ファイアウォールルーター

SRT100 簡単設定ガイド

インターネットのさまざまな脅威から
SOHO・中小企業のシステムを守る
ヤマハのファイアウォールルーター
「SRT100」の機能と設定を学んでいく

ネットワークマガジン NETWORK MAGAZINE

ファイアウォールルーター

SRT 100
簡単設定ガイド

目次

概論

境界線でセキュリティを確保せよ

さまざまな不正プログラムの登場や攻撃により、多くの企業はデータの盗難や改ざんなどの脅威に常時さらされています。こうした脅威を防ぐ基本となるのが、インターネットとLANの境界線に設置されているルーターやファイアウォールでのセキュリティ確保です。

増え続けるインターネットの脅威

インターネットを利用する限り、セキュリティに対しては細心の注意を払わなければなりません。インターネットに接続されているコンピュータは、管理者権限の乗っ取りやデータの詐取などを狙った不正アクセス（クラッキング）の標的となる宿命にあります。インターネットでは、クラッカーや犯罪者などがつねに攻撃対象となるコンピュータを捜しているからです。

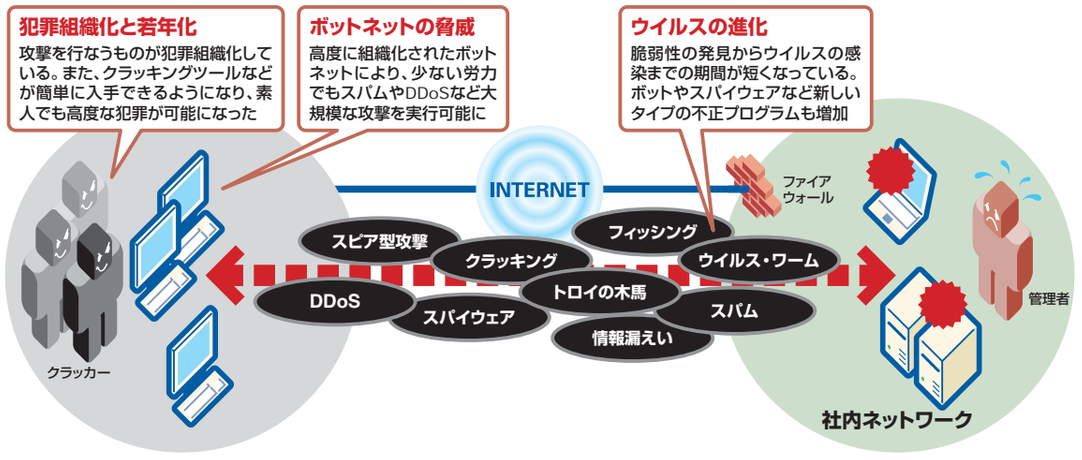
こうした不正アクセスからコンピュータを守るため、従来から利用されてきたのが「ファイアウォール」です。ファイアウォールは、通信の中身を精査することでアクセス制御を行なう機能を指します。専用機やルーターの機能の一部として実装されており、LANとインターネットの境界で動作させることで、LANに攻撃が及ばないようにします。

また、メールやWWWを経由してコンピュータに感染するウイルスも頭の痛い問題です。こうしたウイルスは、データの破壊や改ざん、情報漏えいなどを引き起こす原因となります。こうしたウイルスを防ぐために、コンピュータごとにウイルス対策ソフトを導入するのが一般的です。

従来、インターネットを利用するにあたっては、このようにファイアウォールとウイルス対策ソフトでセキュリティを確保してきました。しかし、ブロードバンドが普及し、インターネットでの犯罪が組織化・巧妙化した現在、すでにこれでは十分とはいえなくなりました。

ウイルスはますます凶悪化し、OSやソフトウェアの脆弱性の発見から、実際に脆弱性を突くウイルスが発見されるまでの期間がきわめて短くなってきました。また、コンピュータの中で情報を収集するスパイウェアや大量の迷惑メールを配信するスパムメール、攻撃を自動化・大規模化する

図1 ますます凶悪化するインターネットでの攻撃



ボットなど、不正プログラムの種類も増えてきました。

また、インターネットを用いて詐欺を行なうフィッシング、特定のアプリケーションの脆弱性につけ込むスピア型攻撃など、従来使ってきたファイアウォールやウイルス対策ソフトでは対抗できない脅威が次々と登場してきています。さらに、最近ではインターネット側からの攻撃だけではなく、社内から社外への情報漏えいも大きな問題となっています。

複数の脅威に対抗するUTMの登場

しかし、それぞれの脅威に対して対抗策を用意するのでは、運用や管理にコストもかかります。そこで2003年以降に登場したのが、「UTM（Unified Threat Management）」と呼ばれる新しいジャンルのセキュリティ装置です。

このUTMは「統合」という名前のとおり、ファイアウォールやVPN、IDS・IPS、アンチウイルス／スパイウェア、アンチスパム、URLフィルタリングなど複数のセキュリティ機能をまとめて搭載しています。多くのベンダーでは、専業ベンダーから供給されたエンジンを用いていますので、検出精度などは問題ありません。このUTMをインターネットとLANの間に設置しておけば、不正アクセスだけではなく、ウイルスやスパイウェアなどの不正なプログラム、スパムメールなどの脅威を一括で遮断できるというわけです。

また、UTMでは「サブスクリプション（購読）」という有料サービスの利用により、最新の攻撃に対抗します。IDS・IPS、アンチウイルス、アンチスパムなど、UTMに搭載されている機能のいくつかでは、通過するトラフィックを最新の攻撃パターンや不正プログラムの特徴などを登録したデータベースと照らし合わせることで、攻撃を検知します。ここで用いるデータベースやファームウェアを入手にするためのオンラインサービスがサブスクリプションです。サブスクリプションの契約期間中は、データベースやファームウェアを常時更新しておくことで、最新の攻撃に対応することができるわけです。

現在、UTMは既存のファイアウォール・VPN機器に代わる新たなセキュリティ装置として注目を集めています。

ファームウェア更新料無料のファイアウォールルーター「SRT100」

このUTMに対するヤマハの答えが、ファイアウォールルーター「SRT100」です。

もとよりヤマハは、SOHOや中小企業のルーター市場で高いシェアを誇っています。ヤマハのルーターでは、基本となるルーティングはもちろん、インターネット接続に必要なNATやパケットフィルタリング、拠点間を安全につなぐためのVPN（Virtual Private Network）など、多彩な機能をオールインワンで提供しています。また、使いやすいGUIや高いパフォーマンス、手頃な価格といった特徴もSOHOや中小企業にとって魅力的といえるでしょう。

図2 複数のセキュリティ製品をまとめた「UTM」

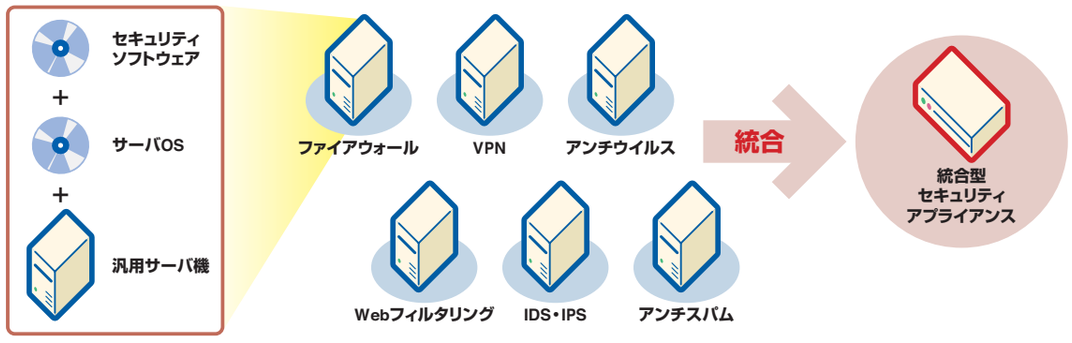


図3 ルーター、VPNゲートウェイ、ファイアウォールなど複数の機能を搭載した「SRT100」

従来、同社の製品はISDNダイヤルアップルーターがメインでしたが、2000年以降は企業での利用を前提としたブロードバンドルーター製品に軸足を移しています。そして、昨今のセキュリティの脅威に対抗するため、セキュリティにフォーカスを当てたのがSRT100というわけです。

SRT100を一言でいえば、「設定の容易さを追求したセキュリティ強化版『RT107e』」です。

2005年に発売されたRT107eは、使いやすさやわかりやすさを追求したSOHO向けVPNルータです。ISDNバックアップに非対応で、VPNスループットが50Mbps、IPsecの対地数が6に留まるものの、同社のIPsec対応機種の中ではもっとも安価な7万1400円（税込・希望小売価格）を実現しています。

SRT100は、このRT107eをベースにしており、筐体もほぼ同一となっています。SRT100の背面にはLAN用ポートは4つ、WAN用ポート「LAN2」ポートが1つ、コンソールポートを搭載されており、RT107eとはUSBポートが搭載されている点だけ異なっています。機能面で見ると、各種ルーティングプロトコルやPPPoE、NAT、ファイアウォール、VPNなどの機能はもちろん、セッションレベルでポートを開け閉めするStateful Inspection方式のファイアウォールや、攻撃パターンのデータベースとの照合により攻撃を検知・遮断するIDS・IPS、Winnyのフィルタなどのセキュリティ機能もRT107eと同等です（詳細は次ページ以降で説明します）。価格も8万1900円（税込）とRT107eと同様に低価格で、SOHOで導入しやすくなっています。

ただ、複数のセキュリティ機能を搭載していますが、既存のUTMとはやや異なります。

まず、UTMの最大の特徴であるアンチウイルスを搭載していません。これはアンチウイルス処理を搭載すると、パフォーマンスが一気に落ちてしまうという弱点があるからです。また、通常は企業のクライアントにすでにウイルス対策ソフトがあるため、ルーターにはあえて搭載しないという考えもあるようです。

一方で、ファームウェアが無料というのも大きなメリットです。前述の通り、サブスクリプションサービスを利用すると、最新の攻撃に対応できますが、毎年購読料金がかかることになります。これに対して、SRT100ではファームウェアはもちろん、IDSなどで検出するための最新の攻撃データベースも無償で提供されます。

そして、SRT100は最大の特徴は、設定管理を容易にする「日本語GUI」です。もとよりファイアウォールやVPNの設定はかなり難解で、企業のネットワーク管理者が簡単に操作できるものでもありません。設定ツールがGUI化されていることも増えていますが、英語のままのメニューが多かったり、難解な用語がそのまま掲載されていたりします。そのため、敷居はやはり高いといわざるをえないでしょう。SRT100は、ここにメスを入れているわけです。

設定の容易さが大きな特徴の「SRT100」

ファイアウォールルーターの導入

今回はSRT100をインターネット接続用のルーターとして利用する例について見ていきましょう。SRT100では、LANとインターネットという異なるネットワークを相互に接続しつつ、インターネット側からの攻撃をファイアウォールで防ぐという役割を果たします。また、インターネット接続している他の拠点とVPNを張り、互いのLANのコンピュータ同士で通信できるようにするのも最近のルーターの重要な役割です。

今回、インターネット接続は、NTT東日本の100Mbpsの光ファイバを占有する「Bフレッツビジネスコース」を前提として説明していきます。ビジネスでのインターネット接続は、スループットや信頼性の劣るADSLより、光ファイバを用いたFTTHサービスのほうがよいでしょう。

USENやKDDIなどのFTTHサービスもありますが、基本的な設定はBフレッツと変わりません。ただ、Bフレッツの場合、光ファイバ回線の契約とは別に、インターネット接続のためのプロバイダ契約が必要になります。VPNの利用を前提とするのであれば、固定のグローバルアドレスを割り当てるサービスを利用しましょう。

設定についての解説は、基本設定として、以下のように進めます。

・基本設定とインターネット接続（6～11ページ）

ルーターの日時合わせ、管理者パスワードの設定やLAN側のIPアドレス設定などの初期設定。また、FTTHやADSLなどブロードバンド回線を経由したインターネット接続も設定します。

・ファイアウォールなどセキュリティ機能の設定（12～23ページ）

入力遮断フィルター、ポリシーフィルター、URLフィルター、不正アクセス検知、セキュリティ診断など、インターネットからの不正アクセスに対抗するためのセキュリティ設定。MACアドレスを元に不正な端末の接続を拒否するDHCP端末認証も説明します。

・拠点間のVPNの設定（29～37ページ）

IPsecを用いたLAN間VPNのための設定。接続先やデータの暗号化に用いる鍵、認証や暗号化のアルゴリズムの選択、パケットの転送先となるネットワークの指定、その他オプションなどの設定を行ないます。また、SRT100にリモートアクセスVPNで接続するためのVPNクライアントの設定も紹介します。

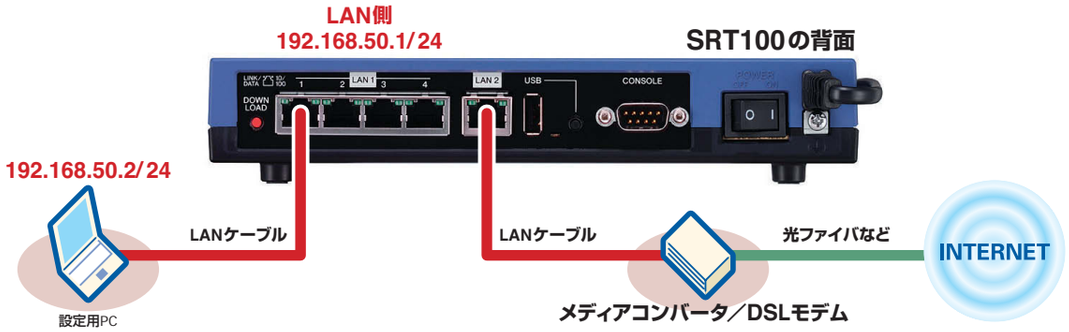
これらの解説をひととおり終えたあと、応用として運用・管理に便利な機能を紹介します。

・統計情報とメール通知、SNMP（40～45ページ）

リソース統計、トラフィック統計、QoS統計などの利用方法とメール通知。また、ファームウェアのリビジョンアップやUSBメモリを用いた設定のバックアップ、SYSLOGの管理などの操作も解説します。

■SRT100の前面と背面

図4 FTTHサービスを使った場合のSRT100の物理的な配線



では、さっそくSRT100の接続と設定に移りましょう。

SRT100の接続とトップページへのアクセス

物理的な接続は、図4のとおりになります。まずFTTHで提供されているメディアコンバータのLANポートと、SRT100のLAN2ポートをUTPケーブルで結線。同じく設定用のPCのLANポートをSRT100のLAN1のポートのいずれかにつなぎます。

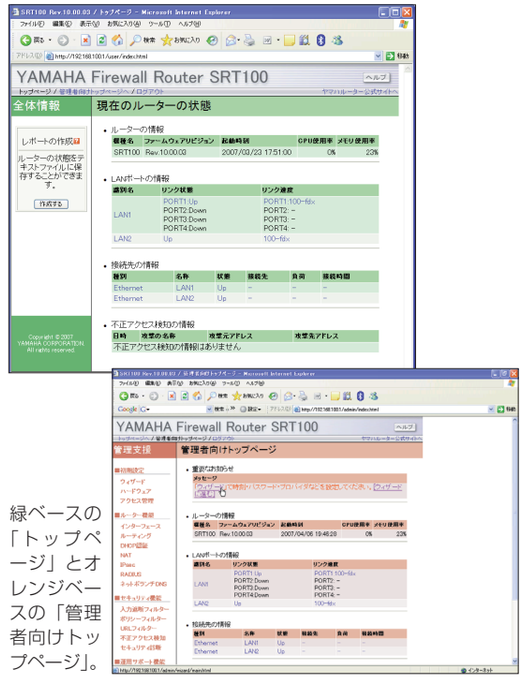
以降のSRT100の設定は、Webブラウザ上で動作するGUIツールから行なえます。SRT100では、初期状態でDHCPサーバが動作していますので、背面の電源ボタンをオンにすると、設定用のPCに自動的にIPアドレスが割り当てられます。あとはWebブラウザのアドレス欄に設定ツールのIPアドレス（初期状態では192.168.100.1）を入力すると、トップページが表示されます。

設定ツールのトップページは、現在の動作状態を一覧するためのもので、ルーターのファームウェアのバージョンやCPU、メモリの使用率、LANポートの状態、接続先、不正アクセス検知の情報などが表示されています。

実際の設定は、上部にある「管理者向けトップページへ」のリンクで開く「管理者向けトップページ」から行ないます。初回は「重要なお知らせ」のリンクから、ウィザードを起動し、初期設定を行ないます。

ウィザードでは日付や時刻、管理者パスワード、LAN側のネットワーク、プロバイダなどをまとめて設定できます。パスワードも、英数字の数や混ざり具合などで強度が判定されるので、安心です。ウィザードが終了すると、利用するアプリケーションの選択やIPsec VPNのオン／オフまでを設定する画面も登場します。SRT100では、このように1回のウィザードで、ルータ自体をかっちりした設定で固めておけます。

次ページから実際のウィザードの操作を見ていきます。

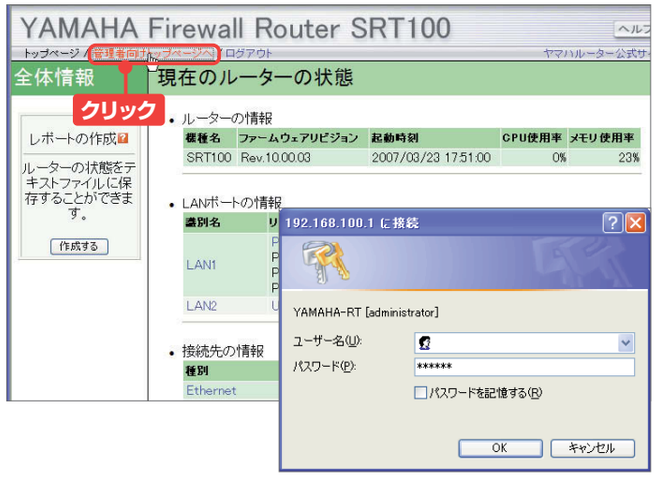


緑ベースの「トップページ」とオレンジベースの「管理者向けトップページ」。

SRT100の基本設定を行なう

1 トップページの表示

SRT100の管理用ページのメニューから、「管理者向けトップページへ」をクリックします。このとき、再度初期パスワードを使って認証を行ないます。

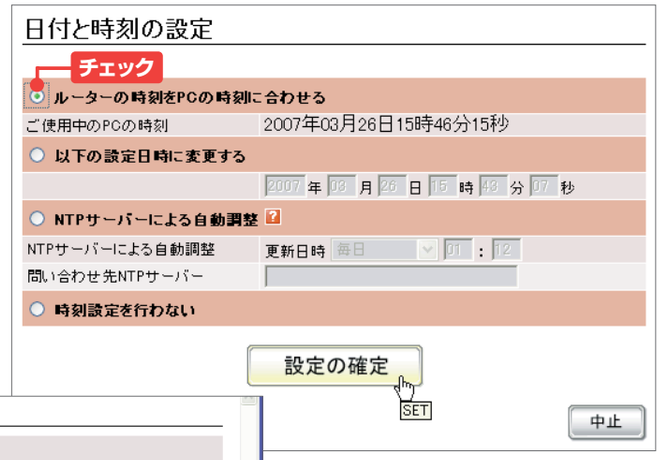


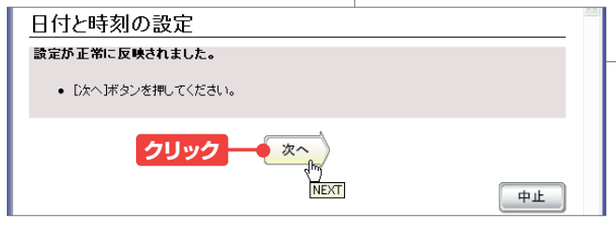
2 設定ウィザードの開始

「重要なお知らせ」のメッセージに記載されたリンク、もしくは「初期設定」メニューの「ウィザード」をクリック。表示された画面の「初期設定」ボタンを押すと、ウィンドウが別途表示されます。

3 日付と時刻の設定

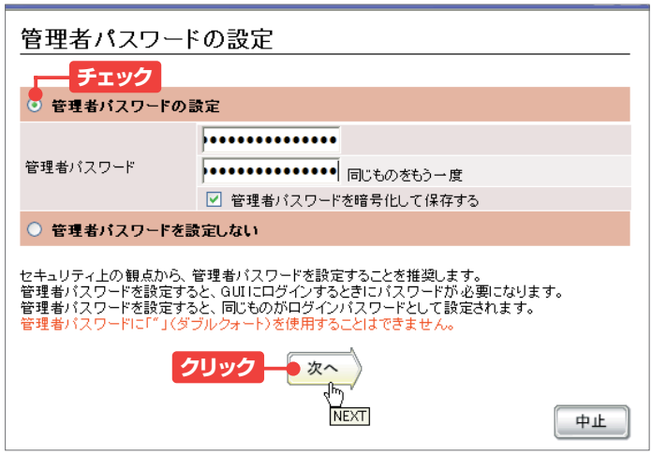
SRT100の日付と時刻を設定します。通常は「ルーターの時刻をPCの時刻に合わせる」を選択すればよいでしょう。設定を終了したら「設定の確定」ボタンを押します。次は時刻の設定が完了したことを表す画面です。「次へ」ボタンを押します。





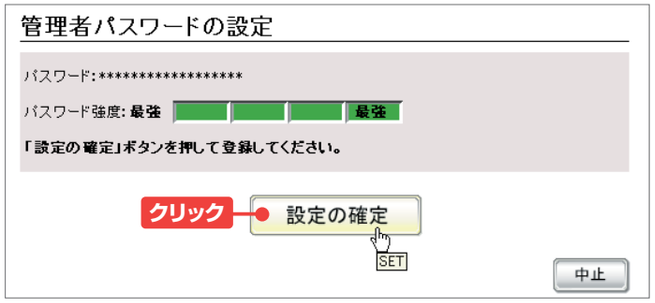
4 管理者パスワードの設定

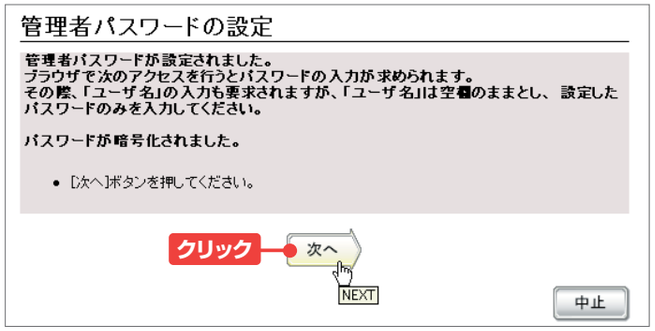
「管理者パスワードの設定」のチェックボックスをオンにして、SRT100にログインするときのパスワードを入力します。なお、SRT100では、アルファベットの大文字／小文字、数字、記号を混ぜた、15文字以上のパスワードが推奨されています。入力が完了したら「次へ」ボタンを押します。



5 設定の確認

パスワードの強度を確認したら、「設定の確定」ボタンを押します。次の画面ではパスワード入力時の注意点や、パスワード暗号化の有無を確認する画面です。





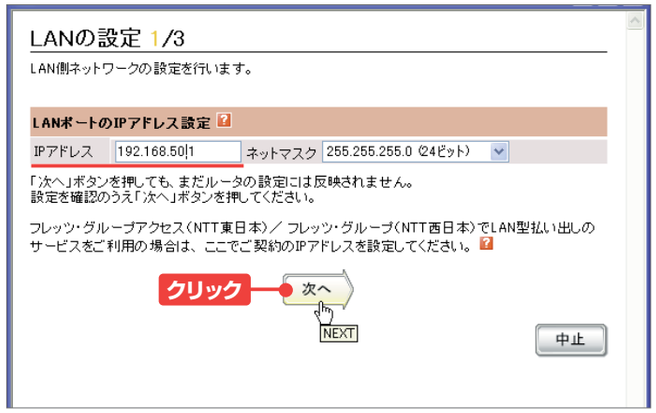
6 管理者のログイン

再度パスワード入力を求めるダイアログが表示されます。認証を通過すると、そのままLANの設定に移ります。

LANのIPアドレスとDHCPを確認しよう

7 IPアドレスの変更

LAN側のIPアドレスを設定します。このとき、異なる拠点のSRT100に、同じIPアドレスを割り振らないよう注意しましょう。たとえば、本社側のSRT100に「192.168.100.1」を設定していたら、支社側のSRT100には「192.168.50.1」を設定します。設定を終了したら「次へ」ボタンを押します。

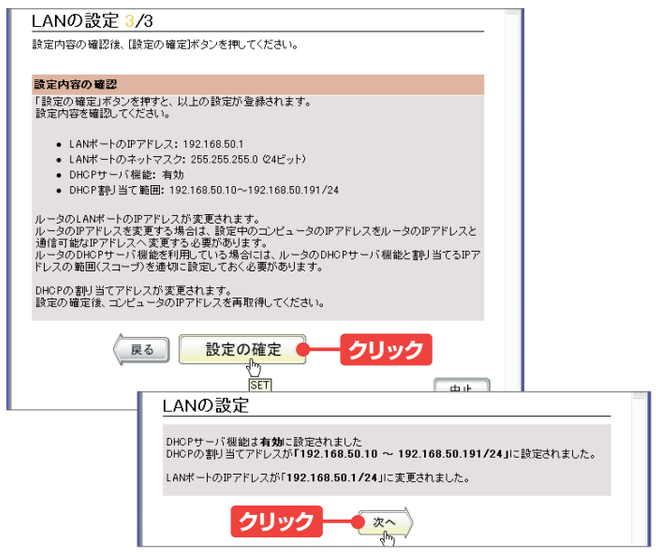


8 DHCPサーバの設定

DHCPサーバの設定でも、LAN側のIPアドレスに合わせて、IPアドレスの割り当て範囲を変えます。たとえば、IPアドレスを「192.168.50.1」に設定していたら、割り当て範囲も「192.168.50.10」～「192.168.50.191」などに変更します。設定を終了したら「次へ」ボタンを押します。

9 設定の確認

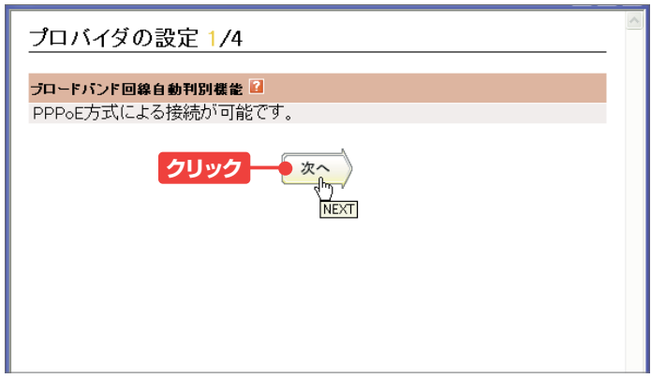
IPアドレスやDHCPサーバ機能の設定を確認する画面です。確認し終えたら「設定の確定」ボタンを押します。次の画面でLAN設定の変更箇所を確認したら、「次へ」ボタンを押します。
なお、ウィザードでIPアドレスを変更した場合は、設定用のPCが再度IPアドレスを取得する必要があります。その場合は、ケーブルをいったん抜いて再接続しましょう。



インターネット接続の設定を行なう

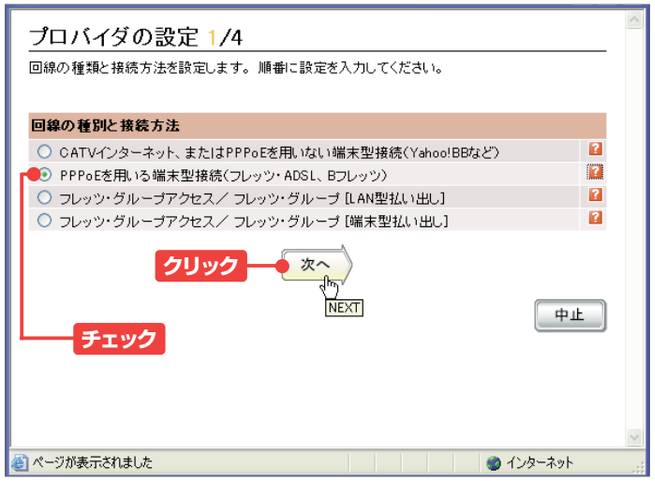
10 回線の自動判別

WANポートにケーブルが挿さっていれば、回線が自動的に判別され、回線の種類と接続方法が表示されます。判別結果を確認したら「次へ」ボタンを押します。



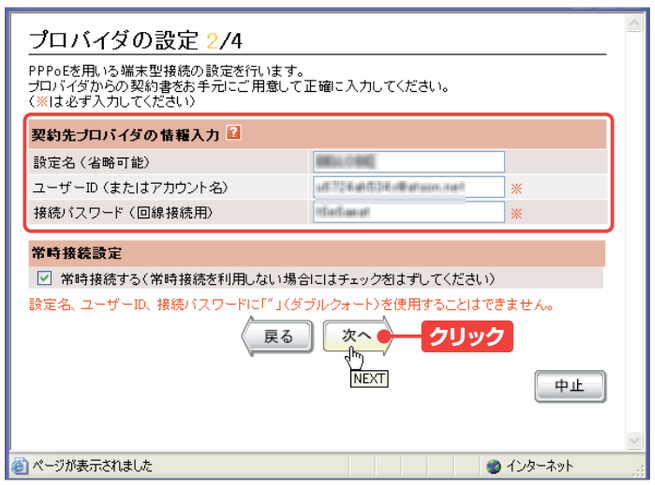
11 回線の自動判別

フレッツ・ADSLや、Bフレッツ（光回線）のような、PPPoEを用いたサービスを利用している場合は、「PPPoEを用いる端末型接続（フレッツ・ADSL、Bフレッツ）」を選択します。設定し終えたら、「次へ」ボタンを押します。



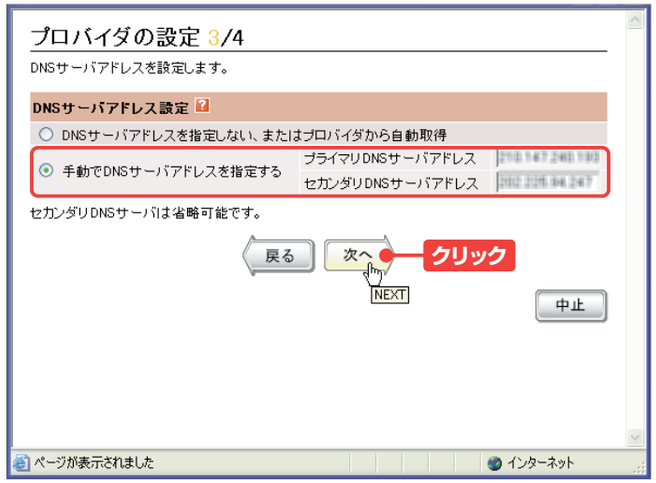
12 ユーザーIDの登録

「設定名」にはプロバイダ名などを入力しますが、省略してもかまいません。「ユーザーID」と「接続パスワード」には、プロバイダの契約書などで指定されたユーザーID（ユーザーアカウント）とパスワードを必ず入力します。通常は半角の英数記号で入力します。1文字でも間違えるとインターネットに接続できないので、正確に入力しましょう。



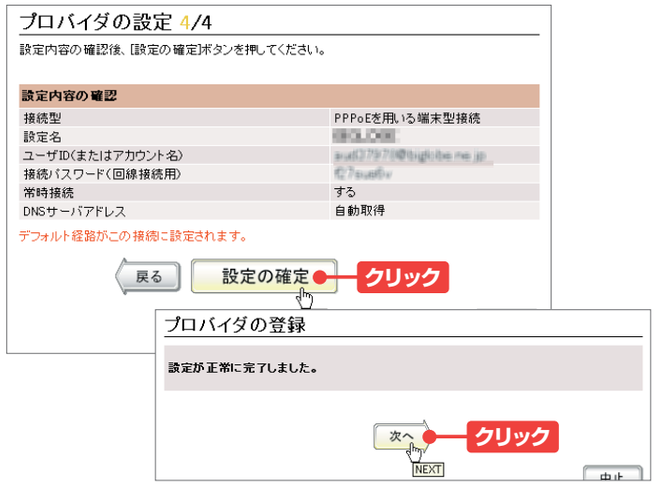
13 DNSサーバの指定

DNSサーバのアドレスを指定する場合は、プライマリDNSサーバアドレス、セカンダリDNSサーバアドレスの欄にプロバイダから指定されたアドレスを入力し、「次へ」のボタンを押します。プロバイダからDNSサーバが指定されていなければ、通常は自動的に取得されます。その場合は、上部の「DNSサーバアドレスを指定しない、またはプロバイダから自動取得」のチェックボックスをオンにして「次へ」ボタンを押せばOKです。



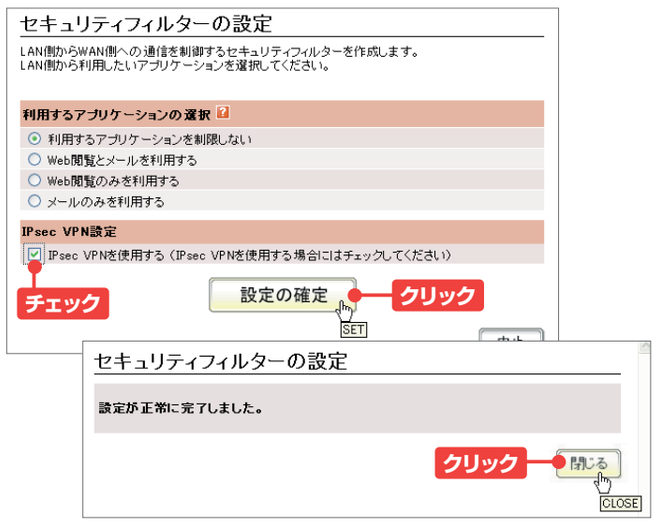
14 設定の確認

ここまでのプロバイダ設定が正しいかどうかを、最後に確認する画面です。正しければ、「設定の確定」ボタンを押します。プロバイダの設定が正常に完了したことを確認したら、「次へ」ボタンを押します。



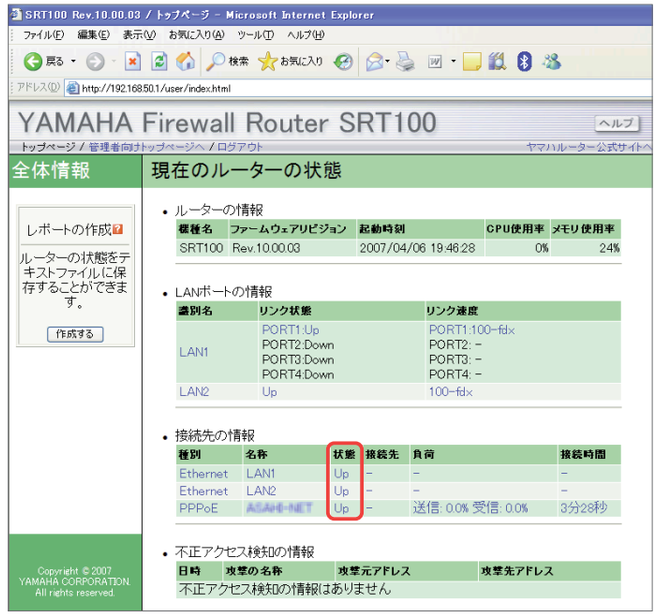
15 セキュリティフィルターの設定

VPNの接続時に利用するアプリケーションを選択します。たとえば、「Web閲覧とメールを利用する」を選択したら、ブラウザとメーラー以外のアプリケーションは通信できなくなります。また、IPsecによるVPNを構築する場合は、チェックボックスをオンにします。
選択を完了したら、「設定の確定」ボタンを押します。設定が正常に完了したことを確認したら、「閉じる」ボタンを押します。



16 接続の確認

無事に接続が行なわれている場合、トップページの「接続先の情報」にある「状態」欄に、「UP」が表示されます。



17 Webページを表示

トップページ右上の「ヤマハルーター公式サイトへ」をクリックして、Webページが正常に表示されることを確認しましょう。

インターネットにつなげなかったら？ Column

電話回線等を使うダイヤルアップ接続の時代と異なり、ADSLやFTTHを利用したインターネット接続の設定は、それほど複雑ではありません。ヤマハのSRT100のように、ルーターの設定も簡単なウィザードを用いることで完了してしまいます。そのため、インターネットに接続できない場合、チェックすべきポイントは少しです。

まずは物理的なケーブルの脱落です。初歩的なミスですが、コネクタのツメが折れていると、外れやすくなるので、注意しましょう。SRT100の前面にLEDがありますので、通信時にきちんと点灯するかチェックしましょう。

設定時の入力ミスとしては、プロバイダのPPPoEアカウントやパスワードなどが挙げられます。特にPPPoEのアカウントは英数字で20文字に及ぶこともありますので、間違いやすいようです。

DNSのアドレスを間違えると、プロバイダへの接続は「通信中」と表示されますが、URLとIPアドレスを相互変換する名前解決が不可能になるため、Webやメールなどが利用できなくなります。

Firewall&IDS

ファイアウォールとIDSの設定

SRT100の最大の特徴は、ファイアウォールをはじめとするセキュリティ設定のしやすさでしょう。日本語のGUIを使った設定ツールにより、不慣れなユーザーにとっても敷居の低いものになっています。ここではファイアウォールの基礎と設定を学びます。

増え続けるインターネットの脅威

ファイアウォールと不正アクセス検知

インターネットに接続する機器は、常時さまざまな攻撃や侵入にさらされます。そのためインターネットとLANの境界で動作するルーターには、ファイアウォール機能が必須になります。

ファイアウォールとは、あらかじめ設定したポリシーに基づき、パケットの通過や遮断を判断するアクセス制御の機能を指します。IPアドレスを元にインターネットからLANへの接続を拒否するというだけではなく、Webとメールは通過してOK、ファイル共有は遮断といった通信の制御が可能です。ルーターやファイアウォール専用機、スイッチなどのネットワーク機器に搭載されているほか、現在ではOSの標準機能としても利用されています。

もっとも一般的なファイアウォールの手法である「パケットフィルタリング」では、パケットのヘッダに書かれた宛先／送信元のIPアドレスやTCP/UDPポート番号などを元に、パケットの通過を判断します。その他、パケットのヘッダだけではなく、運ばれているユーザーのデータ自体を精査することで、高度なアクセス制御を実現する手法もあります。

一方、不正アクセス検知は、通常のファイアウォールでは防げない攻撃を検出する機能で、一般的にはIDS（Intrusion Detection System）と呼ばれます。攻撃パターンを識別したシグネチャと呼ばれるデータベースとパケットを照らし合わせることで、攻撃の検出を実現しています。シグネチャはベンダーから提供されており、インターネット経由で更新することで最新の攻撃に対応できます。

さらに検出するだけではなく、遮断まで行なう機能をIPS（Intrusion Prevention System）と呼びます。

SRTのセキュリティ機能

SRT100では、「入力遮断フィルター」「不正アクセス検知（IDS）」、「ポリシーフィルター」など複数のフィルターを使って、不正アクセスを遮断します。おおまかな流れは右ページの図1のとおりです。

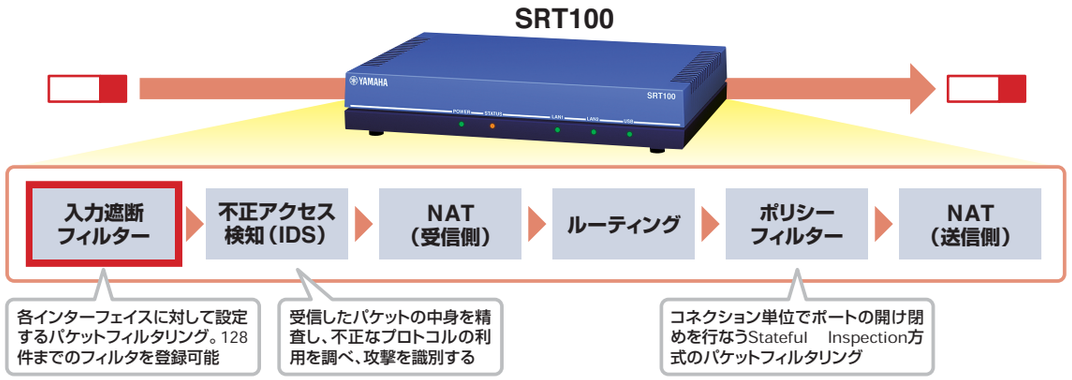
・入力遮断フィルター

静的なパケットフィルタリング。始点／終点のアドレス、プロトコル種別、始点／終点のポート番号などを条件にしたフィルター設定により、パケットの通過と遮断を判断します。フィルター設定は各インターフェイスに対して128件まで付けることができ、パケットを受信すると、フィルターのリストを上から照らし合わせ、指定した動作を行ないます。

・不正アクセス検知

受信したパケットの構造やパラメータなどを精査し、侵入や攻撃を目的にしたパケットを捕捉し遮断するIDS・IPS機能です。入力遮断フィルターの直後に処理を行ないます。

図1 SRT100のセキュリティ処理



・ポリシーフィルター

コネクション単位で通過／遮断が可能なステートフルインスペクション方式のパケットフィルタリングです。始点／終点インターフェイス、始点／終点アドレス、サービスなどで条件を設定でき、入力遮断フィルターより高度なアクセス制御が可能になっています。

このほか、WebサイトのURLを元にフィルタリングすることも可能です。このURLフィルタングは、おもにLAN内のコンピュータを用いる従業員が、不正なWebサイトを閲覧しないよう、外部のデータベースと連携し、アクセスに制限をかけるものです。

SRT100では、ファイアウォールやIDSなどさまざまなセキュリティ設定をGUIで容易に行なえるようにしています。たとえば、各種フィルターの設定画面ではフィルター適応時の動作をアイコンでわかりやすく表示しています。

ファイアウォール設定の基本

具体的な、ファイアウォールの設定についてポリシーフィルターを例に解説していきましょう。

入力遮断フィルターでは、インターフェイスを単位として、パケットのアクセス制御を行ないます。これに対してポリシーフィルターでは、どのインターフェイスからどのインターフェイスに流れるのかといった横断的な条件でフィルターを設定できます。

パケットを特定する条件としては、送受信インターフェイス、宛先／送信元アドレス、サービスなどが利用可能です。実際、「ポリシーフィルター」メニューを開くと、「グループとユーザー定義サービスの一覧」にはあらかじめインターフェイス（Private/PP1/VPNなど）、アドレス（Private、Any）、サービス（HTTP、General）などの「条件」が定義されています。もちろん、ユーザー自身でアドレスやサービスを定義して追加することも可能です。そして、これらの条件に合致したパケットに対して破棄や通過、ログの収集、接続時のみ通過といった実際の「動作」を決めていくわけです。

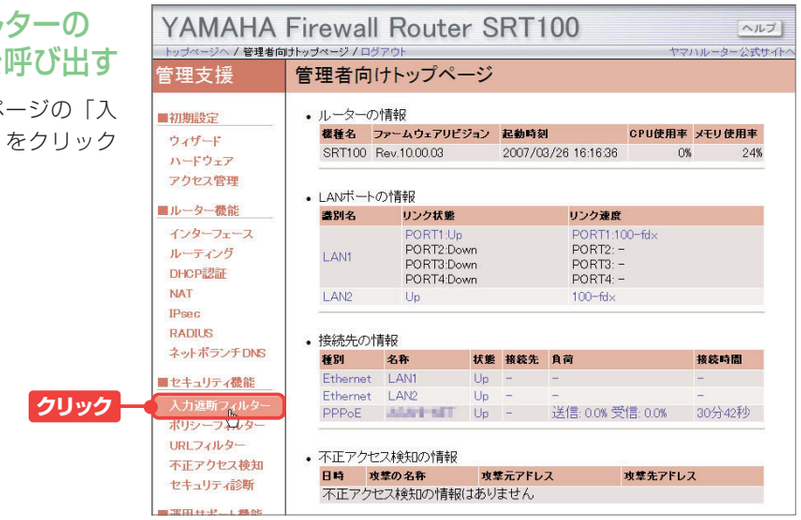
この設定された条件と動作の組み合わせを「ポリシー」と呼び、これらを実行順にまとめたものを「ポリシーセット」と呼びます。初期状態では「Internet Access」というポリシーセットが適用されており、「ポリシーセットの詳細」という条件と動作を階層化表示できます。ポリシーセットは最大128件のポリシーを登録でき、ポリシーセット自体は3件まで設定可能です。

さらにSRT100では新機能として、通信状態により適用するポリシーセットを動的に変更する「動的ポリシー変更機能」が提供されています。たとえば、Winnyのトラフィックを検知した際に、外部の通信を一時的に遮断するといった措置を採ること可能です。

入力遮断フィルターの確認と追加

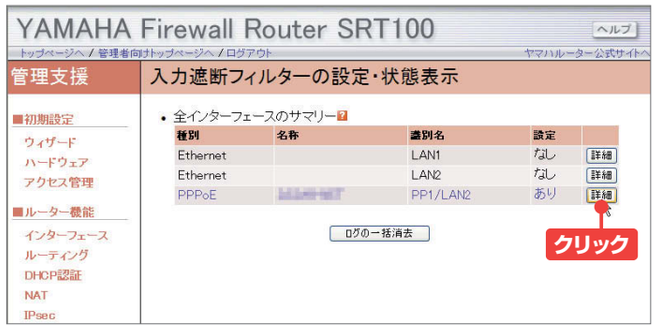
1 入力遮断フィルターの設定メニューを呼び出す

管理者向けトップページの「入力遮断フィルター」をクリックします。



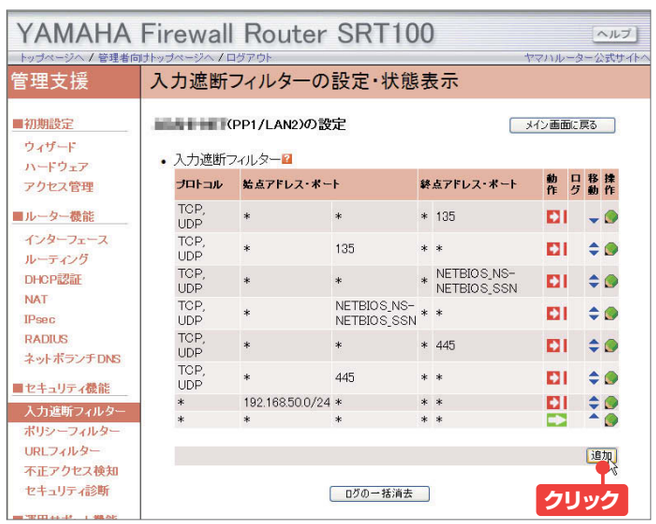
2 確認したいインターフェイスを選択

「全インターフェイスのサマリー」から、インターネット接続を行なっている「PPPoE」の「詳細」ボタンを押します。



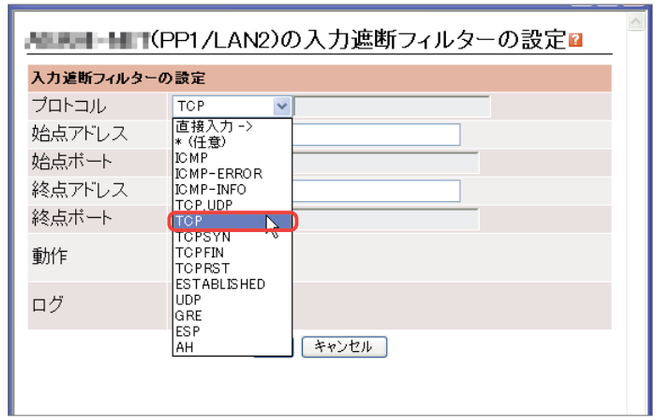
3 初期状態の入力遮断フィルター

デフォルトでは、ポート135/445などを使うWindowsのファイル共有プロトコルのパケットが通らないような設定になっています。
フィルターを追加する場合は「追加」ボタンを押します。



4 入力遮断フィルターの設定

ここではTCP23番ポートを用いるTelnet接続を内側から利用するのを禁止してみましょう。まずは「プロトコル」から「TCP」を選択します。

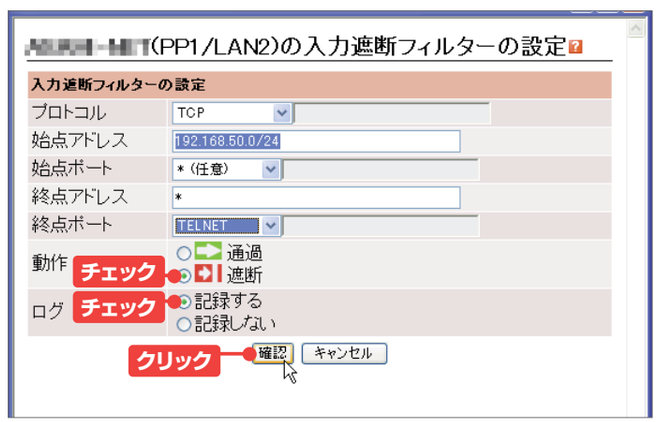


5 始点アドレスとポート

始点アドレスには、対象となるLAN内のホストに割り当てられるアドレスの範囲（ex.192.168.50.0/24）を指定します。終点アドレスは任意を意味する「*」、そして終点ポートは「TELNET」を選択します。

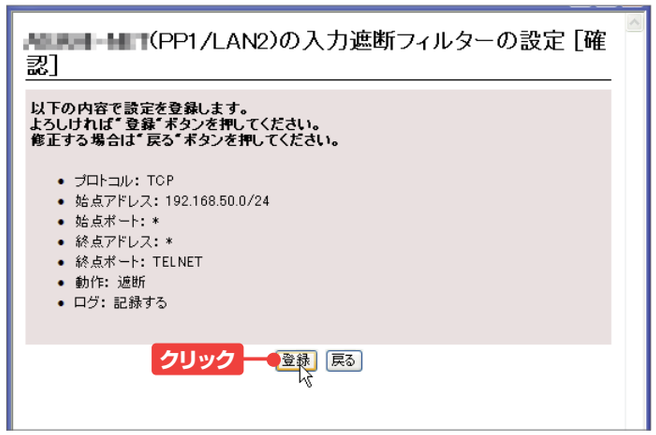
6 入力遮断フィルターの設定

動作は忘れず「遮断」を指定。ログを記録するのであれば「記録する」をオンにします。「確認」ボタンを押します。



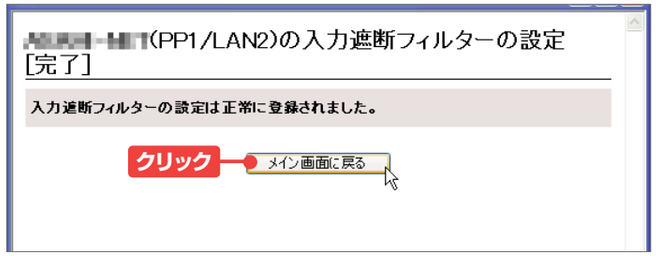
7 登録内容の確認

登録内容が表示されるので、OKであればそのまま「登録」ボタンを押します。



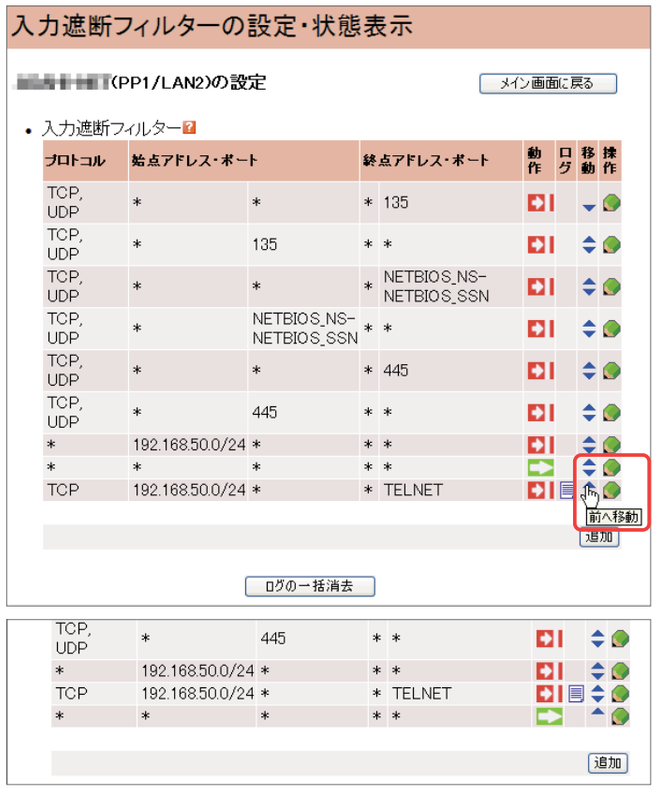
8 登録が完了

登録が完了したら、「メイン画面に戻る」ボタンを押します。



9 入力遮断フィルターの一覧に反映

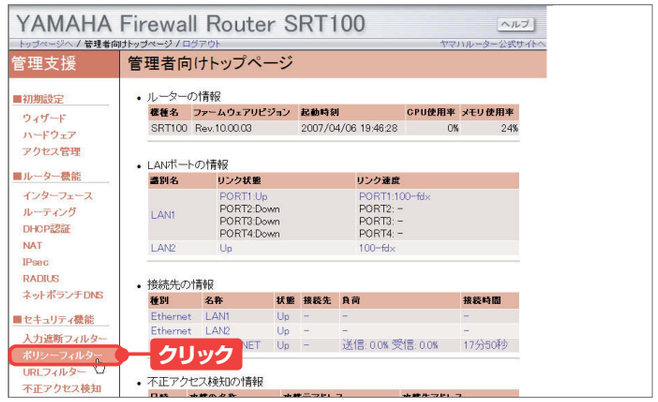
追加した設定はフィルターの最下列に追加されます。フィルターがオンになるよう「移動」メニューで、作成したフィルターを最後列にあるall passフィルターの前へ移動します。



ポリシーセットの追加

1 ポリシーセットの設定メニューを呼び出す

管理者向けトップページの「ポリシーフィルター」をクリックします。

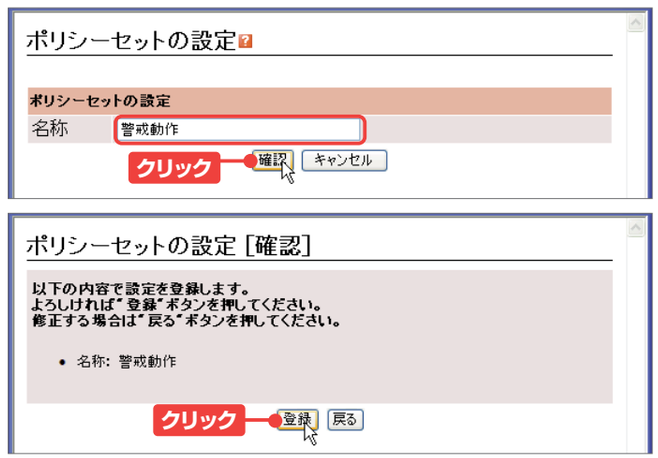


2 ポリシーセットの追加

ポリシーセットは同時に1つのみ稼働させられます。初期設定のウィザードでセキュリティフィルターの設定を行なうと、「Internet Access」というポリシーセットが登録されます。
Winnyのパケットを検知した場合などに、特別なポリシーセットを適用したい場合は、「ポリシーセットの一覧」にある「追加」ボタンを押します。

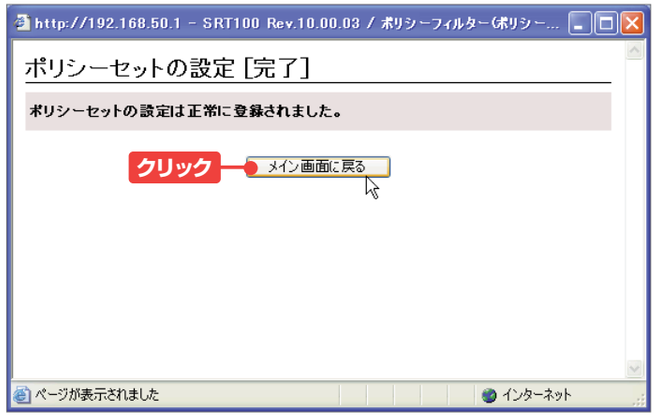
3 ポリシーセットの名称設定

ポリシーセットの内容がわかるような名前を設定します。たとえば、「警戒動作」などとして、「確認」ボタンを押します。ポリシーセットの名前を確認したら、「登録」ボタンを押します。



4 設定の確認

正常に登録されたことを確認したら、「メイン画面に戻る」ボタンを押します。



5 ポリシーセットの詳細設定

新しく作成した「警戒動作」のポリシーセットには、ポリシーフィルターが何も設定されていません。ポリシーフィルターを追加するには、「ポリシーセットの詳細」欄のドロップダウンリストから、新しく作成したポリシーセットを選択します。

6 ポリシーフィルターの追加

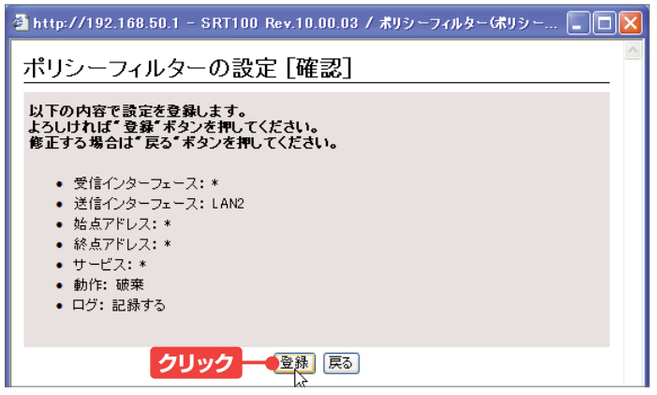
「ポリシーセットの詳細」欄の「追加」ボタンを押します。

7 ポリシーフィルターの設定

ポリシーフィルターの設定画面が表示されます。この画面で、Winnyを検知した場合に適用するためのポリシーフィルターを設定します。
受信/送信インターフェイスのフィルターを設定します。たとえば、WANポートからのパケット送信を禁止する場合は、送信インタフェース「LAN2」（WAN）を選択します。
「動作」の欄で「破棄」のチェックボックスをオンにします。
フィルター動作時のログを取るなら、「記録する」のチェックボックスをオンにします。
すべての設定を完了したら、「確認」ボタンを押します。

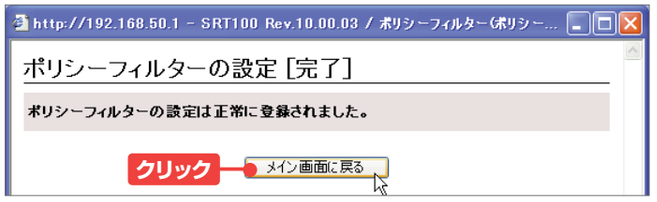
8 設定の登録

ポリシーフィルターの設定内容を確認したら、「登録」ボタンを押します。



9 設定の完了

ポリシーフィルターの設定が正常に登録されたら、「メイン画面に戻る」ボタンを押します。



複数ポリシーセットの自動切り替え

1 ポリシーフィルターの追加

設定したポリシーがポリシーセットに反映されます。さらにポリシーを追加する場合は、「操作」欄の鉛筆アイコンをクリックし、メニューから「並列に追加」を選択します。

2 ポリシーフィルターの設定

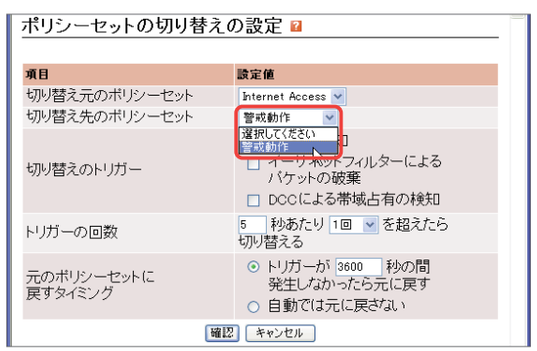
ポリシーフィルターの設定画面が表示されます。WANの送信インタフェース以外はすべて通過を許可するため、ここでは何も設定せずに、「確認」ボタンを押します。あとは、設定を確認－登録し、メイン画面に戻ります。

3 ポリシーセットの自動切り替え

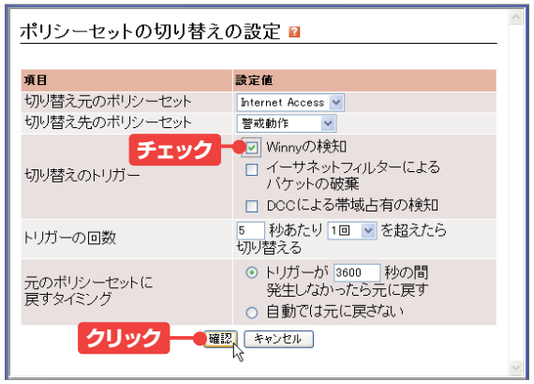
続いて、新しく作成したポリシーを稼動させる条件を設定します。メインで稼動するポリシーセットの下にある「追加」ボタンを押します。

4 自動切り替えの設定

「切り替え先のポリシーセット」のドロップダウンリストから、特別な場合にのみ稼動させたいポリシーセットを選択します。

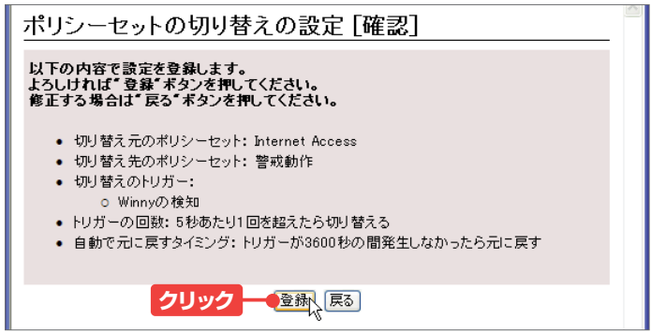


切り替えを実行するトリガー（実行条件）を選択します。
初期設定では、異常を検知してから3600秒間なにも起きなければ、元のポリシーセットに戻ります。この設定は自由に変更することが可能です。また、自動では元に戻さない設定にすることもできます。すべての設定を済ませたら、「確認」ボタンを押します。



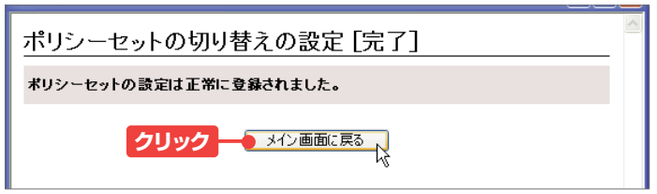
5 設定の登録

設定の内容を確認したら、「登録」ボタンを押します。ここではWinnyを検知すると警戒動作に切り替わります。



6 設定の完了

設定が正常に登録されたことを確認し、「メイン画面に戻る」ボタンを押します。



7 切り替え先の確認

平常時に稼動させるポリシーセットの「切り替え先」欄に、異常時に稼動させるポリシーセットが表示されました。

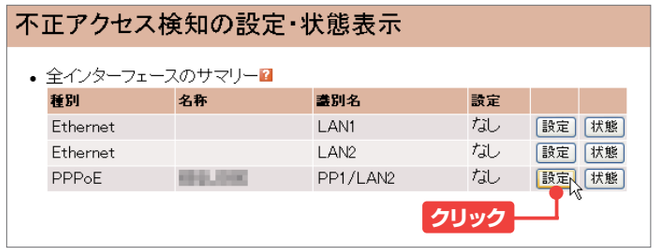
不正アクセス検知

1 設定画面を呼び出す

管理者向けトップページの「不正アクセス検知」をクリックします。

2 インターフェイスの選択

表示されたインターフェイスのなかから、不正アクセス検知機能を設定したいインターフェイスを選んで、「設定」ボタンを押します。

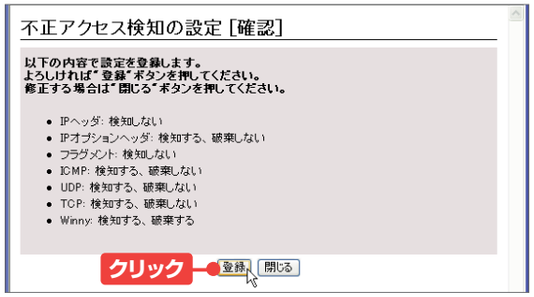


3 不正アクセス検知の設定

不正アクセスの可能性があるパケットのリストが表示されるので、検知したいパケットのチェックボックスをオンにします。検知と同時に削除したい場合は、「破棄」のチェックボックスもオンにします。
すべての設定が完了したら、画面下部の「適用」ボタンを押します。

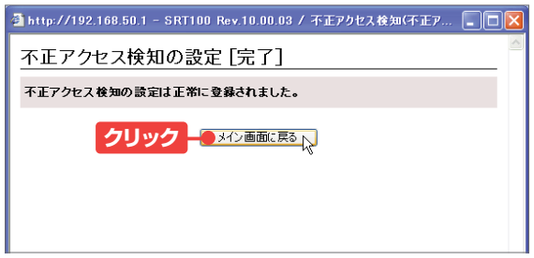
4 設定の確認

不正アクセスの検知を設定したパケットの種類を確認したら、「登録」ボタンを押します。



5 設定の完了

検知の設定が正常に登録されたことを確認したら、「メイン画面に戻る」ボタンを押します。次の画面でも「メイン画面に戻る」ボタンを押します。



6 状態の表示

検知を設定したインターフェイスの「状態」ボタンを押します。

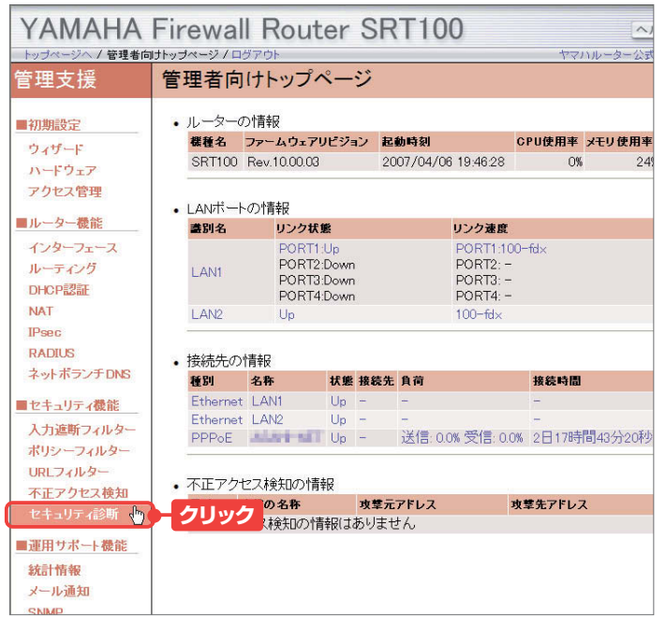
7 検知結果の確認

不正なパケットを検出した場合は、該当するパケットの検知回数が表示されます。

セキュリティ診断

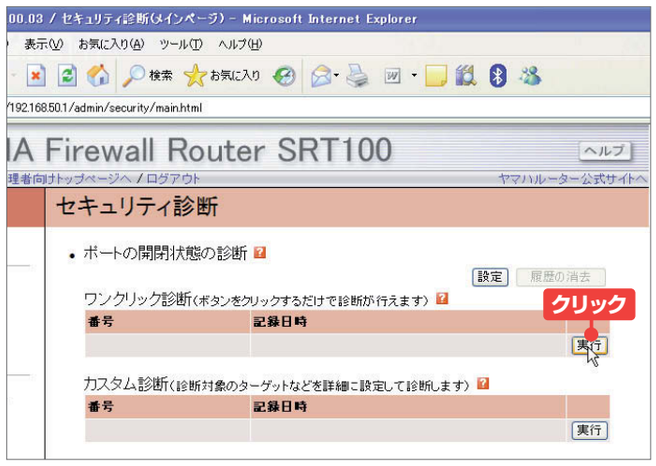
1 セキュリティ診断の画面を呼び出す

解放されているポートを調べます。まず、管理者向けトップページの「セキュリティ診断」をクリックします。



2 ポートの開閉状態を診断

「ワンクリック診断」の「実行」ボタンを押します。

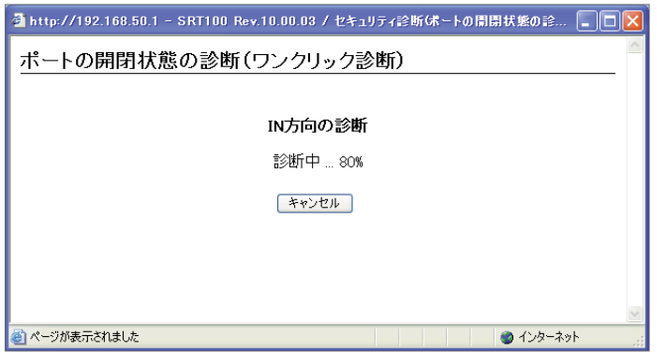


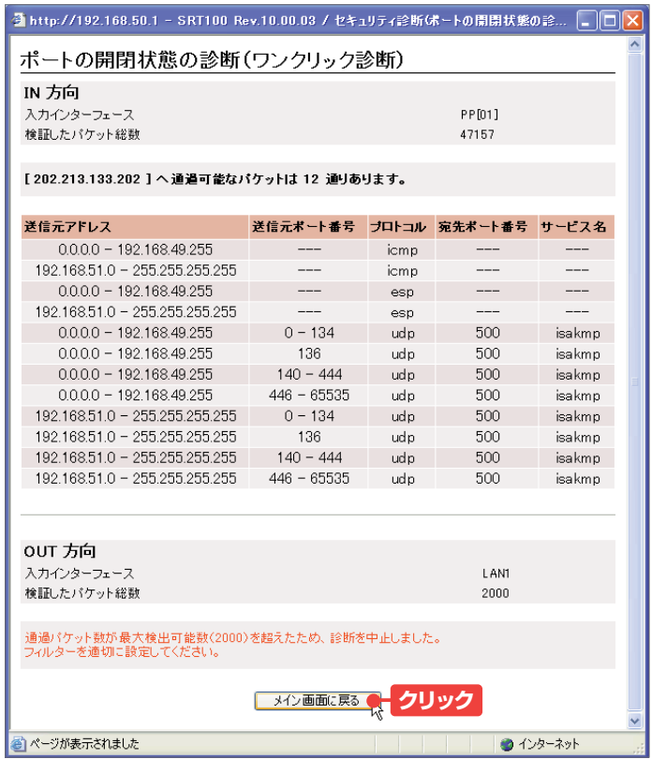
3 診断の実行

診断条件を確認して、「実行」ボタンを押します。診断結果が表示されるまでには、数十秒かかることもあります。

4 診断結果の表示

診断結果が表示され、各入力インターフェイスで通過可能なパケットの種類がリストアップされます。結果を確認したら、画面下部の「メイン画面に戻る」ボタンを押します。





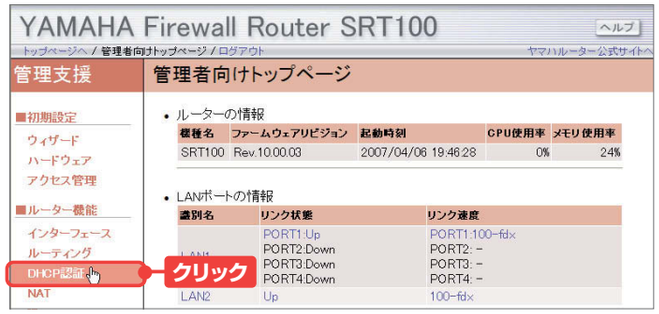
5 診断結果の再表示

「ワンクリック診断」を実行した日時と、実行の順番が表示されます。過去に実行した診断を再表示するには「表示ボタン」を押します。

DHCP認証を設定する

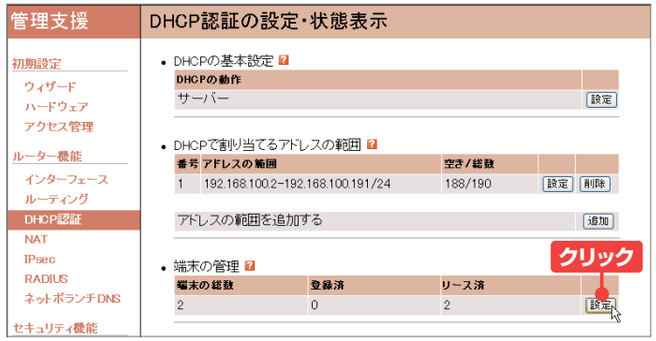
1 DHCP認証のメニューを呼び出す

DHCP認証を設定する前に、接続を許可するコンピュータとSRT100を、LANケーブルで接続します。接続が完了したら、管理者向けトップページの「DHCP認証」をクリックします。



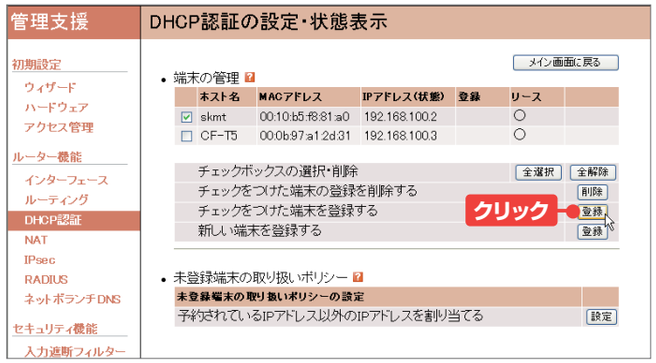
2 端末の管理

「DHCP認証の設定・状態表示」のページで、「端末の管理」の「設定」ボタンを押します。



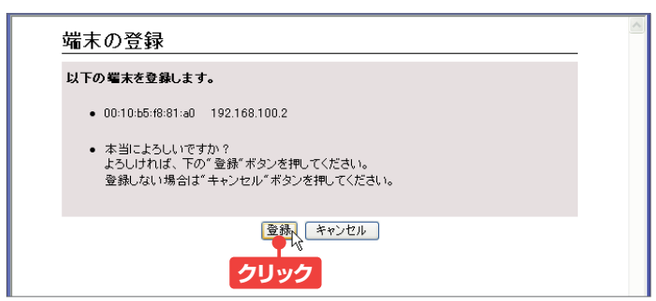
3 端末の登録

接続を許可するコンピュータにチェックを入れ、「登録」ボタンを押します。



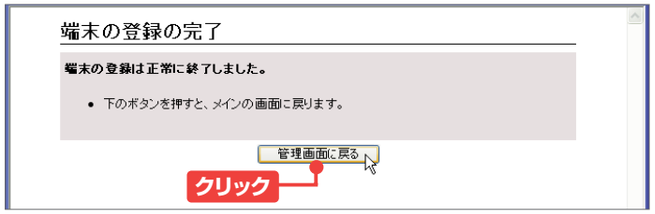
4 設定の確認

登録するコンピュータのMACアドレスとIPアドレスを確認したら、「登録」ボタンを押します。



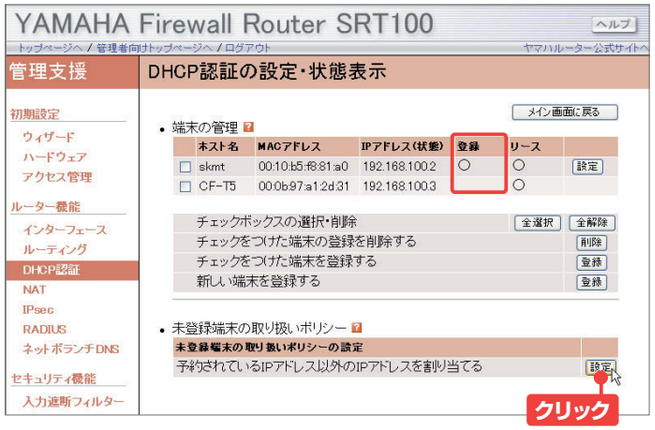
5 登録の完了

「管理画面に戻る」ボタンを押して、「DHCP認証の設定・状態表示」画面に戻ります。



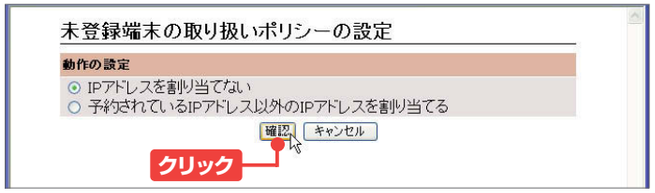
6 未登録端末の設定

登録したコンピュータの「登録」欄に、○のマークが表示されます。登録されたコンピュータを確認したら、「未登録端末の取り扱いポリシー」の「設定」ボタンを押します。



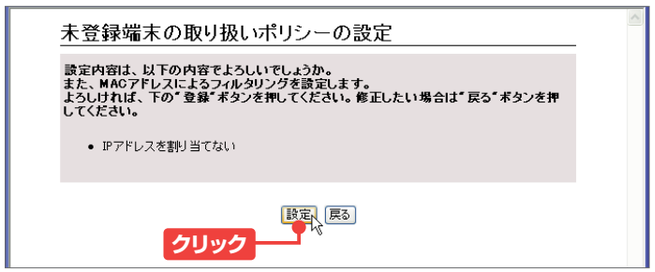
7 通信の禁止

「IPアドレスを割り当てない」のチェックボックスをオンにして、「確認」ボタンを押します。



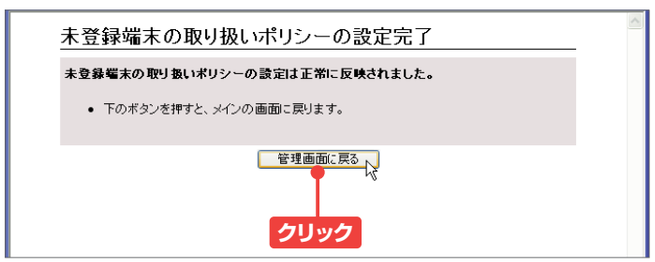
8 設定の確認

変更内容を確認したら、「設定」ボタンを押します。



9 設定の終了

「管理画面に戻る」ボタンを押して、設定を終了します。以降は、登録されたコンピュータだけが、SRT100を経由して、ネットワークを利用できるようになります。



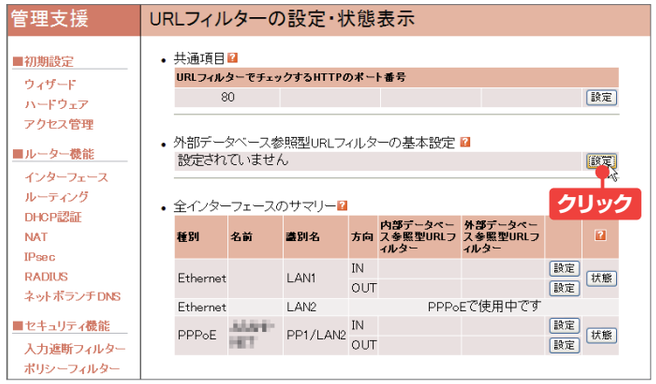
URLフィルターを設定

1 URLフィルターを選択

「セキュリティ機能」から「URLフィルター」を選択します。

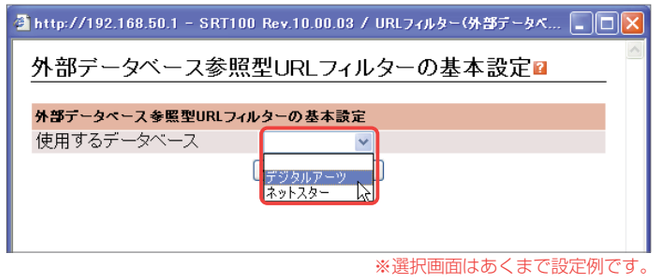
2 外部データベースを参照

URLフィルターはユーザー自身が自前でデータベースを作成して参照させることもできますが、ここではサードパーティのデータベースを利用するURLフィルター設定を行ないます。
外部データベース参照型URLフィルターの基本設定の「設定」ボタンを押します。



3 利用するデータベースを選択

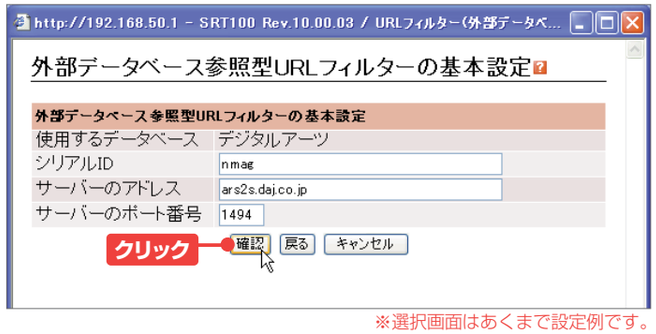
データベースの参照サービスは、ネットスターとデジタルアーツのデータベースが選べます。自身が加入したサービスを選択し、「次へ」のボタンを押します。



※選択画面はあくまで設定例です。

4 シリアルIDの入力

サービスのシリアルIDを入力します。サーバのアドレスやポート番号はあらかじめ入力されています。「確認」ボタンを押して、確認画面が出てきます。あとは「登録」ボタンを押せば設定は完了します。



※選択画面はあくまで設定例です。

VPN

VPNで安全な通信路を構築せよ

本社のLANと支社のLANをつなぐためには、今まで主に専用線を使っていました。しかし、最近ではインターネットを経由して、安価に、しかも安全にLAN同士をつなぐことができます。これを実現するための技術が、VPN（Virtual Private Network）です。

LANやコンピュータ同士を安全につなぐVPN

VPNは、インターネットや通信事業者が持つ公衆ネットワークを使って、企業の拠点間を仮想的に接続する技術の総称です。公衆ネットワークの中に、誰にも邪魔されない専用線を引いてしまう技術ということです。

VPNを実現するための技術はいくつもありますが、その代表はIPsec（Security Architecture for Internet Protocol）というプロトコルを使ったインターネットVPNです。IPsecに対応したルーターで、地理的に離れた拠点のLAN同士にトンネルを張ります。これをユーザーから見ると、遠隔にあるLANがまるで同じ社屋の異なるサブネットにあるかのように利用できます。

VPNやIPsecを理解するうえで、特に重要なのが「トンネリング」と呼ばれる概念です（図1）。トンネリングとは、インターネット上に、あたかもトンネルのように仮想的な専用線を作る（掘る）ことを指します。実際、拠点間をつなぐ通信路のことをトンネルと呼びます。このトンネリングを実現するためには、パケットの「カプセル化」という技術が利用されます。カプセル化とは、元のパケットを別のパケットで包み込むことです。では、なぜこうしたカプセル化が必要になるのでしょうか？

現在、多くのLANのコンピュータには、プライベートアドレスが割り当てられています。プライベートアドレスとは、閉じられたLANで用いることのできるIPアドレスで、インターネットでは利用できません。そこで、前述したカプセル化を利用し、本来LAN内でしかやり取りできないプライベートアドレス宛のパケットを、グローバルアドレスのヘッダでカプセル化し、インターネットに流すのです。

もう少し具体的に見ていきましょう。インターネットVPNで接続されたLAN同士は、図2のようにVPNルータで相互接続されています。LAN内のコンピュータからプライベートアドレス宛の

図1 IPsecのトンネリング

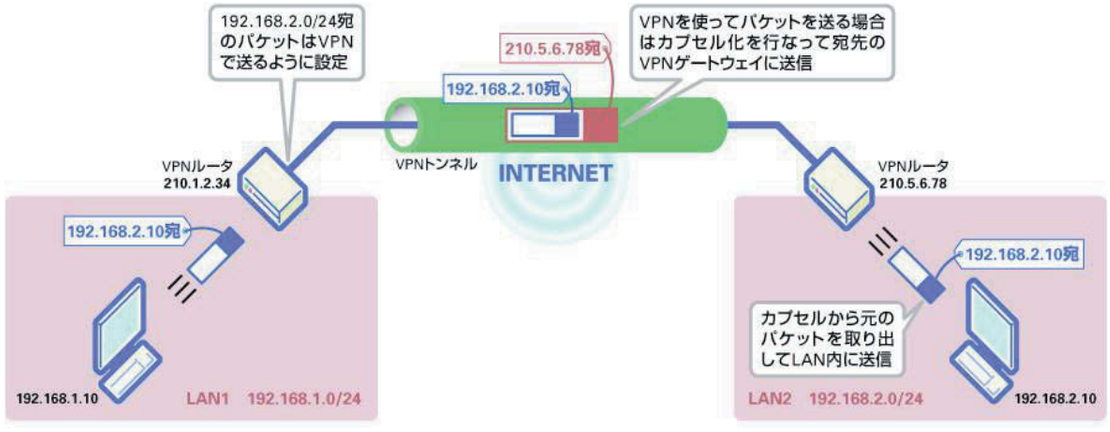
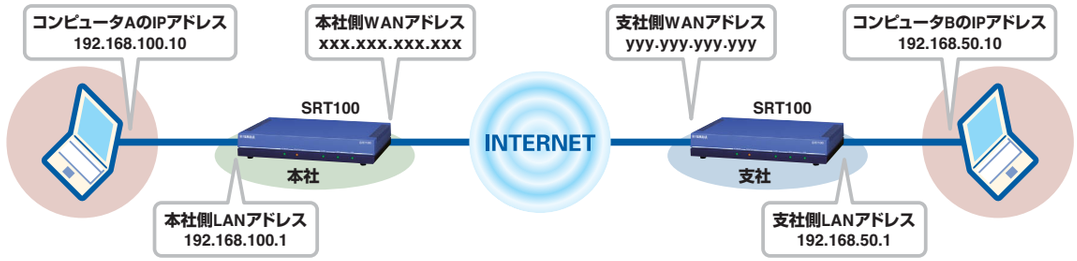


図2 IPsecのセキュリティ機能



パケットがVPNルーターに届くと、VPNルーターはグローバルアドレスをつけて送信します。つまり、LAN間（VPNのトンネル内）でやり取りされるパケットのデータ部（ペイロード）に、プライベートIPアドレスを宛先とした元のパケットがカプセル化されるのです。一方、受信側のVPNルーターは、受け取ったパケットからプライベートIPアドレスのパケットを取り出して宛先のコンピュータに送信します。これにより、グローバルアドレスのみしか使われないインターネット経由で、プライベートアドレスで構築されているLAN同士の通信が行なえるのです。

IPsecでは「ESP（Encyption Security Payload）」や「AH（Authentication Header）」といったプロトコルで、元のIPパケットをカプセル化します。これらのプロトコルは後述するセキュリティの機能も持っており、暗号化や認証などが実現されています。

IPsecのセキュリティ機能

ただし、パケットがインターネット上を平文のまま流れてしまうのは危険です。不特定多数のユーザーが利用する現在のインターネットでは、全員が善良なユーザーだとはいえません。こうした背景からIPsecでは盗聴や改ざん、なりすましなどを想定した接続先認証、パケットの暗号化／認証という各種のセキュリティ機能が用意されています。

まず、VPNのトンネルを構築する相手が正当かどうかを調べる「接続先認証」という機能も持っています。これはVPNのトンネルを構築する機器が「事前共有鍵」という鍵を共有することで、お互いを認証することでなりすましを防止します。

また、IPsecではパケットの中身が暗号化されており、悪意の第三者が勝手に盗聴や改ざんなどを行なえないようになっています。暗号化の方式としては、通信の送り手と受け手が同じ鍵を使ってデータやり取りする共通鍵暗号を採用します。IPsecではアルゴリズムとして、「DES（Data Encryption Standard）」「3DES（トリプルDES）」「AES（Advanced Encryption Standard）」などと呼ばれる方式が採用されています。

通常、この共通鍵暗号を使う場合、安全な鍵の受け渡しをいかに行なうかがテーマになります。しかし、IPsecではIKE（Internet Key Exchange）というプロトコルを使うことで、安全に鍵の交換が行なえます。IKEでは鍵を生成するための素材を交換するだけで、鍵を直接ネットワークに流しません。鍵が漏れなければ、その鍵で暗号化したデータ通信も安全というわけです。

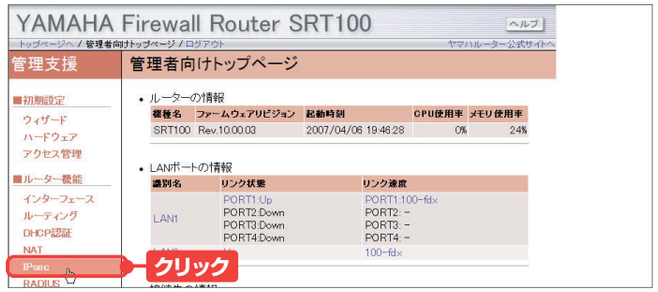
さらに、不正なパケットの改ざんを検出するための「パケット認証」という機能も用意されています。これは「ハッシュ関数」で計算されたダイジェストという数値をパケットに付けることで、実現されています。ダイジェストは、不正に改ざんされると値が変わってしまうので、送信元と接続先でその値を照らし合わせることで送信元のパケットが正しく届いたかが判断できるのです。

こうした一連のVPNの処理を行なうのが、VPNルーターやセキュリティゲートウェイと呼ばれる装置です。今回はヤマハのVPNルーターを使って、IPsecによるVPN構築を試してみます。

トンネルの追加とVPN設定

1 VPN設定のメニューを呼び出す

管理者向けトップページの「ルーター機能」から「IPsec」をクリックします。

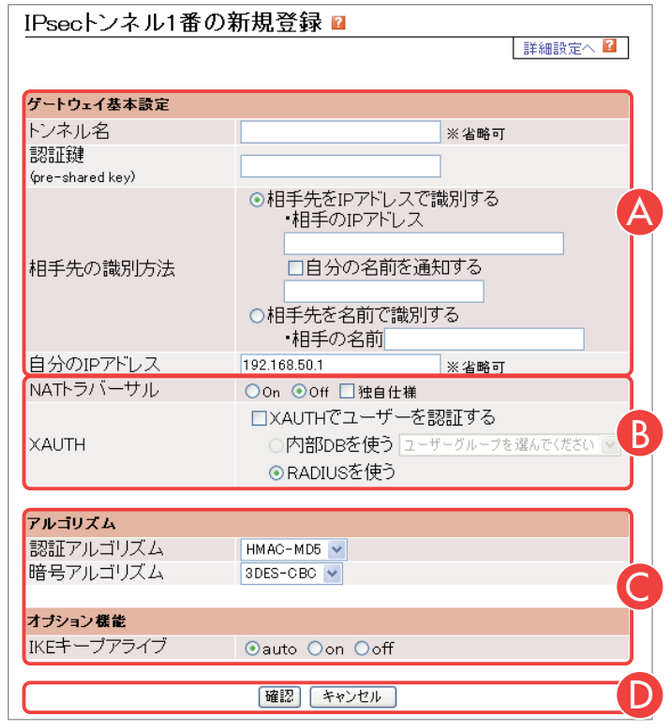


2 VPN接続の設定

「IPsecの設定・状態表示」のページの下部にある「新規登録」ボタンを押します。

3 VPN接続設定の登録

VPN設定の画面が表示されます。このページの設定をひととおり行なえば、IPsecによるトンネルを構築する準備が整います。詳細は次ページ以降で解説します。



トンネル名
接続名を任意に設定します。たとえば、接続先が東京の本社であれば「tokyo-office」、浜松の支社であれば「hamamatsu」などと入力すればよいでしょう。省略も可能です。

認証鍵 (pre-shared key)
IPsecにおいて、データの暗号化に必要な鍵を指定します。鍵といっても実際はパスワードと同じような半角英数字の羅列になります。事前共有鍵(pre-shared key)という名前の通り、対向のルーターには、同じ文字列を入力しなければなりません。

NATトラバーサル
NATの配下にあるVPNルーター／クライアントからのトンネル構築を容易にするNATトラバーサルの有無を選択します（NATトラバーサルに関しては39ページ keyword参照）。ヤマハのルーターやVPNクライアントと利用する場合は、「on」「独自」のチェックボックスをオンにする。

A

ゲートウェイ基本設定	
トンネル名	hamamatsu ※省略可
認証鍵 (pre-shared key)	Qg/B1-iYb~n$A)r8>IO
相手先の識別方法	◉相手先をIPアドレスで識別する ・相手のIPアドレス yyy.yyy.yyy.yyy □自分の名前を通知する ○相手先を名前で識別する ・相手の名前
自分のIPアドレス	192.168.50.1 ※省略可

自分のIPアドレス
LAN側のIPアドレスを入力しますが、省略しても構いません。

相手先の識別方法
接続先のWAN側IPアドレス（例では支社側のWANアドレス）を入力します。両者で固定のグローバルアドレスを使っている場合は、お互いのIPアドレスを入力すればよいわけです。「自分の名前を通知する」のチェックボックスを選択した場合は、主にWAN側のIPアドレスが固定で割り当てられないときに名前で識別します。半角の英数記号で任意の名前を入力します。「名前で識別」の欄には、支社側のルーターが名前を使っていた場合に、その名前を入力する欄です。

B

NATトラバーサル	◉On ○Off □独自仕様
XAUTH	☑XAUTHでユーザーを認証する ○内部DBを使う ユーザーグループを選んでください ◉RADIUSを使う

XAUTH
ヤマハのVPNクライアントソフトウェア「YMS-VPNI」を使い、外部認証機能を利用して、ユーザーを認証する方式を指定します。「XAUTHでユーザーを認証する」を有効にすると、認証サーバー（RADIUS）や内部データベースなどの認証機能を利用することができます。なお、「内部DBを使う」を選択するためには、IPsecの設定でユーザーやユーザーグループを登録する必要があります。

XAUTHとRADIUS
Column

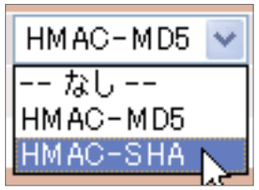
XAUTHは「eXtended AUTHentication」の略で、エックスオースと読みます。IPsecではルーターや端末を認証できても、「機器を操作するユーザー」を認証する仕組みがありません。そのため、認証済みのコンピュータを使用した悪意の第三者に対しては、まったくの無防備になります。この弱点を補うのが、XAUTHです。通常のIPsecの認証に加えて、さらにIDやパスワードで認証することで、端末だけでなく利用者の認証も可能にします。また、認証にRADIUSサーバーを使用すれば、接続時間や操作履歴を記録する「アカウンティング」も可能になります。

SRT100でのRADIUSサーバーの設定は設定ツールの「ルーター機能」の「RADIUS」を選択。開いた画面でRADIUSサーバのIPアドレスや、認証／アカウンティングの有無、ポート番号などを指定すればOKです。

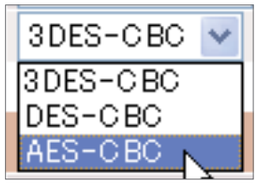
C

アルゴリズム	
認証アルゴリズム	HMAC-SHA
暗号アルゴリズム	AES-CBC
オプション機能	
IKEキープアライブ	◉auto ○on ○off

認証アルゴリズム
IPsecでは通信相手が本物かどうか（本人性確認）、そして経路上でパケットが改ざんされていないかをチェックする（完全性保証）という2つの認証が用いられます。これを実現するアルゴリズムが「MD5」と「SHA」です。SRT100ではさらに鍵を付けて安全性を高める「HMAC」という手法が組み合わせられています。そのため、設定は「なし」、「HMAC-MD5」、「HMAC-SHA」の3つから選択でき、デフォルトは「HMAC-MD5」です。ただし、強度がもっとも高いのは「HMAC-SHA」です。接続先でも同じアルゴリズムを選択する必要があります。



暗号アルゴリズム
パケットの暗号化を行なうためのアルゴリズムを選択します。IPsecでは通信するルーター同士が同じ鍵を使ってパケットを暗号化します。ヤマハルーターではアルゴリズム自体を一新したAESも利用できます。こちらも対向する機器は、同じアルゴリズムを選択する必要があります。



IKEキープアライブ
接続先との間で定期的にパケットをやりとりすることで、接続状態を監視します。「on」を設定すると、監視パケットが定期的に送信されます。パケットを送っても応答がなかった場合には切断と認識され、本体前面の「STATUS」ランプを点灯させ、障害の発生をいち早く知らせます。「auto」に設定すると、接続先から監視パケットを受信したときのみパケット送信します。このとき接続先でも「auto」に設定していると、どちらからもパケットが送信されないため、IKEキープアライブは無効になります。

AESってなに？
Keyword

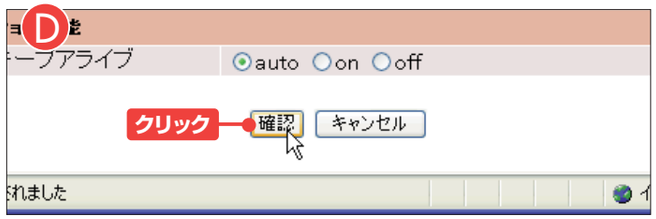
IPsecでは、パケットを暗号化して、インターネットに流す。IPsecではこの暗号化の手順（アルゴリズム）を自由に選択できるようになっており、ヤマハのルータでは、DESと3DES、そしてAES（Advanced Encryption Standard）が選択できます。

暗号強度は歴史の古いDESがもっとも低く、DESの処理を3回行なって強度を高めた3DESがVPNではよく使われます。ただ、最近ではDESに代わる暗号アルゴリズムとしてAESが急速に普及しつつあります。

AESは、ベルギーで開発されたRijndael（ラインダール）と呼ばれるアルゴリズムを用いており、鍵長や情報のブロック化サイズを可変させることができます。3DESよりも強力でDESよりも高速であるため、 DES、3DESの両方の置き換えとして使うことができます。

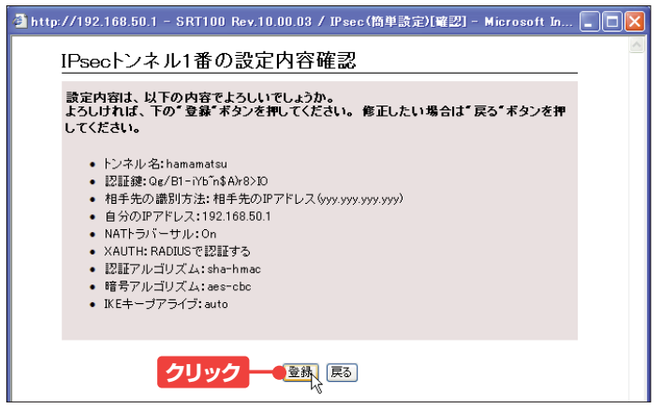
確認ボタンを押す

入力がすべて完了したら「確認」ボタンを押します。



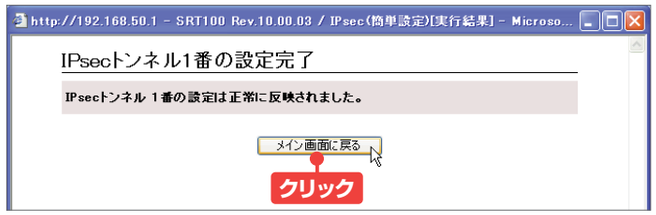
3 設定内容の確認

確認の画面では、設定内容に誤りがないかをチェックし、「登録」ボタンを押します。



4 設定の終了

正常に登録されたことを確認したら、「メイン画面に戻る」ボタンを押します。

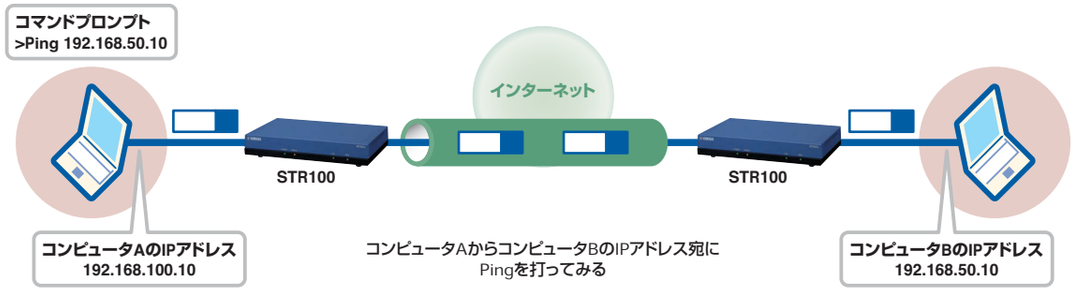


5 IPsecで通信中

IPsec接続が実行されている場合は、「IPsecの設定・状態表示」画面の「現在のIPsec設定」で、状態欄に「UP」が表示されます。

IPsecの導通試験を行なう

図3 Pingでトンネル構築を確認



応答を見る

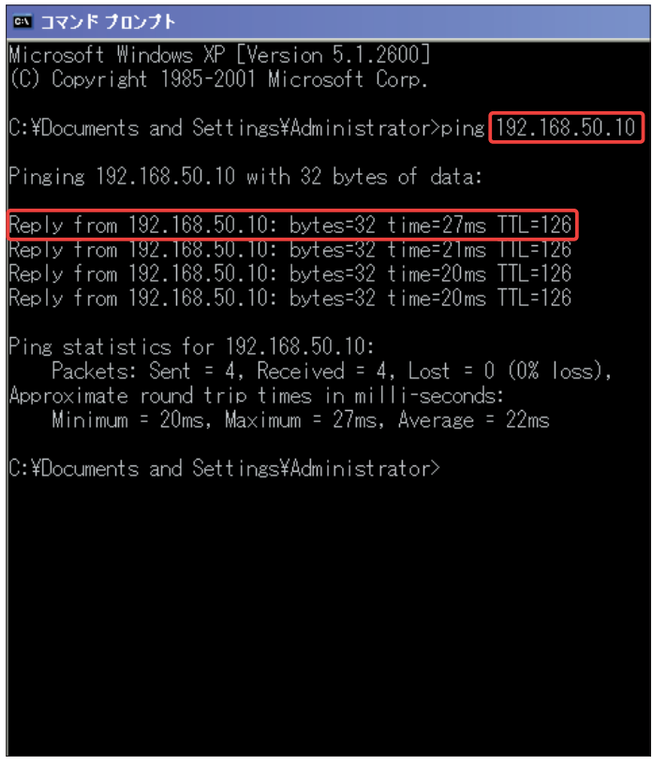
本社側のLANから支店側のLANに対して通信ができているかどうかを調べるためには、Pingを打ってみるとよいでしょう。図3のとおり、本社側のコンピュータA（192.168.100.10）から支社側のコンピュータB（192.168.50.10）に対してきちんと通信ができるかを調べるには、Windowsの「スタートメニュー」から「すべてのプログラム」－「アクセサリ」－「コマンドプロンプト」を開き、

>ping 192.168.50.10

と入力します。これに対して、

Reply from 192.168.50.10: bytes=32 time=27ms TTL=126

のような応答が戻ってきたら、トンネルが構築できていることが確認できます。



Keyword

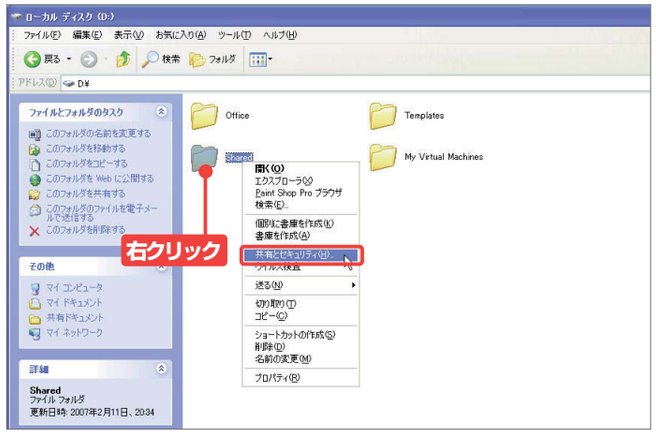
Pingとは?

Packet INternet Groper（gropeは「手探りする」という意味）の略。TCP/IPネットワークにおいて、相手先ホストと通信できるか（導通）を確認するコマンドです。pingは、ICMPのechoコマンドの仕組みを使って実現されており、IPアドレスやホスト名をパラメータに指定するだけでOKです。ただし、相手先のホスト名を指定した場合、その名前解決のためにDNSにアクセスするので、IPアドレスを指定したほうがよいこともあります。また、途中のルータが止まっていたり、コマンドを実行するクライアント自身に問題があると、正しく実行できない場合もあります。

VPN経由ソフトウェアでファイル共有

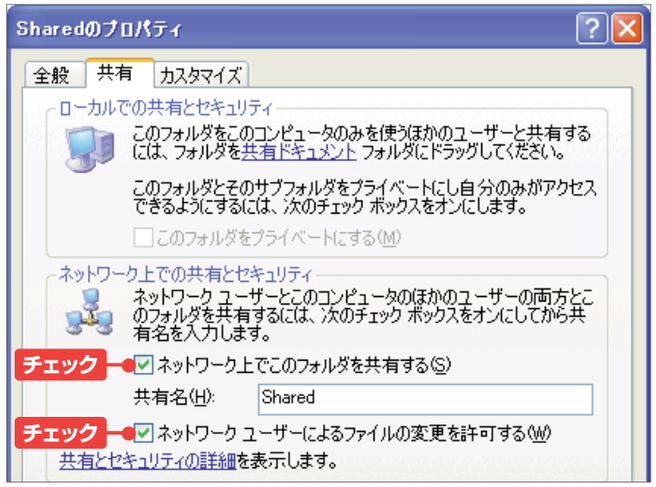
1 コンピュータBでファイル共有

VPN経由でファイル共有を利用するのも、通常のファイル共有と同じ手段を使えばOKです。利用される側のコンピュータBでは、まず共有したいフォルダを選択し、右クリックメニューから「共有とセキュリティ」を選択します。



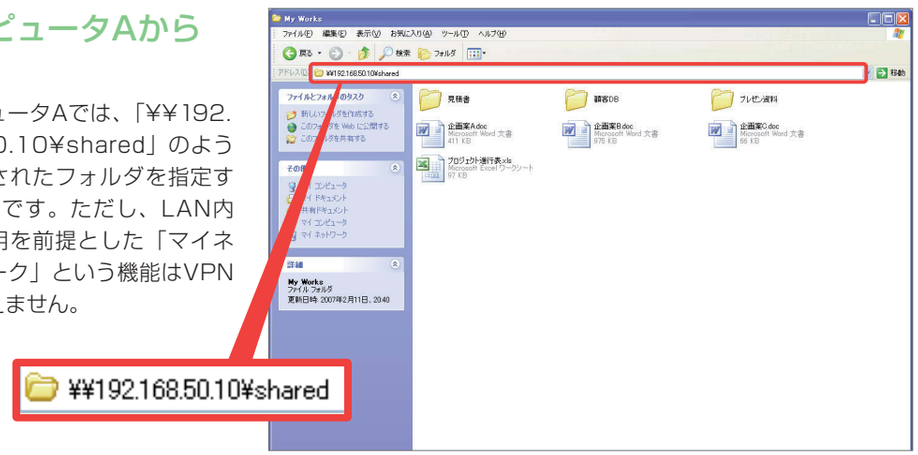
2 共有フォルダの設定

「ネットワーク上の共有とセキュリティ」の「ネットワーク上でこのフォルダを共有する」のチェックボックスをオンにします。参照だけでなく、書き込み等も可能にするのであれば、「ネットワークユーザーによるファイルの変更を許可する」のチェックボックスもオンにします。



3 コンピュータAから利用

コンピュータAでは、「¥¥192.168.50.10¥shared」のように共有されたフォルダを指定すればOKです。ただし、LAN内での利用を前提とした「マイネットワーク」という機能はVPNでは使えません。



VPNクライアントでリモートアクセス

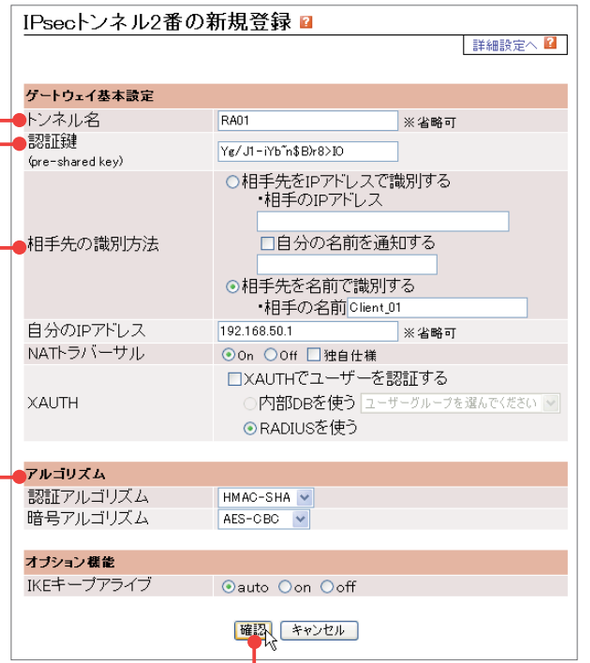
SRT100側の設定

1 新しいトンネルの作成（ルーター側の設定）

管理者向けトップページの「IPsec」をクリックし、「新しい接続先の登録」欄にある「新規登録」ボタンを押します。

以降の手順を実行しても接続が確立されないときは、「設定を調べる」ボタンを押してみましょう。うまくいけば問題箇所を検出して、必要な設定を登録してくれることがあります。

2 VPN接続設定の登録



設定名
任意の接続名を入力します。この名前は省略してもかまいません。

認証鍵
事前共有鍵として使用する文字列を入力します。ここで設定した共有鍵を、クライアント側（YMS-VPN1）にも設定する必要があります。

接続先の識別方法
クライアントの識別方法はIPアドレスではなく名前になるため、「相手先を名前で識別する」のチェックボックスをオンにします。ここで設定した名前と、YMS-VPN1に設定するクライアント名は一致している必要があります。

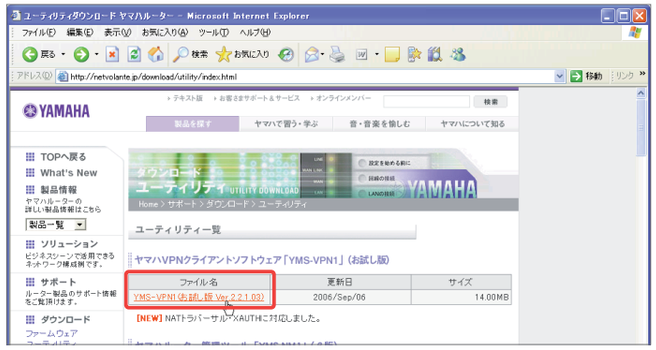
認証／暗号アルゴリズム
認証アルゴリズムと暗号アルゴリズムを設定します。アルゴリズムの種類もクライアント側と一致させなければいけません。

すべての入力が終わったら「設定」ボタンをクリックします。以後の画面で、設定内容を確認して登録します。

クライアント側

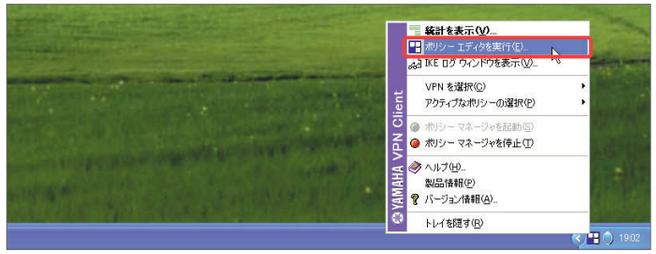
1 YMS-VPN1のインストール（クライアント側の設定）

YAMAHAのユーティリティダウンロードサイト（http://netvolante.jp/download/utility/vpn_client/about.html）から「YMS-VPN1」をダウンロードしてインストールします。

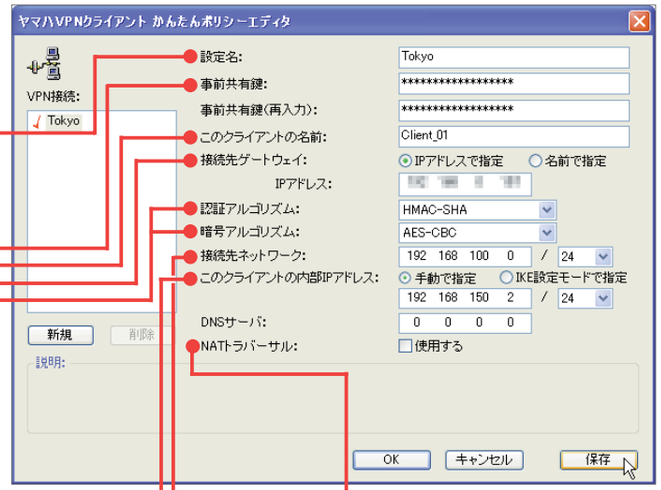


2 ポリシーエディタの起動

インストールが完了したら、タスクトレーにある「YMS-VPN1」のアイコンを右クリックし、「ポリシーエディタを実行」を選択します。



3 かんたんポリシーエディタの設定



設定名
クライアントで使用する接続を設定します。任意の名前でかまいません。

認証鍵
事前共有鍵を入力します。事前共有鍵は、ルーターに設定したものと同じ文字列を使用しなければなりません。

クライアント名の設定
「このクライアントの名前」欄には、ルーター側の「接続先の識別方法」で登録した名前を入力します。

接続先ゲートウェイ
「IPアドレスで指定」のチェックボックスをオンにして、ルーターのWAN側に固定で割り振られたIPアドレスを入力します。

認証／暗号アルゴリズム
認証アルゴリズムと暗号アルゴリズムは、ルーター側で設定したアルゴリズムと一致させる必要があります。なお、YMS-VPN1は、SRT100で利用できるアルゴリズムをすべてサポートしています。

クライアントの内部IPアドレス
VPN接続時に、このクライアントが使用するIPアドレスと、サブネットマスクを入力します。ルーター側には、このアドレスに対する経路が設定されている必要があります。DNSサーバーを使用するなら、そのアドレスを入力しますが、使用しない場合は、空欄もしくは「0.0.0.0」でかまいません。

接続先ネットワーク
接続先ルーターのネットワークアドレスとサブネットマスクを入力します。

NATトラバーサル
接続先ルーターでNATトラバーサルを利用する場合は、「使用する」のチェックボックスをオンにします。

すべての設定が完了したら、「保存」ボタンを押します。

4 VPNで接続する

タスクトレーにある「YMS-VPN1」のアイコンを右クリックし、「VPNを選択」のサブメニューから、作成した接続名を選びます。「YMS-VPN1」がインストールされたPCをネットワークに接続された場合にアイコンが表示されます。対向にあるヤマハルーターと通信可能な状態であることをあらかじめ確認しておいてください。

5 接続の確立

ルーターにアクセスして、VPN接続の確立を試みます。接続か完了したら、接続先のLANを利用できるようになります。

NATトラバーサルとは？ Keyword

IPsecはブロードバンドルータが持つNAT（Network Address Translastion）やNAPT（Network Address & Port Translastion）と相性がよくありません。グローバルアドレスをVPNルータに割り当てられれば問題ないのですが、NAT配下でプライベートアドレスを割り当てられた環境からでは、VPNトンネルを構築できないことも多いのです。

IPsecでは、送信するIPパケットをESPという別のパケットでカプセル化します。しかし、NATルータはNATの対象となるIPヘッダではなく、ESPのヘッダが挿入されているため、アドレス変換が失敗してしまいます。また、IPsecの鍵交換を行なうIKEというプロトコルはUDP500番というポートを固定で使います。そのため、NAPTでポートが変換されてしまうと、IKEのセッションが張れなくなります。

そこで登場したのが、IETFで標準化されたNATトラバーサルという技術です。NATトラバーサルは、まずVPNクライアントがNATルータの配下にいることを検知することから始めます。自らのホストがNAT経由でしかインターネット接続できないとわかった段階で、接続先のVPNゲートウェイにNATトラバーサルを使うことを通知します。これを受けたVPNゲートウェイ側はUDP500番以外のIPsecリクエストを受け入れるように構成したうえで、ESPのパケットをダミーのUDPヘッダでカプセル化して送信するようにします（UDPカプセラレーション）。そのため、パケットを送られてきたNATルータはIPアドレスのほか、ダミーのUDPヘッダに対して、アドレス変換を行なうことになり、めでたくインターネット側にパケットが送られることになります。つまり、NATルータを「騙すことで＝トラバーサル」、VPNトンネルを構築するのです。

NATトラバーサルは、そのほか送信元のIPアドレスがNATで変換されても、IPsecの通信に矛盾が生じないよう、パケット内の一部のデータを書き換えます。これにより、複数でのNAT越えVPNセッションを構築することが可能になります。

これを利用するにはVPNクライアントと接続先のVPNゲートウェイがそれぞれNATトラバーサルに対応しなければなりませんが、経由するNATルーターは特に対応は必要ありません。

Operation & management

便利な運用·管理機能を活用せよ

専任の管理者が確保しにくいSOHOや中小企業にとってみれば、運用や管理の機能は非常に重要です。SRT100では、運用・管理サポート機能が充実しているので、これらを使いこなしましょう。

便利な運用・管理機能を活用

初期設定を行なえば、SRT100はルーターやファイアウォール、VPNゲートウェイとして動作することになります。しかし、SRT100が故障したり、回線がダウンした場合にはいち早く復旧作業を実施しなければなりません。また、インターネット側からの攻撃は日々繰り返し行なわれています。そのため、最新のファームウェアに更新したり、攻撃された痕跡等をきちんと確認しなければなりません。さらに拠点やコンピュータが増えた場合には、追加に必要な設定を行なう必要があるでしょう。こうした運用・管理の作業はSOHOや中小企業にとっては意外と負担の大きな作業です。専門のエンジニアを雇うにはコストがかかりますが、かといって自前でやるのは難しいと感じているユーザーは多いでしょう。しかし、SRT100では日々の運用・管理を容易にする機能が数多く搭載されています。

・ネットワーク障害などを通知するSTATUS LED
・ルーターの状態のレポート作成
・統計情報（リソース、トラフィック、QoSの統計）の表示やメール通知
・ネットワーク管理プロトコルであるSNMPへの対応
・SYSLOGの出力、ファームウェアの更新、設定のコピーなどの保守操作

■USBメモリを用いた運用管理が可能

特に便利なのが、USBメモリを用いた運用管理の機能です。SRT100は背面にUSBポートを搭載しています。ここにUSBメモリを挿入することで、統計情報やSYSLOG、設定情報の保存などが行なえます。操作も横にあるボタンを押すだけで可能です。

運用・管理機能が役立つ場面

こうした運用管理の機能は、あらゆる場面で役に立ちます。まず障害検知という用途では、いち早く障害を知るためのSTATUS LEDやSNMPによる警告などが役に立ちます。また、回線や機器の障害でバックアップ機を使う場合は、設定情報やファームウェアのUSBメモリへの保存機能が有効です。

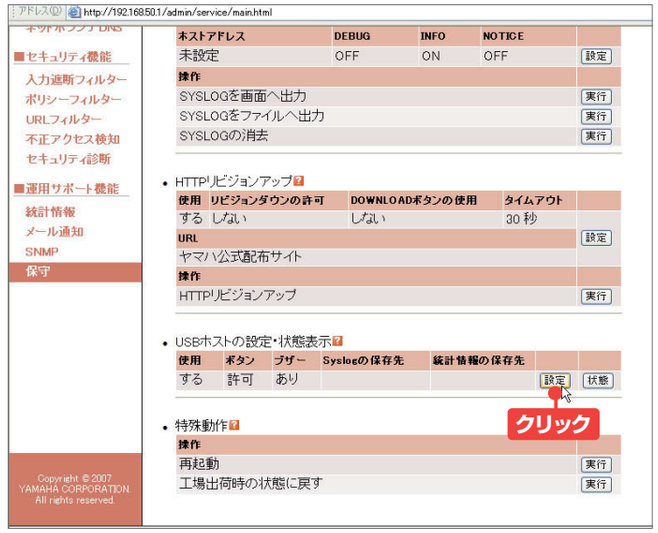
障害の原因を特定したり、日々の運用状態を確認するといった用途では、SYSLOGや統計情報の表示機能が便利でしょう。トラフィックの増減を調べたり、レポートとして回線増強用の資料として使うことが可能です。

安定した動作を実現するには保守においては作業を簡素化してくれるファームウェアの自動アップデート機能が便利です。適切に設定を施せば、ボタンを押すだけでファームウェアを更新してくれるので、専門の人員を派遣する手間とコストもなくなります。

USBホストの設定

1 USBホストの設定を開く

「運用サポート機能」のメニューから「保守」を開き、そこから「USBホストの設定・状態表示」の「設定」ボタンを押す



2 USBホストの設定を行なう

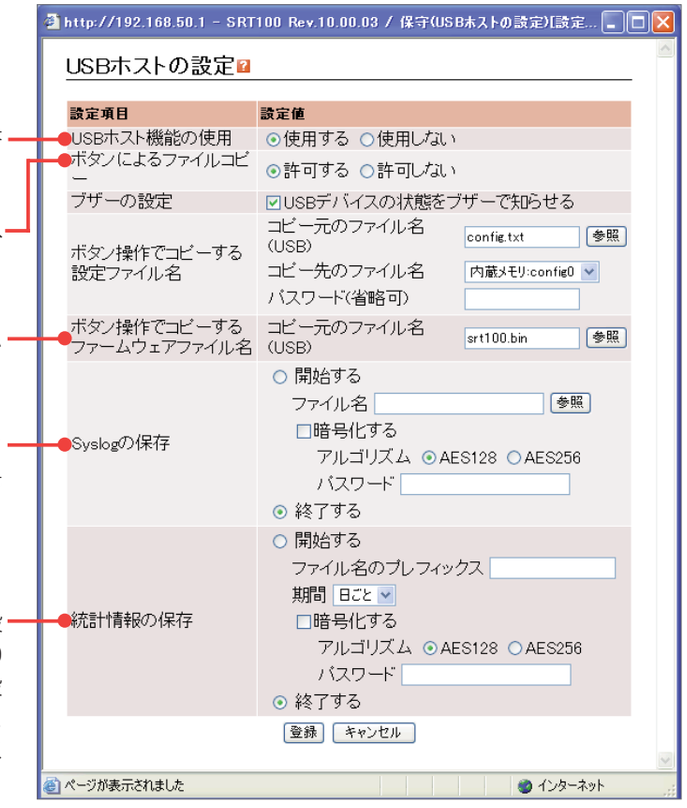
USBホスト機能を利用するか否かの設定

本体設定ファイルのUSBメモリへのコピーについての設定

USBメモリに保存されたファームウェアの読み込み設定

本体SYSLOGファイルのUSBメモリへの保存設定。ファイルの暗号化やパスワード指定も行なえます

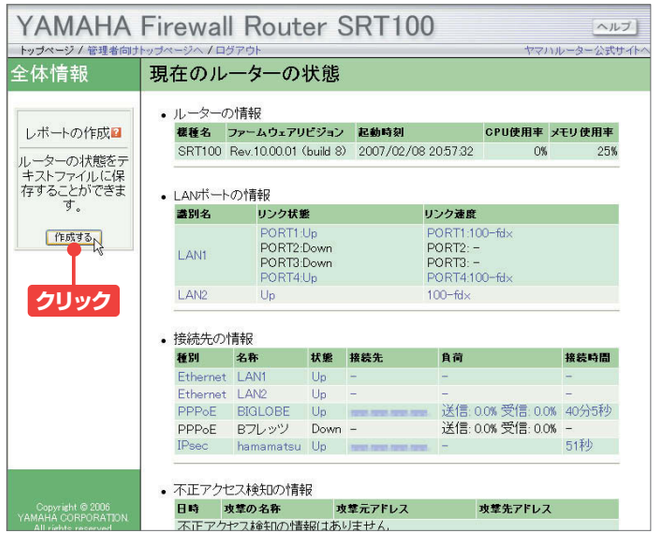
統計情報のUSBメモリへの保存設定。ファイル名に付ける固有ID（プレフィックス）や保存期間の設定が可能です。また、SYSLOGと同じく、ファイルの暗号化やパスワード指定も行なえます



レポート出力

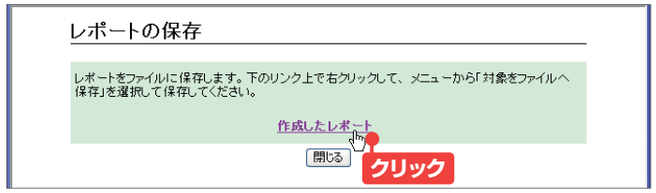
1 レポートの作成

トップページの左メニューの「作成する」ボタンを押します。



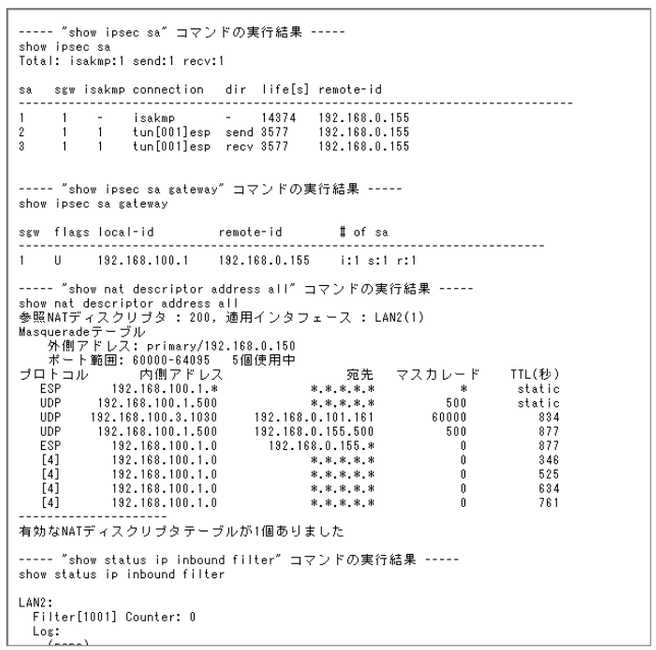
2 レポート保存

SRT100で作成したレポートを、ローカルのPCに保存します。



3 レポートの参照

SRT100のIPsecトンネルの状態や情報もまとめて出力できます。



```
----- "show ipsec sa" コマンドの実行結果 -----
show ipsec sa
Total: isakmp:1 send:1 recv:1

sa   sgw isakmp connection   dir  life[s] remote-id
-------------------------------------------------------------------------------
1     1    -    isakmp       -    14374   192.168.0.155
2     1    1    tun[001]esp  send 3577    192.168.0.155
3     1    1    tun[001]esp  recv 3577    192.168.0.155


----- "show ipsec sa gateway" コマンドの実行結果 -----
show ipsec sa gateway

sgw  flags local-id         remote-id        # of sa
-------------------------------------------------------------------------------
1    U     192.168.100.1    192.168.0.155    i:1 s:1 r:1

----- "show nat descriptor address all" コマンドの実行結果 -----
show nat descriptor address all
参照NATディスクリプタ : 200, 適用インタフェース : LAN2(1)
Masqueradeテーブル
    外側アドレス: primary/192.168.0.150
    ポート範囲: 60000-64095   5個使用中
プロトコル      内側アドレス                宛先    マスカレード     TTL(秒)
   ESP       192.168.100.1.*          *.*.*.*          *       static
   UDP       192.168.100.1.500        *.*.*.*        500       static
   UDP    192.168.100.3.1030     192.168.0.101.161   60000        834
   UDP       192.168.100.1.500     192.168.0.155.500     500       877
   ESP       192.168.100.1.0         192.168.0.155.*       0       877
   [4]       192.168.100.1.0         *.*.*.*.*             0       346
   [4]       192.168.100.1.0         *.*.*.*.*             0       525
   [4]       192.168.100.1.0         *.*.*.*.*             0       634
   [4]       192.168.100.1.0         *.*.*.*.*             0       761
----------------------
有効なNATディスクリプタテーブルが1個ありました

----- "show status ip inbound filter" コマンドの実行結果 -----
show status ip inbound filter

LAN2:
  Filter[1001] Counter: 0
  Log:
```

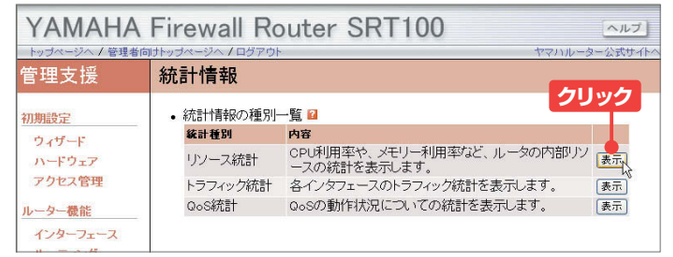
統計情報の表示

1 統計情報の画面を呼び出す

管理者向けトップページの「統計情報」をクリックします。

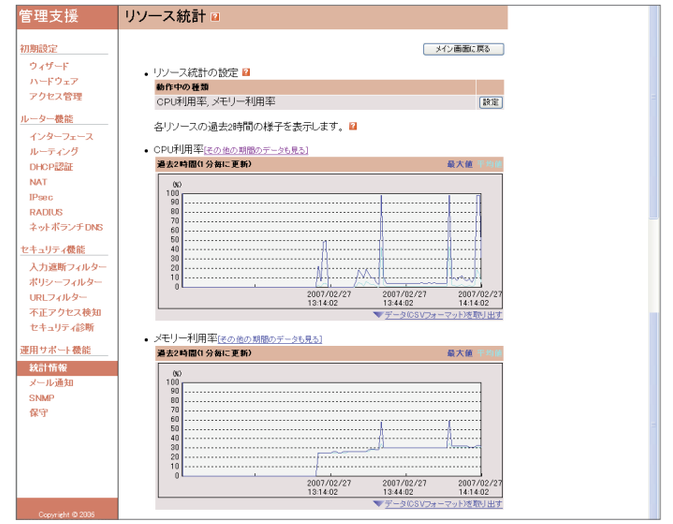
2 統計情報の種別を選択

「SYSLOGの管理」欄にある「リソース統計」「トラフィック統計」「QoS統計」のなかから、閲覧したい統計情報の「表示」ボタンを押します。



3 統計情報の表示

選択した統計情報のグラフが表示されます。たとえば「リソース統計」を選んだ場合は、CPUとメモリーの過去2時間の利用率がグラフ表示されます。

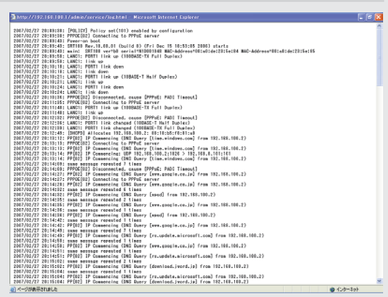


SYSLOGとは？

Column

SYSLOGとは、システムの出力するメッセージをネットワーク経由でやりとりしたり、ファイルに記録する仕組みです。ヤマハのルーターでは、各インターフェイスやフィルタ、各種プロトコルのログが収集されており、これらを以下の手順でSYSLOGとして出力することができます。

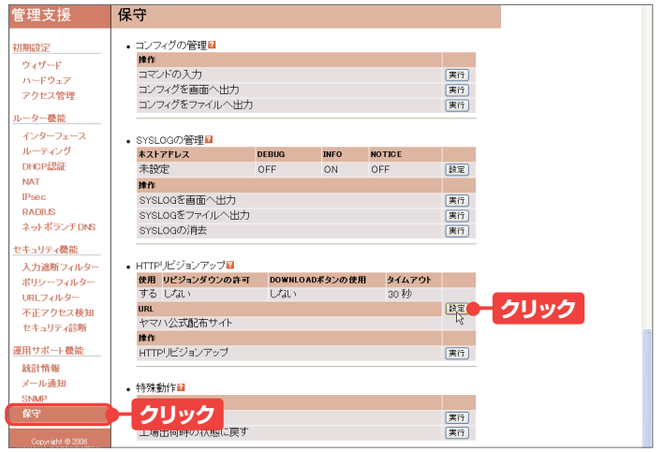
1 まず管理者向けトップページの「保守」をクリックします。
2「SYSLOGを画面に出力」欄の「実行」ボタンを押します。
3 ルーターに記録された動作履歴（SYSLOG）が表示されます。



ファームウェアの自動更新

1 HTTPリビジョンアップの設定を開く

管理者向けトップページの「保守」をクリックします。
「HTTPリビジョンアップ」の欄にある「設定」ボタンを押します。

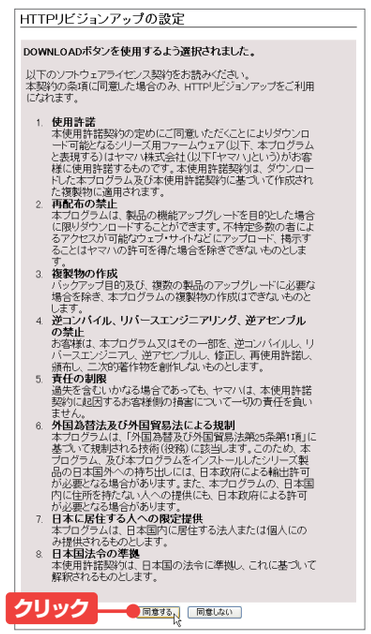


2 リビジョンアップの許可

初期状態ではHTTPリビジョンアップを「しない」設定になっているので、「する」のチェックボックスをオンにします。
SRT100本体のDOWNLOADボタンでリビジョンアップを実行する場合は、「DOWNLOADボタンの使用」の欄で「する」のチェックボックスをオンにします。
設定を確認したら「登録」ボタンを押します。

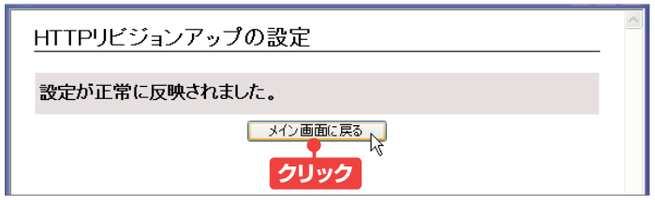
3 ソフトウェアライセンス契約

「DOWNLOADボタンの使用」を「する」に設定すると、ファームウェアの利用に関するライセンス契約の承諾画面に移ります。ひととおり目を通したら、画面の下部にある「同意する」ボタンを押します。



4 設定完了

設定が正常に反映されたことを確認したら、「メイン画面に戻る」ボタンを押します。



5 リビジョンアップの実行

「HTTPリビジョンアップ」の「実行」ボタンを押し、表示されるライセンス契約の承諾画面で、「同意して実行する」ボタンを押せば、最新のファームウェアがダウンロードされインストールされます。

本体のDOWNLOADボタンを押しても、同じように最新のファームウェアがインストールされます。

ファームウェアとは?

Keyword

ファームウェアとは、ルータやスイッチなどのネットワーク機器を動作させるためのソフトウェアを指し、ハードウェアの基本的な動作を制御します。パソコンでこのファームウェアにあたるものが、いわゆるBIOSです。BIOSはマザーボードの書き換え可能なフラッシュメモリに搭載され、ハードウェアとOSの間を取り持っています。こうしたファームウェアをインターネット経由でダウンロードし、インストールすることで、不具合の修正や性能の向上、新機能の追加や強化などが実現されるわけです。

Catalog

ヤマハルーター最新カタログ

企業が求めるネットワークの要件は、実に多種多様です。こうした要件に対応するため、ヤマハでは低価格で安定度の高いルーターを次々リリースしています。ここでは2007年4月時点のヤマハルーターの最新ラインナップを紹介していきましょう。

ヤマハのルーターラインナップ

ヤマハルーターの特徴

ルーターはインターネット接続や社内LANの相互接続に使う機器です。最近では、ファイアウォールや拠点間接続を実現するVPNなどの機能も重要視されるようになっています。

ヤマハのルーターの特徴は、①最先端技術のいち早い導入、②高いコストパフォーマンス、③最新ファームウェアや技術情報の提供といったサポート体制の充実といった3点になるでしょう。また、コマンドラインだけだった操作方法にWebブラウザの設定ツールを追加したり、軽量かつコンパクトなプラスチック筐体を採用したり、国内の企業の大多数を占めるSOHOや中小企業での現場を意識した製品作りを手がけているのも特筆すべき点です。

VPNルーターのラインナップ

こうしたヤマハのルーターの中で、最近の主力製品となっているのが、RTX1000/1100を筆頭とするVPNルーターです（図2）。

企業での拠点間接続の有力手段としてVPNは大きな注目を集めています。しかし、一口にVPNといってもさまざまな種類があり、通信事業者が提供するサービスやインターネットを使って自前で構築するためのVPNゲートウェイの種類も多彩です。もちろん、企業がVPNに求めるニーズも異なっています。これに対してヤマハでは、ユーザーが用途や規模に合った製品を選択できるように、同社のルーターで構築できるVPNを複数のクラスに分類しています。

まずはVPNを使ってみたいという初心者ユーザーに最適な「エントリーVPN」は、VPNのプロトコルにPPTP（Point to Point Tunneling Protocol）を採用したルーターです。PPTPは古くからWindowsでサポートされているため、インターネット経由で遠隔のLANに安全にログインするリモートアクセスVPNの用途で使えるのが最大の特徴といえます。これを実現するのに最適な製品はヤマハの個人・SOHO向けルーター「RT58i」になります。RT58iは量販店で購入できるブロードバンドルーターで、標準4万円という価格が大きな魅力です。

一方、企業で利用するために十分なパフォーマンスやセキュリティを確保した「スタンダードVPN」を実現するのは、今やヤマハルータの標準機ともいえるRTX1000とスペック向上を施したRTX1100です。通常VPNを利用するとスループットが落ちてしまうのが一般的ですが、IPsecの3DESという暗号化処理を行なってもRTX1000で55Mbps、RTX1100では100Mbpsのスループットを確保しています。また、RTX1000/1100はISDNのインターフェイスを搭載しており、ISDNをバックアップ回線として利用できます。

広域EthernetやIP-VPNなど通信事業者の閉域網とインターネットVPNを併用したり、VPNのトンネル内でも通信品質を保ちたいという「アドバンストVPN」の用途であれば、RTX1500がお勧めになります。RTX1500は専用線やフレームリレー、ISDNなどに接続するためのBRIポートを2つ搭載しているため、これらとブロードバンド回線を組み合わせることができます。また、マルチメディア系のパケットの処理能力が高速であるため、TV会議やIP電話などを実現するためにはこの機種が最適です。

さらに、上位機種としてはラックマウント型の「RTX3000」という機種も用意されています。こちらはVPNスループットも最大360Mbps、IPsecの接続対地数最大500というヤマハルーターの最高峰。おもに数多くの拠点VPNルーターの接続を一手に担うセンター側ルーターとしての利用が想定されています。

そして今回紹介した「SRT100」やその前身となる「RT107e」は、ヤマハの考えるVPNのうち「ベーシックVPN」をカバーする製品となります。スタンダードVPNでのRTX1100/1000が実現する100MbpsというVPNスループット、30という接続拠点数に対して、SRT100はVPNスループットが80Mbps、接続拠点数が10となっています。その一方で、SRT100は価格も標準で8万円台に抑えられており、導入コストを重視する中堅・中小企業にとって大きな魅力といえるでしょう。さらにSRT100では、本編で紹介したような導入や管理・構築を簡単に行なうための仕掛けがいくつも用意されています。

図1 ヤマハのルーター製品

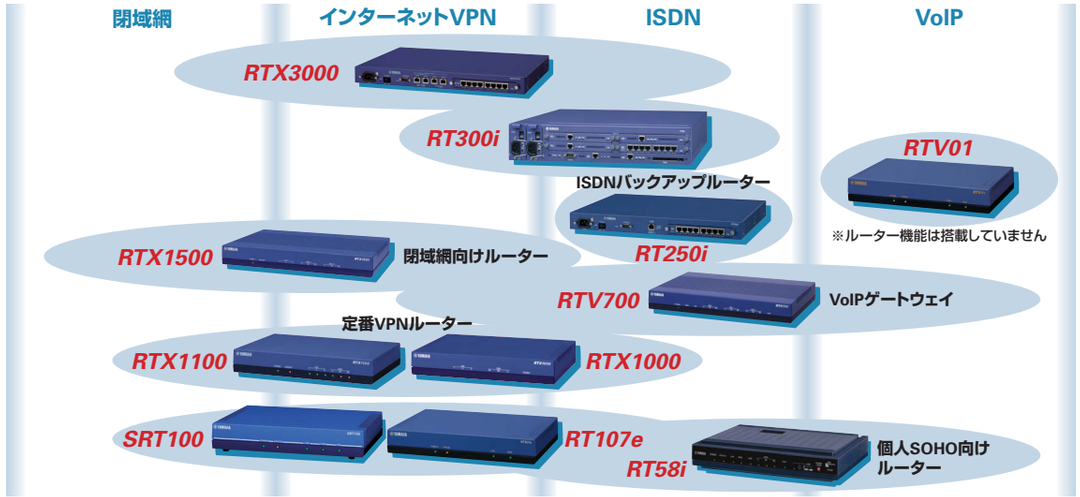
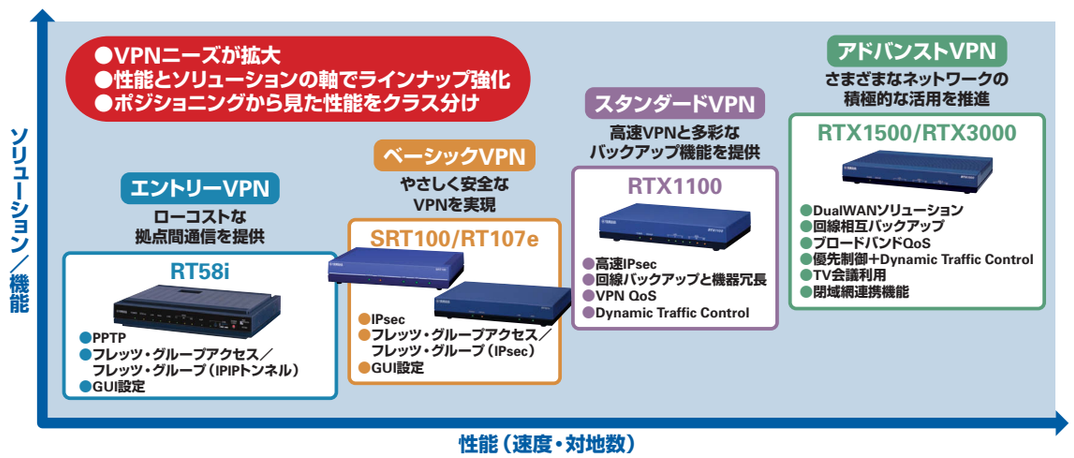


図2 VPNを軸としたルーターのラインナップ



ヤマハルーター Webサイトの紹介

ヤマハルーターの特徴の1つに、充実した情報提供体制が挙げられます。1号機であるRT100iの発売当初から、製品供給元のヤマハ自体がメーリングリストをいち早く立ち上げのも、情報提供の重要性を認識していたからにほかなりません。製品の導入やソリューションの選定、あるいはトラブル対応などあらゆる場面で、以下のWebサイトが役立つでしょう。

ヤマハルーター総合サイト

http://netvolante.jp/

ヤマハルーターの総合情報サイトで、製品情報、ソリューション、サポートなどで構成されています。

●製品情報

RT、RTX、RTV、NetVolanteなどの新旧製品の機能や特徴などが紹介されています。

●ソリューション

各製品によって実現するインターネット接続、VPN、IP電話などのネットワークソリューション例と導入事例を紹介しています。フレッツサービスとの接続やIPマルチキャストの設定なども掲載されています。設定に必要なコンフィグファイルを直接ダウンロードできる点もユニークです。

●サポート・ダウンロード

よくある質問、詳細な質問、設定例週、接続サービス設定ガイドなどが掲載されている（一部は技術情報サイトへのリンク）。設定の仕方がわからない、あるいはトラブルを解決したいといった際には、これらが非常に有効な情報源となるでしょう。また、最新のファームウェアかユーティリティ、マニュアル、カタログなどのダウンロードもここから行なえます。

問い合わせ先

ヤマハルーターお客様ご相談センター

対象機種

【RTXシリーズ】
RTX3000、RTX1500、RTX1100、RTX1000
【RTシリーズ】
RT107e、RT105e、RT300i、RT250i
【SRTシリーズ】
SRT100

電話番号 053-478-2806
FAX番号 053-460-3489
ご相談受付時間 9:00～12:00、13:00～17:00
（土・日・祝日、弊社定休日、年末年始は休業とさせていただきます。）