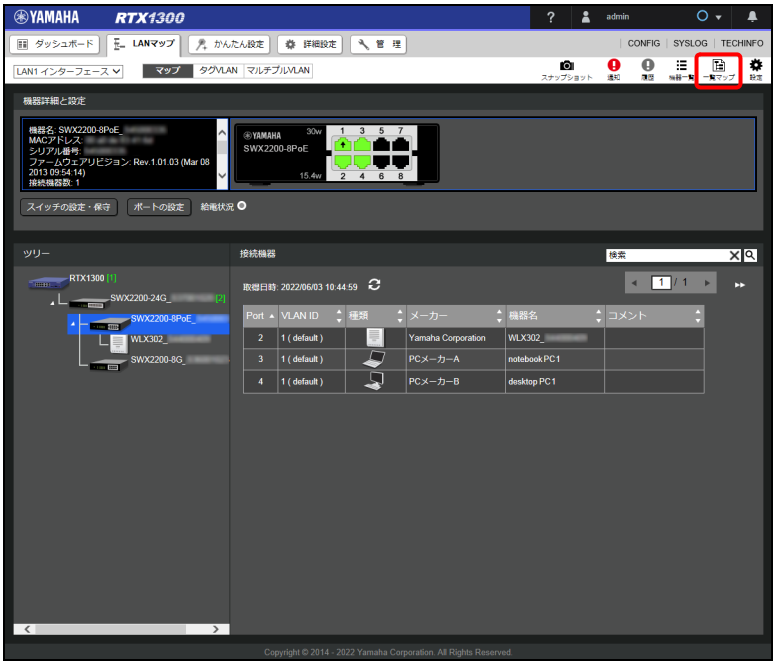
重要

一覧マップの表示設定は Cookie を用いて保存しています。一覧マップの表示設定を保存するには、ウェブブラウザーの Cookie を有効にしてください。ウェブブラウザーの設定を変更し、再度「一覧マップ」画面にアクセスしたときに設定変更が反映されていない場合は、ウェブブラウザーの Cookie が無効になっているか、Cookie が削除された可能性があります。

メモ

機器間のリンク速度（上位の機器のポートのリンク速度）は、機器アイコン間の接続線の色で確認できます。それぞれの色とリンク速度の対応については、画面右上の凡例をご確認ください。また、ヤマハ無線 AP 配下の端末、および機種を識別できないヤマハスイッチは、リンク速度を取得できないため、灰色（リンク速度が不明であることを示す色）の接続線で表示されます。

1. 「  」ボタンをクリックする。



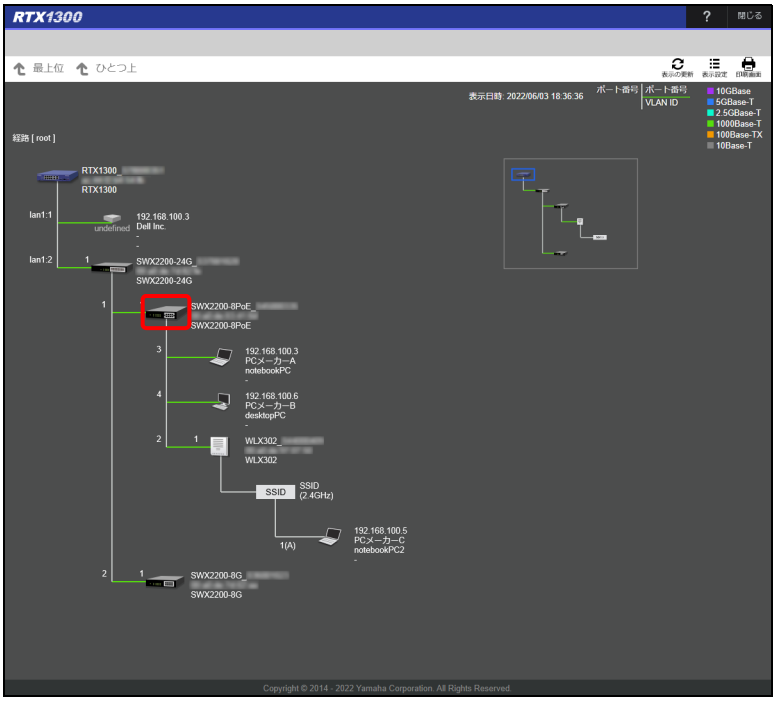
一覧マップが表示され、ネットワークに接続されている機器全体がトポロジーで確認できます。

メモ

・「 表示の更新 」ボタンをクリックすると、「エージェント一覧」画面の表示が、マネージャーが保持している最新の情報に更新されます。

・「 表示設定 」ボタンをクリックすると、一覧マップで表示される機器の情報を設定することができます。

2. 各機器のアイコンをクリックする。



配下のエージェントのみの表示に切り替わります。

メモ

・画面右のマップ内で青枠で囲われている機器（ ）は、現在表示されているトポロジーの起点にあたる機器を示しています。

・「 最上位 」ボタンまたは「 ひとつ上 」ボタンをクリックすると、マネージャーを起点としたトポロジー全体や、ひとつ上の機器を起点とした範囲に戻ります。

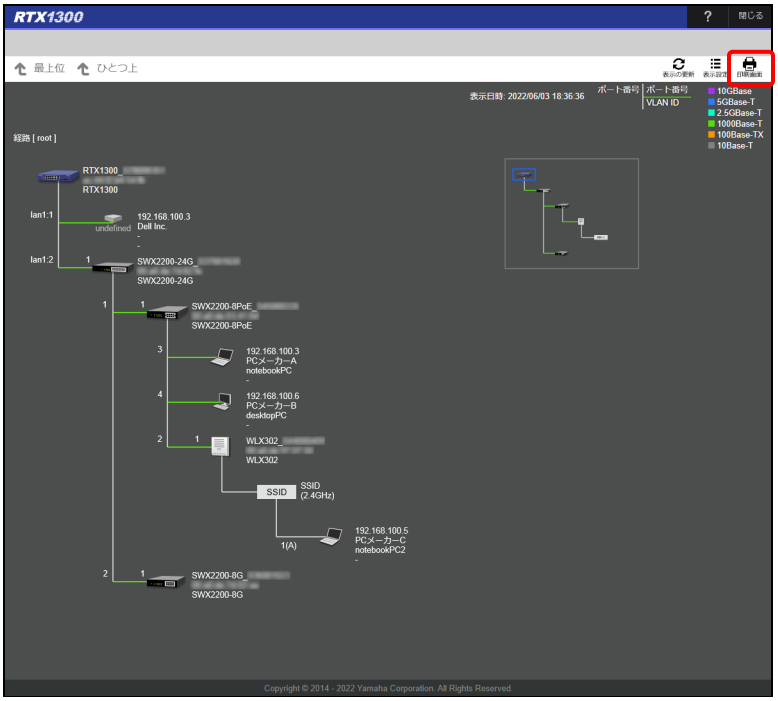
12.13.11 一覧マップを印刷する

印刷画面を表示して、一覧マップを印刷することができます。

メモ

印刷機能を使用する場合は Firefox 以外の推奨ウェブブラウザーからご利用ください。一覧マップはひとつの SVG 画像となっています。Firefox はひとつの SVG 画像の複数枚印刷に対応していないため、印刷対象の一覧マップが大きく印刷枚数が 2 枚以上になる場合、正しく印刷されません。

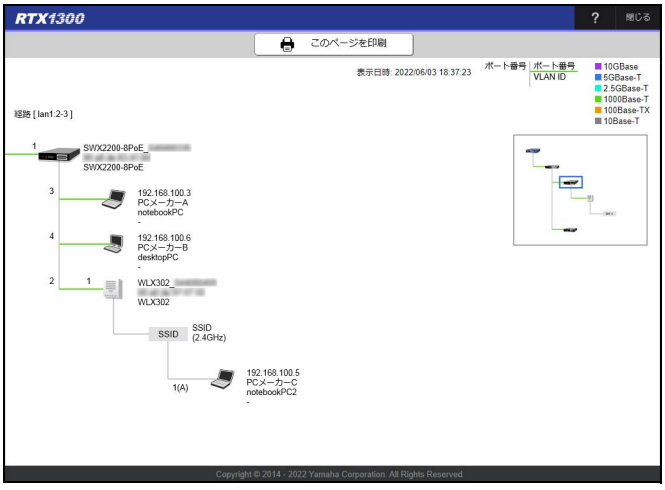
1. 一覧マップで「 印刷画面 」ボタンをクリックする。



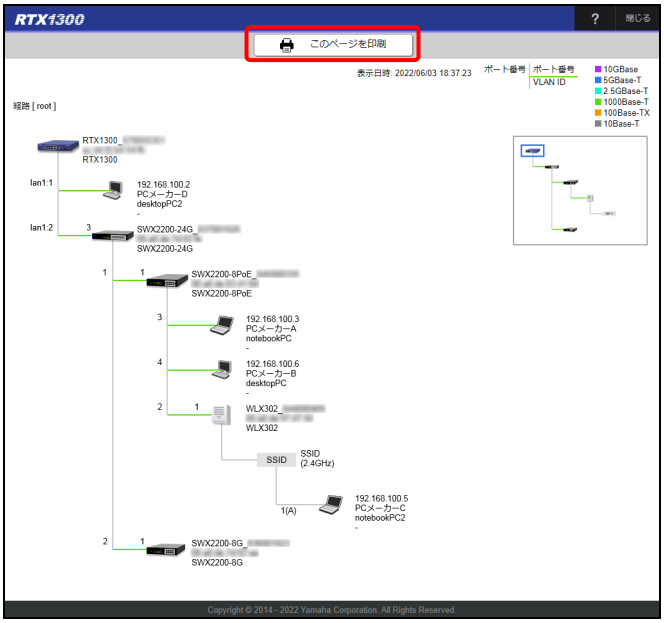
印刷画面が表示されます。

メモ

一覧マップでトポロジーの起点となる機器の表示を変えている場合は、印刷画面でも同じトポロジーが表示されます。



2. 「このページを印刷」ボタンをクリックする。



プリンターの選択画面が表示されます。

3. **プリンターを選択し、必要に応じて印刷設定をして印刷する。**
一覧マップが印刷されます。

第 13 章 セキュリティーを強化する

本章では、セキュリティーについて説明します。インターネットに接続している間は、悪意のある者からルーターやパソコンが攻撃（不正アクセス）される可能性があります。不正アクセスによりルーターの設定を改変されたり、パソコンのシステムやデータを破壊されたりした場合、多大なデータ的被害や金銭的被害に遭うことも十分に考えられます。本製品のフィルター設定などのセキュリティー対策を行って、自己防衛してください。

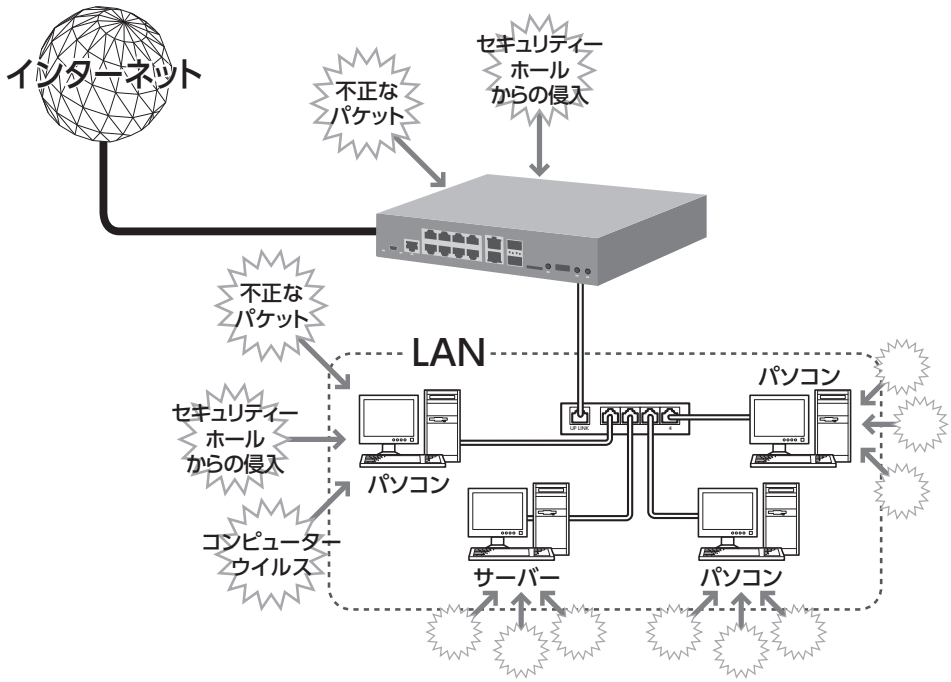
・ 不正アクセスとは？ …235 ページ
・ 不正アクセスに対抗する …236 ページ
・ 不正アクセス検知を有効にする …237 ページ
・ IP フィルターを設定する …242 ページ
・ URL フィルターを設定する …257 ページ
・ 本製品へのアクセスを管理する …288 ページ

13.1 不正アクセスとは？

不正アクセスとは、本来アクセス権限を持たない者が、ネットワークを通じてインターネット側から内部の LAN に侵入する行為を指します。悪意のある者に侵入された場合、ルーターの設定が改変されたり、パソコンのシステムやデータが破壊されたりするといった攻撃を受ける恐れがあります。
ルーターを介してパソコンを接続している場合は、NAT や IP マスカレードといったアドレス変換機能によってインターネット側から内部の LAN へ侵入することができなくなるため、比較的安全が保たれますが、設定の誤りや不足によって、同様の危険にさらされる場合があります。

注意

インターネット経由の不正アクセスだけでなく、マルウェアによる攻撃にも注意が必要です。



13.1.1 グローバル IP アドレスが割り当てられている場合

悪意を持った者が攻撃（不正アクセス）するときに主な足がかりにするのが「グローバル IP アドレス」です。同じグローバル IP アドレスを長時間使用している場合は、不正アクセスの被害に遭う確率が高くなります。固定 IP アドレスサービスの利用時やネットワーク型接続、接続時に割り当てられた動的アドレスを使い続けるブロードバンド回線を使用する場合は、十分なセキュリティー対策を行うことをおすすめいたします。

13.1.2 パスワードを設定していない場合

本製品を初期パスワードのまま使用することは、セキュリティー上大変危険です。単にパスワードを設定するだけでなく、定期的にパスワードを変更するようにしてください。

13.2 不正アクセスに対抗する

インターネットの不正アクセスは、いくつかの侵入経路に分けられます。それぞれの侵入経路に合った対策をしてください。

注意

- **不正アクセスの手段やセキュリティー上の抜け道 / 穴（セキュリティーホール）は、日夜新たに発見されています。本製品の機能を含めて、すべての問題を解決できる完璧なセキュリティー対策は存在せず、インターネット接続には常に危険があることをご理解ください。常に新しい情報を入手し、お客様の自己責任でセキュリティー対策を強化することを強くおすすめいたします。**
- **本製品を使用した結果により発生したあらゆる損失について、弊社では一切その責任を負いかねますので、あらかじめご了承ください。**

13.2.1 インターネット側から内部の LAN への侵入

インターネット側から内部の LAN への侵入を防ぐには、以下の対応が効果的です。

- インターネット接続の切断
- グローバル IP アドレスの変更
- パケットフィルタリング式ファイアウォールの導入
- アプリケーション・ゲートウェイ式ファイアウォールソフトウェアの導入
- NAT によるプライベート IP アドレスの隠蔽

本製品で可能な対策

- 自動切断機能の設定
  接続 / 切断のたびに動的 IP アドレスを変更できます。ただし、サーバー公開用途に本製品を使用する場合には、この対策を実施することは困難となりますので、サーバー側で対策を行ってください。
- 不正アクセス検知の設定
  不正アクセスとして判定されたパケットを検知、または破棄する（237 ページ）ことで、さまざまな種類の攻撃（不正アクセス）を防御します。
- フィルターの設定
  攻撃に使用される特定の種類のパケットを通さないようにフィルターを設定する（242 ページ）ことで、その攻撃を防御できることがあります。

13.2.2 OS やサーバーソフトウェアのセキュリティーホールからの侵入

OS やサーバーソフトウェアのバージョンアップや、適切に設定 / 運用することが効果的です。

本製品で可能な対策

- Web GUI へのアクセス制限の設定
  本製品の設定を変更できるホストを制限して、悪意のある第三者が本製品の設定を勝手に変更することを防止できます（288 ページ）。

・フィルターの設定
攻撃に使用される特定の種類のパケットを通さないようにフィルターを設定する（242 ページ）ことで、その攻撃を防御できることがあります。

13.2.3 電子メールの添付ファイルからの侵入

電子メールに添付されたウイルスが仕込まれたファイルを開くことで、パソコンがウイルスに感染します。不審な添付ファイルは開かないことを徹底するだけでなく、パソコンにウイルス検知ソフトウェアをインストールして、ウイルスを早期発見 / 早期駆除することで、被害を最小限に抑えることができます。

本製品で可能な対策

・メールセキュリティー機能の使用
ヤマハのファイアウォール製品ではメールセキュリティー機能を搭載しています。ファイアウォール製品を本製品と併用することで、パソコンごとに個別にウイルス検知ソフトウェアをインストールしていない環境でも、コンピューターウイルスの感染を防御できるようになります。

13.3 不正アクセス検知を有効にする

悪意のある者からの攻撃（不正アクセス）を検知し、遮断することができます。
不正アクセス検知はインターフェースごとに設定が可能で、不正アクセスの分類ごとに検知の有効・無効を設定することができます。

注意

不正アクセスの手段やセキュリティー上の抜け道 / 穴（セキュリティーホール）は、日夜新たに発見されています。より強固なセキュリティを構築するために、不正アクセス検知に加えて、IP フィルター（242 ページ）や URL フィルター（257 ページ）を設定してください。

13.3.1 不正アクセス検知を設定する

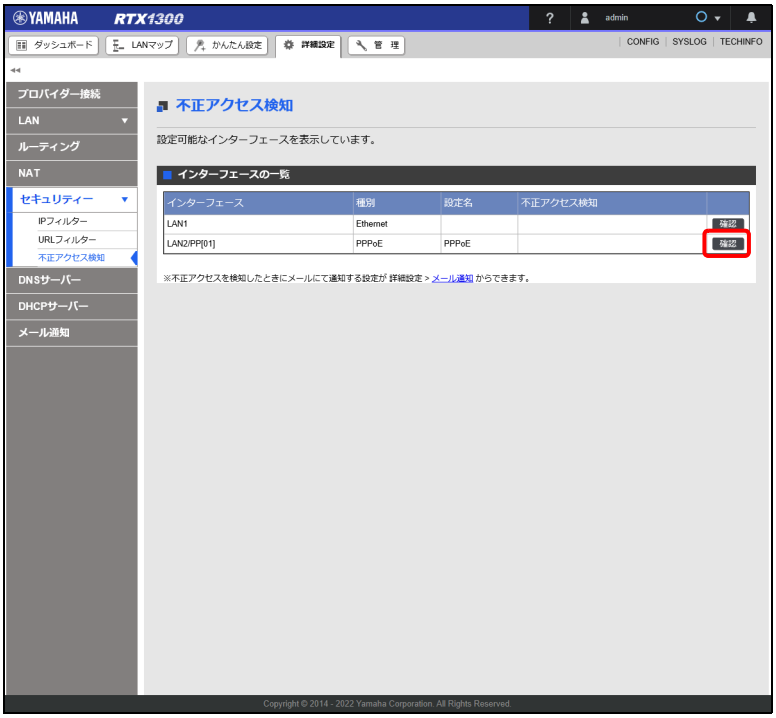
検知対象とする不正アクセス分類と、不正アクセスと判定されたパケットを破棄するか否かを設定します。
本項では、「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定するという前提で説明します。

設定例

不正アクセスを検知する分類：IP ヘッダー
検知したパケットを破棄する分類：設定しない

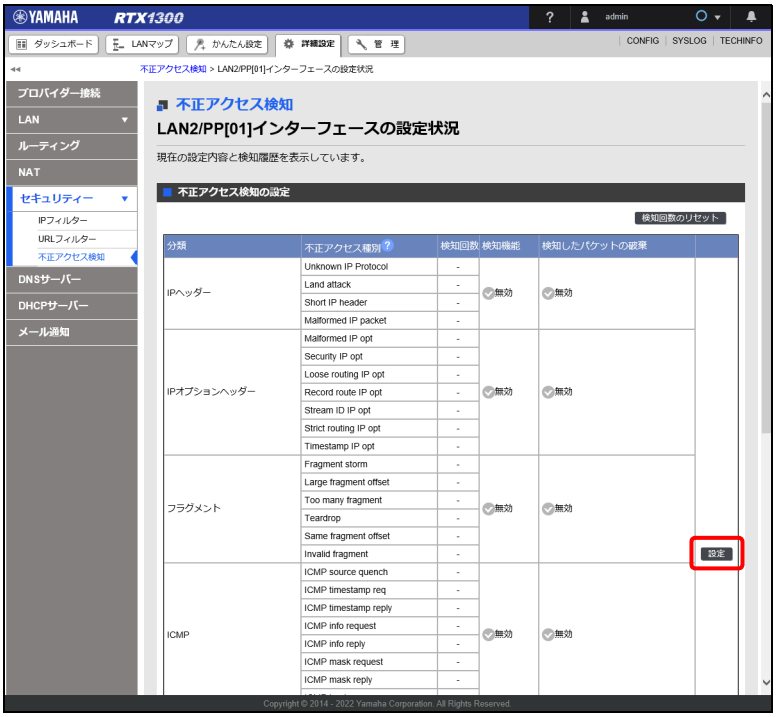
1.「詳細設定」タブ ―「セキュリティー」―「不正アクセス検知」を順に選択する。
「不正アクセス検知」画面が表示されます。

2.「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



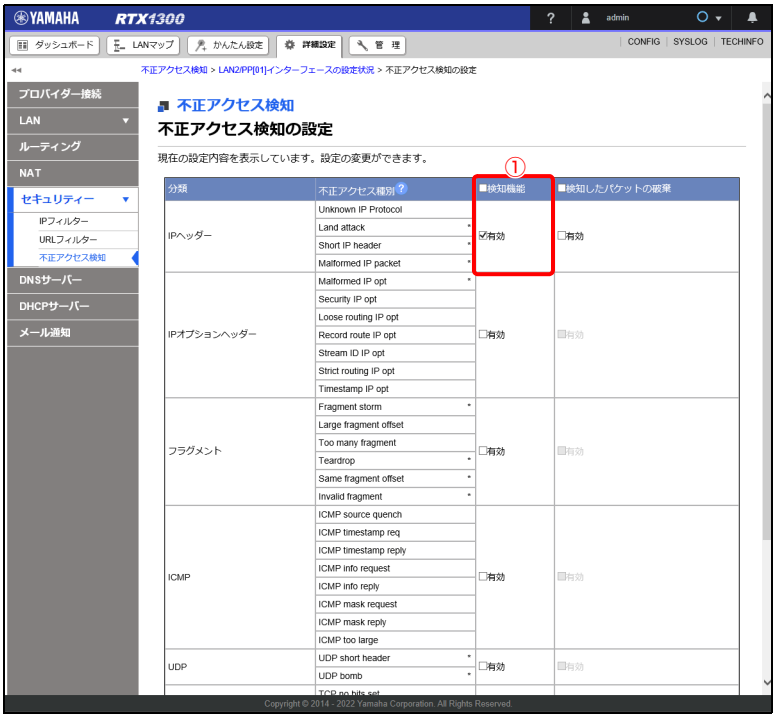
「LAN2/PP[01] インターフェースの設定状況」画面が表示されます。

3.「不正アクセス検知の設定」項目の「設定」ボタンをクリックする。



「不正アクセス検知の設定」画面が表示されます。

4. 不正アクセス検知の設定をする。



① **検知機能：**
IP ヘッダーの「検知機能」の「有効」にチェックを入れます。

メモ

・「不正アクセス種別」の列に「*」マークがある不正アクセス種別については、「検知機能」の「有効」にチェックが入っていれば、「検知したパケットの破棄」の「有効」にチェックが入っていなくてもパケットは破棄されます。
上記の例では、IP ヘッダーの「検知したパケットの破棄」列にチェックを入れていなくても IP ヘッダーの「検知機能」の「有効」にチェックを入れているため、「*」マークがある不正アクセス種別の「Land attack」「Short IP header」「Malformed IP packet」のパケットが破棄されます。
・「検知機能」で「有効」にチェックを入れている分類にのみ、「検知したパケットの破棄」の「有効」にチェックを入れることができます。
・「検知機能」列または「検知したパケットの破棄」列のヘッダーのチェックボックスにチェックを入れると、列全体のチェックボックスが選択されます。ヘッダーのチェックを外すと、全解除されます。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。

設定が反映され、「LAN2/PP[01] インターフェースの設定状況」画面が表示されます。

13.3.2 不正アクセス検知履歴の並び替え / 検索 / 削除をする

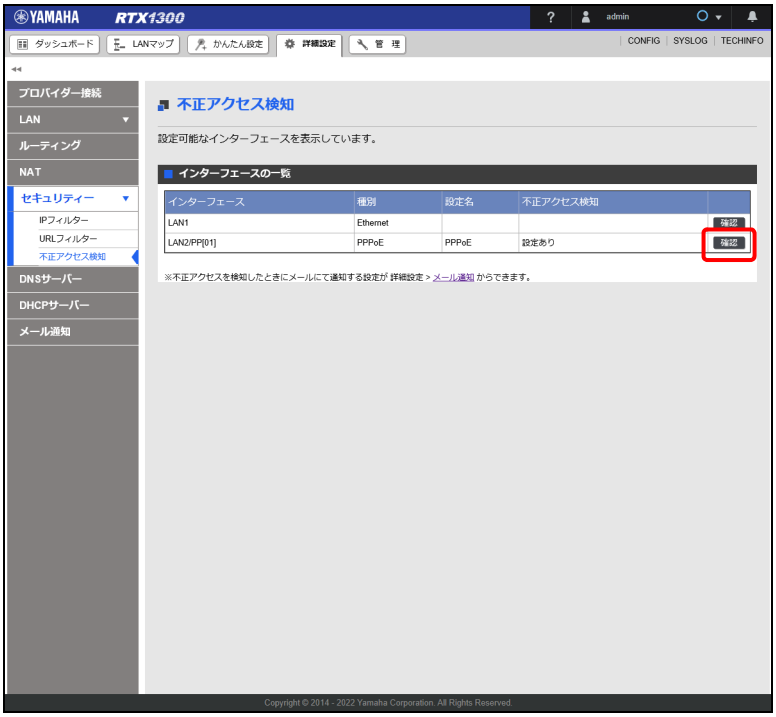
インターフェースで検知した不正アクセスの履歴（検知日時、不正アクセス種別、送信元 IP アドレス、宛先 IP アドレス）の並び替え、検索、削除を行います。
本項では「不正アクセス検知」で、「IP ヘッダー」の「検知機能」を有効に設定している状態（「13.3.1 不正アクセス検知を設定する」（237 ページ）の設定が完了している状態）から設定する前提で説明します。

メモ

- Web GUI で設定できない分類と検知方向の組み合わせを持つ不正アクセスは、履歴に表示されません。
- 履歴の最大保持数（工場出荷状態：50）は ip *interface* intrusion detection report コマンドで変更できます。
- Web GUI で設定できない分類と検知方向の組み合わせを持つ不正アクセスが検出されていた場合、Web GUI で表示される履歴の数は、ip *interface* intrusion detection report コマンドで設定した履歴の最大保持数よりも少なくなります。

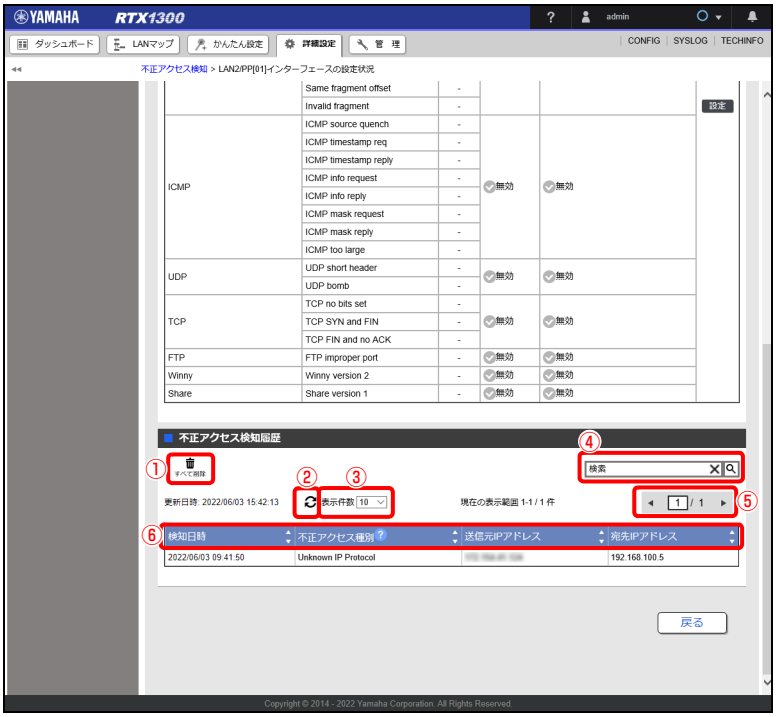
1. 「詳細設定」タブ ―「セキュリティー」―「不正アクセス検知」を順に選択する。
「不正アクセス検知」画面が表示されます。

2.「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



「LAN2/PP[01] インターフェースの設定状況」画面が表示されます。

3.「不正アクセス検知履歴」項目で選択したインターフェースの履歴を検索または削除する。



メモ

不正アクセス検知履歴が一件もない場合は、「検知履歴はありません。」と表示されます。

①「すべて削除」ボタン：
ボタンをクリックすると確認ダイアログが開き、続けて「実行」ボタンをクリックすると検知履歴がすべて削除されます。
検知履歴の削除に伴い、不正アクセス検知回数もリセットされます。

②「🔄」ボタン：
最新の情報に更新されます。

③ 表示件数プルダウンメニュー：
一度に表示する履歴件数を選択できます。

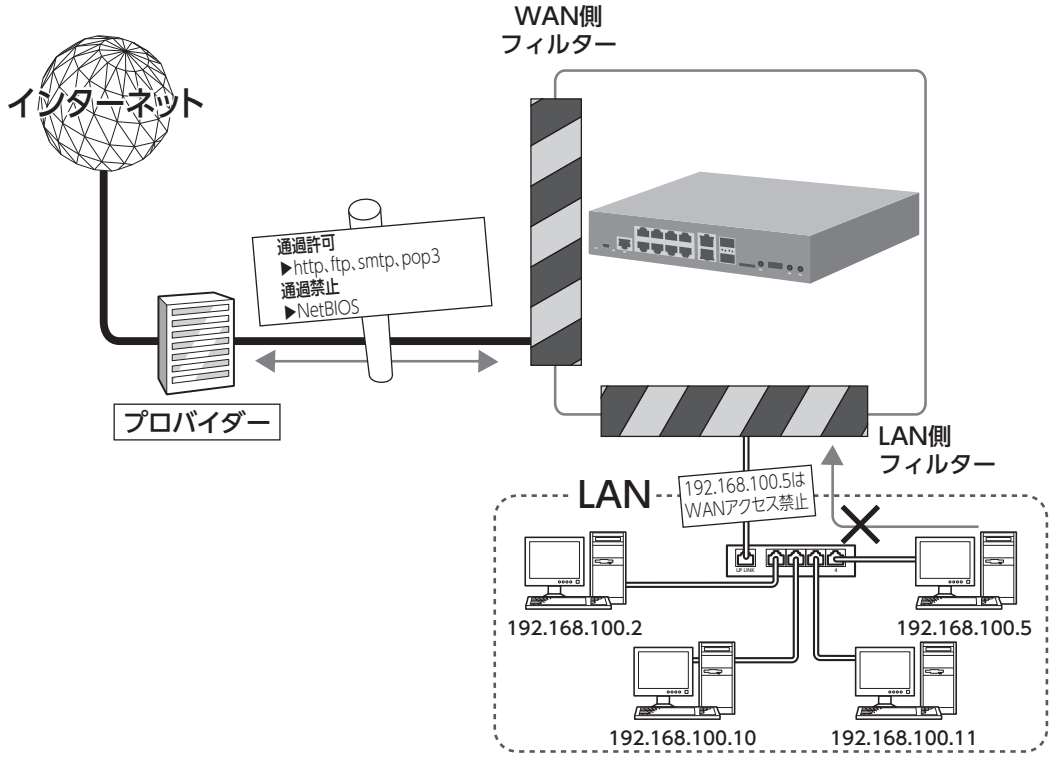
④ 検索ボックス：
任意のキーワードを入力し「🔍」ボタンをクリックすると検索を実行します。「✕」ボタンをクリックするとキーワードがクリアされます。

⑤「◀」「▶」ボタン：
履歴の数が表示件数を超えた場合、表示する履歴の範囲を変更できます。

⑥「⇕」ボタン：
項目ごとのボタンをクリックするとリストを並び替えることができます。再度クリックすると、昇順と降順が切り替わります。
- 「検知日時」：日時順にソートが行われます。初期画面では、検知日時順にソートされています。
- 「不正アクセス種別」：アルファベット順にソートが行われます。
- 「送信元 IP アドレス」：IP アドレス順にソートが行われます。
- 「宛先 IP アドレス」：IP アドレス順にソートが行われます。

13.4 IP フィルターを設定する

本製品では、接続先ごとに 128 個までのフィルターを設定できます。それぞれのフィルターでパケットの送信元や宛先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないよう設定できます。不正アクセスに使われやすいパケットや、正常な通信では発生しない作為的なパケットをルーター通過時に破棄するように設定することで、不正なパケットが LAN 内に入ることを防ぐことができます。



13.4.1 本製品のフィルターの特徴

静的フィルターと動的フィルター

本製品で設定できるフィルターには、次の 2 種類があります。各々の利点を理解し、それぞれのフィルターを併用することをおすすめします。

- 静的フィルター：一度設定すると、データや通信の有無にかかわらず常に有効になります。
- 動的フィルター：通信状態を監視しながら、必要に応じてフィルターが有効になります。例えば「通常はインターネットから LAN への通信はすべて禁止にしておき、LAN 側から FTP の通信が発生したときに、インターネット側からはその応答だけ通過を許可する」といった設定ができます。

プロバイダー接続時のフィルター設定

「かんたん設定」からプロバイダー接続の設定を行った場合は、「IP フィルターの設定」画面（33 ページ）で選択した内容に応じて基本的なフィルターが自動的に適用されます。この基本的なフィルターに加え、必要に応じてフィルターを追加することができます。

メモ

コマンドコンソール画面からプロバイダー接続の設定を行った場合は、フィルターは何も登録されていない状態になります。

フィルター番号

本製品に設定できるフィルター番号は 1 ～ 21474836 ですが、Web GUI から自動的にフィルターが適用される際に不整合が生じないように、Web GUI では用途に応じて所定の番号範囲が予約されています。以下に Web GUI で予約されているフィルター番号を示します。コマンドコンソール画面からフィルターを追加していて、そのフィルターの番号がここに挙げられた番号と重複している場合は、Web GUI で設定変更するとフィルターの設定が意図せず上書きされることがあることにご注意ください。

使用用途	フィルター番号
LAN/Mobile(WAN) インターフェース用	100000 ～ 199999
PP インターフェース用	200000 ～ 299999
トンネルインターフェース用	400000 ～ 499999
フィルター型ルーティング用	500000 ～ 599999
VLAN 間フィルター用	600000 ～ 699999
タグ VLAN インターフェース	1000000 ～ 1999999

注意

設定を間違えるとインターネットからのアクセスに対して無防備になってしまうことがあるため、フィルターの設定変更は機能を十分にご理解のうえ、慎重に行ってください。

メモ

フィルターを多く適用すると処理が複雑になり、インターネットへのアクセス速度が遅くなる場合があります。

13.4.2 フィルター設定の基本

フィルターを設定するときは、以下の考え方を基本にすることをおすすめします。

LAN 側からインターネット側へのアクセス（出力方向）は原則許可し、必要に応じて禁止する

LAN 側からインターネット側へのアクセスを厳しく規制すると非常に使いにくいものになり、管理や設定変更に手間がかかります。原則自由とした上で、問題があればその部分だけ制限します。

インターネット側から LAN 側へのアクセス（入力方向）は原則禁止し、必要に応じて許可する
インターネット側から LAN 側へのアクセスは、原則禁止して外部からのアクセスを防ぎます。Web サーバーの公開など、必要がある場合にのみ、最低限のアクセスだけを許可します。

注意
インターネット側からのアクセスとは、インターネット側から開始する通信のことを指します。

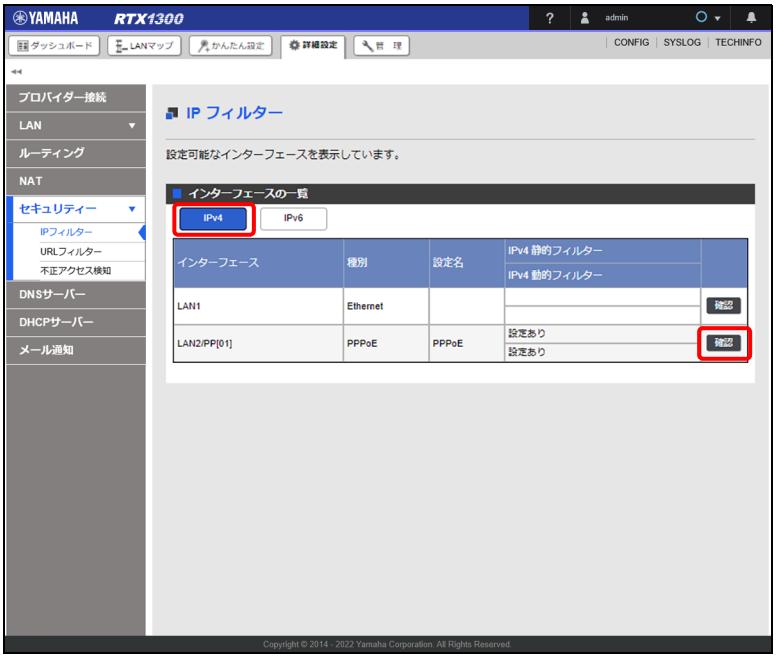
13.4.3 PING を許可する相手を限定する

静的フィルターを設定して、遠隔の特定の端末からの PING を許可する設定をします。固定の IPv4 アドレスが設定されている端末からの PING を許可する場合を例に説明します。
本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

重要
フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルで本製品に接続し、シリアルコンソール画面からフィルターの設定を修正するか、本製品の設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

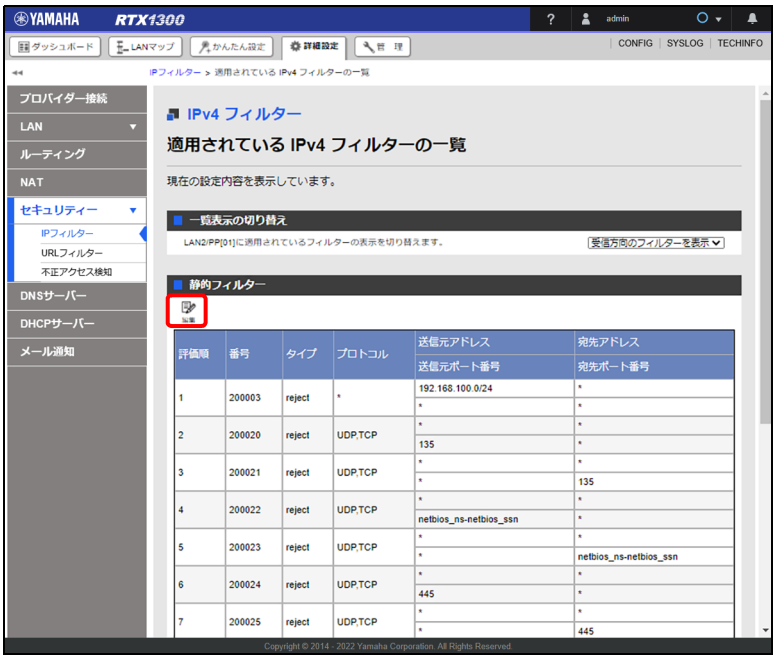
設定例
PING を許可する外部端末の IP アドレス：203.0.113.2

1. **「詳細設定」タブ ―「セキュリティー」―「IP フィルター」を順に選択する。**
   「IP フィルター」画面が表示されます。
2. **「IPv4」タブを選択し、「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。**



「適用されている IPv4 フィルターの一覧」画面が表示されます。

3.「静的フィルター」項目の「 編集 」ボタンをクリックする。



「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

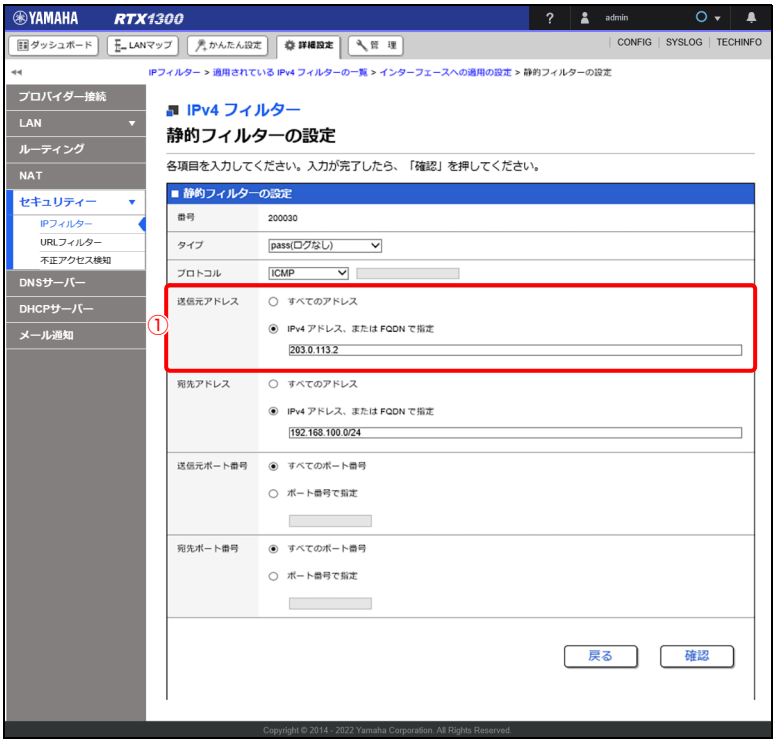
4.「適用フィルター」項目でプロトコルが「ICMP」のフィルターの「設定」ボタンをクリックする。

「静的フィルターの設定」画面が表示されます。

メモ

「ICMP」のフィルターがない場合は、「静的フィルター」項目の「 新規 」ボタンをクリックして ICMP プロトコルに対する IP フィルターを追加してください。新規に追加した「ICMP」フィルターは、チェックボックスにチェックを入れてから「末尾に追加」ボタンをクリックし、「静的フィルター」項目から「適用フィルター」項目へ移動させる必要があります。

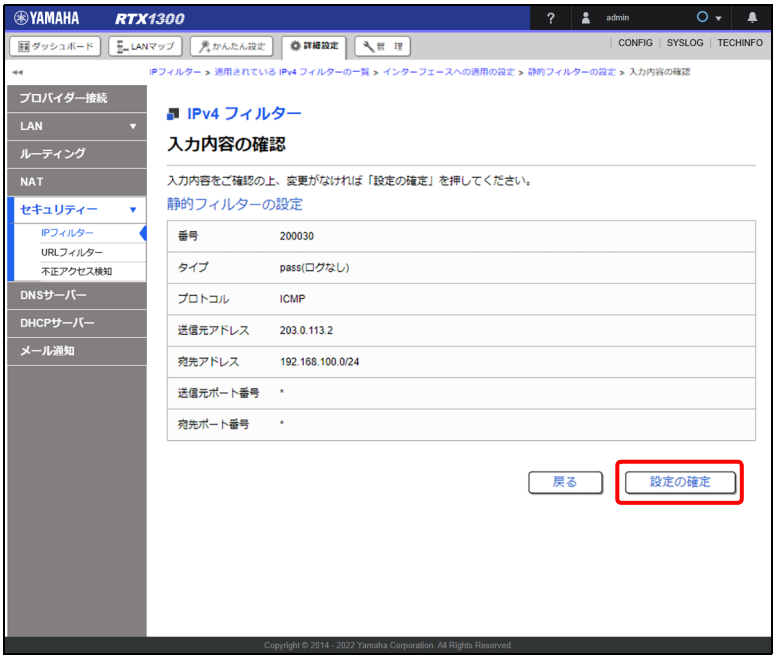
5. **静的フィルターを設定する。**



① **送信元アドレス：**
「203.0.113.2」を入力します。

6. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

13.4.4 遠隔からの PING をすべて破棄する

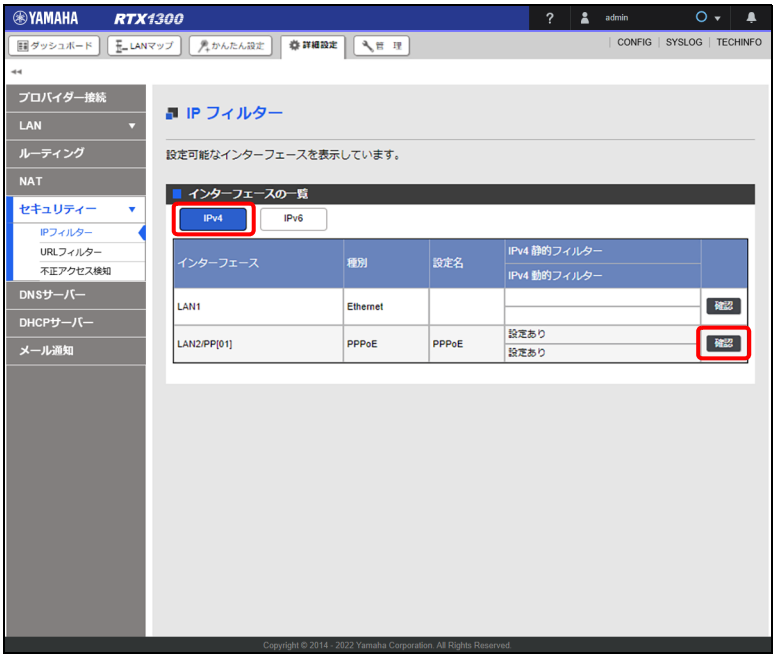
静的フィルターを設定して、インターネット側から来た PING をすべて破棄します。
本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

重要

フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルで本製品に接続し、シリアルコンソール画面からフィルターの設定を修正するか、本製品の設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

1. 「詳細設定」タブ―「セキュリティー」―「IP フィルター」を順に選択する。
「IP フィルター」画面が表示されます。

2.「IPv4」タブを選択し、「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



「適用されている IPv4 フィルターの一覧」画面が表示されます。

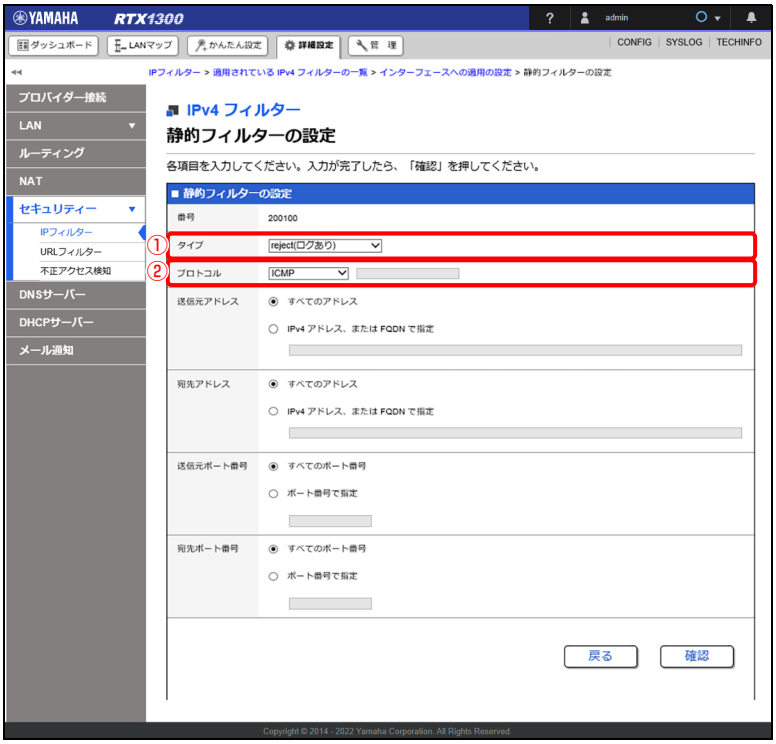
3.「静的フィルター」項目の「 」ボタンをクリックする。

「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

4.「静的フィルター」項目の「新規」ボタンをクリックする。

「静的フィルターの設定」画面が表示されます。

5. 静的フィルターを設定する。



① **タイプ**：
「reject（ログあり）」を選択します。

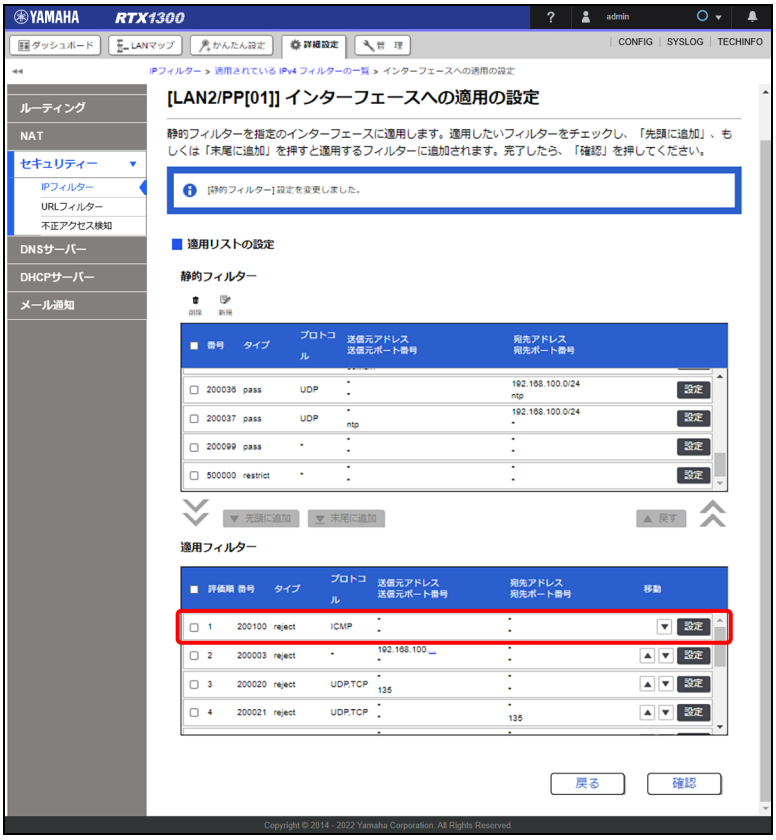
② **プロトコル**：
「ICMP」を選択します。

6. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

7. 内容を確認し、「設定の確定」ボタンをクリックする。

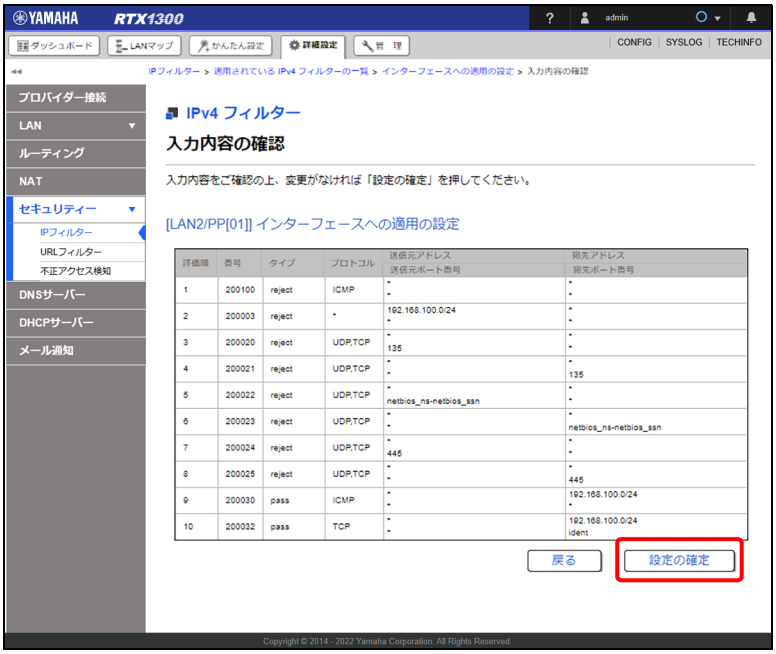
設定が反映され、「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

8. 「静的フィルター」項目のチェックボックスにチェックを入れてから「先頭に追加」ボタンをクリックし、作成したフィルター設定を「適用フィルター」項目の先頭に移動させる。



9.「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

10.内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

13.4.5 特定の端末だけ Web アクセスを許可する

動的フィルターを設定して、LAN 内の特定の端末だけ、外部の Web サーバーへのアクセスを許可します。
本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

重要

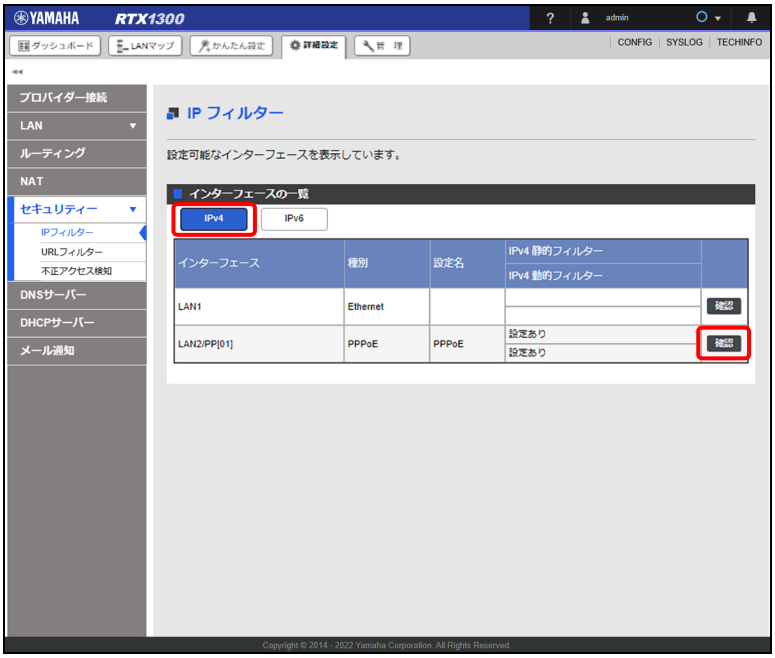
フィルターの設定を誤ると Web GUI へのアクセスもできなくなることがあります。Web GUI へのアクセスができなくなった場合は、シリアルケーブルで本製品に接続し、シリアルコンソール画面からフィルターの設定を修正するか、本製品の設定を工場出荷状態に戻す必要があります。フィルターの設定は慎重に行ってください。

設定例

外部の Web サーバーへのアクセスを許可する端末の IP アドレス：192.168.100.2

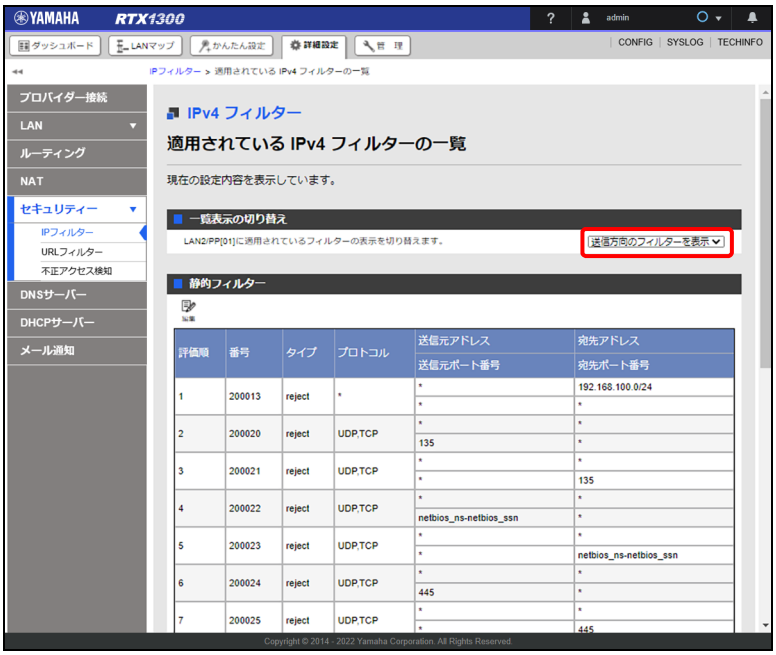
1.「詳細設定」タブ ―「セキュリティー」―「IP フィルター」を順に選択する。
「IP フィルター」画面が表示されます。

2. 「IPv4」タブを選択し、「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。

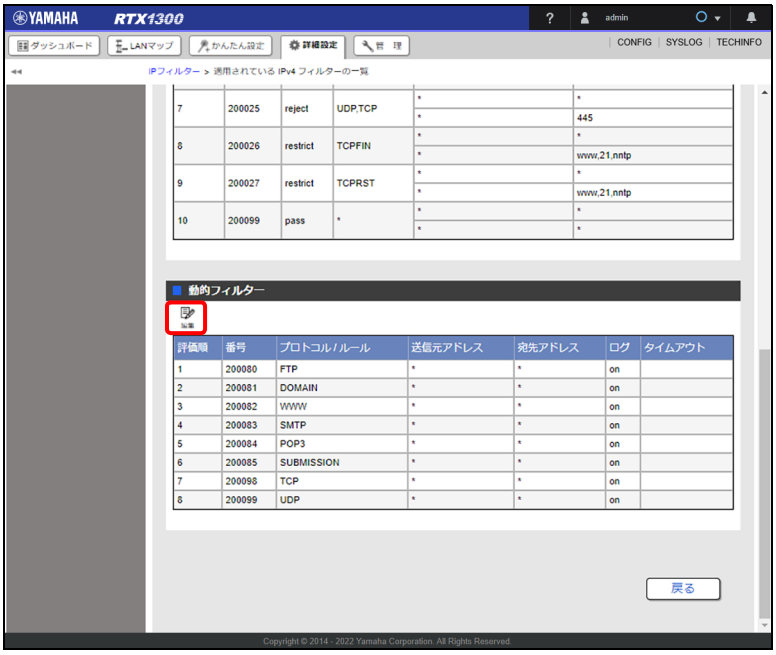


「適用されている IPv4 フィルターの一覧」画面が表示されます。

3. 「一覧表示の切り替え」項目のプルダウンメニューから「送信方向のフィルターを表示」を選択する。

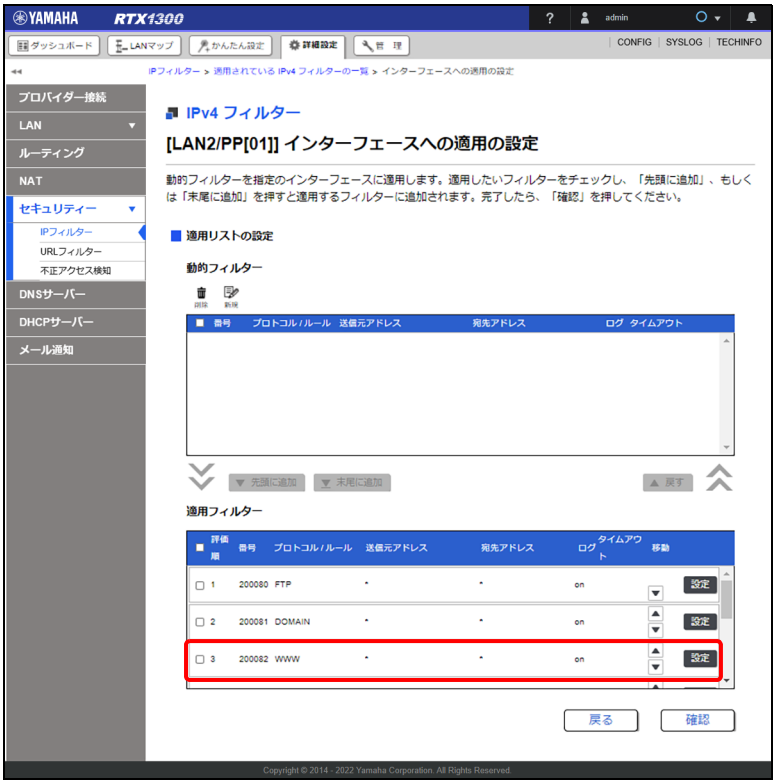


4.「動的フィルター」項目の「  」ボタンをクリックする。



「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

5.「適用フィルター」項目でプロトコルが「WWW」のフィルターの「設定」ボタンをクリックする。

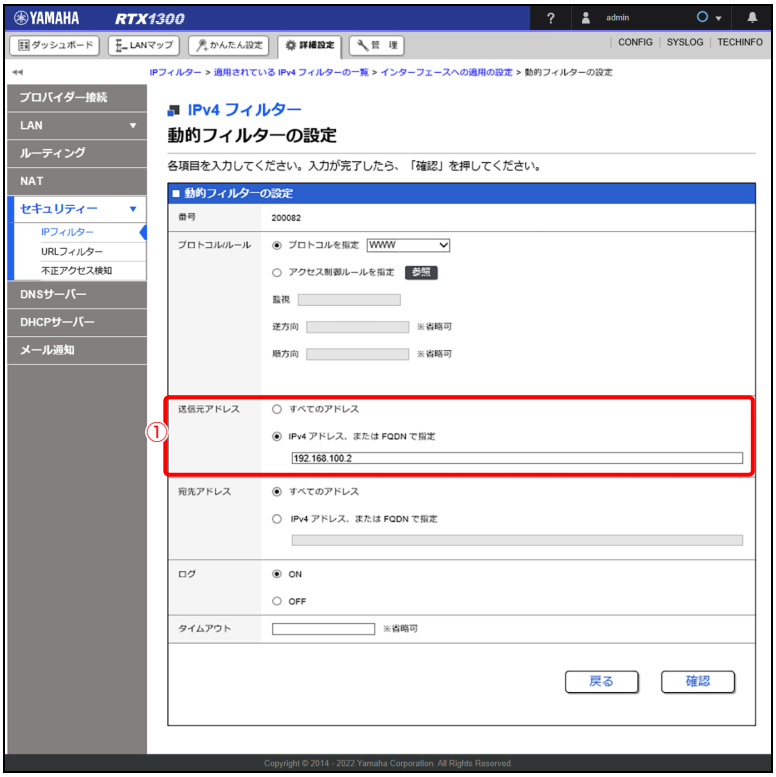


「動的フィルターの設定」画面が表示されます。

メモ

「WWW」のフィルターがない場合は、「動的フィルター」項目の「 新規 」ボタンをクリックして WWW プロトコルに対する IP フィルターを追加してください。新規に追加した「WWW」フィルターは、チェックボックスにチェックを入れてから「末尾に追加」ボタンをクリックし、「動的フィルター」項目から「適用フィルター」項目へ移動させる必要があります。

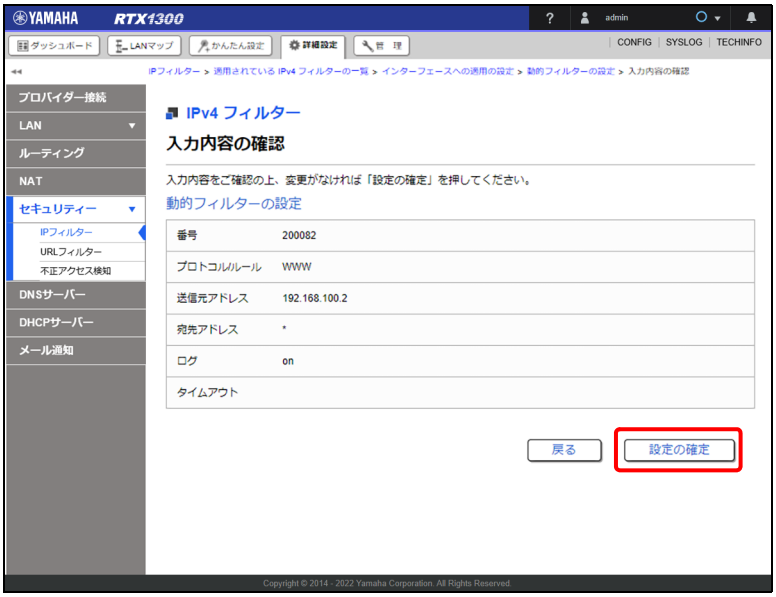
6. **動的フィルターを設定する。**



① **送信元アドレス：**
「192.168.100.2」を入力します。

7. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

8. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

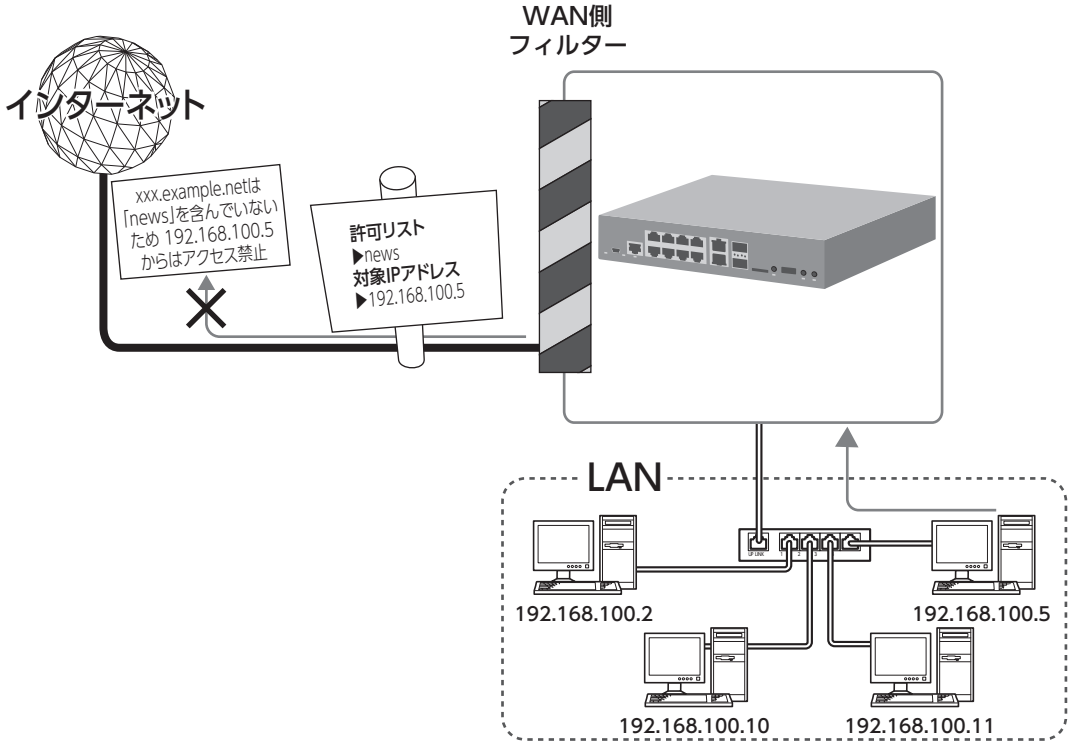
13.5 URL フィルターを設定する

HTTP/1.0 と HTTP/1.1 を対象に URL に含まれるキーワードをチェックし、フィルタリングします。
アクセスを禁止する拒否リストと、アクセスを許可する許可リストを設定できます。

注意

HTTP/2 によるアクセス、および、HTTPS によるアクセスをフィルタリングすることはできません。

下図は、192.168.100.5 の端末に対して、許可リストに「news」を設定した場合に、192.168.100.5 からは「news」を含むアドレスにのみアクセスできる例を示しています。



13.5.1 特定のキーワードを含む URL へのアクセスを禁止する

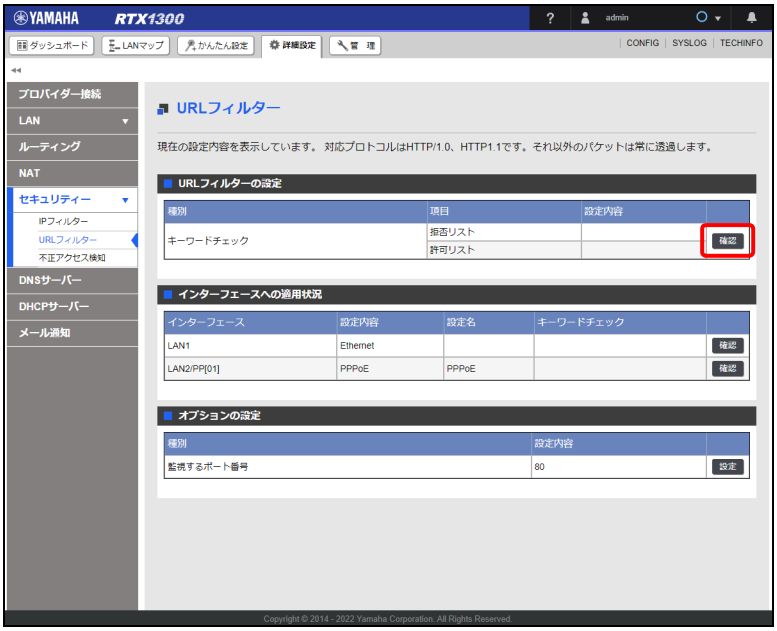
特定のキーワードを含む URL へのアクセスを禁止することで、業務に不適切な内容が掲載されている可能性のある URL やウイルスに感染しやすい URL（有害サイト）へのアクセスを抑止します。
本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

設定例

次のキーワードが含まれる URL へのアクセスを禁止する：「adult」「porn」「sex」
対象端末：全端末

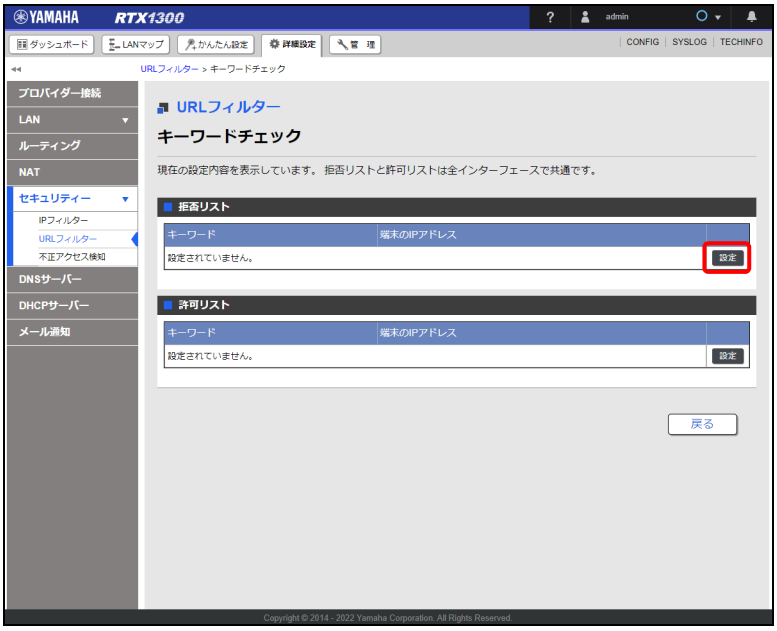
1. **「詳細設定」タブ ―「セキュリティー」―「URL フィルター」を順に選択する。**
   「URL フィルター」画面が表示されます。

2.「URL フィルターの設定」項目の「キーワードチェック」の「確認」ボタンをクリックする。



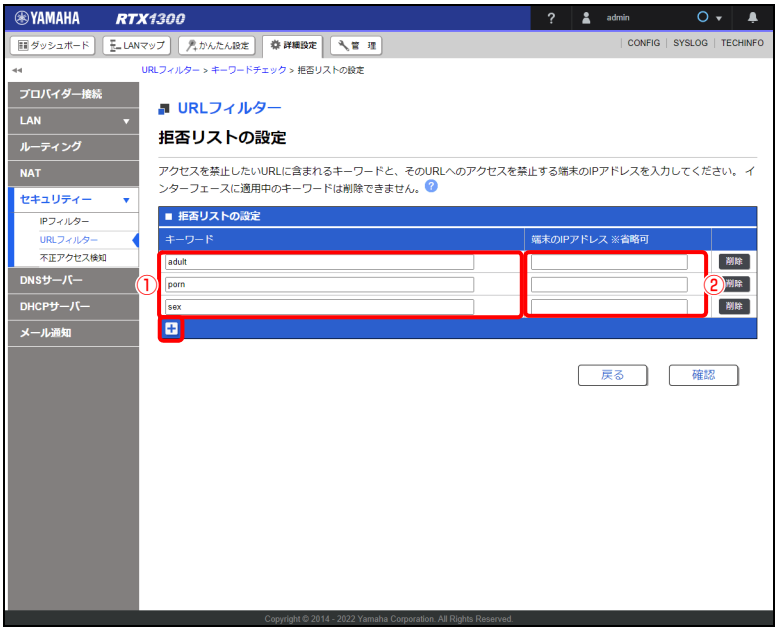
「キーワードチェック」画面が表示されます。

3.「拒否リスト」項目の「設定」ボタンをクリックする。



「拒否リストの設定」画面が表示されます。

4. 拒否リストの「キーワード」と「端末の IP アドレス」を設定する。



① **キーワード：**
「adult」「porn」「sex」を入力します。
キーワードを追加する場合は、入力欄下部の「 ＋ 」ボタンを押してください。キーワードを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

メモ

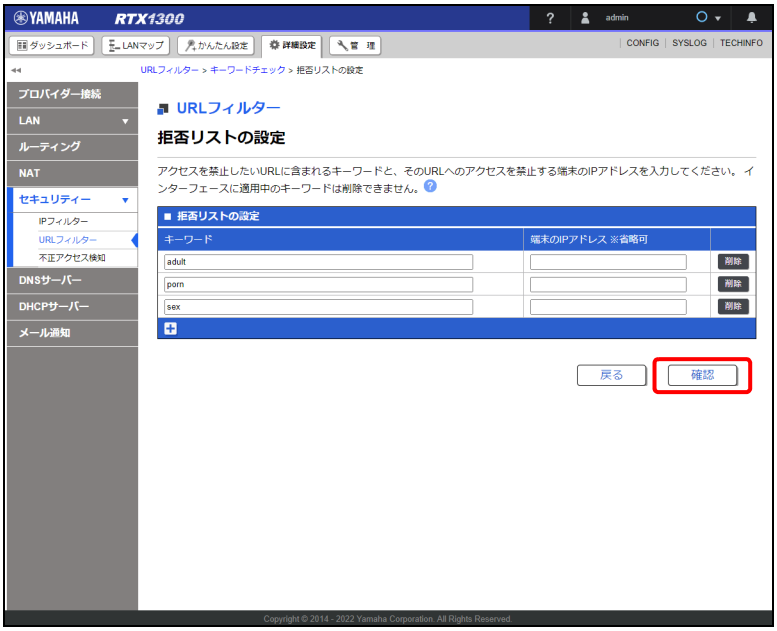
「*」を入力した場合はすべての URL を示します。

② **端末の IP アドレス：**
空欄のままか「*」を入力します。

メモ

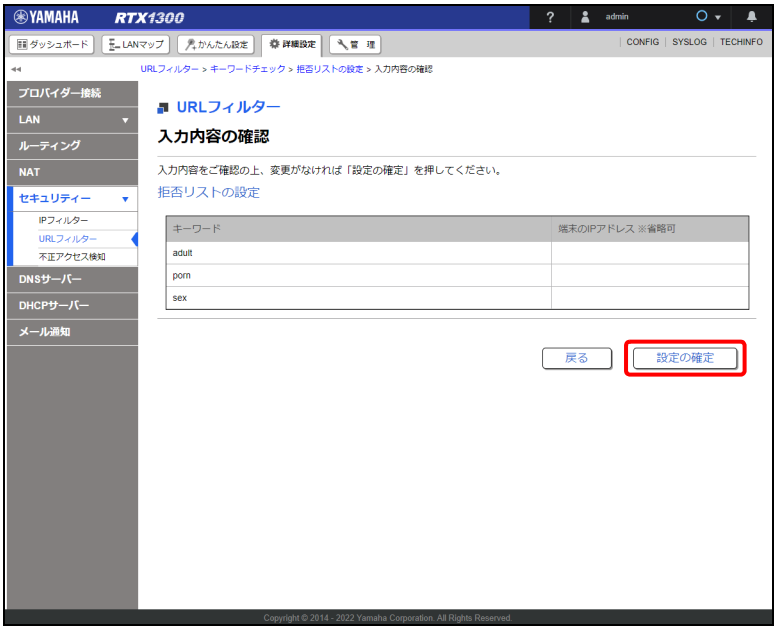
- 指定したキーワードを含む URL へのアクセスを禁止する端末の IP アドレスを入力します。
- 空欄のままか「*」を入力した場合、すべての IP アドレスが対象になります。
- 端末指定：「ネットワークアドレス / サブネットマスク」で端末を指定します。
  例：192.168.100.0/24
- 範囲指定：「-」を使って IP アドレスの範囲を指定します。
  例：192.168.100.2-192.168.100.10
  192.168.100.2-
  -192.168.100.10
- 複数設定：IP アドレスを「,」で区切ります。
  例：192.168.100.2,192.168.100.128/25,192.168.100.6-192.168.100.10

5. 「確認」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。

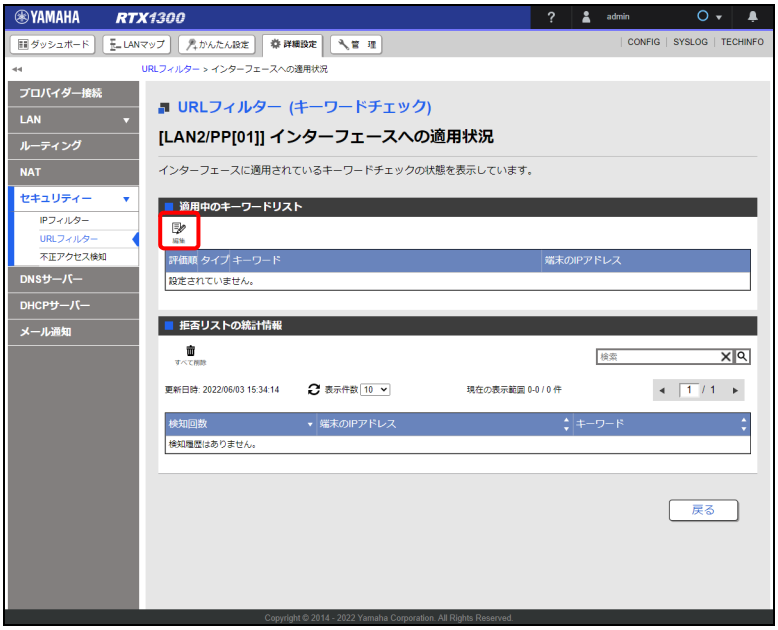


設定が反映され、「キーワードチェック」画面が表示されます。「戻る」ボタンをクリックすると、「URL フィルター」画面が表示されます。

7. 「インターフェースへの適用状況」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。

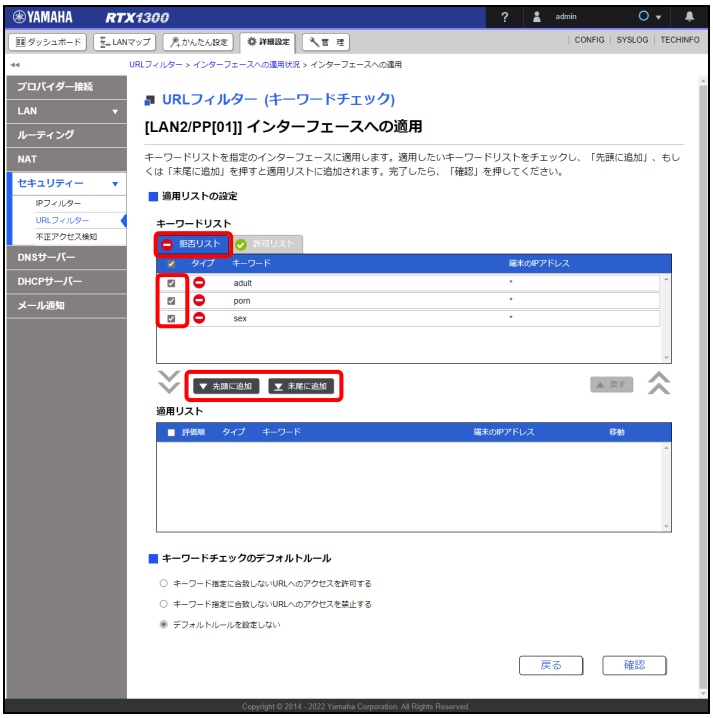
「[LAN2/PP[01]] インターフェースへの適用状況」画面が表示されます。

8. 「適用中のキーワードリスト」項目の「 」ボタンをクリックする。

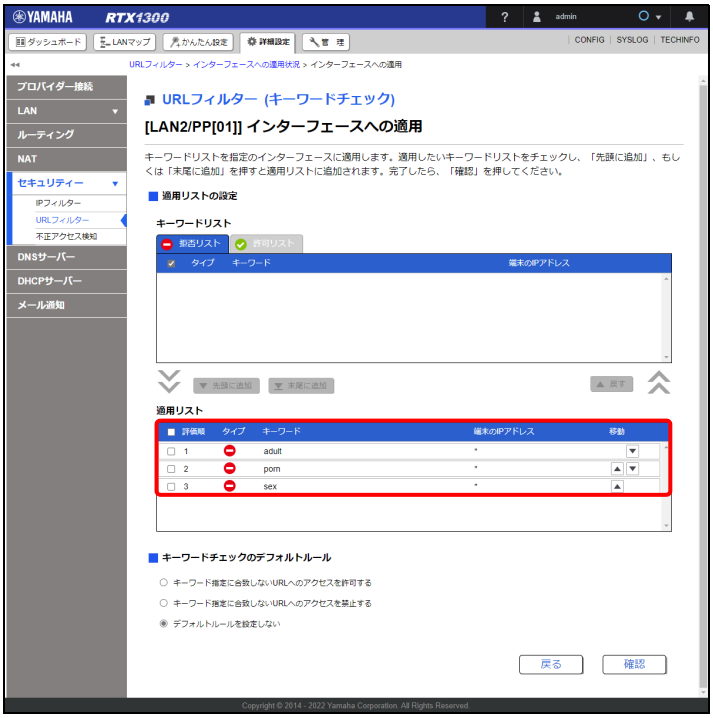


「[LAN2/PP[01]] インターフェースへの適用」画面が表示されます。

9. 「キーワードリスト」の「拒否リスト」タブから「適用リスト」に移動するキーワードをチェックし、「先頭に追加」ボタンまたは「末尾に追加」ボタンをクリックする。



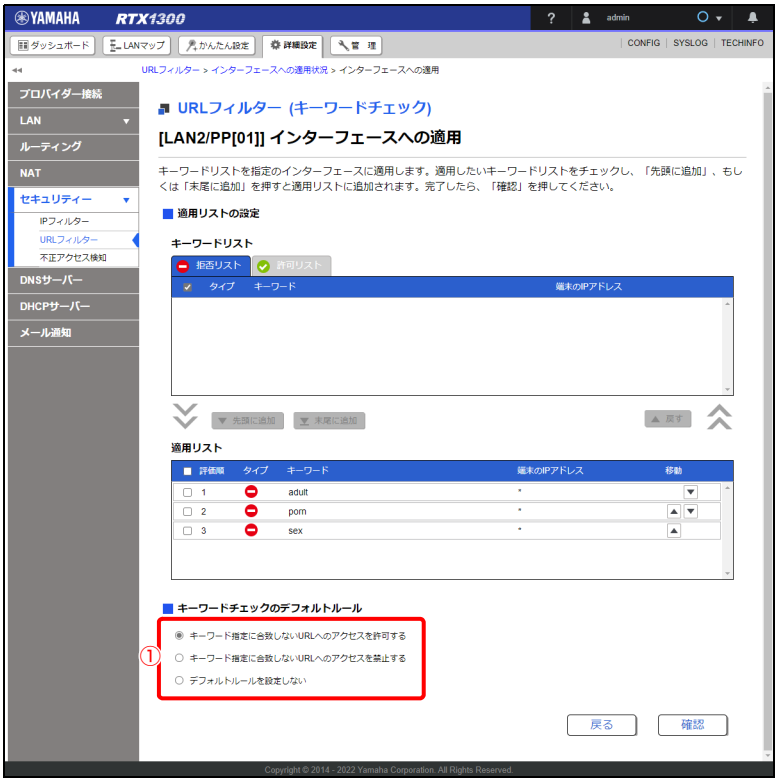
選択した「キーワードリスト（拒否リスト）」が「適用リスト」に移動します。



メモ

適用リストの評価順にしたがって URL のキーワードチェックが行われ、先に合致したルールが優先されます。

10.「キーワードチェックのデフォルトルール」を設定する。



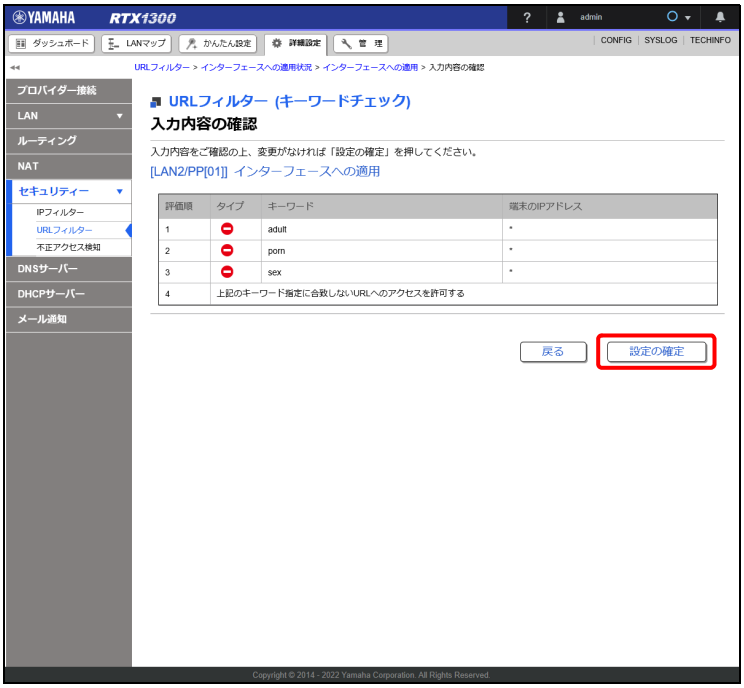
① **キーワードチェックのデフォルトルール：**
「キーワード指定に合致しない URL へのアクセスを許可する」を選択します。

メモ

・ デフォルトルールは拒否リストや許可リストに表示されません。
・ デフォルトルールは拒否リストや許可リストで、「キーワード」と「端末の IP アドレス」に「*」を指定したものと同等です。

11.**「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

12.内容を確認し、「設定の確定」ボタンをクリックする。



「[LAN2/PP[01]] インターフェースへの適用状況」画面が表示されます。

13.5.2 端末ごとにアクセスを許可する URL を変更する

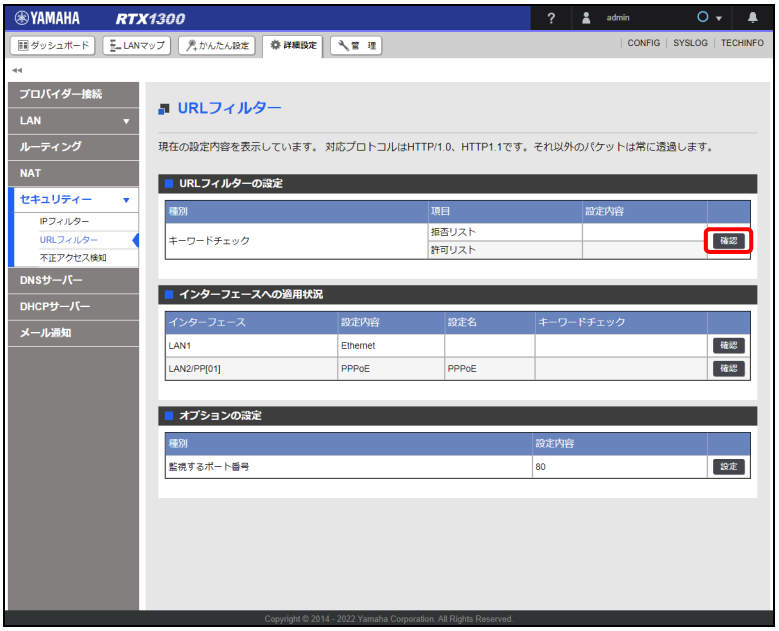
ユーザー（IP アドレス）ごとにアクセスを許可する URL（キーワード）を設定します。
本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

設定例

- 次のキーワードが含まれる URL へのアクセスを許可する：「news」
  対象端末：全端末
- 次のキーワードが含まれる URL へのアクセスを許可する：「netvolante.jp」
  対象端末：192.168.100.2 ～ 192.168.100.10 および 192.168.100.200（管理者）
- 次のキーワードが含まれる URL へのアクセスを許可する：「rtpro」
  対象端末：192.168.100.200（管理者）

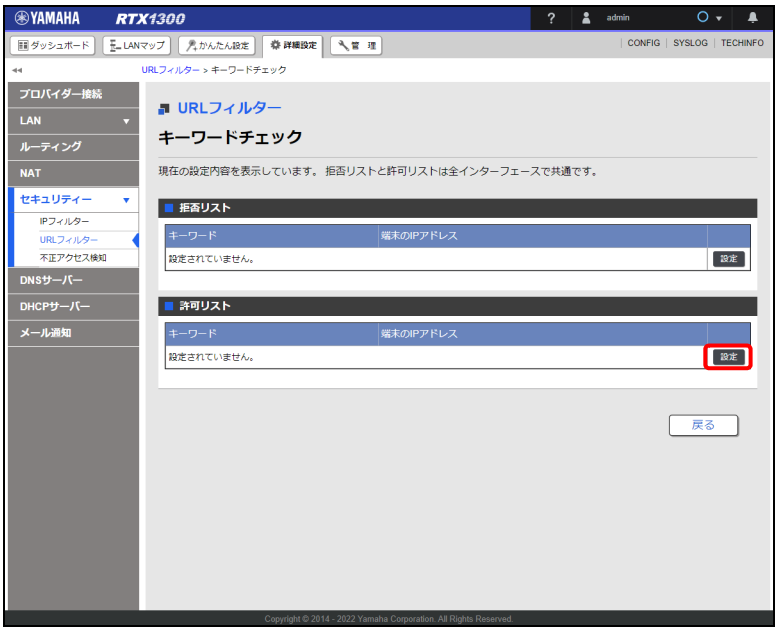
1. **「詳細設定」タブ ―「セキュリティー」―「URL フィルター」を順に選択する。**
   「URL フィルター」画面が表示されます。

2.「URL フィルターの設定」項目の「キーワードチェック」の「確認」ボタンをクリックする。



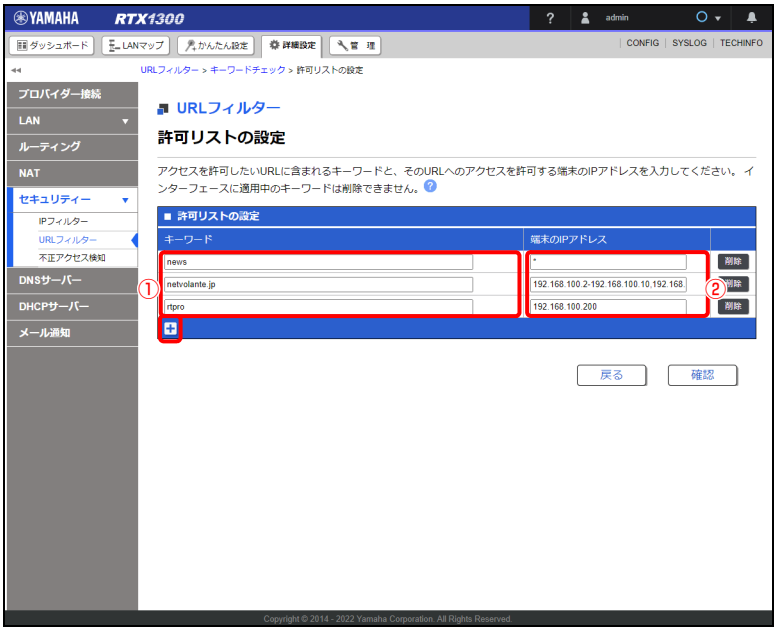
「キーワードチェック」画面が表示されます。

3.「許可リスト」項目の「設定」ボタンをクリックする。



「許可リストの設定」画面が表示されます。

4. 許可リストの「キーワード」と「端末の IP アドレス」を設定する。



① **キーワード：**
「news」「netvolante.jp」「rtpro」を入力します。
キーワードを追加する場合は、入力欄下部の「 ＋ 」ボタンを押してください。キーワードを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

メモ

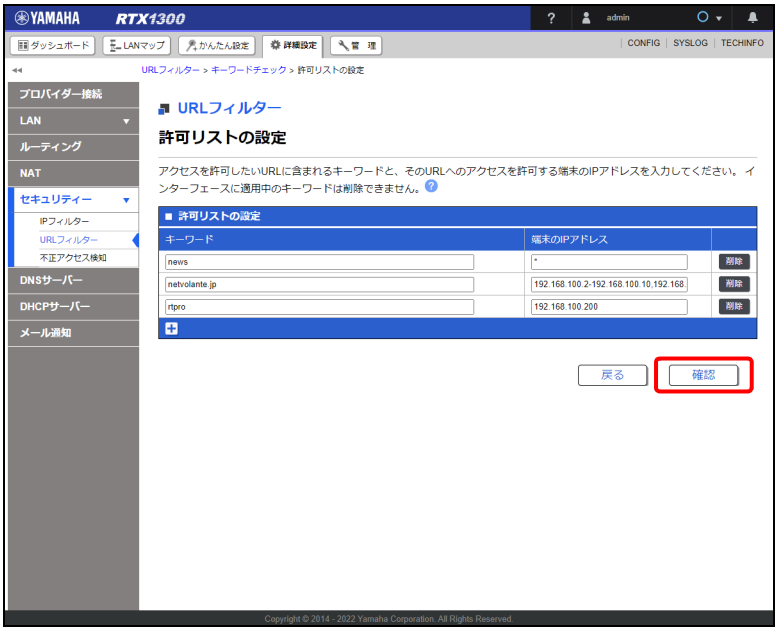
アクセスを許可する URL に含まれるキーワードを入力します。「*」を入力した場合はすべての URL を示します。

② **端末の IP アドレス：**
指定キーワードを含む URL に対して、アクセス可能な端末の IP アドレスを設定します。
「news」：*（すべての端末）
「netvolante.jp」：192.168.100.2-192.168.100.10,192.168.100.200
「rtpro」：192.168.100.200

メモ

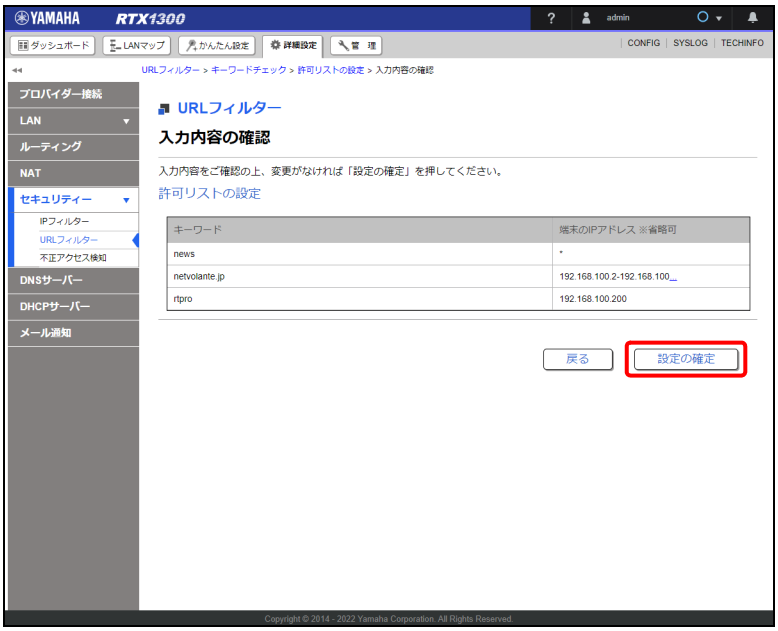
- 指定したキーワードを含む URL へのアクセスを許可する端末の IP アドレスを入力します。
- 端末指定：「ネットワークアドレス / サブネットマスク」で端末を指定します。
  例：192.168.100.0/24
- 範囲指定：「-」を使って IP アドレスの範囲を指定します。
  例：192.168.100.2-192.168.100.10
  192.168.100.2-
  -192.168.100.10
- 複数設定：IP アドレスを「,」で区切ります。
  例：192.168.100.2,192.168.100.128/25,192.168.100.6-192.168.100.10

5. 「確認」ボタンをクリックする。



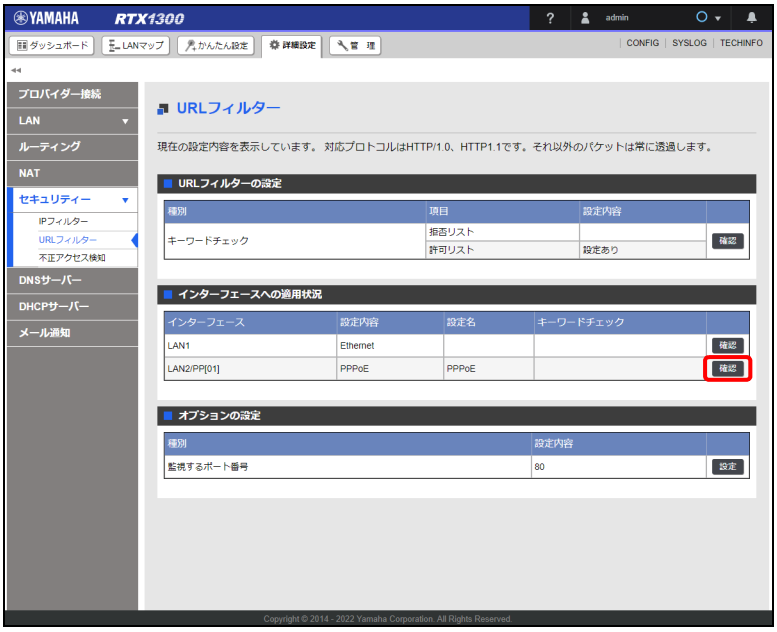
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



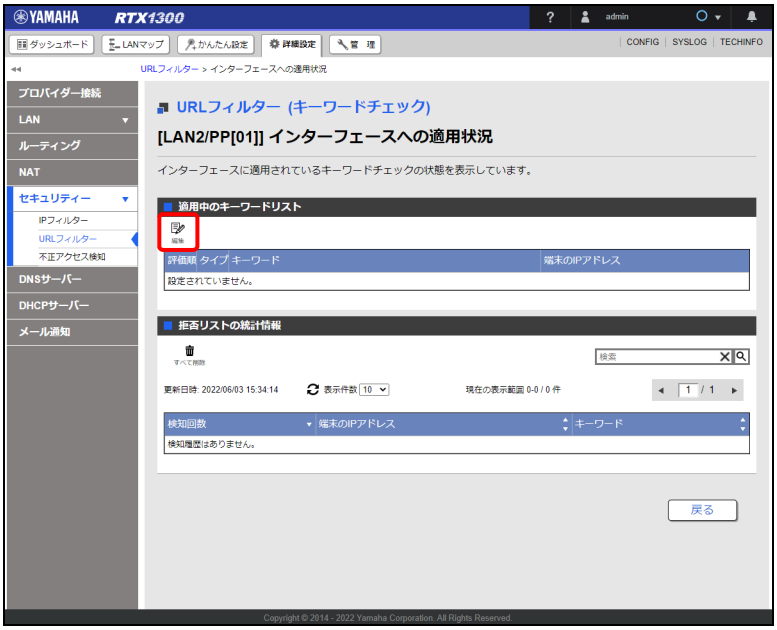
設定が反映され、「キーワードチェック」画面が表示されます。「戻る」ボタンをクリックすると、「URL フィルター」画面が表示されます。

7. 「インターフェースへの適用状況」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



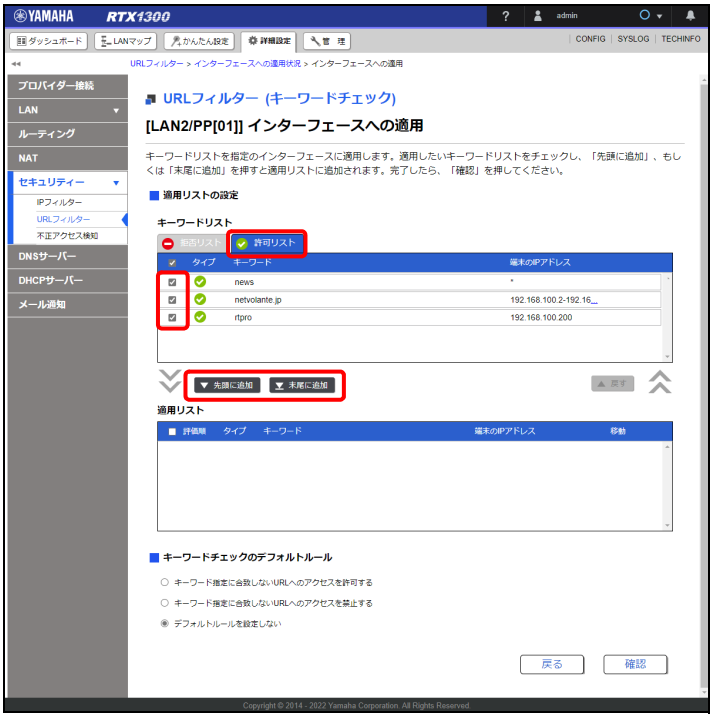
「[LAN2/PP[01]] インターフェースへの適用状況」画面が表示されます。

8. 「適用中のキーワードリスト」項目の「  」ボタンをクリックする。

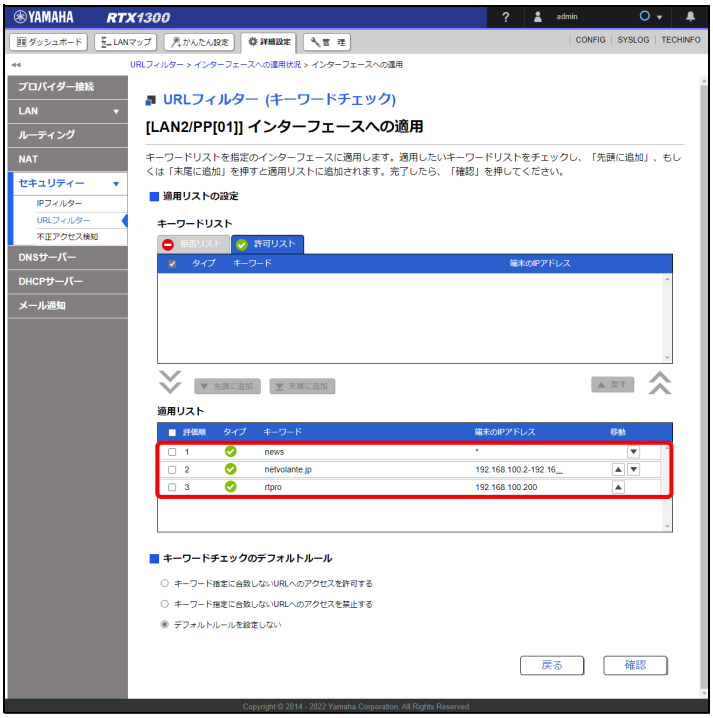


「[LAN2/PP[01]] インターフェースへの適用」画面が表示されます。

9. 「キーワードリスト」の「許可リスト」タブをクリックして表示を切り替え、「適用リスト」に移動するキーワードをチェックし、「先頭に追加」ボタンまたは「末尾に追加」ボタンをクリックする。



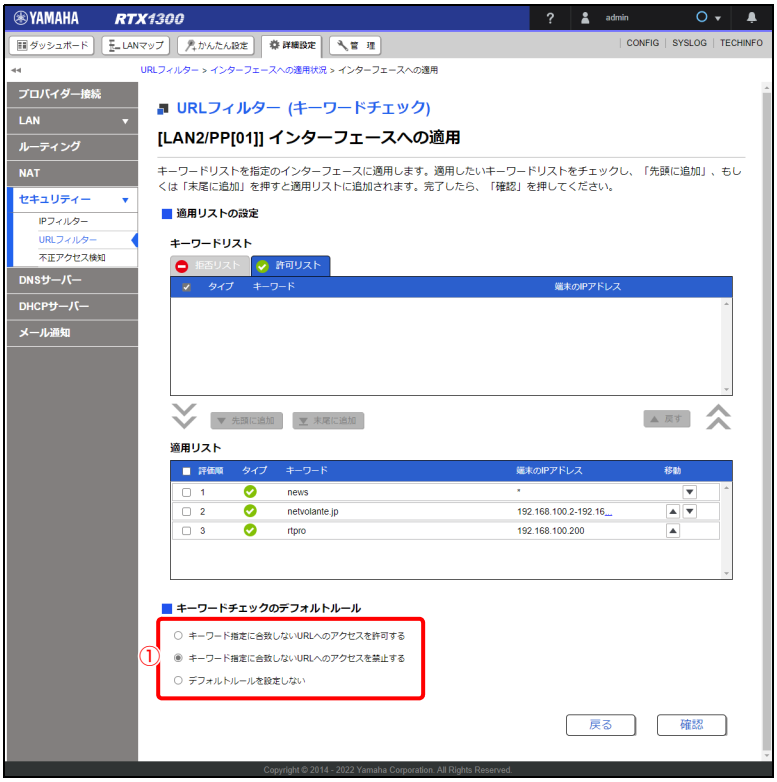
選択した「キーワードリスト（許可リスト）」が「適用リスト」に移動します。



メモ

適用リストの評価順にしたがって URL のキーワードチェックが行われ、先に合致したルールが優先されます。

10.「キーワードチェックのデフォルトルール」を設定する。



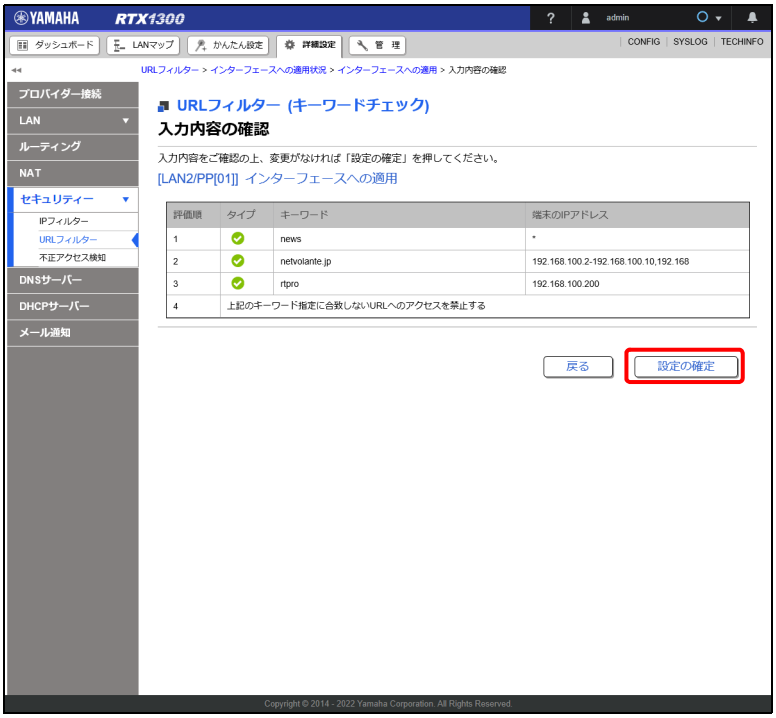
① **キーワードチェックのデフォルトルール：**
「キーワード指定に合致しない URL へのアクセスを禁止する」を選択します。

メモ

・ デフォルトルールは拒否リストや許可リストに表示されません。
・ デフォルトルールは拒否リストや許可リストで、「キーワード」と「端末の IP アドレス」に「*」を指定したものと同等です。

11.「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

12.内容を確認し、「設定の確定」ボタンをクリックする。



「LAN2/PP[01] インターフェースへの適用状況」画面が表示されます。

13.5.3 アクセスを禁止するキーワードの例外条件を設定する

アクセスを禁止するキーワードが含まれていても、例外的にアクセスを許可する URL の設定について説明します。

本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

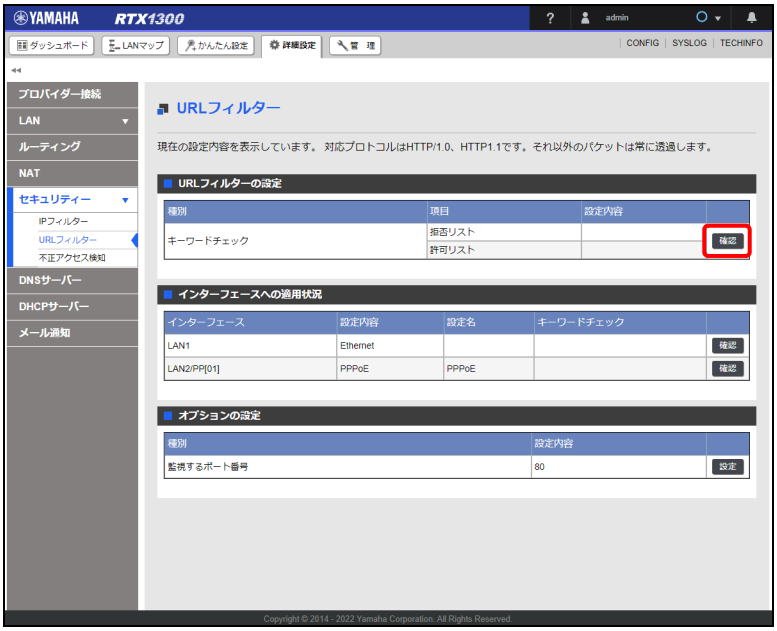
設定例

- 次のキーワードが含まれる URL へのアクセスを禁止する：「http://www.example.net/」
- 次のキーワードが含まれる URL へのアクセスを許可する：「http://www.example.net/example/」
- 禁止 URL 以外の URL へのアクセスは許可する。
- 対象端末：全端末

1.**「詳細設定」タブ ―「セキュリティー」―「URL フィルター」を順に選択する。**

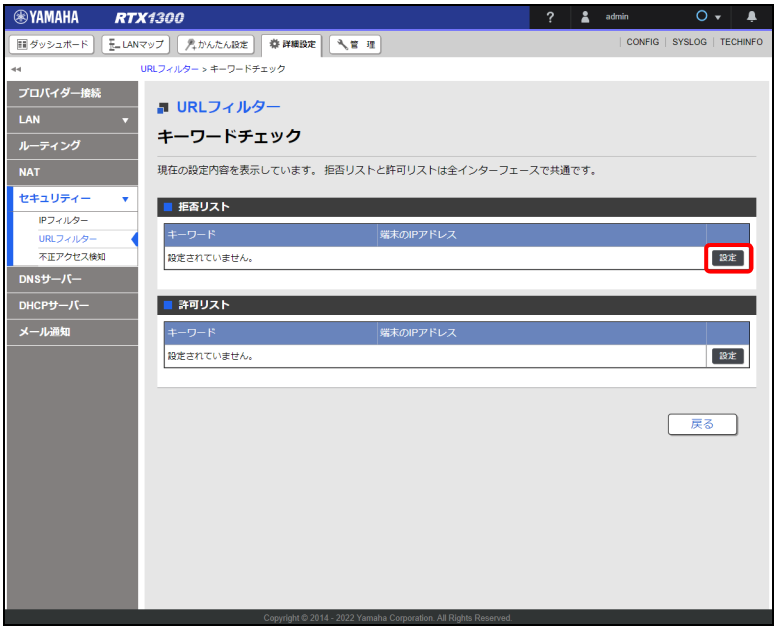
「URL フィルター」画面が表示されます。

2.「URL フィルターの設定」項目の「キーワードチェック」の「確認」ボタンをクリックする。



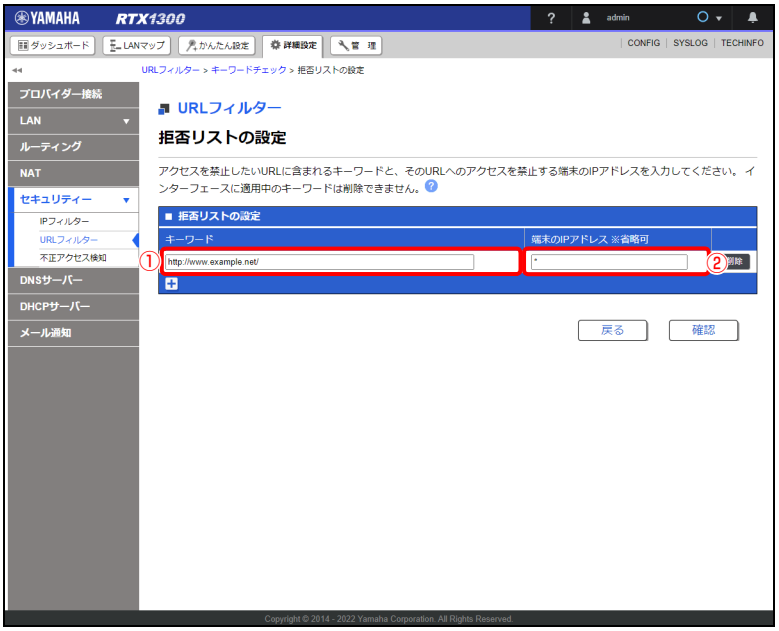
「キーワードチェック」画面が表示されます。

3.「拒否リスト」項目の「設定」ボタンをクリックする。



「拒否リストの設定」画面が表示されます。

4. 拒否リストの「キーワード」と「端末の IP アドレス」を設定する。



① **キーワード：**
「http://www.example.net/」を入力します。

メモ

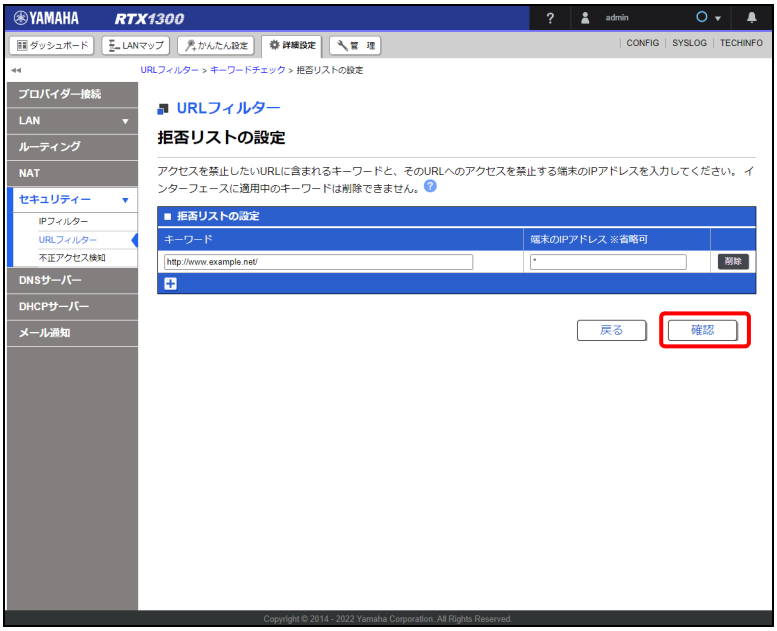
「*」を入力した場合はすべての URL を示します。

② **端末の IP アドレス：**
空欄のままか「*」を入力します。

メモ

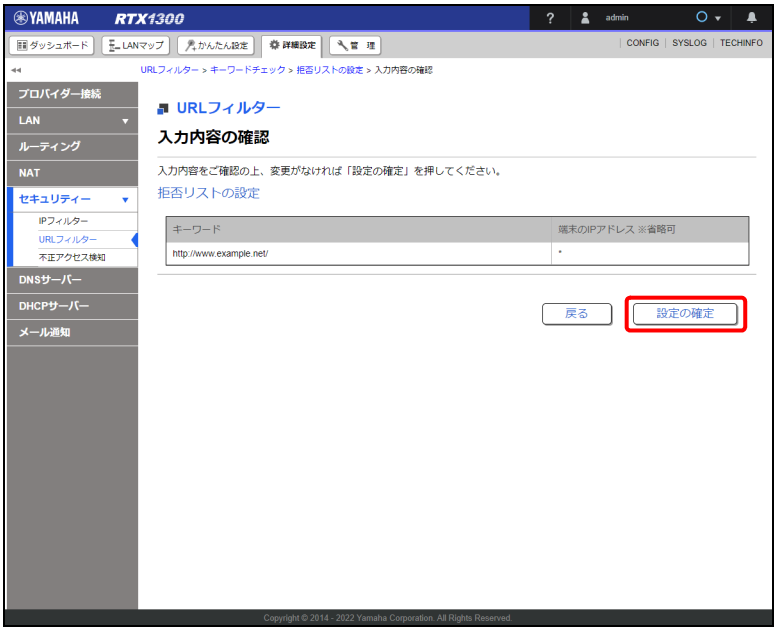
- 指定したキーワードを含む URL へのアクセスを禁止する端末の IP アドレスを入力します。
- 空欄のままか「*」を入力した場合、すべての IP アドレスが対象になります。
- 端末指定：「ネットワークアドレス / サブネットマスク」で端末を指定します。
  例：192.168.100.0/24
- 範囲指定：「-」を使って IP アドレスの範囲を指定します。
  例：192.168.100.2-192.168.100.10
  192.168.100.2-
  -192.168.100.10
- 複数設定：IP アドレスを「,」で区切ります。
  例：192.168.100.2,192.168.100.128/25,192.168.100.6-192.168.100.10

5. 「確認」ボタンをクリックする。



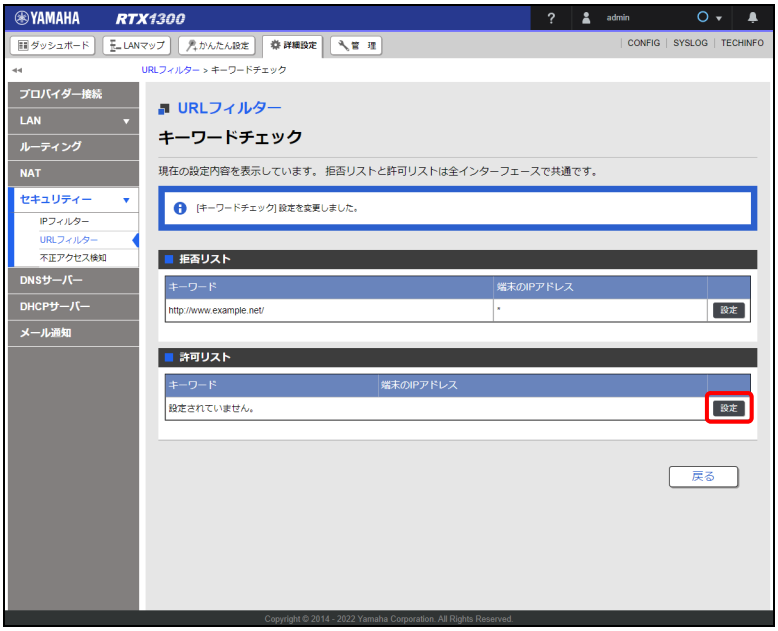
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



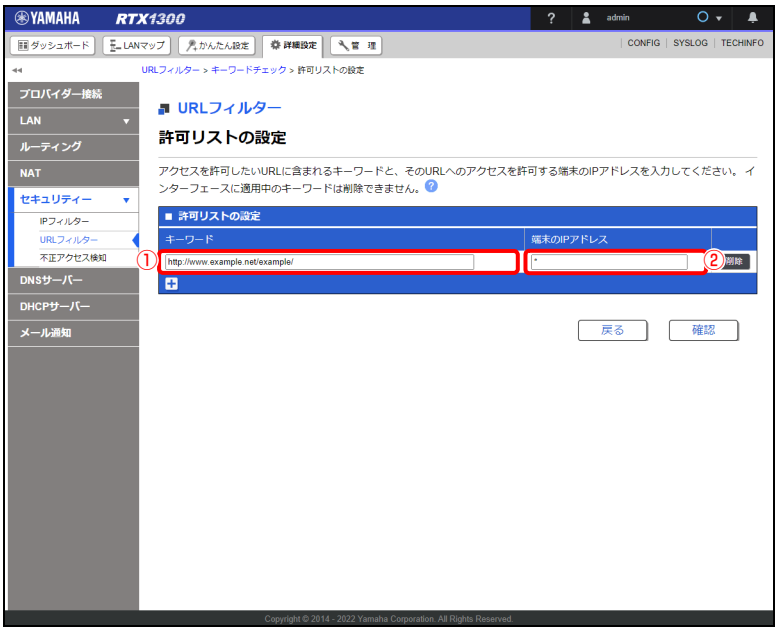
設定が反映され、「キーワードチェック」画面が表示されます。

7. 「許可リスト」項目の「設定」ボタンをクリックする。



「許可リストの設定」画面が表示されます。

8. 許可リストの「キーワード」と「端末の IP アドレス」を設定する。



① **キーワード：**
「http://www.example.net/example/」を入力します。

メモ

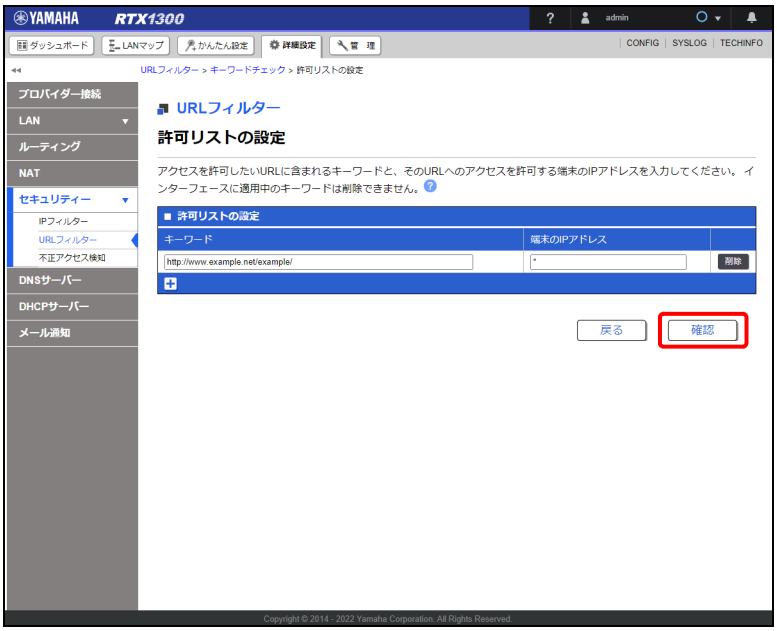
アクセスを許可する URL に含まれるキーワードを入力します。「*」を入力した場合はすべての URL を示します。

② **端末の IP アドレス：**
空欄のままか「*」を入力します。

メモ

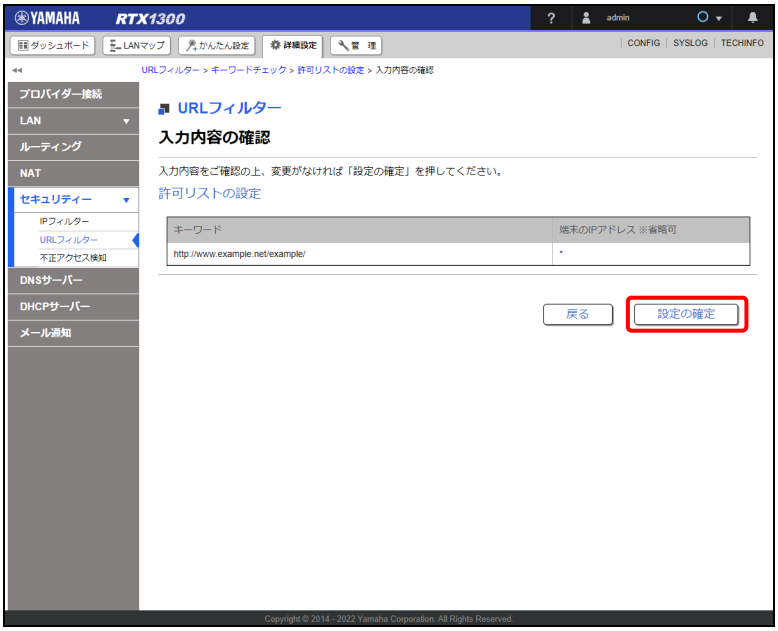
・ 指定したキーワードを含む URL へのアクセスを許可する端末の IP アドレスを入力します。
・ 空欄のままか「*」を入力した場合、すべての IP アドレスが対象になります。
・ 端末指定：「ネットワークアドレス / サブネットマスク」で端末を指定します。
　例：192.168.100.0/24
・ 範囲指定：「-」を使って IP アドレスの範囲を指定します。
　例：192.168.100.2-192.168.100.10
　　192.168.100.2-
　　-192.168.100.10
・ 複数設定：IP アドレスを「,」で区切ります。
　例：192.168.100.2,192.168.100.128/25,192.168.100.6-192.168.100.10

9. **「確認」ボタンをクリックする。**

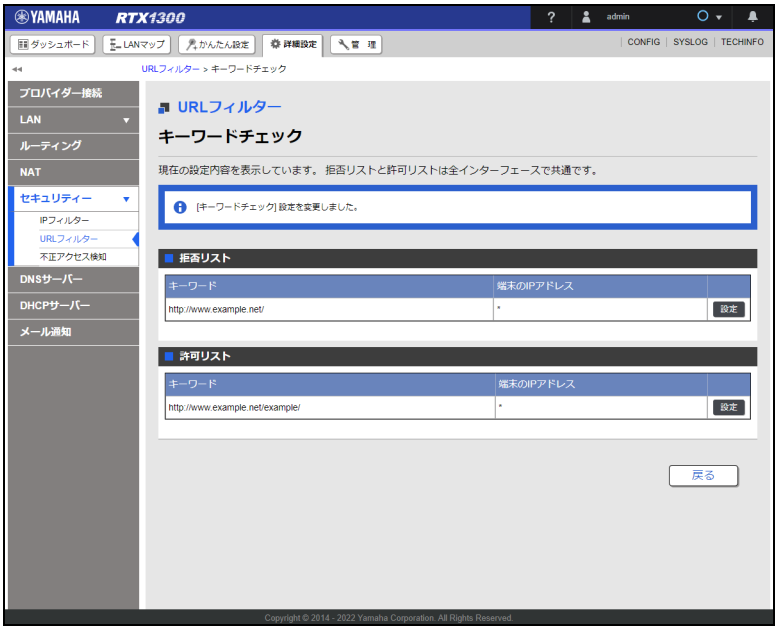


「入力内容の確認」画面が表示されます。

10.内容を確認し、「設定の確定」ボタンをクリックする。

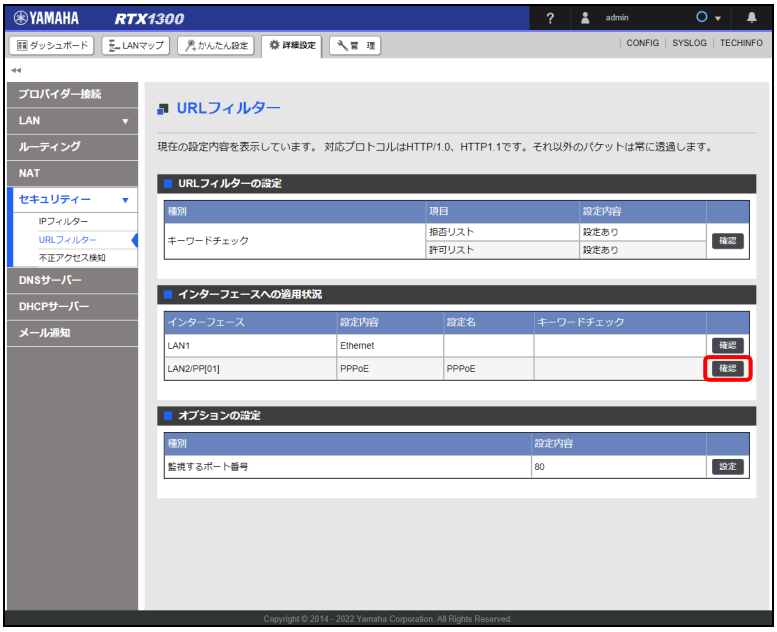


設定が反映され、「キーワードチェック」画面が表示されます。



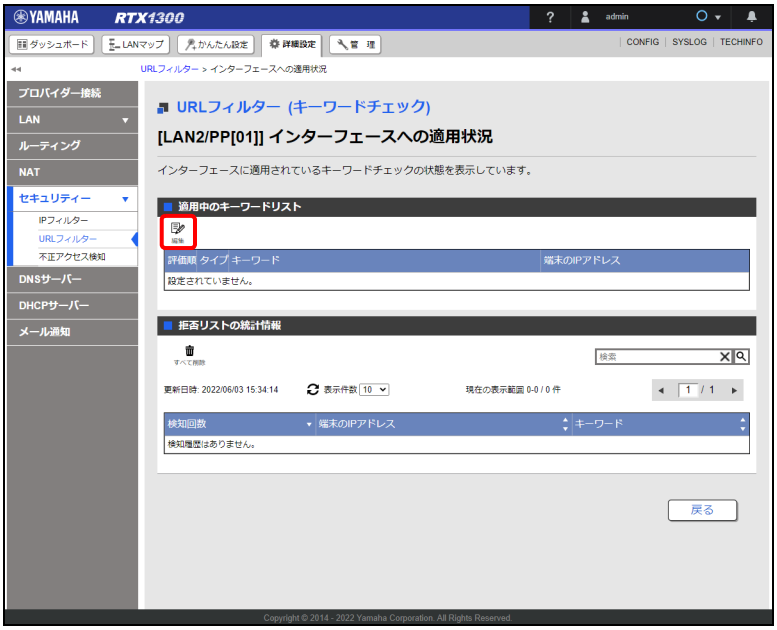
「戻る」ボタンをクリックし、「URL フィルター」画面を表示します。

11.「インターフェースへの適用状況」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



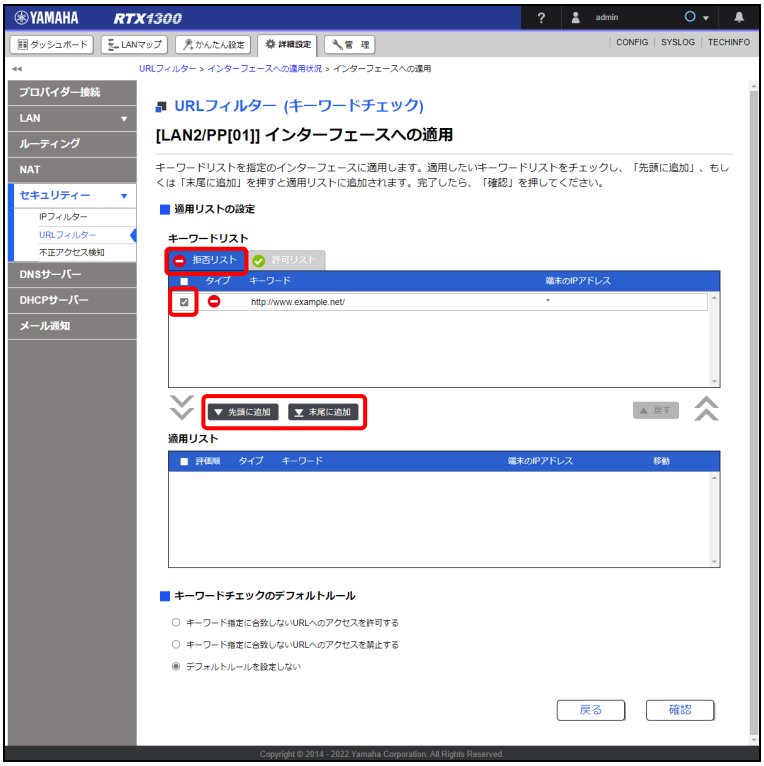
「LAN2/PP[01] インターフェースへの適用状況」画面が表示されます。

12.「適用中のキーワードリスト」項目の「編集」ボタンをクリックする。

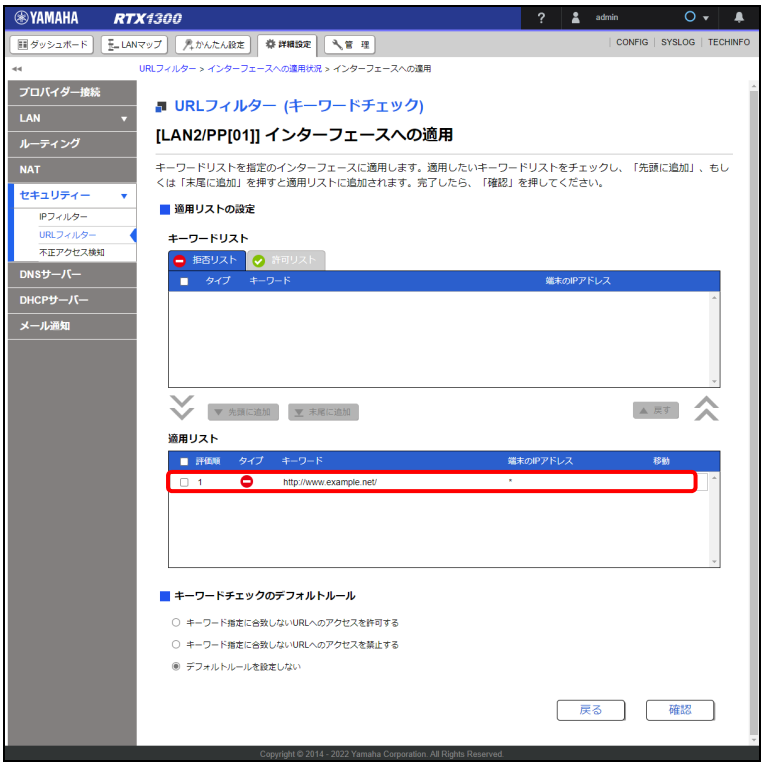


「LAN2/PP[01] インターフェースへの適用」画面が表示されます。

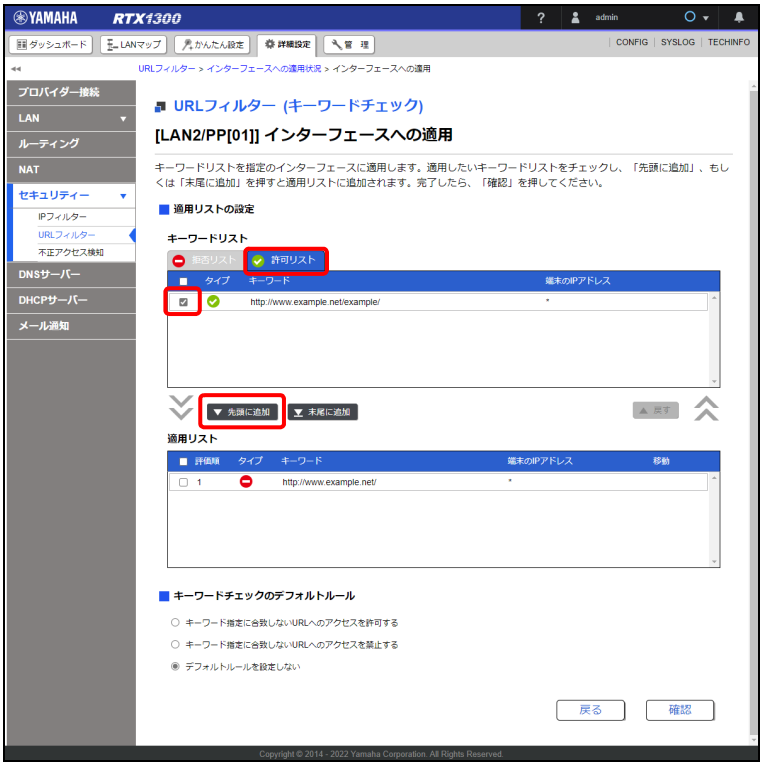
13.「キーワードリスト」の「拒否リスト」タブから「適用リスト」に移動するキーワードをチェックし、「先頭に追加」ボタンまたは「末尾に追加」ボタンをクリックする。



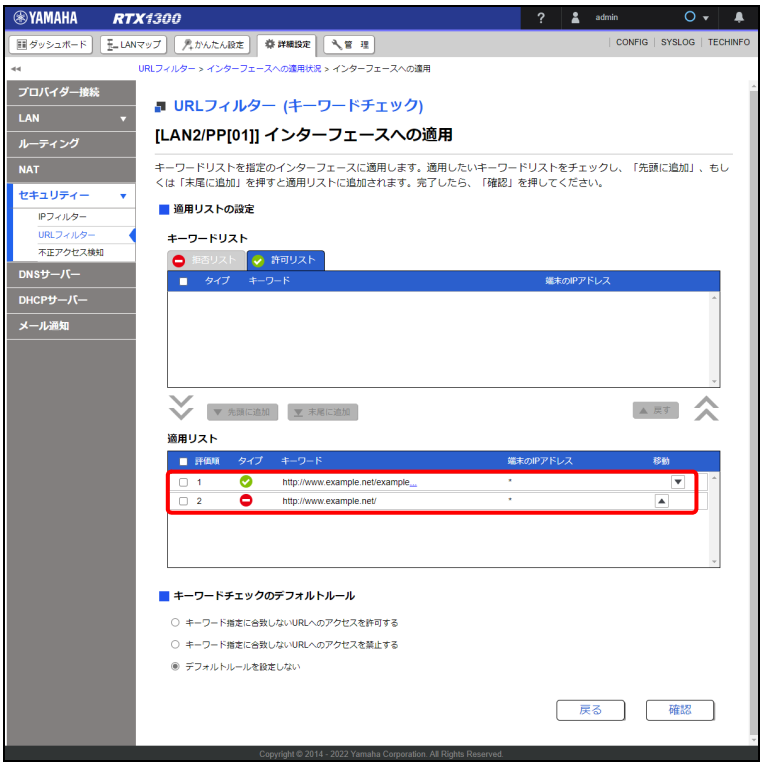
選択した「キーワードリスト（拒否リスト）」が「適用リスト」に移動します。



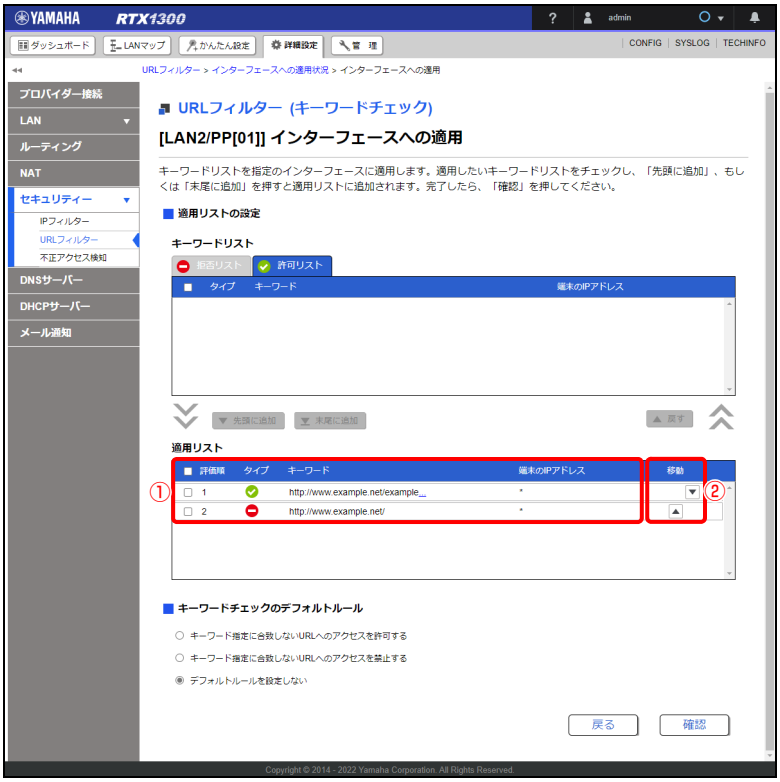
14.「キーワードリスト」の「許可リスト」タブをクリックして表示を切り替え、「適用リスト」に移動するキーワードをチェックし、「先頭に追加」ボタンをクリックする。



選択した「キーワードリスト（許可リスト）」が「適用リスト」の先頭に移動します。



15.「適用リスト」の「評価順」が正しいことを確認する。



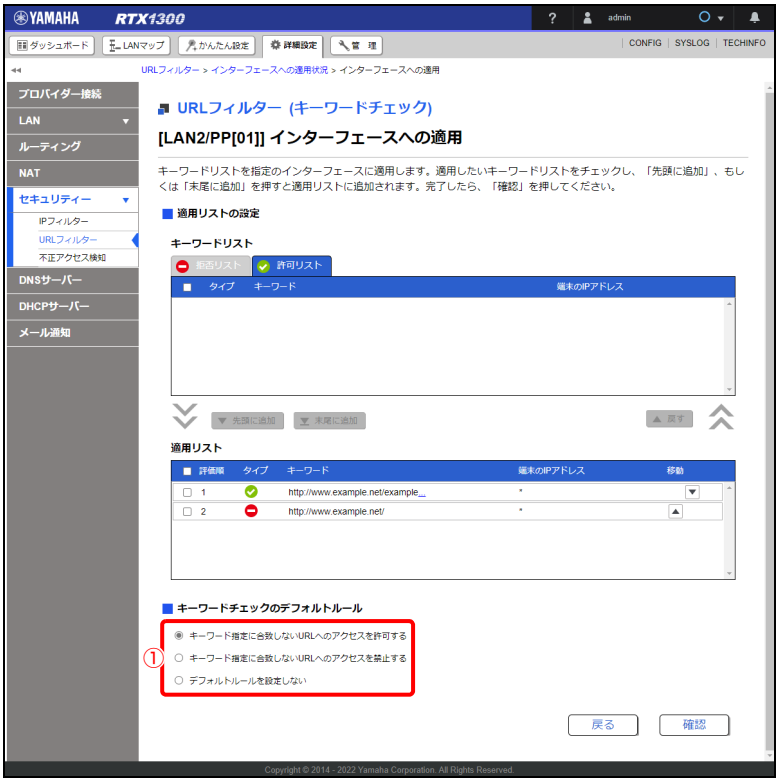
① **評価順：**
先に許可リストの「http://www.example.net/example/」が評価された後、次に拒否リストの「http://www.example.net/」が評価されるようになっていることを確認します。

② **移動：**
評価順が間違っている場合は、「▼」「▲」ボタンで評価順を入れ替えます。

メモ

適用リストの評価順にしたがって URL のキーワードチェックが行われ、先に合致したルールが優先されます。

16.「キーワードチェックのデフォルトルール」を設定する。

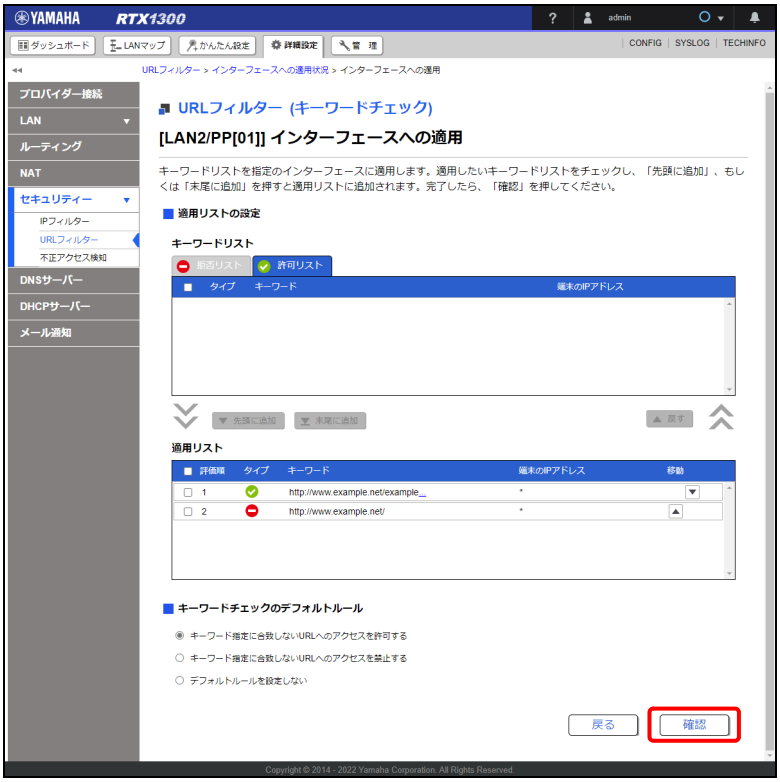


① **キーワードチェックのデフォルトルール：**
「キーワード指定に合致しない URL へのアクセスを許可する」を選択します。

メモ

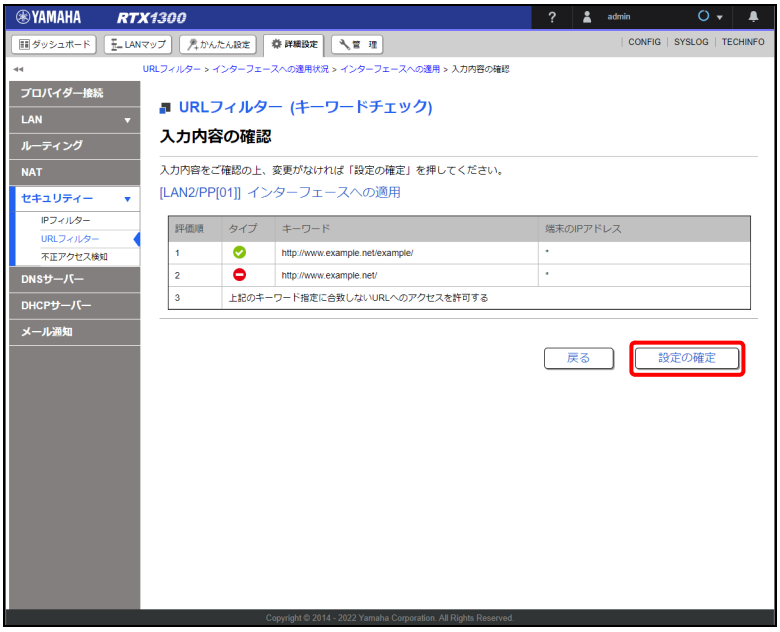
・ デフォルトルールは拒否リストや許可リストに表示されません。
・ デフォルトルールは拒否リストや許可リストで、「キーワード」と「端末の IP アドレス」に「*」を指定したものと同等です。

17.「確認」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

18.内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「[LAN2/PP[01]] インターフェースへの適用状況」画面が表示されます。

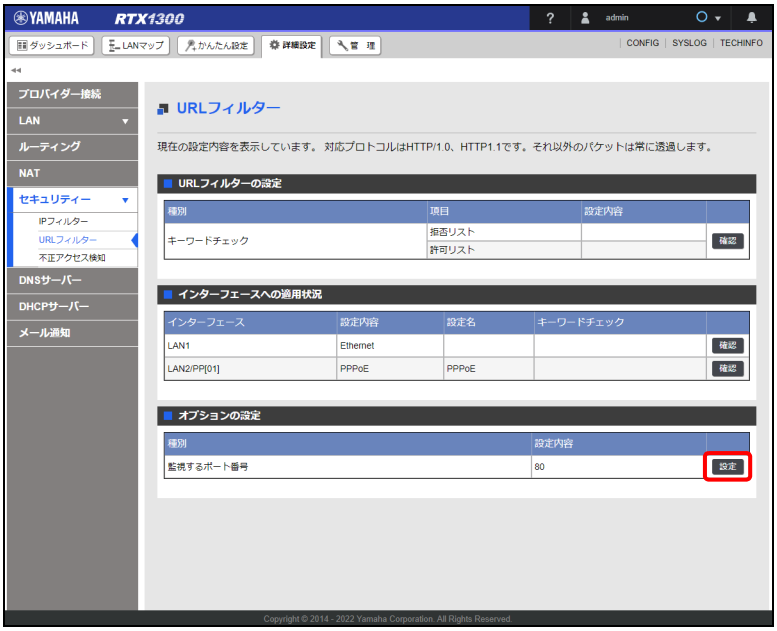
13.5.4 監視するポート番号を増やす

URL フィルターで監視するポート番号を以下の手順で増やします。

設定例

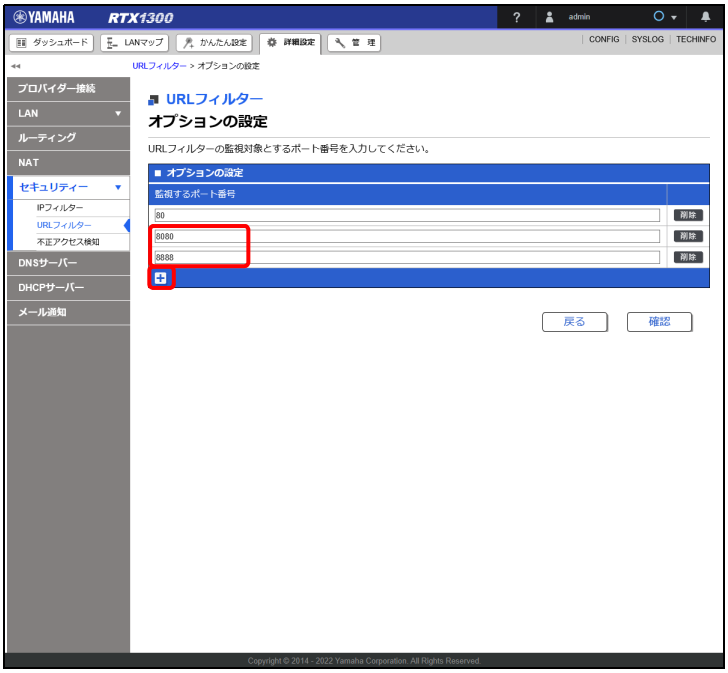
追加するポート番号：8080、8888

1. **「詳細設定」タブ ―「セキュリティー」―「URL フィルター」を順に選択する。**
   「URL フィルター」画面が表示されます。
2. **「オプションの設定」項目の「設定」ボタンをクリックする。**



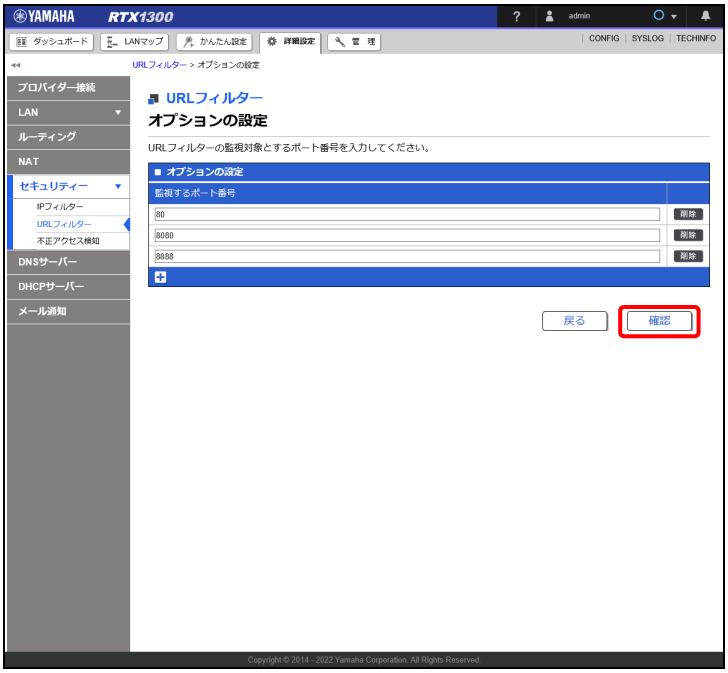
「オプションの設定」画面が表示されます。

3.「監視するポート番号」欄に任意の番号を入力します。



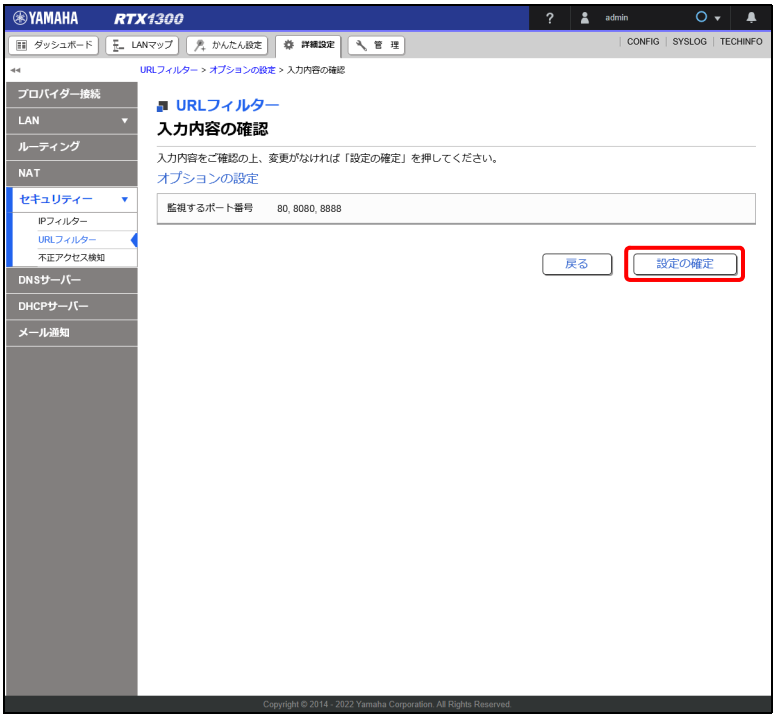
① **監視するポート番号：**
「8080」と「8888」を入力します。
監視するポート番号を追加する場合は、下部の「 ＋ 」ボタンを押してください。ポート番号を追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

4.「確認」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



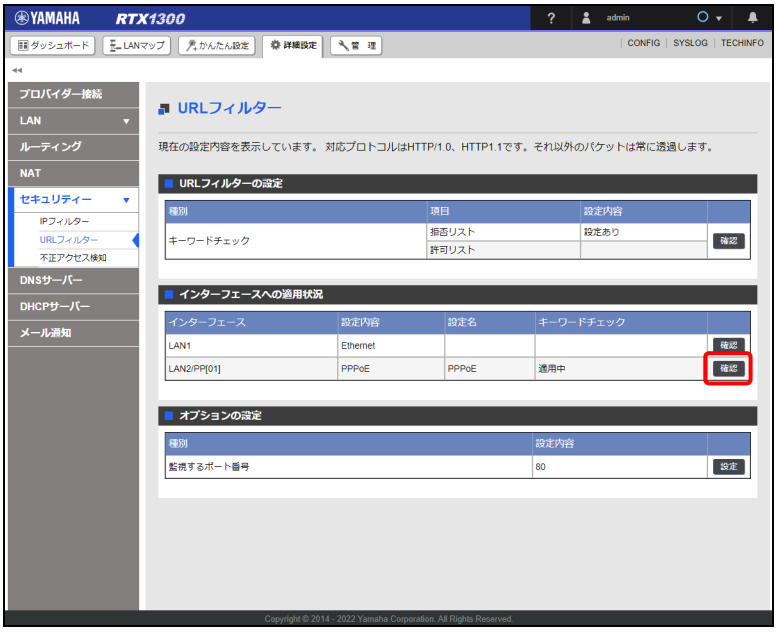
設定が反映され、「URL フィルター」画面が表示されます。

13.5.5 拒否リストの統計情報の並び替え / 検索 / 削除をする

アクセスを禁止している URL へアクセスしようとした端末の統計情報が表示されます。
本項では「拒否リスト」の設定を行った状態（「13.5.1 特定のキーワードを含む URL へのアクセスを禁止する」（257 ページ）の設定が完了している状態）から設定する前提で説明します。

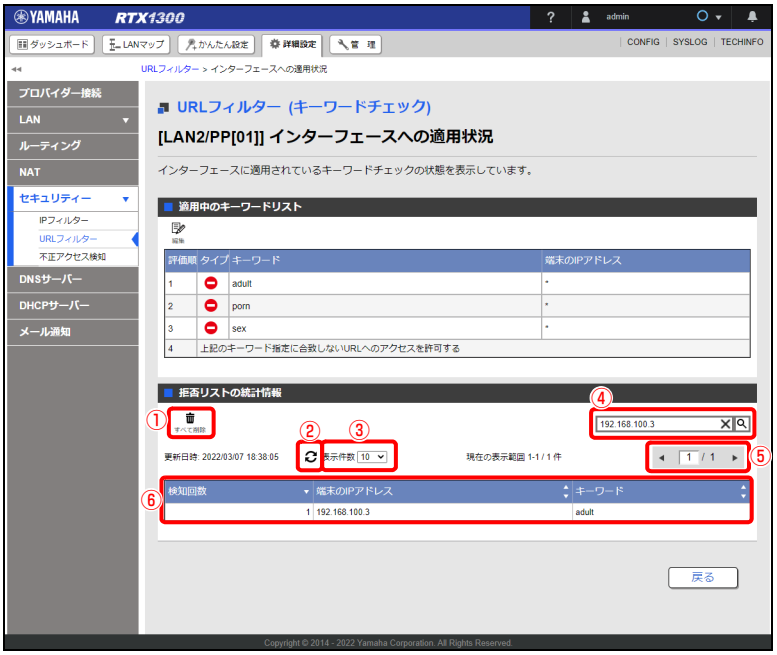
1. **「詳細設定」タブ ー「セキュリティー」ー「URL フィルター」を順に選択する。**
「URL フィルター」画面が表示されます。

2.「インターフェースへの適用状況」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



「[LAN2/PP[01]] インターフェースへの適用状況」画面が表示されます。

3.「拒否リストの統計情報」項目で、統計情報を検索または削除する。



①「すべて削除」ボタン：
ボタンをクリックすると確認ダイアログが開き、続けて「実行」ボタンをクリックすると検知履歴がすべて削除されます。検知履歴の削除に伴い、URL へのアクセス検知回数もリセットされます。

②「🔄」ボタン：
最新の情報に更新されます。

③ **表示件数プルダウンメニュー：**
一度に表示する履歴件数を選択できます。

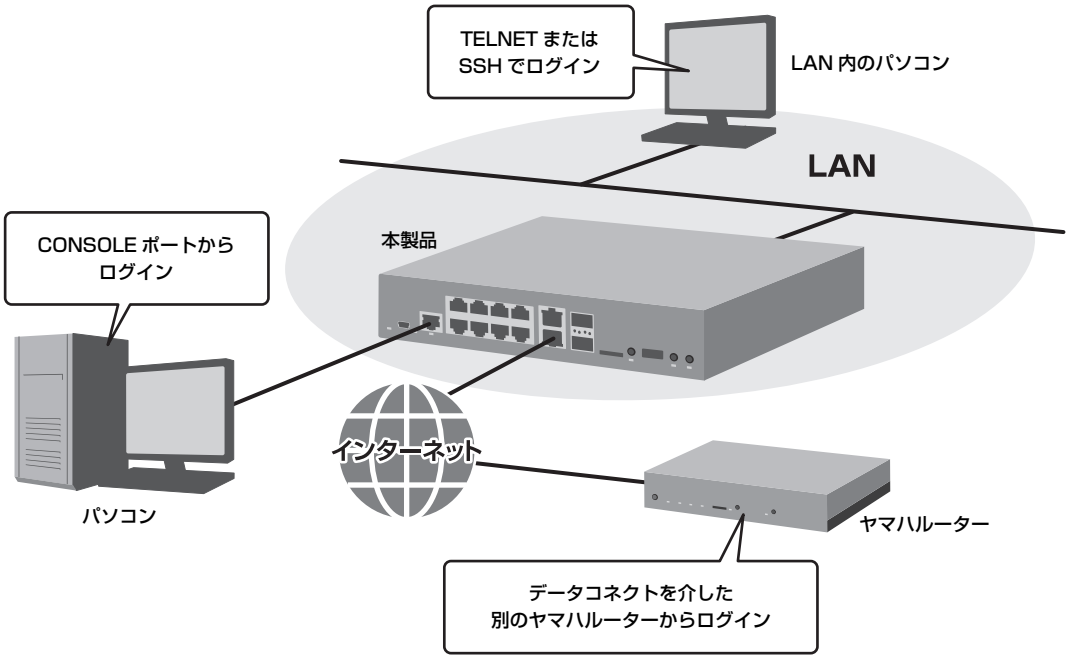
④ **検索ボックス：**
任意のキーワードを入力し「 」ボタンをクリックすると検索を実行します。「 」ボタンをクリックするとキーワードがクリアされます。

⑤ **「 」「 」ボタン：**
履歴の数が表示件数を超えた場合、表示する履歴の範囲を変更できます。

⑥ **「 」ボタン：**
項目ごとのボタンをクリックするとリストを並び替えることができます。再度クリックすると、昇順と降順が切り替わります。
- 「検知回数」：検知回数順にソートが行われます。初期画面では、検知回数順にソートされています。
- 「端末の IP アドレス」：IP アドレス順にソートが行われます。
- 「キーワード」：アルファベット順にソートが行われます。

13.6 本製品へのアクセスを管理する

本製品へのアクセスを許可するユーザーを限定したり、接続手段を限定したりすることができます。セキュリティーを確保するために、これらの機能を活用し、必要最低限のアクセスだけ許可するように設定することをおすすめいたします。



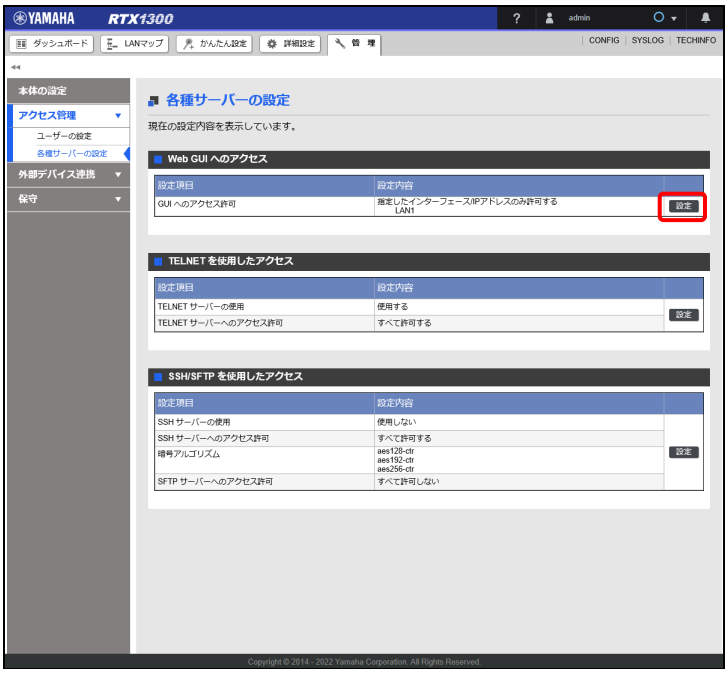
13.6.1 本製品へのアクセスを制限する

本製品が対応している各種サーバー機能へのアクセスを制限します。

Web GUI へのアクセスを設定する

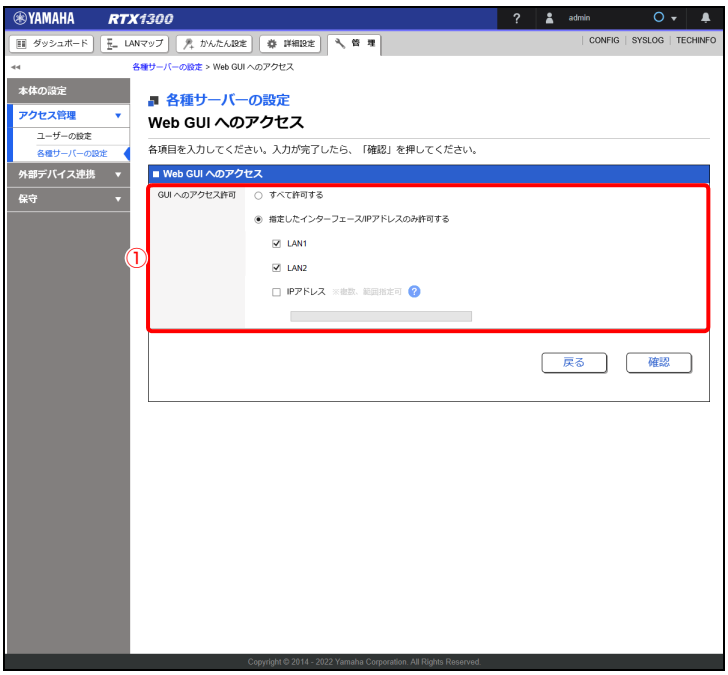
1. **「管理」タブ ―「アクセス管理」―「各種サーバーの設定」を順に選択する。**
   「各種サーバーの設定」画面が表示されます。

2. **「Web GUI へのアクセス」項目の「設定」ボタンをクリックする。**



「Web GUI へのアクセス」画面が表示されます。

3. **Web GUI へのアクセス許可を設定する。**

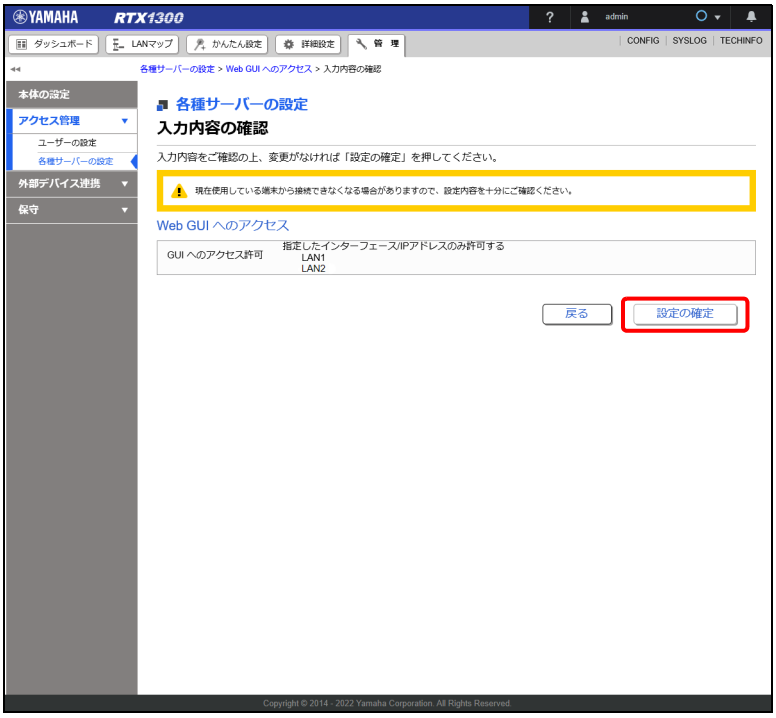


① GUI へのアクセス許可：

- **すべて許可する**
  すべてのインターフェースおよび IP アドレスからのアクセスを許可します。
- **指定したインターフェース /IP アドレスのみ許可する**
  指定したインターフェースや IP アドレスからのアクセスのみを許可します。使用中のインターフェースのみ表示されます。
  「IP アドレス」にチェックを入れるとアクセスを許可する IP アドレスを設定できます。複数の IP アドレスを設定する場合は以下のように入力してください。
  – IP アドレスの範囲を入力する場合は、2 つの IP アドレスをハイフンでつないで記述します。
    例：172.16.0.1-172.16.0.14
  – 複数の IP アドレスや IP アドレスの範囲を設定する場合は、空白で区切って記述します。
    例：172.16.0.1-172.16.0.2 172.16.0.4 172.16.0.6-172.16.0.14

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「各種サーバーの設定」画面が表示されます。

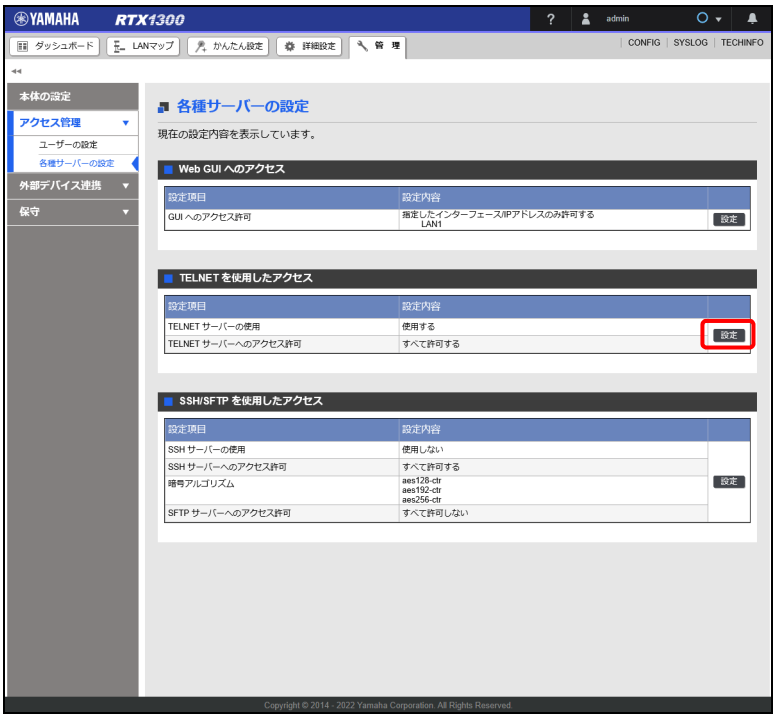
重要

現在使用している端末から接続できなくなる場合がありますので、設定内容を十分にご確認の上、設定を確定してください。

TELNET を使用したアクセスを設定する

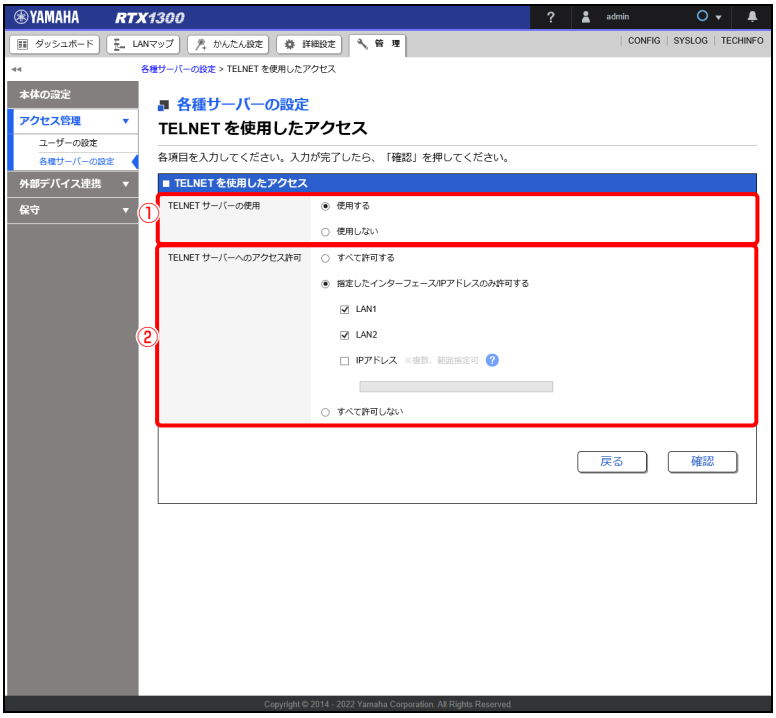
1. 「管理」タブ ―「アクセス管理」―「各種サーバーの設定」を順に選択する。
   「各種サーバーの設定」画面が表示されます。

2. 「TELNET を使用したアクセス」項目の「設定」ボタンをクリックする。



「TELNET を使用したアクセス」画面が表示されます。

3. TELNET を使用したアクセス許可を設定する。



① **TELNET サーバーの使用：**

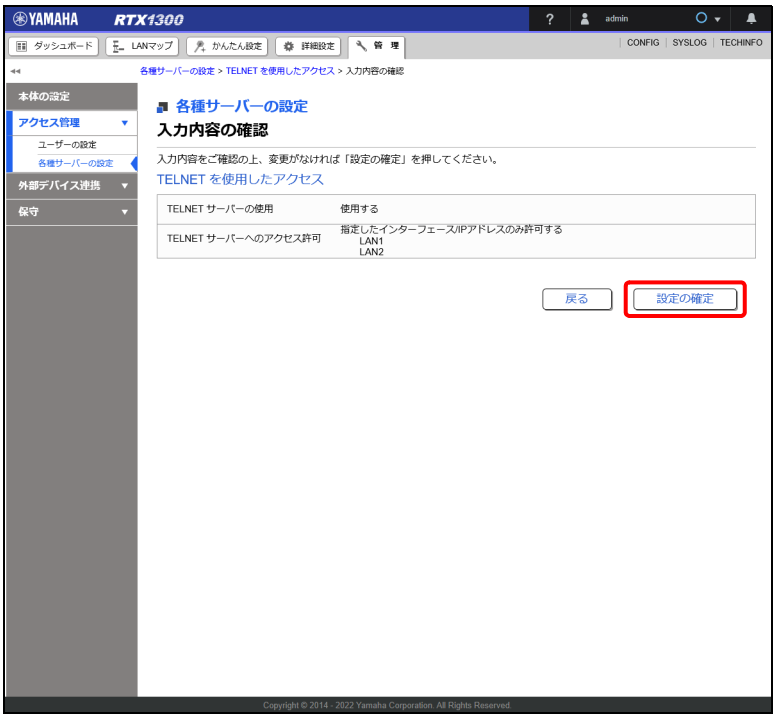
- **使用する**
  TELNET サーバー機能を動作させます。「TELNET サーバーへのアクセス許可」項目の設定が可能になります。
- **使用しない**
  TELNET サーバー機能を動作させません。

② **TELNET サーバーへのアクセス許可：**

- **すべて許可する**
  すべてのインターフェース /IP アドレスからのアクセスを許可します。
- **指定したインターフェース /IP アドレスのみ許可する**
  指定したインターフェースや IP アドレスからのアクセスのみを許可します。使用中のインターフェースのみ表示されます。
  「IP アドレス」にチェックを入れるとアクセスを許可する IP アドレスを設定できます。複数の IP アドレスを設定する場合は以下のように入力してください。
  – IP アドレスの範囲を入力する場合は、2 つの IP アドレスをハイフンでつないで記述します。
    例：172.16.0.1-172.16.0.14
  – 複数の IP アドレスや IP アドレスの範囲を設定する場合は、空白で区切って記述します。
    例：172.16.0.1-172.16.0.2 172.16.0.4 172.16.0.6-172.16.0.14
- **すべて許可しない**
  すべてのインターフェース /IP アドレスからのアクセスを拒否します。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

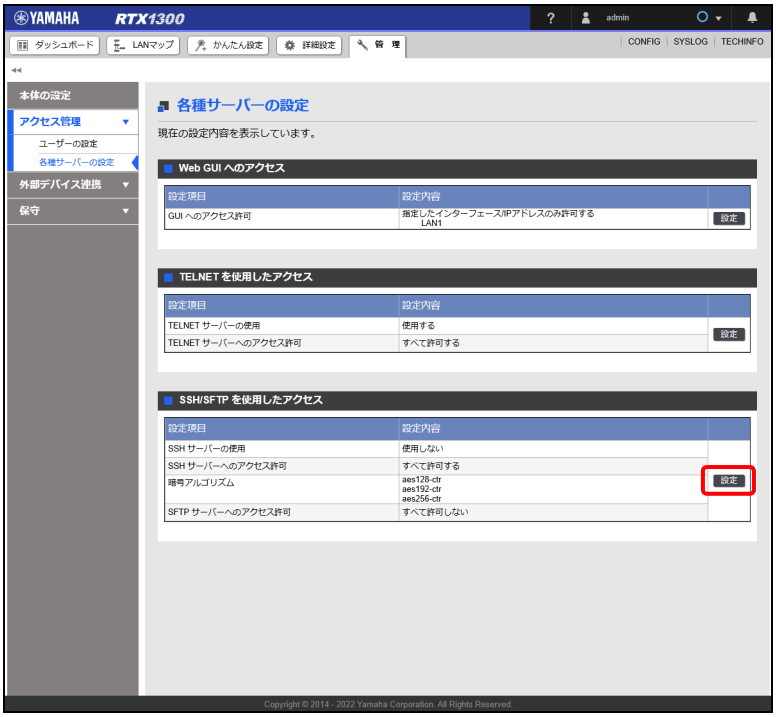
5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「各種サーバーの設定」画面が表示されます。

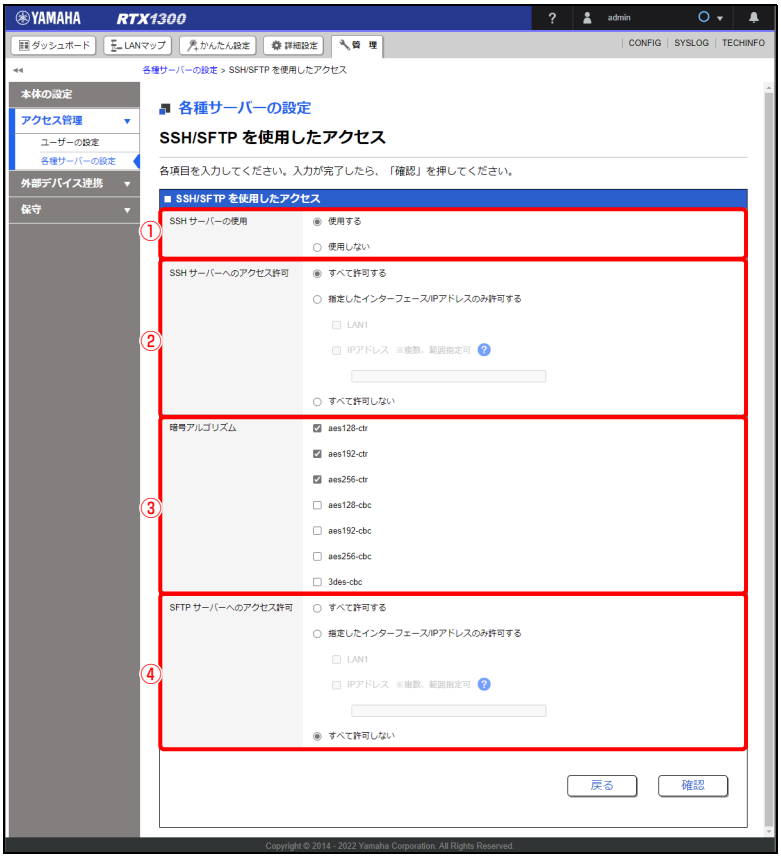
SSH/SFTP を使用したアクセスを設定する

1. 「管理」タブ ―「アクセス管理」―「各種サーバーの設定」を順に選択する。
   「各種サーバーの設定」画面が表示されます。
2. 「SSH/SFTP を使用したアクセス」項目の「設定」ボタンをクリックする。



「SSH/SFTP を使用したアクセス」画面が表示されます。

3. SSH/SFTP を使用したアクセス許可を設定する。



① **SSH サーバーの使用：**

- **使用する**
  SSH サーバー機能を動作させます。SSH サーバーのホスト鍵が設定されていない場合、「使用する」を選択すると設定の確定時にホスト鍵が設定されます。「使用する」を選択した場合に他の項目の設定が可能になります。
- **使用しない**
  SSH サーバー機能を動作させません。SSH サーバーのホスト鍵が設定されている場合、「使用しない」を選択すると設定の確定時にホスト鍵の設定が削除されます。

② **SSH サーバーへのアクセス許可：**

- **すべて許可する**
  すべてのインターフェース /IP アドレスからのアクセスを許可します。
- **指定したインターフェース /IP アドレスのみ許可する**
  指定したインターフェースや IP アドレスからのアクセスのみを許可します。使用中のインターフェースのみ表示されます。
  「IP アドレス」にチェックを入れるとアクセスを許可する IP アドレスを設定できます。複数の IP アドレスを設定する場合は以下のように入力してください。
  - IP アドレスの範囲を入力する場合は、2 つの IP アドレスをハイフンでつないで記述します。
    例：172.16.0.1-172.16.0.14
  - 複数の IP アドレスや IP アドレスの範囲を設定する場合は、空白で区切って記述します。
    例：172.16.0.1-172.16.0.2 172.16.0.4 172.16.0.6-172.16.0.14

- **すべて許可しない**
  すべてのインターフェース /IP アドレスからのアクセスを拒否します。

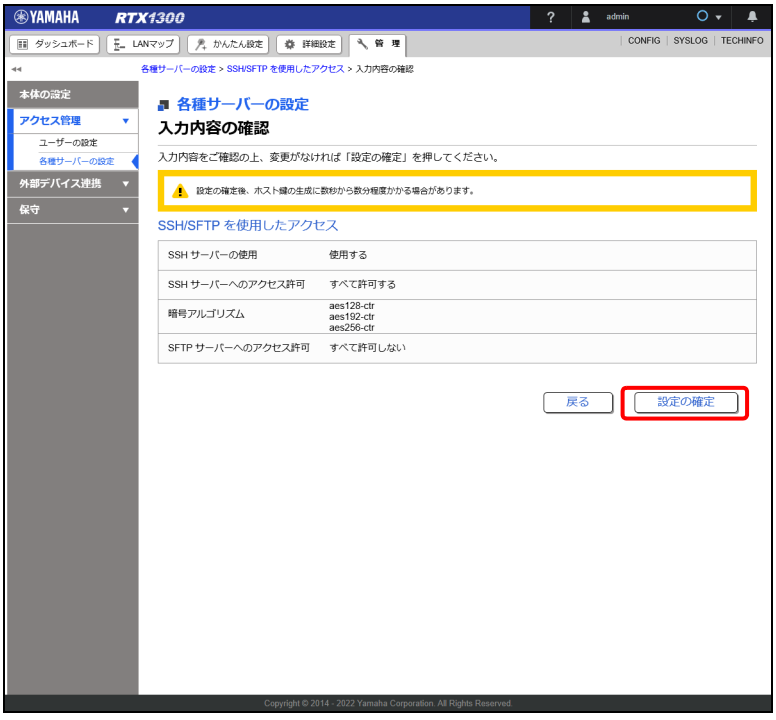
③ **暗号アルゴリズム：**
SSH で使用を許可する暗号アルゴリズムを設定します。

④ **SFTP サーバーへのアクセス許可：**
SSH サーバーへのアクセスが許可されているインターフェース、IP アドレスのみが、SFTP サーバーへのアクセスを許可できる対象となります。

- **すべて許可する**
  すべてのインターフェース /IP アドレスからのアクセスを許可します。
  「SSH サーバーへのアクセス許可」で「すべて許可する」を選択している場合に選択できます。
- **指定したインターフェース /IP アドレスのみ許可する**
  指定したインターフェースや IP アドレスからのアクセスのみを許可します。
  「SSH サーバーへのアクセス許可」で「指定したインターフェース /IP アドレスのみ許可する」を選択している場合、「SSH サーバーへのアクセス許可」で選択されているインターフェースのみ、選択できます。使用中のインターフェースのみ表示されます。
  「IP アドレス」にチェックを入れるとアクセスを許可する IP アドレスを設定できます。複数の IP アドレスを設定する場合は以下のように入力してください。
  – IP アドレスの範囲を入力する場合は、2 つの IP アドレスをハイフンでつないで記述します。
    例：172.16.0.1-172.16.0.14
  – 複数の IP アドレスや IP アドレスの範囲を設定する場合は、空白で区切って記述します。
    例：172.16.0.1-172.16.0.2 172.16.0.4 172.16.0.6-172.16.0.14
- **すべて許可しない**
  すべてのインターフェース /IP アドレスからのアクセスを拒否します。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「各種サーバーの設定」画面が表示されます。

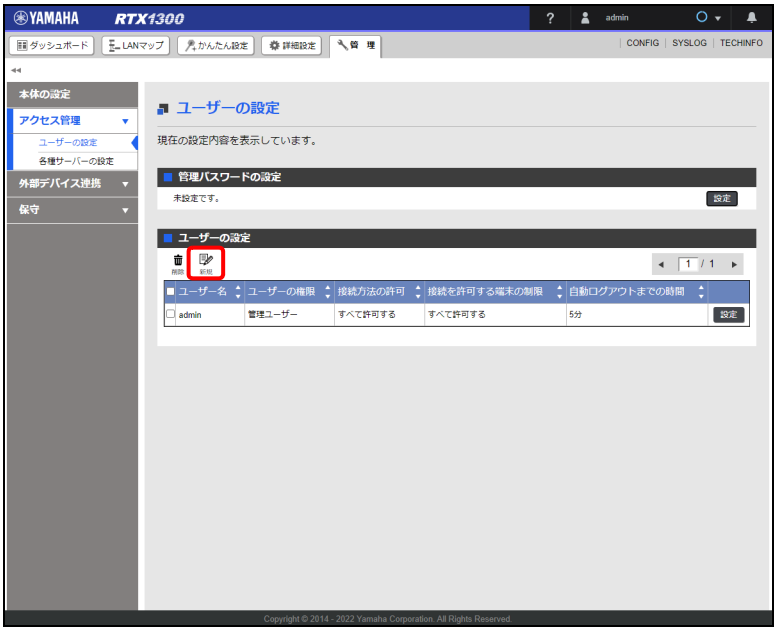
13.6.2 ログインを許可するユーザーを登録する

ユーザーを登録して、本製品にログインできるユーザーを制限します。

設定例

ユーザー名：user
パスワード：password
ユーザーの権限：管理ユーザー
Web GUI 画面の閲覧の許可：すべて許可する
同一ユーザー名による複数接続：許可する

1. **「管理」タブ ―「アクセス管理」―「ユーザーの設定」を順に選択する。**
   「ユーザーの設定」画面が表示されます。
2. **「ユーザーの設定」項目の「 新規 」ボタンをクリックする。**



「ユーザーの設定」画面が表示されます。

3. ユーザー情報を設定する。

① **ユーザー名：**
「user」を入力します。

② **新しいパスワード：**
「password」を入力します。入力したパスワードは、●で表示されます。

③ **新しいパスワード（確認）：**
「password」を入力します。入力したパスワードは、●で表示されます。

④ **ユーザーの権限：**
「管理ユーザー」を選択します。

メモ

「一般ユーザー」を選択し、「管理ユーザーへの昇格を許可する」にチェックを入れた場合は、コマンドコンソール画面上で管理パスワードの入力をすることで管理ユーザーへの昇格が可能です。

⑤ **Web GUI 画面の閲覧の許可：**
「すべて許可する」を選択します。

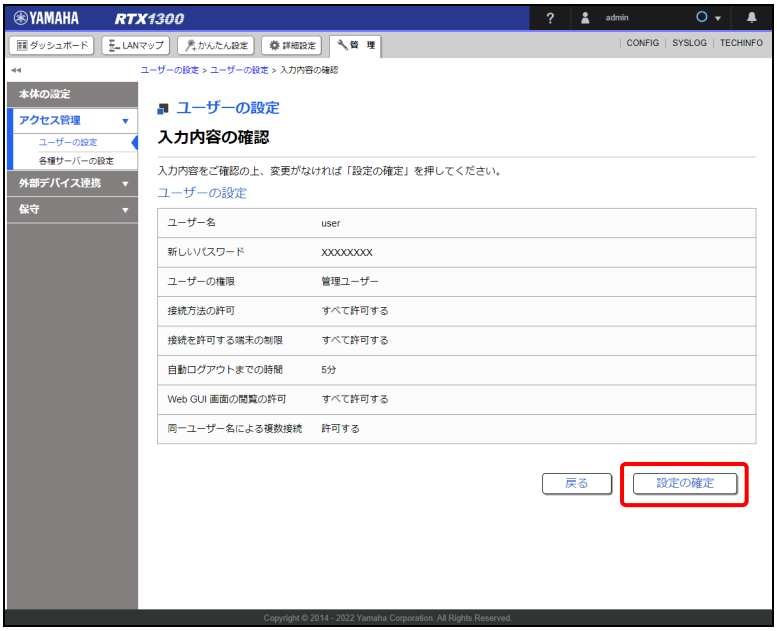
⑥ **同一ユーザー名による複数接続：**
「許可する」を選択します。

メモ

実際に設定するパスワードは、数字や記号を混ぜたり、できるだけ長くしたりするなど、類推しにくい文字列にすることをおすすめいたします。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「ユーザーの設定」画面が表示されます。

13.6.3 ユーザーごとにアクセス方法を制限する

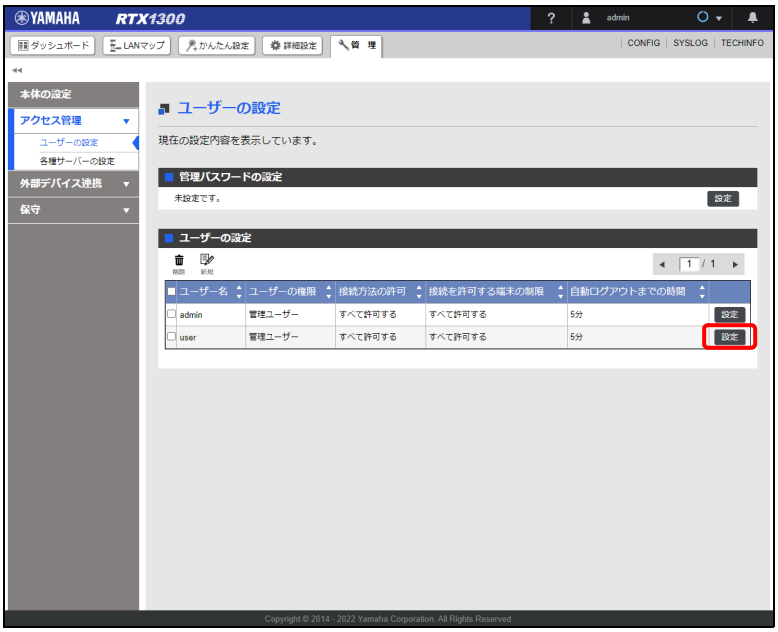
ユーザーごとに、本製品へのアクセス方法を制限します。IP アドレスにより接続を許可する端末を制限したり、ウェブブラウザー（HTTP）や TELNET など接続方法の制限をしたりします。

設定例

アクセス制限を行うユーザー：user
接続方法の許可：TELNET、HTTP
接続を許可する端末の IP アドレス：192.168.100.2

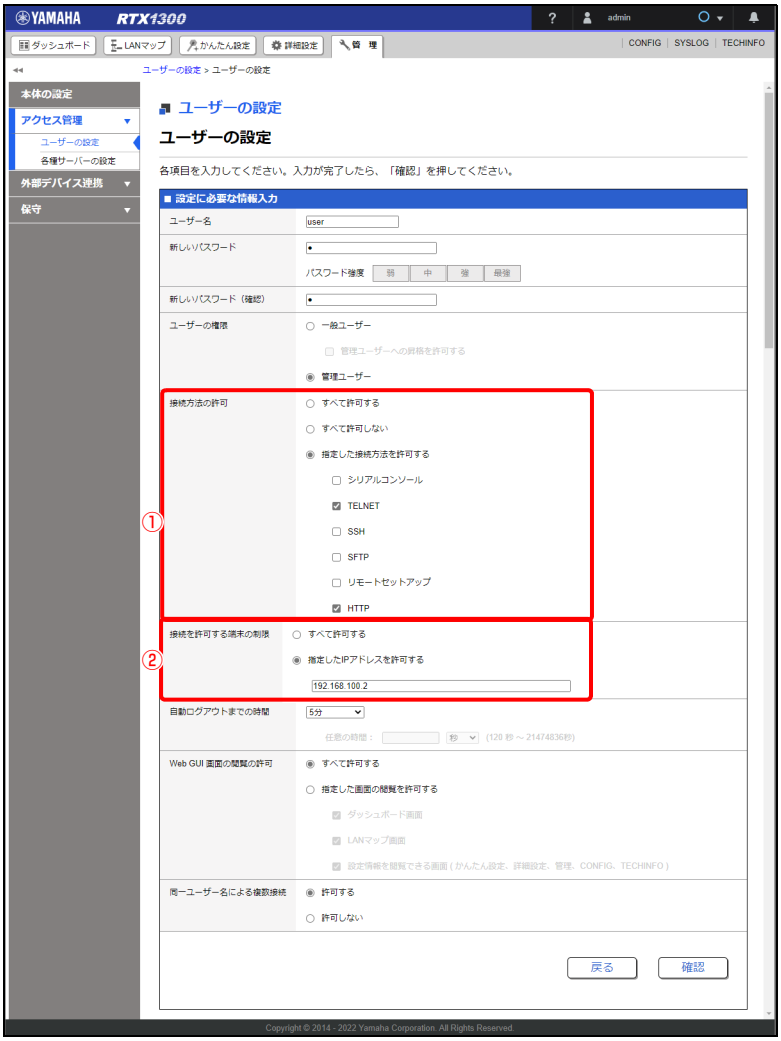
1. **「管理」タブ ―「アクセス管理」―「ユーザーの設定」を順に選択する。**
「ユーザーの設定」画面が表示されます。

2.「ユーザーの設定」項目の user の「設定」ボタンをクリックする。



「ユーザーの設定」画面が表示されます。

3. **ユーザー情報を設定する。**

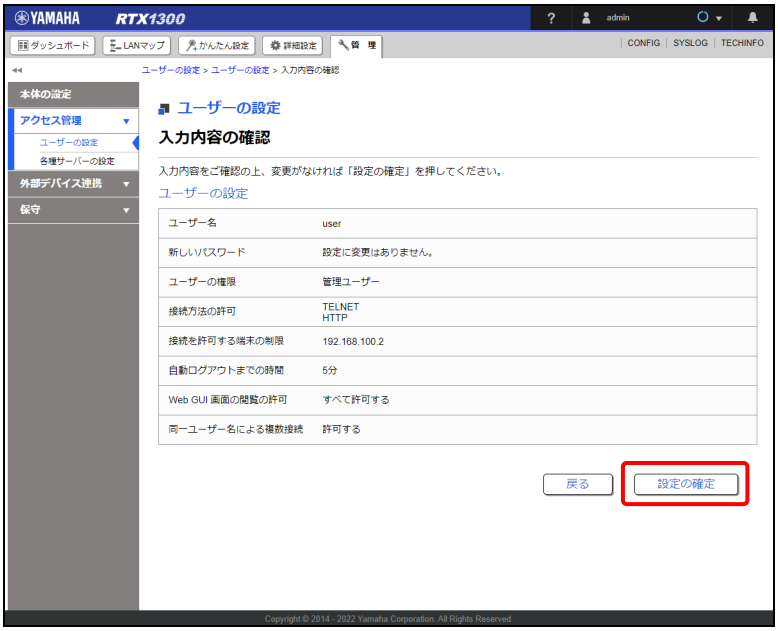


① **接続方法の許可：**
「指定した接続方法を許可する」を選択し、「TELNET」と「HTTP」にチェックを入れます。

② **接続を許可する端末の制限：**
「指定した IP アドレスを許可する」を選択し、「192.168.100.2」を入力します。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「ユーザーの設定」画面が表示されます。

13.6.4 ユーザーのパスワードを変更する

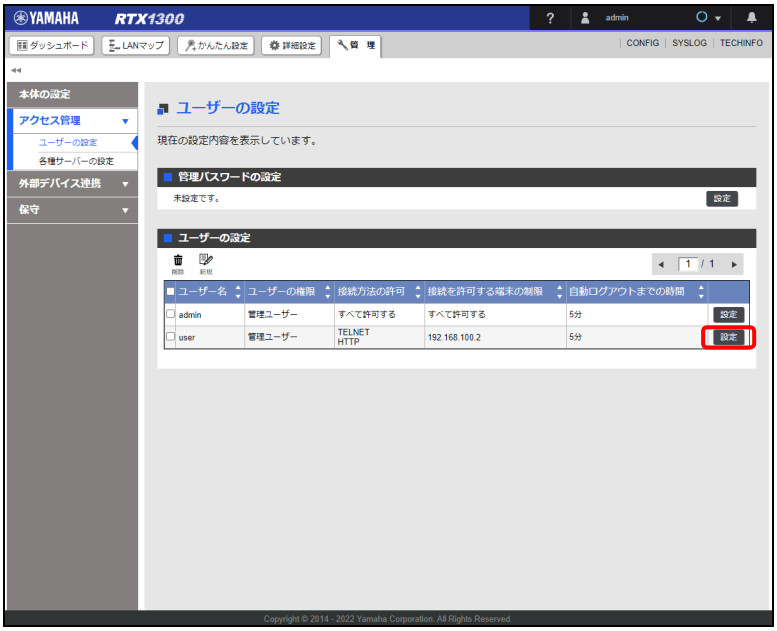
ユーザーのパスワードを変更します。定期的なパスワードの変更は、セキュリティー対策として効果的です。

設定例

パスワードを変更するユーザー：user
パスワード：yamaha

1. **「管理」タブ―「アクセス管理」―「ユーザーの設定」を順に選択する。**
   「ユーザーの設定」画面が表示されます。

2.「ユーザーの設定」項目の user の「設定」ボタンをクリックする。



「ユーザーの設定」画面が表示されます。

3. パスワードを設定する。

① **新しいパスワード：**
「yamaha」を入力します。入力したパスワードは、●で表示されます。

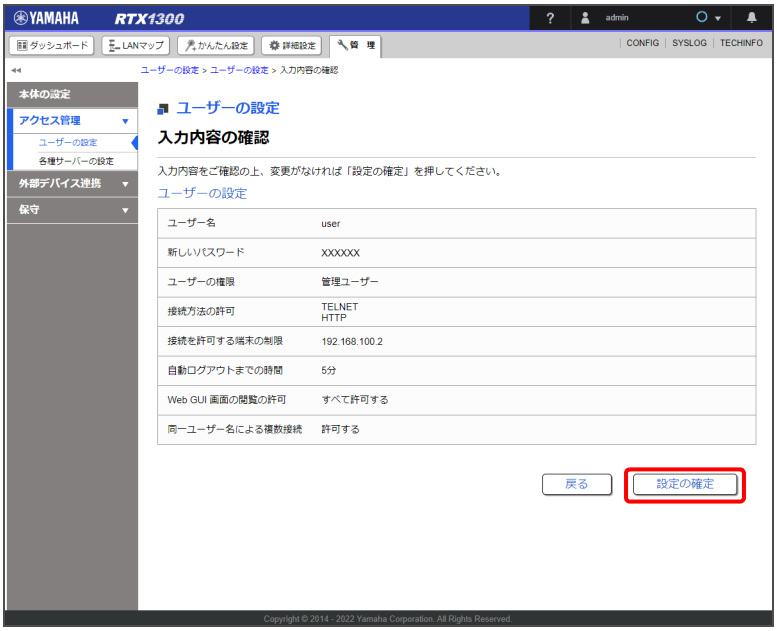
② **新しいパスワード（確認）：**
「yamaha」を入力します。入力したパスワードは、●で表示されます。

メモ

実際に設定するパスワードは、数字や記号を混ぜたり、できるだけ長くしたりするなど、類推しにくい文字列にすることをおすすめいたします。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「ユーザーの設定」画面が表示されます。

第 14 章 詳細設定を行う

本章では、「詳細設定」画面にある各種設定メニューを活用して、外部にサーバーを公開したり、複数の WAN 回線を主回線とバックアップ回線で使い分けたりするなど、本製品の応用的な設定について説明します。

・ プロバイダーの詳細設定を行う …305 ページ
・ LAN のアドレスを設定する …318 ページ
・ グローバル IP アドレスを複数の端末でシェアする …330 ページ
・ 外部にサーバーを公開する …335 ページ
・ 複数のプロバイダーを使用する …343 ページ
・ DNS サーバーを設定する …365 ページ
・ DHCP で端末に IP アドレスを割り当てる …380 ページ
・ 異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる …384 ページ
・ メール通知機能を使う …386 ページ

14.1 プロバイダーの詳細設定を行う

「かんたん設定」では設定を簡素化するために設定項目の数が最小限に抑えられているため、「かんたん設定」の「プロバイダー接続」画面だけではきめ細かな設定ができません。一方、「詳細設定」の「プロバイダー接続」画面では、「かんたん設定」では設定できない内容まで細かく設定することができます。本節では「プロバイダー接続」画面（詳細設定）の代表的な設定について説明します。

かんたん設定の基本的な設定は以下のページをご覧ください。

・ 4.1 ブロードバンド回線でインターネットに接続する …28 ページ
・ 4.2 USB 接続型データ通信端末でインターネットに接続する …39 ページ
・ 5.1 フレッツ光（IPv6 IPoE）でインターネットに常時接続する …46 ページ
・ 5.2 フレッツ光（IPv6 PPPoE）でインターネットに常時接続する …52 ページ

メモ

「ポート開放の設定」については、「14.6 外部にサーバーを公開する」（335 ページ）をご覧ください。

14.1.1 WAN 回線の MTU を設定する

WAN 回線の MTU の値を設定します。使用する WAN 回線によっては、MTU を適切な値に設定しなければ満足な通信速度が得られない場合があります。適切な値については使用するプロバイダーにお問い合わせください。

メモ

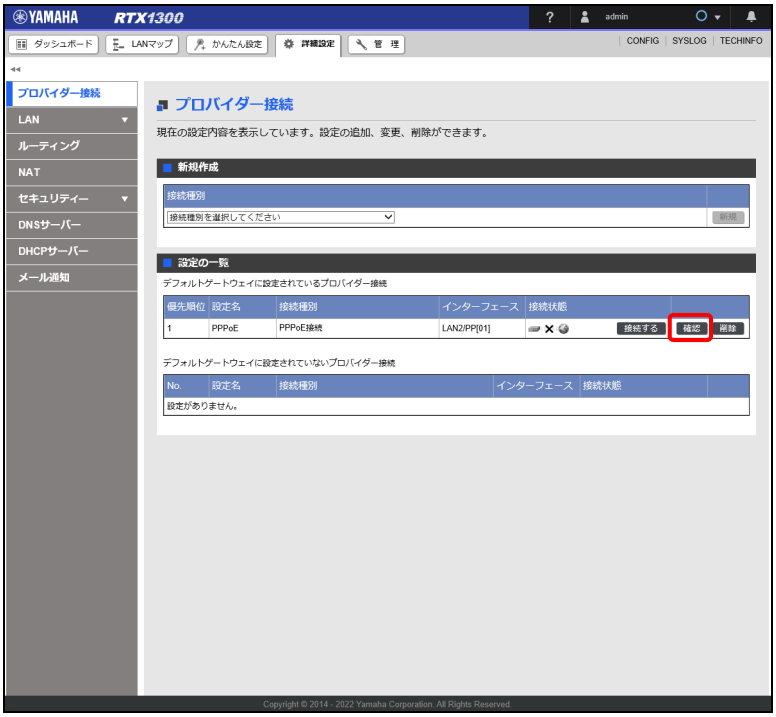
MTU の値は、プロバイダー接続の接続種別で「PPPoE 接続」「IPv6 PPPoE 接続」を選択した場合に設定できます。

本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

1.「詳細設定」タブ ―「プロバイダー接続」を順に選択する。

「プロバイダー接続」画面が表示されます。

2.「設定の一覧」項目の「PPPoE 接続」の「確認」ボタンをクリックする。

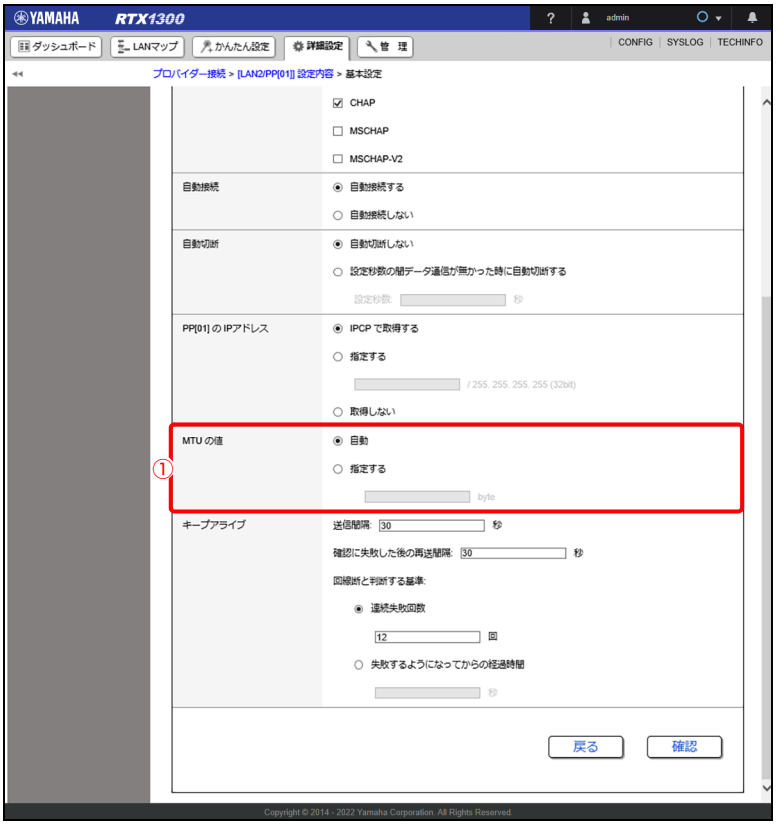


「LAN2/PP[01] 設定内容」画面が表示されます。

3.「基本設定」項目の「設定」ボタンをクリックする。

「基本設定」画面が表示されます。

4. 「MTU の値」を設定する。



① **MTU の値：**

- **「自動」**
  MTU の値が自動で割り当てられます。

メモ

「自動」に設定した状態で、データの送受信が非常に遅い、あるいは途中で止まるという場合には、いったんプロバイダーとの接続を切断して、「指定する」を選択し「1454」などの値を設定した後に、再度接続をしてください。

- **「指定する」**
  64byte から 1500byte までの範囲で任意の値を入力します。

5. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

6. **内容を確認し、「設定の確定」ボタンをクリックする。**
   設定が反映され、「LAN2/PP[01] 設定内容」画面が表示されます。

14.1.2 宛先ネットワークを設定する

「かんたん設定」を使用してプロバイダーを設定した場合は、すべての宛先に対する通信でそのプロバイダーが使用されるように設定されます。「詳細設定」の「プロバイダー接続」画面ではプロバイダーごとに宛先ネットワークを限定することができます。

メモ

宛先ネットワークは、プロバイダー接続の接続種別で「PPPoE 接続」「DHCP、または固定 IP アドレスによる接続」「モバイル接続（モデム方式）」「モバイル接続（イーサネット方式）」を選択した場合に設定できます。

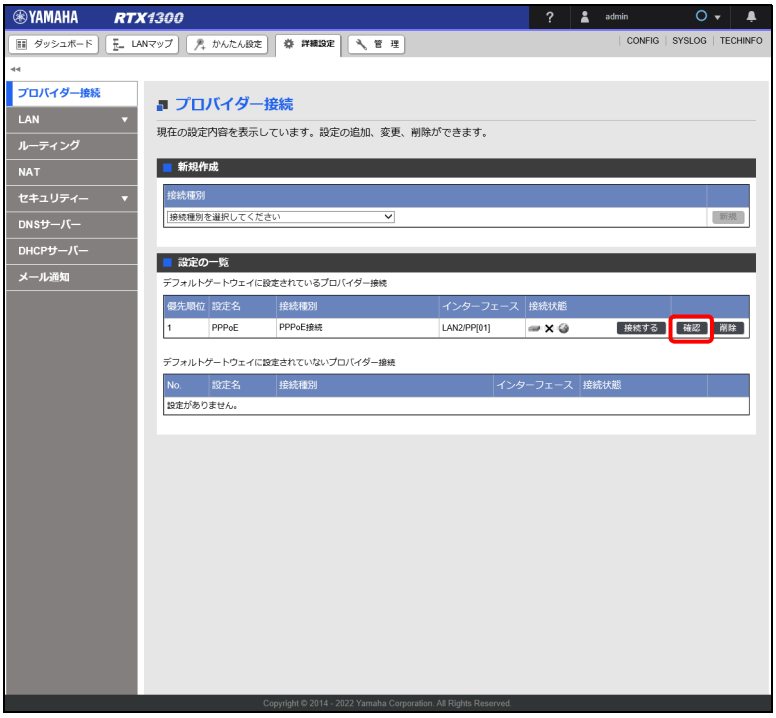
本項では、「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

設定例

設定する宛先ネットワーク：203.0.113.16/28、203.0.113.32/28

1. **「詳細設定」タブ ―「プロバイダー接続」を順に選択する。**
   「プロバイダー接続」画面が表示されます。

2. **「設定の一覧」項目の「PPPoE 接続」の「確認」ボタンをクリックする。**

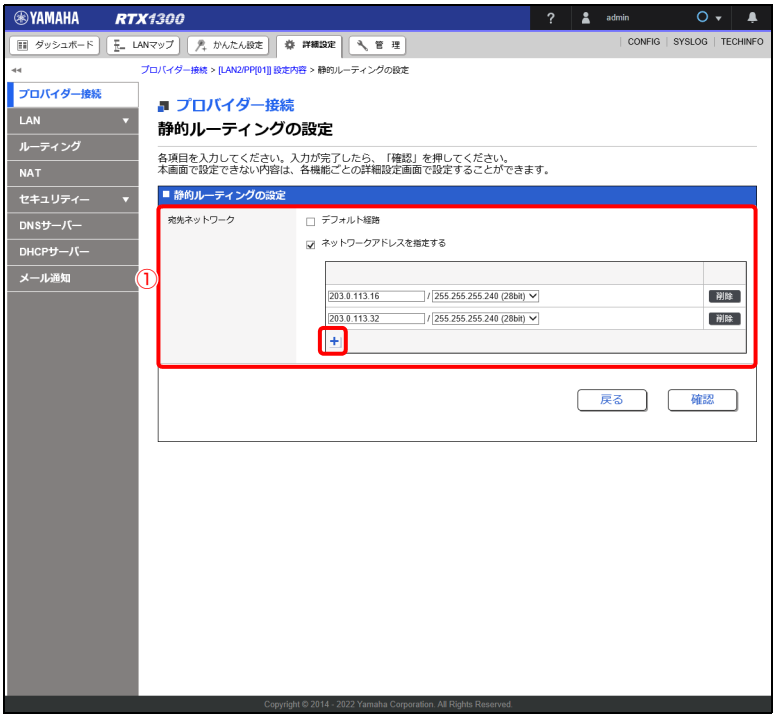


「LAN2/PP[01] 設定内容」画面が表示されます。

3.「静的ルーティングの設定」項目の「設定」ボタンをクリックする。

「静的ルーティングの設定」画面が表示されます。

4.「静的ルーティングの設定」を行う。



① **宛先ネットワーク：**
「デフォルト経路」のチェックを外し「ネットワークアドレスを指定する」にチェックを入れます。「203.0.113.16」を入力し、プルダウンメニューからサブネットマスクを「255.255.255.240（28bit）」に設定します。入力欄下部の「 ＋ 」ボタンを押して、入力欄を増やし「203.0.113.32」を入力し、プルダウンメニューからサブネットマスクを「255.255.255.240（28bit）」に設定します。
宛先ネットワークを追加すると入力欄の右側に「削除」ボタンが表示されます。削除する場合は、入力欄の右側の「削除」ボタンを押してください。

メモ
設定中のプロバイダー接続情報に対して、経路情報を 100 個まで設定できます。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

6. **内容を確認し、「設定の確定」ボタンをクリックする。**
設定が反映され、「LAN2/PP[01] 設定内容」画面が表示されます。

14.1.3 自動切断の設定を行う

「かんたん設定」を使用して PPPoE 接続型のプロバイダーを設定した場合は自動切断は無効になっています。なお、「かんたん設定」でモバイル接続型のプロバイダーを設定した場合は自動切断が有効になります。「詳細設定」の「プロバイダー接続」画面ではプロバイダーごとに所定の無通信時間経過後に自動切断するように設定できます。

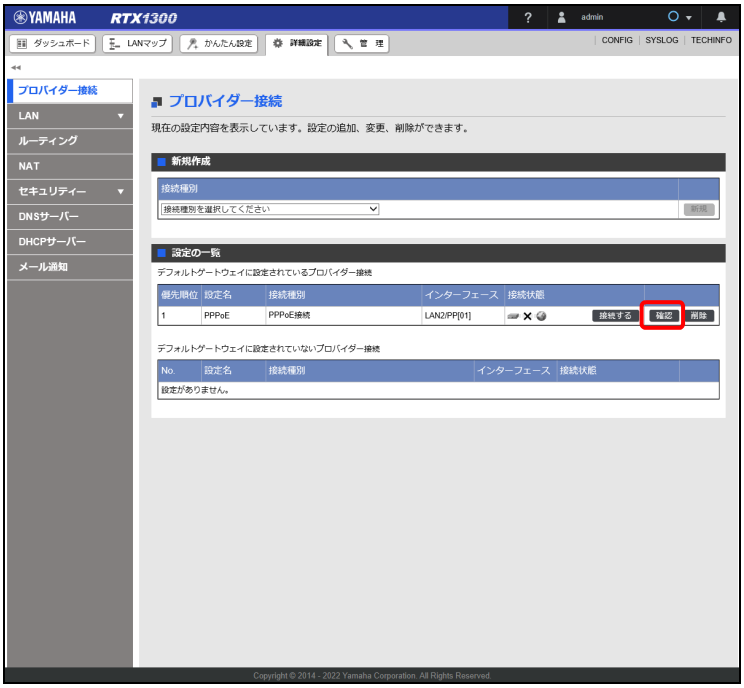
メモ
自動切断は、プロバイダー接続の接続種別で「PPPoE 接続」「モバイル接続（モデム方式）」「モバイル接続（イーサネット方式）」「IPv6 PPPoE 接続」を選択した場合に設定できます。

本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

設定例
切断条件：60 秒間データ通信が無かったら切断する

1. **「詳細設定」タブ ―「プロバイダー接続」を順に選択する。**
「プロバイダー接続」画面が表示されます。

2.「設定の一覧」項目の「PPPoE 接続」の「確認」ボタンをクリックする。



「LAN2/PP[01] 設定内容」画面が表示されます。

3.「基本設定」項目の「設定」ボタンをクリックする。

「基本設定」画面が表示されます。

4.「自動切断」を設定する。

① **自動切断：**
「設定秒数の間データ通信が無かった時に自動切断する」を選択し、設定秒数に「60」を入力します。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

6. **内容を確認し、「設定の確定」ボタンをクリックする。**
設定が反映され、「LAN2/PP[01] 設定内容」画面が表示されます。

14.1.4 発信制限をかける

モバイル接続では、ユーザーが意図しない Windows OS 等の発信により身に覚えのない額が請求される場合があります。また、モバイル接続では、使用するプロバイダーによっては所定の通信量を超えると速度規制がかかる場合があります。このような事態を未然に防ぐ目的で、「詳細設定」の「プロバイダー接続」画面では、事前に設定した金額や通信量に達した時点で発信制限をかける（発信を行えないようにする）設定をすることができます。

メモ

発信制限は、プロバイダー接続の接続種別で「モバイル接続（モデム方式）」「モバイル接続（イーサネット方式）」を選択した場合に設定できます。

本項では「かんたん設定」を使用してモバイルインターフェースにモデム方式のモバイル接続型のプロバイダーが設定されている状態（「4.2 USB 接続型データ通信端末でインターネットに接続する」（39 ページ）の設定が完了している状態）から設定する前提で説明します。

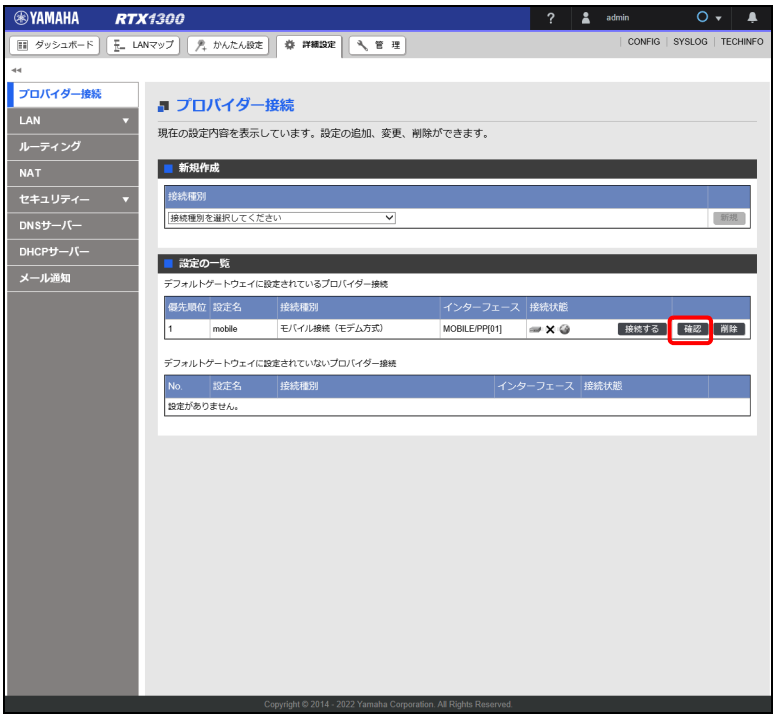
「モバイル接続（モデム方式）」の発信制限を設定する場合

設定例

制限条件：直近 3 日間の累積通信量が 1Gbyte を超えないように、毎日通信量が 300Mbyte に達したら発信制限をかける

1. **「詳細設定」タブ ―「プロバイダー接続」を順に選択する。**
   「プロバイダー接続」画面が表示されます。

2. **「設定の一覧」項目の「モバイル接続」の「確認」ボタンをクリックする。**

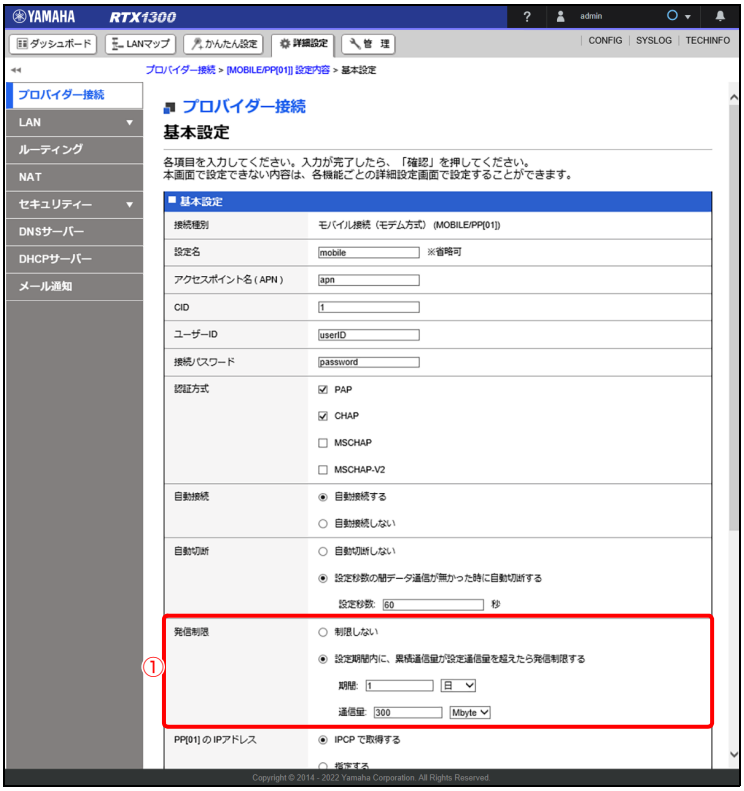


「MOBILE/PP[01] 設定内容」画面が表示されます。

3.「基本設定」項目の「設定」ボタンをクリックする。

「基本設定」画面が表示されます。

4.「発信制限」を設定する。



① **発信制限：**
「設定期間内に、累積通信量が設定通信量を超えたら発信制限する」を選択し、期間に「1」を入力し単位に「日」を選択し、通信量に「300」を入力し単位に「Mbyte」を選択します。

メモ
- 期間は、1 秒から 2592000 秒まで設定できます。
- 通信量は、1byte から 2147483647byte まで設定できます。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

6. **内容を確認し、「設定の確定」ボタンをクリックする。**
設定が反映され、「MOBILE/PP[01] 設定内容」画面が表示されます。

14.1.5 キープアライブ設定を変更する

キープアライブは WAN 回線の障害検知に有効な手段です。「かんたん設定」を使用してプロバイダーを設定した場合でもキープアライブは設定されますが、設定内容は汎用的なものになります。
キープアライブの設定は、使用している回線の状況やネットワーク管理者の要望（回線障害は素早く検知してバックアップ回線に切り替えたい等）に応じて、より適切な設定値に変更しなければならない場合があります。
「詳細設定」の「プロバイダー接続」画面では、キープアライブパケットの送信間隔や回線断と判断する閾値を細かく設定することができます。

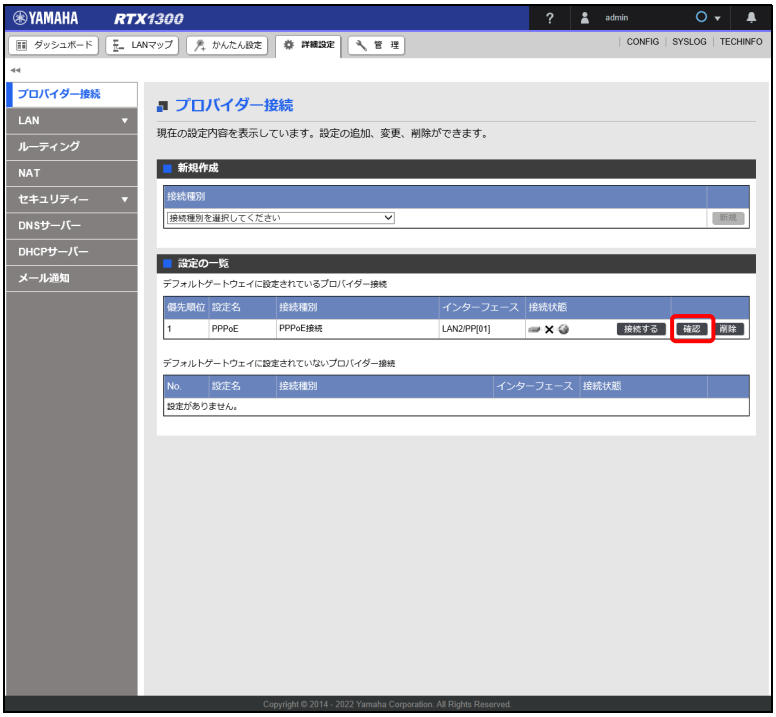
メモ
キープアライブは、プロバイダー接続の接続種別で「PPPoE 接続」「モバイル接続（モデム方式）」「IPv6 PPPoE 接続」を選択した場合に設定できます。

本項では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定する前提で説明します。

設定例
キープアライブパケットの送信間隔：60 秒
応答がないときの再送間隔：10 秒
回線断と判断する基準：6 回連続して応答がない

1. **「詳細設定」タブ ―「プロバイダー接続」を順に選択する。**
「プロバイダー接続」画面が表示されます。

2.「設定の一覧」項目の「PPPoE 接続」の「確認」ボタンをクリックする。

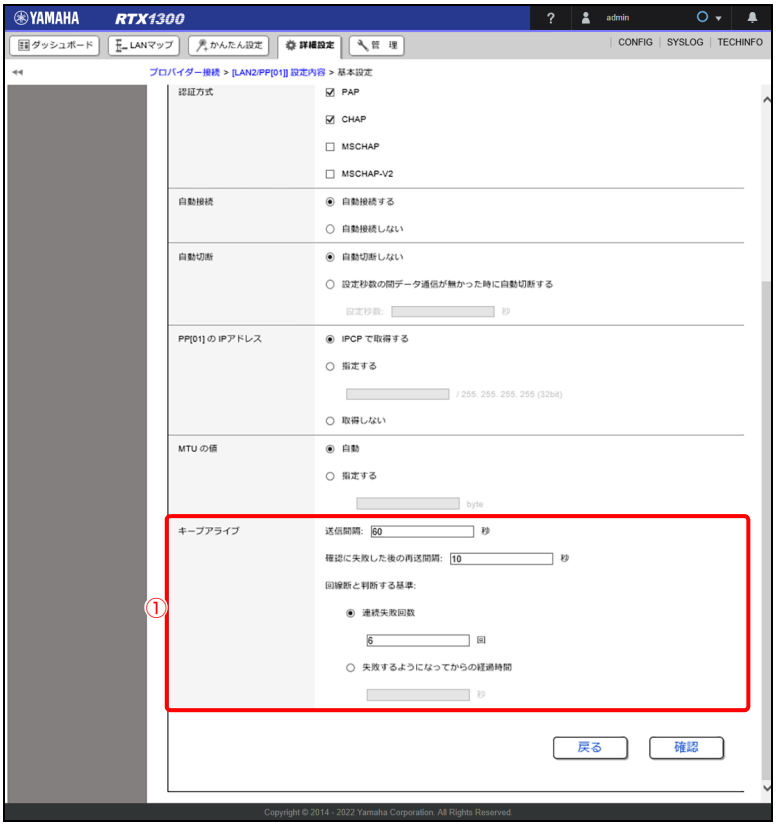


「LAN2/PP[01] 設定内容」画面が表示されます。

3.「基本設定」項目の「設定」ボタンをクリックする。

「基本設定」画面が表示されます。

4. 「キープアライブ」を設定する。



① **キープアライブ**
「送信間隔」に「60」、「確認に失敗した後の再送間隔」に「10」、「回線断と判断する基準」で「連続失敗回数」を選択し「6」を入力します。

注意

回線障害が発生していなくても、回線輻輳時にキープアライブパケットがロスすることがあります。回線断と判断するまでの失敗回数や時間を極端に小さくしてしまうと、これを回線断と誤検知する可能性があることに注意してください。

メモ

- 回線断と判断する基準として、「連続失敗回数」ではなく、「失敗するようになってからの経過時間」を用いることもできます。
- 基準とする経過時間には、送信間隔 +1 秒から 6553500 秒までの秒数を設定できます。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、入力した値とは異なる値が設定されることがあります。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

6. **内容を確認し、「設定の確定」ボタンをクリックする。**
設定が反映され、「LAN2/PP[01] 設定内容」画面が表示されます。

14.2 LAN のアドレスを設定する

本製品の LAN インターフェースのプライマリー IP アドレスとセカンダリー IP アドレスを設定します。IP アドレスは、固定または自動取得（DHCP）に設定できます。

14.2.1 プライマリー IP アドレスを設定する

本製品の LAN1 ～ LAN8 のプライマリー IP アドレスを固定で設定します。

注意

工場出荷状態では、LAN4 ～ LAN8 にアドレスを設定しても使用できません。「14.4 フレキシブル LAN/WAN ポートを設定する」（327 ページ）を参照し、インターフェースにポートを割り当ててください。

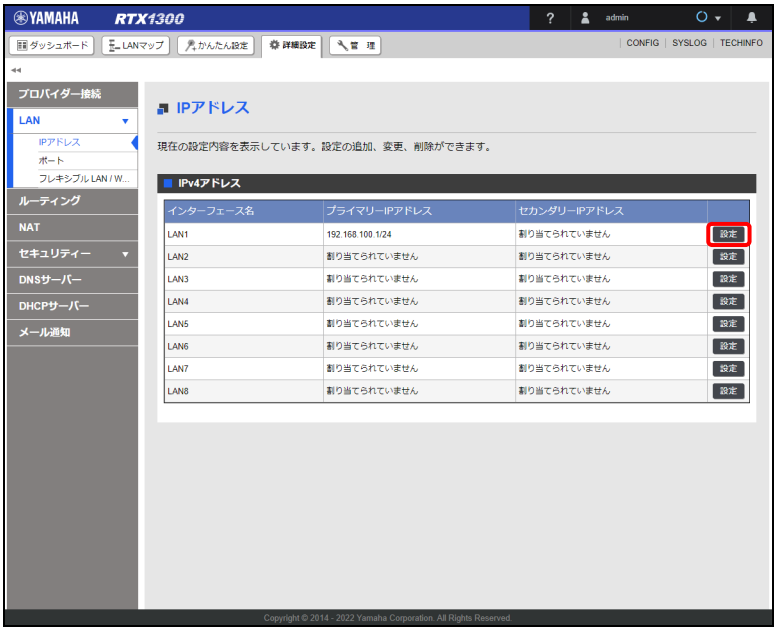
メモ

LAN1 インターフェースに関して、「かんたん設定」を使用してプロバイダー接続の設定が完了している場合は、プロバイダー接続の設定と同時に IP マスカレードも自動的に設定されるため、本節の操作は不要になります。

設定例

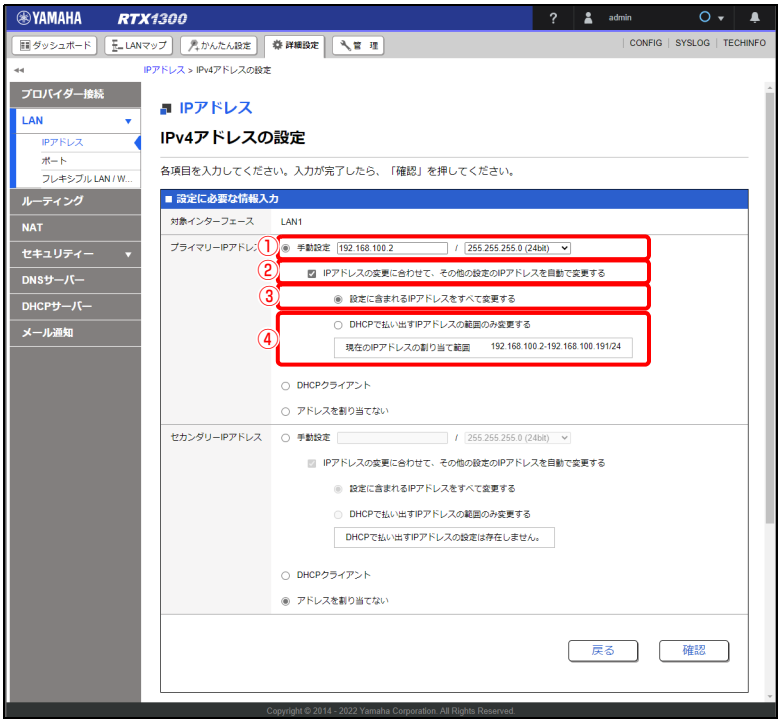
設定するインターフェース：LAN1

1. **「詳細設定」タブー「LAN」ー「IP アドレス」を順に選択する。**
   「IP アドレス」画面が表示されます。
2. **「LAN1」の「設定」ボタンをクリックする。**



「IPv4 アドレスの設定」画面が表示されます。

3. LAN1 の IP アドレスを設定する。



① アドレス入力欄：
「手動設定」を選択し、新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0(2bit)」から「255.255.255.252(30bit)」までの中から選択します。

② IP アドレスの変更に合わせて、その他の設定の IP アドレスを自動で変更する：
選択すると LAN インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。
選択しないときは、IP アドレスの変更後に必要に応じて手動で設定を行ってください。

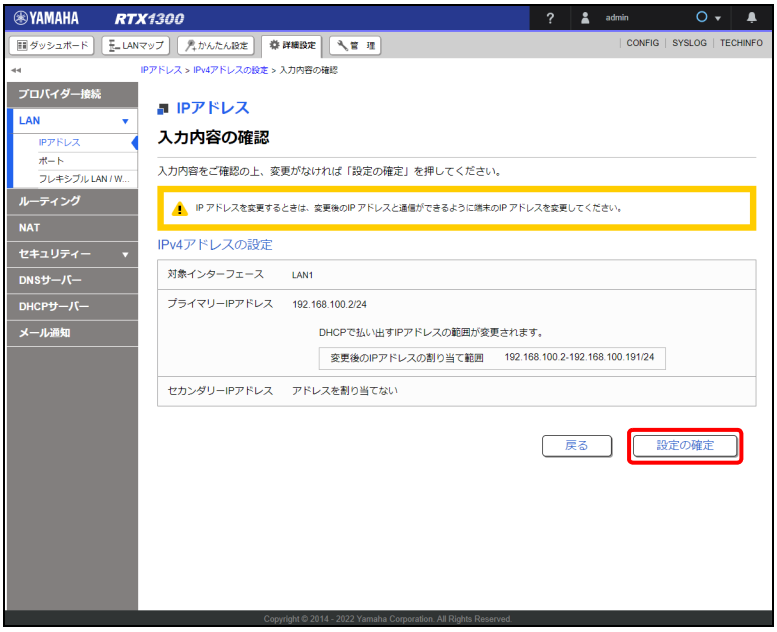
③ 設定に含まれる IP アドレスをすべて変更する：
選択すると、新しい IP アドレスに合わせて各種設定の IP アドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

- **静的 IP フィルター（始点 IP アドレス、終点 IP アドレス）**
- **動的 IP フィルター（始点 IP アドレス、終点 IP アドレス）**
- **NAT ディスクリプター内側アドレス**
- **NAT ディスクリプター静的 NAT（内側アドレス）**
- **NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）**
- **NAT ディスクリプター静的 IP マスカレード（内側アドレス）**
- **DHCP で払い出す IP アドレス**
- **IP キープアライブ（始点 IP アドレス）**
- **トンネルインターフェース端点 IP アドレス（ローカル IP アドレス）**
- **IPsec 自分側 IP アドレス**

④ DHCP で払い出す IP アドレスの範囲のみ変更する：
選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が変更され、「LAN1 アドレスの変更」画面が表示されます。「LAN1 アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

14.2.2 セカンダリー IP アドレスを設定する

本製品の LAN1 ～ LAN8 のセカンダリー IP アドレスを固定で設定します。

注意

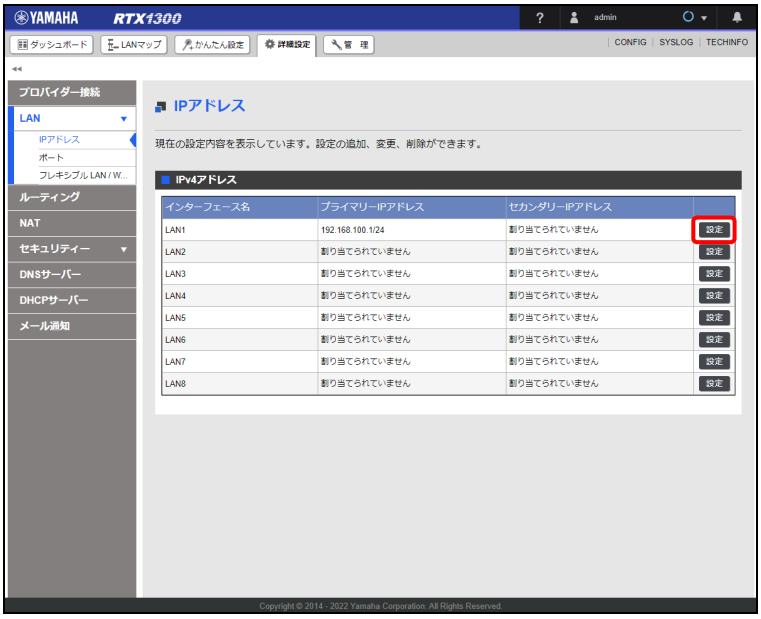
工場出荷状態では、LAN4 ～ LAN8 にアドレスを設定しても使用できません。「14.4 フレキシブル LAN/WAN ポートを設定する」（327 ページ）を参照し、インターフェースにポートを割り当ててください。

設定例

設定するインターフェース：LAN1

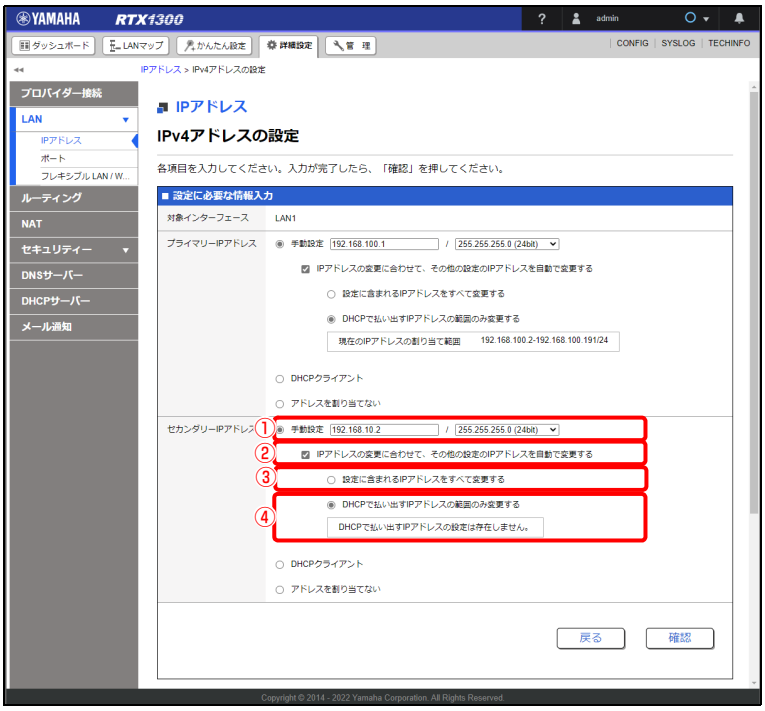
1. **「詳細設定」タブー「LAN」ー「IP アドレス」を順に選択する。**
   「IP アドレス」画面が表示されます。

2. 「LAN1」の「設定」ボタンをクリックする。



「IPv4 アドレスの設定」画面が表示されます。

3. LAN1 のセカンダリー IP アドレスを設定する。



① アドレス入力欄：
「手動設定」を選択し、新しく設定する IPv4 アドレスを入力します。ネットマスクは、「192.0.0.0(2bit)」から「255.255.255.252(30bit)」までの中から選択します。

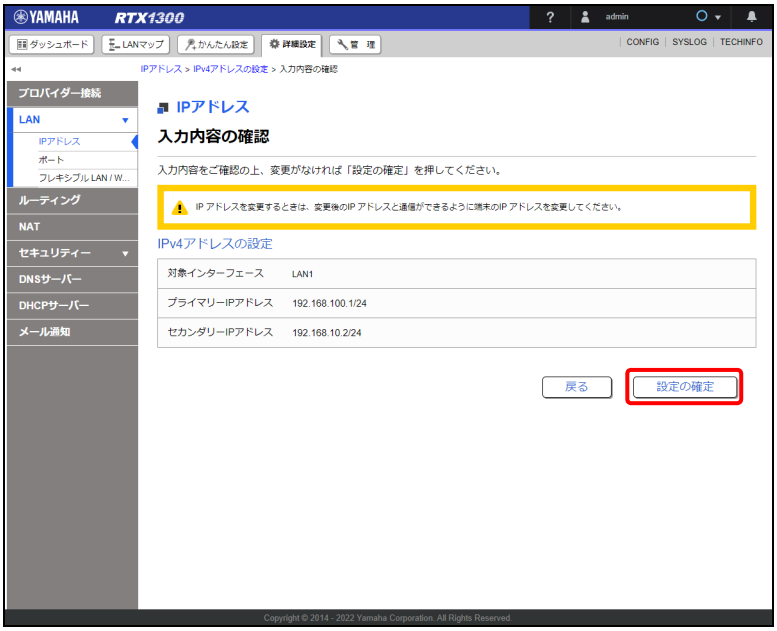
② IP アドレスの変更に合わせて、その他の設定の IP アドレスを自動で変更する：
選択すると LAN インターフェースの IP アドレスの設定変更に合わせて、その他の設定に含まれる IP アドレスのパラメーターを自動的に変換します。
選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

③ 設定に含まれる IP アドレスをすべて変更する：
選択すると、新しい IP アドレスに合わせて各種設定の IP アドレス設定を自動的に変更します。対象となる設定は以下のとおりです。

- 静的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- 動的 IP フィルター（始点 IP アドレス、終点 IP アドレス）
- NAT ディスクリプター内側アドレス
- NAT ディスクリプター静的 NAT（内側アドレス）
- NAT ディスクリプター変換ルールに該当しないパケットの処理（転送先端末のアドレス）
- NAT ディスクリプター静的 IP マスカレード（内側アドレス）
- DHCP で払い出す IP アドレス
- IP キープアライブ（始点 IP アドレス）
- トンネルインターフェース端点 IP アドレス（ローカル IP アドレス）
- IPsec 自分側 IP アドレス

④ DHCP で払い出す IP アドレスの範囲のみ変更する：
選択すると、新しい IP アドレスに合わせて DHCP の設定を自動的に変更します。

4. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。
5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN1 アドレスの変更」画面が表示されます。「LAN1 アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

14.2.3 固定ではなく DHCP で設定する

本製品の LAN1 ～ LAN8 のプライマリー IP アドレスまたはセカンダリー IP アドレスを DHCP で取得します。

注意

工場出荷状態では、LAN4 ～ LAN8 にアドレスを設定しても使用できません。「14.4 フレキシブル LAN/WAN ポートを設定する」（327 ページ）を参照し、インターフェースにポートを割り当ててください。

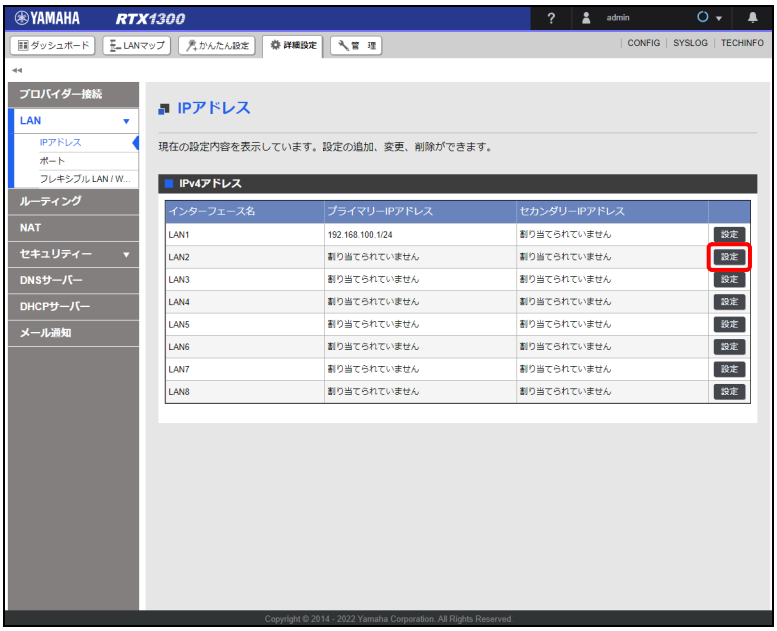
メモ

プライマリー IP アドレス、セカンダリー IP アドレスの両方を「DHCP クライアント」に設定することはできません。

設定例

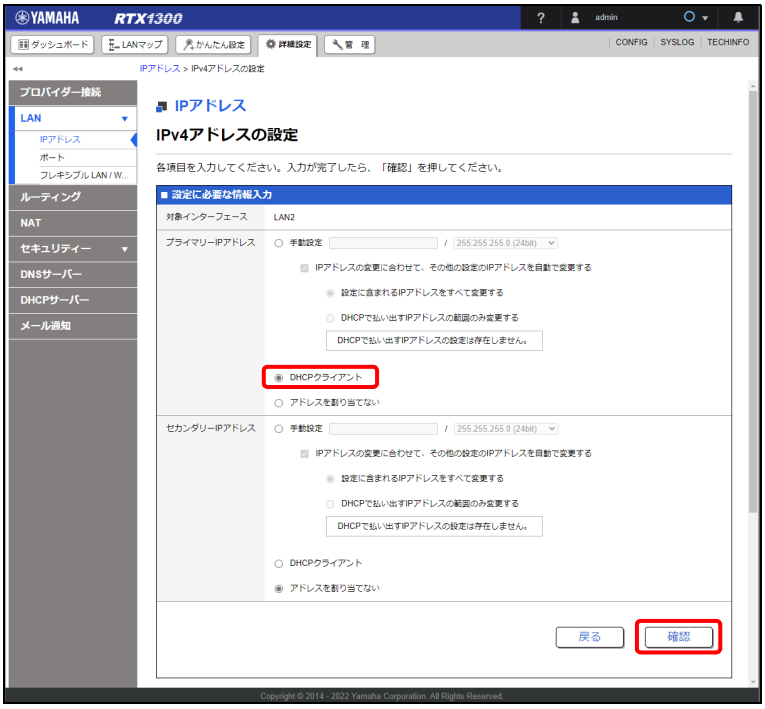
設定するインターフェース：LAN2
DHCP で取得する IP アドレス：プライマリー IP アドレス

1. **「詳細設定」タブー「LAN」ー「IP アドレス」を順に選択する。**
   「IP アドレス」画面が表示されます。
2. **「LAN2」の「設定」ボタンをクリックする。**



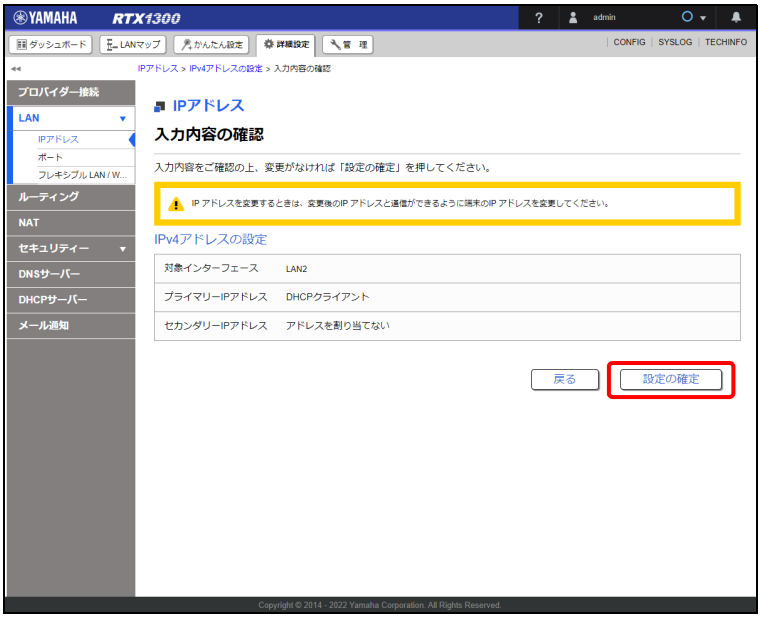
「IPv4 アドレスの設定」画面が表示されます。

3. プライマリー IP アドレスの「DHCP クライアント」を選択し、「確認」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

4. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が変更され、「LAN2 アドレスの変更」画面が表示されます。「LAN2 アドレスの変更」画面の指示にしたがって、Web GUI に再ログインしてください。

14.3 ポートの動作モードを設定する

本製品の LAN インターフェースのポートの動作モードを設定します。

設定例

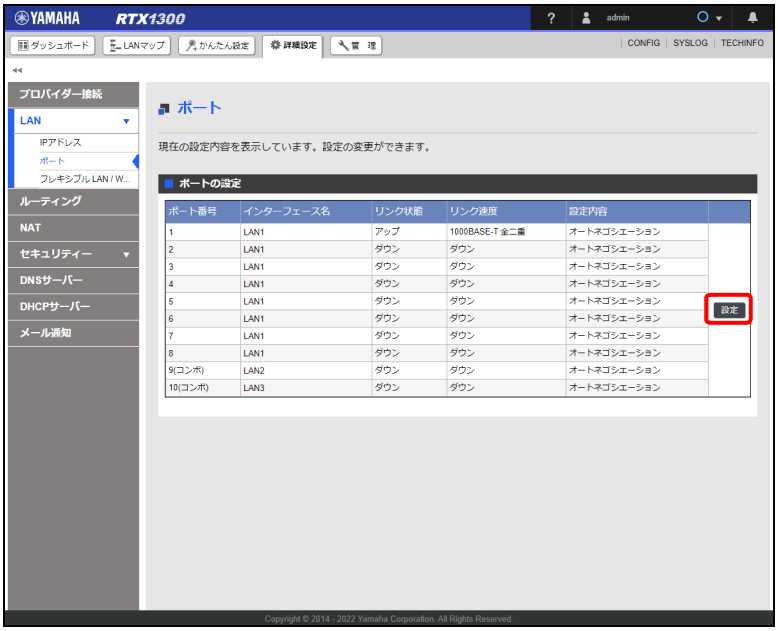
設定するポート番号：1
設定内容：1000BASE-T 全二重

注意

・ ポート 9 とポート 10 のリンクスピードは 10M に設定できません。
・ SFP + ポート のリンクスピードは設定できません。

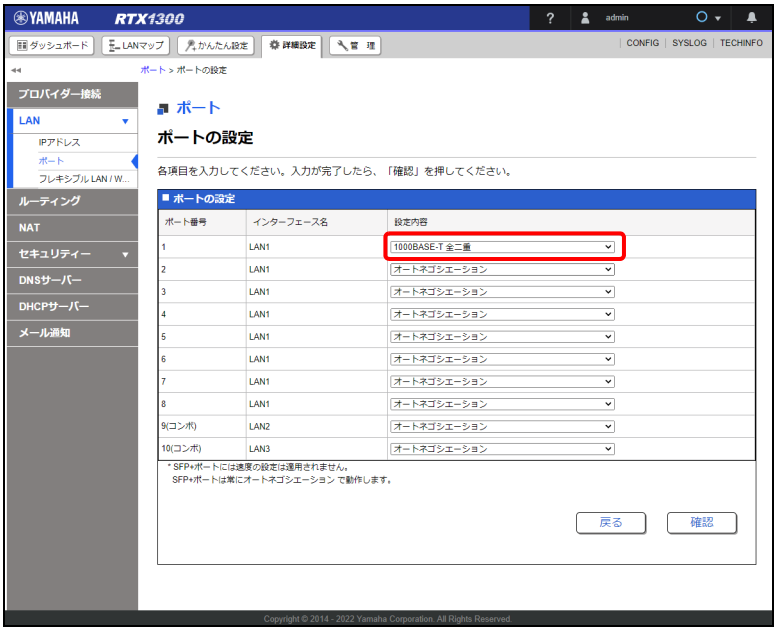
1. **「詳細設定」タブ ― 「LAN」 ― 「ポート」を順に選択する。**
   「ポート」画面が表示されます。

2. **「設定」ボタンをクリックする。**



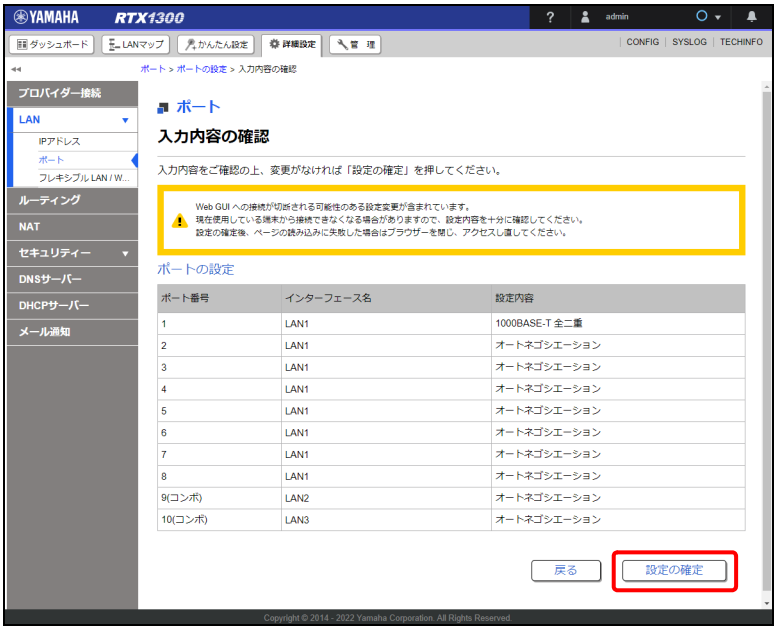
「ポートの設定」画面が表示されます。

3. **ポートの動作モードを設定する。**
   ポート 1 のプルダウンメニューから「1000BASE-T 全二重」を設定します。



4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「ポート」画面が表示されます。

14.4 フレキシブル LAN/WAN ポートを設定する

フレキシブル LAN/WAN ポートとは、従来固定されていた LAN インターフェースの物理ポート構成を、ユーザーがフレキシブルに変更できる機能です。詳しくは、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/flexible-lan/index.html

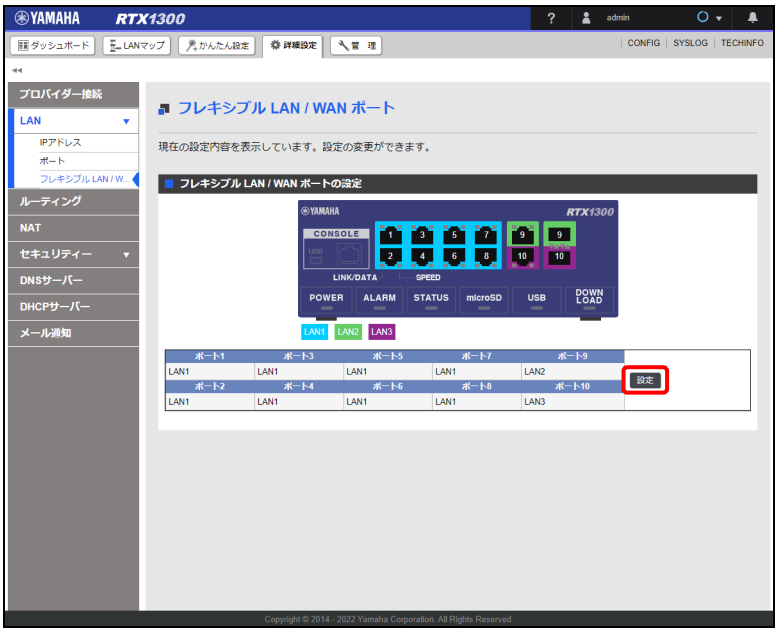
工場出荷状態では、各ポートが次のように割り当てられています。
ポート 1 ～ 8 の割り当て：LAN1
ポート 9 の割り当て：LAN2
ポート 10 の割り当て：LAN3

ポートと LAN インターフェースの構成を、工場出荷状態から変更する場合を例に説明します。

注意
いずれかのポートを LAN1 に割り当てる必要があります。

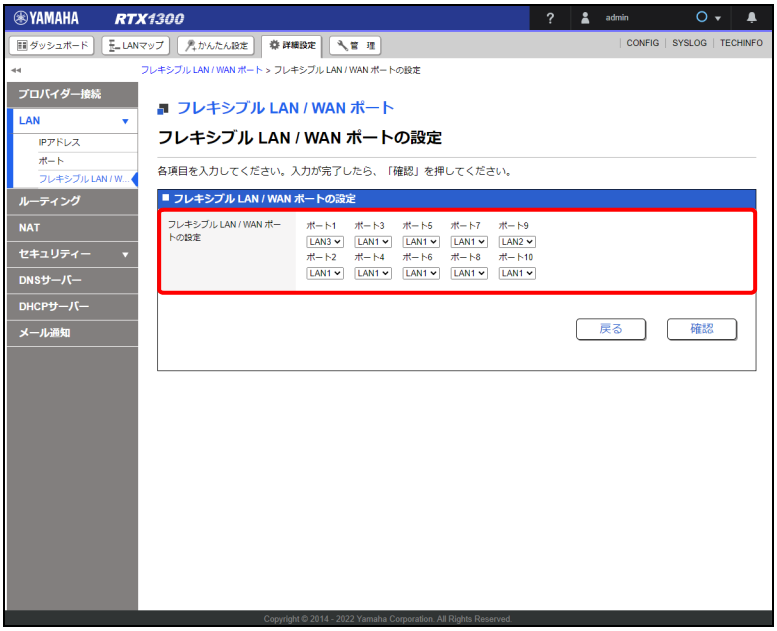
設定例
ポート 1 の割り当て：LAN3
ポート 2 ～ 8、10 の割り当て：LAN1
ポート 9 の割り当て：LAN2

1. **「詳細設定」タブ ―「LAN」―「フレキシブル LAN/WAN ポート」を順に選択する。**
   「フレキシブル LAN/WAN ポート」画面が表示されます。
2. **「フレキシブル LAN /WAN ポートの設定」項目の「設定」ボタンをクリックする。**



「フレキシブル LAN /WAN ポートの設定」画面が表示されます。

3. **フレキシブル LAN /WAN ポートを設定する。**
   各ポートの LAN インターフェースをプルダウンメニューから設定します。



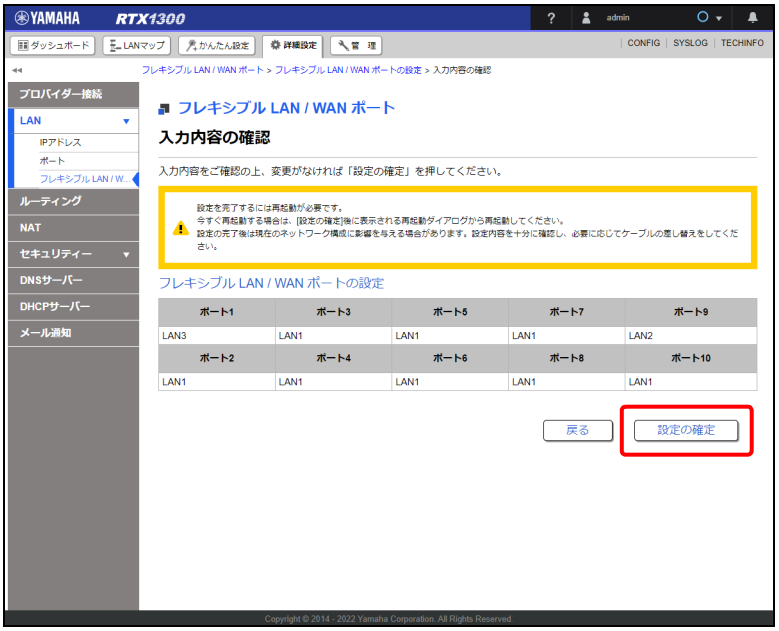
① **ポート 1：**
「LAN3」を選択します。

② **ポート 9：**
「LAN2」を設定します。

③ **ポート 10：**
「LAN1」を設定します。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。

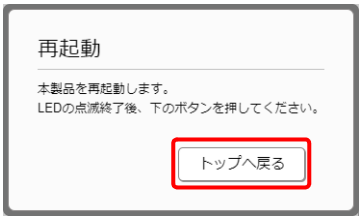


「再起動」ダイアログが表示されます。
すぐに再起動をする場合は、「再起動」ボタンをクリックしてください。

注意

本設定を設定しても、再起動するまで動作に反映されません。

6. 本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

14.5 グローバル IP アドレスを複数の端末でシェアする

グローバル IP アドレスとプライベート IP アドレスを透過的に相互変換することで、一つのグローバル IP アドレスを複数の端末でシェアすることができます（IP マスカレード）。TCP/UDP のポート番号まで動的に変換されるため、一つのグローバル IP アドレスで複数の端末から同時にインターネット接続することが可能です。

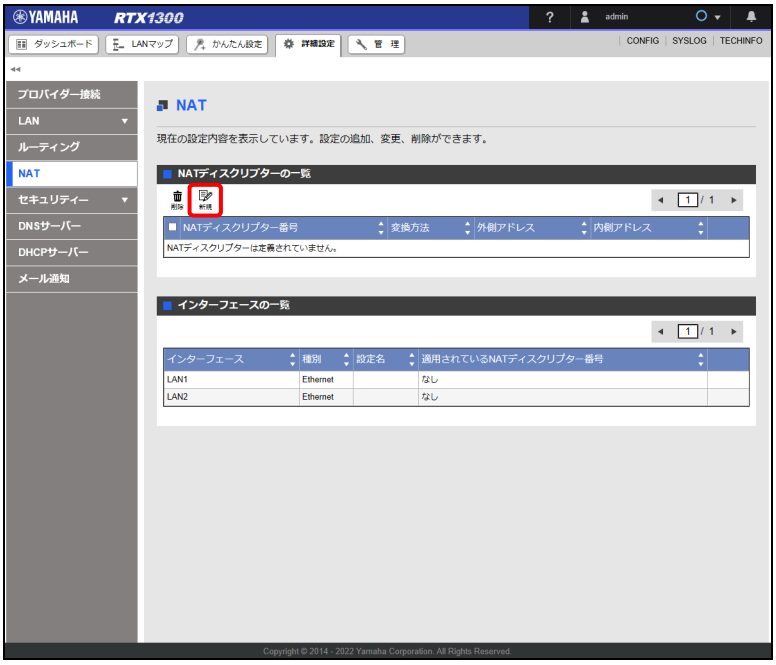
メモ

「かんたん設定」を使用してプロバイダー接続の設定が完了している場合は、プロバイダー接続の設定と同時に IP マスカレードも自動的に設定されるため、本節の操作は不要になります。

設定例

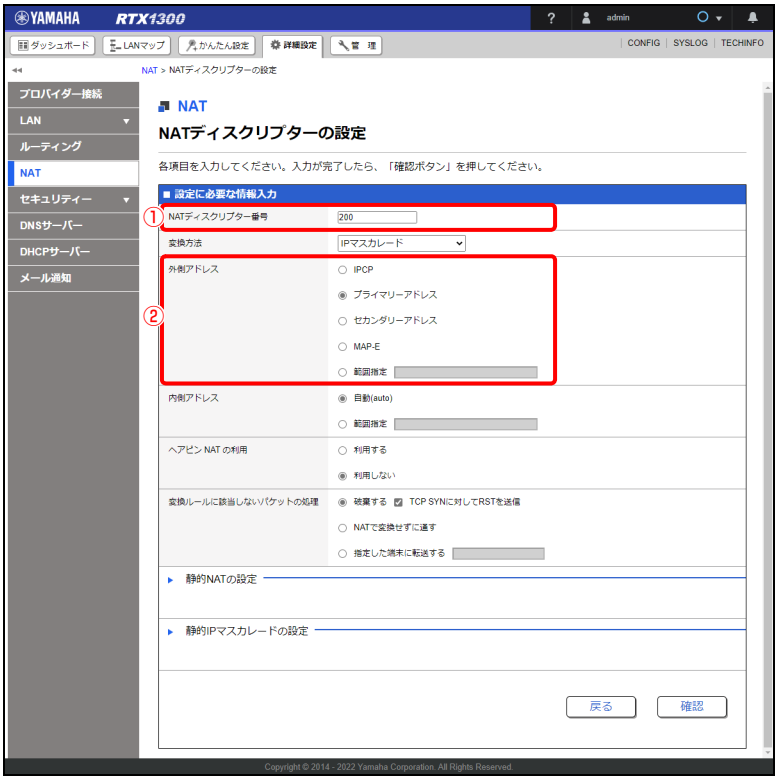
IP マスカレードを設定するインターフェース：LAN2
NAT ディスクリプター番号：200
外側アドレス：プライマリーアドレス

1. **「詳細設定」タブ ― 「NAT」を順に選択する。**
   「NAT」画面が表示されます。
2. **「NAT ディスクリプターの一覧」項目の「 」ボタンをクリックする。**



「NAT ディスクリプターの設定」画面が表示されます。

3. IP マスカレードを設定する。

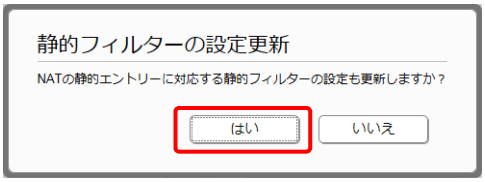


① **NAT ディスクリプター番号：**
「200」を入力します。

② **外側アドレス：**
「プライマリーアドレス」を選択します。

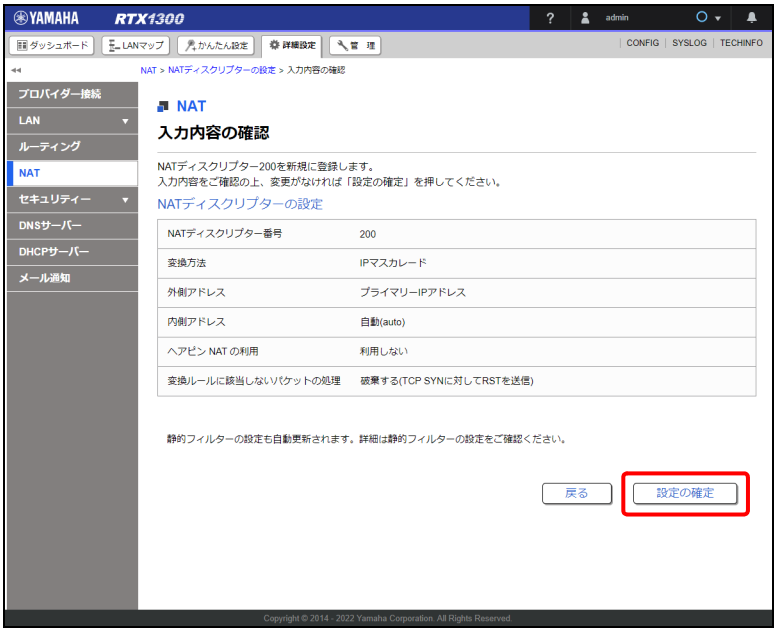
4. **「確認」ボタンをクリックする。**
「静的フィルターの設定更新」ダイアログが表示されます。

5. **「はい」ボタンをクリックする。**



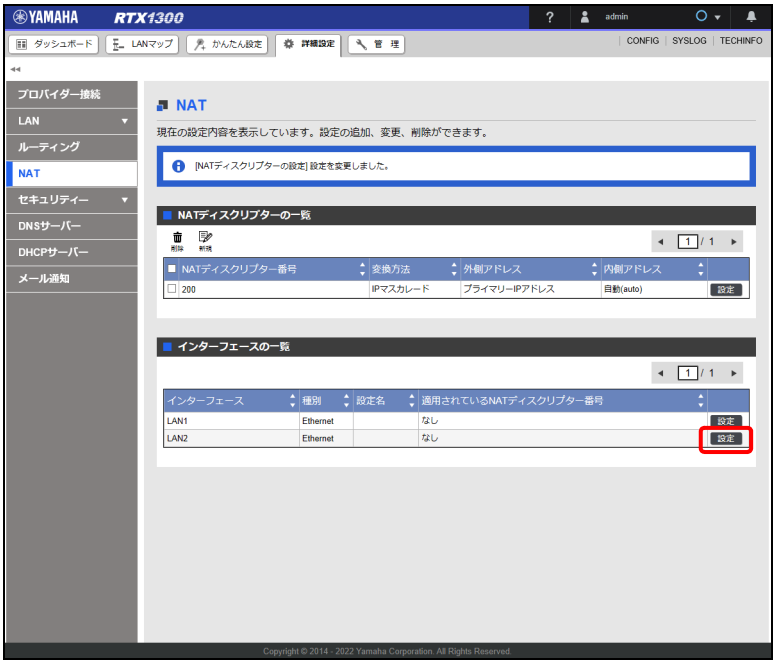
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。



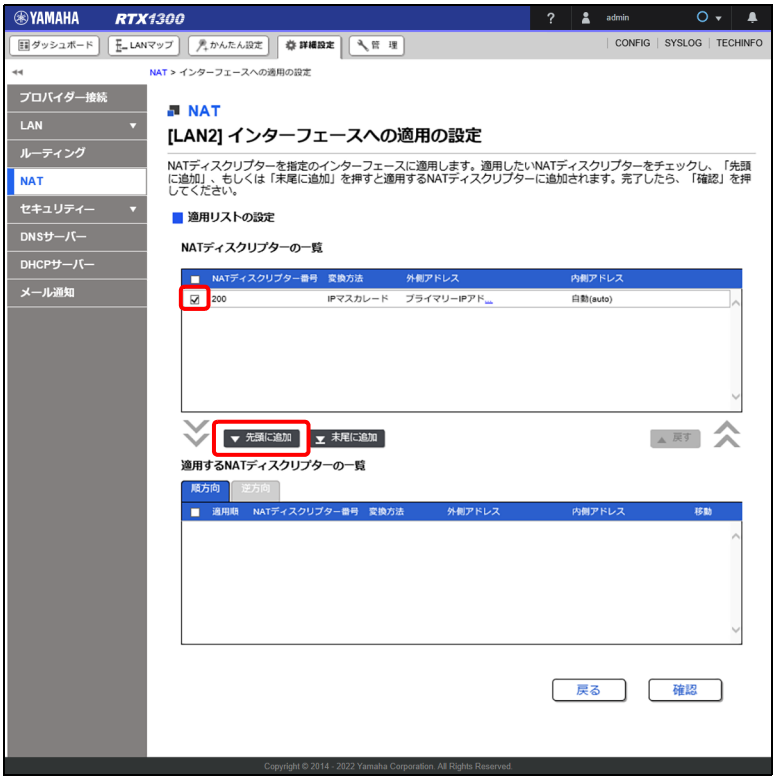
設定が反映され、「NAT」画面が表示されます。

7. 「インターフェースの一覧」項目の「LAN2」の「設定」ボタンをクリックする。



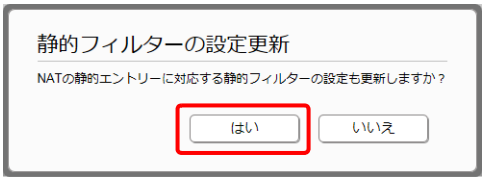
「インターフェースへの適用の設定」画面が表示されます。

8. 「NAT ディスクリプターの一覧」項目のチェックボックスにチェックを入れてから「先頭に追加」ボタンをクリックし、作成した NAT ディスクリプターを「適用する NAT ディスクリプターの一覧」項目の先頭に移動させる。



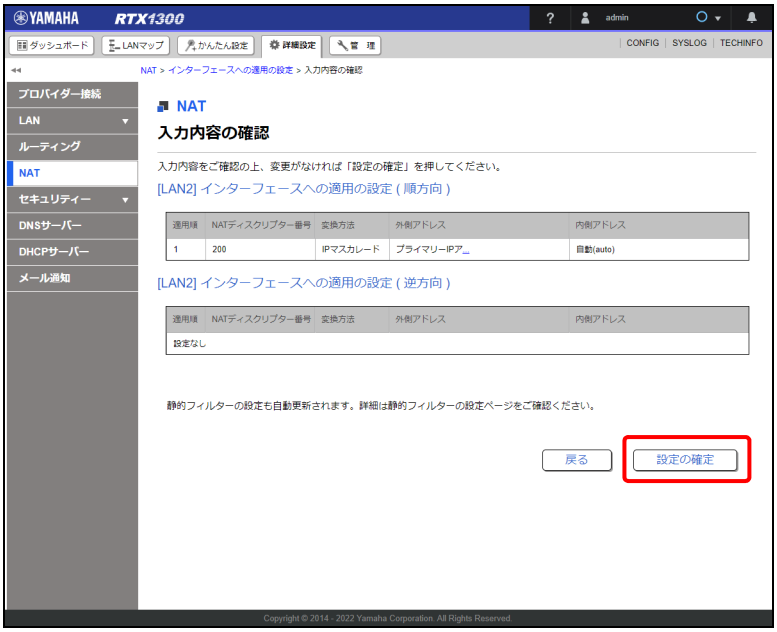
9. 「確認」ボタンをクリックする。
「静的フィルターの設定更新」画面が表示されます。

10.「はい」ボタンをクリックする。



「入力内容の確認」画面が表示されます。

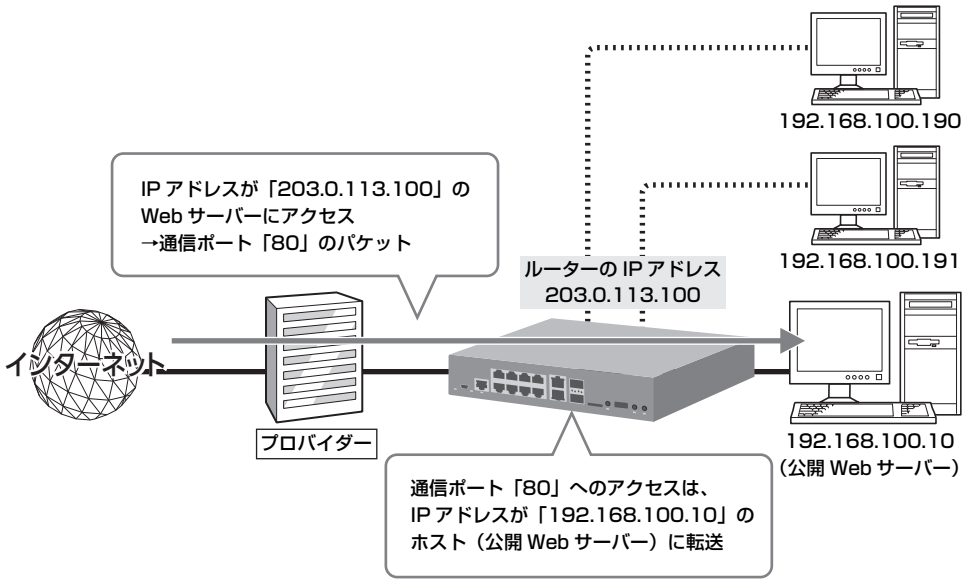
11.内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「NAT」画面が表示されます。

14.6 外部にサーバーを公開する

インターネットへサーバーを公開したい場合は、公開したいサーバーに固定プライベート IP アドレスを設定してから、通信ポートを開放することで、インターネットからサーバーにアクセスできるようになります。サーバーを公開するためには、次の設定が必要です。



サーバーの設定

・ サーバーに固定 IP アドレスを設定する。
・ Web や FTP など、公開するサービスに合わせてファイルサーバーソフトの設定を変更する。

ルーターの設定

通信ポートを開放し、インターネットからの開放した通信ポートへのアクセスを、サーバーに転送する設定を行う（336 ページ）。

本節では「かんたん設定」を使用して LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されている状態（「4.1.2 「PPPoE 接続」の場合」（31 ページ）の設定が完了している状態）から設定するという前提で説明します。

注意

インターネットへサーバーを公開するときは、データを保全するために十分なセキュリティー設定を行ってください。セキュリティー設定が不十分な場合は、LAN に接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などに遭う可能性があります。

メモ

ネットボランチ DNS サービスを利用することで、固定グローバル IP アドレスが割り当てられない接続サービスでも、サーバーを公開して運用できます。ネットボランチ DNS サービスの設定について詳しくは、「第 7 章 ネットボランチ DNS サービスを利用する」（65 ページ）をご覧ください。

14.6.1 ポートを開放する

サーバーの通信ポートを開放し、インターネットからの開放した通信ポートへのアクセスをサーバーに転送する設定を行います。インターネットへ Web サーバーを公開する場合を例に説明します。

メモ

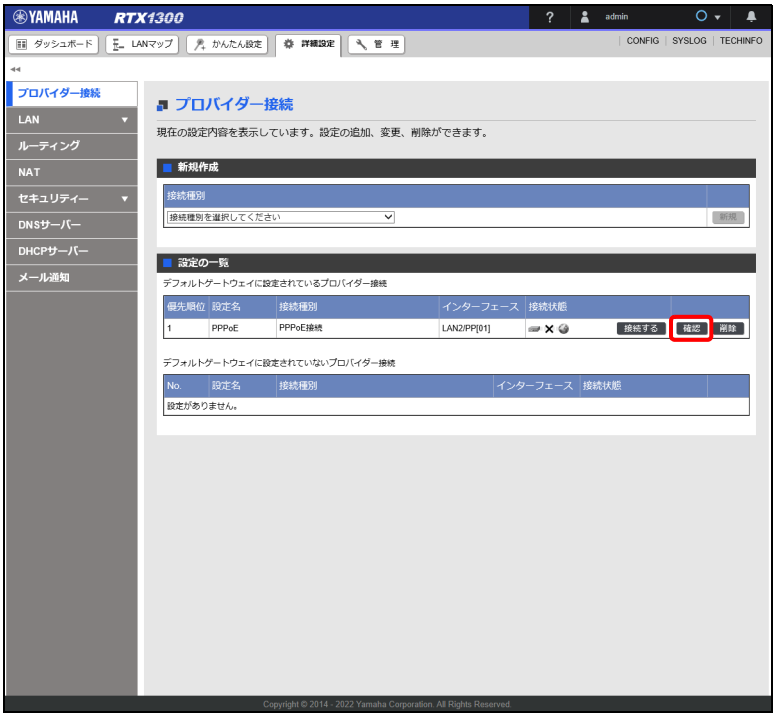
ポート開放の設定は、「PPPoE 接続」「DHCP、または固定 IP アドレスによる接続」「モバイル接続（モデム方式）」「モバイル接続（イーサネット方式）」で有効な項目です。

設定例

Web サーバーのプライベート IP アドレス：192.168.100.10
アプリケーション：HTTP
プロトコル：tcp
ポート番号：80

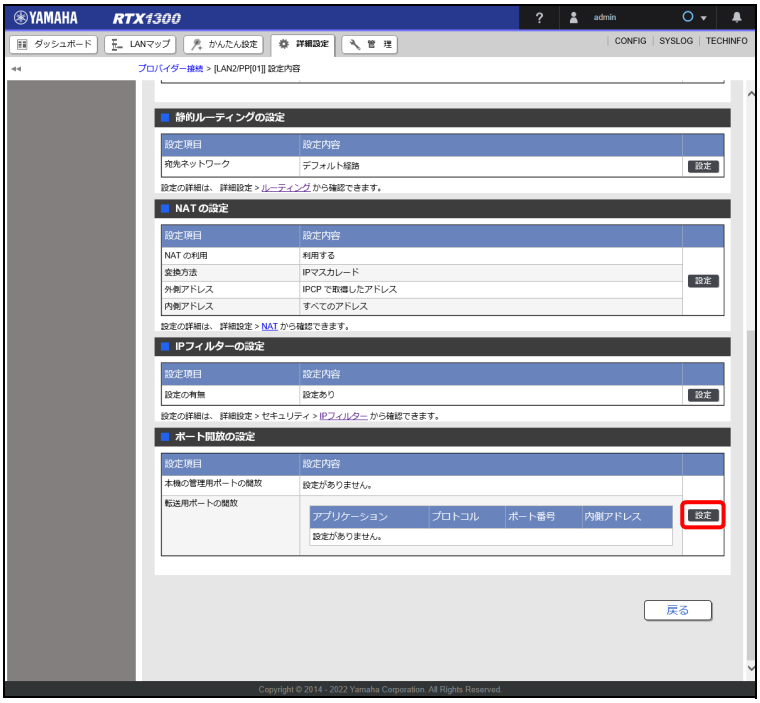
1. **「詳細設定」タブ ―「プロバイダー接続」を順に選択する。**
   「プロバイダー接続」画面が表示されます。

2. **「設定の一覧」項目の「PPPoE 接続」の「確認」ボタンをクリックする。**



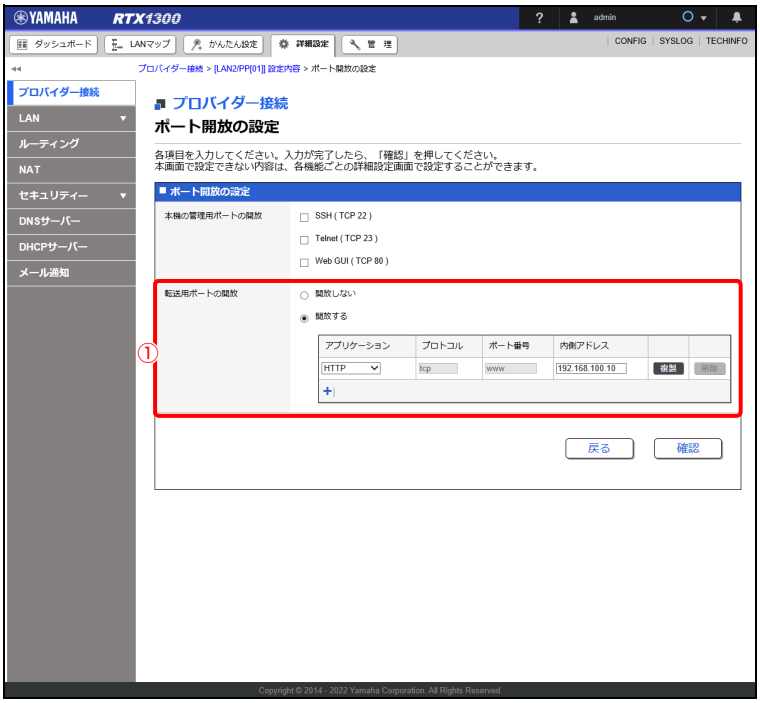
「LAN2/PP[01] 設定内容」画面が表示されます。

3.「ポート開放の設定」項目の「設定」ボタンをクリックする。



「ポート開放の設定」画面が表示されます。

4.「ポート開放の設定」を行う。



① **転送用ポートの開放：**

「開放する」を選択し、「アプリケーション」に「HTTP」を選択します。「内側アドレス」には Web サーバーの IP アドレス「192.168.100.10」を入力します。

「アプリケーション」に「HTTP」を選択すると、自動で「プロトコル」に「tcp」、「ポート番号」に「www」が設定されます。

注意

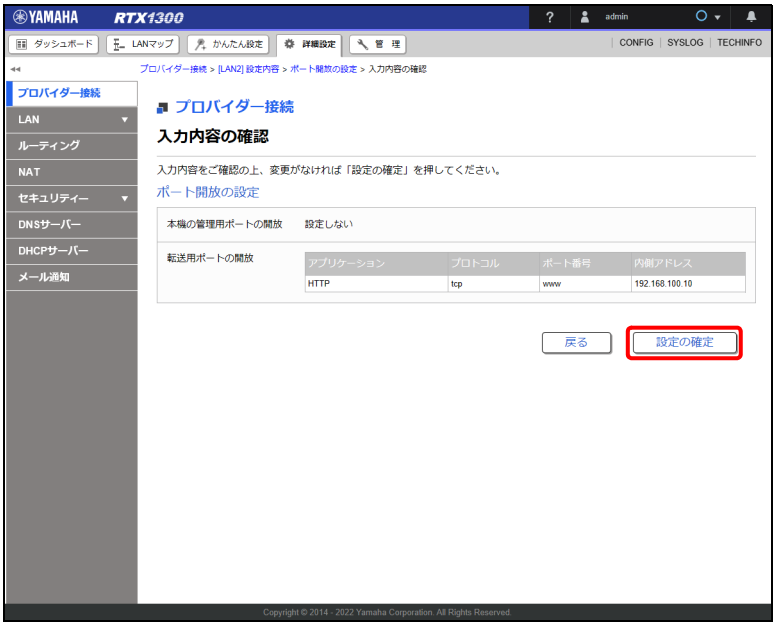
「転送用ポートの開放」で、同一のプロトコルとポート番号の組み合わせを、複数指定することはできません。また、「本機の管理用ポートの開放」のプロトコルとポート番号の組み合わせと重複させることもできません。

メモ

・「転送用ポートの開放」の「内側アドレス」は、インターネット側から本製品の WAN 側の IP アドレスにアクセスした際に転送する宛先となるホストの IP アドレスを設定します。
・選択したアプリケーションの種類に応じて、プロトコルとポート番号が自動で設定されます。選択肢に用意されているアプリケーションでも開放したいポートが異なる場合（例えば、HTTP でも TCP/80 ではなく TCP/8080 を開放したい場合）など、任意の設定を行う場合は、「アプリケーション」に「手動入力」を選択し、「プロトコル」と「ポート番号」を手動で設定してください。

5. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

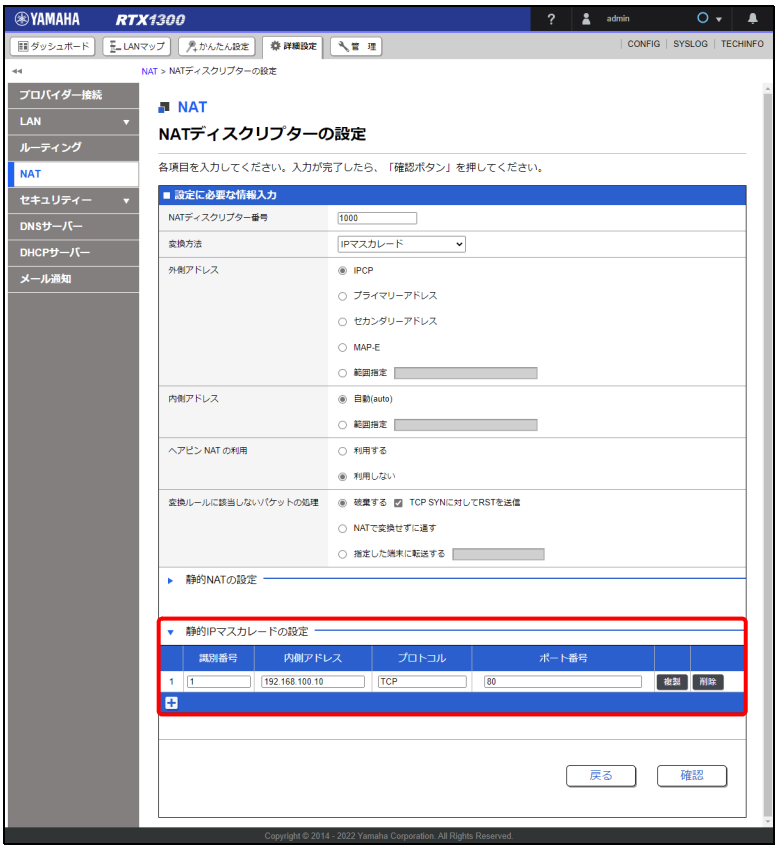
6. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「LAN2/PP[01] 設定内容」画面が表示されます。

メモ

ポートの開放は、「詳細設定」タブ -「NAT」の「静的 IP マスカレードの設定」項目から設定することもできます。



14.6.2 サーバーの公開先を限定する

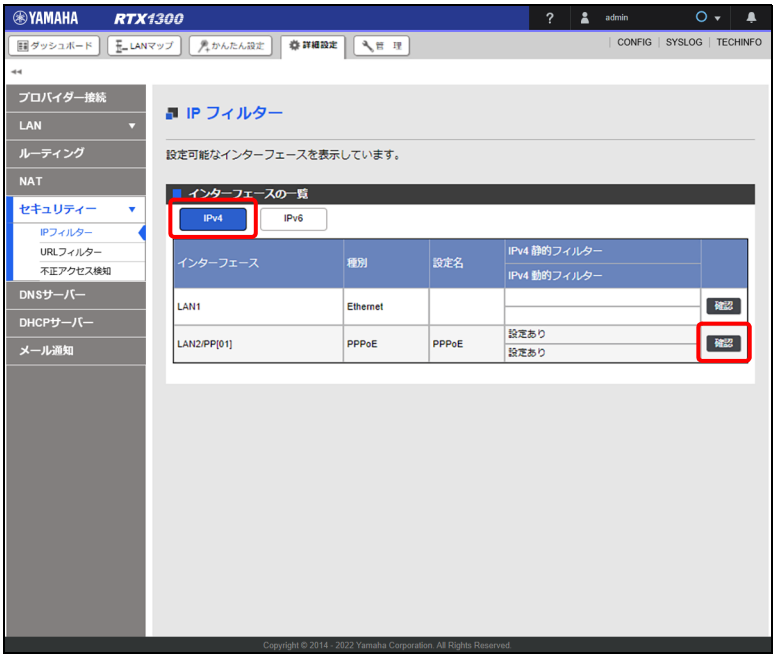
サーバーの公開先を限定します。「14.6.1 ポートを開放する」で設定した公開サーバーのアドレスに対して、下記のネットワークからのみアクセスできるようにする場合を例に説明します。

設定例

公開先：203.0.113.0/24

1. **「詳細設定」タブ ―「セキュリティー」―「IP フィルター」を順に選択する。**
   「IP フィルター」画面が表示されます。

2. 「IPv4」タブを選択し、「インターフェースの一覧」項目の「LAN2/PP[01]」インターフェースの「確認」ボタンをクリックする。



「適用されている IPv4 フィルターの一覧」画面が表示されます。

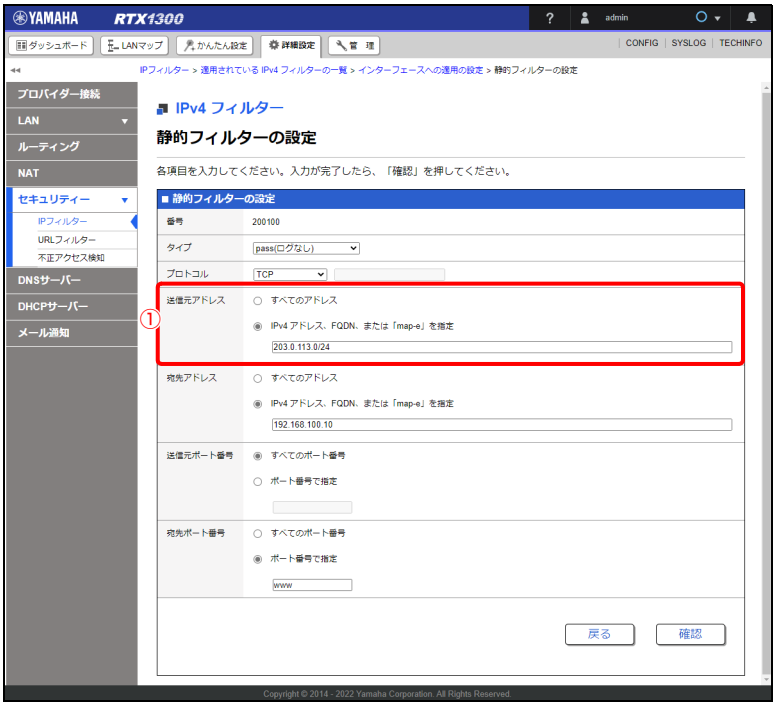
3. 「静的フィルター」項目の「 」ボタンをクリックする。

「[LAN2/PP[01]] インターフェースへの適用の設定」画面が表示されます。

4.「適用フィルター」項目で、以下の内容に合致するフィルターの「設定」ボタンをクリックする。
- タイプ：pass
- プロトコル：TCP
- 宛先アドレス：192.168.100.10
- 宛先ポート番号：www

「静的フィルターの設定」画面が表示されます。

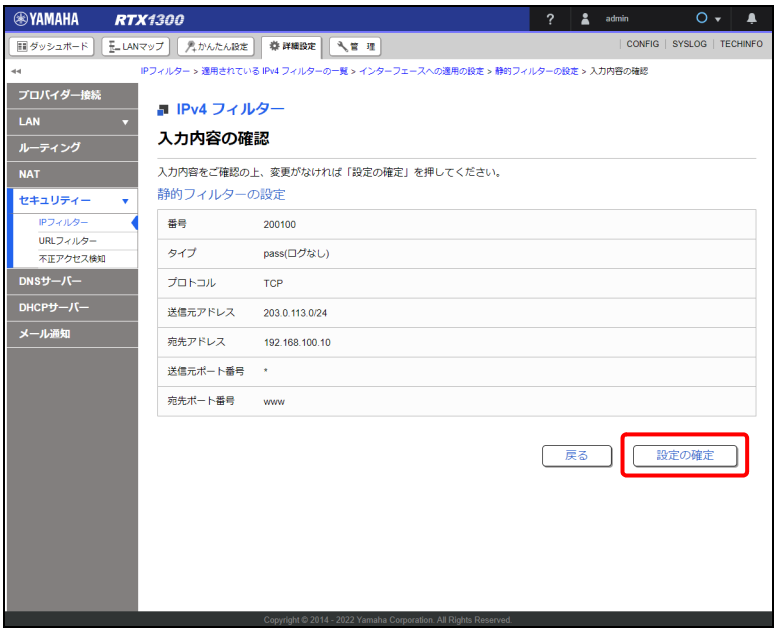
5. **静的フィルターを編集する。**



① 送信元アドレス：
「203.0.113.0/24」を入力します。

6. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

7. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「インターフェースへの適用の設定」画面が表示されます。

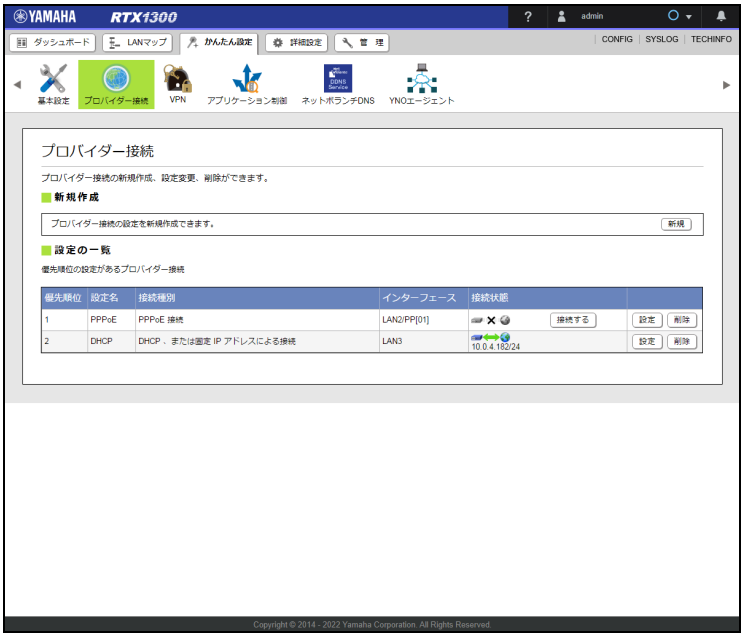
14.7 複数のプロバイダーを使用する

複数のプロバイダーを設定することで、端末ごとに接続プロバイダーを使い分けたり、障害時用のバックアップ回線を用意したりすることができます。

14.7.1 複数のプロバイダーを設定する

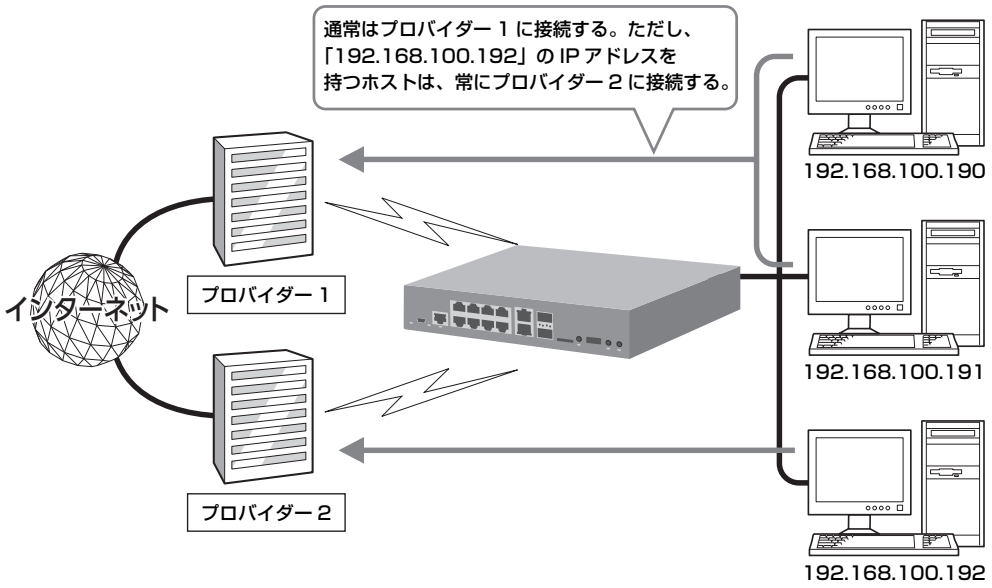
複数のプロバイダーを用途に応じて使い分ける設定を行うためには、事前に「かんたん設定」の「プロバイダー接続」画面から複数のプロバイダーの設定を済ませておく必要があります。プロバイダーの設定方法について詳しくは、「第 4 章 IPv4 アドレスでインターネットに接続する」（28 ページ）をご覧ください。

14.7.2 ～ 14.7.4 の設定方法の説明では、LAN2 インターフェースに PPPoE 接続型のプロバイダー、LAN3 インターフェースに DHCP 接続型のプロバイダーが設定されている状態（下記画像の状態）から設定する前提で説明します。



14.7.2 端末ごとにプロバイダーを使い分ける

端末の IP アドレスと使用する接続プロバイダーの関連づけを行い、端末ごとに接続するプロバイダーを使い分けます。
この場合は、LAN 上のすべての端末の IP アドレスをあらかじめ固定する必要があります。詳しくは、ネットワークの管理者にご相談ください。



設定例

ゲートウェイ 1

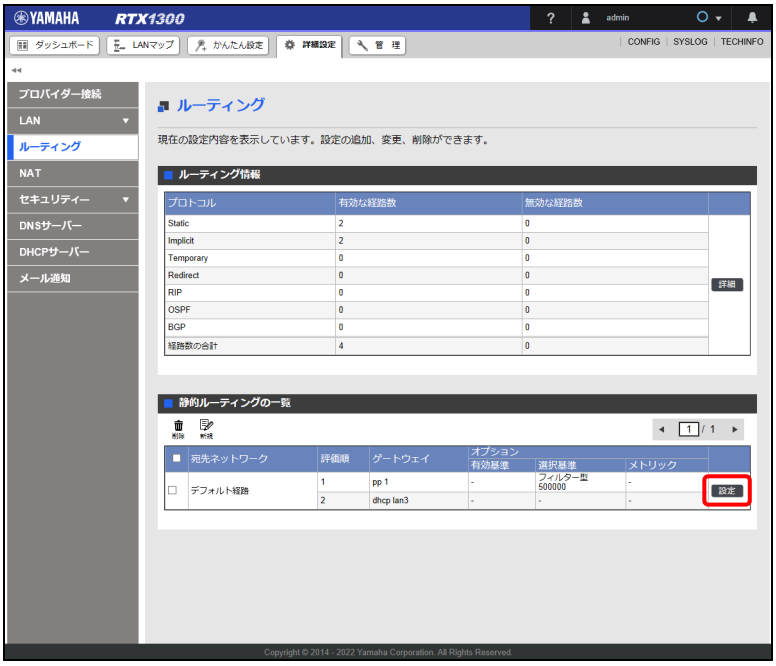
プロバイダー：PPPoE 接続型プロバイダー
使用する端末の IP アドレス：192.168.100.2

ゲートウェイ 2

プロバイダー：DHCP 接続型プロバイダー
使用する端末の IP アドレス：192.168.100.30

1. **「詳細設定」タブ ー「ルーティング」を順に選択する。**
   「ルーティング」画面が表示されます。

2.「静的ルーティングの一覧」項目のデフォルト経路の「設定」ボタンをクリックする。

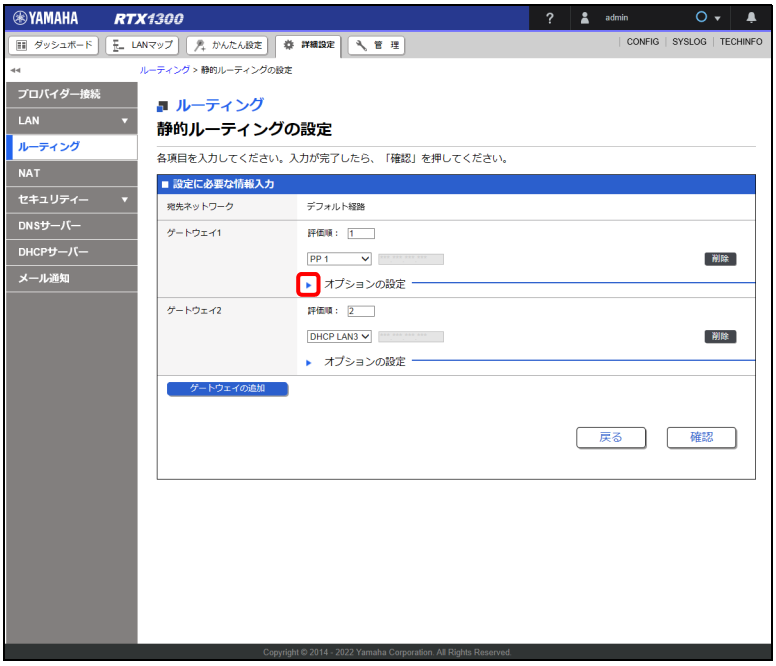


「静的ルーティングの設定」画面が表示されます。

メモ

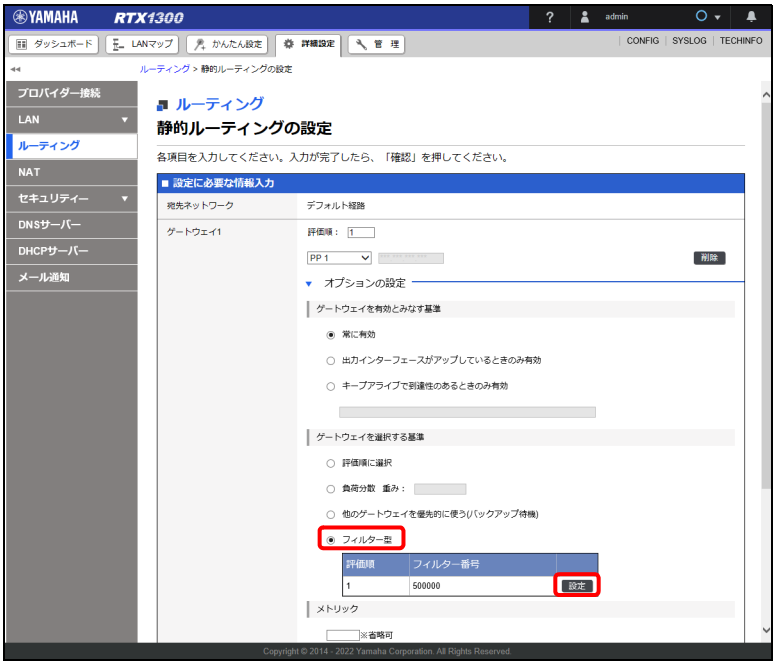
デフォルト経路制御により、経路情報をコンパクトにすることができます。すべての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。デフォルト経路により外側と内側を仕切り、未知のネットワークへのアクセスはデフォルト経路に流すようになっています。

3.「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。



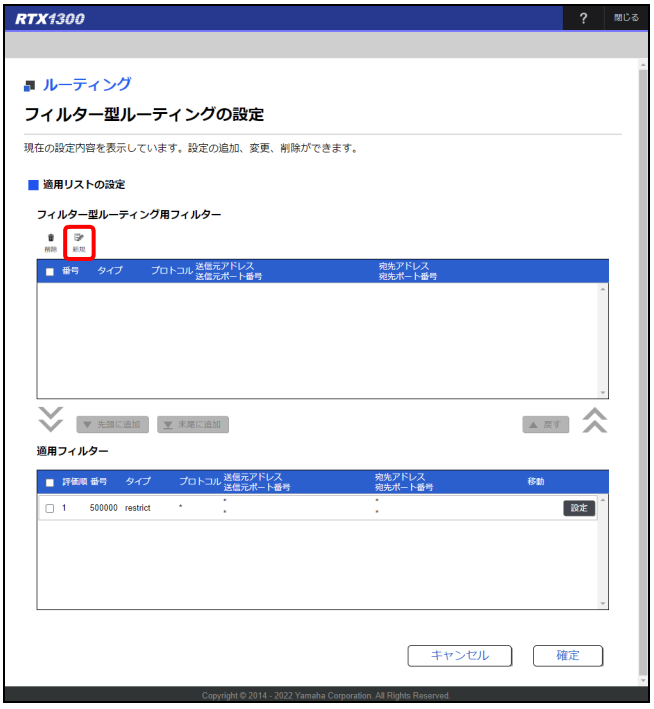
「オプションの設定」が表示されます。

4.「ゲートウェイを選択する基準」欄で「フィルター型」を選択し、「設定」ボタンをクリックする。



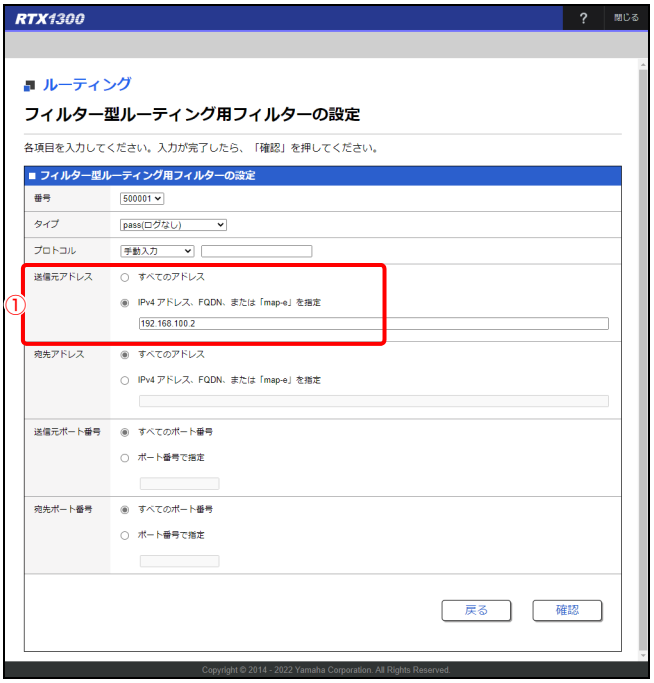
「フィルター型ルーティングの設定」画面が表示されます。

5. 「フィルター型ルーティング用フィルター」項目の「新規」ボタンをクリックする。



「フィルター型ルーティング用フィルターの設定」画面が表示されます。

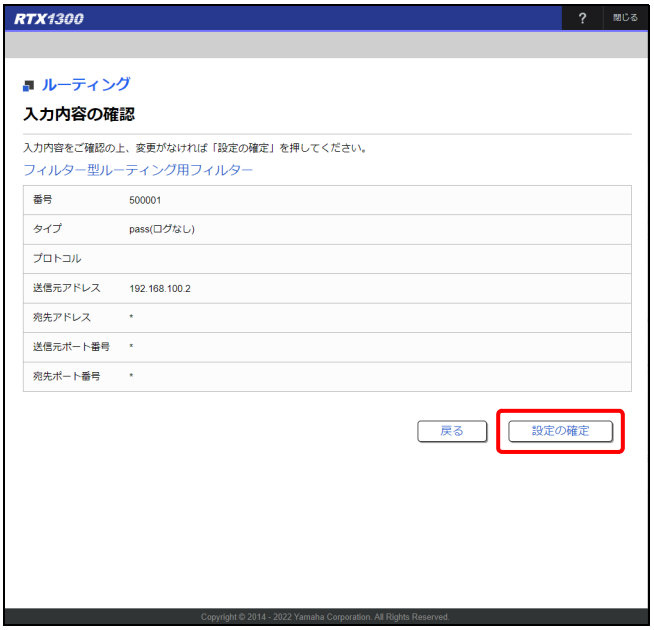
6. ルーティング用フィルターを設定する。



① **送信元アドレス：**
「192.168.100.2」を入力します。

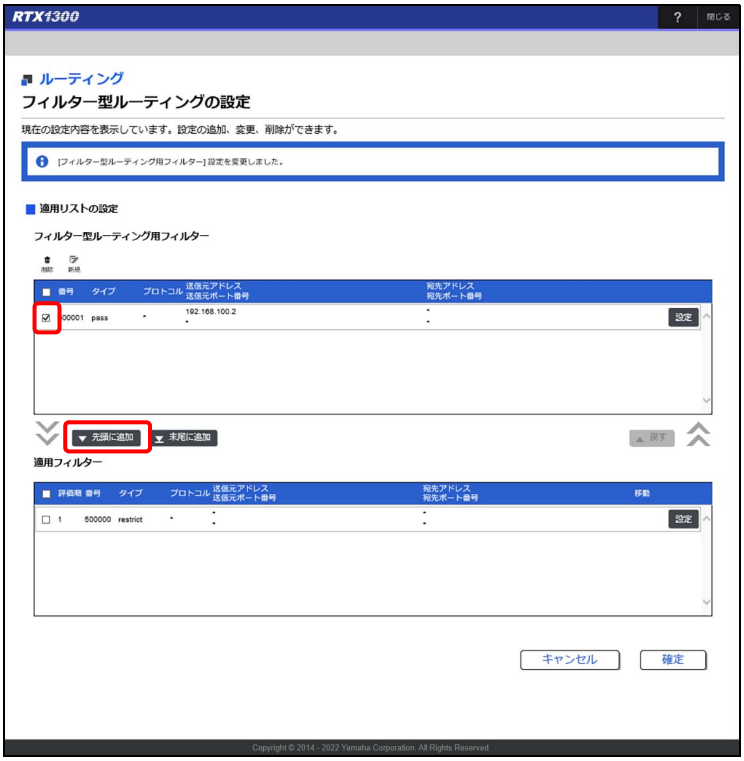
7. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

8. **内容を確認し、「設定の確定」ボタンをクリックする。**

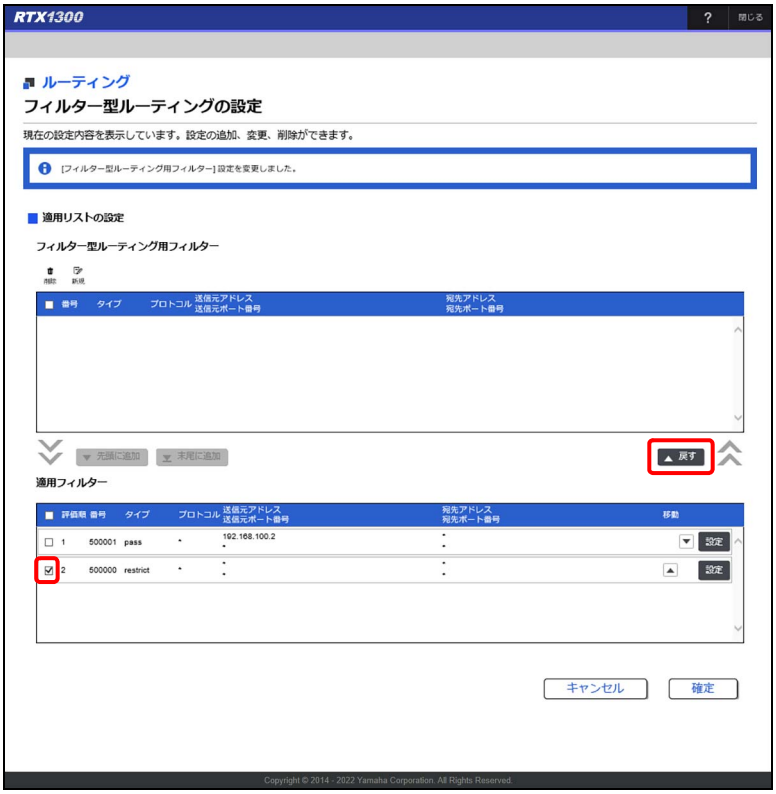


ルーティング用フィルターが作成され、「フィルター型ルーティングの設定」画面が表示されます。

9. **「フィルター型ルーティング用フィルター」項目のチェックボックスにチェックを入れてから「先頭に追加」ボタンをクリックし、作成したフィルター設定を「適用フィルター」項目の先頭に移動させる。**



10.「適用フィルター」項目の 500000 番のフィルターのチェックボックスにチェックを入れてから「戻す」ボタンをクリックし、「フィルター型ルーティング用フィルター」項目に移動させる。



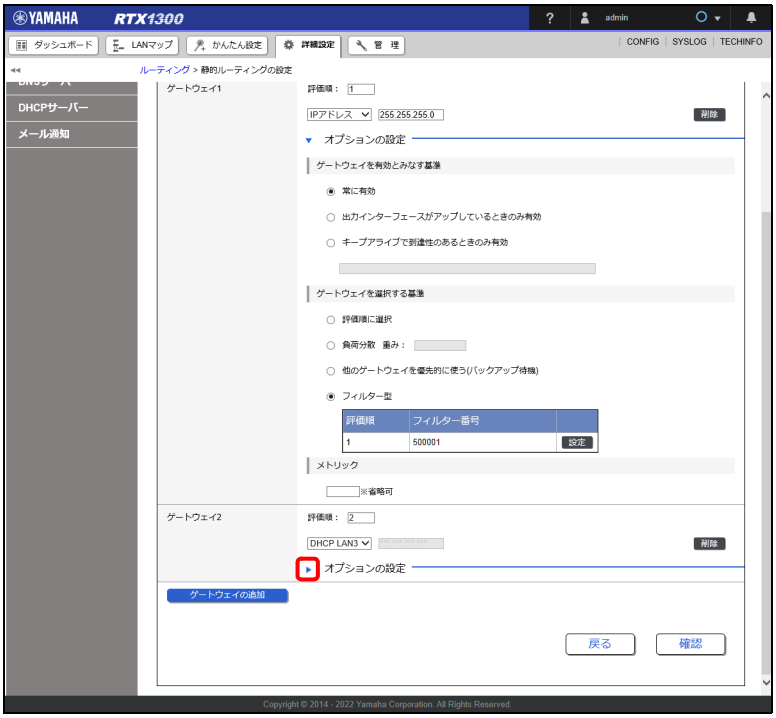
メモ

500000 番のフィルターが適用されたままになっていると、すべての端末がゲートウェイ 1 を使用してしまうため、端末ごとの使い分けができません。

11.「確定」ボタンをクリックする。

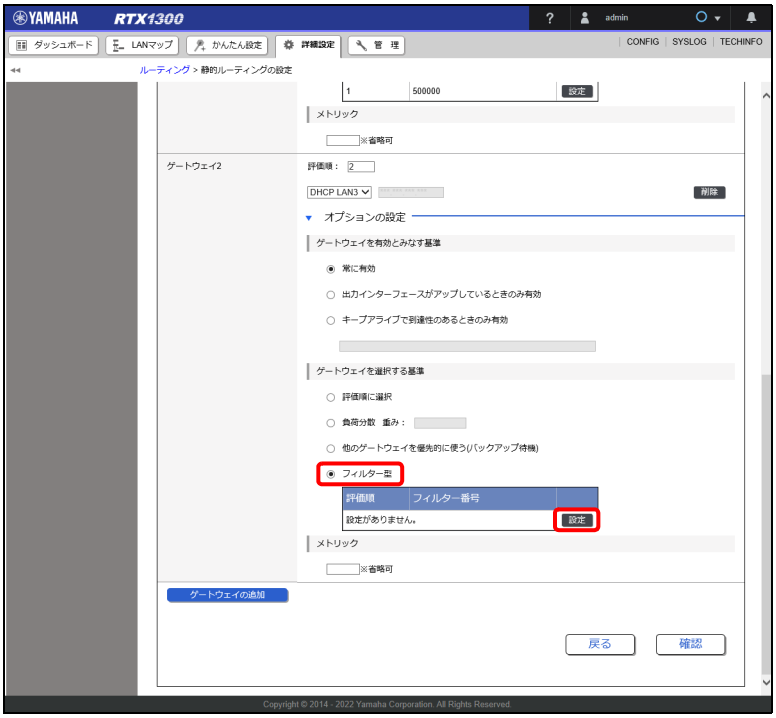
「フィルター型ルーティングの設定」画面が閉じられます。

12.「ゲートウェイ 2」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。



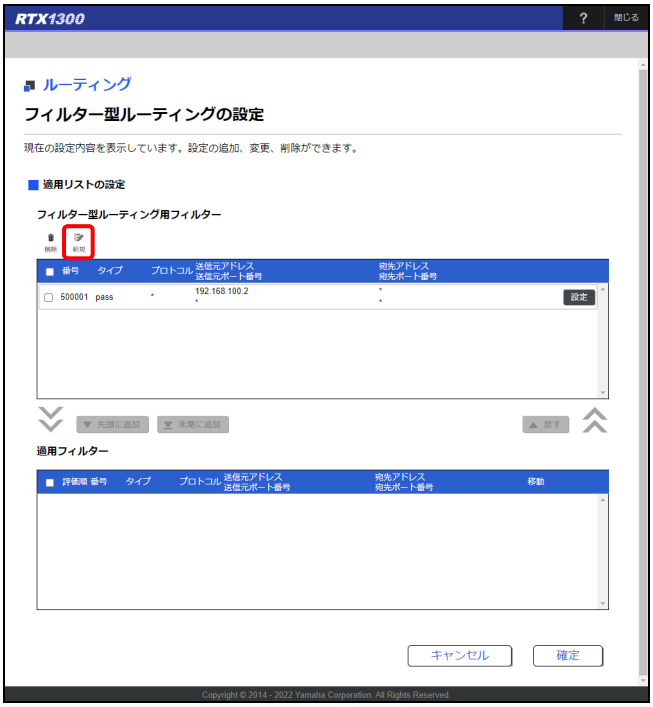
「オプションの設定」が表示されます。

13.「ゲートウェイを選択する基準」欄で「フィルター型」を選択し、「設定」ボタンをクリックする。



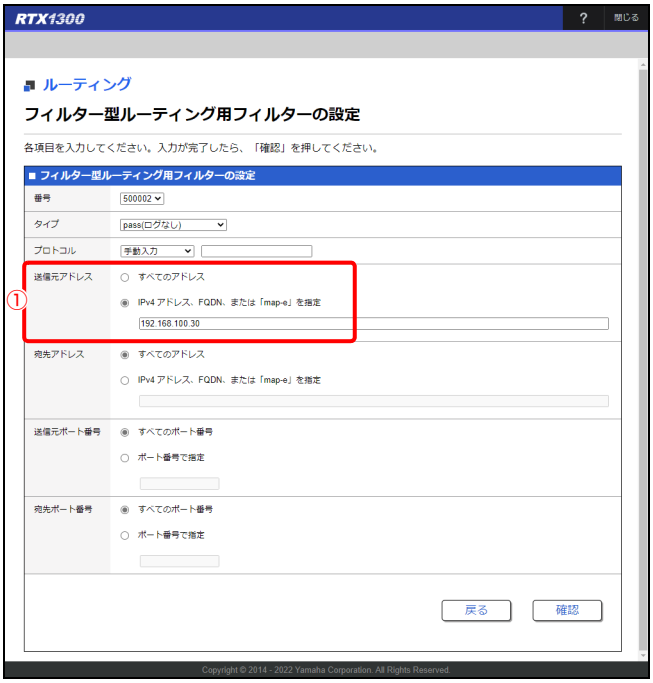
「フィルター型ルーティングの設定」画面が表示されます。

14.「フィルター型ルーティング用フィルター」項目の「新規」ボタンをクリックする。



「フィルター型ルーティング用フィルターの設定」画面が表示されます。

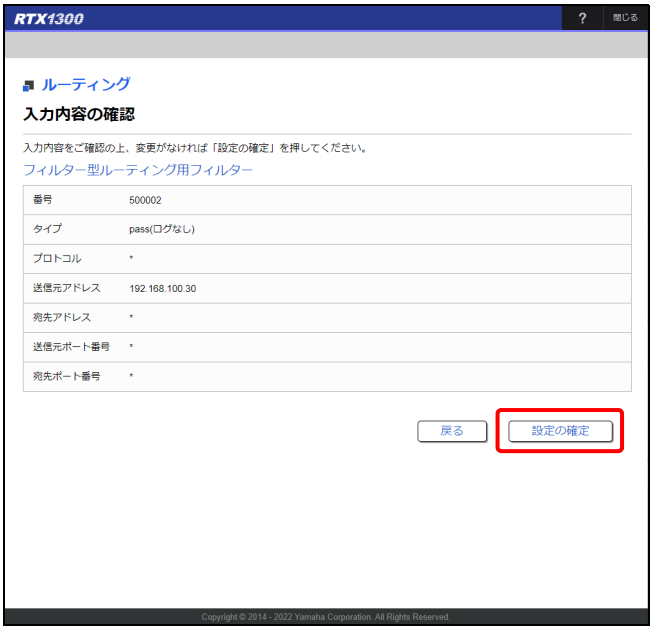
15.ルーティング用フィルターを設定する。



① **送信元アドレス：**
「192.168.100.30」を入力します。

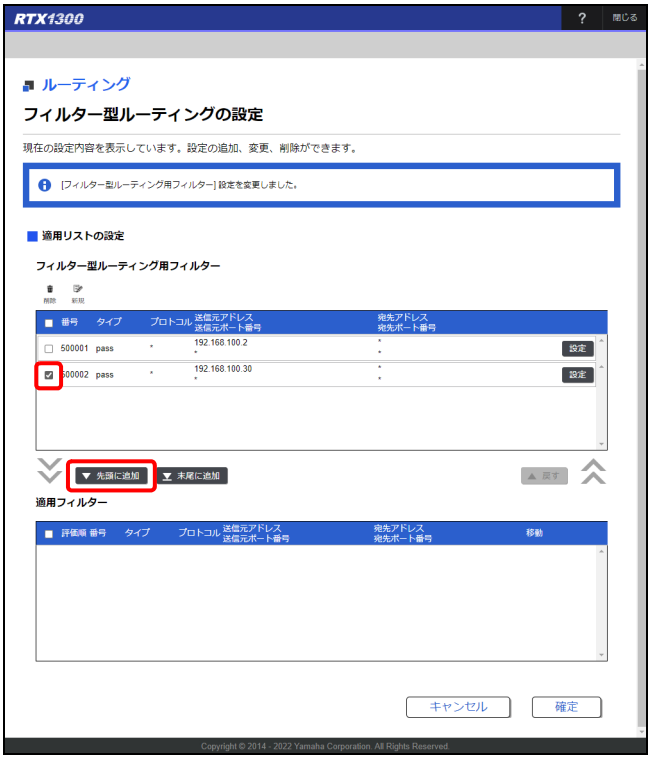
16.「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

17.内容を確認し、「設定の確定」ボタンをクリックする。



ルーティング用フィルターが作成され、「フィルター型ルーティングの設定」画面が表示されます。

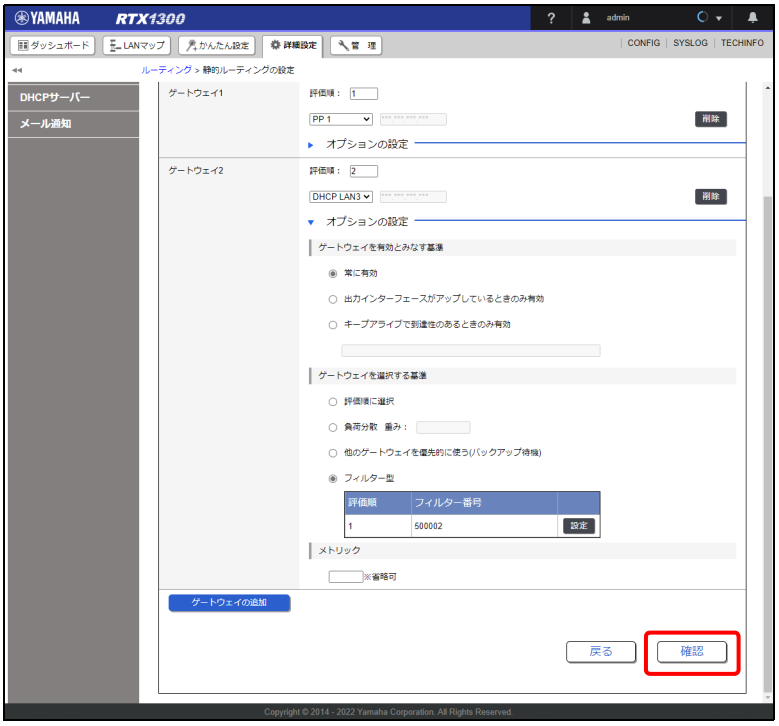
18.「フィルター型ルーティング用フィルター」項目のチェックボックスにチェックを入れてから「先頭に追加」ボタンをクリックし、作成したフィルター設定を「適用フィルター」項目の先頭に移動させる。



19.「確定」ボタンをクリックする。

「フィルター型ルーティングの設定」画面が閉じられます。

20.「確認」ボタンをクリックする。



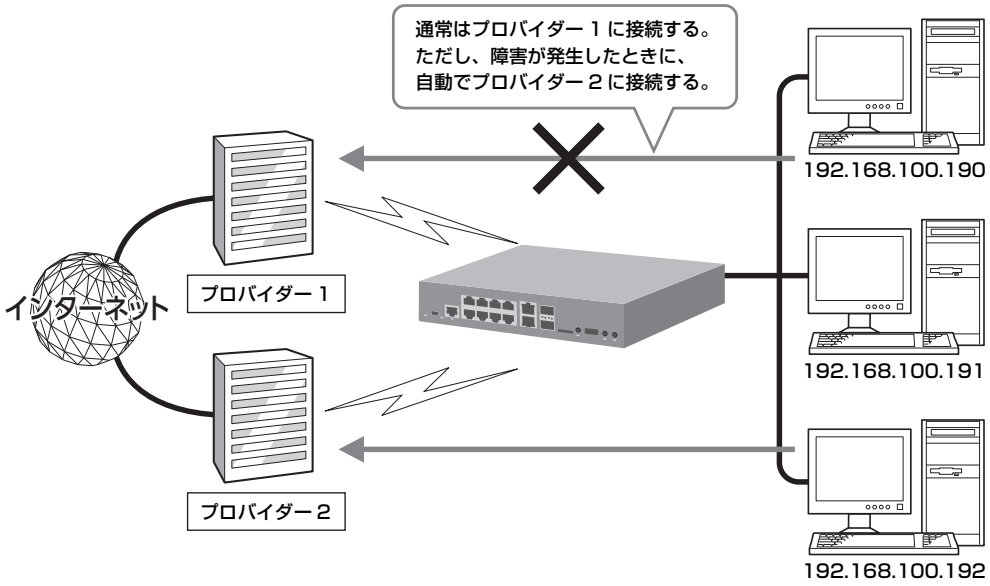
「入力内容の確認」画面が表示されます。

21.内容を確認し、「設定の確定」ボタンをクリックする。

設定が反映され、「ルーティングの設定」画面が表示されます。

14.7.3 バックアップ回線を用意する

主のインターネット回線に障害が発生したときに、予備のインターネット回線に自動で切り替えることができます。



設定例

ゲートウェイ 1

プロバイダー：PPPoE 接続型プロバイダー（主回線）
キープアライブ機能で使用する IP アドレス：203.0.113.1

ゲートウェイ 2

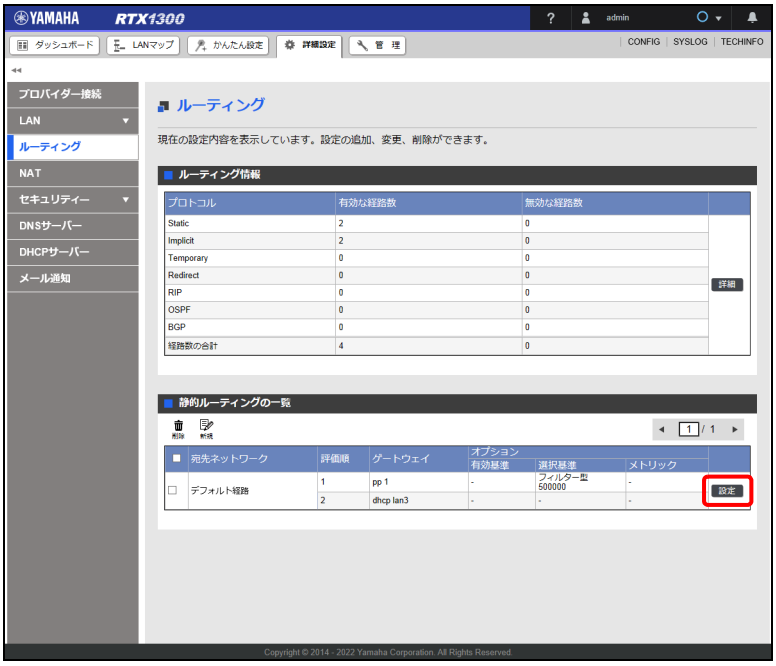
プロバイダー：DHCP 接続型プロバイダー（予備回線）

メモ

キープアライブ機能とは、指定の IP アドレスへ ICMP Echo を送信して到達性を確認し、到達性がある限り、そのゲートウェイを有効とみなす機能のことです。到達性がなくなった場合に予備回線のゲートウェイに切り換わります。宛先の IP アドレスには、安定的に稼動しているサーバーなどの固定グローバル IP アドレスを指定してください。

1. **「詳細設定」タブ ―「ルーティング」を順に選択する。**
   「ルーティング」画面が表示されます。

2.「静的ルーティングの一覧」項目のデフォルト経路の「設定」ボタンをクリックする。

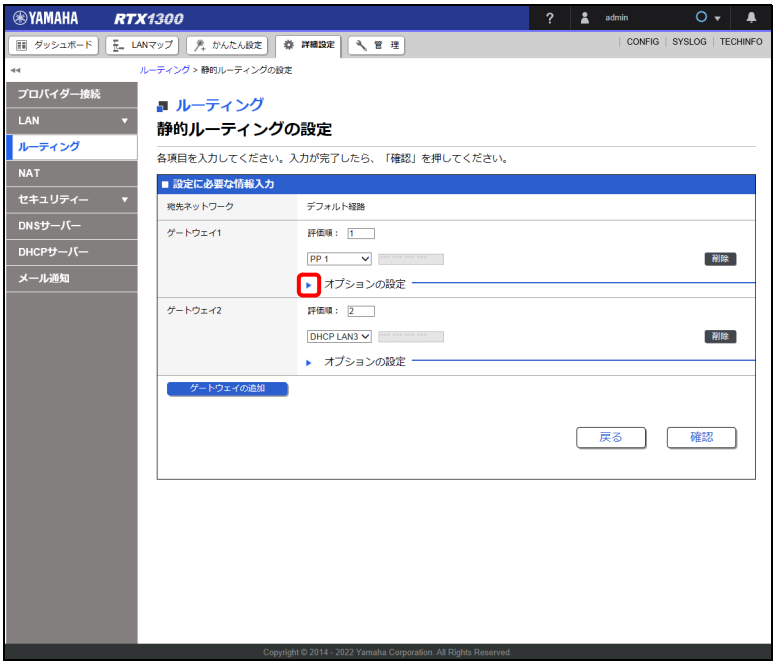


「静的ルーティングの設定」画面が表示されます。

メモ

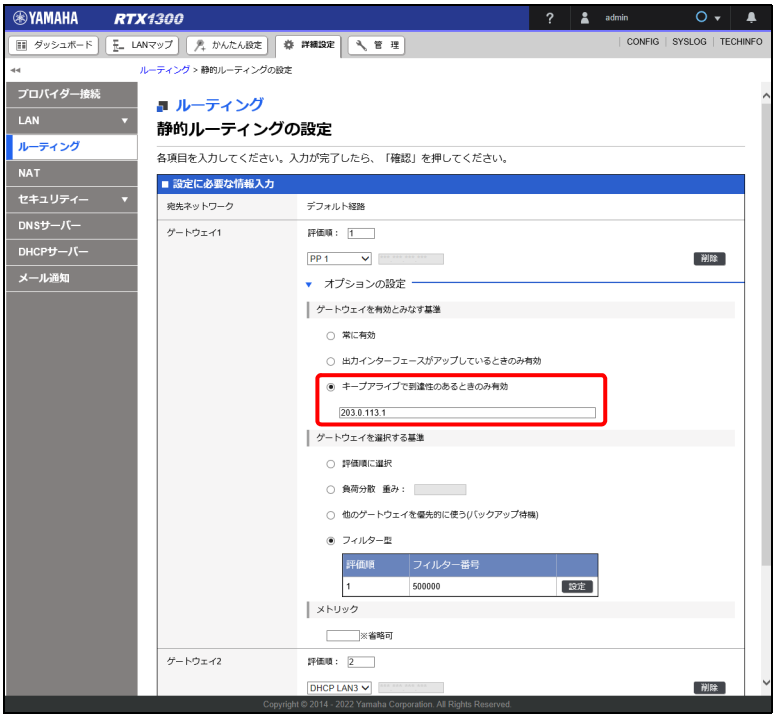
デフォルト経路制御により、経路情報をコンパクトにすることができます。すべての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。デフォルト経路により外側と内側を仕切り、未知のネットワークへのアクセスはデフォルト経路に流すようになっています。

3.「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。

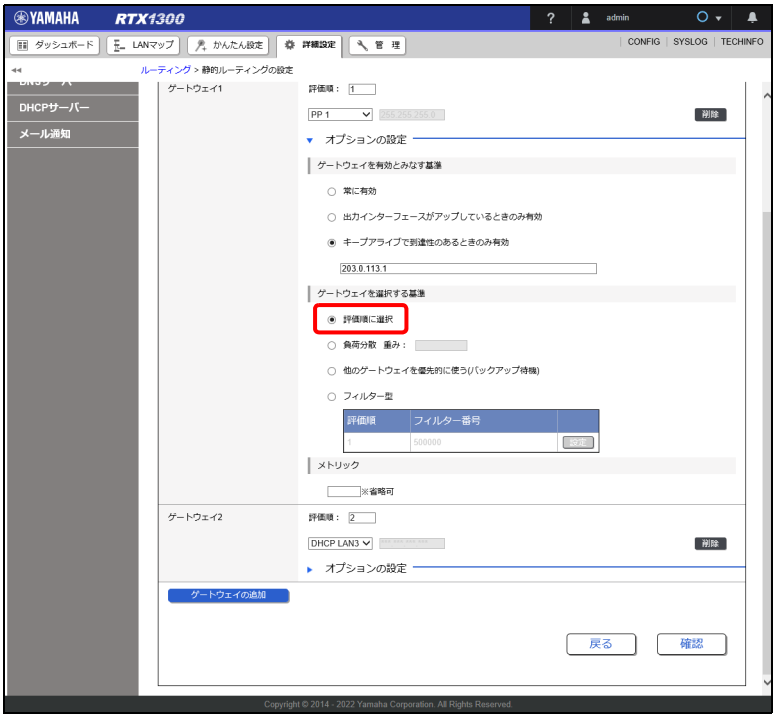


「オプションの設定」が表示されます。

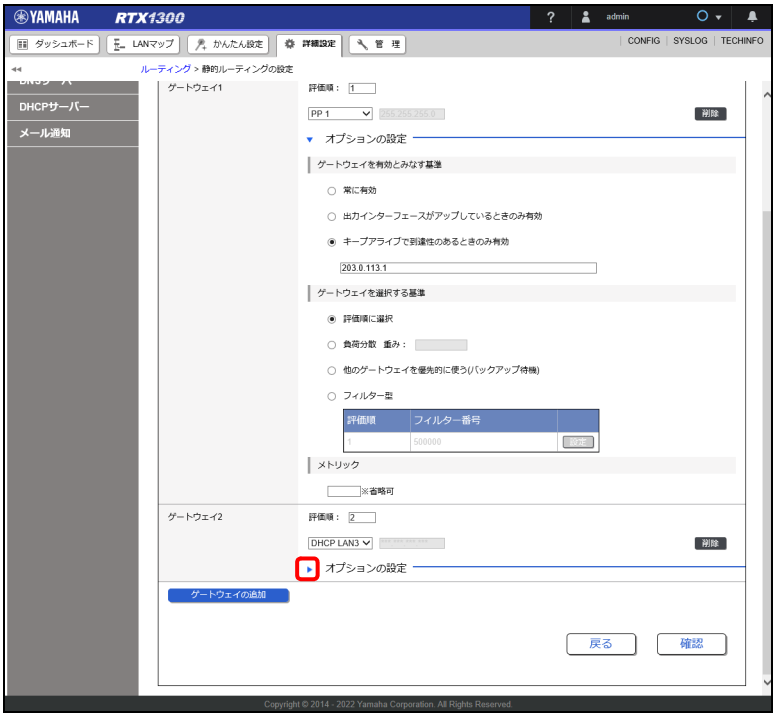
4.「ゲートウェイを有効とみなす基準」欄で「キープアライブで到達性のあるときのみ有効」を選択し、「203.0.113.1」を入力する。



5.「ゲートウェイを選択する基準」欄で「評価順に選択」を選択する。

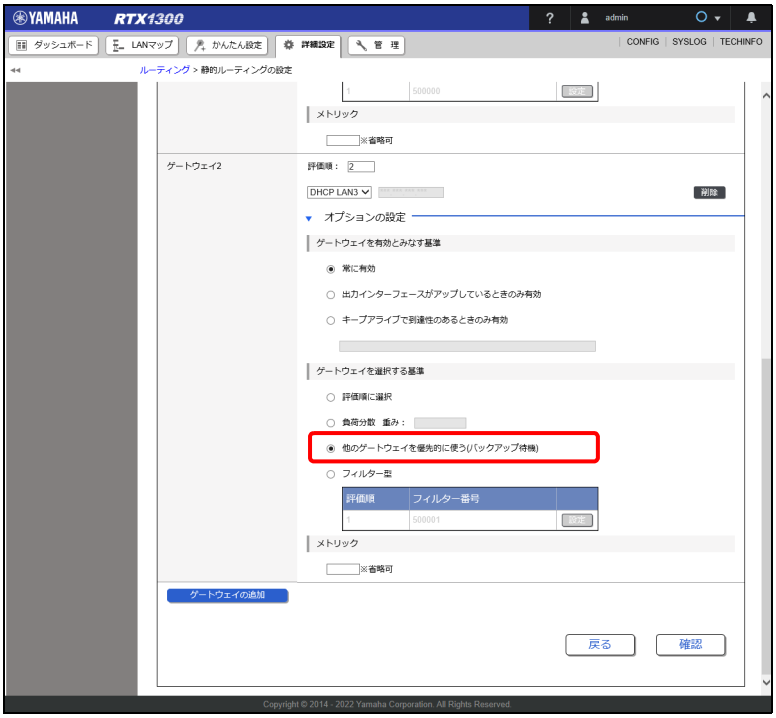


6.「ゲートウェイ 2」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。



「オプションの設定」が表示されます。

7. 「ゲートウェイを選択する基準」欄で「他のゲートウェイを優先的に使う（バックアップ待機）」を選択する。



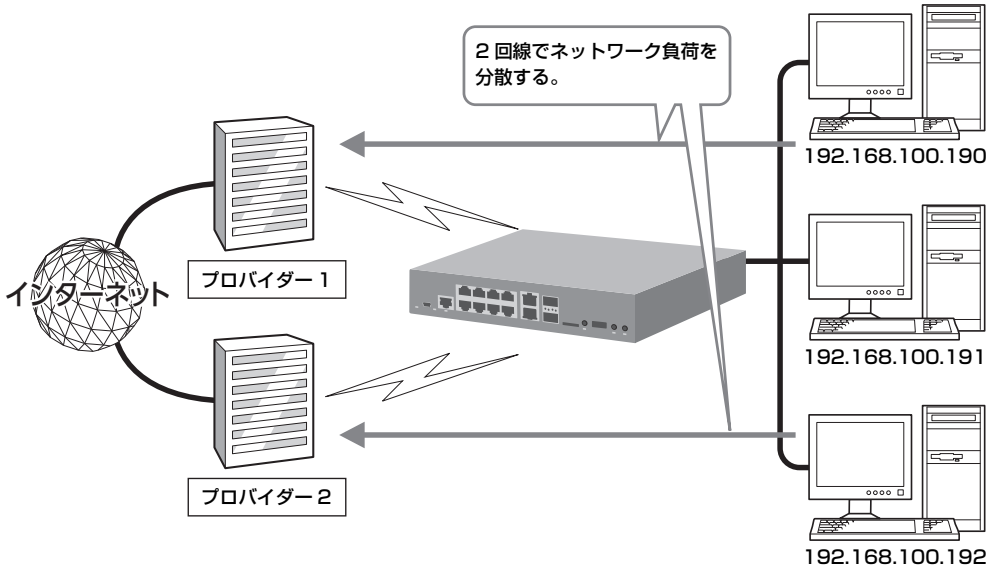
8. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

9. 内容を確認し、「設定の確定」ボタンをクリックする。

設定が反映され、「ルーティングの設定」画面が表示されます。

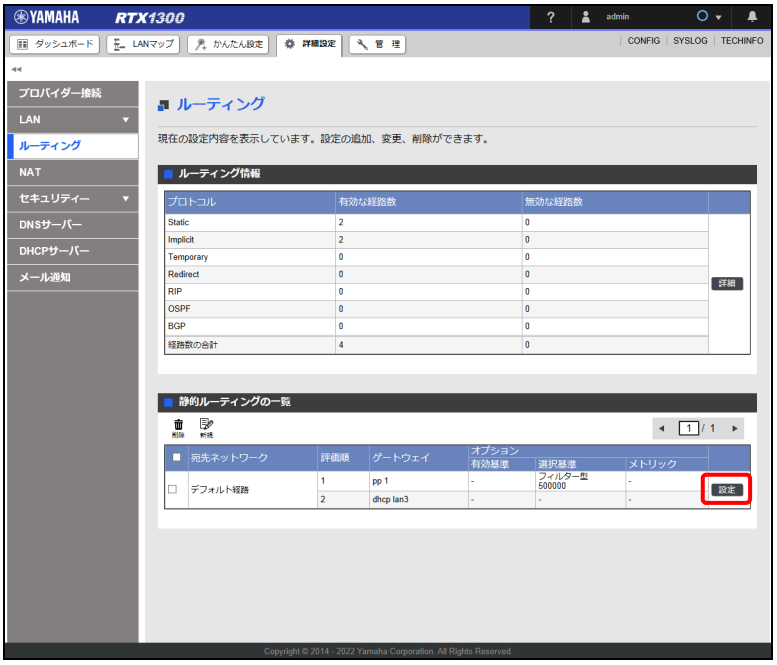
14.7.4 マルチホーミングによる負荷分散を行う

複数のインターネット回線を使用して、ネットワークの負荷を分散することができます。ネットワークの負荷を均等に分散する場合を例に説明します。



1. **「詳細設定」タブ ー「ルーティング」を順に選択する。**
   「ルーティング」画面が表示されます。

2. **「静的ルーティングの一覧」項目のデフォルト経路の「設定」ボタンをクリックする。**

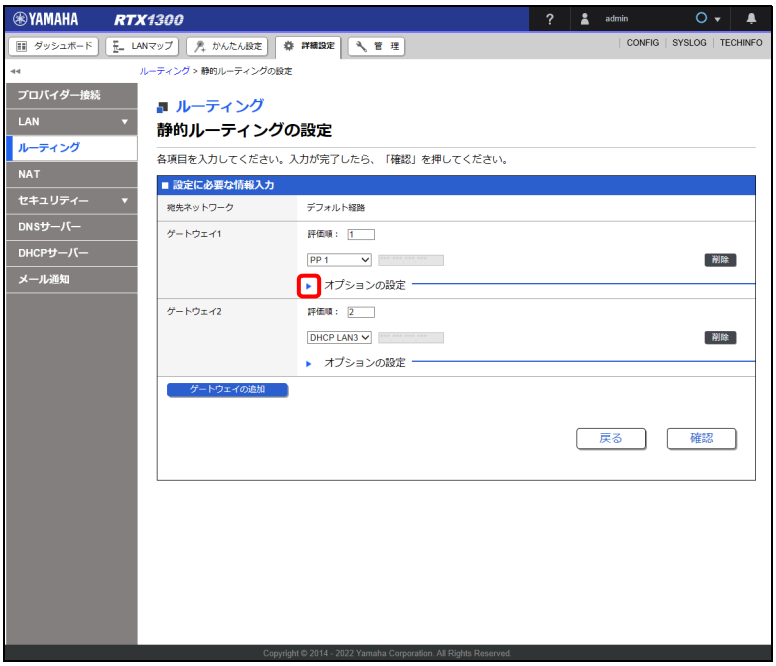


「静的ルーティングの設定」画面が表示されます。

メモ

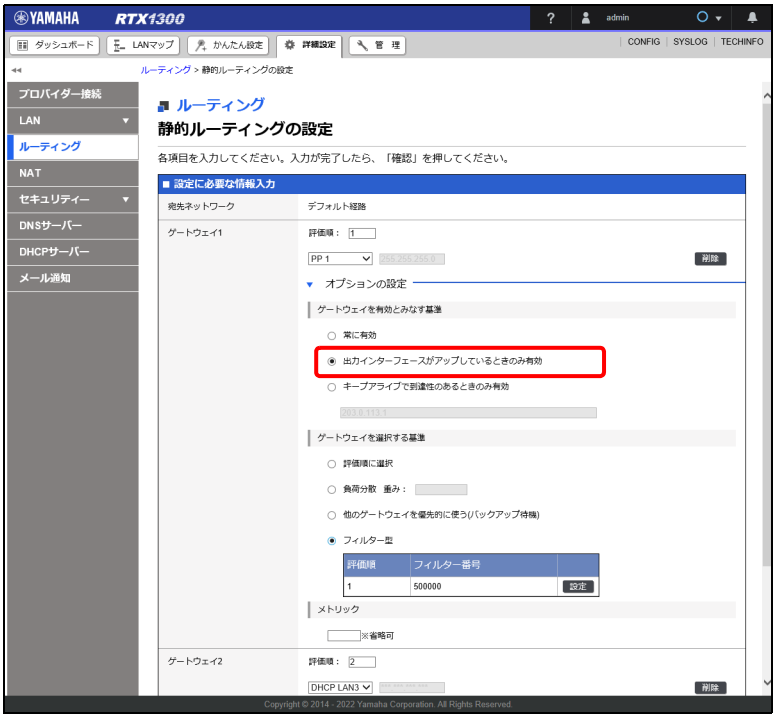
デフォルト経路制御により、経路情報をコンパクトにすることができます。すべての TCP/IP ネットワークの経路情報をルーターが持とうとしても、経路情報が多過ぎて処理できません。デフォルト経路により外側と内側を仕切り、未知のネットワークへのアクセスはデフォルト経路に流すようになっています。

3. 「ゲートウェイ 1」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。



「オプションの設定」が表示されます。

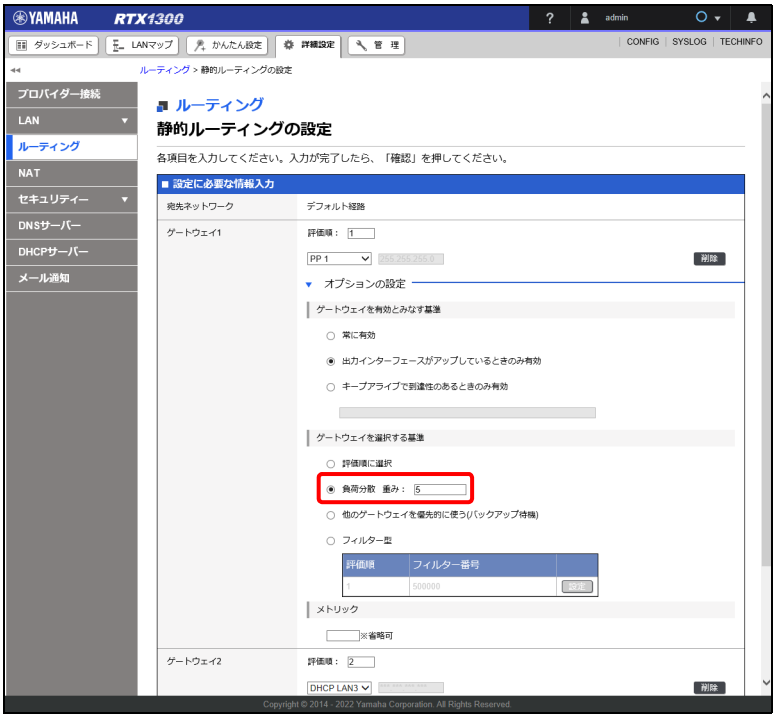
4. 「ゲートウェイを有効とみなす基準」欄で「出力インターフェースがアップしているときのみ有効」を選択する。



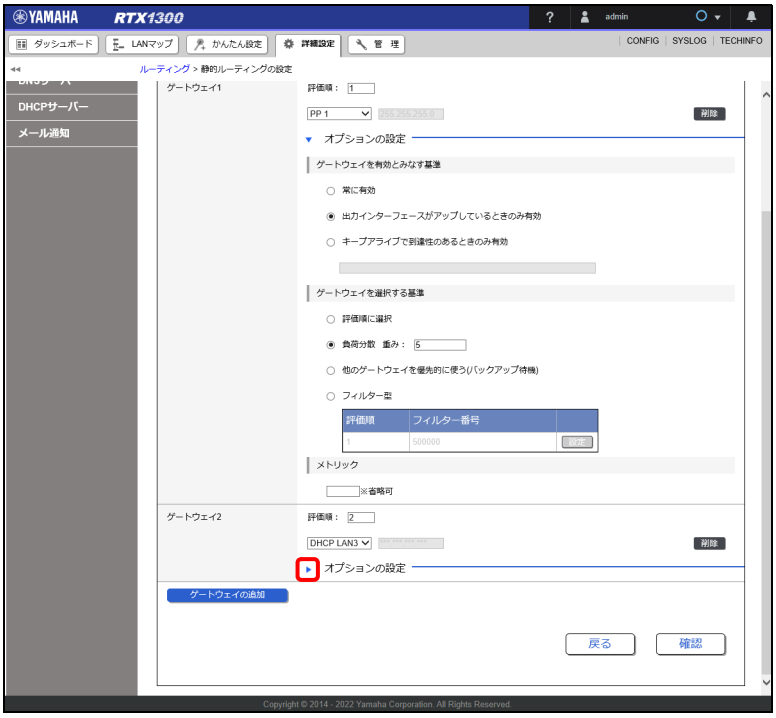
メモ

「出力インターフェースがアップしているときのみ有効」を選択することで、片方に障害が発生しても他方で通信を継続することができます。

5.「ゲートウェイを選択する基準」欄で「負荷分散」を選択し、「5」を入力する。

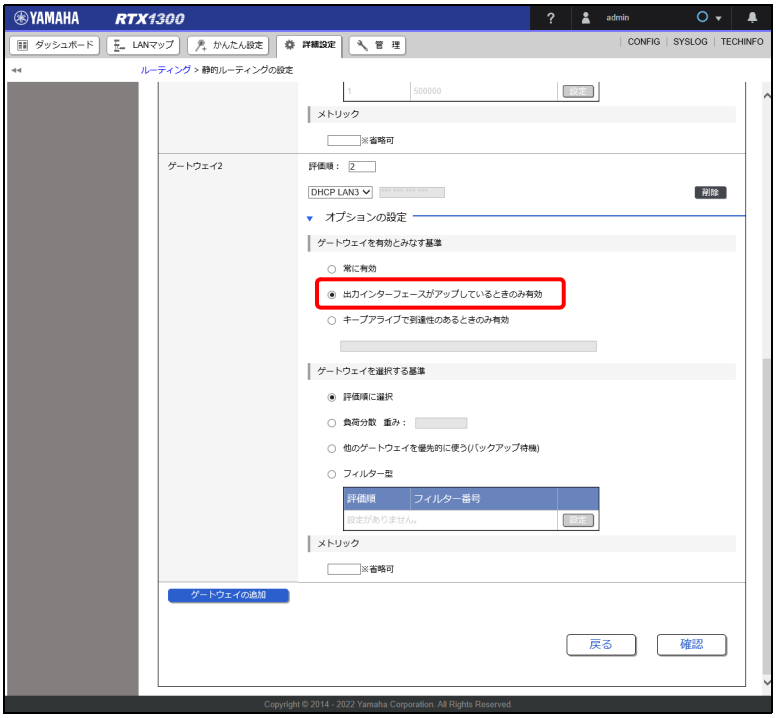


6.「ゲートウェイ 2」項目の「オプションの設定」の先頭にある「 ▶ 」ボタンをクリックする。



「オプションの設定」が表示されます。

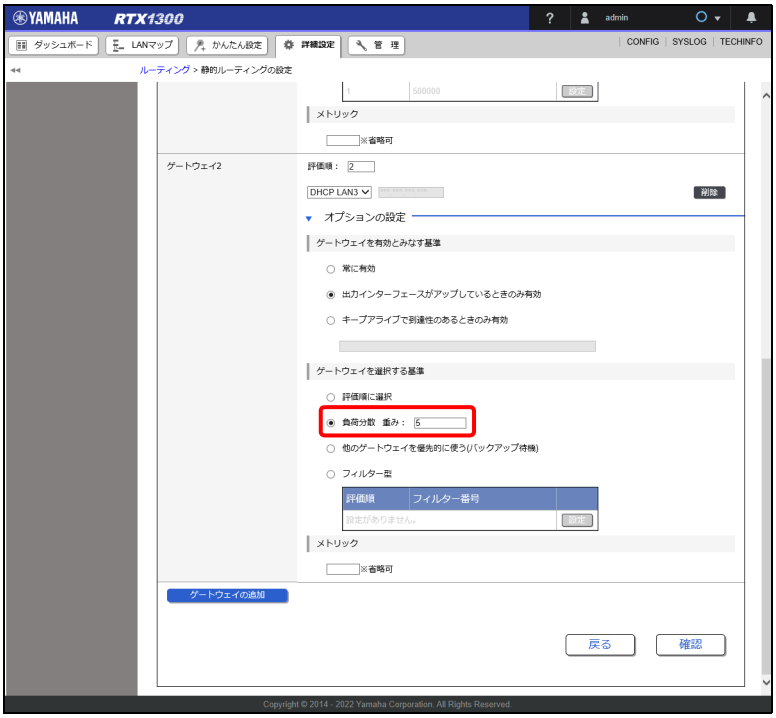
7. 「ゲートウェイを有効とみなす基準」欄で「出力インターフェースがアップしているときのみ有効」を選択する。



メモ

「出力インターフェースがアップしているときのみ有効」を選択することで、片方に障害が発生しても他方で通信を継続することができます。

8. 「ゲートウェイを選択する基準」欄で「負荷分散」を選択し、「5」を入力する。



9. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

10. 「設定の確定」ボタンをクリックする。

設定が反映され、「ルーティングの設定」画面が表示されます。

14.8 DNS サーバーを設定する

DNS サーバー機能の基本的な設定や上位の中継先 DNS サーバーの設定を行います。本製品で DNS の名前解決ができなかった場合や、本製品を介さずに端末が直接上位の DNS サーバーに問い合わせする場合に、中継先 DNS サーバーの設定が必要になります。

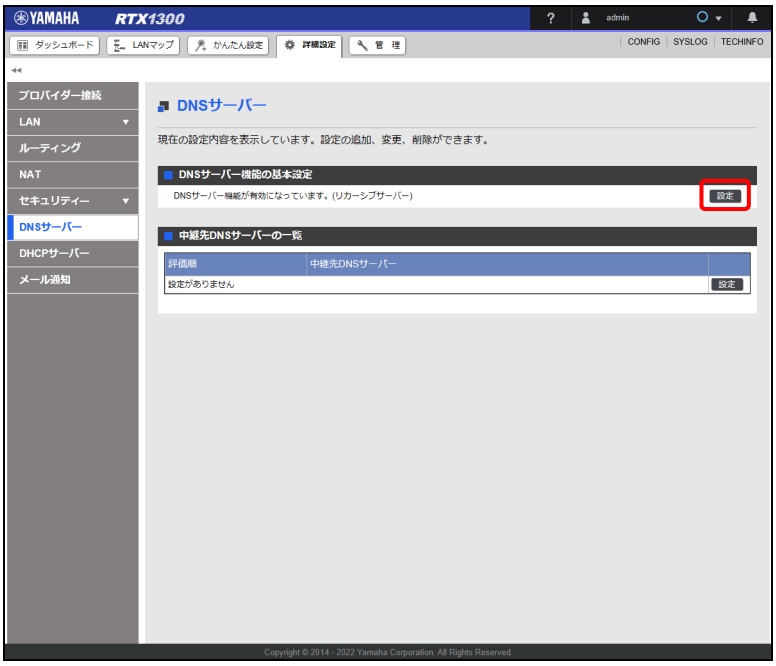
14.8.1 DNS サーバー機能の基本設定を行う

DNS サーバー機能の基本的な設定を行います。本製品を DNS リカーシブサーバーとして動作させる場合を例に説明します。

設定例

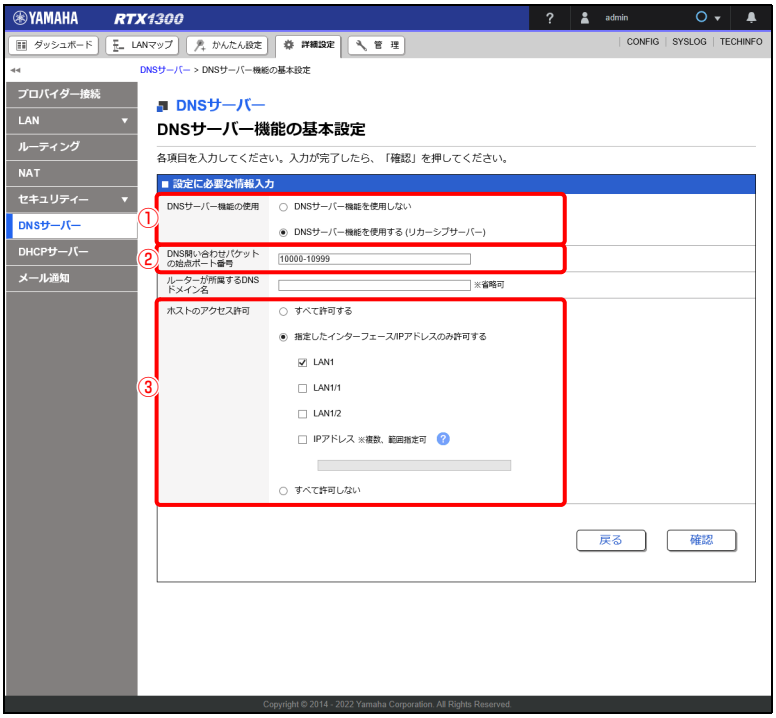
DNS サーバー機能：リカーシブサーバーとして動作させる
DNS 問い合わせパケットの始点ポート番号：10000-10999
DNS 問い合わせを許可するホスト：LAN1 のネットワークに接続しているホスト

1. **「詳細設定」タブ ー「DNS サーバー」を順に選択する。**
   「DNS サーバー」画面が表示されます。
2. **「DNS サーバー機能の基本設定」項目の「設定」ボタンをクリックする。**



「DNS サーバー機能の基本設定」画面が表示されます。

3. DNS サーバーの基本機能を設定する。



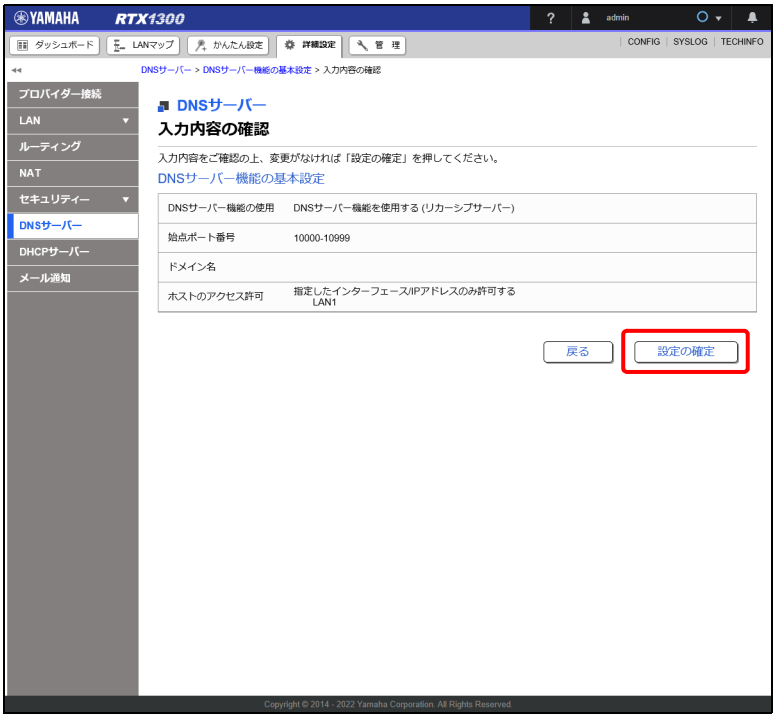
① DNS サーバー機能の使用：
「DNS サーバー機能を使用する（リカーシブサーバー）」を選択します。

② DNS 問い合わせパケットの始点ポート番号：
「10000-10999」を入力します。

③ ホストのアクセス許可：
「指定したインターフェースの IP アドレスのみ許可する」を選択し、「LAN1」を選択します。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「DNS サーバー」画面が表示されます。

14.8.2 中継先 DNS サーバーを設定する

DNS 問い合わせの中継先の DNS サーバーを設定します。
中継先の DNS サーバーを問い合わせ内容に応じて詳細に設定したい場合は「14.8.3 中継先 DNS サーバーを問い合わせ内容に応じて設定する」（372 ページ）をご覧ください。

プロバイダーから DNS サーバーが指定されている場合

設定例

DNS サーバーアドレス：203.0.113.10、203.0.113.20

1. **「詳細設定」タブ ― 「DNS サーバー」を順に選択する。**
「DNS サーバー」画面が表示されます。

2. 「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。

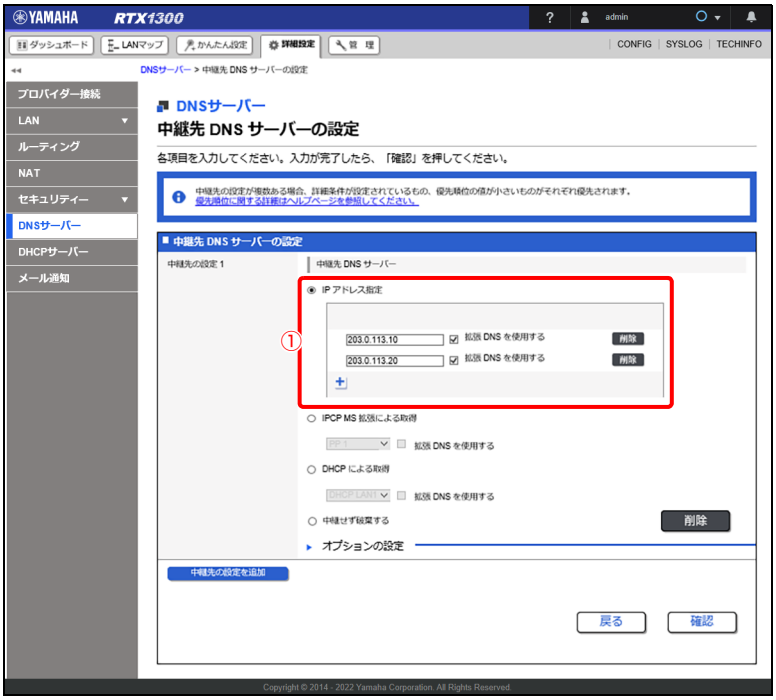
「中継先 DNS サーバーの設定」画面が表示されます。

3. **中継先 DNS サーバーを設定する。**

「中継先の設定を追加」ボタンをクリックすることで、中継先の設定が新たに追加されます。

メモ

中継先 DNS サーバーの設定は、最大 128 個まで追加することが可能です。



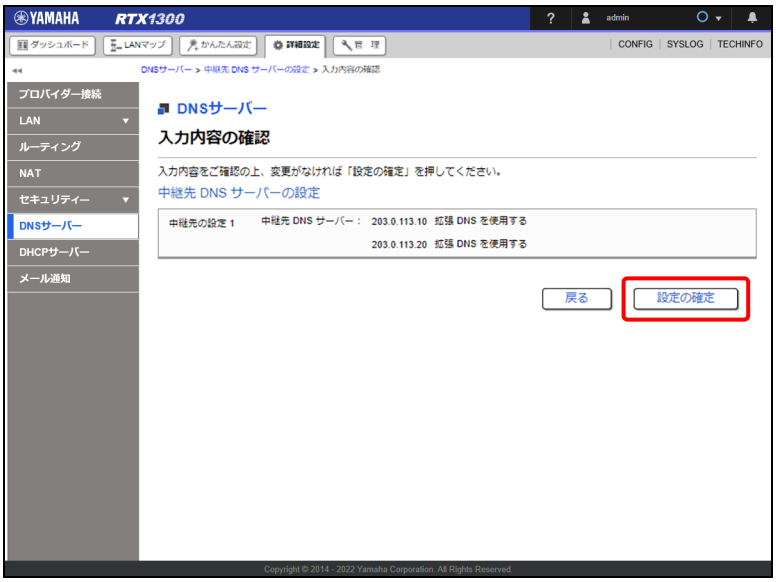
① **IP アドレス指定：**

「203.0.113.10」と「203.0.113.20」を入力します。

「拡張 DNS を使用する」にチェックを入れた場合、拡張 DNS（EDNS）を用いて名前解決を行います。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「DNS サーバー」画面が表示されます。

DNS サーバーアドレスを自動取得する場合

設定例

DNS サーバーアドレス：PP1 インターフェースから自動取得

重要

プロバイダーから通知される DNS サーバーのアドレスを使用するため、事前にプロバイダー接続の設定を済ませておく必要があります。

1. **「詳細設定」タブ ― 「DNS サーバー」を順に選択する。**
   「DNS サーバー」画面が表示されます。

2. 「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。

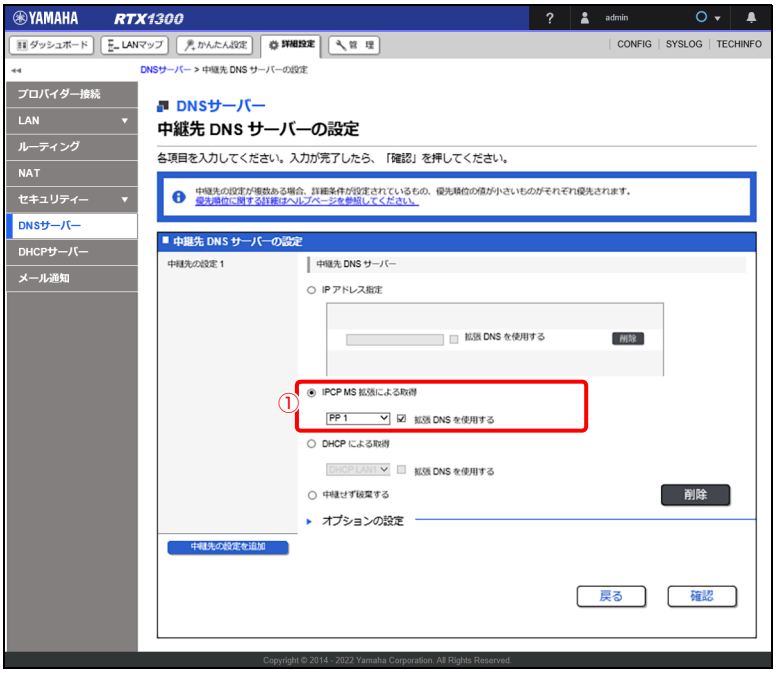
「中継先 DNS サーバーの設定」画面が表示されます。

3. **中継先 DNS サーバーを設定する。**

「中継先の設定を追加」ボタンをクリックすることで、中継先の設定が新たに追加されます。

メモ

中継先 DNS サーバーの設定は、最大 128 個まで追加することが可能です。



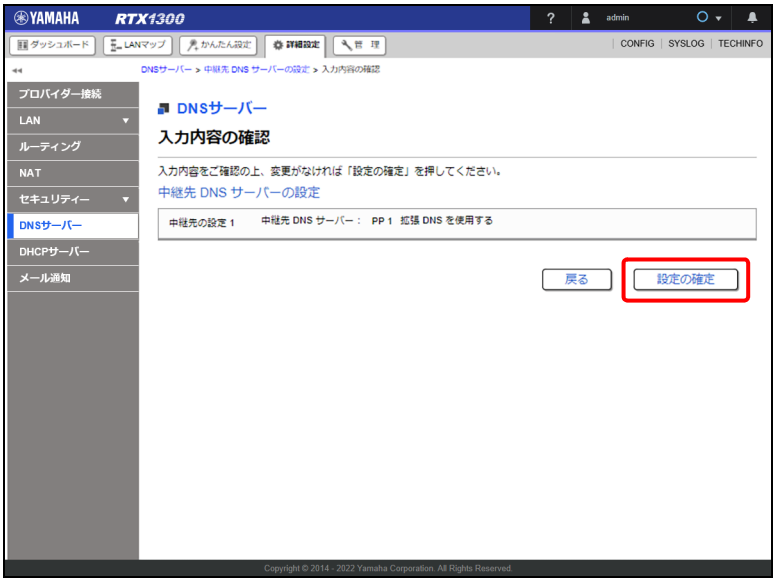
① **IPCP MS 拡張による取得：**

「PP1」を選択します。

「拡張 DNS を使用する」にチェックを入れた場合、拡張 DNS（EDNS）を用いて名前解決を行います。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「DNS サーバー」画面が表示されます。

14.8.3 中継先 DNS サーバーを問い合わせ内容に応じて設定する

DNS のレコード種別や名前解決をしたいホスト名などの問い合わせ内容に応じて、中継先の DNS サーバーを分けて運用したい場合があります。
例えば、社内のイントラネットでのみ有効なホスト名は社内の DNS サーバーでしか名前解決ができないため、イントラネット通信とインターネット通信を同時に行う場合は、それぞれの通信で中継先の DNS サーバーを分ける必要があります。
本項では、“example.net” ドメインを含むホスト名を社内のイントラネットでのみ有効なホスト名と仮定し、“example.net” ドメインを含むホスト名の名前解決は VPN 経由で本社 LAN 内の DNS サーバーで行い、それ以外のホスト名の名前解決は各拠点で契約しているプロバイダーが用意している DNS サーバーで行う場合を例に説明します。

設定例

本社の DNS サーバーアドレス：192.168.100.10
プロバイダーの DNS サーバーアドレス：PP1 インターフェースから自動取得

重要

プロバイダーから通知される DNS サーバーのアドレスを使用するため、事前にプロバイダー接続の設定を済ませておく必要があります。

1. **「詳細設定」タブ ― 「DNS サーバー」を順に選択する。**
   「DNS サーバー」画面が表示されます。

2. **「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。**

「中継先 DNS サーバーの設定」画面が表示されます。

3. **中継先 DNS サーバーを設定する。**
   中継先の設定 1
   「中継先の設定を追加」ボタンをクリックすることで、中継先の設定が新たに追加されます。

メモ

中継先 DNS サーバーの設定は、最大 128 個まで追加することが可能です。

① 中継先 DNS サーバー：

IP アドレス指定にチェックを入れ、「192.168.100.10」を入力します。

「拡張 DNS を使用する」にチェックを入れた場合、拡張 DNS（EDNS）を用いて名前解決を行います。

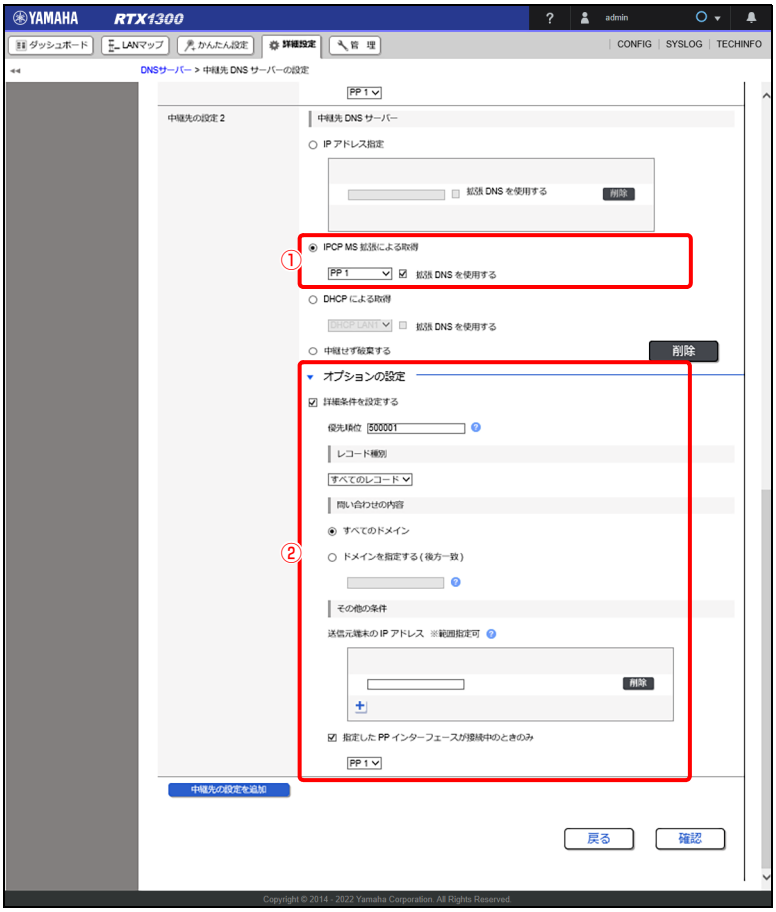
② オプションの設定：

「詳細条件を設定する」にチェックを入れます。

- 優先順位：当該の中継先の設定の優先順位を 1 ～ 2147483647 以下の値で設定します。値が小さい設定から評価され、最初に条件を満たした中継先の設定に対して名前解決が行われます。
- レコード種別：対象とする DNS 問い合わせのレコード種別をプルダウンメニューから選択します。
- 問い合わせの内容：問い合わせ対象のドメイン名を設定します。ドメイン名が “example.net” であれば “www.example.net” など、後方一致で判定されます。
  文字数は最大 255 文字まで設定可能で、前方一致や後方一致で指定する場合はワイルドカードとして '*' を使用することができます。

中継先の設定 2

「中継先の設定を追加」ボタンをクリックし、中継先の設定 2 を追加します。



① 中継先 DNS サーバー：

IPCP MS 拡張による取得にチェックを入れ、プルダウンメニューから「PP 1」を選択します。

「拡張 DNS を使用する」にチェックを入れた場合、拡張 DNS（EDNS）を用いて名前解決を行います。

② オプションの設定：

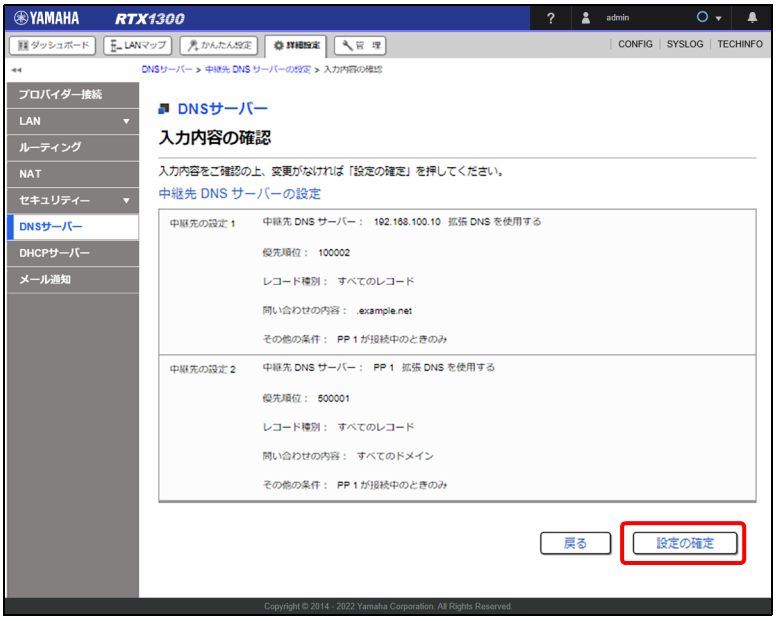
「詳細条件を設定する」にチェックを入れます。

- 優先順位：当該の中継先の設定の優先順位を 1 ～ 2147483647 以下の値で設定します。値が小さい設定から評価され、最初に条件を満たした中継先の設定に対して名前解決が行われます。
- レコード種別：対象とする DNS 問い合わせのレコード種別をプルダウンメニューから選択します。
- 問い合わせの内容：問い合わせ対象のドメイン名を設定します。ドメイン名が “example.net” であれば “www.example.net” など、後方一致で判定されます。
  文字数は最大 255 文字まで設定可能で、前方一致や後方一致で指定する場合はワイルドカードとして '*' を使用することができます。

4.「確認」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「DNS サーバー」画面が表示されます。

14.8.4 特定の DNS 問い合わせパケットを中継せず破棄する

本項では “example.net” を含むドメイン名の名前解決を行わずにパケットを破棄する場合を例に説明します。

1. **「詳細設定」タブ ― 「DNS サーバー」を順に選択する。**
「DNS サーバー」画面が表示されます。

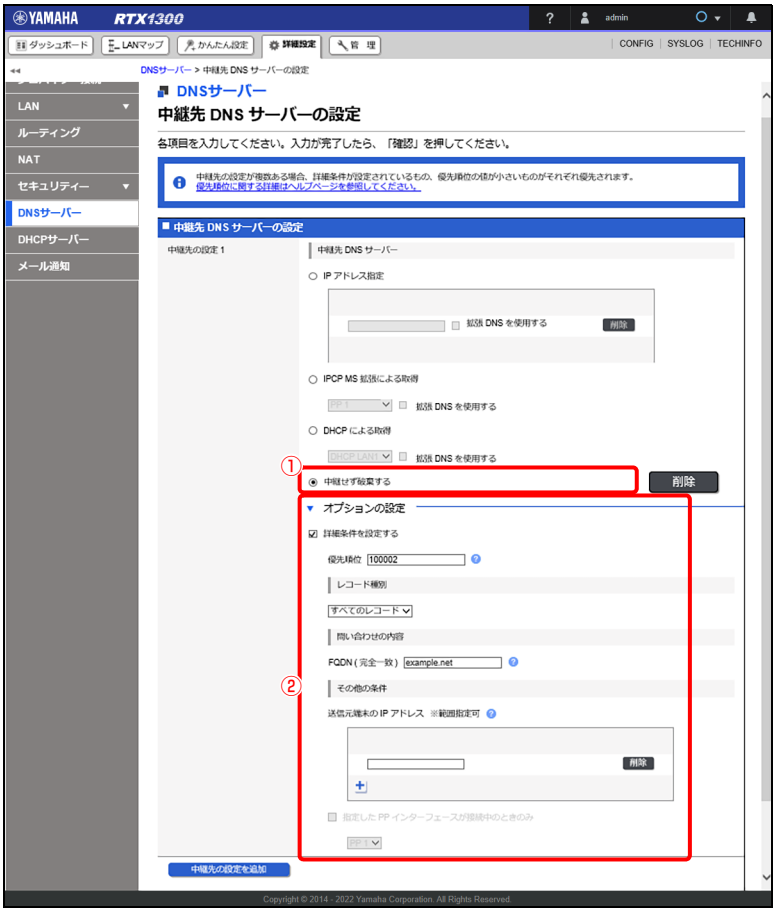
2. **「中継先 DNS サーバーの一覧」項目の「設定」ボタンをクリックする。**

「中継先 DNS サーバーの設定」画面が表示されます。

3. **中継先 DNS サーバーを設定する。**
「中継先の設定を追加」ボタンをクリックすることで、中継先の設定が新たに追加されます。

メモ

中継先 DNS サーバーの設定は、最大 128 個まで追加することが可能です。



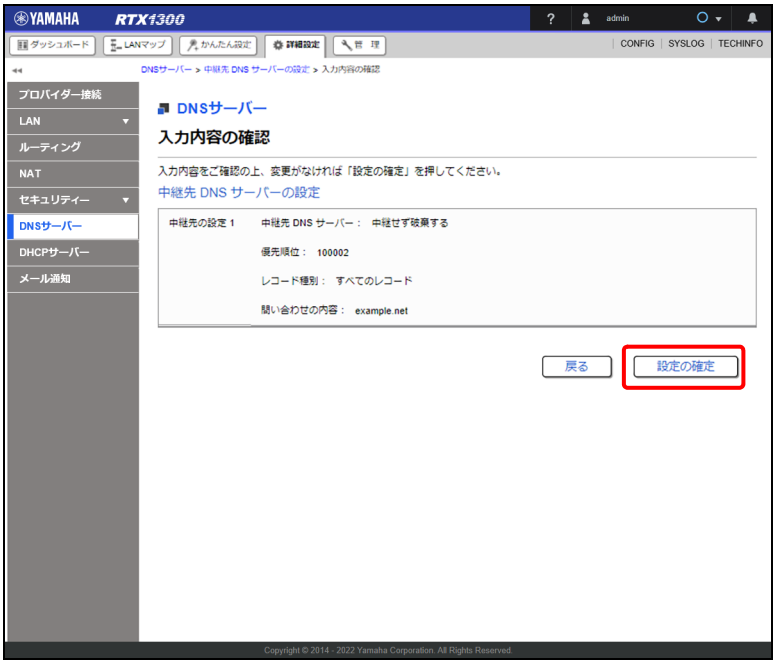
① 中継先 DNS サーバー：
「中継せず破棄する」を選択します。

② オプションの設定：
「詳細条件を設定する」にチェックを入れます。

- 優先順位：当該の中継先の設定の優先順位を 1 ～ 2147483647 以下の値で設定します。値が小さい設定から評価され、最初に条件を満たした中継先の設定に対して名前解決が行われます。
- レコード種別：対象とする DNS 問い合わせのレコード種別をプルダウンメニューから選択します。
- 問い合わせの内容：問い合わせ対象のドメイン名を設定します。ドメイン名が “example.net” であれば “www.example.net” など、後方一致で判定されます。
  文字数は最大 255 文字まで設定可能で、前方一致や後方一致で指定する場合はワイルドカードとして '*' を使用することができます。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「DNS サーバー」画面が表示されます。

14.9 DNS サーバー機能にアクセスできるホストの設定を変更する

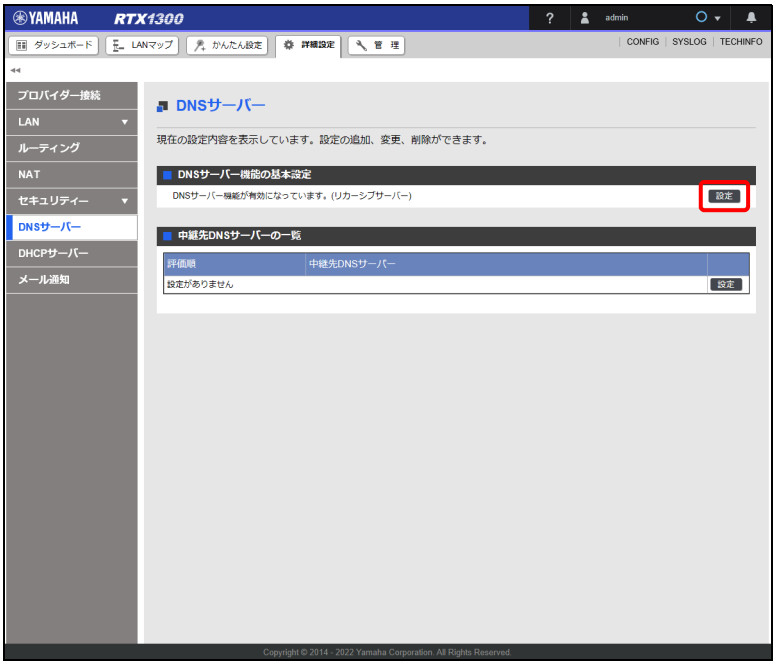
本製品の DNS サーバー機能にアクセスできるホストを変更します。

重要

プロバイダー情報が設定されると、自動的に本製品の DNS サーバー機能にアクセスできるホストが LAN1 に存在するホストに制限されるため、LAN1 に存在するホスト以外はインターネットへのアクセスができなくなります。

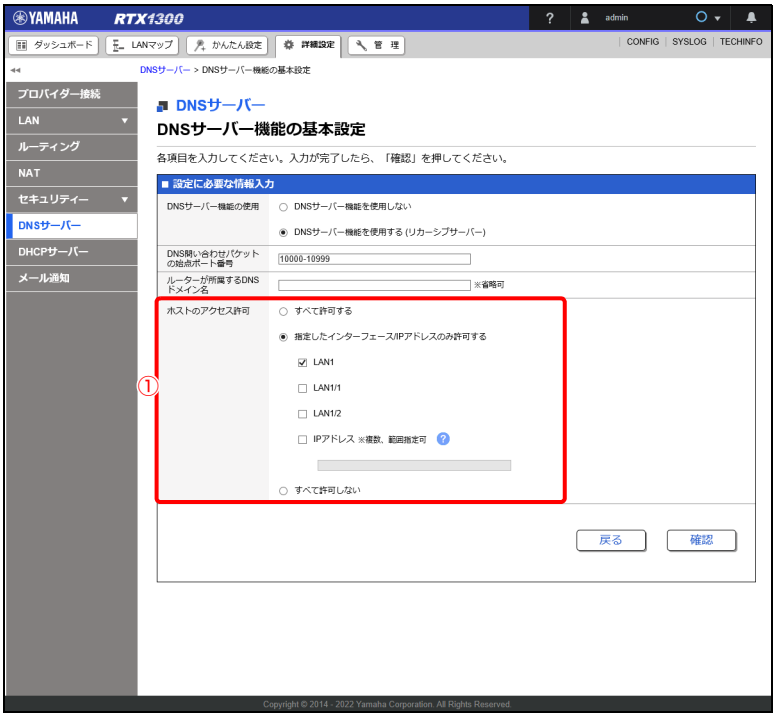
1. 「詳細設定」タブ ― 「DNS サーバー」を順に選択する。
「DNS サーバー」画面が表示されます。

2. 「DNS サーバー機能の基本設定」項目の「設定」ボタンをクリックする。



「DNS サーバー機能の基本設定」画面が表示されます。

3. ホストのアクセス許可を設定する。



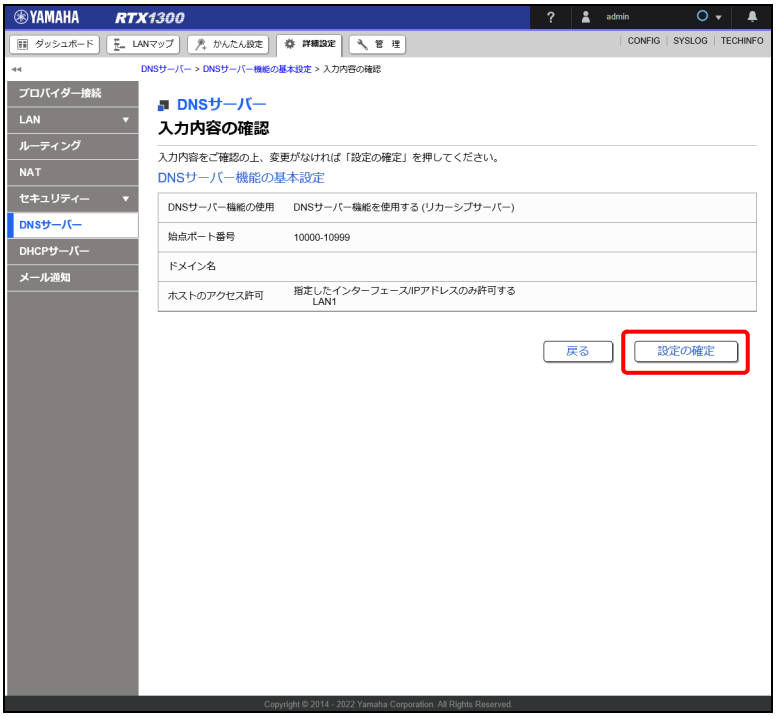
① **ホストのアクセス許可：**
ホストのアクセスを許可するインターフェースや IP アドレスの設定をします。

- **すべて許可する**
  すべてのホストからの DNS サーバー機能へのアクセスを許可します。

- **指定したインターフェース /IP アドレスのみ許可する**
  指定したインターフェースや IP アドレスからのアクセスのみを許可します。インターフェースは有効なもののみ表示されます。
  「IP アドレス」にチェックを入れるとアクセスを許可する IP アドレスを設定できます。複数の IP アドレスを設定する場合は以下のように入力してください。
  - IP アドレスの範囲を入力する場合は、2 つの IP アドレスをハイフンでつないで記述します。
    例：172.16.0.1-172.16.0.14
  - 複数の IP アドレスや IP アドレスの範囲を設定する場合は、空白で区切って記述します。
    例：172.16.0.1-172.16.0.2 172.16.0.4 172.16.0.6-172.16.0.14
- **すべて許可しない**
  すべてのホストからの DNS サーバー機能へのアクセスを禁止します。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

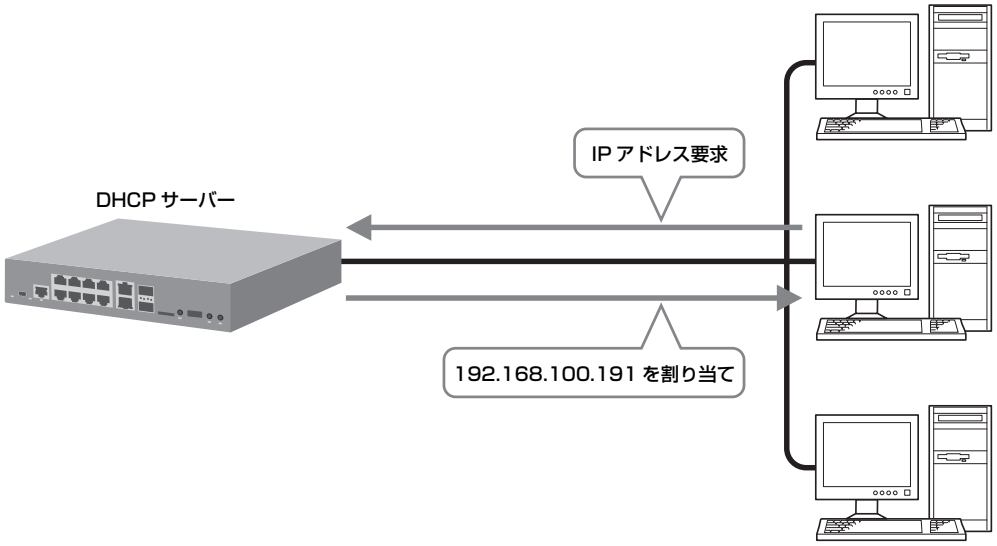
5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「DNS サーバー」画面が表示されます。

14.10 DHCP で端末に IP アドレスを割り当てる

DHCP サーバー機能を使用して端末に IP アドレスを割り当てる設定を行います。



設定例

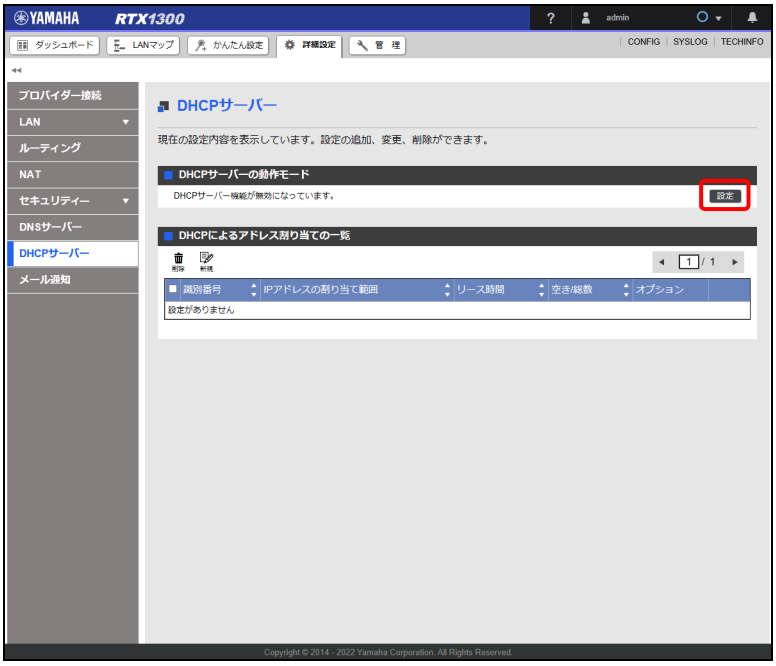
識別番号：1
IP アドレスの割り当て範囲：192.168.100.100-192.168.100.200/24
標準リース時間：24 時間
最大リース時間：72 時間

メモ

パソコン側の設定について詳しくは、「20.1 パソコンの IP アドレスを変更する」（468 ページ）をご覧ください。

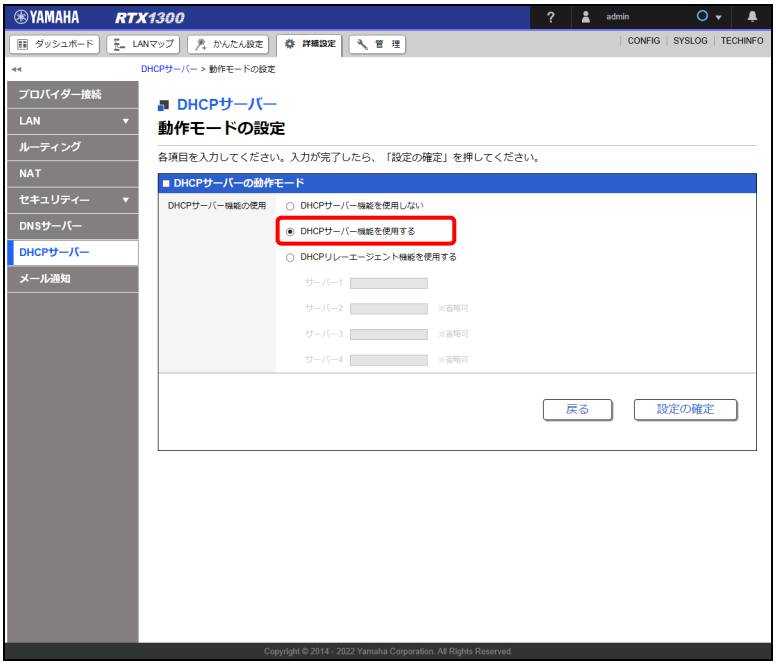
1. **「詳細設定」タブ ―「DHCP サーバー」を順に選択する。**
   「DHCP サーバー」画面が表示されます。

2.「DHCP サーバーの動作モード」項目の「設定」ボタンをクリックする。



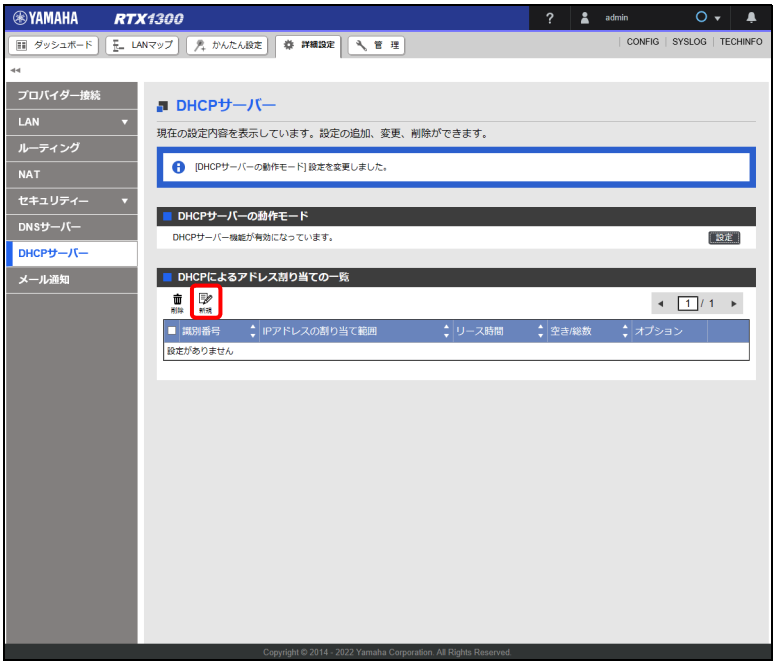
「動作モードの設定」画面が表示されます。

3.「DHCP サーバー機能を使用する」を選択し、「設定の確定」ボタンをクリックする。



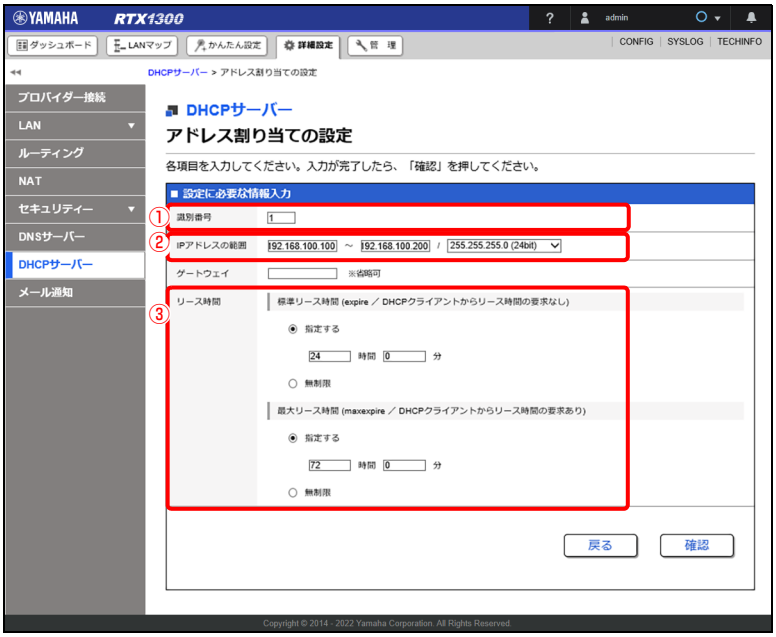
設定が反映され、「DHCP サーバー」画面が表示されます。

4. 「DHCP によるアドレス割り当ての一覧」項目の「新規」ボタンをクリックする。



「アドレス割り当ての設定」画面が表示されます。

5. IP アドレスの割り当て範囲を設定する。



① **識別番号：**
「1」を入力します。

② **IP アドレスの範囲：**
「192.168.100.100」と「192.168.100.200」を入力し、プルダウンメニューから「255.255.255.0（24bit)」を選択します。

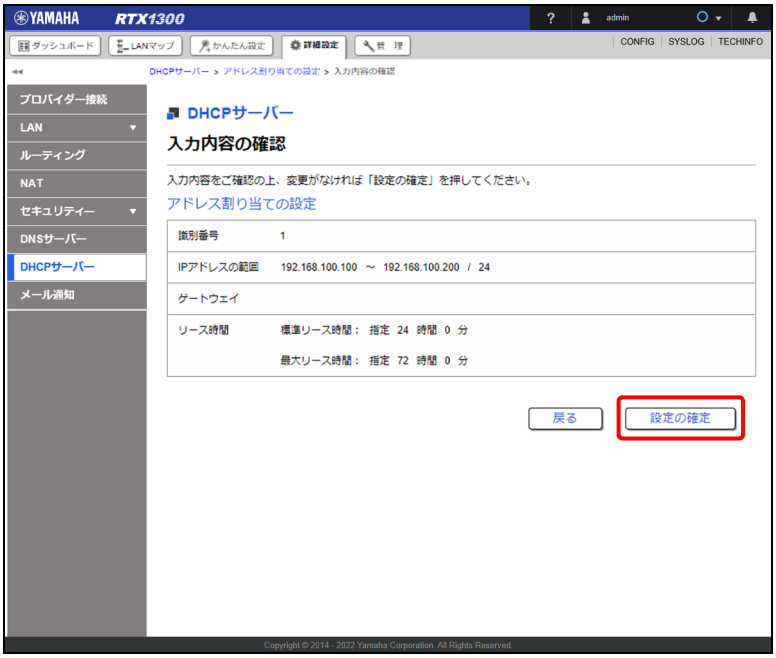
③ リース時間：

- **標準リース時間：「指定する」を選択し、「24」を入力します。**
  DHCP クライアントからリース時間の要求がない場合は、設定された期間まで IP アドレスを割り当てます。
- **最大リース時間：「指定する」を選択し、「72」を入力します。**
  DHCP クライアントからリース時間の要求がある場合は、設定された期間まで IP アドレスを割り当てます。

メモ

「無制限」を選択した場合は、無期限で IP アドレスを割り当てます。

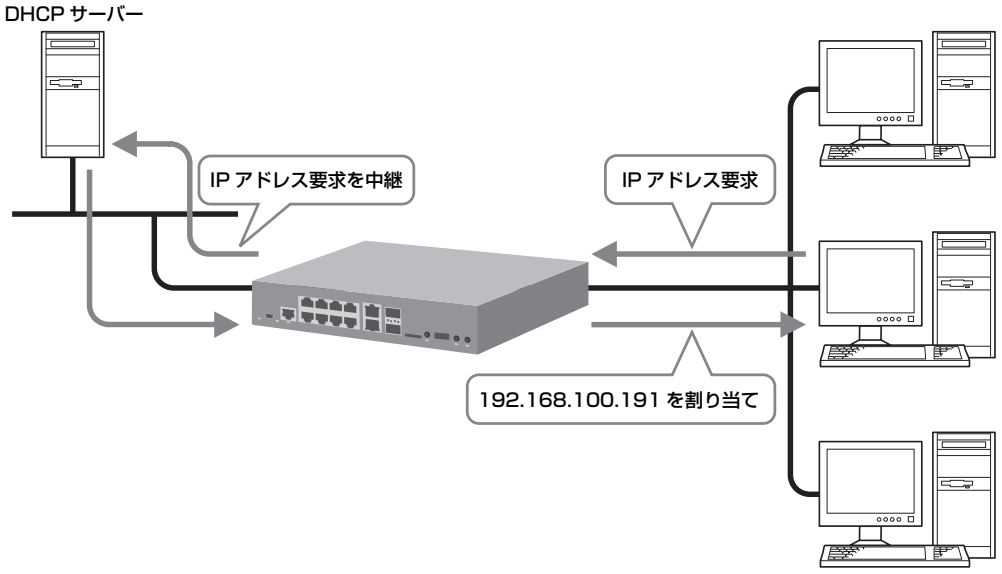
6. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。
7. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「DHCP サーバー」画面が表示されます。

14.11 異なるセグメントの DHCP サーバーから端末に IP アドレスを割り当てる

DHCP はブロードキャストで通信を行うため、DHCP サーバーが端末の存在する LAN セグメントとは異なるネットワーク上に存在する場合、通常は端末に IP アドレスを割り当てることができません。そのような環境においても、本製品を DHCP リレーエージェントとして動作させれば、異なるセグメントに存在する DHCP サーバーから端末に IP アドレスを割り当てることができるようになります。本節では、本製品を DHCP リレーエージェントとして動作させる設定方法について説明します。

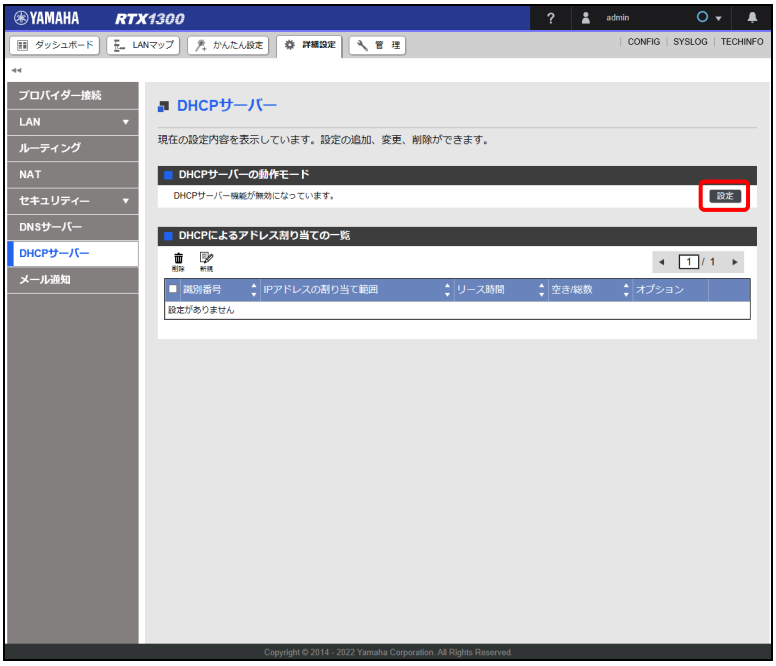


設定例

DHCP サーバーの IP アドレス：192.168.1.1

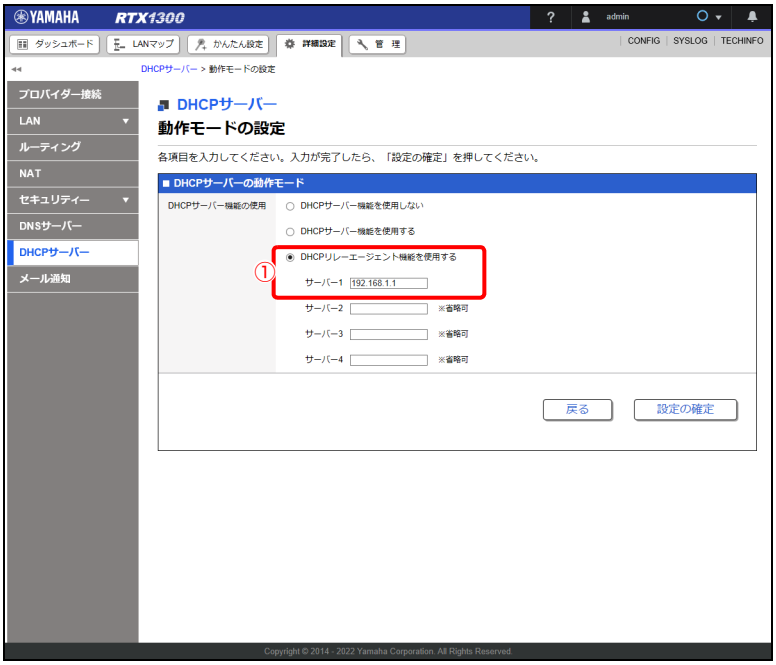
1. **「詳細設定」タブ ―「DHCP サーバー」を順に選択する。**
   「DHCP サーバー」画面が表示されます。

2. 「DHCP サーバーの動作モード」項目の「設定」ボタンをクリックする。



「動作モードの設定」画面が表示されます。

3. DHCP リレーエージェント機能の設定をする。



① **DHCP サーバー機能の使用：**
「DHCP リレーエージェント機能を使用する」を選択し、「192.168.1.1」を入力します。

4. **内容を確認し、「設定の確定」ボタンをクリックする。**
設定が反映され、「DHCP サーバー」画面が表示されます。

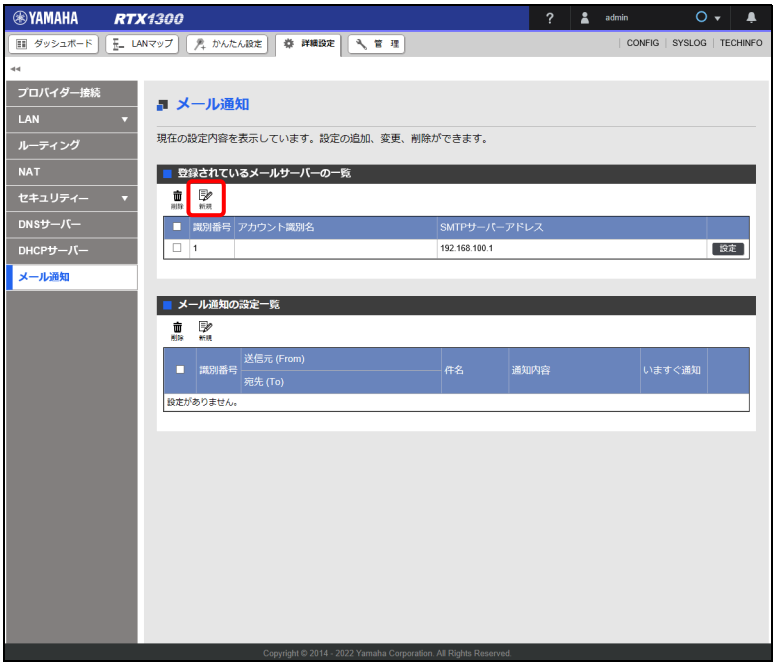
14.12 メール通知機能を使う

ネットワーク上で異常が検知されたときに、指定した宛先にメールで通知する設定を行います。また、インターフェースや経路の情報を、指定した宛先に手動で通知することもできます。

14.12.1 メールサーバーを設定する

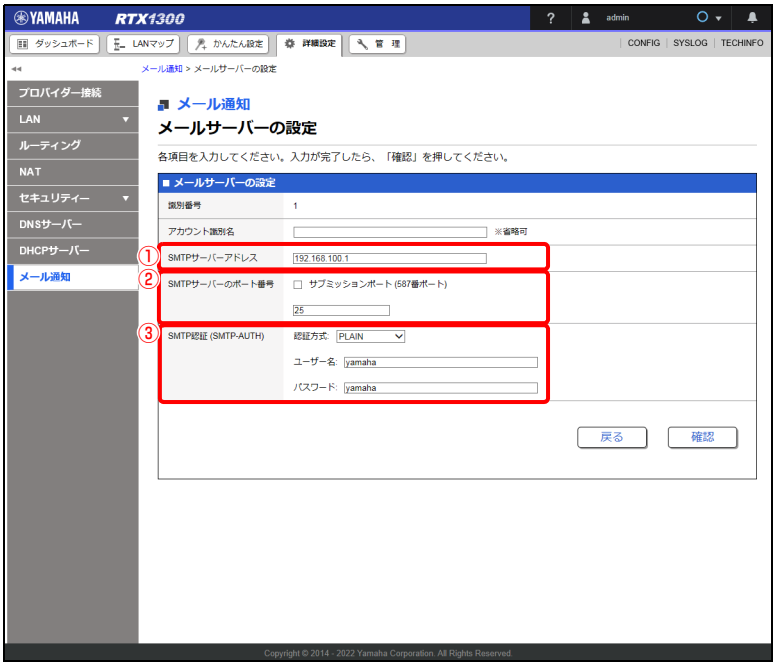
宛先のメールサーバー（SMTP サーバー）を設定します。

1. **「詳細設定」タブ ―「メール通知」を順に選択する。**
   「メール通知」画面が表示されます。
2. **「登録されているメールサーバーの一覧」項目の「** 新規 **」ボタンをクリックする。**



「メールサーバーの設定」画面が表示されます。

3. メールサーバーを設定する。



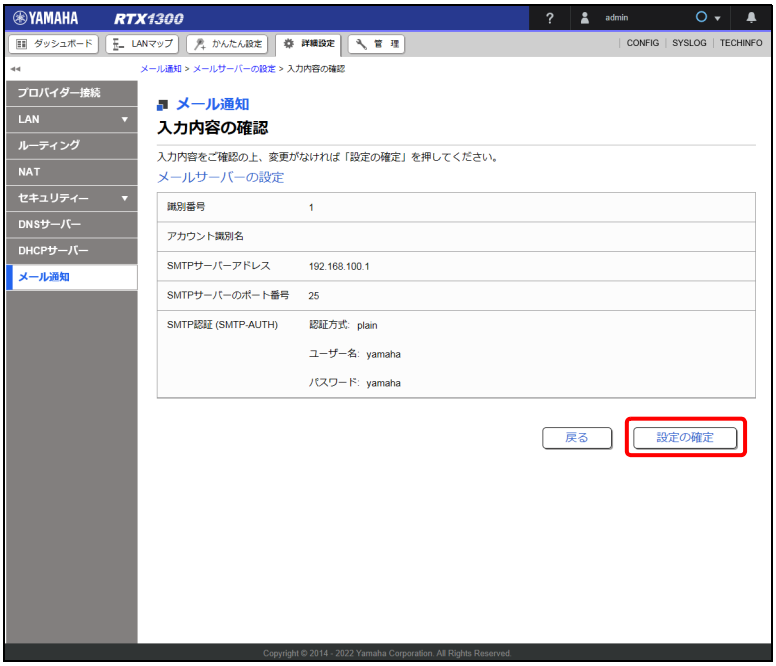
① **SMTP サーバーアドレス：**
メールを送信するときに使用する SMTP サーバーの IP アドレス、またはドメイン名を入力します。

② **SMTP サーバーのポート番号：**
SMTP サーバーのポート番号を入力します。
「サブミッションポート（587 番ポート）」を選択すると、サブミッションポートの 587 番ポートが設定されます。

③ **SMTP 認証（SMTP-AUTH）：**
SMTP サーバーとの認証方式を選択し、ユーザー名とパスワードを入力します。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「メール通知」画面が表示されます。

14.12.2 メール通知を設定する

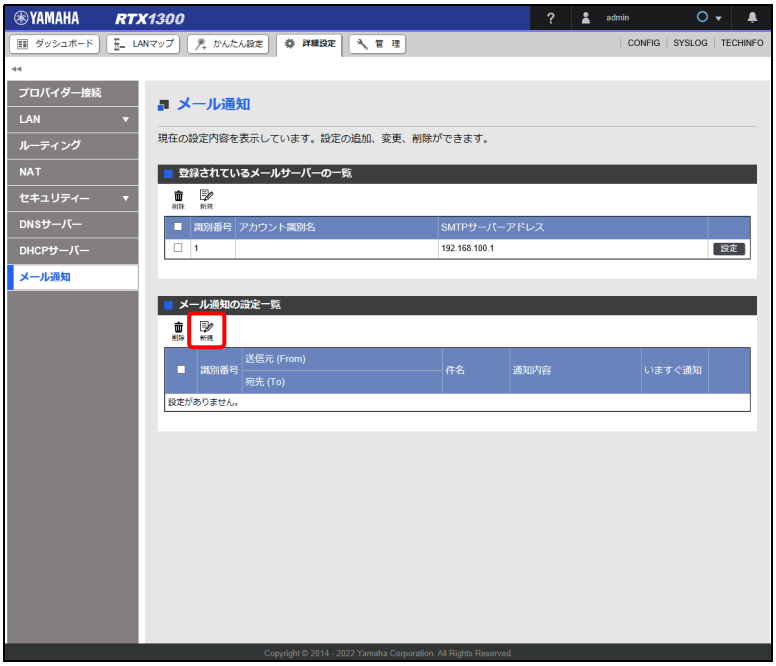
メール通知の送信元、宛先アドレスや、通知内容などを設定します。

重要

メール通知を設定する場合、事前にメールサーバーの設定が必要です。設定の詳細は「14.12.1 メールサーバーを設定する」（386 ページ）をご覧ください。

1. **「詳細設定」タブ ―「メール通知」を順に選択する。**
   「メール通知」画面が表示されます。

2.「メール通知の設定一覧」項目の「新規」ボタンをクリックする。



「メール通知の設定」画面が表示されます。

重要

「メール通知の設定一覧」に新規設定を追加する場合、事前にメールサーバーの設定（「14.12.1 メールサーバーを設定する」（386 ページ））が必要です。

3. メール通知を設定する。

① **送信元（From）：**
メールを送信するときに使用する SMTP サーバーの IP アドレス、またはドメイン名を選択します。

② **宛先（To）：**
送信するメールの宛先のメールアドレスを 4 件まで入力します。

③ **件名：**
送信するメールの件名を入力します。
「既定の件名を使う」を選択すると、既定の件名で送信されます。

④ **通知内容：**
通知内容を選択します。

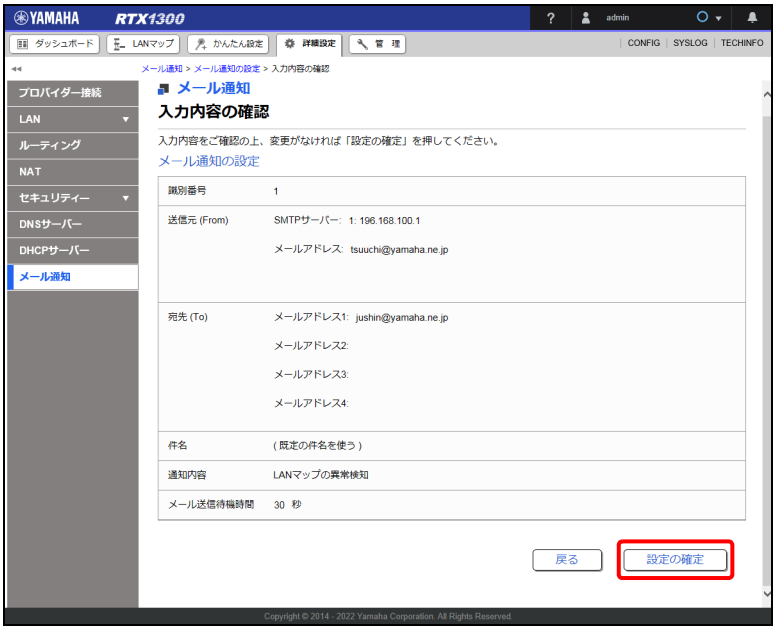
⑤ **メール送信待機時間：**
通知イベントが発生してから、メール送信を待機する時間を入力します。待機中に他の通知イベントが発生した場合、それらの通知内容も一通のメールにまとめて送信されます。

重要

内部状態は自動では送信されません。「メール通知」画面の「進む」ボタンをクリックして、「実行」ボタンをクリックすると、指定した宛先に内部状態が通知されます。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「メール通知」画面が表示されます。

重要

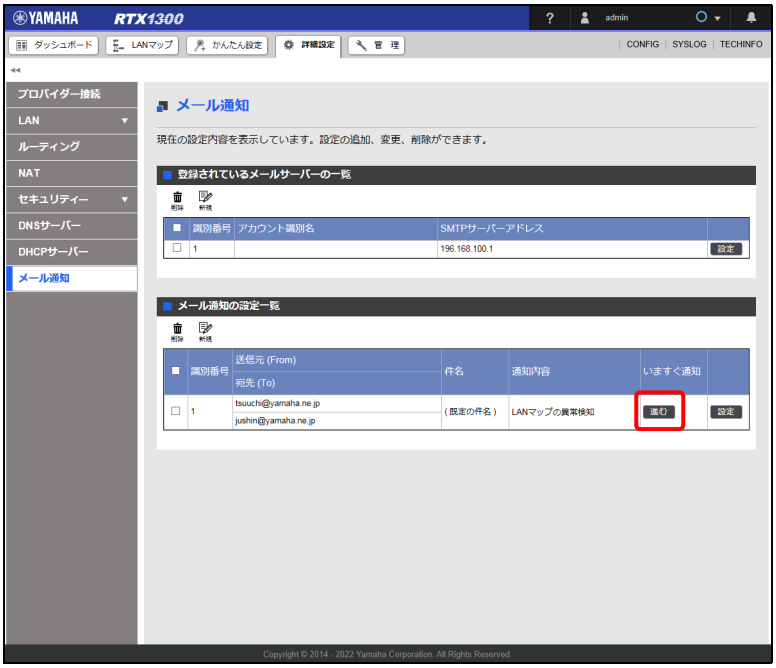
メールサーバーが未設定の場合、メール通知を設定できません。

14.12.3 本製品の内部状態をメールで通知する

本製品の内部状態を登録した宛先へ通知します。

1. **「詳細設定」タブ－「メール通知」を順に選択する。**
   「メール通知」画面が表示されます。

2. 「いますぐ通知」の「進む」ボタンをクリックする。

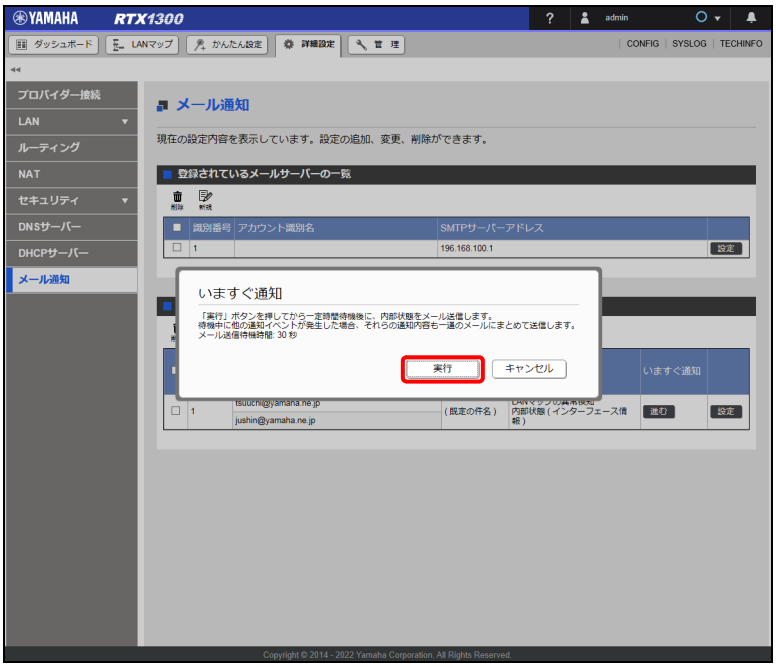


「いますぐ通知」ダイアログが表示されます。

メモ

「進む」ボタンは、「メール通知の設定」画面の通知内容で内部状態を選択している場合に表示されます。

3. 「いますぐ通知」ダイアログの「実行」ボタンをクリックする。



本製品の内部状態が登録した宛先へ通知されます。

第 15 章 本製品を管理する

本章では、ファームウェアの更新を行ったり、CONFIG ファイルを外部メモリーへエクスポートして保存したりするといった、本製品の管理に関連する操作について説明します。

- 本製品の日時を合わせる …393 ページ
- ブザーを設定する …395 ページ
- DOWNLOAD ボタンに機能を割り当てる …397 ページ
- SYSLOG を外部メモリーへ保存する …402 ページ
- 外部メモリー内のファイルを用いて起動する …405 ページ
- 外部メモリー内のファイルをインポートする …408 ページ
- コマンドを実行する …411 ページ
- ファームウェアを更新する …414 ページ
- 設定（CONFIG）を管理する …426 ページ
- SYSLOG を管理する …437 ページ
- 本製品を再起動する …442 ページ
- 本製品を工場出荷時の状態へ戻す …444 ページ

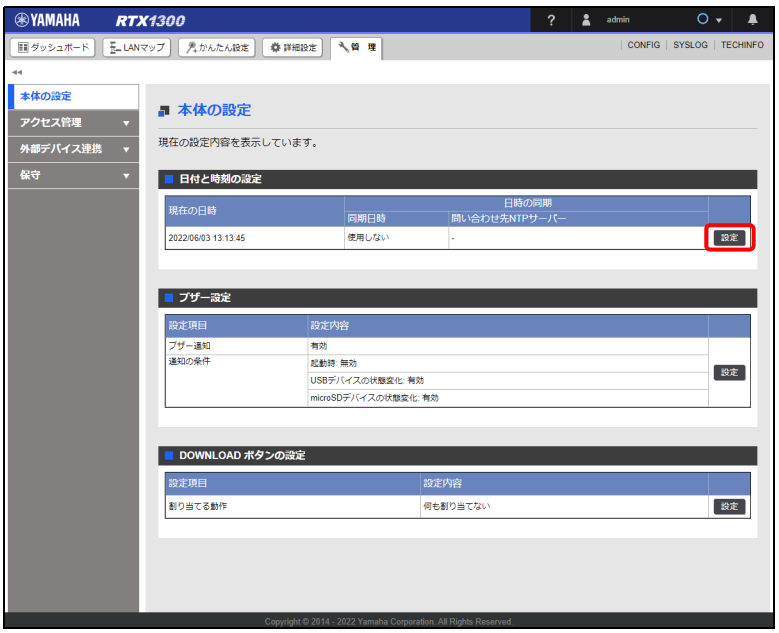
15.1 本製品の日時を合わせる

現在日時の設定や、NTP サーバーとの同期の設定を行います。

15.1.1 日付と時刻を設定する

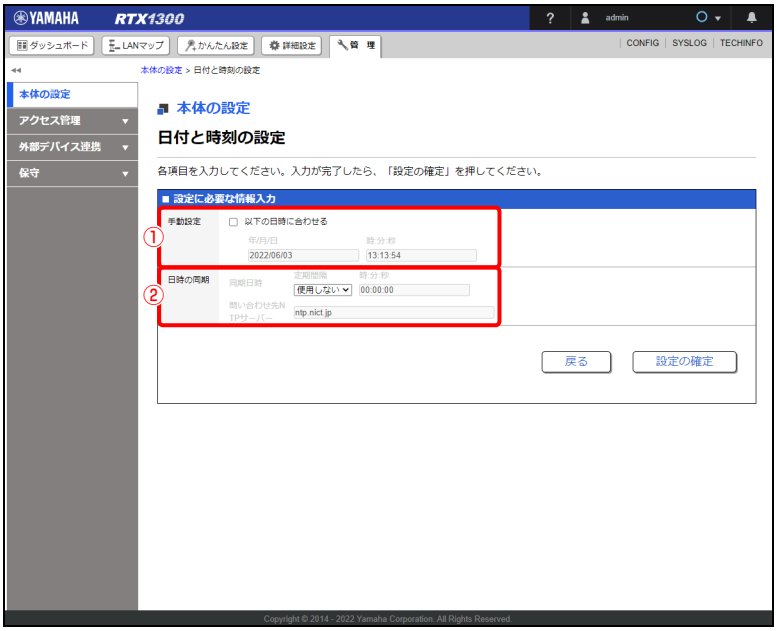
1. **「管理」タブ ― 「本体の設定」を順に選択する。**
   「本体の設定」画面が表示されます。

2. **「日付と時刻の設定」項目の「設定」ボタンをクリックする。**



「日付と時刻の設定」画面が表示されます。

3. 日付と時刻を設定する。



① 手動設定：

日時の設定を更新する場合は、「以下の日時に合わせる」にチェックを入れます。

・「年 / 月 / 日」：日付を YYYY/MM/DD 形式で入力します。「年 / 月 / 日」欄にマウスカーソルを重ねてクリックするとカレンダーが表示され、カレンダーから日付を選択することもできます。

・「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にマウスカーソルを重ねてクリックすると時刻のリストが表示され、リストから時刻を選択することもできます。

② 日時の同期：

日時を自動的に補正したい場合は、日時同期のスケジュールと問い合わせ先の NTP サーバーを設定します。

・定期間隔：NTP サーバーとの同期する間隔を選択します。

・「時 : 分 : 秒」：時刻を hh:mm:ss 形式で入力します。「時 : 分 : 秒」欄にマウスカーソルを重ねてクリックすると時刻のリストが表示され、リストから時刻を選択することもできます。

・問い合わせ先 NTP サーバー：同期を行う NTP サーバーのホスト名または IP アドレスを入力します。

メモ

・NTP サーバーの負荷を分散させるためにも、00 分 00 秒のようにアクセスが集中しやすい時刻を避けた同期日時に設定することをおすすめします。

・日付と時刻の設定、および、NTP サーバーとの同期の設定は、「かんたん設定」―「基本設定」―「日付と時刻の設定」画面から行うこともできます。

4. 「設定の確定」ボタンをクリックする。

設定が反映され、「本体の設定」画面が表示されます。

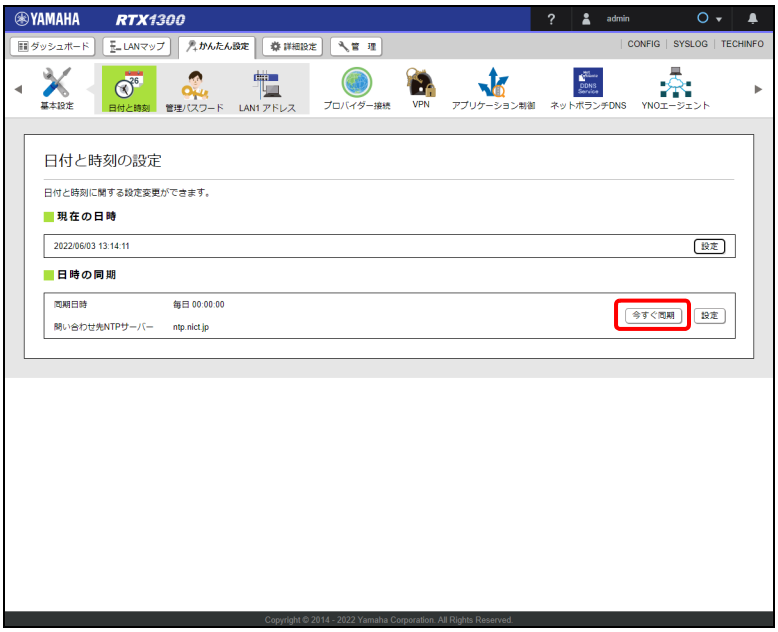
15.1.2 NTP サーバーと今すぐ同期する

重要

日時同期のスケジュールと問い合わせ先 NTP サーバーが設定され、インターネットに接続している場合のみ行えます。

1. **「かんたん設定」タブ ―「基本設定」―「日付と時刻」ボタンを順に選択する。**
   「日付と時刻の設定」画面が表示されます。

2. **「日時の同期」項目の「今すぐ同期」ボタンをクリックする。**



NTP サーバーとの同期が開始されます。

15.2 ブザーを設定する

ブザーの有効 / 無効の切り換えや通知条件の設定を行います。

Web GUI で設定できるブザー

- microSD 機能に関連するブザー
- USB ホスト機能に関連するブザー
- 起動時のブザー

メモ

Web GUI で設定できるブザーは、コマンドでも設定することができます。

コマンドで設定できるブザー

- バッチファイル実行機能に関連するブザー（alarm batch）
- HTTP リビジョンアップ機能に関連するブザー（alarm http revision-up）
- HTTP アップロード機能に関連するブザー（alarm http upload）
- Lua スクリプト機能に関連するブザー（alarm lua）
- 携帯端末の接続時のブザー（alarm mobile）

メモ

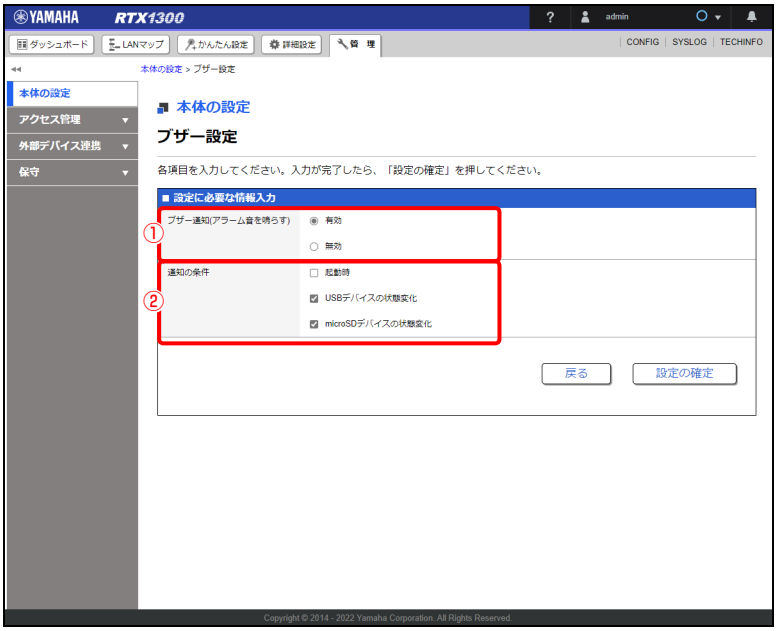
Web GUI で設定できないブザーの設定方法について詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

1. **「管理」タブ ―「本体の設定」を順に選択する。**
   「本体の設定」画面が表示されます。

2. **「ブザー設定」項目の「設定」ボタンをクリックする。**

「ブザー設定」画面が表示されます。

3. **ブザーを設定する。**



① **ブザー通知（アラーム音を鳴らす）：**
ブザー通知を有効にするか無効にするかを選択します。

② **通知の条件：**
ブザー通知を行う条件にチェックを入れます。

4. **「設定の確定」ボタンをクリックする。**
設定が反映され、「本体の設定」画面が表示されます。

15.3 DOWNLOAD ボタンに機能を割り当てる

本製品の DOWNLOAD ボタンを 3 秒以上押したときに、実行する動作を割り当てます。

DOWNLOAD ボタンに割り当てられる動作

- 何も動作を割り当てない
- ネットワーク経由でファームウェアを更新する
- USB 接続型データ通信端末の電波受信レベルを取得する

メモ

工場出荷状態では、DOWNLOAD ボタンには何も割り当てられていません。DOWNLOAD ボタンに動作を割り当てる場合は、以下のいずれかの設定を行ってください。

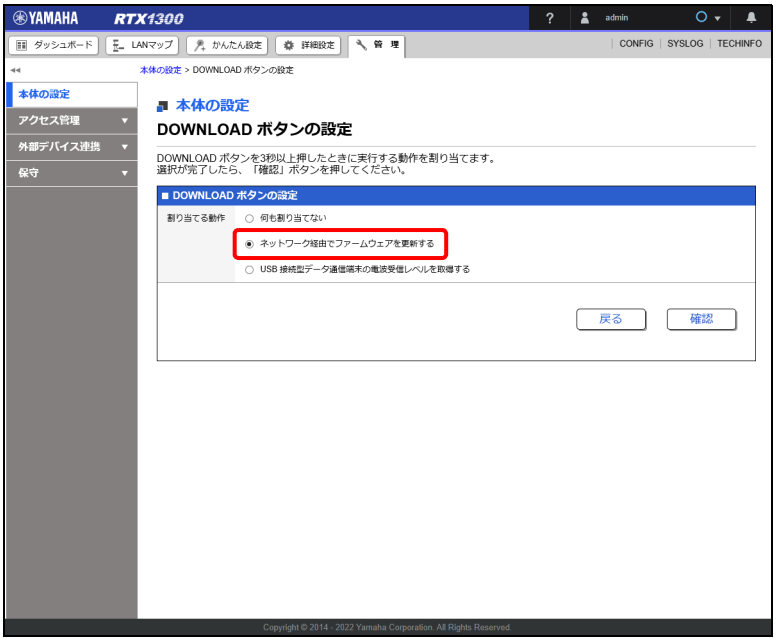
15.3.1 ネットワーク経由でファームウェアを更新する

1. **「管理」タブ ―「本体の設定」を順に選択する。**
「本体の設定」画面が表示されます。

2. **「DOWNLOAD ボタンの設定」項目の「設定」ボタンをクリックする。**

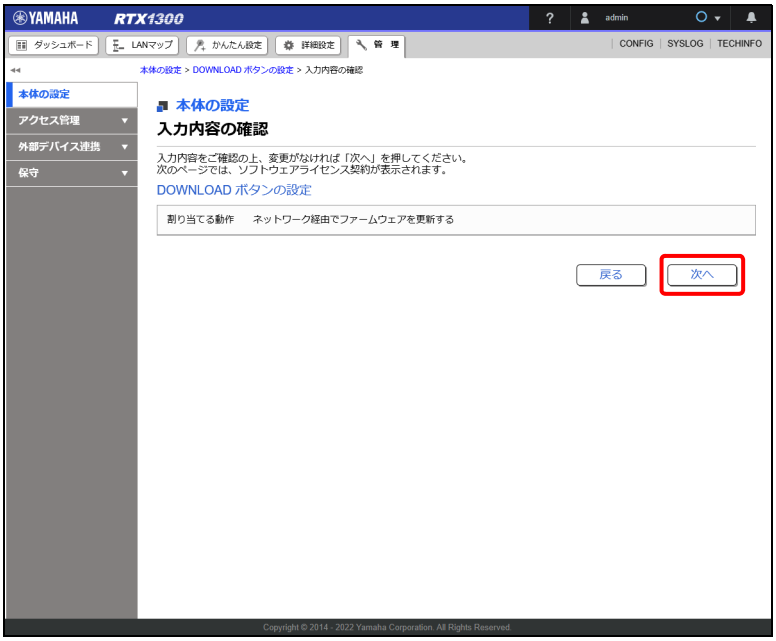
「DOWNLOAD ボタンの設定」画面が表示されます。

3. 「ネットワーク経由でファームウェアを更新する」を選択する。



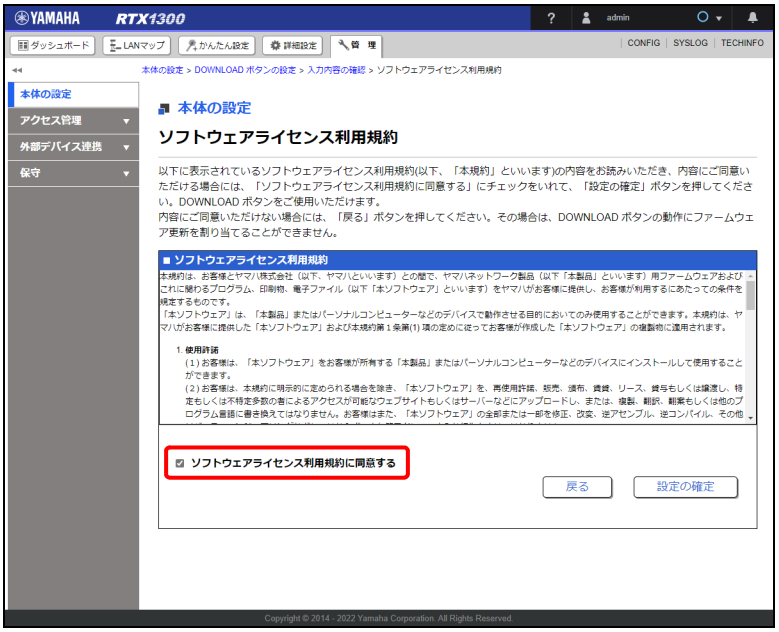
4. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

5. 入力内容を確認し、問題がなければ「次へ」ボタンをクリックする。



「ソフトウェアライセンス利用規約」画面が表示されます。

6. ソフトウェアライセンス利用規約の内容をよく確認し、「ソフトウェアライセンス利用規約に同意する」のチェックボックスにチェックを入れます。



7. 「設定の確定」ボタンをクリックする。
   設定が反映され、「本体の設定」画面が表示されます。

メモ

本設定を行った後、本製品の DOWNLOAD ボタンを 3 秒以上押すと、ネットワーク経由でファームウェアが更新されます。すでにファームウェアリビジョンが最新になっている場合や、本製品がインターネットに接続されていない場合は、ファームウェアは更新されません。

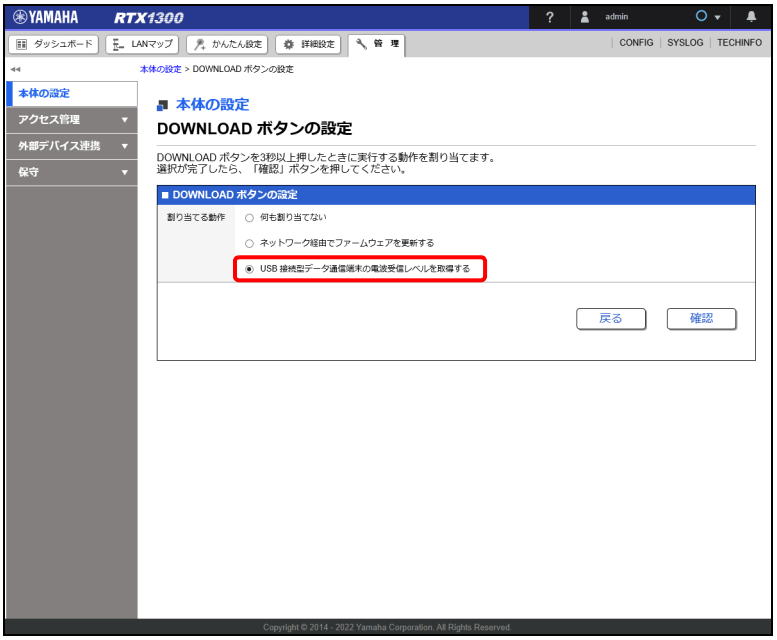
15.3.2 USB 接続型データ通信端末の電波受信レベルを取得する

1. **「管理」タブ ―「本体の設定」を順に選択する。**
   「本体の設定」画面が表示されます。

2. **「DOWNLOAD ボタンの設定」項目の「設定」ボタンをクリックする。**

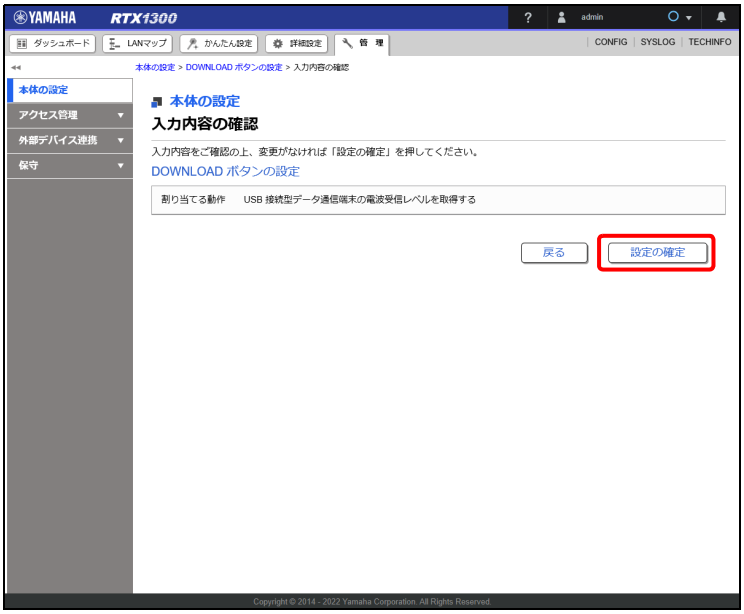
「DOWNLOAD ボタンの設定」画面が表示されます。

3. **「USB 接続型データ通信端末の電波受信レベルを取得する」を選択する。**



4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

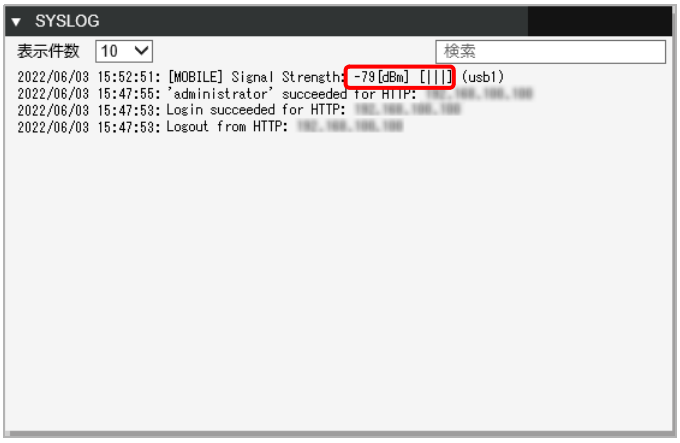
5. 入力内容を確認し、「設定の確定」ボタンをクリックする。



設定が反映され、「本体の設定」画面が表示されます。

メモ

- 本設定を行った後、本製品の DOWNLOAD ボタンを 3 秒以上押すと、USB 端子に接続している USB 接続型データ通信端末の電波受信レベルが、SYSLOG に表示されます。
- 電波受信のレベルは、dBm 値またはレベル値と、4 段階の縦線（0 本～ 3 本）で表示されます。dBm 値とレベル値のどちらが表示されるかは接続している通信端末に依存します。



15.4 SYSLOG を外部メモリーへ保存する

SYSLOG を、本製品の USB ポートや microSD スロットに接続している外部メモリーに保存するための設定を行います。

注意

本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損させることがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。

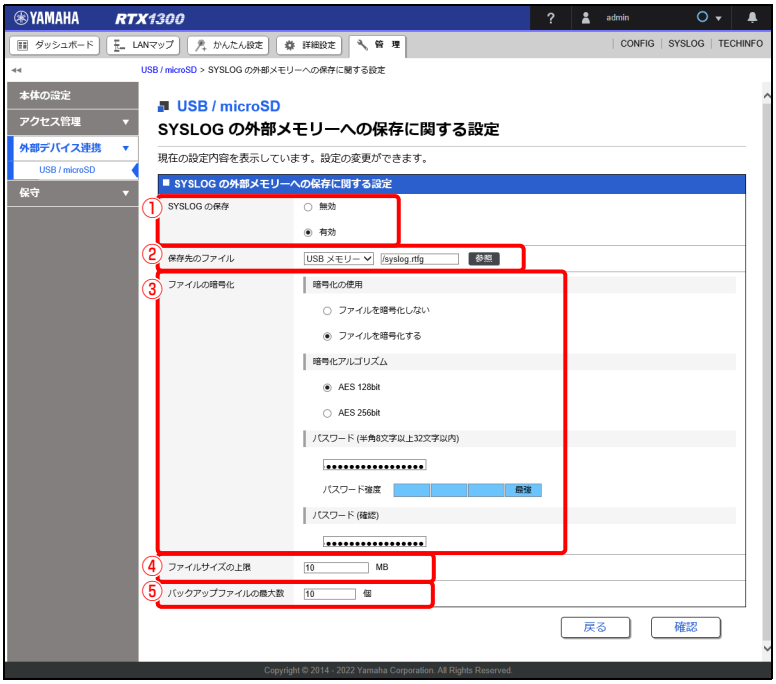
メモ

SYSLOG を外部ホストに出力する設定や、SYSLOG へ書き出す内容の設定については、「15.10 SYSLOG を管理する」（437 ページ）をご覧ください。

1. **「管理」タブ —「外部デバイス連携」—「USB/microSD」を順に選択する。**
   「USB/microSD」画面が表示されます。
2. **「SYSLOG の外部メモリーへの保存」項目の「設定」ボタンをクリックする。**

「SYSLOG の外部メモリーへの保存に関する設定」画面が表示されます。

3. SYSLOG の外部メモリーへの保存に関する設定を行う。



① **SYSLOG の保存：**
SYSLOG を外部メモリーに保存する場合は、「有効」を選択します。

② **保存先のファイル：**
挿し込んだ外部メモリーを選択し、既存のファイルへ保存する場合は「参照」ボタンをクリックし、「ファイルの一覧」画面で保存先のファイルを選択します。新規のファイルへ保存する場合は、任意のファイル名を入力します。ファイルパスの指定も認識されます。

メモ

- 拡張子が「.bak」のファイルは指定できません。また、「ファイルを暗号化しない」を選択した場合は、拡張子が「.rtfg」のファイルは指定できません。「ファイルを暗号化する」を選択した場合は、拡張子が「.rtfg」のファイルか、拡張子がついていないファイルのみ指定できます。
- 「ファイルを暗号化する」を選択し、かつ拡張子がついていないファイルを指定した場合は、自動で拡張子「.rtfg」が付与されます。
- 指定できるファイルパスは、全体の長さが半角 230 文字以内で、1 つのディレクトリ名が半角 99 文字以内です。
- 指定できるファイル名の長さは、「ファイルを暗号化する」を選択し、かつファイル名に拡張子がついていない場合は半角 78 文字以内、それ以外の場合は半角 83 文字以内です。

③ **ファイルの暗号化：**
保存する SYSLOG ファイルを暗号化する場合は、「ファイルを暗号化する」を選択してから、暗号化アルゴリズムを選択し、任意のパスワードを入力します。

メモ

- 暗号化した SYSLOG ファイルは、Windows アプリケーションの「RT-FileGuard」で復号できます。「RT-FileGuard」は、http://www.rtpro.yamaha.co.jp/RT/utility/ からダウンロードできます。
- パスワードは、長さ 8 ～ 32 文字の半角英数字と半角記号が使用できます。英字の大文字と小文字は区別されます。
  以下の半角記号を使用することができます。
  !"#$%&'()=~|-^\`{@[+*};:]<>?_,./\

④ **ファイルサイズの上限：**
SYSLOG を保存するファイルのファイルサイズの上限を設定します。

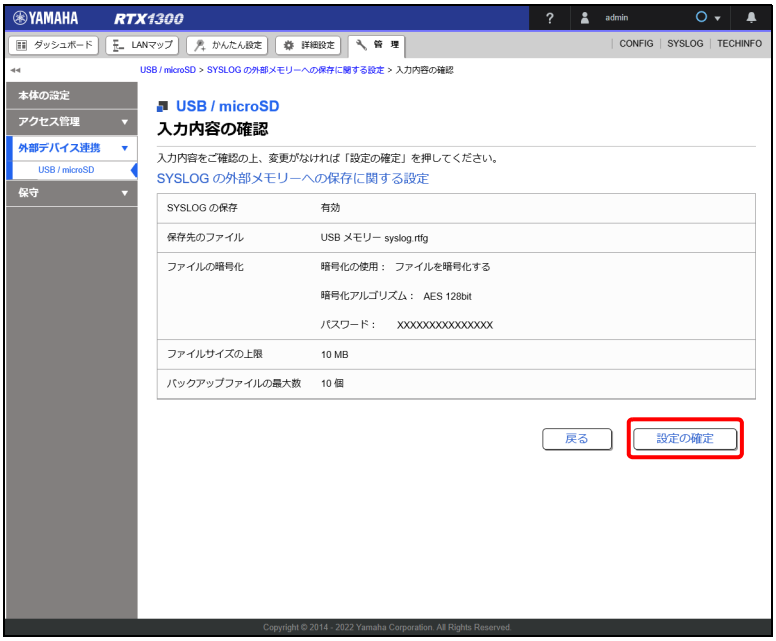
メモ
ファイルサイズが上限値に達した場合は、ファイル名の末尾に「_yyyymmdd_hhmmss」(_ 年月日 _ 時分秒）が付与されたバックアップファイルが自動で生成されます。

⑤ **バックアップファイルの最大数：**
生成されるバックアップファイルの最大数を設定します。

メモ
バックアップファイル数が最大数に達した場合は、最も古いバックアップファイルが削除されてから、新しいバックアップファイルが生成されます。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **入力内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「USB/microSD」画面が表示されます。

メモ
外部メモリーに保存した SYSLOG ファイルを参照する場合は、外部メモリーをパソコンに接続し、該当のファイルをテキストエディタなどで表示します。SYSLOG ファイルを暗号化している場合は、「RT-FileGuard」でいったん復号してからテキストエディタなどで表示します。

15.5 外部メモリー内のファイルを用いて起動する

本製品に接続している外部メモリーに保存している CONFIG ファイルや、ファームウェアファイルを用いて本製品を起動するための設定を行います。設定後、本製品を再起動すると、外部メモリー内の CONFIG ファイルやファームウェアファイルが使用されます。

注意

- 本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損させることがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。
- 管理者権限を持つユーザーの設定がない CONFIG ファイルを使用して本製品を起動した場合は、初期管理ユーザー「admin」が追加されます。なお、初期管理ユーザーのパスワードを変更するまでの間は、WAN 側の通信が制限されます。

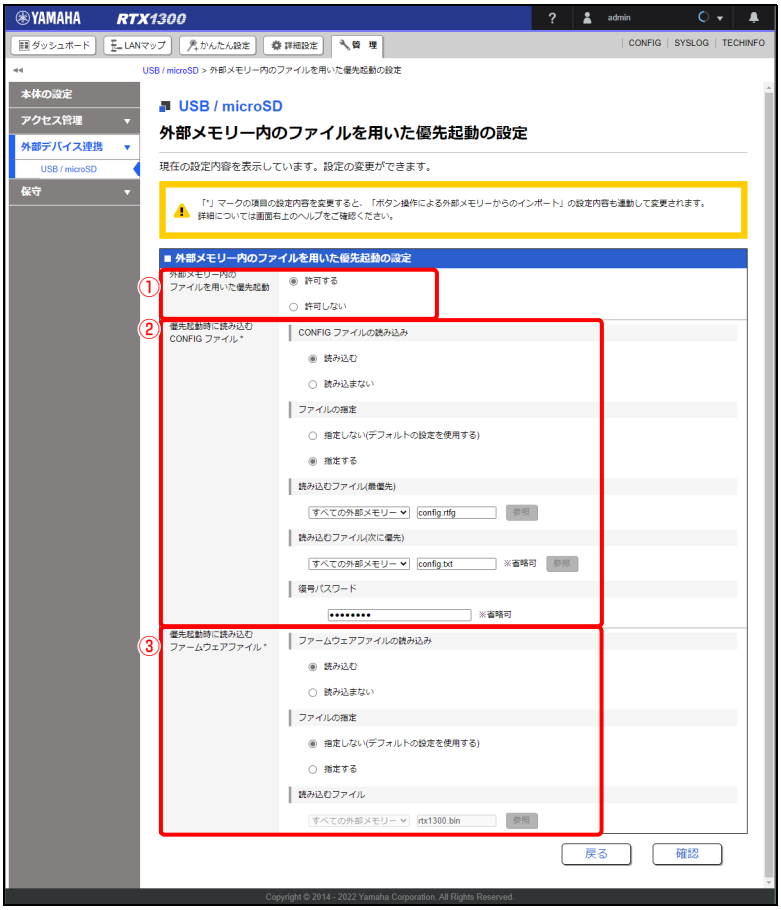
メモ

外部メモリー内の CONFIG ファイルを使用して本製品を起動している場合は、本製品の設定を変更すると、変更内容が起動時に使用した外部メモリー内の CONFIG ファイルに保存されます。

1. **「管理」タブ ―「外部デバイス連携」―「USB/microSD」を順に選択する。**
   「USB/microSD」画面が表示されます。
2. **「外部メモリー内のファイルを用いた優先起動」項目の「設定」ボタンをクリックする。**

「外部メモリー内のファイルを用いた優先起動の設定」画面が表示されます。

3. 外部メモリー内のファイルを用いた優先起動に関する設定を行う。



① 外部メモリー内のファイルを用いた優先起動：
本製品に接続した外部メモリー内の CONFIG ファイル、およびファームウェアファイルからの起動を許可するか設定します。

② 優先起動時に読み込む CONFIG ファイル：
本製品起動時に外部メモリーから CONFIG ファイルを読み込む場合は、「CONFIG ファイルの読み込み」項目の「読み込む」を選択します。
任意のファイルを指定する場合は、「ファイルの指定」項目の「指定する」を選択し、「読み込むファイル（最優先）」項目で参照する外部メモリーを選択してから、「参照」ボタンをクリックして CONFIG ファイルを選択します。
CONFIG ファイルが暗号化されている場合は、「復号パスワード」項目にパスワードを入力します。

メモ

- 「ファイルの指定」項目で「指定しない」を選択した場合は、microSD カード、USB メモリーの順に、デフォルト設定のファイル名「*:config.rtfg」または「*:config.txt」を検索し使用します。デフォルト設定のファイル名が見つからない場合は、本製品内蔵の不揮発性メモリー内の CONFIG ファイルを使用します。
- 「読み込むファイル（最優先）」項目および「読み込むファイル（次に優先）」項目で「すべての外部メモリー」を選択した場合は、読み込むファイルを microSD カード、USB メモリーの順で検索し使用します。
- 「読み込むファイル（最優先）」項目で設定したファイルが見つからない場合、「読み込むファイル（次に優先）」項目で設定したファイルが使用されます。
- 指定できる CONFIG ファイルのファイル名の長さは、半角 99 文字以内です。

・「優先起動時に読み込む CONFIG ファイル」項目の設定を変更すると、「ボタン操作による外部メモリーからのインポートに関する設定」—「インポートする CONFIG ファイル」項目も連動して変更されます。

③ 優先起動時に読み込むファームウェアファイル：

本製品起動時に外部メモリーからファームウェアファイルを読み込む場合は、「ファームウェアファイルの読み込み」項目の「読み込む」を選択します。

任意のファイルを指定する場合は、「ファイルの指定」項目の「指定する」を選択し、「読み込むファイル（最優先）」項目で参照する外部メモリーを選択してから、「参照」ボタンをクリックしてファームウェアファイルを選択します。

メモ

・「ファイルの指定」項目で「指定しない」を選択した場合は、microSD カード、USB メモリーの順に、デフォルト設定のファイル名「*:rtx1300.bin」を検索し使用します。デフォルト設定のファイル名が見つからない場合は、本製品内蔵の不揮発性メモリー内のファームウェアファイルを使用します。

・「読み込むファイル（最優先）」項目および「読み込むファイル（次に優先）」項目で「すべての外部メモリー」を選択した場合は、読み込むファイルを microSD カード、USB メモリーの順で検索し使用します。

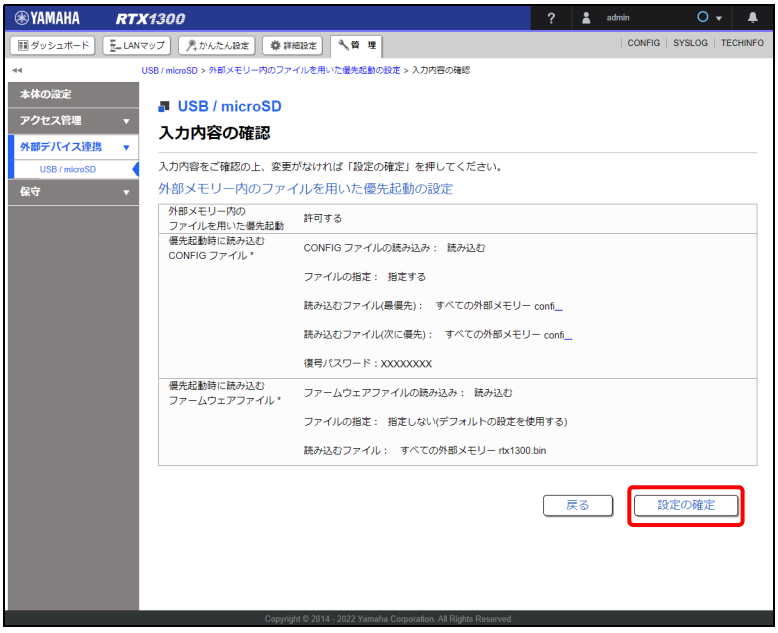
・指定できるファームウェアファイルのファイル名の長さは、半角 99 文字以内です。

・「優先起動時に読み込むファームウェアファイル」項目の設定を変更すると、「ボタン操作による外部メモリーからのインポートに関する設定」—「インポートするファームウェアファイル」項目も連動して変更されます。

4. **「確認」ボタンをクリックする。**

「入力内容の確認」画面が表示されます。

5. **入力内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「USB/microSD」画面が表示されます。

メモ

本設定を行った後、本製品を再起動すると、外部メモリー内の CONFIG ファイル、およびファームウェアファイルを使用して起動します。

15.6 外部メモリー内のファイルをインポートする

外部メモリー内に格納されている CONFIG ファイルやファームウェアファイルを本製品にインポートするために必要な設定を行います。設定後、本製品の microSD ボタン、または USB ボタンを押しながら DOWNLOAD ボタンを 3 秒以上押し続けると、microSD カード、または USB メモリーから CONFIG ファイル、およびファームウェアファイルが内蔵不揮発性メモリーにインポートされます。

注意

本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損させることがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。

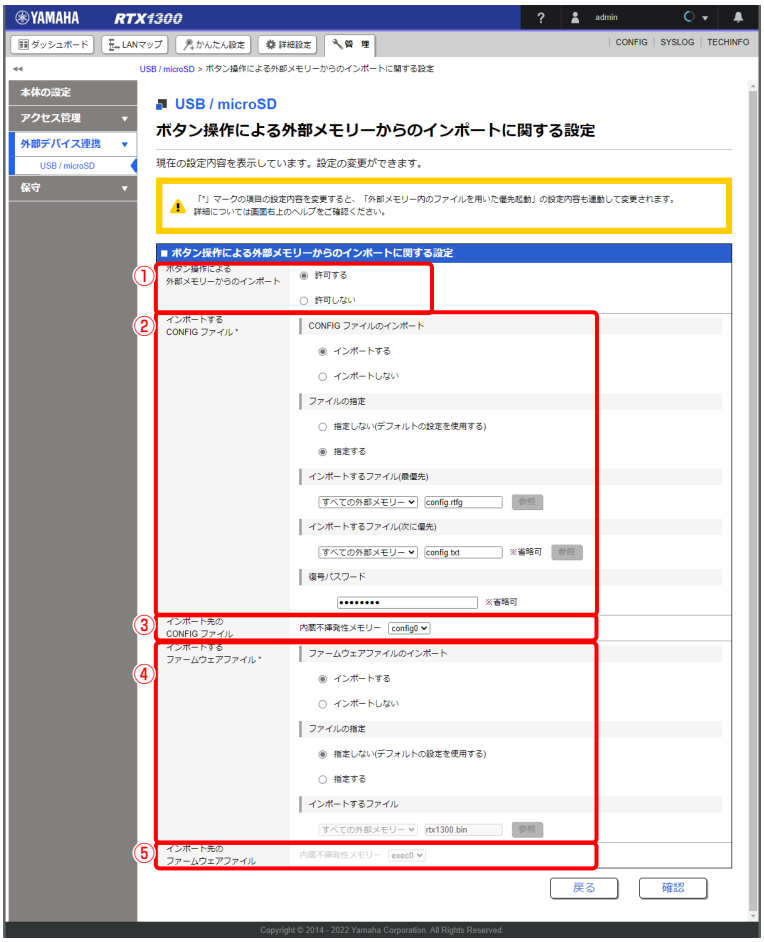
メモ

インポートとは、本製品内蔵の不揮発性メモリーに保存することを意味します。

1. **「管理」タブ ―「外部デバイス連携」―「USB/microSD」を順に選択する。**
   「USB/microSD」画面が表示されます。
2. **「ボタン操作による外部メモリーからのインポート」項目の「設定」ボタンをクリックする。**

「ボタン操作による外部メモリーからのインポートに関する設定」画面が表示されます。

3. ボタン操作による外部メモリーからのインポートに関する設定を行う。



① ボタン操作による外部メモリーからのインポート：
外部メモリー内の CONFIG ファイル、およびファームウェアファイルを、本製品の不揮発性メモリーへインポートすることを許可するか設定します。

② インポートする CONFIG ファイル：
外部メモリーから CONFIG ファイルをインポートする場合は、「CONFIG ファイルのインポート」項目の「インポートする」を選択します。
任意のファイルを指定する場合は、「ファイルの指定」項目の「指定する」を選択し、「インポートするファイル（最優先）」項目で参照する外部メモリーを選択してから、「参照」ボタンをクリックして CONFIG ファイルを選択します。
CONFIG ファイルが暗号化されている場合は、「復号パスワード」項目にパスワードを入力します。

メモ

- 「ファイルの指定」項目で「指定しない」を選択した場合は、microSD カード、USB メモリーの順に、デフォルト設定のファイル名「*:config.rtfg」または「*:config.txt」を検索しインポートします。デフォルト設定のファイル名が見つからない場合は、インポートは行われません。
- 「インポートするファイル（最優先）」項目および「インポートするファイル（次に優先）」項目で「すべての外部メモリー」を選択した場合は、インポートするファイルを microSD カード、USB メモリーの順で検索しインポートします。
- 「インポートするファイル（最優先）」項目で設定したファイルが見つからない場合、「インポートするファイル（次に優先）」項目で設定したファイルがインポートされます。
- 指定できる CONFIG ファイルのファイル名の長さは、半角 99 文字以内です。

・「インポートする CONFIG ファイル」項目の設定を変更すると、「外部メモリー内のファイルを用いた優先起動の設定」—「優先起動時に読み込む CONFIG ファイル」項目も連動して変更されます。

③ インポート先の CONFIG ファイル：
インポート先となる内蔵不揮発性メモリーの CONFIG ファイルを選択します。

④ インポートするファームウェアファイル：
外部メモリーからファームウェアファイルをインポートする場合は、「ファームウェアファイルのインポート」項目の「インポートする」を選択します。
任意のファイルを指定する場合は、「ファイルの指定」項目の「指定する」を選択し、「インポートするファイル」項目で参照する外部メモリーを選択してから、「参照」ボタンをクリックしてファームウェアファイルを選択します。

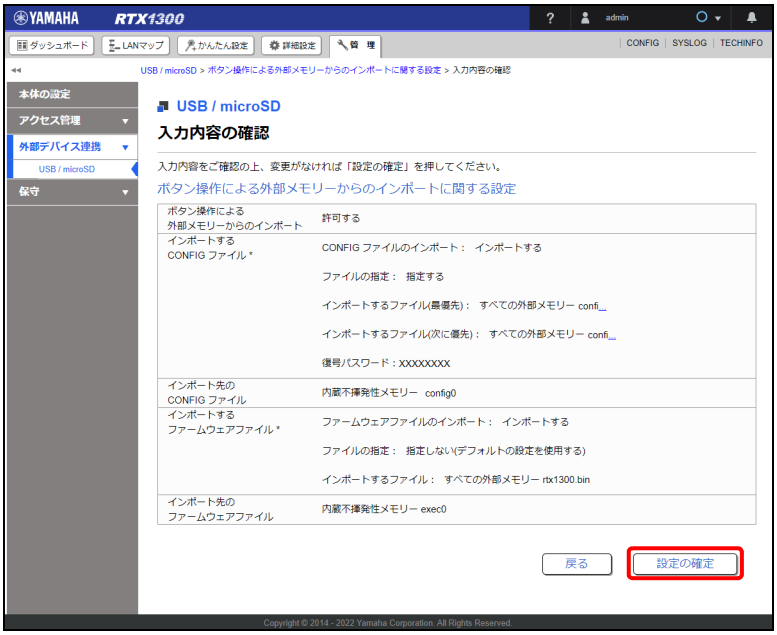
メモ

・「ファイルの指定」項目で「指定しない」を選択した場合は、microSD カード、USB メモリーの順に、デフォルト設定のファイル名「*:rtx1300.bin」を検索しインポートします。デフォルト設定のファイル名が見つからない場合は、インポートは行われません。
・「インポートするファイル」項目で「すべての外部メモリー」を選択した場合は、インポートするファイルを microSD カード、USB メモリーの順で検索しインポートします。
・指定できるファームウェアファイルのファイル名の長さは、半角 99 文字以内です。
・「インポートするファームウェアファイル」項目の設定を変更すると、「外部メモリー内のファイルを用いた優先起動の設定」—「優先起動時に読み込むファームウェアファイル」項目も連動して変更されます。

⑤ インポート先のファームウェアファイル：
インポート先となる内蔵不揮発性メモリーのファームウェアファイルを選択します。
「インポートするファームウェアファイル」の「ファイルの指定」項目で「指定する」を選択すると、選択が可能になります。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **入力内容を確認し、「設定の確定」ボタンをクリックする。**



設定が反映され、「USB/microSD」画面が表示されます。

メモ

本設定を行った後、本製品の microSD ボタン、または USB ボタンを押しながら DOWNLOAD ボタンを 3 秒以上押し続けると、microSD カード、または USB メモリーから CONFIG ファイル、およびファームウェアファイルが内蔵不揮発性メモリーにインポートされます。
また、「管理」タブ ―「保守」―「CONFIG ファイルの管理」から CONFIG ファイルをインポートすることも可能です。

15.7 コマンドを実行する

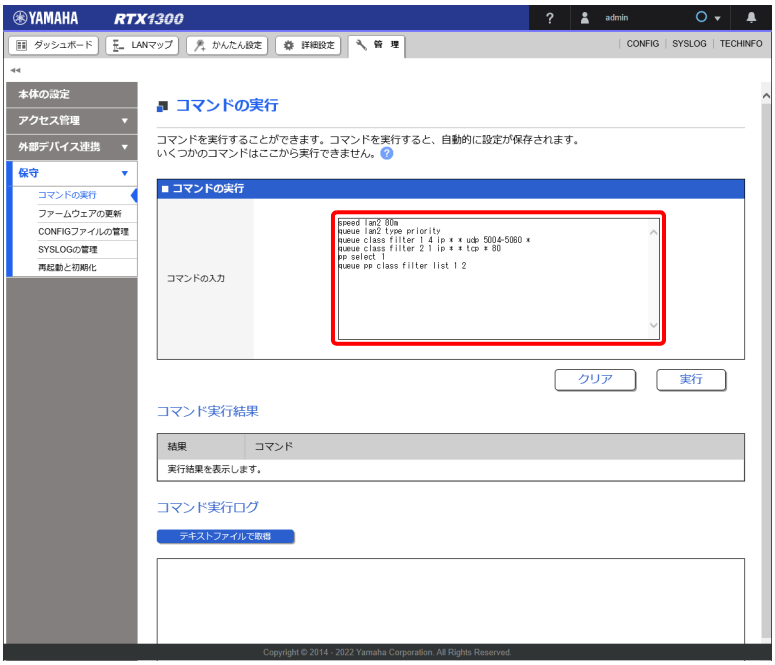
Web GUI のコマンドコンソール画面でコマンドを実行したり、コマンドの実行結果をテキスト形式で取得したりすることができます。Web GUI には設定項目がない機能を使用したい場合などに役立ちます。
まず、以下の条件で QoS（優先制御）を設定する場合を例に説明します。なお、LAN2 インターフェースに PPPoE 接続型のプロバイダーが設定されているものとします。

設定例

インターフェース速度：80Mbit/s
最高優先度（クラス 4）：VoIP
最低優先度（クラス 1）：WWW

1. **「管理」タブ ―「保守」―「コマンドの実行」を順に選択する。**
   「コマンドの実行」画面が表示されます。

2. **「コマンドの実行」項目にコマンドを入力する。**



コマンドの入力例

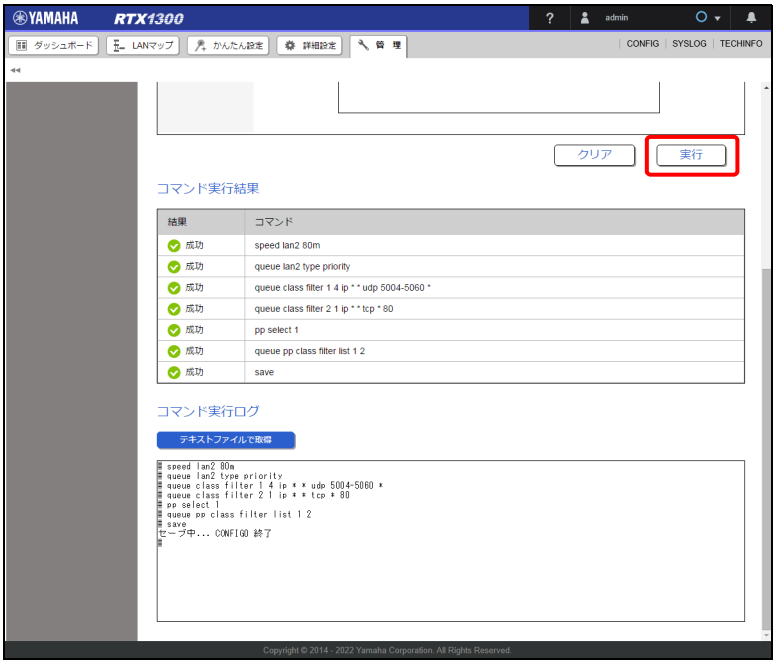
```
speed lan2 80m
queue lan2 type priority
queue class filter 1 4 ip * * udp 5004-5060 *
queue class filter 2 1 ip * * tcp * 80
pp select 1
queue pp class filter list 1 2
```

メモ

改行で区切ることによって、複数のコマンドをまとめて入力することができます。

3. **「実行」ボタンをクリックする。**

コマンドの実行結果が表示されます。



メモ

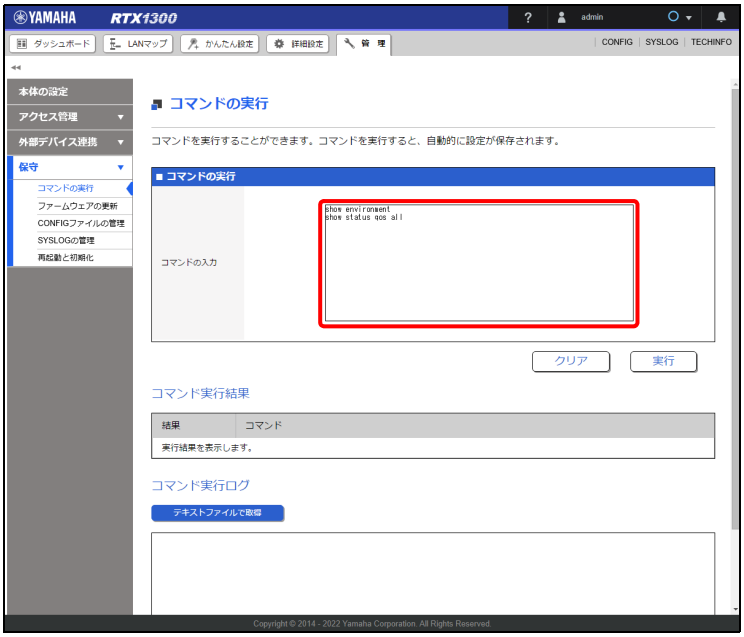
設定系コマンドを実行すると自動的に save コマンドも実行され、設定が自動的に保存されます。

次に、以下の表示系コマンドの実行例を示します。

表示系コマンドの例

機器状態の表示：show environment
QoS ステータスの表示：show status qos all

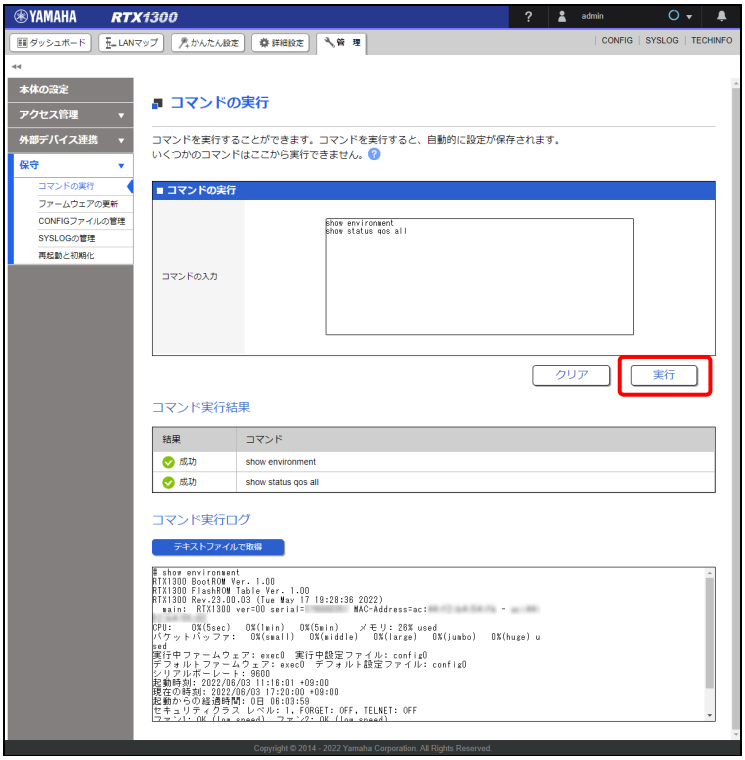
1. 「コマンドの実行」項目にコマンドを入力する。



コマンドの入力例

```
show environment
show status qos all
```

2. 「実行」ボタンをクリックする。
コマンドの実行結果が表示されます。



メモ

「テキストファイルで取得」ボタンをクリックすると、コマンドの実行結果をテキストファイルで取得することができます。取得したテキストファイルは UTF-8 でエンコードされています。

15.8 ファームウェアを更新する

本製品のファームウェアを更新する方法について説明します。

メモ

起動中のファームウェアを更新する場合は、ファームウェアの更新が正常に完了すると自動的に本製品が再起動します。本製品が再起動するまで他の操作は絶対に行わないでください。

15.8.1 外部メモリーを使用してファームウェアを更新する

外部メモリー（USB メモリーまたは microSD カード）に保存したファームウェアファイルを本製品に読み込ませて、ファームウェアを更新します。

注意

本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損させることがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。

重要

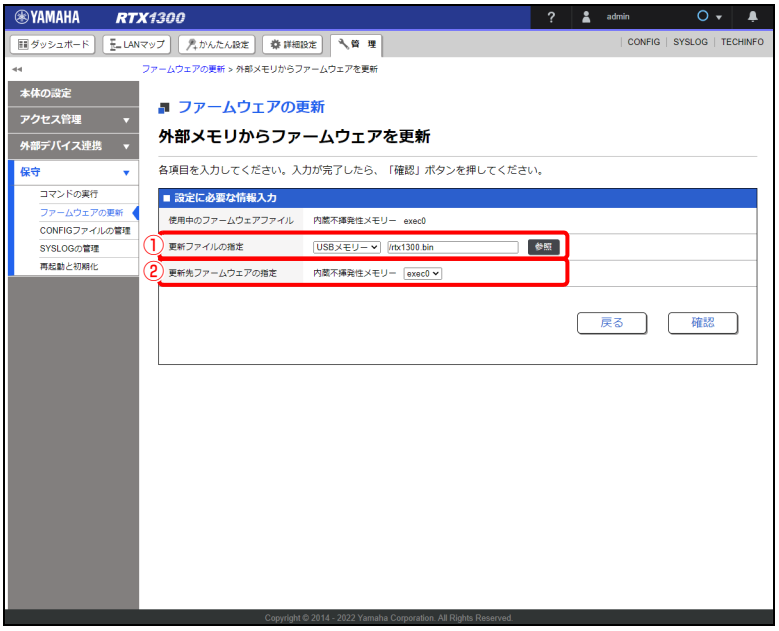
- USB 延長ケーブルを介して接続した場合は、正常に動作しないことがあります。USB メモリーは本製品の USB ポートに直接挿入してご使用ください。
- FAT または FAT32 形式でフォーマットされていない外部メモリーは、本製品で使用できません。
- USB ハブを介して、複数の USB メモリーなどの外部メモリーを本製品に接続することはできません。

1. **ファームウェアファイルを保存した外部メモリーを用意する。**
   ファームウェアファイルはヤマハネットワーク周辺機器技術情報ページから入手できます。
   http://www.rtpro.yamaha.co.jp/
2. **外部メモリーを本製品の USB ポートまたは microSD スロットに挿し込む。**
   外部メモリーを認識するとブザーが鳴り、本製品の USB インジケーターまたは microSD インジケーターが点灯します。
3. **「管理」タブ ―「保守」―「ファームウェアの更新」を順に選択する。**
   「ファームウェアの更新」画面が表示されます。

4. 「外部メモリからファームウェアを更新」項目の「進む」ボタンをクリックする。

「外部メモリからファームウェアを更新」画面が表示されます。

5. 外部メモリーから読み込みたいファームウェアファイルを指定する。



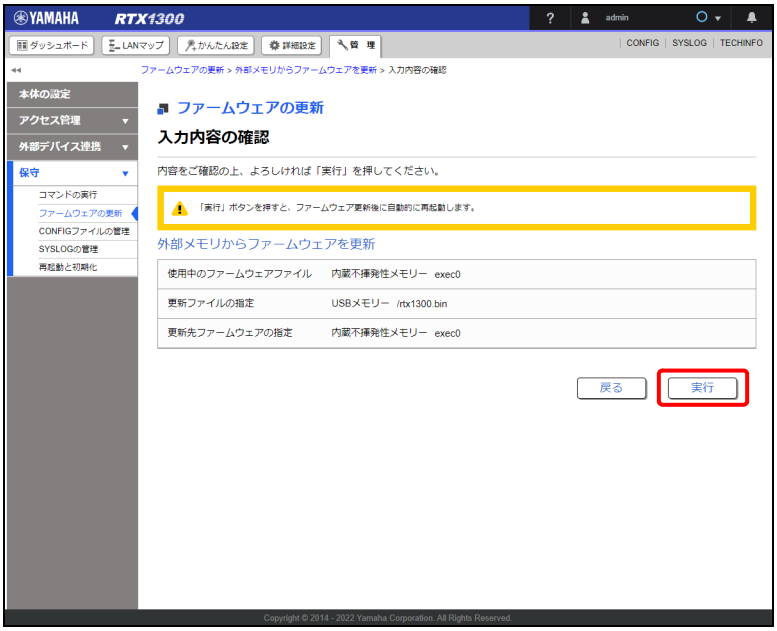
① **更新ファイルの指定：**
挿し込んだ外部メモリーを選択して「参照」ボタンをクリックし、「ファイルの一覧」画面から保存したファームウェアファイルを選択します。

② **更新先ファームウェアの指定：**
更新先の内蔵不揮発性メモリーのファームウェア番号を選択します。

メモ

更新先ファームウェアに指定したファームウェア番号が起動中のファームウェア番号と同じ場合は、ファームウェアの更新完了後に自動的に本製品が更新後のファームウェアで再起動します。ファームウェア番号が異なる場合は、再起動は行われず起動中のファームウェアは変化しません。

6. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。
7. **内容を確認し、「実行」ボタンをクリックする。**



「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、本製品は自動的に再起動します。

メモ

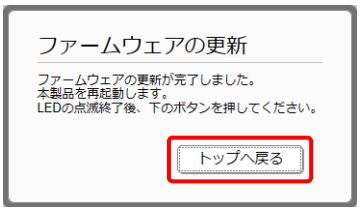
起動中のファームウェア番号と更新先ファームウェアに指定したファームウェア番号が異なる場合は、再起動は行われず起動中のファームウェアも変化しません。手順 8 以降は、起動中のファームウェア番号と更新先ファームウェアに指定したファームウェア番号が同じ場合に行ってください。

8. **本製品の再起動中（LED が全点灯している間）に、外部メモリーを取り外す。**

メモ

本製品の LED が全点灯している間に外部メモリーを取り外してください。その際に USB ボタン / microSD ボタンを押す必要はありません。
外部メモリーを取り外さなかった場合、外部メモリー内にファームウェアまたは CONFIG ファイルが存在すると、その外部メモリー内のファイルを使用して起動します。

9. **本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。**



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

15.8.2 パソコンからファームウェアを更新する

パソコンに保存したファームウェアファイルを本製品に読み込ませて、ファームウェアの更新を行います。

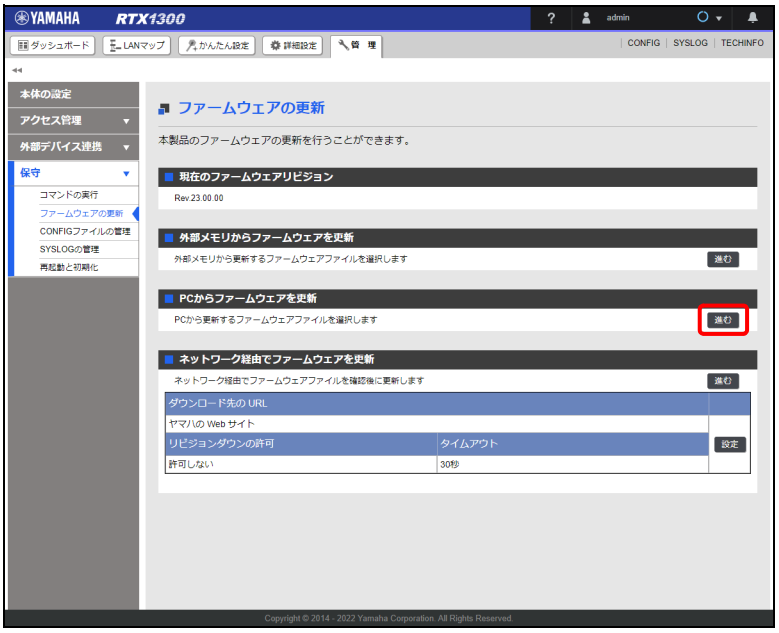
1. **パソコンにファームウェアファイルを保存する。**

メモ

ファームウェアファイルはヤマハネットワーク周辺機器技術情報ページから入手できます。
http://www.rtpro.yamaha.co.jp/

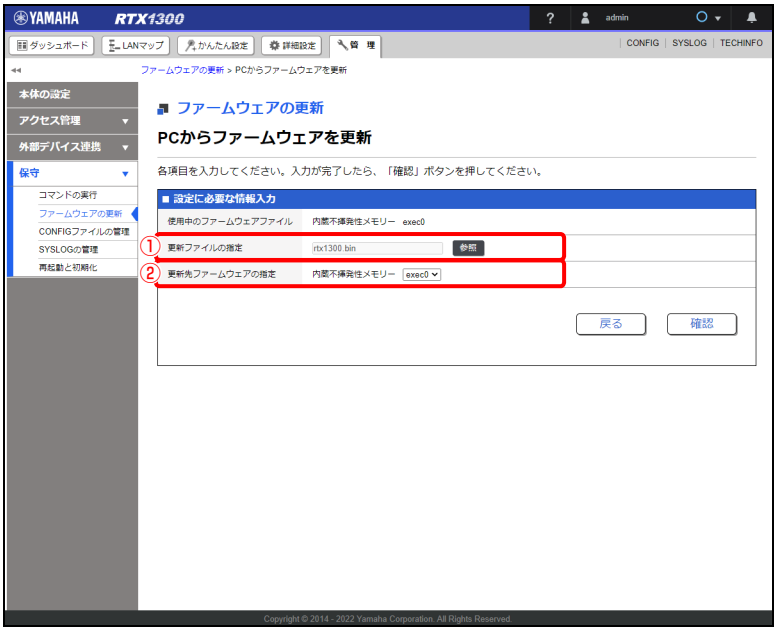
2. **「管理」タブ ―「保守」―「ファームウェアの更新」を順に選択する。**
「ファームウェアの更新」画面が表示されます。

3. **「PC からファームウェアを更新」項目の「進む」ボタンをクリックする。**



「PC からファームウェアを更新」画面が表示されます。

4. パソコンから読み込みたいファームウェアファイルを指定する。



① 更新ファイルの指定：
「参照」ボタンをクリックし、エクスプローラーのファイル選択ダイアログから保存したファームウェアファイルを選択します。

メモ

macOS、または iPadOS で更新ファイルの指定を行う場合、macOS では Finder、iPadOS はファイルアプリから保存したファームウェアファイルを選択します。

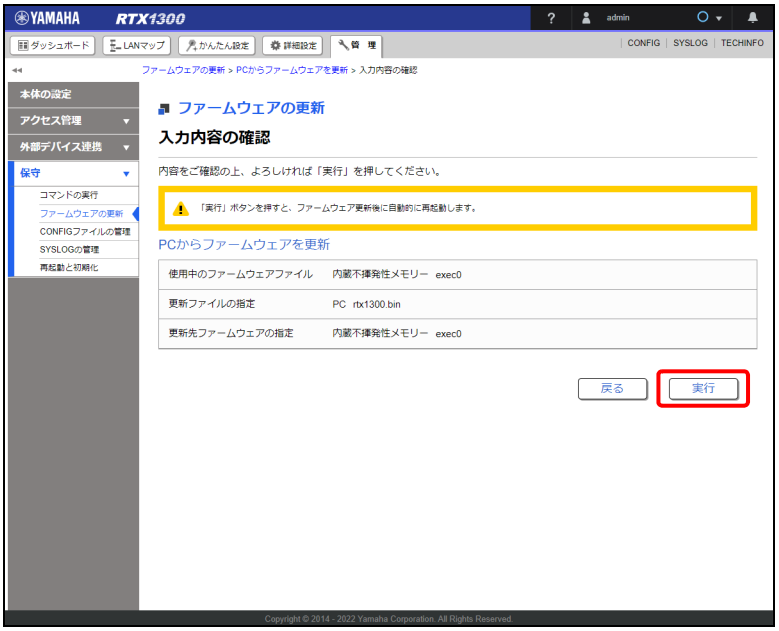
② 更新先ファームウェアの指定：
更新先の内蔵不揮発性メモリーのファームウェアファイルを選択します。

メモ

更新先ファームウェアに指定したファームウェア番号が起動中のファームウェア番号と同じ場合は、ファームウェアの更新完了後に自動的に本製品が更新後のファームウェアで再起動します。ファームウェア番号が異なる場合は、再起動は行われず起動中のファームウェアは変化しません。

5. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「実行」ボタンをクリックする。

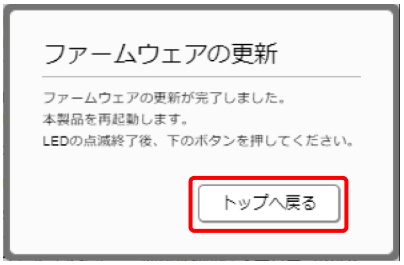


「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、本製品は自動的に再起動します。

メモ

起動中のファームウェアファイルと更新先ファームウェアの指定が異なる場合は、再起動は行われず起動中のファームウェアファイルも変化しません。手順 7 以降は、起動中のファームウェアファイルと更新先ファームウェアの指定が同じ場合に行ってください。

7. 本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

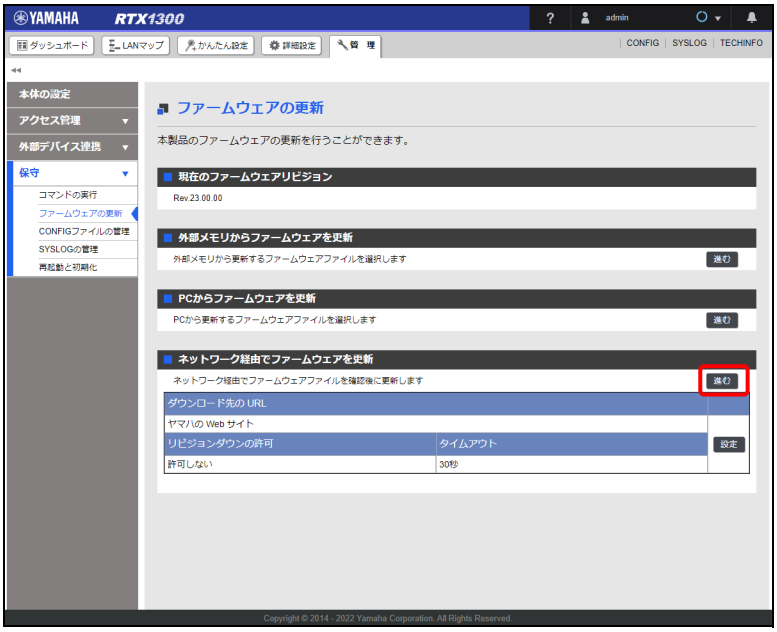
15.8.3 ヤマハのウェブサイトからネットワーク経由でファームウェアを更新する

ヤマハの公式ウェブサイト上に置かれたファームウェアファイルをダウンロードして、ファームウェアの更新を行います。

メモ

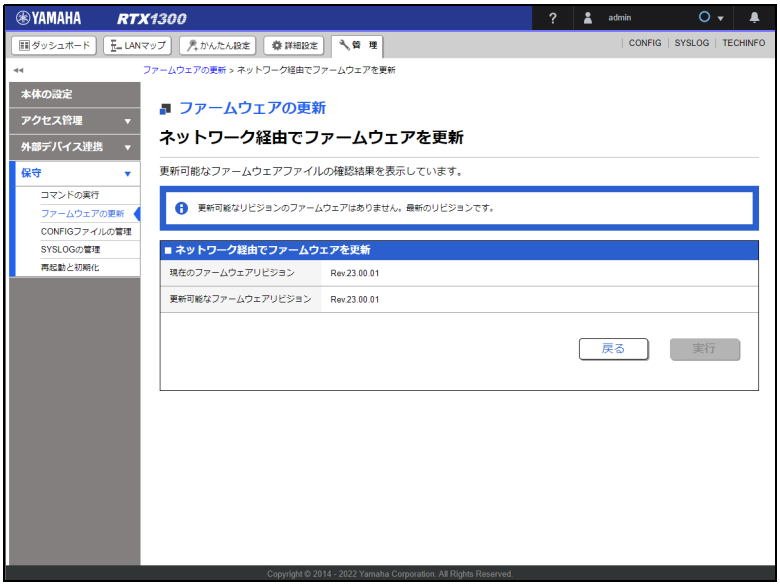
ヤマハの公式ウェブサイトで公開されている RTX1300 のファームウェアファイルの URL は以下になります。
http://www.rtpro.yamaha.co.jp/firmware/revision-up/rtx1300.bin
上記 URL はウェブブラウザーからアクセスすることはできません。

1. **「管理」タブ ― 「保守」 ― 「ファームウェアの更新」を順に選択する。**
   「ファームウェアの更新」画面が表示されます。
2. **「ネットワーク経由でファームウェアを更新」項目の「進む」ボタンをクリックする。**

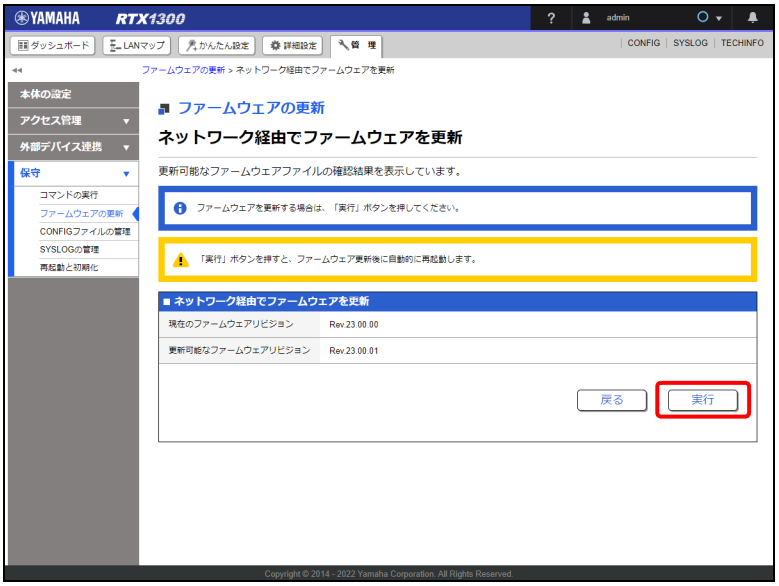


更新可能なファームウェアの確認が行われ、「ネットワーク経由でファームウェアを更新」画面が表示されます。

最新のファームウェアを使用している場合は以下のような画面が表示されます。この場合はファームウェアを更新する必要はありません。

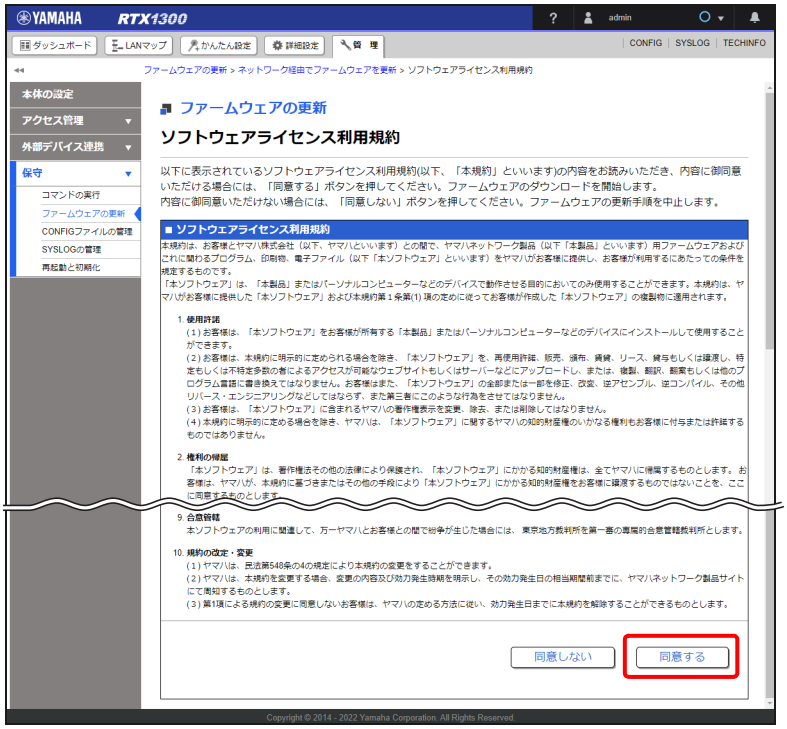


3. 内容を確認し、「実行」ボタンをクリックする。



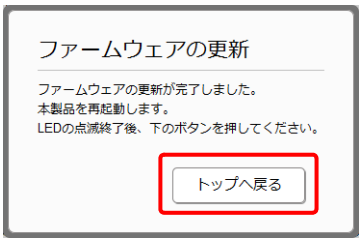
「ソフトウェアライセンス利用規約」画面が表示されます。

4. ソフトウェアライセンス利用規約の内容をよく確認し、「同意する」ボタンをクリックする。



「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、本製品は自動的に再起動します。

5. 本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードの Live 画面が表示されます。

メモ

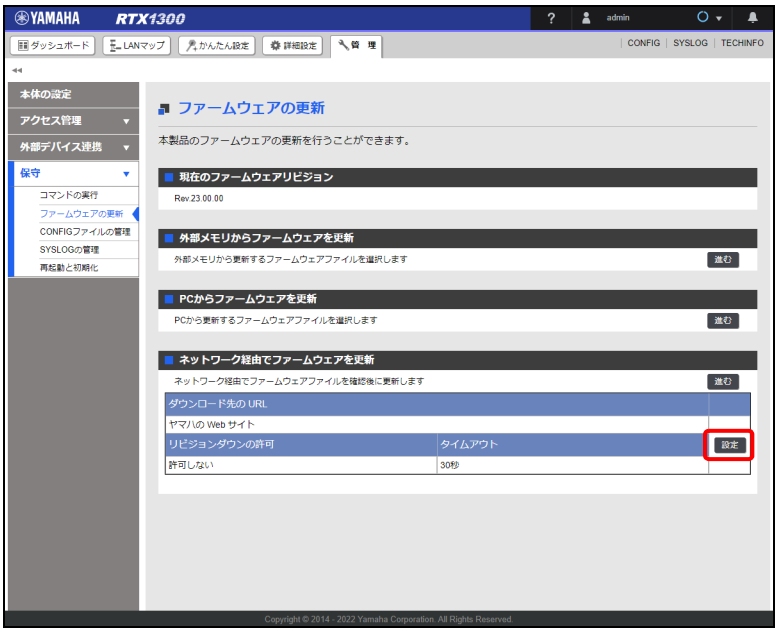
再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

15.8.4 社内サーバーからネットワーク経由でファームウェアを更新する

社内サーバー上に置かれたファームウェアファイルをダウンロードして、ファームウェアの更新を行います。

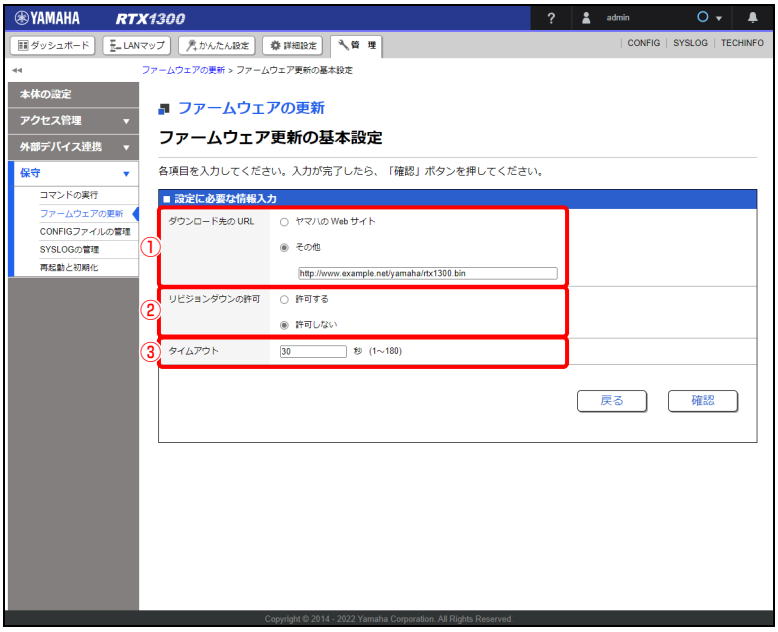
1. **「管理」タブ―「保守」―「ファームウェアの更新」を順に選択する。**
   「ファームウェアの更新」画面が表示されます。

2. **「ネットワーク経由でファームウェアを更新」項目の「設定」ボタンをクリックする。**



「ファームウェア更新の基本設定」画面が表示されます。

3. **ファームウェア更新の基本設定を行う。**



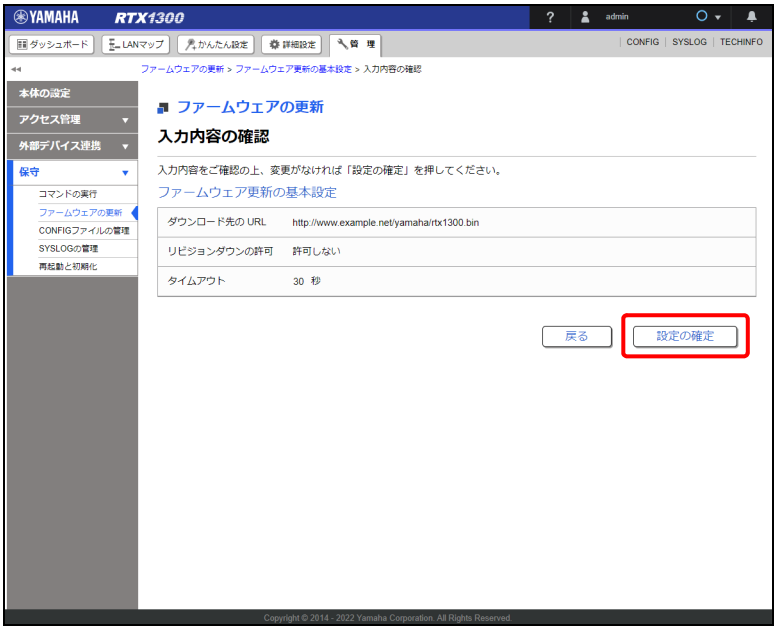
① **ダウンロード先の URL：**
ファームウェアの置かれている URL を設定します。社内サーバーからダウンロードする場合は、「その他」を選択し社内サーバーの URL を入力します。

② **リビジョンダウンの許可：**
古いバージョンのファームウェアへの書き換えを許可するか否かを設定します。

③ **タイムアウト：**
ネットワーク経由でファームウェアを更新する処理のタイムアウト時間を入力します。

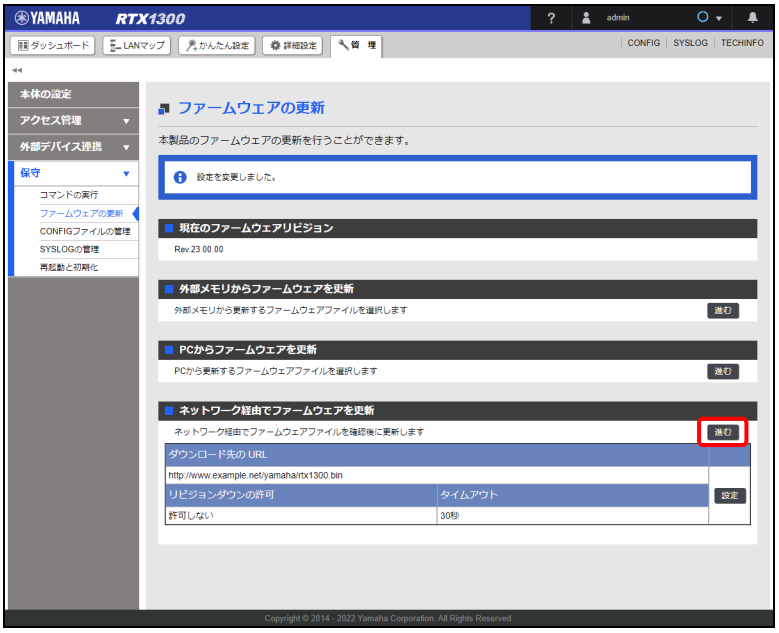
4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**



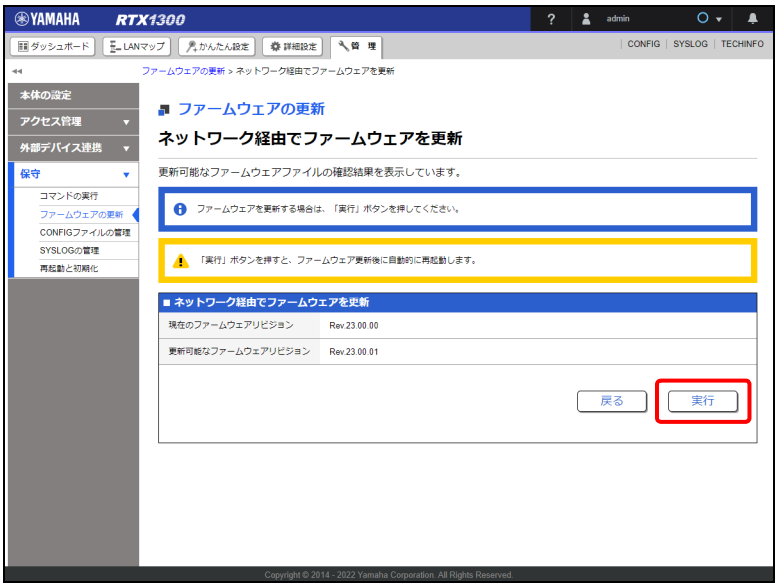
設定が反映され、「ファームウェアの更新」画面が表示されます。

6. 「ネットワーク経由でファームウェアを更新」項目の「進む」ボタンをクリックする。



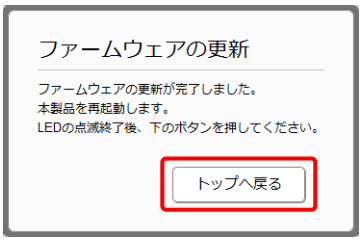
更新可能なファームウェアの確認が行われ、「ネットワーク経由でファームウェアを更新」画面が表示されます。

7. 内容を確認し、「実行」ボタンをクリックする。



「ファームウェアの更新」ダイアログが表示され、ファームウェアの更新が開始されます。ファームウェアの更新が完了すると、本製品は自動的に再起動します。

8. 本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

15.9 設定（CONFIG）を管理する

設定（CONFIG）を外部メモリーへエクスポートしたり、外部メモリーからインポートしたりすることができます。本製品は CONFIG に従って動作しています。CONFIG は複数のコマンドで構成されており、Web GUI から設定した内容もすべてコマンド形式で CONFIG に保存されます。

注意

- 本製品の USB インジケーターまたは microSD インジケーターが点灯 / 点滅している間は、外部メモリーを取り外さないでください。外部メモリー内のデータを破損させることがあります。USB ボタンまたは microSD ボタンを 2 秒以上押し続けるとブザーが鳴り、USB インジケーターまたは microSD インジケーターが消灯し、外部メモリーを取り外すことができるようになります。
- 管理者権限を持つユーザーの設定がない CONFIG ファイルを使用して本製品を起動した場合は、初期管理ユーザー「admin」が追加されます。なお、初期管理ユーザーのパスワードを変更するまでの間は、WAN 側の通信が制限されます。

重要

- USB 延長ケーブルを介して接続した場合は、正常に動作しないことがあります。USB メモリーは本製品の USB ポートに直接挿入してご使用ください。
- FAT または FAT32 形式でフォーマットされていない外部メモリーは、本製品で使用できません。
- USB ハブを介して、複数の USB メモリーなどの外部メモリーを本製品に接続することはできません。

メモ

コマンド仕様について詳しくは、「コマンドリファレンス」（ウェブサイト）をご覧ください。

15.9.1 設定（CONFIG）をパソコンにエクスポートする

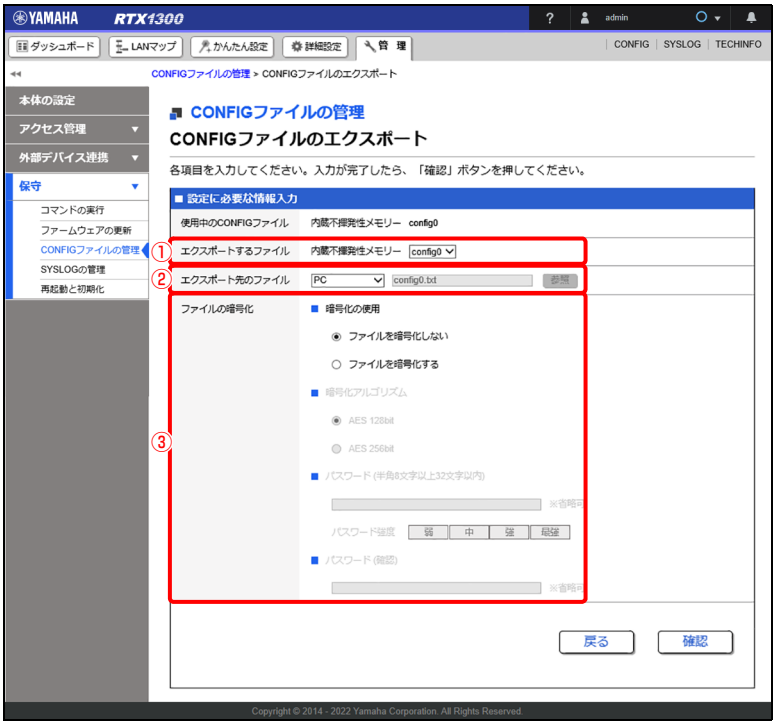
本製品内に保存されている設定（CONFIG）をパソコンにエクスポートします。

1. **「管理」タブ ―「保守」―「CONFIG ファイルの管理」を順に選択する。**
   「CONFIG ファイルの管理」画面が表示されます。

2. **「CONFIG ファイルのエクスポート」項目の「進む」ボタンをクリックする。**

「CONFIG ファイルのエクスポート」画面が表示されます。

3. 設定（CONFIG）ファイルのエクスポートに必要な情報を入力する。



① エクスポートするファイル：
エクスポートしたい内蔵不揮発性メモリーの CONFIG ファイルを選択します。

② エクスポート先のファイル：
プルダウンメニューから「PC」を選択します。
「PC」を選択した場合、自動的に①で選択した内蔵不揮発性メモリーの CONFIG ファイル名が付与されます。拡張子は暗号化するか否かによって以下のように分かれます。

拡張子	説明
txt	暗号化しない場合
rtfg	暗号化する場合

③ ファイルの暗号化：
エクスポートする際に CONFIG ファイルを暗号化するか否かを選択します。CONFIG ファイルを暗号化して保存する場合は、「ファイルを暗号化する」を選択してから暗号化アルゴリズムを選択し、任意の暗号化パスワードを入力します。パスワードを入力せずに暗号化することも可能です。暗号化パスワードを設定した場合は、CONFIG ファイルのインポート時に同じパスワードを入力して復号する必要があるため、パスワードは忘れないでください。

メモ

- 暗号化した CONFIG ファイルは、Windows アプリケーションの「RT-FileGuard」で復号できます。「RT-FileGuard」は、http://www.rtpro.yamaha.co.jp/RT/utility/ からダウンロードできます。
- パスワードは、長さ 8 ～ 32 文字の半角英数字と半角記号が使用できます。英字の大文字と小文字は区別されます。
  以下の半角記号を使用することができます。
  !"#$%&'()=~|-^\`{@[+*};:]<>?_,./\

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「実行」ボタンをクリックする。**

パソコンに CONFIG ファイルがエクスポートされます。

重要

「実行」ボタンをクリックした後の動作は、使用しているウェブブラウザーの設定によって異なります。
ファイルの保存場所を毎回指定する設定になっている場合は、保存先のフォルダーの選択画面が表示され、選択したフォルダーにダウンロードされます。ファイルを常に特定のフォルダーに保存する設定になっている場合は、指定されているフォルダーにダウンロードされます。

メモ

パソコンに CONFIG ファイルが、正しくエクスポートされていることを確認してください。

15.9.2 設定（CONFIG）をパソコンからインポートする

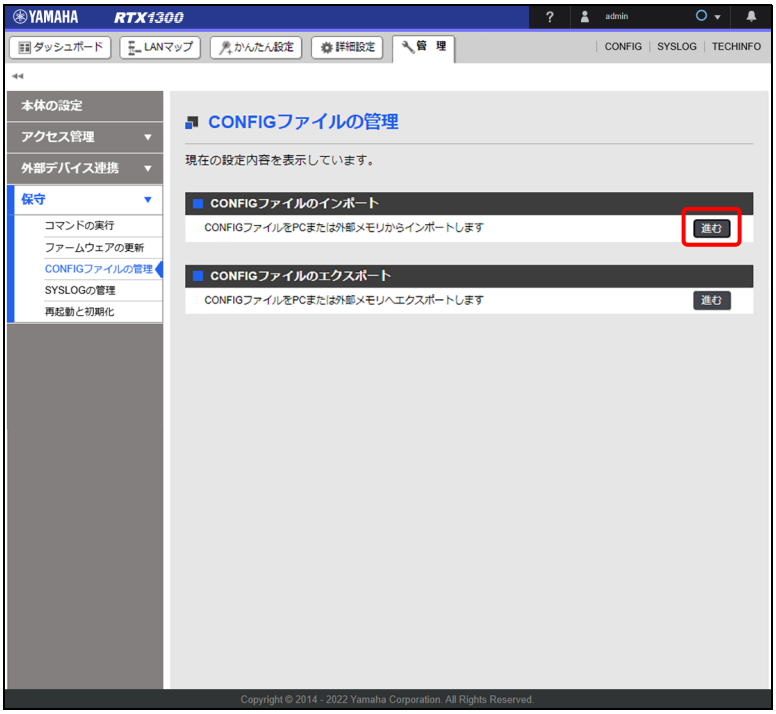
パソコンに保存されている設定（CONFIG）をインポートし、本製品の設定（CONFIG）を更新します。

注意

使用中の設定（CONFIG）を更新する場合は、設定（CONFIG）の更新が正常に完了すると自動的に本製品が再起動します。本製品が再起動するまで他の操作は絶対に行わないでください。

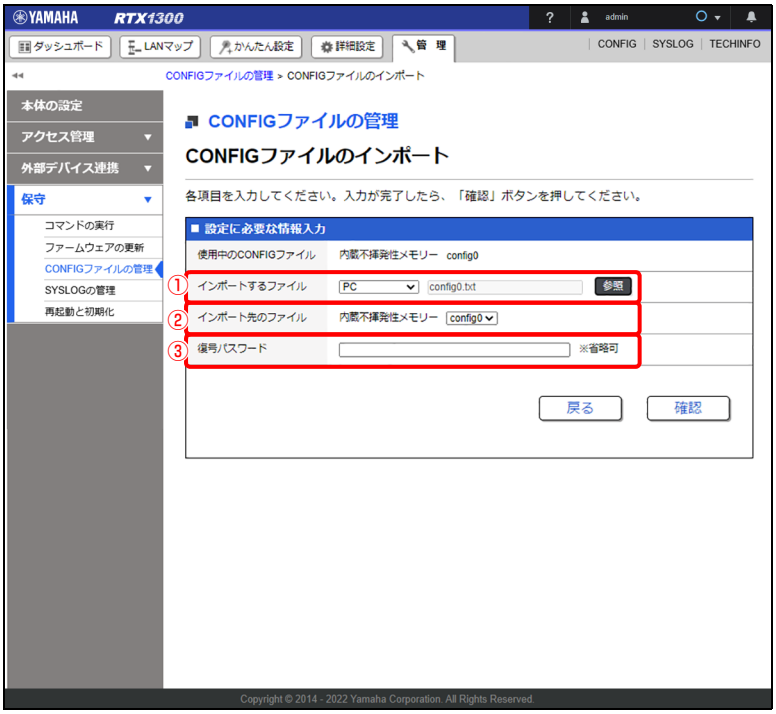
1. **「管理」タブ ―「保守」―「CONFIG ファイルの管理」を順に選択する。**
   「CONFIG ファイルの管理」画面が表示されます。

2. 「CONFIG ファイルのインポート」項目の「進む」ボタンをクリックする。



「CONFIG ファイルのインポート」画面が表示されます。

3. 設定（CONFIG）ファイルのインポートに必要な情報を入力する。



① **インポートするファイル：**
「PC」を選択後「参照」ボタンをクリックし、エクスプローラーのファイル一覧からインポートしたい CONFIG ファイルを選択します。

② **インポート先のファイル：**
インポート先の内蔵不揮発性メモリーの CONFIG ファイルを選択します。

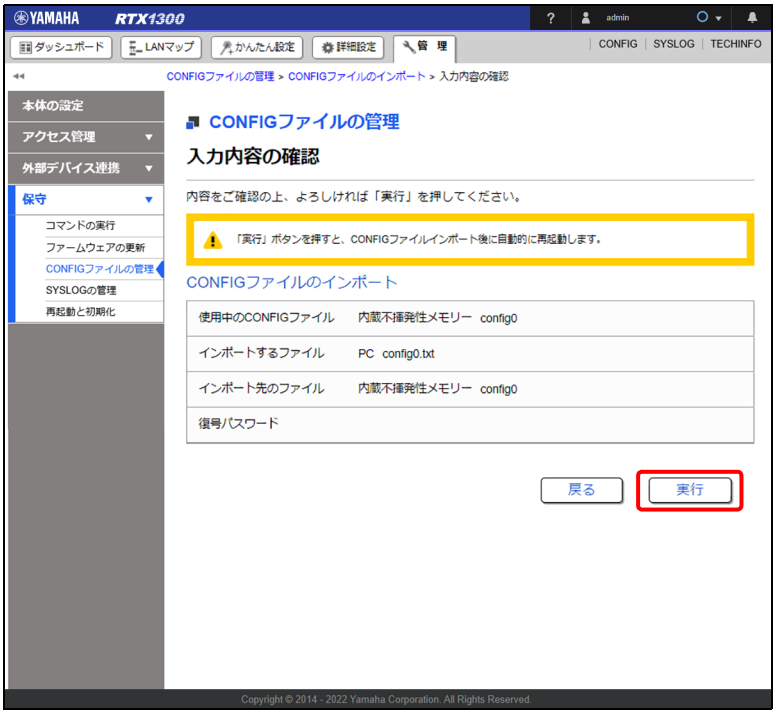
メモ

使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が同じ場合は、インポートの完了後に本製品が再起動します。また、指定が異なる場合は、再起動は行われず使用中の CONFIG ファイルは変化しません。

③ **復号パスワード：**
暗号化されている CONFIG ファイルをインポートする場合は、エクスポートする際に設定した暗号化パスワードを入力します。暗号化パスワードを設定していない場合は入力不要です。

4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「実行」ボタンをクリックする。**

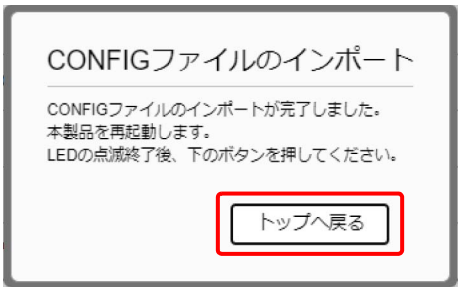


「CONFIG ファイルのインポート」ダイアログが表示され、設定（CONFIG）ファイルがインポートされます。設定（CONFIG）ファイルのインポートが完了すると、本製品は自動的に再起動します。

メモ

使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が異なる場合は、再起動は行われず使用中の CONFIG ファイルも変化しません。手順 6 以降は、使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が同じ場合に行ってください。

6. **本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。**



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

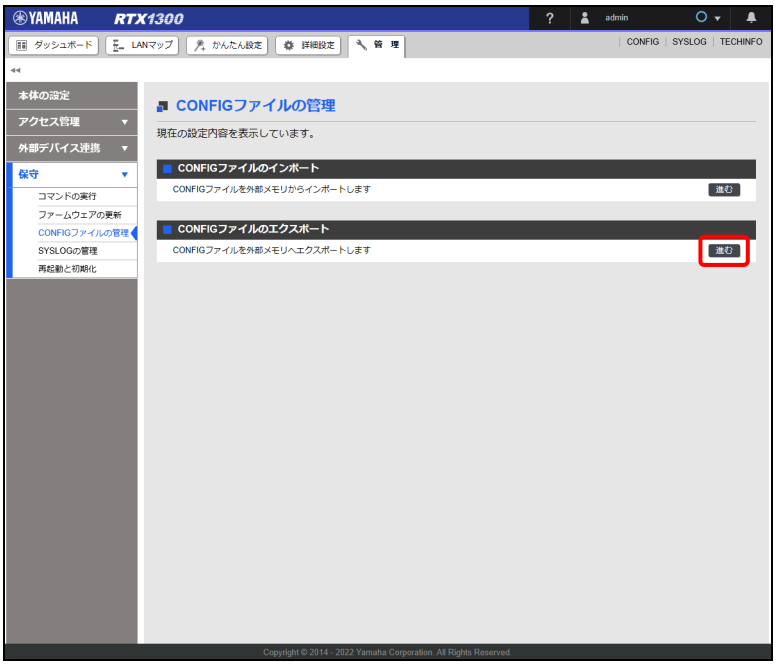
15.9.3 設定（CONFIG）を外部メモリーにエクスポートする

本製品内に保存されている設定（CONFIG）を外部メモリーにエクスポートします。

1. **外部メモリーを本製品の USB ポートまたは microSD スロットに挿し込む。**
   外部メモリーを認識するとブザーが鳴り、本製品の USB インジケーターまたは microSD インジケーターが点灯します。

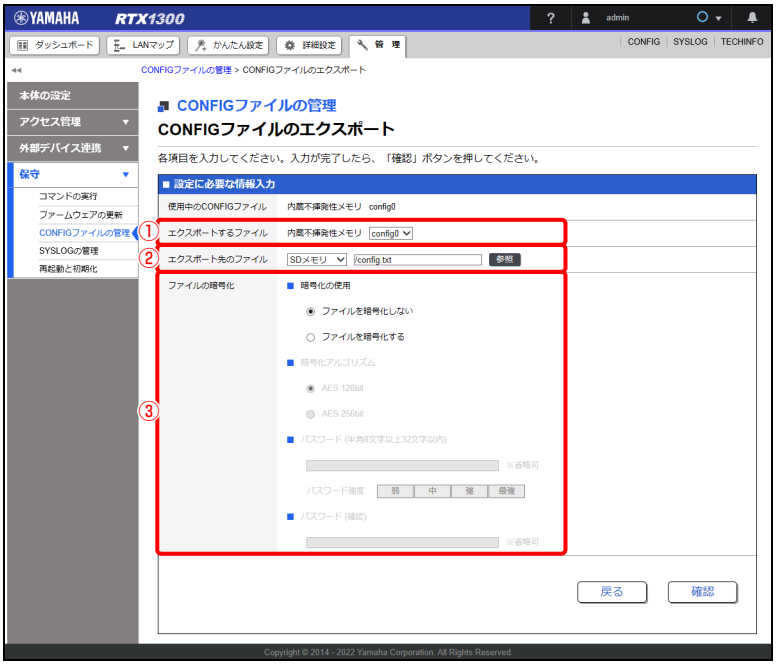
2. **「管理」タブ ―「保守」―「CONFIG ファイルの管理」を順に選択する。**
   「CONFIG ファイルの管理」画面が表示されます。

3. **「CONFIG ファイルのエクスポート」項目の「進む」ボタンをクリックする。**



「CONFIG ファイルのエクスポート」画面が表示されます。

4. 設定（CONFIG）ファイルのエクスポートに必要な情報を入力する。



① エクスポートするファイル：
エクスポートしたい内蔵不揮発性メモリーの CONFIG 番号を選択します。

② エクスポート先のファイル：
挿し込んだ外部メモリーを選択し、エクスポート先のファイル名を入力します。

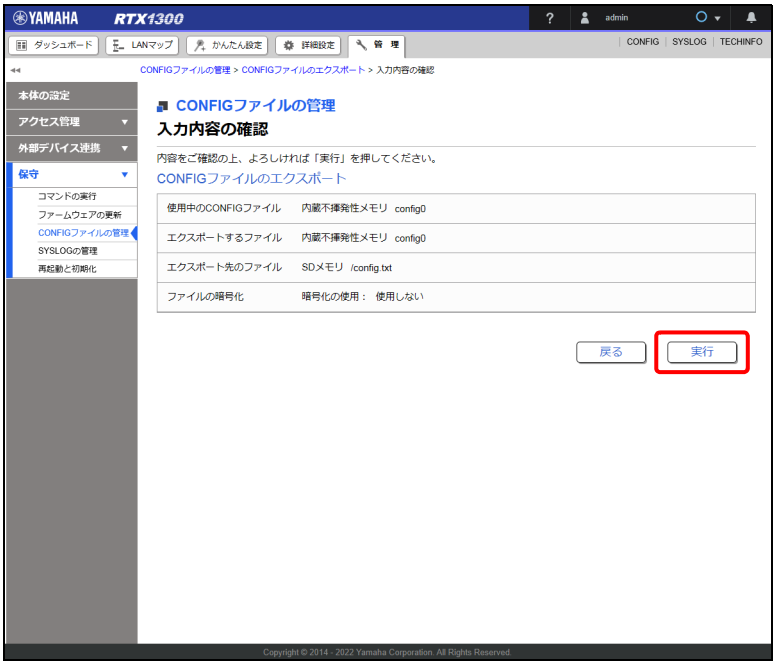
③ ファイルの暗号化：
エクスポートする際に CONFIG ファイルを暗号化するか否かを選択します。CONFIG ファイルを暗号化して保存する場合は、「ファイルを暗号化する」を選択してから暗号化アルゴリズムを選択し、任意の暗号化パスワードを入力します。パスワードを入力せずに暗号化することも可能です。暗号化パスワードを設定した場合は、CONFIG ファイルのインポート時に同じパスワードを入力して復号する必要があるため、パスワードは忘れないでください。

メモ

- 暗号化した CONFIG ファイルは、Windows アプリケーションの「RT-FileGuard」で復号できます。「RT-FileGuard」のダウンロードは、以下の URL をご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/utility/
- パスワードは、長さ 8 ～ 32 文字の半角英数字と半角記号が使用できます。英字の大文字と小文字は区別されます。
  以下の半角記号を使用することができます。
  !"#$%&'()=~|-^\`{@[+*};:]<>?_,./\

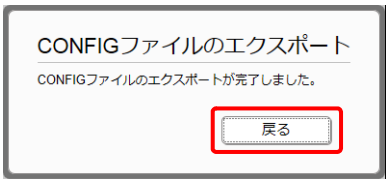
5. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

6. 内容を確認し、「実行」ボタンをクリックする。



「CONFIG ファイルのエクスポート」ダイアログが表示され、外部メモリーに CONFIG ファイルがエクスポートされます。

7. 「CONFIG ファイルのエクスポートが完了しました。」というメッセージが表示されたら、「戻る」ボタンをクリックする。



「CONFIG ファイルの管理」画面が表示されます。

メモ

外部メモリーに CONFIG ファイルが、正しくエクスポートされていることを確認してください。

15.9.4 設定（CONFIG）を外部メモリーからインポートする

外部メモリーに保存されている設定（CONFIG）をインポートし、本製品の設定（CONFIG）を更新します。

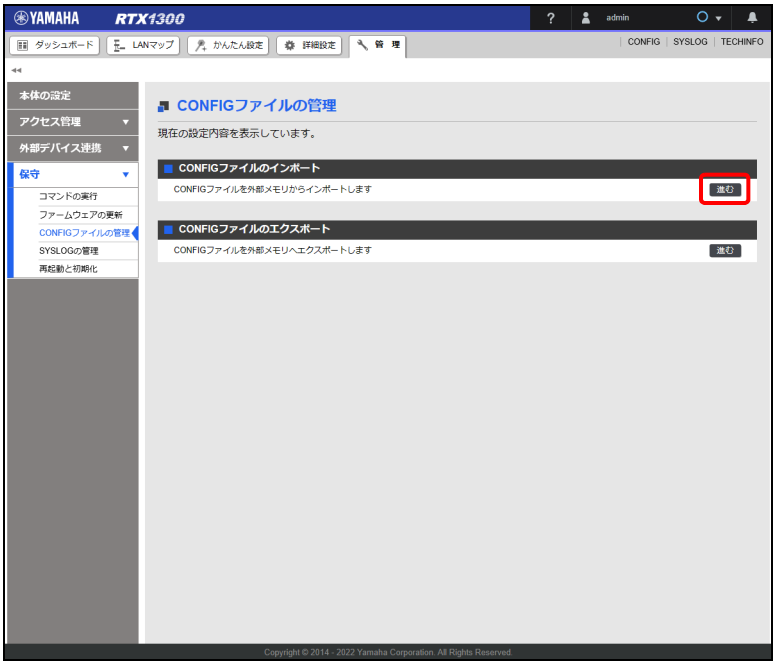
注意

使用中の設定（CONFIG）を更新する場合は、設定（CONFIG）の更新が正常に完了すると自動的に本製品が再起動します。本製品が再起動するまで他の操作は絶対に行わないでください。

1. CONFIG ファイルが保存されている外部メモリーを用意する。
2. 外部メモリーを本製品の USB ポートまたは microSD スロットに挿し込む。
   外部メモリーを認識するとブザーが鳴り、本製品の USB インジケーターまたは microSD インジケーターが点灯します。

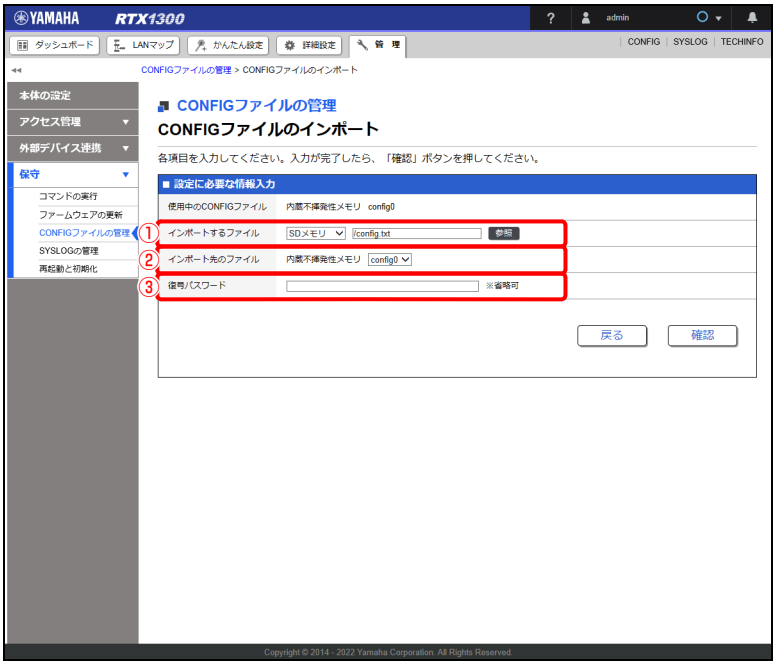
3. 「管理」タブ ―「保守」―「CONFIG ファイルの管理」を順に選択する。
「CONFIG ファイルの管理」画面が表示されます。

4. 「CONFIG ファイルのインポート」項目の「進む」ボタンをクリックする。



「CONFIG ファイルのインポート」画面が表示されます。

5. 設定（CONFIG）ファイルのインポートに必要な情報を入力する。



① インポートするファイル：
挿し込んだ外部メモリーを選択し、「参照」ボタンをクリックします。「ファイルの一覧」画面でインポートしたい CONFIG ファイルを選択します。

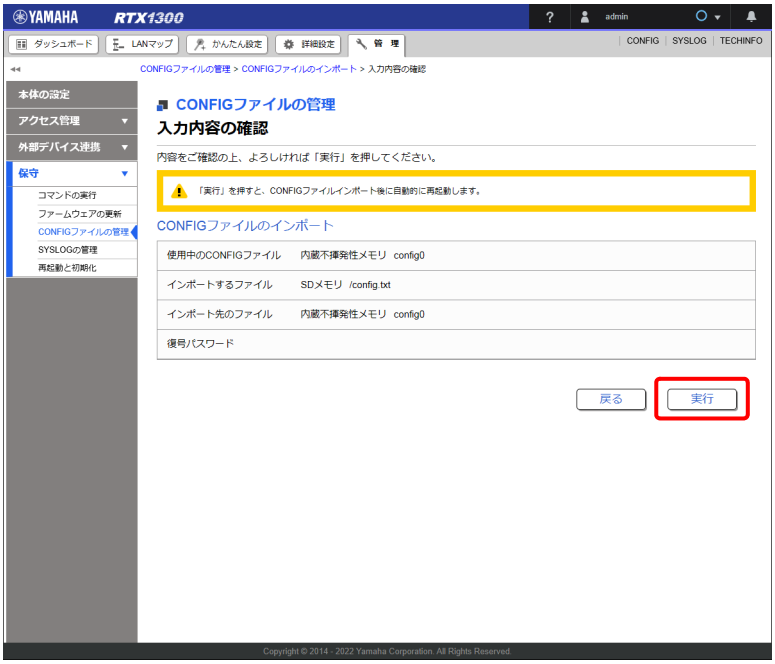
② インポート先のファイル：
インポート先の内蔵不揮発性メモリーの CONFIG 番号を選択します。

メモ
使用中の CONFIG ファイルとインポート先の CONFIG ファイルの指定が同じ場合は、インポートの完了後に本製品が再起動します。また、指定が異なる場合は、再起動は行われず使用中の CONFIG ファイルは変化しません。

③ 復号パスワード：
暗号化されている CONFIG ファイルをインポートする場合は、エクスポートする際に設定した暗号化パスワードを入力します。暗号化パスワードを設定していない場合は入力不要です。

6. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

7. **内容を確認し、「実行」ボタンをクリックする。**



「CONFIG ファイルのインポート」ダイアログが表示され、設定（CONFIG）ファイルがインポートされます。設定（CONFIG）ファイルのインポートが完了すると、本製品は自動的に再起動します。

メモ
使用中の CONFIG 番号とインポート先の CONFIG 番号が異なる場合は、再起動されず使用中の CONFIG も変化しません。手順 8 以降は、使用中の CONFIG 番号とインポート先の CONFIG 番号が同じ場合に行ってください。

8. **本製品の再起動中に、外部メモリーを取り外す。**

重要

- 本製品の LED が全点灯している間に外部メモリーを取り外してください。その際に USB ボタン / microSD ボタンを押す必要はありません。
- 外部メモリーを取り外さなかった場合、外部メモリー内にファームウェアまたは CONFIG ファイルが存在すると、その外部メモリー内のファイルを使用して起動します。

9. **本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。**

ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

15.10 SYSLOG を管理する

SYSLOG 機能の設定を行います。本製品の動作履歴はログファイル（SYSLOG）に保存されています。SYSLOG は本製品の不揮発性メモリーに保存されるだけでなく、指定のサーバー（SYSLOG ホスト）へ送信することもできます。

メモ

SYSLOG で本製品の動作履歴を確認することで、ネットワーク障害を解決するヒントが得られる場合があります。

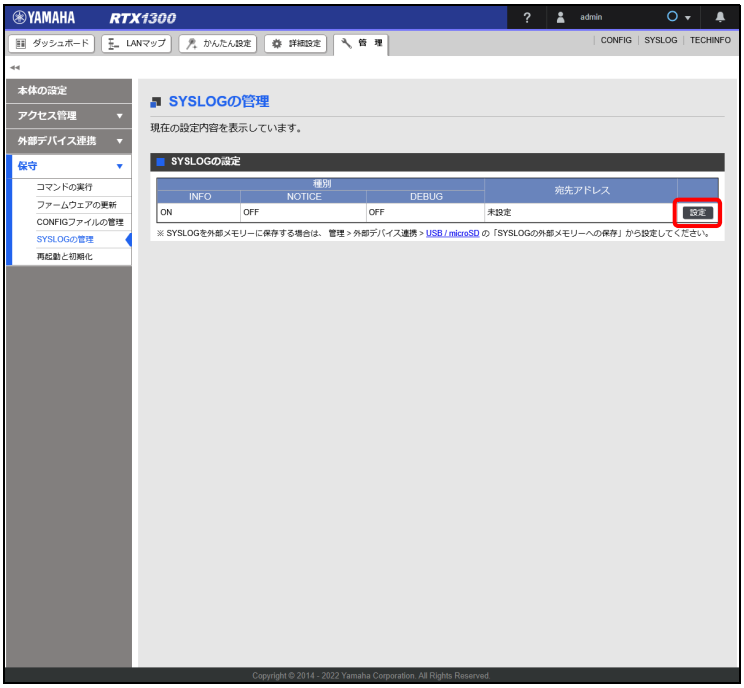
15.10.1 SYSLOG に出力する種別を変更する

SYSLOG に出力する種別（INFO / NOTICE / DEBUG）を変更します。

INFO：本製品の動作状況に関する情報が出力されます。
NOTICE：各種フィルター機能などで検出したパケット情報が出力されます。
DEBUG：デバッグ用の情報が出力されます。

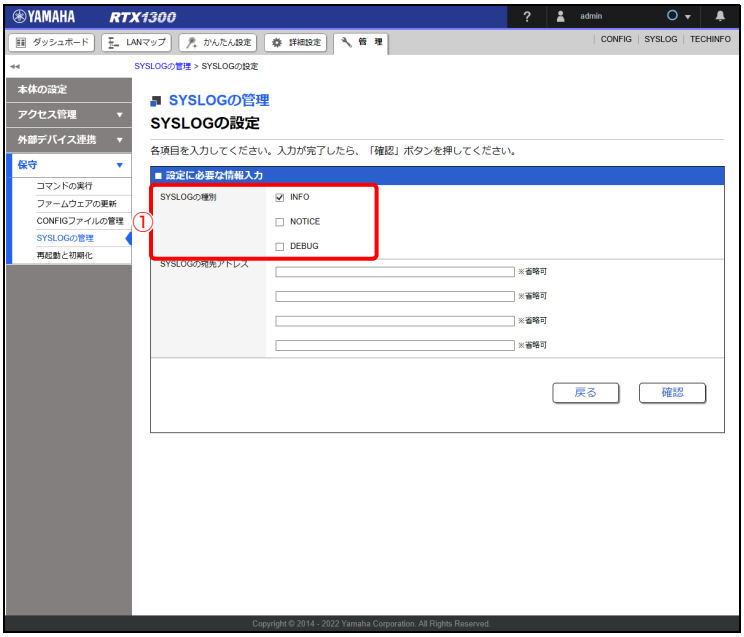
1. **「管理」タブ ―「保守」―「SYSLOG の管理」を順に選択する。**
「SYSLOG の管理」画面が表示されます。

2. 「SYSLOG の設定」項目の「設定」ボタンをクリックする。



「SYSLOG の設定」画面が表示されます。

3. SYSLOG に出力する種別を設定する。



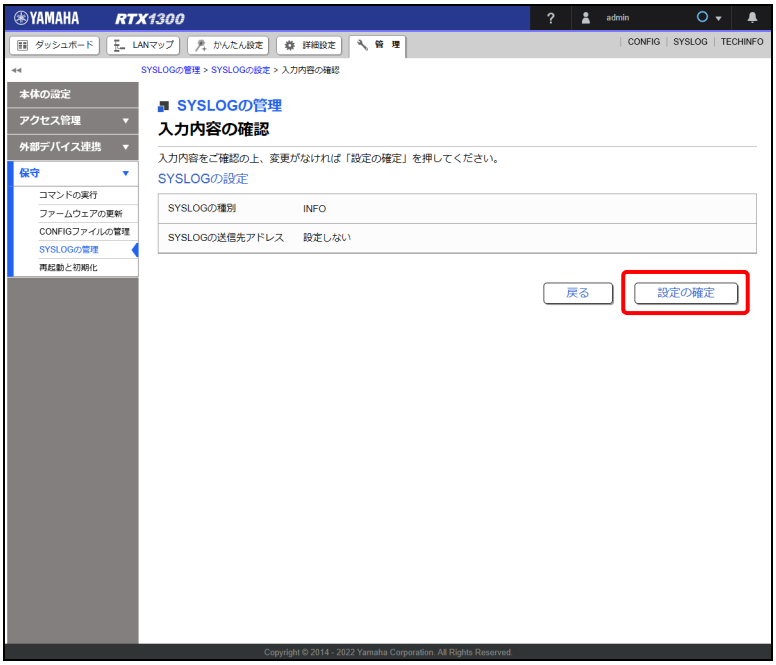
① SYSLOG の種別：
SYSLOG に出力したい種別のチェックボックスにチェックを入れます。

- INFO
  本製品の動作状況に関する情報を出力したい場合にチェックを入れます。
- NOTICE
  各種フィルター機能などで検出したパケット情報を出力したい場合にチェックを入れます。

- DEBUG
  デバッグ用の情報を出力したい場合にチェックを入れます。

4. **「確認」ボタンをクリックする。**
   「入力内容の確認」画面が表示されます。

5. **内容を確認し、「設定の確定」ボタンをクリックする。**

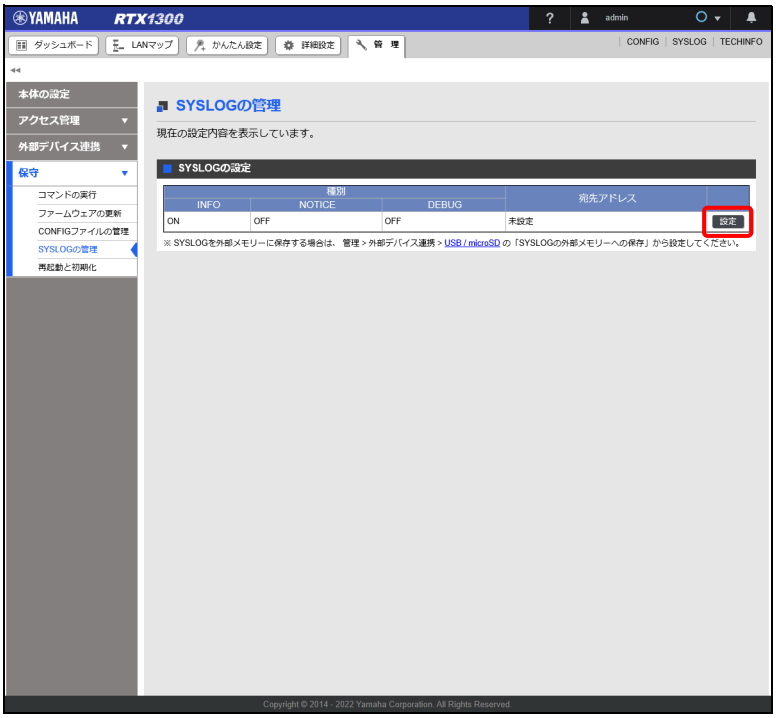


設定が反映され、「SYSLOG の管理」画面が表示されます。

15.10.2 SYSLOG をサーバーへ送信する

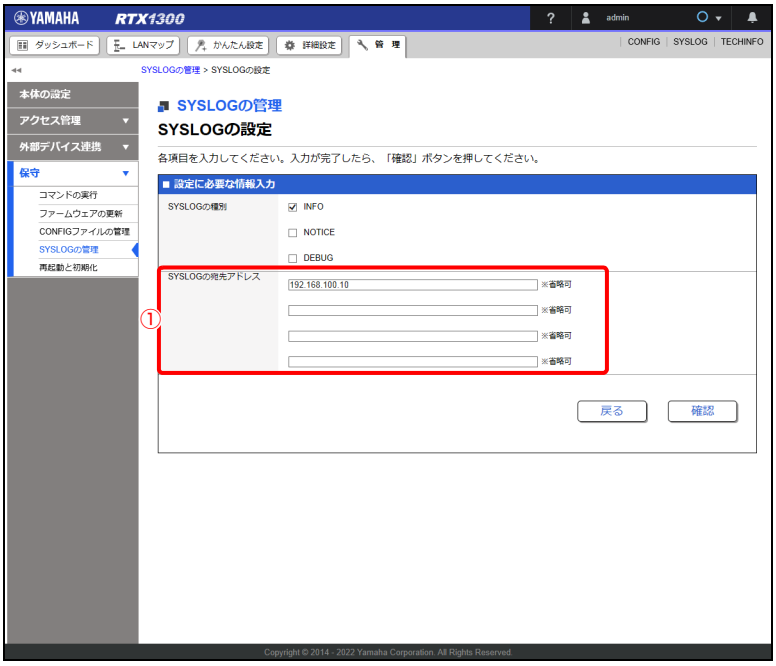
SYSLOG を SYSLOG ホストに送信する場合に、宛先の SYSLOG ホストの IP アドレスを設定します。

1. **「管理」タブ ―「保守」―「SYSLOG の管理」を順に選択する。**
   「SYSLOG の管理」画面が表示されます。
2. **「SYSLOG の設定」項目の「設定」ボタンをクリックする。**



「SYSLOG の設定」画面が表示されます。

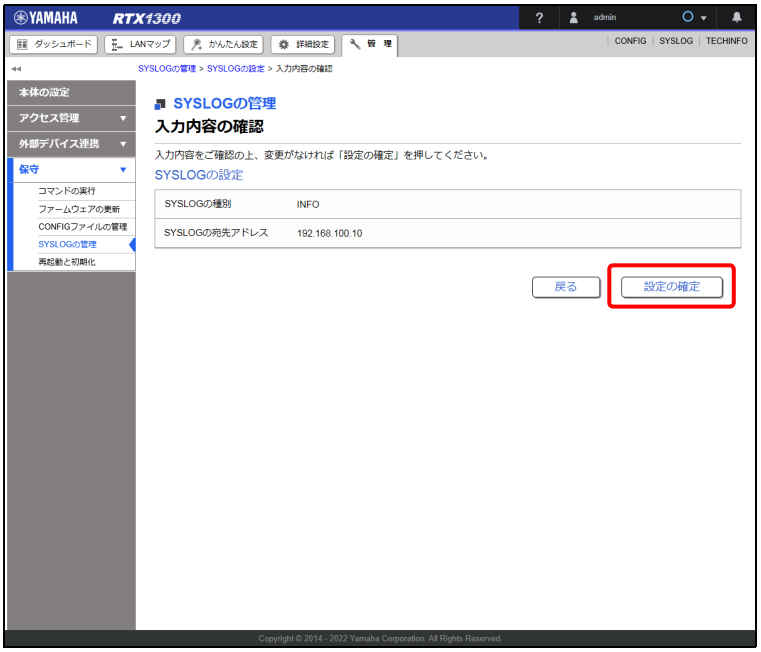
3. SYSLOG の宛先アドレスを設定する。



① SYSLOG の宛先アドレス：
SYSLOG の宛先のサーバー（SYSLOG ホスト）の IPv4 アドレスまたは IPv6 アドレスを入力します。最大で 4 つまで指定することができます。

4. 「確認」ボタンをクリックする。
「入力内容の確認」画面が表示されます。

5. 内容を確認し、「設定の確定」ボタンをクリックする。



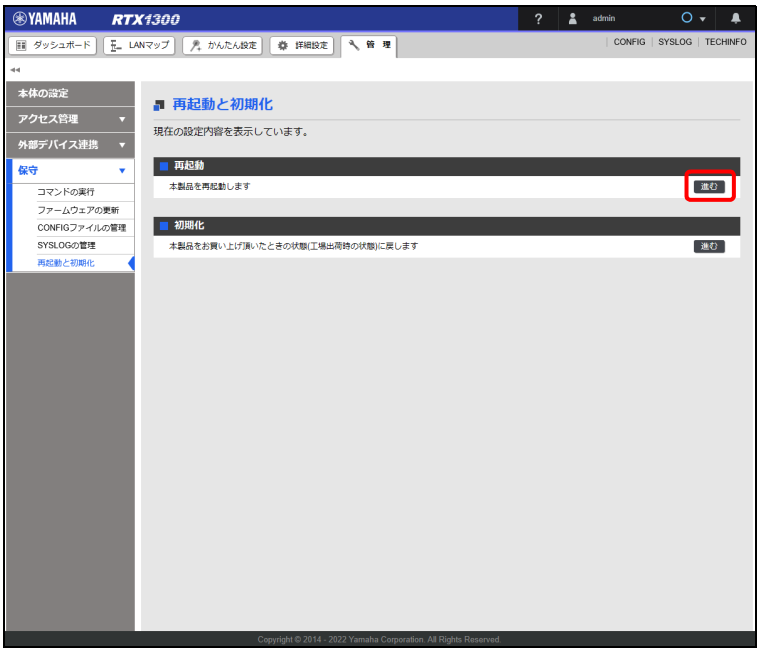
設定が反映され、「SYSLOG の管理」画面が表示されます。

15.11 本製品を再起動する

本製品の再起動を行います。

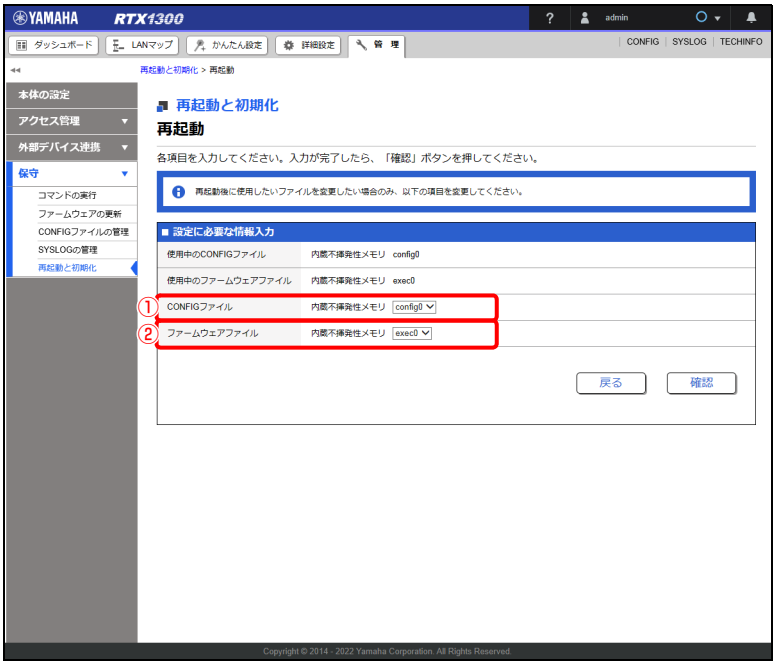
1. **「管理」タブ ―「保守」―「再起動と初期化」を順に選択する。**
   「再起動と初期化」画面が表示されます。

2. **「再起動」項目の「進む」ボタンをクリックする。**



「再起動」画面が表示されます。

3. **再起動後に使用するファイルを設定する。**



① **CONFIG ファイル：**
再起動後に使用したい設定（CONFIG）ファイルを選択します。

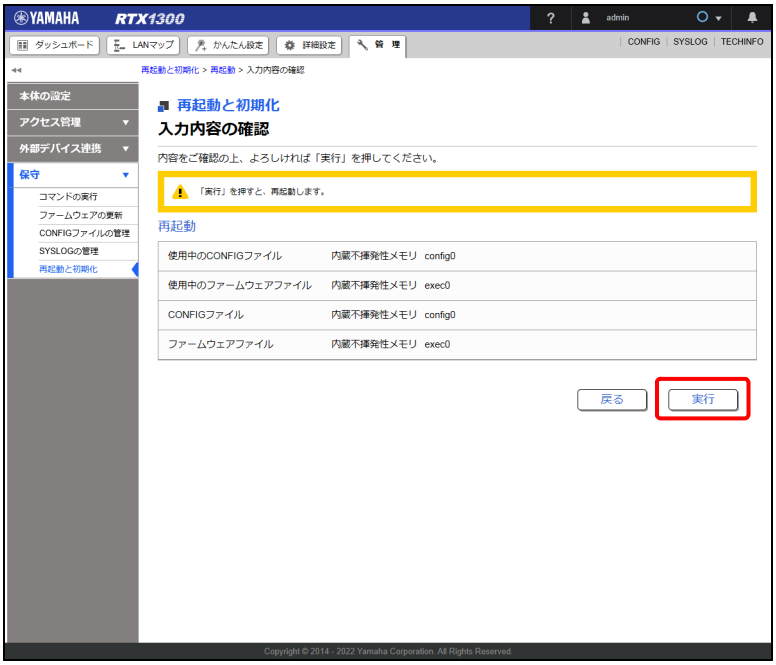
② **ファームウェアファイル：**
再起動後に使用したいファームウェアファイルを選択します。

メモ

再起動後も現在使用中のものと同じ CONFIG ファイル / ファームウェアファイルを使用する場合は、設定を変更せずに手順 4 へ進んでください。

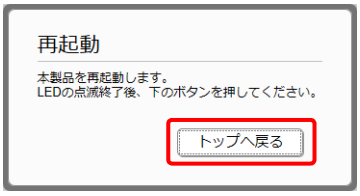
4. **「確認」ボタンをクリックする。**
「入力内容の確認」画面が表示されます。

5. **内容を確認し、「実行」ボタンをクリックする。**



「再起動」ダイアログが表示され、本製品が再起動します。

6. **本製品の再起動完了後、「トップへ戻る」ボタンをクリックする。**



ダッシュボードの Live 画面が表示されます。

メモ

再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「トップへ戻る」ボタンをクリックしてください。

15.12 本製品を工場出荷時の状態へ戻す

設定内容や SYSLOG などを消去し、本製品を工場出荷時の状態へ戻します。なお、ファームウェアは変更されません。

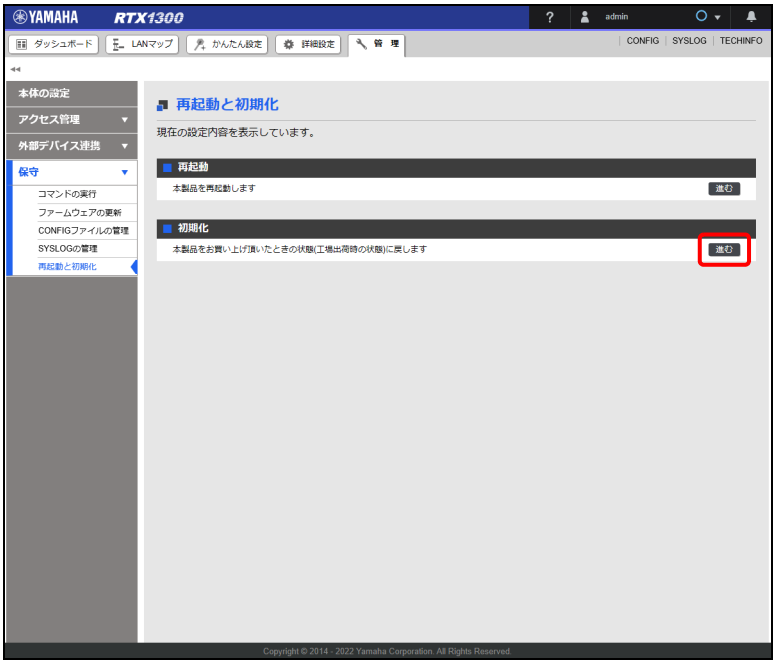
注意

工場出荷時の状態へ戻す場合は、以下の点にご注意ください。

- 実行した直後にすべての通信が切断されます。
- 本製品の LAN1 アドレスが初期設定値（192.168.100.1）に戻ります。
- 工場出荷時の状態に戻した後は設定内容を復元することはできません。必要に応じて、事前に外部メモリーなどに設定内容を退避してください。外部メモリーにエクスポートする方法について詳しくは、「15.9.3 設定（CONFIG）を外部メモリーにエクスポートする」（432 ページ）をご覧ください。

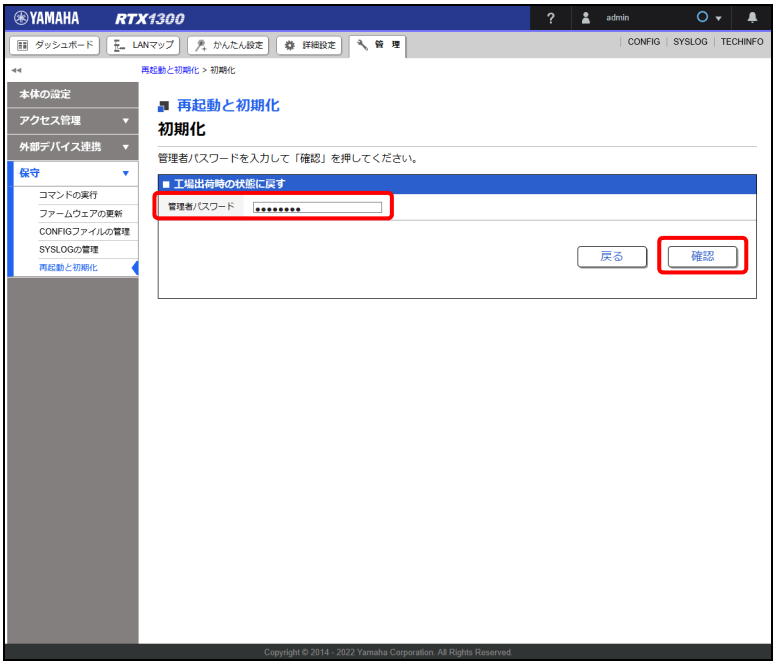
1. **「管理」タブ ―「保守」―「再起動と初期化」を順に選択する。**
   「再起動と初期化」画面が表示されます。

2. **「初期化」項目の「進む」ボタンをクリックする。**



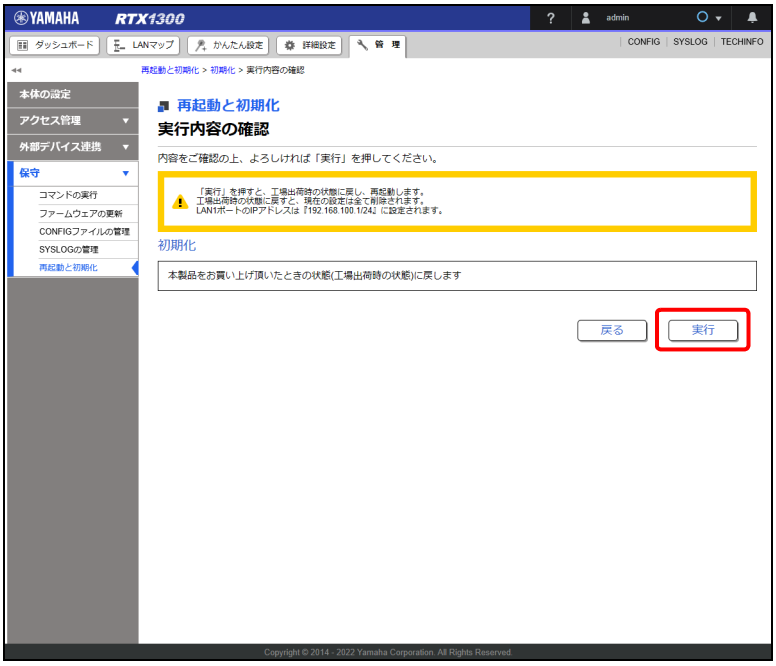
「初期化」画面が表示されます。

3. 管理パスワードを入力し、「確認」ボタンをクリックする。



「実行内容の確認」画面が表示されます。

4. 内容を確認し、「実行」ボタンをクリックする。



本製品が工場出荷時の状態に戻ります。また、「初期化」ダイアログが表示され、本製品が再起動します。

5. 本製品の再起動完了後、Web GUI へ再度アクセスする。

メモ

・ 再起動が完了するまでには数十秒ほどかかります。再起動が完了し本製品との通信状態が復旧してから「192.168.100.1/24」をクリックしてください。
・ 本製品の LAN1 アドレスが 192.168.100.1 に戻ります。Web GUI へ再度アクセスする際には 192.168.100.1 へアクセスしてください。

第 16 章 アプリケーション制御（DPI）を利用する

本章では、アプリケーション制御機能を利用するための設定について説明します。

16.1 アプリケーション制御とは？

アプリケーション制御は、DPI（Deep Packet Inspection）の技術を利用して、通信内容をアプリケーションごとに識別し、識別結果に基づいて経路の選択、フィルタリング、QoS による帯域制御を行うことのできる機能です。
Web GUI では、主要アプリケーション群のフィルタリングと経路の選択を簡単に行うことができます。また、通信トラフィックを可視化して識別したアプリケーションごとに Web GUI 上でグラフ表示することもできます。（147 ページ）

重要

- アプリケーション制御を利用するには、DPI ライセンスの購入が必要です。
- LMS によるライセンス認証やシグネチャーのダウンロードはインターネット経由で行われるため、アプリケーション制御を利用する前にインターネット接続の設定が必要です。
- アプリケーション制御機能による経路選択は IPv4 の通信のみ対応しています。IPv6 の通信では利用できません。

注意

コマンドコンソール画面からフィルター番号が 600000 ～ 699999 の DPI フィルターを設定している場合は、Web GUI でアプリケーション制御の設定を変更すると、DPI フィルターの設定が意図せず上書きされることがあります。

メモ

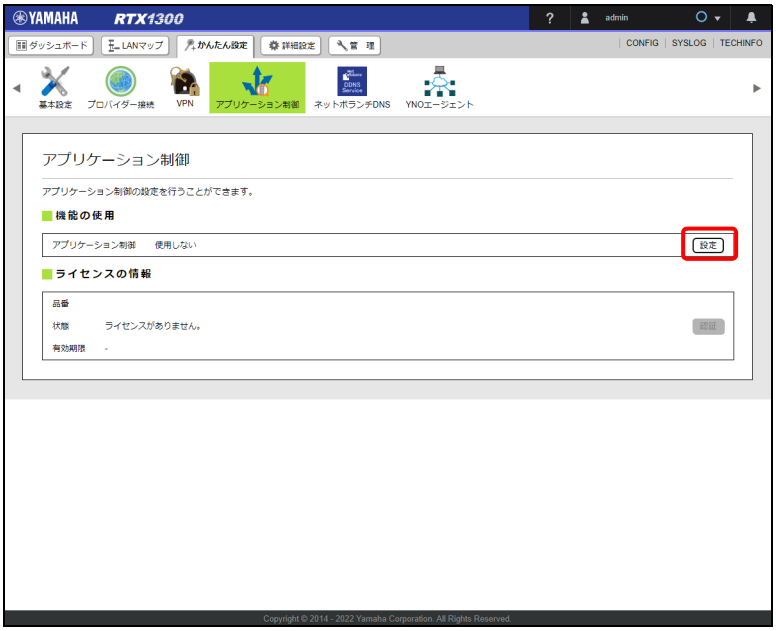
- アプリケーション制御を利用するには、ノーマルパスで処理する必要があります。Web GUI からアプリケーション制御を使用する設定を行うと、ノーマルパスに設定されます。
- トラフィック情報の統計を記録するには、統計情報の記録機能を有効にする必要があります。設定方法について詳しくは、「11.4.1 統計情報の記録を開始する」（138 ページ）をご覧ください。
- QoS による帯域制御は、本製品のコマンドコンソール画面から設定できます。
  設定方法について詳しくは、以下の URL をご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/dpi/

16.2 アプリケーション制御を有効にする

アプリケーション制御を使用するための設定方法を説明します。アプリケーション制御を有効にすることで、識別した通信トラフィックのグラフ表示や、経路の選択、フィルタリングの設定ができるようになります。

1. **「かんたん設定」タブ －「アプリケーション制御」を順に選択する。**
   「アプリケーション制御」画面が表示されます。

2. **「機能の使用」項目の「設定」ボタンをクリックする。**



「機能の使用」画面が表示されます。

3. **「使用する」を選択し、「次へ」ボタンをクリックする。**

「フィルターと経路の設定」画面が表示されます。

4. フィルターと経路を設定する。

Web GUI で設定できるアプリケーション

- Office365
- Windows/Apple Update
- 動画＆音楽配信
- ゲーム
- P2P
- SNS

① フィルタリング：

「破棄する」のチェックボックスにチェックを入れると、該当するアプリケーションのパケットが破棄されます。

② 経路：

経路のプルダウンメニューから経路を選択すると、選択したインターフェース経由でパケットを送信します。

メモ

その他のアプリケーションの詳細な設定は、本製品のコマンドコンソールから設定できます。

5. 「次へ」ボタンをクリックする。

「シグネチャーの保存設定」画面が表示されます。

6. シグネチャーの保存方法を設定する。

① **シグネチャーを保存する：**
ダウンロードしたシグネチャーを外部メモリーまたは内蔵不揮発性メモリーに保存する場合に選択します。本製品の USB ポートや microSD スロットに挿し込んだ外部メモリーまたは内蔵不揮発性メモリーを選択し、「参照」ボタンをクリックして「ディレクトリーの一覧」画面で保存先のディレクトリーを選択します。

メモ

- シグネチャーを外部メモリーまたは内蔵不揮発性メモリーに保存しない場合、次回アプリケーション制御を使用するときにもシグネチャーをダウンロードする必要があります。
- 最新のシグネチャーが利用可能な場合には、ダウンロード、および使用中のシグネチャーとの置き換えを自動で行います。

7. 「次へ」ボタンをクリックする。
「利用規約の確認」画面が表示されます。

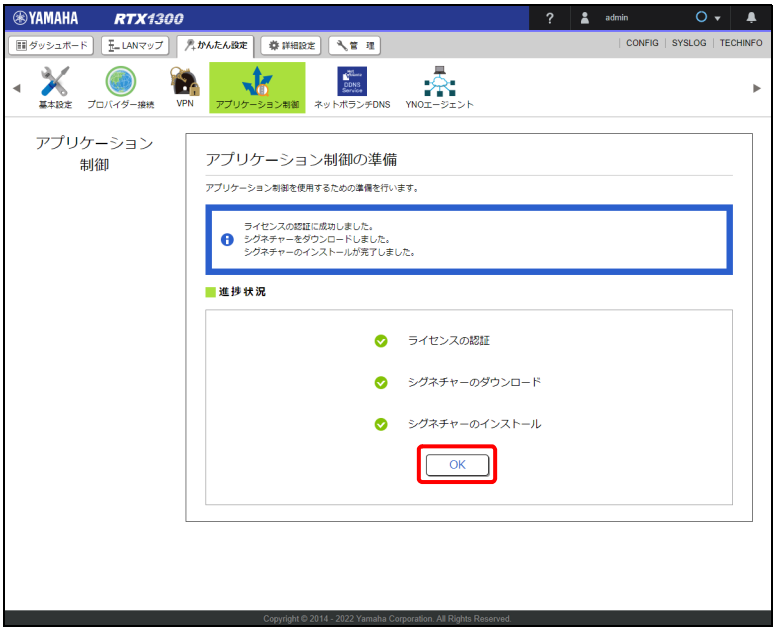
8. 利用規約の内容をよく確認し、「はい」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

9. 内容を確認し、「設定の確定」ボタンをクリックする。

「アプリケーション制御の準備」画面が表示され、アプリケーション制御を使用するための準備が行われます。

10.すべての処理が完了したことを確認して、「OK」ボタンをクリックする。



メモ

実行に失敗した項目がある場合は、処理が中止されます。エラーボックスのメッセージを確認し、設定を見直してください。

第 17 章 YNO（統合管理サービス）を利用する

本章では、YNO を利用して本製品の遠隔管理をするための設定について説明します。

17.1 YNO とは？

YNO は Yamaha Network Organizer の略で、ご利用いただいているヤマハネットワーク機器をクラウド上で監視・管理することのできるサービスです。
YNO では、管理対象となるヤマハネットワーク機器を YNO エージェント、クラウド上の管理サーバーを YNO マネージャーと呼びます。YNO マネージャーは、YNO エージェントの情報を収集したり、設定変更やコマンド実行などの制御命令を YNO エージェントに送信したりできます。本製品を YNO の管理対象に加えるには YNO エージェント機能を有効にする必要があります。
YNO のサービス内容について詳しくは、以下の URL をご覧ください。

Yamaha Network Organizer（YNO）製品情報
https://network.yamaha.com/products/software_service/ysl-yno/index

重要

- YNO を利用するには、ライセンスの購入が必要です。
- YNO エージェント機能の設定はインターネットに接続した状態で行う必要があるため、YNO を利用する前にインターネット接続の設定が必要です。
- YNO で使用しているオペレーター ID とアクセスコードを YNO エージェントにも設定する必要があるため、事前に用意してください。

注意

- YNO エージェント機能は YNO マネージャーと定常的に通信するほか、以下の操作により大容量のデータ通信が発生する場合があります。
  - ファイルサイズの大きな SYSLOG・CONFIG・ファームウェアの送受信
  - GUI Forwarder によるヤマハネットワーク機器の GUI の表示
  - LAS による各種ログの送信
- GUI Forwarder 経由でヤマハルーターにアクセスしている状態では、ダッシュボードの Live 画面や LAN マップ の自動更新は 3 分で停止します。
  その他 YNO をご利用いただく上での注意事項や制約については、以下の URL をご覧ください。

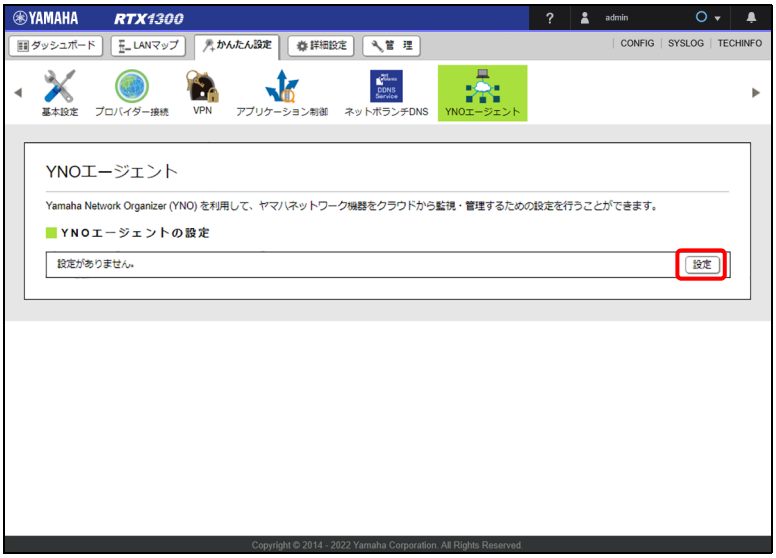
  YNO エージェント機能
  http://www.rtpro.yamaha.co.jp/RT/docs/yno/agent/index.html

17.2 YNO エージェント機能を有効にする

YNO エージェント機能を有効にして YNO の管理対象に加える方法を説明します。本製品に YNO エージェント機能の設定をすることで、YNO マネージャーから監視・管理を行うことができるようになります。

1. **「かんたん設定」タブ ― 「YNO エージェント」を順に選択する。**
   「YNO エージェント」画面が表示されます。

2.「設定」ボタンをクリックする。



「YNO エージェントの設定」画面が表示されます。

3. YNO エージェント機能の設定をする。

① オペレーター ID：
本製品を管理するオペレーターのオペレーター ID を入力します。

② アクセスコード：
YNO マネージャーに設定したアクセスコードを入力します。

③ 機器の説明：
任意の情報を入力します。この情報は YNO マネージャー側に通知されるため、一意に識別できる情報を設定しておくと、YNO マネージャー側で制御したい本製品を簡単に見つけられるようになります。

④ HTTPS プロキシー：
本製品の上位に HTTPS プロキシーサーバーが存在する場合は「使用する」を選択し、アドレスとポート番号を入力します。HTTPS プロキシーサーバーが存在しない場合は「使用しない」を選択します。

4. 「次へ」ボタンをクリックする。
「ライセンスの確認」画面が表示されます。

5. 利用規約の内容をよく確認し、「はい」ボタンをクリックする。

「入力内容の確認」画面が表示されます。

6. 内容を確認し、「設定の確定」ボタンをクリックする。

メモ

本製品の監視・管理は YNO マネージャーから行うことができます。
YNO マネージャーの使用方法について詳しくは、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/yno/manual/index.html

第 18 章 独自の GUI を作成する（カスタム GUI）

本製品に標準搭載されている Web GUI 画面とは別に、独自の Web GUI 画面を作成して本製品に組み込むことができます（カスタム GUI）。カスタム GUI を利用すれば、以下のようなことが実現できるようになります。

- ログインするユーザーに応じて個別のトップページを表示させる
- ユーザーごとに GUI でできることを変更する
- 必要最低限の機能に関してのみ、GUI から設定や情報参照ができるようにする
- 標準の GUI では対応していない機能の設定を行う
- GUI 画面上のボタンを一回クリックするだけで、全拠点に共通する基本的な設定（複数のコマンド群）を登録させる

カスタム GUI の使用方法について詳しくは、以下の URL をご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/custom-gui/
なお、カスタム GUI を使用するためには、HTTP プロトコルや HTML、JavaScript に関する基礎的な知識が必要となります。

第 19 章 困ったときは

本章では、Web GUI の使用時に直面しやすい問題、および、Web GUI から設定した機能において直面しやすい問題とその対処方法を記載します。本章の内容をご確認のうえ、症状に応じた対策を行ってください。

Web GUI で設定できない …457 ページ
インターネットに接続できない …458 ページ
VPN 通信できない …459 ページ
LAN マップに関する問題 …462 ページ
その他の問題 …466 ページ

それでも問題が解決しない場合は
サポート窓口までご相談ください（467 ページ）。

19.1 Web GUI で設定できない

症状	原因	対策
Web GUI を表示できない	本製品がパソコンを認識していない（LAN ポートの LINK/DATA インジケーターが点灯していない）	• 本製品および本製品に接続した機器の電源が入っていることを確認する。LAN ポートに機器を正しく接続しても、接続した機器の電源が入っていないときは、本製品の LAN インジケーターは点灯しない。 • 本製品側、パソコンおよび HUB 側共に、LAN ケーブルをコネクタからいったん外してから、もう一度カチッと音がするまで差し込む。 • 他の LAN ケーブルと取り替えてみる。 • パソコンの LAN ボード（カード）が正しくインストールされ、正しく動作していることを確認する。 • パソコンの LAN ボード（カード）と本製品の通信速度および接続（二重）モードが合っているか確認する。
	パソコンのネットワーク設定が不適切（LAN 上の他のパソコンやネットワークプリンタも使用できない）	• LAN ボードや LAN カードの設定をやり直して、パソコンを再起動する。 • IP アドレスをリセットする。
	本製品が誤動作している	本製品を工場出荷状態に戻してから、設定をやり直す（444 ページ）。
	本製品の URL が不適切である	本製品を初めて使うときや工場出荷状態に戻した後は、「http://192.168.100.1/」にアクセスする。
	本製品の IP アドレスを変更した	• 本製品に設定した IP アドレス「http://（本製品の IP アドレス）/」にアクセスする。 • 本製品と LAN に接続しているすべてのパソコンを再起動する。すべてのパソコンの再起動が困難な場合は、パソコンを 1 台だけ本製品に接続し、それ以外の LAN ケーブルを取り外してから、本製品とパソコンを再起動する。 • パソコンの設定が同じ IP アドレス範囲になっているか、他の機器と IP アドレスが重なっていないか確認する。
	ウェブブラウザーとして Internet Explorer を使用している	「1.3.1 推奨ウェブブラウザー」（15 ページ）にあるブラウザーを使用する。

症状	原因	対策
Web GUI を表示できない	初期管理ユーザーのパスワードが初期状態のとき WAN 側からアクセスしようとしている。	初期管理ユーザーの初期パスワードを変更する。
パスワードを入力しても Web GUI が表示されない	パスワードが間違っている（パスワードエラーが表示される）	「第 2 章 Web GUI へログインする」（18 ページ）の記載内容を確認し、再度ログイン操作を行う。
	初期管理ユーザーのパスワードが初期状態のとき初期管理ユーザー以外がアクセスしようとしている。	初期管理ユーザーの初期パスワードを変更する。
設定内容が元に戻ってしまう	設定後に「設定の確定」ボタンをクリックしていない	Web GUI で設定を変更したときは、必ず「設定の確定」ボタンをクリックして設定を保存する。
	設定可能範囲外の値や、設定不可能な値を入力した	正しい値を入力する。

19.2 インターネットに接続できない

症状	原因	対策
フレッツ・ADSL やフレッツ光で接続できない	本製品がブロードバンド回線を認識していない（LAN の LINK/DATA インジケーターが点灯していない）	• ADSL モデムやケーブルモデム、ONU の電源を入れる。 • ブロードバンド回線を接続している本製品の LAN ポートおよび ADSL モデムやケーブルモデム、ONU の配線をいったん外してから、もう一度カチッと音がするまで差し込む。 • ADSL モデムやケーブルモデム、ONU とパソコンを接続するものと、同じタイプのケーブルで本製品と接続する。
	ユーザー ID またはパスワードが間違っている	プロバイダーから指定されたユーザー ID に加えて、プロバイダー名まで指定する必要がある（例：username@xxx.ne.jp）。フレッツ・ADSL（またはフレッツ光）とプロバイダーの設定資料を参照して、正しく入力する。
	プロバイダーに接続されない	プロバイダー設定後に「かんたん設定」—「プロバイダー接続」画面の「接続する」ボタンをクリックして接続状態にする。
ダイヤルアップで接続できない	自動接続先のプロバイダー情報が登録されていない	•「かんたん設定」—「プロバイダー接続」画面から接続するプロバイダーを設定する。 • プロバイダー設定後に「かんたん設定」—「プロバイダー接続」画面の「接続する」ボタンをクリックして接続状態にする。

症状	原因	対策
インターネット上のウェブサイトが表示されない / 表示が遅い	プロバイダー設定の DNS サーバーアドレスが間違っている	• 「かんたん設定」—「プロバイダー接続」画面、または、「詳細設定」—「DNS サーバー」画面から、DNS サーバーアドレスの設定が正しいことを確認する。 • 各パソコンの DNS サーバーアドレス設定に本製品の IP アドレスを入力してから、パソコンを再起動する。 • Web サーバーや DNS サーバーが混雑または停止している可能性がある。しばらく時間をおいてから、アクセスしなおす。
	本製品のフィルターで遮断されている	プロバイダーから与えられた IP アドレスがプライベートアドレスで、フィルターを適用している場合は、フィルターの設定を変更する（242 ページ）。
	プロバイダーから与えられた IP アドレスと本製品に設定した IP アドレスが重複している	「かんたん設定」—「基本設定」—「LAN1 アドレス」画面で、本製品の IP アドレスをプロバイダーから与えられたものと重複しないアドレスに変更する（25 ページ）。その際、「設定に含まれる IP アドレスを自動的に変更する。」（25 ページの手順 3）のチェックボックスにチェックを入れ、本製品のフィルター設定も変更する必要がある。
	パソコンのネットワーク設定が不適切	• LAN ボードや LAN カードの設定をやり直して、パソコンを再起動する。 • IP アドレスをリセットする。
	回線やプロバイダー、Web サーバーが混雑している	時間帯などによっては、非常に遅くなる場合がある。回線速度に比べて非常に遅い状態が続く場合は、利用の回線業者やプロバイダーに問い合わせる。
インターネット上のサーバーから PING の応答が返ってこない	パソコンのファイアウォールまたはウィルス対策ソフトで PING がブロックされている。	パソコンのファイアウォールまたはウィルス対策ソフトを無効にするか、PING をブロックしないように設定を変更する。
	サーバーもしくは途中の経路で PING が破棄されている。	別のサーバーに対して PING を実行する。

19.3 VPN 通信できない

症状	原因	対策
IPsec を用いた拠点間接続が確立しない	プロバイダーからプライベート IP アドレスが割り当てられている	本製品にグローバル IP アドレスが割り当てられていない環境では、IPsec 関連の機能は利用できない。
	インターネットに接続していない	• インターネットに接続する設定を行っているかを確認する。 • 「19.2 インターネットに接続できない」（458 ページ）の説明に従って、問題を解決する。
	IPsec 接続先のルーターと通信ができない	IPsec 接続先のルーターの WAN 側 IP アドレスに対して ping コマンドを実行して、応答が返ってくるかどうかを確認する。 応答が返ってこない場合は、接続先の機器が通信可能な状態になっていることを確認する。

症状	原因	対策
拠点間接続（IPsec）経由の VPN 通信ができない	IPsec を用いた拠点間接続が確立していない	• IPsec の接続先と同じ認証鍵（pre-shared key）、認証アルゴリズム、暗号アルゴリズムを設定しているかを確認する。 • 接続先の IP アドレスまたはホスト名に、正しい値を設定しているかを確認する。
	経路情報が誤って設定されている	経路情報に接続先の LAN のネットワークアドレスが正しく設定されていることを確認する。
	接続先の LAN 内に設置されているパソコンの設定が誤っている	• 通信に使用するアプリケーションソフトウェアの設定を確認する。 • パソコンのファイアウォールまたはウィルス対策ソフトが有効になっている場合は、パソコンのファイアウォールまたはウィルス対策ソフトを無効にするか、通信に使用されているパケットをブロックしないように、ファイアウォールまたはウィルス対策ソフトの設定を変更する。
拠点間接続（IPsec）経由の VPN 通信が遅い	インターネットの通信が遅い	「19.2 インターネットに接続できない」の「インターネット上のウェブサイトが表示されない / 表示が遅い」（459 ページ）の説明に従って、問題を解決する。
L2TP/IPsec を用いたリモートアクセスができない	L2TP/IPsec の設定が間違っている	L2TP/IPsec の設定が正しいか確認する。
	ユーザー名とパスワードの設定が間違っている	ユーザー名とパスワードが正しいか確認する。
	YMS-VPN8 の設定が間違っている	• 接続先の IP アドレスまたはホスト名が正しいか確認する。 • L2TP/IPsec の事前共有鍵が正しいか確認する。 • ユーザー名とパスワードが正しいか確認する。 • YMS-VPN8 の設定に関しては、「9.2.3 YMS-VPN8 の設定をする」（101 ページ）を参照する。
	スマートフォンの設定が間違っている	• 接続先の IP アドレスまたはホスト名が正しいか確認する。 • L2TP/IPsec の事前共有鍵が正しいか確認する。 • ユーザー名とパスワードが正しいか確認する。 • スマートフォンの設定に関しては、スマートフォンのマニュアルを参照する。
	アクセスを試みているユーザーが登録されていない	「9.2.2 接続ユーザーを追加する」（99 ページ）を参照して、ユーザーを登録する。
	パソコン（YMS-VPN8）やスマートフォンと通信ができない	パソコン（YMS-VPN8）やスマートフォンの IP アドレスに対して ping コマンドを実行して、応答が返ってくることを確認する。 応答が返ってこない場合は、パソコン（YMS-VPN8）やスマートフォンの機器が通信可能な状態になっていることを確認する。
	パソコン（YMS-VPN8）やスマートフォン側で IP アドレスを取得できていない	パソコン（YMS-VPN8）やスマートフォン側で、VPN 接続先で使用する IP アドレスが取得できているかを確認する。
L2TP/IPsec 接続がすぐに切断される	スマートフォンの電波状況が悪い	スマートフォンの電波状況を確認して、電波状態の良い場所に移動する。

症状	原因	対策
PPTP を用いた拠点間接続が確立しない	プロバイダーからプライベート IP アドレスが割り当てられている	本製品にグローバル IP アドレスが割り当てられていない環境では、PPTP 関連の機能は利用できない。
	インターネットに接続していない	• インターネットに接続する設定を行っているかを確認する。 •「19.2 インターネットに接続できない」（458 ページ）の説明に従って、問題を解決する。
	PPTP 接続先のルーターと通信ができない	PPTP 接続先のルーターの WAN 側 IP アドレスに対して ping コマンドを実行して、応答が返ってくるかどうかを確認する。 応答が返ってこない場合は、接続先の機器が通信可能な状態になっていることを確認する。
拠点間接続（PPTP）経由の VPN 通信ができない	PPTP を用いた拠点間接続が確立していない	• PPTP サーバー / クライアントの設定が、自分側と相手側で正しく設定されているかを確認する。 • PPTP の接続先と同じユーザー ID と接続パスワードを設定しているかを確認する。 • 接続先の IP アドレスまたはホスト名に、正しい値を設定しているかを確認する。 • PPTP 設定後に「かんたん設定」—「プロバイダー接続」画面の「接続する」ボタンをクリックする。
	経路情報が誤って設定されている	経路情報に接続先の LAN のネットワークアドレスが正しく設定されていることを確認する。
	接続先の LAN 内に設置されているパソコンの設定が間違っている	• 通信に使用するアプリケーションソフトウェアの設定を確認する。 • パソコンのファイアウォールまたはウィルス対策ソフトが有効になっている場合は、パソコンのファイアウォールまたはウィルス対策ソフトを無効にするか、通信に使用されているパケットをブロックしないように、ファイアウォールまたはウィルス対策ソフトの設定を変更する。
PPTP を用いたリモートアクセスができない	PPTP の設定が間違っている	PPTP の設定が正しいか確認する。
	ユーザー名とパスワードの設定が間違っている	ユーザー名とパスワードが正しいか確認する。
	パソコンやスマートフォンの設定が間違っている	• 接続先の IP アドレスまたはホスト名が正しいか確認する。 • ユーザー名とパスワードが正しいか確認する。 • ユーザー認証方式が正しいか確認する。
	アクセスを試みているユーザーが登録されていない	「9.3.2 接続ユーザーを追加する」（108 ページ）を参照して、ユーザーを登録する。
	パソコンやスマートフォンと通信ができない	パソコンやスマートフォンの IP アドレスに対して ping コマンドを実行して、応答が返ってくることを確認する。 応答が返ってこない場合は、パソコンやスマートフォンの機器が通信可能な状態になっていることを確認する。
	パソコンやスマートフォン側で IP アドレスを取得できていない	パソコンやスマートフォン側で、VPN 接続先で使用する IP アドレスが取得できているかを確認する。

19.4 LAN マップに関する問題

19.4.1 LAN マップが使用できない

症状	原因	対策
「LAN マップ」画面が表示されない / インターフェース選択プルダウンメニューに LAN インターフェースが表示されない	LAN マップが有効になっていない	「12.3 LAN マップを有効にする」（153 ページ）を参照して、LAN マップを有効にする。
「LAN マップの設定」ダイアログに LAN インターフェースが表示されない	LAN インターフェースに IP アドレスが設定されていない	LAN インターフェースに IP アドレスを設定する。
「LAN マップの設定」ダイアログにブリッジインターフェースが表示されない	ブリッジインターフェースに IP アドレスが設定されていない	ip bridge1 address コマンドでブリッジインターフェースに IP アドレスを設定する。
	ブリッジインターフェースに LAN インターフェースが収容されていない	bridge member コマンドで LAN インターフェースをブリッジインターフェースに収容する。
LAN インターフェースで LAN マップを有効にできない	当該 LAN インターフェースを収容しているブリッジインターフェースで LAN マップが有効になっている	LAN インターフェースと当該 LAN インターフェースを収容しているブリッジインターフェースで、LAN マップを併用することはできない。
ブリッジインターフェースで LAN マップを有効にできない	ブリッジインターフェースに収容されている LAN インターフェースで LAN マップが有効になっている	LAN インターフェースと当該 LAN インターフェースを収容しているブリッジインターフェースで、LAN マップを併用することはできない。

19.4.2 エージェントが正しく表示されない

症状	原因	対策
エージェントが検出されない	エージェントが正しく接続されていない	LAN ケーブルをコネクタからいったん外してから、もう一度カチッと音がするまで差し込む。
	接続されているネットワーク機器が LAN マップに対応していない	LAN マップ未対応のヤマハネットワーク機器、および、他社製 L2 スイッチをエージェントとして検出することはできない。
エージェントルーターが検出されない	ルーターがエージェントモードで動作していない	エージェントとして動作させるルーターの Web GUI にアクセスしてエージェントモードを設定する。 エージェントモードの設定方法については、当該ルーターの Web GUI マニュアルを参照する。
	エージェントルーターの接続インターフェースで L2MS が有効化されていない	エージェントとして動作させるルーターの Web GUI にアクセスして接続インターフェースで L2MS を有効化する。 L2MS を有効にするインターフェースの設定方法については、当該ルーターの Web GUI マニュアルを参照する。

症状	原因	対策
エージェントが現れたり消えたりする	マネージャーに LAN マップ以外の機能による高負荷がかかっている	「12.3 LAN マップを有効にする」（153 ページ）を参照して、エージェントの監視時間間隔とエージェントの消失検出までの監視回数を延長する。
	エージェント数が推奨管理台数を越えている	• 「12.3 LAN マップを有効にする」（153 ページ）を参照して、エージェントの監視時間間隔とエージェントの消失検出までの監視回数を延長する。 • エージェント台数を推奨管理台数以下に減らす。エージェントの推奨管理台数は 64 台である。

19.4.3 端末が正しく表示されない

症状	原因	対策
端末が検出されない	端末の監視が有効になっていない	「12.3 LAN マップを有効にする」（153 ページ）を参照して、「端末も監視、管理する」を有効にする。
	端末が正しく接続されていない	LAN ケーブルをコネクタからいったん外してから、もう一度カチッと音がするまで差し込む。
	接続されている端末が通信を行っていない	定期的に何らかのパケットを送信している端末のみ永続的な検出が可能であるため、長時間パケットを送信していない端末は消失することがある。そのような端末を監視したい場合は、ping などで定期的に通信を行わせるようにする。
	端末がヤマハ無線 AP に接続されている	ヤマハ無線 AP に接続されている端末は、接続 / 切断を即時に検出することができない。ヤマハ無線 AP WLX302 のファームウェアリビジョンが Rev.12.00.15 以前の場合は、端末情報の監視時間間隔の設定した時間が経過するのを待つか、またはヤマハ無線 AP が接続されているエージェントの「接続機器ビュー」で「取得」ボタンをクリックする。ヤマハ無線 AP WLX302 のファームウェアリビジョンが Rev.12.00.16 以降の場合は、無線 AP 配下の端末情報の監視時間間隔に設定した時間が経過するのを待つか、またはヤマハ無線 AP が接続されているエージェントの「接続機器ビュー」で「取得」ボタンをクリックする。
	端末が他社製 L2 スイッチに接続されている	• 他社製 L2 スイッチに端末と LAN マップ対応ヤマハネットワーク機器の両方が接続されている構成では、他社製 L2 スイッチに接続されている端末を検出することはできない。 • 上記以外の構成においても、他社製 L2 スイッチまたは他社製無線 AP に接続されている端末は、接続 / 切断を即時に検出することができない。端末情報の監視時間間隔に設定した時間が経過するのを待つか、他社製 L2 スイッチまたは他社製無線 AP が接続されているエージェントの「接続機器ビュー」で「取得」ボタンをクリックする。
端末の経路が異なる	端末がヤマハ無線 AP WLX302 に接続されている	ヤマハ無線 AP WLX302 のファームウェアリビジョンが Rev.12.00.15 以前の場合は、ヤマハ無線 AP に接続されている端末は、ヤマハ無線 AP 直下ではなく、ヤマハ無線 AP と同じ場所（同じ経路）に接続されているものと見なされる。WLX302 のファームウェアを Rev.12.00.16 以降にリビジョンアップすることで、ヤマハ無線 AP 直下に表示される。
	端末が他社製 L2 スイッチに接続されている	他社製 L2 スイッチに接続されている端末は、他社製 L2 スイッチ直下ではなく、他社製 L2 スイッチと同じ場所（同じ経路）に接続されているものと見なされる。なお、他社製 L2 スイッチは表示されない。

19.4.4 スナップショット機能が動作しない

症状	原因	対策
スナップショット機能による警告メッセージが表示されない	スナップショット機能が有効になっていない	「12.3 LAN マップを有効にする」（153 ページ）を参照して、スナップショット機能を有効にする。
	スナップショットが保存されていない	「12.5.2 ネットワークの接続状態を監視する」（158 ページ）を参照して、スナップショットを保存する。

症状	原因	対策
スナップショット機能による端末に対する警告メッセージが表示されない	端末の監視が有効になっていない	「12.3 LAN マップを有効にする」（153 ページ）を参照して、「端末も監視、管理する」を有効にする。
	端末がスナップショットの比較対象になっていない	「12.3 LAN マップを有効にする」（153 ページ）を参照して、「端末も比較対象に含める」を有効にする。
	端末ごとの設定で監視対象に含まれていない	「12.13.2 端末の情報を編集する」（219 ページ）を参照して、「機器情報の編集」画面でスナップショット機能の「監視対象に含める」を選択する。
	端末がヤマハ無線 AP または他社製ネットワーク機器に接続されている	ヤマハ無線 AP または他社製ネットワーク機器に接続されている端末は、接続 / 切断を即時に検出することができない。ファームウェアリビジョンが Rev.12.00.15 以前のヤマハ無線 AP WLX302 に接続されている場合や、他社製ネットワーク機器に接続されている場合は、端末情報の監視時間間隔に設定した時間が経過すると警告メッセージが表示される。ファームウェアリビジョンが Rev.12.00.16 以降のヤマハ無線 AP WLX302 に接続されている場合は、無線 AP 配下の端末情報の監視時間間隔に設定した時間が経過すると警告メッセージが表示される。

19.4.5 タグ VLAN 間の通信を制限できない

症状	原因	対策
タグ VLAN 間で通信ができてしまう	VLAN 間フィルターが設定されていない	• 「12.11.5 タグ VLAN 間フィルターを設定する」（212 ページ）を参照して、VLAN 間の通信をすべて遮断する VLAN 間フィルターを設定する。 • 新規にタグ VLAN グループを作成した場合は、既存のタグ VLAN グループとの通信が開放されているため、再度上記の設定を行う必要がある。

19.4.6 ウェブブラウザーが操作できない

症状	原因	対策
ウェブブラウザーの動作が重い / ウェブブラウザーが反応しない	接続されている端末数が推奨管理台数を越えている	「12.3 LAN マップを有効にする」（153 ページ）を参照して、「端末も監視、管理する」を無効にするか、端末数を推奨管理台数（200 台）以下に減らす。

19.4.7 エージェントの Web GUI にアクセスできない

症状	原因	対策
エージェントルーターの Web GUI に HTTP プロキシー経由でアクセスできない	エージェントルーターで HTTP プロキシー経由での Web GUI アクセスが許可されていない	エージェントルーターの Web GUI に直接アクセスして、HTTP プロキシー経由での Web GUI アクセスを許可する。 HTTP プロキシー経由での Web GUI アクセスを許可する方法については、当該ルーターの Web GUI マニュアルを参照する。
L2VPN の対向機となっているエージェントルーターの Web GUI にアクセスできない	L2VPN の対向機となっているエージェントルーターでブリッジインターフェースからの Web GUI アクセスが許可されていない	L2VPN の対向機となっているエージェントルーターの httpd host コマンドでブリッジインターフェースからの Web GUI アクセスを許可する。

19.5 その他の問題

症状	原因	対策
本製品やパソコンで、NTP サーバーを使った時刻合わせができない	NTP サーバーの IP アドレスやドメイン名が間違っている	• 入手した NTP サーバー情報と比較し、正しく設定されていることを確認する。 • NTP サーバーに対して ping を実行し、NTP サーバーが稼動していることを確認する。
	登録されている NTP サーバーへの経路が設定されていない	プロバイダー設定や経路設定を確認する。
ネットボランチ DNS サービスでホストアドレスを取得できない	プロバイダーによっては、登録／更新してすぐに名前解決ができない場合がある	しばらく時間をおいてから、再度試してみる。
	ネットワーク型プロバイダー接続で接続している	ネットワーク型プロバイダー接続で接続している場合は、ネットボランチ DNS サービスは利用できない。IP アドレスを直接指定して接続する。
	プロバイダーからプライベート IP アドレスが割り当てられている	本製品にグローバル IP アドレスが割り当てられていない環境では、ネットボランチ DNS サービスは利用できない。
パスワードを忘れてしまった		「19.6 パスワードを忘れてしまった場合は」（467 ページ）を参照して、問題を解決する。

19.6 パスワードを忘れてしまった場合は

ログインパスワードを忘れてしまうと、Web GUI にログインできなくなります。

microSD、USB、DOWNLOAD の 3 つのボタンを押しながら電源を入れると、本製品が工場出荷時の状態に戻ります。工場出荷状態では、ユーザー名「admin」、パスワード「admin」を入力することで Web GUI にログインできます。

19.7 サポート窓口のご案内

弊社の担当者が技術サポートに必要な情報（TECHINFO）や設定情報（CONFIG）を確認させていただくことがあります。TECHINFO や CONFIG を問題の症状とあわせてお知らせいただくことで、問題の解決が早まることがあります。TECHINFO/CONFIG は、Web GUI の「TECHINFO」ボタンおよび「CONFIG」ボタンから取得することができます。TECHINFO/CONFIG の取得方法について詳しくは、「1.1.6 CONFIG」（13 ページ）、または、「1.1.8 TECHINFO」（14 ページ）をご覧ください。

第 20 章 付録

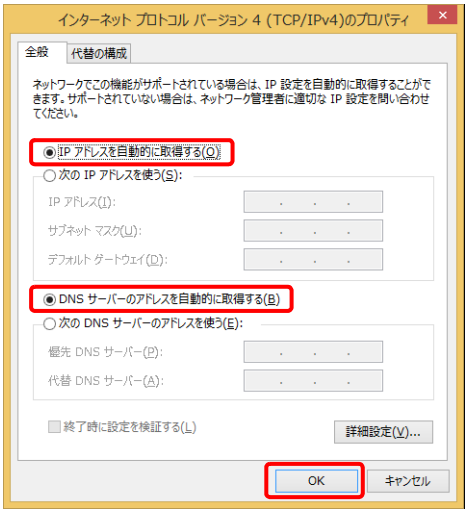
20.1 パソコンの IP アドレスを変更する

パソコンの IP アドレスを変更するには、以下の手順で操作します。

20.1.1 Windows 8.1 の場合

IP アドレスを自動取得するように設定する

1. 「デスクトップ」画面で、マウスカーソルを右上隅または右下隅に移動する。
2. チャームから「設定」―「コントロールパネル」―「ネットワークの状態とタスクの表示」―「アダプターの設定の変更」の順に選択する。
   「ネットワーク接続」画面が表示されます。
3. 変更する接続を右クリックし、「プロパティ」をクリックする。
4. 「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」を選択し、「OK」ボタンをクリックする。



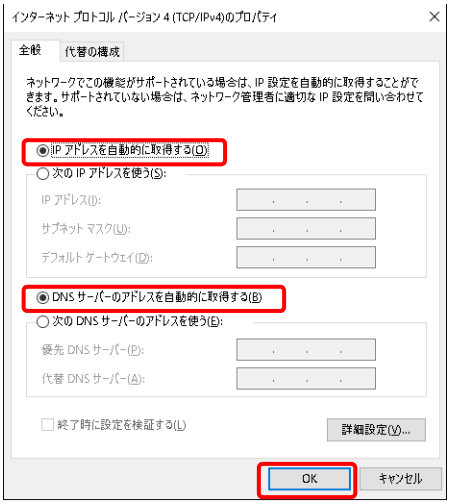
動的 IP アドレスの再割り当てを行う

1. 「デスクトップ」画面で、「スタート」を右クリックし、「コマンドプロンプト」を選択する。
2. 「ipconfig /release」と入力し、Enter キーを押す。
   パソコンに割り当てられていた IP アドレスが解放されます。
3. 「ipconfig /renew」と入力し、Enter キーを押す。
   新たな IP アドレスがパソコンに割り当てられます。

20.1.2 Windows 10 / Windows 11 の場合

IP アドレスを自動取得するように設定する

1. 「スタート」メニューから「コントロールパネル」を選択する。
2. 画面右上の「表示方法」を「大きいアイコン」に変更する。
   「すべてのコントロールパネル項目」画面が表示されます。
3. 「ネットワークと共有センター」をクリックする。
   「ネットワークと共有センター」画面が表示されます。
4. 「アダプターのオプションを変更する」をクリックする。
5. 変更する接続を右クリックし、「プロパティ」をクリックする。
6. 「インターネットプロトコル（TCP/IP)」を選択し、「プロパティ」ボタンをクリックする。
7. 「IP アドレスを自動的に取得する」と「DNS サーバーのアドレスを自動的に取得する」を選択し、「OK」ボタンをクリックする。



動的 IP アドレスの再割り当てを行う

1. 「スタート」を右クリックし、「コマンドプロンプト」を選択する。
2. 「ipconfig /release」と入力し、Enter キーを押す。
   パソコンに割り当てられていた IP アドレスが解放されます。
3. 「ipconfig /renew」と入力し、Enter キーを押す。
   新たな IP アドレスがパソコンに割り当てられます。

20.2 本製品を譲渡 / 廃棄する際のご注意

本製品を譲渡 / 廃棄する際は、以下の操作を行ってください。

1. **ネットボランチ DNS ホスト名の登録を解除する**

2. **設定内容を初期化する**
   初期化の仕方については、「15.12 本製品を工場出荷時の状態へ戻す」（444 ページ）をご覧ください。

注意

- 先に設定内容を初期化してしまうと、ネットボランチ DNS サーバーに登録されたホストアドレスを削除できなくなります。必ずネットボランチ DNS ホスト名の登録を解除してから、設定内容を初期化するようにしてください。
- 保存されている設定内容には、プロバイダーへの接続に必要な ID やパスワードも含まれています。設定内容を初期化せずに譲渡 / 廃棄すると、これらの情報が悪意のある第三者によって悪用されるおそれがあります。

重要

ネットボランチ DNS ホスト名の登録の解除は、ネットボランチ DNS ホスト名を登録したお客様のみ行ってください。

メモ

本製品を譲渡する際は、製品付属のマニュアル類もあわせて譲渡してください。

ヤマハ株式会社

2022年7月 発行 IP-A1