FWX120

ファイアウォール

取扱説明書

ヤマハFWX120をお買い上げいただきありがとうございます。
お使いになる前に本書をよくお読みになり、正しく設置や設定を行ってください。
本書中の警告や注意を必ず守り、正しく安全にお使いください。
本書はなくさないように、大切に保管してください。

はじめにお読みください

お買い上げいただき、ありがとうございます。
本製品は中・小規模の企業ネットワークに適した、ファイアウォールです。

付属品をご確認ください

- LANケーブル（1本）
- はじめにお読みください
- CD-ROM（1枚）
- 保証書（「はじめにお読みください」 19ページ）

本書の主な内容

ネットワークに接続するための情報

日々の運用管理に必要な情報

問題が発生した場合に、問題を解決するための情報

その他、本製品の機能を使いこなすための情報

他の説明書もご覧ください

本書は基本的な機能を使用するための情報のみを記載しています

用途に合わせて、以下の説明書／ヘルプをご覧ください。

- **コマンドリファレンス（付属CD-ROMに収録）**：コンソールコマンドを用いた、より詳細な設定方法が記載されています。
- **「かんたん設定ページ」のヘルプ**：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。「かんたん設定ページ」の「ヘルプ」をクリックしてください。

目次

第5章 VPNで拠点間接続する

第6章 本製品を使いこなす

第7章 本製品の運用管理

第8章
困ったときは

第9章
付録

本書の表記について

略称について

本書ではそれぞれの社名・製品について、以下のように略称で記載しています。

- Yamaha FWX120：本製品
- Microsoft® Windows®：Windows
- Microsoft® Windows® 7：Windows 7
- Microsoft® Windows Vista®：Windows Vista
- Microsoft® Windows® XP：Windows XP
- 10BASE-T/100BASE-TX/1000BASE-Tケーブル：LANケーブル
- 東日本電信電話株式会社：NTT東日本
- 西日本電信電話株式会社：NTT西日本

設定例について

本書に記載されているIPアドレスやドメイン名、URLなどの設定例は、説明のためのものです。実際に設定するときは、お使いの環境に合わせたものをお使いください。

詳細な技術情報について

本製品を使いこなすためには、インターネットやネットワークに関する詳しい知識が必要となる場合があります。付属の説明書などではこれらの情報について解説しておりませんので、詳しくは市販の解説書などを参考にしてください。

安全上のご注意

本製品を安全にお使いいただくために、下記の注意事項をよくお読みになり、必ず守ってお使いください。

7〜12ページに示した注意事項は、製品を安全に正しくご使用いただき、お客様や他の方々への危害や財産への損害を未然に防止するためのものです。

お読みになったあとは、使用される方がいつでも見られる所に必ず保管してください。

「警告」と「注意」について

以下、誤った取り扱いをすると生じることが想定される内容を、危害や損害の大きさと切迫の程度を明示するために、「警告」と「注意」に区分して掲載しています。

⚠ 警告

この表示の欄は、「死亡する可能性または重傷を負う可能性が想定される」内容です。

⚠ 注意

この表示の欄は、「傷害を負う可能性または物的損害が発生する可能性が想定される」内容です。

記号表示について

本書に表示されている記号には、次のような意味があります。

	「〜しないでください」という禁止を示します。
	「実行してください」という強制を示します。

⚠警告

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

- **本製品は一般オフィス向けの製品であり、人の生命や高額財産などを扱うような高度な信頼性を要求される分野に適応するようには設計されていません。**
- **本製品を誤って使用した結果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。**

 必ず実行	**下記の場合には、すぐに電源コードをコンセントから抜く。** **• 異常なにおいや音がする** **• 煙が出る** **• 破損した** **• 水がかかった** そのまま使用すると、火災や感電の原因になります。 必ず販売店に修理や点検をご依頼ください。
 ぬれ手禁止	**ぬれた手で本製品を扱わない。** 感電や故障の原因になります。
 禁止	**パネルのすき間から金属や紙片など異物を入れない。** 火災や感電、故障の原因になります。
 分解禁止	**分解・改造は絶対にしない。** 火災や感電、故障の原因になります。
 禁止	**ケーブルを傷つけない。** **• 重いものを上に載せない** **• 加工をしない** **• ステープルで止めない** **• 無理な力を加えない** **• 熱器具には近づけない** 火災や感電、故障の原因になります。
 必ず実行	**必ず日本国内AC100V(50/60Hz)の電源電圧で使用する。** 海外など異なる電源電圧で使用すると、火災や感電、故障の原因になります。
 必ず実行	**電源プラグは、見える位置で、手が届く範囲のコンセントに接続する。** 万一の場合、電源プラグを容易に引き抜くためです。

 必ず実行	**電源プラグは、コンセントに根元まで、確実に差し込む。** 差し込みが不十分なまま使用すると感電したり、プラグにほこりが堆積して発熱や火災の原因になります。
 必ず実行	**コンセントやテーブルタップの電流容量を確認し、本製品を使用してもこの容量を越えないことを確認する。** テーブルタップなどが過熱、劣化して火災の原因になります。
 必ず実行	**各ポートの規格に適合したケーブルを接続する。** 本来とは異なるケーブルを接続すると、火災や故障の原因になります。
 禁止	**ポート部を指や金属で触れない。** 感電や故障の原因になります。
 禁止	**本製品を落下させたり、強い衝撃を与えない。** 内部の部品が破損し、感電や火災、故障の原因となります。
 禁止	**ほこりや湿気の多い場所、油煙や湯気があたる場所、腐蝕性ガスがかかる場所に設置しない。** 火災や感電、故障の原因になります。
 禁止	**放熱を妨げない。** **• 布やテーブルクロスをかけない** **• 通気性の悪い狭いところへは押し込まない** **• 通風口をふさがない** 本製品の内部に熱がこもり、火災や故障の原因になります。
 接触禁止	**雷が鳴りはじめたら、本体や電源ケーブルには触れない。** 感電の恐れがあります。
 必ず実行	**電源ケーブルのゴミやほこりは、定期的に取り除く。** ほこりがたまったまま使用を続けると、火災の原因になります。

⚠注意

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

 禁止	**不安定な場所や振動する場所には設置しない。** 本製品が落下や転倒して、けがや故障の原因になります。
 禁止	**直射日光のあたる場所や、温度が異常に高くなる場所(暖房機のそばなど)には設置しない。** 故障の原因になります。
 禁止	**環境温度が急激に変化する場所では使用しない。** 環境温度が急激に変化すると、本製品に結露が発生することがあります。そのまま使用すると故障の原因になるため、結露が発生したときは電源を入れない状態で乾くまでしばらく放置してください。
 禁止	**本製品を他の機器と重ねて置かない。** 熱がこもり、故障の原因になります。
 禁止	**電源を入れたままケーブル類を接続しない。** 本製品および接続機器の故障の原因になります。
	**本製品に触れるときは、人体や衣服から静電気を除去する。** 静電気によって故障するおそれがあります。
	**アースコードを接続することで、静電気対策やノイズ防止に効果があります。** アース接続は必ず、電源コードをコンセントに繋ぐ前に行ってください。 また、アース接続を外す場合は、必ず電源コードをコンセントから取り外してから行ってください。

使用上のご注意

- 本製品のUSBポートにUSBデータ通信端末を接続して、3G/LTEモバイル網を利用したワイヤレスWAN接続ができます。データ通信端末のご契約が定額制であっても、設定を誤って使用すると従量制の通信料金がかかる場合があります。本製品の使用方法や設定を誤って使用した結果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。
- 本製品のUSBポートおよびmicroSDスロットは、すべてのUSBメモリおよびmicroSDカードの動作を保証するものではありません。
- USBメモリおよびmicroSDカードの動作確認は、「かんたん設定ページ」−「詳細設定と情報」−「外部デバイスの設定」画面の「外部メモリの性能テスト」欄で行うことができます。また、USBメモリおよびmicroSDカードについて詳しくは、以下のURLをご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/external-memory/
- USBメモリおよびmicroSDカード上のデータは定期的にバックアップすることをお勧めします。本製品のご利用にあたりデータが消失、破損したことによる被害については、弊社はいかなる責任も負いかねますので、あらかじめご了承ください。
- 本製品の使用方法や設定を誤って使用した結果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。
- 本製品は磁界が強い場所に設置しないでください。
- 本製品の同一電源ライン上にノイズを発生する機器を接続しないでください。
- 本製品のご使用にあたり、周囲の環境によっては電話、ラジオ、テレビなどに雑音が入る場合があります。この場合は本製品の設置場所、向きを変えてみてください。
- 1000BASE-T でご使用になる場合は、エンハンスドカテゴリー５（CAT5e）以上のLAN ケーブルをご使用ください。
- 本製品を譲渡する際は、「はじめにお読みください」および付属CD-ROMも合わせて譲渡してください。
- 本製品では、時計機能の電源バックアップのためにリチウム電池を使用しています。廃棄する際はお住まいの自治体の指示に従ってください。
- 本製品を譲渡/廃棄する際は、「本製品を譲渡／廃棄する際のご注意」(232ページ)をご覧の上、以下の操作を行ってください。
  1.ネットボランチDNSの登録を削除する
  2.設定内容を初期化する

重要なお知らせ

セキュリティー対策と本製品のファイアウォール機能について

インターネットを利用すると、ホームページで世界中の情報を集めたり、電子メールでメッセージを交換したりすることができ、とても便利です。その一方で、お使いのパソコンが世界中から不正アクセスを受ける危険にさらされることになります。

特にインターネットに常時接続したり、サーバーを公開したりする場合には、不正アクセスの危険性を理解して、セキュリティー対策を行う必要があります。本製品はそのためのファイアウォール機能を装備していますが、不正アクセスの手段や抜け道(セキュリティーホール)は、日夜新たに発見されており、それを防ぐ完璧な手段はありません。**インターネット接続には、常に危険がともなうことをご理解いただくとともに、常に新しい情報を入手し、自己責任でセキュリティー対策を行うことを強くおすすめいたします。**

通信料金について

本製品を従量課金型回線サービス(データコネクト、3G/LTEモバイル網など)でお使いになる場合には、自動発信の機能をよくご理解の上ご使用ください。本製品をパソコンやLANに接続した場合、本製品はパソコンのソフトウェア(電子メールソフトウェアやWebブラウザなど)が送信するデータや、LAN上を流れるデータの宛先を監視します。LAN以外の宛先があると、あらかじめ設定された内容に従って自動的に回線への発信を行います。

そのため、**設定間違いや回線切断忘れがあると、ソフトウェアや機器が定期的にパケットを送信して、予想外の通信料金やプロバイダ接続料金がかかる場合があります。**

ときどき通信記録を調べて、意図しない発信がないかご確認ください。また、本製品の設定やリビジョンアップなどの最新情報を得るために、定期的にヤマハネットワーク周辺機器ホームページ(http://jp.yamaha.com/products/network/)をご覧になることを強くおすすめいたします。

以下の場合に、予想外の通信料金がかかっていることがあります

- 本製品を使い始めたとき
- 本製品のプロバイダ接続設定を変更したとき
- パソコンに新しいソフトウェアをインストールしたとき
- ネットワークに新しいパソコンやネットワーク機器、周辺機器などを接続したとき
- 本製品のファームウェアをリビジョンアップしたとき
- その他、いつもと違う操作を行ったり、通信の反応に違いを感じたときなど

ご注意

- プロバイダ契約を解除／変更した場合は、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。削除しないままお使いになると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- プロバイダ側の状態(アクセスポイントの変更、メンテナンス、障害など)によって、予想外の通信料金がかかる場合があります。プロバイダからの告知情報には常にご注意ください。

本製品の累積接続時間管理について

本製品を従量課金型回線サービス(3G/LTEモバイル網など)に接続して使用する場合、累積送受信データによる発信制限や、累積接続時間による発信制限をかけることができます。これらの機能は、本製品が計算する累積送受信データや累積接続時間に基づいて行われるため、サービス割引などによる異なる料金算出方法や、プロバイダ独自の通信時間算出方法には対応できません。

従って、実際の運用においては、発信制限動作が意図した通りにならない場合があります。正確を期す場合は、一定期間試験運用をするなどしてずれがないかを確認してください。

電波障害自主規制について

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

高調波について

JIS C 61000-3-2適合品

JIS C 61000-3-2適合品とは、日本工業規格「電磁両立性－第3-2部：限度値－高調波電流発生限度値（1相当たりの入力電流が20A以下の機器）」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

商標について

- 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。
- 本製品は、RSA Security Inc.のRSA® BSAFE™ ソフトウェアを搭載しております。RC4およびBSAFEはRSA Security Inc.の米国およびその他の国における登録商標です。

本製品で使用しているオープンソースソフトウェア

- PCRE
- MT19937
- OpenSSL
- Original SSLeay
- Net-SNMP

ライセンス条文について詳しくは、「ライセンス条文」（233ページ）をご覧ください。

DOWNLOADボタンご使用時のソフトウェアライセンス契約について

本製品の設定を変更することにより、DOWNLOADボタンを操作して、本製品の内蔵ファームウェアをリビジョンアップすることができます。
リビジョンアップを許可するように設定を変更する、および、DOWNLOADボタンを押してリビジョンアップを実行する、という操作は、ソフトウェアライセンス契約(以下「本契約書」)に同意したこととみなされます。ご使用になられる前に、必ず本契約書をお読みください。
本契約書の内容に同意していただけない場合には、DOWNLOADボタンの操作によるファームウェアのリビジョンアップを許可する設定に変更しないでください。過失を含むいかなる場合であっても、ヤマハは、本ソフトウェアに起因するお客様側の損害について一切の責任を負いません。
DOWNLOADボタンの詳しい操作方法は、「DOWNLOADボタンでリビジョンアップする」(189ページ)にてご確認ください。
本書はお使いになる方がなくさないように大切に保管してください。

ソフトウェアライセンス契約

本契約は、お客様とヤマハ株式会社(以下、ヤマハといいます)との間の契約であって、ヤマハファイアウォール製品(以下「本製品」といいます)用ファームウェアおよびこれに関わるプログラム、印刷物、電子ファイル(以下「本ソフトウェア」といいます)をヤマハがお客様に提供するにあたっての条件を規定するものです。
「本ソフトウェア」は、「本製品」で動作させる目的においてのみ使用することができます。
本契約は、ヤマハがお客様に提供した「本ソフトウェア」および本契約第1条第(1)項の定めに従ってお客様が作成した「本ソフトウェア」の複製物に適用されます。

1. 使用許諾

(1) お客様は、「本ソフトウェア」をお客様が所有する「本製品」またはパーソナルコンピュータ等のデバイスにインストールして使用することができます。

(2) お客様は、本契約に明示的に定められる場合を除き、「本ソフトウェア」を、再使用許諾、販売、頒布、賃貸、リース、貸与もしくは譲渡し、特定もしくは不特定多数の者によるアクセスが可能なウェブ・サイトもしくはサーバー等にアップロードし、または、複製、翻訳、翻案もしくは他のプログラム言語に書き換えてはなりません。お客様はまた、「本ソフトウェア」の全部または一部を修正、改変、逆アセンブル、逆コンパイル、その他リバース・エンジニアリング等してはならず、また第三者にこのような行為をさせてはなりません。

(3) お客様は、「本ソフトウェア」に含まれるヤマハの著作権表示を変更、除去、または削除してはなりません。

(4) 本契約に明示的に定める場合を除き、ヤマハは、「本ソフトウェア」に関するヤマハの知的財産権のいかなる権利もお客様に付与または許諾するものではありません。

2. 所有権

「本ソフトウェア」は、著作権法その他の法律により保護され、ヤマハにより所有されています。お客様は、ヤマハが、本契約に基づきまたはその他の手段により「本ソフトウェア」に係る所有権および知的財産権をお客様に譲渡するものではないことを、ここに同意するものとします。

DOWNLOADボタンご使用時のソフトウェアライセンス契約について（つづき）

3. 輸出規制

お客様は、当該国のすべての適用可能な輸出管理法規や規則に従うものとし、また、かかる法規や規則に違反して「本ソフトウェア」の全部または一部を、いかなる国へ直接もしくは間接に輸出もしくは再輸出してはなりません。

4. サポートおよびアップデート

ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取扱者および頒布者は、「本ソフトウェア」のメンテナンスおよびお客様による「本ソフトウェア」の使用を支援することについて、いかなる責任も負うものではありません。また、本契約に基づき「本ソフトウェア」に対してアップデート、バグの修正あるいはサポートを行う義務もありません。

5. 責任の制限

(1)「本ソフトウェア」は、『現状のまま（AS-IS)』の状態で使用許諾されます。ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取扱者および頒布者は、「本ソフトウェア」に関して、商品性および特定の目的への適合性の保証を含め、いかなる保証も、明示たると黙示たるとを問わず一切しないものとします。

(2) ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取扱者および頒布者は、「本ソフトウェア」の使用または使用不能から生ずるいかなる損害（逸失利益およびその他の派生的または付随的な損害を含むがこれらに限定されない）について、一切責任を負わないものとします。たとえ、ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取扱者および頒布者がかかる損害の可能性について知らされていた場合でも同様です。

(3) ヤマハ、ヤマハの子会社、それらの販売代理店および販売店、並びに、その他「本ソフトウェア」の取扱者および頒布者は、「本ソフトウェア」の使用に起因または関連してお客様と第三者との間に生じるいかなる紛争についても、一切責任を負わないものとします。

6. 有効期間

(1) 本契約は、下記（2）または（3）により終了されるまで有効に存続します。

(2) お客様は、「本製品」にインストール済みのすべての「本ソフトウェア」を消去することにより、本契約を終了させることができます。

(3) お客様が本契約のいずれかの条項に違反した場合、本契約は直ちに終了します。

(4) お客様は、上記（3）による本契約の終了後直ちに、「本製品」にインストール済みのすべての「本ソフトウェア」を消去するものとします。

(5) 本契約のいかなる条項にかかわらず、本契約第２条から第６条の規定は本契約の終了後も効力を有するものとします。

7. 分離可能性

本契約のいかなる条項が無効となった場合でも、本契約のそれ以外の部分は効力を有するものとします。

8. U.S. GOVERNMENT RESTRICTED RIGHTS NOTICE:

The Software is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (Oct 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.72024 (June 1995), all U.S. Government End Users shall acquire the Software with only those rights set forth herein.

9. 一般条項

お客様は、本契約が本契約に規定されるすべての事項についての、お客様とヤマハとの間の完全かつ唯一の合意の声明であり、口頭あるいは書面による、すべての提案、従前の契約またはその他のお客様とヤマハとのあらゆるコミュニケーションに優先するものであることに同意するものとします。本契約のいかなる修正も、ヤマハが正当に授権した代表者による署名がなければ効力を有しないものとします。

10. 準拠法

本契約は、日本国の法令に準拠し、これにもとづいて解釈されるものとします。

本製品のお客様サポートについて(サポート規定)

ヤマハ株式会社は本製品を快適に、またその性能・機能を最大限に活かしたご利用が可能となりますように以下の内容・条件にてサポートをご提供いたします。

1.サポート方法

① FAQ、技術情報、設定例、ソリューション例等のWeb 掲載
② 電話でのご質問への回答
③ お問い合わせフォームからのご質問への回答
④ カタログ送付
⑤ 代理店・販売店からの回答

ご質問内容によっては代理店・販売店へご質問内容を案内し、代理店・販売店よりご回答させていただく場合がありますので予めご了承のほどお願い致します。

2.サポート項目

① 製品仕様について
② お客様のご利用環境に適した弊社製品の選定について
③ 簡易なネットワーク構成での利用方法について
④ お客様作成の config の確認、及び log の解析
⑤ 製品の修理について
⑥ 代理店または販売店のご紹介

3.免責事項・注意事項

① 回答内容につきましては正確性を欠くことのないように万全の配慮をもって行いますが、回答内容の保証、及び回答結果に起因して生じるあらゆる事項について弊社は一切の責任を負うことはできません。

また、サポートの結果又は製品をご利用いただいたことによって生じたデータの消失や動作不良等によって発生した経済的損失、その対応のために費やされた時間的・経済的損失、直接的か間接的かを問わず逸失利益等を含む損失及びそれらに付随的な損失等のあらゆる損失について弊社は一切の責任を負うことはできません。

尚、これらの責任に関しては弊社が事前にその可能性を知らされていた場合でも同様です。但し、契約及び法律でその履行義務を定めた内容は、その定めるところを遵守するものと致します。

② ファームウェアの修正は弊社が修正を必要と認めたものについて生産終了後２年間行います。
③ 質問受付対応、修理対応は生産終了後５年間行います。
④ 実ネットワーク環境での動作保証、性能保証は行っておりません。
⑤ 期日・時間指定のサポート、及び海外での使用、日本語以外でのサポートは行っていません。
⑥ お問い合わせの回答を行うにあたって、必要な情報のご提供をお願いする場合があります。情報のご提供がない場合は適切なサポートができない場合があります。
⑦ 再現性がない、及び特殊な環境でしか起きない等の事象に関しては、解決のための時間がかかったり適切なサポートが行えない場合があります。
⑧ オンサイト保守・定期保守等は代理店にて有償で行います。詳細な内容は代理店にご確認をお願い致します。
⑨ 他社サービス、他社製品、及び他社製品との相互接続に関してのサポートは弊社 Web 上に掲載している範囲に限定されます。
⑩ やむを得ない事由により本製品の返品・交換が生じた場合は、ご購入店経由となります。尚、返品・交換に際しましてはご購入店、ご購入金額を証明する証憑が必要となります。
⑪ 製品の修理は代理店・販売店経由で受付けさせていただきます。弊社への直接持ち込みはできません。また、着払いでの修理品受付は致しておりません。発送は弊社指定の通常宅配便(国内発送のみ)にて行わせていただきます。修理完了予定期間は変更になる場合がありますのでご了承のほどお願い致します。尚、保証期間中の無償修理（無償例外事項）等の詳細規定は保証書に記載しております。
⑫ 上記サポート規定は予告なく変更されることがあります。

本製品でできること

本製品は中・小規模の企業ネットワークに適した、ギガビットイーサネット対応のファイアウォールです。

透過型ファイアウォール機能

透過型ファイアウォール機能により、ネットワークの変更が難しい環境でも手軽にセキュリティーを高めることができます。既存のネットワークの設定を変更せずに導入ができるため、運用を止めることなくファイアウォール機能を追加することができます。

セキュリティーアドバイス機能

セキュリティーアドバイス機能は、「診断機能」「監視機能」「レポート機能」の3つで構成されています。
「診断機能」は、運用前に脆弱な設定がされていないかをチェックします。
「監視機能」は、運用中に攻撃者による侵入行為や攻撃行為をモニタリングします。
「レポート機能」を利用し、トラフィックや異常発生状況を表示することで、直感的にネットワーク状況を判断することができます。

URLフィルター機能

URLフィルターの機能は、「内部データベース参照型URLフィルター」と「外部データベース参照型URLフィルター」の機能が搭載されています。
内部データベース参照型URLフィルターは、URLの全部または一部をキーワードとして登録し、そのキーワードと一致した文字列を含むURLへのアクセスを制限することができます。また、フィルター設定時に送信元IPアドレスを指定することで、特定のホストまたはネットワークからの接続を制限することもできます。また、本製品をプロキシサーバーとして動作させることでHTTPSによるWebアクセスを制限することができます。
外部データベース参照型URLフィルターは、外部のURLフィルタリングサービス事業者のデータベースに問い合わせて、アクセスを制限することもできます。これにより、組織内のネットワーク利用者のWeb閲覧を簡単かつ的確に制限することができます。

ポリシーベースのフィルタリング設定

セキュリティーの設定は、階層的にポリシーを記述でき、設定意図もわかりやすく管理も容易にできます。おおまかなルールを決めて次第に詳細化することができます。

ファイル共有ソフトウェアの利用把握や制限が可能

ファイル共有ソフトウェア「Winny」「Share」による通信の検出/遮断に対応しています。ファイアウォール機能の不正アクセス検知機能を有効にすることで、「Winny」「Share」が利用するパケットを検出するとともに、該当パケットを破棄し、通信を遮断します。また、「Winny」「Share」のパケットを検出した場合、不正アクセス検知の履歴に記録するため、「Winny」「Share」を使用した端末の特定にも有効です。

ギガビットイーサ、3G/LTEモバイル通信に対応

FTTHやCATV、ADSLなどのブロードバンド回線用モデムに接続できるWAN接続用のポートを装備しています。また、USBポートに3G/LTEモバイル網に対応したデータ通信端末を接続して、モバイルインターネットを利用することもできます。

IPsec、L2TP/IPsecによる仮想プライベートネットワーク

本製品はIPsec、L2TP/IPsecに対応しているため、インターネット（ブロードバンド）回線を利用した仮想プライベートネットワーク（VPN）を構築する場合でも、より安全にデータをやりとりできます。

データコネクトに対応

フレッツ 光ネクストの「データコネクト」に対応しています。データコネクトを利用して、帯域が保証された通信で拠点間接続することができます。

かんたん操作

- 本製品は設定のための「かんたん設定ページ」を内蔵していますので、パソコンのWebブラウザを使って本製品の基本的な設定を変更できます。
- DOWNLOADボタンを押すだけで、内蔵ファームウェアをリビジョンアップ（バージョンアップ）できます。ご購入後に新しい機能が追加されても、リビジョンアップすることで最新の機能が利用できます。ファームウェアは本体に直接ダウンロードする以外に、パソコンからの転送やUSBメモリまたはmicroSDカードに保存したファームウェアを使用することもできます。

さまざまな外部メモリに対応

本製品の設定ファイルやログを、市販のUSBメモリ/microSDカードに保存できます。また、USBメモリ/microSDカードに保存したファームウェアや設定ファイルで、本製品を起動することもできます。

ヤマハスイッチの設定・管理が可能

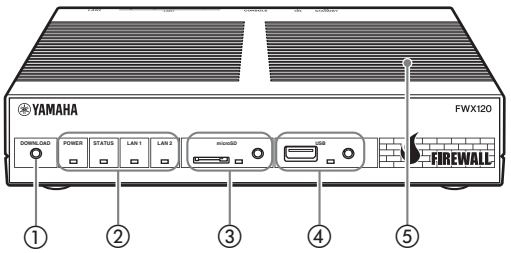
本製品はヤマハスイッチと連携して、ネットワーク構成やポート状態を「かんたん設定ページ」で表示することができます。また、ヤマハスイッチの各ポートの個別設定や、本製品とヤマハスイッチ双方を含むVLAN設定も一括で行うことができます。

充実のヤマハネットワーク周辺機器ホームページ

ヤマハネットワーク周辺機器ホームページ（http://jp.yamaha.com/products/network/、http://www.rtpro.yamaha.co.jp/）で、ヤマハファイアウォールを使用した高度な活用例や詳しい解説をご覧いただけます。

各部の名称とはたらき

前面／上面



① DOWNLOADボタン

DOWNLOADボタンによるリビジョンアップを許可するように設定している場合は、このボタンを3秒間押し続けるとファームウェアのリビジョンアップを開始します。詳しくは、「最新の機能を利用する（リビジョンアップ）」（189ページ）をご覧ください。

② ランプ

本製品の動作状態を示します。ランプの点灯状態と本製品の動作の関係については、「前面ランプの点灯状態」（19ページ）をご覧ください。

- **POWER**：本製品の電源の状態を示します。
- **STATUS**：接続先の機器との通信状態を示します。
- **LAN1**：LAN1 ポートの使用状態を示します。
- **LAN2**：LAN2 ポートの使用状態を示します。

③ microSDランプ、ボタン、スロット

市販のmicroSDカードを使用して、設定ファイルのコピー（181、195ページ）やログの保存（194ページ）、リビジョンアップ（191ページ）を実行できます。

microSDカードを取り外す際は、microSDボタンを2秒間押し続けて接続を解除してから、microSDカードを取り外してください。

ご注意

挿入されているmicroSDカードを取り出して再度挿入する場合は、microSDカード全体を取り出してから、挿入してください。

④ USBランプ、ボタン、ポート

市販のUSBメモリを接続して、設定ファイルのコピー（181、195ページ）やログの保存（194ページ）、リビジョンアップ（191ページ）を実行できます。また、USB接続のデータ通信端末を接続して、3G/LTEモバイル網を利用した通信を行うこともできます（73ページ）。

USBデバイスを取り外す際は、USBボタンを2秒間押し続けて接続を解除してから、USBデバイスを取り外してください。

ご注意

USBメモリとUSBデータ通信端末以外のUSBデバイスは接続しないでください。本製品が故障する可能性があります。

⑤ 通風口

内部の熱を逃がすための穴です。

前面ランプの点灯状態（◉点灯 ◌ 点滅 ◎消灯）

POWERランプ

◉ 電源が入っています。

◌ 電源スイッチをONにした直後の起動中、または電源スイッチをSTANDBYにした直後のシャットダウン動作中です。

◎ 電源が切れているか、または停電しています。

STATUSランプ

◉ 通信が不可能な状態になっています。
「STATUSランプが点灯しているときは」(188ページ)をご覧ください。

◎ 通信が可能な状態です。

LAN1 ランプ

◉ LAN1 が使用可能な状態です。

◌ LAN1 にデータが流れています。

◎ LAN1 が使用不可能な状態です。

LAN2ランプ

◉ LAN2が使用可能な状態です。

◌ LAN2にデータが流れています。

◎ LAN2が使用不可能な状態です。

microSDランプ

◉ microSDカードがmicroSDスロットに挿さっていますが、アクセスしていません。

◌ microSDカードにアクセスしています。

◎ microSDカードがmicroSDスロットに挿し込まれていません。または、スロットに挿し込まれているmicroSDカードを取り外すことができる状態です。

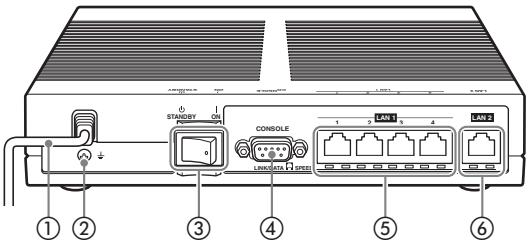
USBランプ

◉ USBデバイスがUSBポートに挿さっていますが、アクセスしていません。

◌ USBデバイスにアクセスしています。

◎ USBデバイスがUSBポートに挿し込まれていません。または、ポートに挿し込まれているUSBデバイスを取り外すことができる状態です。

背面



① 電源コード

② アース端子
アースコードを接続します。

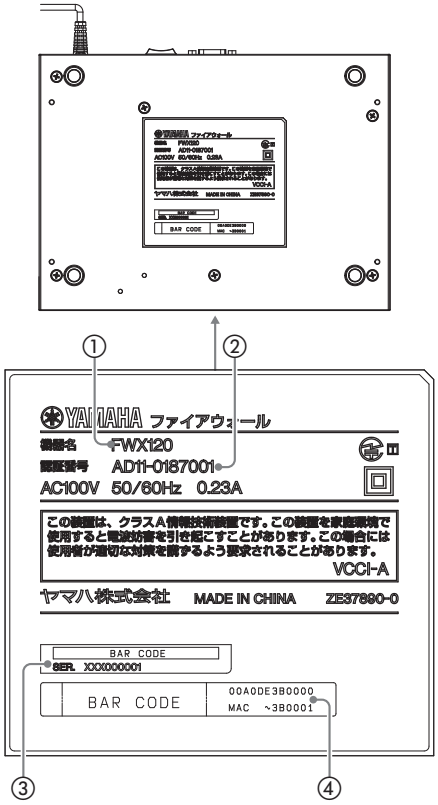
③ POWERスイッチ
本製品の電源のON/STANDBYを切り替えます。

④ CONSOLEポート
コンソールからの設定を行う場合に、パソコンのRS-232C端子（シリアルコネクタ）と接続します。詳しくは、「CONSOLEポートから設定する」（179ページ）をご覧ください。

⑤ LAN1ポート
パソコンのLANポートまたはハブのポートとLANケーブルで接続します。
各LAN1ポートの下部には、LINK/DATAランプ（左側）とSPEEDランプ（右側）があります。
- **LINK/DATAランプ**：リンク状態によって、消灯（リンク喪失）または点灯（リンク確立）、点滅（データ転送中）します。
- **SPEEDランプ**：接続速度によって、消灯（100BASE-TX/10BASE-T）または点灯（1000BASE-T）します。

⑥ LAN2ポート
ファイアウォールとして既存ネットワークに接続する場合は、ルーター、ハブとLANケーブルで接続します。WAN回線と接続する場合は、ケーブルモデムやADSLモデム、ONUとLANケーブルで接続します。
LAN2ポートの下部には、LINK/DATAランプ（左側）とSPEEDランプ（右側）があります。
動作については、LAN1ポートのランプと同様です。

底面



① 機器名
本製品の機器名が記載されています。

② 認証番号
本製品の認証番号が記載されています。

③ シリアル番号
製品を管理／区分するための製造番号が記載されています。

④ MACアドレス
LAN1側とLAN2側それぞれに付与されている機器固有のネットワーク識別番号が記載されています。「00A0DE3B0000」、「MAC ～3B0001」という上図の例の場合、LAN1側とLAN2側それぞれのMACアドレスは以下のようになります。
- **LAN1側MACアドレス**：00A0DE3B0000
- **LAN2側MACアドレス**：00A0DE3B0001

準備の流れ

本製品を透過型ファイアウォールとして利用するには、以下の順序で準備を行う必要があります。

ネットワーク接続設定に必要な準備を行う

準備1 本製品にパソコンや回線を接続して、電源を入れる ▶23ページ

▼

準備2 「かんたん設定ページ」を開く ▶25ページ

▼

準備3 本製品のパスワードを設定する ▶27ページ

▼

準備4 本製品の日付・時刻を合わせる ▶32ページ

▼

準備5 透過型ファイアウォールを設定する ▶34ページ

準備を始める前にご用意ください

LANケーブル

パソコンの台数や距離に合わせて、LANケーブルをご用意ください。

ハブ

本製品のLAN1ポートには、パソコンを4台まで直接接続できます。5台以上のパソコンを接続したい場合は、10BASE-Tまたは100BASE-TX、1000BASE-T対応のハブ(スイッチングハブなど)をご用意ください。

本製品を設置するネットワークの情報

本製品のLAN側に設定するIPアドレスを、あらかじめ決定しておいてください。

ご注意

DHCPサーバーを使用しているネットワークに本製品を接続するときは、本製品のDHCPサーバー機能を動作しないようにする必要があります。
本製品のDHCPサーバー機能を動作しないようにする場合は、36ページをご覧ください。

設置作業の際の注意事項

本製品の設置を行うときは6ページからの「安全上のご注意」をよくお読みになり必ず守ってください。

本製品を19インチラックに設置する場合は、別売のラックマウントキットYMO-RACK1Uをご使用ください。

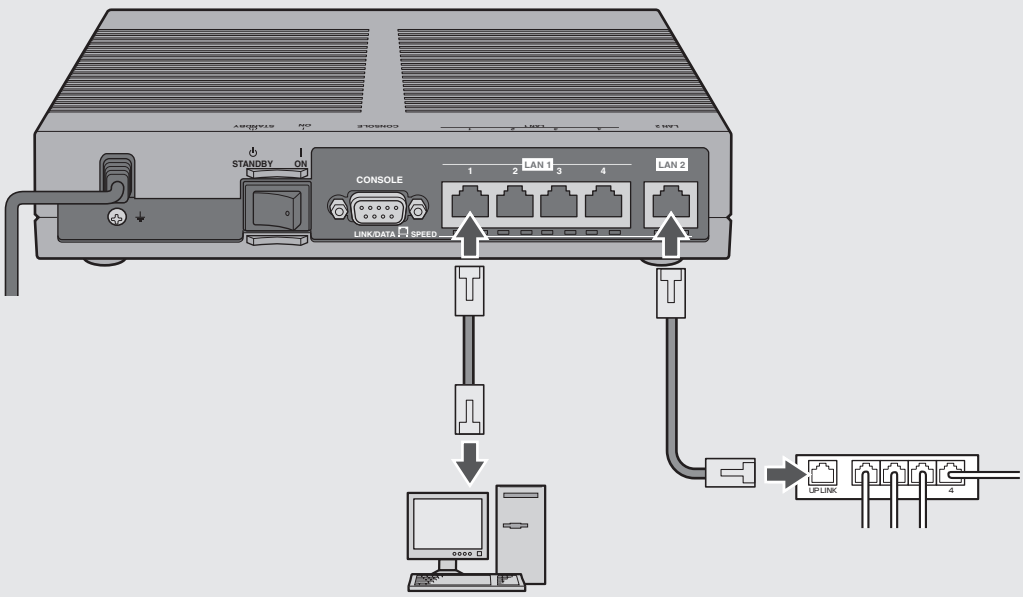
本製品を壁に取り付ける場合には、別売のウォールマウントキットYWK-1200Bをご使用ください。

準備 1

接続する

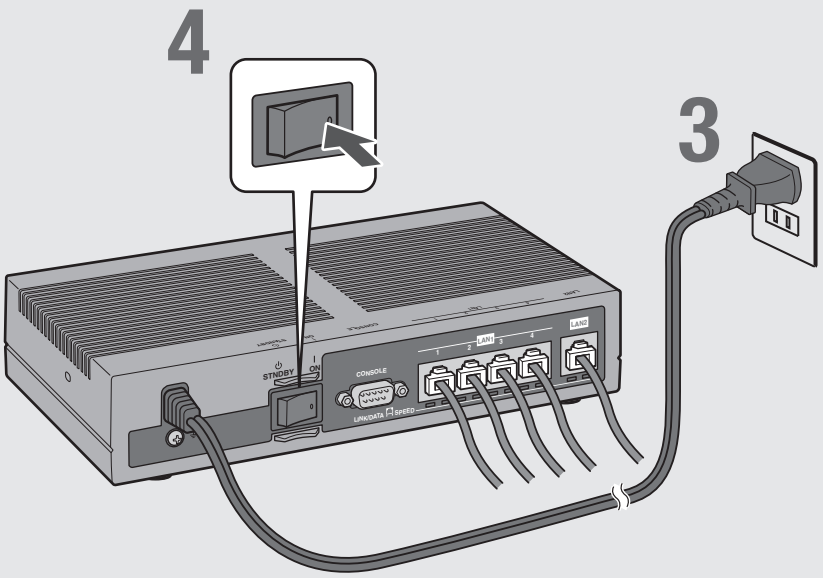
ヒント

- 本製品をルーターとして利用する場合は「ルーターとしてインターネットに接続する」(40ページ)をご覧ください。
- アースコードを接続することで静電気対策やノイズ防止に効果があります。アースコードを接続して使用する場合は「アースコードを接続する」(227ページ)をご覧ください。



1 パソコンのLANポートと本製品のLAN1ポートを、LANケーブルで接続する。

2 ルーターやハブのLANポートと本製品のLAN2ポートを、LANケーブルで接続する。



3 本製品の電源コードをコンセントに接続する。

4 本製品のPOWER（電源）スイッチを「ON」にして、電源を入れる。

POWERランプが何回か点滅した後に点灯します。

5 パソコンやハブの電源を入れる。

本製品のLAN1ランプとLAN2ランプが点灯または点滅すれば正常です。

LAN1ランプが点灯または点滅しない場合は

- LANケーブルが正しく接続されているか、パソコンやハブの電源が入っているかを確認してください。
- 本製品に接続したすべてのパソコンおよびハブの電源が入っていないときは、LAN1ランプは点灯または点滅しません。

LAN2ランプが点灯または点滅しない場合は

本製品とルーター（ハブ）が正しく接続されているか、ルーター（ハブ）の電源が入っているかを確認してください。

これで本製品の接続操作は終了しました。
引き続き、他の準備を行ってください。

▶25ページをご覧ください。

準備 2

「かんたん設定ページ」を開く

本製品の設定の変更は、本製品に接続したパソコンのWebブラウザから本製品の「かんたん設定ページ」を開いて行います。

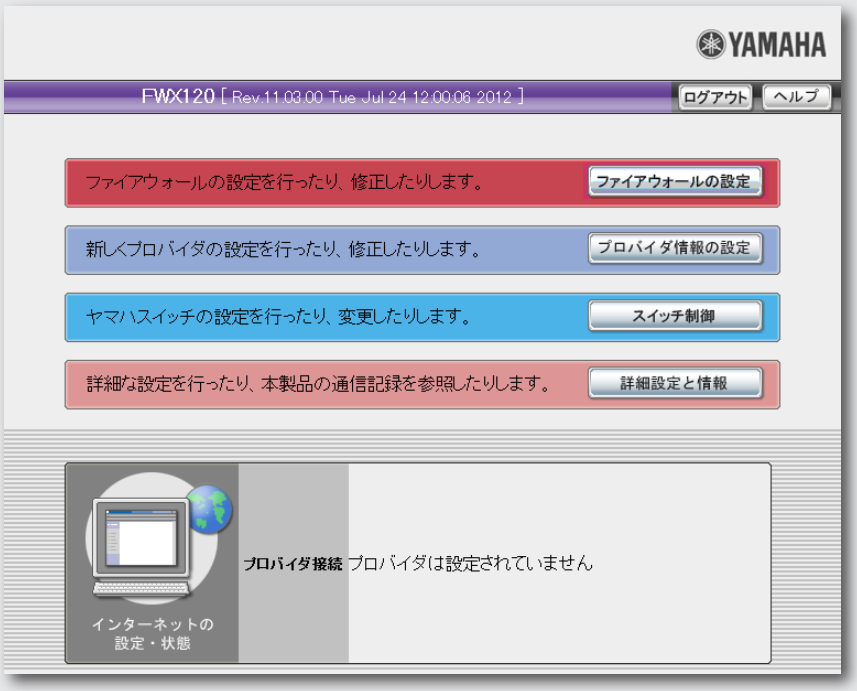
「かんたん設定ページ」を開くには、以下の手順で操作します。

ご注意

- 「かんたん設定ページ」を使用するには、Windows 版 Internet Explorer 8 以降の Web ブラウザが必要です。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。

ヒント

TELNETソフトウェアでコンソール画面からコマンドを入力して、「かんたん設定ページ」よりも詳細な設定を行うことができます(コンソールコマンド)。TELNETソフトウェアで本製品に接続する方法については177ページ、本製品で使用できるコマンドについては「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。



1 本製品の電源が入っていることを確認する。

2 パソコンでInternet Explorerを起動する。

3 アドレスバーに「http://192.168.100.1/」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。

ご注意

LAN1 ポートのIPアドレスを変更してある場合は、アドレスバーには設定されているIPアドレスを入力してください。

4 「パスワード」欄に半角英字で「doremi」と入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページが表示されます。

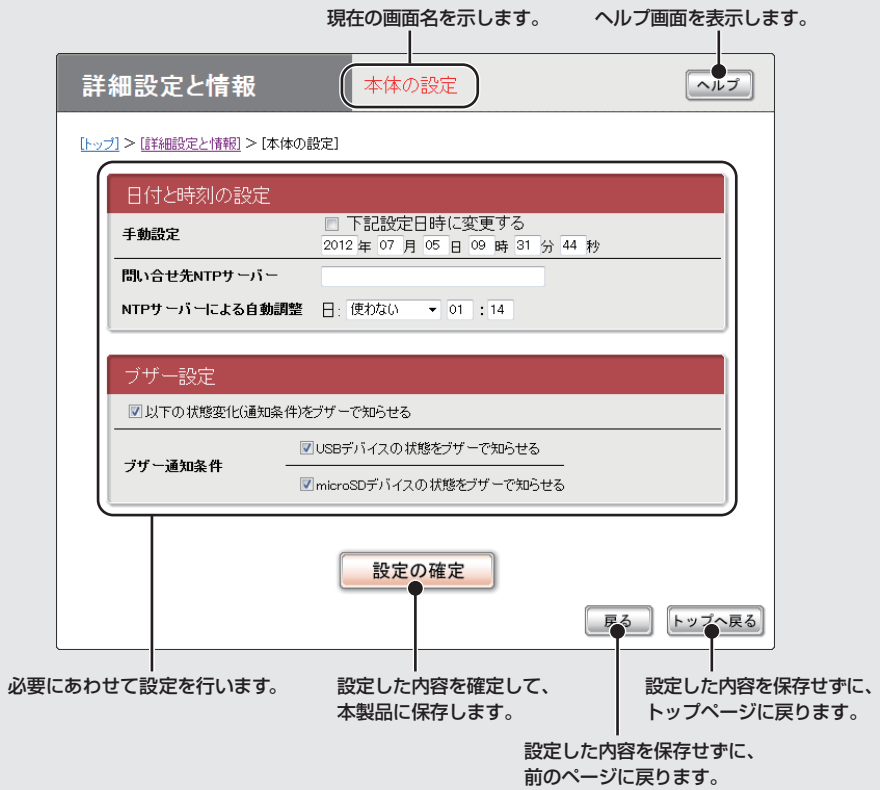
ご注意

ユーザーやパスワードを設定した場合は、設定したユーザー名とパスワードを入力してください。

「かんたん設定ページ」のトップページが表示されないときは

「『かんたん設定ページ』で設定できない」(203ページ)をご覧ください。

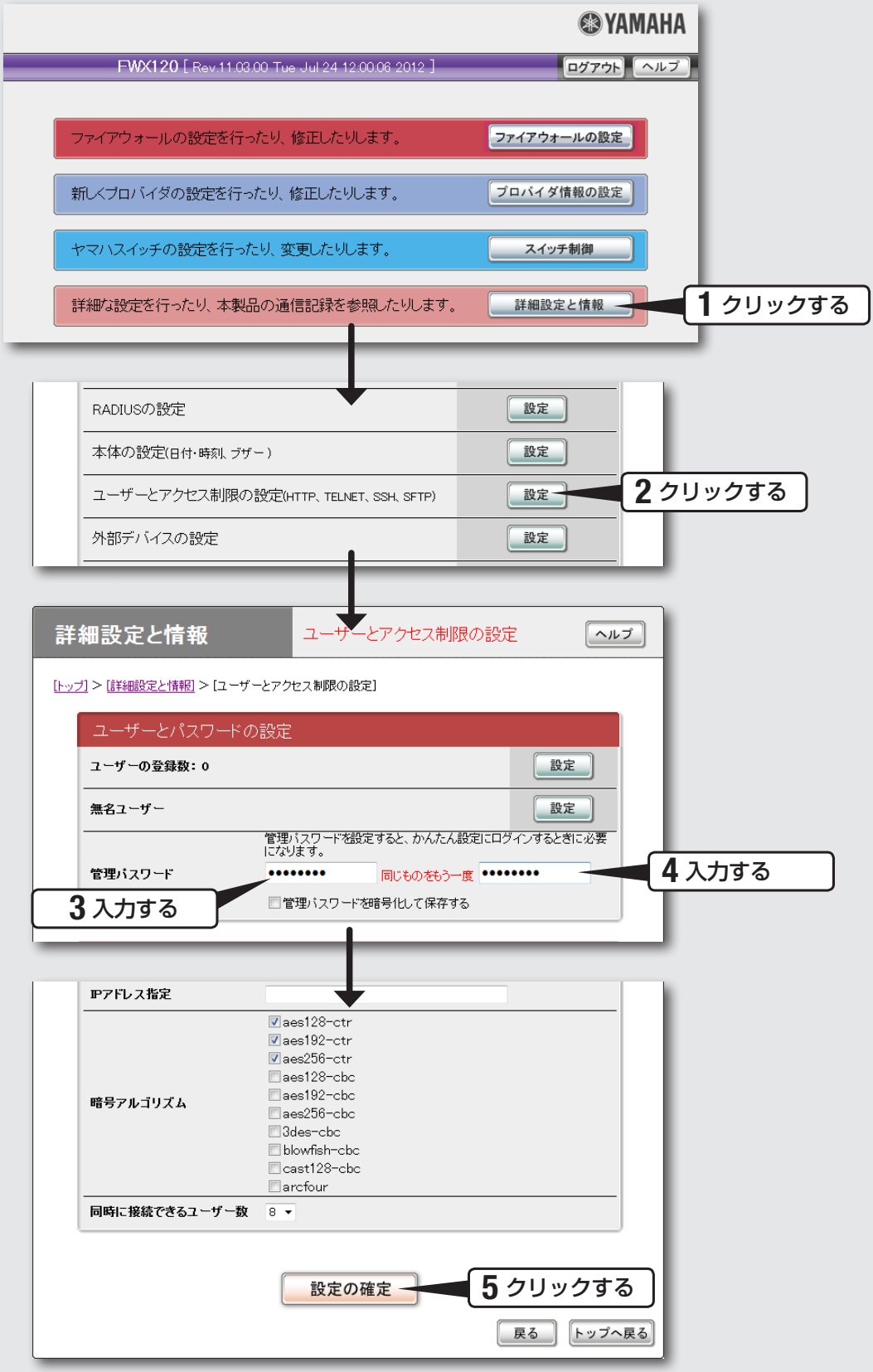
「かんたん設定ページ」の見かた



準備 3

パスワードを設定する

工場出荷時は、初期パスワードとして「doremi」が設定されています。
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。パスワードを設定すると、本製品にアクセスする際にパスワード入力が必要となるので、第三者が本製品の設定を変更することが困難になります。
セキュリティーの問題を防ぐためにも、28ページの手順に従ってパスワードを登録／変更することをおすすめいたします。


YAMAHA
FWX120 [Rev.11.03.00 Tue Jul 24 12:00:06 2012]
ログアウト
ヘルプ
ファイアウォールの設定を行ったり、修正したりします。
ファイアウォールの設定
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
ヤマハスイッチの設定を行ったり、変更したりします。
スイッチ制御
詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
1 クリックする
RADIUSの設定
設定
本体の設定(日付・時刻、ブザー)
設定
ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)
設定
2 クリックする
外部デバイスの設定
設定
詳細設定と情報
ユーザーとアクセス制限の設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定]
ユーザーとパスワードの設定
ユーザーの登録数: 0
設定
無名ユーザー
設定
管理パスワードを設定すると、かんたん設定にログインするときに必要になります。
管理パスワード
同じものをもう一度
4 入力する
3 入力する
管理パスワードを暗号化して保存する
IPアドレス指定
暗号アルゴリズム
aes128-ctr
aes192-ctr
aes256-ctr
aes128-cbc
aes192-cbc
aes256-cbc
3des-cbc
blowfish-cbc
cast128-cbc
arcfour
同時に接続できるユーザー数
8
設定の確定
5 クリックする
戻る
トップへ戻る

1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」をクリックする。

「ユーザーとアクセス制限の設定」画面が表示されます。

3 「管理パスワード」欄に本製品のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

4 手順3で入力した本製品のパスワードを再度入力する。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「設定の確定」をクリックする。

設定したパスワードが有効になります。

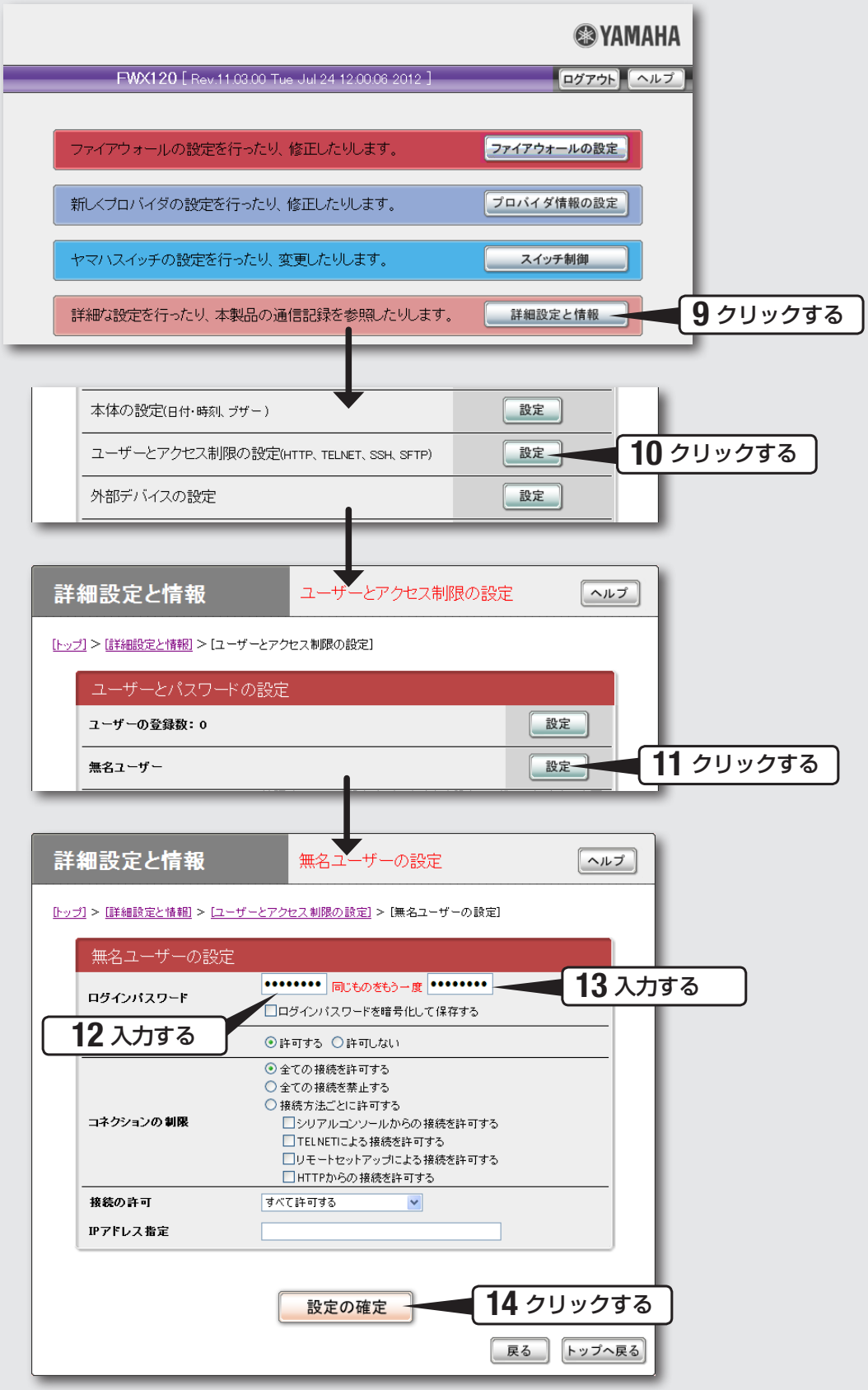
7 「トップへ戻る」をクリックする。

「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。

8 手順3で入力した本製品のパスワードを「パスワード」欄に入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページに戻ります。
引き続き、本製品のログインパスワードを設定します。

ヒント
「ユーザー名」欄には、何も入力する必要はありません。


YAMAHA
FWX120 [Rev.11.03.00 Tue Jul 24 12:00:06 2012]
ログアウト
ヘルプ
ファイアウォールの設定を行ったり、修正したりします。
ファイアウォールの設定
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
ヤマハスイッチの設定を行ったり、変更したりします。
スイッチ制御
詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
9 クリックする
本体の設定(日付・時刻、ブザー)
設定
ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)
設定
10 クリックする
外部デバイスの設定
設定
詳細設定と情報
ユーザーとアクセス制限の設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定]
ユーザーとパスワードの設定
ユーザーの登録数: 0
設定
無名ユーザー
設定
11 クリックする
詳細設定と情報
無名ユーザーの設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定] > [無名ユーザーの設定]
無名ユーザーの設定
ログインパスワード
同じものをもう一度
13 入力する
ログインパスワードを暗号化して保存する
12 入力する
許可する
許可しない
コネクションの制限
全ての接続を許可する
全ての接続を禁止する
接続方法ごとに許可する
シリアルコンソールからの接続を許可する
TELNETによる接続を許可する
リモートセットアップによる接続を許可する
HTTPからの接続を許可する
接続の許可
すべて許可する
IPアドレス指定
設定の確定
14 クリックする
戻る
トップへ戻る

9 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

10 「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」をクリックする。

「ユーザーとアクセス制限の設定」画面が表示されます。

11 「無名ユーザー」欄の「設定」をクリックする。

「無名ユーザーの設定」画面が表示されます。

12 「ログインパスワード」欄に、ログイン用のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

13 手順11で入力したログイン用パスワードを再度入力する。

14 「設定の確定」をクリックする。

確認画面が表示されます。

15 「設定の確定」をクリックする。

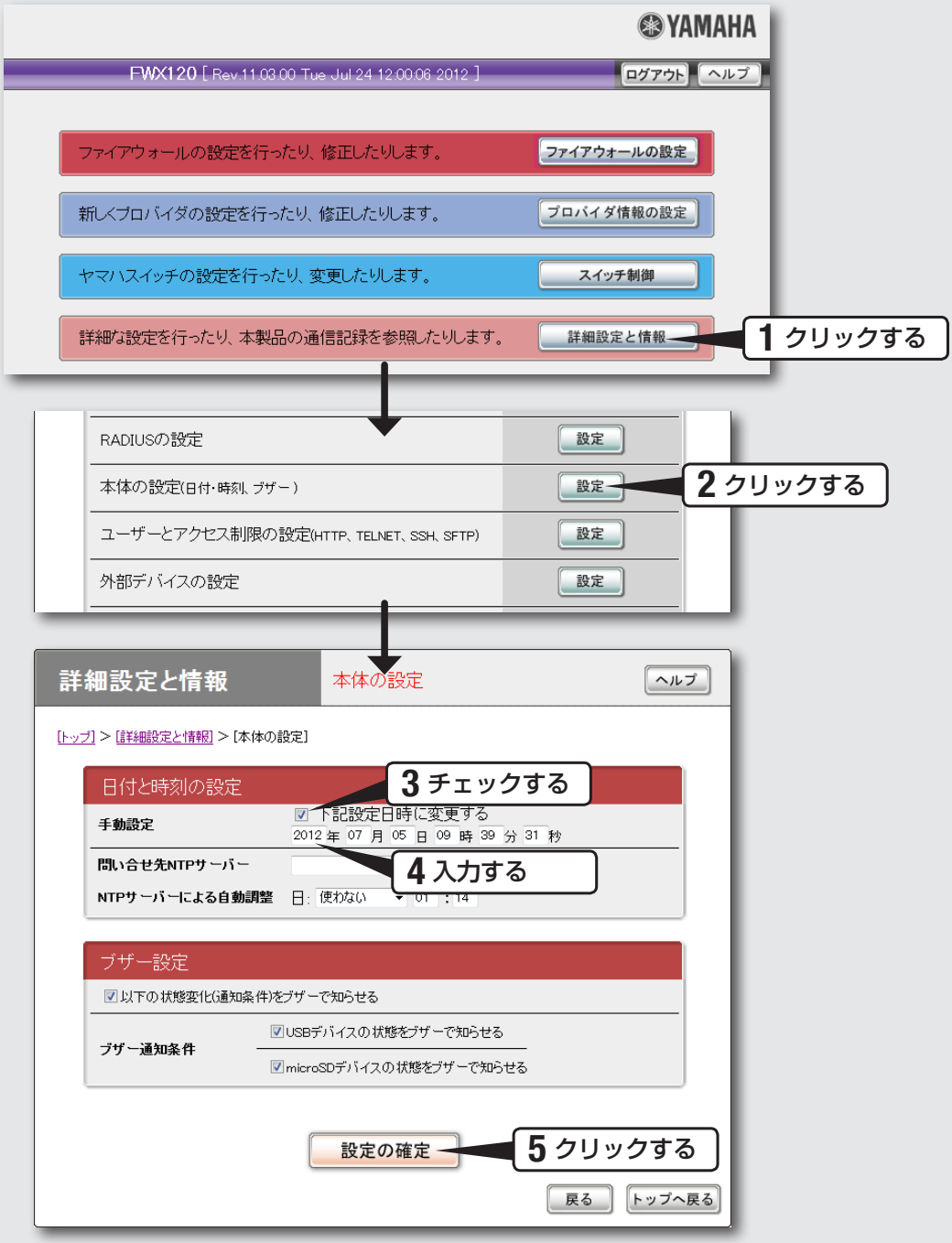
設定したパスワードが有効になります。

16 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

日付・時刻を合わせる

「本体の設定」画面で、本製品の日付と時刻を合わせます。



1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「本体の設定(日付・時刻、ブザー)」の「設定」をクリックする。

「本体の設定」画面が表示されます。

3 「日付と時刻の設定」欄の、「下記設定日時に変更する」にチェックを付ける。

4 日付と時刻を入力する。

ヒント
あらかじめ少し先の時刻を入力しておき、時報と同時に「設定の確定」をクリックするとより正確に時刻合わせできます。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

本製品の時刻を自動的に合わせたいときは

インターネット上のNTPサーバー(時刻配信サーバー)を利用して、本製品の時刻を自動的に合わせることができます。

ご注意
本製品のセキュリティー設定によっては、本製品だけでなくLAN内のパソコンからもNTPサーバーを利用して時刻を合わせられない場合があります。外部のNTPサーバーを利用する場合は、フィルターの設定を変更してください(99ページ)。

透過型ファイアウォールを設定する

本製品の「かんたん設定ページ」でIPアドレスを設定して、既存のネットワークに接続します。

本製品をルーターとして利用する場合は、「ルーターとしてインターネットに接続する」(40ページ)をご覧ください。

設定する前に

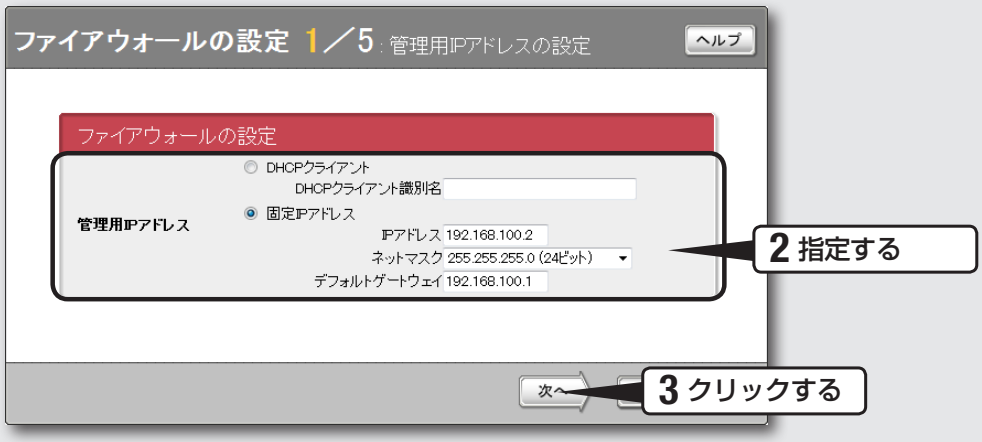
ご注意

- 本書ではInternet Explorer 8の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。
- 透過型ファイアウォールを設定すると設定できなくなる項目があります。詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

既存のネットワークに接続するには、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)。

- IPアドレス
- ネットマスク
- ネームサーバーアドレス(DNSサーバーアドレス、ネームサーバー IPアドレス、DNSサーバー IPアドレス)
- デフォルトゲートウェイアドレス

1　管理用IPアドレスを指定する



1　「かんたん設定ページ」のトップページで、「ファイアウォールの設定」をクリックする。

「ファイアウォールの設定１／５」画面が表示されます。

2　管理用IPアドレスを指定する。

DHCPサーバーからIPアドレスを取得する場合

「DHCPクライアント」をクリックして選びます。

DHCPクライアント識別名を指定されている場合は、「DHCPクライアント識別名」欄に指定された識別名を入力します（指定されていない場合は、入力する必要はありません）。

IPアドレスを固定する場合

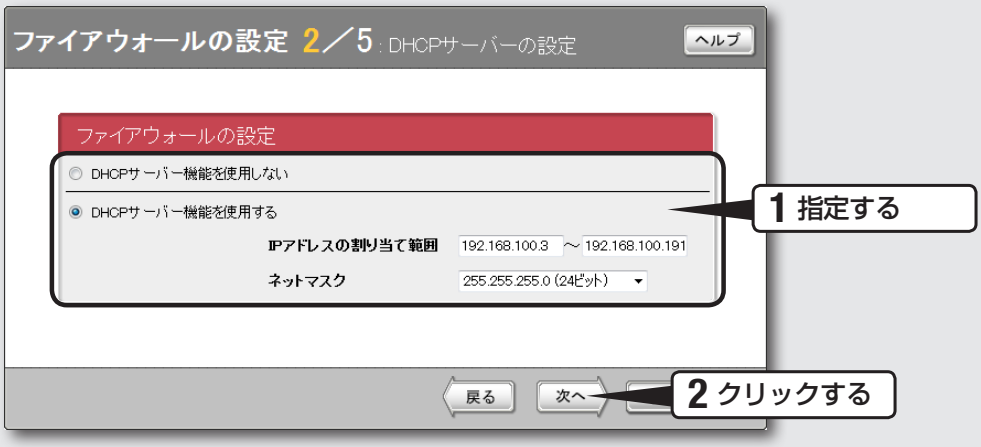
「固定IPアドレス」をクリックして選んでから、以下の設定を行います。

- **IPアドレス**：IPアドレスを半角数字で入力します。
- **ネットマスク**：ネットマスクを選びます。
- **デフォルトゲートウェイ**：デフォルトゲートウェイアドレスを半角数字で入力します。

3　「次へ」をクリックする。

「ファイアウォールの設定２／５」画面が表示されます。

2　DHCPサーバー機能を指定する



1　DHCPサーバー機能を指定する。

ご注意

「ファイアウォールの設定１／５」画面で「DHCPクライアント」を選んだ場合は「DHCPサーバー機能を使用しない」が選ばれます。

本製品をDHCPサーバーとして使用しない場合

「DHCPサーバー機能を使用しない」をクリックして選びます。

本製品をDHCPサーバーとして使用する場合

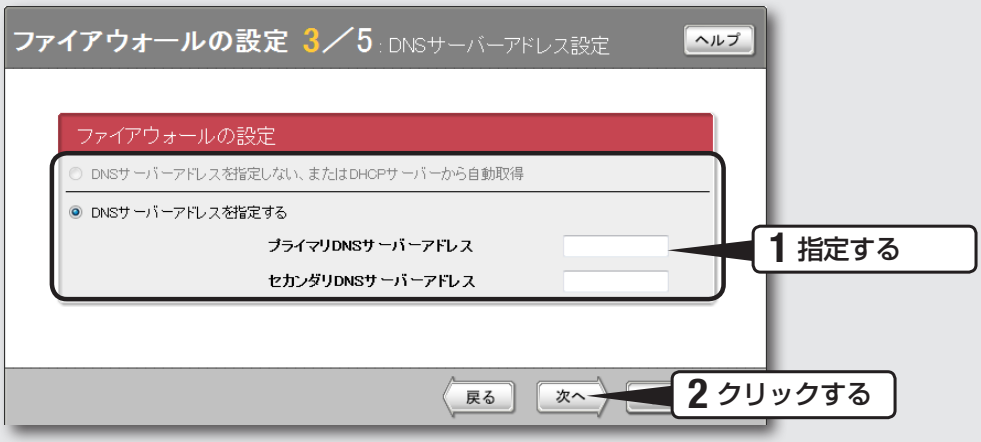
「DHCPサーバー機能を使用する」をクリックして選んでから、以下の設定を行います。

- IPアドレスの割り当て範囲：本製品のIPアドレスとは重複しないように、割り当てるIPアドレスの範囲を半角数字で入力します。
- ネットマスク：本製品のネットマスクと同じ値を選びます。

2　「次へ」をクリックする。

「ファイアウォールの設定３／５」画面が表示されます。

3　DNSサーバーアドレスを指定する



1　DNSサーバーアドレスを指定する。

ご注意

「ファイアウォールの設定2 ／ 5」画面で「DHCPサーバー機能を使用する」を選んだ場合は「DNSサーバーアドレスを指定しない、またはDHCPサーバーから自動取得」を選択することはできません。

DNSサーバーアドレスが指定されていない場合

「DNSサーバーアドレスを指定しない、またはDHCPサーバーから自動取得」をクリックして選びます。

DNSサーバーアドレスが指定されている場合

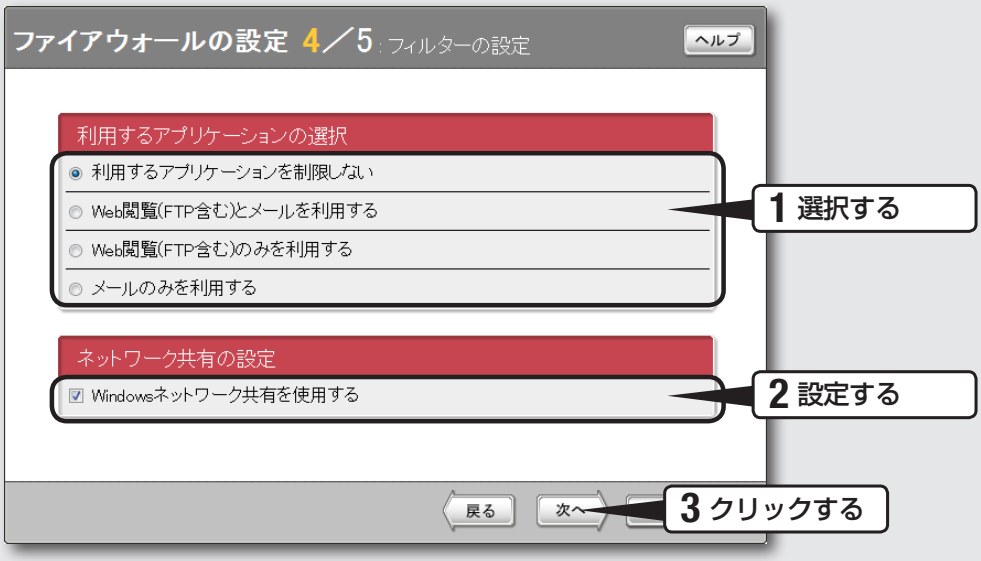
「DNSサーバーアドレスを指定する」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス**：DNSサーバーアドレスを半角数字で入力します。
- **セカンダリDNSサーバーアドレス**：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）。

2　「次へ」をクリックする。

「ファイアウォールの設定4 ／ 5」画面が表示されます。

4　フィルター機能を指定する



1　利用するアプリケーションを選択する。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

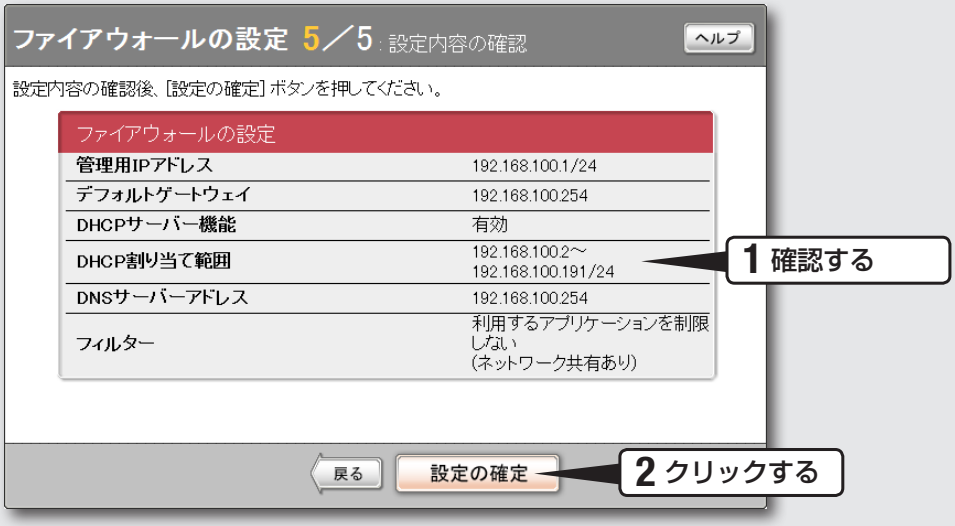
2　ネットワーク共有を設定する。

Windowsのネットワーク共有機能を使用しない場合は、「Windowsネットワーク共有を使用する」のチェックを外してください。

3　「次へ」をクリックする。

「ファイアウォールの設定5 ／ 5」画面が表示されます。

5　設定内容を確認する



1　表示された設定内容に問題がないかを確認する。

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2　「設定の確定」をクリックする。

表示された確認画面で「トップへ戻る」をクリックすると、本製品は自動的に既存のネットワークに接続して「かんたん設定ページ」のトップページに戻ります。

ご注意

「1 管理用IPアドレスを指定する」で管理IPアドレスを指定したり、管理IPアドレスの設定を変更した場合には、本製品は自動で再起動します。
再起動した後はInternet Explorerのアドレスバーに指定したIPアドレスまたは変更したIPアドレスを入力してかんたん設定ページを開き直してください。

3　既存のネットワークに接続しているかを確認する。

画面下部の表示を見て、本製品が既存のネットワークに接続していることを確認してください。

▼

設定終了

これで既存のネットワークへの接続設定は終了です

►インターネットに接続できない場合は

Check 1　本製品とルーターやハブの接続を確認してください。
Check 2　35 ～ 38ページの設定内容をもう一度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」(200ページ)を参考にして、問題を解決してください。

準備の流れ

本製品をルーターとして利用するには、以下の順序で準備を行う必要があります。

ネットワーク接続設定に必要な準備を行う

準備1	本製品にパソコンや回線を接続して、電源を入れる	▶42ページ
準備2	「かんたん設定ページ」を開く	▶44ページ
準備3	本製品のパスワードを設定する	▶46ページ
準備4	本製品の日付・時刻を合わせる	▶51ページ
準備5	本製品のLAN1側IPアドレスを設定する	▶53ページ
準備6	LAN内のパソコンのIPアドレスを変更する	▶55ページ
準備7	プロバイダ情報を設定する	▶56ページ

準備を始める前にご用意ください

LANケーブル

パソコンの台数や距離に合わせて、LANケーブルをご用意ください。

ハブ

本製品のLAN1ポートには、パソコンを4台まで直接接続できます。5台以上のパソコンを接続したい場合は、10BASE-Tまたは100BASE-TX、1000BASE-T対応のハブ(スイッチングハブなど)をご用意ください。

本製品を設置するネットワークの情報

本製品のLAN側に設定するIPアドレスを、あらかじめ決定しておいてください。

ご注意

DHCPサーバーを使用しているネットワークに本製品を接続するときは、本製品のDHCPサーバー機能を動作しないようにする必要があります。本製品のDHCPサーバー機能を動作しないようにする場合は、111ページをご覧ください。

設置作業の際の注意事項

本製品の設置を行うときは6ページからの「安全上のご注意」をよくお読みになり必ず守ってください。

本製品を19インチラックに設置する場合は、別売のラックマウントキットYMO-RACK1Uをご使用ください。

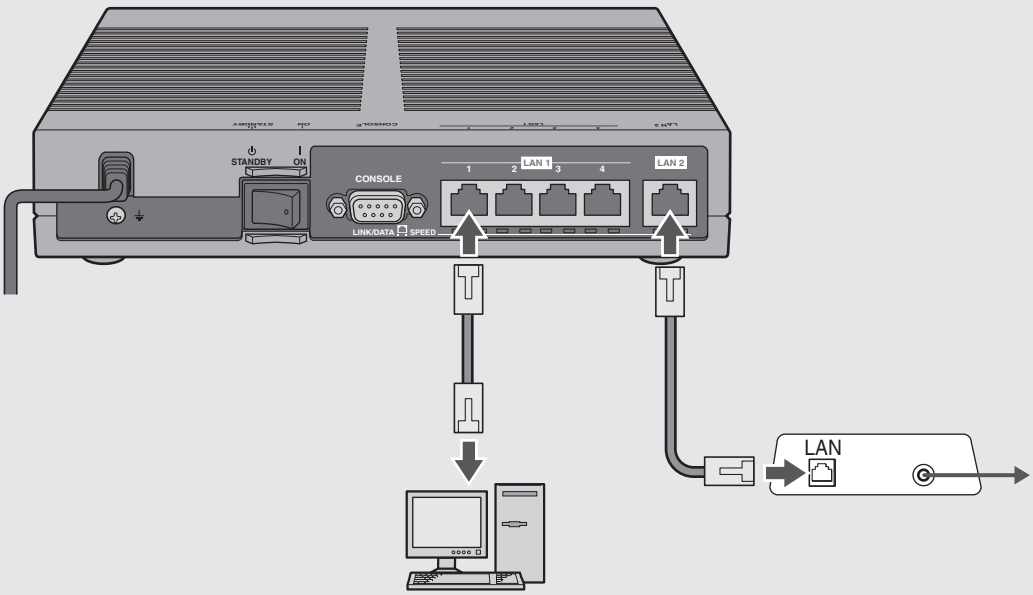
本製品を壁に取り付ける場合には、別売のウォールマウントキットYWK-1200Bをご使用ください。

準備 1

接続する

ヒント

- 本製品をファイアウォールとして利用する場合は「透過型ファイアウォールとして(既存のネットワークに)接続する」(21ページ)をご覧ください。
- USB接続のデータ通信端末でインターネットに接続する場合は「USBデータ通信端末でインターネットへ接続する」(73ページ)をご覧ください。
- アースコードを接続することで静電気対策やノイズ防止に効果があります。アースコードを接続して使用する場合は「アースコードを接続する」(227ページ)をご覧ください。



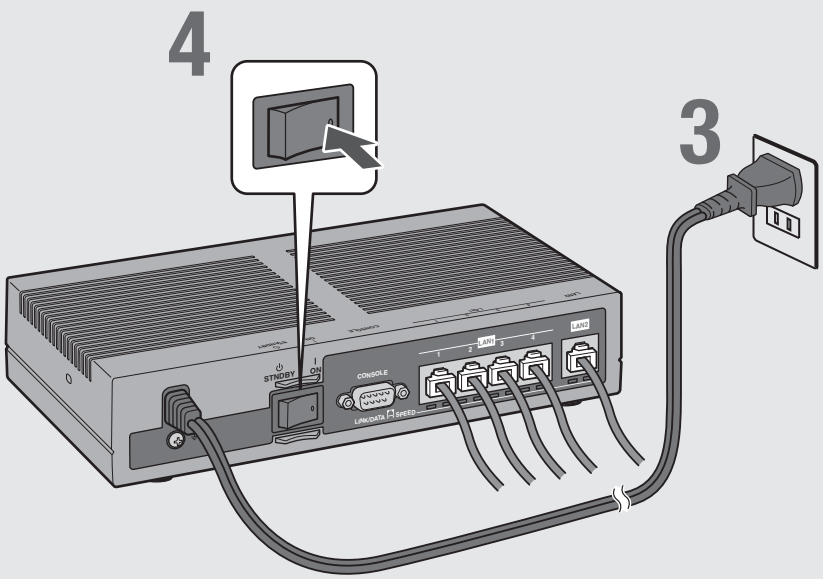
1 パソコンのLANポートと本製品のLAN1ポートを、LANケーブルで接続する。

2 ケーブルモデムやADSLモデム、ONUのLANポートと本製品のLAN2ポートを、LANケーブルで接続する。

プロバイダの資料やADSLモデム、ONUの取扱説明書もあわせてご覧ください。

ご注意

ケーブルモデムやADSLモデム、ONUとパソコンを直接接続している環境を本製品との接続に切り替えたり、設置されていたルーターを本製品に置き換えた場合に、アドレスが取得できないなどの原因で正常接続できないことがあります。そのため、環境の変更後に何らかの設定やリセット操作、指定時間(例:20分以上)待つこと、などが必要となる場合があります。詳しくは、それらの取扱説明書の指示に従ってください。



3 本製品の電源コードをコンセントに接続する。

4 本製品のPOWER（電源）スイッチを「ON」にして、電源を入れる。

POWERランプが何回か点滅した後に点灯します。

5 パソコンやハブの電源を入れる。

本製品のLAN1ランプとLAN2ランプが点灯または点滅すれば正常です。

LAN1ランプが点灯または点滅しない場合は

- LANケーブルが正しく接続されているか、パソコンやハブの電源が入っているかを確認してください。
- 本製品に接続したすべてのパソコンおよびハブの電源が入っていないときは、LAN1ランプは点灯または点滅しません。

LAN2ランプが点灯または点滅しない場合は

本製品とADSLモデム（またはケーブルモデムやONU）が正しく接続されているか、ADSLモデム（またはケーブルモデムやONU）の電源が入っているかを確認してください。

これで本製品の接続操作は終了しました。
引き続き、他の準備を行ってください。

▶44ページをご覧ください。

準備 2

「かんたん設定ページ」を開く

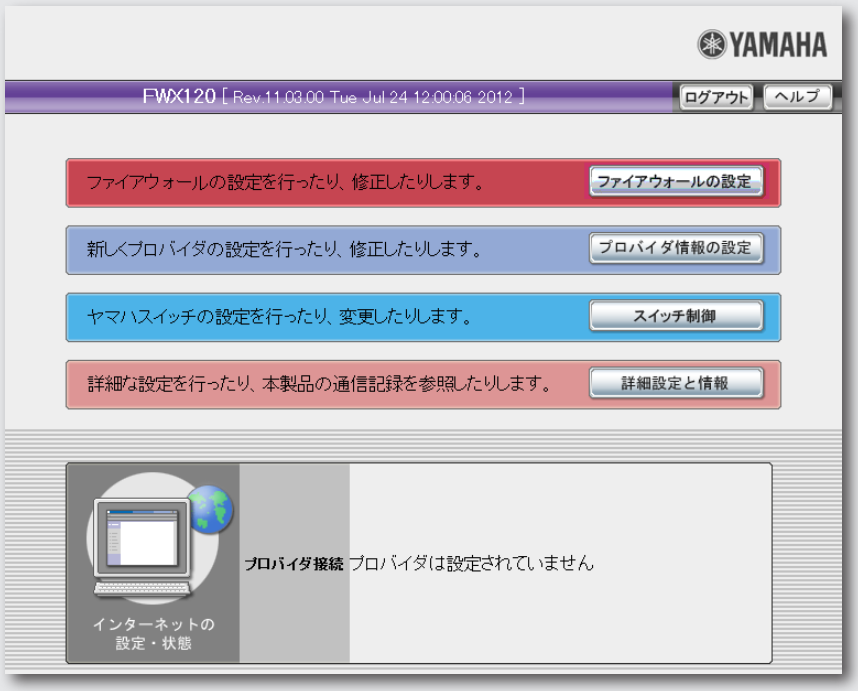
本製品の設定の変更は、本製品に接続したパソコンのWebブラウザから本製品の「かんたん設定ページ」を開いて行います。
「かんたん設定ページ」を開くには、以下の手順で操作します。

ご注意

- 「かんたん設定ページ」を使用するには、Windows 版 Internet Explorer 8 の Web ブラウザが必要です。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。

ヒント

TELNETソフトウェアでコンソール画面からコマンドを入力して、「かんたん設定ページ」よりも詳細な設定を行うことができます（コンソールコマンド）。TELNETソフトウェアで本製品に接続する方法については177ページ、本製品で使用できるコマンドについては「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。



1 本製品の電源が入っていることを確認する。

2 パソコンでInternet Explorerを起動する。

3 アドレスバーに「http://192.168.100.1/」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。

ご注意

LAN1ポートのIPアドレスを変更してある場合は、アドレスバーには設定されているIPアドレスを入力してください。

4 「パスワード」欄に半角英字で「doremi」と入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページが表示されます。

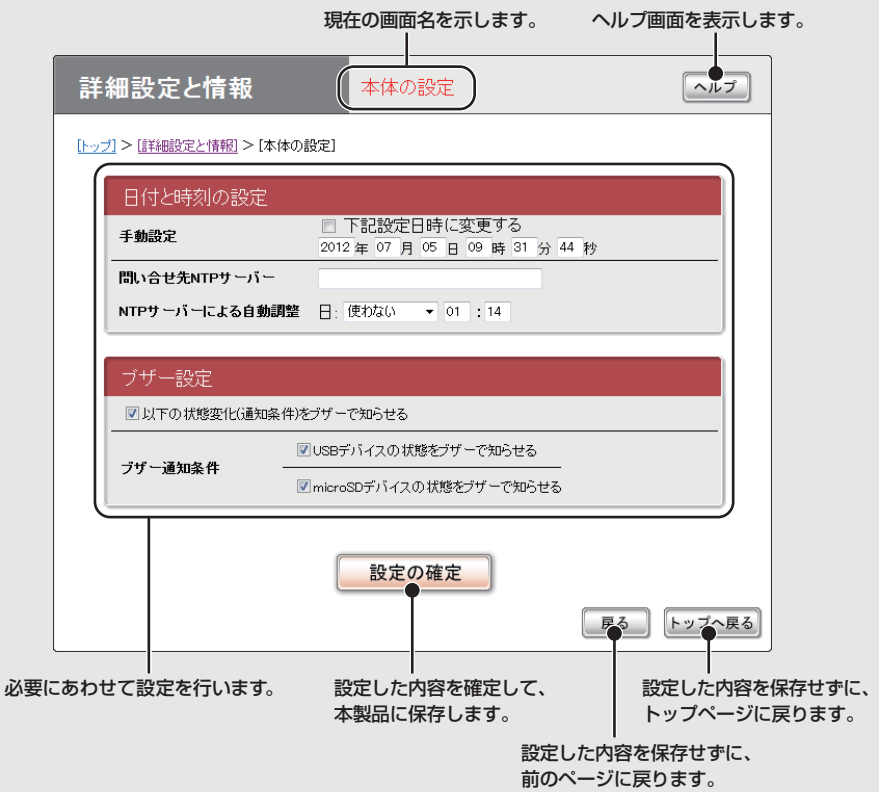
ご注意

ユーザーやパスワードを設定した場合は、設定したユーザー名とパスワードを入力してください。

「かんたん設定ページ」のトップページが表示されないときは

「『かんたん設定ページ』で設定できない」(203ページ)をご覧ください。

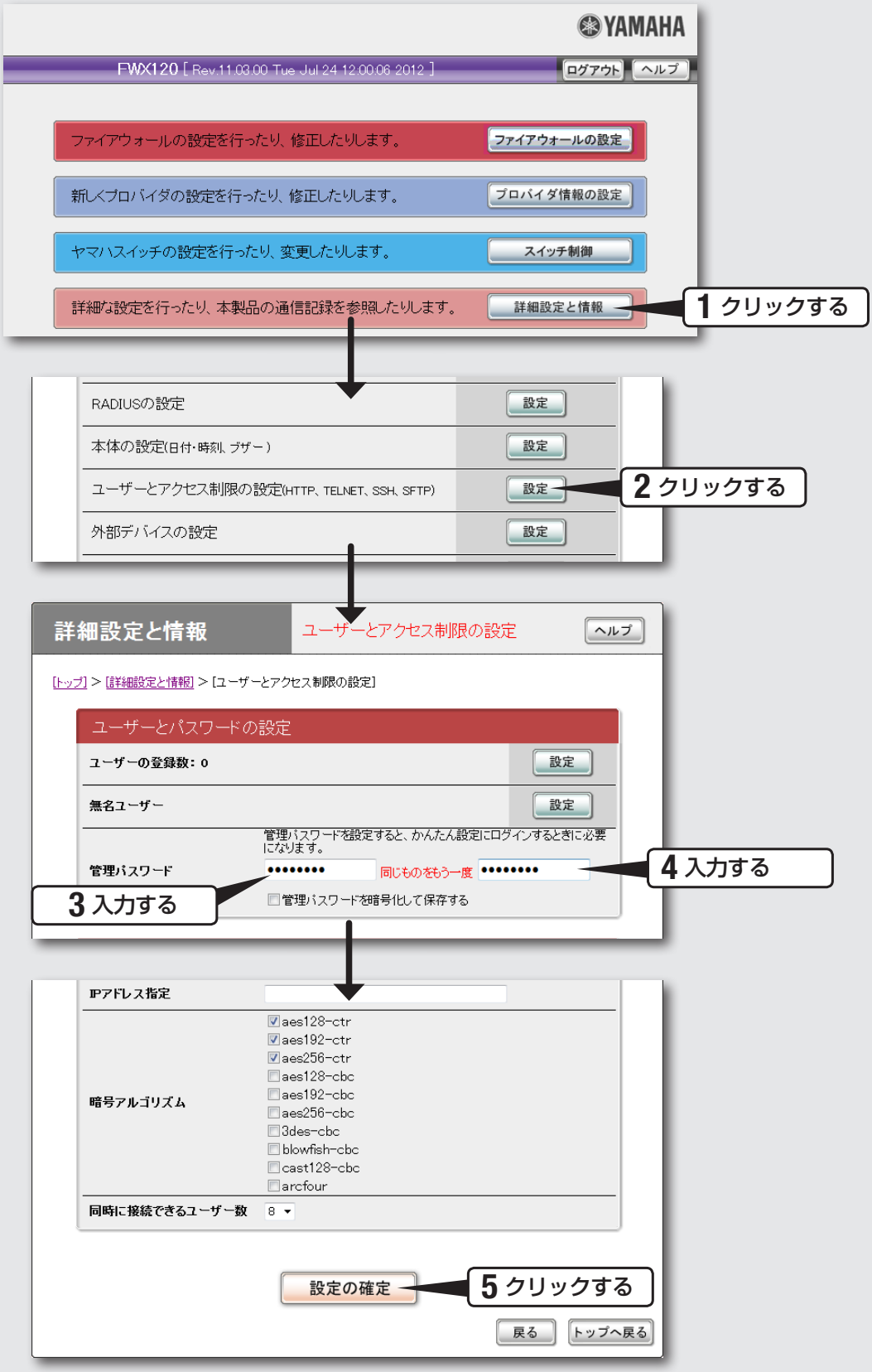
「かんたん設定ページ」の見かた



準備 3

パスワードを設定する

工場出荷時は、初期パスワードとして「doremi」が設定されています。
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。パスワードを設定すると、本製品にアクセスする際にパスワード入力が必要となるので、第三者が本製品の設定を変更することが困難になります。
セキュリティーの問題を防ぐためにも、47ページの手順に従ってパスワードを登録／変更することをおすすめいたします。


YAMAHA
FWX120 [Rev.11.03.00 Tue Jul 24 12:00:06 2012]
ログアウト
ヘルプ
ファイアウォールの設定を行ったり、修正したりします。
ファイアウォールの設定
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
ヤマハスイッチの設定を行ったり、変更したりします。
スイッチ制御
詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
1 クリックする
RADIUSの設定
設定
本体の設定(日付・時刻、ブザー)
設定
ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)
設定
2 クリックする
外部デバイスの設定
設定
詳細設定と情報
ユーザーとアクセス制限の設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定]
ユーザーとパスワードの設定
ユーザーの登録数: 0
設定
無名ユーザー
設定
管理パスワードを設定すると、かんたん設定にログインするときに必要になります。
管理パスワード
同じものをもう一度
4 入力する
3 入力する
管理パスワードを暗号化して保存する
IPアドレス指定
暗号アルゴリズム
aes128-ctr
aes192-ctr
aes256-ctr
aes128-cbc
aes192-cbc
aes256-cbc
3des-cbc
blowfish-cbc
cast128-cbc
arcfour
同時に接続できるユーザー数
8
設定の確定
5 クリックする
戻る
トップへ戻る

1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」をクリックする。

「ユーザーとアクセス制限の設定」画面が表示されます。

3 「管理パスワード」欄に本製品のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

4 手順3で入力した本製品のパスワードを再度入力する。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「設定の確定」をクリックする。

設定したパスワードが有効になります。

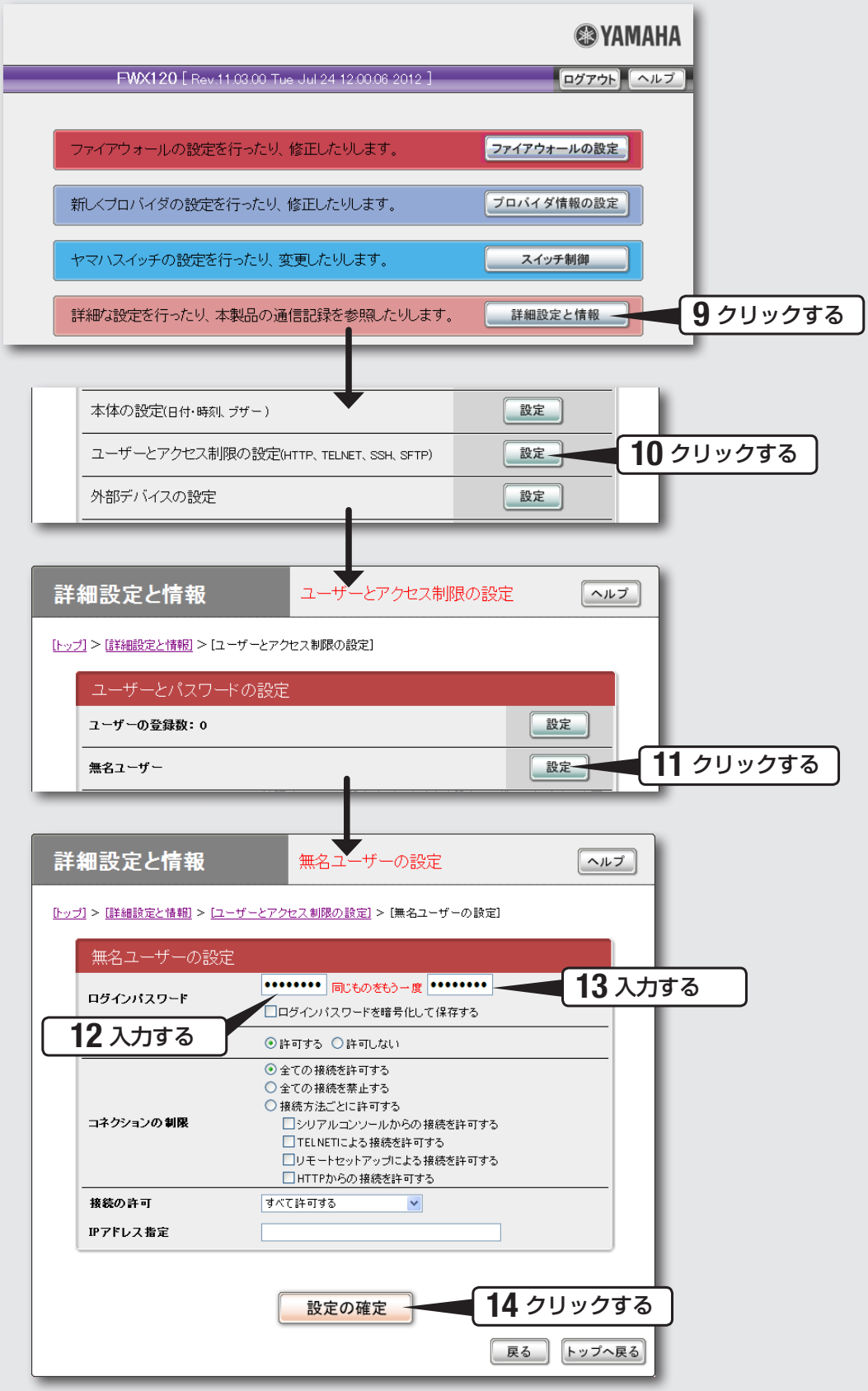
7 「トップへ戻る」をクリックする。

「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。

8 手順3で入力した本製品のパスワードを「パスワード」欄に入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページに戻ります。
引き続き、本製品のログインパスワードを設定します。

ヒント
「ユーザー名」欄には、何も入力する必要はありません。


YAMAHA
FWX120 [Rev.11.03.00 Tue Jul 24 12:00:06 2012]
ログアウト
ヘルプ
ファイアウォールの設定を行ったり、修正したりします。
ファイアウォールの設定
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
ヤマハスイッチの設定を行ったり、変更したりします。
スイッチ制御
詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
9 クリックする
本体の設定(日付・時刻、ブザー)
設定
ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)
設定
10 クリックする
外部デバイスの設定
設定
詳細設定と情報
ユーザーとアクセス制限の設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定]
ユーザーとパスワードの設定
ユーザーの登録数: 0
設定
無名ユーザー
設定
11 クリックする
詳細設定と情報
無名ユーザーの設定
ヘルプ
[トップ] > [詳細設定と情報] > [ユーザーとアクセス制限の設定] > [無名ユーザーの設定]
無名ユーザーの設定
ログインパスワード
同じものをもう一度
13 入力する
ログインパスワードを暗号化して保存する
12 入力する
許可する
許可しない
コネクションの制限
全ての接続を許可する
全ての接続を禁止する
接続方法ごとに許可する
シリアルコンソールからの接続を許可する
TELNETによる接続を許可する
リモートセットアップによる接続を許可する
HTTPからの接続を許可する
接続の許可
すべて許可する
IPアドレス指定
設定の確定
14 クリックする
戻る
トップへ戻る

9 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

10 「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」をクリックする。

「ユーザーとアクセス制限の設定」画面が表示されます。

11 「無名ユーザー」欄の「設定」をクリックする。

「無名ユーザーの設定」画面が表示されます。

12 「ログインパスワード」欄に、ログイン用のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

13 手順11で入力したログイン用パスワードを再度入力する。

14 「設定の確定」をクリックする。

確認画面が表示されます。

15 「設定の確定」をクリックする。

設定したパスワードが有効になります。

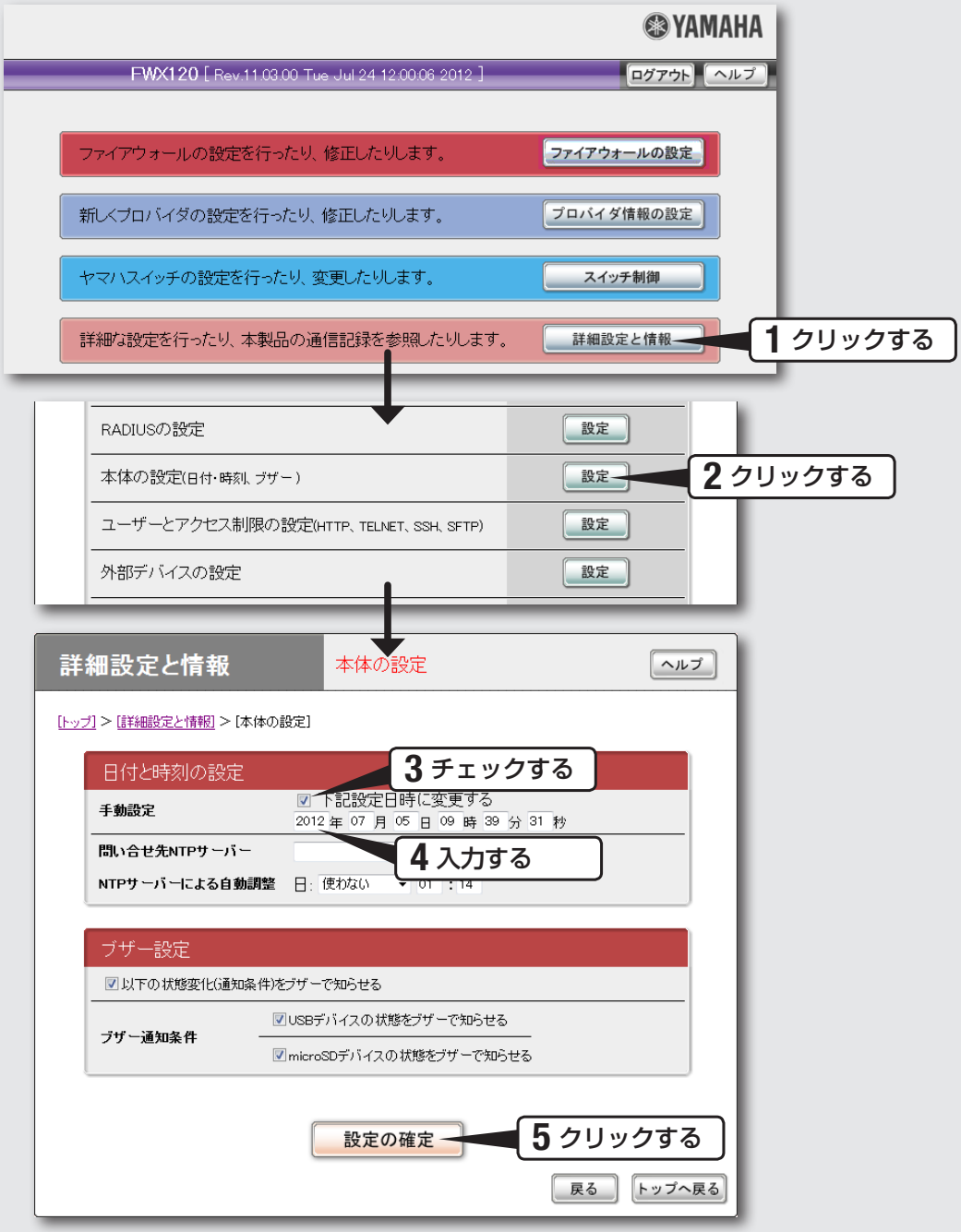
16 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

準備 4

日付・時刻を合わせる

「本体の設定」画面で、本製品の日付と時刻を合わせます。



1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「本体の設定(日付・時刻、ブザー)」の「設定」をクリックする。

「本体の設定」画面が表示されます。

3 「日付と時刻の設定」欄の、「下記設定日時に変更する」にチェックを付ける。

4 日付と時刻を入力する。

ヒント
あらかじめ少し先の時刻を入力しておき、時報と同時に「設定の確定」をクリックするとより正確に時刻合わせできます。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

本製品の時刻を自動的に合わせたいときは

インターネット上のNTPサーバー(時刻配信サーバー)を利用して、本製品の時刻を自動的に合わせることができます。

ご注意
本製品のセキュリティー設定によっては、本製品だけでなくLAN内のパソコンからもNTPサーバーを利用して時刻を合わせられない場合があります。外部のNTPサーバーを利用する場合は、フィルターの設定を変更してください(99ページ)。

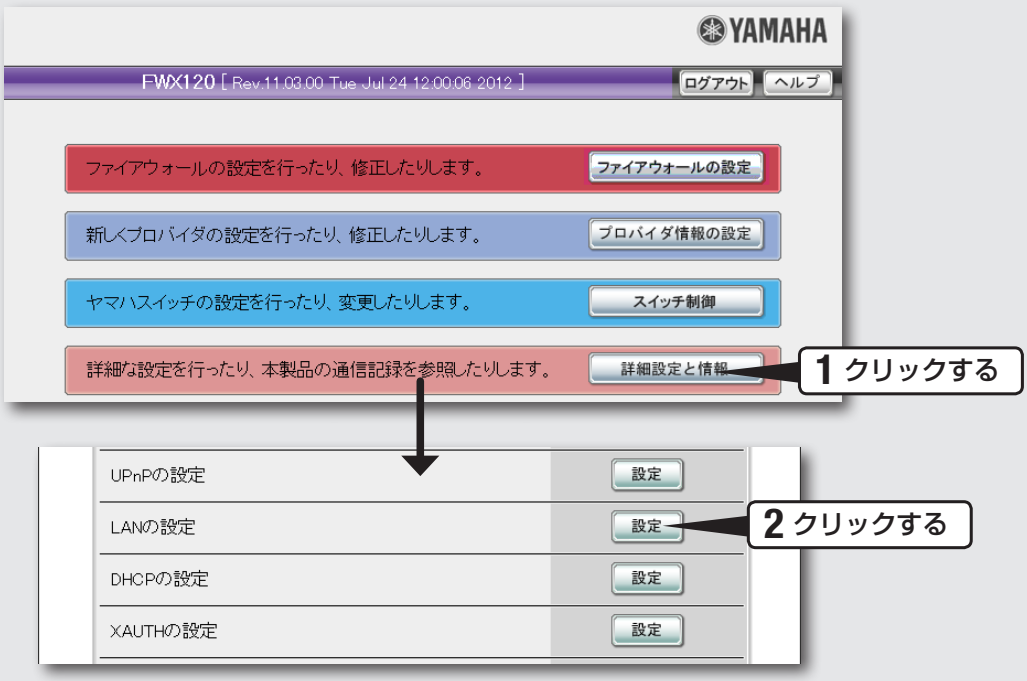
準備 5

LAN1 側IPアドレスを設定する

ブロードバンド回線を経由して異なる場所のLAN同士を接続する場合は、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する必要があります。それぞれのLANの新たなネットワークアドレスを決めて、本製品とパソコンに新たな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設定してください。

ご注意

すでに異なるネットワークアドレスが設定されている場合には、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。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。

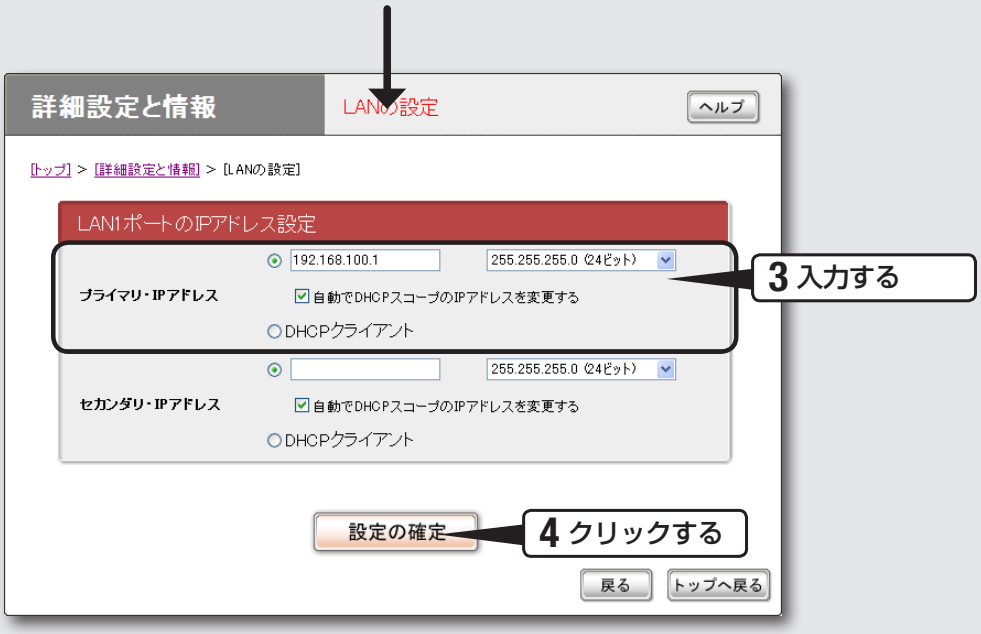


1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「LANの設定」の「設定」をクリックする。

「LANの設定」画面が表示されます。



3 「LAN1ポートのIPアドレス設定」欄に、本製品のLAN1側IPアドレスを入力する。

プライマリ・IPアドレス

新たに決めたネットワークアドレスに応じたIPアドレスを入力し、ネットマスクを選択します。設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

4 「設定の確定」をクリックする。

確認画面が表示されます。

5 「実行」をクリックしてから、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、55ページからの説明をご覧ください。

準備 6

LAN内のパソコンのIPアドレスを変更する

LANのネットワークアドレスを変更した場合には、本製品以外にもLAN内のパソコンのIPアドレスとネットマスクも変更する必要があります。なお、LAN内にパソコン以外の機器も設置されている場合には、それらの機器のIPアドレスとネットマスクもあわせて変更する必要があります。それらの機器の設定方法については、各機器の取扱説明書をご覧ください。

ご注意

本製品を設置したLANのネットワークアドレスを変更していない場合は、LAN内のパソコンのIPアドレスを変更する必要はありません。

パソコンのIPアドレスの変更方法は、OSのバージョンによって異なります。

詳しくは、「パソコンのIPアドレスを変更する」(229ページ)をご覧ください。

準備 7

プロバイダ情報を設定する

インターネットへの接続方法を選ぶ

本製品はさまざまな回線接続方法に対応しています。接続方法によって必要な回線契約やプロバイダ(インターネット接続業者)との接続契約が異なりますので、接続方法に合わせて説明をご覧ください。

ブロードバンド回線でインターネットへ常時接続する ▶57ページ

ネットワーク型接続サービスでインターネットへ常時接続する ▶67ページ
- ネットワーク型PPPoE接続：67ページ
- unnumbered接続：67ページ

USBデータ通信端末でインターネットへ接続する ▶73ページ

フレッツ 光ネクスト回線でインターネットへ接続する(IPv6 IPoE方式) ▶81ページ

フレッツ 光ネクスト回線でインターネットへ接続する(IPv6 PPPoE方式) ▶86ページ

ご注意

- プロバイダ契約を解除／変更した場合は、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。削除しないままお使いになると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- 本製品をルーターとしてお使いになる前（または新たにプロバイダ契約を行う前）に、必ずルーター経由による複数パソコンの同時接続が、プロバイダによって禁止されていないかどうかご確認ください。プロバイダによっては、禁止もしくは別の契約が必要な場合があります。契約に違反して本製品を使用すると、予想外の料金を請求される場合があります。禁止されている場合は、プロバイダと別途必要な契約を行うか、同時接続を禁止していない他のプロバイダと契約してください。

ブロードバンド回線で インターネットへ常時接続する (PPPoE/CATV)

本製品の「かんたん設定ページ」で接続先を設定して、インターネットに接続します。
ネットワーク型PPPoE接続やunnumbered接続を使用する場合は、「ネットワーク型接続サービスで常時接続する(フレッツ・VPN ワイド接続)」(67ページ)をご覧ください。

設定する前に

ご注意

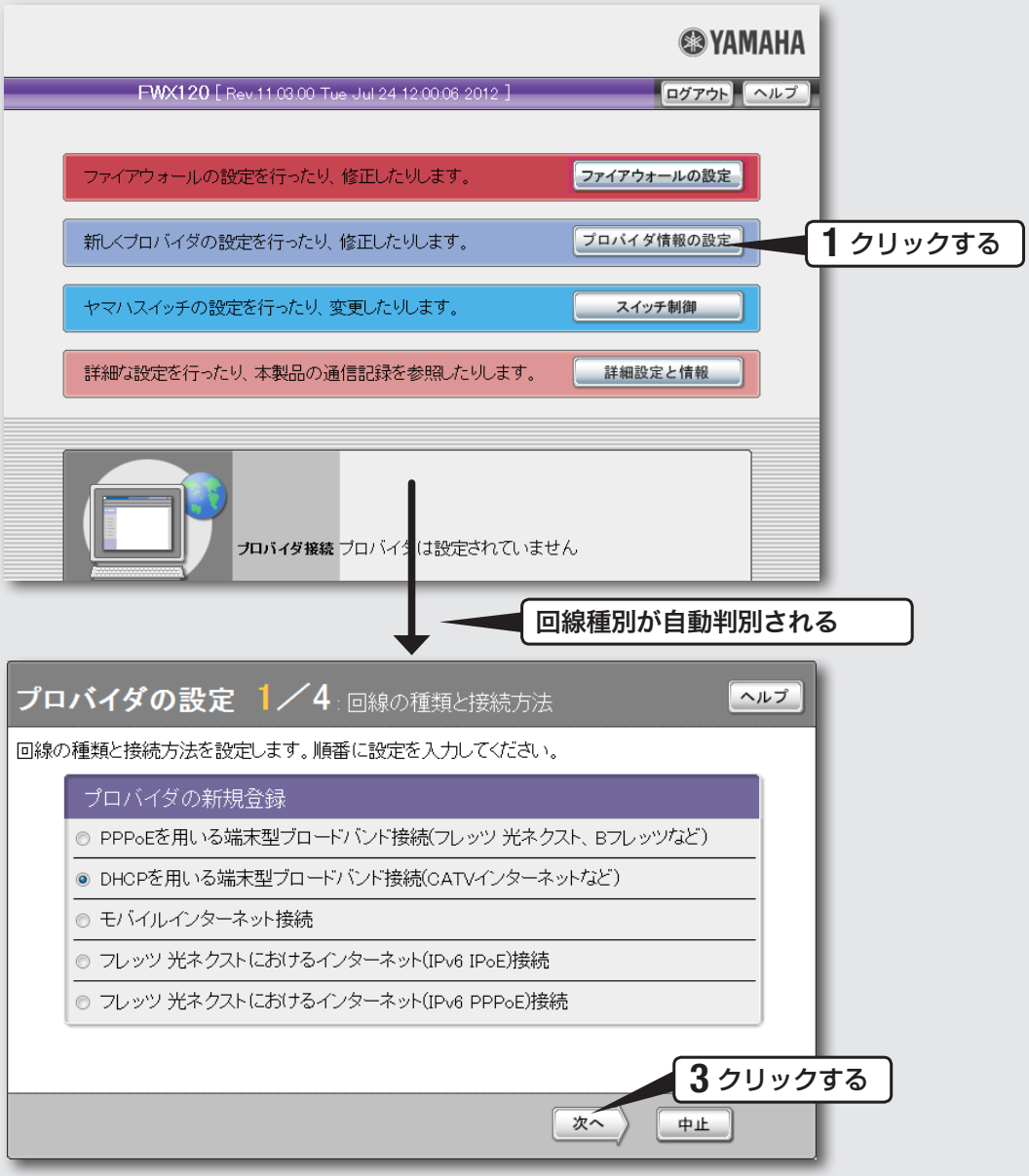
- プロバイダ契約を解除または変更した時は、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分ご注意の上、お使いください。詳しくは「セキュリティーを強化する」(92 ページ)をご覧ください。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。

プロバイダの設定資料を用意してください

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(DNSサーバーアドレス、ネームサーバー IPアドレス、DNSサーバー IPアドレス)
- デフォルトゲートウェイアドレス

1　接続方法を確認する



1　「かんたん設定ページ」のトップページで、「プロバイダ情報の設定」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、接続した回線に合わせた接続方法が選ばれた画面が表示されます。

ご注意

ブロードバンド回線自動判別機能は、一度実行すると次回から自動判別を行わないため、本製品のLAN2ポートにブロードバンド回線が接続されているか確認してから行ってください。

2 自動判別された接続方法を確認し、「次へ」をクリックする。

「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」が選ばれた場合

「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」が選ばれる代表的な接続サービスは、以下の通りです。

- フレッツ 光ネクスト
- Bフレッツ
- フレッツ・ADSL
- イー・アクセス（ADSLモデムがブリッジモードの場合）

「DHCPを用いる端末型ブロードバンド接続（CATVインターネットなど）」が選ばれた場合

「DHCPを用いる端末型ブロードバンド接続（CATVインターネットなど）」が選ばれる代表的な接続サービスは、以下の通りです。

- Yahoo! BB
- イー・アクセス（ADSLモデムがルーターモードの場合）
- プロバイダ独自のADSL接続サービス
- 各種CATVインターネット接続サービス

3 「次へ」をクリックする。

接続回線に合わせた設定画面が表示されます。
以降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。

何も選ばれなかった場合は

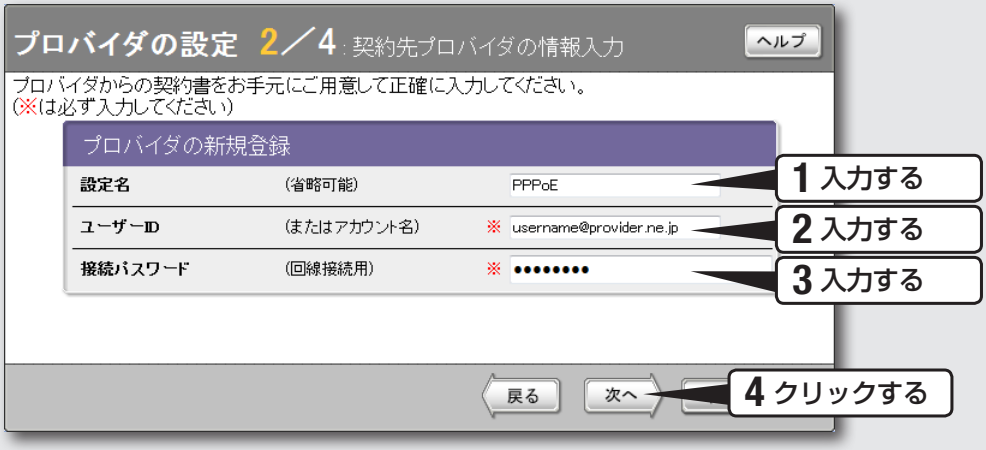
▶ブロードバンド回線の自動判別に失敗しました。

接続回線に合わせて「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」または「DHCPを用いる端末型ブロードバンド接続（CATVインターネットなど）」を選んでから、「次へ」をクリックしてください。
どちらかわからない場合は、契約書を確認するかプロバイダにお問い合わせください。

A 「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」が選ばれた場合 ▶60ページをご覧ください。

B 「DHCPを用いる端末型ブロードバンド接続（CATVインターネットなど）」が選ばれた場合 ▶64ページをご覧ください。

A PPPoE端末型 (59ページから) 2—プロバイダの情報を指定する



1 設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 ユーザー IDを入力する。

プロバイダから指定された、接続用のユーザー IDを入力します。必ず書類を確認して、間違いのないように入力してください。

ご注意

フレッツ・ADSLやBフレッツで接続する場合は、ユーザー IDの後にプロバイダ名を入力する必要があります。詳しくはフレッツ・ADSLまたはBフレッツの契約の際にNTTから送付された資料や、プロバイダからの資料をご覧ください。

ユーザー IDがusernameの場合の例：

username@provider.ne.jp

username@aaa.provider.ne.jp（サブドメインが付加される場合）

3 接続パスワードを入力する。

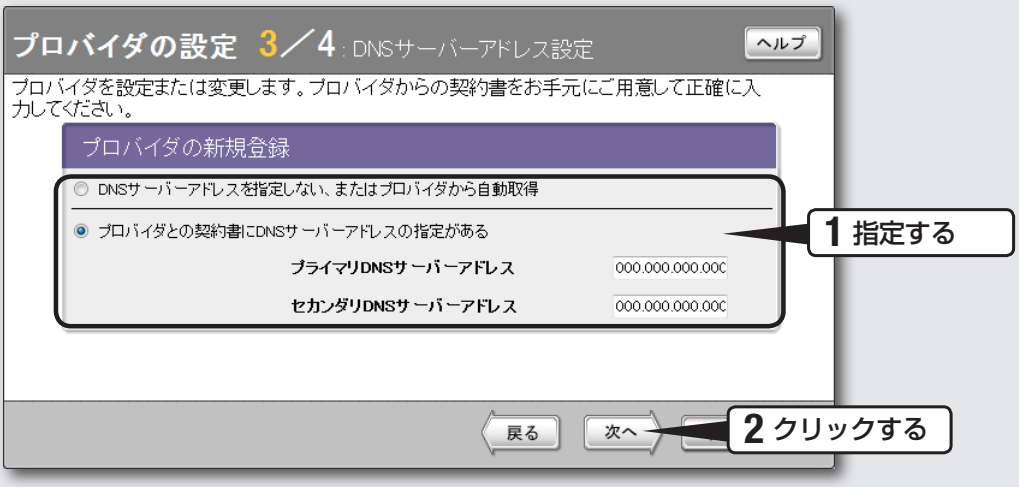
プロバイダから指定されたパスワード(または自分で変更したパスワード)を入力します。半角英数字で、大文字小文字も正確に入力してください。

入力したパスワードの文字は●で表示されます。

4 「次へ」をクリックする。

「プロバイダの設定３／４」画面が表示されます。

A PPPoE端末型 (59ページから) 3—DNSサーバーアドレスを指定する



1 DNSサーバーアドレスを指定する。

プロバイダからDNSサーバーアドレスが指定されていない場合

「DNSサーバーアドレスを指定しない、またはプロバイダから自動取得」をクリックして選びます。

プロバイダからDNSサーバーアドレスが指定されている場合

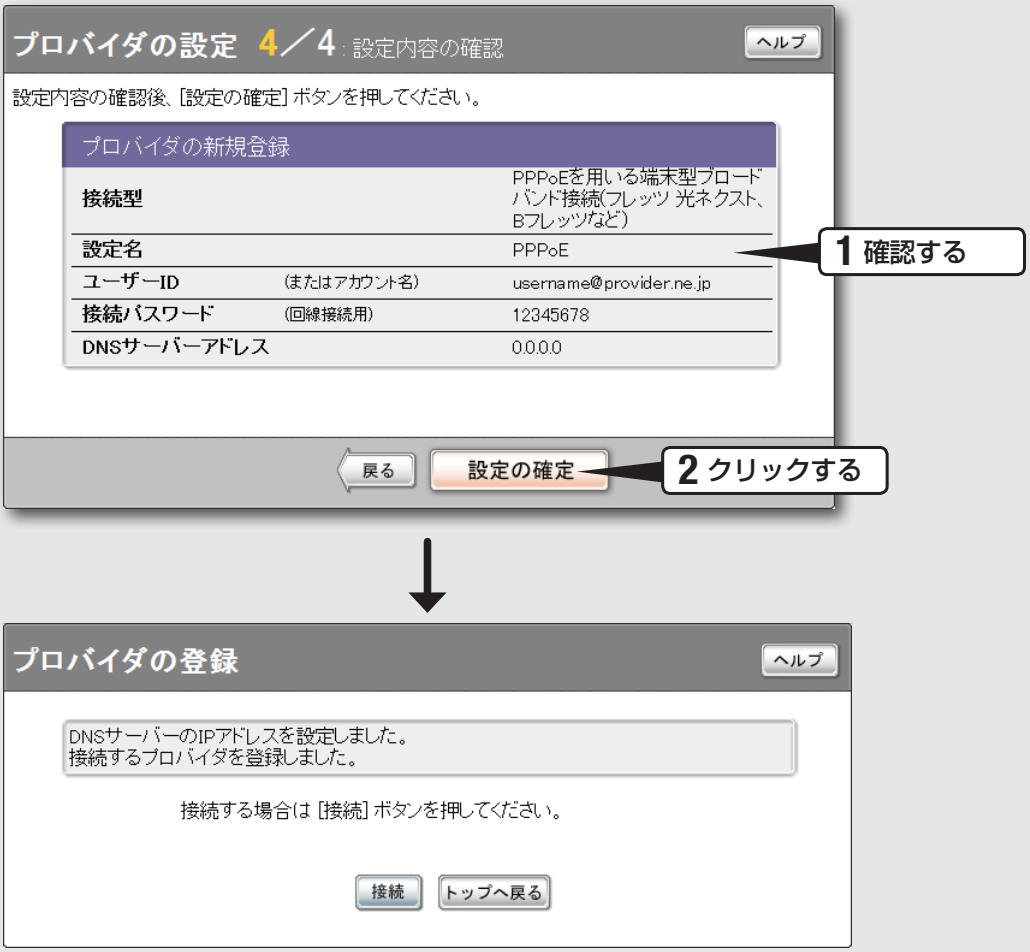
「プロバイダとの契約書にDNSサーバーアドレスの指定がある」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス**：プロバイダから指定されているDNSサーバーアドレスを半角数字で入力します。
- **セカンダリDNSサーバーアドレス**：プロバイダ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）。

2 「次へ」をクリックする。

「プロバイダの設定4 ／ 4」画面が表示されます。

A PPPoE端末型 (59ページから) 4―設定内容を確認する



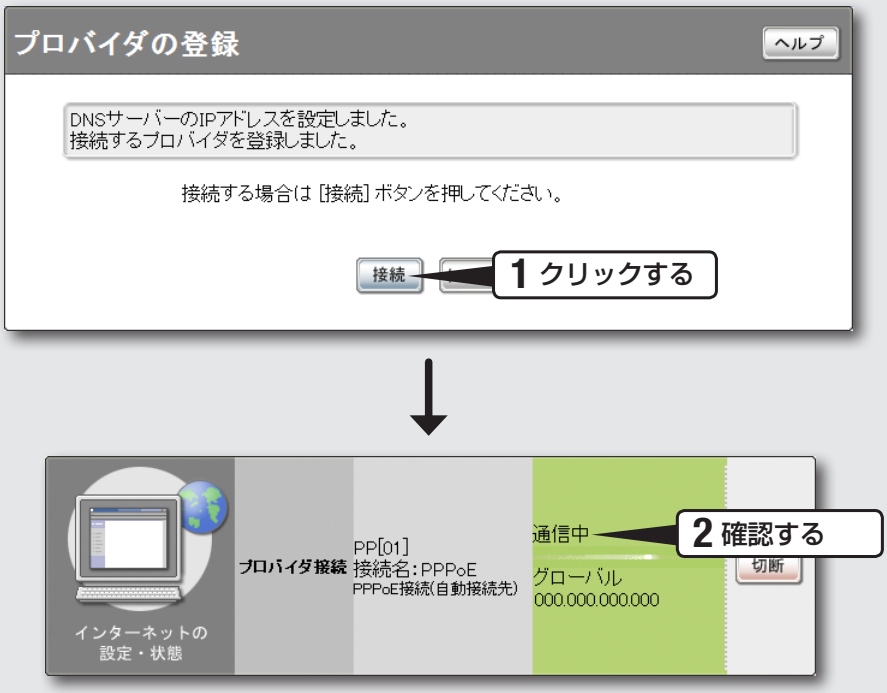
1 **表示された設定内容が、プロバイダから送付された設定資料と合っているかを確認する。**

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2 **「設定の確定」をクリックする。**

「プロバイダの登録」画面が表示されます。

A PPPoE端末型 (59ページから) 5—インターネットに接続する



1 「接続」をクリックする。

インターネットに接続して、「プロバイダへの接続／切断」画面が表示されます。
「トップへ戻る」をクリックすると、「かんたん設定ページ」のトップページに戻ります。

2 インターネットに接続しているかを確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

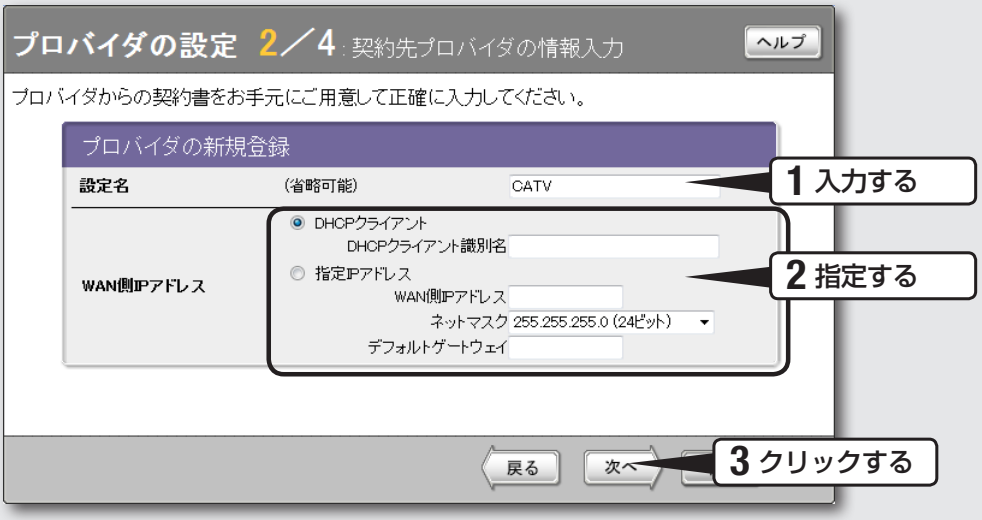
設定終了

これでインターネットへの接続設定は終了です

►インターネットに接続できない場合は

Check 1 本製品とパソコン、ADSLモデムやONUの接続を確認してください。
Check 2 60～61ページの設定内容をもう一度確認してください。
Check 3 それでも問題が解決しない場合は、「困ったときは」(200ページ)を参考にして、問題を解決してください。

B CATVインターネット（59ページから） 2―プロバイダの情報を指定する



1 設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 WAN側IPアドレスを指定する。

プロバイダからIPアドレスを指定されていない場合

「DHCPクライアント」をクリックして選びます。

プロバイダからDHCPクライアント識別名を指定されている場合は、「DHCPクライアント識別名」欄に指定された識別名を入力します（指定されていない場合は、入力する必要はありません）。

プロバイダからIPアドレスを指定されている場合

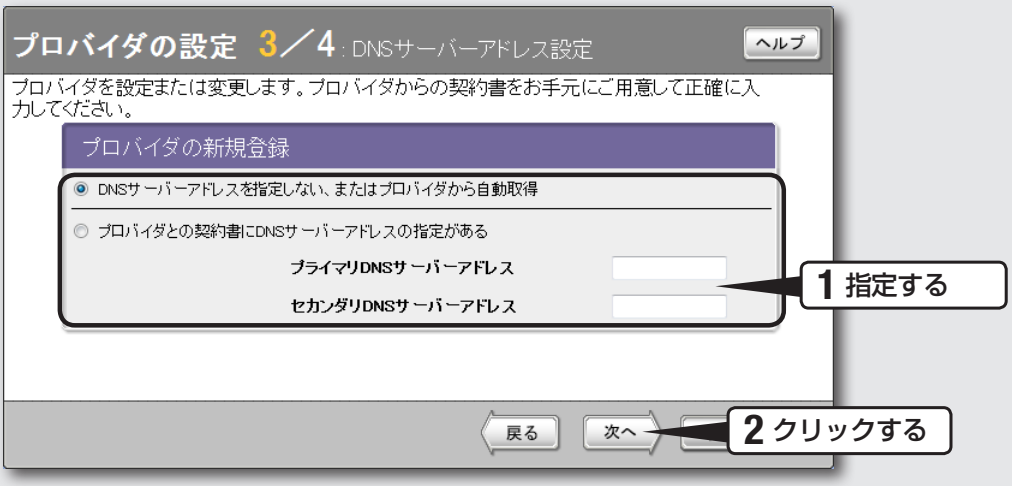
「指定IPアドレス」をクリックして選んでから、以下の設定を行います。

- **WAN側IPアドレス**：プロバイダから指定されたIPアドレスを、半角数字で入力します。
- **ネットマスク**：プロバイダから指定されたネットマスクを選びます。
- **デフォルトゲートウェイ**：プロバイダから指定されたデフォルトゲートウェイアドレスを、半角数字で入力します。

3 「次へ」をクリックする。

「プロバイダの設定３／４」画面が表示されます。

B CATVインターネット（59ページから） 3―DNSサーバーアドレスを指定する



1 DNSサーバーアドレスを指定する。

プロバイダからDNSサーバーアドレスが指定されていない場合

「DNSサーバーアドレスを指定しない、またはプロバイダから自動取得」をクリックして選びます。

プロバイダからDNSサーバーアドレスが指定されている場合

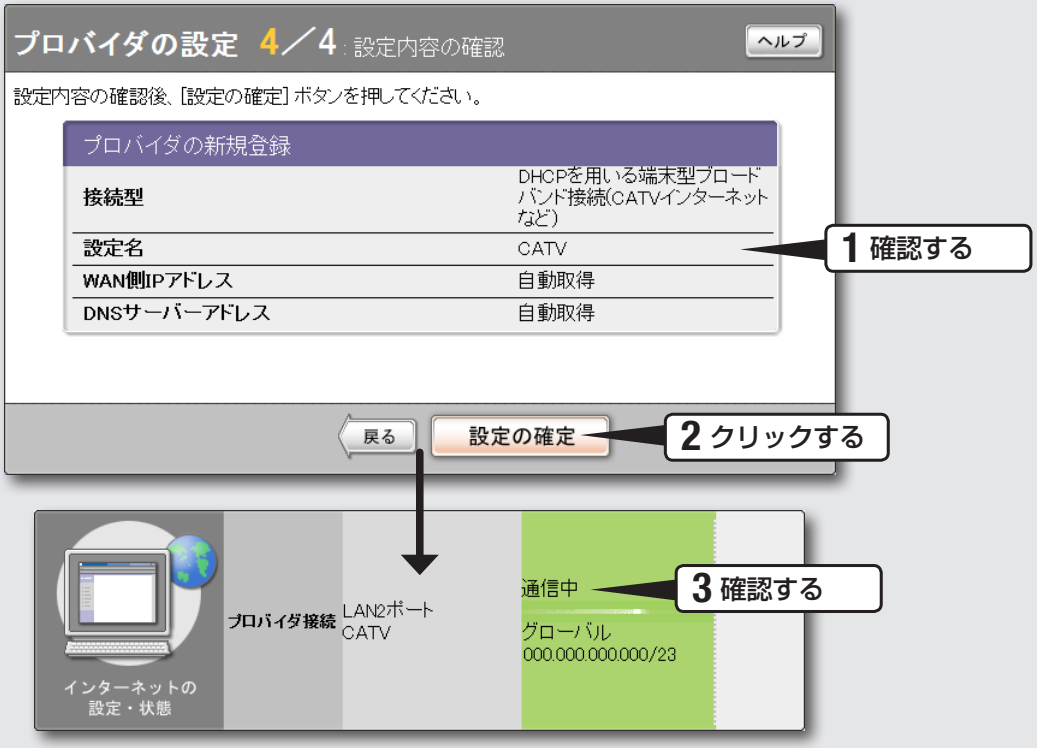
「プロバイダとの契約書にDNSサーバーアドレスの指定がある」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス**：プロバイダから指定されているDNSサーバーアドレスを半角数字で入力します。
- **セカンダリDNSサーバーアドレス**：プロバイダ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）。

2 「次へ」をクリックする。

「プロバイダの設定4 ／ 4」画面が表示されます。

B CATVインターネット（59ページから） 4―設定内容を確認して、インターネットに接続する



1 **表示された設定内容が、プロバイダから送付された設定資料と合っているかを確認する。**

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2 **「設定の確定」をクリックする。**

表示された確認画面で「トップへ戻る」をクリックすると、本製品は自動的にインターネットに接続して「かんたん設定ページ」のトップページに戻ります。

3 **インターネットに接続しているかを確認する。**

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

▼

設定終了

これでインターネットへの接続設定は終了です

▶インターネットに接続できない場合は

Check 1　本製品とパソコン、ADSLモデムやケーブルモデムの接続を確認してください。

Check 2　64～65ページの設定内容をもう一度確認してください。

Check 3　それでも問題が解決しない場合は、「困ったときは」（200ページ）を参考にして、問題を解決してください。

ネットワーク型接続サービスで常時接続する

（フレッツ・VPN ワイドなど）

本製品の「かんたん設定ページ」で接続先を設定して、インターネットに接続します。
unnumbered接続を使用する場合も、この説明をご覧ください。
フレッツ 光ネクストやBフレッツなどの各種フレッツ接続サービスや光ファイバ接続サービスで、IPアドレスを１つだけ割り当てられるサービスを使用する場合は、「ブロードバンド回線でインターネットへ常時接続する（PPPoE/CATV）」（57ページ）をご覧ください。

設定する前に

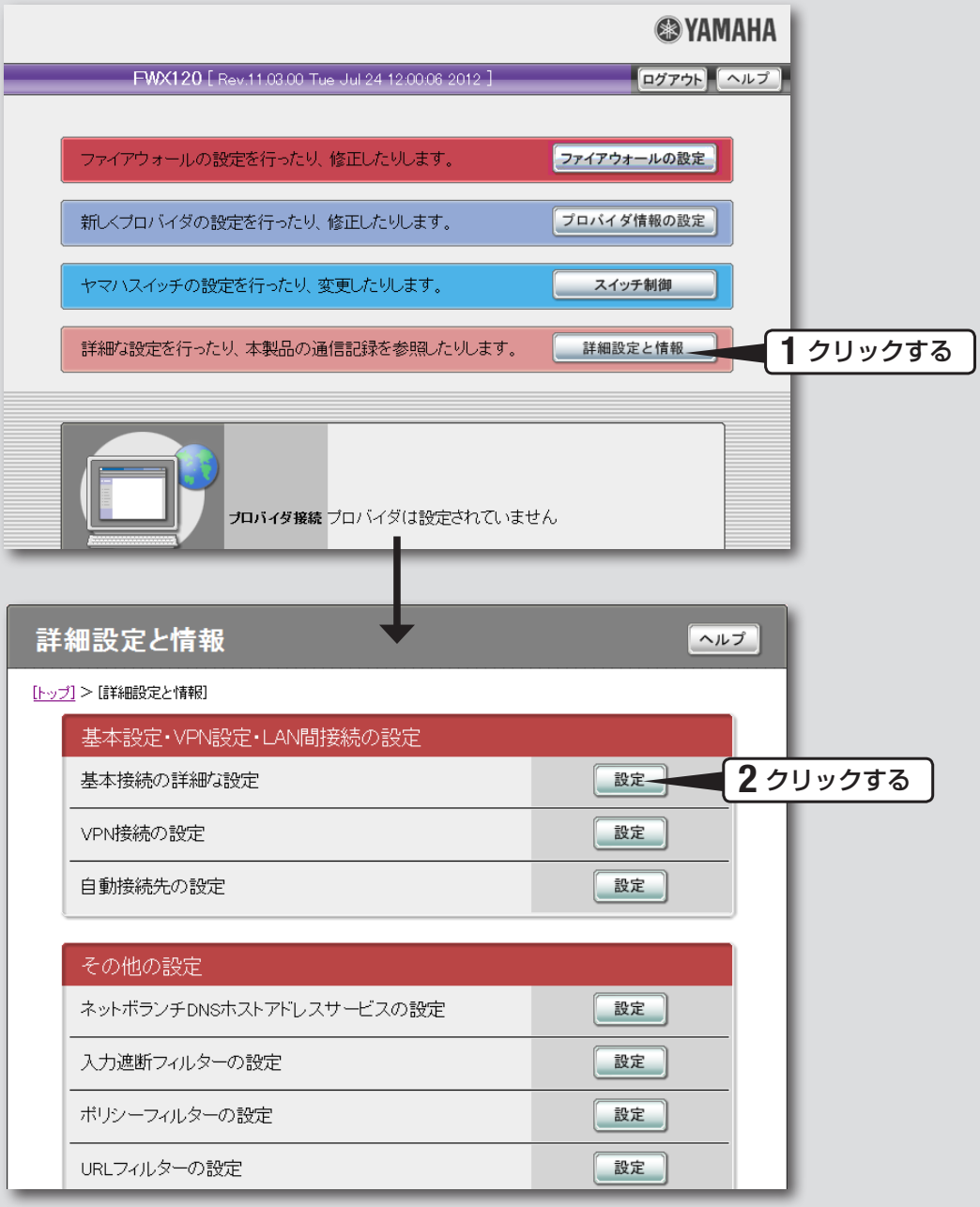
ご注意

- プロバイダ契約を解除または変更した時は、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。
- インターネットへ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「セキュリティーを強化する」（92 ページ）をご覧ください。
- 本書では Internet Explorer 8の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。

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（DNSサーバーアドレス、ネームサーバー IPアドレス、DNSサーバー IPアドレス）
- デフォルトゲートウェイアドレス

1　接続方法を指定する

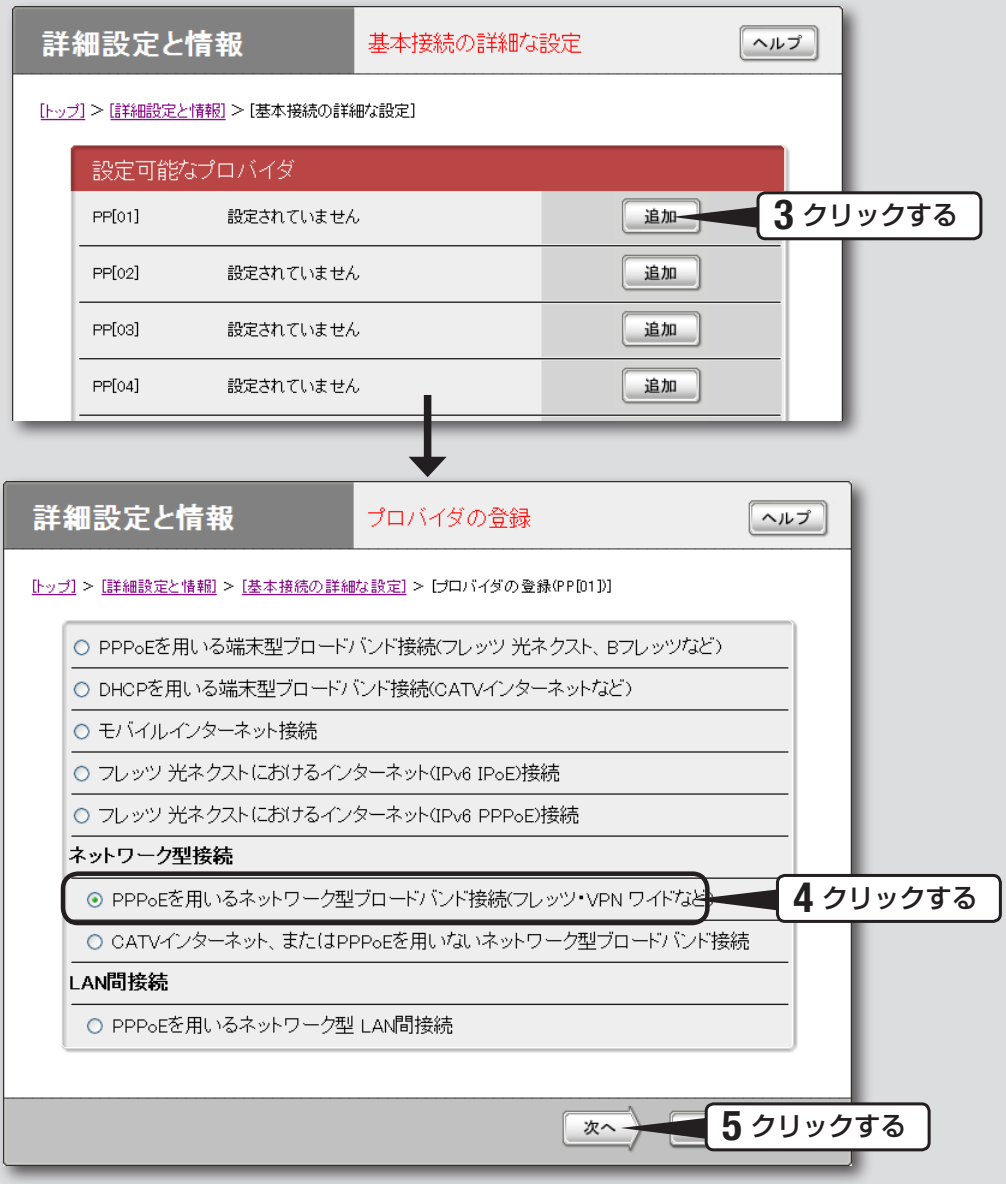


1　**「詳細設定と情報」をクリックする。**

「詳細設定と情報」画面が表示されます。

2　**「基本接続の詳細な設定」の「設定」をクリックする。**

「基本接続の詳細な設定」画面が表示されます。



3 「追加」をクリックする。

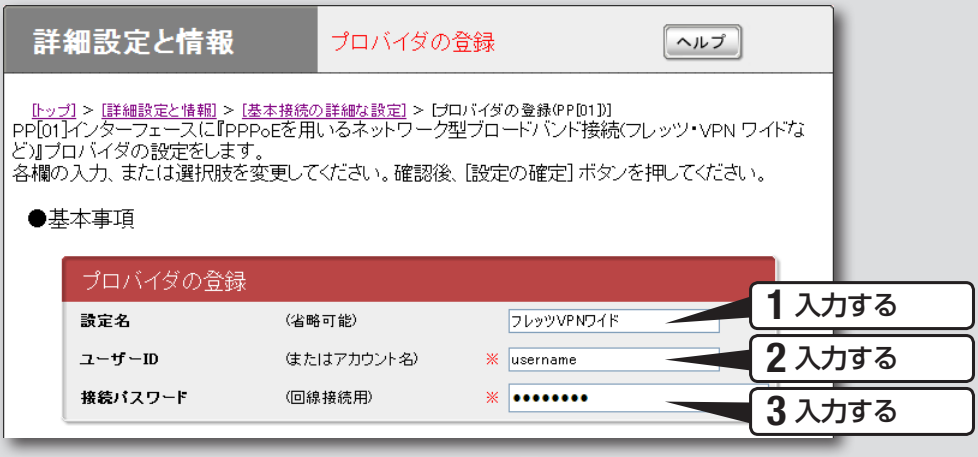
「プロバイダの登録」画面が表示されます。

4 「PPPoEを用いるネットワーク型ブロードバンド接続(フレッツ・VPN ワイドなど)」をクリックする。

5 「次へ」をクリックする。

「プロバイダの登録」画面が表示されます。

2　プロバイダの情報を指定する



1　設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2　ユーザー IDを入力する。

プロバイダから指定された、接続用のユーザー IDを入力します。必ず書類を確認して、間違いのないように入力してください。

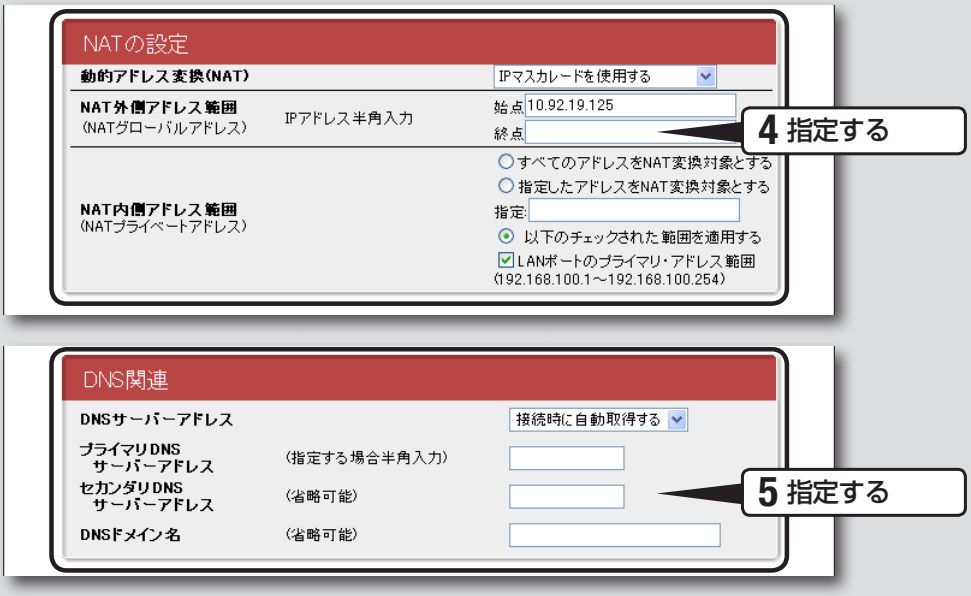
ご注意

フレッツ・VPN ワイドで接続する場合は、ユーザー IDの後に識別子を入力する必要があります。詳しくはフレッツ・VPN ワイドの契約の際にNTTから送付された資料や、プロバイダからの資料をご覧ください。

ユーザー IDがusernameの場合の例：
username@識別子

3　接続パスワードを入力する。

プロバイダ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。半角英数字で、大文字小文字も正確に入力してください。
入力したパスワードの文字は●で表示されます。



4 アドレス変換(NAT)の設定を指定する。

動的アドレス変換(NAT)
回線側とLAN側のアドレス変換方法を選びます。

- NATを使用する：回線側とLAN側のアドレスを1対1で変換する場合
- IPマスカレードを使用する：回線側とLAN側のアドレスを1対多で変換する場合
- NATとIPマスカレードを併用する：LAN側の機器にグローバルIPアドレスとプライベートIPアドレスを混在して割り当てる場合
- 使用しない：アドレス変換を行わない場合

NAT外側アドレス範囲
回線側に割り当てる共用グローバルIPアドレスを入力します。

NAT内側アドレス範囲
アドレス変換を行うプライベートIPアドレスの範囲を入力します。

5 DNSサーバーアドレスを指定する。

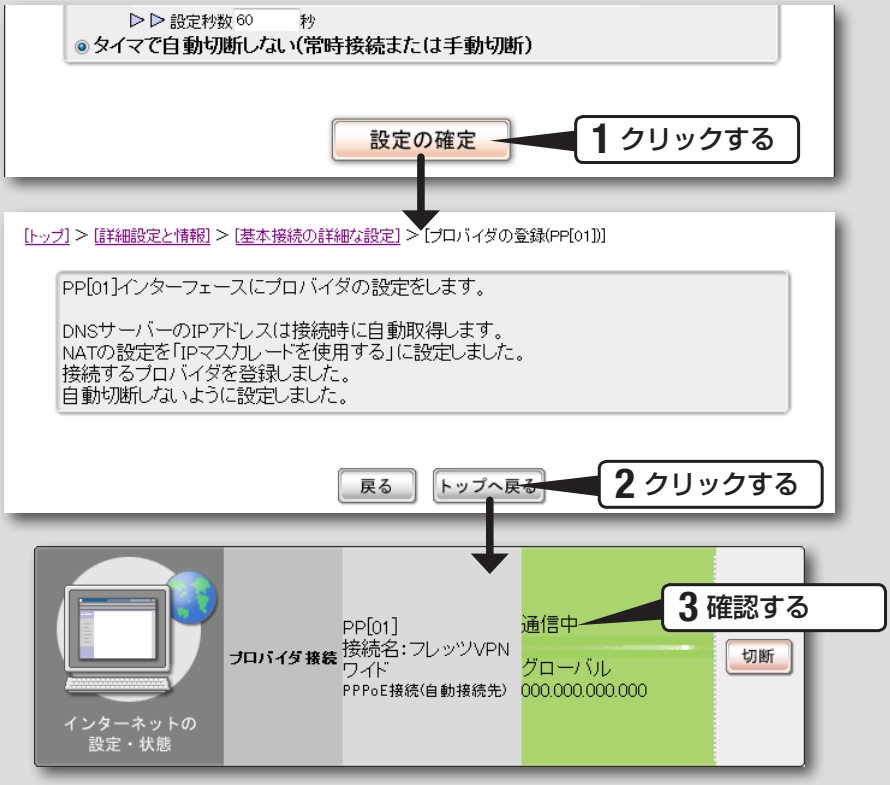
プロバイダからDNSサーバーアドレスが指定されていない場合
「接続時に自動取得する」を選びます。

プロバイダからDNSサーバーアドレスが指定されている場合
「IPアドレスを指定する」を選んでから、以下の設定を行います。

- プライマリDNSサーバーアドレス：プロバイダから指定されているDNSサーバーアドレスを半角数字で入力します。
- セカンダリDNSサーバーアドレス：プロバイダ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)。

プロバイダからドメイン名が指定されている場合
指定されたドメイン名を「DNSドメイン名」欄に入力します。

3　インターネットに接続する



1　「設定の確定」をクリックする。

「プロバイダの登録」画面が表示されます。

2　「トップへ戻る」をクリックする。

自動的にインターネットに接続して、「かんたん設定ページ」のトップページに戻ります。

3　インターネットに接続しているかを確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

▼

設定終了

これでインターネットへの接続設定は終了です

►インターネットに接続できない場合は

Check 1　本製品とパソコン、ADSLモデムやONUの接続を確認してください。
Check 2　70～71ページの設定内容をもう1度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」(200ページ)を参考にして、問題を解決してください。

USBデータ通信端末で インターネットへ接続する

USBポート対応の市販の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できます。USBデータ通信端末を接続してから本製品の「かんたん設定ページ」で接続先を設定して、インターネットに接続します。

設定する前に

ご注意

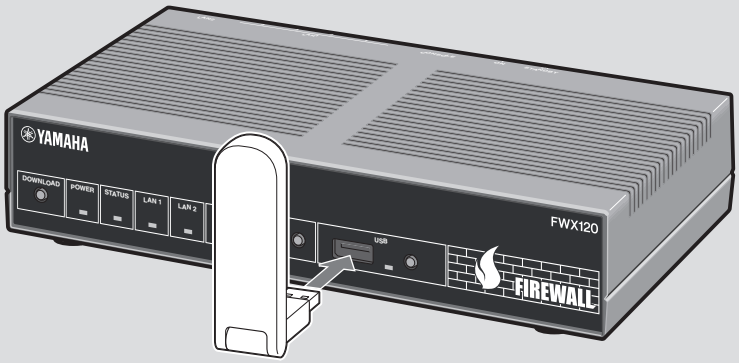
- プロバイダ契約を解除または変更した時は、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- データ通信（パケット通信）の契約が従量制である場合、あるいはデータ通信が定額制の契約の対象外である場合、長時間通信したり大量のデータをやりとりすると高額な料金が発生します。ご使用にあたっては、通信料金について十分ご注意ください。通信時間や通信量を、接続ごとあるいは累積で監視して警告を出したり接続を制限する機能もあります。必要に応じてご利用ください。
- インターネットへ常時接続する場合は、インターネッ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「セキュリティーを強化する」（92 ページ）をご覧ください。
- 通信端末は、ご利用になる携帯端末の取扱説明書に指定されている使いかたや、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。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。

プロバイダの設定資料を用意してください

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（DNSサーバーアドレス、ネームサーバー IPアドレス、DNSサーバー IP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）

1　USBデータ通信端末を接続する



本製品のUSBポートに、USBデータ通信端末を接続する。

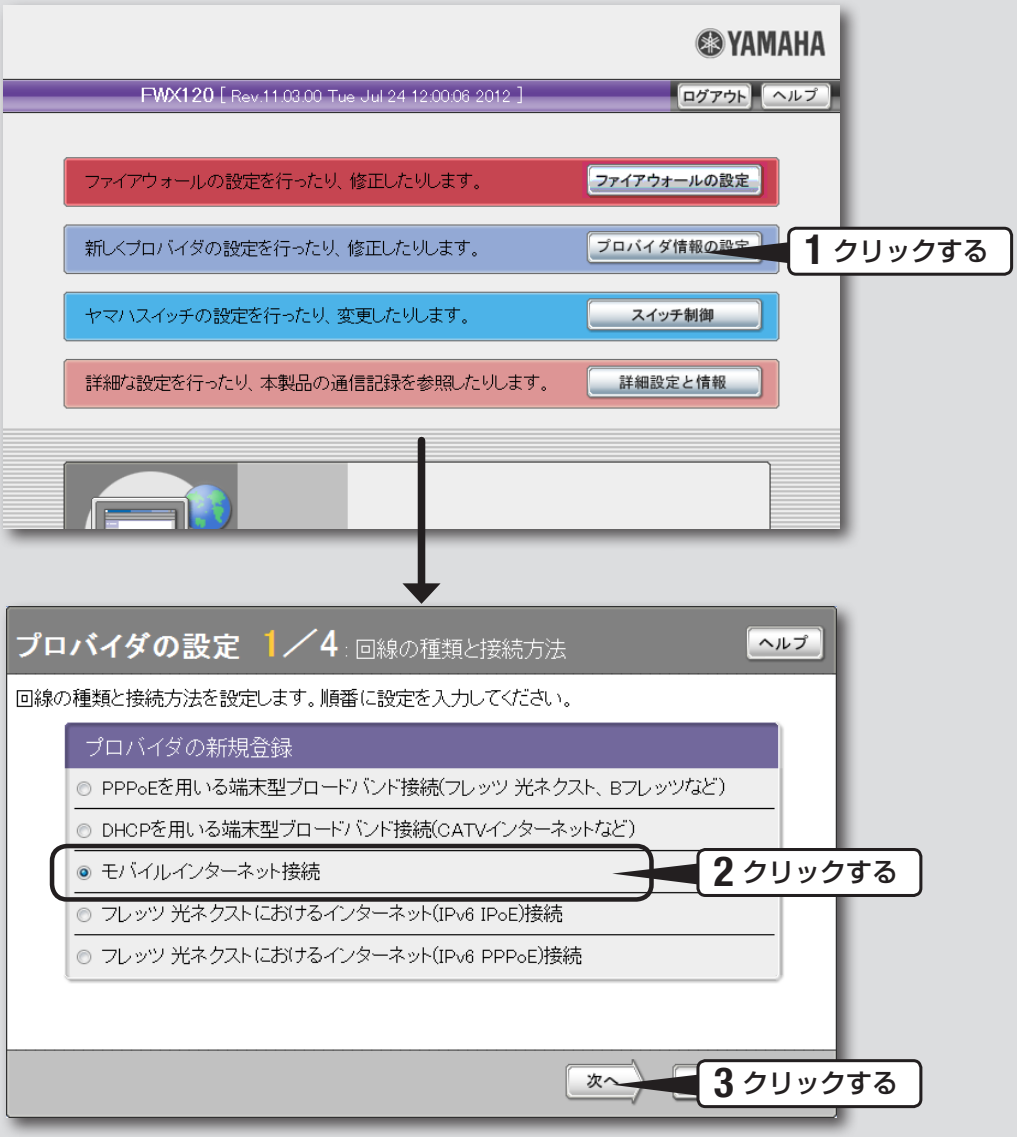
USBランプが点灯／点滅します。

ヒント

USBデータ通信端末の接続時にブザー音が鳴ります。ブザー音については「ブザー音の設定を変更する」(184ページ)をご確認ください。

最新の動作確認済USBデータ通信端末の一覧は、http://jp.yamaha.com/products/network/から本製品の製品情報ページをご覧ください。

2　接続方法を指定する



1　**「かんたん設定ページ」のトップページで、「プロバイダ情報の設定」をクリックする。**

「プロバイダの設定１／４」画面が表示されます。

2　**「モバイルインターネット接続」をクリックする。**

3　**「次へ」をクリックする。**

「プロバイダの設定２／４」画面が表示されます。

3　プロバイダの情報を指定する

1　接続インターフェースを選択する。

接続インターフェースを選びます。
USBデータ通信端末が指定のUSBポートに挿入されていると、自動判別によって決定されます。
挿入していない場合は、USBデータ通信端末を接続してからやり直してください。

2　設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

3　アクセスポイント名を入力する。

キャリアまたはプロバイダから指定された、アクセスポイント名を入力します。契約プランによって入力内容が異なる場合がありますので、必ず書類を確認して、間違いのないように入力してください。

4　CID（Context Identifier)番号を入力する。

キャリアまたはプロバイダから指定された、CID番号を入力します。契約プランによって入力内容が異なる場合がありますので、必ず書類を確認して、間違いのないように入力してください。

5　ユーザー IDを入力する。

プロバイダから指定された、ユーザー IDを入力します。必ず書類を確認して、間違いのないように入力してください。

6 **接続パスワードを入力する。**

プロバイダ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。半角英数字で、大文字小文字も正確に入力してください。
入力したパスワードの文字は●で表示されます。

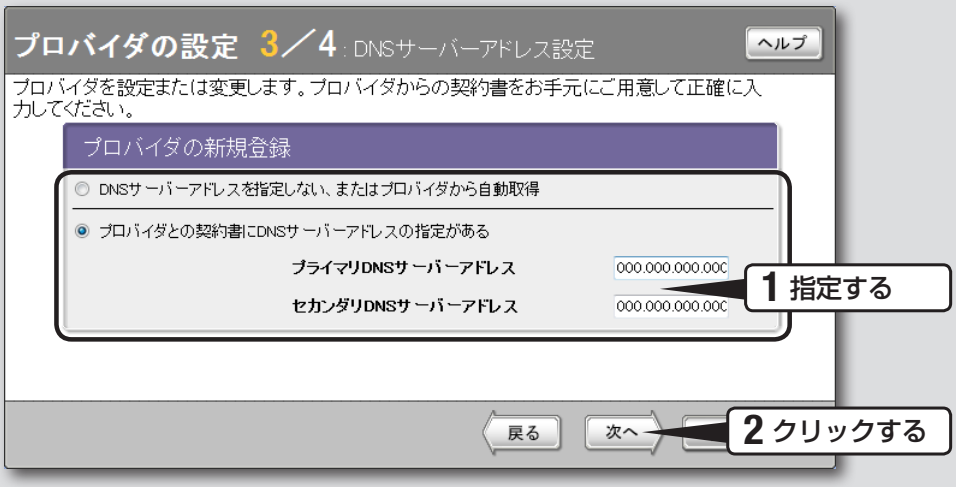
7 **発信規制を選択する。**

累積送受信データ、累積接続時間による発信規制を設定します。契約プランによって長時間の接続により異常課金となる場合がありますので、契約プランを確認してから設定してください。

8 **「次へ」をクリックする。**

「プロバイダの設定3 ／ 4」画面が表示されます。

4　DNSサーバーアドレスを指定する



1　DNSサーバーアドレスを指定する。

プロバイダからDNSサーバーアドレスが指定されていない場合

「DNSサーバーアドレスを指定しない、またはプロバイダから自動取得」をクリックして選びます。

プロバイダからDNSサーバーアドレスが指定されている場合

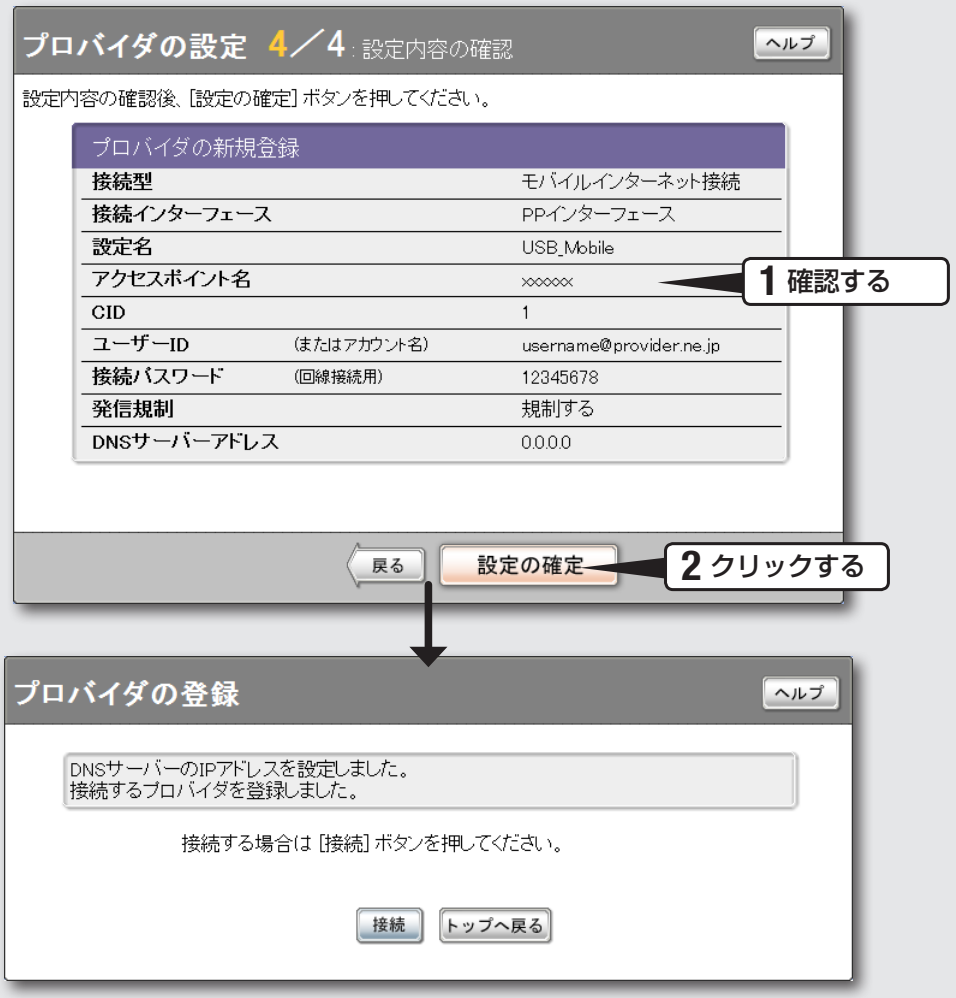
「プロバイダとの契約書にDNSサーバーアドレスの指定がある」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス**：プロバイダから指定されているDNSサーバーアドレスを半角数字で入力します。
- **セカンダリDNSサーバーアドレス**：プロバイダ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）。

2　「次へ」をクリックする。

「プロバイダの設定4 ／ 4」画面が表示されます。

5　設定内容を確認する



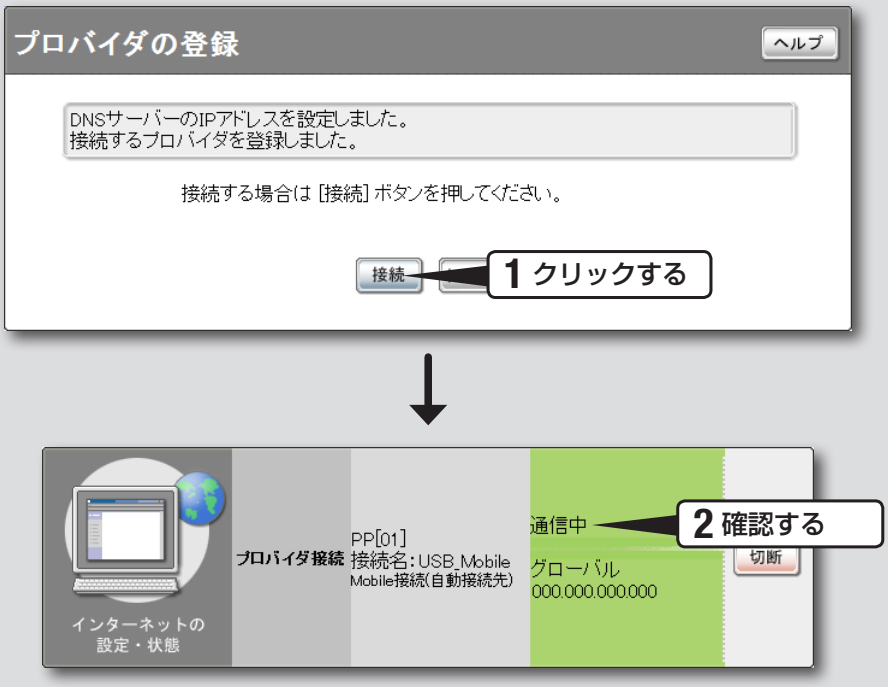
1　**表示された設定内容が、プロバイダから送付された設定資料と合っているかを確認する。**

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2　**「設定の確定」をクリックする。**

「プロバイダの登録」画面が表示されます。

6　インターネットに接続する



1　「接続」をクリックする。

インターネットに接続して、「プロバイダへの接続／切断」画面が表示されます。
「トップへ戻る」をクリックすると、「かんたん設定ページ」のトップページに戻ります。

2　インターネットに接続しているかを確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

▼

設定終了

これでインターネットへの
接続設定は終了です

►インターネットに接続できない場合は

Check 1　本製品とパソコン、USBデータ通信端末の接続を確認してください。
Check 2　76～78ページの設定内容をもう1度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」(200ページ)を参考にして、問題を解決してください。

フレッツ 光ネクスト回線で インターネットへ接続する

(IPv6 IPoE方式)

本製品の「かんたん設定ページ」で接続先を設定して、インターネットに接続します。

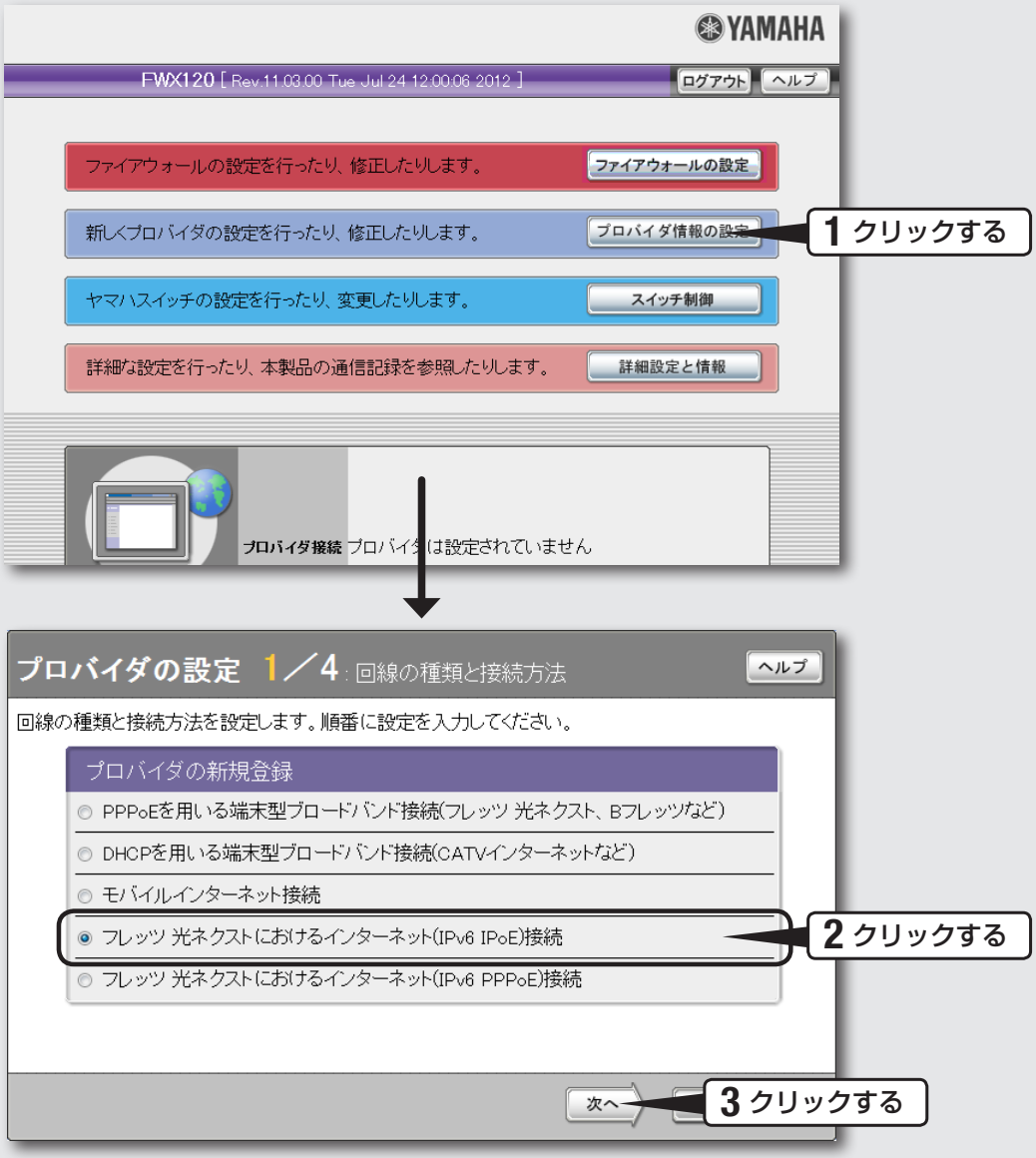
設定する前に

ご注意

- プロバイダ契約を解除または変更した時は、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。
- インターネットへ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「セキュリティーを強化する」(92 ページ) をご覧ください。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。
- 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。

フレッツ 光ネクスト回線の契約で「ひかり電話の契約の有無」を確認してください。

1　接続方法を確認する



1　**「かんたん設定ページ」のトップページで、「プロバイダ情報の設定」をクリックする。**

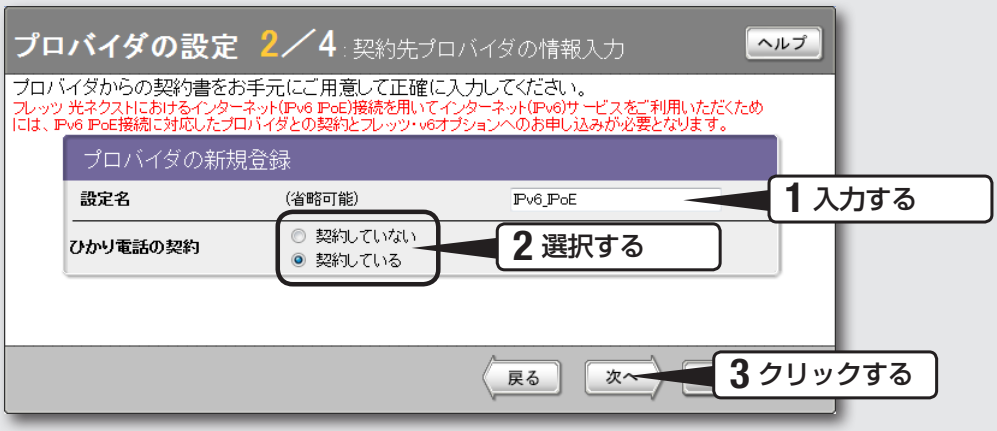
「プロバイダの設定１／４」画面が表示されます。

2　**「フレッツ 光ネクストにおけるインターネット(IPv6 IPoE)接続」をクリックする。**

3　**「次へ」をクリックする。**

「プロバイダの設定２／４」画面が表示されます。

2　プロバイダの情報を指定する



1　設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2　ひかり電話の契約の有無を選択する。

フレッツ 光ネクスト回線の契約内容を確認し、ひかり電話の契約の有無を指定してください。

ご注意

ひかり電話を契約している場合と、契約していない場合とで接続方法が異なります。契約内容に合わせて正しく設定を行ってください。

3　「次へ」をクリックする。

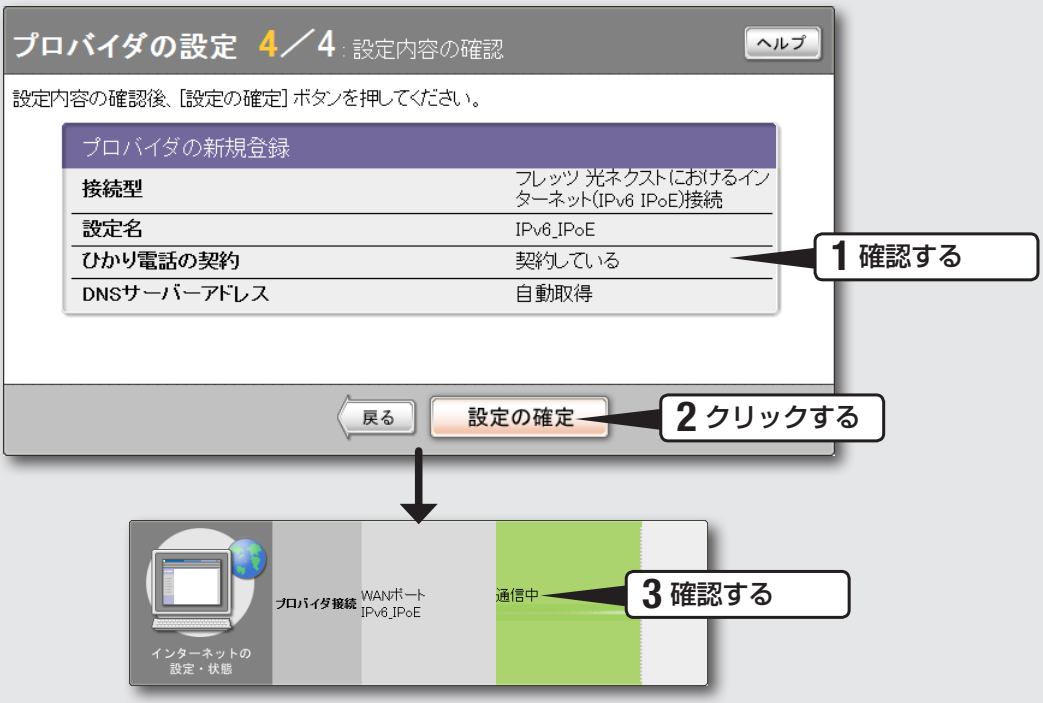
「プロバイダの設定３／４」画面が表示されます。

3　DNSサーバーアドレスの設定をする

1　**「次へ」をクリックする。**

「プロバイダの設定４／４」画面が表示されます。

4　設定内容を確認して、インターネットに接続する



1　**表示された設定内容が、プロバイダから送付された設定資料と合っているかを確認する。**

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2　**「設定の確定」をクリックする。**

表示された確認画面で「トップへ戻る」をクリックすると、本製品は自動的にインターネットに接続して「かんたん設定ページ」のトップページに戻ります。

3　**インターネットに接続しているかを確認する。**

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

▼

設定終了

これでインターネットへの接続設定は終了です

▶インターネットに接続できない場合は

Check 1　本製品とパソコン、ONUの接続を確認してください。
Check 2　83ページの設定内容をもう一度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」(200ページ)を参考にして、問題を解決してください。

フレッツ 光ネクスト回線でインターネットへ接続する

(IPv6 PPPoE方式)

本製品の「かんたん設定ページ」で接続先を設定して、インターネットに接続します。

設定する前に

ご注意

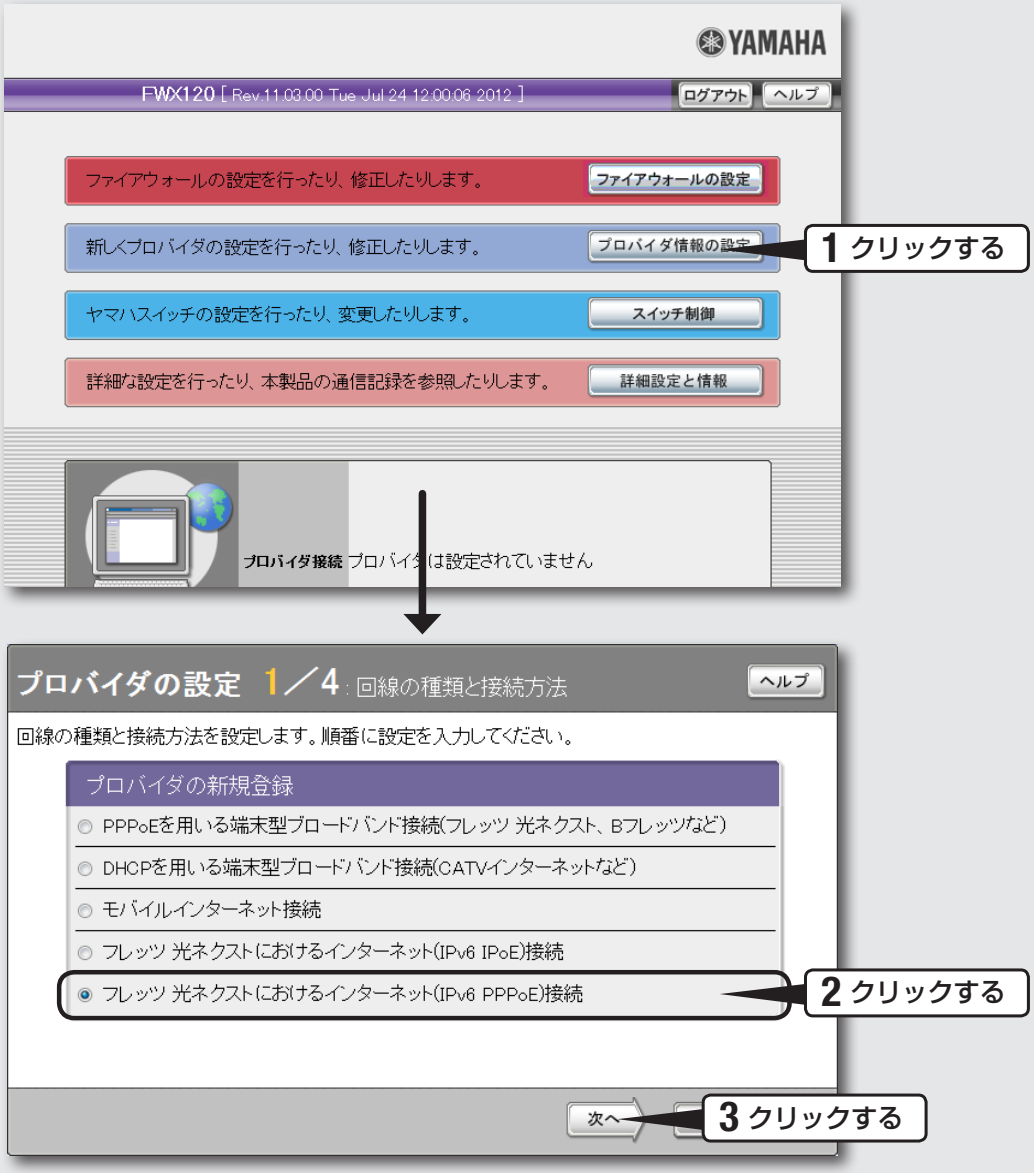
- プロバイダ契約を解除または変更した時は、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティーには十分ご注意の上、お使いください。詳しくは「セキュリティーを強化する」(92 ページ) をご覧ください。
- 本書では Internet Explorer 8 の画面を例に説明します。他の環境の場合は画面表示が多少異なりますが、操作は同じです。
- フレッツ 光ネクストにおけるインターネット (IPv6 PPPoE) 接続を用いてインターネット (IPv6) サービスをご利用いただくためには、IPv6 PPPoE 接続に対応したプロバイダとの契約が必要となります。なお、本製品では、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 等の一部のサービスと同時にご利用いただくことはできません。

プロバイダの設定資料を用意してください

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(DNSサーバーアドレス、ネームサーバー IPアドレス、DNSサーバー IPアドレス)
- デフォルトゲートウェイアドレス

1　接続方法を確認する



1　**「かんたん設定ページ」のトップページで、「プロバイダ情報の設定」をクリックする。**

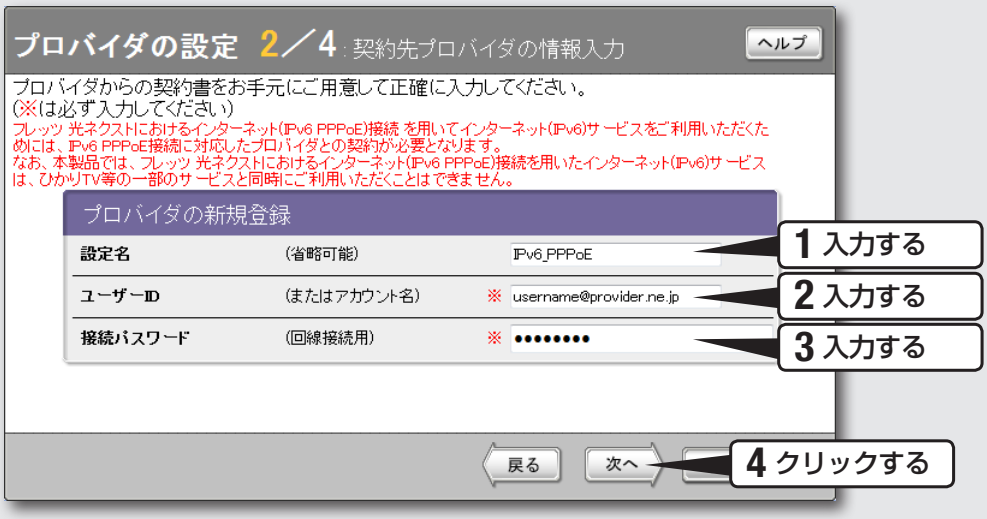
「プロバイダの設定１／４」画面が表示されます。

2　**「フレッツ 光ネクストにおけるインターネット(IPv6 PPPoE)接続」をクリックする。**

3　**「次へ」をクリックする。**

「プロバイダの設定２／４」画面が表示されます。

2　プロバイダの情報を指定する



1　設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2　ユーザー IDを入力する。

プロバイダから指定された、接続用のユーザー IDを入力します。必ず書類を確認して、間違いのないように入力してください。

ご注意

ユーザー IDの後にプロバイダ名を入力する必要があります。詳しくはフレッツ 光ネクストの契約の際にNTTから送付された資料や、プロバイダからの資料をご覧ください。

ユーザー IDがusernameの場合の例：

username@provider.ne.jp

username@aaa.provider.ne.jp（サブドメインが付加される場合）

3　接続パスワードを入力する。

プロバイダ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。半角英数字で、大文字小文字も正確に入力してください。

入力したパスワードの文字は●で表示されます。

4　「次へ」をクリックする。

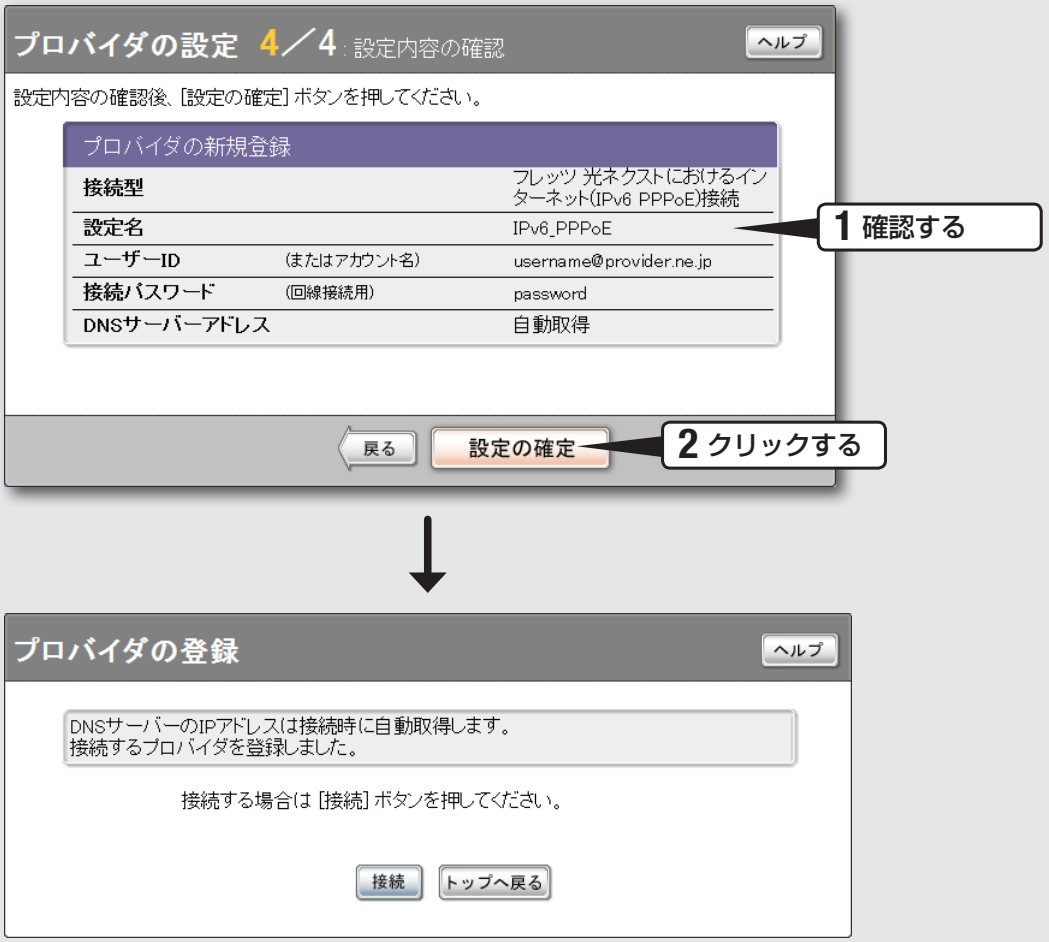
「プロバイダの設定３／４」画面が表示されます。

3　DNSサーバーアドレスの設定をする

1　**「次へ」をクリックする。**

「プロバイダの設定４／４」画面が表示されます。

4　設定内容を確認する



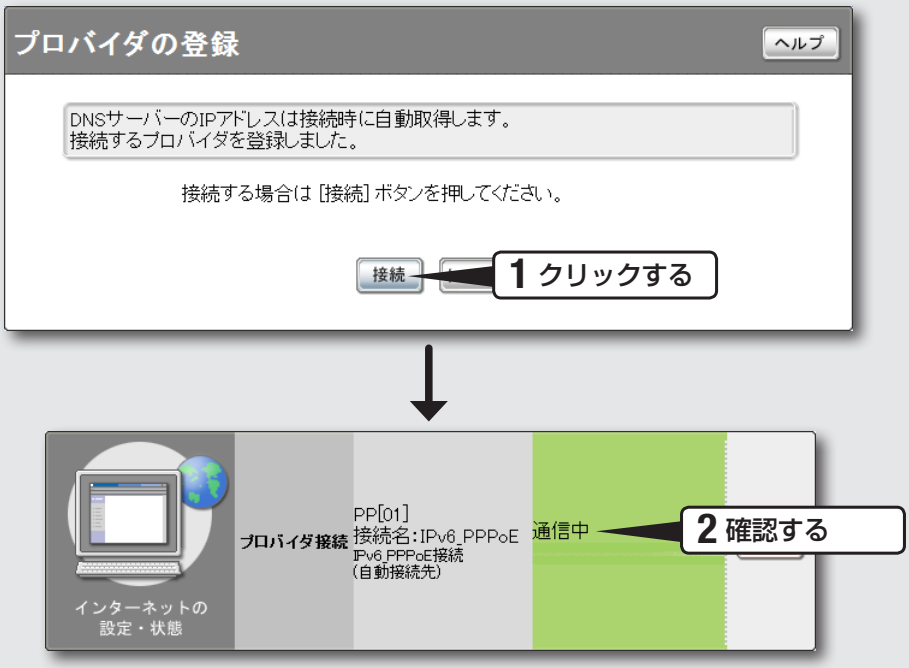
1　**表示された設定内容が、プロバイダから送付された設定資料と合っているかを確認する。**

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示し、正しく設定し直してください。

2　**「設定の確定」をクリックする。**

「プロバイダの登録」画面が表示されます。

5　インターネットに接続する



1　「接続」をクリックする。

インターネットに接続して、「プロバイダへの接続／切断」画面が表示されます。
「トップへ戻る」をクリックすると、「かんたん設定ページ」のトップページに戻ります。

2　インターネットに接続しているかを確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

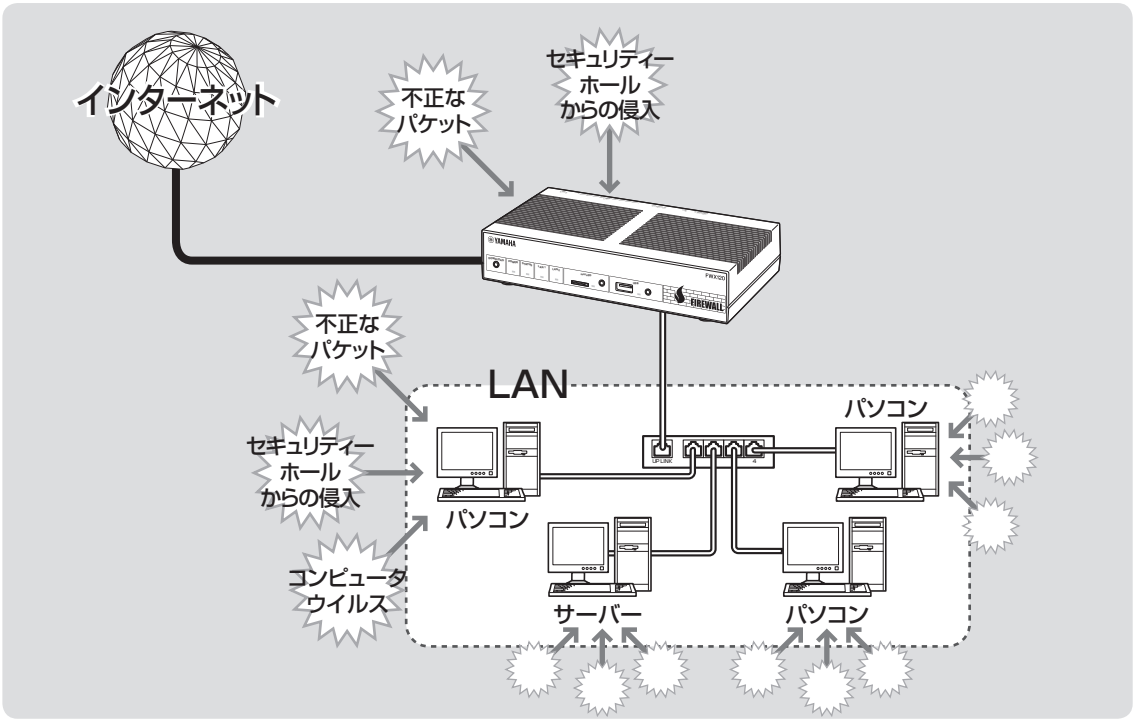
設定終了

これでインターネットへの接続設定は終了です

▶インターネットに接続できない場合は

Check 1　本製品とパソコン、ONUの接続を確認してください。
Check 2　88ページの設定内容をもう一度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」（200ページ）を参考にして、問題を解決してください。

不正アクセスとセキュリティー対策の概要



インターネットからの不正アクセスとは

- インターネットに接続している間は、悪意のある者からパソコンやルーターがアタック(不正なアクセス)されデータを破壊されたり、回線を無断利用されたりする可能性があります。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比較的安全ですが、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。
- また、インターネット経由の不正アクセスだけでなく、コンピュータウイルスによる攻撃にも注意が必要です。
- 本製品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場合、多大なデータ的被害や金銭的被害にあうことも十分に考えられます。本製品のフィルターを設定する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。

グローバルIPアドレスが割り当てられている場合には、特にご注意ください

悪意を持った者がアタックを行う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あ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CATVやADSL、フレッツ・ADSLなどで接続する場合は、十分なセキュリティーの設定をすることをおすすめいたします。

パスワード設定にもご注意ください

本製品にパスワードを設定しない状態で使用することは、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。

不正アクセスに対抗するには

インターネットの不正アクセスは、いくつかの種類に分けられます。それぞれの種類について、以下のように対策してください。

ご注意

- 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設定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。

1. 不正なパケットで侵入するもの

- インターネットへの接続の切断や、グローバルIPアドレスの変更がもっとも効果的です。
- パケットフィルタリング式ファイアウォールで、不要なパケットを通さないことも、ある程度効果があります。
- 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も、整合性のないパケットや不審なActiveX、Javaアプレットをパソコンに受け入れないようにするため、かなり効果があります。ウイルス検知ソフトと組み合わせて使うこともできます。ただしこの場合は、ファイアウォール用サーバーを設けて、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をインストールする必要があります。

本製品での対策

- 自動切断機能を設定することで、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。
- 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(96、99ページ)ことで、その攻撃を防御できることがあります。

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侵入するもの

OSやサーバーソフトウェアのバージョンアップや、適切な設定／運用を行うことで、かなり防止できます。

本製品での対策

- 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(120ページ)。
- 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(96、99ページ)ことで、その攻撃を防御できることがあります。

3. 電子メールの添付ファイルとして侵入するもの(コンピュータウイルス)

添付ファイルを開くことで感染します。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。

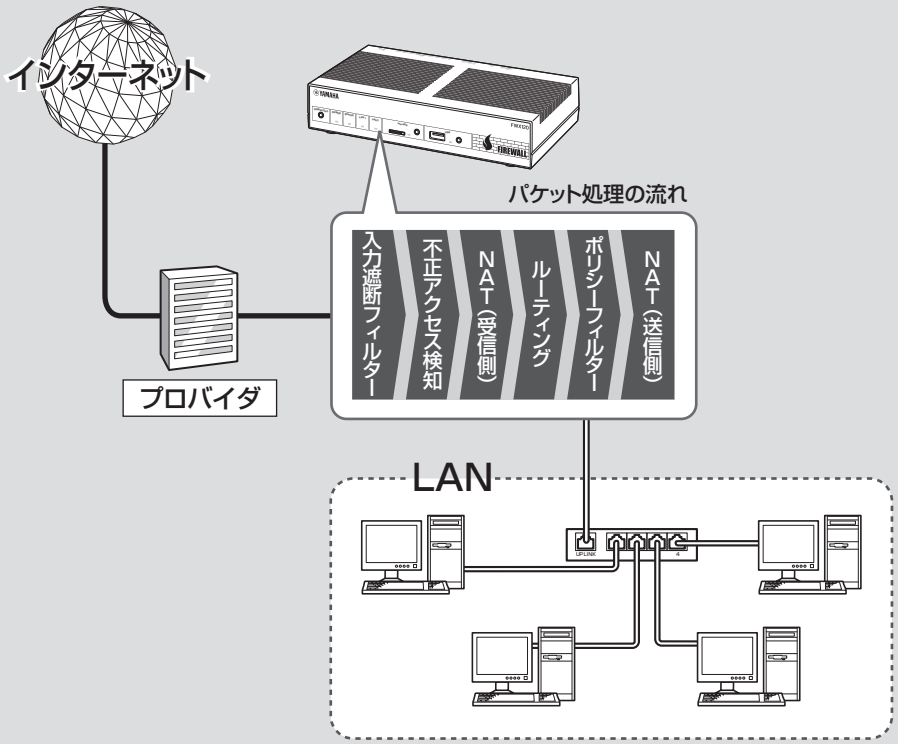
本製品での対策

- 本製品のセキュリティー強化機能は、コンピュータウイルスには効果がありません。
- パソコン用のウイルス検知ソフトウェアを別途ご用意ください。

本製品のセキュリティー機能の概要

外部からの攻撃に対するセキュリティー機能

本製品を接続しているLANを外部の攻撃から保護するために、本製品は各種のフィルター機能と不正アクセス検知機能を搭載しています。



フィルター機能

以下の2つのフィルターを装備しています。

- **入力遮断フィルター（96ページ）**：不要なパケットを早い段階で破棄するために利用します。
- **ポリシーフィルター（99ページ）**：ステートフル・インスペクション方式のフィルタリングを行います（動的フィルター）。コネクションを単位として、アクセス制御を実現できます。

不正アクセス検知機能（107ページ）

受信パケットを入力遮断フィルターでチェックした後に、外部からの攻撃と思われる不正なパケットを検知します。検知したパケットについては、その段階で破棄するか通過させるかを種別ごとに設定できます。

LAN内の端末管理のための セキュリティー機能

クライアントごとにアクセス権を設定する(DHCP認証)(110ページ)

使用を許可されているクライアント(登録済み端末)と許可されていないクライアント(未登録端末)をネットワーク上で区別し、許可の有無によってそれぞれのクライアントがアクセスできるネットワークを制御できます。例えば、登録済み端末は社内・社外すべてのネットワークへアクセスできる一方で、未登録端末は社内の特定セグメントのみへのアクセスに制限されるなど、クライアントごとに異なるアクセス権を設定できます。

特定URLに対するアクセスを制限する(URLフィルター)(114ページ)

管理者側で設定した任意のURLに対して、ネットワーク内のクライアントからのアクセスを制限できます。また、外部のURLフィルタリングサービス事業者のデータベースに問い合わせて、アクセスを制限することもできます。

ファイル共有ソフトウェアの利用把握や制限が可能(不正アクセス検知機能)(107ページ)

不正アクセス検知機能を有効にすることで、「Winny」「Share」が利用するパケットを検出するとともに、該当パケットを破棄し、通信を遮断できます。また、「Winny」「Share」のパケットを検出した場合、不正アクセス検知の履歴に記録するため、「Winny」「Share」を使用した端末を特定することができます。

その他のセキュリティー機能

セキュリティー設定を検証する(118ページ)

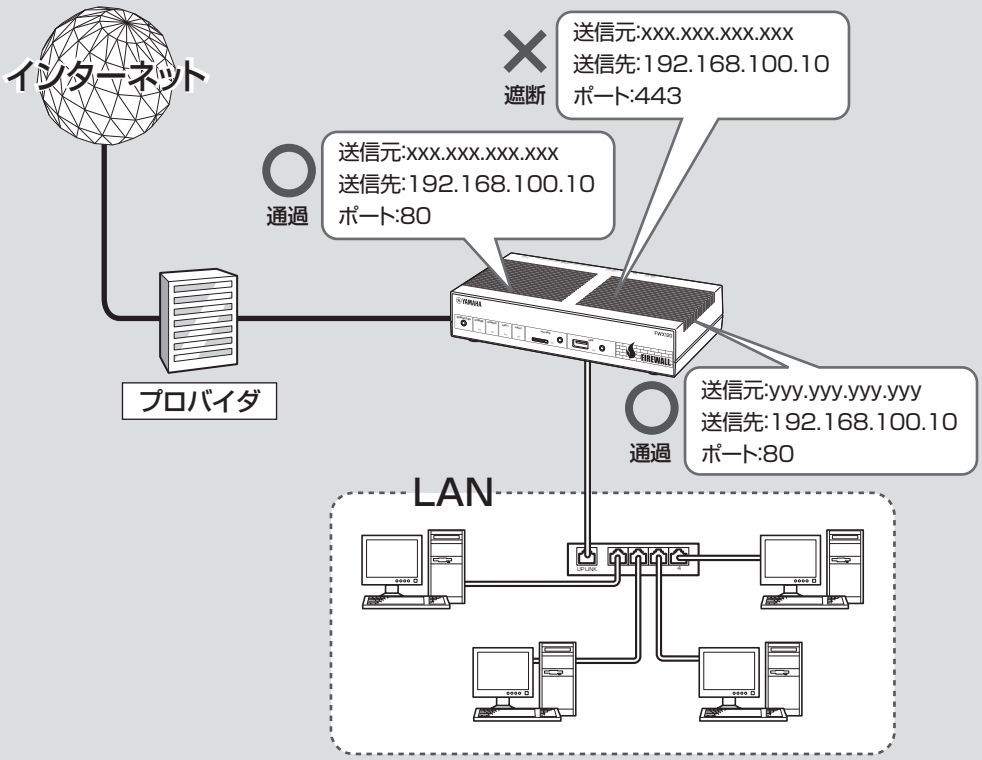
接続設定終了後にセキュリティーの診断機能を使用すると、ポートの開閉状態を診断できます。
詳しい検証項目および内容については、「ポートスキャンを実行してポートの開閉状態を確認する」(118ページ)をご覧ください。

本製品の設定を変更できるホストを制限する(120ページ)

本製品自体のセキュリティーを確保するために、第三者が不正に本製品の設定を変更できないように設定できます。本製品へのアクセス方法としてはWebブラウザ(HTTP)やTELNET、SSHソフトウェアを使用できますが、それぞれについて個別に制限内容を設定できます。

不要なパケットを破棄する（入力遮断フィルター）

入力遮断フィルターを使用すると、始点／終点アドレスやプロトコル、ポート番号を基にして、受信したパケットを破棄・遮断できます。ポリシーフィルターと比較して、本製品の動作にかける負荷をそれほど増やすことなく、不要なパケットを早い段階で処理できます。なお、入力遮断フィルターはインターフェースごとに設定できます。



入力遮断フィルターを登録する

入力遮断フィルターは、インターフェースごとに設定できます。設定したいインターフェースの「入力遮断フィルターの登録」画面で、入力遮断フィルターを登録(インターフェースごとに最大128個まで)します。

ご注意

- 入力遮断フィルターは、フィルターリストの先頭から順に処理を行います。入力遮断フィルターに登録されていない種類のパケットは通過できないため、すべてのパケットを通過させるフィルターを末尾に登録する必要があります。
- ただし入力遮断フィルターが1つも設定されていない場合は、パケットをすべて通過させます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「入力遮断フィルターの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「入力遮断フィルターの設定」の「設定」
▶入力遮断フィルターを設定したいインターフェースの「実行」
(IPv4で接続している場合は「IPv4入力遮断フィルター」の「実行」、IPv6で接続している場合は「IPv6入力遮断フィルター」の「実行」をクリックします。)
▶「IPv4 入力遮断フィルターの一覧」画面の「追加」

入力遮断フィルターのリストを編集する

「入力遮断フィルターの一覧」画面で、登録したフィルターの一覧を確認したり、フィルターの処理順序を変更したりできます。

入力遮断フィルターのリスト中のアイコンをクリックすると、フィルターのリストを編集できます。

- をクリックするとポップアップメニューが表示され、フィルターの内容を編集できます。
  - 既存のフィルターの設定を修正する:「設定」を選びます。
  - フィルターを削除する:「削除」を選びます。
  - 選択したフィルターの上(先に処理)にフィルターを追加する:「上に追加」を選びます。
  - 選択したフィルターの下(後に処理)にフィルターを追加する:「下に追加」を選びます。
- ▲(上に移動)または▼(下に移動)をクリックすると、フィルターの位置を上(先に処理)／下(後で処理)へ移動できます。

設定内容について詳しくは、設定画面の[ヘルプ]をクリックして、表示される説明をご覧ください。

「入力遮断フィルターの一覧」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「入力遮断フィルターの設定」の「設定」
▶入力遮断フィルターを編集したいインターフェースの「実行」
(IPv4で接続している場合は「IPv4入力遮断フィルター」の「実行」、IPv6で接続している場合は「IPv6入力遮断フィルター」の「実行」をクリックします。)

入力遮断フィルターの動作状態を確認する

「入力遮断フィルターのログの表示」画面で、入力遮断フィルターの動作回数を確認できます。

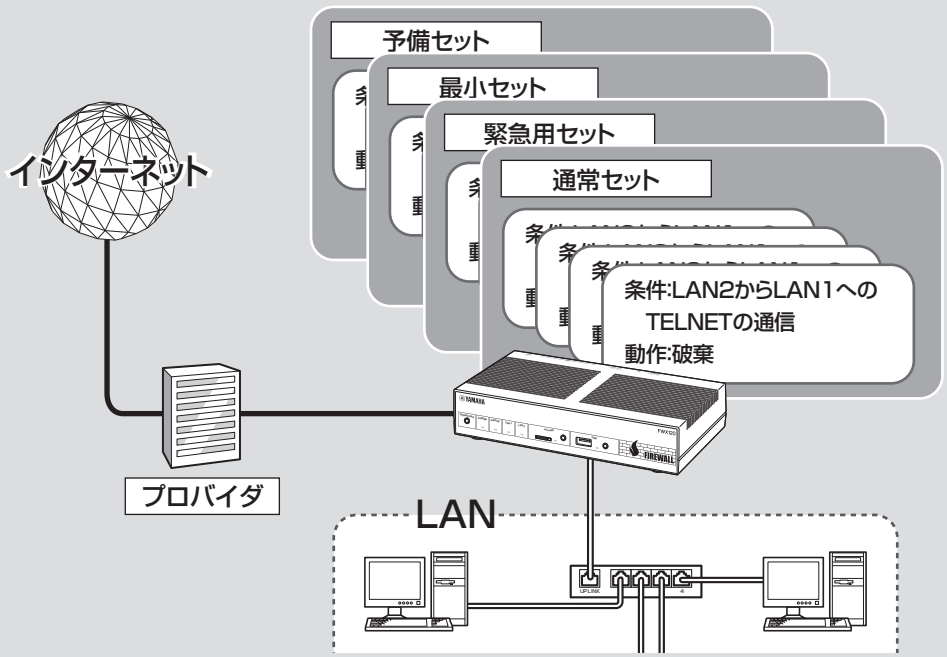
「入力遮断フィルターのログの表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「入力遮断フィルターの情報の表示」の「実行」
▶入力遮断フィルターの情報を確認したいインターフェースの「実行」
(IPv4で接続している場合は「IPv4入力遮断フィルターのログの表示」の「実行」、IPv6で接続している場合は「IPv6入力遮断フィルターのログの表示」の「実行」をクリックします。)

動的フィルターで必要なパケットのみ通過させる(ポリシーフィルター)

「LAN2からLAN1へ抜けるTELNETの通信を破棄する」などのように、人間の思考に近い形で表現された条件と動作の組み合わせを、ポリシーと呼びます。ポリシーフィルターを利用することで、ステートフル・インスペクション方式のフィルタリングを簡単に実現できます。



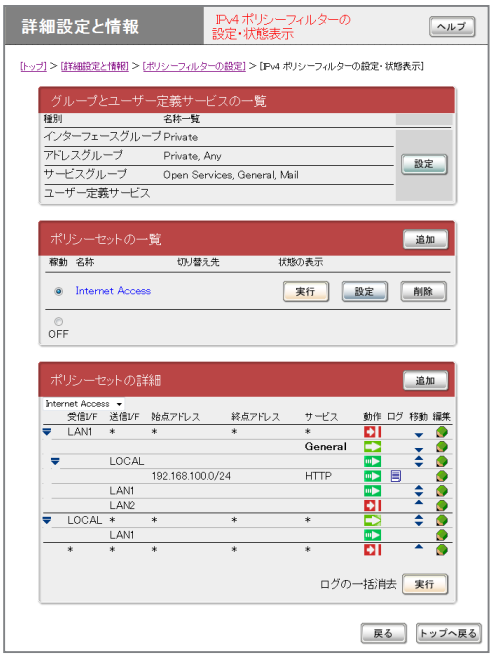
- 受信/送信インターフェースおよび始点/終点アドレス、サービスを指定して、パケット単位ではなくコネクション単位で通過と破棄を指定します。
- 通信状態を監視しながら、必要に応じてフィルターを適用します。例えば「通常はインターネットからLANへのデータはすべて破棄し、LAN側からftpのアクセスが発生した場合のみ戻りのパケットを通過させる」といったように、セッションの状態を反映したフィルターを設定できます。
- ポリシーのリスト(ポリシーセット)は最大で3セットまで登録できます。通常の運用に使用するポリシーセットと、緊急時に最低限のコネクションのみ通過させるポリシーセットなどをあらかじめ登録しておき、状況に応じてポリシーを即座に切り替えたいような場合に便利です。

ヒント

- 同じポリシーを適用したいインターフェースやアドレス、サービスを、グループとして登録することもできます(104ページ)。例えば「WAN」グループに「LAN2、PP1、TUNNEL1」インターフェースを登録しておくことで、ポリシーフィルターの登録の際にインターフェースとして「WAN」グループを指定すれば、LAN2およびPP1、TUNNEL1のインターフェースそれぞれについて個別に登録する手間が省けます。
- サービスとは基本的に各アプリケーションに対応する概念で、TELNET、SMTP、POP、FTP、WWWなどの値を取ります。なお、プロトコルとポートを指定して任意のサービス(ユーザー定義サービス)を登録して、ポリシーフィルターの登録の際に指定するサービスとして使用することもできます(106ページ)。
- 登録済み端末(110ページ)のIPアドレスのグループに対してポリシーフィルターを適用して、登録済み端末の一部だけに特定ネットワーク(社内セキュリティー重視ネットワークなど)へのアクセスを許可する、といったアクセス管理も実現できます。

ポリシーセットの内容を確認する／編集する

「ポリシーフィルターの設定・状態表示」画面で、登録したポリシーの一覧を確認したり、ポリシーの処理順序や階層構造を変更したりできます。



ポリシーのリスト中のアイコンをクリックすると、ポリシーのリストを編集できます。

- をクリックするとポップアップメニューが表示され、ポリシーの内容を編集できます。
  - 既存のポリシーの設定を修正する：「設定」を選びます。
  - ポリシーを削除する：「削除」を選びます。
  - 選択したポリシーと同一階層にポリシーを追加する：「並列に追加」を選びます。詳しくは「同一階層にポリシーを追加する」（102ページ）を御覧ください。
  - 選択したポリシーの下位階層にポリシーを追加する：「配下に追加」を選びます。詳しくは「下位階層にポリシーを追加する」（102ページ）を御覧ください。
  - ポリシーを一時的に無効にする／有効にする：「無効化」または「有効化」を選びます。
- ▲（上に移動）または▼（下に移動）をクリックすると、ポリシーの位置を上（先に処理）／下（後で処理）へ移動できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ポリシーフィルターの設定・状態表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）

ポリシーを追加する

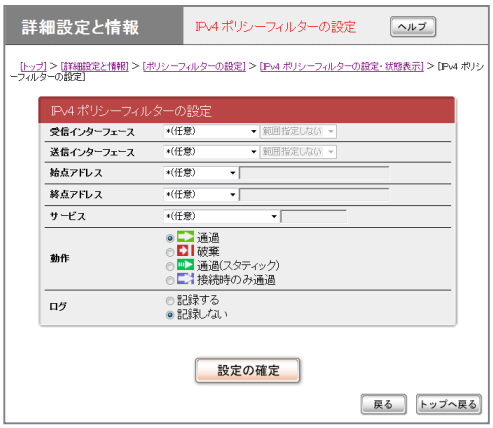
設定したいインターフェースの「ポリシーフィルターの設定状態表示」画面で、ポリシーを登録（ポリシーセットごとに最大256個まで）します。

ご注意

- ポリシーは、ポリシーリストの先頭から順に処理を行います。ポリシーに登録されていない種類のコネクションは通過できないため、すべてのコネクションを通過させるポリシーを末尾に登録する必要があります。
- ただしポリシーが１つも設定されていない場合は、すべてのコネクションを通過させます。

ヒント

ポリシーを追加する際に、グループという単位でインターフェースやアドレス、サービスをまとめて指定することもできます。詳しくは、「インターフェースやアドレス、サービスをグループ化して管理する」（104ページ）をご覧ください。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ポリシーフィルターの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーを追加したいインターフェースの「実行」（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）
▶「ポリシーセット詳細」欄でポリシーを設定したいポリシーセットを選択し「追加」

階層を指定してポリシーを追加する場合は

「ポリシーフィルターの設定・状態表示」画面で、上位階層のポリシーの条件を下位階層のポリシーで絞り込むようなフィルタリングを実現できます（最大4階層まで）。
例えば、WWWのアクセスを許可する一方で、下位階層で例外条件（始点アドレスが172.16.0.1であれば拒否する）を追加するというように、条件を絞り込んで例外的なポリシーを追加したい場合などに便利です。

同一階層にポリシーを追加する

ポリシーを追加したい位置の1つ上の行で、をクリックしてから「並列に追加」を選びます。
「ポリシーフィルターの設定」画面でポリシーの設定が終わると、をクリックした行の1つ下に、設定したポリシーが同じ階層で追加されます。

ご注意

この方法でポリシーを追加した場合は同じ階層でポリシーが追加されるので、条件の絞り込みとしては機能しません。

下位階層にポリシーを追加する

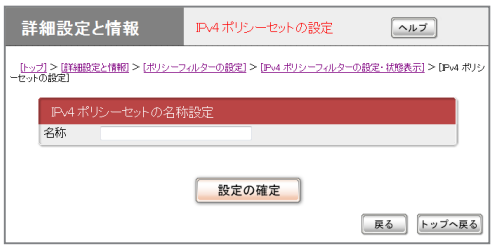
下位階層にポリシーを追加したいポリシーの行で、をクリックしてから「配下に追加」を選びます。
「ポリシーフィルターの設定」画面でポリシーの設定が終わると、をクリックした行の1つ下に、設定したポリシーが下位階層に追加されます。

複数のポリシーセットを管理する

ポリシーのリスト（ポリシーセット）は最大で3セットまで登録できます。通常の運用に使用するポリシーセットと、緊急時に最低限のコネクションのみ通過させるポリシーセットなどをあらかじめ登録しておき、状況に応じてポリシーを即座に切り替えたいような場合に便利です。

ポリシーセットを追加する

「ポリシーセットの設定」画面で、ポリシーセットを追加できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

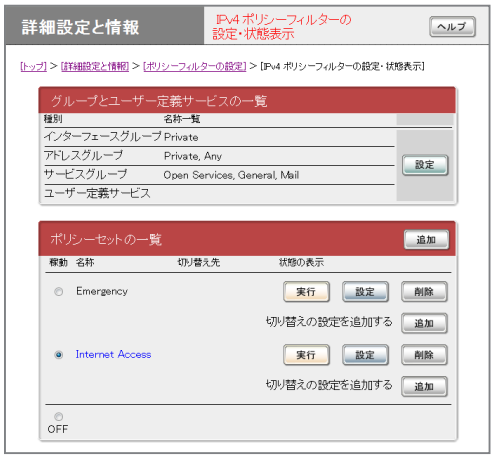
「ポリシーセットの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）
▶「ポリシーセットの一覧」の「追加」

ポリシーセットを手動で切り替える

「ポリシーフィルターの設定・状態表示」画面で、有効にしたいポリシーセットの「稼働」欄をクリックして選びます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ポリシーフィルターの設定・状態表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

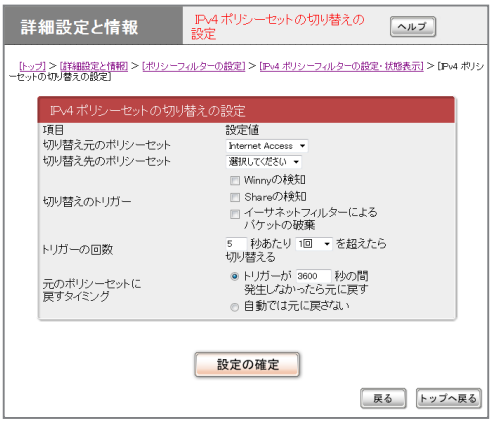
▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）

ポリシーセットを自動で切り替えるための条件を設定する

「ポリシーセットの切り替えの設定」画面で、ポリシーセットを自動的に切り替えるための条件を設定できます。

ご注意

「ポリシーセットの切り替えの設定」画面は、複数のポリシーセットを登録している場合にのみ表示できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ポリシーセットの切り替えの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）
▶「ポリシーセットの一覧」欄の条件を設定したいポリシーセットの「追加」

インターフェースやアドレス、サービスをグループ化して管理する

任意のインターフェースやアドレス、サービスをそれぞれグループとして登録・管理できます。登録したグループを指定するだけで、複数のインターフェースやアドレス、サービスに対して同一のポリシーを適用できるようになります。個別にポリシーを適用する必要がなくなるため、ポリシー管理の手間を軽減できます。

ヒント

- サービスとは基本的に各アプリケーションに対応する概念で、TELNET、SMTP、POP、FTP、WWWなどの値を取ります。
- プロトコルとポートを指定して任意のサービス(ユーザー定義サービス)を登録して、ポリシーフィルターの登録の際に指定するサービスとして使用することもできます(106ページ)。

例:「LAN2、PP1、TUNNEL1」インターフェースを「WAN」グループとして登録した場合

ポリシー設定の際にインターフェースとして「WAN」グループを指定するだけで、LAN2およびPP1、TUNNEL1のインターフェースについて同一のポリシーを適用できます。

登録できるグループの種類

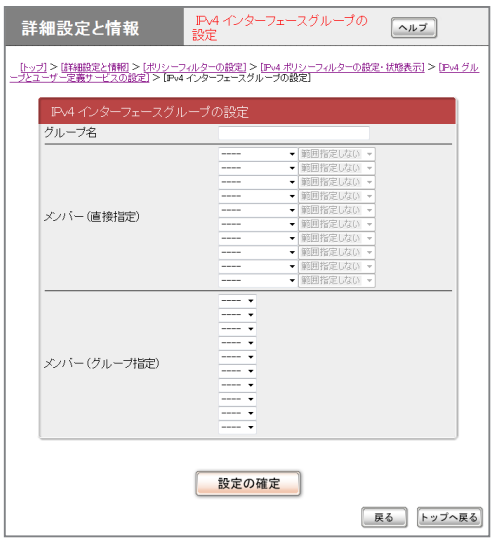
本製品で登録できるグループは、インターフェースグループ、アドレスグループ、サービス(プロトコル)グループの3種類です。それぞれの種類のグループについて、最大100個まで定義できます。

ご注意

- グループを階層化して定義することもできますが、階層の深さは2階層までです。
- アドレスグループの中にサービスグループを含めるなど、異なる種類のグループを混在させることもできません。

インターフェースグループを登録する

「インターフェースグループの設定」画面で登録します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

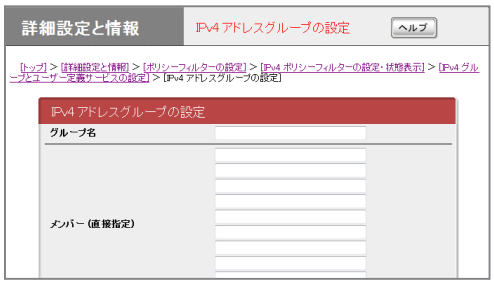
「インターフェースグループの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
(IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。)
▶「グループとユーザー定義サービスの一覧」の「設定」
▶「インターフェースグループの設定」の「追加」

アドレスグループを登録する

「アドレスグループの設定」画面で登録します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

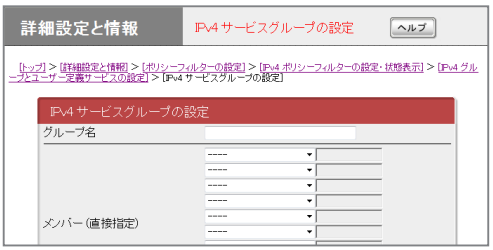
「アドレスグループの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）
▶「グループとユーザー定義サービスの一覧」の「設定」
▶「アドレスグループの設定」の「追加」

サービスグループを登録する

「サービスグループの設定」画面で登録します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「サービスグループの設定」画面を開くには

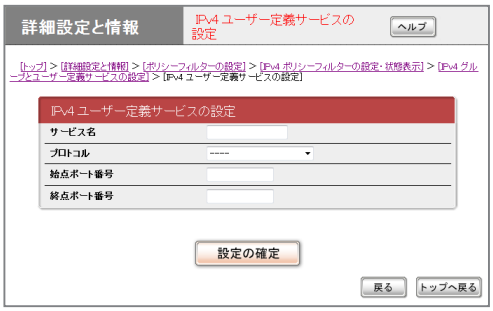
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
（IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。）
▶「グループとユーザー定義サービスの一覧」の「設定」
▶「サービスグループの設定」の「追加」

ユーザー定義サービスを登録する

あらかじめ本製品に登録されているサービス(システム定義サービス)の他に、独自のサービスを追加することもできます(ユーザー定義サービス)。登録したユーザー定義サービスはポリシーフィルターで指定するサービスとして使用するだけでなく、サービスグループのメンバーとして指定することもできます。

ユーザー定義サービスを登録するには、「ユーザー定義サービスの設定」画面でサービスの名称とプロトコル、ポートを指定します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

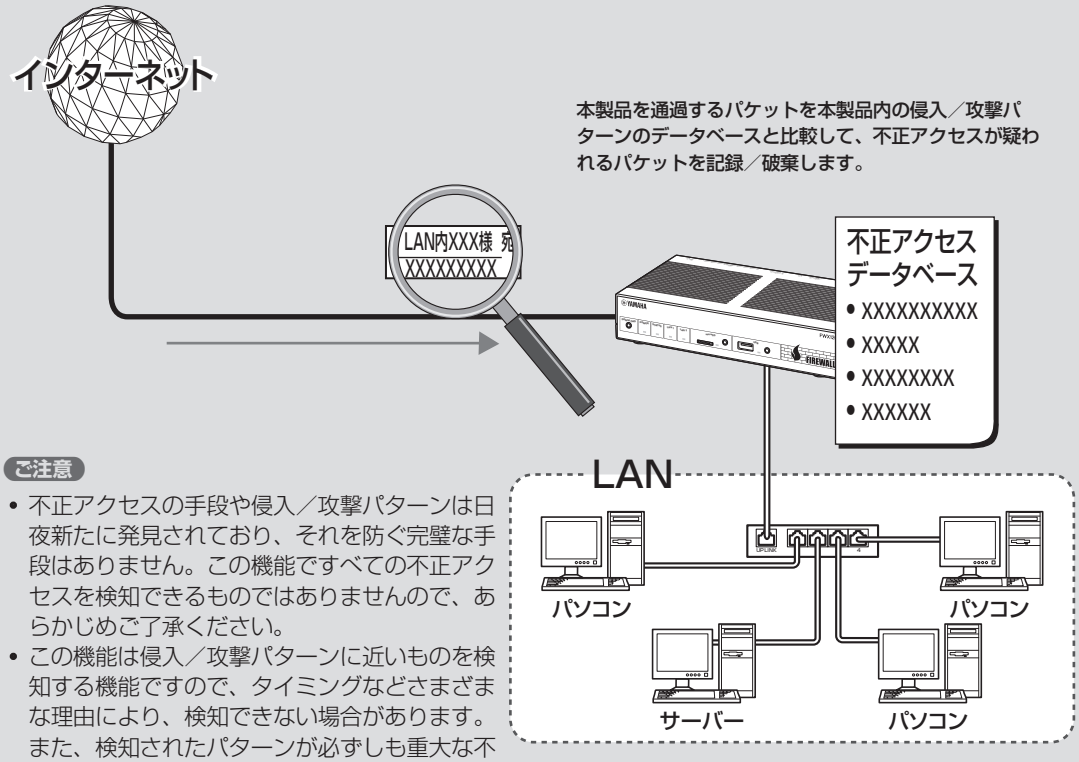
「ユーザー定義サービスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ポリシーフィルターの設定」の「設定」
▶ポリシーフィルターを確認したいインターフェースの「実行」
(IPv4で接続している場合は「IPv4ポリシーフィルターの設定・状態表示」の「実行」、IPv6で接続している場合は「IPv6ポリシーフィルターの設定・状態表示」の「実行」をクリックします。)
▶「グループとユーザー定義サービスの一覧」の「設定」
▶「ユーザー定義サービスの設定」の「追加」

不正アクセスを検出して警告する

不正アクセス検知機能(IDS、Intrusion Detection System)は、インターネットからの侵入や攻撃などを検出して、警告する機能です。検知情報を元に不審な発信元やアプリケーションを通さないフィルターを設定することで、よりセキュリティーを高めることができます。



ご注意

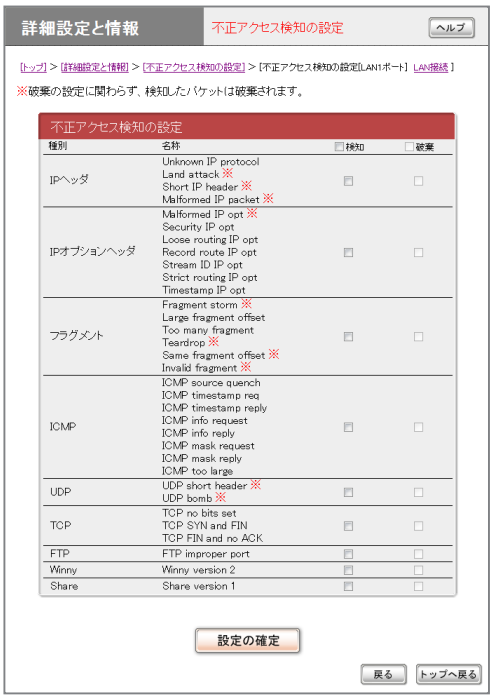
- 不正アクセスの手段や侵入／攻撃パターンは日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入／攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、検知されたパターンが必ずしも重大な不正アクセスであることを判断するものではありません。あくまでセキュリティー管理の目安であることをご理解の上、ご利用ください。
- 本機能は各インターフェースに適用できます。
- 本機能を使用すると、インターネットなどへのアクセス速度が遅くなります。

不正アクセス検知機能を設定する

「不正アクセス検知の設定」画面で、DHCP型やPPPoE型接続などの接続種別ごとに、検知するパケットの種類や検知時の処理方法(破棄または通過)を設定できます。

ご注意

不正アクセス検知機能は各インターフェースに適用できますが、適用数によってはインターネットなどへのアクセス速度が遅くなります。



この機能で検知できる不正アクセスの種類および設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「不正アクセス検知の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「不正アクセス検知の設定」の「設定」
▶不正アクセス検知機能を設定したいインターフェースの「設定」

不正アクセス検知履歴を確認する

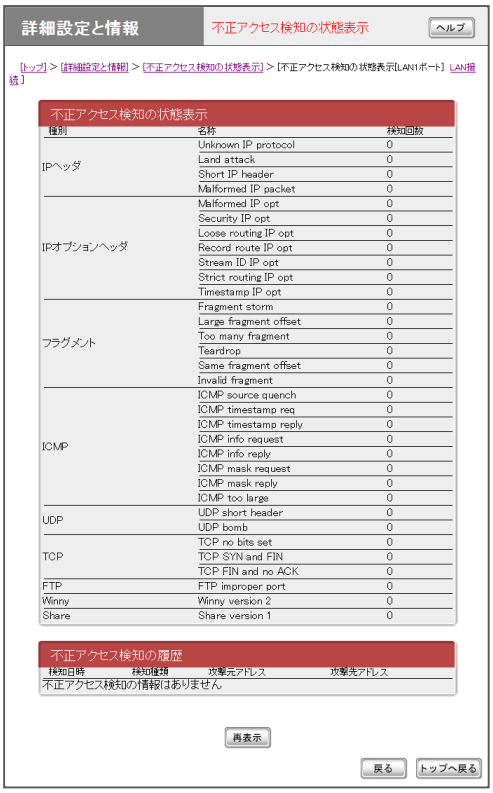
「不正アクセス検知の状態表示」画面で、不正アクセスの検知回数と検知履歴を確認できます。

ご注意

- 不正アクセスの手段や侵入／攻撃パターンは日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入／攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、パターンが検知された場合でも、それが重大な不正アクセスであるとは限りません。あくまでセキュリティー管理の目安であることをご理解の上、ご利用ください。

ヒント

不正アクセスの検知結果は、InfoレベルのSyslogにも出力されます(194ページ)。



「不正アクセス検知の状態表示」画面を開くには

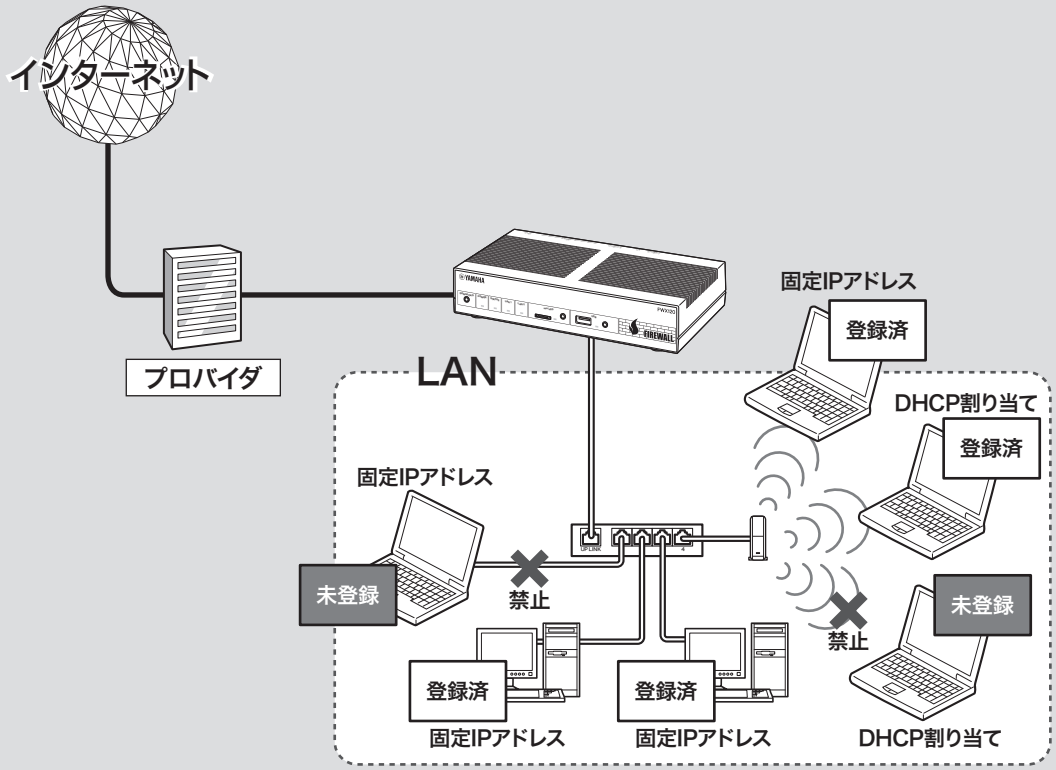
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「不正アクセス検知の状態表示」の「実行」
▶不正アクセス検知の状態を表示したいインターフェースの「実行」

登録された端末の通信のみを許可する（DHCP認証）

使用許可したクライアント（登録済み端末）のみ、本製品を経由して通信できるように設定できます。また、登録済み端末のIPアドレスのグループに対してポリシーフィルター（99ページ）を適用することで、登録済み端末の一部だけに特定ネットワーク（社内セキュリティー重視ネットワークなど）へのアクセスを許可する、といったアクセス管理も実現できます。

- MACアドレスを本製品にあらかじめ登録しておくことで、DHCPによって割り当てられるIPアドレスを登録済み端末用に予約します。
- 固定IPアドレスを割り当てられている端末も、登録済み端末として管理できます。



ご注意

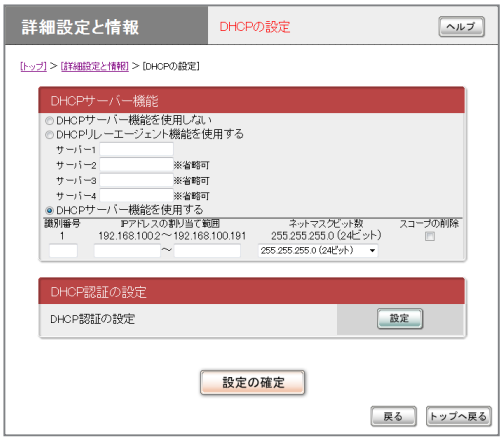
DHCP認証機能はMACアドレスを用いたフィルタリングを併用しているため、未登録端末に固定IPアドレスを設定した場合でも、許可されない通信はできません。

ヒント

- クライアントが接続する1つの物理ネットワークで、2つの論理ネットワーク（プライマリネットワークとセカンダリネットワーク）を構成できます。この状態でdhcp scope lease typeコマンドを使用して、登録済み端末にはプライマリネットワークに対応するIPアドレス、未登録端末にはセカンダリネットワークに対応するIPアドレスを割り当てて、登録済み端末と未登録端末を区別することもできます。
- この機能を利用することで、登録済み端末は社内・社外すべてのネットワークへアクセスできる一方で、未登録端末は社内の特定セグメントのみへのアクセスに制限するなど、クライアントごとに異なるアクセス権を設定することが可能になります。
- dhcp scope lease typeコマンドについて詳しくは、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

DHCPサーバーを設定する

DHCP認証機能を利用するには、本製品のDHCPサーバー機能が動作している必要があります。「DHCPの設定」画面の「DHCPサーバー機能」欄で、DHCPサーバー機能の動作を設定できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DHCPの設定」画面を開くには

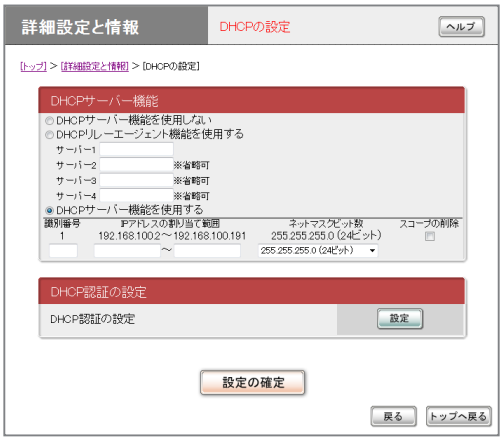
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「DHCPの設定」の「設定」

DHCPサーバー機能でIPアドレスを割り当てている端末をまとめて登録する

端末を1台ずつ登録する必要がなく、現状の割り当て状態をDHCP認証機能の端末登録にまとめて利用できるので便利です。

1 「DHCPの設定」画面の「DHCP認証の設定」欄で「設定」をクリックする。



「DHCPの設定」画面を開くには

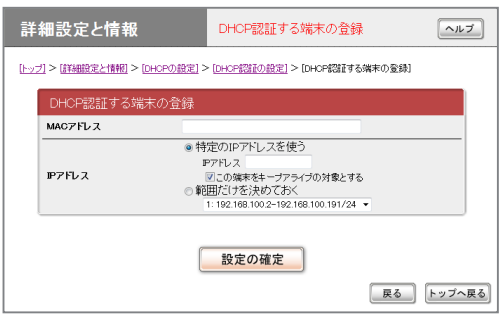
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「DHCPの設定」の「設定」

2 「DHCP認証の設定」画面の「端末の管理」欄で「適用」を選択してから、「設定の設定」をクリックする。

端末を1台ずつ登録する

DHCPを使用しない端末(固定IPアドレスを割り当てている既存サーバーなど)や追加導入した端末を登録する場合などは、1台ずつ端末を登録することもできます。「DHCP認証する端末の登録」画面で、端末のMACアドレスおよびIPアドレスの割り当てを登録します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DHCP認証する端末の登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「DHCPの設定」の「設定」
▶「DHCP認証の設定」の「設定」
▶「端末の管理」欄の「追加」

未登録端末の扱いを指定する

「DHCP認証の設定」画面の「未登録端末の取り扱いポリシーの設定」欄で、未登録端末に対するIPアドレス割り当てポリシーを指定します。

ご注意

設定操作を行うパソコンを含む、LAN1側の端末を登録してから未登録端末の扱いを設定してください。LAN1側の端末が正しく登録されていない状態で未登録端末の扱いの設定を変更すると、設定画面にアクセスできなくなる場合があります。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DHCP認証の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「DHCPの設定」の「設定」
▶「DHCP認証の設定」の「設定」

端末の接続状態を確認する

「DHCP認証の設定」画面の「端末の管理」欄で、端末の現在の状態を確認できます。

端末の状態について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DHCP認証の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

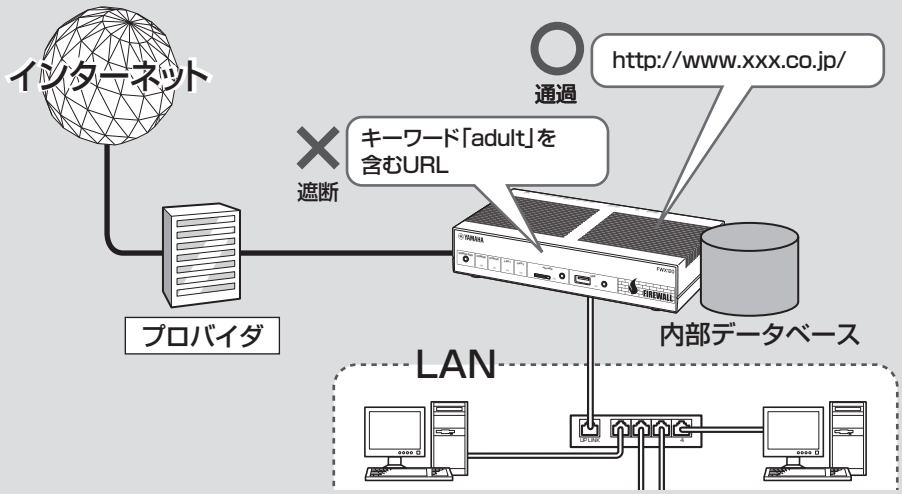
▶トップページの「詳細設定と情報」
▶「DHCPの設定」の「設定」
▶「DHCP認証の設定」の「設定」

Webアクセスを制限する（URLフィルター）

本製品では、内部データベース参照型および外部データベース参照型の2種類のURLフィルター機能を利用して、ネットワーク内のクライアントからのWebアクセスを制限できます。

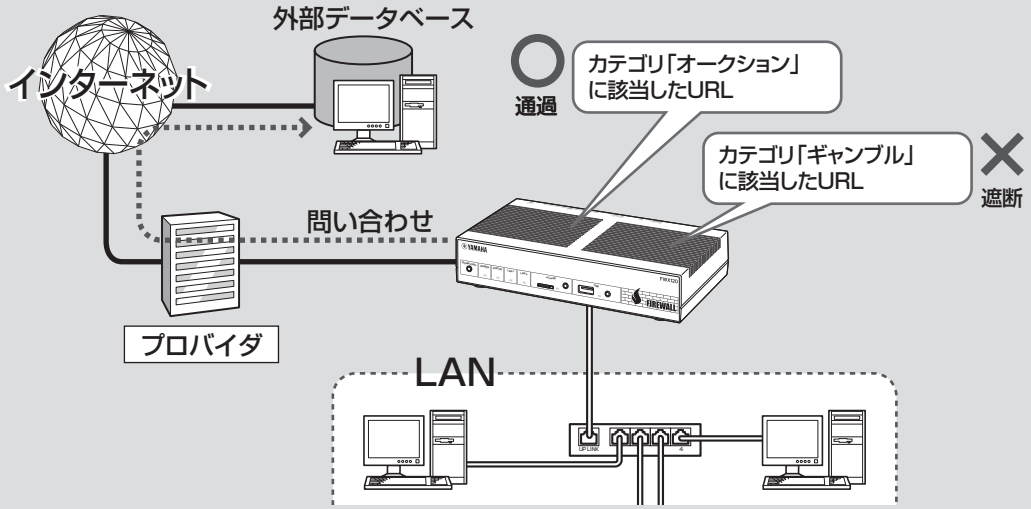
内部データベース参照型URLフィルター

管理者側で設定した任意のURLの全部または一部をキーワードとして、そのキーワードと一致した文字列を含むURLへのアクセスを制限します。また、本製品をプロキシサーバーとして動作させることでHTTPSによるWebアクセスを制限します。



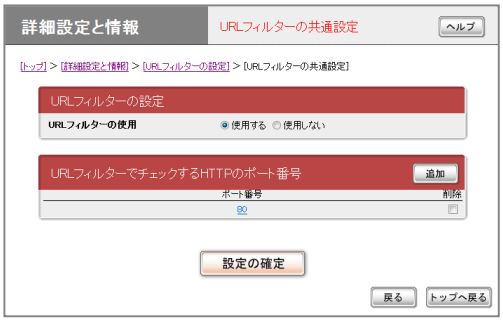
外部データベース参照型URLフィルター

外部のURLフィルタリングサービス事業者のデータベースに問い合わせて、通知された当該URLのカテゴリ分類でアクセスを制限します。



URLフィルターを設定する

「URLフィルターの共通設定」画面で、URLフィルターを使用するために設定を変更します。また、URLフィルターの対象となるHTTP通信が使用するポート番号を指定できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

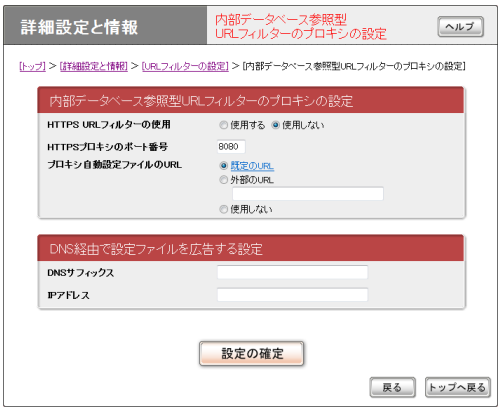
「URLフィルターの共通設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「URLフィルターの設定」の「設定」
▶「URLフィルターの共通設定」の「設定」

内部データベース参照型URLフィルターのプロキシを設定する

「内部データベース参照型URLフィルターのプロキシの設定」画面で、内部データベース参照型URLフィルターでHTTPSによるWebアクセスを制限するためのプロキシサーバーを設定できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「内部データベース参照型URLフィルターのプロキシの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「URLフィルターの設定」の「設定」
▶「内部データベース参照型URLフィルターのプロキシの設定」の「設定」

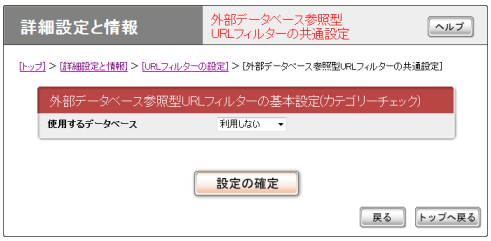
外部データベース参照型URLフィルターを設定する

「外部データベース参照型URLフィルターの共通設定」画面で、URLフィルターで使用する外部データベースを設定できます。

ヒント

内部データベース参照型URLフィルターと外部データベース参照型URLフィルターを、併用することもできます。

- 先に内部データベース参照型URLフィルターによるチェックが行われます。
- 内部データベース参照型URLフィルターのキーワードと一致しなかったURLについては、続いて外部データベース参照型URLフィルターでのチェックが行われます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「外部データベース参照型URLフィルターの共通設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「URLフィルターの設定」の「設定」
▶「外部データベース参照型URLフィルターの共通設定」の「設定」
▶「使用するデータベース」の「設定」

本製品で利用できるフィルタリングサービスについて

本製品で利用できるフィルタリングサービスおよび導入環境、価格などについて詳しくは、ヤマハネットワーク周辺機器ホームページ（http://jp.yamaha.com/products/network/、http://www.rtpro.yamaha.co.jp/）をご覧の上、フィルタリングサービス事業者、もしくはフィルタリングサービスのお取扱い事業者まで直接お問い合わせください。

インターフェースごとにURLフィルターを設定する

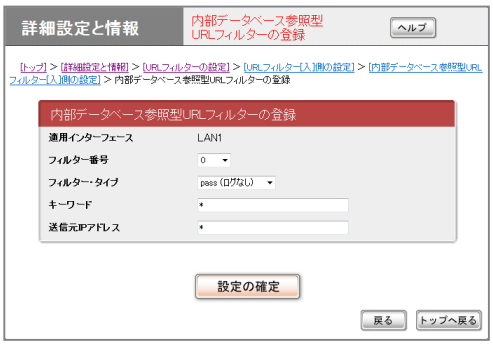
本製品の各インターフェースのIN/OUTそれぞれの方向について、URLフィルターの条件を個別に設定できます。

ご注意

本製品のURLフィルターは、LAN1インターフェースのINやLAN2インターフェースのOUTなど、本製品に接続されたクライアントから本製品の外のネットワークへ向かう方向に対して設定してください。

内部データベース参照型URLフィルターを設定する

「内部データベース参照型URLフィルターの登録」画面で、アクセス制限の対象となるキーワードやURLを登録します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「内部データベース参照型URLフィルターの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

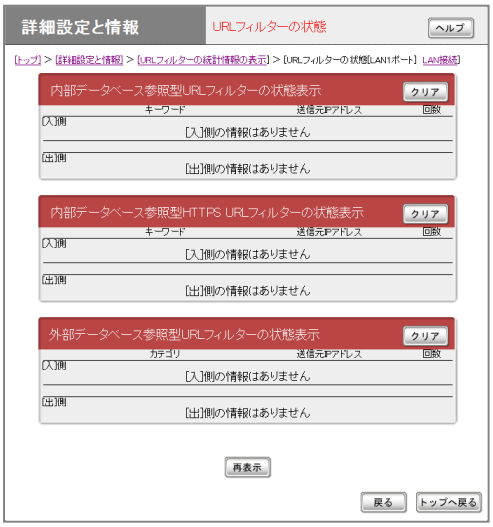
▶トップページの「詳細設定と情報」
▶「URLフィルターの設定」の「設定」
▶「URLフィルターの設定インターフェース」欄のURLフィルターを登録したいインターフェースの「設定」
▶「内部データベース参照型URLフィルター」の「設定」
▶使用するURLフィルターの「追加」

URLフィルターの動作状態を確認する

「URLフィルターの状態」画面で、URLフィルターの動作回数を確認できます。

ヒント

URLフィルターの動作は、NoticeレベルのSyslogにも出力されます（194ページ）。



「URLフィルターの状態」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

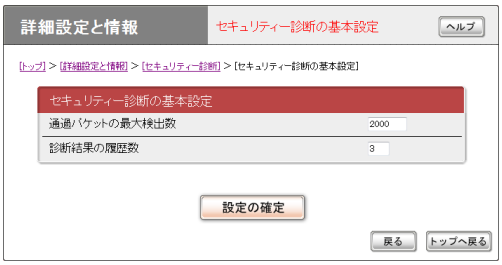
▶トップページの「詳細設定と情報」
▶「URLフィルターの統計情報の表示」の「実行」
▶URLフィルターの状態を表示したいインターフェースの「実行」

ポートスキャンを実行して ポートの開閉状態を確認する

本製品に対してポートスキャンを実行し、各種フィルターでポートの開閉状態が適切に設定されているかを確認できます。IN/OUT方向の設定をまとめて検証する「ワンクリック診断」と、インターフェースやプロトコル、送信元アドレスなどの情報を指定して検証する「カスタム診断」の2種類があります。目的に合わせて使い分けると便利です。

セキュリティー診断の基本設定を行う

「セキュリティー診断の基本設定」画面で、通過パケットの最大検出数や診断結果の履歴数を設定できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「セキュリティー診断の基本設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「セキュリティー診断」の「実行」
▶「セキュリティー診断の基本設定」の「設定」

IN/OUT方向の設定をまとめて検証する（ワンクリック診断）

「ワンクリック診断」画面で検証します。初期設置の際など、設定全体に問題がないか検証する際に便利です。

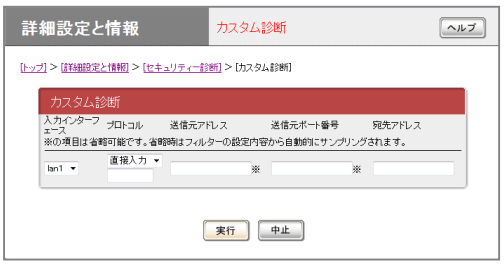
「ワンクリック診断」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「セキュリティー診断」の「実行」
▶「ワンクリック診断」の「実行」

インターフェースやプロトコル、送信元アドレスなどの情報を指定して検証する（カスタム診断）

「カスタム診断」画面で検証します。ネットワークに新しいサービスを導入したり、ネットワーク構成を変更したりした場合に、特定の問題を想定して検証する際に便利です。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

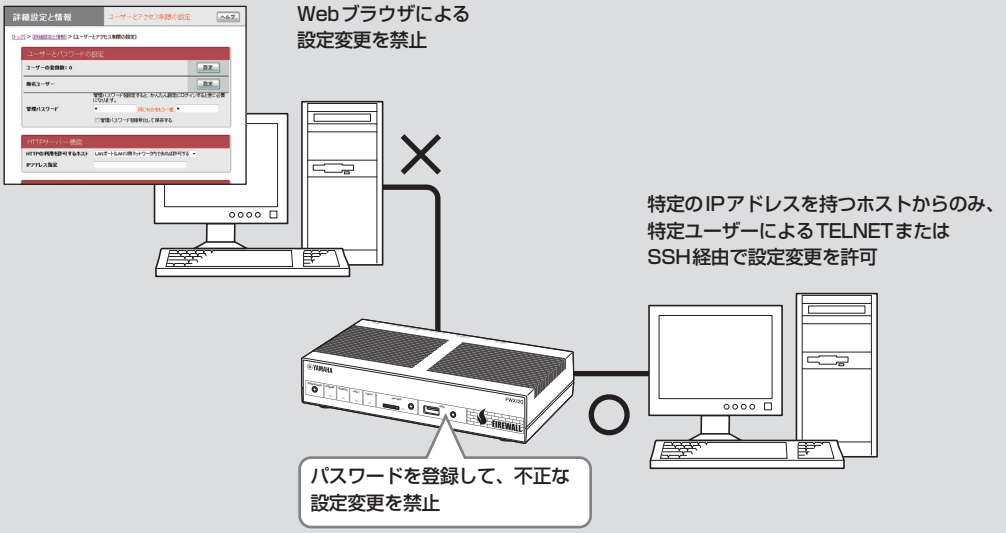
「カスタム診断」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「セキュリティー診断」の「実行」
▶「カスタム診断」の「実行」

本製品の設定を変更できるホストを制限する

本製品には、本製品自体のセキュリティーを確保するために、パスワード機能や利用ホスト制限機能を装備しています。これらの機能を利用することで、第三者が不正に本製品の設定を変更できないように設定できます。本製品へのアクセス方法としてはWebブラウザ(HTTP)やTELNET、SSH、SFTPソフトウェアを使用できますが、それぞれについて個別に制限内容を設定できます。



個別のサービスごとに制限を設定する

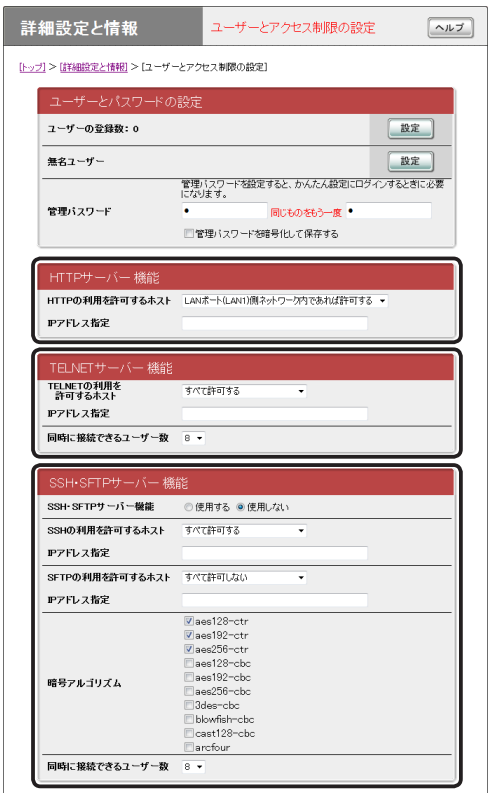
「ユーザーとアクセス制限の設定」画面で、Webブラウザ(HTTP)やTELNET、SSH、SFTPソフトウェアを使って本製品の設定を変更できるホストを制限できます。個別のサービスごとに本製品にアクセスできるホストのIPアドレスを制限するだけでなく、同時接続ユーザー数を制限することもできます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザーとアクセス制限の設定」画面を開くには

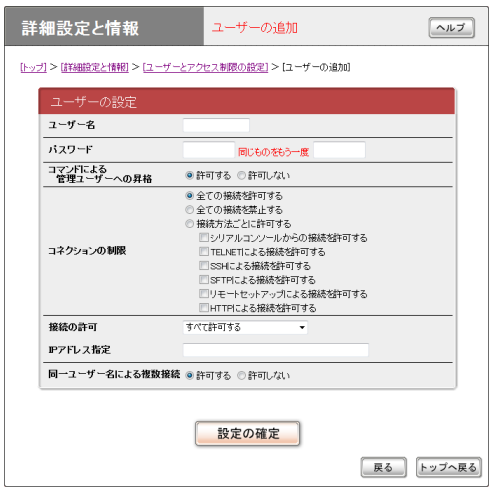
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」



本製品にログインするユーザーを登録する

「ユーザーの追加」画面で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できます。設定に使用できるサービスなど、それぞれのユーザーごとに詳細な権限を指定することもできるため、きめ細やかなアクセス制限を行いたい場合に便利です。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

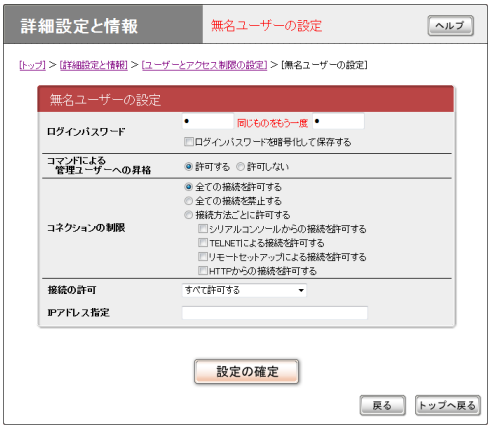
「ユーザーの追加」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」
▶「ユーザーの登録数」欄の「設定」

無名ユーザーのアクセスを制限する

「無名ユーザーの設定」画面で、無名ユーザーを使用する場合のアクセス制限を設定できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「無名ユーザーの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」
▶「無名ユーザー」欄の「設定」

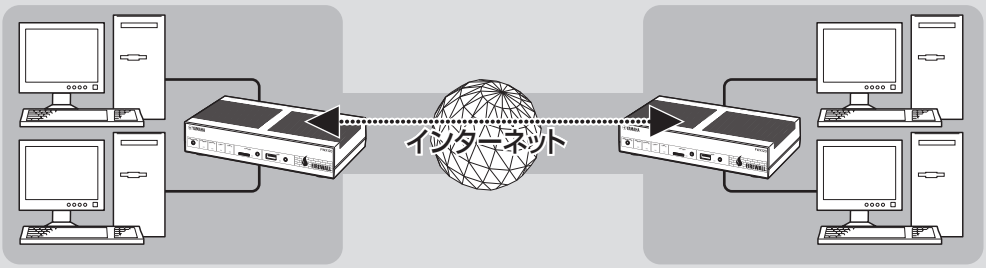
IPsecを利用してVPNを構築する（IPsec-LAN間接続）

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

本製品をブロードバンド回線に接続していれば、仮想プライベートネットワーク（VPN）を構築して、LAN同士を接続することができます。IPsecを利用して接続するため、インターネット経由の接続でもセキュリティーを保つことができます。

ADSLなどの通常のブロードバンド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。なお、本製品のLAN間接続機能は、TCP/IPプロトコルのサーバーソフトウェアに対応しています。



IPsecを利用して、VPNを構築する

本製品で利用できるIPsecについて

- 鍵交換プロトコルはIKE（Internet Key Exchange）を使用します。必要な鍵はIKEにより自動的に生成されますが、鍵の種となる事前共有鍵をあらかじめ登録しておく必要があります（ipsec ike pre-shared-keyコマンド）。
- 鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA（Security Association）で管理します。
- セキュリティゲートウェイとなる、相手機器のプログラムのリビジョンにご注意ください。IPsecリリース2とIPsecリリース3には相互接続性がありますが、後者の設定を前者に合わせる必要があります。なお、本製品で利用できるセキュリティゲートウェイの識別子は1～30、トンネルインターフェース番号も同様に1～30となります。
- 本製品はメインモードとアグレッシブモードに対応していますが、モードを自由に選択することはできません。
  - VPNを構成する両方のルーターが固定グローバルIPアドレスを持つ場合はメインモード、一方のルーターのみ固定グローバルIPアドレスを持つ場合（ダイヤルアップVPNなど）はアグレッシブモードを使用します。
  - メインモードを使用する場合は、対向のルーターのIPアドレスを設定する必要があります。
  - アグレッシブモードを使用する場合は、固定のグローバルIPアドレスを持つかどうかによって、設定が異なります。
- 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」（付属CD-ROMに収録）をご覧ください。

ご注意

- ブロードバンド接続した状態でIPsecのトンネル設定を行うため、IPsecを利用したLAN間接続の設定前にブロードバンド接続の設定が必要です。
- IPsecを利用したLAN間接続は、プロバイダからグローバル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間接続を利用するときは、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、双方の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。
- 本製品のLAN間接続機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

IPsecには2種類の通信モードがあります

IPsecによる通信には、大きく分けてトンネルモードとトランスポートモードの2種類があります。トンネルモードとトランスポートモードは併用が可能ですが、それぞれを二重に適用することはできません。

トンネルモード

IPsecによるVPNを利用するための通信モードです。ルーターがセキュリティゲートウェイとなり、LAN上に流れるIPパケットデータを暗号化して、対向のセキュリティゲートウェイとの間でデータをやりとりします。ルーターがIPsecに必要な処理をすべて行うので、LAN上の始点や終点となるホストには特別な設定を必要としません。
トンネルモードを使用する場合は、「トンネルインターフェース」という仮想的なインターフェースを定義し、処理すべきIPパケットがトンネルインターフェースに流れるように経路を設定します。個々のトンネルインターフェースは、トンネルインターフェース番号で管理されます。

トランスポートモード

ルーター自身が始点または終点になる通信に対してセキュリティーを保証する、特殊な通信モードです。ルーターからリモートのルーターへtelnetでアクセスするなどの特殊な場合に利用できます。

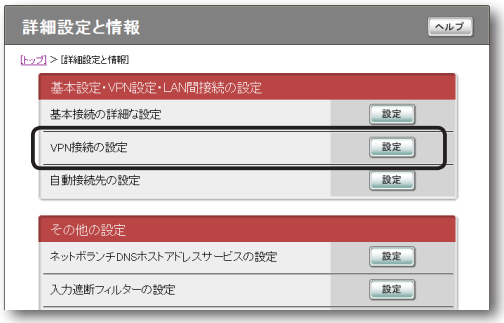
設定する前に

- 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。
- すでに異なるネットワークアドレスが設定されているLANに本製品を設置する場合には、設置するネットワークに合わせて本製品の設定を変更してください。詳しくは「LAN1側IPアドレスを設定する」（53ページ）をご覧ください。

IPsecを使用できるように設定する

本製品でIPsec通信するために必要な設定を行います。

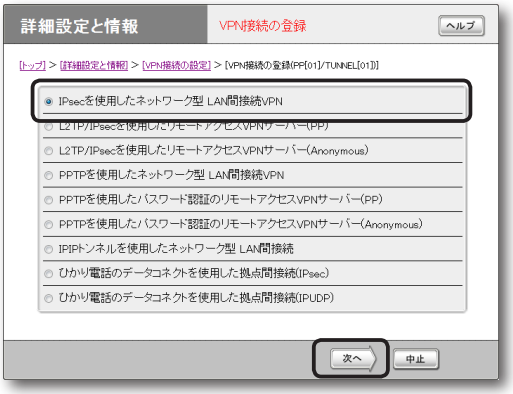
1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「VPN接続の設定」の「設定」をクリックする。



2 登録したい接続先の「追加」をクリックする。

3 **「IPsecを使用したネットワーク型LAN間接続VPN」を選んでから、「次へ」をクリックする。**

「VPN接続設定の登録／修正」画面が表示されます。



4 **必要な設定を行ってから、「設定の確定」をクリックする。**

接続相手が登録されます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

IPsecで接続する

双方の拠点で認証が成功すると、IPsecの通信は自動的に確立されます(特に操作は必要ありません)。IPsec接続が完了すると、「かんたん設定ページ」のトップページに「通信中」と表示されます。

ご注意

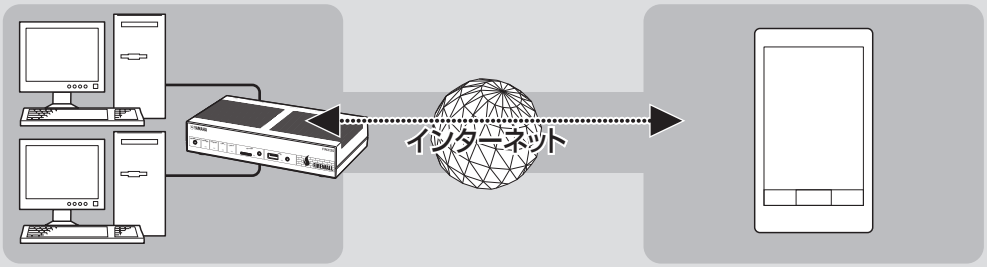
- IPsec接続をするには、双方の拠点で同じ認証鍵(pre-shared key)を設定する必要があります。
- 認証鍵(pre-shared key)はパスワードに相当する重要な情報です。英大文字および英小文字、数字、記号を組み合わせた分かりにくく長い値を設定して、十分に注意して管理してください。

L2TP/IPsecを利用して リモートアクセスする

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

本製品はL2TP/IPsec（Layer-2 Tunneling Protocol）に対応しているため、ブロードバンド回線に接続していれば、外出先からでもVPN（仮想プライベートネットワーク）としてLAN上のパソコンへアクセスできます。IPsecを利用して接続するため、PPTPよりもセキュリティーを保つことができます。リモートアクセスをするときは、本製品にリモートアクセスユーザーのユーザー IDやパスワードを登録し、リモートのパソコンにはVPN接続の設定を行います。



L2TP/IPsecを利用して、リモートアクセスする

本製品で利用できるL2TP/IPsecについて

- IPsecのデータ暗号化をサポートしています。
- 鍵交換プロトコルはIKE(Internet Key Exchange)を使用します。必要な鍵はIKEにより自動的に生成されますが、鍵の種となる事前共有鍵をあらかじめ登録しておく必要があります(ipsec ike pre-shared-keyコマンド)。
- 鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA（Security Association）で管理します。
- 切断タイマが通信状態を監視しているため、L2TP/IPsecのトンネル中をデータが一定時間通過しない場合は、L2TP/IPsecのセッションは切断されます。

ご注意

- 回線を接続した状態でL2TP/IPsecのトンネル設定を行うため、L2TP/IPsecを利用したリモートアクセスの設定前にブロードバンド接続の設定が必要です。
- L2TP/IPsecを利用したリモートアクセスは、プロバイダからグローバル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
- 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。
- 本製品のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

必要な設定

リモートアクセスするときは、本製品やパソコン、スマートフォンなどに次のような設定が必要です。

本製品の設定

- ブロードバンド接続の設定をする。
  - 本製品のWAN側またはPP側にグローバルIPアドレスが割り当てられている必要があります。
  - WAN側またはPP側アドレスが動的に割り当てられる端末型接続の場合は、ネットボランチDNSサービス(163ページ)を利用して、使用できるホスト名を取得する必要があります。
  - ネットワーク型接続の場合は、WAN側またはPP側に割り当てられるグローバルIPアドレスを確認してください。
- 接続相手を登録する(次項)。

LAN内のサーバーまたはパソコンに必要な設定

- 固定プライベートIPアドレスを設定する。
- ファイルサーバーソフトの設定を変更する。

リモートアクセスするスマートフォンなどに必要な設定

- リモートアクセスするスマートフォンなどの設定を変更する(130、132ページ)。

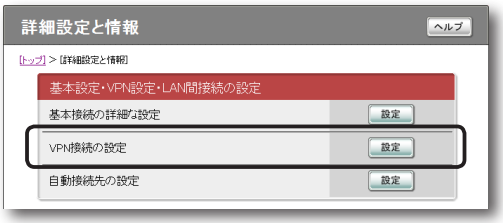
接続相手を登録する

接続相手を登録します。

ご注意

- PP接続で登録できるユーザー数は最大30個です。L2TP/IPsecのトンネル接続はAnonymousで利用しているものも合わせて、同時に30個までとなります。
- Anonymous接続で登録できるユーザー数に制限はありませんが、実際のL2TP/IPsecのトンネル接続はPP接続で利用しているものも合わせて、同時に30個までとなります。

1 **「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「VPN接続の設定」の「設定」をクリックする。**

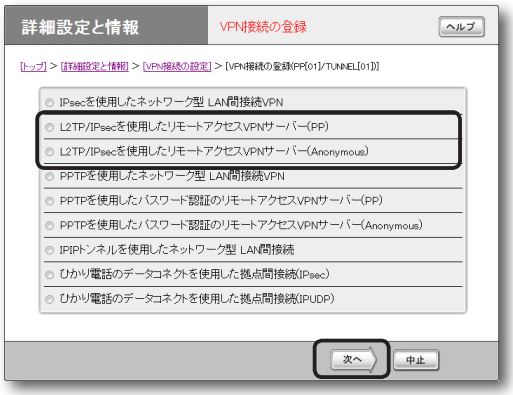


2 **登録したい接続先の「追加」をクリックする。**

3 **使用したい認証方式を選んでから、「次へ」をクリックする。**

「VPN接続設定の登録／修正」画面が表示されます。

- **PP**：指定されたホスト名またはIPアドレスのみを接続先としてユーザーIDとパスワードで認証を行います。
- **Anonymous**：接続先の制限は行わずに、ユーザーIDとパスワードで認証を行います。



4 必要な設定を行ってから、「設定の確定」をクリックする。

接続相手が登録されます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

(手順3で「PP」を選んだ場合の画面例)

LAN内のサーバーやパソコンを設定する

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。

ご注意

- 本製品のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

サーバーやパソコンのIP アドレスを設定する

お互いのLAN上のサーバーまたはパソコンで外部からのアクセスを許可するパソコンには、固定プライベートIPアドレスを設定します。

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、公開するフォルダやユーザー ID、パスワードを設定します。

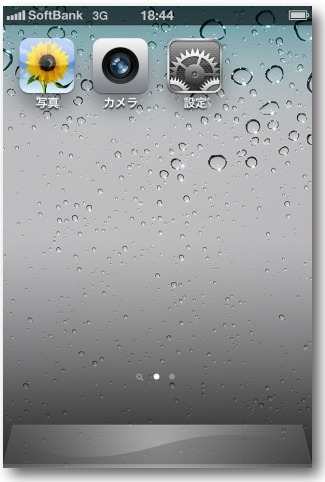
iOSからリモートアクセスする

ご注意

ご使用の端末のバージョンによって、画面が一部異なる場合があります。

リモートアクセスする スマートフォンなどの設定を変更する

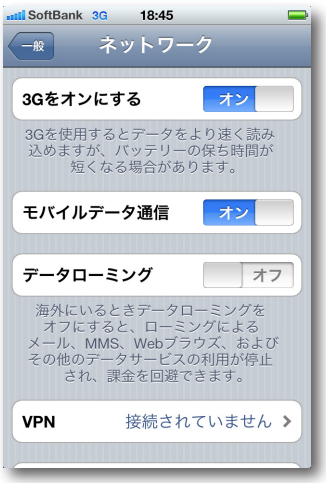
1 「設定」をタップする。



2 「一般」をタップする。

3 「ネットワーク」をタップする。

4 「VPN」をタップする。



5 「VPN構成を追加」をタップする。

6 「L2TP」を選択し、必要な設定情報を入力する。

説明
L2TPクライアントの名前「Yamaha-vpn」を入力する。

サーバ
ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスを入力する。

アカウント
129ページ の手順4で設定した接続ユーザーIDを入力する。

RSA SecurID
オフを選択する。

パスワード
129ページの手順4で設定した接続パスワードを入力する。

シークレット
本製品に設定した事前共有鍵を入力する。

すべての信号を送信
オンを選択する。

プロキシ
オフを選択する。

7 「保存」をタップする。

これで、リモートアクセス接続の設定が完了しました。

本製品へアクセスする

1 本製品のブロードバンド接続を接続状態にする。

2 「設定」をタップする。

3 「一般」をタップする。

4 「ネットワーク」をタップする。

5 「VPN」をタップする。

6 「Yamaha - vpn」をタップし、「VPN」欄をオンにする。

本製品へのVPN接続を開始します。

アンドロイドからリモートアクセスする

ご注意

アンドロイドの説明に使用している画面と、ご使用の端末の画面では一部異なる場合があります。

リモートアクセスする スマートフォンなどの設定を変更する

1 メニュー画面を開き、「設定」をタップする。

2 「無線とネットワーク」をタップする。

3 「VPN設定」をタップする。

4 「VPNの追加」をタップする。

5 「L2TP/IPsec PSK VPNを追加」をタップする。

6 必要な設定情報を入力する。

VPN名
L2TPクライアントの名前「Yamaha-vpn」を入力する。

VPNサーバーの設定
ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスを入力する。

IPsec事前共有鍵の設定
本製品に設定した事前共有鍵を入力する。

7 **バックキーを押す。**

これで、リモートアクセス接続の設定が完了しました。

本製品へアクセスする

1 **本製品のブロードバンド接続を接続状態にする。**

2 **メニュー画面を開き、「設定」をタップする。**

3 **「無線とネットワーク」をタップする。**

4 **「VPN設定」をタップする。**

5 **「Yamaha - vpn」をタップする。**

6 **「ネットワークに接続」をタップする。**

7 **「ユーザー名」と「パスワード」欄に、129ページの手順4で設定した接続ユーザー IDと接続パスワードを入力し、「接続」をタップする。**

本製品へのVPN接続を開始します。

ご注意

「ユーザー名を保存」にチェックを付けると、次回から接続ユーザー IDの入力が不要になります。チェックしない場合は、接続のたびに接続ユーザー ID入力が必要になります。

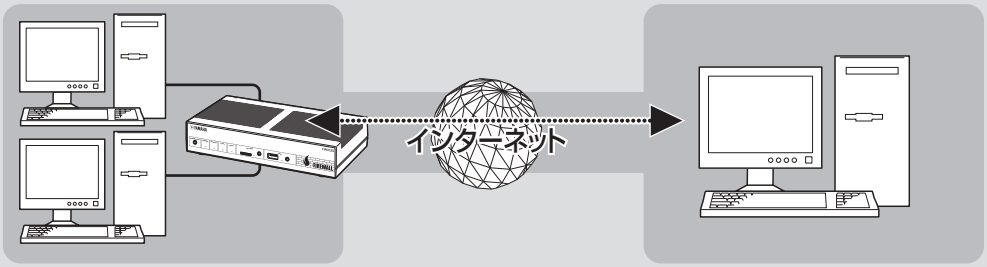
PPTPを利用してリモートアクセスする

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

本製品はPPTP（Point to Point Tunneling Protocol）に対応しているため、ブロードバンド回線に接続していれば、外出先からでもVPN（仮想プライベートネットワーク）としてLAN上のパソコンへアクセスできます。

リモートアクセスをするときは、本製品にリモートアクセスユーザーのユーザーIDやパスワードを登録し、リモートのパソコンにはVPN接続の設定を行います。



PPTPを利用して、リモートアクセスする

本製品で利用できるPPTPについて

- PPTPのデータ暗号化をサポートしています。暗号化アルゴリズムとしてRC4（鍵長40bitまたは128bit)を使います。
- MS-CHAP、MS-CHAPv2によるユーザー／パスワード認証をサポートしています。
- MPPEで暗号化方式が成立しなかった場合に、着信拒否するか否かを設定できます(アクセス制御)。
- 圧縮には対応していません。PPTPクライアント側のPPPの設定で、「ソフトウェアによる圧縮を行う」のチェックを外してください。
- PPTPでは、トンネル制御にTCPのポート1723をデータ通信にGREのプロトコル番号47を使います。ファイアウォールの内側にPPTPサーバーを設置したり、NATとリモートアクセスVPNサーバーを併用する場合などは、TCPのポート番号1723とGREのプロトコル番号47を通すようにしてください。詳しくはネットワーク管理者にご相談ください。
- 切断タイマが通信状態を監視しているため、PPTPトンネル中をデータが一定時間通過しない場合は、PPTPのセッションは切断されます。
- PPPフォワーディング機能はサポートしていません。

ご注意

- 回線を接続した状態でPPTPのトンネル設定を行うため、PPTPを利用したリモートアクセスの設定前にブロードバンド接続の設定が必要です。
- PPTPを利用したリモートアクセスは、プロバイダからグローバル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
- 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。
- 本製品のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

必要な設定

リモートアクセスするときは、本製品やパソコンに次のような設定が必要です。

本製品の設定

- ブロードバンド接続の設定をする。
  - 本製品のWAN側またはPP側にグローバルIPアドレスが割り当てられている必要があります。
  - 動的にWAN側またはPP側アドレスが割り当てられる端末型接続の場合は、ネットボランチDNSサービス(163ページ)を利用して、使用できるホスト名を取得する必要があります。
  - ネットワーク型接続の場合は、WAN側またはPP側に割り当てられるグローバルIPアドレスを確認してください。
- 接続相手を登録する(次項)。

LAN内のサーバーまたはパソコンに必要な設定

- 固定プライベートIPアドレスを設定する。
- ファイルサーバーソフトの設定を変更する。

リモートアクセスするパソコンに必要な設定

- リモートアクセスするパソコンの設定を変更する(139、142、145ページ)。

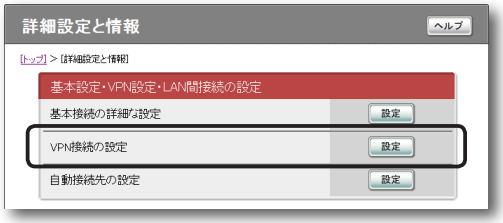
接続相手を登録する

接続相手を登録します。

ご注意

- PP接続で登録できるユーザー数は最大30個です。PPTPのトンネル接続はAnonymousで利用しているものも合わせて、同時に30個までとなります。
- Anonymous接続で登録できるユーザー数に制限はありませんが、実際のPPTPのトンネル接続はPP接続で利用しているものも合わせて、同時に30個までとなります。

1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「VPN接続の設定」の「設定」をクリックする。

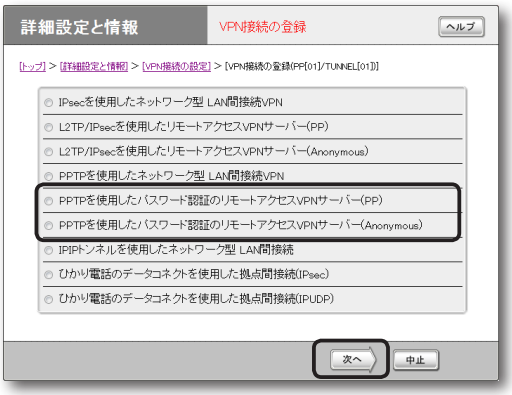


2 登録したい接続先の「追加」をクリックする。

3 使用したい認証方式を選んでから、「次へ」をクリックする。

「VPN接続設定の登録／修正」画面が表示されます。

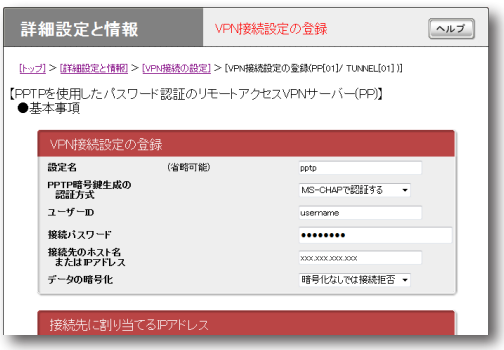
- **PP**：指定されたホスト名またはIPアドレスのみを接続先としてユーザーIDとパスワードで認証を行います。
- **Anonymous**：接続先の制限は行わずに、ユーザーIDとパスワードで認証を行います。



4 必要な設定を行ってから、「設定の確定」をクリックする。

接続相手が登録されます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。



（手順3で「PP」を選んだ場合の画面例）

LAN内のサーバーやパソコンを設定する

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。

ご注意

- 本製品のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有する場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

サーバーやパソコンのIP アドレスを設定する

お互いのLAN上のサーバーまたはパソコンで外部からのアクセスを許可するパソコンには、固定プライベートIPアドレスを設定します。

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、公開するフォルダやユーザーID、パスワードを設定します。

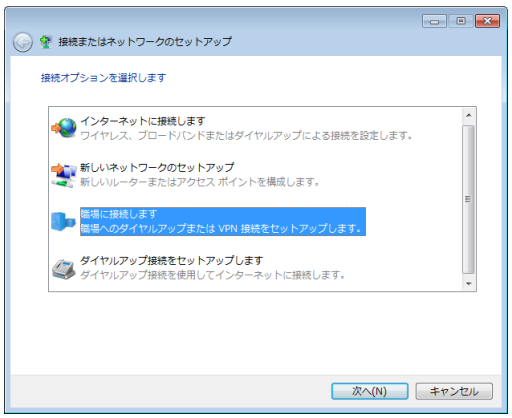
Windows 7搭載パソコンからリモートアクセスする

リモートアクセスするパソコンの設定を変更する

1 「コントロールパネル」の「ネットワークの状態とタスクの表示」をクリックする。

2 「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。

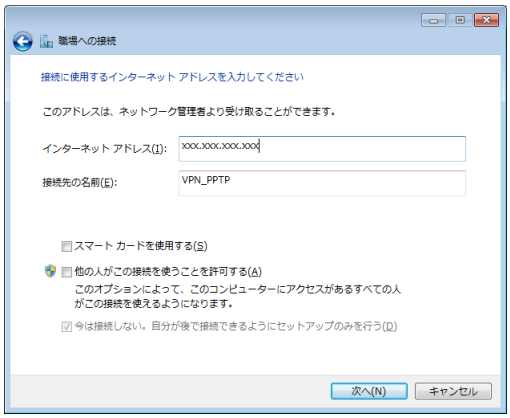
3 「職場に接続します」を選んでから、「次へ」をクリックする。



4 「インターネット接続(VPN)を使用します」をクリックする。

5 「インターネットアドレス」にネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスを入力する。

6 「接続先の名前」に「VPN_PPTP」と入力する。



7 「今は接続しない。自分が後で接続できるようにセットアップのみを行う」を選んでから、「次へ」をクリックする。

8 「作成」をクリックする。

9 「閉じる」をクリックする。

これで、リモートアクセス接続の設定が完了しました。

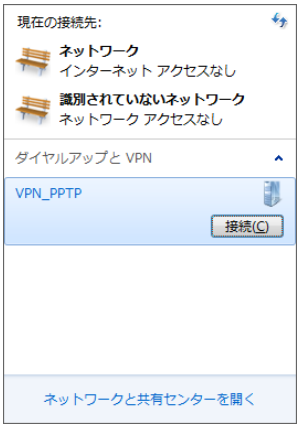
本製品へアクセスする

1 本製品のブロードバンド接続を接続状態にする。

2 「コントロールパネル」の「ネットワークの状態とタスクの表示」をクリックする。

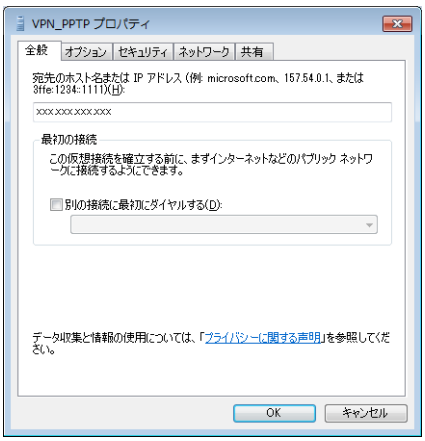
3 「ネットワークに接続」をクリックする。

4 「VPN_PPTP」アイコンを選択し、「接続」をクリックする。



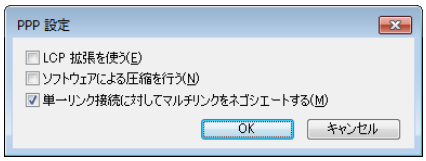
5 「プロパティ」をクリックする。

6 「全般」タブをクリックしてから、「宛先のホスト名またはIPアドレス」欄に、ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスが入力されていることを確認する。



7 「オプション」タブをクリックしてから、「PPP設定」をクリックする。

8 以下のように設定してから、「OK」をクリックする。



- **LCP拡張を使う**：チェックを外す。
- **ソフトウェアによる圧縮を行う**：チェックを外す。
- **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**：チェックを付ける。

9 「セキュリティ」タブをクリックしてから、「VPNの種類」で「自動」を選ぶ。

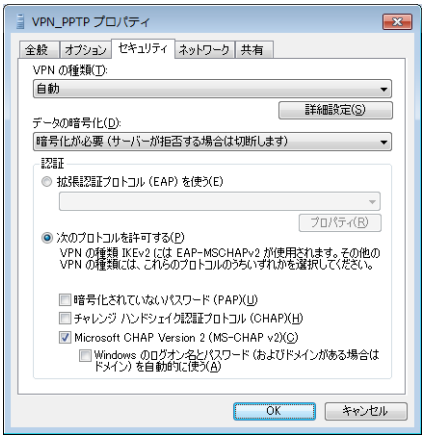
10 暗号形式を選ぶ。

138ページの手順3で使用したい認証方式として「PP」を選択した場合は、138ページの手順4で行った設定に合わせて、暗号形式を選びます。

- **本製品で「暗号化なしでは接続拒否」を選んだ場合**：「暗号化が必要（サーバーが拒否する場合は切断します）」を選びます。
- **本製品で「暗号化なしでも接続許可」を選んだ場合**：希望する暗号化のレベルを選びます。

138ページの手順3で使用したい認証方式として「Anonymous」を選択した場合は、希望する暗号化のレベルを選びます。

11 「認証」から「次のプロトコルを許可する」を選び、以下のように設定してから「OK」をクリックする。



- **暗号化されていないパスワード(PAP)**：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)**：チェックを外す。
- **Microsoft CHAP Version 2 (MS-CHAPv2)**：チェックを付ける。
- **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**：チェックを外す。

ご注意

Windows 7では、Microsoft CHAP Version 1 (MS-CHAP)はサポートされていません。138ページの手順4で行った設定内容をご確認ください。

12 「VPN_PPTPのプロパティ」画面の「OK」をクリックして、「VPN_PPTPのプロパティ」画面を閉じる。

13 「ユーザー名」と「パスワード」欄に、138ページの手順4で設定したユーザーIDと接続パスワードを入力し、「接続」をクリックする。

本製品へのVPN接続を開始します。

ご注意

「次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する」にチェックを付けると、次回からユーザー名とパスワードの入力が不要になります。

接続を解除する場合は

「切断」をクリックすると、本製品との接続が解除されます。

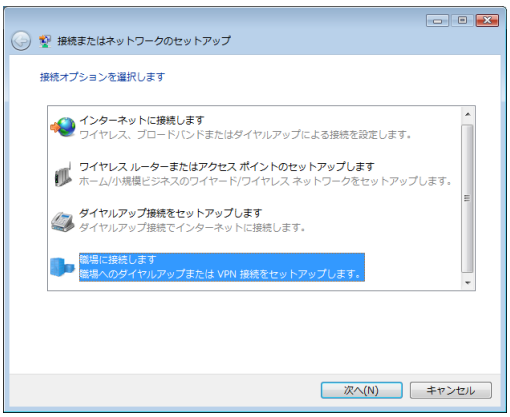
Windows Vista搭載パソコンからリモートアクセスする

リモートアクセスする パソコンの設定を変更する

1 「コントロールパネル」の「ネットワークの状態とタスクの表示」をクリックする。

2 「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。

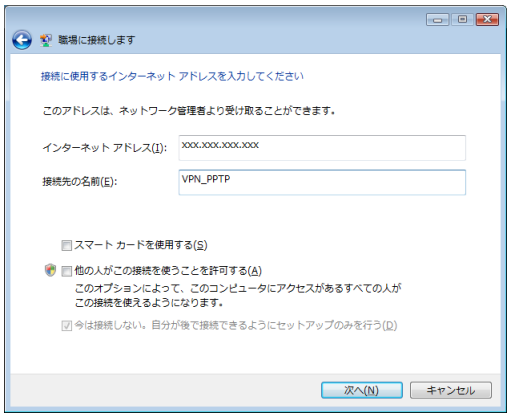
3 「職場に接続します」を選んでから、「次へ」をクリックする。



4 「インターネット接続(VPN)を使用します」をクリックする。

5 「インターネットアドレス」にネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスを入力する。

6 「接続先の名前」に「VPN_PPTP」と入力する。



7 「今は接続しない。自分が後で接続できるようにセットアップのみを行う」を選んでから、「次へ」をクリックする。

8 「作成」をクリックする。

9 「閉じる」をクリックする。

これで、リモートアクセス接続の設定が完了しました。

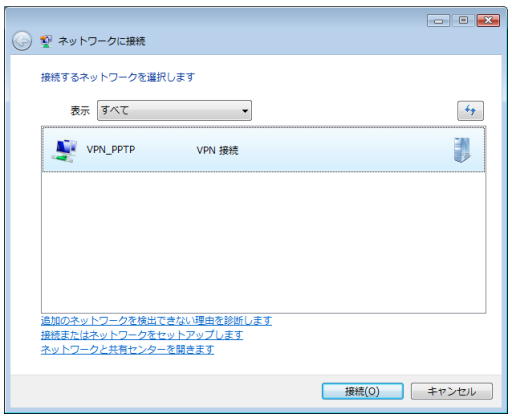
本製品へアクセスする

1 本製品のブロードバンド接続を接続状態にする。

2 「コントロールパネル」の「ネットワークの状態とタスクの表示」をクリックする。

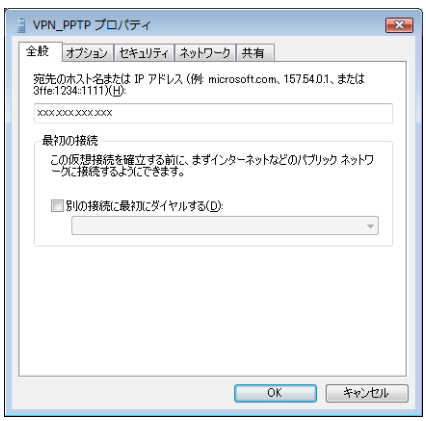
3 「ネットワークに接続」をクリックする。

4 「VPN_PPTP」アイコンを選択し、「接続」をクリックする。



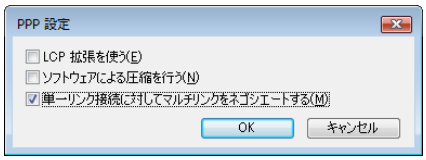
5 「プロパティ」をクリックする。

6 「全般」タブをクリックしてから、「宛先のホスト名またはIPアドレス」欄に、ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスが入力されていることを確認する。



7 「オプション」タブをクリックしてから、「PPP設定」をクリックします。

8 以下のように設定してから、「OK」をクリックする。



- **LCP拡張を使う**：チェックを外す。
- **ソフトウェアによる圧縮を行う**：チェックを外す。
- **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**：チェックを付ける。

9 「セキュリティ」タブをクリックしてから、セキュリティオプションの「詳細(カスタム設定)」を選び、「設定」をクリックする。

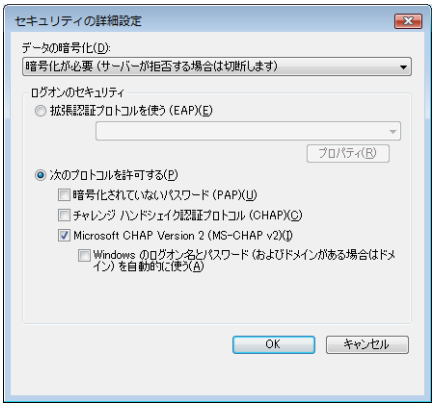
10 暗号形式を選ぶ。

138ページの手順3で使用したい認証方式として「PP」を選択した場合は、138ページの手順4で行った設定に合わせて、暗号形式を選びます。

- **本製品で「暗号化なしでは接続拒否」を選んだ場合**：「暗号化が必要(サーバーが拒否する場合は切断します)」を選びます。
- **本製品で「暗号化なしでも接続許可」を選んだ場合**：希望する暗号化のレベルを選びます。

138ページの手順3で使用したい認証方式として「Anonymous」を選択した場合は、
希望する暗号化のレベルを選びます。

11 「ログオンのセキュリティ」から「次のプロトコルを許可する」を選び、以下のように設定してから「OK」をクリックする。



- **暗号化されていないパスワード(PAP)**：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)**：チェックを外す。
- **Microsoft CHAP Version 2 (MS-CHAP v2)**：チェックを付ける。
- **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**：チェックを外す。

ご注意

Windows Vistaでは、Microsoft CHAP Version 1 (MS-CHAP)はサポートされていません。138ページの手順4で行った設定内容をご確認ください。

12 「ネットワーク」タブをクリックしてから、「VPNの種類」で「自動」を選ぶ。

13 「VPN_PPTPのプロパティ」画面の「OK」をクリックして、「VPN_PPTPのプロパティ」画面を閉じる。

14 「ユーザー名」と「パスワード」欄に、138ページの手順4で設定したユーザーIDと接続パスワードを入力し、「接続」をクリックする。

本製品へのVPN接続を開始します。

ご注意

「次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する」にチェックを付けると、次回からユーザー名とパスワードの入力が不要になります。

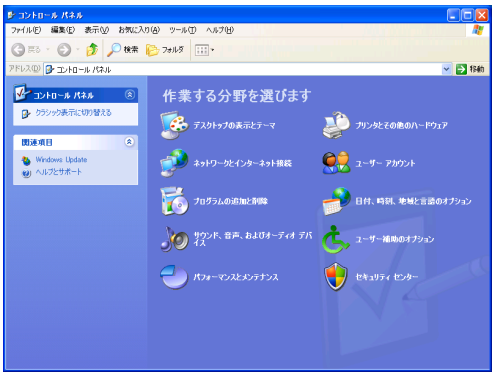
接続を解除する場合は

「切断」をクリックすると、本製品との接続が解除されます。

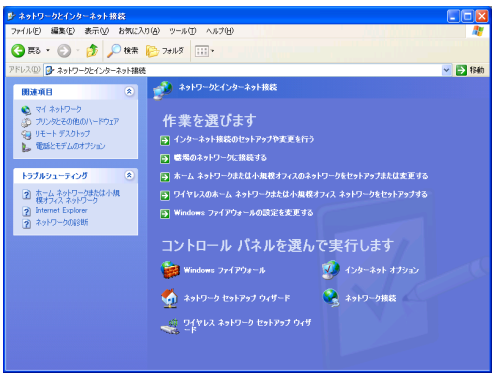
Windows XP搭載パソコンからリモートアクセスする

リモートアクセスする パソコンの設定を変更する

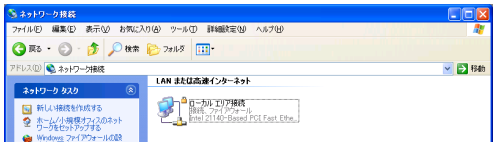
1 「コントロールパネル」の「ネットワークとインターネット接続」をクリックする。



2 「ネットワーク接続」をクリックする。

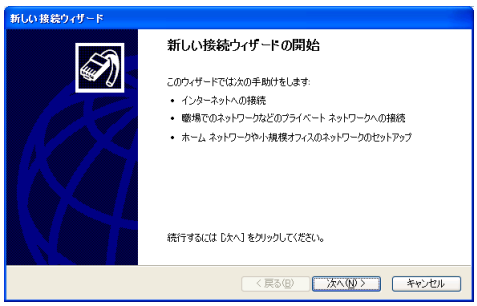


3 「新しい接続を作成する」をクリックする。

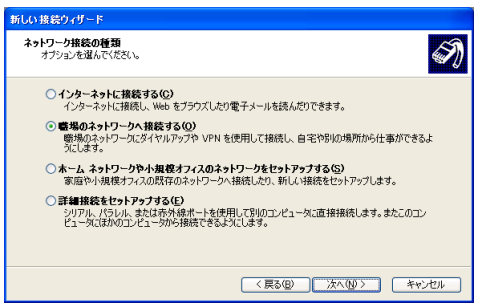


「新しい接続ウィザードの開始」画面が表示されます。
「所在地情報」画面が表示された場合は、市外局番を入力してから、「OK」をクリックしてください。

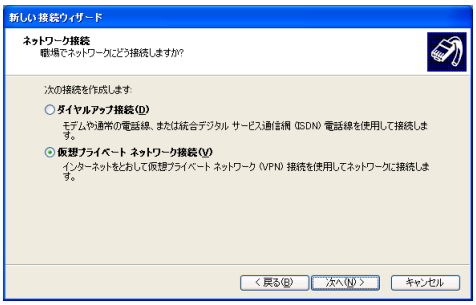
4 「次へ」をクリックする。



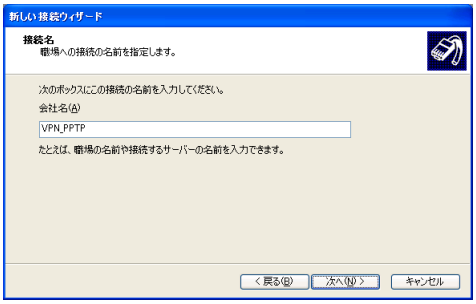
5 「職場のネットワークへ接続する」を選んでから、「次へ」をクリックする。



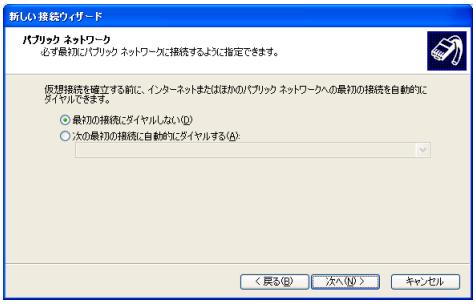
6 「仮想プライベート ネットワーク接続」を選んでから、「次へ」をクリックする。



7 「会社名」に「VPN_PPTP」と入力してから、「次へ」をクリックする。



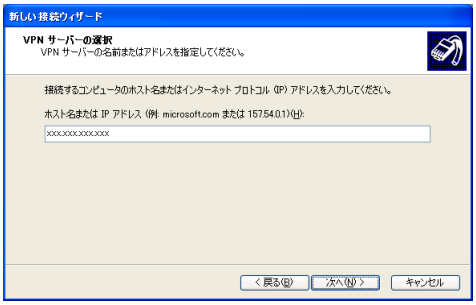
8 「最初の接続にダイヤルしない」または「次の最初の接続に自動的にダイヤルする」を選んでから、「次へ」をクリックする。



ヒント

この画面は、既に別のダイヤルアップの設定がある場合に表示されます。設定がない場合は表示されません。

9 ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスを入力してから、「次へ」をクリックする。



10 「完了」をクリックする。

これで、リモートアクセス接続の設定が完了しました。

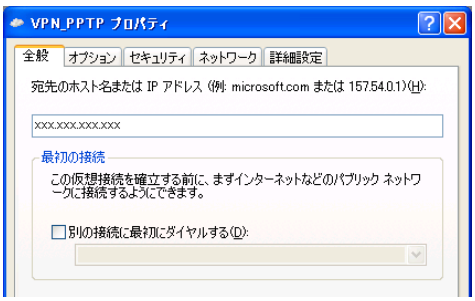
本製品へアクセスする

1 **本製品のブロードバンド接続を接続状態にする。**

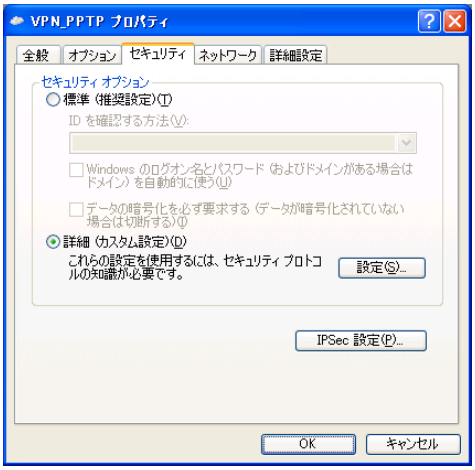
2 **「VPN_PPTP」アイコンをダブルクリックして、接続画面を表示する。**

3 **「プロパティ」をクリックする。**

4 **「全般」タブをクリックしてから、「宛先のホスト名またはIPアドレス」欄に、ネットボランチDNSサービスで取得したホストアドレスまたは本製品のWAN側IPアドレスが入力されていることを確認する。**



5 **「セキュリティ」タブをクリックしてから、セキュリティオプションの「詳細(カスタム設定)」を選び、「設定」をクリックする。**

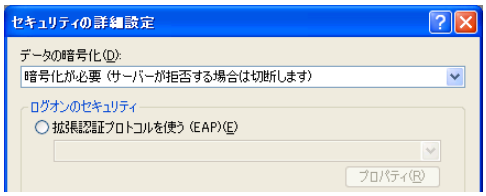


6 **暗号形式を選ぶ。**

138ページの手順3で使用したい認証方式として「PP」を選択した場合は、138ページの手順4で行った設定に合わせて、暗号形式を選びます。

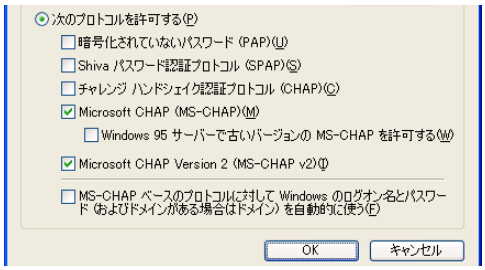
- **本製品で「暗号化なしでは接続拒否」を選んだ場合**：「暗号化が必要(サーバーが拒否する場合は切断します)」を選びます。
- **本製品で「暗号化なしでも接続許可」を選んだ場合**：希望する暗号化のレベルを選びます。

138ページの手順3で使用したい認証方式として「Anonymous」を選択した場合は、
希望する暗号化のレベルを選びます。

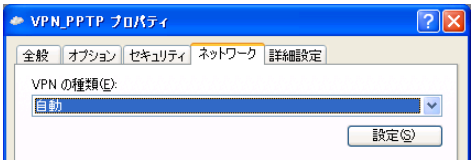


7 **「ログオンのセキュリティ」から「次のプロトコルを許可する」を選び、以下のように設定してから「OK」をクリックする。**

- 暗号化されていないパスワード(PAP)：チェックを外す。
- Shivaパスワード認証プロトコル(SPAP)：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)：チェックを外す。
- Microsoft CHAP (MS-CHAP)：チェックを付ける。
- Windows 95サーバーで古いバージョンのMS-CHAPを許可する：チェックを外す。
- Microsoft CHAP Version 2 (MS-CHAP v2)：チェックを付ける。
- MS-CHAPベースのプロトコルに対して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：チェックを外す。

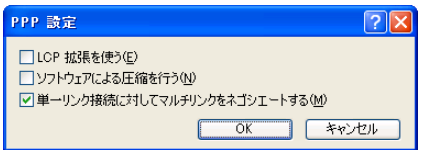


8 「ネットワーク」タブをクリックしてから、「VPNの種類」で「自動」を選び、「設定」をクリックする。



9 以下のように設定してから、「OK」をクリックする。

- LCP拡張を使う：チェックを外す。
- ソフトウェアによる圧縮を行う：チェックを外す。
- 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：チェックを付ける。



10 「VPN_PPTPのプロパティ」画面の「OK」をクリックして、「VPN_PPTPのプロパティ」画面を閉じる。

11 「ユーザー名」と「パスワード」欄に、138ページの手順4で設定したユーザーIDと接続パスワードを入力する。

12 「接続」をクリックする。

本製品へのVPN接続を開始します。
接続すると、「ダイヤル アップネットワーク（プロバイダ名）」画面が表示され、接続速度と接続時間が表示されます。

ご注意

「次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する」にチェックを付けると、次回からユーザー名とパスワードの入力が不要になります。

接続を解除する場合は

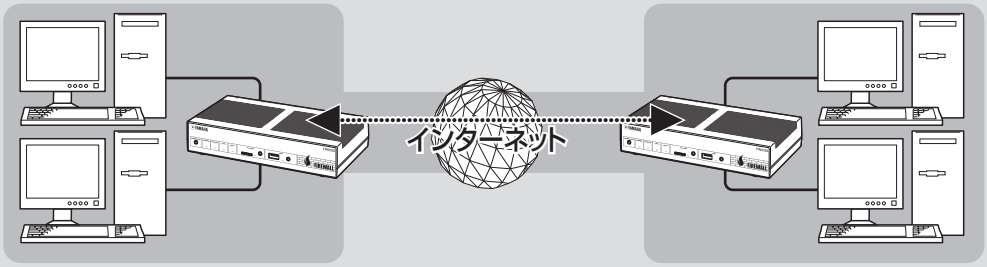
「切断」をクリックすると、本製品との接続が解除されます。

PPTPを利用してVPNを構築する（PPTP-LAN間接続）

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

本製品をブロードバンド回線に接続していれば、PPTPを利用して仮想プライベートネットワーク（VPN）を構築して、LAN同士を接続することができます。
ADSLなどの通常のブロードバンド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。なお、本製品のLAN間接続機能は、TCP/IPプロトコルのサーバーソフトウェアに対応しています。



PPTPを利用して、VPNを構築する

本製品で利用できるPPTPについて

- PPTPのデータ暗号化をサポートしています。暗号化アルゴリズムとしてRC4（鍵長40bitまたは128bit)を使います。
- MS-CHAP、MS-CHAPv2によるユーザー／パスワード認証をサポートしています。
- MPPEで暗号化方式が成立しなかった場合に、着信拒否するか否かを設定できます(アクセス制御)。
- 圧縮には対応していません。PPTPクライアント側のPPPの設定で、「ソフトウェアによる圧縮を行う」のチェックを外してください。
- PPTPでは、トンネル制御にTCPのポート1723を、データ通信にGREのプロトコル番号47を使います。ファイアウォールの内側にPPTPサーバーを設置したり、NATとリモートアクセスVPNサーバーを併用する場合などは、TCPのポート番号1723とGREのプロトコル番号47を通すようにしてください。詳しくはネットワーク管理者にご相談ください。
- 切断タイマが通信状態を監視しているため、PPTPトンネル中をデータが一定時間通過しない場合は、PPTPのセッションは切断されます。
- PPPフォワーディング機能はサポートしていません。

ご注意

- ブロードバンド接続した状態でPPTPのトンネル設定を行うため、PPTPを利用したLAN間接続の設定前にブロードバンド接続の設定が必要です。
- PPTPを利用したLAN間接続は、プロバイダからグローバル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間接続を利用するときは、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、双方の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。
- 本製品のLAN間接続機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けます。

設定する前に

- 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。
- すでに異なるネットワークアドレスが設定されているLANに本製品を設置する場合には、設置するネットワークに合わせて本製品の設定を変更してください。詳しくは「LAN1側IPアドレスを設定する」(53ページ)をご覧ください。

PPTPを使用できるように設定する

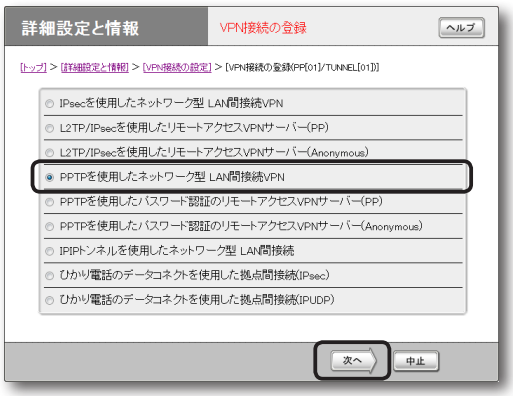
本製品をPPTPサーバー／PPTPクライアントとして動作させるために必要な設定を行います。接続する側のLANに設置した本製品はPPTPクライアント、接続される側のLANに設置した本製品はPPTPサーバーとして設定してください。

1 **「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「VPN接続の設定」の「設定」をクリックする。**

2 **登録したい接続先の「追加」をクリックする。**

3 **「PPTPを使用したネットワーク型LAN間接続VPN」を選んでから、「次へ」をクリックする。**

「VPN接続設定の登録／修正」画面が表示されます。



4 **必要な設定を行ってから、「設定の確定」をクリックする。**

接続相手が登録されます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

PPTPで接続する

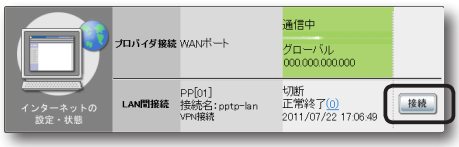
PPTPサーバーに接続します。

ご注意

- PPTPサーバーに接続するには、以下の操作を行う本製品がPPTPクライアントとして設定されている必要があります。
- 「接続」、「切断」ボタンはPPTPクライアントの時に表示されます。

「かんたん設定ページ」のトップページで、「LAN間接続」から接続したいPPTP設定の「接続」をクリックする。

登録したPPTPサーバーに接続して、PPTP-LAN間接続します。



PPTP-LAN間接続を切断するには

「かんたん設定ページ」のトップページで、「LAN間接続」の「切断」をクリックします。

ご注意

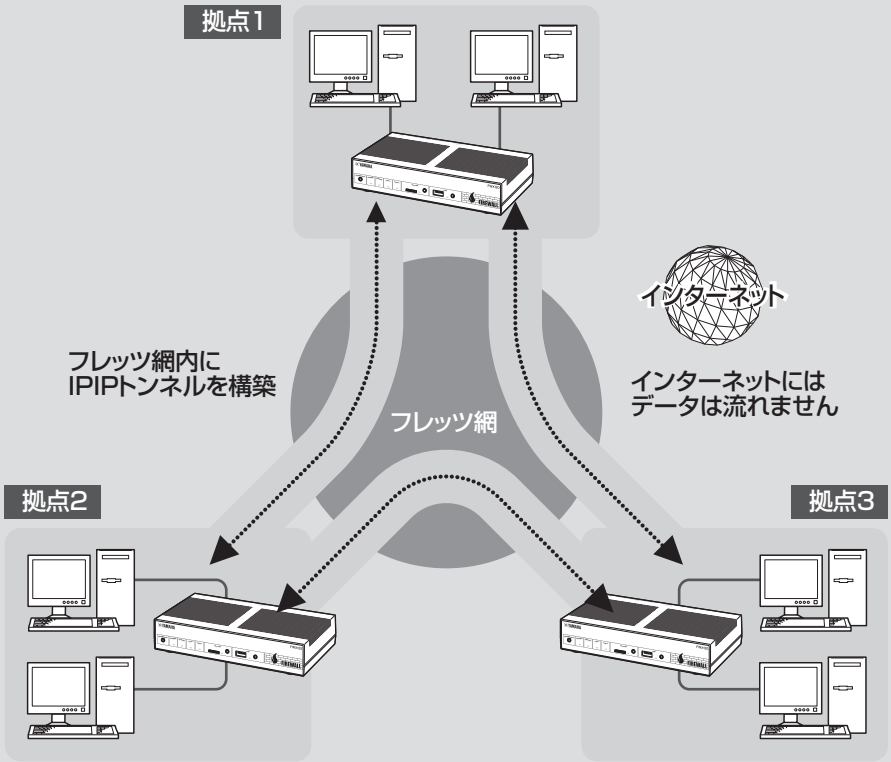
「切断」をクリックしてもPPTPのセッションが終了するだけで、プロバイダに対する接続は切断されません。

フレッツ網を使用して、LAN同士をIPIPトンネル接続する

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

インターネット経由でLAN同士を接続する場合は、データの盗聴や改ざんの危険性があるため、データを暗号化する必要があります。しかし、フレッツ網のように機密性の高いネットワークではデータの暗号化の必要性が低下するため、IPIP トンネルによる接続でもデータの機密性を確保できます。
ここでは、フレッツ・VPN ワイドのように、固定IPアドレスが１つだけ払い出される契約（端末型払い出し）でフレッツ網に接続して、IPIP トンネルでLAN同士を接続するときの設定方法を説明します。



設定する前に

- 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。
- すでに異なるネットワークアドレスが設定されているLANに本製品を設置する場合には、設置するネットワークに合わせて本製品の設定を変更してください。詳しくは「LAN1側IPアドレスを設定する」（53ページ）をご覧ください。

ご注意

- IPIPトンネル接続では、データが暗号化されずに転送されます。データが暗号化されないIPIPトンネル接続をインターネットで使用することは、非常に危険です。IPIPトンネル接続をインターネット上で使用しないでください。
- IPIPトンネル接続の設定前に、フレッツ網などの閉域網への接続の設定が必要になります。
- LAN間接続を利用するときは、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、双方の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。
- 本製品のLAN間接続機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。
- Macintoshでファイル共有をする場合は、システム環境設定の「共有」で「パーソナルファイル共有」にチェックを付けてください。

フレッツ網に接続できるように設定する

本製品をフレッツ網に接続するために、「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」画面で必要な設定を行います。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶「設定可能なプロバイダ」から設定を追加したい接続先の「追加」
▶「PPPoEを用いる端末型ブロードバンド接続（フレッツ 光ネクスト、Bフレッツなど）」を選んでから、「次へ」

1 **必要な設定情報を入力する。**

設定名
接続先がわかるような名前を入力します。

ユーザー ID
指定されたユーザー IDを入力します。

接続パスワード
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。

接続先の宛先情報

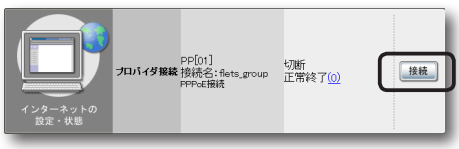
- **宛先アドレス**：「その他」をクリックして選んでから、以下の設定を行います。
  - **経路のアドレス情報**:接続相手に割り当てられるIPアドレスを入力します。
  - **経路のネットマスク情報**:「255.255.255.255（32ビット）」を選びます。
- **宛先ドメイン名**：「なし」をクリックして選びます。

2 **「設定の確定」をクリックする。**
「プロバイダの登録」画面が表示されます。

3 **複数のLANと接続する場合は、「戻る」をクリックしてから「接続先の宛先情報」を繰り返し設定する。**
接続相手に割り当てられるすべてのIPアドレスを経路に指定してください。
接続相手の宛先アドレスの設定がすべて終わったら、「トップへ戻る」をクリックして、「かんたん設定ページ」のトップページに戻ります。

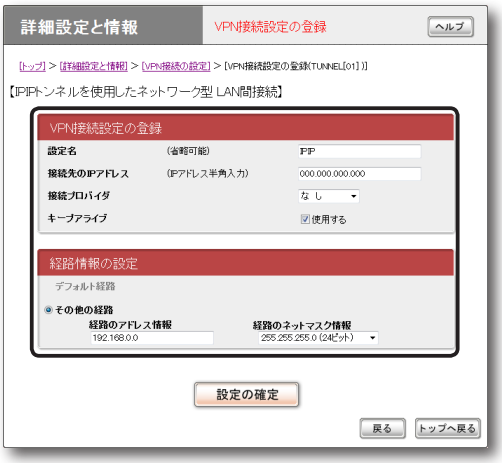
フレッツ網に接続する

「かんたん設定ページ」のトップページで、「プロバイダ接続」からフレッツ網接続用の設定の「接続」をクリックする。



IPIPトンネルを使用できるように設定する

本製品と相手機器をIPIPトンネルで接続して使用するために、「IPIPトンネルを使用したネットワーク型 LAN間接続」画面で必要な設定を行います。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「IPIP トンネルを使用したネットワーク型 LAN間接続」画面を開くには
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「VPN接続の設定」の「設定」
▶「設定可能なVPN設定」から設定を追加したいVPN接続先の「追加」
▶「IPIPトンネルを使用したネットワーク型LAN間接続」を選んでから、「次へ」

1 **必要な設定情報を入力する。**

設定名
接続先がわかるような名前を入力します。

接続先のIPアドレス
接続相手に割り当てられるIPアドレスを入力します。

接続プロバイダ
フレッツ網の接続に使用する設定（154ページで行った設定）を指定します。

ご注意
インターネット接続用のPPPoE接続を別に設定している場合は、インターネット接続用の接続設定を誤って指定しないようにご注意ください。

経路情報の設定
「経路のアドレス情報」と「経路のネットマスク情報」に、接続先のLANのネットワークアドレスを入力します。

2 **「設定の確定」をクリックする。**

「VPN接続設定の登録」画面が表示されます。

3 **複数のLANと接続する場合は、「戻る」をクリックしてから「経路情報の設定」を繰り返し設定する。**

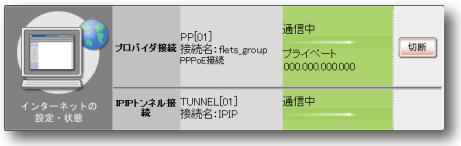
接続相手ごとの経路情報をすべて設定してください。

ご注意
接続相手に割り当てられるIPアドレスと、その接続先のLANのネットワークアドレスの組み合わせを間違えないように設定してください。

接続相手の経路情報の設定がすべて終わったら、「トップへ戻る」をクリックして、「かんたん設定ページ」のトップページに戻ります。

IPIPトンネル接続する

これまでの設定が終わると、IPIPトンネルの通信は自動的に確立されます（特に操作は必要ありません）。IPIPトンネル接続が完了すると、「かんたん設定ページ」のトップページに「通信中」と表示されます。

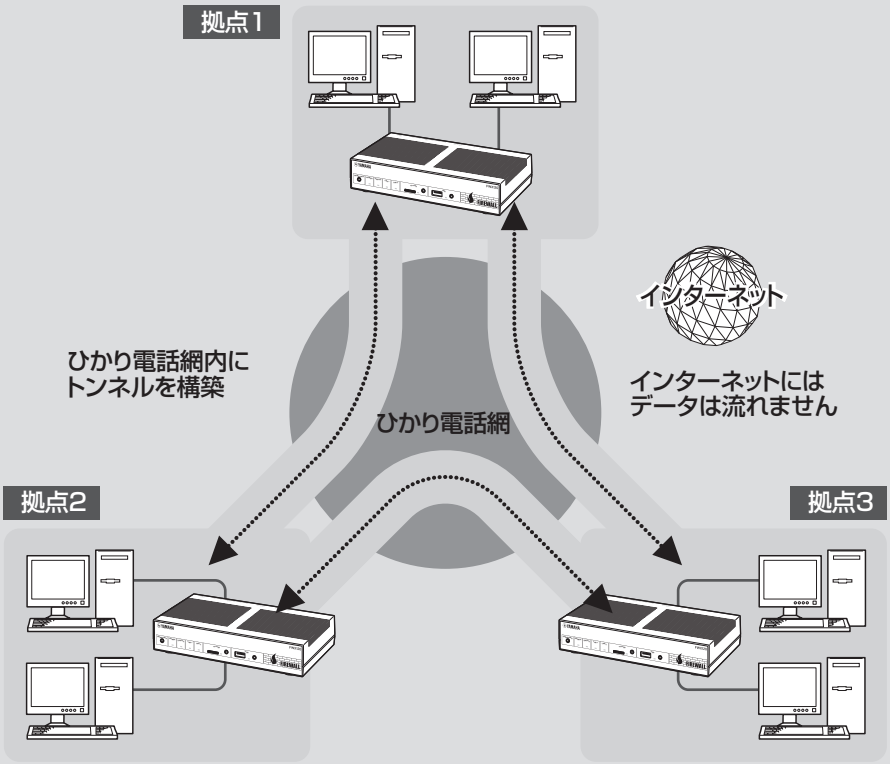


データコネクトを使用して、LAN同士を接続する

ご注意

本製品を透過型ファイアウォールとして利用している場合は、この機能を使用することができません。

本製品は、NTT東日本およびNTT西日本の「フレッツ 光ネクスト」で「ひかり電話」を利用した帯域確保型データ通信サービス「データコネクト」に対応しています。ここでは、データコネクトを使用してLAN同士を接続するときの設定方法を説明します。



設定する前に

- 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あらかじめ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。
- すでに異なるネットワークアドレスが設定されているLANに本製品を設置する場合には、設置するネットワークに合わせて本製品の設定を変更してください。詳しくは、「LAN1側IPアドレスを設定する」(53ページ)をご覧ください。

ご注意

- WAN側はONUと直結してください。HGWまたはONU一体型HGWに接続した場合、データコネクトを使用したLAN間接続はできません。
- ひかり電話ナンバー・ディスプレイが利用可能な回線を使用してください。ナンバー・ディスプレイに対応されていない回線では、データコネクトを使用したLAN間接続はできません。
- 従量課金制である場合、長時間通信したり大量のデータをやりとりすると高額な料金が発生します。ご使用にあたっては、通信料金について十分ご注意ください。
- LAN間接続を利用するときは、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、双方の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。
- データコネクトを使用したLAN間接続では、データが暗号化されずに転送されます。
- 本製品のLAN間接続機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- 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。

データコネクトでLAN間接続できるように設定する

本製品と相手機器をデータコネクトでLAN間接続して使用するために、「ひかり電話のデータコネクトを使用した拠点間接続」画面で必要な設定を行います。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ひかり電話のデータコネクトを使用した拠点間接続」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「VPN接続の設定」の「設定」
▶「設定可能なVPN設定」から設定を追加したいVPN接続先の「追加」
▶「ひかり電話のデータコネクトを使用した拠点間接続」を選んでから、「次へ」

- **IPsec**：IPsecを利用して接続します。
- **IPUDP**:IPIPトンネルを利用して接続します。

1 「ひかり電話のデータコネクトを使用した拠点間接続」画面で、必要な設定情報を入力する。

IPsecを選んだ場合

- **設定名：**接続先がわかるような名前を入力します。
- **認証鍵：**データの暗号化に使用する共有鍵を入力します。
- **本製品のひかり電話番号：**本製品に接続した回線の契約電話番号を市外局番から入力します。
- **接続相手のひかり電話番号：**接続相手の契約電話番号を市外局番から入力します。
- **使用帯域：**データ通信で使用する帯域を設定します。

ご注意

使用する帯域に応じて通信料金が異なりますのでご注意ください。

- **発信と着信：**本製品の発着信を許可するかどうかを設定します。
- **経路情報の設定：**「経路のアドレス情報」と「経路のネットマスク情報」に、接続先のLANのネットワークアドレスを入力します。
- **切断タイマ関連：**一定時間データの送受信がない場合に、セッションを自動切断するまでの時間を指定します。

IPUDPを選んだ場合

- **設定名：**接続先がわかるような名前を入力します。
- **本製品のひかり電話番号：**本製品に接続した回線の契約電話番号を市外局番から入力します。
- **接続相手のひかり電話番号：**接続相手の契約電話番号を市外局番から入力します。
- **使用帯域：**データ通信で使用する帯域を設定します。

ご注意

使用する帯域に応じて通信料金が異なりますのでご注意ください。

- **発信と着信：**本製品の発着信を許可するかどうかを設定します。
- **経路情報の設定：**「経路のアドレス情報」と「経路のネットマスク情報」に、接続先のLANのネットワークアドレスを入力します。
- **切断タイマ関連：**一定時間データの送受信がない場合に、セッションを自動切断するまでの時間を指定します。

2 「設定の確定」をクリックする。

「VPN接続設定の登録」画面が表示されます。

3 複数のLANと接続する場合は、「戻る」をクリックしてから「経路情報の設定」を繰り返し設定する。

接続相手ごとの経路情報をすべて設定してください。接続相手の経路情報の設定がすべて終わったら、「トップへ戻る」をクリックして、「かんたん設定ページ」のトップページに戻ります。

データコネクトで LAN間接続する

「かんたん設定ページ」のトップページで、「データコネクト接続」から接続したい相手の「接続」をクリックする。

設定した相手との間でLAN間接続します。

ご注意

設定した相手宛のパケットが発生した場合も、自動接続します。

データコネクトのLAN間接続を切断するには

「かんたん設定ページ」のトップページで、「データコネクト接続」の「切断」をクリックします。

ご注意

切断タイマが通信状態を監視しているため、データが一定時間通過しない場合は、セッションを自動切断します。

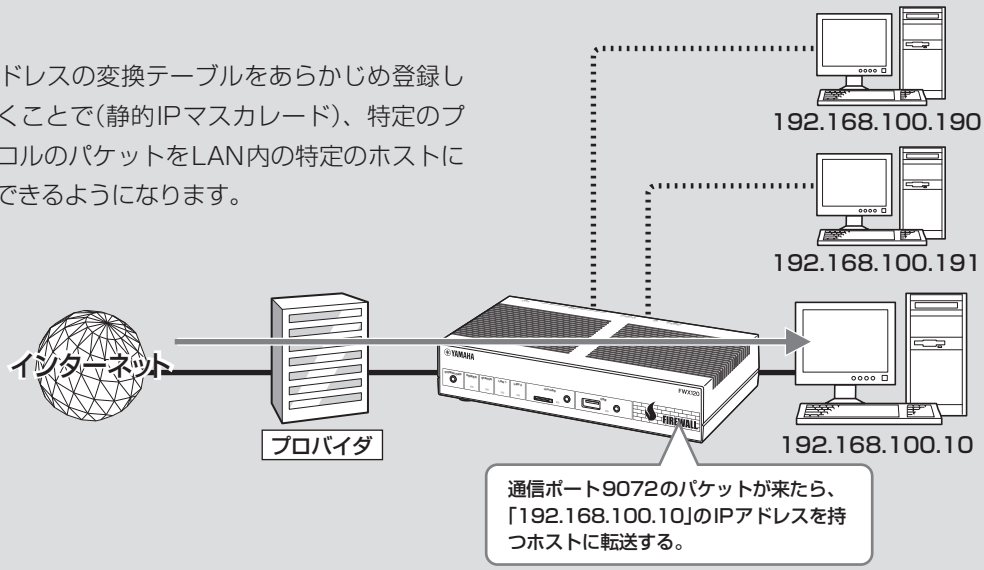
グローバルIPアドレスが必要なサービスをLAN内から利用する

グローバルIPアドレスが必要なアプリケーションソフトウェアを本製品のLAN側から利用しようとしても、正しく動作しない場合があります。以下のいずれかの方法で問題を解決してください。

1.プロトコルとポート番号、ホストのIPアドレスの変換テーブルを登録する(静的IPマスカレード)。
2.DMZホスト機能を利用する。

1. 静的IPマスカレード設定で問題を解決する

IPアドレスの変換テーブルをあらかじめ登録しておくことで(静的IPマスカレード)、特定のプロトコルのパケットをLAN内の特定のホストに送信できるようになります。



1. パソコンのIPアドレスを設定する

外部からのアクセスを許可するパソコンに、固定プライベートIPアドレスを設定します。

2. IPアドレスの変換テーブルを登録する

「静的IPマスカレードの登録」画面で、通信プロトコルとポート番号、ホストのIPアドレスの変換テーブルを登録します(静的IPマスカレード設定)。

ご注意

- プロトコルやポート番号については、利用するソフトウェアやサービスの説明書をご覧ください。
- 代表的なソフトウェアについては、「静的IPマスカレードの登録」画面で「ヘルプ」をクリックすると、使用するポート番号などの設定例を確認できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「静的IPマスカレードの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

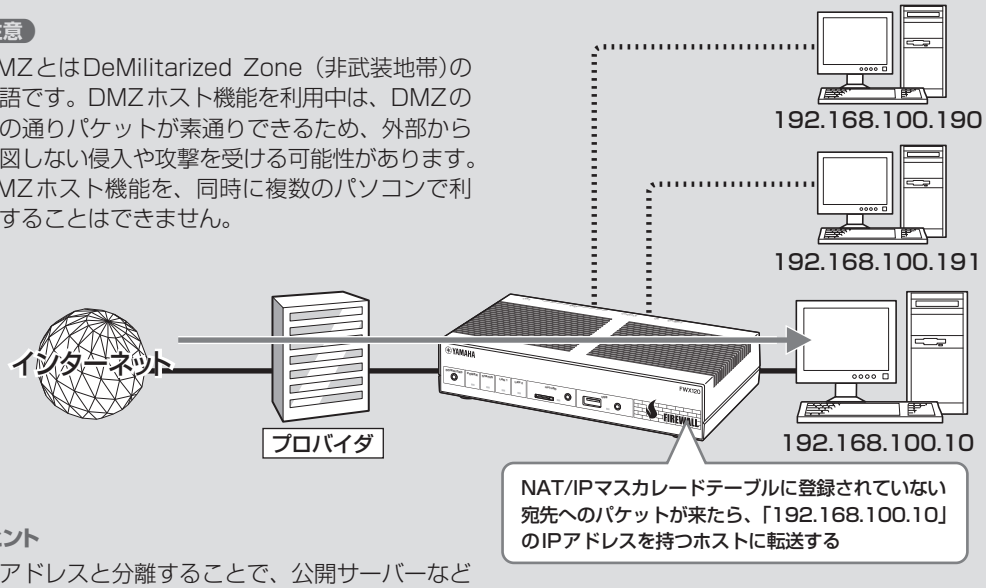
▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶「設定されているプロバイダの一覧」から設定を変更したい接続先の「設定」
▶「静的IPマスカレード関連」欄の「追加」

2. DMZホスト機能を使って問題を解決する

本製品がNAT/IPマスカレードテーブルに登録されていない宛先へのパケットを受信したときに、特定のIPアドレスのホストに転送するように設定できます（DMZホスト機能）。

ご注意

- DMZとはDeMilitarized Zone（非武装地帯）の略語です。DMZホスト機能を利用中は、DMZの名の通りパケットが素通りできるため、外部から意図しない侵入や攻撃を受ける可能性があります。
- DMZホスト機能を、同時に複数のパソコンで利用することはできません。



ヒント

内部アドレスと分離することで、公開サーバーなどが攻撃を受けても、他の内部アドレスのホストへの被害を防ぐことができます。

1. パソコンのIPアドレスを設定する

外部からのアクセスを許可するパソコンに、固定プライベートIPアドレスを設定します。

2. DMZホストのアドレスを指定する

「プロバイダの登録／修正」画面で、DMZホストのアドレスを設定します。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「プロバイダの登録／修正」画面を開くには

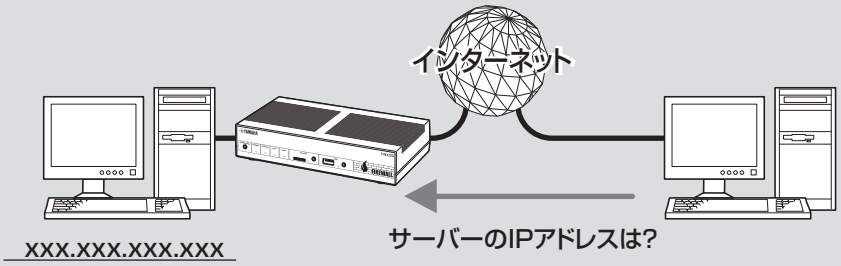
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶「設定されているプロバイダの一覧」から設定を変更したい接続先の「設定」

ネットボランチDNSサービスを利用する

ネットボランチDNSサービスとは?

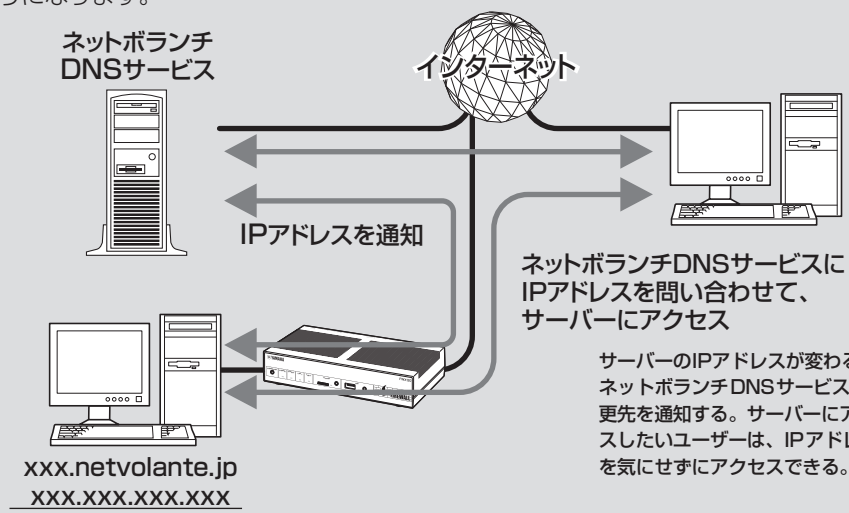
サーバーを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、サーバーのグローバルIPアドレスがわかっている必要があります。
しかし、インターネットに常時接続している場合でも、割り当てられるグローバルIPアドレスは再接続時または時間によって変更される場合があります。そのため、グローバルIPアドレスが固定で割り当てられない接続サービスを利用していると、サーバーを構築して公開することは困難でした。



サーバーのIPアドレスが変わってしまうので、接続する側がサーバーのIPアドレスを確認しながらアクセスする必要がある。

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ごとに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IPアドレスサービスを契約していなくて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とりしたりできるようになります。



サーバーのIPアドレスが変わると、ネットボランチDNSサービスに変更先を通知する。サーバーにアクセスしたいユーザーは、IPアドレスを気にせずにアクセスできる。

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ごとに設定を変更する必要がなくなり、便利です。

ご注意

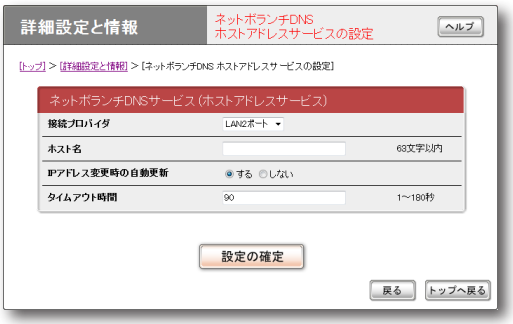
- ネットボランチDNSサービスは、端末型プロバイダ接続に対してのみ設定できます。ネットワーク型接続やLAN間接続には設定できません。なお、端末型CATVプロバイダ接続の設定でも、WAN側IPアドレスが固定アドレスの場合は設定できません。
- ホストアドレスは本製品1台につき1つしか取得できません。
- 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ネットボランチDNSサービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミックDNSサーバーに登録することはできません。
- 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。

ネットボランチDNSサービスでホストアドレスを取得する

ネットボランチDNSサービスを利用するには、「ネットボランチDNSホストアドレスサービスの設定」画面を使用します。

ご注意

- ホストアドレスは本製品1台につき1つしか取得できません。
- ホストアドレスサービスを設定するときは、希望のホスト名のみを「ホスト名」欄に入力してください。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ネットボランチDNSホストアドレスサービスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

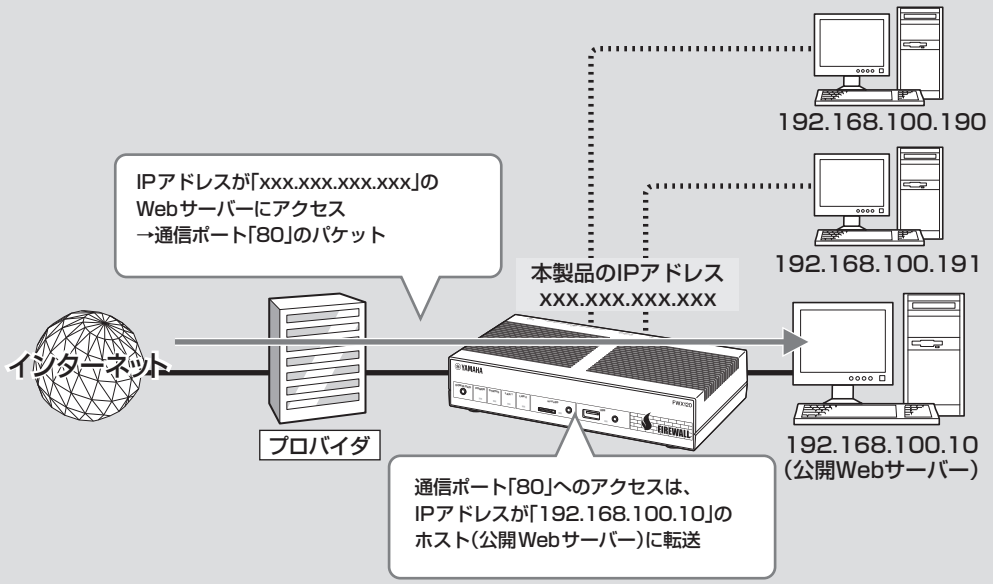
▶「ネットボランチDNSホストアドレスサービスの設定」の「設定」

ホストアドレスを取得できない場合は

- 契約プロバイダによっては、登録／更新してすぐに名前解決ができない場合があります。しばらく時間をおいてから再度試してみてください。
- プロバイダからグローバルIPアドレスが割り当てられているかどうかを確認してください。
- プロバイダの設定で指定したDNSサーバーのIPアドレスが正しいかどうかを確認してください。

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、IPアドレスの変換テーブルを登録します(静的IPマスカレード)。このあとに本製品にLAN外からのアクセスを許可するフィルターを設定すれば、特定のプロトコルのパケットをLAN内のサーバーに送信できるようになるため、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。



ご注意

LANの外部に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、破壊などにあう可能性があります。

ヒント

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。詳しくは「ネットボランチDNSサービスを利用する」(163ページ)をご覧ください。

設定の流れ

サーバーを公開するためには、次の設定が必要です。

本製品の設定

- プロトコルとポート番号、サーバーのIPアドレスの変換テーブルを登録する(静的IPマスカレード、166ページ)。

サーバーの設定

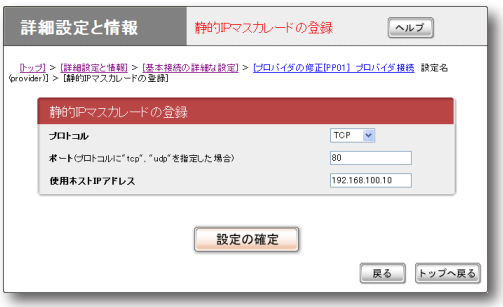
- サーバーのIPアドレスを設定する。
- WebやFTPなど、公開するサービスに合わせてファイルサーバーソフトの設定を変更する。

IPアドレスの変換テーブルを登録する

「静的IPマスカレードの登録」画面で、通信プロトコルとポート番号、サーバーのIPアドレスの変換テーブルを登録します（静的IPマスカレード設定）。

ご注意

- プロトコルやポート番号については、利用するソフトウェアやサービスの説明書をご覧ください。
- 代表的なソフトウェアについては、「静的IPマスカレードの登録」画面で「ヘルプ」をクリックすると、使用するポート番号などの設定例を確認できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

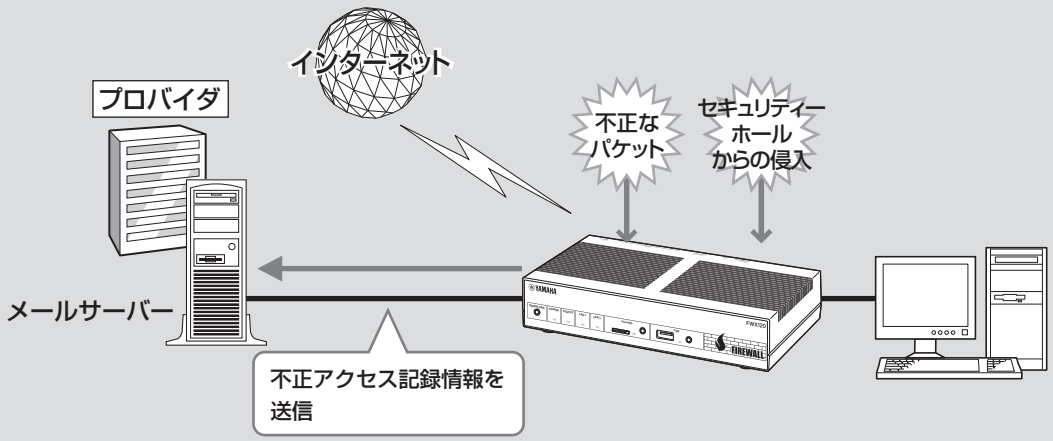
「静的IPマスカレードの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶「設定されているプロバイダの一覧」から設定を変更したい接続先の「設定」
▶「静的IPマスカレード関連」欄の「追加」

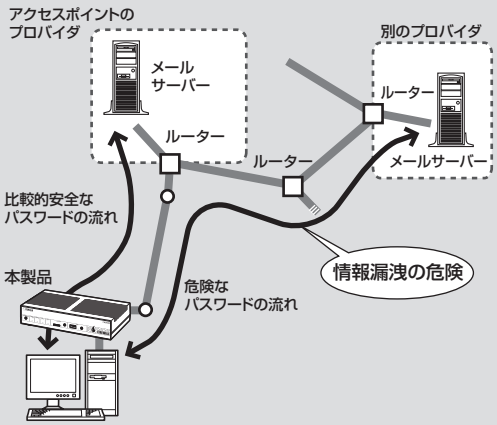
メール通知機能を使う

本製品の不正アクセス検知機能（107ページ）で検知した不正アクセス記録を、指定したメールアドレスへ送信できます（メール通知機能）。



ご注意

- SMTP認証を使用しないとパスワード情報などが暗号化されずにインターネット上に流れてしまいますので、十分ご注意ください。
  対応している認証方式についてはプロバイダにご確認ください。
- 電子メールソフトウェアでメールサーバーにメールを残すように設定している場合は、メールを確認するたびに新着メールが着信していることになります。新着メールがあるかどうかを正確に確認したい場合は、受信済みメールをサーバーに残さないように電子メールソフトウェアの設定を変更してください。



メール通知に使用するメールサーバーを登録する

「メールサーバーの設定」画面で、通知先のメール送信に使用するメールサーバーを登録します。

ご注意

接続先プロバイダは、プロバイダの設定画面で設定したプロバイダになります。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「メールサーバーの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「メール通知機能の設定」の「設定」
▶「メールサーバーの設定」欄の「追加」

メールサーバー登録を削除する場合は

「メール通知機能の設定」画面で、登録を削除したいメールサーバーの「削除」をクリックします。

不正アクセス検知をメールで通知する

本製品の不正アクセス検知機能（107ページ）で検知した不正アクセス記録を、指定したメールアドレスへ定期的に送信できます。外出先から不正アクセスや意図しない自動接続がないかどうか監視するときに便利です。

「通知内容の設定」画面で、送信先と送信する日時を設定します。

ご注意

接続先プロバイダは、自動接続先として設定されているプロバイダになります。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「通知内容の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「メール通知機能の設定」の「設定」
▶「通知内容の設定」欄の「追加」

IPv6環境で使う

本製品は次世代インターネットプロトコルである「IPv6」(Internet Protocol Version 6)をサポートしています。従来の「IPv4」に関する機能も継承しているため、既存のネットワークに影響を与えずに、IPv6を利用できます。

ご注意

プロバイダがIPv6に対応していない場合、IPv6環境でインターネットに接続できません。契約しているプロバイダがIPv6接続サービスを提供しているかどうか、あらかじめご確認ください。

IPv6を導入する前に

IPv6とIPv4環境を混在させる場合は

IPv6はIPv4との互換性がないため、両者をネットワーク上で混在させる場合は、移行技術(Transition Mechanism)と総称される仕組みが必要です。また、一般的にはIPv4からIPv6への移行は複数の段階を踏むことになるため、それぞれの段階に応じた移行技術が必要になります。

本製品では、IPv4ネットワークを経由してIPv6ネットワークを接続するための「IPv6 over IPv4トンネリング」、IPv6ネットワークを経由してIPv4ネットワークを接続するための「IPv4 over IPv6トンネリング」を移行技術としてサポートしています。

プロバイダからの設定情報を確認する

IPv6接続サービスを契約すると、以下の情報がプロバイダから提供されます。

- プレフィックス(アドレスブロック)
- 接続方法(ネイティブ接続／デュアルスタック接続／トンネル接続)
- トンネルの終端アドレス(トンネル接続の場合)
- 経路制御方法(RIPngを使うか使わないか。特に記載がない場合、RIPngは使用しません。)
- 接続の確認方法(pingの相手アドレスや、閲覧するWebサイトなど)

パソコン側にIPv6を導入する

Windows 7、Windows Vista でIPv6を導入する

Windows 7およびWindows Vistaでは、追加の設定をしなくてもIPv6を使用できます。

Windows XPでIPv6を導入する

コマンド プロンプトで、以下のコマンドを入力します。

```
ipv6 install
```

ヒント

IPv6環境の導入について詳しくは、「スタート」－「ヘルプとサポート」をクリックして表示される、Windows XPのヘルプをご覧ください。「検索」欄に「IPv6」と入力すると、関連する情報が表示されます。

本製品側でIPv6を使えるように設定する

設定を始める前に、「IPv6の設定」画面でIPv6で接続する相手（プロバイダ）を登録します。

ご注意

プロバイダを登録していない場合は、IPv6接続の操作を行ってもエラーが発生します。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「IPv6の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「IPv6の設定」の「設定」

IPv6接続を確認する

以下の手順で、IPv6環境が正しく設定されているかどうか確認します。

ご注意

本書ではWindows 7を例に説明します。
Windows XPの場合はコマンドがping6になりますが、操作は同じです。

ヒント

本製品とパソコンは、LANケーブルで接続した時点で通信可能になります。パソコン側での設定は、特に必要ありません。

1 LAN側の接続を確認する。

LAN1ポートに接続されたパソコンから、本製品のLAN1アドレスにpingを実行します。

応答があれば、正しく設定されています。

ヒント

本製品のLAN1アドレスは、プレフィックスに「1」をつけたアドレスになります。
例：プレフィックスが「fec0:12ab::/64」の場合

- LAN1アドレスは「fec0:12ab::1/64」になります。
- 本製品のLAN1アドレスにpingを実行するには、パソコンのコマンドプロンプトで「ping fec0:12ab::1」と入力してから、Enterキーを押します。

2 LAN側とWAN側の接続を確認する。

プロバイダへpingを実行したり、専用のWebサイトを閲覧するなど、プロバイダから指定されている確認手順を行います。

UPnP機能の動作設定を変更する

UPnP機能とは？

UPnPとはUniversal Plug and Playの略で、ネットワーク上でUPnP対応OSがUPnP対応機器を自動的に検出して、相互接続しやすくするための仕組みのことです。本製品はUPnPをサポートしているため、本製品を設置したLAN内にあるWindows搭載パソコンからWindows Live Messengerの音声チャットなどを利用できます。

ご注意

- 本製品のUPnP機能は、UPnP Forumで規定されている機能すべてに対応しているわけではありません。
- CATV接続など、プロバイダから割り当てられるIPアドレスがプライベートIPアドレスの場合は、UPnP機能を使用したWindows Live Messengerによる音声チャットは使用できません。
- 「かんたん設定ページ」でUPnP機能の設定を行うには、あらかじめ接続プロバイダを登録しておく必要があります。
- プロバイダを登録せずにWindows Live MessengerなどのUPnP環境を必要とするソフトウェアを起動すると、本製品との通信に時間がかかるようになります。この場合は、接続プロバイダを登録するか、UPnP機能を停止してください。
- Windows Live Messengerの終了／起動を繰り返したり、本製品の再起動や回線の切断などによってパソコンと本製品でUPnP機能の情報が異なると、正常に接続できなくなることがあります。
  この場合は、回線を接続した状態でいったんWindows Live Messengerをサインアウトしてから、Windows Live Messengerを再起動します。それでも接続できない場合は、パソコンを再起動してください。

UPnP機能を使えるように設定する

本製品のUPnP機能は工場出荷状態では「使用しない」になっているため、起動するために設定を変更してください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「UPnPの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「UPnPの設定」の「設定」

パソコン側でUPnP機能を使えるか確認する

以下の手順で、お使いのパソコンがUPnP機能を使える状態かどうか確認してください。

ヒント

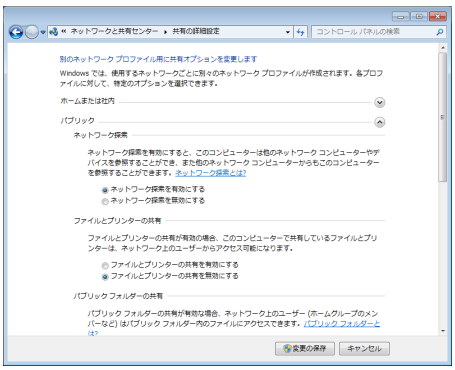
UPnP環境の導入について詳しくは、「スタート」−「ヘルプとサポート」をクリックして表示される、ヘルプをご覧ください。「検索」欄に、Windows 7およびWindows Vistaでは「ネットワーク探索」、Windows XPでは「UPnP」と入力すると、関連する情報が表示されます。

Windows 7の場合

1 **「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。**

2 **「ネットワークとインターネット」から「ネットワークの状態とタスクの表示」をクリックする。**

3 **「共有の詳細設定の変更」をクリックして、「ネットワーク探索」の「ネットワーク探索を有効にする」にチェックが付いているかを確認する。**



- チェックが付いている場合は、パソコン側でUPnP機能が利用できるようになっています。
- チェックが付いていない場合は、チェックを付けてから、「変更の保存」をクリックします。

Windows Vistaの場合

1 **「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。**

2 **「ネットワークとインターネット」から「ネットワークの状態とタスクの表示」をクリックする。**

3 **「共有と探索」の「ネットワーク探索」をクリックしてから、「ネットワーク探索を有効にする」にチェックが付いているかを確認する。**

- チェックが付いている場合は、パソコン側でUPnP機能が利用できるようになっています。
- チェックが付いていない場合は、チェックを付けてから、「適用」をクリックします。

Windows XPの場合

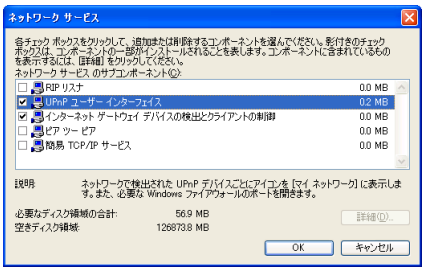
1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

2 「プログラムの追加と削除」をクリックする。

3 画面左側の「Windowsコンポーネントの追加と削除」をクリックする。

4 「ネットワーク サービス」をクリックして選んでから、「詳細」をクリックする。

5 「UPnP ユーザー インターフェイス」にチェックが付いているかを確認する。



- チェックが付いている場合は、パソコン側でUPnP機能が利用できるようになっています。
- チェックが付いていない場合は、引き続き手順6以降の操作を行います。

6 「UPnP ユーザー インターフェイス」にチェックを付けてから、「OK」をクリックする。

7 「次へ」をクリックする。

以後は画面の指示に従って、インストールを行ってください。

ヤマハスイッチを制御する

本製品の設定画面から、ヤマハスイッチの設定変更や状態確認が行えます。
ヤマハスイッチの設定変更や状態確認をするには、下記の手順で操作します。

1 スイッチ制御の「基本設定」画面で、必要な設定項目を変更する。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

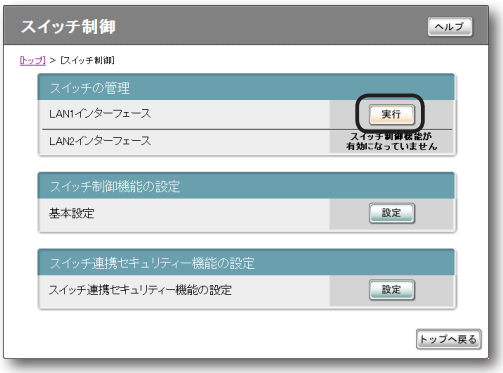
スイッチ制御の「基本設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「スイッチ制御」
▶「基本設定」の「設定」

2 「設定の確定」をクリックしてから、「トップへ戻る」をクリックする。

3 「スイッチ制御」画面で、ヤマハスイッチを接続したLANインターフェースの「実行」をクリックする。



選んだLANインターフェースに接続されているヤマハスイッチがツリー表示されます。
設定内容について詳しくは、ヤマハスイッチの取扱説明書をご覧ください。

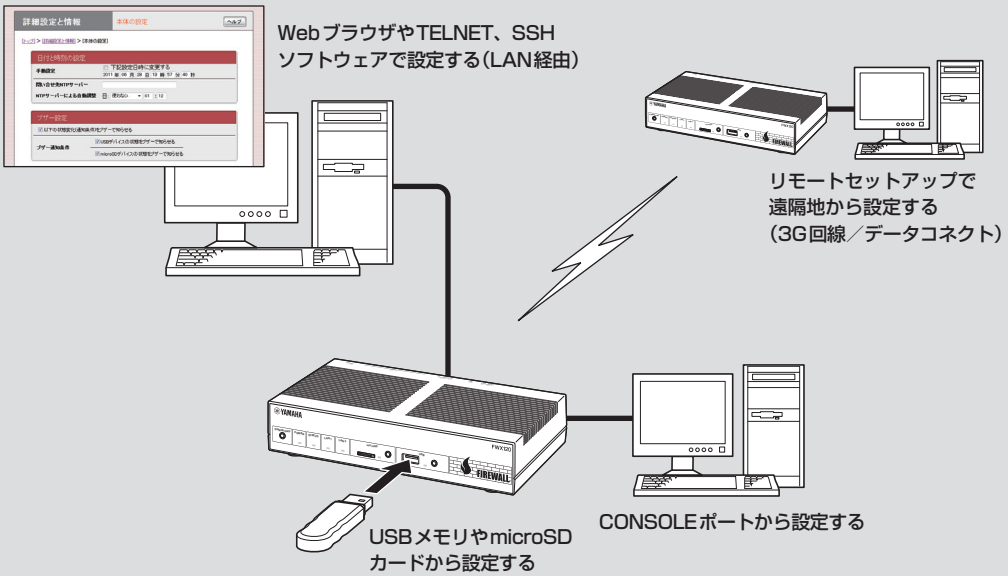
「スイッチ制御」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「スイッチ制御」

本製品の設定を変更する

本製品の機能は、以下の操作方法で設定したり、設定を確認したりできます。
一番操作しやすい方法でお使いください。



利用できる設定方法の種類

パソコンのWebブラウザで設定する(25、44ページ)
本製品にパソコンを接続している場合は、Webブラウザで本製品内蔵の「かんたん設定ページ」を開いて本製品の状態を見たり、各種機能を設定したりすることができます。

コンソールコマンドで設定する(176ページ)
TELNET、SSHソフトウェアを使ってコンソール画面からコマンドを入力して、本製品の状態を確認したり、各種機能を設定できます。
また、本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、コマンドを入力することもできます。コンソールコマンドを使うと、他の方法よりも、より詳細な設定を行うことができます。

外部メモリで設定する(181ページ)
市販の外部メモリ(USBメモリまたはmicroSDカード)に保存した設定ファイルを本製品に読み込ませて、設定を変更できます。

コンソールコマンドで設定する

本製品に直接コマンド(コンソールコマンド)を送って、本製品の機能を設定できます。TELNET、SSH経由で設定を変更するだけでなく、「かんたん設定ページ」からコンソールコマンドを入力して実行することもできます。TELNET、SSH経由で設定を変更する場合は、お使いの環境に対応したTELNET、SSHソフトウェアをご用意ください。

コンソールコマンドとは？

コンソールコマンドは、本製品に直接命令を送って、機能を設定する方法です。コンソールコマンドを使うと、他の方法よりも、詳細な設定を行うことができます。コンソールコマンドの詳細については、「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

ご注意

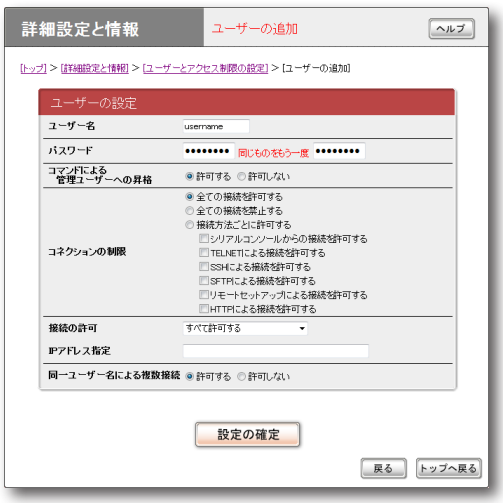
コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。「かんたん設定ページ」で設定後にコンソールコマンドで設定を変更すると、意図しない動作につながることがあります。設定後に意図した動作をするか、必ずご確認ください。

ヒント

本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、本製品をコンソールコマンドで設定することもできます(179ページ)。

TELNET、SSH、SFTPのユーザーを登録する

「ユーザーの追加」画面でTELNET、SSHでログインするユーザーを登録します。TELNETでは、ユーザーを登録しなくても無名ユーザーとしてログインすることができますが、SSHでは登録ユーザーでなければログインすることができません。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザーの追加」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」
▶「ユーザーとパスワードの設定」欄にある「ユーザーの登録数」の「設定」

SSHでログインできるように設定する

本製品のSSHサーバー機能は工場出荷状態では「使用しない」になっています。SSHでログインするためには、「ユーザーとアクセス制限の設定」画面の「SSH・SFTPサーバー機能」欄で設定を「使用する」に変更してください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザーとアクセス制限の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「ユーザーとアクセス制限の設定(HTTP、TELNET、SSH、SFTP)」の「設定」

SSHで接続する

ご使用になるSSHソフトウェアの使用方法に従ってください。

TELNETで接続する

パソコンからの接続について、Windows 7標準のTELNETを使用する場合を例に説明します。

ヒント

Windows 7では、あらかじめ以下の方法でTELNETを有効にする必要があります。

1 「コントロールパネル」−「プログラム」−「プログラムと機能」で、「Windowsの機能の有効化または無効化」を選ぶ。

2 「Windowsの機能」画面で「Telnetクライアント」にチェックを付けてから、「OK」をクリックする。

1 「スタート」メニューから「プログラムとファイルの検索」を選ぶ。

2 「telnet 192.168.100.1」と入力してからEnterキーを押す。

本製品のIPアドレスを変更している場合には、「192.168.100.1」のかわりに本製品のIPアドレスを入力します。

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

何も表示されないときは、一度Enterキーを押します。

TELNETの場合、ここで入力するパスワードは、無名ユーザーのログインパスワードです。

無名ユーザーとしてではなく、登録ユーザーとしてログインするときは

何も入力せずにEnterキーのみを押すと、「Username:」というプロンプトが表示されます。また、すでに無名ユーザーでログインしている場合および無名ユーザーでのログインを禁止している場合は、最初から「Username:」というプロンプトが表示されます。

「Username:」に対して登録ユーザー名を入力すると「Password:」が表示されるので、登録ユーザーのログインパスワードを入力します。

パスワードを設定していない無名ユーザーでログインするときは

「Username:」とそれに続く「Password:」に対して何も入力せずに、Enterキーを押します。

「>」が表示されると、コンソールコマンドを入力できるようになります。

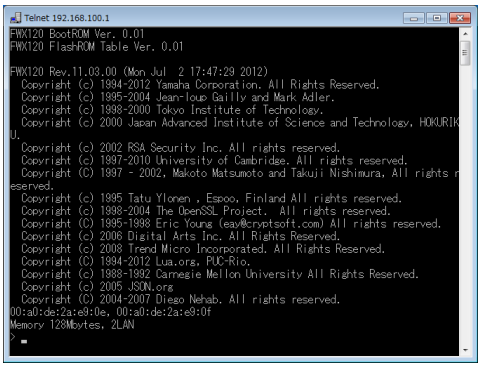
ヒント

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

4 「administrator」と入力してから、Enterキーを押す。

5 「Password:」と表示されたら、管理パスワードを入力する。

「#」が表示されると、各種のコンソールコマンドを入力できます。



6 コンソールコマンドを入力して、設定する。

7 設定が終わったら、「save」と入力してからEnterキーを押す。

コンソールコマンドで設定した内容が、本製品の内蔵メモリに保存されます。

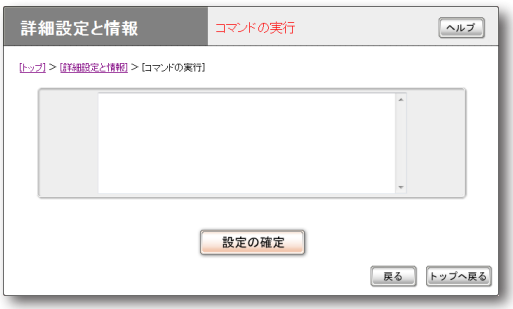
8 設定を終了するには、「quit」と入力してからEnterキーを押す。

9 コンソール画面を終了するには、もう一度「quit」と入力してからEnterキーを押す。

「かんたん設定ページ」でコンソールコマンドを使用する

「コマンドの実行」画面で行います。

コンソールコマンドを入力してから「実行」をクリックすると、コマンドの実行結果が表示されます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「コマンドの実行」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「コマンドの実行」の「実行」

CONSOLEポートから設定する

本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、本製品をコンソールコマンドで設定できます。

「ユーザーとアクセス制限の設定」画面で、Webブラウザ(HTTP)やTELNET、SSH、SFTPソフトウェアからのアクセスを禁止しておけば(120ページ)、本製品の設定を変更できるのは本製品に物理的にアクセスできる立場のユーザーだけになり、セキュリティーを強化するために役立ちます。

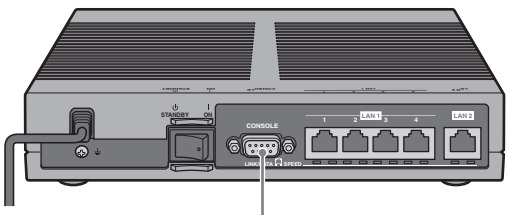
起動時に使用する設定ファイルを、ターミナルソフトウェアから指定することもできます。

ご注意

- ここではWindows XPのハイパーターミナルを使用した場合の操作を説明します。Windows Vista以降のWindowsにはハイパーターミナルが搭載されていないため、各社から提供されているシリアルデバイス制御用のターミナルソフトウェアをお使いください。
- ターミナルソフトウェアの使用方法について詳しくは、各ソフトウェアの取扱説明書をご覧ください。

CONSOLEポートとパソコンを接続する

本製品のCONSOLE ポートとパソコンのシリアルポートを、クロスタイプのシリアルケーブルで接続します。



CONSOLEポート

ヒント

シリアルケーブルの両端のコネクタは、本製品(D-sub9ピン、オス)とパソコンに適合したタイプをご使用ください。

CONSOLEポート番号を確認する

接続に使用するパソコンのシリアルポートが、どのCOMポート番号に割り当てられているのかを確認します。

1 「スタート」メニューから「マイ コンピュータ」をクリックする。

2 「マイ コンピュータ」画面左側の「システムのタスク」欄にある、「システム情報を表示する」をクリックする。

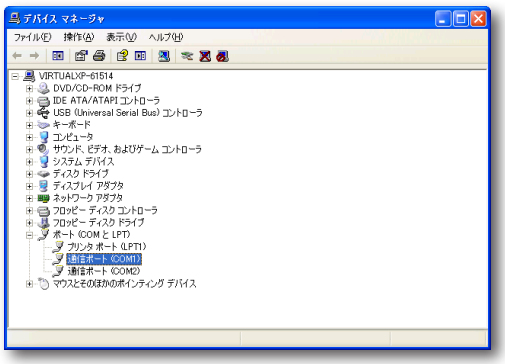
「システムのプロパティ」画面が表示されます。

3 「ハードウェア」タブをクリックする。

4 「デバイス マネージャ」をクリックする。

「デバイス マネージャ」画面が表示されます。

5 「ポート(COMとLPT)」を展開して、「通信ポートのポート番号」(COMx)を確認する。



通常は「COM1」が割り当てられています。

6 「デバイス マネージャ」画面と「システムのプロパティ」画面を閉じる。

CONSOLEポートを指定して接続する

CONSOLEポートに接続しているパソコンからターミナルソフトウェアで本製品にログインし、コンソールコマンドを送信して設定します。ここでは、Windows XPのハイパーターミナルを使用する場合を例に説明します。

ご注意

コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。「かんたん設定ページ」で設定後にコンソールコマンドで設定を変更すると、意図しない動作につながることがあります。設定後に意図した動作をするか、必ずご確認ください。

ヒント

コンソールコマンドの詳細については、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

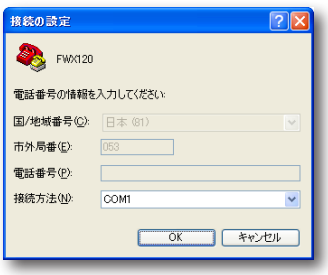
1 **「スタート」メニューから「すべてのプログラム」−「アクセサリ」−「通信」−「ハイパーターミナル」をクリックする。**

「接続の設定」画面が表示されます。

2 **「名前」欄に接続名を入力してから、「OK」をクリックする。**

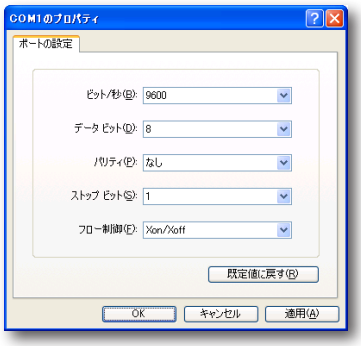
接続名は自由に設定してください。

3 **179 ページの「CONSOLEポート番号を確認する」で確認したパソコンのシリアルポート番号を選んでから、「OK」をクリックする。**



「COMxのプロパティ」画面が表示されます。

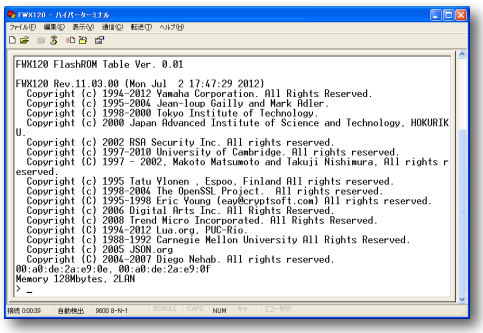
4 **通信設定を以下の値に変更する。**



- ビット/秒：9600
- データビット：8
- パリティ：なし
- ストップビット：1
- フロー制御：Xon/Xoff

5 **「OK」をクリックする。**

ハイパーターミナルの画面が表示されます。



以後の操作は、「TELNETで接続する」（177ページ）の手順3以降と同じです。

外部メモリから設定する

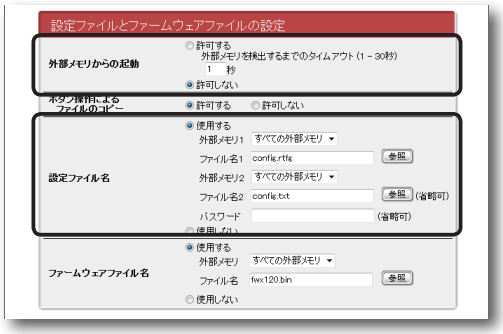
市販の外部メモリ（USBメモリ／microSDカード）に保存した設定ファイルを本製品に読み込ませて、設定を変更できます。複数の本製品の設定を変更したい場合などに便利です。

ご注意

- 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メモリなどの外部メモリを本製品に接続することはできません。
- USB延長ケーブルは、種類によっては動作しないことがあります。USBメモリは本製品のUSBポートに直接挿入してご使用ください。
- 本製品のUSBランプまたはmicroSDランプが点灯／点滅している間は、外部メモリを取り外さないでください。外部メモリ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ランプまたはmicroSDランプが消灯していることを確認してから外部メモリを取り外してください。

外部メモリ内の設定ファイルを本製品に読み込めるように、設定を変更する

「外部デバイスの設定」画面の「外部メモリからの起動」欄で、「許可しない」を選びます。また、「設定ファイル名」欄で、本製品にコピーする設定ファイルのファイル名を指定します。



「外部デバイスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「外部デバイスの設定」の「設定」

本製品の前面ボタンを押して設定ファイルを読み込む

1 設定ファイルを保存した外部メモリを用意する。

ファイル名は「外部デバイスの設定」画面の「設定ファイル名」欄で指定したファイル名と同じにします。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 USBボタンまたはmicroSDボタンを押しながらDOWNLOADボタンを3秒間押し続ける。

手順1で用意した設定ファイルが本製品に読み込まれ、読み込みが終わると本製品は自動的に再起動します。再起動後は、読み込んだ設定ファイルの設定で動作します。

ご注意

「外部デバイスの設定」画面の「外部メモリからの起動」欄で「許可する」が選ばれていると、外部メモリ内の設定ファイルから起動していますので、外部メモリを取り外さないでください。

ヒント

「外部デバイスの設定」画面の「ファームウェアファイル名」欄で指定したファイル名のファームウェアファイルが外部メモリ内に存在する場合は、引き続きファームウェアファイルのコピーが始まります。

4 USBボタンまたはmicroSDボタンを2秒間押し続ける。

本製品のUSBランプまたはmicroSDランプが消灯します。

5 外部メモリを取り外す。

ご注意

外部メモリからの設定ファイルの読み込みに失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

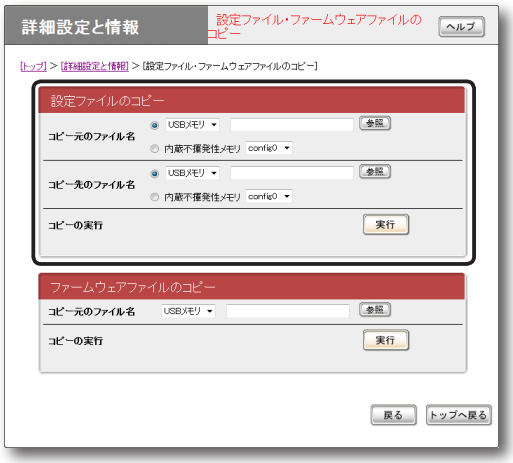
「かんたん設定ページ」から外部メモリ内の設定ファイルを読み込む

1 設定ファイルを保存した外部メモリを用意する。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 「設定ファイル・ファームウェアファイルのコピー」画面の「コピー元のファイル名」欄で、外部メモリから本製品に読み込ませたい設定ファイル名を指定する。



「設定ファイル・ファームウェアファイルのコピー」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「設定ファイル・ファームウェアファイルのコピー」の「実行」

4 「コピー先のファイル名」欄で、「内蔵不揮発性メモリ」を選び、config番号を指定する。

ヒント

「内蔵不揮発性メモリ」の代わりに他の外部メモリを指定すると、本製品を使用して設定ファイルを他の外部メモリにコピーすることもできます。

5 「実行」をクリックする。

確認画面が表示されます。

6 「実行」をクリックする。

手順1で用意した設定ファイルが本製品に読み込まれます。設定ファイルの読み込みが終わると、本製品は自動的に再起動します。

再起動後は、読み込んだ設定ファイルの設定で動作します。

ご注意

「外部デバイスの設定」画面の「外部メモリからの起動」欄で「許可する」が選ばれていると、外部メモリ内の設定ファイルから起動していますので、外部メモリを取り外さないでください。

7 USBボタンまたはmicroSDボタンを2秒間押し続ける。

本製品のUSBランプまたはmicroSDランプが消灯します。

8 外部メモリを取り外す。

ご注意

外部メモリからの設定ファイルの読み込みに失敗した場合は、「USBデバイスが使用できない」（213ページ）をご確認ください。

外部メモリ内の設定ファイルで本製品を運用する

市販の外部メモリ（USBメモリ／microSDカード）に保存した設定ファイルで本製品を運用できます。本製品内の設定ファイルを変更することなく、緊急用の設定ファイルを外部メモリに保存しておき、必要に合わせて使用したい場合などに便利です。

外部メモリ内の設定ファイルで本製品を起動できるように、設定を変更する

「外部デバイスの設定」画面の「外部メモリからの起動」欄で、「許可する」を選びます。

「外部デバイスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「外部デバイスの設定」の「設定」

外部メモリ内の設定ファイルで本製品を起動する

1 設定ファイルを保存した外部メモリを用意する。

ファイル名は「外部デバイスの設定」画面の「設定ファイル名」欄で指定したファイル名と同じ名前にします。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 本製品を再起動する。

再起動をすると、手順1で指定した設定ファイルが自動で読み込まれます。

ヒント

本製品内に保存されている設定ファイルの内容は上書きされません。ただし、再起動後に設定を変更した場合は、本製品内に保存されている設定ファイルに上書きされます。

ご注意

外部メモリからの設定ファイルの読み込みに失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

ブザー音の設定を変更する

本製品にはブザーが内蔵されており、工場出荷状態では以下の場合にブザー音が鳴るように設定されています。

- USBデバイスの状態が変化したとき
- microSDデバイスの状態が変化したとき

ヒント

その他のブザー音設定については、「コマンドリファレンス」（付属CD-ROMに収録）の各種アラーム音の設定をご覧ください。

「本体の設定」画面で、ブザー音の設定を変更できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「本体の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「本体の設定（日付・時刻、ブザー）」の「設定」

運用状況を統計グラフで確認する

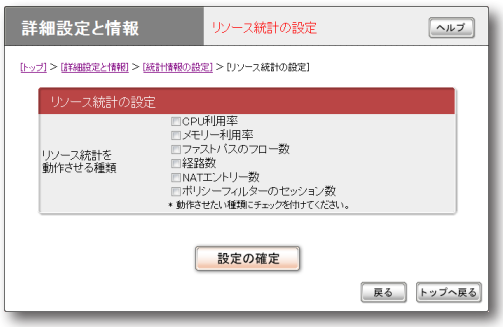
内部リソース状況と本製品で管理しているトラフィック状況について、統計情報を視覚的に表示できます。本製品を運用・管理するにあたっての基本的な情報として、役立てることができます。

本製品のリソースの統計を確認する

本製品のCPUや内部メモリの利用率、FLOW数や経路数、NATエントリー数を過去30日間分統計表示できます。

リソース統計を設定する

リソース統計は初期設定では表示しないようになっています。「リソース統計の設定」画面でリソース統計を表示するように設定を変更して、表示対象となる情報を指定します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「リソース統計の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「統計情報の設定」の「設定」
▶「リソース統計」欄の「設定」
▶「リソース統計の設定」の「設定」

リソース統計を表示する

「リソース統計の表示」画面で、リソースの情報を確認できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「リソース統計の表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

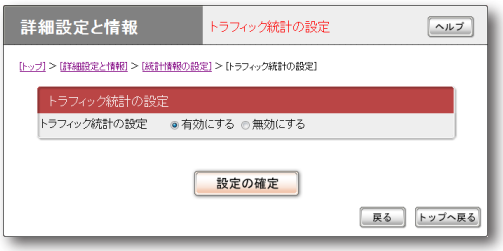
▶トップページの「詳細設定と情報」
▶「統計情報の表示」の「実行」
▶「リソース統計」欄の「実行」

トラフィック統計を確認する

本製品の各インターフェースのトラフィック状況を過去30日間分統計表示できます。

トラフィック統計を設定する

トラフィック統計は初期設定では表示しないようになっています。「トラフィック統計の設定」画面で、トラフィック統計を表示するように設定を変更します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「トラフィック統計の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「統計情報の設定」の「設定」
▶「トラフィック統計」欄の「設定」
▶「トラフィック統計の設定」の「設定」

トラフィック統計を表示する

「トラフィック統計の表示」画面で、トラフィックの情報を確認できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「トラフィック統計の表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「統計情報の表示」の「実行」
▶「トラフィック統計」欄の「実行」

QoSの動作状況を確認する

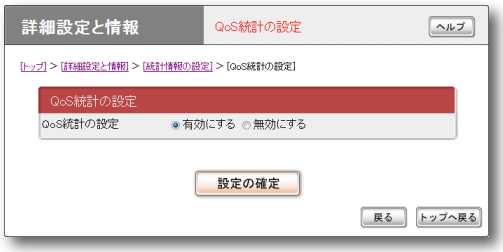
本製品でQoS機能を利用している場合に、各クラスの状態を過去20分間分統計表示できます。

ヒント

QoS機能を利用するには、コマンドで設定を行う必要があります。詳しくは「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

QoS統計を設定する

QoS統計は初期設定では表示しないようになっています。「QoS統計の設定」画面で、QoS統計を表示するように設定を変更します。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

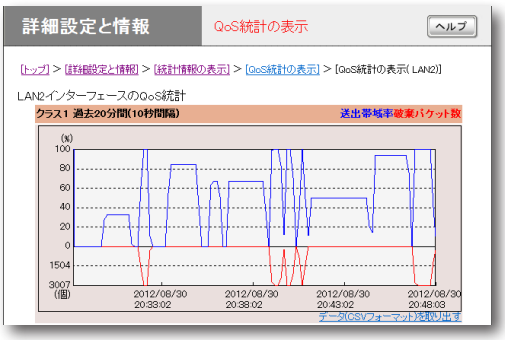
「QoS統計の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「統計情報の設定」の「設定」
▶「QoS統計」欄の「設定」
▶「QoS統計の設定」の「設定」

QoS統計を表示する

「トラフィック統計の表示」画面で、トラフィックの情報を確認できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

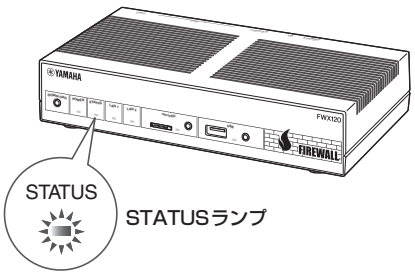
「QoS統計の表示」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「統計情報の表示」の「実行」
▶「QoS統計」欄の「実行」

STATUSランプで通信状態を確認する

本各接続設定でキープアライブ機能を有効にしている場合は、接続先の機器との通信が不可能な状態になっているか、本製品のSTATUSランプで確認できます。



「かんたん設定ページ」のトップページを表示せずに通信状態を確認できるので便利です。

ヒント

- 「かんたん設定ページ」からプロバイダ接続やVPN接続(IPsec、L2TP/IPsec、PPTPのLAN間接続、IPIPトンネル)を設定する場合は、初期設定画面のキープアライブ機能は「有効」になっています。
- キープアライブが有効になっているかを確認するには、それぞれの接続の設定画面をご覧ください。

「PPPoEを用いる端末型ブロードバンド接続(フレッツ 光ネクスト、Bフレッツなど)」接続の設定画面の例

STATUSランプが点灯しているときは

キープアライブ機能を有効に設定した接続において、接続先の機器との通信が不可能な状態になっています。

ご注意

- キープアライブ機能は通信が不可能な状態を検出するまでに時間がかかります。そのため、STATUSランプが点灯していない状態でも、接続先の機器と通信ができない場合があります。
- DOWNLOADボタンからファームウェアのリビジョンアップを実行した場合も、STATUSランプは点灯します。DOWNLOADボタンからリビジョンアップを行った時の動作については「DOWNLOADボタンでリビジョンアップする」(189ページ)をご覧ください。

問題が解消すると

STATUSランプは消灯します。

最新の機能を利用する（リビジョンアップ）

インターネットから本製品の機能を管理するプログラム（ファームウェア）をダウンロードして、最新の機能をご利用いただけます（リビジョンアップ）。

ご注意

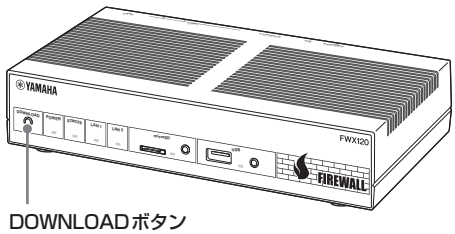
- リビジョンアップを始めたら、完了して本製品が再起動するまで他の操作は絶対に行わないでください。万一、中断したときは本製品が使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- リビジョンアップ中は、POWERランプ以外の前面ランプが順番に点滅します。
- リビジョンアップ中は、すべての通信が切断されます。
- リビジョンアップ中は、絶対にケーブル類を抜かないでください。本製品が使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- 「かんたん設定ページ」の「リビジョンアップの実行」画面では、正式にリリースされたバージョンのファームウェアにのみリビジョンアップできます。ヤマハによる正式な動作保証のないβ版のファームウェアは、「かんたん設定ページ」を使ってリビジョンアップすることはできません。

ヒント

「かんたん設定ページ」の「リビジョンアップの実行」画面で、「リビジョンダウンの許可」を「許可する」に変更すると、リビジョンダウン（旧バージョンのファームウェアに更新）も実行できます。詳しくは「リビジョンアップの実行」画面のヘルプをご覧ください。

DOWNLOADボタンでリビジョンアップする

「DOWNLOADボタンの設定」画面でリビジョンアップを「許可する」に設定している場合は、本製品前面のDOWNLOADボタンを3秒間押し続けるだけで、リビジョンアップを実行できます。



DOWNLOADボタン

ご注意

リビジョンアップを実行する前に「DOWNLOADボタンご使用時のソフトウェアライセンス契約について」（13ページ）をご確認ください。

ヒント

DOWNLOADボタンでリビジョンアップを実行する場合、本製品のランプでリビジョンアップの状態を確認できます。
ファームウェアのダウンロードが完了して、リビジョンアップが開始されると、POWERランプ以外の前面ランプが順番に点滅します。

DOWNLOADボタンによるリビジョンアップを許可する

「DOWNLOADボタンの設定」画面で行います。

DOWNLOADボタンによるリビジョンアップを行いたいときは、「リビジョンアップ」を選びます。設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DOWNLOADボタンの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「DOWNLOADボタンの設定」の「設定」

DOWNLOADボタンを押してリビジョンアップする

DOWNLOADボタンを3秒間押し続けると、新しいリビジョンのファームウェアの有無をチェックします。新しいリビジョンのファームウェアが見付かった場合は、自動的にファームウェアをダウンロードしてから、リビジョンアップが実行されます。

ご注意

ファームウェアのダウンロード、またはリビジョンアップに失敗した場合は、「DOWNLOADボタンが機能しない」(212ページ)をご確認ください。

リビジョンアップが終了すると

本製品が再起動します。

「かんたん設定ページ」でリビジョンアップする

「リビジョンアップの実行」画面で行います。

「実行」をクリックすると、新しいリビジョンのファームウェアの有無をチェックします。新しいリビジョンのファームウェアが見付かった場合は、画面に今のリビジョン番号と新しいリビジョン番号が表示されます。その状態でもう一度「実行」をクリックすると、ファームウェアのダウンロード後に自動でリビジョンアップが実行されます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

ヒント

「リビジョンアップの実行」画面で「リビジョンダウンの許可」を「許可する」に変更すると、リビジョンダウン(旧バージョンのファームウェアに更新)も実行できます。

「リビジョンアップの実行」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「リビジョンアップの実行」の「実行」

リビジョンアップが終了すると

本製品が再起動します。

外部メモリから リビジョンアップする

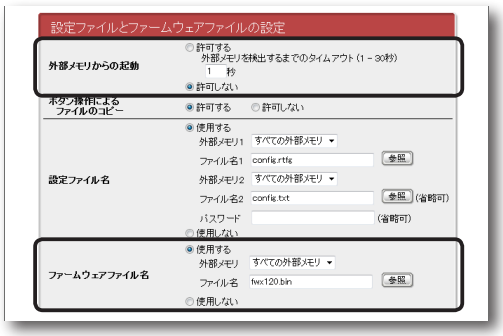
市販の外部メモリ（USBメモリ／microSDカード）に保存したファームウェアを本製品に読み込ませて、リビジョンアップできます。ファームウェアのバージョンを管理したり、複数の本製品のファームウェアを変更したい場合などに便利です。

ご注意

- 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メモリなどの外部メモリを本製品に接続することはできません。
- USB延長ケーブルは、種類によっては動作しないことがあります。USBメモリは本製品のUSBポートに直接挿入してご使用ください。
- 本製品のUSBランプまたはmicroSDランプが点灯／点滅している間は、外部メモリを取り外さないでください。外部メモリ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ランプまたはmicroSDランプが消灯していることを確認してから外部メモリを取り外してください。

外部メモリからリビジョンアップできるように設定を変更する

「外部デバイスの設定」画面の「外部メモリからの起動」欄で、「許可しない」を選びます。また、「ファームウェアファイル名」欄で、リビジョンアップに使用するファームウェアのファイル名を指定します。



「外部デバイスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「外部デバイスの設定」の「設定」

本製品の前面ボタンを押してリビジョンアップを実行する

1 ファームウェアを保存した外部メモリを用意する。

ファイル名は「外部デバイスの設定」画面の「ファームウェアファイル名」欄で指定したファイル名と同じ名前にします。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 USBボタンまたはmicroSDボタンを押しながらDOWNLOADボタンを3秒間押し続ける。

手順1で用意したファームウェアが本製品に読み込まれ、ファームウェアの読み込みが終わるとリビジョンアップが始まります。

リビジョンアップが終了すると、本製品は自動的に再起動します。

ご注意

「外部デバイスの設定」画面の「外部メモリからの起動」欄で「許可する」が選ばれていると、外部メモリ内のファームウェアから起動していますので、外部メモリを取り外さないでください。

ヒント

「外部デバイスの設定」画面の「設定ファイル名」欄で指定したファイル名の設定ファイルが外部メモリ内に存在する場合は、設定ファイルのコピーが先に行われます。

4 USBボタンまたはmicroSDボタンを2秒間押し続ける。

本製品のUSBランプまたはmicroSDランプが消灯します。

5 外部メモリを取り外す。

ご注意

外部メモリからのリビジョンアップに失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

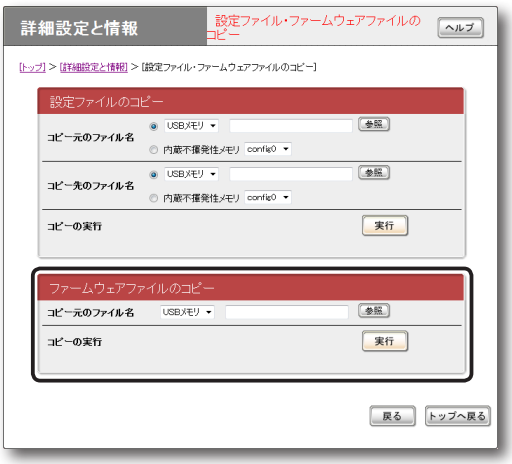
「かんたん設定ページ」から外部メモリ内のファームウェアでリビジョンアップする

1 ファームウェアを保存した外部メモリを用意する。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 「設定ファイル・ファームウェアファイルのコピー」画面の「コピー元のファイル名」欄で、外部メモリから本製品に読み込ませたいファームウェアファイル名を指定する。



「設定ファイル・ファームウェアファイルのコピー」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「設定ファイル・ファームウェアファイルのコピー」の「実行」

4 「実行」をクリックする。

確認画面が表示されます。

5 「実行」をクリックする。

手順1で用意したファームウェアが本製品に読み込まれます。ファームウェアの読み込みが終わると、リビジョンアップが始まります。

リビジョンアップが終了すると、本製品は自動的に再起動します。

ご注意

「外部デバイスの設定」画面の「外部メモリからの起動」欄で「許可する」が選ばれていると、外部メモリ内のファームウェアから起動していますので、外部メモリを取り外さないでください。

6 USBボタンまたはmicroSDボタンを2秒間押し続ける。

本製品のUSBランプまたはmicroSDランプが消灯します。

7 外部メモリを取り外す。

ご注意

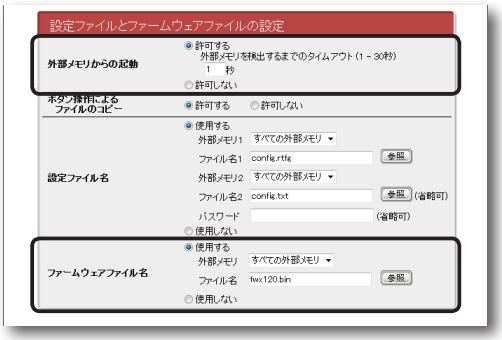
外部メモリからのリビジョンアップに失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

外部メモリ内のファームウェアで本製品を運用する

市販の外部メモリ（USBメモリ／microSDカード）に保存したファームウェアで本製品を運用できます。本製品内のファームウェアをリビジョンアップすることなく、緊急用のファームウェアや試験導入版のファームウェアを外部メモリに保存しておき、必要に合わせて使用したい場合などに便利です。

外部メモリ内のファームウェアファイルで本製品を起動できるように、設定を変更する

「外部デバイスの設定」画面の「外部メモリからの起動」欄で、「許可する」を選びます。



「外部デバイスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「外部デバイスの設定」の「設定」

外部メモリ内のファームウェアで本製品を起動する

1 ファームウェアを保存した外部メモリを用意する。

ファイル名は「外部デバイスの設定」画面の「ファームウェアファイル名」欄で指定したファイル名と同じ名前にします。

2 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

3 本製品を再起動する。

再起動をすると、手順1で指定したファームウェアが自動で読み込まれます。

ヒント

本製品内に保存されているファームウェアは上書きされません。

ご注意

外部メモリからのファームウェアファイルの読み込みに失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

本製品の設定情報とログを確認する

本製品の設定情報を確認する

プロバイダに接続するために必要な情報や各種の設定情報は、本製品の内部で１つの設定ファイル(config)として管理されています。この設定ファイルをパソコンに保存すると、設定のバックアップとして利用したり、設定ファイルをパソコンで編集したりできるので便利です。また、サポート窓口にお問い合わせいただく場合にも、設定ファイルの内容がわかった方がトラブルの早期解決につながることがあります。

1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「本製品の全設定(config)のレポート作成」の「実行」をクリックする。

「本製品の全設定(config)のレポート作成」画面に本製品の全設定情報が表示されます。

2 表示された設定情報をコピーして、「メモ帳」などのソフトウェアに貼り付けて保存する。

ヒント

パソコンで編集した設定ファイルを本製品に転送したいときは、あらかじめテキスト形式の設定ファイルの内容をクリップボードにコピーしておいてから、「コマンドの実行」画面(178ページ)に貼り付けます。

本製品のログを確認する

本製品の動作履歴は、ログファイル(Syslog)として管理されています。ログファイルで本製品の動作履歴を確認することで、ネットワークの障害を解決するヒントになる場合があります。

ヒント

ログファイルの保存方式には、いくつかの段階があります。詳しくは「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「本製品のログ(Syslog)のレポート作成」の「実行」をクリックする。

「本製品のログ(Syslog)のレポート作成」画面に本製品のログが表示されます。

2 表示されたログをコピーして、「メモ帳」などのソフトウェアに貼り付けて保存する。

外部メモリに設定情報とログを保存する

市販の外部メモリ（USBメモリ／microSDカード）に本製品の設定情報やログを保存できます。パソコン経由でのバックアップと比較して、運用管理に必要な情報をより手軽に収集できます。

ご注意

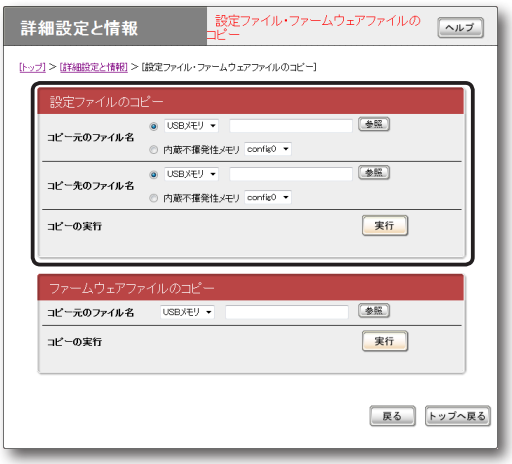
- FATまたはFAT32形式でフォーマットされていない外部メモリは、本製品では使用できません。
- USBハブを介して、複数のUSBメモリなどの外部メモリを本製品に接続することはできません。
- USB延長ケーブルは、種類によっては動作しないことがあります。USBメモリは本製品のUSBポートに直接挿入してご使用ください。
- 本製品のUSBランプまたはmicroSDランプが点灯／点滅している間は、外部メモリを取り外さないでください。外部メモリ内のデータを破損することがあります。USBボタンまたはmicroSDボタンを2秒間押し続けて、USBランプまたはmicroSDランプが消灯していることを確認してから外部メモリを取り外してください。

外部メモリに本製品の設定情報を保存する

1 外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

2 「設定ファイル・ファームウェアファイルのコピー」画面の「コピー元のファイル名」欄で、「内蔵不揮発性メモリ」を選び、config番号を指定する。



「設定ファイル・ファームウェアファイルのコピー」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「設定ファイル・ファームウェアファイルのコピー」の「実行」

3 「コピー先のファイル名」欄で、外部メモリに本製品の設定情報を保存する際のファイル名を入力する。

4 「実行」をクリックする。

確認画面が表示されます。

5 **「実行」をクリックする。**

本製品の設定ファイルが外部メモリに書き込まれます。

ヒント

「ファイルを暗号化する」にチェックを付けると、設定ファイルを暗号化できます（暗号化された設定ファイルを読み込む際には、この画面で入力したパスワードが必要です）。

6 **USBボタンまたはmicroSDボタンを2秒間押し続ける。**

本製品のUSBランプまたはmicroSDランプが消灯します。

7 **外部メモリを取り外す。**

ご注意

外部メモリへの設定ファイルの保存に失敗した場合は、「USBデバイスが使用できない」（213ページ）をご確認ください。

外部メモリに本製品のログを保存する

1 **外部メモリを本製品のUSBポートまたはmicroSDスロットに挿し込む。**

本製品のUSBランプまたはmicroSDランプが点灯／点滅します。

2 **「外部デバイスの設定」画面の「syslogの保存」欄で「開始する」を選んでから、ログのファイル名を入力する。**

「外部デバイスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「外部デバイスの設定」の「設定」

ヒント

「暗号化する」にチェックを付けると、ログを暗号化できます（暗号化されたログを読み込む際には、この画面で入力したパスワードが必要です）。

3 **「設定の確定」をクリックする。**

本製品のログが、外部メモリに書き込まれます。以後、ログの保存を停止するまで、本製品のログが外部メモリに書き込まれ続けます。書き込まれるログの容量などについて詳しくは、「保存されるログについてのご注意」（197ページ）をご覧ください。

4 ログの保存を停止する場合は、「外部デバイスの設定」画面の「syslogの保存」欄で「終了する」を選んでから、「設定の確定」をクリックする。

5 USBボタンまたはmicroSDボタンを2秒間押し続ける。

本製品のUSBランプまたはmicroSDランプが消灯します。

6 外部メモリを取り外す。

ご注意

- 起動直後、USBメモリを挿した直後、および、USBメモリを取り外す直前のログは記録されません。
- USBメモリの書き込み準備が完了するまでは、書き込みはできません。
- 外部メモリへのログの保存に失敗した場合は、「USBデバイスが使用できない」(213ページ)をご確認ください。

保存されるログについてのご注意

ログの保存を実行すると、USBメモリまたはmicroSDカード内に以下のログファイルが生成されます。

- ログが現在書き出されているファイル：「外部デバイスの設定」画面の「管理情報の保存」欄で指定したファイル名のファイル
- 一定容量ごとに生成されるバックアップファイル：上記ファイル名に、保存した日時が付加されたファイル

バックアップファイルの制限

バックアップファイル数が設定された上限数に達した場合、もしくは外部メモリの空き容量がなくなった場合、最も古いバックアップファイルから削除されます。

ご注意

外部メモリに十分な空き容量がない場合は、設定されたログファイルのサイズやバックアップするファイル数が実際に作成されたものと異なることがあります。

導入環境に合わせて動作をカスタマイズする（Luaスクリプト／カスタムGUI）

LuaスクリプトやカスタムGUI機能を利用することで、より導入環境に適した運用を実現できます。

Luaスクリプト

本製品でLuaスクリプトを実行できます。Luaスクリプトにヤマハルーター専用APIを埋め込むことで、本製品の状態に応じ、本製品の設定変更やアクションをプログラミングできるようになります。

スクリプトの例：

- configのプログラム設定から自動で設定する。
- 特定のアドレスへ通信できなくなったときに管理者へメールを送信する。
- トンネルがダウンしたときに経路を変更する。

その他、本製品で利用できるLuaスクリプトについて詳しくは、以下のURLをご覧ください。
http://www.rtpro.yamaha.co.jp/RT/docs/lua/

言語仕様

ヤマハが実装しているLua言語の仕様については、以下のURLをご覧ください。

Lua言語の文法
http://www.rtpro.yamaha.co.jp/RT/docs/lua/tutorial/syntax.html

ライブラリ関数
http://www.rtpro.yamaha.co.jp/RT/docs/lua/tutorial/library.html

Luaチュートリアル（プログラミング初心者向けのチュートリアル）
http://www.rtpro.yamaha.co.jp/RT/docs/lua/tutorial/

ご注意

外部メモリや本製品内蔵の不揮発性メモリは、実行対象のスクリプトファイルを保存する用途としてのみ使用してください。これらのデバイスへの頻繁な書き込みは、デバイスの消耗を早めることになります。特に本製品内蔵の不揮発性メモリについては、頻繁なファイル書き込みを行ったことが原因で故障に至った場合、保証期間内であっても無償修理の保証対象外になりますので、ご注意ください。

ヒント

- Luaスクリプトについて詳しくは、http://www.lua.org/をご覧ください。オリジナルのLua言語の仕様について詳しくは、Lua 5.1 Reference Manual（http://www.lua.org/manual/5.1/）をご覧ください。
- ヤマハルーター専用APIは、以下のURLで公開しています（APIは随時追加予定）。
  http://www.rtpro.yamaha.co.jp/RT/docs/lua/rt_api.html

カスタムGUI

本製品の設定を行うためのGUI(Webブラウザに対応するユーザーインターフェース)を、独自に設計して組み込むことができます(カスタムGUI)。

- 本製品にはホストからHTTPで設定を転送するためのインターフェースが用意されているため、JavaScriptを使用してGUIを作成できます。
- カスタムGUIを複数組み込むと、例えばログインするユーザー毎に画面を切り替えるような使い方もできます。
- 単純に本製品へのアクセス権限を制御するだけでなく、GUIの変更による機能アクセスへの制限をあわせて利用できるため、便利です。
- カスタムGUIの設定について詳しくは、以下のURLをご覧ください。
  http://www.rtpro.yamaha.co.jp/RT/docs/custom-gui/

故障かな？と思ったら

お問い合わせになる前に

本書の内容をご覧になり、問題を解決してみましょう。

問題を解決する

症状ごとの説明ページをご覧ください。

- **Q1：ランプ類が消灯している**(201ページ)
- **Q2：「かんたん設定ページ」で設定できない**(203ページ)
- **Q3：インターネットに接続できない**(205ページ)
- **Q4：VPN通信できない**(207ページ)
- **Q5：DOWNLOADボタンが機能しない**(212ページ)
- **Q6：USBデバイスが使用できない**(213ページ)
- **Q7：その他の問題**(215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(225ページ)。

Q1 ランプ類が消灯している

症状▶	原因▶	対策
ランプがひとつも点灯しない	POWERスイッチがSTANDBY になっている	POWERスイッチをONにする。
	電源コードがコンセントに接続されていない	コンセントから外れているときは、正しく差し込み直す。
	主ブレーカーや配線別ブレーカーが切れている	• ブレーカーが「切」になっている場合は、「入」にする。 • ブレーカーが「入」になっている場合は、一度「切」にしてから「入」にし直す。
	停電している	停電中は、復旧するまでお待ちください。
	コンセントに電気が来ていない（他の電気製品も使えない）	• 他の製品が動かないときは、コンセントや電気配線の修理を依頼してください。 • 他の製品が動くときは、本製品の修理を依頼してください。
LAN1 ランプが点灯しない	ハブやパソコンの電源が入っていない LAN1 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LAN1 ランプは点灯しない	本製品に接続した機器の電源を入れる。
	正しく接続されていない	本製品側、パソコンおよびハブ側共にコネクタ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。
	LAN用のケーブルを使用していない ISDNケーブルを使用している（コネクタ形状が全く同じなので注意が必要）	LAN用のケーブルを使用する。
	ケーブルが断線している	他のLANケーブルと取り替える。
	パソコンのLAN（ネットワーク）カードが正しく動作していない、または接続モードが本製品と合っていない	• 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。

Q1 ランプ類が消灯している（つづき）

症状▶	原因▶	対策
LAN2ランプが点灯しない	ADSLモデムやケーブルモデム、ONUの電源が入っていない	電源を入れる。
	ADSLモデムやケーブルモデム、ONUと正しく接続されていない	本製品のLAN2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。
	正しいケーブルを使用していない	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接続する。

02 「かんたん設定ページ」で設定できない

症状▶	原因▶	対策
「かんたん設定ページ」を表示できない	本製品がパソコンを認識していない(LAN1ランプが点灯していない)	「LAN1ランプが点灯しない」(201ページ)の説明に従って、問題を解決する。
	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アドレスを取得し直す。
	本製品が誤動作している	本製品を初期状態に戻してから、設定をやり直す(221ページ)。
	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。再起動または電源を切ることができないときは、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、本製品とパソコンの電源を入れる。 • パソコンのIPアドレスが本製品のネットワークアドレスと同じになっているか、他の機器とIPアドレスが重なっていないかを確認し、誤りがあれば適切なIPアドレスに変更する。
	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。
	パソコンのWebブラウザの接続経路設定が、LAN経由になっていない	Windows版Internet Explorerの場合、「インターネットオプション」の「接続」タブでダイヤルアップ接続をする設定になっていると、「かんたん設定ページ」にアクセスできないので、「ダイヤルしない」に変更する。
	パソコンのWebブラウザでProxy(プロキシ)サーバーを使用している	プロキシの設定が正しくないと、「かんたん設定ページ」が表示できない。プロキシの設定を確認する。

Q2 「かんたん設定ページ」で設定できない（つづき）

症状▶	原因▶	対策
「かんたん設定ページ」を表示できない（つづき）	パソコンをWebブラウザ経由で遠隔操作している	• IPアドレスによるアクセス制限機能が働いていると、許可されていないホストからのアクセスに対しては、「Error503 This server is available to members only. I'm sorry, your host is not member.」と表示される。遠隔操作する場合は、「HTTPの利用を許可するホスト」の設定を変更する（120ページ）。
パスワードを入力しても「かんたん設定ページ」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）	• パスワードは、全角／半角や大文字／小文字の違いも区別される。必ず半角の英数字で大文字／小文字まで正確に入力する。 • Webブラウザに認証情報（ユーザー名、パスワード）が残っていると、それを自動的に送信するため、エラーになる場合がある。ユーザー名を削除してからパスワードを入力し直すか、ブラウザをいったん終了してから「かんたん設定ページ」を開き直す。
	ログインパスワードを入力している（管理パスワードを設定している）	パスワードを設定している場合は、管理パスワードを入力する。
設定内容が元に戻ってしまう	設定後に「設定の確定」をクリックしていない	「かんたん設定ページ」で設定を変更したときは、必ず「設定の確定」をクリックして設定を保存する。「設定の確定」をクリックせずに「トップに戻る」をクリックしたり画面を閉じたりすると、設定内容は保存されない。
	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。
「かんたん設定ページ」を開く際に、Webブラウザにパスワードを保存できない	「ユーザー名」と「パスワード」を入力する画面で、ユーザー名を空欄にしている	Webブラウザによっては、パスワードを保存するためにユーザー名の入力が必要な場合がある。この場合は、任意の文字列を入力する。

03 インターネットに接続できない

症状▶	原因▶	対策
フレッツ 光ネクストやBフレッツで接続できない	本製品がブロードバンド回線を認識していない(LAN2ランプが点灯していない)	「LAN2ランプが点灯しない」(202ページ)の説明に従って、問題を解決する。
	ユーザーIDまたはパスワードが間違っている	• プロバイダから指定されたユーザーIDに加えて、プロバイダ名まで指定する必要がある(例:username@xxx.ne.jp)。 • フレッツ 光ネクスト(またはBフレッツ)とプロバイダの設定資料を参照して、正しく入力する。
ホームページが表示されない／表示が遅い	プロバイダ設定のDNSサーバーアドレスが間違っている	• プロバイダ接続設定にDNSサーバーアドレスが設定されているか確認する。 • 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、アクセスし直す。
	本製品のフィルターが動作している	• 複雑なポリシーフィルター(99ページ)を適用していないか、不要なポリシーを適用していないかを確認し、ポリシーの適用を見直す。 • 入力遮断フィルター(96ページ)やポリシーフィルター(99ページ)でhttp通信のポートを制限していないか、表示しようと指定したホームページがURLフィルター(114ページ)によるフィルタリングの対象となっていないかを確認し、フィルタリングの設定を見直す。

Q3 インターネットに接続できない（つづき）

症状▶	原因▶	対策
ホームページが表示されない/表示が遅い（つづき）	回線の種類に問題がある（PPPoE方式ADSL接続時のみ）	ADSL回線の種類によっては、標準的な設定のままでは、一部のホームページのデータが受信できないか、データの受信が非常に遅くなることがある。 いったん接続を切断してから、「かんたん設定ページ」の「詳細設定と情報」ー「基本接続の詳細な設定」ー「プロバイダの修正」画面でMTUに1454などの値を設定して、接続し直す。
	プロバイダから与えられた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	「かんたん設定ページ」の「LANの設定」画面で、本製品のIPアドレスをプロバイダから与えられたものと重複しないアドレスに変更する（53ページ）。この場合、本製品の各種フィルターは再適用する必要がある。
	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アドレスを取得し直す。
	回線やプロバイダ、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、ご利用の回線業者やプロバイダにお問い合わせください。

Q4 VPN通信できない

症状▶	原因▶	対策
「かんたん設定ページ」のトップページでIPsecトンネル接続が「通信中」と表示されない	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。 • 「Q3 インターネットに接続できない」(205ページ)の説明に従って、問題を解決する。
	IPsec接続の接続先と通信ができない	IPsecの接続先のIPアドレスに対してpingコマンドを実行して、応答が返ってくるかどうかを確認する。応答が返ってこなければ、接続先の機器が通信可能な状態になっているかを確認する。
IPsec接続のVPN通信ができない	IPsec接続が確立していない	• IPsecの接続先と同じ認証鍵(pre-shared key)を設定しているかを確認する。 • 接続先の識別方法で、正しいIPアドレスまたは正しい名前を設定しているかを確認する。 • IPsecの接続先と同じ認証アルゴリズム、暗号アルゴリズムを設定しているかを確認する。
	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を正しく設定する。
	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機能が有効になっている場合には、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、ファイアウォール機能の設定を変更する。 Windows 7では、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。
IPsec接続のVPN通信が遅い	インターネットの通信が遅い	「Q3 インターネットに接続できない」(205ページ)の説明に従って、問題を解決する。
端末にL2TP/IPsecを設定できない	端末がL2TP/IPsecに対応していない	L2TP/IPsecに対応した端末を準備する。設定方法は、端末のマニュアルを参照してください。

Q4 VPN通信できない（つづき）

症状▶	原因▶	対策
L2TP/IPsec接続 VPN接続ができない	L2TP/IPsecのサービスが有効になっていない	L2TP/IPsecのサービスを有効にする。 (l2tp service onを設定する)
	IPsecの設定に間違いがある	• IPsecの事前共有鍵が正しいか確認する。 • トンネルインターフェースの種別を確認する。 (tunnel encapsulation l2tp)
	PPPの設定に間違いがある	• PPP認証のIDとパスワードが正しいか確認する。 • PPインターフェースでトンネルインターフェースがバインドされていることを確認する。 (pp bind tunnel1)
	端末の設定が誤っている	• 接続先のアドレスまたはホスト名が正しいか確認する。 • IPsecの事前共有鍵が正しいか確認する。 • PPP認証のユーザーIDとパスワードが正しいかを確認し、誤りがあれば正しいユーザーIDとパスワードに変更する。 • 端末の設定に関しては、端末のマニュアルを参照してください。
	接続先と通信ができない	接続先の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、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。
L2TP/IPsec接続がすぐに切断される	端末の電波状況が悪い	端末の電波状況を確認して、電波状態の良い場所に移動する。
	L2TP/IPsecの切断タイマが設定されている	L2TP/IPsecの切断タイマを適切な時間に設定する。
	L2TP/IPsecキープアライブの設定が不適切	L2TP/IPsecキープアライブのインターバルと回数を適切に設定する。 電波状態が悪いところでは一時的にキープアライブの応答をロスすることがあります。

症状▶	原因▶	対策
VPN接続先のネットワークにいる端末と通信できない	IPアドレスを取得できていない	VPN接続先で使用するIPアドレスが取得できているか端末で確認する。 IPアドレスの確認方法は端末のマニュアルを参照してください。
	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を正しく設定する。
	代理ARPの設定が無い	VPN接続先のLAN内で代理ARPを動作させる。(ip lan1 proxyarp on)
「かんたん設定ページ」のトップページでPPTPトンネル接続が「通信中」と表示されない	プロバイダからプライベート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。 • 「Q3インターネットに接続できない」(205ページ)の説明に従って、問題を解決する。
	PPTP接続の接続先と通信ができない	PPTPの接続先の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。

Q4 VPN通信できない（つづき）

症状▶	原因▶	対策
PPTP接続のVPN通信ができない	PPTP接続が確立していない	• 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。 • 接続先のホスト名またはIPアドレスに、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を正しく設定する。
	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機能が有効になっている場合には、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、ファイアウォール機能の設定を変更する。Windows 7では、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。
「かんたん設定ページ」のトップページでIPIPトンネル接続が「通信中」と表示されない	フレッツ網に接続していない	フレッツ網に接続する設定を行っているかを確認する。
	IPIPトンネル接続の接続先と通信ができない	IPIPトンネルの接続先のIPアドレスに対してpingコマンドを実行して、応答が返ってくるかどうかを確認する。応答が返ってこなければ、接続先の機器が通信可能な状態になっているかを確認する。

症状▶	原因▶	対策
IPIPトンネル接続のVPN通信ができない	IPIPトンネル接続が確立していない	• 接続先のIPアドレスに、フレッツ網から接続先に払い出されたIPアドレスが正しく設定されているかを確認する。 • 「かんたん設定ページ」の「詳細設定と情報」-「VPN接続の設定」のIPIPトンネル接続の設定画面で、「接続プロバイダ」にフレッツ網との接続に使用されているインターフェースが選択され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を正しく設定する。
	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機能が有効になっている場合には、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、ファイアウォール機能の設定を変更する。Windows 7では、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。
IPIPトンネル接続のVPN通信が遅い	フレッツ網の通信が遅い	回線状態に問題がないかを回線事業者にお問い合わせください。

Q5 DOWNLOADボタンが機能しない

症状▶	原因▶	対策
DOWNLOADボタンを押してもリビジョンアップされない	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。「Q3インターネットに接続できない」(205ページ)の説明に従って、問題を解決する。
	ファームウェアのダウンロード先URLの設定が間違っている	「かんたん設定ページ」の「詳細設定と情報」−「リビジョンアップの実行」画面で「ダウンロードするURL」を正しく設定する。
	DOWNLOADボタンの使用を許可する設定になっていない	「かんたん設定ページ」の「詳細設定と情報」−「DOWNLOADボタンの設定」画面でリビジョンアップを許可する設定に変更する。
	最新リビジョンのファームウェアを使用している	そのまま使い続けてください。
前面のランプが順番に点灯し始めた	ファームウェアを不揮発性メモリに書き込んでいる(正常な状態)	そのままの状態でお待ちください。ケーブルを抜いたり、電源を切ったりしないでください。

Q6 USBデバイスが使用できない

症状▶	原因▶	対策
USBランプが点灯しない	USBポートの使用が許可されていない	USBポートの使用を許可するように設定する。
	USBメモリ以外のデバイスを挿入している	USBメモリを挿入する。 USBメモリのご利用について詳しくは、以下のURLをご覧ください。 http://www.rtpro.yamaha.co.jp/RT/docs/external-memory/index.html
	USBメモリが壊れている	USBメモリが使用できるかどうか、パソコンなどで確認する。
	USBハブを経由して、USBメモリを挿入している	USBハブには対応していない。本製品のUSBポートに、USBメモリを直接挿入する。
	USB延長ケーブルを経由して、USBメモリを挿入している	USBメモリを本製品のUSBポートに直接挿入して使用する。
USBランプが点滅したままの状態で、USBメモリを使用できない	過電流保護機能により、USB機能の使用が中断されている	消費電流の小さいUSBメモリを使用する。機能を復旧させるには、USBボタンを1秒以上押し続ける。
USBボタンとDOWNLOADボタンを押してもコピーされない	ボタン操作によるファイルのコピーが許可されていない	ボタン操作によるファイルのコピーを許可するよう設定する。
	ボタン操作でコピーする設定ファイルまたはファームウェアファイルが、USBメモリ内に存在しない	「かんたん設定ページ」で設定した名前のファイルを、パソコンなどを使ってUSBメモリにコピーする。
USBメモリに保存されたSyslogに、記録漏れがある	起動直後、USBメモリを挿した直後、および、USBメモリを取り外す直前のログは記録されない	USBメモリの書き込み準備が完了するまでは、書き込みできない。
	Syslogの量が多過ぎて、USBメモリへの書き込みが間に合わない	ログの保存モードを変更するなどして、Syslogの量を減らす。 **ヒント** USB 1.1対応のUSBメモリを使用している場合は、より高速なUSB 2.0対応のUSBメモリを使用することで症状が改善することがある。
コマンドにより手動でファームウェアをコピーしたが、反映されない	コマンドにより手動でファームウェアをコピーしただけでは、実動作に反映されない	手動でコピーしたあとに、本製品を再起動する。

Q6 USBデバイスが使用できない（つづき）

症状▶	原因▶	対策
コマンドにより手動で設定ファイルをコピーしたが、設定が反映されない	コマンドにより手動で設定ファイルをコピーしただけでは、実動作に反映されない	手動でコピーしたあとに、本製品を再起動する。

07 その他の問題

症状▶	原因▶	対策
「かんたん設定ページ」のトップページでデータコネクト接続が「通信中」と表示されない	フレッツ 光ネクストの回線に接続していない	フレッツ 光ネクストの回線に接続していることを確認する。
	回線サービスの契約が不足している	• フレッツ 光ネクストの回線がひかり電話を利用する契約になっているか確認する。 • ひかり電話でナンバー・ディスプレイサービスを利用する契約になっているか確認する。
	HGWまたはONU一体型HGWに接続している	WAN側をONUに直結する。
	データコネクト接続の接続先と通信できない	データコネクト接続の接続先のIPアドレスに対してpingコマンドを実行して、応答を確認する。 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か確認する。
データコネクト接続のVPN通信ができない	電話番号が誤って設定されている	• 本製品のひかり電話番号を正しく設定する。 • 接続相手のひかり電話番号を正しく設定する。
	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を正しく設定する。
	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機能が有効になっている場合は、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、ファイアウォール機能の設定を変更する。Windows 7では、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。

Q7 その他の問題（つづき）

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	プロバイダ設定や経路設定を確認する。
	本製品のフィルターが動作している	入力遮断フィルターやポリシーフィルターで、NTPポート（ポート番号123）の通信を遮断していないかを確認し、NTPポートの通信を遮断しているのであればフィルターの設定を見直す。
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接続で接続している	ネットワーク型プロバイダ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。
通信料金に異常がある	パソコンのソフトウェアや機器が自動的にインターネットへ接続している（自動接続機能でインターネットへ接続している場合）	「USBデータ通信端末の通信料金に異常がある」（217ページ）の説明に従い、問題を解決する。
パスワードを忘れてしまった		「パスワードを忘れてしまった場合は」（223ページ）を読んで、問題を解決する。

USBデータ通信端末の通信料金に異常がある

プロバイダ設定を確認する

USBデータ通信端末のご契約が定額制であっても、設定を誤って使用すると従量制の通信料金がかかる場合があります。「かんたん設定ページ」の「詳細設定と情報」−「基本接続の詳細な設定」−「プロバイダの修正」画面で、設定が間違えていないか確認してください。

通信履歴を確認する

自動接続機能でインターネットへ接続している場合は、パソコンのソフトウェアや機器が自動的にインターネットへ接続している疑いがあります。また、ソフトウェアによっては、パソコンを起動しているだけで自動的に動作するものがあり、知らないうちに自動発信を繰り返している場合があります。USBデータ通信端末のご契約が従量制の場合、多額の通信料金になる時がありますので、こまめに通信履歴を確認してください。

次のような場合は、特にご注意ください

- 本製品を使い始める時
- 本製品のプロバイダ接続設定を変更する時
- パソコンのダイヤルアップネットワーク設定を変更する時
- パソコンに新しいソフトウェアをインストールする時
- ネットワークに新しいパソコンやネットワーク機器、周辺機器などを接続する時
- 本製品のファームウェアをリビジョンアップする時
- その他、いつもと違う操作を行ったり、通信の反応に違いを感じた時など

ご注意

- プロバイダ契約を解除または変更する時は、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から意図しない料金を請求される場合があります。
- プロバイダ側の状態(アクセスポイントの変更、メンテナンス、障害など)によって予想外の通信料金がかかる場合がありますので、プロバイダからの告知情報には常に注意してください。
- ここで使用している画面や設定項目は、各ソフトウェアのバージョンにより内容が異なります。

「通信履歴のレポート作成」画面で確認する

「かんたん設定ページ」－「詳細設定と情報」－「通信履歴のレポート作成」画面で、各ポート毎の通信履歴を確認できます。

発着信日付、発着信時刻、通信種別、通信時間、切断コードが新しい順に100件まで表示されます。通信種別がPPxxとなっている通信が、プロバイダ（またはLAN間接続相手）へ接続した通信です。

ログ情報で確認する

「かんたん設定ページ」－「詳細設定と情報」－「本製品のログ（Syslog）のレポート作成」画面で、自動接続のきっかけになったアクセスの情報を確認できます。

意図しないアクセスが多いときは、Syslog表示の中で一番下から順に「IP Commencing」の行を探します。IP Commencing行のパソコンIPアドレスやアクセス先ホストのIPアドレス、アクセス時間（もしくは間隔）などを手がかりに、どのソフトウェア（または機器）がアクセス要求を出しているかを調べて、原因を探してください。

アクセス例1

```
PP[01] IP Commencing : UDP 192.168.
100.1 : 53 >  xxx.xxx.xxx.xxx : 53
(DNS Query [windowsmedia.com] from
192.168.100.2)
```

- PP［01］：プロバイダ番号
- 192.168.100.2：パソコンのIPアドレス
- xxx.xxx.xxx.xxx：アクセス先のIPアドレス

この例では、LAN内のパソコン（192.168.100.2）からDNSサーバーへインターネットのホスト（windowsmedia.com）のIPアドレスを調べる問い合わせ要求をきっかけに、プロバイダへの自動接続を開始しています。

アクセス例2

```
PP[01] IP Commencing : TCP 192.168.
100.2:1311 > xxx.xxx.xxx.xxx:80
```

この例では、LAN内のパソコン（192.168.100.2）からインターネットのホスト（xxx.xxx.xxx.xxx）へのアクセス要求をきっかけに、プロバイダへの自動接続を開始しています。

原因になりやすい設定を確認する

不審なインターネットアクセスの原因になる設定項目には、次のようなものがあります。OSを使い始めるときや、新しいソフトウェアをインストールしたときは、以下の例を参考にして設定をご確認ください。

頻繁に発信している場合は

パソコンのネットワーク設定のDNS設定値を確認してください。インターネット上のDNSサーバーのIPアドレスが指定されていると、頻繁にアクセスする場合があります。

パソコンを起動するたびに発信している場合は

パソコンの起動と同時に起動するソフトウェアがある場合は、設定内容によって起動するたびにインターネットへ接続することがあります。ソフトウェアの設定を確認し、自動アップデートなどの機能が有る場合は、設定を変更してください。

Windows XPの設定

デスクトップにWebページを設定していると、パソコンを起動するたびにインターネットへ接続してWebページの内容を更新するため、パソコンを起動するごとに通信料金がかかります。必要がなければ、設定を解除してください。

定期的に発信している場合は

- 1日に何回も発信している場合は：Windows Updateを利用している場合や、電子メールの自動送受信が設定されている場合などが考えられます。本製品のLANに接続しているパソコンの、該当するソフトウェア設定を確認してください。
- 1日に数回以内の場合は：ハードウェアのメンテナンスプログラムやNTPサーバー（インターネット自動時刻サーバー）の設定を確認してください。

ホームページのバナー広告

バナー広告が掲載されているホームページでは、何も操作しなくても定期的に自動更新する場合があります。そのページを開いたままWebブラウザを放置すると、定期的にインターネットへアクセスし続け、そのたびに料金がかかります。見終ったらWebブラウザを閉じることで、不要なアクセスを防ぐことができます。

コンテンツの購読

Internet ExplorerのフィードとWeb スライスを使用している場合は、指定した間隔でコンテンツ内容の更新のためインターネットへ接続します。更新のたびに料金がかかるため、購読する場合は更新間隔をよく確認してお使いください。
不要な場合は、設定を解除してください。

電子メールソフトウェアの設定

電子メールソフトウェアには、新着メールを定期的に確認する機能があります。この機能を利用している場合は、定期的にインターネット上のメールサーバーにアクセスするため、そのたびに料金がかかります。この機能を利用する場合は、確認する頻度を十分考慮してください。
必要なければ設定を解除して、手動でメールを確認するようにしてください。

OSの自動アップデート機能

OSの自動アップデート機能を利用している場合は、定期的にインターネット上のサーバーにアクセスし、そのたびに料金がかかります。不要であれば、設定を手動更新に変更して、インターネットに接続しているときに手動で更新してください。

ソフトウェアを起動するたびに発信している場合は

インストールしたソフトウェアの環境設定（初期設定）を確認して、自動アップデートなどの機能が有る場合は、設定を変更してください。

ソフトウェアの設定

ソフトウェアの自動アップデート機能を利用している場合は、ソフトウェアを起動するたびにインターネットへ接続するため、そのたびに料金がかかります。
不要であれば設定を解除してください。

Windows Media Playerの環境設定

Windows Media Playerをインストールすると、Media Playerを開くたびにガイドページの情報を得るためにインターネットへ接続するため、そのたびに料金がかかります。
不要であれば、ヘルプに従って設定を解除してください。

本製品の設定を初期化する

本製品の設定内容を工場出荷状態に戻すことができます。

ご注意

設定内容を工場出荷時の状態に戻す場合は、以下の点にご注意ください。

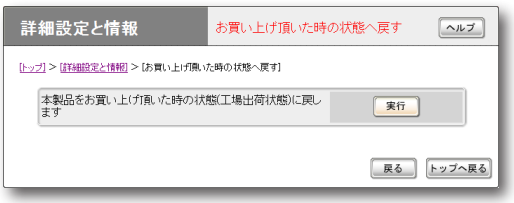
- 実行した直後にすべての通信が切断されます。
- 初期設定値が存在する設定は、初期設定値に変更されます。
- フィルター定義や登録されたアドレスは消去されます。
- saveコマンドなしで、不揮発性メモリの内容が書き換えられます。
- 操作を完了した後に、設定内容を元の状態に戻すことはできません。

ヒント

初期化する前に設定内容を外部メモリへ保存しておけば、初期化後に元の状態に戻すことができます。設定を保存する方法については、「本製品の設定情報とログを確認する」(194ページ)をご覧ください。

「かんたん設定ページ」から初期化する

本製品の設定内容を工場出荷状態に戻したいときは、「お買い上げ頂いた時の状態へ戻す」画面で設定を初期化できます。



設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「お買い上げ頂いた時の状態へ戻す」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「お買い上げ頂いた時の状態へ戻す」の「実行」

「かんたん設定ページ」から初期化できないときは

本製品のIPアドレスを誤って設定した場合など、本製品の「かんたん設定ページ」から初期化できない場合には、CONSOLEポートに接続したパソコン、または本製品のボタン操作で初期化できます。

CONSOLEポートに接続したパソコンから初期化する

1 本製品の電源を切る。

2 本製品のCONSOLEポートとパソコンのシリアルポートを、シリアルケーブルで接続する。

接続、パソコンの設定については179ページをご覧ください。

3 パソコンでターミナルソフトウェアを起動する。

詳しくは180ページをご覧ください。

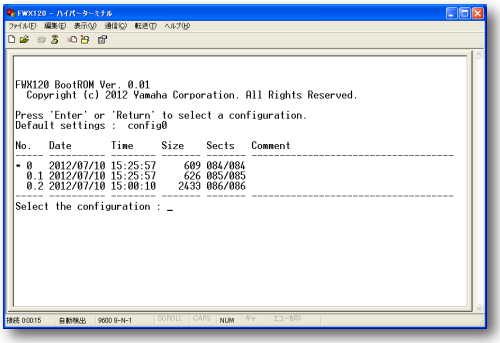
4 本製品の電源を入れる。

パソコンのターミナルソフトウェアの画面に本製品のROMのバージョンが表示され、Enterキーの入力待ち状態になります。

5 「Will start automatically in～ 」のカウントダウンが終わらないうちに、Enterキーを押す。

「Will start automatically in～ 」のカウントダウンが終わると通常状態で起動してしまいます。起動してしまった場合は、本製品の電源を切ってから10秒以上の時間をおき、もう一度電源を入れ直して操作してください。

6 **設定ファイルの選択待ち状態になったら、0～4.2のうちで表示されていない設定ファイルを指定してからEnterキーを押す。**



ファームウェアが起動すると、ファームウェアのリビジョンなどが表示されます。

7 **10秒程度待ってから、Enterキーを押す。**

8 **「Password:」と表示されたら、半角英字で「doremi」と入力してからEnterキーを押す。**

「>」が表示されると、コンソールコマンドを入力できるようになります。

ヒント

ログインパスワードを設定している場合は、ログインパスワードを入力してください。

9 **「administrator」と入力してから、Enterキーを押す。**

10 **「Password:」と表示されたら、半角英字で「doremi」と入力してからEnterキーを押す。**

ヒント

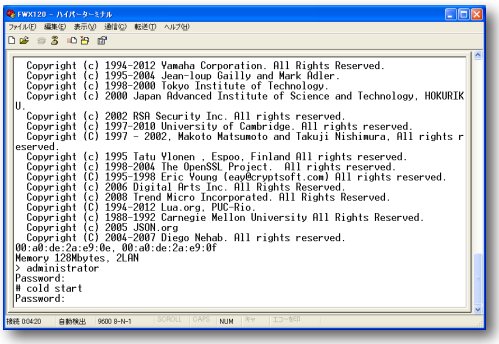
管理パスワードを設定している場合は、管理者パスワードを入力してください。

11 **「#」が表示されたら、「cold start」と入力してからEnterキーを押す。**

12 **「Password:」と表示されたら、半角英字で「doremi」と入力してからEnterキーを押す。**

ヒント

管理パスワードを設定している場合は、管理者パスワードを入力してください。

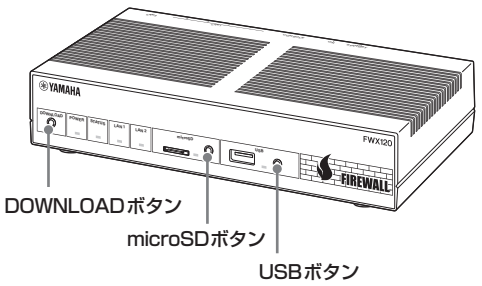


本製品の設定が初期化されます。

本製品のボタン操作で初期化する

DOWNLOAD、microSD、USBの3つのボタンを押しながら電源を入れることでも工場出荷時の状態に設定が変更されます。

1 **DOWNLOAD、microSD、USBの3つのボタンを押しながら、本製品の電源を入れる。**



本体前面のランプが何度か点滅します。

2 **本製品の電源を入れてから3秒経過後、DOWNLOAD、microSD、USBの3つのボタンを離す。**

本製品の設定が初期化されます。

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や管理パスワードとして設定した文字列を忘れてしまうと、本製品にログインできなくなります。このような場合でも、CONSOLEポートに接続したシリアル端末から以下の非常用パスワードを入力すると、本製品にログインできます。

非常用パスワード

「w,IXIma」（ダブリュー、カンマ、エル、エックス、エル、エム、エー）

ヒント

CONSOLEポートへの接続、パソコンの設定については179ページをご覧ください。

非常用パスワードを使ってログインすると最初から管理モードに入れますので、忘れてしまったログインパスワードや管理パスワードを再設定してください。パスワード設定の際に要求される古いパスワードも、この非常用パスワードが利用できます。

ご注意

この機能は、security classコマンドの設定で禁止することもできます。security classコマンドの第2パラメータで「on」が指定されていない場合は、この方法でもログインできません。その際は、「本製品のボタン操作で初期化する」（222ページ）に従い本製品を初期化してください。
security classコマンドについては「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

本製品の保守サービスについて

保証期間

ご購入日から1年間です。

保証書について

保証書は「はじめにお読みください」の19ページに印刷されております。お買い上げ年月日・販売店などが確認できるレシートなどと一緒に保管してください。万一紛失なさいますと、保証期間中であっても実費を頂戴します。

保証期間中の修理

保証期間中に万一故障した場合には、ご購入の販売店またはヤマハルーターお客様ご相談センターまでご連絡の上、製品をご送付ください。その際必ず保証書を同封してください。

保証期間後の修理

保証期間終了後の修理は有料となりますが、引続き責任をもって対応させていただきます。ご購入の販売店またはヤマハルーターお客様ご相談センターまでご連絡ください。

ただし、修理対応期間は製造打ち切り後5年間です。

ご注意

- 本製品を修理等の理由により輸送される場合には、お客様の責任において必ず本製品の設定を別の環境に保存してください。
- 本製品の設定を保存する方法につきましては、「本製品の設定情報とログを確認する」(194ページ)をご覧ください。
- 修理の内容によっては、設定を工場出荷時の状態にさせていただく場合がございます。あらかじめご了承ください。

サポート窓口のご案内

お問い合わせの前に

本書をもう一度ご確認ください

本書をよくお読みになり、問題が解決できるかご確認ください。

ログ情報や設定情報をご確認ください

お客様が使用されている本製品の状態を把握するために、弊社の担当者がログ(Syslog)情報や設定(config)情報を確認させていただくことがあります。ログ情報や設定情報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。
ログ情報や設定情報は、以下の方法でご確認ください。

1 パソコンでInternet Explorerを起動する。

2 アドレスバーに「http://192.168.100.1」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。

ご注意

LAN1 ポートのIPアドレスを変更してある場合は、設定されているIPアドレスをアドレスバーに入力してください。

3 「ユーザー名」欄は空欄とし、「パスワード」欄に半角英字で「doremi」と入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページが表示されます。

ご注意

ユーザーが登録されている、またはパスワードが変更されている場合には、設定されているユーザー名とパスワードを入力してください。

4 「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

5 ログ情報を確認したいときは「本製品のログ(Syslog)のレポート作成」、設定情報を確認したいときは「本製品の全設定(config)のレポート作成」の「実行」をクリックする。

本製品のログ情報または全設定情報が表示されます。

「本製品の設定情報とログを確認する」(194ページ)もあわせてご覧ください。

お問い合わせ窓口

本製品に関する技術的なご質問やお問い合わせは、下記へご連絡ください。

ヤマハルーターお客様ご相談センター

TEL：03-5651-1330
FAX：053-460-3489

ご相談受付時間

9:00 ～ 12:00 13:00 ～ 17:00（土・日・祝日、弊社定休日、年末年始は休業とさせていただきます）

お問い合わせページ

http://jp.yamaha.com/products/network/
からサポートページにお進みください。

主な仕様

外形寸法(幅×高さ×奥行き):
220 mm×42.6 mm×160.5 mm
(突起部、ケーブル端子類は含まず)

質量:
本体 870g

電源:
AC100 V(50/60 Hz)

消費電力:
最大11W

動作環境条件:
周囲温度 0～50 ℃
周囲湿度 15～80 %(結露しないこと)

保管環境条件:
周囲温度 -20～50 ℃
周囲湿度 10～90 %(結露しないこと)

電波障害規格:
VCCI クラスA

認証番号:
AD11-0187001

LAN1インターフェース:
イーサネット(RJ-45)
10BASE-T/100BASE-TX/1000BASE-T
4ポートスイッチングハブ
ストレート/クロス自動判別

LAN2インターフェース:
イーサネット(RJ-45)
10BASE-T/100BASE-TX/1000BASE-T
1ポート
ストレート/クロス自動判別

シリアルインターフェース:
DTE固定
(パソコンとの接続はクロスケーブル)
ポート数:1
非同期シリアル:RS-232C
コネクタ:D-sub 9ピン
データ転送速度:9600bit/s
データビット長:8ビット
パリティチェック:なし
ストップビット数:1ビット
フロー制御:ソフトウェア(Xon/Xoff)

USBインターフェース:
USB 2.0 High-Speed 対応
給電電流:最大500mA
ポート数:1
コネクタ:USB Type-Aコネクタ

microSDインターフェース:
ポート数:1
コネクタ:microSDスロット

表示機能(LED)
前面:POWER、STATUS、LAN1、LAN2、microSD、USB
背面:LINK/DATA、SPEED

付属品:
LANケーブル(3m、RJ-45、ストレート)(1本)
はじめにお読みください
保証書
(「はじめにお読みください」に印刷)
CD-ROM(1枚)
(「はじめにお読みください」「取扱説明書(本書)」「コマンドリファレンス」などを収録)

アースコードを接続する

準備を始める前にご用意ください

アースコード

アースコードを接続することで静電気対策やノイズ防止に効果があります。

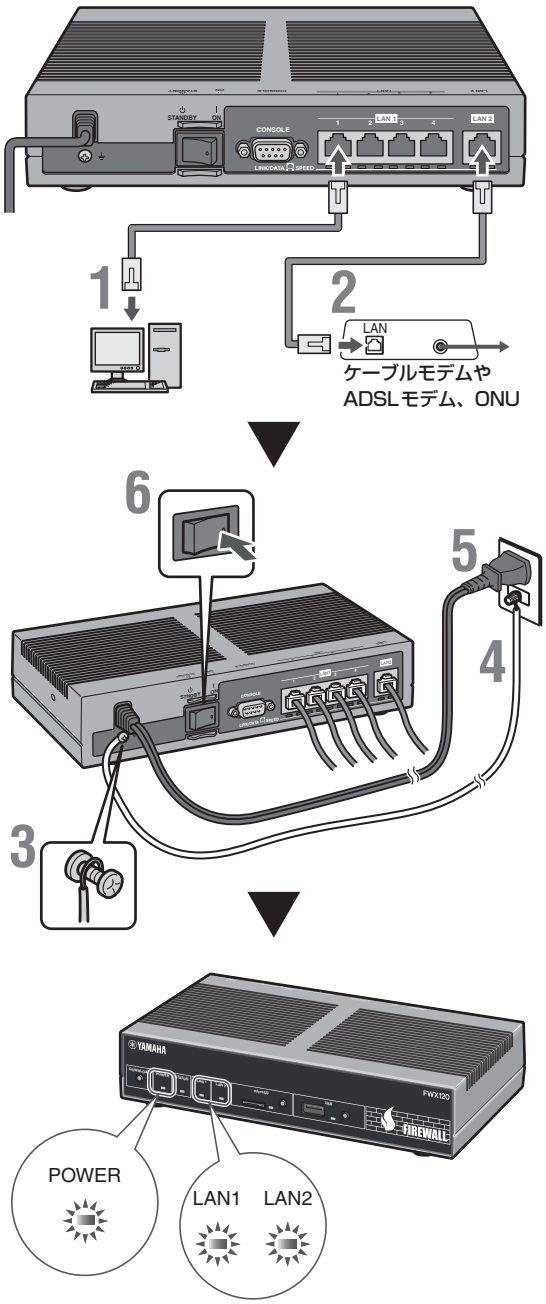
LANケーブル

パソコンの台数や距離に合わせて、LANケーブルをご用意ください。

ハブ

本製品のLAN1ポートには、パソコンを4台まで直接接続できます。5台以上のパソコンを接続したい場合は、10BASE-Tまたは100BASE-TX、1000BASE-T対応のハブ(スイッチングハブなど)をご用意ください。

接続して電源を入れる



アースコードを接続する（つづき）

1 **パソコンのLANポートと本製品のLAN1ポートを、LANケーブルで接続する。**

2 **ケーブルモデムやADSLモデム、ONUのLANポートと本製品のLAN2ポートを、LANケーブルで接続する。**

プロバイダの資料やADSLモデム、ONUの取扱説明書もあわせてご覧ください。

ご注意

ケーブルモデムやADSLモデム、ONUとパソコンを直接接続している環境を本製品との接続に切り替えたり、設置されていたルーターを本製品に置き換えた場合に、アドレスが取得できないなどの原因で正常接続できないことがあります。場合により、環境の変更後に何らかの設定やリセット操作、指定時間(例:20分以上)待つこと、などが必要となる場合があります。詳しくは、それらの取扱説明書の指示に従ってください。

3 **アース端子のネジをプラスドライバーで少しゆるめてから、アースコードをアース端子に接続して固定する。**

アースコードを接続することで静電気対策やノイズ防止に効果があります。

4 **アースコードをコンセントのアース端子へ接続する。**

ご注意

アースコードは必ずコンセントのアース端子に接続してください。ガス管などには、絶対に接続しないでください。

5 **本製品の電源コードをコンセントに接続する。**

電源コードを取り外す場合は

先に電源コードを取り外してから、アースコードを取りはずしてください。

6 **本製品のPOWER(電源)スイッチを「ON」にして、電源を入れる。**

POWERランプが何回か点滅した後に点灯します。

7 **パソコンやハブの電源を入れる。**

本製品のLAN1ランプとLAN2ランプが点灯または点滅すれば正常です。

ご注意

LAN1ランプまたはLAN2ランプが点灯または点滅しない場合は、「ランプ類が消灯している」(201 ページ)をご確認ください。

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。

Windows 7の場合

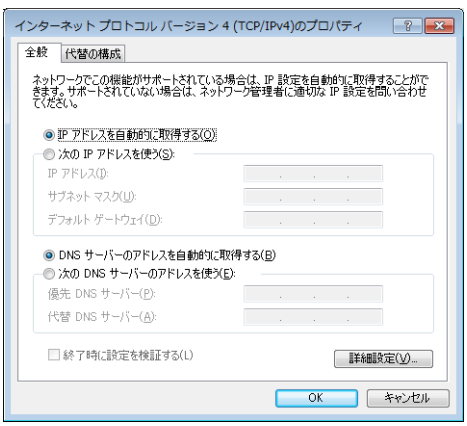
1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

2 「コントロールパネル」右上の検索欄に「アダプター」と入力して、「ネットワークと共有センター」の「ネットワーク接続の表示」をクリックする。

3 変更する接続を右クリックして、表示されたショートカットメニューから「プロパティ」をクリックする。

4 「ネットワーク」タブをクリックする。

5 「この接続は次の項目を使用します」欄で「インターネット プロトコル バージョン4(TCP/IPv4)」をクリックして選んでから、「プロパティ」をクリックする。



6 「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」を選んでから、「OK」をクリックする。

7 「ローカルエリア接続のプロパティ」画面で「閉じる」をクリックする。

8 「スタート」ボタンをクリックして、「すべてのプログラム」-「アクセサリ」-「コマンド プロンプト」をクリックする。

9 「ipconfig /release」と入力してから、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。

10 「ipconfig /renew」と入力してから、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。

11 LAN上のすべてのパソコンに対して手順1～10の操作を繰り返し、すべてのパソコンが異なるIPアドレスを持つように設定する。

Windows Vistaの場合

1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

2 「ネットワークとインターネット」をクリックする。

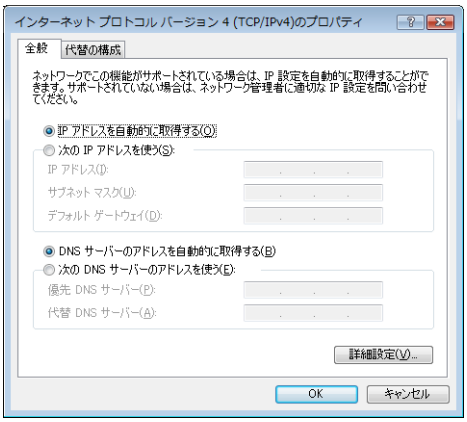
3 「ネットワークと共有センター」をクリックする。

4 画面左側の「ネットワーク接続の管理」をクリックする。

5 変更する接続を右クリックして、表示されたショートカットメニューから「プロパティ」をクリックする。

6 「ネットワーク」タブをクリックする。

7 「この接続は次の項目を使用します」欄で「インターネット プロトコル バージョン 4 (TCP/IPv4)」をクリックして選んでから、「プロパティ」をクリックする。



8 「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」を選んでから、「OK」をクリックする。

9 「ローカルエリア接続のプロパティ」画面で「閉じる」をクリックする。

10 「スタート」ボタンをクリックして、「すべてのプログラム」-「アクセサリ」-「コマンド プロンプト」を右クリックし、「管理者として実行」を選択する。

11 「ipconfig /release」と入力してから、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。

12 「ipconfig /renew」と入力してから、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。

13 LAN上のすべてのパソコンに対して手順1～12の操作を繰り返し、すべてのパソコンが異なるIPアドレスを持つように設定する。

Windows XPの場合

1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

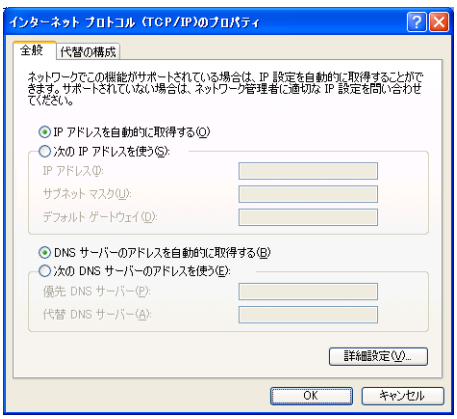
2 「ネットワークとインターネット接続」をクリックする。

3 「ネットワーク接続」をクリックする。

4 「ローカルエリア接続」のアイコンをクリックする。

5 「この接続の設定を変更する」をクリックする。

6 「インターネットプロトコル(TCP/IP)」を選んでから、「プロパティ」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」を選んでから、「OK」をクリックする。

8 「ローカルエリア接続のプロパティ」画面で「OK」をクリックする。

9 「スタート」ボタンをクリックして、「すべてのプログラム」-「アクセサリ」-「コマンド プロンプト」をクリックする。

10 「ipconfig /release」と入力してから、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。

11 「ipconfig /renew」と入力してから、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。

12 LAN上のすべてのパソコンに対して手順1～11の操作を繰り返し、すべてのパソコンが異なるIPアドレスを持つように設定する。

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の登録を削除する
2. 設定内容を初期化する

ご注意

- 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の登録を削除してから、設定内容を初期化するようにしてください。
- ネットボランチDNSの登録の削除は、ネットボランチDNS（ホストアドレスサービス）を登録したお客様のみ必要になります。
- 本製品を譲渡する際は、付属のマニュアル類もあわせて譲渡してください。

ネットボランチDNSの登録を削除する

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の登録の削除にご協力ください。
「ネットボランチDNSホストアドレスサービスの設定」画面で、「削除」をクリックします。

「ネットボランチDNSホストアドレスサービスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ネットボランチDNSホストアドレスサービスの設定」の「設定」

設定内容を初期化する

保存されている設定内容には、プロバイダへの接続に必要な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。
初期化の方法は、「本製品の設定を初期化する」（221ページ）をご覧ください。

ライセンス条文

PCRE License

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Copyright © 1997-2004 University of Cambridge All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MT19937 License

A C-program for MT19937, with initialization improved 2002/1/26.

Coded by Takuji Nishimura and Makoto Matsumoto.

Before using, initialize the state by using init_genrand(seed) or init_by_array(init_key, key_length).

Copyright © 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Any feedback is very welcome.

http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html

email: m-mat @ math.sci.hiroshima-u.ac.jp (remove space)

OpenSSL License

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

Original SSLeay License

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-) .
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Net-SNMP License

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ヤマハルーターお客様ご相談センター
TEL : 03-5651-1330
FAX : 053-460-3489

ご相談受付時間
9:00 ～ 12:00 13:00 ～ 17:00
（土・日・祝日、弊社定休日、年末年始は休業とさせていただきます）

お問い合わせページ
http://jp.yamaha.com/products/network/

ヤマハ株式会社（2012年8月 第1版）