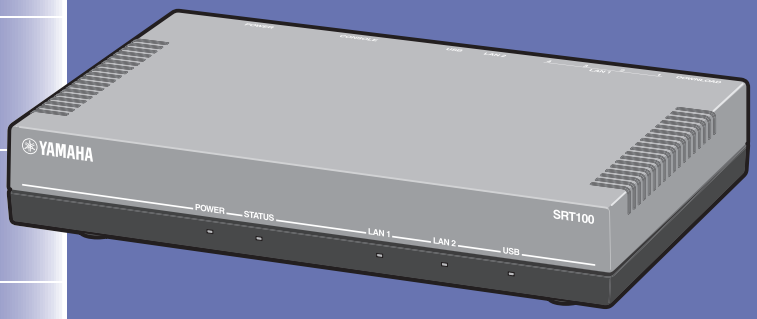
# SRT100

ファイアウォールルーター






## 取扱説明書

ヤマハSRT100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。

# 安全上のご注意

## 本製品を安全にお使いいただくために

以下の点を必ず守ってお使いください。

### 安全のための注意事項を守る

詳しくは、7〜8ページをご覧ください。

### 故障したら使用を中止する。

お買い上げの販売店またはヤマハのお問い合わせ窓口(177ページ)にご連絡ください。

## マークの意味

本書および本製品では、本製品を安全にお使いいただくため、守っていただきたい事項に次のマークを表示していますので、必ずお読みください。また、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。

### ⚠警告

人体に危険を及ぼしたり、装置に大きな損害を与える可能性があることを示しています。必ず守ってください。

### ⚠注意

機能停止を招いたり、各種データを消してしまう可能性があることを示しています。十分注意してください。

# 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、ファイアウォールルーターです。

## 付属品をご確認ください

- LANケーブル(1本)
- CD-ROM（1枚）
- 取扱説明書(本書)(1冊)
- 保証書(1枚)

## 本書の主な内容

### インターネットに接続するために必要な情報



### 拠点間接続のために必要な情報



IPsec通信による拠点間接続およびVPNクライアントによるIPsec接続、IPIPトンネル通信、閉域網での接続について説明しています。

### 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



**ご注意**

- 本書は、本製品の基本的な機能を使用するための情報を提供するためのものです。
- 「コマンドリファレンス」(付属CD-ROMに収録)や設定画面のヘルプには、より詳細な情報が掲載されています。必要にあわせてご覧ください。

**その他、本書には多くの情報が記載されています。詳しくは目次をご覧ください。**


▶4 ページをご覧ください。

# 目次



## はじめに



## インターネットに接続する（PPPoE/CATV）



## 拠点間接続する



**IPsecで接続する**



**閉域網（フレッツ網など）を使用して拠点間を接続する**

# セキュリティ機能を使いこなす



# ルーターとして活用する

# 本製品の運用管理



# 困ったときは



# 付録

# ⚠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、当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。
- 本製品から発煙や異臭がするとき、内部に水分や薬品類が入ったとき、および電源コードが発熱しているときは、直ちに電源コードをコンセントから抜いてください。そのまま使用を続けると、火災や感電のおそれがあります。
- 濡れた手で電源コードを触らないでください。感電や故障のおそれがあります。
- 電源コードを傷付けたり、無理に曲げたり、引っ張ったりしないでください。火災や感電、故障、ショート、断線の原因となります。
- 本製品の電源部は日本国内用AC100V（50/60Hz)の電源専用です。他の電源で使用すると、火災や感電、故障の原因となります。
- 安全のため、電源コードは容易に外すことのできるコンセントに接続してください。家具の後ろなど手の届かない場所にあるコンセントには接続しないでください。
- 本製品をご使用にならないときは、電源コードを必ずコンセントから外してください。
- 本製品を落下させたり、強い衝撃を与えたりしないでください。内部の部品が破損し、感電や火災、故障の原因となります。
- 本製品を分解したり、改造したりしないでください。火災や感電、故障の原因となります。
- 本製品の通風口を塞いだ状態で使用しないでください。火災や感電、故障の原因となります。
- 電源を入れたままケーブル類を接続しないでください。感電や故障、本製品および接続機器の破損の恐れがあります。
- LAN1/LAN2ポートなどの通信ポートには、本来接続される信号と異なる信号ケーブルを接続しないでください。火災や故障の原因となります。
- 本製品のポートに指や異物を入れないでください。感電や故障、ショートの原因となります。
- 本製品を他の機器と重ねて置かないでください。熱がこもり、火災や故障の原因となることがあります。
- 近くに雷が発生したときは、電源コードやケーブル類を取り外し、使用をお控えください。落雷によって火災や故障の原因となることがあります。

# ⚠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。

- 直射日光や暖房器等の風が当たる場所、温度や湿度が高い場所には、置かないでください。故障や動作不良の原因となります。
- 極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所で使用しないでください。故障や動作不良の原因となります。結露が発生した場合は、電源コードをコンセントから抜き、乾燥させ、充分に室温に慣らしてから使用してください。
- ほこりが多い場所や油煙が飛ぶ場所、腐蝕性ガスがかかる場所、磁界が強い場所に置かないでください。故障や動作不良の原因となります。
- 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ようにしてください。故障や動作不良の原因になります。
- アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。アース接続は必ず、電源コードをコンセントにつなぐ前に行ってください。また、アース接続をはずす場合は、必ず電源コードをコンセントから取りはずしてから行ってください。
- 本製品を修理や移動等の理由により輸送する場合には、必ず本製品の設定を保存してください。
- 本製品に触れる際には、人体や衣服から静電気を除去する等、静電気対策を十分に行ってください。静電気によって故障する恐れがあります。

# 使用上のご注意

- 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、当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。
- 本製品を譲渡する際は、マニュアル類も同時に譲渡してください。
- 本製品を廃棄する場合には不燃物ゴミとして廃棄してください。または、お住まいの自治体の指示に従ってください。本製品はコイン型リチウム電池を内蔵しています。
- 本製品のUSBポートは、すべてのUSBメモリの動作を保証するものではありません。
- USBメモリの内部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。

# 重要なお知らせ

## セキュリティ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対策を行うことを強くおすすめいたします。**

## プロバイダ契約について

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。

## 電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス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。

## 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。

## 輸出について

本製品は「外国為替及び外国貿易法」で定められた規制対象貨物(および技術)に該当するため、輸出または国外への持ち出しには、同法および関連法令の定めるところに従い、日本国政府の許可を得る必要があります。

# 本書の表記について

## 略称について

本書ではそれぞれの製品について、以下のように略称で記載しています。

- YAMAHA SRT100：本製品
- Microsoft® Windows®：Windows
- Microsoft® Windows® XP：Windows XP
- Microsoft® Windows Vista™：Windows Vista
- 10BASE-T（100BASE-TX）ケーブル：LANケーブル

## 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、必ずプロバイダから指定され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。付属のマニュアル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。

## 商標について

- イーサネットは富士ゼロックス社の登録商標です。
- Microsoft 、Windowsは米国Microsoft社の米国およびその他の国における登録商標です。
- Adobe 、Acrobatは米国Adobe Systems社の登録商標です。

# 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

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」）（次ページ参照）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てはなりません。過失を含むいかなる場合であっても、ヤマハは、本使用許諾契約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。

なお、DOWNLOADボタンを使用しないでリビジョンアップする方法も提供しております。そちらをご利用される方はhttp://NetVolante.jpをご参照ください。

DOWNLOADボタンの詳しい操作方法は、本書144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

本機を使用する際には、以下のソフトウェアライセンス契約に同意いただく必要があります。

## 1. 使用許諾

ヤマハルーター製品・サーバー製品(以下、「本製品」という)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」という)は、ヤマハ株式会社( 以下、「ヤマハ」という) がお客様に使用許諾するものです。本ソフトウェアは、本製品に関わる目的でのみ使用することができます。本使用許諾契約は、ヤマハから提供した本ソフトウェア及び本使用許諾契約に基づいて作成された複製物に適用されます。

## 2. 再配布の禁止

お客様は、ヤマハの許可を得た場合を除き、本ソフトウェアを第三者に配布したり、不特定多数の者によるアクセスが可能なウェブ・サイトなどにアップロード、掲示することはできません。

## 3. 複製物の作成

お客様は、バックアップ及び、本製品で動作させることを目的とする場合を除き、本ソフトウェアの複製物を作成することはできません。

## 4. 逆コンパイル、リバースエンジニアリング、逆アセンブルの禁止

お客様は、本ソフトウェア又はその一部を、逆コンパイル、リバースエンジニアリング、逆アセンブルもしくは修正等し、またはこれらの二次的著作物を創作することはできません。また、お客様は、これらを第三者に対し頒布しまたは再使用許諾等をすることはできません。

## 5. 責任の制限

ヤマハは、本使用許諾契約に起因するお客様や第三者の損害について一切の責任を負いません。また、ヤマハは、お客様に対し、本ソフトウェアの使用目的への適合性、商業性等ならびに第三者の権利非侵害について一切保証しません。なお、ヤマハは、独自の判断にもとづき、本ソフトウェアの仕様または内容等を予告なく変更、修正等することができるものとします。

## 6. 外国為替法及び外国貿易法による規制

本ソフトウェアは、「外国為替及び外国貿易法第25条第1項に基づいて規制される技術(役務) に該当します。このため、本ソフトウェア、及び本ソフトウェアをインストールした本製品の日本国外への持ち出しには、日本政府による輸出許可が必要となる場合があります。また、本ソフトウェアの、日本国内に住所を持たない人への提供にも、日本政府による許可が必要となる場合があります。

## 7. 日本に居住する人への限定提供

本ソフトウェアは、日本国内に居住する法人または個人にのみ提供されるものとします。

## 8. 日本国法令の準拠

本使用許諾契約は、日本国の法令に準拠し、これに基づいて解釈されるものとします。

# ヤマハルーター製品のお客様サポートについて（サポート規定）

ヤマハ株式会社はルーター製品を快適に、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

①FAQ、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頂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にて行います。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ヤマハルーターの返品・交換が生じた場合は、ご購入店経由となります。尚、交換、返品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頂きます。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)にて行わせて頂きます。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。

# SRT100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、ファイアウォールルーターです。

## ファイアウォールルーターとしての特徴

### 直感的に操作できる、「日本語GUI」搭載

コマンドを使用することなく、Webブラウザからの設定操作でポリシーベースのフィルタリングを実現できます。階層型にポリシーを記述できるため、設定と管理の手間も軽減できます。

- **入力遮断フィルター**：受信したパケットに対して、IPアドレスやプロトコル、ポート番号を基準に通過・破棄を判別します(102ページ)。
- **ポリシーフィルター**：Stateful Inspection方式による、コネクションを単位とするアクセス制御を実現します(104ページ)。ポリシーは最大4階層まで階層的に並べて定義できるので、「上位階層で大まかなルールを決めてから、次第に詳細化する」といった設定も実現できます。

### 設定や運用の問題を確認できる、セキュリティアドバイス機能

実際に運用を始める前に、設定の安全性を確認するための機能を装備しています。セキュリティを向上させるだけでなく、構成したセキュリティ機能が適切に動作しているか確認するために役立ちます。

- **診断機能**：WAN側に攻撃に遭いやすいポートが開かれていないかを診断します(119ページ)。また、IPsec-VPNや拠点・センター間経路、ファームウェア、接続許容端末、パスワードについては、設定操作の段階で脆弱性がないかどうか確認が行われます。
- **監視機能**：攻撃や異常性の高いトラフィックが発生した場合に、検知した結果を表示します(111ページ)。また、未登録のMACアドレスを持つ端末からの接続を監視できます。
- **レポート機能**：診断結果や監視結果を確認できます。設定画面で確認できるだけでなく、メールによる通知も利用できます(140ページ)。

### 導入後の効果を確認できる、統計機能

本製品の内部リソース情報やトラフィック情報、IDS情報などを、統計情報として保存・参照できます。設定画面でグラフ表示を確認するだけでなく、統計情報をCSVファイルでダウンロードすることもできるため、ネットワークの利用状況や傾向を分析する際に便利です。市販のUSBメモリに統計情報を自動保存することもできます。

- **リソース統計**：CPU使用率やメモリー使用率、FLOW数、NATエントリー数を記録・集計し、出力します(131ページ)。
- **トラフィック統計**：インターフェースごとにトラフィック状態を集計します(132ページ)。
- **不正アクセス検知の統計**：検知された攻撃回数を、攻撃の種別や攻撃先アドレス別に分類して出力できます(111ページ)。

### 不正なデータを遮断できる、LANセキュリティ機能

- **Winnyフィルタ機能**：ファイル共有ソフトウェア「Winny」が利用するパケットを検出すると共に、該当パケットを破棄し、通信を遮断します（111ページ）。
- **DHCP端末認証機能**：あらかじめ使用を許可した端末（登録済端末）と、許可していない端末（未登録端末）とをネットワーク上で区別します（112ページ）。許可の有無によって、それぞれの端末がアクセス可能なネットワークを制御できます。
- **Dynamic Class Control機能**：帯域を圧迫している特定パソコンの使用帯域を、制限・遮断できます（101ページ）。詳しくは「コマンドリファレンス」をご覧ください。

## 充実した基本機能

### ブロードバンド&IPsec対応

- 各種ブロードバンド回線用モデムと本製品をLANケーブルで接続して、FTTHやADSL、CATVなどのブロードバンド回線でインターネットなどに接続できます。
- IPsecに対応しているため、ブロードバンド回線を利用したVPN（仮想プライベートネットワーク）を構築する場合でも、より安全にデータをやり取りできます。

### 保守管理の負荷の低減

- DOWNLOADボタンを押すだけで、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（144ページ）。ヤマハルーターホームページから最新版をダウンロードする以外に、USBメモリに保存したファームウェアを使用することもできます。
- STATUSランプの状態を確認することで、接続先の機器との通信が不可能な状態になっていないか確認できます（134ページ）。
- 本製品の設定ファイルやログを、市販のUSBメモリに保存できます（137ページ）。

### その他のルーター機能

- SNMP（Simple Network Management Protocol）に対応しています（149ページ）。RFC1157（SNMP）およびRFC1213（MIB-II）準拠の機能を搭載しています。
- 動的経路制御プロトコルRIPおよびRIP2、OSPF、BGP-4に対応しています。これらのプロトコルに対応している他の機器との間で、経路情報をやり取りできます。
- VRRP（Virtual Router Redundancy Protocol）に対応しています。他のVRRP対応ルーターと併設することで、機器を冗長構成にすることができます。
- QoS連携機能（帯域検出機能と負荷通知機能）に対応しています。詳しくは「コマンドリファレンス」およびヤマハルーターホームページをご覧ください。
- タグVLAN（IEEE802.1Q）に対応しています。詳しくは「コマンドリファレンス」およびヤマハルーターホームページをご覧ください。
- NATトラバーサルに対応しています（55、66ページ）。

**ヤマハルーターホームページのご案内**

ヤマハルーターホームページで、ヤマハルーターを使った高度な活用例や詳しい解説がご覧いただけます。

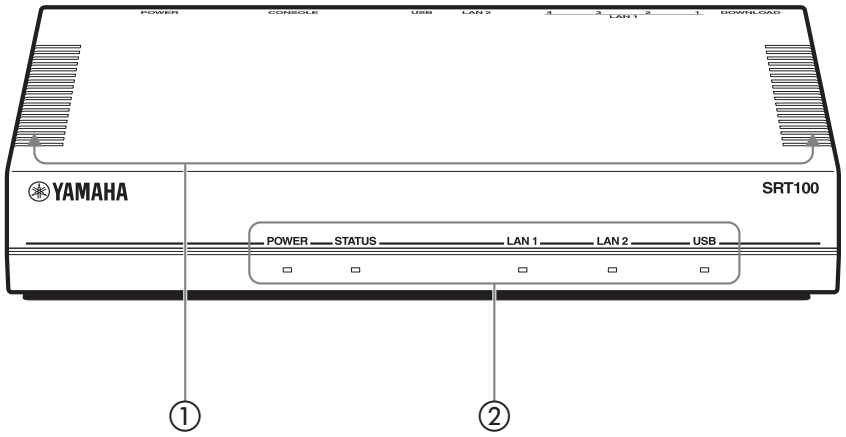
http://NetVolante.jp/

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

# 各部の名称とはたらき



## 前面




### ① 通風口

内部の熱を逃がすための穴です。

### 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」(次ページ)をご覧ください。

- **POWER**：本製品の電源の状態を示します。電源が入っているときは点灯します。
- **STATUS**：接続先の機器との通信が不可能な状態になっているかどうかを示します(134ページ)。
- **LAN1**：LAN1ポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- **LAN2**：LAN2ポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- **USB**：USB機器の接続、使用状態を示します。

## 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」(134ページ)をご覧ください。
◎ 通信が不可能な状態になっていません。

**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。

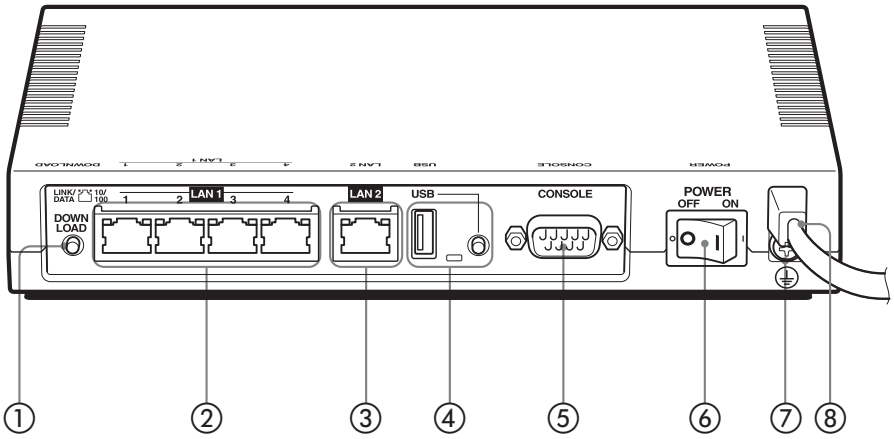
**LAN2ランプ**

◉ 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。

**USBランプ**

◉ USBデバイスがUSBポートに差さっていて、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。
エラー音が鳴る場合は、過電流保護機能によりUSB機能の使用が中断されているか、FOMAリモートセットアップ機能(158ページ)使用時にFOMAを認識できない状態です。
◎ USBデバイスがUSBポートに差し込まれていません。または、ポート に差し込まれているUSBデバイスを取り外すことができる状態です。

# 背面




## ① 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、このスイッチを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)」(144ページ)をご覧ください。

## ② LAN1ポート

パソコンのLANポートまたはHUBのポートとLANケーブルで接続します。
各LAN1ポートの上部には、LINKランプ(左側)とSPEEDランプ(右側)があります。

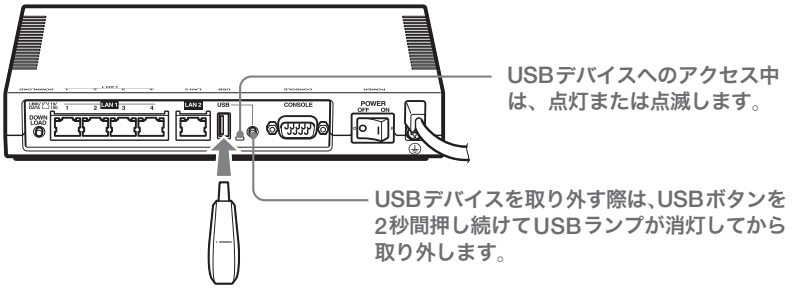
- **LINKランプ**：リンク状態によって、消灯(リンク喪失)または点灯(リンク確立)、点滅(データ転送中)します。
- **SPEEDランプ**:接続速度によって、消灯(10BASE-T接続)または点灯(100BASE-TX)します。

## ③ LAN2ポート

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ポートの上部には、LINKランプ(左側)とSPEEDランプがあります。動作については、LAN1ポートのランプと同様です。

## ④ USBポートとボタン

市販のUSBメモリを使用して、設定ファイルのコピー（137ページ）やログの保存（138ページ）、リビジョンアップ（147ページ）を実行できます。また、FOMAを接続してリモートアクセスによる設定変更を行うこともできます（158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USBランプが消灯してから、USBデバイスを取り外してください。

## ⑤ 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」（154ページ）をご覧ください。

## ⑥ POWERスイッチ

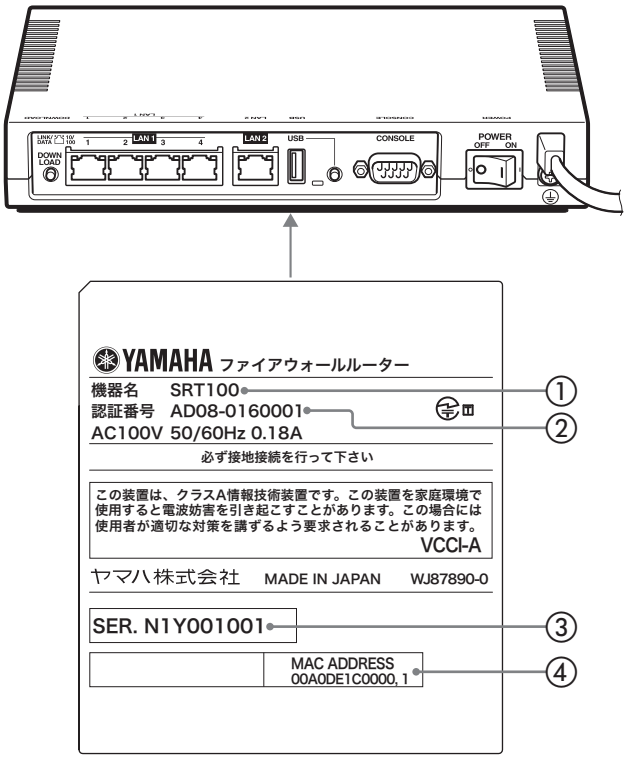
本製品の電源を入／切します。

## ⑦ アース端子

アースコードを接続します。必ず接続してください。

## ⑧ 電源コード

# 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です。

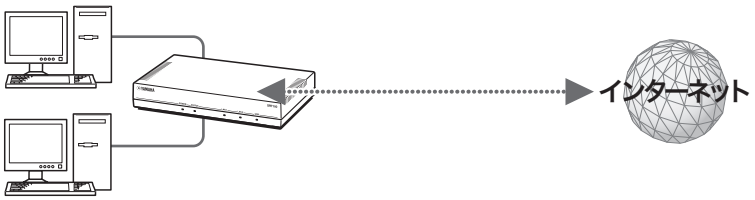
## ④ MACアドレス

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。「00A0DE1C0000, 1」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：**00A0DE1C0000
- **LAN2側MACアドレス：**00A0DE1C0001

# インターネット接続の概要

ここでは、CATVインターネットやPPPoEを用いない端末型接続(Yahoo!BBなど)、およびPPPoEを用いる端末型接続(フレッツ・ADSL、Bフレッツなど)で、インターネットに接続する方法について説明します。




**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「セキュリティ機能を使いこなす」(98ページ)をご覧ください。

# 準備を始める前にご用意ください

## アースコード

アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

## LANケーブル

パソコンの台数や距離に合わせて、10BASE-Tまたは100BASE-TX対応のLANケーブルをご用意ください。

## HUB

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対応のHUB（またはスイッチングHUB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場合は、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。「4.LAN側IPアドレスを設定する」（35ページ）で、本製品のDHCP機能を動作させないように設定してください。

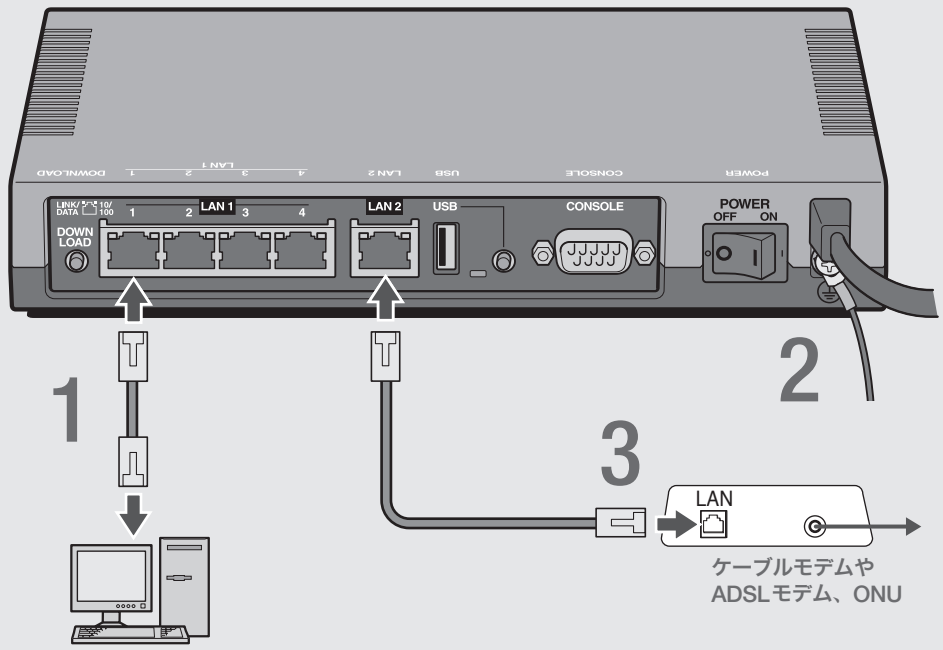
## プロバイダの設定資料

接続先を設定してインターネットに接続するには、プロバイダ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

# ケーブルと電源を接続する






## 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 アース端子のネジを+ドライバ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。

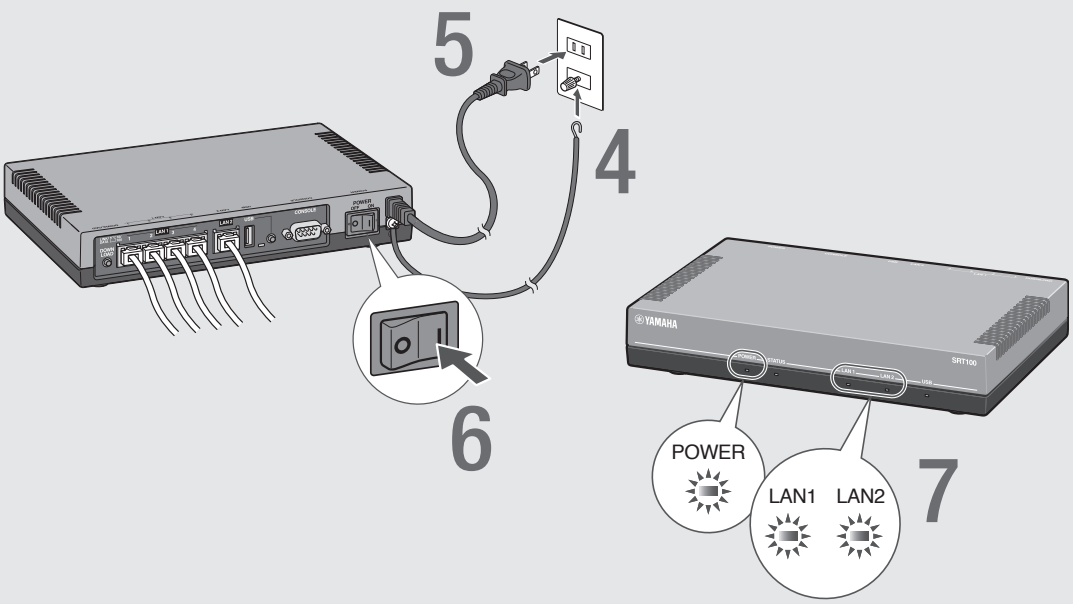
アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

## 3 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。




## 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。

**電源コードを取りはずす場合は**

先に電源コードを取りはずしてから、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。

ランプが何回か点滅した後、POWERランプが点灯します。

## 7 パソコンやHUB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どうか、パソコンやHUBの電源が入っているかどうか確認してください。
- 本製品に接続したすべてのパソコンおよびHUB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どうか、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どうか確認してください。

# 本製品の設定画面を開く

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設定画面を開いて行います。

**ご注意**

設定画面を使用するには、Windows版Internet Explorer 6.0以降のWebブラウザが必要です。

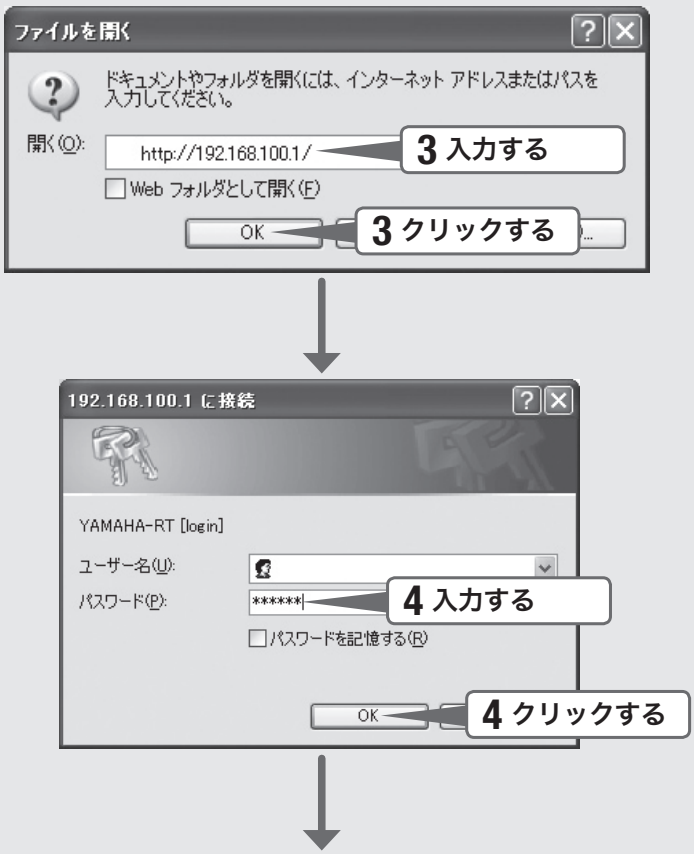
**ヒント**

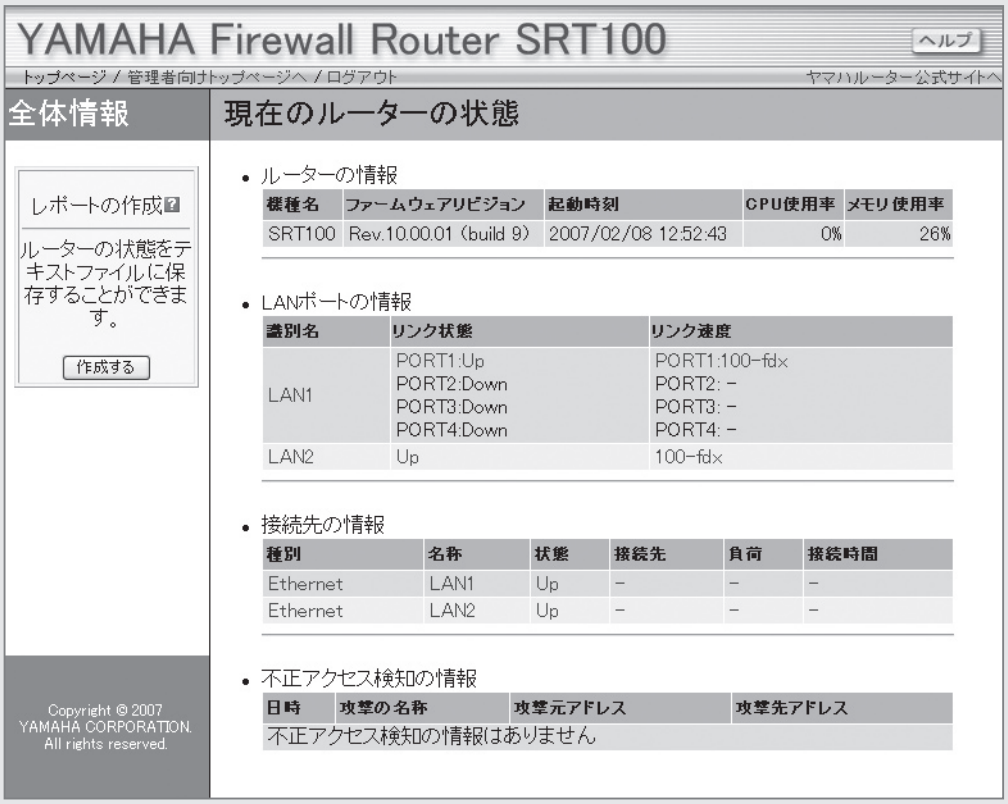
TELNETソフトウェアでコンソール画面からコマンドを入力して、設定画面よりも詳細な設定を行うことができます(コンソールコマンド)。TELNETソフトウェアで本製品に接続する方法については150ページ、本製品で使用できるコマンドについては「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。



## 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Webブラウザを起動して、「ファイル」メニューから「開く」を選ぶ。






## 3 「http://192.168. 100.1/」と半角英字で入力してから、「OK」をクリックする。

「192.168.100.1に接続」画面が表示されます。

## 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。

本製品の設定画面のトップページが表示されます。

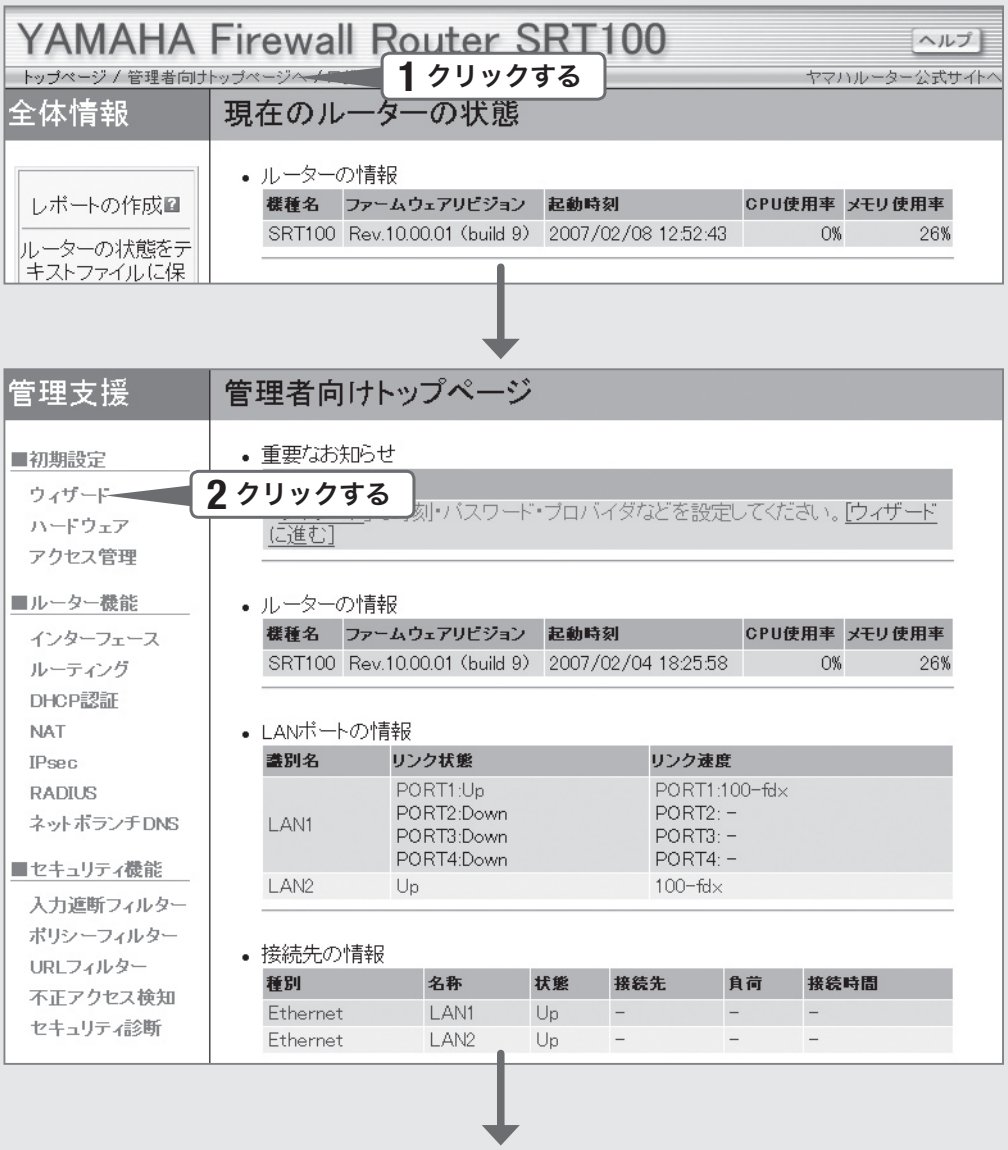
**設定画面のトップページが表示されないときは**

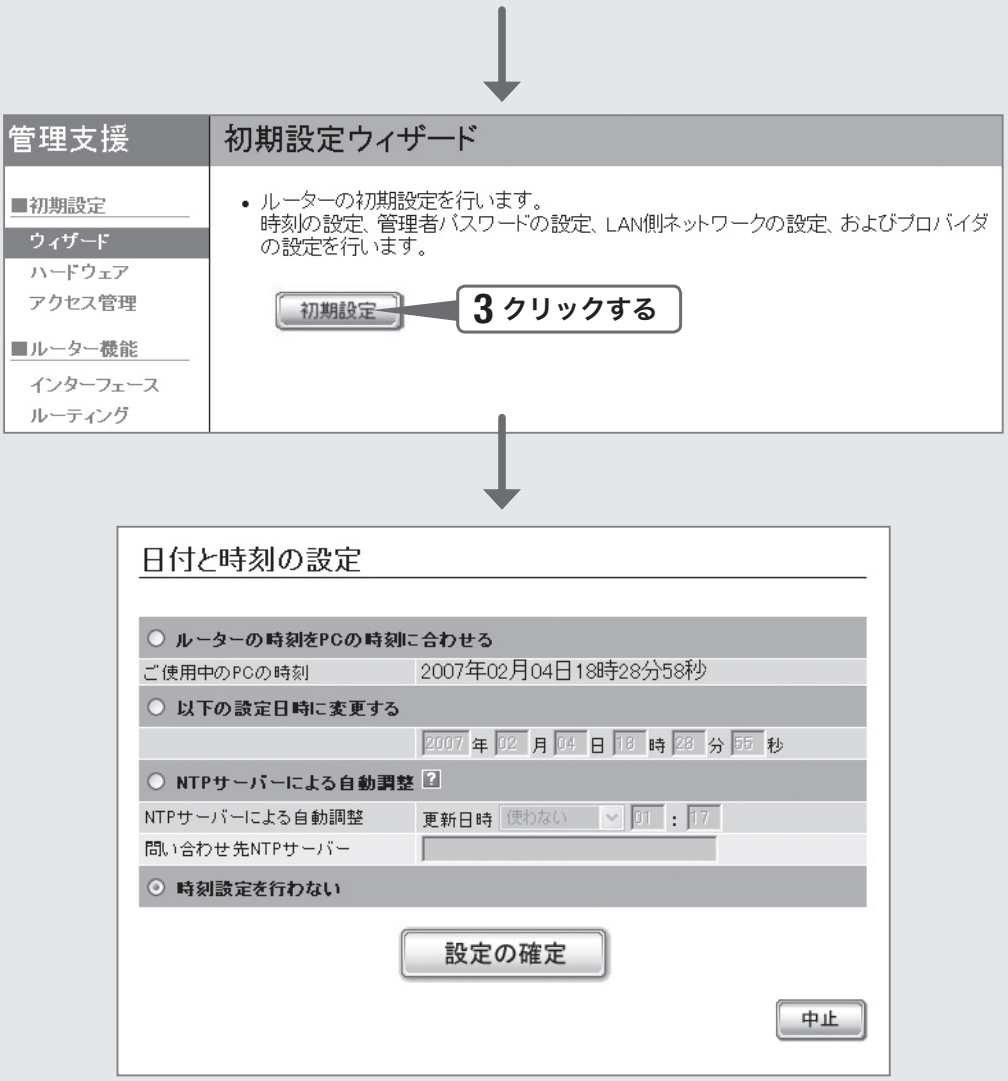
「設定画面で設定できない」(162ページ)をご覧ください。

# 「初期設定ウィザード」で接続設定する

## 1.「初期設定ウィザード」を開く

「初期設定ウィザード」を使用して、本製品をネットワーク上で使用するための基本的な設定をまとめて行うことができます。「初期設定ウィザード」を開くには、以下の手順で操作します。






## 1 「管理者向けトップページへ」をクリックする。

管理者向けトップページが表示されます。

## 2 「ウィザード」をクリックする。

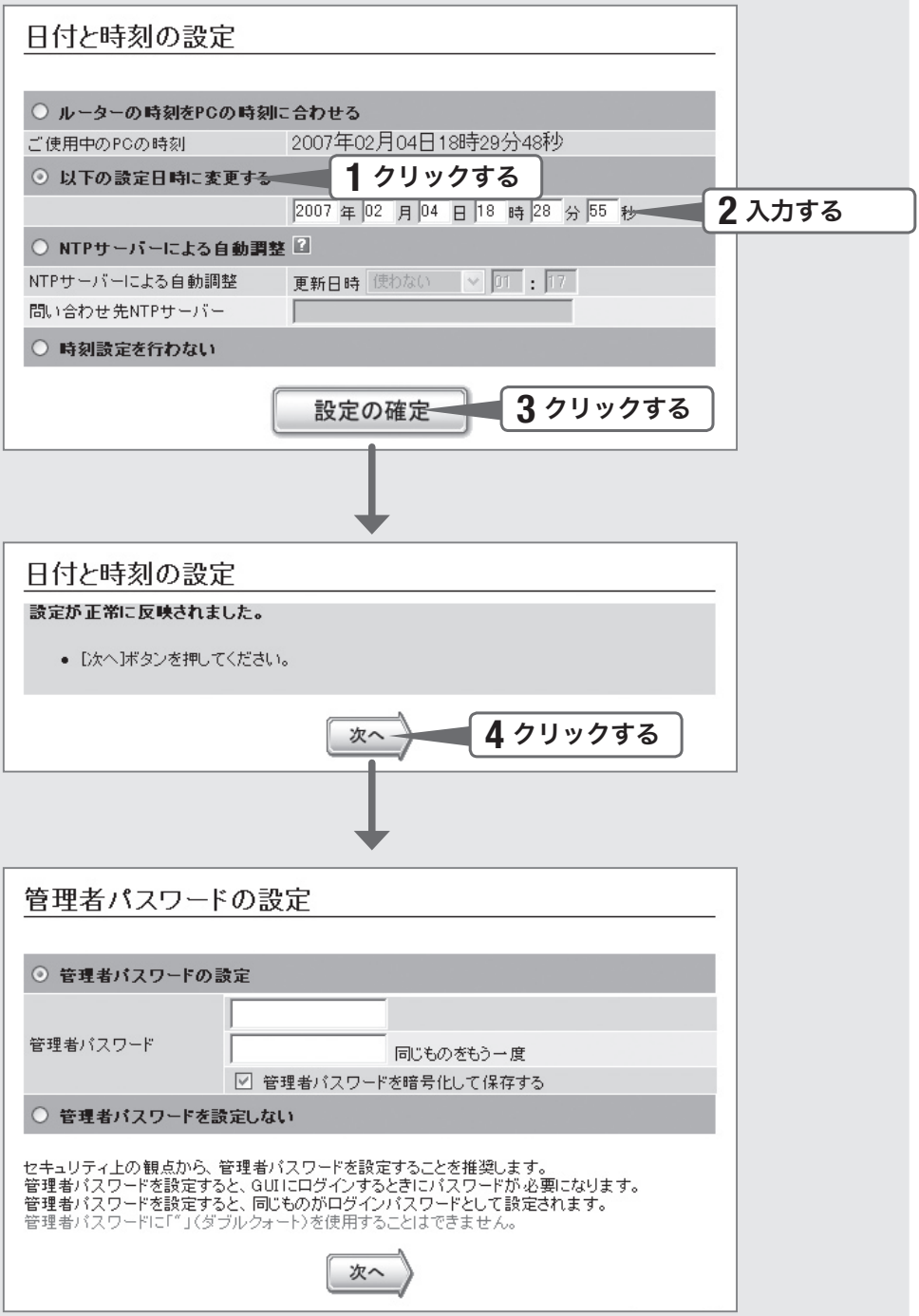
「初期設定ウィザード」画面が表示されます。

## 3 「初期設定」をクリックする。

「初期設定ウィザード」の「日付と時刻の設定」画面が別画面で表示されます。

# 2. 日付・時刻を合わせる

「日付と時刻の設定」画面で、本製品の日付と時刻を合わせます。



## 1 「日付と時刻の設定」画面で、「以下の設定日時に変更する」をクリックして選ぶ。

### 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。また、NTPサーバーを利用して手動で時刻を合わせたり、時刻を直接入力して合わせたりすることもできます。
詳しくは、「本体の設定」画面のヘルプをご覧ください。

**ご注意**

本製品のセキュリティ設定によっては、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（104ページ）。

## 2 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。

## 3 「設定の確定」をクリックする。

確認画面が表示されます。

## 4 「次へ」をクリックする。

「管理者パスワードの設定」画面が表示されます。

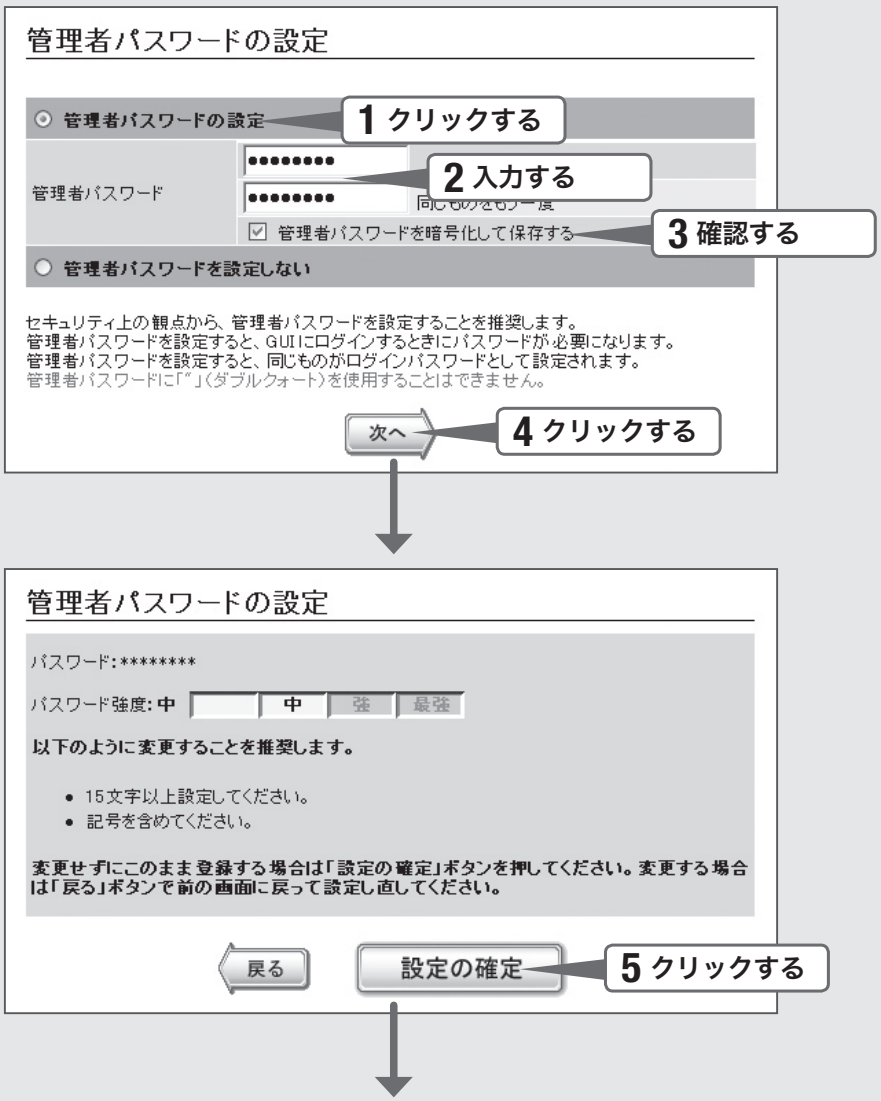
# 3.パスワードを設定する

セキュリティ対策を行う上でも、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。

**ヒント**

工場出荷時は、「doremi」が初期パスワードとして設定されています。セキュリティの問題を防ぐためにも、以下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。





## 1 「管理者パスワードの設定」画面で、「管理者パスワードの設定」をクリックして選ぶ。

## 2 「管理者パスワード」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。

### 安全なパスワードを設定するためのヒント

第三者から本製品へのアクセスを防ぐために、以下の点を考慮してパスワードの強度を上げるようにしてください。

- パスワードは15文字以上にする。
- 英字の大文字・小文字、数字を混在させる。
- 記号を使用する。

## 3 「管理者パスワードを暗号化して保存する」にチェックが付いていることを確認する。

チェックを付けるとパスワードが暗号化されて本製品の設定ファイル(config)に記録されるため、第三者がconfigファイルを入手した場合でも、本製品の設定を保護できます。

## 4 「次へ」をクリックする。

確認画面が表示されます。

### パスワード強度が低い場合は

パスワードの強度確認画面が表示されます。

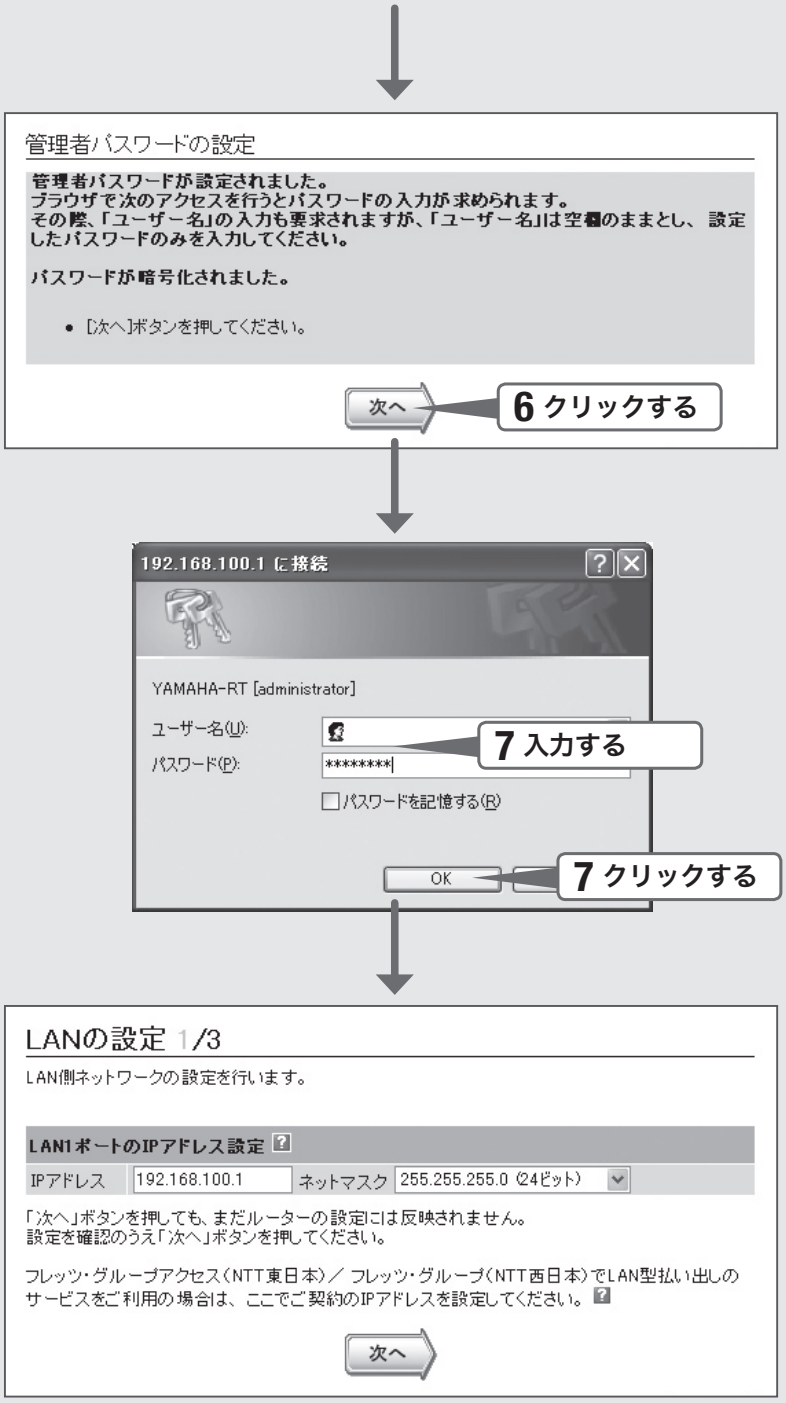
- **パスワードを修正する場合は**:「戻る」をクリックして手順2の操作からやり直します。手順2の「安全なパスワードを設定するためのヒント」を考慮してパスワードを修正してください。
- **そのまま使用する場合は**:「設定の確定」をクリックします。

## 5 「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、確認画面が表示されます。

## 6 「次へ」をクリックする。

パスワード入力画面が表示されます。




## 7 「パスワード」欄に手順2で設定したパスワードを入力してから、「OK」をクリックする。

「LANの設定 1/3」画面が表示されます。

**ヒント**

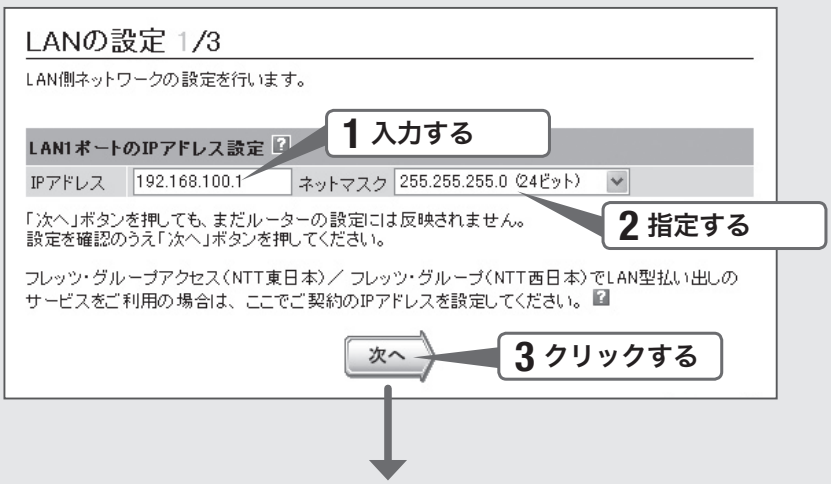
「ユーザー名」欄には何も入力する必要はありません。

# 4.LAN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。

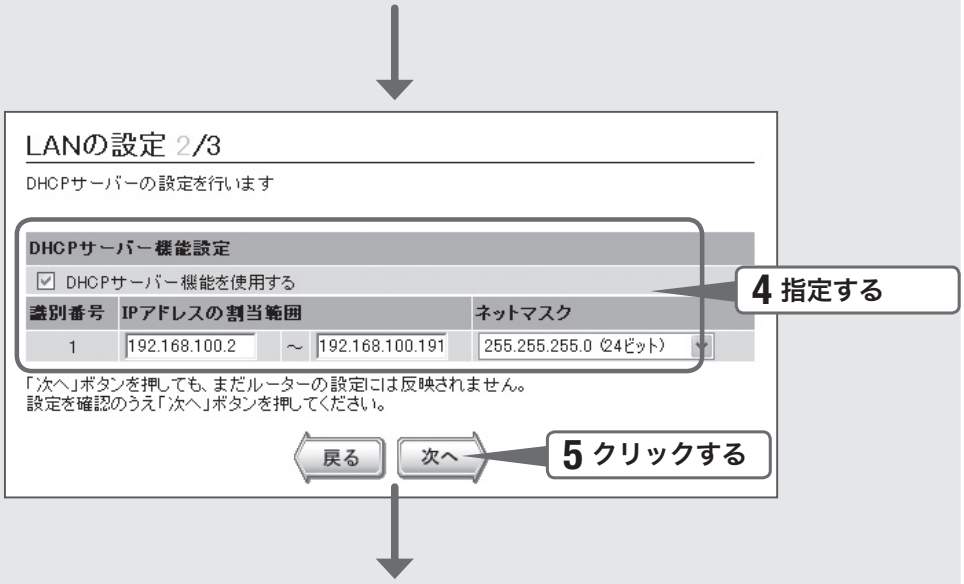



**1** **「LANの設定 1/3」画面で、「IPアドレス」欄に、本製品のLAN側IPアドレスを入力する。**

**2** **「ネットマスク」欄で、本製品のLAN側ネットマスクを選ぶ。**

**3** **「次へ」をクリックする。**

「LANの設定 2/3」画面が表示されます。




## 4 本製品のDHCPサーバー機能の設定を確認して、必要に応じて設定を変更する。

### 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場合は

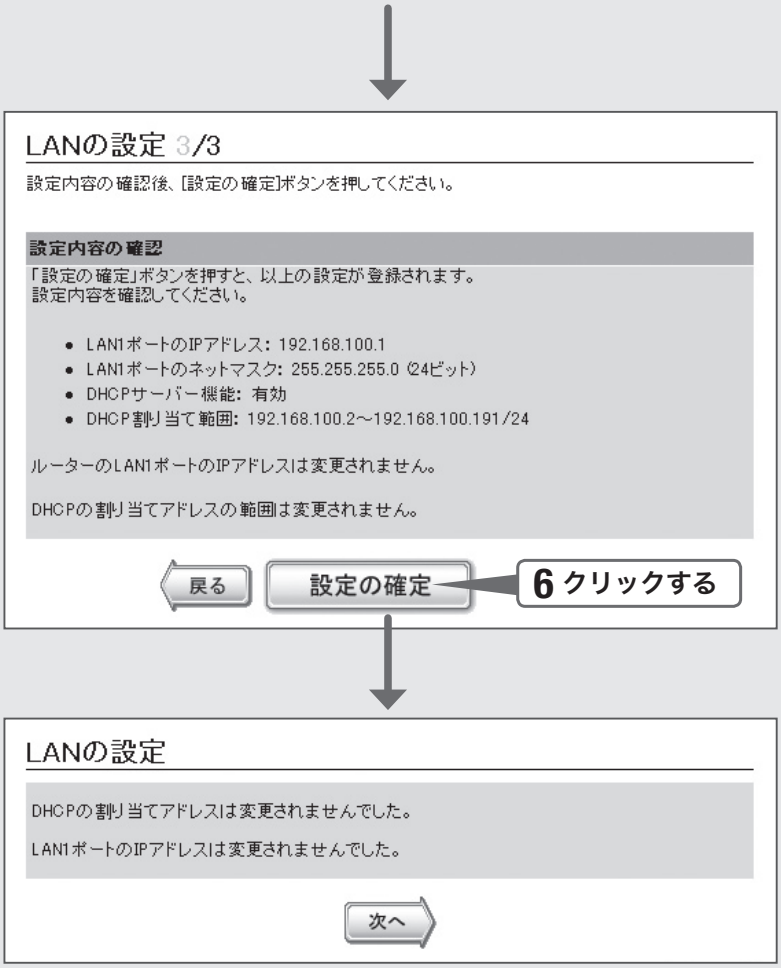
本製品のDHCPサーバー機能を無効にする必要があります。
「DHCPサーバー機能を使用する」をクリックして、チェックを外してください。

### DHCPサーバー機能によるIPアドレスの割り当て範囲を変更したい場合は

「DHCPサーバー機能を使用する」をクリックしてチェックを付けてから、割り当て範囲とネットマスクを指定します。

## 5 「次へ」をクリックする。

「LANの設定 3/3」画面が表示されます。




## 6 「設定の確定」をクリックする。

「LANの設定」画面が表示されます。

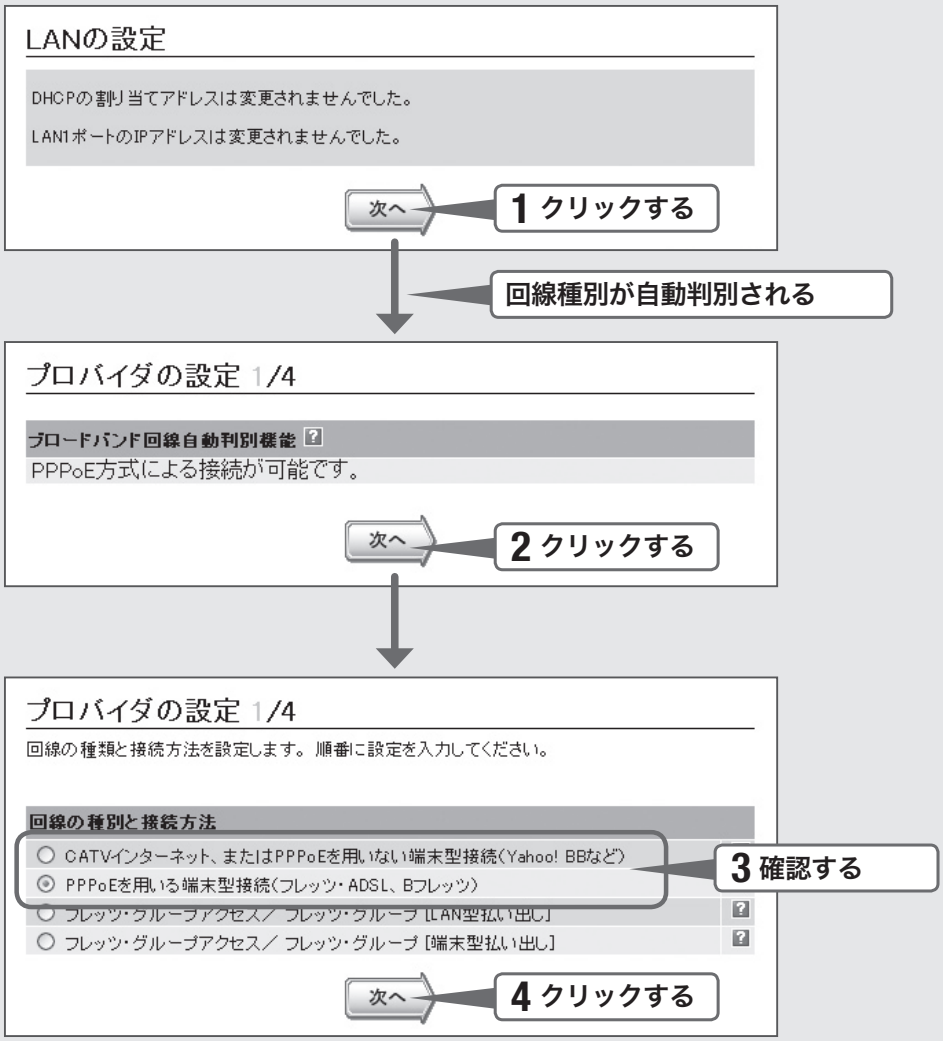
## 7 本製品のLAN側IPアドレスやDHCPサーバー機能によるIPアドレスの割り当て範囲を変更した場合は、パソコンのIPアドレスを変更する。

パソコンのIPアドレスを変更するには、「LAN内のパソコンのIPアドレスを変更する」(178ページ)をご覧ください。

### 引き続き、インターネットへの接続設定を行います

そのまま次ページの操作に進んでください。

# 5. 接続方法を確認する




## 1 「LANの設定」画面で、「次へ」をクリックする。

本製品のブロードバンド回線自動判別が動作して、判別結果の回線の種類が表示されます。

**ご注意**

- 本製品のLAN2ポートにブロードバンド回線を接続していない場合は、自動判別機能は動作しません。
- 回線自動判別機能を一度実行すると、次回から自動判別は行いません。

## 2 「次へ」をクリックする。

回線自動判別の結果に応じた項目が選択された状態で、「プロバイダの設定1/4」画面が表示されます。

## 3 自動判別された接続方法を確認する。

### A 「CATVインターネット、またはPPPoEを用いない端末型接続」が選ばれた場合

「CATVインターネット、またはPPPoEを用いない端末型接続」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
- アッカ・ネットワークス（ADSLモデムがルーターモードの場合）
- 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

### B 「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ）」が選ばれた場合

「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ）」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・ADSL
- Bフレッツ
- アッカ・ネットワークス（ADSLモデムがブリッジモードの場合）
- イー・アクセス（ADSLモデムがブリッジモードの場合）

### 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「CATVインターネット、またはPPPoEを用いない端末型接続」または「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ）」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。

## 4 「次へ」をクリックする。

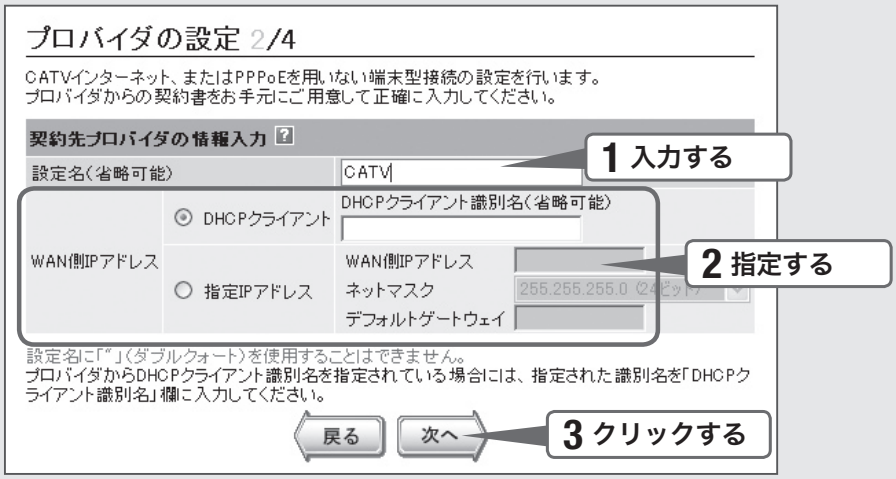
接続回線に合わせた設定画面が表示されます。

以下の設定は接続回線によって異なりますので、選んだ接続回線の説明をご覧ください。


A 「CATVインターネット、またはPPPoEを用いない端末型接続」が選ばれた場合 ▶40 ページをご覧ください。

B 「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ）」が選ばれた場合 ▶44 ページをご覧ください。

# A CATVインターネット（39ページから） 6. プロバイダの情報を指定する




## 1 「設定名」欄に、インターネット接続の設定名を入力する。

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アドレスが指定されていない場合は**

「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は**

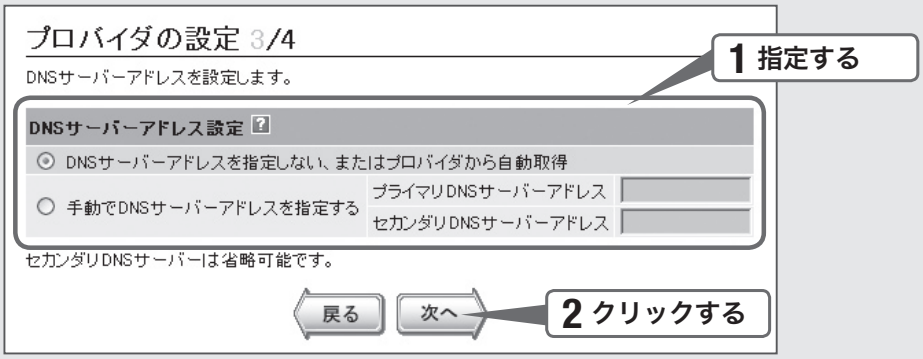
「指定IPアドレス」をクリックして選んでから、以下の設定を行います。

- **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。

# A CATVインターネット 7.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は**

「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は**

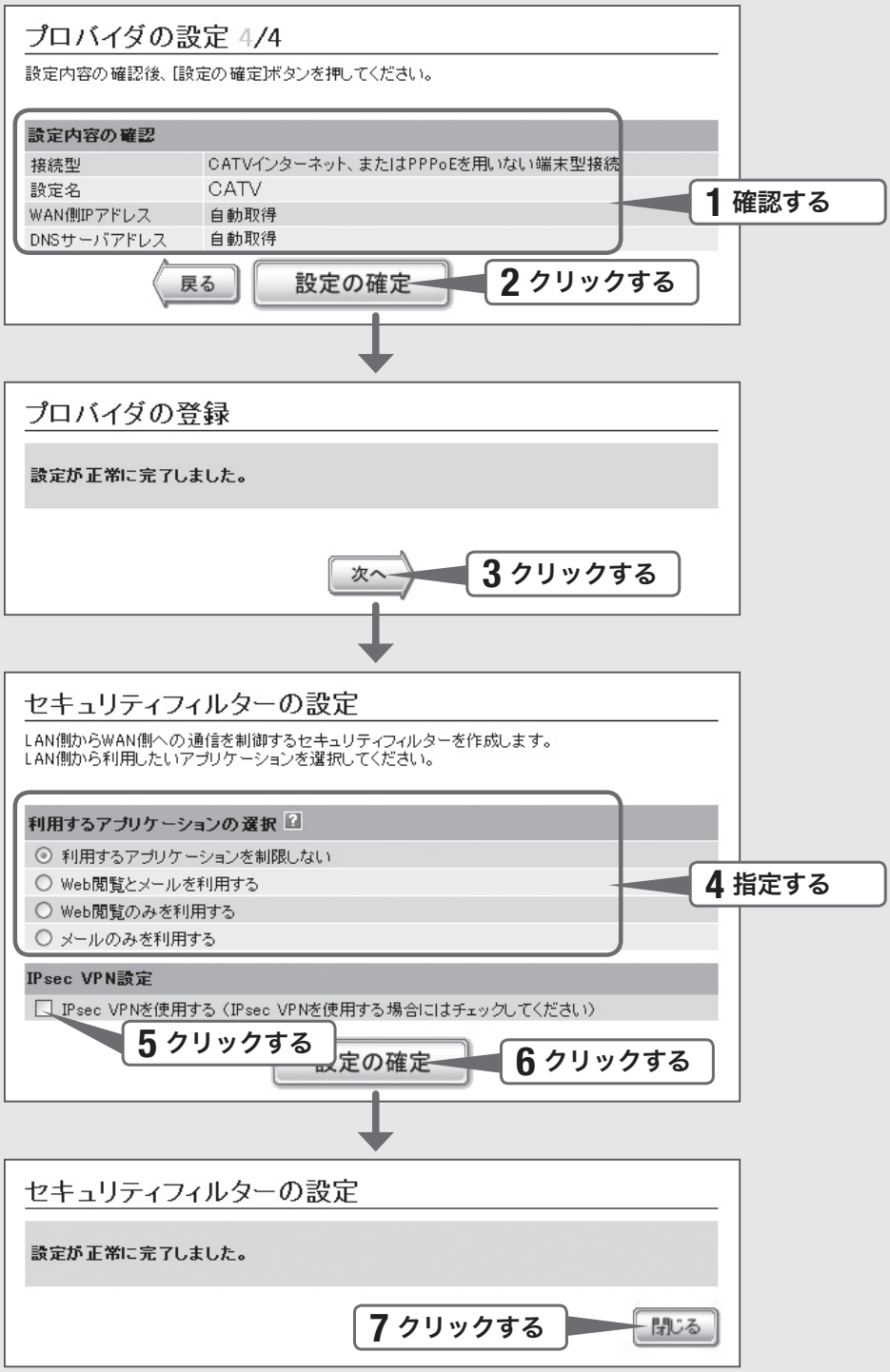
「手動でDNSサーバーアドレスを指定する」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス：**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 CATVインターネット 8.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どうか確認する。**

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て、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。**

確認画面が表示されます。

**3** **「次へ」をクリックする。**

「セキュリティフィルターの設定」画面が表示されます。

**4** **本製品を設置する拠点でのネットワークの利用方法を選ぶ。**

**5** **登録した接続設定でIPsec接続を利用する場合は、「IPsec VPNを使用する」をクリックしてチェックを付ける。**

チェックを付けると、IPsec接続を利用するために必要なNATやフィルターが設定されます。IPsec接続について詳しくは、50ページをご覧ください。

**6** **「設定の確定」をクリックする。**

**7** **「閉じる」をクリックする。**

本製品は自動的にインターネットに接続します。

**8** **「ヤマハルーター公式サイトへ」をクリックする。**

ヤマハルーター公式サイトのWebページ（http://netvolante.jp/）が表示されれば、インターネットへ接続できています。


# 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**

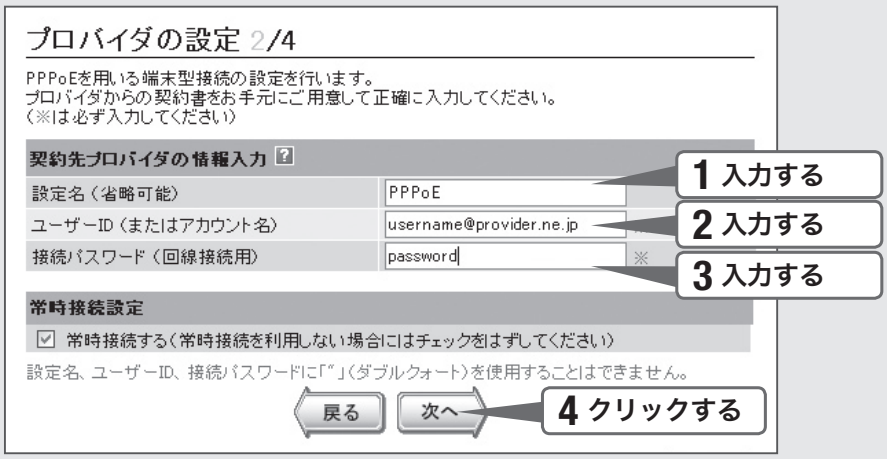
**▶インターネットに接続できない場合は**

**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** 40～41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」を参考にして、問題を解決してください。

# B PPPoE端末型（39ページから） 6. プロバイダの情報を指定する




## 1 「設定名」欄に、インターネット接続の設定名を入力する。

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」欄にユーザー 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 」欄に接続パスワードを入力する。

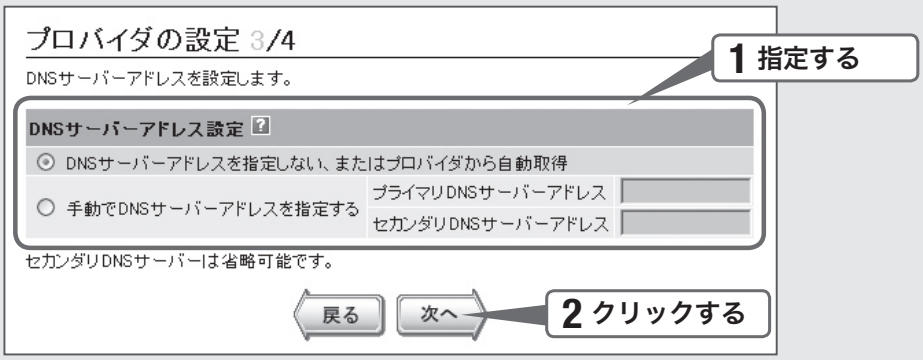
プロバイダから指定されたパスワード（または自分で変更したパスワード）を入力します。半角英数字で、大文字小文字も正確に入力してください。

## 4 必要な場合のみインターネットへ手動で接続したい場合は、「常時接続する」をクリックしてチェックを外す。

## 5 「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 PPPoE端末型 7.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は**

「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は**

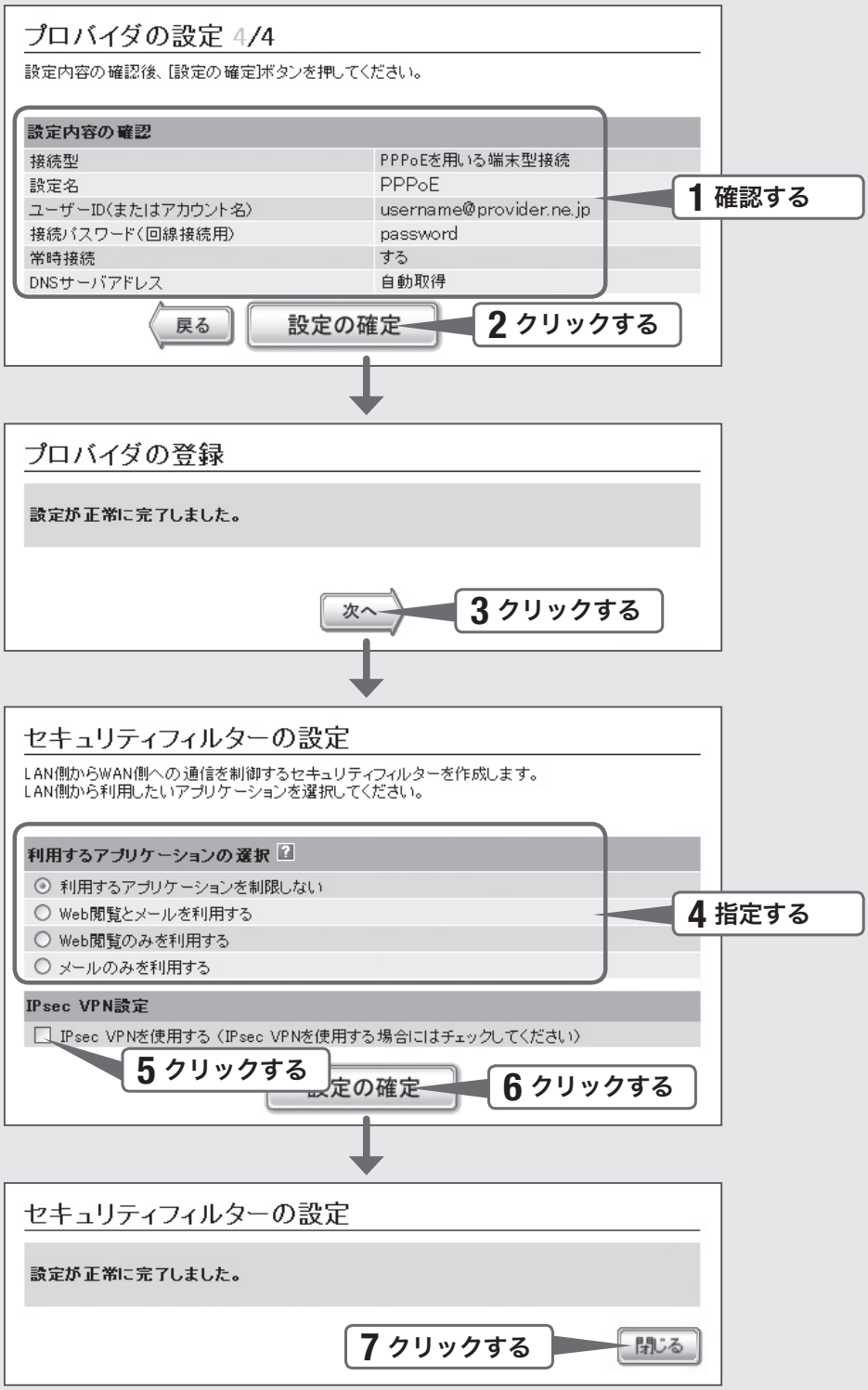
「手動でDNSサーバーアドレスを指定する」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバーアドレス：**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 PPPoE端末型 8.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どうか確認する。**

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て、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。**

確認画面が表示されます。

**3** **「次へ」をクリックする。**

「セキュリティフィルターの設定」画面が表示されます。

**4** **本製品を設置する拠点でのネットワークの利用方法を選ぶ。**

**5** **登録した接続設定でIPsec接続を利用する場合は、「IPsec VPNを使用する」をクリックしてチェックを付ける。**

チェックを付けると、IPsec接続を利用するために必要なNATやフィルターが設定されます。IPsec接続について詳しくは、50ページをご覧ください。

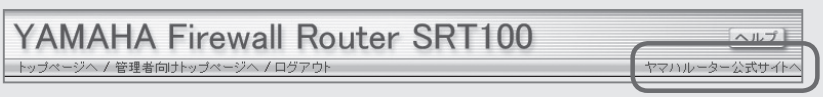
**6** **「設定の確定」をクリックする。**

**7** **「閉じる」をクリックする。**

本製品は自動的にインターネットに接続します。

**8** **「ヤマハルーター公式サイトへ」をクリックする。**

ヤマハルーター公式サイトのWebページ(http://netvolante.jp/)が表示されれば、インターネットへ接続できています。




# 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** 44～45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」を参考にして、問題を解決してください。

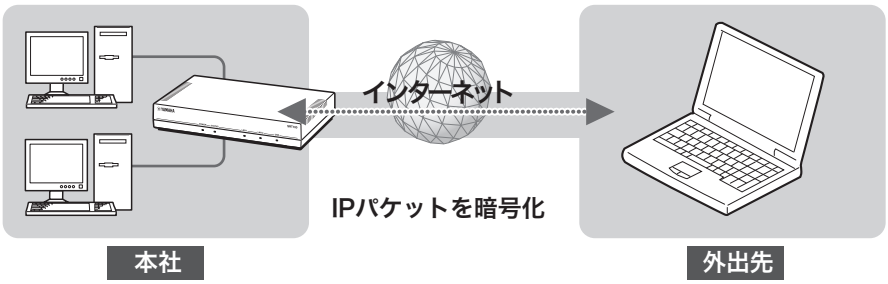
# 本製品で利用できる拠点間接続の概要

## IPsecを利用した拠点間接続(52ページ)

IPsecを利用するとIPパケットを暗号化した状態でやり取りできるため、セキュリティを保った状態でインターネット経由でLAN同士を接続できます(仮想プライベートネットワーク、VPN)。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。

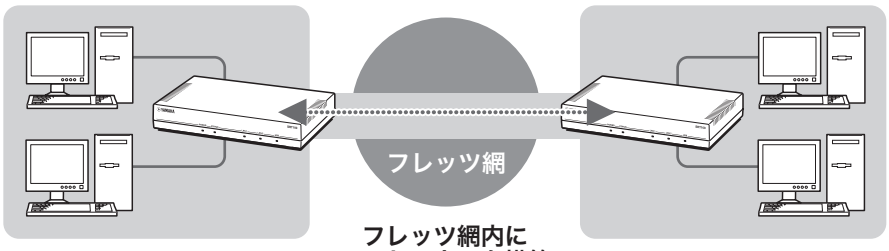

## VPNクライアントからのIPsec経由での接続(59ページ)

外部のVPNクライアントから拠点にIPsecを使用して接続することで、データを暗号化した状態で外出先からインターネット経由で拠点内の情報にアクセスすることもできます。



# フレッツ網を利用したIPIPトンネル接続(70ページ)

IPIPトンネルを利用することで、端末型契約のIPアドレスを使用して拠点間のネットワークを接続できます。ただしIPIPトンネルは暗号化通信をサポートしていないため、高度な機密データをインターネット経由で通信する用途には向いていません。フレッツ網など、機密性の高いネットワーク内で使用するようおすすめいたします。




**フレッツ網内に
IPIPトンネルを構築**

### IPIPトンネル接続以外に、インターネット接続も行う場合は

本製品を別の拠点とのIPIPトンネル通信だけでなくインターネットへの接続ゲートウェイとしても使用する場合は、IPIPトンネルの設定終了後に以下の流れでインターネット接続の設定を行ってください。

- 設定画面左側の「ウィザード」–「プロバイダ情報の設定」をクリックして、初期設定ウィザードを表示します。
- 「プロバイダの追加登録」の「追加」をクリックして、インターネット接続の設定を行います。詳しくは、「インターネットへ接続する(PPPoE/CATV)」の38ページ以降の説明をご覧ください。

# 閉域網での接続(97ページ)

広域LANなどで使用する場合に、拠点のルーターとして本製品を使用できます。セキュリティ機能(98ページ)を活用することで、端末単位のアクセス制限やURLフィルタリングなどを拠点側でも実行でき、便利です。

### 使用例・設定例について詳しくは、ネットボランチホームページをご覧ください

ネットボランチホームページ(http://netvolante.jp/)には、システム例や設定ファイルの構成例など、さまざまな情報が記載されています。

# IPsecの接続設定を行う前に

## 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1～10、トンネルインターフェース番号も同様に1～10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。

### 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。

# IPsecの設定を行う前に

### 本製品をインターネットへ接続できるようにする必要があります

IPsec接続の設定を行う前に基本的なインターネット接続設定を行い、本製品がインターネットに接続できる状態にする必要があります。「インターネットへ接続する(PPPoE/CATV)」(22ページ)の説明に従って、本製品の接続および設定を行ってください。

**ご注意**

IPsec接続を利用する場合は、インターネット接続設定の際に、「セキュリティフィルターの設定」画面で「IPsec VPNを使用する」にチェックを付ける必要があります。チェックを付けていない場合には、設定を変更してください(次ページ)。

### 接続方法によって設定が異なります

接続方法に合わせて、必要な設定を行ってください。

**IPsecを使用して拠点間接続する場合**

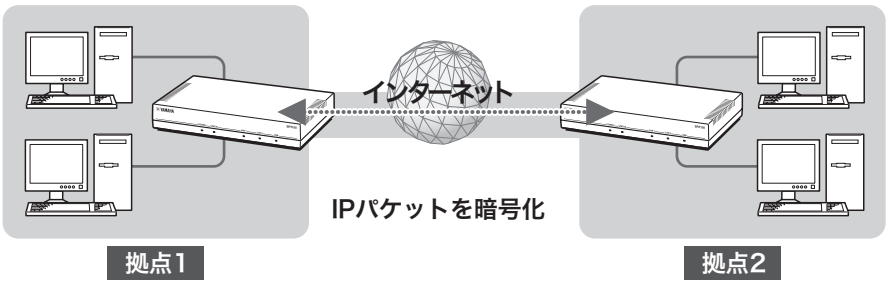
「IPsecで拠点間接続する」(次ページ)をご覧ください。

**VPNクライアントから拠点にIPsecを使用して接続する場合**

「VPNクライアントとIPsecで接続する」(59ページ)をご覧ください。

# IPsecで拠点間接続する

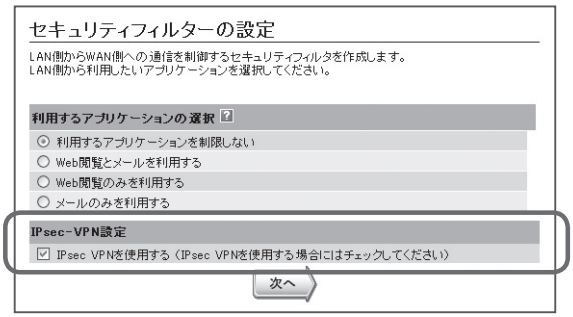
IPsecを利用するとIPパケットを暗号化した状態でやり取りできるため、セキュリティを保った状態でインターネット経由でLAN同士を接続できます(仮想プライベートネットワーク、VPN)。ADSLなどの通常のブロードバンド回線をそのまま利用してVPNを構築できるため、専用線を導入する場合と比較して、低コストでVPNを実現できます。






## 「IPsec VPNを使用する」にチェックを付けてください

IPsec接続を利用する場合は、インターネット接続設定の「セキュリティフィルターの設定」画面で、「IPsec VPNを使用する」にチェックを付ける必要があります。

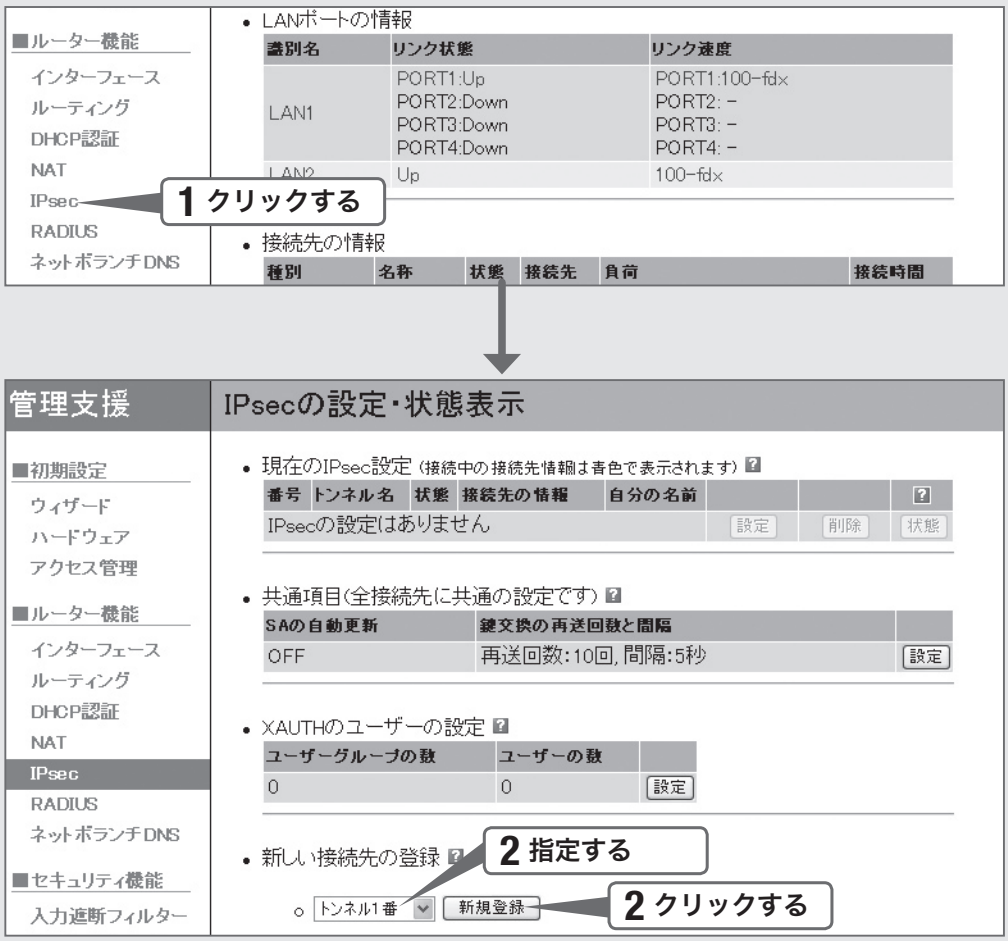



チェックを付けていない場合には、以下の手順で設定を変更してください。

1. **画面左側の「ウィザード」をクリックする。**
2. **「プロバイダ情報の設定」をクリックする。**
3. **「プロバイダの修正／削除」欄で、登録されているインターネット接続設定の「設定」をクリックする。**
4. **以後、40ページ(CATV接続の場合)または44ページ(PPPoE接続の場合)の手順に従って操作する。**
5. **「セキュリティフィルターの設定」画面で「IPsec VPNを使用する」にチェックが付いていない場合は、クリックしてチェックを付けてから「次へ」をクリックする。**
   チェックが付いている場合は、そのまま「次へ」をクリックします。
6. **「閉じる」をクリックする。**

# 1.トンネル接続番号を指定する

IPsec接続を管理するための管理番号(トンネル接続番号)を指定します。




## 1

### 「IPsec」をクリックする。

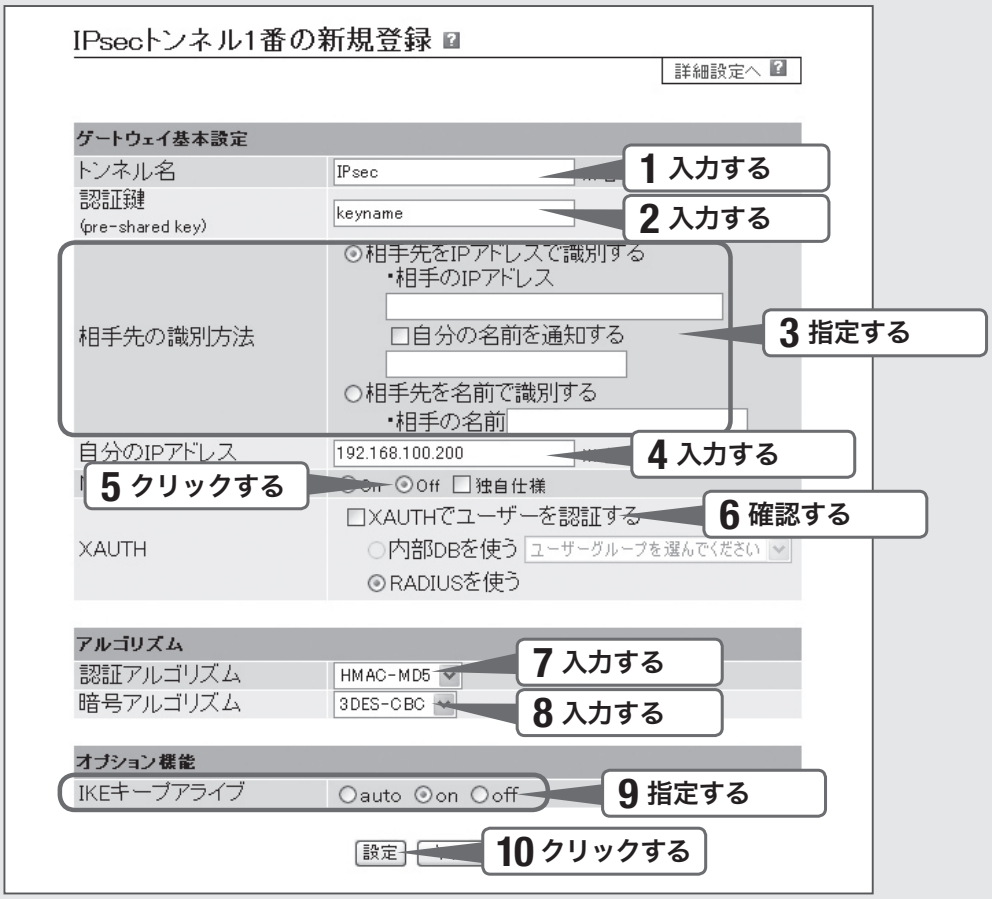
「IPsecの設定・状態表示」画面が表示されます。

## 2

### 「新しい接続先の登録」欄で任意のトンネル接続番号を指定してから、「新規登録」をクリックする。

「IPsecトンネル(指定したトンネル接続番号)の新規登録」画面が表示されます。

# 2. IPsec接続に必要な情報を指定する




## 1 「トンネル名」欄で、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 「認証鍵」欄で、認証鍵を入力する。

データの暗号化に使用する事前共有鍵(半角英数字で最大32文字)を入力します。
センター側と拠点側で同じ値に設定してください。

## 3 「相手先の識別方法」欄で、接続先の識別方法を指定する。

### IPアドレスで識別する場合

- 「相手先をIPアドレスで識別する」をクリックして選んでから、接続先のIPアドレスを入力します。
- 本製品に固定IPアドレスが割り当てられていない場合は、「自分の名前を通知する」にチェックを付けてから自分の名前を入力します。

### 名前で識別する場合

「相手先を名前で識別する」をクリックして選んでから、接続先の名前(半角英数字で最大32文字)を入力します。

**4** **必要に応じて、「自分のIPアドレス」欄に本製品のLAN側IPアドレスを入力する。**

**5** **「NATトラバーサル」欄で、「off」をクリックして選ぶ。**

ご注意

接続先の機器までの間に別のNAT機器が存在する場合は、「on」に設定してください。

**6** **「XAUTH」欄で、「XAUTHでユーザーを認証する」にチェックが付いていないことを確認する。**

**7** **「認証アルゴリズム」欄で、認証アルゴリズムを指定する。**

- IKEのフェーズ2で使用する、認証に使用するアルゴリズムを設定します。
- 接続先の機器と同じ設定にしてください。

**8** **「暗号アルゴリズム」欄で、暗号アルゴリズムを指定する。**

- IKEのフェーズ2で使用する、暗号化に使用するアルゴリズムを設定します。
- 接続先の機器と同じ設定にしてください。

**9** **IPsec接続を常に維持したい場合は、「IKEキープアライブ」欄で「on」をクリックして選ぶ。**

**10** **「設定」をクリックする。**

確認画面が表示されます。

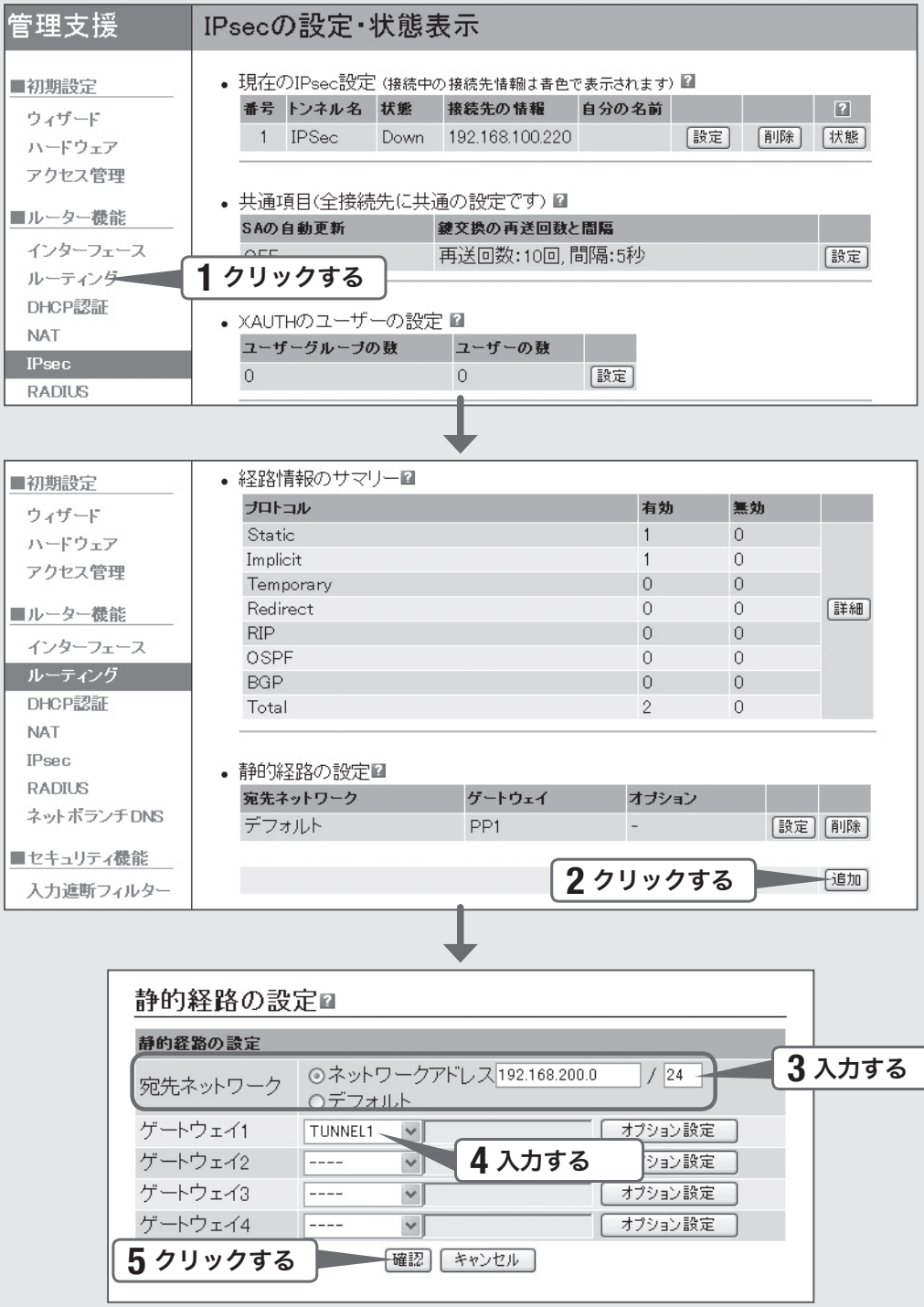
**11** **「登録」をクリックする。**

**12** **「メイン画面に戻る」をクリックする。**

「IPsecの設定・状態表示」画面に戻ります。

# 3. 経路情報を設定する

接続先のLANのネットワークアドレスを指定します。



1 **「ルーティング」をクリックする。**

「ルーティングの設定・状態表示」画面が表示されます。

2 **「静的経路の設定」欄で、「追加」をクリックする。**

「静的経路の設定」画面が表示されます。

3 **「宛先ネットワーク」欄で、接続先のLANのネットワークアドレスを入力する。**

**ご注意**

双方でネットワークアドレスが重複している場合は、どちらかのネットワークアドレスを変更してください。

4 **「ゲートウェイ1」欄で、指定したトンネル接続番号を指定する。**

5 **「確認」をクリックする。**

確認画面が表示されます。

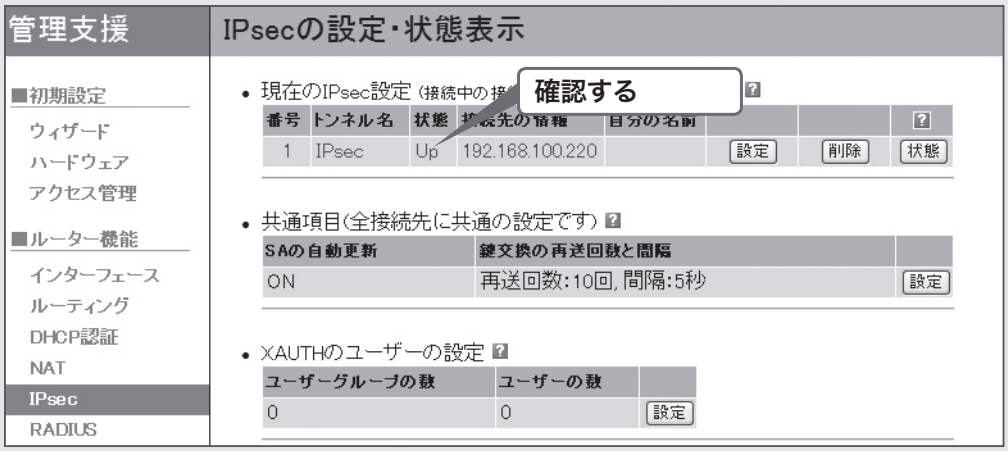
6 **「登録」をクリックする。**

7 **「メイン画面に戻る」をクリックする。**

「ルーティングの設定・状態表示」画面に戻ります。

# 4. IPsec接続する

センター側および拠点側の認証が成功すると、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、「IPsecの設定・状態表示」画面に「Up」と表示されます。




**ご注意**

- 「IKEキープアライブ」欄(55ページ)で「on」を指定した場合は、キープアライブパケットを契機としてトンネル接続されるため、設定完了の時点で状態表示が「Up」になります。「auto」または「off」を指定した場合は、相手先への何らかの通信が発生してトンネル接続が完了した時点で「Up」になります。
- IPsec接続をするには、センター側と拠点側で同じ認証鍵(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。

## 設定終了

**これでIPsec通信の設定は終了です**

**▶IPsec接続できない場合は**

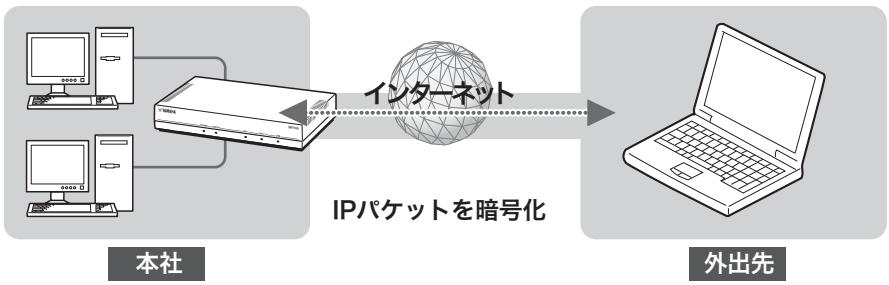
**Check 1** 本製品とパソコン、ADSLモデムやケーブルモデム、ONUの接続を確認してください。

**Check 2** 54～57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」を参考にして、問題を解決してください。

# VPNクライアントとIPsecで接続する

外部のVPNクライアントから拠点にIPsecを使用して接続することで、データを暗号化した状態で外出先からインターネット経由で拠点内の情報にアクセスすることもできます。外出先からパソコンでアクセスするために使用するVPNクライアント製品としては、VPNクライアントソフトウェアYMS-VPN1（別売り）をおすすめいたします。




本製品に接続するVPNクライアントユーザーを登録してから、IPsec接続の設定を行います。次ページ以降の操作説明に従って、設定してください。

**ヒント**

- YMS-VPN1について詳しくは、ネットボランチホームページ（http://NetVolante.jp/）をご覧ください。
- XAUTHでRADIUS認証を使用する場合は、あらかじめ「RADIUSの設定」画面（69ページ）で必要な設定を行っておく必要があります。

## VPNクライアント側での設定も必要です

本書では、VPNサーバー側（本製品側）の設定について説明しています。VPNクライアント側の設定については、お使いのVPNクライアント製品の取扱説明書をご覧ください。

## VPNクライアントの管理単位（ユーザーとユーザーグループ）

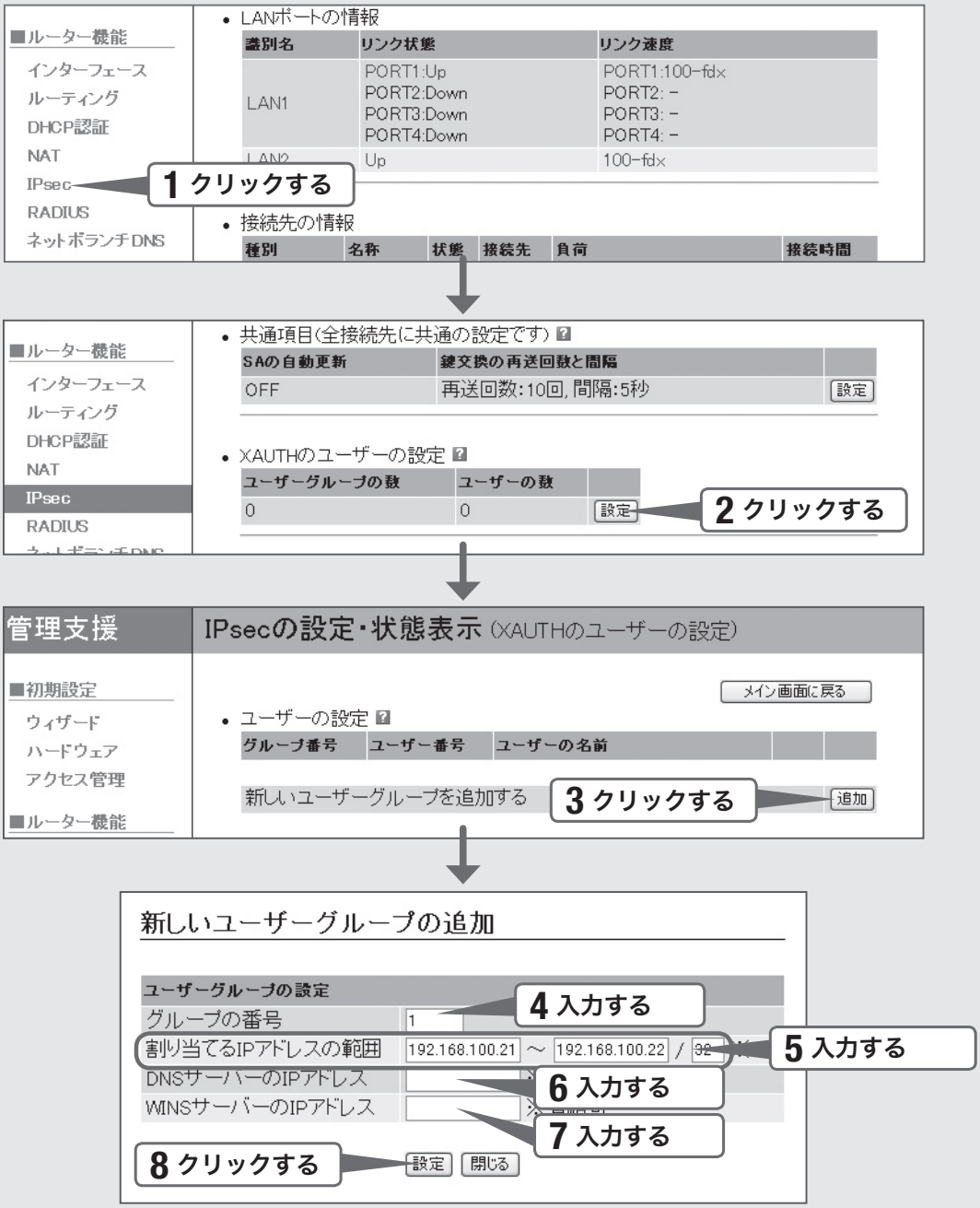
- 本製品では、個々のVPNクライアントユーザーは任意のユーザーグループに所属している必要があります。したがって、初めてユーザーを登録する場合は、あらかじめユーザーグループを作成しておく必要があります。
- ユーザーグループおよびユーザーごとに、アクセスしてきたユーザーに割り当てるIPアドレスの範囲や、DNSサーバーおよびWINSサーバーを指定できます。
- 個々のユーザーに指定されているIPアドレスの範囲や、DNSサーバーおよびWINSサーバーと、ユーザーグループに指定されているそれらの設定が異なる場合は、個々のユーザーに指定されている設定が優先されます。個々のユーザーに何も指定されていない場合は、ユーザーグループに指定されている設定が個々のユーザーに適用されます。

# 1.ユーザーグループを登録する

VPNクライアントユーザーが所属するユーザーグループを登録します。

**ヒント**

すでにユーザーグループが存在する場合は、「2.ユーザーを登録する」(62ページ)に進んでください。



1 **「IPsec」をクリックする。**

「IPsecの設定・状態表示」画面が表示されます。

2 **「XAUTHのユーザーの設定」欄の「設定」をクリックする。**

「IPsecの設定・状態表示(XAUTHのユーザーの設定)」画面が表示されます。

3 **「新しいユーザーグループを追加する」欄の「追加」をクリックする。**

「新しいユーザーグループの追加」画面が表示されます。

4 **「グループの番号」欄で、ユーザーグループの番号を入力する。**

1～500の範囲で、任意の番号を指定できます。

5 **必要に応じて、「割り当てるIPアドレスの範囲」欄に現在設定中のユーザーグループに所属するユーザーに割り当てるIPアドレスの範囲を入力する。**

6 **必要に応じて、「DNSサーバーのIPアドレス」欄に現在設定中のユーザーグループに所属するユーザーに割り当てるDNSサーバーのIPアドレスを入力する。**

7 **必要に応じて、「WINSサーバーのIPアドレス」欄に現在設定中のユーザーグループに所属するユーザーに割り当てるWINSサーバーのIPアドレスを入力する。**

8 **「設定」をクリックする。**

確認画面が表示されます。

9 **「登録」をクリックする。**

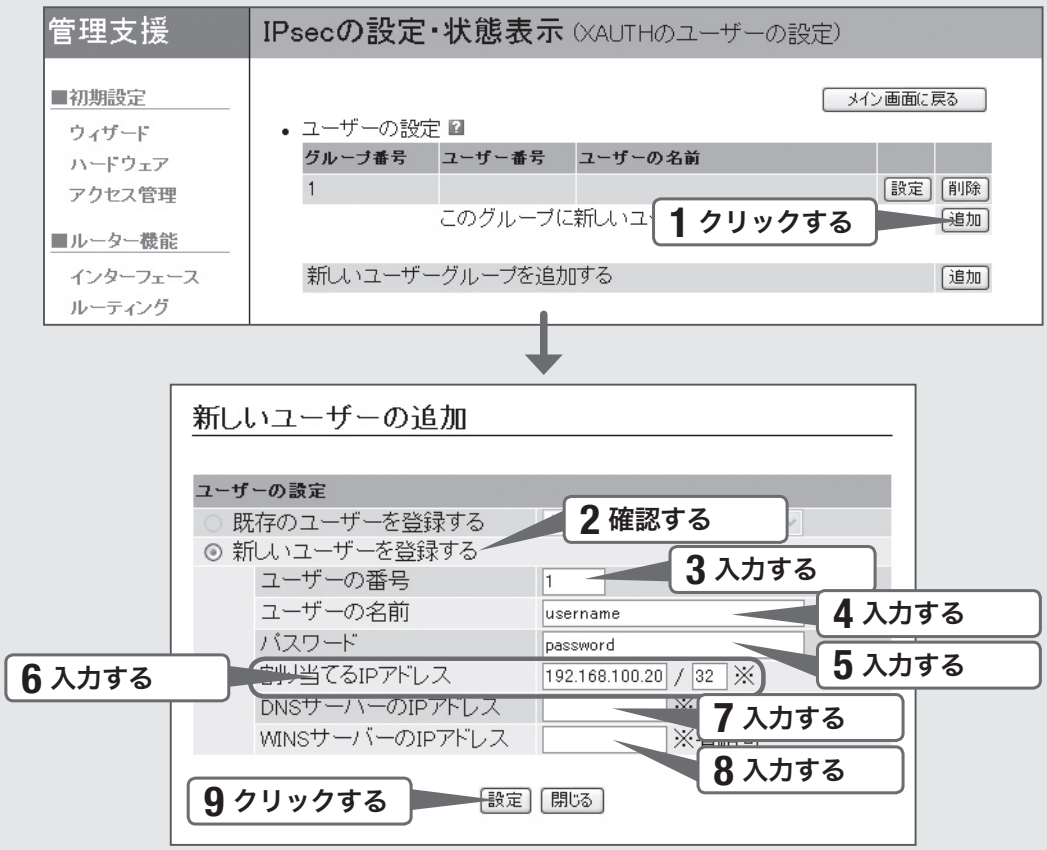
確認画面が表示されます。

10 **「戻る」をクリックする。**

「IPsecの設定・状態表示(XAUTHのユーザーの設定)」画面に戻ります。

# 2.ユーザーを登録する

本製品に接続するVPNクライアントの認証に使用する、ユーザー名およびパスワードを登録します。




**1** **「IPsecの設定・状態表示(XAUTHのユーザーの設定)」画面で、「このグループに新しいユーザーを追加する」欄の「追加」をクリックする。**

「新しいユーザーの追加」画面が表示されます。

**2** **「新しいユーザーを登録する」が選ばれていることを確認する。**

**3** **「ユーザーの番号」欄で、ユーザーの番号を入力する。**

1～500の範囲で、任意の番号を指定できます。

4 **「ユーザーの名前」欄で、ユーザー名を入力する。**

最大32文字(半角英数字)まで入力できます。

5 **「パスワード」欄で、手順4で指定したユーザーのログインパスワードを入力する。**

最大32文字(英数字のみ)まで入力できます。

6 **必要に応じて、「割り当てるIPアドレス」欄に現在設定中のユーザーに割り当てるIPアドレスを入力する。**

ユーザーに対してIPアドレスを指定しないと、ユーザーグループで設定したアドレス(61ページ)の範囲から割り当てられます。

7 **必要に応じて、「DNSサーバーのIPアドレス」欄に現在設定中のユーザーに割り当てるDNSサーバーのIPアドレスを入力する。**

8 **必要に応じて、「WINSサーバーのIPアドレス」欄に現在設定中のユーザーに割り当てるWINSサーバーのIPアドレスを入力する。**

9 **「設定」をクリックする。**

確認画面が表示されます。

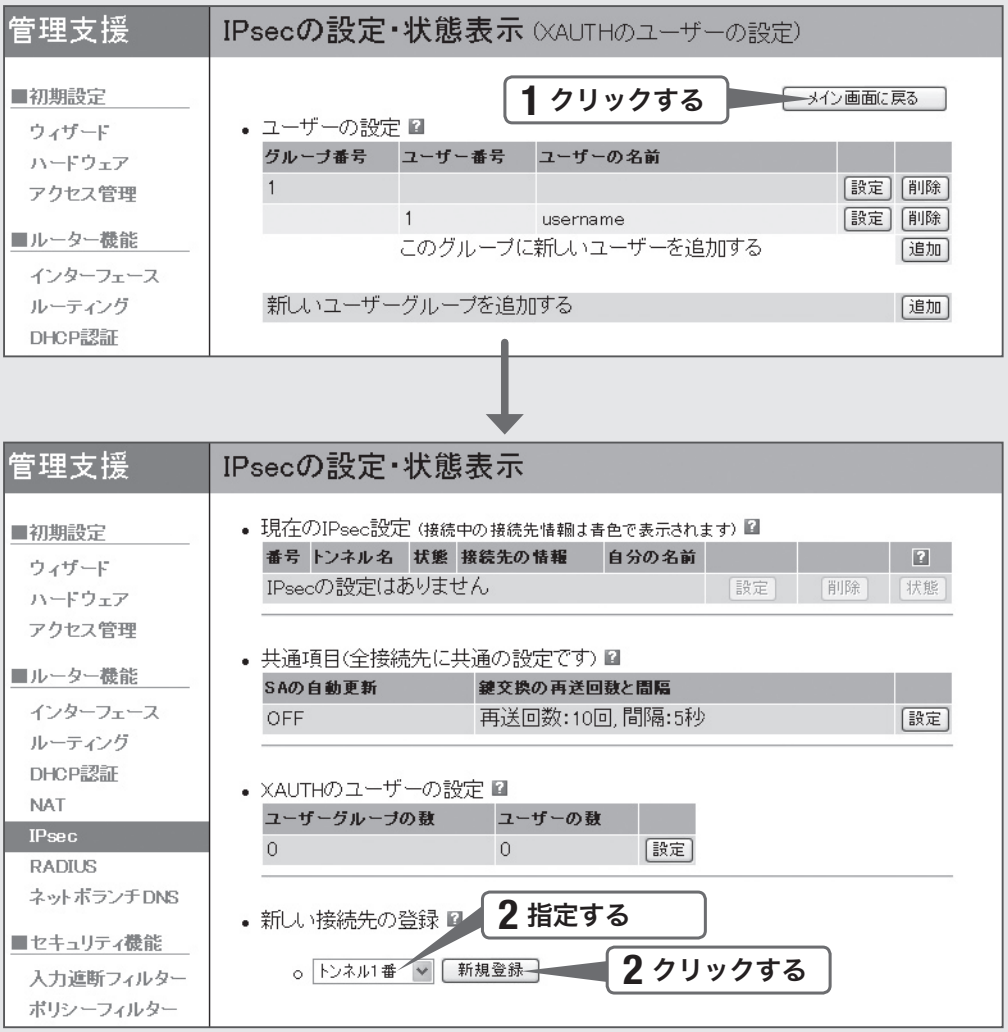
10 **「登録」をクリックする。**

確認画面が表示されます。

11 **「完了」をクリックする。**

「IPsecの設定・状態表示(XAUTHのユーザーの設定)」画面に戻ります。

# 3. トンネル接続番号を指定する



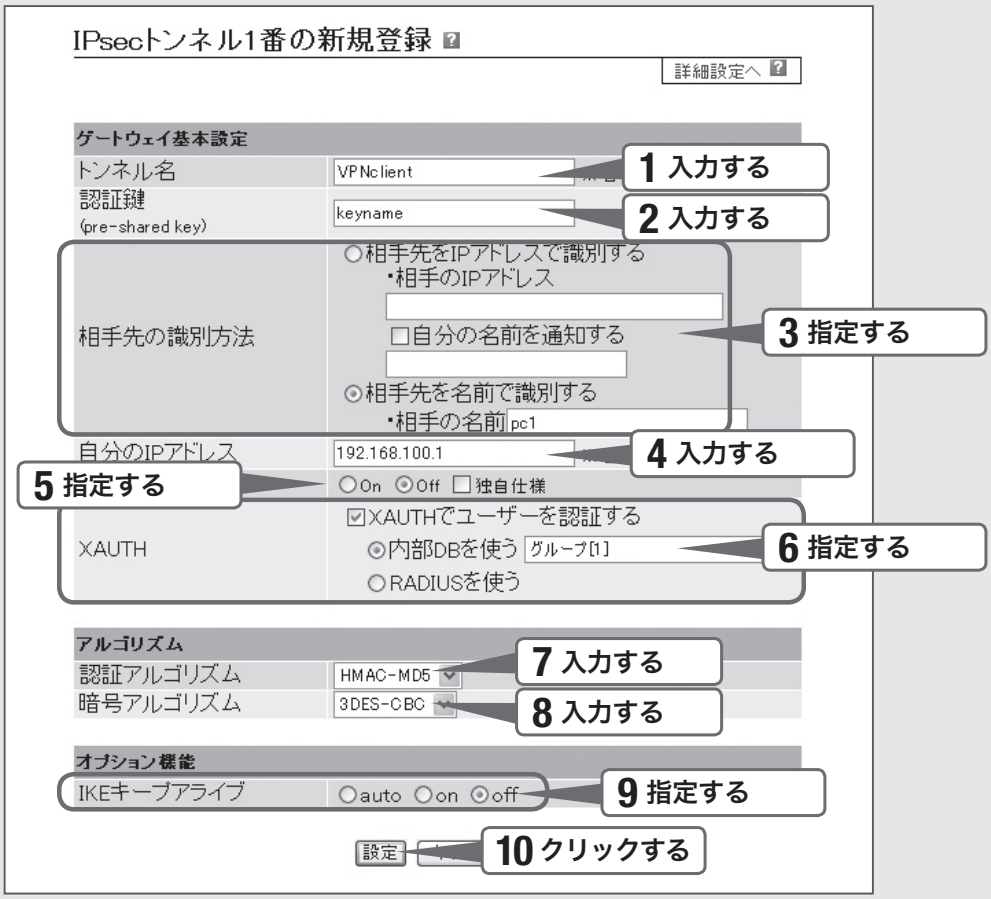

**1** 「IPsecの設定・状態表示（XAUTHのユーザーの設定）」画面で、「メイン画面に戻る」をクリックする。

「IPsecの設定・状態表示」画面が表示されます。

**2** 「新しい接続先の登録」欄で任意のトンネル接続番号を指定してから、「新規登録」をクリックする。

「IPsecトンネル（指定したトンネル接続番号）の新規登録」画面が表示されます。

# 4. IPsec接続に必要な情報を指定する




## 1 「トンネル名」欄で、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 「認証鍵」欄で、認証鍵を入力する。

データの暗号化に使用する事前共有鍵(半角英数字で最大32文字)を入力します。
VPNクライアントソフトウェアでも同じ値に設定してください。

**3** 「相手先の識別方法」欄で、接続先の識別方法を指定する。

### 名前で識別する場合

「相手先を名前で識別する」をクリックして選んでから、接続先の名前(半角英数字で最大32文字)を入力します。

### IPアドレスで識別する場合

「相手先をIPアドレスで識別する」をクリックして選んでから、接続先のIPアドレスを入力します。

**4** 必要に応じて、「自分のIPアドレス」欄に本製品のLAN側IPアドレスを入力する。

**5** 「NATトラバーサル」欄で、VPNクライアント側の設定に合わせて「on」または「off」をクリックして選ぶ。

**ご注意**

VPNクライアントとの間に別のNAT機器が存在する場合は、「on」に設定してください。

**6** 「XAUTH」欄で、「XAUTHでユーザーを認証する」をクリックしてチェックが付けてから「内部DBを使う」をクリックして選び、VPNクライアントが所属するユーザーグループ(60ページ)を指定する。

**ヒント**

XAUTHでRADIUS認証を使用する場合は、「RADIUS」を選びます。ただし、RADIUS認証を使用する場合はあらかじめ「RADIUSの設定」画面(69ページ)で必要な設定を行っておく必要があります。

**7** 「認証アルゴリズム」欄で、認証アルゴリズムを指定する。

- IKEのフェーズ2で使用する、認証に使用するアルゴリズムを設定します。
- 接続先の機器と同じ設定にしてください。

**8** 「暗号アルゴリズム」欄で、暗号アルゴリズムを指定する。

- IKEのフェーズ2で使用する、暗号化に使用するアルゴリズムを設定します。
- 接続先の機器と同じ設定にしてください。

9 **「IKEキープアライブ」欄で「off」をクリックして選ぶ。**

VPNクライアントは、IKEキープアライブに対応していません。

10 **「設定」をクリックする。**

確認画面が表示されます。

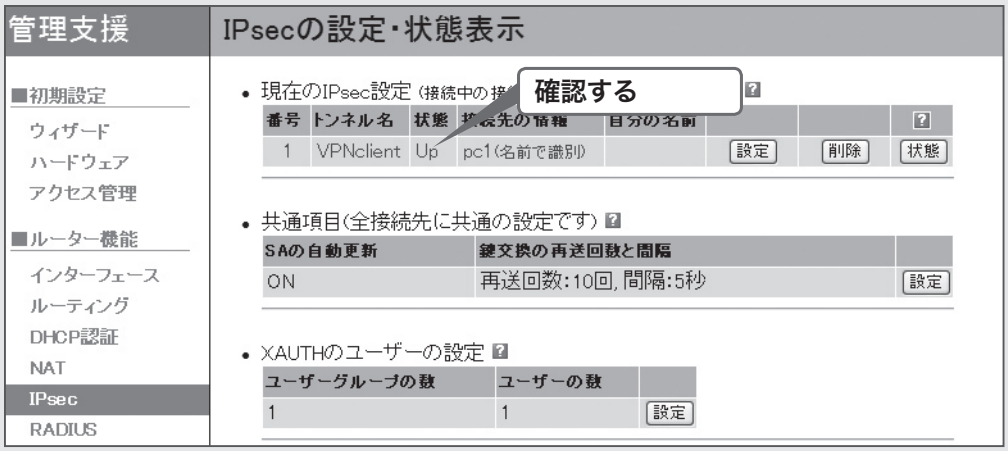
11 **「登録」をクリックする。**

12 **「メイン画面に戻る」をクリックする。**

「IPsecの設定・状態表示」画面に戻ります。

# 5. IPsec接続する

VPNクライアント側で接続操作を行ってから拠点側の認証が成功すると、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、「IPsecの設定・状態表示」画面に「Up」と表示されます。




**ご注意**

- IPsec接続をするには、VPNクライアント側でも同じ認証鍵(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。

## 設定終了

**これでIPsec通信の設定は終了です**

**▶IPsec接続できない場合は**

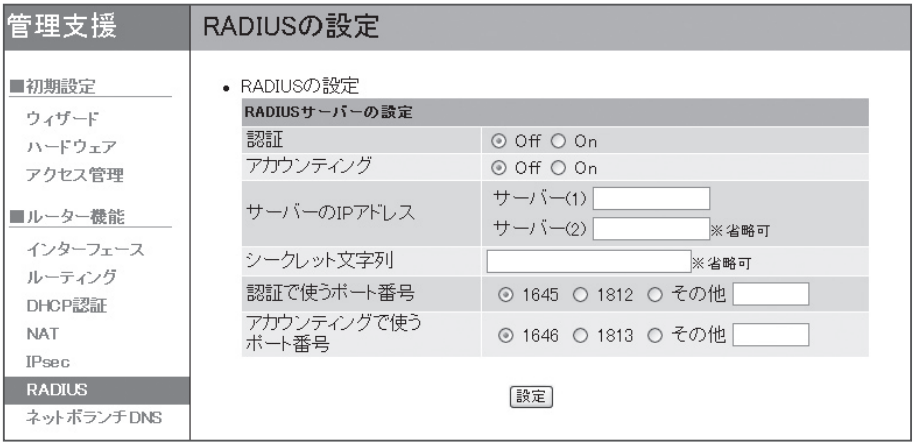
**Check 1** 本製品とパソコン、ADSLモデムやケーブルモデム、ONUの接続を確認してください。

**Check 2** 65～67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」を参考にして、問題を解決してください。

# RADIUS認証を使用する場合は

VPNクライアントからの接続要求に対してRADIUS認証を使用する場合は、あらかじめ「RADIUSの設定」画面で必要な設定を行ってください。




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

**「RADIUSの設定」画面を開くには**

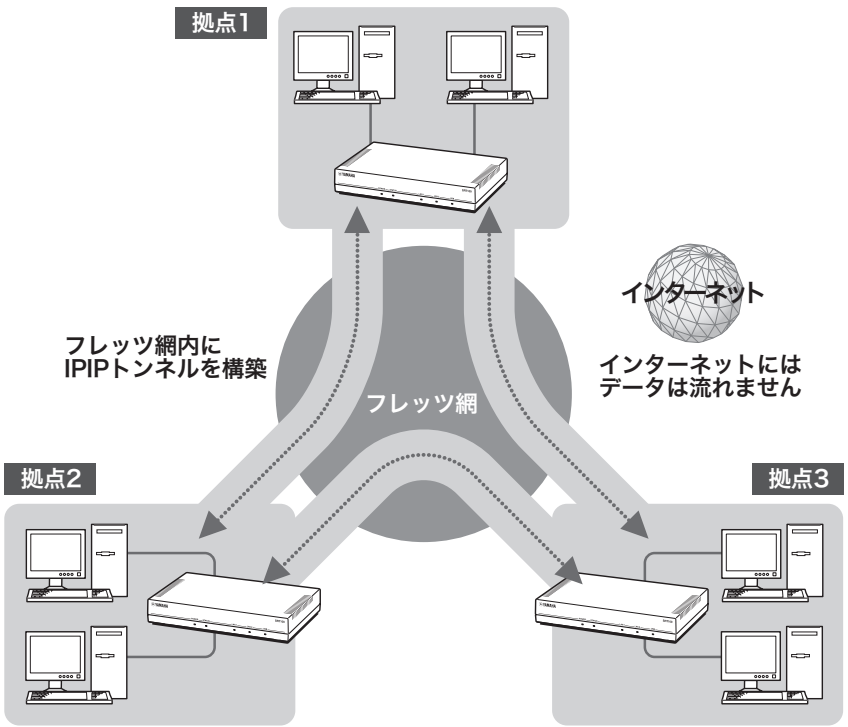
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「RADIUS」

# フレッツ網を使用して IPIPトンネル接続する



IPIPトンネルを利用することで、端末型契約のIPアドレスを使用して拠点間のネットワークを接続できます。ただしIPIPトンネルは暗号化通信をサポートしていないため、高度な機密データをインターネット経由で通信する用途には向いていません。フレッツ網など、機密性の高いネットワーク内で使用するようおすすめいたします。
ここでは、NTT東日本の「フレッツ・グループアクセス ライト」やNTT西日本の「フレッツ・グループ ベーシックメニュー」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。




**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設定を行ってください。セキュリティ設定が不十分の場合は、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WindowsNTサーバーやWindows2000サーバーを用意する必要があります。

# IPIPトンネルの接続設定を行う前に

## 設定を始める前にご確認ください

- 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「6.LAN側IPアドレスを設定する」(83ページ)をご参照ください。

## IPIPトンネル接続以外に、インターネット接続も行う場合は

IPIPトンネルの設定終了後に、以下の流れでインターネット接続の設定を行ってください。

- 設定画面左側の「ウィザード」–「プロバイダ情報の設定」をクリックして、初期設定ウィザードを表示します。
- 「プロバイダの追加登録」の「追加」をクリックして、インターネット接続の設定を行います。詳しくは、「インターネットへ接続する(PPPoE/CATV)」の38ページ以降の説明をご覧ください。

## 準備を始める前にご用意ください

### アースコード

アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

### LANケーブル

パソコンの台数や距離に合わせて、10BASE-Tまたは100BASE-TX対応のLANケーブルをご用意ください。

### HUB

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対応のHUB（またはスイッチングHUB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。

### フレッツ・グループアクセスまたはフレッツ・グループの設定資料

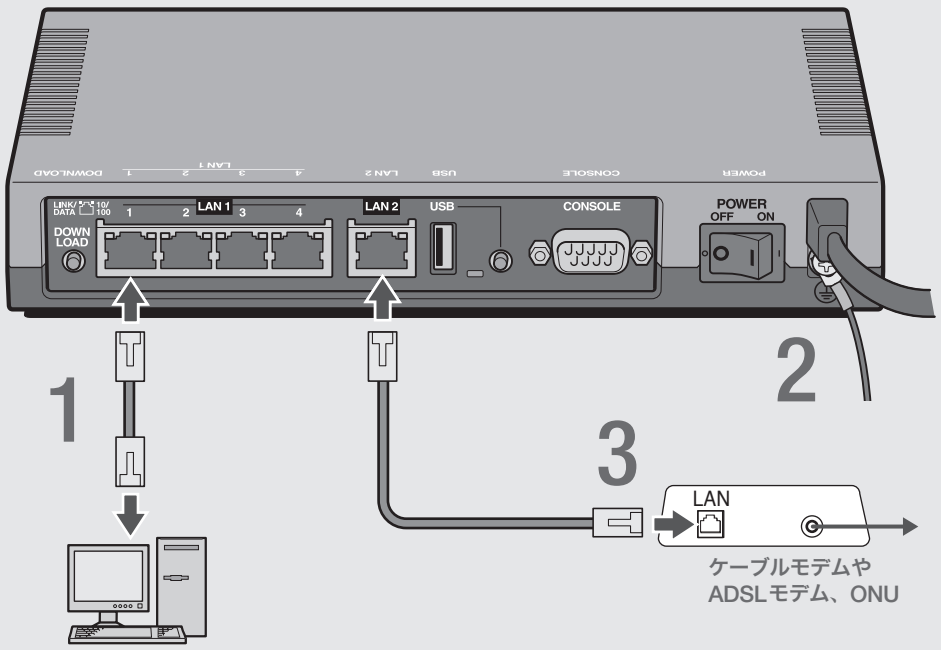
接続先を設定してフレッツ網に接続するには、NTTから通知される以下の情報が必要です。

- ユーザー ID
- パスワード
- IPアドレス
- ネットマスク

**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場合は、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。「6.LAN側IPアドレスを設定する」(83ページ)で、本製品のDHCP機能を動作させないように設定してください。

# 1.ケーブルと電源を接続する




## 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 アース端子のネジを+ドライバ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。

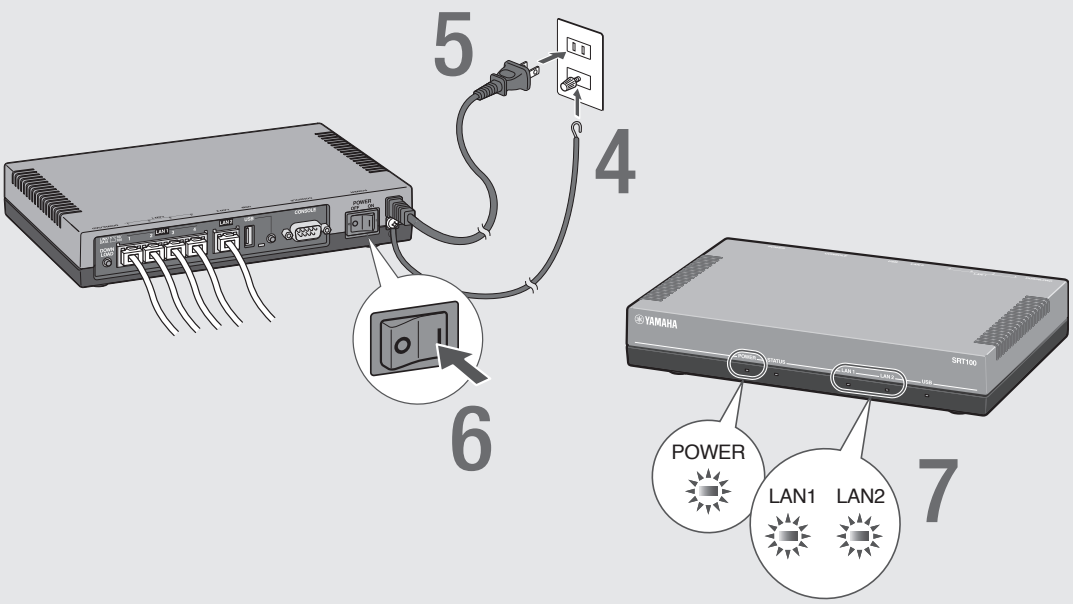
アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

## 3 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。




## 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。

**電源コードを取りはずす場合は**

先に電源コードを取りはずしてから、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。

ランプが何回か点滅した後、POWERランプが点灯します。

## 7 パソコンやHUB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どうか、パソコンやHUBの電源が入っているかどうか確認してください。
- 本製品に接続したすべてのパソコンおよびHUB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どうか、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どうか確認してください。

# 2. 本製品の設定画面を開く

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設定画面を開いて行います。

**ご注意**

設定画面を使用するには、Windows版Internet Explorer 6.0以降のWebブラウザが必要です。

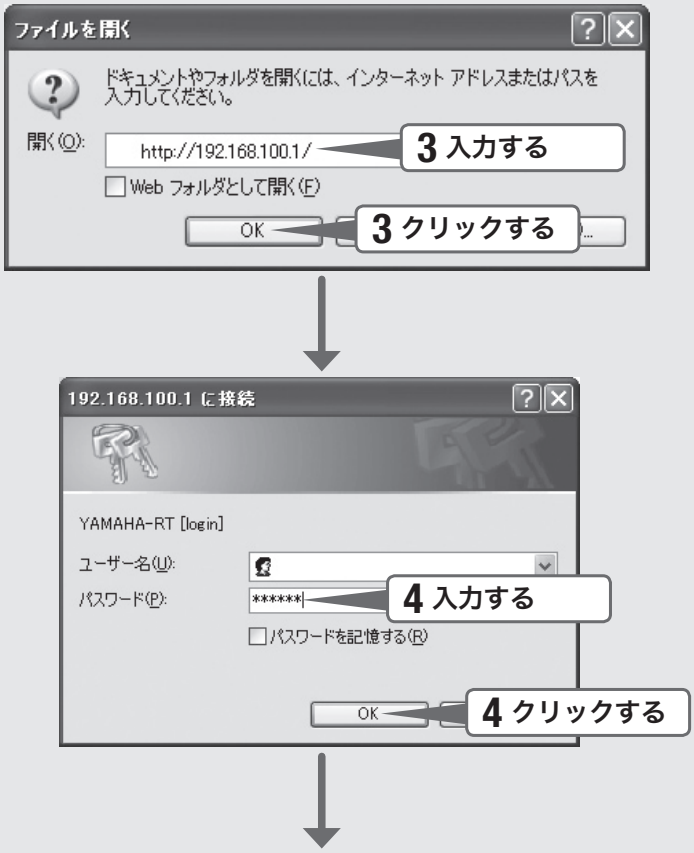
**ヒント**

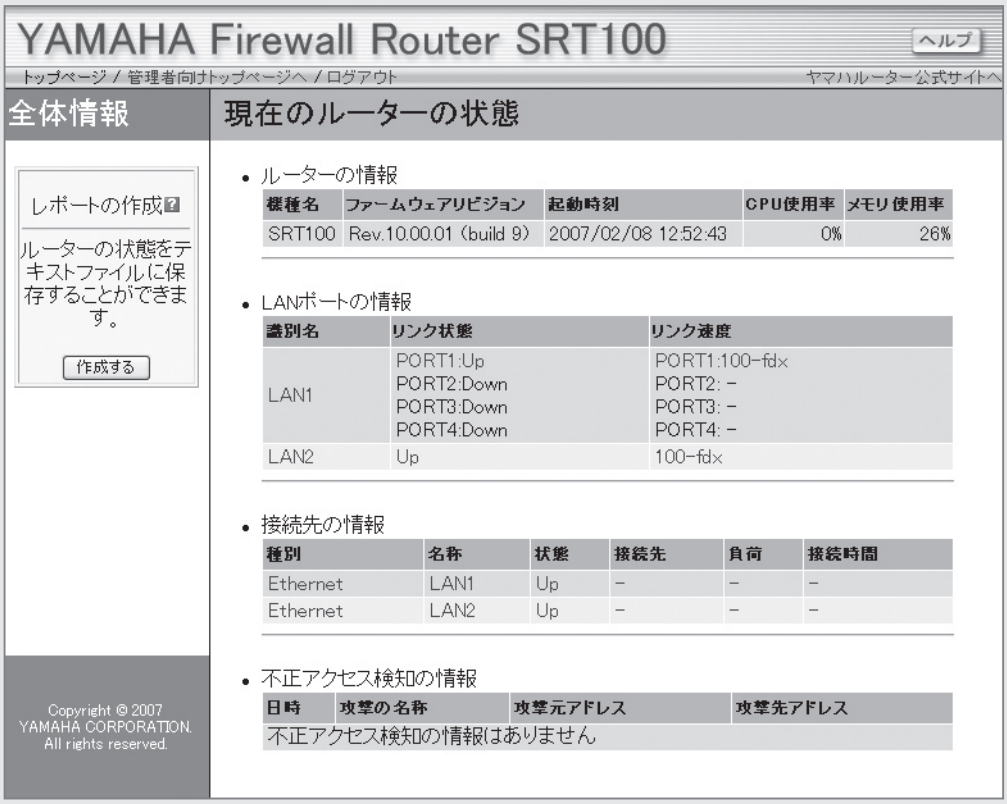
TELNETソフトウェアでコンソール画面からコマンドを入力して、設定画面よりも詳細な設定を行うことができます(コンソールコマンド)。TELNETソフトウェアで本製品に接続する方法については150ページ、本製品で使用できるコマンドについては「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。



## 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Webブラウザを起動して、「ファイル」メニューから「開く」を選ぶ。






## 3 「http://192.168. 100.1/」と半角英字で入力してから、「OK」をクリックする。

「192.168.100.1 に接続」画面が表示されます。

## 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。

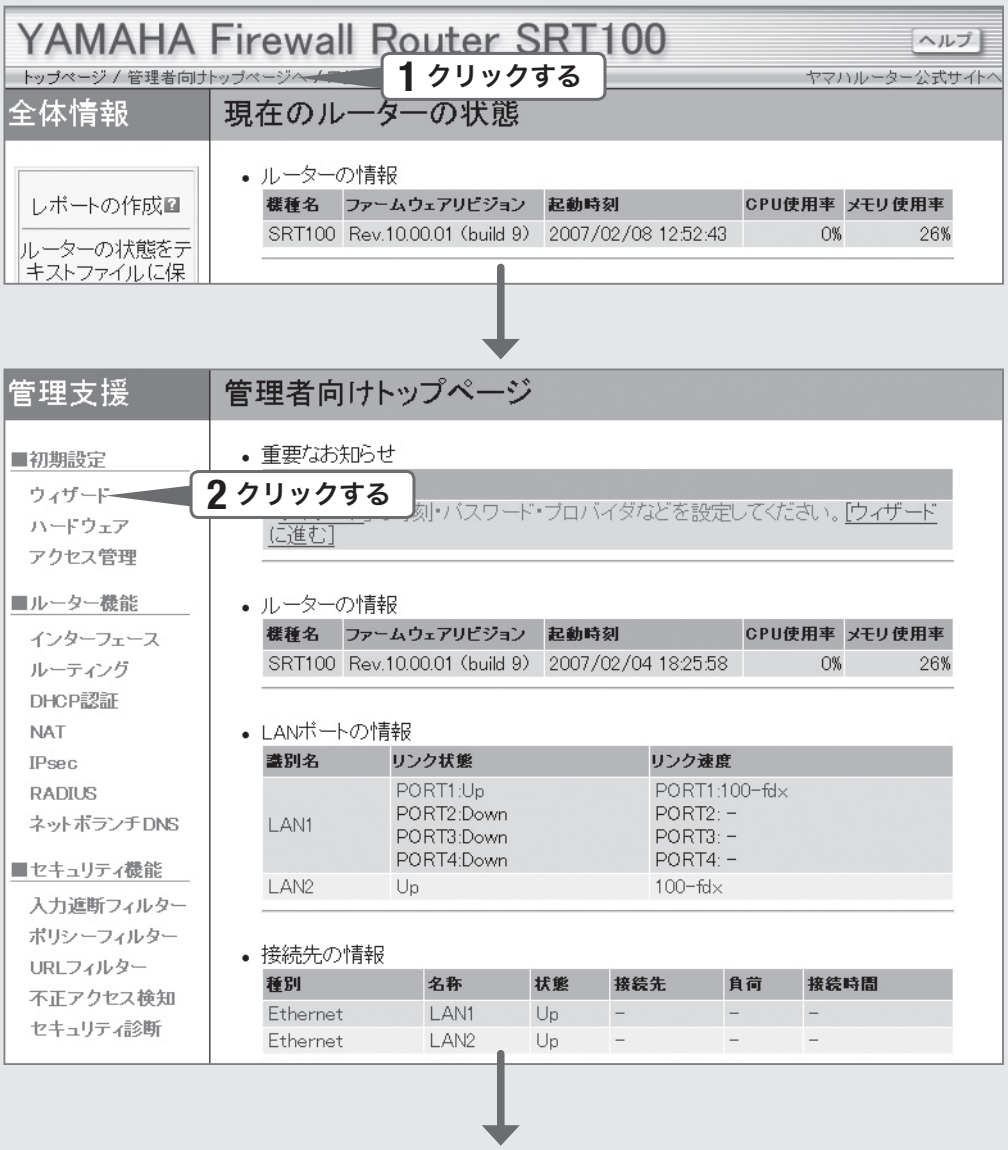
本製品の設定画面のトップページが表示されます。

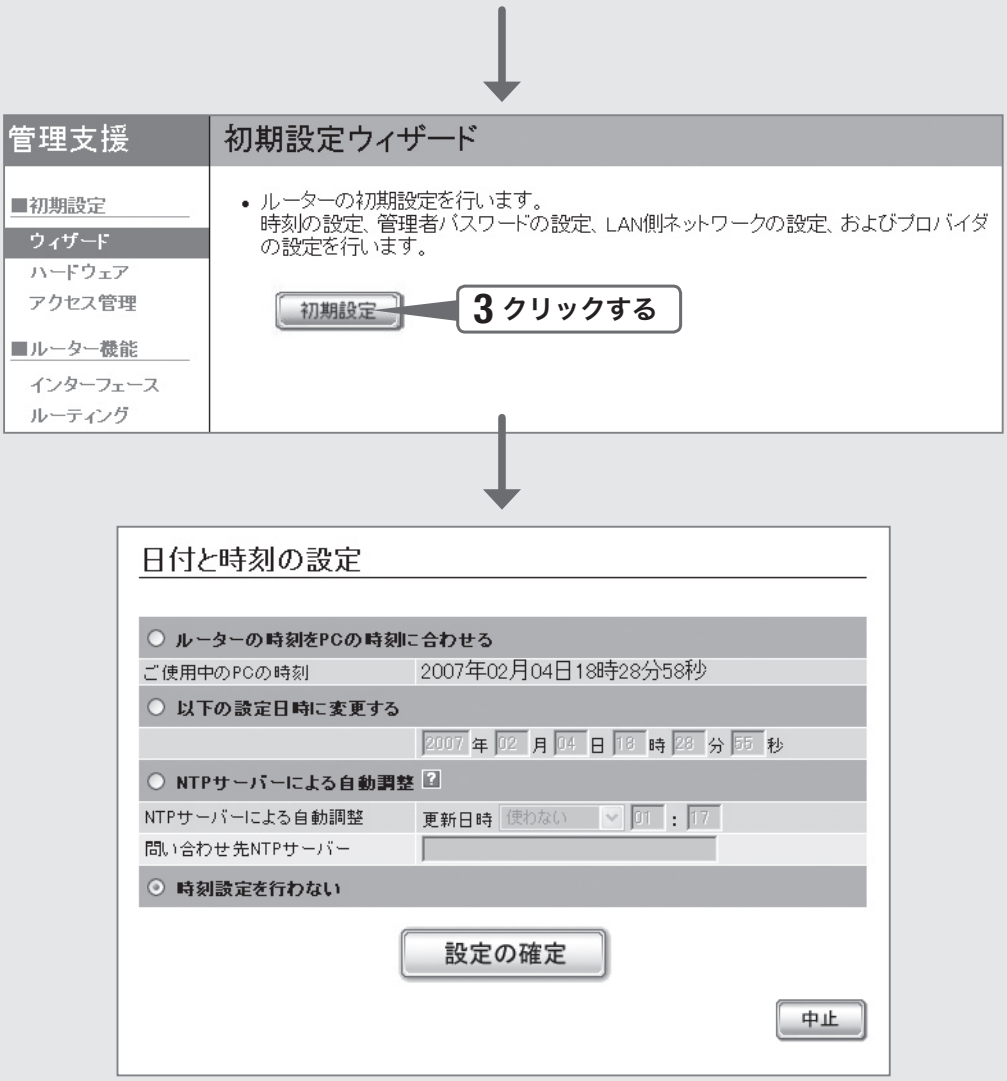
**設定画面のトップページが表示されないときは**

「設定画面で設定できない」(162ページ)をご覧ください。

# 3.「初期設定ウィザード」を開く

「初期設定ウィザード」を使用して、本製品をネットワーク上で使用するための基本的な設定をまとめて行うことができます。「初期設定ウィザード」を開くには、以下の手順で操作します。








## 1 「管理者向けトップページへ」をクリックする。

管理者向けトップページが表示されます。

## 2 「ウィザード」をクリックする。

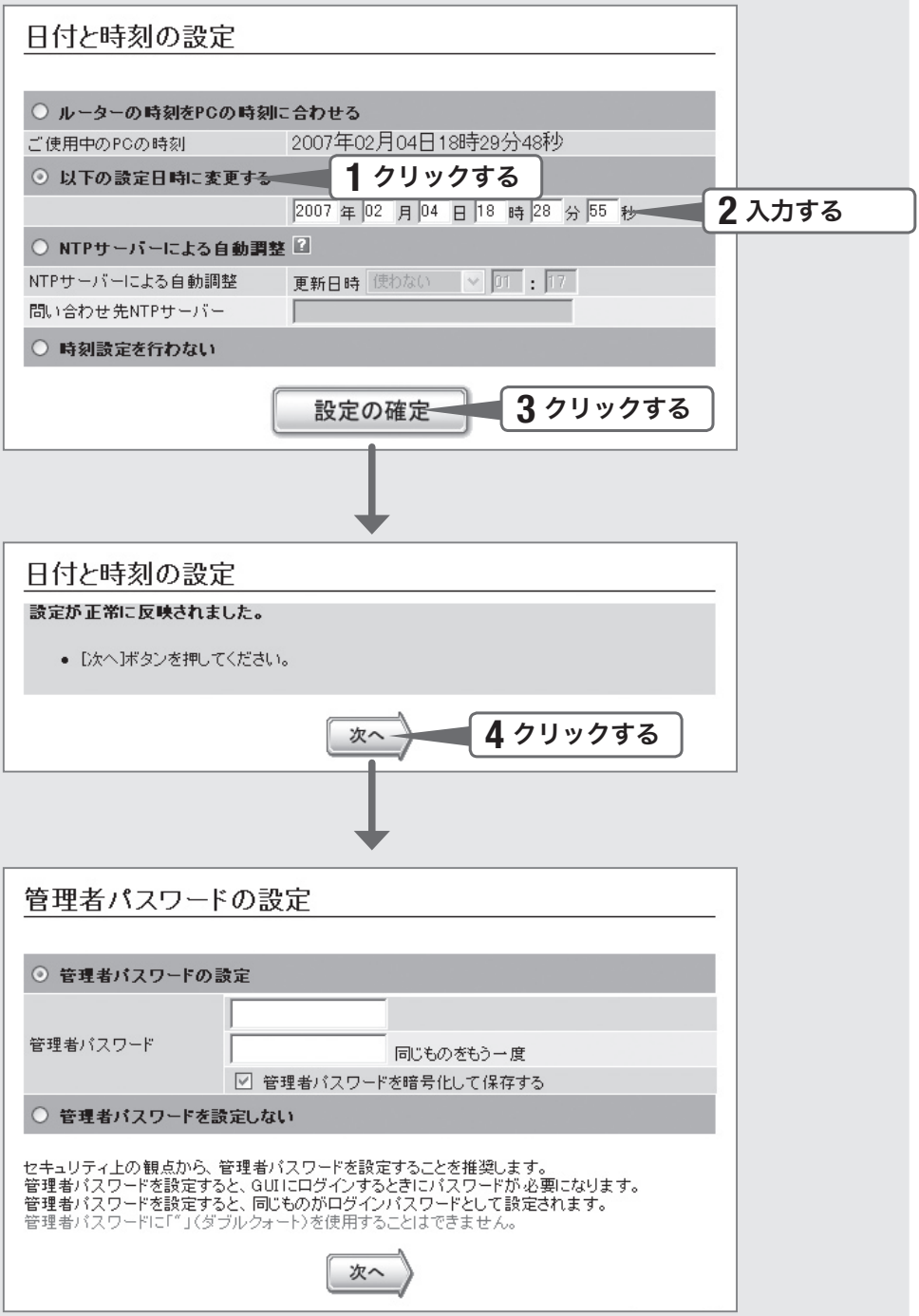
「初期設定ウィザード」画面が表示されます。

## 3 「初期設定」をクリックする。

「初期設定ウィザード」の「日付と時刻の設定」画面が別画面で表示されます。

# 4. 日付・時刻を合わせる

「日付と時刻の設定」画面で、本製品の日付と時刻を合わせます。



## 1 「日付と時刻の設定」画面で、「以下の設定日時に変更する」をクリックして選ぶ。

### 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。また、NTPサーバーを利用して手動で時刻を合わせたり、時刻を直接入力して合わせたりすることもできます。
詳しくは、「本体の設定」画面のヘルプをご覧ください。

**ご注意**

本製品のセキュリティ設定によっては、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(104ページ)。

## 2 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。

## 3 「設定の確定」をクリックする。

確認画面が表示されます。

## 4 「次へ」をクリックする。

「管理者パスワードの設定」画面が表示されます。

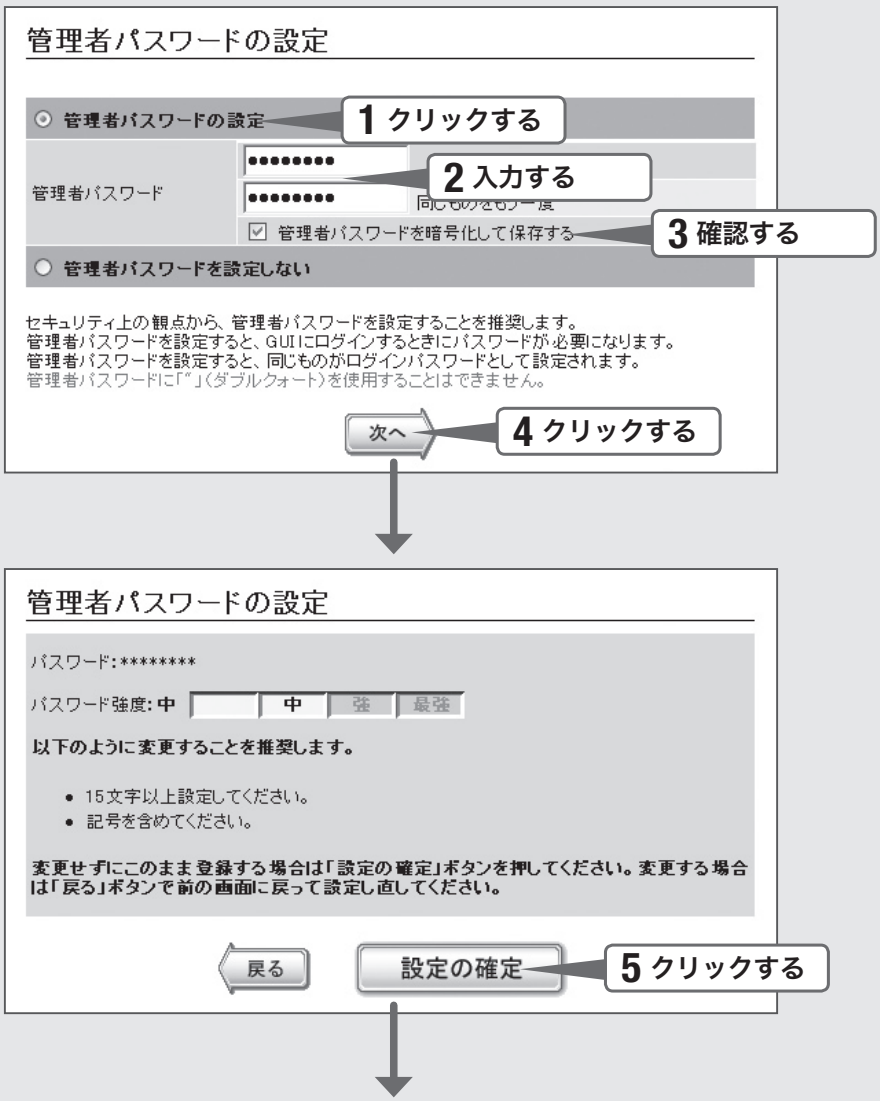
# 5.パスワードを設定する

セキュリティ対策を行う上でも、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。

**ヒント**

工場出荷時は、「doremi」が初期パスワードとして設定されています。セキュリティの問題を防ぐためにも、以下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。





**1** 「管理者パスワードの設定」画面で、「管理者パスワードの設定」をクリックして選ぶ。

**2** 「管理者パスワード」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。

### 安全なパスワードを設定するためのヒント

第三者から本製品へのアクセスを防ぐために、以下の点を考慮してパスワードの強度を上げるようにしてください。

- パスワードは15文字以上にする。
- 英字の大文字・小文字、数字を混在させる。
- 記号を使用する。

**3** 「管理者パスワードを暗号化して保存する」にチェックが付いていることを確認する。

チェックを付けるとパスワードが暗号化されて本製品の設定ファイル(config)に記録されるため、第三者がconfigファイルを入手した場合でも、本製品の設定を保護できます。

**4** 「次へ」をクリックする。

パスワードの強度確認画面が表示されます。

### パスワード強度が低い場合は

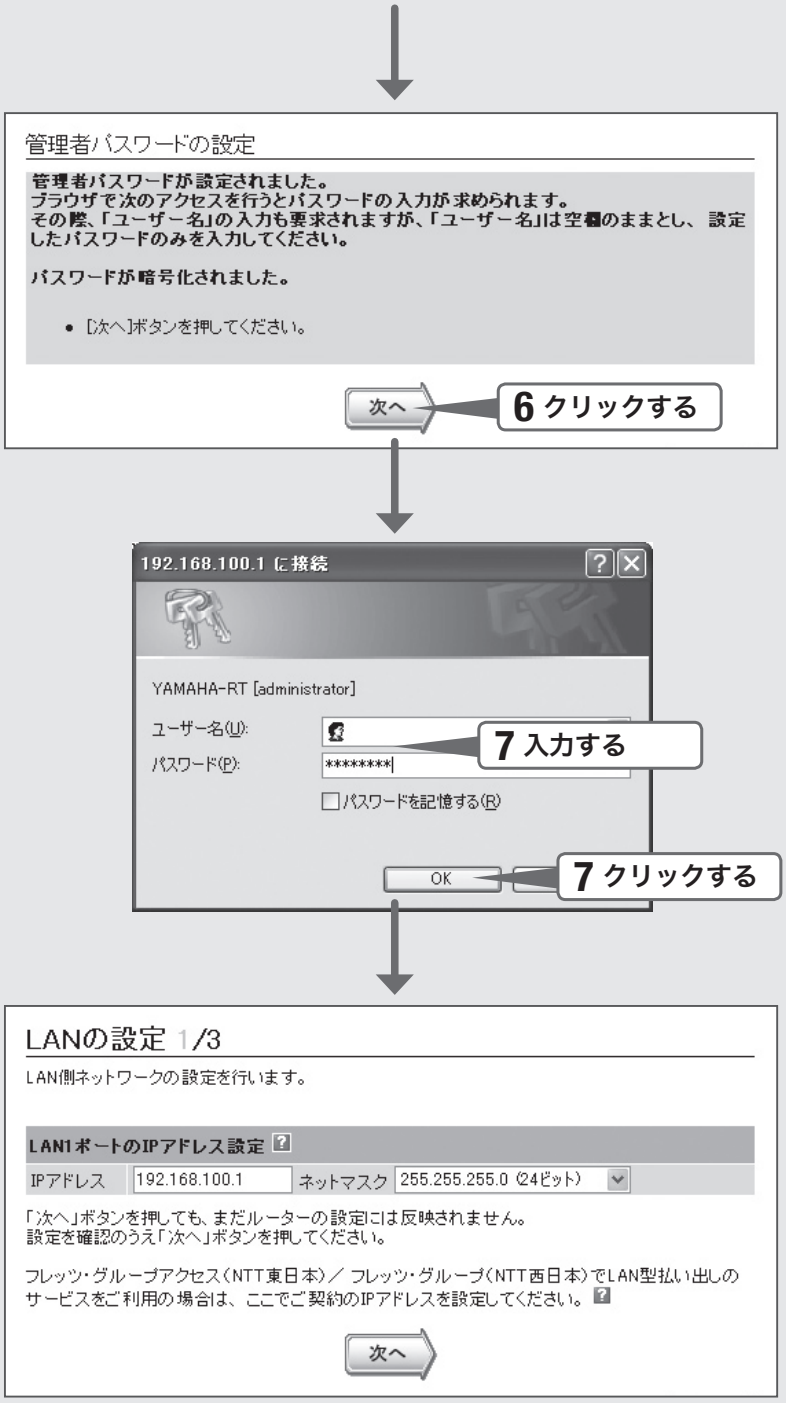
- **パスワードを修正する場合は**：「戻る」をクリックして手順2の操作からやり直します。手順2の「安全なパスワードを設定するためのヒント」を考慮してパスワードを修正してください。
- **そのまま使用する場合は**：「設定の確定」をクリックします。

**5** 「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、確認画面が表示されます。

**6** 「次へ」をクリックする。

パスワード入力画面が表示されます。




## 7 「パスワード」欄に手順2で設定したパスワードを入力してから、「OK」をクリックする。

「LANの設定 1/3」画面が表示されます。

**ヒント**

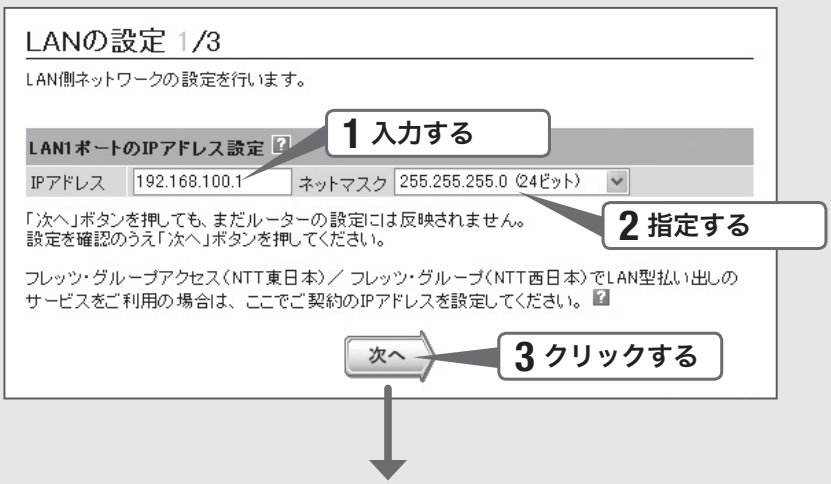
「ユーザー名」欄には何も入力する必要はありません。

# 6.LAN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。

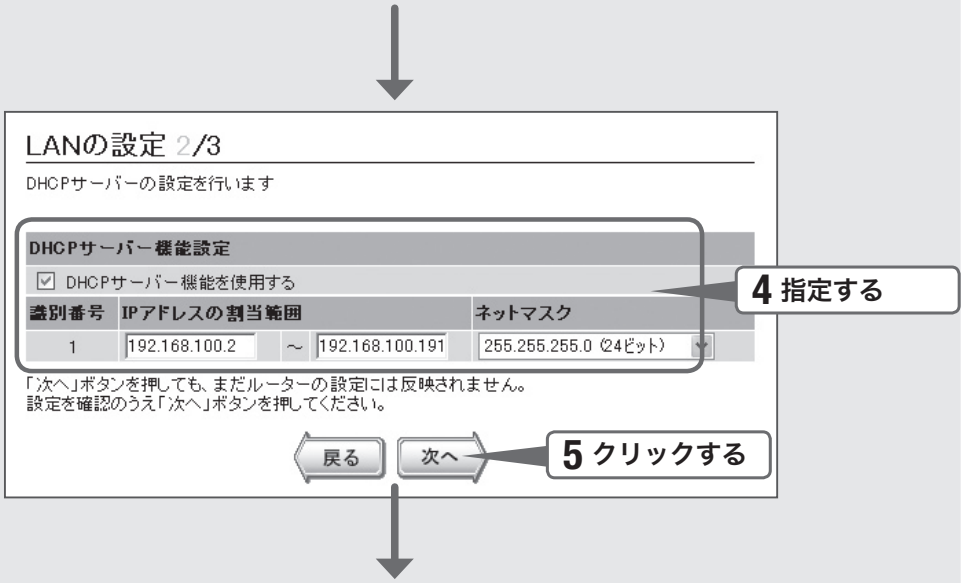



**1** 「LANの設定 1/3」画面で、「IPアドレス」欄に、本製品のLAN側IPアドレスを入力する。

**2** 「ネットマスク」欄で、本製品のLAN側ネットマスクを選ぶ。

**3** 「次へ」をクリックする。

「LANの設定 2/3」画面が表示されます。






## 4 本製品のDHCPサーバー機能の設定を確認して、必要に応じて設定を変更する。

### 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場合は

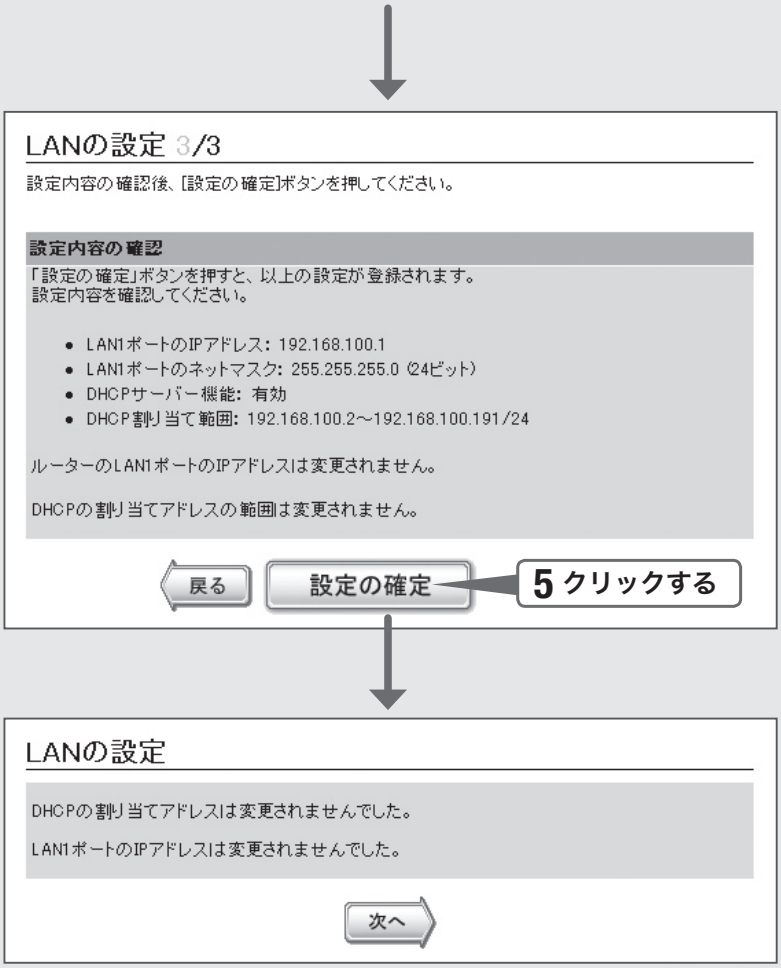
本製品のDHCPサーバー機能を無効にする必要があります。
「DHCPサーバー機能を使用する」をクリックして、チェックを外してください。

### DHCPサーバー機能によるIPアドレスの割り当て範囲を変更したい場合は

「DHCPサーバー機能を使用する」をクリックしてチェックを付けてから、割り当て範囲とネットマスクを指定します。

## 5 「次へ」をクリックする。

「LANの設定 3/3」画面が表示されます。




## 6 「設定の確定」をクリックする。

「LANの設定」画面が表示されます。

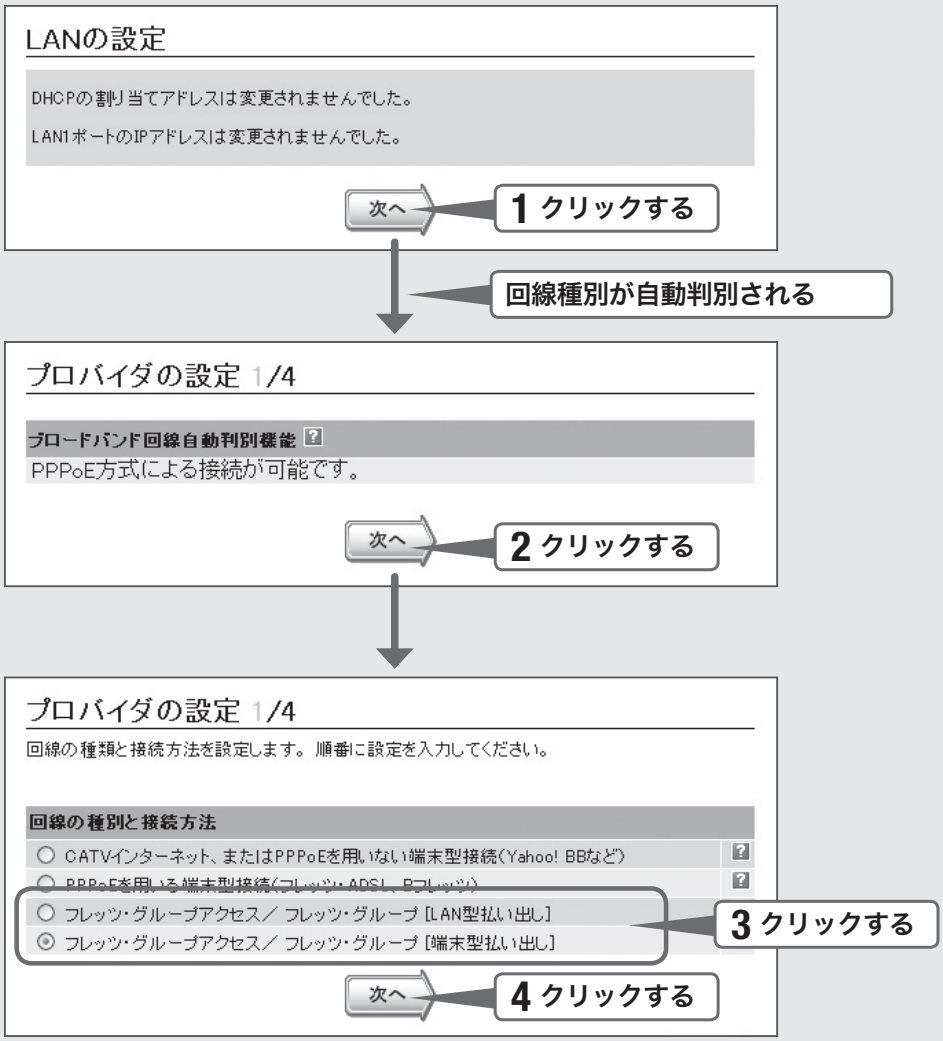
## 7 本製品のLAN側IPアドレスやDHCPサーバー機能によるIPアドレスの割り当て範囲を変更した場合は、パソコンのIPアドレスを変更する。

パソコンのIPアドレスを変更するには、「LAN内のパソコンのIPアドレスを変更する」(178ページ)をご覧ください。

### 引き続き、インターネットへの接続設定を行います

そのまま次ページの操作に進んでください。

# 7. 接続方法を指定する


LANの設定
DHCPの割り当てアドレスは変更されませんでした。
LAN1ポートのIPアドレスは変更されませんでした。
次へ
1 クリックする
回線種別が自動判別される
プロバイダの設定 1/4
ブロードバンド回線自動判別機能
PPPoE方式による接続が可能です。
次へ
2 クリックする
プロバイダの設定 1/4
回線の種類と接続方法を設定します。順番に設定を入力してください。
回線の種別と接続方法
CATVインターネット、またはPPPoEを用いない端末型接続(Yahoo! BBなど)
フレッツ・グループアクセス／ フレッツ・グループ [LAN型払い出し]
フレッツ・グループアクセス／ フレッツ・グループ [端末型払い出し]
3 クリックする
次へ
4 クリックする

## 1 「LAN側ネットワークの設定」画面で、「次へ」をクリックする。

本製品のブロードバンド回線自動判別が動作して、判別結果の回線の種類が表示されます。

**ご注意**

- 本製品のLAN2ポートにブロードバンド回線を接続していない場合は、自動判別機能は動作しません。
- 回線自動判別機能を一度実行すると、次回から自動判別は行いません。

## 2 「次へ」をクリックする。

回線自動判別の結果に応じた項目が選択された状態で、「プロバイダの設定1/4」画面が表示されます。

## 3 契約したフレッツ・グループアクセスまたはフレッツ・グループの接続方法(LAN型払い出しまたは端末型払い出し)をクリックする。

LAN型か端末型かわからない場合は、NTTから送付された資料をご覧ください。それでもわからない場合は、NTTまでお問い合わせください。

### 「LAN型払い出し」契約の場合は

「フレッツ・グループアクセスまたはフレッツ・グループ[LAN型払い出し]」をクリックして選びます。

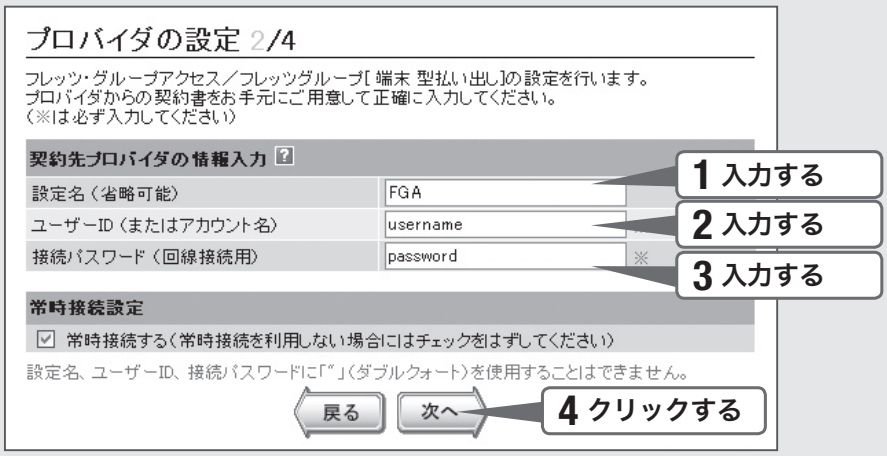
### 「端末型払い出し」契約の場合は

「フレッツ・グループアクセスまたはフレッツ・グループ[端末型型払い出し]」をクリックして選びます。

## 4 「次へ」をクリックする。

接続方法に合わせた設定画面が表示されます。

# 8. 接続情報を指定する






## 1 「設定名」欄に、インターネット接続の設定名を入力する。

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」欄にユーザー 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 」欄に接続パスワードを入力する。

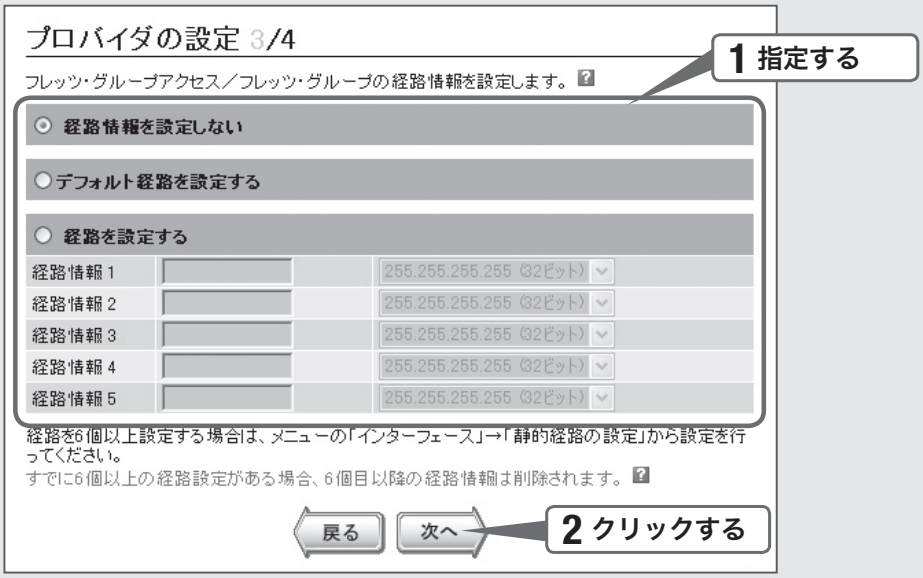
プロバイダから指定されたパスワード（または自分で変更したパスワード）を入力します。半角英数字で、大文字小文字も正確に入力してください。

## 4 必要な場合のみフレッツ網へ（手動で）接続したい場合は、「常時接続する」をクリックしてチェックを外す。

## 5 「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。

# 9.経路情報を指定する

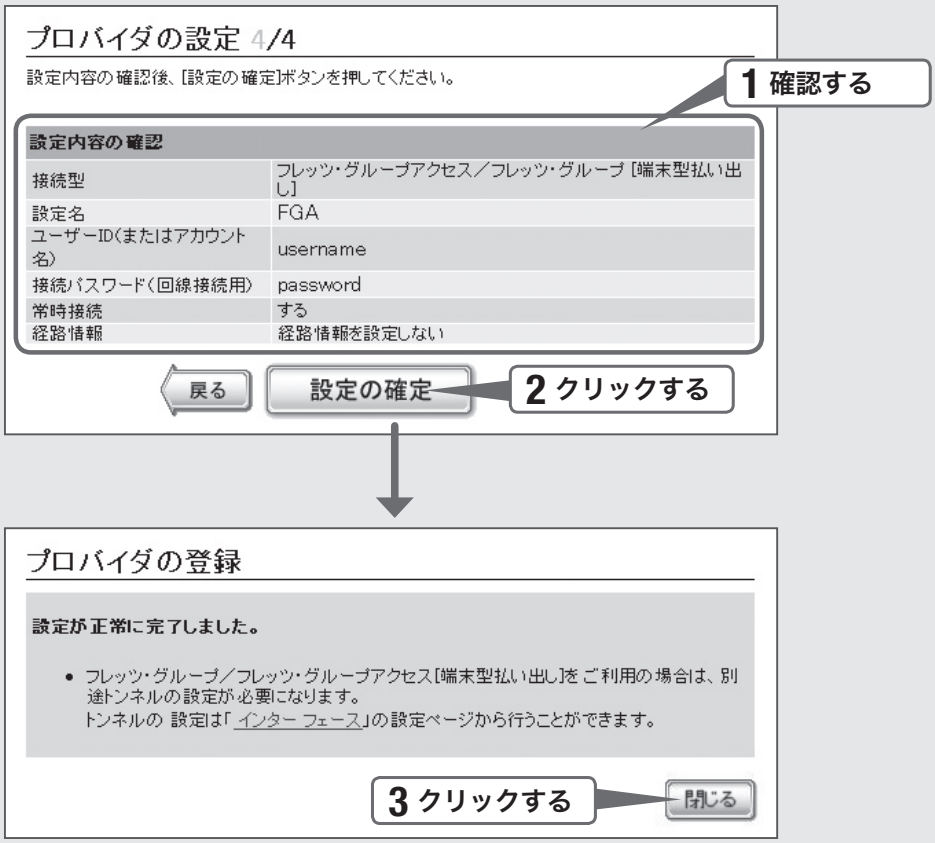



**1** **経路情報を指定する場合は、「経路を設定する」をクリックしてから、経由するIPアドレスおよびネットマスクを指定する。**

**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。

# 10. 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どうか確認する。

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て、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。

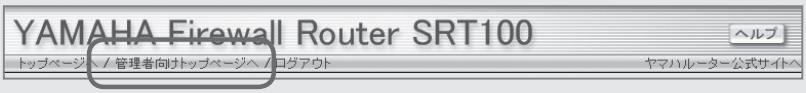
確認画面が表示されます。

## 3 「閉じる」をクリックする。

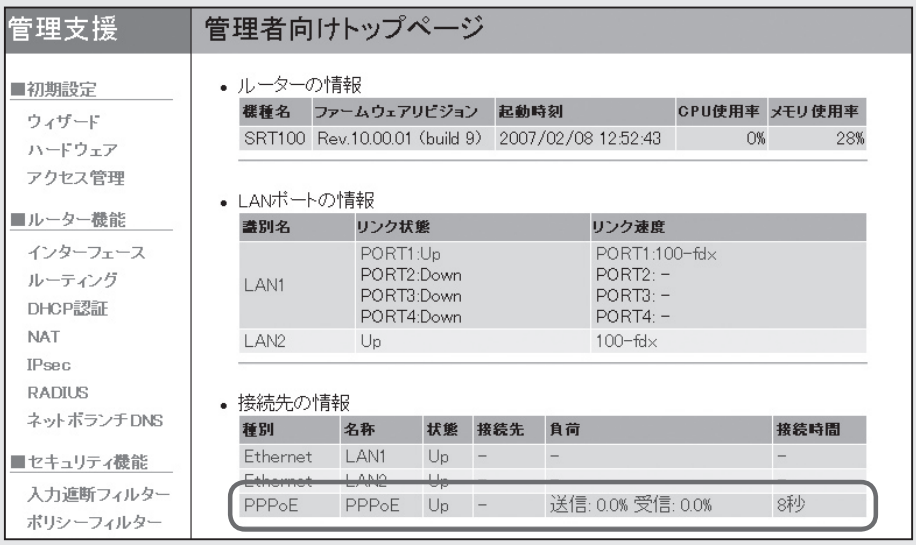
本製品は自動的にフレッツ網に接続します。

## 4 「管理者向けトップページへ」をクリックする。

管理者向けトップページが表示されます。



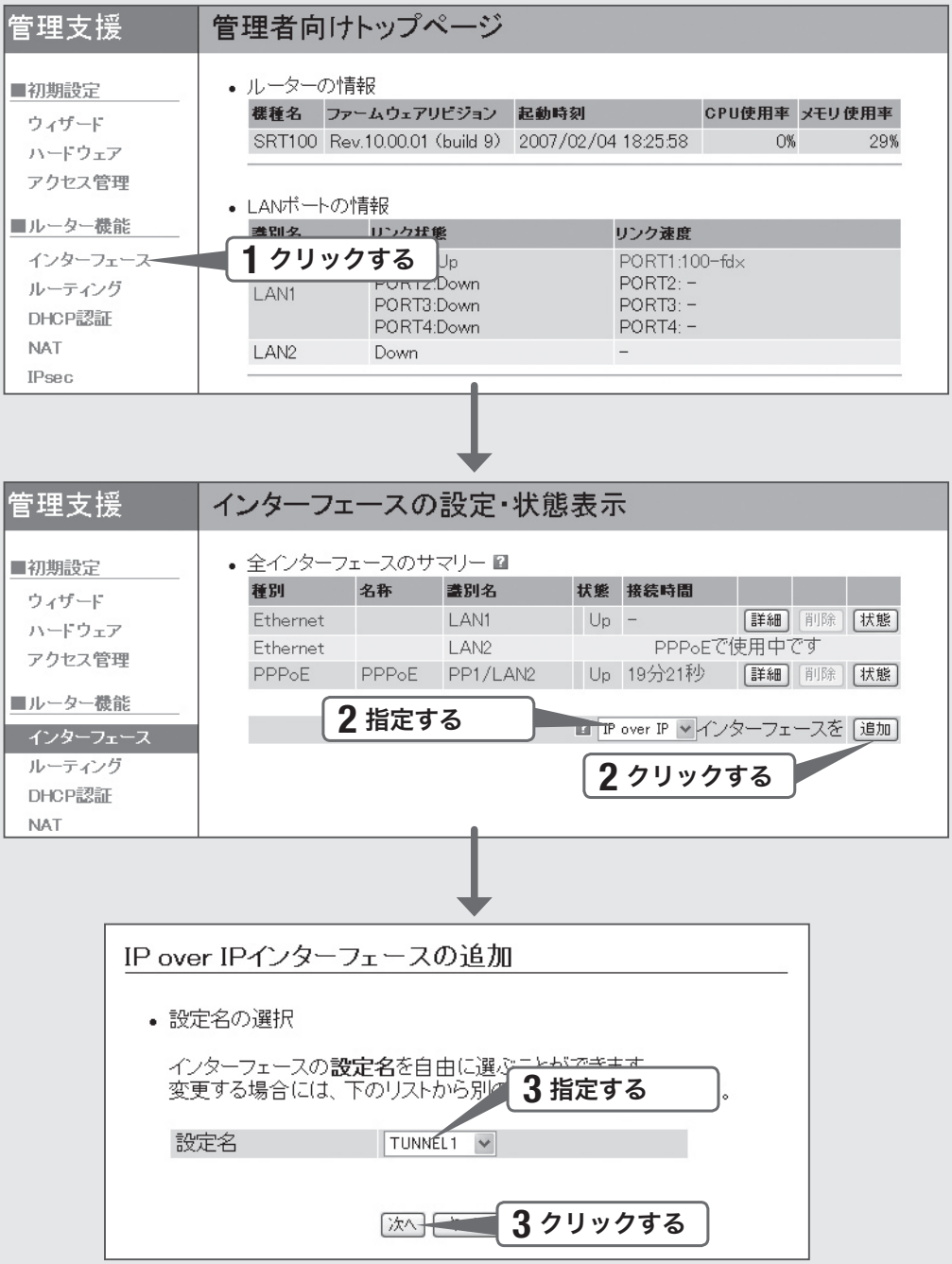

## 5 フレッツ網へ接続できていることを確認する。




## 引き続き、IPIPトンネルの接続設定を行います

次ページの操作に進んでください。

# 11.「トンネル接続番号を指定する



**1** **管理者向けトップページの「インターフェース」をクリックする。**

「インターフェースの設定・状態表示」画面が表示されます。

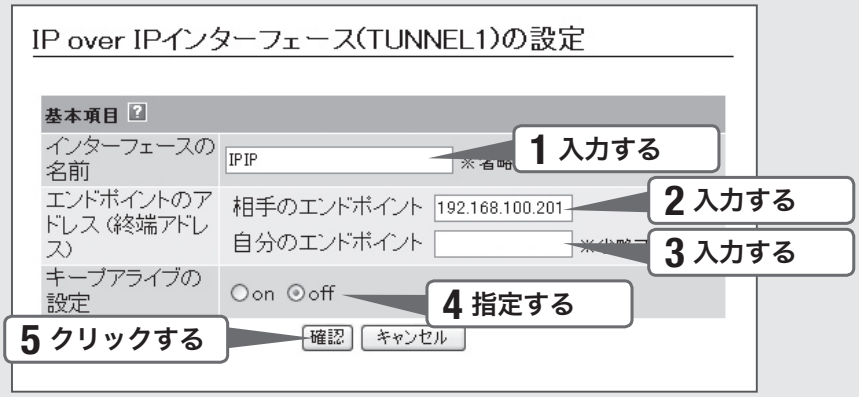
**2** **「インターフェースを追加」欄で「IP over IP」を選んでから、「追加」をクリックする。**

「IP over IPインターフェースの追加」画面が表示されます。

**3** **「設定名」欄で任意のトンネル接続番号を指定してから、「次へ」をクリックする。**

「IP over IPインターフェース(指定したトンネル接続番号)の設定」画面が表示されます。

# 12. IPIPトンネル接続に必要な情報を指定する






**1** **「インターフェースの名前」欄で、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** **「相手のエンドポイント」欄に、接続先のIPアドレスを入力する。**

接続相手に割り当てられるIPアドレスを入力します。

**3** **必要に応じて「自分のエンドポイント」欄に、本製品のIPアドレスを入力する。**

**4** **IPIPトンネル接続の状態を監視したい場合は、「キープアライブ」欄で「on」をクリックして選ぶ。**

**5** **「確認」をクリックする。**

確認画面が表示されます。

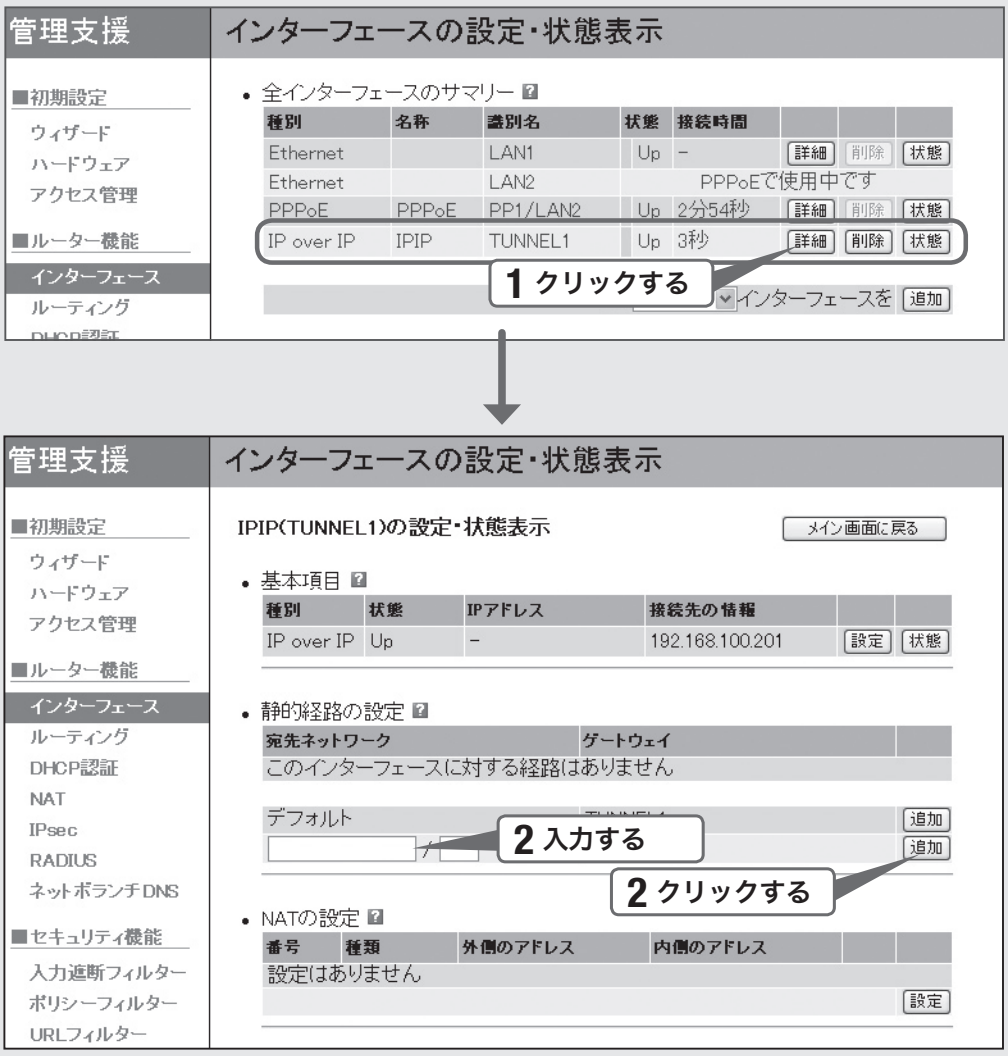
**6** **「登録」をクリックする。**

確認画面が表示されます。

**7** **「メイン画面に戻る」をクリックする。**

「インターフェースの設定・状態表示」画面に戻ります。

# 13. 経路情報を指定する




## 1 追加した「IP over IP」インターフェース欄の「詳細」をクリックする。

「(指定したトンネル名称)(指定したトンネル接続番号)の設定・状態表示」画面が表示されます。

## 2 「静的経路の設定」欄に経路のアドレス情報および経路のネットマスク情報を入力してから、「追加」をクリックする。

確認画面が表示されます。

## 3 「登録」をクリックする。

確認画面が表示されます。

## 4 「メイン画面に戻る」をクリックする。

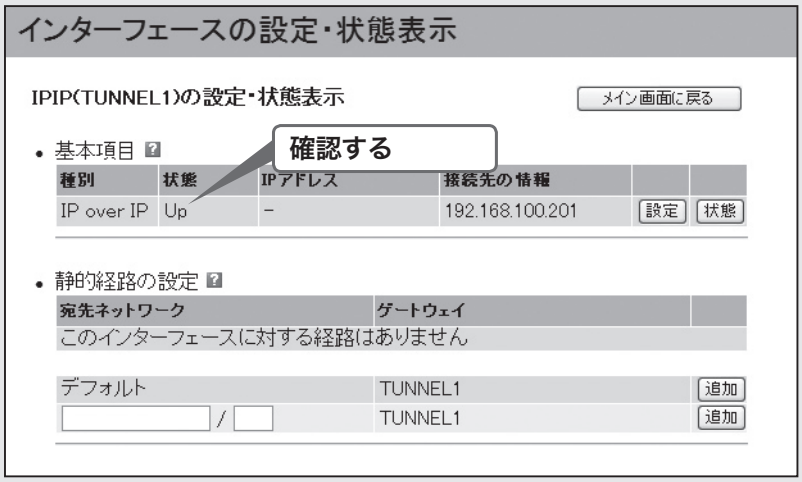
「インターフェースの設定・状態表示」画面に戻ります。
これまでの設定が終わると、IPIPトンネルの通信は自動的に確立されます（特に操作は必要ありません）。

## 5 複数のLANと接続する場合は、手順1～4を繰り返す。

接続相手ごとの経路情報をすべて指定してください。

**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、間違わないように設定してください。

## 6 「インターフェースの設定・状態表示」画面で、IPIPトンネル接続できていることを確認する。




# 設定終了

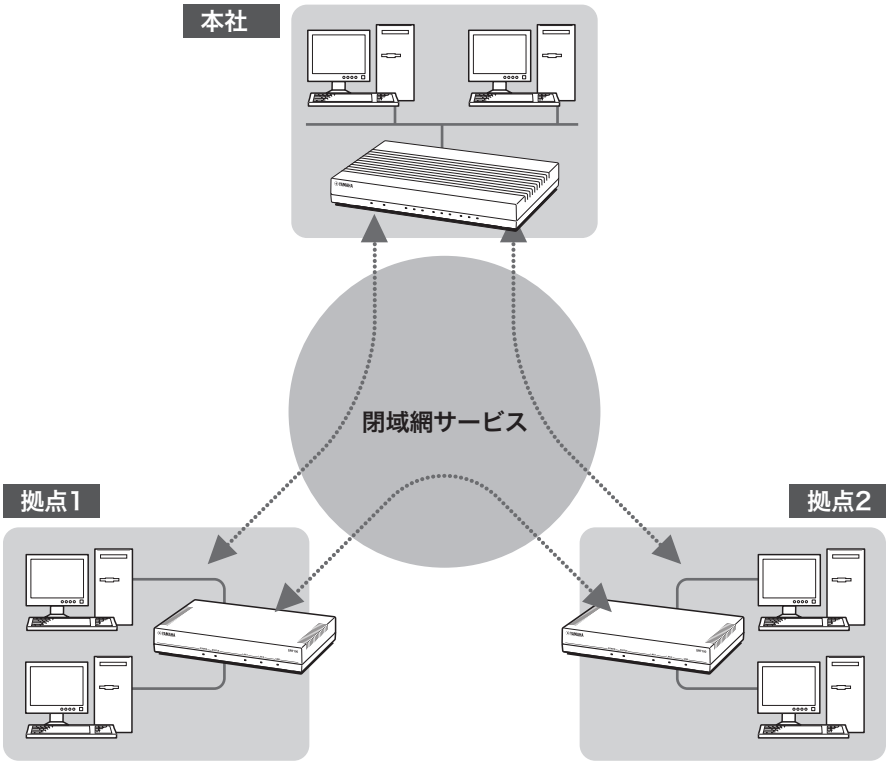
**これでトンネル接続の設定は終了です**

**▶トンネル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** 94～96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」を参考にして、問題を解決してください。

# 広域LANなどの閉域網で使用する

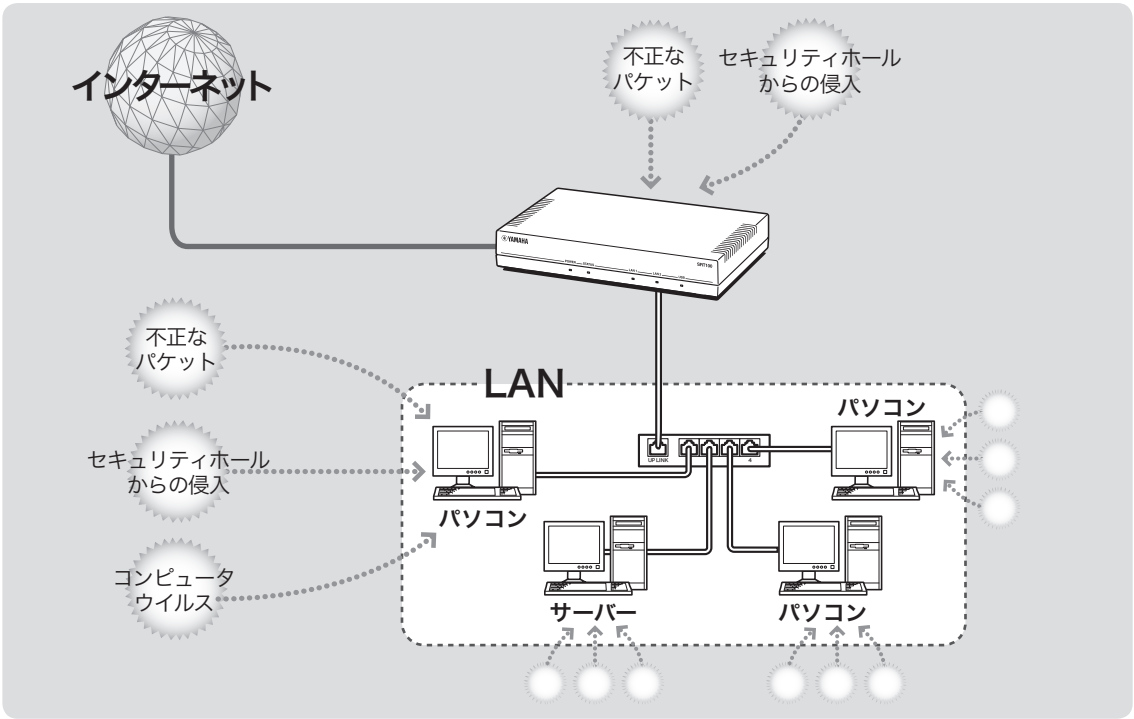
広域LANなどで使用する場合に、拠点のルーターとして本製品を使用できます。セキュリティ機能(98ページ)を活用することで、端末単位のアクセス制限やURLフィルタリングなどを拠点側でも実行でき、便利です。




## 使用例・設定例について詳しくは、ネットボランチホームページをご覧ください

ネットボランチホームページ(http://netvolante.jp/)には、システム例や設定ファイルの構成例など、さまざまな情報が記載されています。

# 不正アクセスとセキュリティ対策の概要






## 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。
- これらの攻撃により本製品の設定が改変されたり、パソコンのシステムやデータが破壊された場合、多大なデータ的被害や金銭的被害に遭うことも十分に考えられます｡本製品のフィルターを設定するなどのセキュリティ対策を行って、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を設定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上の抜け道／穴(セキュリティホール)は、日々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、当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。

**本製品で可能な対策**

- 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(102、104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。

**本製品で可能な対策**

- 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(102、104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などから侵入するもの(コンピュータウイルス)

電子メールの添付ファイルを開いたり、インターネット・LAN上のウイルスファイルにアクセスすることで感染します。不審なファイルを開かないよう徹底するだけでなく、パソコンのウイルス検知ソフトを利用して被害を最小限に抑えることができます。

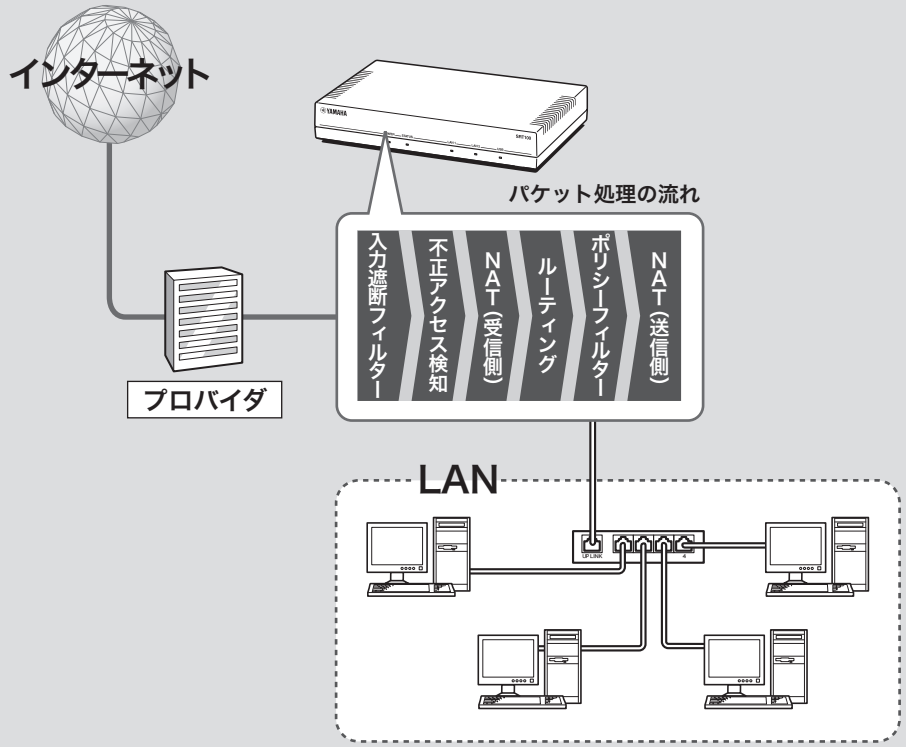
**本製品で可能な対策**

- 本製品のセキュリティ強化機能は、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機能の概要

## 外部からの攻撃に対するセキュリティ機能

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**（**102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**（**104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**(**110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 セキュリティ機能

## クライアントごとにアクセス権を設定する(DHCP認証)(112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)(116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フィルターソフトウェアのデータベースを参照して、アクセスを制限することもできます。

## クライアント単位で使用帯域を制限する(DCC、Dynamic Class Control)

クラスごとに優先度や帯域を割り当てて、クラス単位の使用帯域制御を行う(QoS)だけでなく、パソコンをはじめとするクライアント単位で使用帯域を監視できます。P2Pソフトウェアを使用している場合など、必要以上の帯域を使用しているクライアントのみの帯域を制限したり、通信を遮断したりすることができるので、便利です。

**ヒント**

DCCを設定するには、コマンドによる設定が必要です。詳しくは「コマンドリファレンス」をご覧ください。

# その他のセキュリティ機能

## セキュリティ設定を検証する(119ページ)

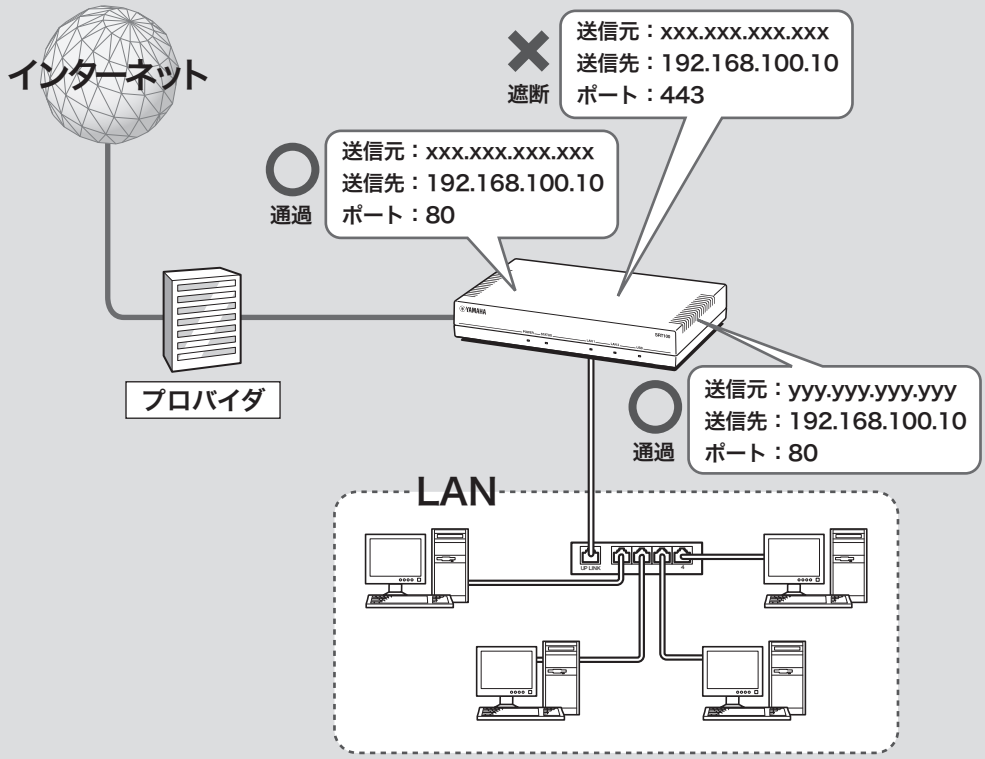
接続設定終了後にセキュリティの診断機能を使用すると、ポートの開閉状態を診断できます。
詳しい検証項目および内容については、「ポートスキャンを実行してポートの開閉状態を確認する」(119ページ)をご覧ください。

## 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。

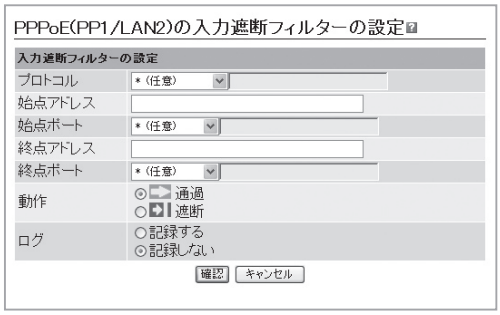


# 入力遮断フィルターを登録する

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設定」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 ? をクリックして、表示される説明をご覧ください。

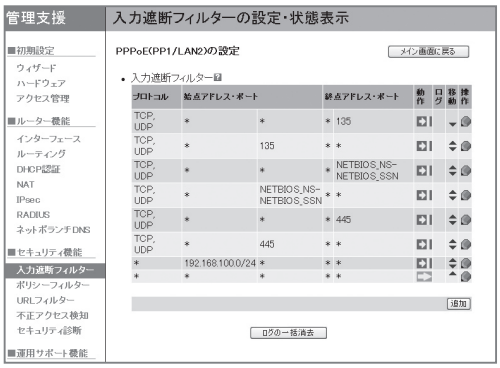
**「入力遮断フィルターの設定」画面を開くには**

管理者向けトップページから、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「入力遮断フィルター」
▶入力遮断フィルターを設定したいインターフェースの「詳細」
▶「入力遮断フィルター」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設定・状態表示」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。
  - フィルタ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、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 ? をクリックして、表示される説明をご覧ください。

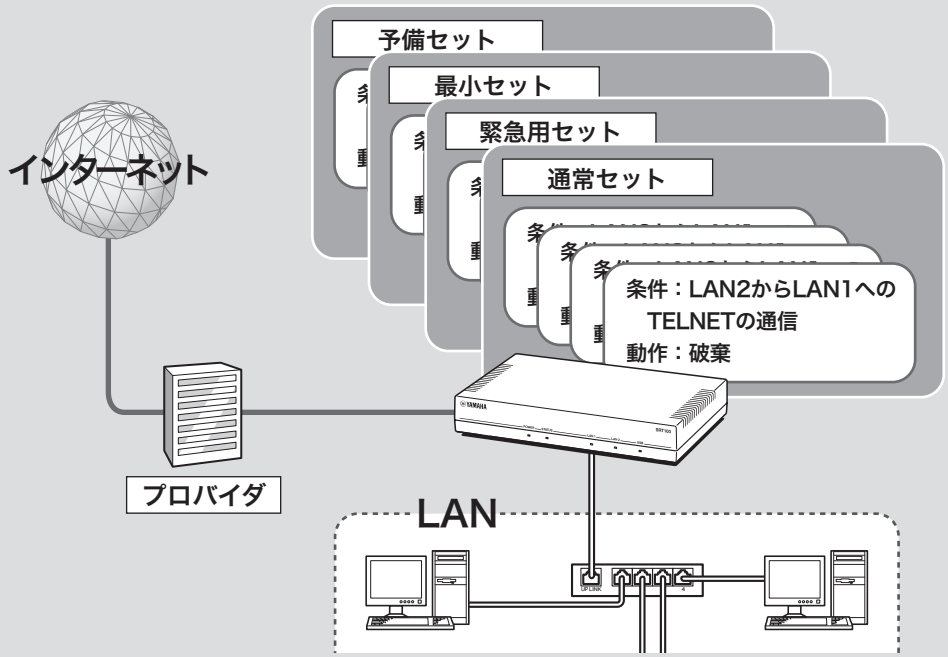
**「入力遮断フィルターの設定」画面を開くには**

管理者向けトップページから、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「入力遮断フィルター」
▶入力遮断フィルターを設定したいインターフェースの「詳細」

# 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。



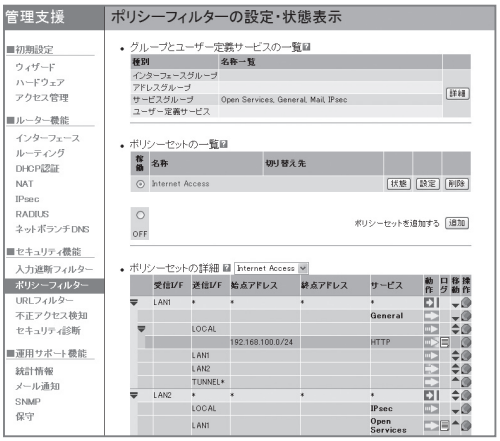

- 受信／送信インターフェースおよび始点／終点アドレス、サービスを指定して、パケット単位ではなくコネクション単位で通過と破棄を指定します。
- 通信状態を監視しながら、必要に応じてフィルターを適用します。例えば「通常はインターネットからLANへのデータはすべて破棄し、LAN側からftpのアクセスが発生した場合のみ戻りのパケットを通過させる」といったように、セッションの状態を反映したフィルターを設定できます。
- ポリシーのリスト(ポリシーセット)は最大で4セットまで登録できます。通常の運用に使用するポリシーセットと、緊急時に最低限のコネクションのみ通過させるポリシーセットなどをあらかじめ登録しておき、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(108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(109ページ)。
- 登録済み端末(112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。
  - 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 ? 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**

管理者向けトップページから、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「ポリシーフィルター」

# ポリシーを追加する

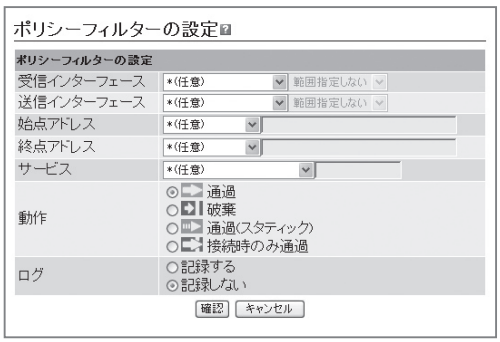
設定したいインターフェースの「ポリシーフィルターの設定」画面で、ポリシーを登録（ポリシーセットごとに最大128個まで）します。

**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」（108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 ? 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**

管理者向けトップページから、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「ポリシーフィルター」

▶ポリシーを設定したいポリシーセット詳細欄の「追加」

# 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）（つづき）

## 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同じ階層で追加されます。

# 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4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。

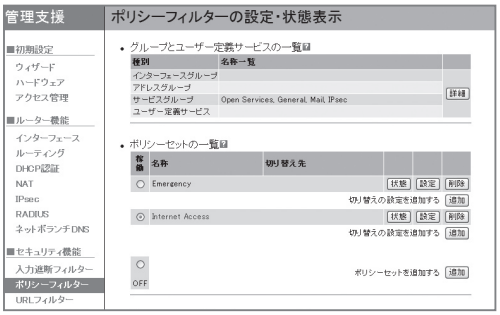

設定内容について詳しくは、設定画面の？をクリックして、表示される説明をご覧ください。

### 「ポリシーセットの設定」画面を開くには

管理者向けトップページから、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「ポリシーフィルター」
▶ポリシーセットの一覧欄の「ポリシーセットを追加する」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。




確認画面が表示されるので、「登録」をクリックしてください。

### 「ポリシーフィルターの設定・状態表示」画面を開くには

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

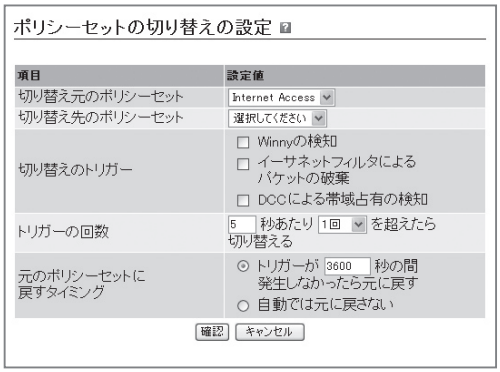
▶トップページの「ポリシーフィルター」

## 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 ? 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

管理者向けトップページから、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「ポリシーフィルター」

▶ポリシーセットの一覧欄の「切り替えの設定を追加する」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（109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

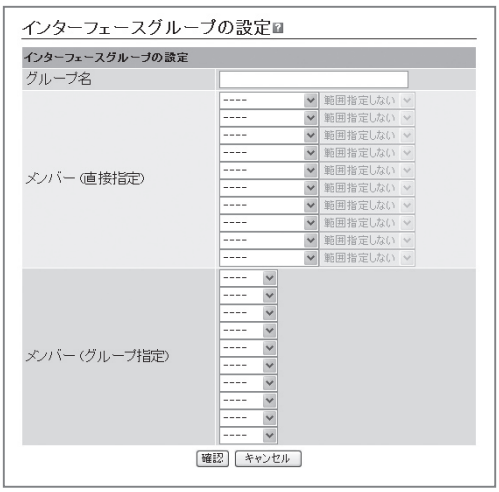
本製品で登録できるグループは、インターフェースグループ、アドレスグループ、サービス（プロトコル）グループの3種類です。それぞれの種類のグループについて、最大32個まで定義できます。

**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 ? をクリックして、表示される説明をご覧ください。

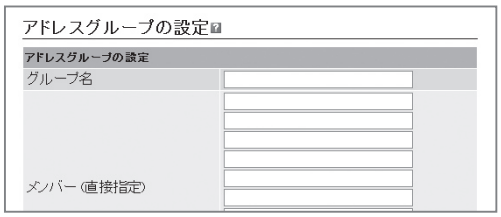
**「インターフェースグループの設定」画面を開くには**

管理者向けトップページから、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「ポリシーフィルター」
▶グループとユーザー定義サービスの一覧の「詳細」
▶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 ? 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**

管理者向けトップページから、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「ポリシーフィルター」
▶グループとユーザー定義サービスの一覧の「詳細」
▶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 ? 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**

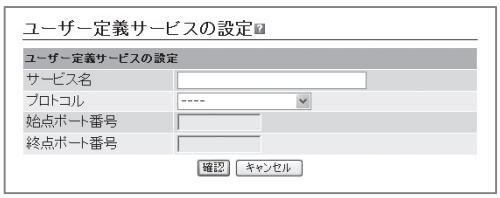
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「ポリシーフィルター」
▶グループとユーザー定義サービスの一覧の「詳細」
▶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 ? をクリックして、表示される説明をご覧ください。

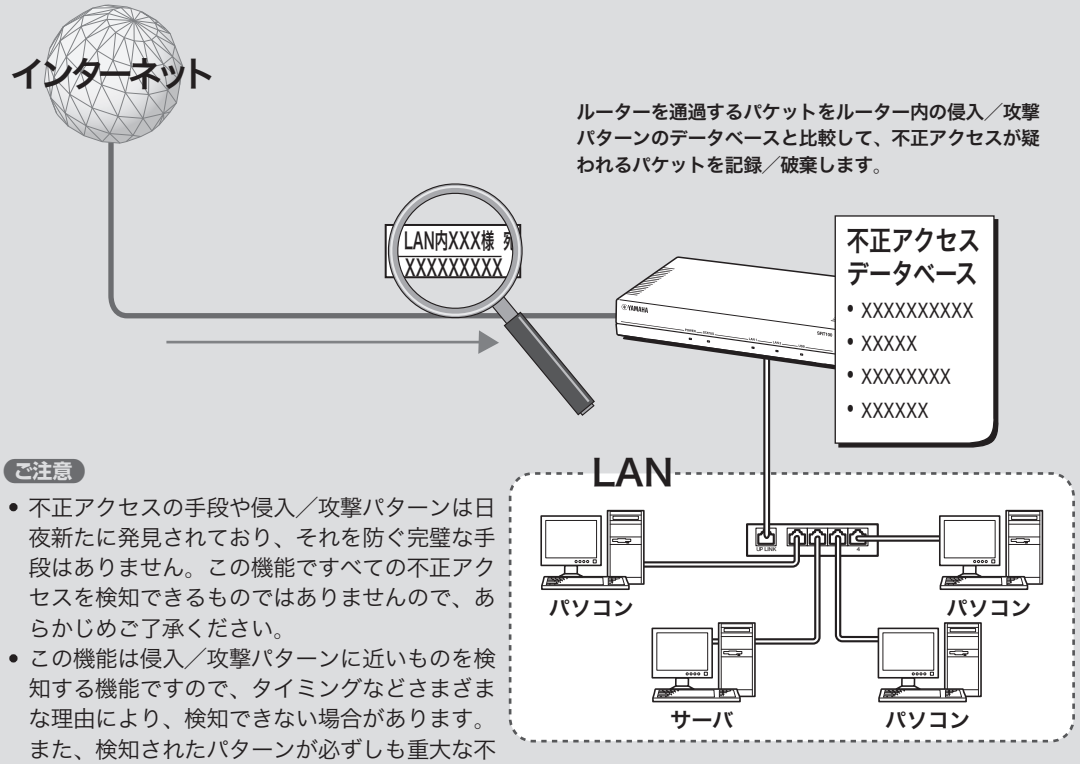
**「ユーザー定義サービスの設定」画面を開くには**

管理者向けトップページから、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「ポリシーフィルター」
▶グループとユーザー定義サービスの一覧の「詳細」
▶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**

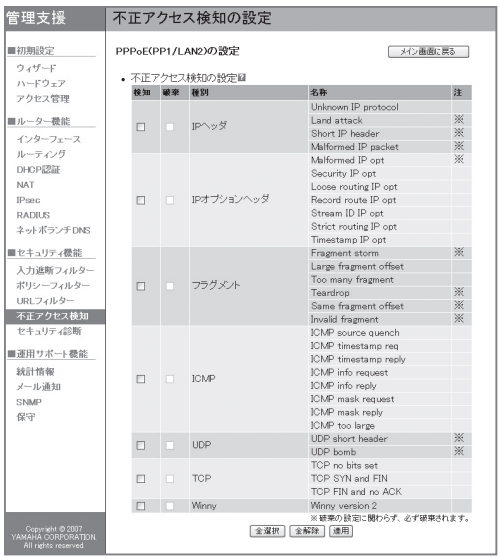
- 不正アクセスの手段や侵入／攻撃パターンは日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入／攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、検知されたパターンが必ずしも重大な不正アクセスであることを判断するものではありません。あくまでセキュリティ管理の目安であることをご理解の上、ご利用ください。
- 本機能は各インターフェースに適用できます。
- 本機能を使用すると、インターネットなどへのアクセス速度が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

# 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、EthernetやPPPoE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 ? 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

管理者向けトップページから、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「不正アクセス検知」

▶不正アクセス検知機能の設定を変更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

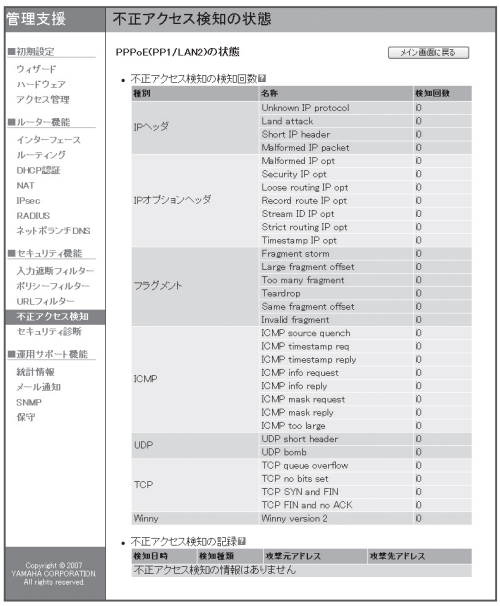
「不正アクセス検知の状態」画面で、不正アクセスの検知回数と検知履歴を確認できます。

**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(136ページ)。




### 「不正アクセス検知の状態」画面を開くには

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

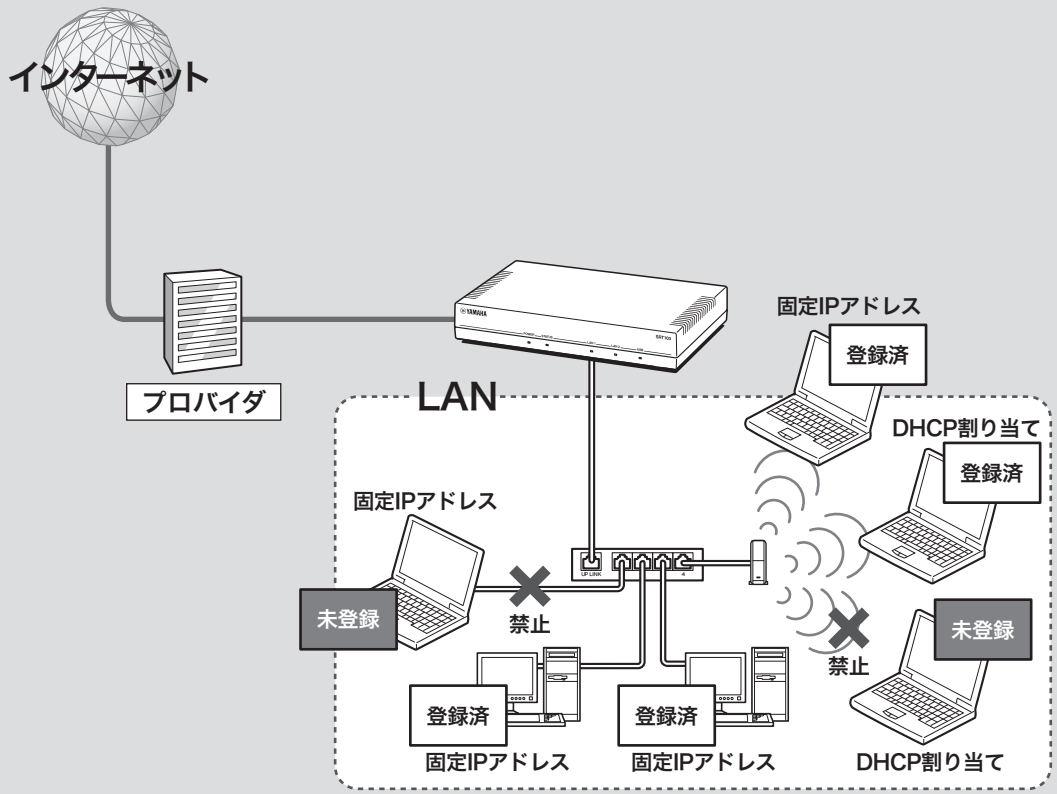
▶トップページの「不正アクセス検知」

▶不正アクセス検知機能の状態を確認したいインターフェースの「状態」

# 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、ルーター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（104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**

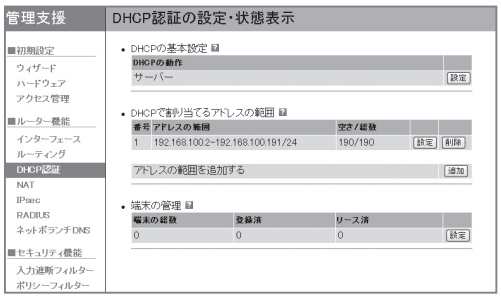
- クライアントが接続する1つの物理ネットワークで、2つの論理ネットワーク（プライマリネットワークとセカンダリネットワーク）を構成できます。この状態でdhcp scope lease typeコマンドを使用して、登録済み端末にはプライマリネットワークに対応するIPアドレス、未登録端末にはセカンダリネットワークに対応するIPアドレスを割り当てて、登録済み端末と未登録端末を区別することもできます。
- この機能を利用することで、登録済み端末は社内・社外すべてのネットワークへアクセスできる一方で、未登録端末は社内の特定セグメントのみへのアクセスに制限するなど、クライアントごとに異なるアクセス権を設定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

# DHCPサーバーの動作状態を確認する

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認証の設定・状態表示」画面で、「DHCPの動作」欄に「サーバー」と表示されていることを確認します。

**ヒント**

- 本製品の初期設定では、DHCPサーバー機能は動作するように設定されています。
- DHCPで割り当てるIPアドレスの範囲を指定するには、「DHCP認証の設定・状態表示」画面の「DHCPで割り当てるアドレスの範囲」欄の「設定」(既存の割り当て範囲を変更する場合)または「追加」(新規の割り当て範囲を設定する場合)をクリックします。




**「動作しない」と表示されている場合は**

「DHCPの動作」欄の「設定」をクリックして、DHCPサーバーを動作するよう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 ? をクリックして、表示される説明をご覧ください。

**「端末管理の設定・状態表示」画面を開くには**

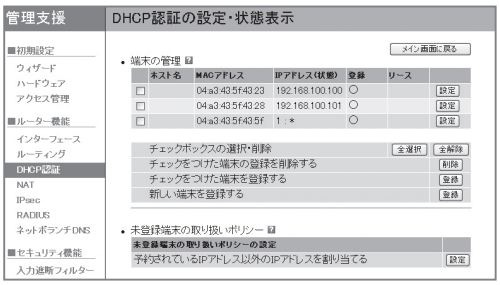
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「DHCP認証」

# 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認証の設定・状態表示」画面の「端末の管理」欄で「全選択」をクリックして、すべての端末にチェックを付ける。**




**「端末管理の設定・状態表示」画面を開くには**

管理者向けトップページから、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「DHCP認証」

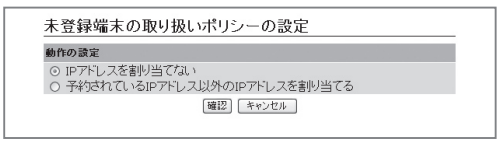
▶「端末の管理」の「設定」

**2 「チェックをつけた端末を登録する」欄の「登録」をクリックする。**

確認画面が表示されます。

**3 「登録」をクリックしてから、「管理画面に戻る」をクリックする。**

**4 「未登録端末の取り扱いポリシーの設定」画面で「IPアドレスを割り当てない」をクリックしてから、「確認」をクリックする。**



**「未登録端末の取り扱いポリシーの設定」画面を開くには**

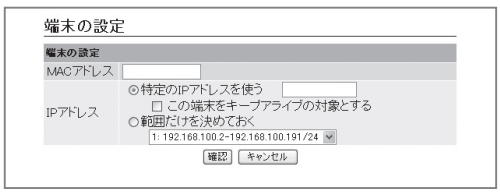
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「DHCP認証」
▶「端末の管理」の「設定」
▶「未登録端末の取り扱いポリシー」の「設定」

**5 「設定」をクリックしてから、「管理画面に戻る」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。「端末の設定」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 ? をクリックして、表示される説明をご覧ください。

**「端末の設定」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

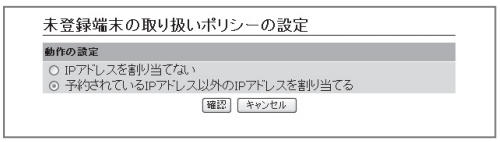
▶トップページの「DHCP認証」
▶「端末の管理」の「設定」
▶「端末の管理」の「新しい端末を登録する」欄の「登録」

# 未登録端末の扱いを指定する

「未登録端末の取り扱いポリシーの設定」画面で、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、LAN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。LAN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 ? をクリックして、表示される説明をご覧ください。

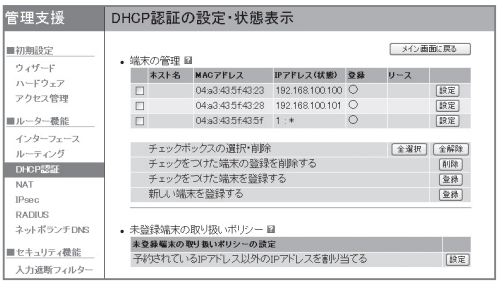
**「未登録端末の取り扱いポリシーの設定」画面を開くには**

管理者向けトップページから、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「DHCP認証」
▶「端末の管理」の「設定」
▶「未登録端末の取り扱いポリシー」の「設定」

# 端末の接続状態を確認する

「端末管理の設定・状態表示」画面で、端末の現在の状態を確認できます。




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

**「端末管理の設定・状態表示」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

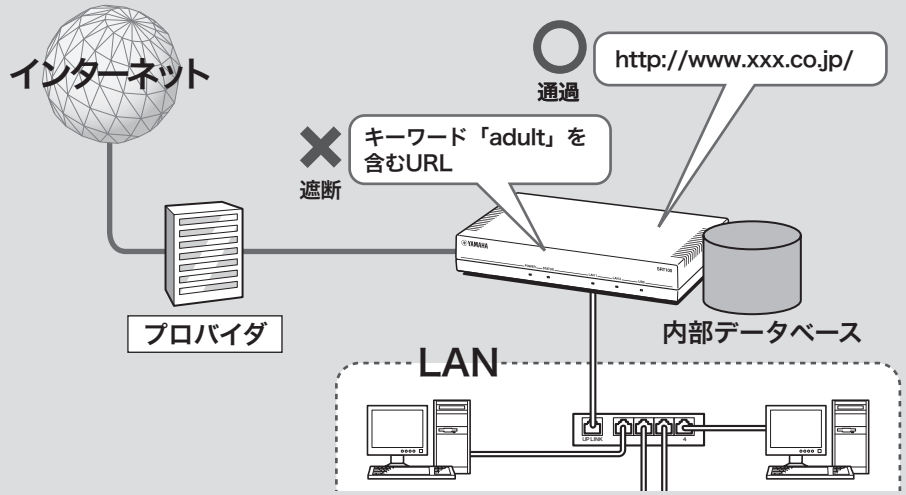
▶トップページの「DHCP認証」
▶「端末の管理」の「設定」

# 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。

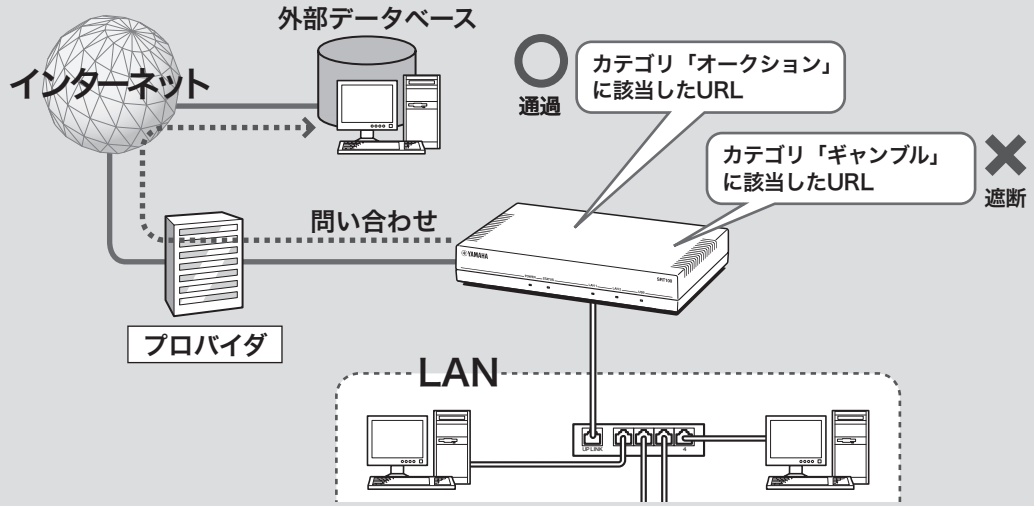
## 内部データベース参照型URLフィルター

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。



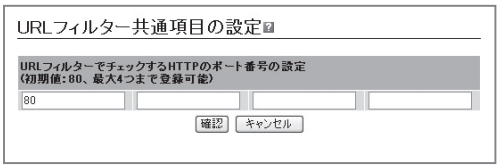

## 外部データベース参照型URLフィルター

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フィルターの対象となるポート番号を指定する

「URLフィルター共通項目の設定」画面で、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、最大4つまで指定できます。




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

**「URLフィルター共通項目の設定」画面を開くには**

管理者向けトップページから、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「URLフィルター」
▶「共通項目」の「設定」

# 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、WANへの上り方向(LANインターフェースのINやWANインターフェースのOUTなど)、つまりネットワーク内のクライアントからインターネットへ向かう通信にのみ機能します。

## 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フィルターの設定」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 ? 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フィルターの設定」画面を開くには**

管理者向けトップページから、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「URLフィルター」
▶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「追加」

## 外部データベース参照型URLフィルターを設定する

本製品から外部のURLフィルタリングサービス事業者のデータベースを参照して、アクセス制限を行うこともできます。インターフェースごとにフィルターを設定する際に任意のカテゴリを指定できるなど、より高度なフィルタリングを実現できます。

**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。

### 本製品で利用できるフィルタリングサービスについて

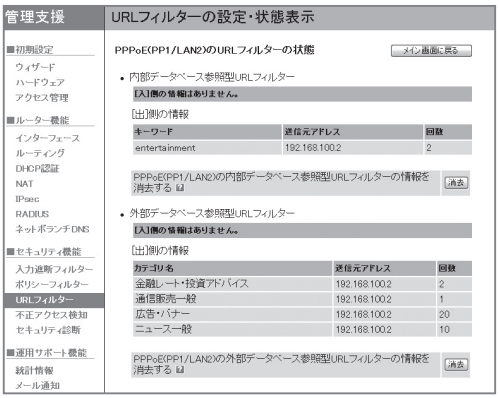
本製品で利用できるフィルタリングサービスおよび導入環境、価格などについて詳しくは、ヤマハルーターホームページ(http://NetVolante.jp/、http://www.rtpro.yamaha.co.jp/)をご覧の上、フィルタリングサービス事業者、もしくはフィルタリングサービスのお取扱い事業者まで直接お問い合わせください。

# URLフィルターの動作状態を確認する

「URLフィルターの設定・状態表示」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、debugレベルのSyslogにも出力されます(136ページ)。




### 「URLフィルターの設定・状態表示」画面を開くには

管理者向けトップページから、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「URLフィルター」

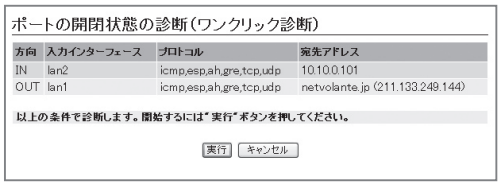
▶URLフィルターの状態を確認したいインターフェースの「状態」

# 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て、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どうかを確認できます。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種類を、目的に合わせて使い分けると便利です。

## IN/OUT方向の設定をまとめて検証する（ワンクリック診断）

「ポートの開閉状態の診断（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どうか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 ? をクリックして、表示される説明をご覧ください。

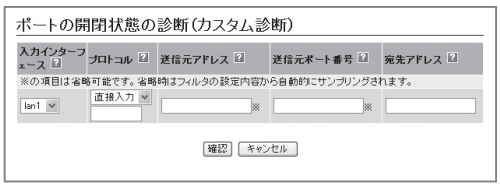
**「ポートの開閉状態の診断（ワンクリック診断）」画面を開くには**

管理者向けトップページから、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「セキュリティ診断」
▶「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）

「ポートの開閉状態の診断（カスタム）」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 ? をクリックして、表示される説明をご覧ください。

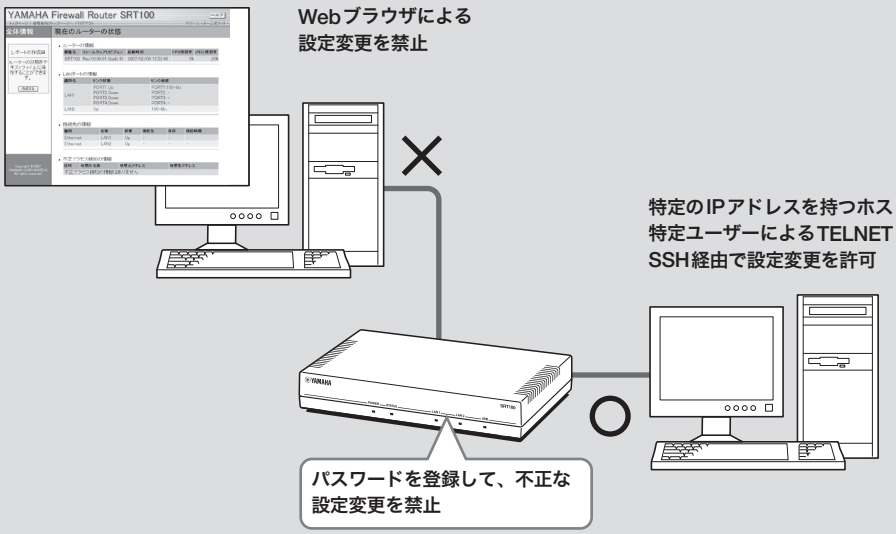
**「ポートの開閉状態の診断（カスタム診断）」画面を開くには**

管理者向けトップページから、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「セキュリティ診断」
▶「カスタム診断」の「実行」

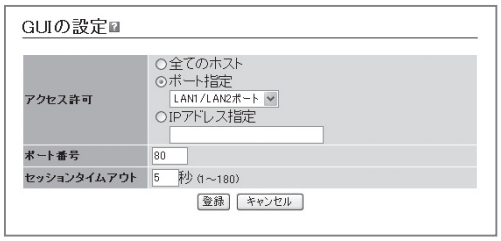
# 本製品の設定を変更できるホストを制限する

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、第三者が不正にルーター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。



## 設定画面を利用できるホストを制限する

「GUIの設定」画面で、Webブラウザ(HTTP)を使って本製品の設定を変更できるホストをIPアドレスで制限したり、本製品のポートに接続しているホストのみに制限したりできます。




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

**「GUIの設定」画面を開くには**

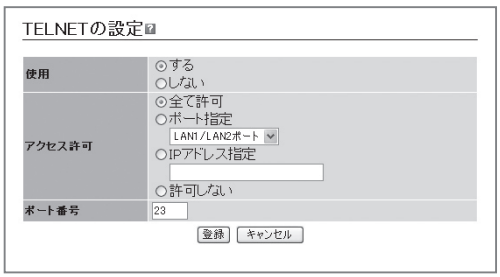
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「アクセス管理」

▶「GUIの設定」の「設定」

## TELNETを利用できるホストを制限する

「TELNETの設定」画面で、TELNET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IPアドレスで制限したり、本製品のポートに接続しているホストのみに制限したりできます。




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

**「TELNETの設定」画面を開くには**

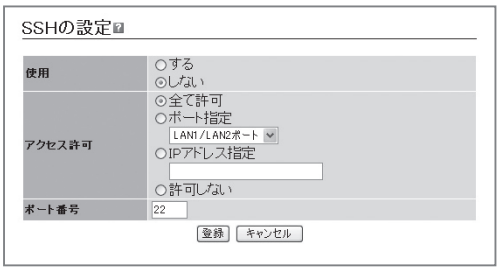
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「アクセス管理」

▶「TELNETの設定」の「設定」

## SSHを利用できるホストを制限する

「SSHの設定」画面で、SSH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IPアドレスで制限したり、本製品のポートに接続しているホストのみに制限したりできます。




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

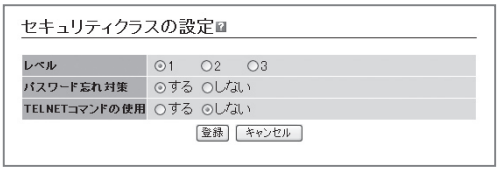
**「TELNETサーバーの設定」画面を開くには**

管理者向けトップページから、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「アクセス管理」
▶「SSHの設定」の「設定」

## セキュリティクラスを指定する

「セキュリティクラスの設定」画面で、本製品にログインできるアクセス方法を制限できます。




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

**「セキュリティクラスの設定」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

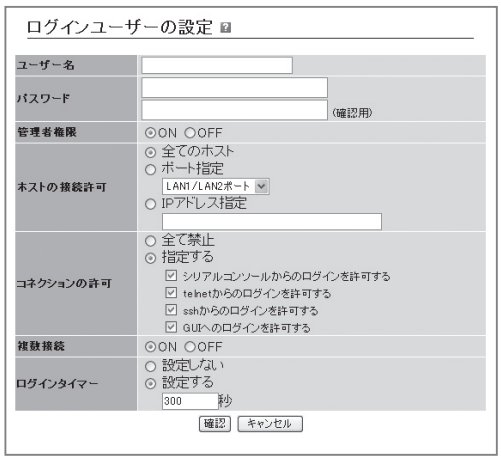
▶トップページの「アクセス管理」
▶「セキュリティクラスの設定」の「設定」

# 本製品にログインできるユーザーを登録する

「ログインユーザーの設定」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。

**ご注意**

- ここで設定するパスワードは一般ユーザーとしてトップページにアクセスするためのもので、初期設定ウィザードで設定した全ユーザー共通の管理者パスワードとは異なります。管理者パスワードを変更したい場合は、管理者向けトップページから「アクセス管理」–「パスワードの設定」の「設定」をクリックして、「パスワードの設定」画面で設定します。
- 設定画面を閉じる場合は、設定画面上部の「ログアウト」をクリックしてログアウトしてください。ログアウトせずにブラウザを終了すると、ログインタイマーが切れるまで、同じIPアドレスのパソコンから他のユーザーがログインできません。




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

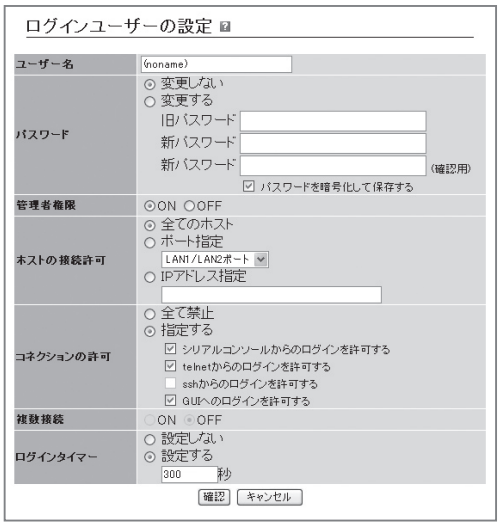
**「ログインユーザーの設定」画面を開くには**

管理者向けトップページから、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「アクセス管理」
▶「ログインユーザーの設定・状態表示」の「設定」
▶「新しいユーザーを追加する」の「追加」

## 無名ユーザーのアクセスを制限することもできます

本製品の工場出荷時に設定されている無名ユーザー（noname）の設定を「ログインユーザーの設定」画面で変更すると、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 ? をクリックして、表示される説明をご覧ください。

**「ログインユーザーの設定」画面で無名ユーザーの設定を変更するには**

管理者向けトップページから、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「アクセス管理」
▶「ログインユーザーの設定・状態表示」の「設定」
▶ユーザー名「(noname)」欄の「編集」

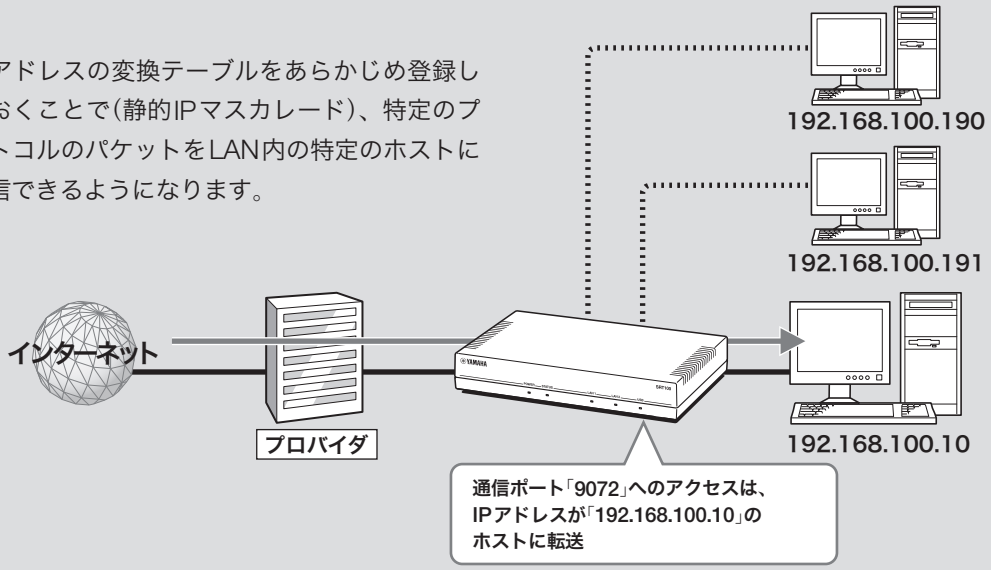
# グローバルIPアドレスが必要なサービスをLAN内で利用する

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ルーターのLAN側で利用しようとしても、正しく動作しない場合があります。以下の順序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。

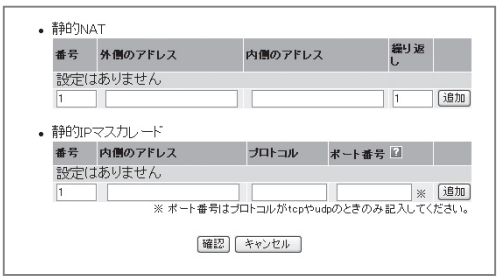
### 2. IPアドレスの変換テーブルを登録する

「変換ルールの設定」画面の「静的IPマスカレード」欄で、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 ? 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 ? をクリックして、表示される説明をご覧ください。




**「変換ルールの設定」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

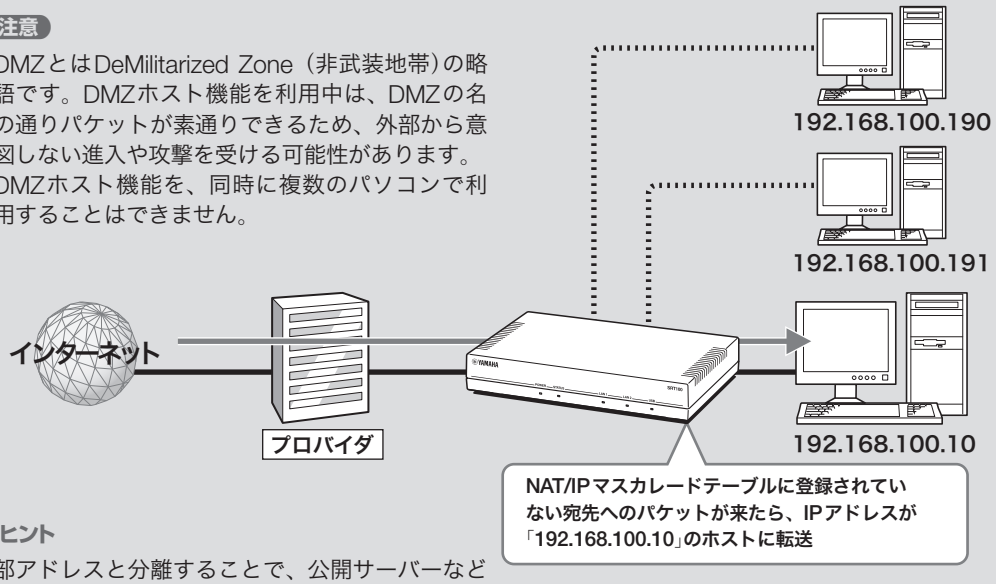
▶トップページの「NAT」
▶変換テーブルを登録したいインターフェースのの「設定」
▶「IPマスカレード」の「設定」

# 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進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、内側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

「変換ルールの設定」画面の「基本設定」欄で、変換ルールに該当しないパケットの処理として、「指定した端末に転送する」を選んでから、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 ? クリックして、表示される説明をご覧ください。

**「変換ルールの設定」画面を開くには**

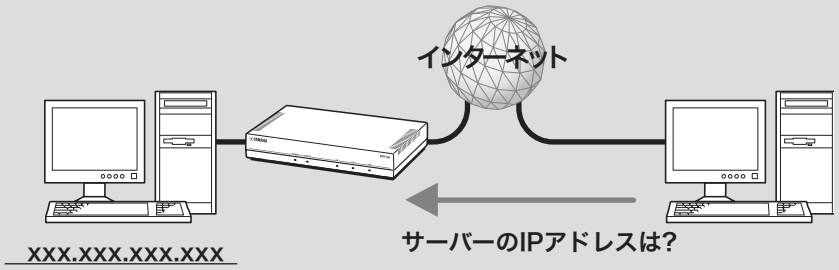
管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

▶トップページの「NAT」
▶変換テーブルを登録したいインターフェースの「設定」
▶「IPマスカレード」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?

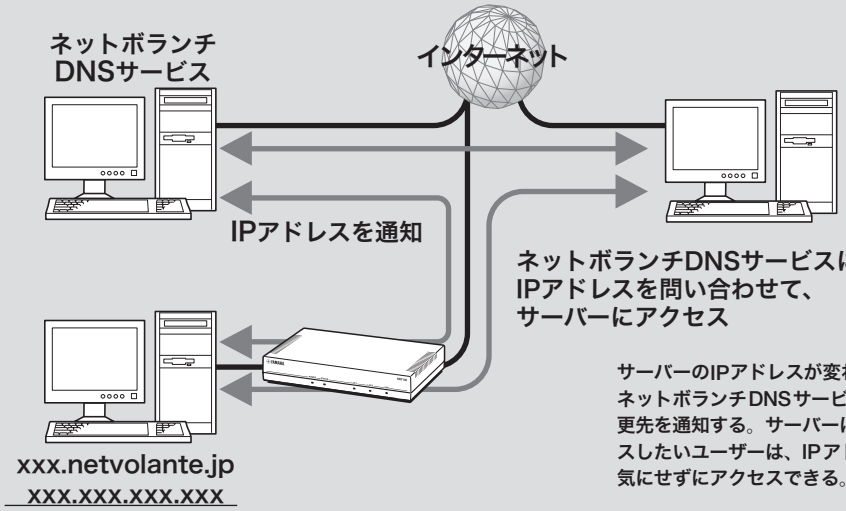
サーバーを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、相手のグローバルIPアドレスがわかっている必要があります。
しかし、インターネットに常時接続している場合でも、割り当てられるグローバルIPアドレスは再接続時または時間によって変更される場合があります。そのため、グローバルIPアドレスが固定で割り当てられない接続サービスを利用していると、サーバーを構築して公開することは困難でした。




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アドレスがサーバーへ通知されるため、固定のホスト名を持つことが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を利用してVPNを構築して、外部とデータをやり取りしたりできるようになります。




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**

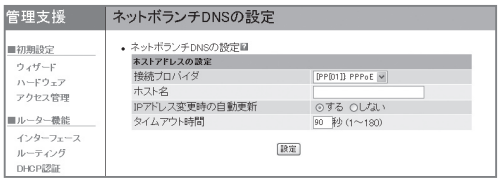
- ネットボランチDNSサービスは、端末型プロバイダ接続に対してのみ設定できます。ネットワーク型接続やLAN間接続には設定できません。なお、端末型CATVプロバイダ接続の設定でも、LAN2側IPアドレスが固定アドレスの場合は設定できません。
- ホストアドレスはルーター１台につき1つしか取得できません。
- 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ネットボランチDNSサービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミックDNSサーバーに登録することはできません。
- ネットボランチDNSサービスは、プロバイダからグローバル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の設定」画面を使用します。

**ご注意**

- ホストアドレスはルーター１台につき1つしか取得できません。
- 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 ? 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の設定」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

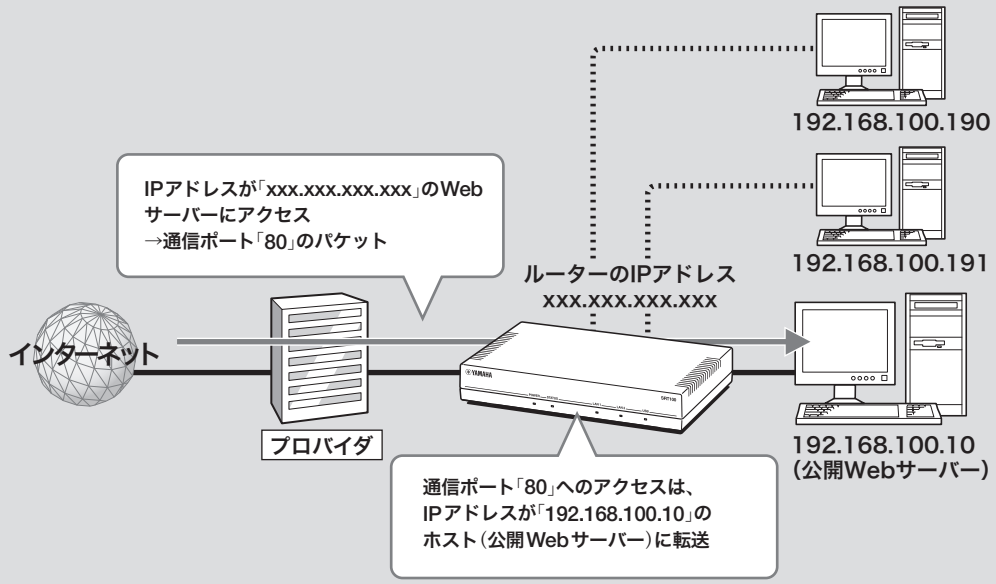
▶トップページの「ネットボランチDNS」

## 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設定を行ってください。セキュリティ設定が不十分の場合は、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。

**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」(126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。

**ルーターの設定**

- 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、次ページ)。
- アクセスを許可する設定に変更する(次ページ)。

**サーバーの設定**

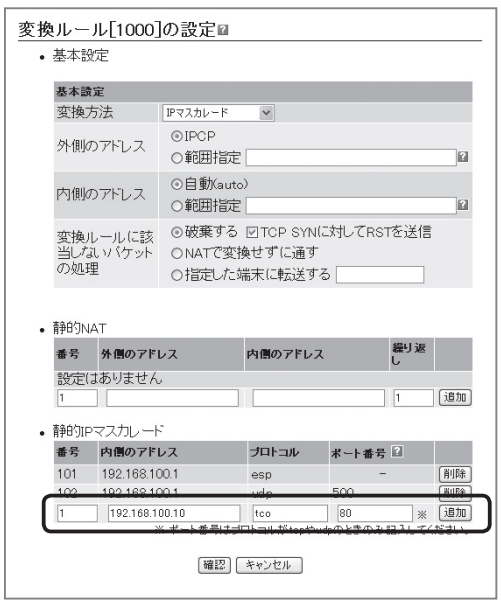
- パソコンのIPアドレスを設定する。
- WebやFTPなど、公開するサービスに合わせてサーバーソフトウェアの設定を変更する。

# IPアドレスの変換テーブルを登録する

「変換ルールの設定」画面の「静的IPマスカレード」欄で、通信プロトコルと公開したいサービスで使用するポート番号、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 ? 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。




(Webサーバーを公開する場合の例)

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

**「変換ルールの設定」画面を開くには**

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

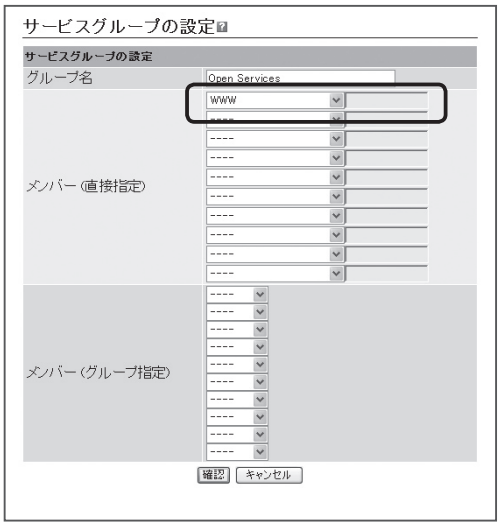
▶トップページの「NAT」
▶変換テーブルを登録したいインターフェースのの「設定」
▶「IPマスカレードの「設定」

# アクセスを許可する設定に変更する

サーバーに対するアクセスを許可するためのポリシーフィルターを設定します。この場合、LAN内のその他のパソコンに外部からアクセスすることはできません。

## 1.ユーザ定義サービスの「Open Services」設定を変更する

「Open Services」の「サービスグループの設定」画面で、公開したいサービスを「Open Services」のメンバーに指定します。




(Webサーバーを公開する場合の例)

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

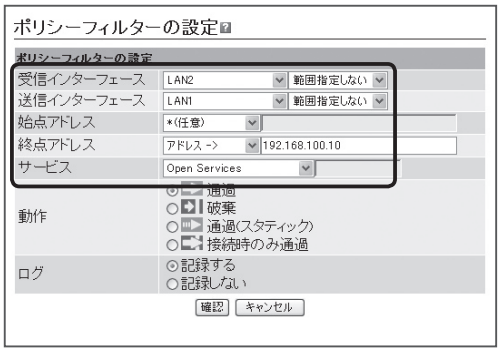
**「Open Services」の「サービスグループの設定」画面を開くには**

管理者向けトップページから、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「ポリシーフィルター」
▶グループとユーザー定義サービスの一覧の「詳細」
▶「サービスグループの設定」欄の「Open Services」の「設定」

## 2.ポリシーフィルタを変更する

「ポリシーフィルターの設定」画面で、設定を変更した「Open Services」グループに対するポリシーを変更します。公開するサーバーを限定するために、「終点アドレス」にIPアドレスを設定します。




（Webサーバーを公開する場合の例）

**ご注意**

公開する相手を限定したい場合は、「始点アドレス」欄に相手のIPアドレスを指定します。

設定内容について詳しくは、設定画面の ? 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**

管理者向けトップページから、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「ポリシーフィルター」
▶ポリシーを設定したいポリシーセット詳細欄で、「Open Services」が定義されている行の（右クリック）
▶表示されたポップアップメニューの「設定」

# 運用状況を統計グラフで確認する

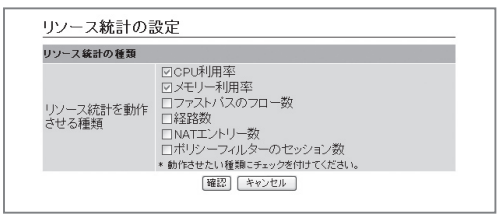
内部リソース状況と本製品で管理しているトラフィック状況について、統計情報を視覚的に表示できます。本製品を運用・管理するにあたっての基本的な情報として、役立てることができます。

## 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。

### リソース統計を表示する

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に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。



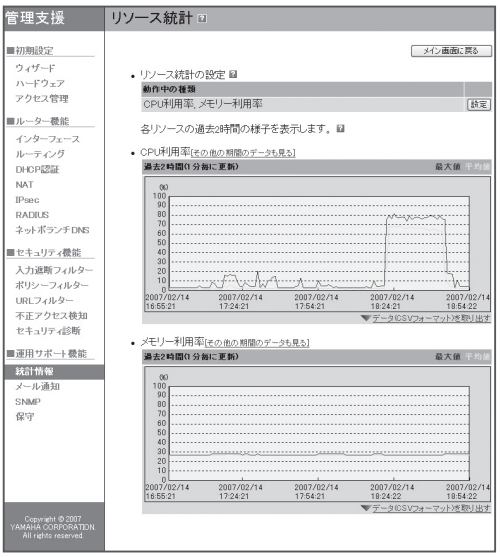

設定内容について詳しくは、設定画面の ? をクリックして、表示される説明をご覧ください。

**「リソース統計の設定」画面を開くには**

管理者向けトップページから、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「統計情報」
▶「リソース統計」の「表示」
▶「リソース統計の設定」の「設定」

### リソース統計の表示例



# 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表示する

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。

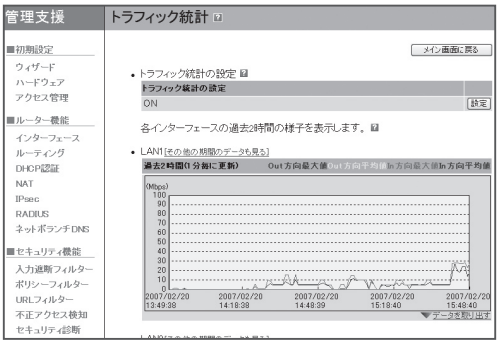

設定内容について詳しくは、設定画面の ? をクリックして、表示される説明をご覧ください。

**「トラフィック統計の設定」画面を開くには**

管理者向けトップページから、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「統計情報」
▶「トラフィック統計」の「表示」
▶「トラフィック統計の設定」の「設定」

## トラフィック統計の表示例



# 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」をご覧ください。

## QoS統計を表示する

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。

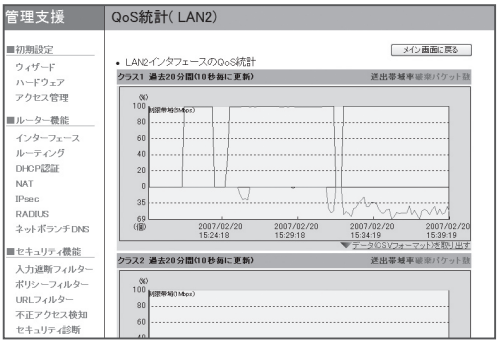

設定内容について詳しくは、設定画面の ? をクリックして、表示される説明をご覧ください。

### 「QoS統計の設定」画面を開くには

管理者向けトップページから、以下の順に設定画面のボタンをクリックします。

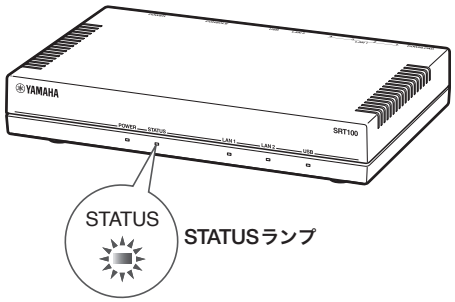
▶トップページの「統計情報」
▶「QoS統計」の「表示」
▶「QoS統計の設定」の「設定」

## QoS統計の表示例



# STATUSランプで通信状態を確認する

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どうか、本製品のSTATUSランプで確認できます。

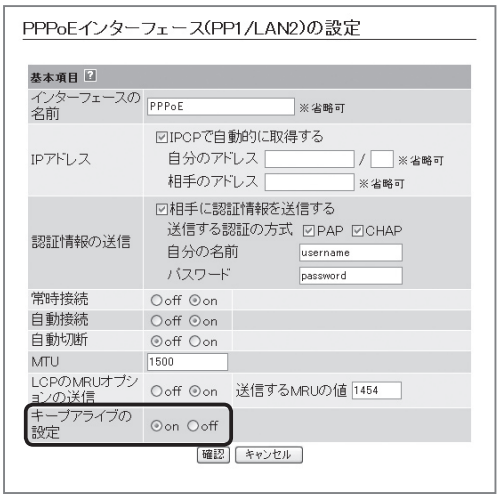



設定画面を表示せずに通信状態を確認できるので便利です。

**ヒント**

- 管理者向け設定画面からプロバイダとの接続やIPsecによるVPN接続、IPIPによるトンネル接続を設定する場合は、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どうかを確認するには、それぞれの接続の設定画面をご覧ください。

**「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ」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設定において、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」(144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。

# 本製品の状態を確認する

## 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。

**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、「コマンドの入力」画面(153ページ)に貼り付けます。

### 設定情報を画面で確認する

**1** **管理者向けトップページで「保守」をクリックする。**

「保守」画面が表示されます。

**2** **「設定の管理」–「設定を画面へ出力」欄の「実行」をクリックする。**

本製品の全設定情報が表示されます。

```
#         SRT100 Rev.10.00.01 (build 9) (Thu Jan 25 16:21:53 2007)
#                 MAC Address : 00:a0:de:07:fa:89, 00:a0:de:07:fa:8a
#                 Memory 32Mbytes, 2LAN
#                 main:  MINUET ver=c0 serial=X00000329 MAC-Address=00:a0:de:07
login password encrypted *
administrator password encrypted *
ip route default gateway pp 1
ip lan1 address 192.168.100.1/24
pp select 1
 description pp PRY/PPPoE/0:PPPoE
 pp keepalive interval 30 retry-interval=30 count=12
 pp always-on on
 pppoe use lan2
 pppoe auto disconnect off
 pp auth accept pap chap
 pp auth myname username password
 ppp lcp mru on 1454
 ppp ipcp ipaddress on
 ppp ipcp msext on
 ppp ccp type none
 ip pp inbound filter list 1001 1002 1003 1004 1005 1006 1007 1008
 ip pp nat descriptor 1000
 pp enable 1
ip inbound filter 1001 reject-nolog * * tcp,udp * 135
ip inbound filter 1002 reject-nolog * * tcp,udp 135 *
ip inbound filter 1003 reject-nolog * * tcp,udp * netbios_ns-netbios_ssn
```

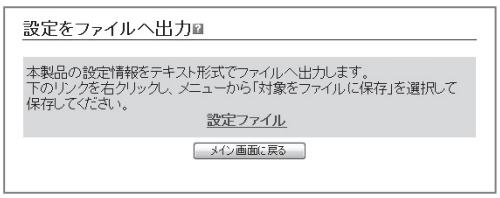
### 設定情報をファイルに出力する

**1** **管理者向けトップページで「保守」をクリックする。**

「保守」画面が表示されます。

**2** **「設定の管理」–「設定をファイルへ出力」欄の「実行」をクリックする。**

「設定をファイルへ出力」画面が表示されます。




**3** **「設定ファイル」を右クリックして「対象をファイルに保存」を選び、設定情報を保存する。**

# 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。

**ご注意**

本製品の電源を切った場合には、ログファイルの内容は全て消去されます。

**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。

## ログを画面で確認する

**1 管理者向けトップページで「保守」をクリックする。**

「保守」画面が表示されます。

**2 「SYSLOGの管理」–「SYSLOGを画面へ出力」欄の「実行」をクリックする。**

本製品のログが表示されます。

```
2007/02/04 20:14:56: [PCI] Initializing PCI bus failed.
2007/02/04 20:15:01: Power-on boot
2007/02/04 20:15:01: SRT100 Rev.10.00.01 (build 9) (Thu Jan 25 16:21:53 2007) s
2007/02/04 20:15:01: main:  MINUET ver=c0 serial=X00000329 MAC-Address=00:a0:de
2007/02/04 20:15:20: Login failed for Serial
2007/02/04 20:15:43: Login succeeded for Serial
2007/02/04 20:15:55: 'administrator' succeeded for Serial user
2007/02/04 20:16:21: Logout from Serial
2007/02/04 20:16:21: Restarting router
2007/02/04 20:16:40: [PCI] Initializing PCI bus failed.
2007/02/04 20:16:45: Restart by cold start command
2007/02/04 20:16:45: SRT100 Rev.10.00.01 (build 9) (Thu Jan 25 16:21:53 2007) s
2007/02/04 20:16:45: main:  MINUET ver=c0 serial=X00000329 MAC-Address=00:a0:de
2007/02/04 20:37:10: LAN1: PORT1 link up (10BASE-T Half Duplex)
```

## ログの設定を変更する

「SYSLOGの設定」画面で行います。

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

**「SYSLOGの設定」画面を開くには**

管理者向けトップページから、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「保守」

▶「SYSLOGの管理」の「設定」

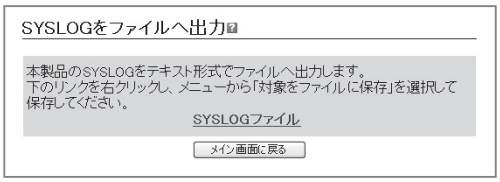
## ログをファイルに出力する

**1 管理者向けトップページで「保守」をクリックする。**

「保守」画面が表示されます。

**2 「SYSLOGの管理」–「SYSLOGをファイルへ出力」欄の「実行」をクリックする。**

「SYSLOGをファイルへ出力」画面が表示されます。




**3 「SYSLOGファイル」を右クリックして「対象をファイルに保存」を選び、設定情報を保存する。**

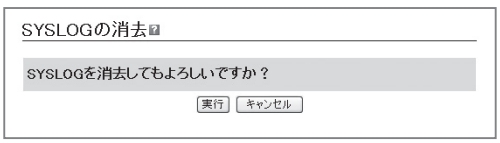
## ログを削除する

**1 管理者向けトップページで「保守」をクリックする。**

「保守」画面が表示されます。

**2 「SYSLOGの管理」–「SYSLOGの消去」欄の「実行」をクリックする。**

「SYSLOGの消去」画面が表示されます。




**3 「実行」をクリックする。**

**4 「メイン画面に戻る」をクリックする。**

# USBメモリに設定情報とログを保存する

市販のUSBメモリ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**

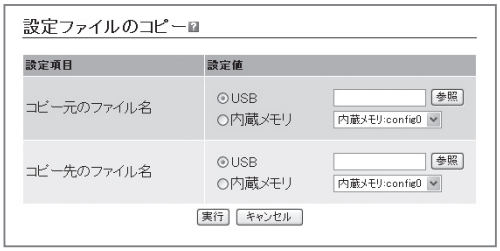
- FATまたはFAT32形式でフォーマットされていないUSBメモリは、本製品で使用できません。
- USBハブを介して、複数のUSBメモリを本製品に接続することはできません。
- USB延長ケーブルは、種類によっては動作しないことがあります。本製品のUSBポートに直接挿入してご使用ください。
- 本製品のUSBランプが点灯／点滅している間は、USBメモリを取り外さないでください。USBメモリ内のデータを破損することがあります。USBボタンを2秒間押し続けて、USBランプが消灯していることを確認してからUSBメモリを取り外してください。

## USBメモリに本製品の設定情報を保存する

**1 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**2 「設定ファイルのコピー」画面の「コピー元のファイル名」で、「内蔵メモリ」をクリックして選ぶ。**




**「設定ファイルのコピー」画面を開くには**

管理者向けトップページから、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「保守」

▶「設定ファイルのコピー」の「実行」

**3 「コピー先のファイル名」で「USB」をクリックして選んでから、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。**

本製品の設定ファイルがUSBメモリに書き込まれます。

**5 USBボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

**6 USBメモリを取り外す。**

**ご注意**

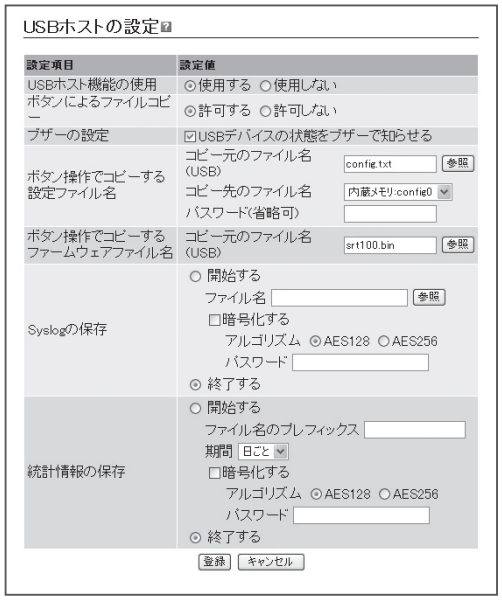
USBメモリへの設定ファイルの保存に失敗した場合は、「USBデバイスが使用できない」(170ページ)をご確認ください。

## USBメモリに本製品のログを保存する

**1 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**2 「USBホストの設定」画面の「Syslogの保存」欄で「開始する」を選んでから、ログの保存先とファイル名を指定する。**




**「USBホストの設定」画面を開くには**

管理者向けトップページから、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「保守」

▶「USBホスト機能の設定・状態表示」の「設定」

**3 「登録」をクリックする。**

本製品のログが、USB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USB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」(次ページ)をご覧ください。

**4 ログの保存を停止する場合は、「USBホストの設定」画面の「Syslogの保存」欄で「終了する」を選んでから、「登録」をクリックする。**

**5 USBボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

**6 USBメモリを取り外す。**

**ご注意**

USBメモリへのログ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」(170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メモリ内には以下のログファイルが生成されます。

- ログが現在書き出しされているファイル(mainファイル)：USBホスト機能の設定」画面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：上記ファイル名で、拡張子が「.bak」のファイル

### ログの容量

USBメモリ内の空き容量から、設定ファイル保存用の容量を除いた値の1/2が、ログファイルの最大容量になります。mainファイルの容量が最大容量を超えると、ログの内容は自動的にバックアップファイルに退避されます。それ以降に発生したログは、新しく生成されたmainファイルに書き込まれます。

**ご注意**

書き込み途中にUSBメモリ内の空き容量が変化して、mainファイルに上限サイズまで書き込めなかった場合は、その時点でのmainファイルをバックアップファイルとして退避させ、使用領域の再計算が行われます。

### バックアップファイルの制限

バックアップファイルは1つしか存在できません。そのため、ログの容量が再度上限に達してバックアップファイルが新たに生成されると、それまでに存在したバックアップファイルは上書きされてしまいますのでご注意ください。

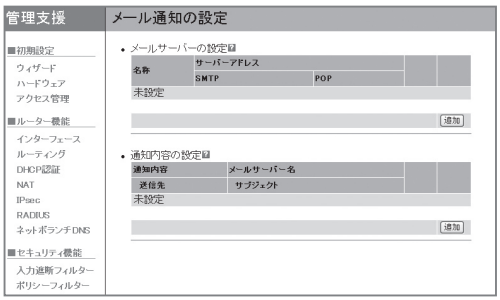
# 本製品の状態をメールで通知する

あらかじめ設定した条件を満たした場合に、本製品の状態をメールで通知するように設定できます。

## メールサーバーを登録する

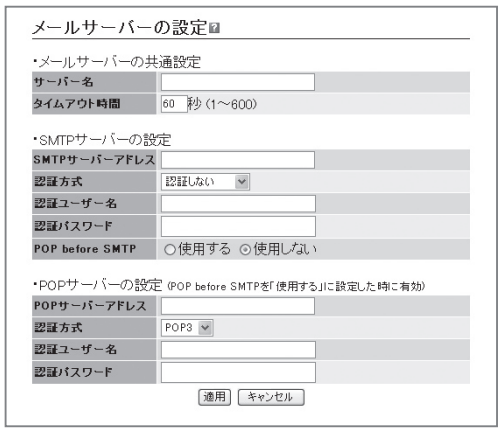
**1** **管理者向けトップページの「メール通知」をクリックする。**

「メール通知の設定」画面が表示されます。




**2** **「メールサーバーの設定」欄で、「追加」をクリックする。**

「メールサーバーの設定」画面が表示されます。




**3** **「サーバー名」欄に、登録するメールサーバーの名前を入力する。**

**4** **「タイムアウト時間」欄に、サーバーへの接続待ち時間を入力する。**

サーバーへの接続がタイムアウトすると、一定時間後に3回まで再送が行なわれます。

**5** **「SMTPサーバーアドレス」欄に、送信サーバー（SMTPサーバー）のアドレスを入力する。**

**6** **メール送信時にSMTP認証が必要な場合は、「認証方式」欄で、メール送信時の認証方式を指定する。**

**7** **「認証ユーザー名」欄に、メールアカウントを入力する。**

**8** **「認証パスワード」欄に、手順7で指定したアカウントのパスワードを入力する。**

**9** **メール送信時にPOP before SMTPを使用する場合は、「POP before SMTP」欄の「使用する」をクリックする。**

POP before SMTPを使用しない場合は、手順10～13の操作は不要です。

**10** **「POPサーバーアドレス」欄に、受信サーバー（POPサーバー）のアドレスを入力する。**

**11** **「認証方式」欄で、メール受信時の認証方式を指定する。**

**12** **「認証ユーザー名」欄に、メールアカウントを入力する。**

**13** **「認証パスワード」欄に、手順12で指定したアカウントのパスワードを入力する。**

**14** **「適用」をクリックする。**

確認画面が表示されます。

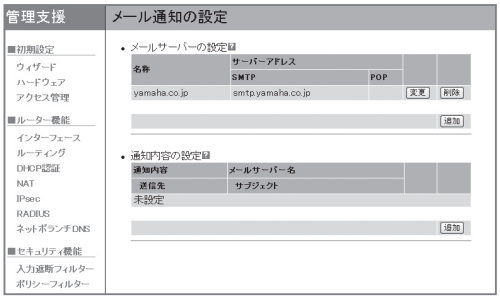
**15** **「メイン画面に戻る」をクリックする。**

「メール通知の設定」画面に戻ります。

## メールの送信内容を指定する

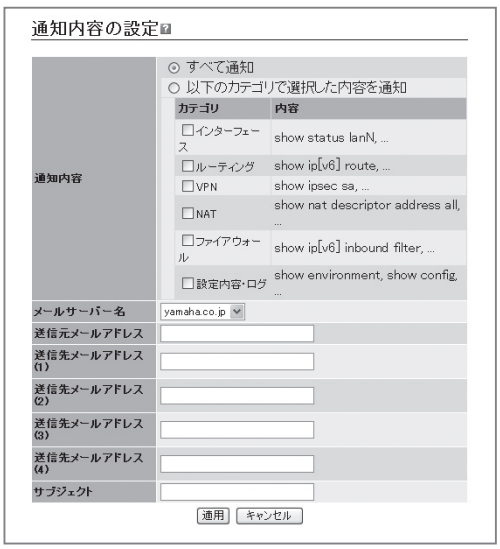
**1** **管理者向けトップページの「メール通知」をクリックする。**

「メール通知の設定」画面が表示されます。




**2** **「通知内容の設定」欄で、「追加」をクリックする。**

「通知内容の設定」画面が表示されます。




**3** **「通知内容」欄で、メールの送信内容を指定する。**

- **すべての情報を送信する場合**：「すべて通知」をクリックして選びます。
- **特定の情報だけを送信する場合**：「以下のカテゴリで選択した内容を通知」をクリックして選んでから、送信したい情報にチェックを付けます。

**4** **「メールサーバー名」欄で、登録したメールサーバーを指定する。**

**5** **「送信元メールアドレス」欄に、状態メールの差出人メールアドレスを入力する。**

送信元メールアドレスは、サーバーによる送信失敗時のエラーメールの通知先および返信時の送信先メールアドレスとして使用されることがあります。

**6** **「送信先メールアドレス」欄に、不正アクセス検知メールの宛先メールアドレスを入力する。**

**7** **「サブジェクト」欄に、不正アクセス検知メールの題名を入力する。**

**8** **「適用」をクリックする。**

確認画面が表示されます。

**9** **「メイン画面に戻る」をクリックする。**

「メール通知の設定」画面に戻ります。

# 本製品の設定ファイルを管理する

## 本製品の起動時に設定ファイルを切り替える

本製品は設定ファイル(config)を最大5つ持つことができ、CONSOLEポートから設定する場合にのみそれらのファイルを切り替えることができます。

**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。**

接続およびパソコンの設定については、154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。**

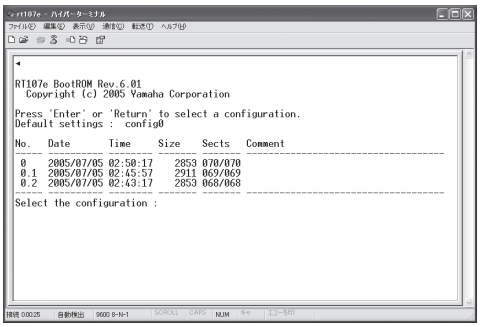
詳しくは155ページをご覧ください。

**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ファームウェア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。**

設定ファイル待ち状態になります。




ヒント

「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** **0～4.2のうちで、使用したい設定ファイル名を指定してからEnterキーを押す。**

指定した設定ファイルを使用して、本製品が起動します。

ご注意

- 本製品の電源を入れ直す場合には、電源を切ってから再度電源を入れるまでの間に、10秒以上の時間をおいてください。
- CONSOLEポートにパソコンが接続されていない場合や、接続されていてもパソコンからのキー入力が無い場合には、10秒後にデフォルト設定ファイルで自動的に起動します。
  - –工場出荷設定では、設定ファイル0で起動します。
  - –set-default-configコマンドが設定されている場合は、指定されたデフォルト設定ファイルで起動します。
  - –デフォルト設定ファイルが存在しない場合は、「何も設定されていない」状態で起動します。

# 設定ファイル管理上のご注意

## saveコマンドと設定ファイルの関係

本製品は5個の設定ファイル(config0～config4)を内蔵の不揮発性メモリに保持して、起動時に切り替えて使用できます。また、これらの設定ファイルには最大2個の退避ファイル(「configX.1」および「configX.2」と表示されるバックアップファイル)を保持できます。

退避ファイルは、saveコマンドを実行するごとに自動生成されます。saveコマンドを実行する場合には、現在動作中の設定ファイルの系列を把握しておくよう、ご注意ください。

### 例:config1で動作中にsaveコマンドを実行した場合の動作

- 不揮発性メモリ上のconfig1の内容が退避ファイルconfig1.1となります。
- 現在の動作環境設定がconifg1に上書きされます。
- config1.1がすでに存在する場合は、config1.1の内容はconfig1.2に上書きされます。
  config1.2がすでに存在する場合は、saveコマンド実行に伴ってconfig1.2の内容は破棄されます(config1.1の内容で上書きされます)。

**ヒント**

- 現在動作中の設定ファイルの番号を知りたい場合には、show environmentコマンドを実行します。
- すべての設定ファイルと退避ファイルの一覧を表示させるには、show config listコマンドを実行します。

## 設定ファイルを途中で切り替えたい場合は

restartコマンドを実行して本製品の起動プロセスに戻ってから、起動に使用する設定ファイルを選択できます。

**ご注意**

現在の動作環境が不揮発性メモリに保存されていない場合は、restartコマンド入力時に設定を保存するかどうか確認を求められます。ここで設定を保存すると、saveコマンド実行時と同様に退避ファイルが生成・上書きされます。

## 通常使用する設定ファイルを指定することもできます

set-default-configコマンドを使用して、起動プロセスにおいて設定ファイルを指定しない場合に自動選択される設定ファイル(デフォルト設定ファイル)を指定できます。TELNETで本製品にアクセスしている場合は起動プロセスで設定ファイルを指定できませんので、特定の設定ファイルで起動させたいときはこのコマンドを使用します。

**ご注意**

- デフォルト設定ファイルとして退避ファイルを指定している場合は、起動後にsaveコマンドを実行すると現在の動作環境が設定ファイルに上書きされてしまいます。必要であれば、使用したい設定ファイルの内容を別の設定ファイルにコピーしてから、saveコマンドを実行するようにしてください。
- 設定ファイル、退避ファイルを別の番号系列の設定ファイルに保存または削除する場合には、copy config、delete configコマンドを使用します。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。

# 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**

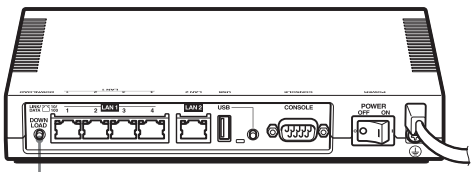
- リビジョンアップを始めたら、完了して本製品が再起動するまで他の操作は絶対しないでください。万一、中断したときは本製品が使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- リビジョンアップ中は、STATUS、LAN1、LAN2ランプが順番に点灯します。
- リビジョンアップが完了すると、本製品は自動的に再起動されるため、すべての通信が切断されます。
- リビジョンアップ中は、絶対にケーブルを抜かないでください。ルーターが使えなくなり、持ち込み修理が必要となる場合があります。
- 管理者向け設定画面の「HTTPリビジョンアップの実行」画面では、正式にリリースされたバージ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、管理者向け設定画面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**

管理者向け設定画面の「HTTPリビジョンアップの設定」画面(次ページ)で、「リビジョンダウンの許可」を「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

「HTTPリビジョンアップの設定」画面で「DOWNLOADボタンの使用」を「する」に設定している場合は、本製品背面のDOWNLOADボタンを3秒間押し続けることで、リビジョンアップを実行できます。




DOWNLOADボタン

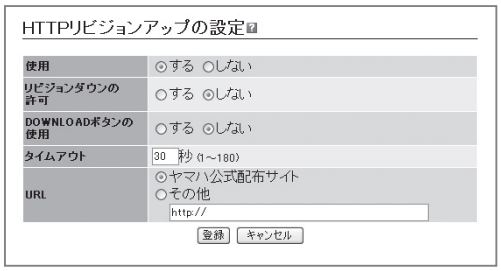
**ヒント**

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。

- ファームウェアをダウンロードしている間は、STATUSランプが点滅します。
- 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、STATUS、LAN1、LAN2、USBランプが順番に点灯します。
- ダウンロードやリビジョンアップに失敗した場合は、STATUSランプが点灯します。DOWNLOADボタンを1秒間押して、点灯を解除してください。

## DOWNLOADボタンによるリビジョンアップを許可する

「HTTPリビジョンアップの設定」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、「DOWNLOADボタンの使用」を「する」に設定します。

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

**「HTTPリビジョンアップの設定」画面を開くには**

管理者向けトップページから、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「保守」

▶「HTTPリビジョンアップ」の「変更」

## DOWNLOADボタンを押してリビジョンアップする

DOWNLOADボタンを押すと、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あった場合は、自動的にファームウェアをダウンロードしてから、リビジョンアップを実行します。

**ご注意**

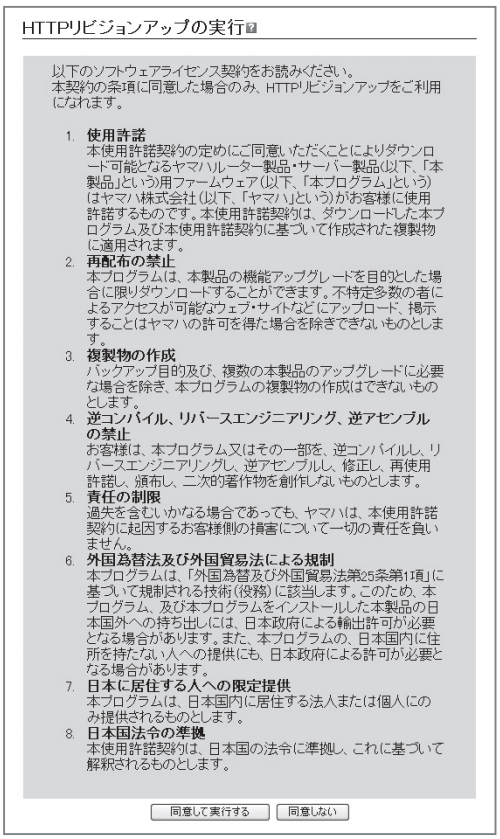
- ファームウェアのダウンロードまたはリビジョンアップに失敗すると、STATUSランプが点灯します。その場合はDOWNLOADボタンを1秒間押すと、STATUSランプが消灯します。
- ファームウェアのダウンロード、またはリビジョンアップに失敗した場合は、「DOWNLOADボタンが機能しない」(169ページ)をご確認ください。

**リビジョンアップが終了すると**

本製品が再起動します。

## 管理者向け設定画面でリビジョンアップする

「HTTPリビジョンアップの実行」画面で行います。




「同意して実行する」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あった場合は、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を実行します。

設定内容について詳しくは、設定画面の ? 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設定」画面で「リビジョンダウンの許可」を「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。

**「HTTPリビジョンアップの実行」画面を開くには**

管理者向けトップページから、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「保守」

▶「HTTPリビジョンアップ」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。

管理者向けトップページの「ルーターの情報」欄に、リビジョン番号が表示されます。リビジョン番号が更新されていることを確認してください。

# USBメモリから リビジョンアップする

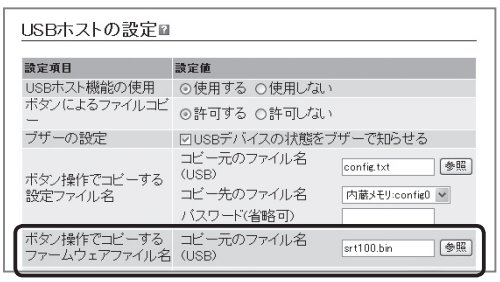
市販のUSBメモリに保存したファームウェアを本製品に読み込ませて、リビジョンアップできます。ファームウェアのバージョンを管理したり、複数台の本製品のファームウェアを変更したい場合などに便利です。

**ご注意**

- FATまたはFAT32形式でフォーマットされていないUSBメモリは、本製品で使用できません。
- USBハブを介して、複数のUSBメモリ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。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ランプが点灯／点滅している間は、USBメモリを取り外さないでください。USBメモリ内のデータを破損することがあります。USBボタンを2秒間押し続けて、USBランプが消灯していることを確認してからUSBメモリを取り外してください。

## USB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

「USBホストの設定」画面の「ボタン操作でコピーする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。




**「USBホストの設定」画面を開くには**

管理者向けトップページから、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「保守」

▶「USBホスト機能の設定・状態表示」の「設定」

## USBボタンを押してリビジョンアップを実行する

**1 「USBホストの設定」画面の「ボタン操作でコピーする設定ファイル名」欄で指定したファイル名のファームウェアを用意して、パソコンなどを使ってUSBメモリにコピーする。**

**2 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**3 USB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、リビジョンアップ動作が始まります。

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。

**ヒント**

「USBホストの設定」画面の「ボタン操作でコピーする設定ファイル名」欄で指定したファイル名の設定ファイルが同時に存在する場合は、設定ファイルのコピーが先に始まります。

**4 USBボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

**5 USBメモリを取り外す。**

**ご注意**

USB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」(170ページ)をご確認ください。

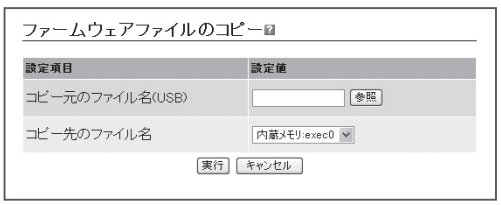
## 本製品の設定画面から USBメモリ内のファームウェアで リビジョンアップする

**1 ファームウェアを用意して、パソコンなどを使ってUSBメモリにコピーする。**

**2 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**3 「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（USB）」で「参照」をクリックして、リビジョンアップに使用するファームウェアファイルを指定する。**




**「ファームウェアファイルのコピー」画面を開くには**

管理者向けトップページから、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「保守」

▶「ファームウェアファイルのコピー」の「実行」

**ご注意**

本製品で管理できるファームウェアは1つだけです。「コピー先のファイル名」欄で、コピー先を指定することはできません。

**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、リビジョンアップ動作が始まります。

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。

**6 USBボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

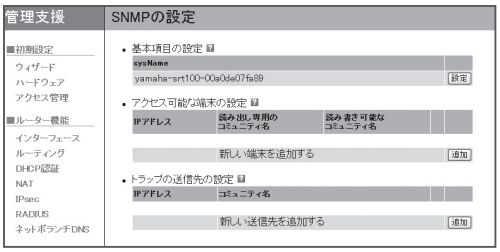
**7 USBメモリを取り外す。**

**ご注意**

USB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」（170ページ）をご確認ください。

# SNMPで本製品を管理する

本製品はRFC1157（SNMP、Simple Network Management Protocol）およびRFC1213（MIB-II）準拠の機能を搭載しています。「SNMPの設定」画面でSNMPの設定を行うことで、SNMPクライアントに対してネットワーク管理情報を監視して、必要に応じて変更することができます。




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

**「SNMPの設定」画面を開くには**

管理者向けトップページから、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「SNMP」

# コンソールコマンドで本製品の設定を変更する

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またはSSH経由で設定を変更するだけでなく、管理者向け設定画面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、お使いの環境用のTELNETまたは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、ルーター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、より詳しい設定が行えます。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。管理者向け設定画面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どうか、必ずご確認ください。

**ヒント**

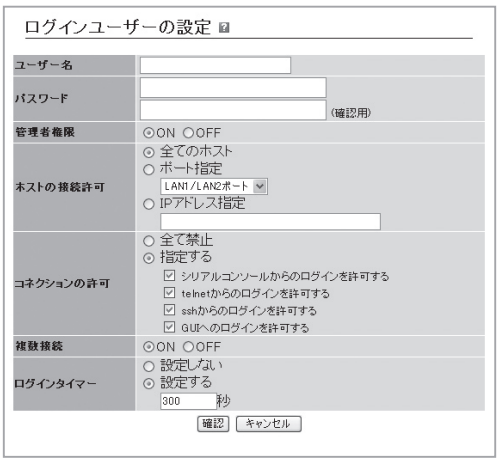
- コンソールコマンドの詳細については、「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。
- 本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、本製品をコンソールコマンドで設定することもできます(154ページ)。

## TELNET、SSHでコンソールコマンドを使用する

LAN1ポートに接続しているパソコンからTELNETまたはSSH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。

### TELNET、SSHのユーザーを登録する

「ログインユーザーの設定」画面でTELNETまたは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ログインできますが(無名ユーザー)、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 ? をクリックして、表示される説明をご覧ください。

**「ログインユーザーの設定」画面を開くには**

管理者向けトップページから、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「アクセス管理」
▶「ログインユーザーの設定・状態表示」の「設定」
▶「新しいユーザーを追加する」の「追加」

## 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、「SSHの設定」画面の「使用」欄で設定を「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 ? をクリックして、表示される説明をご覧ください。

**「SSHの設定」画面を開くには**

管理者向けトップページから、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「アクセス管理」

▶「SSHの設定」の「設定」

## TELNET、SSHで接続する

パソコンからの接続について、Windows標準のTELNETを使用する場合を例に説明します。SSHについてはご使用になるSSHソフトウェアの使用方法に従ってください。

**ご注意**

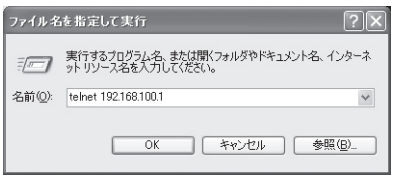
Windows Vistaでは、Windows標準のTELNETを使用するためには、Windowsの設定を変更する必要があります。詳しくは、「Windows VistaでTELNETを使用する場合は」(153ページ)をご覧ください。

**1 「スタート」メニューから「ファイル名を指定して実行」を選ぶ。**

Windows Vistaの場合は、「スタート」メニューから「すべてのプログラム」–「アクセサリ」–「ファイル名を指定して実行」を選びます。

**2 「telnet 192.168.100.1」と入力してから、「OK」をクリックする。**

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(前ページで設定したパスワード)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(TELNET)**

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や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:」と表示されるので、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(TELNET)**

「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。

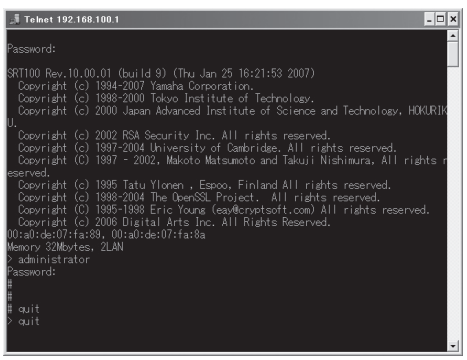
**ヒント**

- 「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、管理者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。**

## Windows VistaでTELNETを使用する場合は

Windows Vistaでは、Windows標準のTELNETを使用するためには、Windowsの設定を変更する必要があります。

**1** **「スタート」メニューから「コントロール パネル」を選ぶ。**

「コントロール パネル」画面が表示されます。

**2** **「プログラム」をクリックする。**

「プログラム」画面が表示されます。

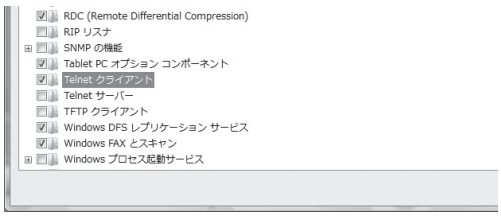
**3** **「プログラムと機能」欄の「Windowsの機能の有効化または無効化」をクリックする。**


「ユーザーアカウント制御」画面が表示されます。

**4** **「続行」をクリックする。**

「Windowsの機能」画面が表示されます。

**5** **「Telnetクライアント」をクリックしてチェックを付けてから、「OK」をクリックする。**




TELNETソフトウェアがインストールされ、Windows XP同様の手順(151ページ)で利用できるようになります。

# 管理者向け設定画面でコンソールコマンドを使用する

「コマンドの入力」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 ? をクリックして、表示される説明をご覧ください。

**「コマンドの入力」画面を開くには**

管理者向けトップページから、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「保守」

▶「設定の管理」–「コマンドの入力」欄の「実行」

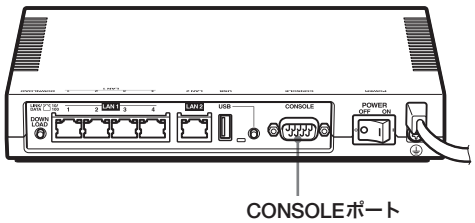
# CONSOLEポートから設定する

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。

- 管理者向け設定画面にパスワードを設定してTELNETでの設定を禁止しておけば(121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、セキュリティを強化するために役立ちます。
- 本製品に保存されている複数の設定ファイルから、どの設定で起動するのかをターミナルソフトウェアを使用してパソコンから指定することもできます。

## 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。




**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。**

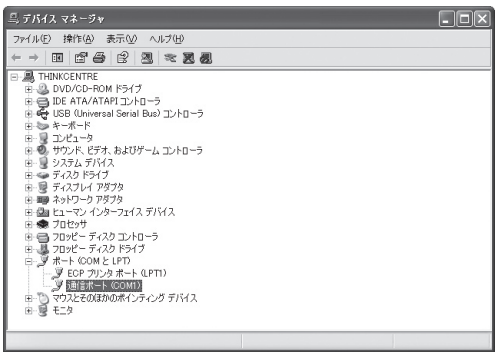
「システムのプロパティ」画面が表示されます。

**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。**

### Windows Vistaの場合は

「デバイス マネージャ」画面を表示するには、「コントロールパネル」画面で「システムとメンテナンス」をクリックしてから、「デバイスマネージャ」をクリックしてください。

## 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標準の「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**

- Windows Vistaには「ハイパーターミナル」などの標準通信ソフトウェアが用意されていません。シリアルポート(RS-232C)経由の通信に対応する、市販のソフトウェアを別途ご用意ください。なお、ボーレートやデータビット、パリティなどRS-232Cの通信設定については、手順4と同様に設定してください。
- コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。管理者向け設定画面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どうか、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。

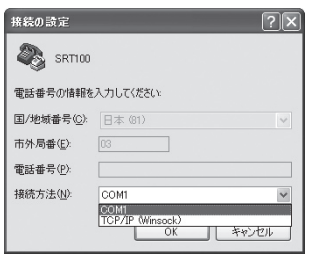
**1 「スタート」メニューから「すべてのプログラム」–「アクセサリ」–「通信」–「ハイパーターミナル」をクリックする。**

「接続の設定」画面が表示されます。

**2 「名前」欄に接続名を入力する。**

接続名は自由に設定してください。

**3 「接続方法」で前ページ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。**



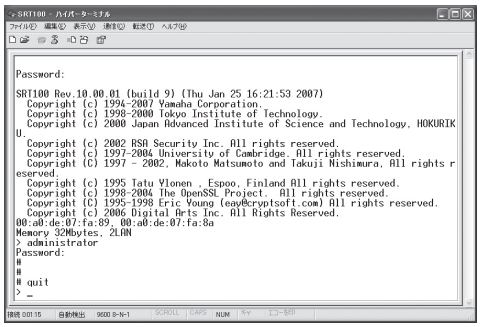

「COMxのプロパティ」画面が表示されます。

**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、SSHで接続する」(151ページ)の手順3以降と同じです。

# USBメモリから本製品の設定を変更する

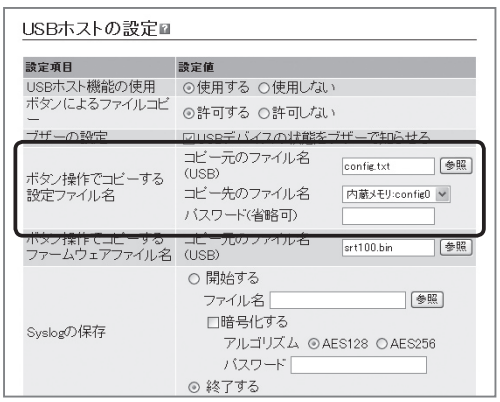
市販のUSBメモリに保存した設定ファイルを本製品に読み込ませて、設定を変更できます。複数台の本製品の設定を変更したい場合などに便利です。

**ご注意**

- FATまたはFAT32形式でフォーマットされていないUSBメモリは、本製品で使用できません。
- USBハブを介して、複数のUSBメモリ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。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ランプが点灯／点滅している間は、USBメモリを取り外さないでください。USBメモリ内のデータを破損することがあります。USBボタンを2秒間押し続けて、USBランプが消灯していることを確認してからUSBメモリを取り外してください。

## USBメモリ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

「USBホストの設定」画面の「ボタン操作でコピーする設定ファイル名」欄で、本製品にコピーする設定ファイルのファイル名および保存先の設定ファイル番号を指定します。




**「USBホストの設定」画面を開くには**

管理者向けトップページから、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「保守」

▶「USBホスト機能の設定・状態表示」の「設定」

## USBボタンを押して設定ファイルを読み込む

**1 「USBホストの設定」画面の「ボタン操作でコピーする設定ファイル名」欄で指定したファイル名の設定ファイルを用意して、パソコンなどを使ってUSBメモリにコピーする。**

**2 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**3 USB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。

**ヒント**

「USBホストの設定」画面の「ボタン操作でコピーする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同時に存在する場合は、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ボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

**5 USBメモリを取り外す。**

**ご注意**

USB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」(170ページ)をご確認ください。

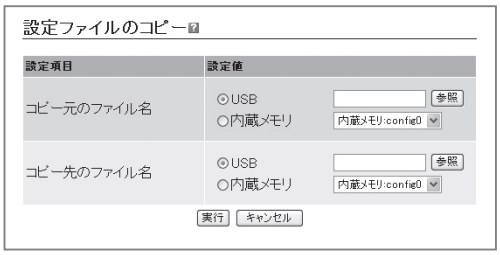
## 本製品の設定画面から USBメモリ内の設定ファイルを読み込む

**1 設定ファイルを用意して、パソコンなどを使ってUSBメモリにコピーする。**

**2 USBメモリを本製品のUSBポートに差し込む。**

本製品のUSBランプが点灯／点滅します。

**3 「設定ファイルのコピー」画面の「コピー元のファイル名」で「USB」をクリックして選んでから、本製品にコピーしたいファイルを指定する。**




**「設定ファイルのコピー」画面を開くには**

管理者向けトップページから、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「保守」

▶「設定ファイルのコピー」の「実行」

**4 「コピー先のファイル名」で「内蔵メモリ」をクリックして選んでから、保存先の設定ファイル番号を選ぶ。**

本製品内部での設定ファイルの管理方法について詳しくは、「設定ファイル管理上のご注意」(143ページ)をご覧ください。

**5 「実行」をクリックする。**

パスワードの入力画面が表示されます。

暗号化されたファイルをコピーする場合は、パスワードを入力してください。

**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。

**7 USBボタンを2秒間押し続ける。**

本製品のUSBランプが消灯します。

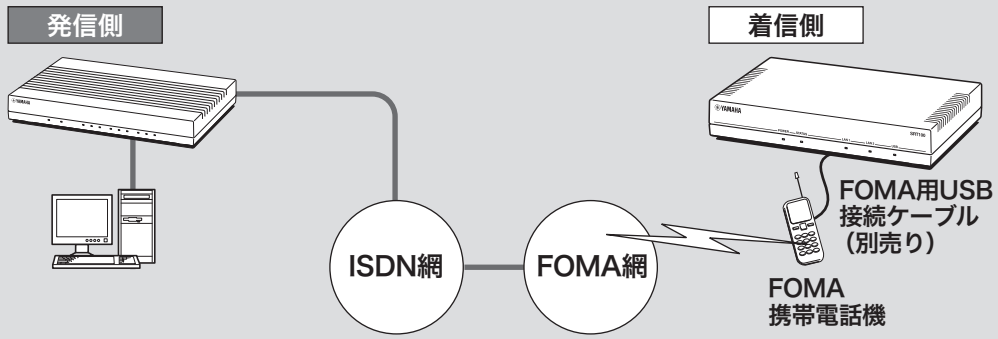
**8 USBメモリを取り外す。**

**ご注意**

USB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」(170ページ)をご確認ください。

# FOMAでリモートアクセスを受けて、本製品の設定を変更する

本製品のUSBポートにFOMAをUSB接続ケーブルで接続して、ISDNポートを持つルーターから本製品へリモートセットアップを実行できます(FOMAリモートセットアップ)。




**ご注意**

- 発信側にはISDNの通話料がかかります。
- リモートセットアップにはFOMAの64kデータ通信を使用します。
- 本製品側からのリモートセットアップの発信はできません。

**ヒント**

コンソールへの表示や入力方法などは、通常のリモートセットアップ機能と同様です。



## FOMAリモートセットアップに必要な環境

FOMAリモートセットアップを利用するには、以下の機器・環境が必要です。

### リモートセットアップ発信側

- RTX1100またはRTX1500（対応ファームウェア搭載）
- パソコン(RTX1100またはRTX1500コンソール操作用)

**ご注意**

- 発信側機器はISDNインタフェースを持ち、再送制御に対応したリモートセットアップ機能に対応したファームウェアを導入している必要があります。
- 対応ファームウェアは、ヤマハルーターホームページ(http://NetVolante.jp/)で公開予定です。

### リモートセットアップ着信側(本製品側)

- SRT100（本製品）
- 64kデータ通信の着信機能を持つFOMA端末
- FOMA用USB接続ケーブル

**ご注意**

- login timerを長めに設定すると、長時間に渡って接続が保持された状態となり、高額な通信料金を請求される場合があります。login timerを長めに設定した場合は、通信状態には十分ご注意ください。
- FOMA端末によっては、64kデータ通信の着信が利用できない機種があります。動作確認済みのFOMA端末をご使用ください。動作確認機種は、ヤマハルーターホームページ(http://NetVolante.jp/)で公開予定です。
- 接続ケーブルは、NTTドコモ社純正のFOMA USB接続用ケーブルを使用してください。

## 操作の流れ

以下の流れでFOMAリモートセットアップを行います。

**ご注意**

- 複数のSRT100に対して、同時にリモートセットアップの発信を行うことはできません。
- リモートセットアップ発信中は、リモートセットアップの着信もできません。
- show logなど、結果表示の量が多くなるコマンドを入力した場合、表示に時間がかかる場合があります。
- 一度に多くのコマンドを送信すると、送信し切れずに途中で破棄される場合があります。

**1 FOMAの電源が入っていることを確認する。**

**2 本製品とFOMAを、FOMA用USB接続ケーブルで接続する。**

接続が完了すると「ピポッ」と確認音が鳴り、本製品のUSBランプが点灯します。

**「ピーピーピーピー」というエラー音が鳴り、USBランプがゆっくり点滅した場合は**

FOMAカードが挿入されていないか、64kデータ通信を利用できない端末を接続しているため、FOMAリモートセットアップを利用できません。

**3 RTX1100またはRTX1500側から、以下のリモートセットアップコマンドを実行する。**

```
remote setup bri1［FOMA電話番号］
retransmission
```

これでRTX1100またはRTX1500側から本製品にログインして、設定を変更できるようになります。

**FOMA電話番号が090xxxxyyyyの場合の例**

```
remote setup bri1 090xxxxyyyy
retransmission
```

**4 必要に応じて、本製品の設定を変更する。**

**5 設定が終わったら、exitコマンドなどでログアウトする。**

FOMAリモートセットアップが終了します。

**ご注意**

接続が保持された状態が続いていると、高額な通信料金を請求される場合があります。確実に通信が終了していることを確認してください。

# 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。

### 基本的なチェック

- **POWERランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。
- **LAN2ランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。
- **LAN1ランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。

### STATUSランプの状態を確認してください

点灯している場合は、通信に障害が発生しています。134ページをご覧ください。

### USBランプの状態を確認してください

アクセスできないのに点滅している場合は、障害が発生しています。170ページをご覧ください。

## 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**（次ページ）
- **Q2：設定画面で設定できない**（162ページ）
- **Q3：インターネットに接続できない**（164ページ）
- **Q4：VPN通信ができない**（166ページ）
- **Q5：STATUSランプが機能しない**（168ページ）
- **Q6：DOWNLOADボタンが機能しない**（169ページ）
- **Q7：USBデバイスが使用できない**（170ページ）
- **Q8：FOMAリモートセットアップが利用できない**（171ページ）
- **Q9：その他の問題**（173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（177ページ）。

## パスワードを忘れてしまった／設定を初期化したい

「パスワードを忘れてしまった場合は」（176ページ）および「本製品の設定を初期化する」（174ページ）をご覧ください。

# 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** | 本製品の電源が入っていない | POWER（電源）スイッチを「ON」にして、電源を入れる。 |
| | 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。<br>• 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。<br>• 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** | HUBやパソコンの電源が入っていない | 本製品および本製品に接続した機器の電源が入っていることを確認する。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。 |
| | 正しく接続されていない | 本製品側、パソコンおよびHUB側共にコネクタをいったん外してから、もう一度カチッとロックするまで差し込む。 |
| | LAN用のケーブルを使っていない | • ISDNケーブルを使用していないかどうか確認する（コネクタ形状が全く同じなので注意が必要）。<br>• 他のLANケーブルと取り替えてみる。 |
| | 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 | • 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。<br>• 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。 |
| **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。 |

# Q2 設定画面で設定できない

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **設定画面を表示できない** | 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」(前ページ)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。<br>• IPアドレスをリセットする(178ページ)。 |
| | 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(174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。<br>• 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。<br>• パソコンの設定が同じIPアドレス範囲になっているか、他の機器とIPアドレスが重なっていないか確認する。 |
| | ルーターの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InternetExplorer6 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、設定画面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、設定画面が表示できなくなる。<br>• Windows版InternetExplorer6の場合：メニューから「ツール」→「インターネットオプション」→「接続」タブ→「LANの設定」を開き、「プロキシサーバーを使用する」のチェックをはずす。 |

| 症状▶ | 原因▶ | 対策 |
| --- | --- | --- |
| **設定画面を表示できない（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 membersonly. I'm sorry, your host is notmember.」と表示される。遠隔操作する場合は、「GUIの設定」画面で「IPアドレス指定」の設定を変更する（121ページ）。 |
| **パスワードを入力しても設定画面が表示されない** | 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。<br>• 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設定画面を開き直す。 |
| | ログインパスワードでは設定画面にアクセスできない | 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する（123ページ）。 |
| **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 | 設定画面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。 |
| **設定画面を開く際に、Webブラウザにパスワードを保存できない** | 「ネットワークパスワードの入力」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。 |

# Q3 インターネットに接続できない

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **フレッツ・ADSLや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」(161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)。<br>• フレッツ・ADSL(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。<br>• 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。<br>• 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(104ページ)を適用している。不要なポリシーを適用していないかどうか、ポリシーを確認する。<br>• 入力遮断フィルター(102ページ)やポリシーフィルター(104ページ)でhttp通信のポートを制限している、表示しようと指定したホームページがURLフィルター(116ページ)によるフィルタリングの対象となっている。フィルタリングの設定を見直してください。 |
| | 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。<br>いったん接続を切断してから、管理者向け設定画面の「インターフェース」ー「PPPoE」欄の「詳細」ー「基本項目」欄の「設定」ー「PPPoEインターフェースの設定」画面でMTUに1454などの値を設定して、接続し直す。 |

| 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)** | プロバイダから与えられたIPアドレスと、本製品のLAN1ポートに設定したIPアドレスが重複している | 管理者向け設定画面で「インターフェース」をクリックしてからLAN1の「詳細」–基本項目の「設定」をクリックして、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。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。<br>• IPアドレスをリセットする(178ページ)。 |
| | 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通信ができない

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **管理者向けトップページで「IPsec」が「Up」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。<br>• 「インターネットに接続できない」(164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。<br>• 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。<br>• 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。<br>• 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。<br>WindowsXP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。 |
| | インターネット接続設定の「セキュリティフィルターの設定」画面で、「IPsec VPNを使用する」にチェックを付けていない | 「セキュリティフィルターの設定」画面で、「IPsec VPNを使用する」にチェックを付ける(52ページ)。 |

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **IPsec接続のVPN通信が遅い** | インターネットの通信が遅い | 「インターネットに接続できない」(164ページ)の説明に従って、問題を解決する。 |
| **管理者向けトップページで「IP over IP」が「Up」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。 |
| **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。<br>• 管理者向け設定画面で「インターフェース」をクリックしてからIP over IPの「詳細」をクリックして、宛先ネットワークとして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。<br>• 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。<br>WindowsXP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 STATUSランプが機能しない

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **通信障害が発生していないのにSTATUSランプが点灯している** | DOWNLOADボタンによるリビジョンアップが行われている | リビジョンアップが完了した後に、再度STATUSランプを確認する。 |
| **通信障害が発生しているのにSTATUSランプが点灯しない** | キープアライブ機能が有効になっていない | 管理者向け設定画面で「インターフェース」をクリックしてからプロバイダ接続やVPN接続の「詳細」−基本項目の「設定」をクリックして、キープアライブ機能が有効になっているかを確認する。 |
| | キープアライブ機能が通信障害を未だ検出していない | 数分間待ってから、再度STATUSランプを確認する。 |
| | PPPoE接続が切断タイマによって切断された | タイマで自動切断しないように設定を変更する。 |
| **STATUSランプの点灯を解除できない** | 通信障害から復旧していない | 「インターネットに接続できない」(164ページ)、「VPN通信ができない」(166ページ)の説明に従って、問題を解決する。 |

# Q6 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。「インターネットに接続できない」(164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 | 「HTTPリビジョンアップの設定」画面(145ページ)で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 | 「HTTPリビジョンアップの設定」画面(145ページ)で、「使用」を「する」に設定する。 |
| | 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。 |
| **STATUSランプが点滅し始めた** | ファームウェアをサーバーからダウンロードしている(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。 |
| **STATUS、LAN1、LAN2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。 |
| **STATUSランプが点灯したままの状態になった** | リビジョンアップに失敗した | 「DOWNLOADボタンを押してもリビジョンアップされない」(本ページ)の説明に従って、問題を解決する。<br>STATUSランプの点灯を解除する場合は、DOWNLOADボタンを1秒間押す。 |
| **DOWNLOADボタンを1秒間押しても、STATUSランプが消灯しない** | 通信障害が発生している | 「STATUSランプが機能しない」(前ページ)の説明に従って、問題を解決する。 |

# Q7 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ホスト機能の使用」を「する」に設定する(147ページ)。 |
| | USBメモリ以外のデバイスを挿入している | 本製品でサポートしているUSBメモリを挿入する。 |
| | 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 | 「ボタンによるファイルコピー」を「許可する」に設定する(147ページ)。 |
| | 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 | 設定画面で設定した名前のファイル(147ページ)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。<br>**ヒント**<br>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。 |
| **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。 |

# Q8 FOMAリモートセットアップが利用できない

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **エラー音が鳴り、USBランプが点滅している** | FOMAを認識できない | • FOMAにFOMAカードが入っていることを確認する。<br>• 64kデータ通信ができる機種であることを確認する。<br>• FOMAの電源を入れてしばらくしてから接続する。 |
| **USBランプが点灯しない** | FOMAを認識できない | • 管理者向け設定画面の「保守」–「USBホストの設定・状態表示」画面で、USBポートを使用する設定になっていることを確認する。<br>• FOMA USBケーブルが正常であることを確認する。 |
| **FOMAに接続できない** | 電話番号が間違っている（発信側のログに「Invalid number format（address incomplete）(28)」などと表示される） | 電話番号が正しいことを確認する。 |
| | FOMAがUSBポートに接続されていない（発信側のログに「Destination out of order（27）」と表示される） | FOMAの電源を入れて、本製品のUSBポートに接続する。 |
| | FOMAの電源が「切」になっている、またはFOMAにFOMAカードが挿入されていない（発信側のログに「No user responding（18）」と表示される） | FOMAにFOMAカードが挿入されていることを確認してから、FOMAの電源を入れて本製品のUSBポートに接続する。 |
| | 64kデータ通信ができない（発信側のログに「Incompatible destination (88)」と表示される） | 64kデータ通信に対応している、動作確認済のFOMAを接続する。 |
| | FOMAが話中（発信側のログに「User busy（17）と表示される） | FOMAでは64kデータ通信と音声通話を同時に使用できない。通話を切断後に、再度接続する。 |

# Q8 FOMAリモートセットアップが利用できない(つづき)

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **FOMAに接続できない(つづき)** | 再送制御なしのリモートセットアップで発信している(発信側のログには正常切断と表示される) | リモートセットアップコマンドでretransmissionキーワードを付与して、再送制御ありのリモートセットアップで発信する。<br>`remote setup bri1 NUMBER retransmission` |
| **電波状態が悪化して切断されると、再接続できない** | FOMAの機種によっては、電波状態が悪化して切断されるとFOMAが正常に復旧しない場合がある | FOMAをUSBポートからいったん取り外してから接続し直して、FOMAを正常な状態に復旧させる。 |
| **通信速度やエコーが遅い** | 電波状態が悪い | FOMA側の電波状態を改善する。 |
| | FOMAの網に遅延がある | FOMA網では1秒近く遅れることがある。 |
| | FOMAの機種によっては、エコーにかかる時間が遅い場合がある | 別機種のFOMAで試してみる。 |

# Q9 その他の問題

| 症状▶ | 原因▶ | 対策 |
|---|---|---|
| **本製品やパソコンで、NTPサーバーを使った時刻合わせができない** | NTPサーバーのIPアドレスやドメイン名が間違っている | • 入手したNTPサーバー情報と比較し、正しく設定されていることを確認する。<br>• 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どうか確認する。 |
| **ネットボランチDNSサービスでホストアドレスを取得できない** | プロバイダによっては、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。 |

# 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。

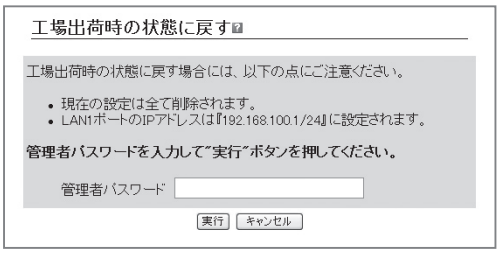
**ご注意**

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。

## 設定画面から初期化する

本製品の設定内容を工場出荷状態に戻したいときは、「工場出荷時の状態に戻す」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 ? をクリックして、表示される説明をご覧ください。

**「工場出荷時の状態に戻す」画面を開くには**

管理者向けトップページから、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「保守」

▶「工場出荷時の状態に戻す」の「実行」

## 設定画面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、本製品の設定画面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を使用して本製品を初期化できます。

**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。**

接続およびパソコンの設定については、154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155ページをご覧ください。

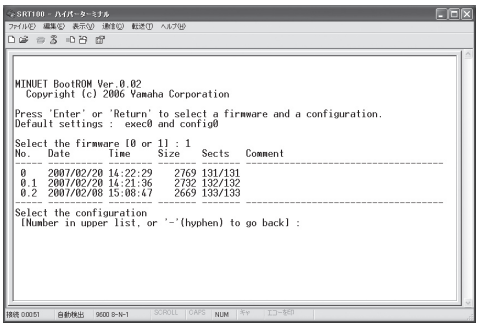
**4 本製品の電源を入れる。**

パソコンのターミナルソフトウェアの画面に本製品のファームウェア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、Enterキーを押す。**

管理者パスワードを設定している場合は、パスワードを入力してからEnterキーを押してください

「>」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。

**9 「administrator」と入力してから、Enterキーを押す。**

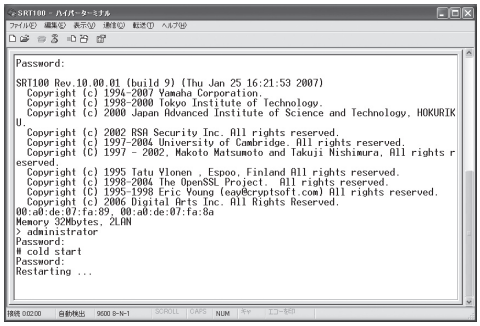
**10 「Password:」と表示されたら、Enterキーを押す。**

管理者パスワードを設定している場合は、パスワードを入力してからEnterキーを押してください

**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、Enterキーを押す。**

管理者パスワードを設定している場合は、パスワードを入力してからEnterキーを押してください




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

## 非常用パスワードでログインする

ログインパスワードや管理者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,lXlma」(ダブリュ -、カンマ、エル、エックス、エル、エム、エー)

**ヒント**

CONSOLEポートへの接続およびパソコンの設定については、154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者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。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。
- 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。

## 工場出荷時の初期パスワード

「doremi」が工場出荷時の初期パスワードとして設定されています。

本製品を初期化した場合は、パスワードも初期化されます。初期化の直後に本製品にログインするには、パスワードとして「doremi」を使用してください。なお、ログイン後は速やかにパスワードを登録／変更するようおすすめいたします。

# 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どうかご確認ください。

### ログ情報や設定情報をご確認ください

お客様のルーター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Webブラウザを起動して、ファイルメニューの「開く」を選ぶ。**
   「ファイルを開く」画面が表示されます。
2. **「http://192.168.100.1/」と半角英字で入力してから、「OK」をクリックする。**
   設定画面のトップページが表示されます。
3. **「管理者向けトップページへ」をクリックする。**
4. **「保守」をクリックする。**
5. **ログ情報を確認したいときは「SYSLOGを画面へ出力」、設定情報を確認したいときは「設定を画面へ出力」の「実行」をクリックする。**
   本製品のログ表示または全設定情報が表示されます。
   「本製品の設定情報を確認する」(135ページ)および「本製品のログを確認する」(136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：053-478-2806
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頂きます。)
**お問い合わせページ**
http://NetVolante.jp/
http://www.rtpro.yamaha.co.jp/

# 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**

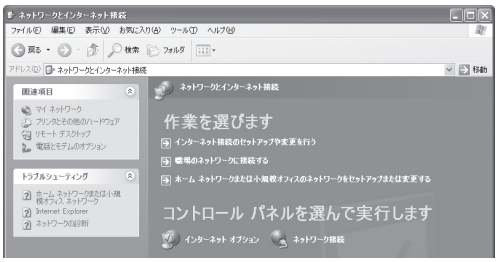
本製品を設置したLANのネットワークアドレスを変更していない場合は、LAN内のパソコンのIPアドレスを変更する必要はありません。

## 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。

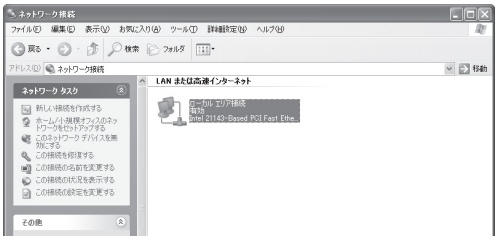
**2** 「ネットワークとインターネット接続」をクリックする。


**3** 「ネットワーク接続」をクリックする。

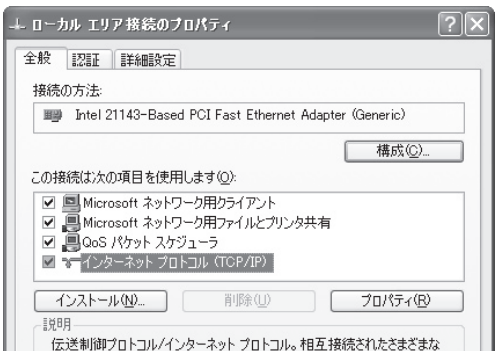



**4** 「ローカルエリア接続」のアイコンをクリックする。

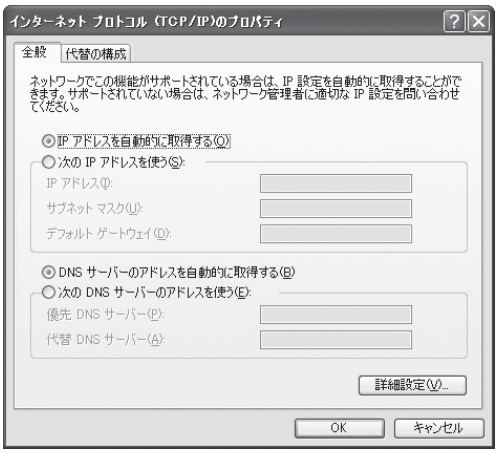

**5** 「この接続の設定を変更する」をクリックする。




**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。

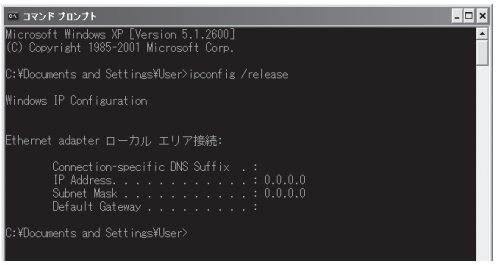



**8** 「ローカルエリア接続のプロパティ」画面で「OK」をクリックする。

付録

**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。

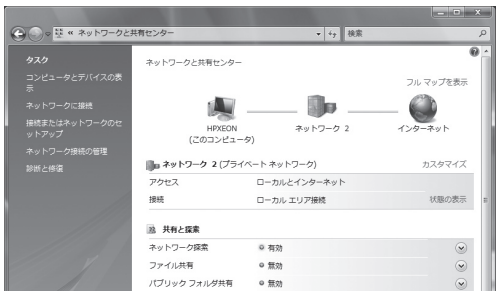
## Windows Vistaの場合

**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** 「ネットワークの状態とタスクの表示」をクリックする。


「ネットワークと共有センター」画面が表示されます。

**3** 「ローカル エリア接続」の「状態の表示」をクリックする。




「ローカル エリア接続の状態」画面が表示されます。

# LAN内のパソコンのIPアドレスを変更する(つづき)

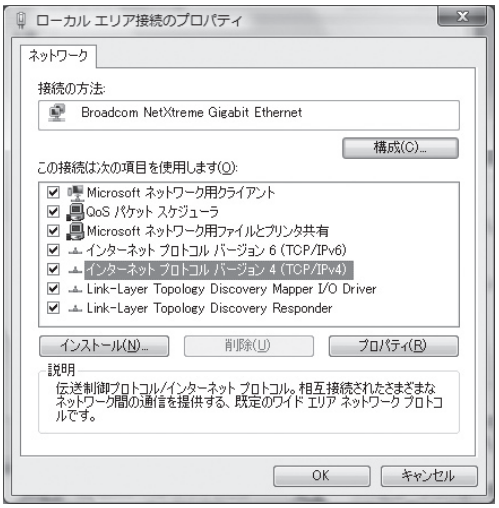
**4** **「プロパティ」をクリックする。**


確認画面が表示されます。

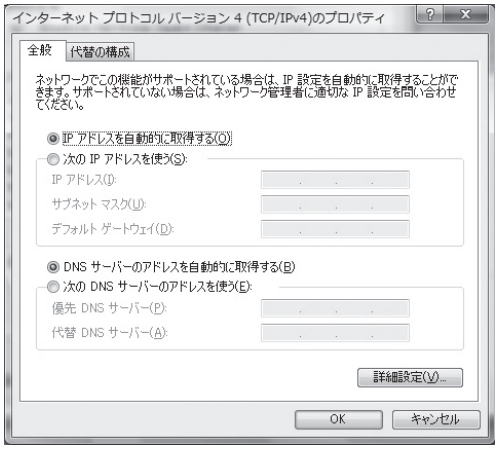
**5** **「続行」をクリックする。**

「ローカル エリア接続のプロパティ」画面が表示されます。

**6** **「インターネットプロトコル バージョン4(TCP/IPv4)」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** **「インターネットプロトコル バージョン4(TCP/IPv4)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、検索欄に「コマンド プロンプト」を入力する。**

検索結果欄に「コマンド プロンプト」が表示されます。

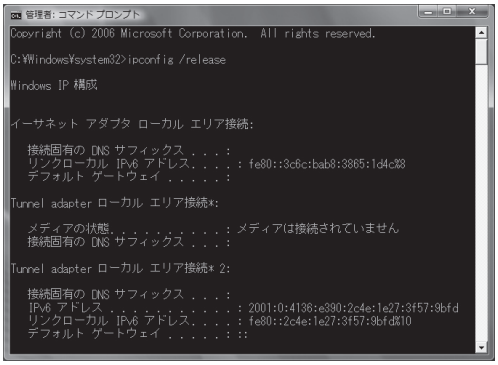
**10** **検索結果欄の「コマンド プロンプト」を右クリックして、「管理者として実行」を選ぶ。**

確認画面が表示されます。

**11** **「続行」をクリックする。**

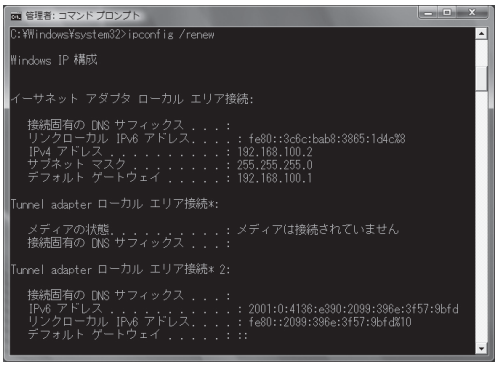
付録

**12**「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。

**13**「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。

**14 LAN上のすべてのパソコンに対して手順1～13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。**

# 主な仕様

**外形寸法（幅×高さ×奥行き）：**
220 mm×42.6 mm×141.5 mm

**質量：**
700 g

**電源：**
AC100 V（50/60 Hz）

**消費電流：**
最大0.18A

**動作環境条件：**
周囲温度 0～40 ℃
周囲湿度 15～80 %（結露しないこと）

**保管環境条件：**
周囲温度 ー 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：**
AD08-0160001

**LAN1インターフェース：**
イーサネット 10BASE-T/100BASE-TX
4ポートスイッチングHUB
プロトコル：IEEE802.3/IEEE802.3u
通信モード：オートネゴシエーション、
固定設定
コネクタ：RJ-45
MACアドレス：本製品ラベルに表示
極性：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 10BASE-T/100BASE-TX
1ポート
プロトコル：IEEE802.3/IEEE802.3u
通信モード：オートネゴシエーション、
固定設定
コネクタ：RJ-45
MACアドレス：本製品ラベルに表示
極性：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**
USB2.0
給電電流：最大500mA
ポート数：1
コネクタ：USB Type-Aコネクタ

**表示機能（LED）**
前面：POWER、STATUS、LAN1、LAN2、
USB
背面：LINK、SPEED、USB

**付属品：**
LANケーブル（3 m、RJ-45、ストレート）（1本）
取扱説明書（本書）（1冊）
CD-ROM（1枚）
保証書（1枚）

# 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

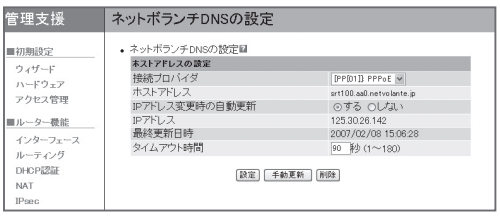
**ご注意**

- 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行ってください。
- 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**

管理者向けトップページから、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。

初期化のしかたについては、「本製品の設定を初期化する」(174ページ)をご覧ください。

# 索引

## 英数字



## 五十音順

### ア行



### カ行



### サ行

## タ行



## ナ行



## ハ行



## マ行



## ラ行

●ヤマハルーターお客様ご相談センター
TEL 053-478-2806
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頂きます。）
**お問い合わせページ**
http://NetVolante.jp/
http://www.rtpro.yamaha.co.jp/

WV26790

PRINTED WITH SOY INK

この取扱説明書は大豆油インクで印刷しています。
この取扱説明書は無塩素紙（ECF：無塩素紙漂白パルプ）を使用しています。

（2010年2月 第3版）