インターネットVPNをヤマハルーターで構築

ヤマハの最新ルーター
「RT107e」を使った
インターネットVPNの
構築法を完全解説。
これがあれば、
安全で高速な拠点間通信が
今日から実現する。

ネットワークマガジン
NETWORK MAGAZINE

ECO-PULP
エコパルプ
このパンフレットは無塩素漂白（ECF）パルプを使用しています。

PRINTED WITH SOY INK
このパンフレットは大豆油インクで印刷しております。

●本書に記載されている内容は2006年1月現在のものです。その後変更になっている可能性もあります。予めご了承ください。
●本書に記載されている会社名、製品名は各社の登録商標または商標です。
●本書によって生じたいかなる損害についても、株式会社アスキーは責任を負いかねますので、予めご了承ください。

インターネット VPNを ヤマハルーターで 構築

目次

概論

インターネットVPNとヤマハルーター

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。

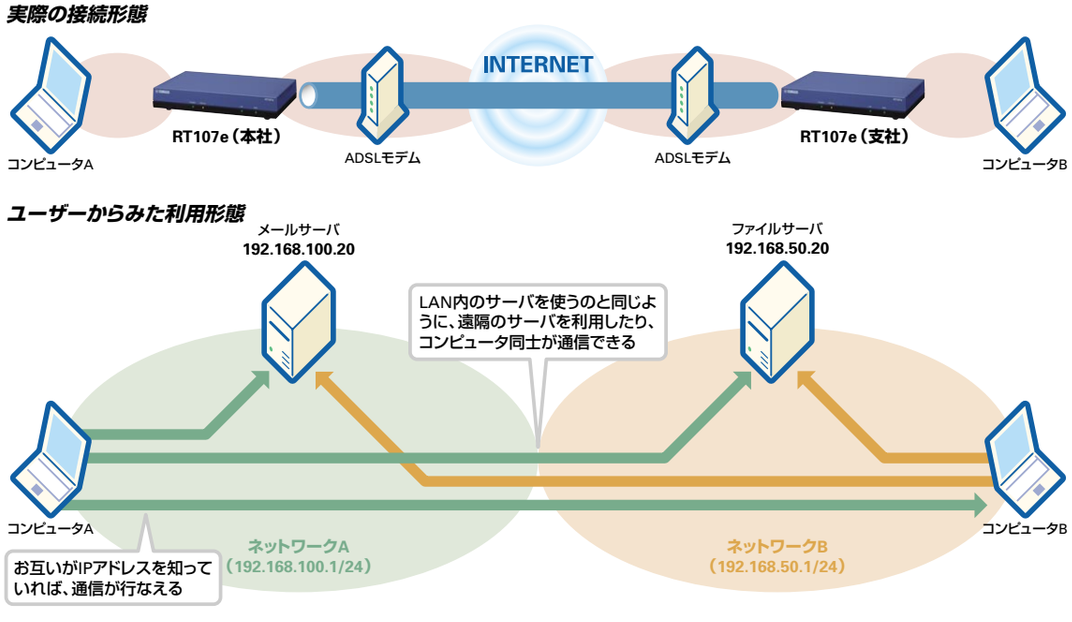
安価で安全なインターネットVPN

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。

VPNが使われるようになったのは、インターネットの普及が大きく貢献しています。インターネットは誰でも利用でき、異なるネットワークを相互接続できるという特徴を持つ一方で、ブロードバンドの普及により、接続料金は低く抑えられています。こうした状況でインターネットを拠点間接続に使うというのは、非常によいアイデアといえるでしょう。

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（IPsecurity）というプロトコルを使ったインターネットVPNです。IPsecに対応したヤマハのRT107eのようなルーターで、地理的に離れた拠点のLAN同士をIPsecで接続します（図1）。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。たとえば、本社のLANのコンピュータAは支社のファイルサーバから必要なファイルを取り出すことができます。もちろん、コンピュータAとコンピュータB同士が直接通信してメッセージやファイル　をやりとりすることも可能です。

図1 VPNの接続形態と実際の利用



ユーザーからは、遠隔にありながらLAN同士が接続されているように見えます

トンネリングとセキュリティ

トンネリングの概念

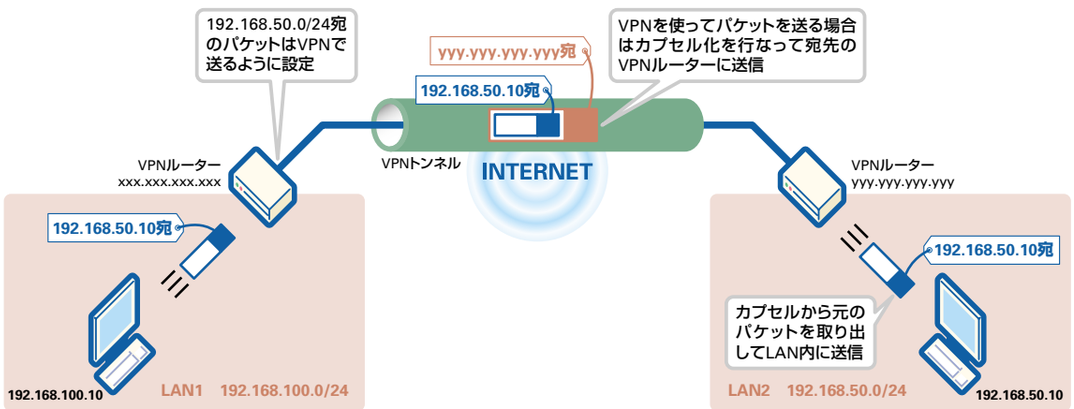
VPNやIPsecを理解するうえで、特に重要なのが「トンネリング」と呼ばれる概念です。トンネリングとは、インターネット上に、あたかもトンネルのように仮想的な専用線を作る（掘る）ことを指します。実際、拠点間をつなぐ通信路のことを「トンネル」と呼びます。このトンネリングを実現するためには、パケットの「カプセル化」という技術が利用されます。カプセル化とは、元のパケットを別のパケットで包み込むことです。では、なぜこうしたカプセル化が必要になるのでしょうか？

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のみ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技術を利用し、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で包み込み、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LAN1とLAN2は、図2のようにVPNルーターで相互接続されています。LAN1のコンピュータからLAN2のプライベートアドレス（192.168.50.10）宛のパケットがVPNルーターに届くと、VPNルーターはグローバルアドレス（yyy.yyy.yyy.yyy）をつけて送信します。つまり、拠点間（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。

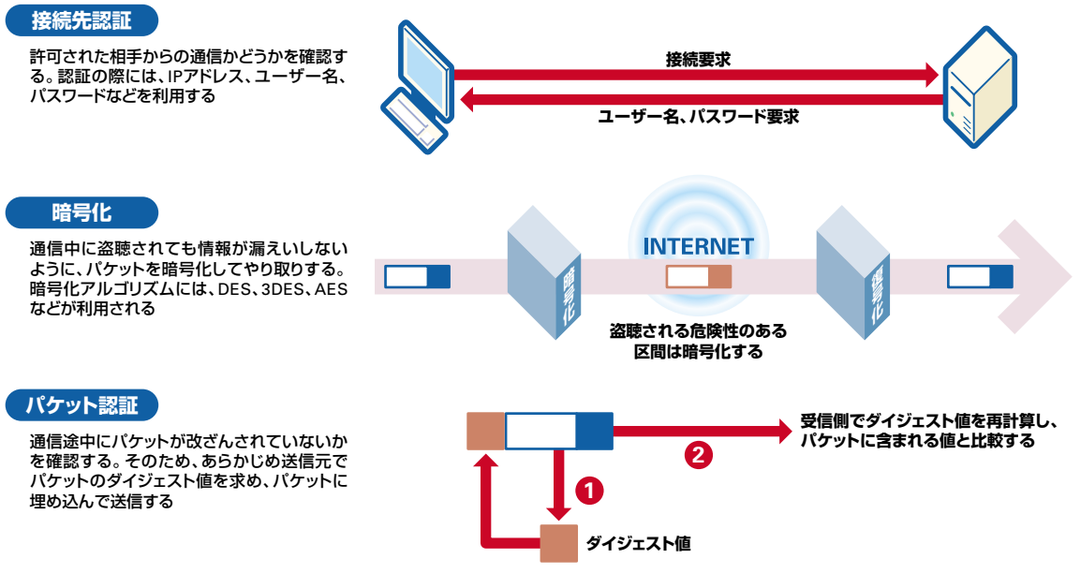
IPsecでは「ESP（Encyption Security Payload）」や「AH（Authentication Header）」といったプロトコルで、元のIPパケットをカプセル化します。これらは後述するセキュリティの機能も持っており、暗号化や認証などが実現されています。一方、IPパケットを別のIPパケットでカプセル化したIPIP（IP over IP）のようなプロトコルもあります。こちらは閉域網などのセキュリティが不要なWANで用いられます。

図2 IPsecでのトンネリング



カプセル化を行なうことで、インターネット経由でプライベートアドレスのパケットが流せます

図3 IPsecのセキュリティ 接続先の認証やパケットの暗号化、認証などで盗聴や改ざん、なりすましなどを防ぎます



IPsecのセキュリティ機能

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するというものです。

また、IPsecではパケットの中身が暗号化されており、悪意の第三者に盗聴されても情報が漏れない仕組みになっています。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ではこの共通鍵暗号のアルゴリズム（数学の関数）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って、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。

また、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送信する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、送信元と宛先がそれぞれ算出した値とパケットに付いてきたダイジェスト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。本冊子はヤマハのVPNルーターを使って、IPsecによるVPN構築を試してみます。

インターネットVPNに必要なもの

インターネット接続の契約と必須の設定情報

インターネットVPNの構築にあたっては、当然ながら各拠点でインターネット接続の契約が必要になります。

インターネットVPNのメリットはブロードバンド回線を拠点間接続の手段として有効活用できる点にあります。そのため、少なくともADSL、可能であれば高速なFTTHサービスを導入すべきです。特にBフレッツ（NTT東西）やTEPCOひかり（東京電力）など光ファイバを使うFTTHのサービスは高速で、安定度も高いので、おすすめできます。

プロバイダは、接続する全拠点で同じプロバイダを選んだほうが無難でしょう。同じプロバイダ同士の接続の方が、別のネットワークをまたがないので、遅延が少なく、安定度も高いからです。また、コストはかかりますが、安定性を考えれば固定のグローバルアドレスを最低1つは取得すべきです。

インターネット接続サービスを契約すると、プロバイダから接続に必要な情報が記載された書類が郵送されてきます。書類にはユーザーID（アカウント）とパスワード、場合によってはDNSサーバやメールサーバなどが掲載されています。これはインターネット接続の際に必要なので、確認しておきましょう。

ただ、フレッツ・ADSLやBフレッツなどのフレッツ・アクセスサービスを申し込んだ場合は、プロバイダとはまったく別の契約になります。開通のご案内ということで、「お客さまID」と「アクセスキー」などが記載された書類がNTT東西からの郵送されますが、これはインターネット接続やVPNの設定では使いません。これらの情報はNTT東西のフレッツ・アクセスサービスのオプションサービスの申し込みなどを行なう際に必要なのです。

インターネットVPN構築に必要な機材は？

次にユーザー側で必要となる機器と配線等をまとめておきましょう。必要なのは、①VPNルーター、②ブロードバンド回線用の宅内装置、③（設定用の）コンピュータ、④各機器を接続するケーブルなどです。

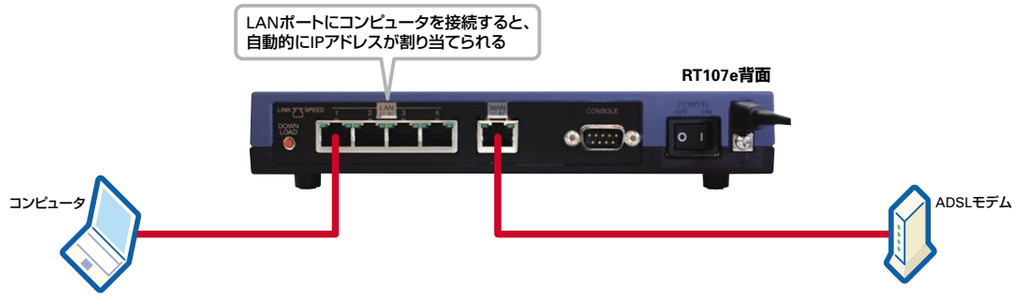
①のVPNルーターはIPsecのプロトコルなどを使って、トンネルを構築する機器です。もともとルーターは異なるネットワーク同士で、相互にパケットを中継するための機器です。VPNルーターは、トンネルを介して、異なるネットワーク同士をつなぐ役割を果たすわけです。インターネットVPN構築のもっともキモとなる機材です。

②のブロードバンド用の宅内機器は、ADSLであればADSLモデム、FTTHであればメディアコンバータやVDSLモデムなどになります。通信事業者からレンタルされるのがほとんどで、イーサネットでRT107eと接続されます。

■今回紹介するヤマハの新製品「RT107e」

低価格で設定も容易な企業向けルーターです

図4 関係する機器の結線図



ルーターやコンピュータ、ADSLモデムなどを以上のように接続する

③の設定用のコンピュータは、Webブラウザが利用できれば、Windowsでも、Macintoshでもかまいません。

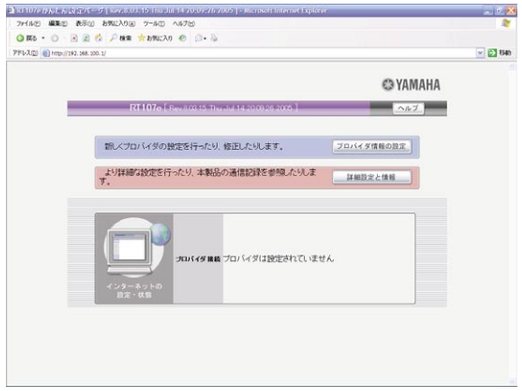
④のケーブルは、イーサネットで使うUTPケーブルです。ほとんどは機器とともに同梱されますが、配線の作業上、長さが足りなくなったり、太くてドアをまたげないということもあります。その場合には、さまざまな特徴のケーブルが市販されていますので、用途にあったケーブルを用意します。

RT107eの初期設定

本冊子では、ヤマハの最新VPNルーター「RT107e」を使います。2005年10月に発売されたばかりのRT107eは7万円台に抑えられた低価格なIPsec対応ルーターです。VPNのスループットも50Mbpsと高速で、さらに導入や管理・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。

これらの機器の物理的な配線は、図4のとおりになります。RT107の背面には、全部で5つの100Mbpsのイーサネットインターフェイスがあり、そのうち4つがLANポート、1つがWANポートとして機能しています。もちろん、4ポートだけでは足りないことも多いので、別途スイッチングハブなどを増設して、接続するコンピュータの数を増やします。

WANポートは通常ADSLモデムやFTTHのメディアコンバータなどと結線します。最近ではADSLモデム自体にルーターの機能が統合されていることが多いのですが、そのまま使うとVPNの設定が複雑になってしまいます。そのため、VPNを構築する際はルーターの機能をオフにし、ブリッジとして動作させるようにしておきましょう。こうしておけば、WANポートに直接グローバルアドレスが割り当てられ、VPNの設定はシンプルになります。



Webブラウザのアドレス欄にIPアドレスを入力すると、かんたん設定ページが表示される

LANポートはスイッチングハブとして動作しており、「192.168.100.1」というIPアドレスが割り当てられています。このLANポートにコンピュータを接続し、コンピュータの電源を入れると、ルーターのDHCPサーバにより、自動的にIPアドレスが割り当てられます。あとはWebブラウザを立ち上げ、「アドレス」に「192.168.100.1」を入力すれば、設定ツールが起動します。

基本編①

インターネットへの接続

インターネットVPNの構築に際しては、まずADSLやFTTHを介してインターネットに接続する必要があります。ここではWebブラウザの設定やLANでのIPアドレスの割り当て、そして実際の接続設定までを見ていきましょう。

LANのIPアドレスを確認しよう

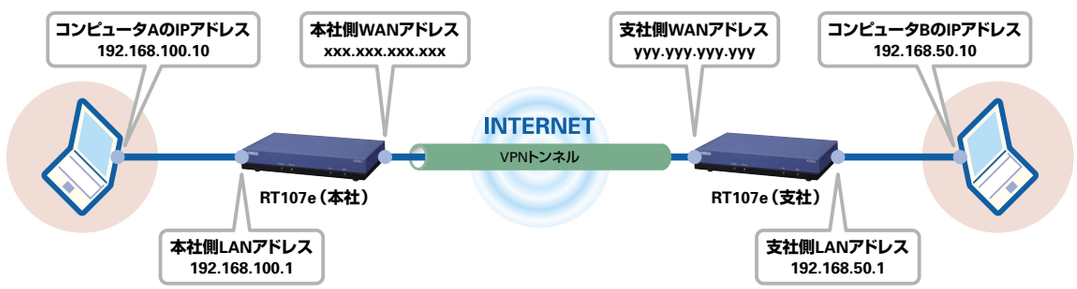
設定を行なう前に、インターネットVPN構築後のIPアドレスの構成を考えてみましょう。まずRT107eのWAN側にはプロバイダからグローバルアドレスが割り当てられます。これらWAN側のアドレスは重複することはないのですが、LAN側のアドレスは拠点同士で同じになる可能性があります。RT107eでは初期設定でLAN側に「192.168.100.1/24」というプライベートアドレスが割り当てられています。また、LAN側ではDHCPサーバが動作しており、接続するコンピュータには自動的に「192.168.100.2～192.168.100.191」までのIPアドレスが割り当てられます。2つの異なる拠点でそれぞれインターネットに接続している限りは、これでも問題ありません。しかし、これらのLAN同士をRT107eでVPN接続するとなると、同じアドレスが重複してしまうことになります。そのため、VPNで拠点間を接続するにあたっては、それぞれの異なったネットワークアドレスを割り当てる必要があります。

では、どのようにネットワークアドレスを割り当てればよいのでしょうか？ 一般的にプライベートアドレスとしては、クラスCの192.168.0.0～192.168.255.255という範囲がよく用いられます。そのため、「192.168.×××.0」の×××部分に0～255の数字を重ならないように割り当て、各拠点のネットワークアドレスにして使うとよいでしょう。

今回は下の図5のように本社のルーターは、初期状態の「192.168.100.1/24」のまま使います。DHCPサーバの設定もそのままです。一方で、支社側のLANアドレスを「192.168.50.1/24」に、DHCPで割り当てるアドレスも「192.168.50.10～192.168.50.191」に変更しておきます。右ページではRT107eでのIPアドレス変更の設定を示しました。

IPアドレスやDHCPの設定を変更すると、かんたん設定ページのアドレスも変わってしまいます。そのため、設定しているコンピュータのLANポートを切断・再接続し、新しいアドレスを取得しましょう。

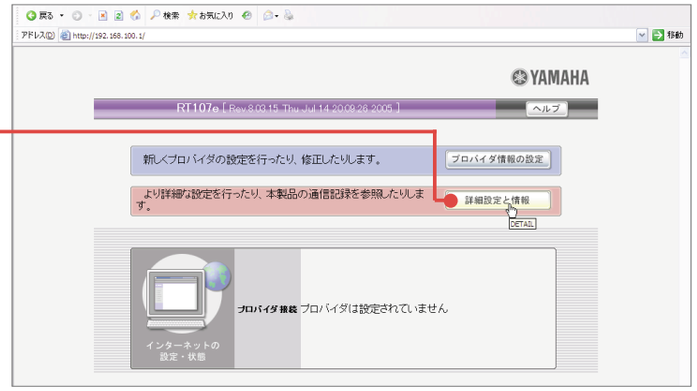
図5 LANのIPアドレスを確認



接続するLAN同士でIPアドレスが重ならないように注意しましょう

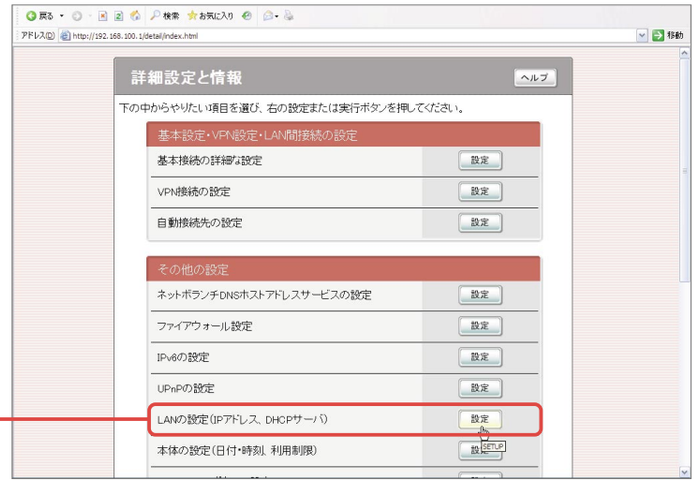
1 トップページ

「詳細設定と情報」ボタンを押します。



2 LANの設定

「その他の設定」の「LANの設定（IPアドレス、DHCPサーバ）の「設定」ボタンを押します。



3 IPアドレスの変更

「プライマリ・IPアドレス」を初期状態の「192.168.100.1」から「192.168.50.1」に書き換えます。

「DHCPサーバ機能」でも、プライマリ・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、「192.168.50.10」～「192.168.50.191」に変更します。

設定を終了したら「設定の確定」を押します。

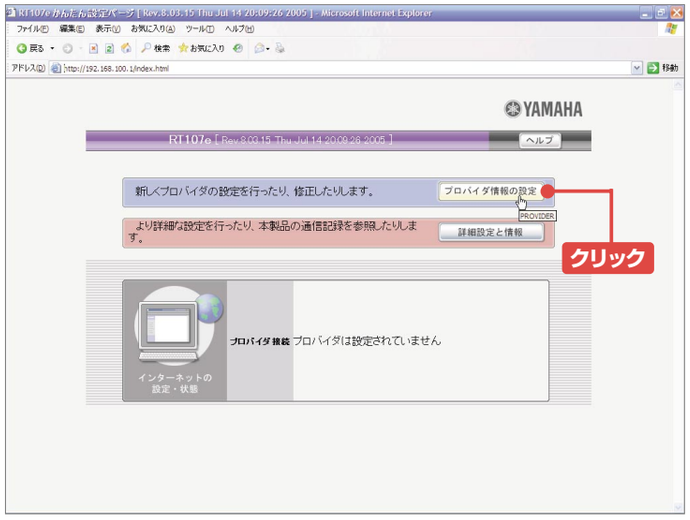
インターネット接続の設定を行なう

1 アドレスの指定

Webブラウザ(ここではInternet Explorer)を起動し、アドレス欄にRT107e（本社）のLAN側アドレスである「http://192.168.100.1」を入力します。
支社のRT107eの設定を行なう場合は、この欄に「http://192.168.50.1」を入力します。

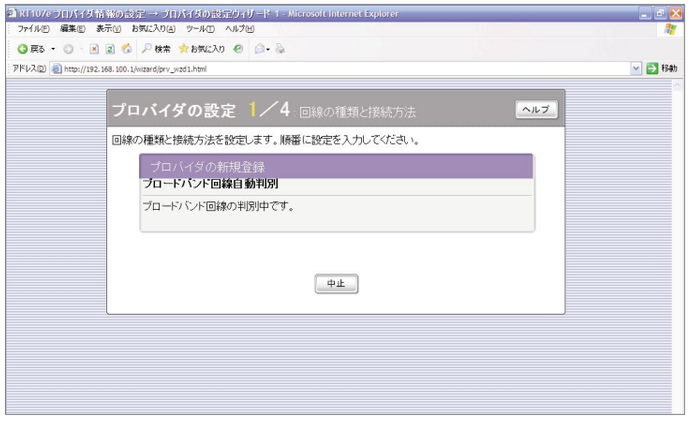
2 トップページの表示

RT107eの「かんたん設定ページ」のトップページが表示されます。まずは「プロバイダ情報の設定」ボタンを押します。



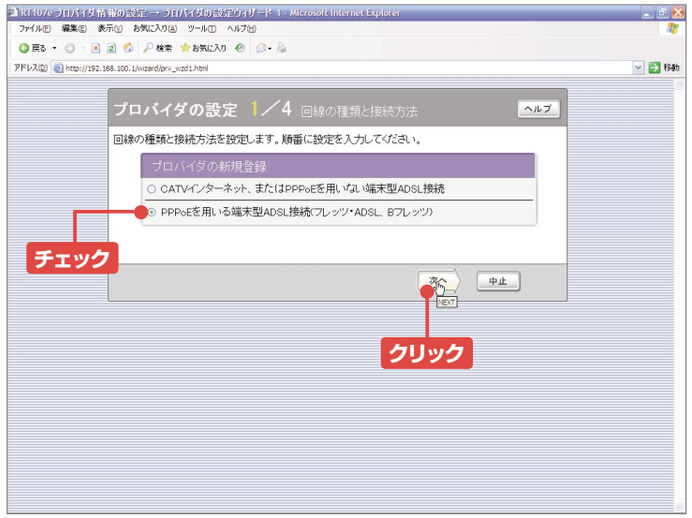
3 回線の自動判別

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。



4 回線種別の選択

フレッツ・ADSLやBフレッツのような、PPPoEを用いるサービスを利用している場合は、下のチェックボックスをオンにしましょう。設定し終えたら、下部の「次へ」ボタンを押します。



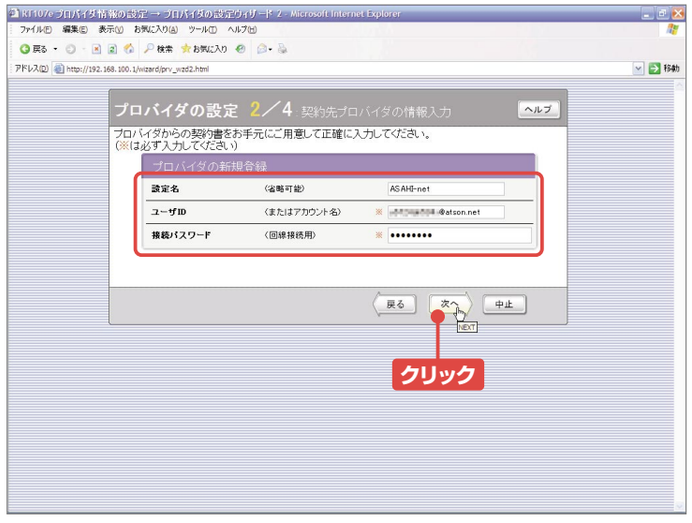
Keyword

PPPoEとは?

PPP over Ethernetの略で、文字通りイーサネット上でPPPの認証等を実現する機能を指します。NTT東西のフレッツ・ADSLやBフレッツはプロバイダを自由に選択でき、複数のプロバイダを使うことも可能です。そのため、異なるプロバイダでそれぞれユーザー認証ができるよう、こうしたプロトコルが使われます。

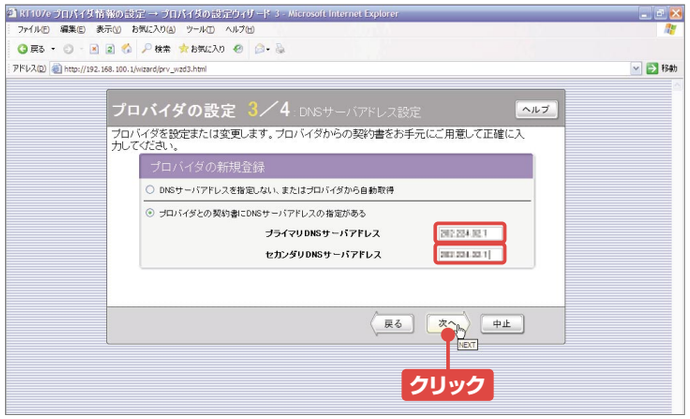
5 ユーザーIDの登録

「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。



6 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。そのため、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。



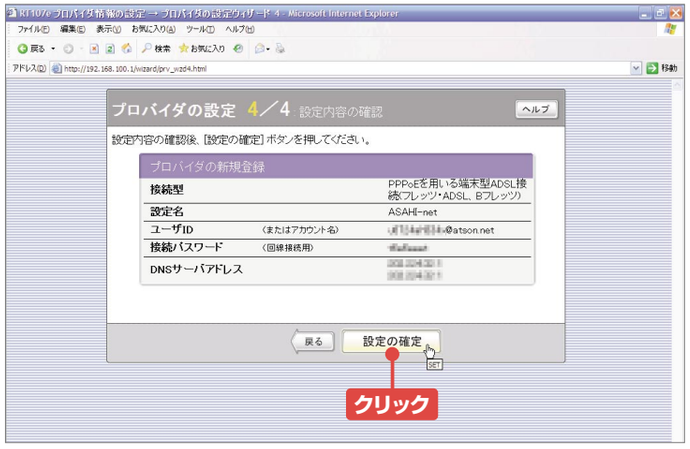
Keyword

DNSサーバとは?

Webサイトなどを指定する際、通常は「http://www.yamaha.co.jp/」のようにアルファベットのわかりやすい名前で指定できます。しかし、コンピュータが実際に接続する際には「10.0.0.1」といったIPアドレスが必要になります。この両者を変換するのが、DNS（Domain Name System）です。Webサイトだけでなく、「yamaha@yamaha.co.jp」のようなメールアドレスが利用できるのも、このDNSのおかげです。

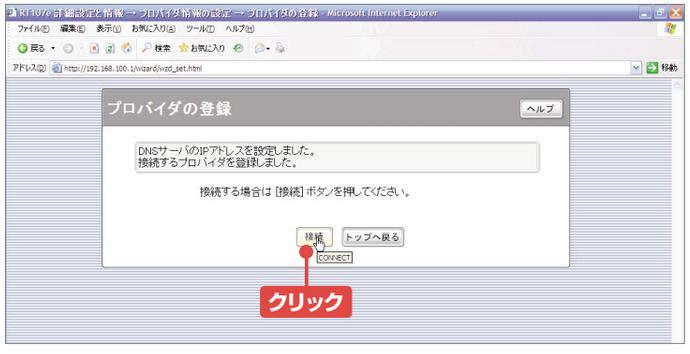
7 設定の確認

今までの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、「接続の確定」ボタンを押します。



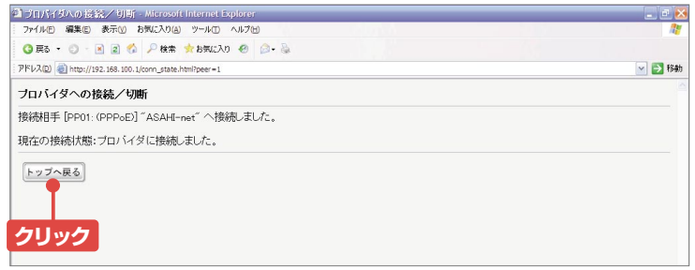
8 設定の完了と接続

これにより設定が行なわれたので、接続ボタンで実際につないでみましょう。



9 接続完了

「現在の接続状態：プロバイダに接続しました。」が表示されると、無事に接続が完了します。「トップへ戻る」のボタンを押します。



10 通信中のトップページ

トップページでは無事に接続が行なわれている場合、「インターネットの設定・状態」に「通信中」のアニメーションが表示されます。また、「グローバル」にIPアドレスが表示されます。このグローバルがVPNでの接続で必要なIPアドレスになります。

11 Webページを表示

http://www.yamaha.co.jp など、インターネット上のWebページを開いてみましょう。

Column

ネットボランチDNSサービスとは?

サーバを構築してホームページを公開したり、ファイルをインターネット上で共有したりするためには、自分のグローバルIPアドレスが相手にわかっている必要があります。ところが、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、インターネットに常時接続していても、再起動時に割り当てられるグローバルIPアドレスが変更されることがあり、サーバの公開が困難でした。これを解決する手段として、ヤマハでは「ネットボランチDNSサービス」と名付けたダイナミックDNS機能を運営し、無償で提供しています。

この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アドレスを告知してくれるため、固定ホスト名の使用が可能。固定IPアドレスサービスを契約していなくても、自宅で独自ドメインを使った各種サーバーを公開・運用したり、VPNを使って外部とデータをやり取りすることができるようになります。（なお、ネットボランチDNSサービスは、予告なくサービスを停止する場合があります）

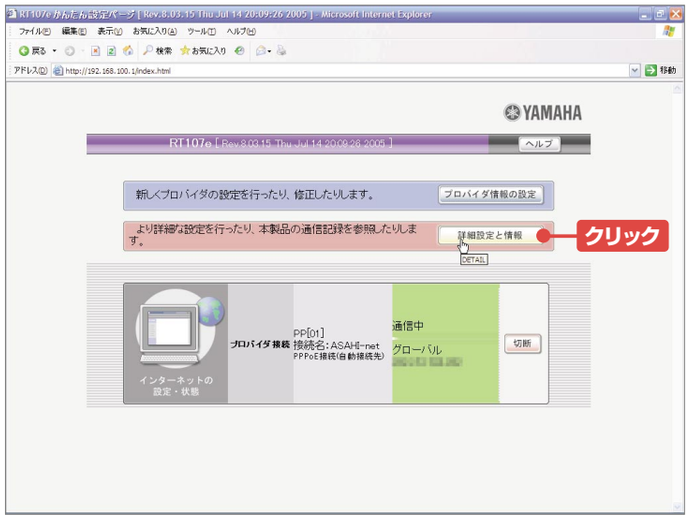
VPNを構築する

インターネットへの接続が完了したら、次はいよいよVPNの設定を行ないます。IPsecは難解なセキュリティ技術の固まりですが、ヤマハのRT107eは簡単に設定できるようになっています。

トンネルの追加とVPN設定

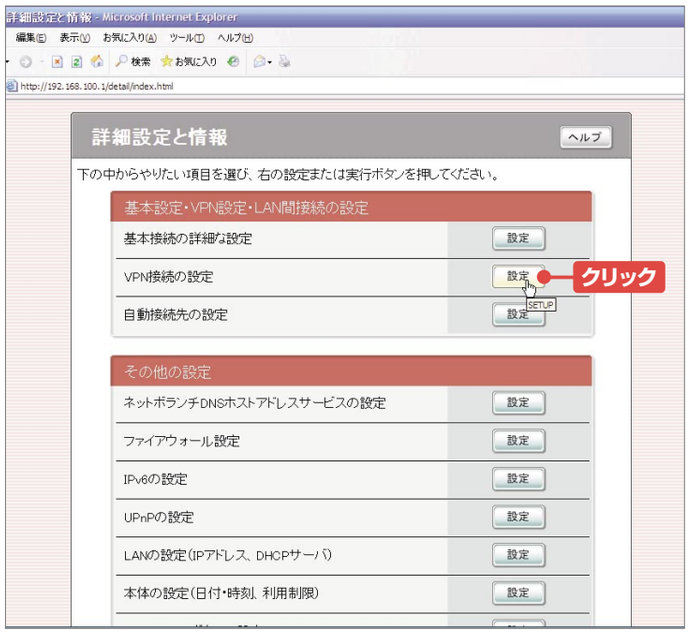
1 VPN設定のメニューを呼び出す

トップページの「詳細設定と情報」ボタンを押します。



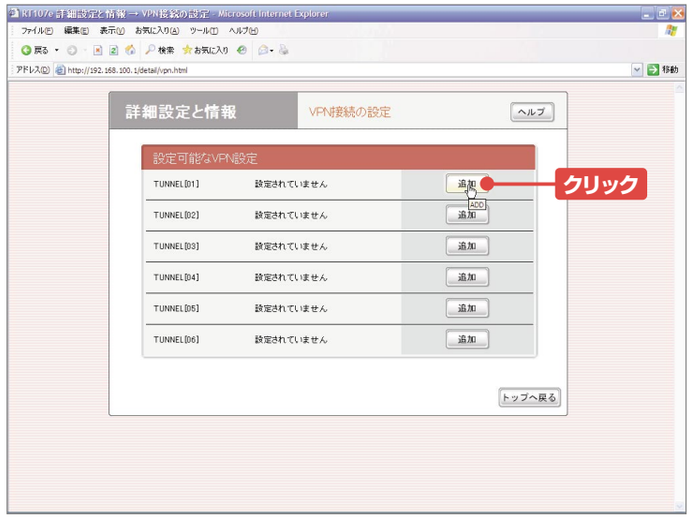
2 VPN接続の設定

「詳細設定と情報」のページの上部にある「VPN接続の設定」ボタンを押します。



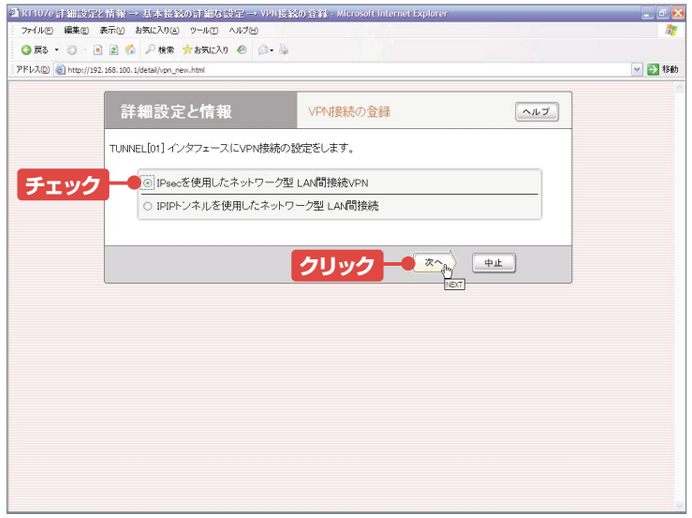
3 トンネルの追加

設定可能なVPN設定で「TUNNEL［01］」の「追加」ボタンを押します。



4 「TUNNEL［01］」の設定

インターネットVPNの場合は、「IPsecを使用したネットワーク型LAN間接続VPN」を選択します。「IPIPトンネルを使用したネットワーク型LAN間接続」は主にNTT東日本の「フレッツ・グループアクセス」、NTT西日本の「フレッツ・グループ」のサービスを用いたVPNを構築する際に利用されます。



フレッツ・グループアクセス／フレッツ・グループとは？

Column

NTT東西が展開するフレッツ網用のVPNサービスで、NTT東日本が「フレッツ・グループアクセス」、NTT西日本が「フレッツ・グループ」というサービス名称になっています。ADSLやBフレッツなどで接続されたユーザー同士の端末、もしくはインターネットを介さずLAN同士をフレッツ網内で接続できます。

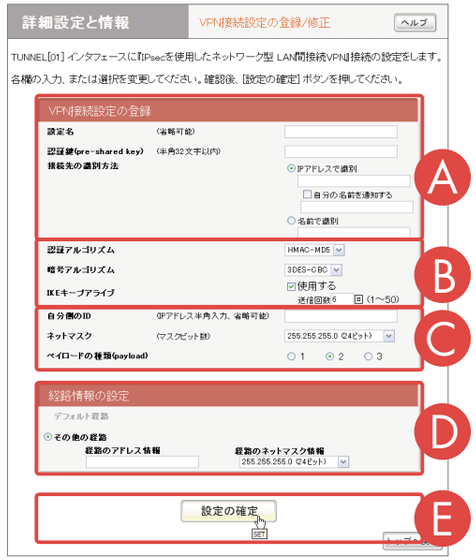
NTTの運営する閉域ネットワーク内で拠点間接続ができるため安全かつ信頼性も高いです。

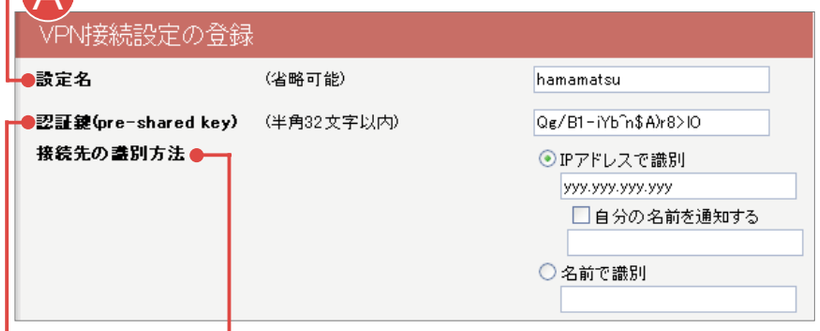
また、最大10拠点までという制限はありますが、「フレッツ・グループアクセス ライト」という月額735円（税込）の料金が安価なサービスもあります。

IPsecの詳細設定を行なう

5 VPN接続設定の登録／修正

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によるトンネルが構築される準備が整います。詳細は次ページ以降で解説します。





設定名

名前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、対向するルーターには、同じ文字列を入力しなければなりません。

接続先の識別方法

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。

注意！

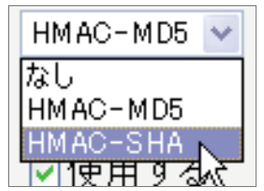
IPsecでの接続先の識別

IPsecでは接続先のルーターを識別する方法として、IPアドレスと名前を利用できます。IPアドレスを使う場合、接続のたびに異なるIPアドレスが割り当てられると、接続する側でIPアドレスをいちいち変更しなければなりません。そのため、安定的な運用のためには、固定のグローバルアドレスを取得するのが望ましいのです。なお、自分のIPアドレスは「自分側のID」に入力します。

一方、名前はIPアドレスが固定されない場合に使うもので、動的にIPアドレスを割り当てられるルーターでは、相手に名前を通知し、自らが正当な接続装置であることを知らせる必要があります。ただし、「接続先」の設定はIPアドレスで指定するので、両方で「名前で識別」を使うことはできません。

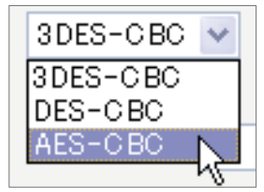
認証アルゴリズム

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。RT107e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、強度としては「HMAC-SHA」がもっとも高いです。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

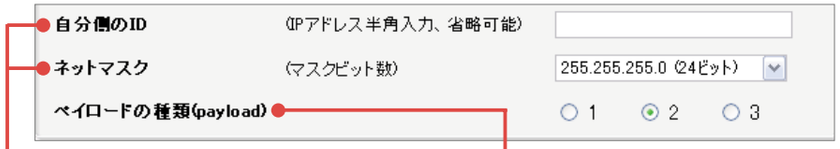
接続先との間で定期的にパケットをやりとりすることで、接続状態を監視します。「使用する」をオンにすると、監視パケットが定期的に送信されます。送信回数の数字を指定すると、その回数分パケットを送っても応答がなかった場合に切断されたと認識、前面の「STATUSランプ」を点滅させ、障害の発生をいち早く知らせます（P21参照）。

AESってなに？ Column

IPsecでは、パケットを暗号化して、インターネットに流します。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、ヤマハのルーターでは、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が標準で使われています。AESは、DESに代わる暗号アルゴリズムとして急速に普及しつつあります。

AESは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。

C



自分側のIDとネットマスク

「自分側のID」と「ネットマスク」は指定しないようにします。

ペイロードの種類

通常は2のままでよい。古いバージョンのヤマハルータや他社のルータと接続する際のみ変更する必要があります。

D

経路情報の登録

パケットの宛先に対する経路を設定する。ここでは支社側のネットワーク（192.168.50.0/24）を宛先とするパケットをVPNのトンネル経由で送り出すよう設定しています。

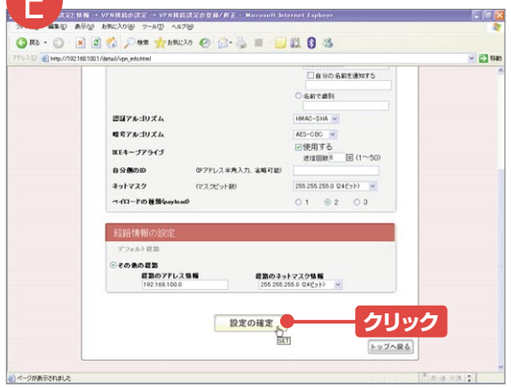
本社側ルーターのIPsec設定

設定名は接続先となるhamamatsuを登録。接続先は支社側ルーターWAN側のIPアドレス、自分側のIDにもWAN側のIPアドレスを設定します。経路は支社側ルーターのネットワークである「192.168.50.0」、サブネットマスク「255.255.255.0」を設定します。

支社側ルーターのIPsec設定

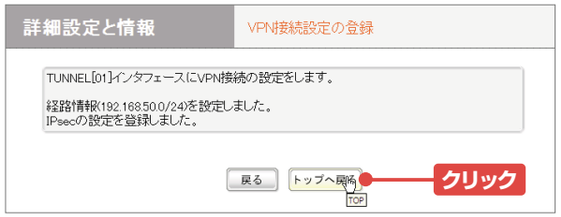
設定名は接続先となるTokyoを登録。接続先は本社側ルーターWAN側のIPアドレス、自分側のIDにもWAN側のIPアドレスを設定します。経路は本社側ルーターのネットワークである「192.168.100.0」、サブネットマスク「255.255.255.0」を設定します。あとの設定は本社側ルーターと同じです。

E



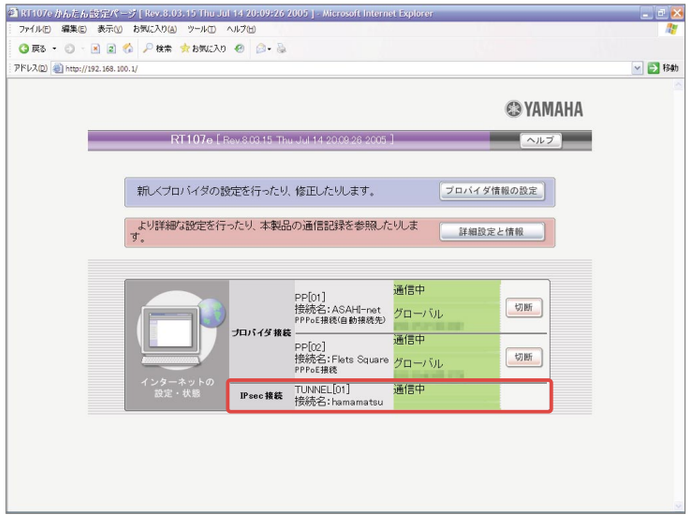
確定ボタンを押す

設定を確認したら、確認ボタンを押します。入力したIPsecの設定と経路情報が登録されますので、「トップへ戻る」を押して、トップページに戻ります。



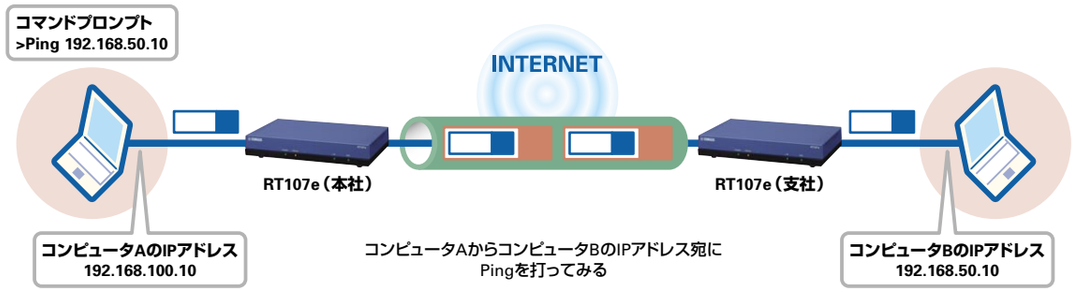
6 IPsecで通信中

IPsec接続が実行されている場合は、トップ画面の「IPsec接続」のTUNNEL［01］で通信中と表示されます。プロバイダ接続とは別途に拠点間でのVPNが構築されたことがわかるでしょう。



IPsecの導通試験を行なう

図6 Pingで導通確認



トンネル経由でもPingを使えば、ホストへの到達が調べられます。

応答を見る

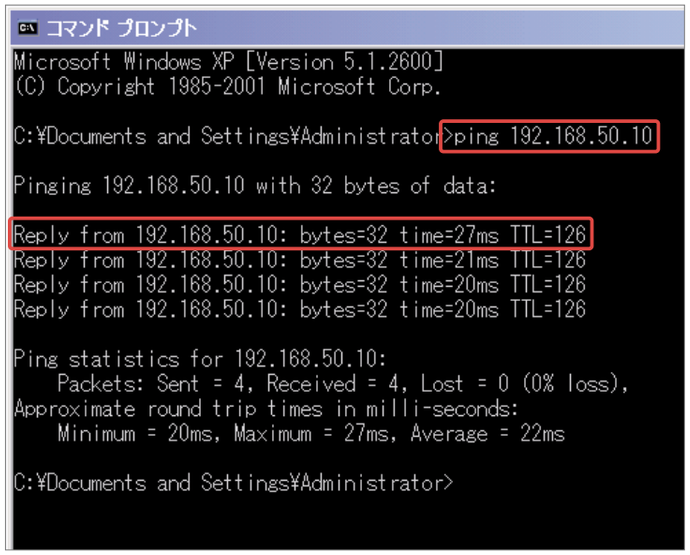
本社側のLANから支店側のLANに対して通信ができているかどうかを調べるためには、Pingを打ってみるとよいでしょう。上図のとおり、本社側のコンピュータA（192.168.100.10）から支社側のコンピュータB（192.168.50.10）に対してきちんと通信ができるかを調べるには、Windowsの「スタートメニュー」から「すべてのプログラム」−「アクセサリ」−「コマンドプロンプト」を開き、

>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、きちんとトンネルが構築できています。



Keyword

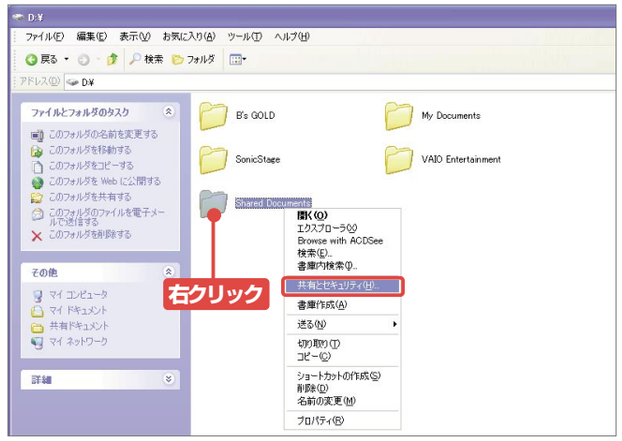
Pingとは?

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。pingは、ICMPのechoコマンドの仕組みを使って実現されている。使い方は、IPアドレスやホスト名をパラメータに指定するだけでよい。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る。また、途中のルーターが止まっていたり、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る。

VPN経由でファイル共有

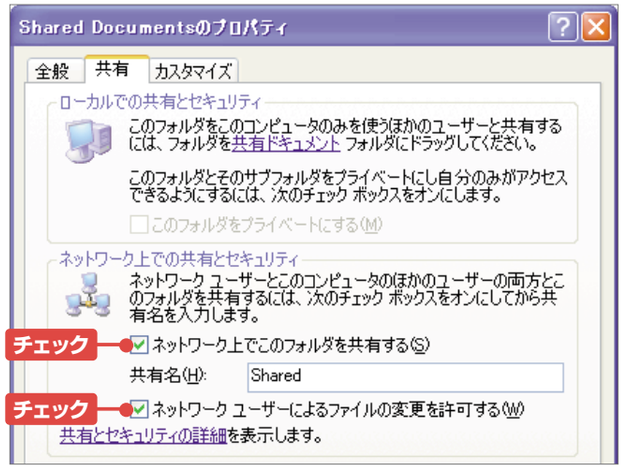
1 コンピュータBでファイル共有

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よい。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」を開きます。



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経由では使えません。

管理編

VPNを管理する

無事にVPNが開通しても、安定して使えなければ意味がありません。そのため、日々の運用・管理の作業がきわめて重要になります。ヤマハのRT107eは、こうした管理・運用を助ける便利な機能をいくつも持っています。

便利な運用・管理機能

GUI画面で設定や状態を把握

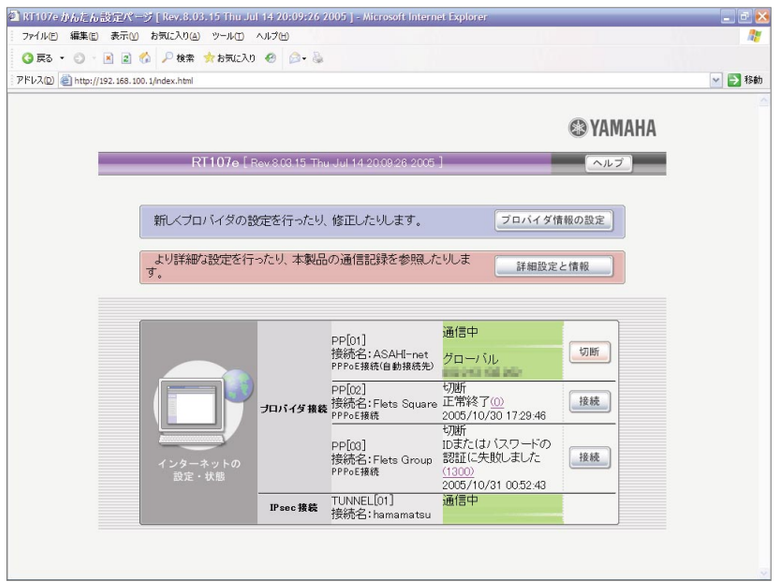
RT107eは、コマンドでの設定だけではなくWebブラウザのGUIで操作が可能です。設定だけではなく運用・管理に便利な機能も知っておきましょう。

まずインターネットやVPN、フレッツ・スクウェアなどへの接続状態はトップページで確認できます。接続で利用されているIPアドレスや通信中／接続中／切断といったステータス、あるいは切断理由や終了時間などもまとめて表示されるので、通常はこのトップページを表示しておけばよいでしょう。

ルーターの詳細な設定を見たい場合は、「詳細設定と情報」のボタンを押し、「レポートの作成・コマンド実行・初期化」の「本製品の全設定(config)のレポート作成」や「システム情報のレポート作成」を実行しましょう。特にシステム情報のレポート作成は、ルーター全体や各インターフェイス、DHCPサーバや経路の設定、IPsecの接続情報等が日本語でまとめて表示されるので、初心者でもわかりやすいです。

また、通信の履歴を示すログのレポートもここで作成できます。こちらは時間軸に沿って、通信の履歴がまとめて表示されています。通信の断絶やスループットの低下などのトラブルシューティングの際に役立つでしょう。

さらに、ルーターの設定を管理者以外に触らせないようにするために、アクセス制限をかける必要もあるでしょう。Webブラウザを使えば、誰

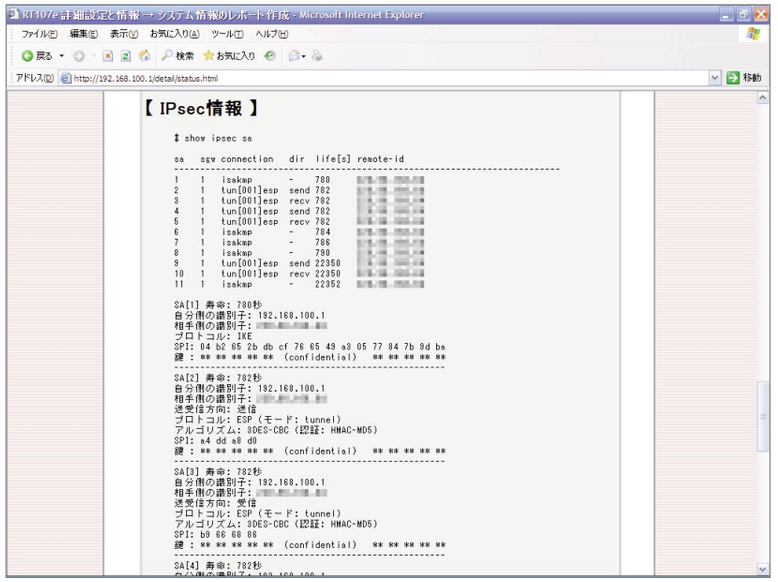


■RT107eのトップページ

通信中、切断など通信状態が一見できるRT107eのトップページ

■システム情報のレポート作成

IPsecのトンネルの状態や情報もまとめて出力できます



しも設定ページにアクセスできてしまうからです。この場合は「その他の設定」の「本体の設定」で、ログイン時のパスワードを設定しておきましょう。

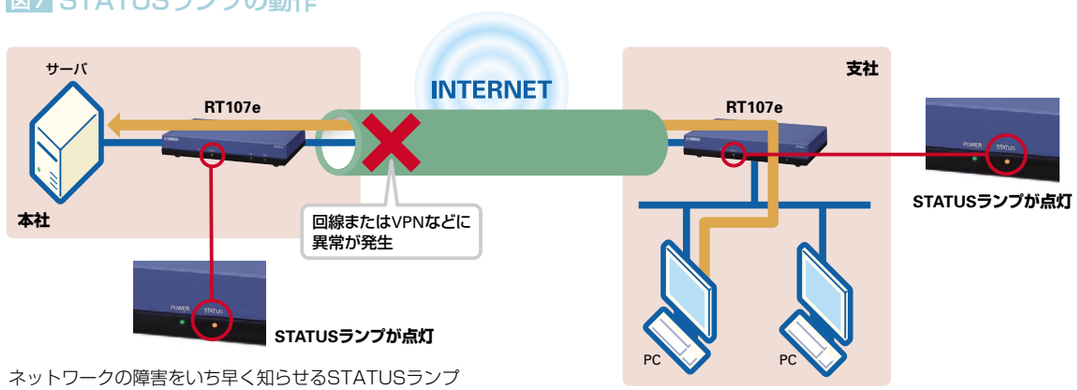
障害を知らせるSTATUSランプ

インターネットVPNは拠点間をつなぐいわば専用線と同じような使い方をするため、いったんつながったら常時通信できていて当たり前という状態になります。そのため、いざ障害が発生して、通信ができなくなると業務に影響が出てくるでしょう。回線等で障害が発生した場合には、それをいち早く知り、復旧させなければなりません。そのために便利なのが、筐体前面に用意されている「STATUSランプ」です。

これはあらかじめ指定された経路の状態を表示する機能です。指定した経路上で異常が発生するとランプが点灯するので、管理者はいち早く障害を知ることができます。IPsecやIPIPトンネルのキープアライブ機能は初期状態で有効になっているので、初期設定は特に必要ありません。ただし、ランプの点灯がわかるよう、見えやすいところに設置する必要があります。

高価な管理ツールや保守サービスを導入できない中堅・中小企業にとってみれば、こうした細かい機能追加がとても重要といえるでしょう。

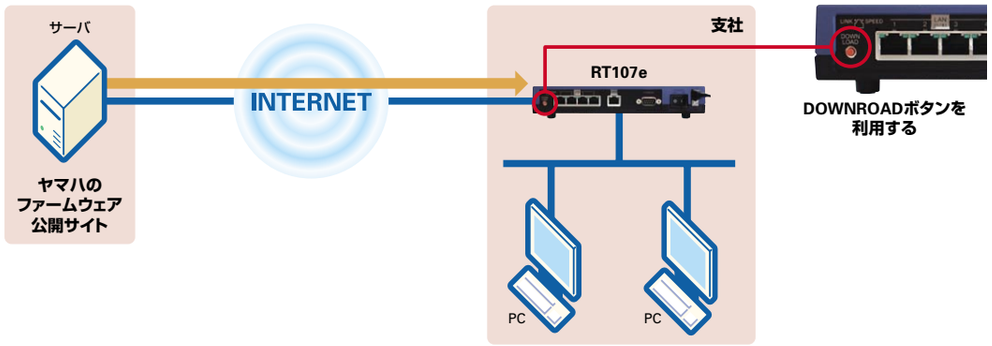
図7 STATUSランプの動作



ネットワークの障害をいち早く知らせるSTATUSランプ

ファームウェアの自動更新

図8 更新を自動化



ボタンを長押しすると、自動的にファームウェアをインストール

ファームウェアを自動更新してくれる「DOWNLOADボタン」も利用価値が高い機能です。

ファームウェアとは、ルータを動かすためのソフトウェアを指しており、最新版をインターネット経由で入手することで更新できます（リビジョンアップ）。ヤマハのルーターは、このファームウェアの更新により、不具合の解消だけでなく、機能強化やパフォーマンスの向上などを実現しているので、リビジョンアップはとても重要です。

しかし、実際のファームウェア更新はソフトウェアをPCにいったんダウンロードして、ルーター本体に書き込むという処理が必要なので、初心者にとってはやや敷居が高かったのも事実です。

ですが、RT107eではDOWNLOADボタンを使えば、いざ最新版のファームウェアが登場したときにはボタンを押すだけで、自動的に更新作業が行なえます。実際には1秒間以上長押しすると処理が開始されます。

これだけ簡単であれば、ネットワークに詳しくない人でも作業が可能です。たとえば、本社の管理者が支社や営業所の従業員に「背面の赤いボタンを1回押してください」と頼めば、作業は無事終了することになります。

ただし、初期状態では自動更新が許可されていませんので、以下の設定を行なって、利用可能にしましょう。

1 DOWNLOADボタンの設定を開く

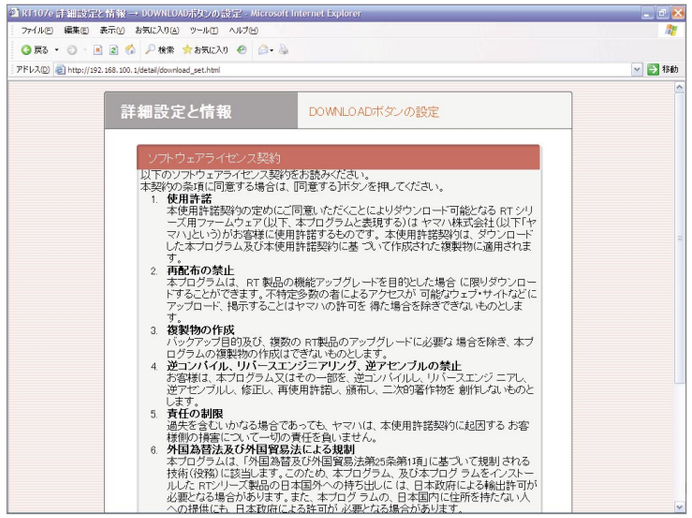
トップ画面の「詳細設定と情報」ボタンを押します。さらに「その他の設定」から「DOWNLOADボタンの設定」ボタンを押します。

2 リビジョンアップの許可

初期状態では「許可しない」になっているので、「許可する」のチェックボタンをオンにし、「設定の確定」ボタンを押します。

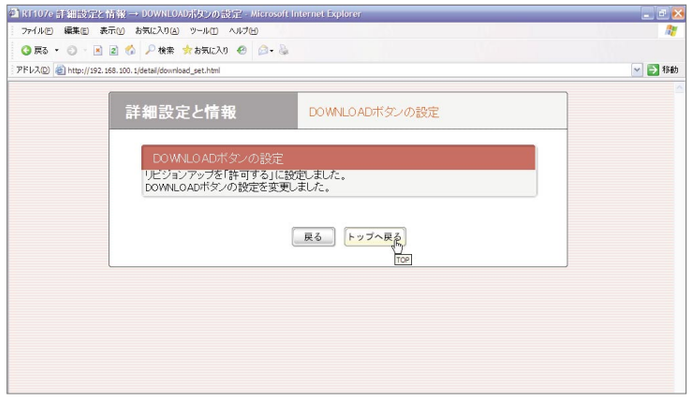
3 ソフトウェアライセンス契約

ファームウェアの利用に関するライセンス契約の許諾画面に移ります。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

設定は完了し、DOWNLOADボタンを押せば、最新のファームウェアがダウンロード、インストールされます。



注意！

ファームウェアのダウンロード中はSTATUS、LAN、WANランプが順番に点滅します。そしてリビジョンアップの作業が完了すると、自動的に再起動します。この間、電源を落としたり、ケーブルを抜いたりしてはいけません。製品が利用できなくなる可能性があり、修理が必要になります。

応用編

内線VoIPを使ってみよう

VPNで拠点同士をつないだら、内線VoIPの利用も検討したいところです。インターネットを経由するので、あらたに通信費もかかりませんし、音質や使い勝手も既存の電話と変わりません。ここではRT57iを使ったVoIPの利用方法を紹介します。

トンネル内に音声パケットを通す

RT107eで構築したIPsecのトンネルを使うことで、拠点間でさまざまなアプリケーションが利用できます。Webグループウェアやメール、ファイル／プリンタ共有などがありますが、IP電話（VoIP：Voice over IP）もその1つです。

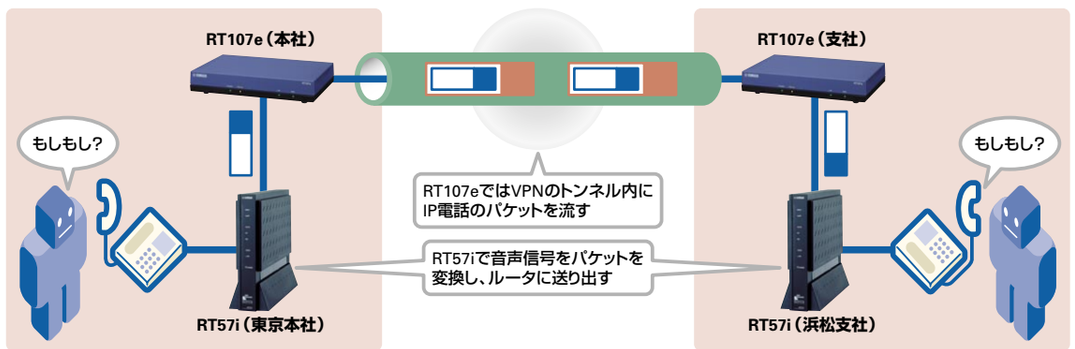
IP電話とは、音声をパケットに変換し、IPネットワーク経由で送ることで、低価格な通話を実現する技術です。IP電話の導入としては、公衆回線などへの外線通話の料金を安価に抑えるパターンと、拠点間の内線をIP化することで、回線や機器のコストを削減するパターンがあります。ヤマハのVoIPルーターは、外線と内線のいずれのIP電話の用途でも使えます。以下、RT107eで構築したVPNとヤマハのVoIPルーター「RT57i」を組み合わせた、低価格な内線VoIPのソリューションを見ていきましょう。

RT57iは、個人とSOHOでの利用を想定した低価格なVoIPルーターで、VoIPゲートウェイの機能を持っています。VoIPゲートウェイとは、音声とIPパケットを相互に変換する機能で、これを利用すると既存のアナログ電話機を使ってVoIPが実現できます。

今回構築する内線VoIPの構成は、下図のとおりで、東京本社のサブネットが「192.168.100.0/24」、浜松支社のサブネットが「192.168.50.0/24」になります。

すでにRT107eでVPNが構築されている環境にVoIPルーターであるRT57iを追加するというイメージになります。RT107eに特に設定の変更はありません。一方、RT57iはまずTELポートに電話機を、WANポートをRT107eのLANポートにつなぎます。あとは、RT107eと同じようにWebブラウザで設定ページを呼び出し、各種の設定を行なえばOKです。作業としては大きく、①WANポートに固定のプライベートアドレスを割り当てる、②VoIPの基本設定を行なう、③通話相手のアドレスを電話帳に登録する、という流れになります。

図9 VPN経由でVoIPを実現する

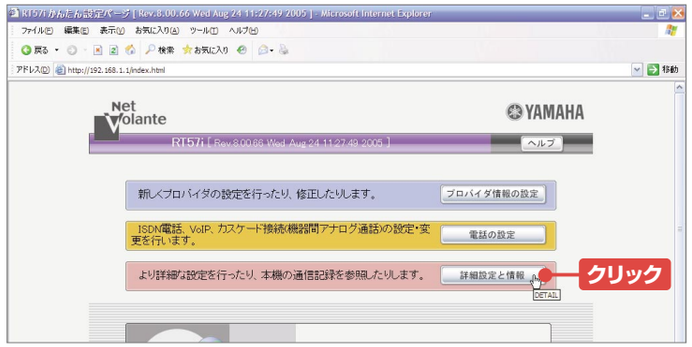


利用するネットワーク構成はVPNの際と同じで、東京本社と浜松支社のRT107eでIPsecのトンネルが構築されています

RT57iをLAN内に設置

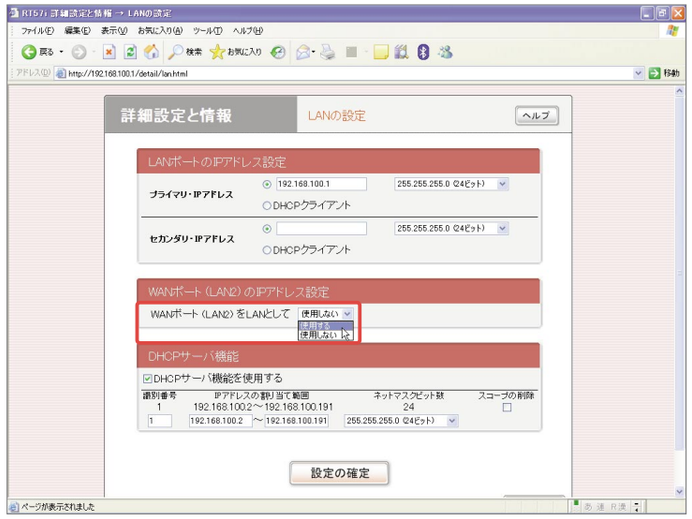
1 RT57iのトップページ

RT57iのトップページで「詳細設定と情報」ボタンを押します。「その他の設定」から「LANの設定（IPアドレス、DHCPサーバ）」の設定ボタンを押します。



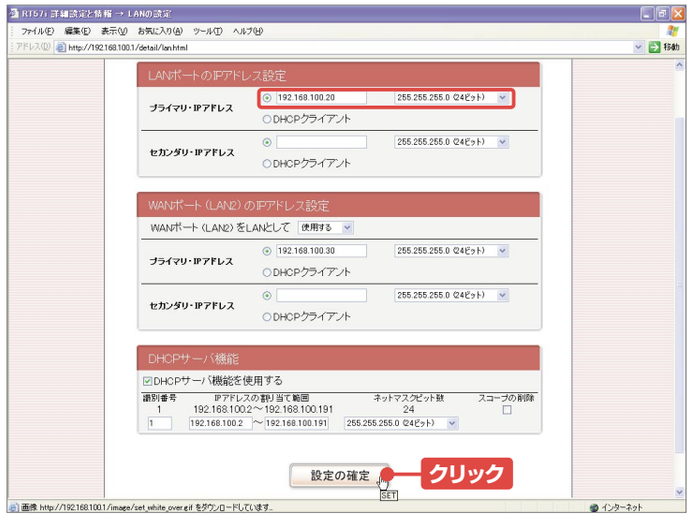
2 WANポートをLANポートとして利用

「WANポート（LAN2）のIPアドレス設定」で「使用する」を選択し、下の「設定の確定」ボタンを押します。PPPoEなどのインターネット接続設定がすでにあると設定できないので、あった場合は削除しておきます。



3 LANポートのIPアドレスを設定

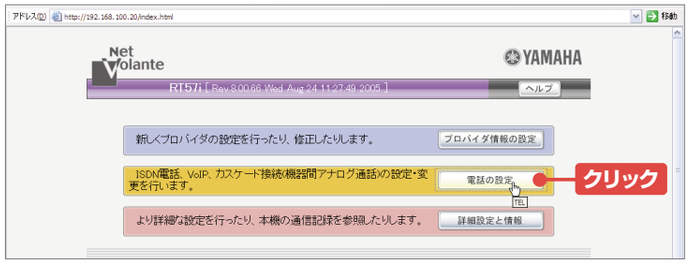
トップページに戻り、再び同じ設定ページを表示し、IPアドレスを入力します。LANポートとWANポートにRT107eと同じネットワークアドレスの異なるIPアドレスを指定しましょう。あとは「設定の確定」を押せば設定は完了です。



RT57iのIP電話設定

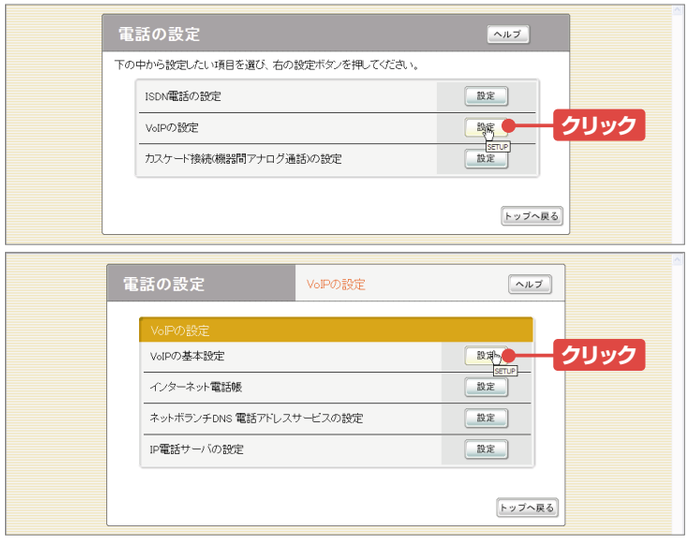
4 電話の設定

RT57iのかんたん設定ページで「電話の設定」のボタンを押します。

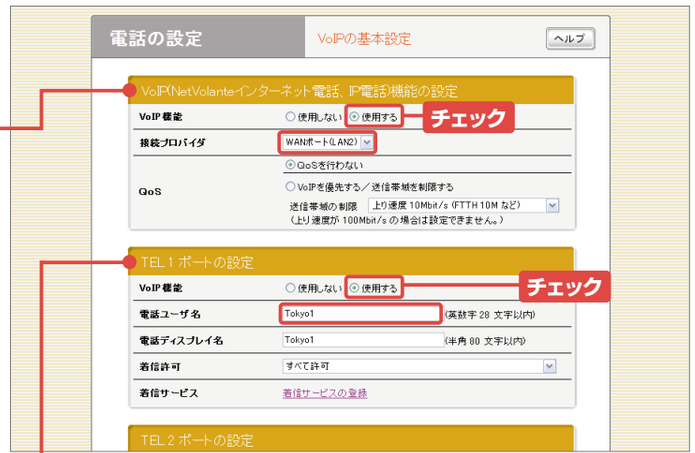


5 VoIPの基本設定を開く

「電話の設定」が開いたら「VoIPの設定」のボタン、続いて「VoIPの基本設定」のボタンを押します。



6 VoIPの基本設定



「VoIP（NetVolanteインターネット電話、IP電話）機能の設定」
「VoIP機能」で、「使用する」のチェックボックスをオンにするとVoIP機能が利用可能になります。また、「接続プロバイダ」は先ほど設定した「WANポート（LAN2）」を選択します。

TEL1ポートの設定
電話機をつないだTELポート個別の設定を行ないます。VoIP機能が「使用する」になっているのを確認し、「Tokyo01」や「hamamatsu01」といった電話ユーザー名を指定します。

7 インターネット電話帳を選択

通話相手の電話番号を登録するため「VoIPの設定」の「インターネット電話帳」を選択します。

8 インターネット電話番号の登録

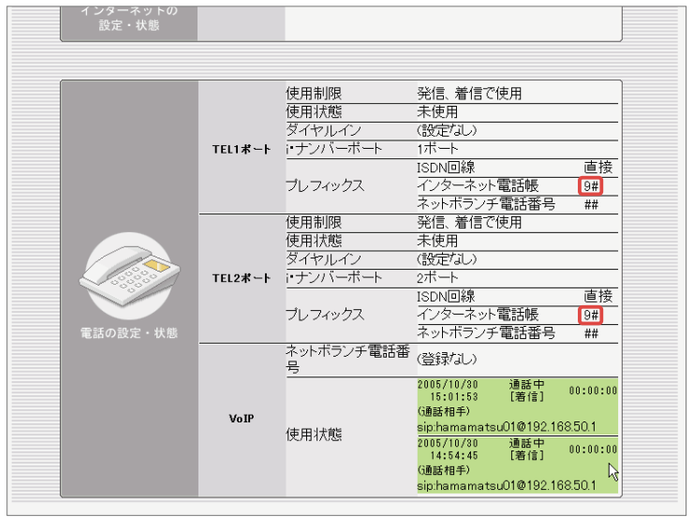
宛先名
「hamamatsu01」のような内線電話の宛先を登録します。

インターネット電話番号
「501」のようなユーザーが実際に指定する内線番号を入力します。半角数字32文字までです。

相手sipアドレス
インターネット電話番号では、このsipアドレスで指定された相手を呼び出すことになります。SIPアドレスはメールアドレスやWebのURLと同じ種類のもので、IP電話ではこのアドレスを元に相手を識別します。形式は電話ユーザー名@ホストアドレス（IPアドレスなど）になります。電話ユーザー名は先ほどTEL1ポートで指定した名前で、ホストアドレスはIPアドレスを入力します。そのため、通常は「hamamatsu01@192.168.50.20」のようなアドレスになります。「設定の確定」ボタンを押せば、登録が完了です。

7 プレフィックスを付けて発信

通話をする際は、インターネット電話番号であることを示すプレフィックス「9#」を内線番号に付けて発信します。501が内線の場合は、「9#501」でトンネルの先にある内線電話機を呼び出し、音声通話が行なえます。



カタログ

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。ここではヤマハの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VPN＋VoIPルーター

ヤマハルーターとは？

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。

今から10年前、ルーターは外資系のベンダーの製品がほとんどで、非常に高価な機器でした。そのため、LANやインターネットの重要性を理解しつつも、特に中堅・中小企業では導入するのが難しかったのです。そこに登場したのが、低価格で高品質を売りにしたヤマハのISDNルーター「RT100i」です。他社製品に比べて約半額の20万円を切る価格で発売されたRT100iは、市場に大きなインパクトを与えました。

その後、1998年には個人・SOHO向けのISDNリモートルーター「NetVolante RTA50i」、2002年にはブロードバンド対応の企業向けルーターである「RTX1000」を発表。2005年で累計出荷台数100万台を超すという偉業をなしとげています。

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、軽量なプラスチック筐体を採用したり、国内の大多数を占める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。

図10 ヤマハの企業向けルーターラインナップ

センター向けや拠点向けなど豊富なラインナップが用意されています

図11 VPNルーターとクラス

ヤマハではVPNルーターを用途や規模に応じて4つのクラスに分けています

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たのも、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。

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、RTX1100を筆頭とするVPNルーターです。

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自前で構築するためのVPN機器の種類も多彩です。もちろん、企業がVPNに求めるニーズも異なっています。数拠点を接続するような小規模なネットワークを想定している中堅・中小企業であれば、使いやすさや安価な導入コスト等を求める傾向が強いでしょう。これに対して多くの拠点を接続しなければならない大企業であれば、パフォーマンスや信頼性、拡張性などに重点が置かれるでしょう。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（図11）。

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）を採用したものです。PPTPはWindowsでサポートされているため、手軽に利用できるのが最大の特徴です。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「RT57i」になります。また、NTT東日本のVPNサービスであるフレッツ・グループアクセスの拠点間接続を想定した「IPIPトンネル」というVPNも利用できます。デザインも個人宅で設置するのに違和感がない黒の縦型ルーターで、ケーブルなどを本体の後部に隠せるようになっています。

また、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、今やヤマハルーターの標準機ともいえるRTX1000とスペック向上を施したRTX1100です。RTX1000/1100はインターネット上にVPNを構築する他の標準プロトコルがIPsecをサポートしています。IPsecは文字通りIPの通信にセキュリティ機能を追加する

もので、暗号化やパケット・接続先の認証などを併用することで、非常に強固なセキュリティを実現しています。IPsecプロトコルにより誰でも利用できるインターネットでも安全に拠点間接続が行なえるわけです。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、RTX1000で最大55Mbit/s（3DES：双方向）、RTX1100では最大120Mbit/s（AES：双方向）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、バックアップ回線として利用できます。つまり、メインのインターネットVPNがなんらかの理由でダウンした場合は、自動的にISDN回線に切り替えて通信を継続することが可能です。

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がお勧めです。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、パケット処理能力が高いため、音声やビデオなどのマルチメディア系のTV会議やIP電話を実現するためにRTX1500は最適な機種です。

VPNの敷居を下げるRT107e

そして10月に発売されたばかりの新製品「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。RT107eという製品名を見ればわかるとおり、製品的には個人・SOHO向けのRT57iの兄貴分にあたるVPNルーターです。

スタンダードVPNである、RTX1100が実現する最大120Mbit/sというスループット（AES：双方向）、30という接続拠点数に対して、RT107eはVPNスループットが50Mbit/s（AES：双方向）、接続拠点数が6となっています。その一方で、RT107eは価格も7万円台で、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RT107eでは、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。

VoIP機能をルーターでも搭載

VPN以外にヤマハが力を入れているソリューションとして、VoIP（Voice over IP）が挙げられます。音声をIPパケットに変換して、リアルタイムにIPネットワークに流すというVoIPゲートウェイの機能を一部のルーターに追加しています。

代表的な製品が個人・SOHO向けの「NetVolante RT57i」です。最大同時2通話をサポートし、企業向けの050対応のIP電話サービスでも利用できます。そして、RT57iを拡張した企業向けのVoIPゲートウェイが「RTV700」になります。RTV700はPBXやISDN対応のビジネスホンと直接接続ができ、最大同時6通話をサポートしています。さらにIPsecの機能も搭載しているので、VPNルーターとして利用することも可能になっています。

さらに最新製品として「RTV01」というユニークな電話帳サーバーも登場しています。RTV01はIP電話で利用する電話番号を一元管理するための専用機で、最大5台と連携することで2500の電話番号を管理できます。2台を連携させた冗長構成も可能なので、非常に堅牢で拡張性の高いIP電話システムが構築できます。

■電話帳サーバー「RTV01」

RT57iやRTV700と連携し、IP電話番号を管理する専用機です。

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://www.yamaha.co.jp/router/

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。

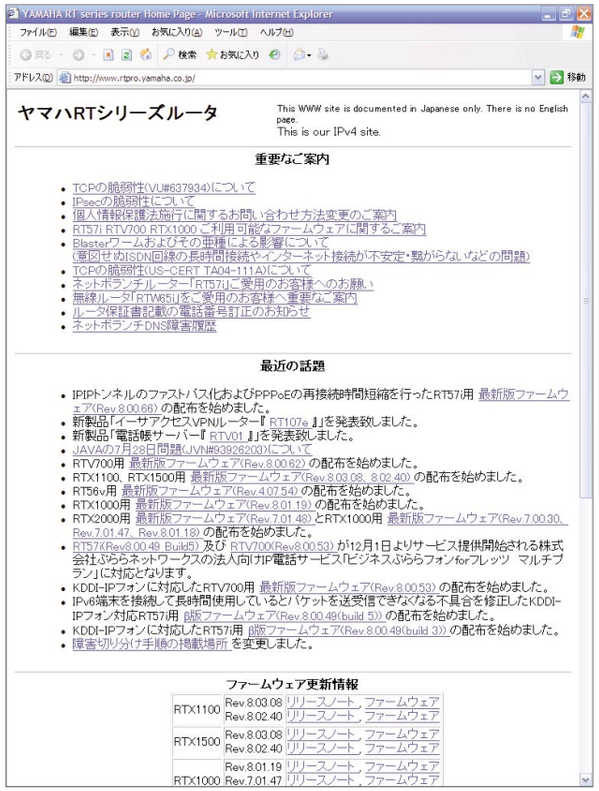
●ソリューション

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

よくある質問、詳細な質問、設定例集、接続サービス設定ガイドなどが掲載されています（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、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。

ホームページの内容は予告なく変更することがございます。予めご了承下さい。



ヤマハRTシリーズルータ

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

技術情報が盛りだくさんのWebサイトで、ヤマハルーターの情報サイトはもともとこちらが元祖です。ファームウェアの更新情報やリリースノートが掲載されているほか、既存の技術情報がまとめてアーカイブされています。VPNやルーティングプロトコル、QoS、NAT/IPマスカレードなどの汎用的な技術情報や、導入や設定、機能、機種別の詳細なFAQ、あるいはシスコやネットスクリーン製品との相互接続事例集なども掲載されています。ヤマハユーザーのみならず、ネットワーク技術者は必見のWebサイトです。

製品に関する問い合わせ先

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、RTX2000、RTX1500、RTX1100、RTX1000
【RTシリーズ】
RT107e、RT250i、RT300i
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。）

ネットボランチ・コールセンター

対象機種
【NetVolanteシリーズ】
RT57i
【RTVシリーズ】
RTV700、RTV01
電話番号 03-5715-0350
##6259-4341（ネットボランチインターネット電話お問い合わせ先）
ご相談受付時間 9:00～12:00、13:00～17:00、17:00～18:00（臨時）（日・祝日、年末年始は休業とさせていただきます。）