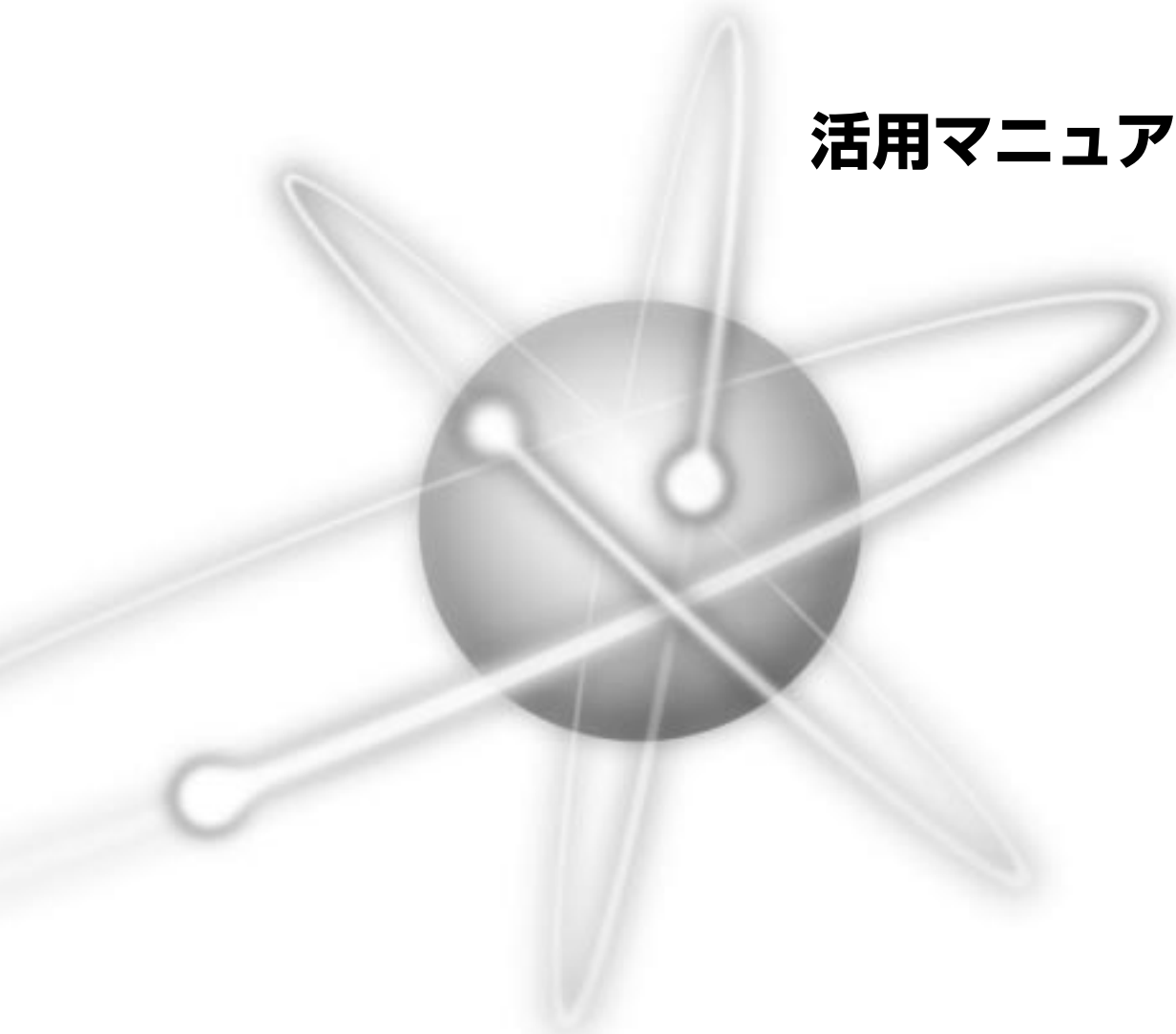
YAMAHA

Net Volante

ブロードバンド無線ルータ

RTW65b

活用マニュアル



本機を活用したいときにお読みください

本機の機能や便利な使いかたを知りたいときは、本書をよく読んで設定を行ってください。
本書中の警告や注意を必ず守り、正しく安全にお使いください。

付属マニュアルのご案内

本機の機能を十分に活用していただくために、下記のマニュアルを用意致しました。目的にあわせてマニュアルをお選びください。

設定マニュアル

本機を使い始めるときに読むマニュアルです。

設置のしかたや設定のしかただけでなく、CATV/ADSLなどのブロードバンドルータとしての基本的な使いかたについて説明しています。

活用マニュアル(本書)

本機の機能を活用するために読むマニュアルです。

ファイアウォールの設定やブロードバンドターミナルアダプタ(TA)としての使いかたについて、その解説と設定方法を説明しています。また、困ったときの対処方法についてもまとめて説明しています。

コマンドリファレンス(PDF形式)

コマンドを使って高度な設定を行いたいときに読むマニュアルです。本機のコンソールコマンドについて解説しています。

マークのマニュアルは付属のCD-ROMにPDF形式で収録しており、お読みになるにはAcrobat Readerが必要です。先にCD-ROMのAcrobat Readerをインストールしてください(102ページ)。

重要なお知らせ

◆ プロバイダ契約について

本機をルータとしてお使いになる前(または新たにプロバイダ契約を行う前)に、必ずルータ経由による複数パソコンの同時接続が、プロバイダによって禁止されていないかどうかご確認ください。**プロバイダによっては、禁止もしくは別の契約が必要な場合があります。**

禁止されている場合は、プロバイダと別途必要な契約を行うか、同時接続を禁止していない他のプロバイダと契約してください。

◆ セキュリティ対策と本機のファイアウォール機能について

インターネットに接続すると、世界中のホームページを閲覧したり、電子メールで自由に情報を交換したりすることができ、とても便利です。しかし同時に、お使いのパソコンに対する不正アクセスの危険に、世界中からさらされることになります。

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

◆ 無線LANの電波に関する注意

- 本製品に使用している無線装置は、電波法に基づく小電力データ通信システムの無線設備として、特定無線設備の認証を受けています。従って、本製品を使用するときに無線局の免許は必要ありません。また、本製品は日本国内でのみ使用できます。
- 心臓ペースメーカーを使用している人の近くで、本製品をご使用にならないでください。心臓ペースメーカーに電磁妨害を及ぼし、生命の危険があります。
- 医療機器の近くで本製品を使用しないでください。医療機器に電磁妨害を及ぼし、生命の危険があります。
- 電子レンジの近くで本製品を使用しないでください。電子レンジによって本製品の無線通信への電磁妨害が発生します。
- 本製品の無線装置は、電波法に基づく認証を受けていますので、以下の事項を行なうと法律で罰せられることがあります。
  - 本製品を分解／改造すること
  - 本製品の背面および無線カードに貼ってある証明ラベルをはがすこと。
- この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか、工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を要する無線局)及び特定小電力無線局(免許を要しない無線局)が運用されています。

  本製品の無線チャネルを工場出荷時以外に設定して使用する場合は、以下の事項に注意してください。但し、本製品の無線チャネルが工場出荷状態の場合は、移動体識別用の無線局と電波干渉をすることはありません。
  - この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認してください。
  - 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに本製品の使用周波数を変更して、電波干渉を回避してください。
  - その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、弊社ネットボランチコールセンター(101ページ)へお問い合わせください。
- 本製品に内蔵されている以外の無線LANカードは使用しないでください。

使用周波数帯域	2.4 GHz
変調方式	DS-SS方式
想定干渉距離	40 m以下
周波数変更の可否	全帯域を使用し、かつ移動体識別装置の帯域を回避可能

◆ 電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

目次

第8章 困ったときは

第9章 その他の情報

本書の表記について

◆ マークの意味

本書では、本機を安全にお使いいただくため、守っていただきたい事項に次のマークを表示していますので、必ずお読みください。

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

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

◆ 略称について

本書では、YAMAHA　RTW65bのことを本機、Microsoft® Windows® をWindows、Microsoft® Windows 95® をWindows95、Microsoft® Windows 98® をWindows98、Microsoft® Windows 98 Second Edition® をWindows98SE、Microsoft® Windows NT® をWindowsNT、Microsoft® Windows 2000® をWindows2000、Microsoft® Windows Millennium Edition® をWindowsMe、Microsoft® Windows XP® をWindowsXP、INSネット64のことをISDN、10BASE-T（100BASE-TX）ケーブルのことをLANケーブルと記載しています。

◆ 設定例について

本書に記載されているIPアドレスやドメイン名、URLなどの設定例は、説明のためのものです。実際に設定するときは、必ずプロバイダから指定されたものをお使いください。

◆ 商標について

- イーサネットは富士ゼロックス社の登録商標です。
- Apple、Macintosh、MacOSは米国Apple社の登録商標および商標です。
- Microsoft、Windowsは米国Microsoft社の米国およびその他の国における登録商標です。
- Adobe、Acrobatは米国AdobeSystems社の登録商標です。
- Stac LZSは米国Hi/fn社の登録商標です。

安全にお使いいただくために

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

⚠ 警告

- 本機は家庭および一般小規模オフィス向けの製品であり、人の生命や高額財産などを扱うような高度な信頼性を要求される分野に適応するようには設計されていません。

  誤って本機を使用した結果、発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。
- 本機から発煙や異臭がするとき、内部に水分や薬品類が入ったとき、およびACアダプタや電源コードが発熱しているときは、直ちに電源スイッチを切ってACアダプタをコンセントから抜いてください。そのまま使用を続けると、火災や感電のおそれがあります。
- 濡れた手でACアダプタや電源コードを触らないでください。感電や故障のおそれがあります。
- 電源コードを傷付けたり、無理に曲げたり、引っ張ったりしないでください。火災や感電、故障、ショート、断線の原因となります。
- ACアダプタは必ず本機に付属のもの(P10V1.2A)をお使いください。他のACアダプタを使用すると、火災や感電、故障の原因になります。
- 付属のACアダプタは日本国内用AC100V(50/60Hz)の電源専用です。他の電源で使用すると、火災や感電、故障の原因となります。
- 安全のため、ACアダプタは容易に外すことのできるコンセントに接続してください。
- 本機を落下させたり、強い衝撃を与えたりしないでください。内部の部品が破損し、感電や火災、故障の原因となります。
- 本機を分解したり、改造したりしないでください。火災や感電、故障の原因となります。
- 本機の通風口を塞いだ状態で使用しないでください。火災や感電、故障の原因となります。
- 電源を入れたまま、USBケーブル以外のケーブル類を接続しないでください。感電や故障、本機および接続機器の破損の恐れがあります。
- USBポートに指や異物を入れないでください。感電や故障、ショートの原因となります。

⚠ 注意

- 直射日光や暖房器等の風が当たる場所、温度や湿度が高い場所には、置かないでください。故障や動作不良の原因となります。
- 極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所で使用しないでください。故障や動作不良の原因となります。結露が発生した場合は、ACアダプタをコンセントから抜き、乾燥させるか、充分室温に慣らしてから使用してください。
- ほこりが多い場所や油煙が飛ぶ場所、腐蝕性ガスがかかる場所、磁界が強い場所に置かないでください。故障や動作不良の原因となります。
- 本機を他の機器と重ねて置かないでください。熱がこもり、火災や故障の原因となることがあります。
- 近くに雷が発生したときは、ACアダプタやケーブル類を取り外し、使用をお控えください。落雷によって火災や故障の原因となることがあります。
- 本機のアースコードは必ず接続してください。感電防止やノイズ防止の効果があります。アース接続は必ず、ACアダプタをコンセントにつなぐ前に行ってください。又、アース接続をはずす場合は、必ずACアダプタをコンセントから切り離してから行ってください。
- 本機を修理や移動等の理由により輸送する場合には、必ず本機の設定を保存してください。

使用上のご注意

- 無線LANを使用する場合は、金属製の壁や机、電子レンジ、他の無線LAN装置の近くへの設置を避けるようにしてください。また、遮蔽物があると、通信可能距離が短くなる場合があります。
- 本機の工場出荷状態では、無線LANによる本機へのアクセスが可能になっています。無線を使った第三者による回線の不正使用を防ぐため、WEP(暗号化機能)をONにして使用することを強くおすすめします。また、無線LANを使用しない場合は、不正アクセスを防ぐために「RTW65iかんたん設定ページへ行く前に」画面で、[無線LANを使用する]のチェックを外すか、または「無線設定」画面で無線モードを[オフ]にしてください。
- 本機のご使用にあたり、周囲の環境によっては電話、ラジオ、テレビなどに雑音が入る場合があります。この場合は本機の設置場所、向きを変えてみてください。
- 本機を譲渡する際は、マニュアル類も同時に譲渡してください。
- 本機を廃棄する場合には不燃物ゴミとして廃棄してください。または、お住まいの自治体の指示に従ってください。

第 1 章
ルータについて

この章では、本機の特長やインターネットのしくみ、ネットワークについての基礎知識について解説しています。本機を使いこなすためやトラブルを避けるために、必ずご一読ください。

ネットボランチRTW65bでできること

本機は、ブロードバンドルータ、ブロードバンドTA、無線LANアクセスポイントの機能をすべて内蔵した、多機能ルータです。CATV／ADSL接続と無線LANを利用したインターネット接続まで対応できます。

◆ ブロードバンド対応

CATVやADSLなどのブロードバンド回線用モデムに接続できるWANポートを装備しています。

◆ 無線LAN& 有線LAN（10BASE-T/100BASE-TX）両対応

IEEE802.11b準拠の11Mbit/s無線LANアクセスポイントを内蔵しているため、配線なしでインターネットやLANに接続できます。また、複数のRTW65bを使うことで、離れたLANどうしをつなげるブリッジ機能や、移動しても無線アクセスポイントを自動切り替えできるローミング機能にも対応しています。

◆ ファイアウォール機能

静的／動的の2種類のフィルタによるパケットフィルタリング機能で、外部からの不正アクセスに対してセキュリティを強化できます。不正アクセスや攻撃を検出した場合にお知らせする、不正アクセス検知機能も搭載しています。

◆ かんたん設定

付属のユーティリティソフトウェア「RTW65bパソコンセットアップ」でパソコンのネットワーク設定を自動的に行えます。本機は設定のためのホームページ「RTW65bかんたん設定ページ」を内蔵しているため、本機の基本的な設定はパソコンのWebブラウザで変更できます。

◆ メール着信確認／メール着信転送機能

登録したメールアドレスへのメール着信を通知するメール着信確認機能を搭載しているため、パソコンの電源を入れなくても、メール着信の有無を確認できます。メール着信を確認するだけでなく、着信したメールを携帯電話やPHSの電子メールなどの他のメールアドレスに転送できる、メール着信転送機能も搭載しています。

◆ ブロードバンドTA(ターミナルアダプタ)機能搭載

Windows98SE/Me/2000/XP、Mac OS9のパソコンから、本機をUSB接続のブロードバンドTA(PPPoE方式のみ対応)として使うことができます。常時接続回線契約をしていても、セキュリティ面で心配なときに便利です。

◆ LANポートのないパソコンでも、USBポート経由でアクセス可能

USBポートに接続したパソコンをLANに接続できる擬似LAN機能を搭載しているため、LANボードを装着できないパソコンでも、USB経由でLANへアクセスできます。

◆ 充実のNetVolanteホームページ

NetVolanteシリーズのホームページ(http://NetVolante.jp/)では、NetVolanteシリーズの最新情報や機能の設定方法、FAQ、リビジョンアッププログラムなど、NetVolanteを活用するための情報を満載しています。本機の「かんたん設定ページ」画面左上の[ネットボランチホームページ]をクリックするだけでアクセスできます。

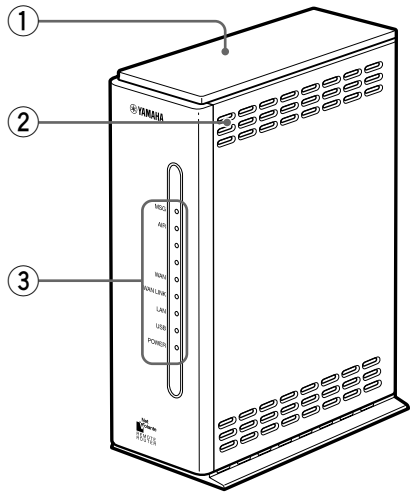
また、ヤマハルータRTシリーズホームページ(http://www.rtpro.yamaha.co.jp/)では、RTシリーズルータを使った高度な活用例や詳しい解説がご覧いただけます。

◆ リビジョンアップによる最新機能の利用

ご購入後に新しい機能が追加されても、本機内蔵ソフトウェアのリビジョンアップ(バージョンアップ)を行うことで、最新の機能が利用できます。リビジョンアップを行うには、NetVolanteシリーズのホームページ(http://NetVolante.jp/)からリビジョンアップ・プログラムをパソコンにダウンロードして、パソコンでこのプログラムを実行するだけです。

各部の名称とはたらき

前面



① 外部アンテナ用カバー
本機に無線LAN用の外部アンテナを取り付けるときに、取りはずします(58ページ)。

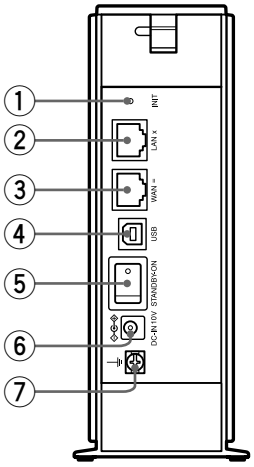
② 通風口
内部の熱を逃がすための穴です。

③ ランプ
本機の動作状態を示します。

- MSG:登録したメールアドレスへメールが着信しているときに、点滅します(23ページ)。
- AIR:無線LANの状態を示します。接続中は点灯、通信中は点滅します。
- WAN:WANポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- WAN LINK:WANポート経由でインターネットに接続しているときに点灯します。
- LAN:LANポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- USB:USBポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- POWER:本機の電源の状態を示します。電源が入っているときは点灯します。

動作状態と点灯動作の関係について詳しくは、別冊の「設定マニュアル」の「本機の動作状態を確認する」(66ページ)をご覧ください。

背面



① INITスイッチ
このスイッチを押しながら本機の電源を入れると、本機の設定を工場出荷状態に戻すことができます(93ページ)。

② LANポート
パソコンのLANポートまたはHUBのポートとLANケーブルで接続します。

③ WANポート
ケーブルモデムやADSLモデムとLANケーブルで接続します。

④ USBポート
本機をコンソールや擬似LAN、ブロードバンドTAとして使う場合に、パソコンのUSBポートとUSBケーブルで接続します。

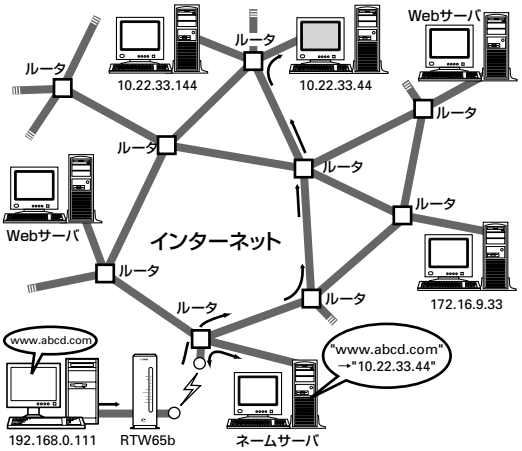
⑤ STANDBY-ON(電源)スイッチ
本機の電源を入／切します。

⑥ DC-IN 10Vコネクタ
付属のACアダプタを接続します。

⑦ アース端子
アースコードを接続します。必ず接続してください。

インターネットは、世界中のさまざまなネットワークを接続したネットワークです。そしてネットワークどうしをつなぐ装置が「ルータ」です。

インターネットでは、世界中のコンピュータから1台のコンピュータを識別するために、「192.168.0.250」のように4つの数字からなる「IPアドレス」という識別番号を使っています。ルータは流れてきたデータをIPアドレスで判断し、送り先を決めています。1つのデータが目的のコンピュータへ届くまでには、数多くのルータを通過していきます。このような通信ルールを「TCP/IP」と呼びます。



例：パソコンでホームページのアドレス（URL）を入力すると

1. プロバイダのネームサーバ（DNS）でURLがIPアドレスに変換されます。
2. そのアドレスのWebサーバまで「ホームページのデータを送れ」という要求（リクエスト）が届けられます。
3. その要求を受けて、Webサーバはホームページや画像データを要求元のパソコンのIPアドレスへ送り返します。

このように、誰から誰へ送れば良いのかはすべてIPアドレスで管理されているので、インターネットに接続するときは必ずIPアドレスが必要になります。

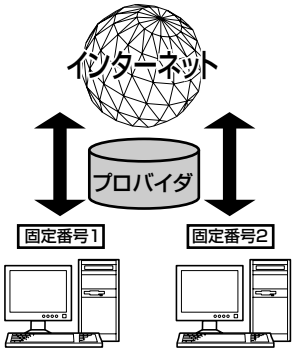
◆ IPアドレスの入手方法は、インターネットへの接続方法によって異なります

フレッツ・ADSLなどのPPPoE方式での接続の場合は

プロバイダに接続するたびに、プロバイダが持っているIPアドレスの中から、そのとき限りのIPアドレスが割り当てられます。このIPアドレスは、接続を切るまで有効です。次に接続したときは、以前接続したときとは異なるIPアドレスが割り当てられます。

CATV／ADSL（PPPoE方式以外）接続の場合は

プロバイダと契約すると、あらかじめ指定されたIPアドレスを、必要な数だけ割り当ててもらえます。割り当てられたIPアドレスを個々のパソコンに設定することで、インターネットへ接続できるようになります。

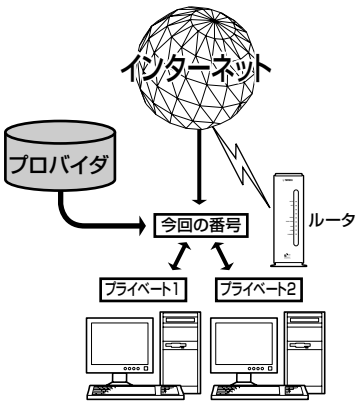


アドレス変換機能を持ったブロードバンドルータで接続する場合は

ルータからLAN内専用のプライベートIPアドレスが各パソコンに割り当てられます。

インターネットに接続するときは、ルータが個々のプライベートIPアドレスをプロバイダから割り当てられたグローバルIPアドレスに変換してインターネットへ送ります。もどってきたデータは、元のプライベートIPアドレスに変換してLAN内のパソコンへ送ります。

この変換機能を「NAT機能」と「IPマスカレード機能」と呼び、この機能によって端末型ダイヤルアップ契約でも複数のパソコンからインターネットが使えるようになっています。



プロバイダと契約すると、必ずIPアドレスの情報が通知されます。重要な情報なので必ず確認し、大切に保管してください。

IPアドレスとは？

IPアドレスは、「192.168.0.250」のような、0～255までの4つの数字からなる識別番号です。インターネットでは、世界中のコンピュータから1台のコンピュータを識別するために、IPアドレスを使っています。IPアドレスには、インターネット上で通用する「グローバルIPアドレス」と、自分のLAN内だけで通用する「プライベートIPアドレス」の2種類があります。

◆ グローバルIPアドレス

グローバルIPアドレスは、インターネットで世界中につながっているコンピュータの中から、1つのコンピュータを特定するためのIPアドレスです。グローバルIPアドレスは重複することができませんので、正式な手続きを経て取得する必要があります。CATV／ADSL（PPPoE方式以外）接続の契約を申し込むと、グローバルIPアドレスが割り当てられます。フレッツ・ADSLなどのPPPoE方式での接続の契約では、接続するたびにプロバイダが取得したグローバルIPアドレスを一時的に借りてインターネットに接続しています。

ご注意

接続業者によっては、プライベートIPアドレスが割り当てられる場合があります。

◆ プライベートIPアドレス

プライベートIPアドレスは、自分のLAN内に限って使用できるIPアドレスです。約43億通りのIPアドレスのうち、以下の範囲のIPアドレスを使用できます。

- 10.0.0.0～10.255.255.255
- 172.16.0.0～172.31.255.255
- 192.168.0.0～192.168.255.255

ヒント

本機の初期設定値は「192.168.0.1」に設定されています。

◆ ネットマスク

ネットワークのIPアドレス範囲を表わす数値を「ネットマスク」といいます。ネットマスクの仕組みは、以下のようになっています。

例：ネットワーク番号192.168.11.0/26を使う場合

192.168.11.0を2進数で表わすと、32桁になります。左からネットマスクの個数分1を並べ、残りに0を並べます。1の範囲がそのネットワークを示す識別番号となり、0の範囲がネットワーク内の各機器を示す識別する番号となります。

- ネットワーク番号
  （10進数表示）：192.168.11.0
  （2進数表示）：
  11000000.10101000.00001011.00000000
- ネットマスク（2進数表示）：
  11111111.11111111.11111111.11000000

IPアドレスの範囲をわかりやすい10進数で表わすと、次のようになります。

- IPアドレスの最初（10進数表示）：192.168.11.0
- IPアドレスの最後（10進数表示）：192.168.11.63

ヒント

- ネットマスクは、「192.168.11.0/26」の他に「26ビット」や「255.255.255.192」と表記されることもあります。
- 本機の初期設定値は「192.168.0.0/24」に設定されています。

◆ IPアドレスのルール

LAN型の契約でプロバイダから割り当てられたグローバルIPアドレスの範囲や、プライベートIPアドレスとして設定した範囲のうち、始めの番号は「ネットワークアドレス」、最後の番号は「ブロードキャストアドレス」に割り当てる決まりになっています。この2つの番号は、パソコンなどに割り当てて使用することはできません。

例：「172.16.128.112/28」のIPアドレスを割り当てられた場合

割り当てられた番号は「172.16.128.112」～ 「172.16.128.127」の16個ですが、以下のように実際にルータやパソコンなどに使える番号は、「172.16.128.113」～「172.16.128.126」の14個となります。このルールは、ご自分のLANにプライベートIPアドレスを設定して使うときにも適用されますので、ご注意ください。

IPアドレス範囲最初→ 172.16.128.112
（**ネットワークアドレス**）

自由に使える範囲
- 172.16.128.113（ルータ）
- 172.16.128.114（サーバA）
- 172.16.128.115（パソコン1）
- 172.16.128.116（サーバB）
- 172.16.128.117（パソコン2）
- 172.16.128.118（パソコン3）
- 172.16.128.119
- ：
- 172.16.128.120
- 172.16.128.121
- 172.16.128.122
- 172.16.128.123
- 172.16.128.124
- 172.16.128.125
- 172.16.128.126

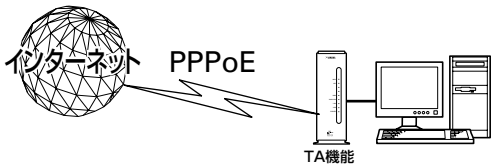
IPアドレス範囲最後→ 172.16.128.127
（**ブロードキャストアドレス**）

ブロードバンドTAとルータの違いは？

CATV／ADSL回線を利用してインターネットへ接続するための機器としてはブロードバンドTAとルータの2種類があり、それぞれ特徴が違います。

◆ ブロードバンドTA(ターミナルアダプタ)の機能

本機のブロードバンドTA機能は、フレッツ·ADSLなどのPPPoE方式の回線を1台のパソコンで占有するための機能です。一般回線のモデムやISDNのTAに相当し、本機とUSBで接続してWindowsやMacOSに標準搭載の接続ソフトを使って、手動でインターネットへ接続します。



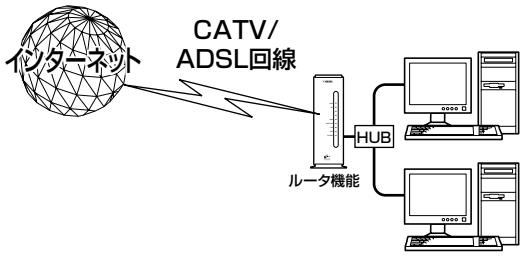
ブロードバンドTAの場合は、パソコン1台につき1つのブロードバンドTAと回線が必要です。また、プロバイダ接続情報をパソコンに設定して使うので、パソコンごとに設定作業が必要になります。

ブロードバンドTAでインターネットへ接続すると、パソコンにプロバイダのグローバルIPアドレスが割り当てられますので、ネットワークゲームやICQなど、グローバルIPアドレスを利用したサービスを利用できます。

◆ ルータの機能

ルータは、LAN内のデータの宛先を監視して、データの流れを制御(ルーティング)する機器です。ブロードバンドルータは、LAN内のデータにインターネット宛てのものを見つけると、ルータが自動的にCATV/ADSL回線へアクセスしてインターネットに接続します。

ルータは1つの回線で接続するため、1つのプロバイダ接続契約でLAN内の複数のパソコンから、同時にインターネットに接続できます。また、プロバイダ接続情報はルータに設定するだけですので、パソコンが何台増えてもルータ以外に管理する必要はありません。



ただし、ルータでは、LAN内のプライベートIPアドレスをグローバルIPアドレスに変換して接続するため、ネットワークゲームやICQなど、グローバルIPアドレスを利用したソフトウェアやサービスを利用できない場合があります。

◆ ルータのNAT機能とは？

インターネット上のコンピュータはすべてグローバルIPを持つ必要があるため、LAN内のプライベートIPアドレスでは、インターネットに接続できません。本機では、内蔵のNAT(Network Address Translator)機能を利用して、プロバイダから割り当てられたグローバルIPアドレスに変換することで、LAN内のパソコンからインターネットへ接続できるようにしています。

IPマスカレード機能

さらに、本機のIPマスカレード機能を利用することで、複数のパソコンのプライベートIPアドレスを1つのグローバルIPアドレスに自動的に変換して、端末型ダイヤルアップ接続でも複数のパソコンからインターネットに接続できるようにしています。

また、LAN型の契約で割り当てられているグローバルIPアドレスの数が足りない場合でも、NAT機能とIPマスカレード機能を使うことで、より多くのパソコンを接続することができるようになります。

第2章 本機の設定を変更する

この章では、本機の機能やいくつかの設定方法について紹介しています。一番操作しやすい方法でお使いください。

利用できる設定方法の種類

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

パソコンのWebブラウザで設定する（16ページ）
本機にパソコンを接続している場合は、Webブラウザで本機内蔵の「かんたん設定ページ」を開いて本機の状態を見たり、各種機能を設定したりすることができます。

ATコマンドで設定する（18ページ）
本機のUSBポートにパソコンを接続している場合は、パソコン通信ソフトを使って、本機のTA機能を設定できます。

コンソールコマンドで設定する（19ページ）
TELNETソフトウェアを使ってコンソール画面からコマンドを入力して、本機の状態を確認したり、各種の機能を設定できます。

Webブラウザで設定する

本機をLAN接続で使っている場合は、Internet ExplorerやNetscape NavigatorなどのWebブラウザを使って本機を設定できます。

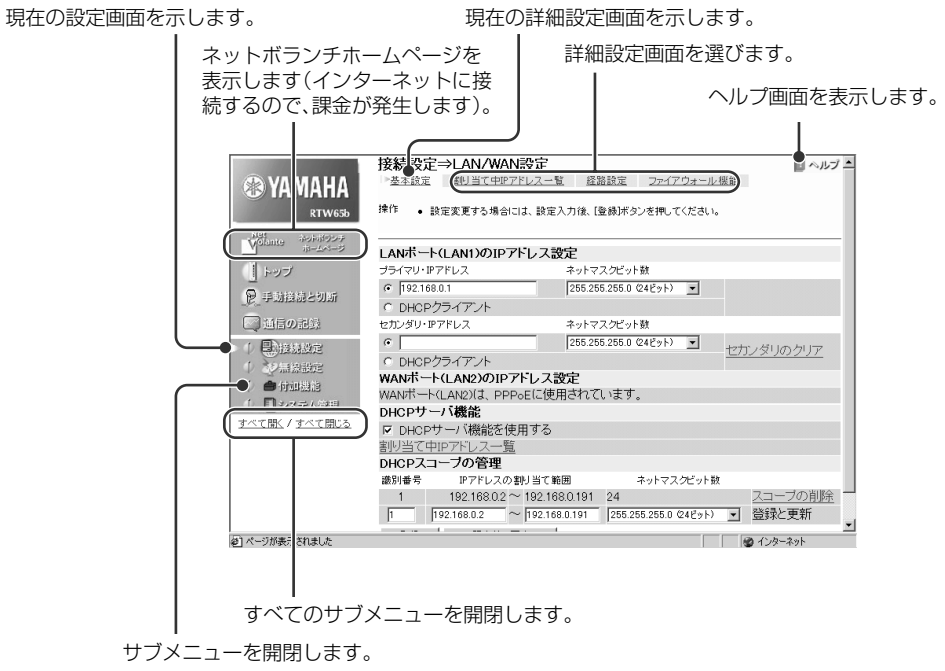
ご注意

- 「かんたん設定ページ」を使用するには、Internet Explorer 4.0以降またはNetscape Navigator 3.0以降(6.0以降を除く)のWebブラウザが必要です。
- 本機をブロードバンドTAとして使っている場合は、Webブラウザで設定することはできません。擬似LAN接続の設定を行ってから、擬似LAN接続で本機に接続してください(44ページ)。

ヒント

- 「かんたん設定ページ」の設定項目については、「Webブラウザ設定ページ項目一覧」(108ページ)をご覧ください。
- 「かんたん設定ページ」各設定に関する詳細情報については、各画面の[ヘルプ]をクリックして表示される「ヘルプ」画面をご覧ください。

かんたん設定ページ画面の見かた



設定のしかた

◆ 通信記録を見る場合の例

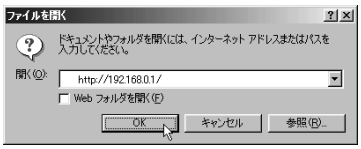
インターネット接続などで通信した記録を調べることができます。

1 パソコンでWebブラウザを起動して、ファイルメニューの[開く]を選ぶ。

「ファイルを開く」画面が表示されます。

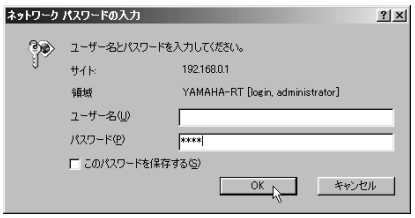
2 「http://setup.netvolante.jp/」と半角英字で入力してから、[OK]をクリックする。

本機のIPアドレス(工場出荷時は192.168.0.1)を半角英数字で入力して開くこともできます。



「ネットワーク パスワードの入力」画面が表示されます。

3 [パスワード]欄にルータの管理パスワードを入力してから、[OK]をクリックする。



4 画面左側の[通信の記録]をクリックする。

メール着信件数、メール転送件数、通信履歴が表示されます。

5 確認が終わったら、画面下の[終了]をクリックする。

◆ ルータのパスワードについて

「かんたん設定ページ」を開くときに入力するルータのパスワードには、「管理パスワード」と「ログインパスワード」の2種類があります。

- **管理パスワードを入力すると:** すべての画面を見ることができ、各画面の設定内容を変更できます。ルータを管理する人だけが使うことをお勧めします。
- **ログインパスワードを入力すると:** 「手動接続と切断」画面と「通信の記録」画面のみを見ることができ、設定ページは表示できません。管理者以外のユーザにはログインパスワードを知らせれば、設定を勝手に変更されることなく、手動切断したり、メール着信を確認してもらうことができます。

ヒント

- 「かんたん設定ページ」を初めて開いたときに設定したパスワードが、「管理パスワード」と「ログインパスワード」の両方に設定されます。どちらかのパスワードを変更したいときは、「システム管理」画面で設定できます。
- ログインパスワードを設定しない場合でも、パスワードを入力せずに「手動接続と切断」と「通信の記録」画面を確認できます。

ATコマンドで設定する

本機のUSBポートにパソコンを接続している場合は、ATコマンドを使って本機のTA機能を設定できます。

ご注意

ATコマンドで設定するには、USB接続の設定が必要です（29ページ）。

ATコマンドとは？

米国Hayes社が開発した、モデムを制御するためのコマンドで、モデムやTAを使用したパソコン通信でよく使われています。本機をTAとして使用してプロバイダにアクセスするための設定を行ったり、プロバイダへ接続したりする場合に使います。

ATコマンドを使用するためには、本機のUSBポートへパソコンを接続し、そのパソコン上でターミナルソフトと呼ばれるアプリケーションを起動して、設定や操作を行います。

ATコマンドに関連した用語として、以下の用語があります。

用語	説明
リザルトコード	ATコマンドを実行した結果、パソコンまたは通信相手から返ってくる返事です。
Sレジスタ	ATコマンドによる設定や実行結果内容などを保存する記憶場所です。Sレジスタには番号があり、番号によって記憶内容や役割があらかじめ決められています。
INFファイル	ターミナルソフトウェアやダイヤルアップソフトウェアが本機の使用を開始する際に参照する、Windows用のファイルです。中身はATコマンドなどで記述されています。
CCLファイル	Macintosh用のモデム記述ファイルです。WindowsのINFファイルに相当します。
モデム初期化コマンド	モデムを使用して通信を始める前に自動的にモデムやTAに実行させるコマンドです。INFファイルやCCLファイルによる設定以外のオプショナル設定コマンドなどを記述します。

設定のしかた

ATコマンドによる設定は、一般的に以下のような流れになります。

ヒント

ATコマンドについて詳しくは、「ATコマンド一覧」（110ページ）をご覧ください。

1 ターミナルソフトを起動する。

ターミナルソフトでは本機が接続されている通信（COM）ポートを指定する必要があります。

MacOSの場合は

［USB Modem］を選びます。

Windowsの場合は

通信（COM）ポート番号は以下の方法で調べることができます。

- **Windows98SE/Meの場合：**［コントロールパネル］－［システム］－［デバイスマネージャ］－［モデム］の［RTW65b USB xxxx］をダブルクリックして、［モデム］タブでCOMポート番号を確認します。
- **Windows2000/XPの場合：**［コントロールパネル］－［システム］の［ハードウェア］タブでデバイスマネージャ］－［モデム］の［YAMAHA RTW65b USB］を開き、［モデム］タブでCOMポート番号を確認します。

ご注意

ターミナルソフトで本機のUSBポートにアクセスしている間は、絶対にUSBケーブルを抜いたり、本機の電源を切らないでください。

2 「AT」と入力してから、Enterキーを押す。

「OK」という文字が表示されるのを確認します。

3 ATコマンド一覧を参照して、「AT&V」コマンドで設定内容を調べてから、必要な設定を行う。

4 設定した内容を本機に保存するには、「AT&W」と入力してからEnterキーを押す。

5 ターミナルソフトを終了する。

ご注意

- 手順4の&Wコマンドを実行しないと、設定した内容が本機の内蔵メモリに保存されません。内蔵メモリに保存しないと、本機の電源を切ると、設定内容が失われます。
- ATコマンドに関する設定の保存と、ルータ機能に関する設定の保存は同じ内蔵メモリに対して行われます。ただし、ATコマンドで設定を保存すると、ATコマンドに関する設定だけが内蔵メモリに保存されますので、ご注意ください。

◆ ATコマンド使用上のご注意

ATコマンドを使用するときは、以下の点にご注意ください。

- **入力文字**:半角のASCII文字だけを使用できます。
- **先頭文字**:「AT」または「at」のみ使用できます。「At」や「aT」というように、大文字と小文字を混在することはできません。
- **繰り返し**:「A/」または「a/」を入力すると、直前のコマンドを繰り返して実行できます。
- **連続実行**:複数のコマンドを1回で入力できます。
  例:「AT&D0」と「AT$M1」というコマンドをまとめて、「AT&D0$M1」と入力できます。

コンソールコマンドで設定する

本機に直接コマンドを送って、機能を設定できます。コンソールコマンドはTELNETソフトウェアから入力しますので、お使いの環境用のTELNETソフトウェアをご用意ください。

コンソールコマンドとは?

コンソールコマンドは、ルータに直接命令を送って、機能を設定する方法です。コンソールコマンドを使うと、他の方法よりも、より詳しい設定が行えます。コンソールコマンドの詳細については、コマンドリファレンスをご覧ください。

ヒント

本機のUSBポートに接続したパソコンからターミナルソフトを使って、本機をコンソールコマンドで設定することもできます。

設定のしかた

LANポートに接続しているパソコンからTELNETソフトウェアで本機にログインし、コンソールコマンドを送信して設定します。ここでは、Windows標準のTELNETを使用する場合を例に説明します。Macintoshではフリーウェアなどをお使いください(MacOS Xでは、MacOS Xに付属のTerminalソフトウェアを使用できます)。

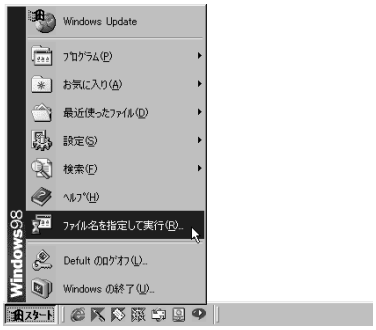
ご注意

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

ヒント

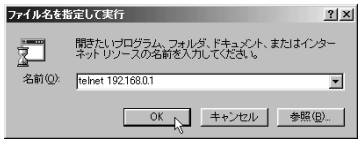
コンソールコマンドの詳細については、コマンドリファレンスをご覧ください。

1 **[スタート]メニューから[ファイル名を指定して実行]を選ぶ。**



2 「telnet 192.168.0.1」と入力してから、［OK］をクリックする。

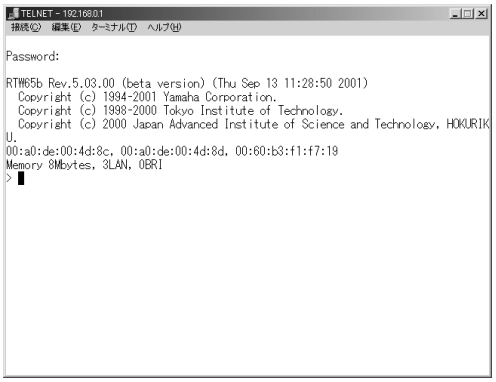
本機のIPアドレスを変更している場合には、「192.168.0.1」のかわりに本機のIPアドレスを入力します。



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

何も表示されないときは、1度Enterキーを押します。

「>」が表示されると、コンソールコマンドを入力できるようになります。



ヒント

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

4 「administrator」と入力してから、Enterキーを押す。

5 「Password:」と表示されたら、管理パスワードを入力する。

「#」が表示されると、各種のコンソールコマンドを入力できます。

6 コンソールコマンドを入力して、設定を行う。

コンソールコマンドについて詳しくは、付属のコマンドリファレンス(PDFファイル)をご覧ください。

7 設定が終わったら、「save」と入力してからEnterキーを押す。

コンソールコマンドで設定した内容が、本機のメモリに保存されます。

8 設定を終了するには、「quit」と入力してからEnterキーを押す。

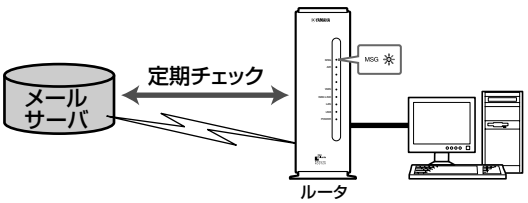
9 コンソール画面を終了するには、もう1度「quit」と入力してからEnterキーを押す。

第 3 章
メール確認／通知機能を使う

この章では、メール着信確認機能の設定方法や使いかた、メールで本機の各種情報を受け取る方法について紹介しています。よくお読みいただき、本機のメール機能を十分活用してください。

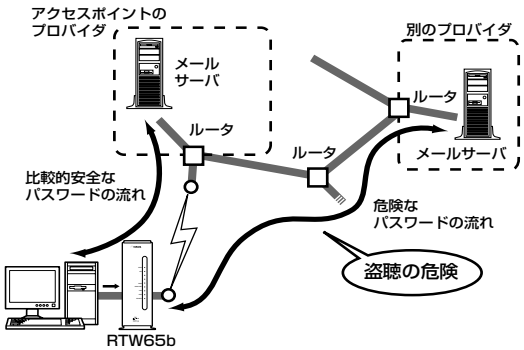
メール着信確認機能とは？

メール着信確認機能は、新しい電子メールが届いているかどうか、本機がプロバイダのメールサーバを定期的に確認する機能です。メールが届いていると、本機前面のMSGランプが点滅するため、パソコンの電源を入れなくてもメール着信の有無を確認でき、便利です。メールアドレスは、4つまで登録できます。



ご注意

- 現在接続中のプロバイダ以外のメールサーバに対してこのコマンドを実行すると、パスワード情報などが暗号化されずにインターネット上に流れてしまいますので、十分ご注意ください。



- 電子メールソフトウェアでメールサーバにメールを残すように設定している場合は、メールを確認するたびに新着メールが着信していることになります。新着メールがあるかどうかを正確に確認したい場合は、受信済みメールをサーバに残さないように電子メールソフトウェアの設定を変更してください。

確認したいメールアドレスを登録する

「かんたん設定ページ」の「メール機能」画面で、確認したいメールアドレスを登録します。メールアドレスは、4つまで登録できます。

1 Webブラウザを起動して、本機の「かんたん設定ページ」を開く。

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

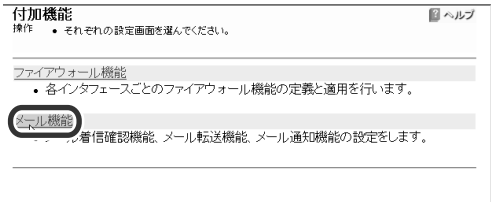
「ネットワーク パスワードの入力」画面が表示されます。

2 [パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。

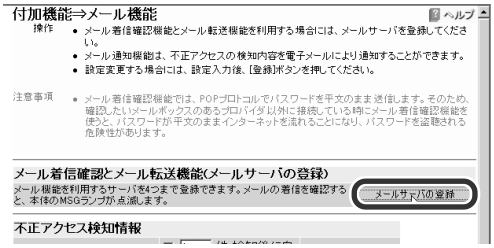
「トップ」画面が表示されます。

3 [付加機能]をクリックする。

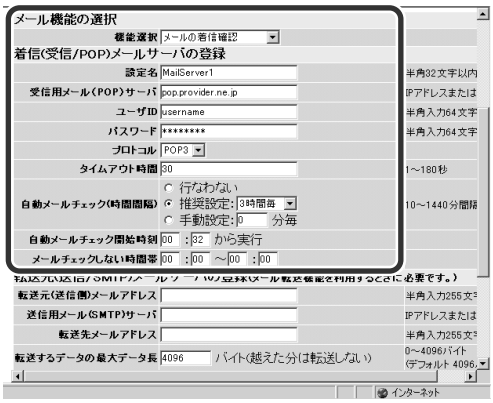
4 [メール機能]をクリックする。



5 [メールサーバの登録]をクリックする。



6 確認するメールアカウントの各項目を設定する。



機能選択　[メールの着信確認]を選びます。

設定名　メールアカウントの名前を半角英数字32文字以内で入力します。

受信用メール(POP)サーバ
確認するメールの受信サーバ名を入力します。

ユーザID　メール受信用のアカウント名を入力します。メールアドレスとは異なる場合がありますので、プロバイダの書類を確認してください。

パスワード　メール受信用のパスワードを入力します。接続用パスワードとは異なる場合がありますので、プロバイダの書類を確認してください。

タイムアウト時間
メールサーバの応答を待つ時間を設定します。この時間以内に応答がないと、エラーを表示します。

プロトコル

- **POP3**：通常はこちらを選びます。
- **APOP**：認証を行う際に暗号を使用するメール受信手順です。プロバイダのメールサーバが対応している場合は、こちらを選びます。

自動メールチェック
メールを定期的にチェックする間隔を設定します。

- **行わない**：毎回手動で行いたい場合に選びます。
- **推奨設定**：3、6、12、24時間の中から選びます。
- **手動設定**：分単位で設定できます。時間は10～1440分（24時間）の間で設定してください。

自動メールチェック開始時刻
メールの確認を始める時間を設定します。

メールチェックしない時間帯
メールを確認しない時間帯を設定します。

7 **[登録]をクリックする。**

メッセージに従ってボタンをクリックすると、設定が登録されて「メール機能」画面に戻ります。

ご注意

接続先プロバイダは、「プロバイダ接続管理」画面で設定したプロバイダになります。

メールの着信を確認する

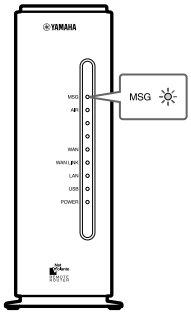
メールが届いていると、本機前面のMSGランプが点滅します。Webブラウザから手動で確認することもできます。

ご注意

電子メールソフトウェアでメールサーバにメールを残すように設定している場合は、メールを確認するたびに新着メールが着信していることになります。新着メールがあるかどうかを正確に確認したい場合は、受信済みメールをサーバに残さないように電子メールソフトウェアの設定を変更してください。

◆ 定期的に確認する

指定された時刻に本機がメールサーバをチェックし、メールが着信していると、MSGランプが点滅します。



MSGランプの点滅は次の状態を表しています。

- 「ピカッ」(1回点滅):メールサーバ1にメール着信あり
- 「ピカッピカッ」(2回点滅):メールサーバ2にメール着信あり
- 「ピカッピカッピカッ」(3回点滅):メールサーバ3または4にメール着信あり

◆ 手動で確認する

メール着信の確認は、「かんたん設定ページ」の「付加機能」画面で行います。

1 **22ページの手順1～4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

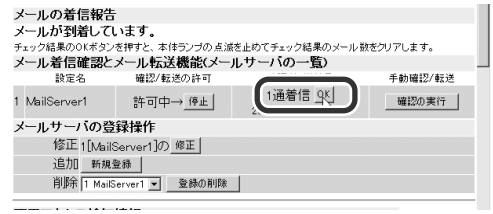
2 **登録したメールサーバの名称に対応する「手動確認/転送」欄の、[確認の実行]をクリックする。**

メールサーバに新規メールが届いているかどうか確認されます。確認した結果は、[確認/転送結果]欄に表示されます。

ご注意

現在接続中のプロバイダ以外のメールサーバに対してこのコマンドを実行すると、パスワード情報などが暗号化されずにインターネット上に流れてしまいますので、十分ご注意ください。

3 **確認が終わったら、「確認/転送結果」欄の[OK]をクリックする。**



対応したサーバ番号に対応するMSGランプ点滅パターンが停止します。

着信したメールを自動転送する

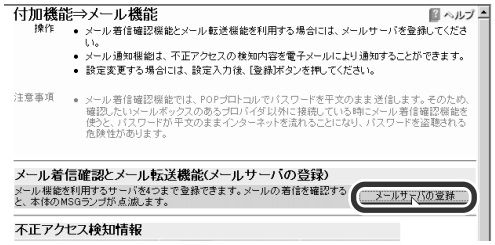
メール着信転送は、着信したメールを登録したメールアドレスへ転送する機能です。転送文字数を設定したり、送信元や題名などの、さまざまな転送条件を設定することもできます。

着信したメールを自動転送するには、「かんたん設定ページ」の「メール機能」画面で設定します。インターネットメールをサポートする機器(携帯電話、PHS、電話機を含む)であれば、どの機器／アドレスにも転送できます。

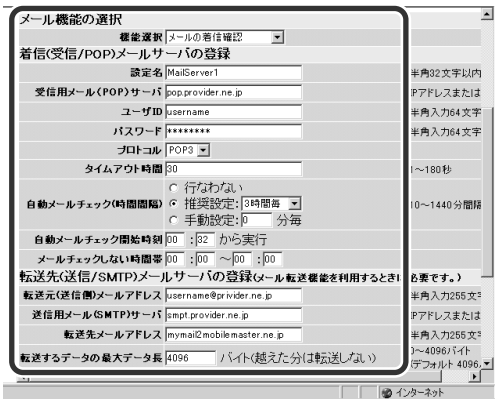
1 **22ページの手順1～4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

2 **[メールサーバの登録]をクリックする。**

すでに登録してあるメールサーバの場合は、そのメールサーバの[登録の修正]をクリックします。



3 **着信確認するメールアドレス情報と、転送先のメールアドレス情報を入力する。**



機能選択　[メールの着信確認と転送]を選びます。

転送元(送信側)メールアドレス
通常は受信メールアドレスと同じものを入力します。

送信用メール(SMTP)サーバ
送信サーバ名を入力します。転送元メールアドレスで利用可能な送信サーバを入力してください。

転送先メールアドレス
転送先のメールアドレスを入力します。

転送するデータの最大データ長
転送するデータの大きさを設定します。データの先頭から指定された長さまでのデータのみが転送されます。

転送条件　転送するメール内容の条件を設定します。条件は4つまで設定できます。

- **以下のすべての条件が満たされたとき:**すべての条件を満たしたメールのみ転送されます。
- **以下のどれかひとつの条件が満たされたとき:**4つの条件のいずれかに該当したメールが転送されます。

4 **[登録]をクリックする。**

メッセージに従ってボタンを押すと、設定が登録されて「メール機能」画面に戻ります。

ご注意

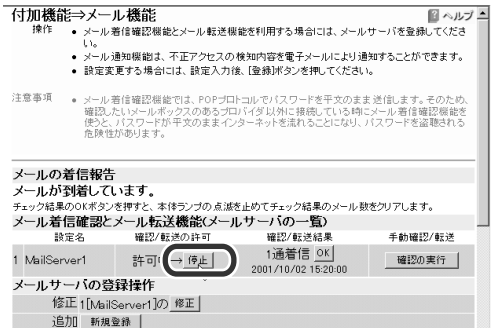
受信メール容量が最大長(工場出荷値は10240byte)を超えている場合、メールは転送されません。受信メールの最大長は、コンソールコマンドの「mail-transfer receive maxlength」で変更できます。詳しくはコマンドリファレンスをご覧ください。

メールの確認や転送を中止する

メール着信確認／転送を一時的に停止したり、再開したりしたい場合は、「かんたん設定ページ」の「メール機能」画面で設定します。

1 **22ページの手順1〜4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

2 **停止したいメールサーバの[確認/転送の許可]の[停止]をクリックする。**



メール確認や転送が中止されます。
再開したいときは、[再開]をクリックします。

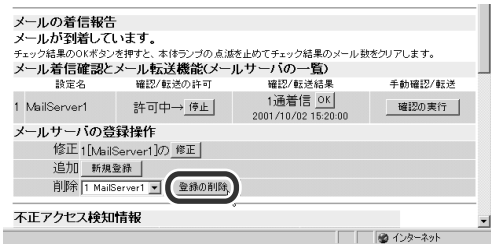
3 **他のメールサーバのメールも中止したいときは、手順2の操作を繰り返す。**

メールサーバ登録を削除する

メール確認／転送で不要になったメールサーバの登録を削除するには、「かんたん設定ページ」の「メール機能」画面で設定します。

1 **22ページの手順1〜4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

2 **［メールサーバの登録操作］で削除したいメールサーバを選んでから、［登録の削除］をクリックする。**



メールサーバの登録内容が削除されます。

3 **他のメールサーバの登録も削除したいときは、手順2の操作を繰り返す。**

不正アクセス検知をメールで通知する

本機のファイアウォール機能（60ページ）で検知した不正アクセス記録を、指定したメールアドレスへ定期的に送信できます。

「かんたん設定ページ」の「メール機能」画面で、送信先と送信する日時を設定します。

1 **22ページの手順1〜4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

2 **「不正アクセス検知情報」の［自動通知する］にチェックを付けてから、通知の送付先メールアドレス、題名、通知間隔などを入力する。**

検知回数設定

チェックを付けて、不正アクセスを何件検知するごとにメールを送るかを指定します。

設定名　通知機能の名称を任意の半角英数字32文字以内で入力します。

送信用メールサーバ（SMTP）

送信サーバ名を入力します。送信元メールアドレスで利用可能な送信サーバを入力してください。

通知元メールアドレス（From）、通知先メールアドレス（To）

それぞれ送信元、通知先のメールアドレスを入力します。

通知メールの題名（Subject）

通知の題名を入力します。

送信するデータの最大データ長

通知するデータの大きさを設定します。データの先頭から指定された長さまでのデータのみが送信されます。

タイムアウト時間

メールサーバの応答を待つ時間を設定します。この時間以内に応答がないと、エラーを表示します。

自動通知　通知を定期的に送信する間隔を設定します。

自動通知時刻

通知を送信する時刻を設定します。

ご注意

接続先プロバイダは、「プロバイダ接続管理」画面で設定したプロバイダになります。

第 4 章
USB 接続機能を活用する

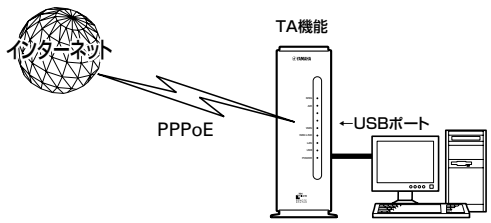
この章では、USB接続で本機のブロードバンドTA機能や擬似LAN機能を使う場合の接続／設定方法について説明しています。利用する機能やOSに合わせて、接続およびパソコンの設定を行ってください。

USBポートでネットワークに接続する

◆ 本機をブロードバンドTAとして使い、ネットワークに接続する（35ページ）

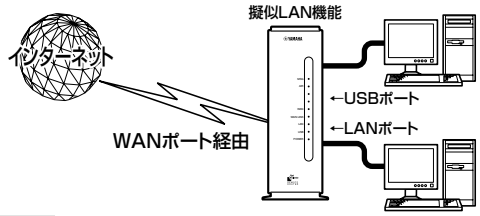
PPPoE方式のブロードバンド回線でWindows98SE（Second Edition）/Me/2000/XP、MacOS9以降のパソコンをお使いの場合、パソコンを本機のUSBポートに接続して、本機をPPPoEを利用したブロードバンドTAとして使うことができます。

ネットワークゲームやICQがうまく動作しないときは、ブロードバンドTAとしてお使いください。



◆ 擬似LAN機能でネットワークに接続する（44ページ）

本機のUSBポートには擬似LAN機能があり、LANポートのないパソコンでも、TCP/IPプロトコルでLANに接続できます。ただし、アクセスできるのはTCP/IPプロトコルに対応したファイルサーバやWebサーバです。AppleShareなどのファイル共有は利用できません。



ご注意

- ブロードバンドTA接続はPPPoE方式の回線でのみ使用できます。
- 工場出荷状態では、ブロードバンドTA接続を行うと、現在使用中のルータ接続はいったん切断されます。
- USBケーブルを抜く前に、必ずパソコンの電源を切ってください。電源を入れたままUSBケーブルの抜き差しすると、パソコンの動作が不安定になる場合があります。
- USBによる通信を行った後にWindowsを終了する場合、終了するまでに5分以上かかることがあります。この問題を回避するには、終了する前にいったん再起動してから終了するようにしてください。
- Windows 95/98/NTやMacOS8.6以前のパソコンをお使いの場合、USB経由で本機とパソコンを接続することはできません。
- ブロードバンドTA接続の場合は、本機の「かんたん設定ページ」を開くことはできません。「かんたん設定ページ」を使いたい場合は、擬似LAN接続でLANに接続してください（44ページ）。

USBポート経由の接続を準備する

USBポートを使用する前に、あらかじめ別冊の「はじめにお読みください」の説明にしたがって、本機の設置から回線の接続までの準備を行う必要があります。

ルータや回線の準備が終わったら、以下の手順でパソコンにUSBドライバやモデムをインストールします。インストール方法は、お使いの環境によって異なります。

インストールには、OSのインストールCD-ROMが必要になる場合があります。あらかじめご用意ください。

ご注意

Windowsの場合、ドライバのインストールが正常に行えなかった時は、付属のCD-ROMの[USB]フォルダー[UnUSB]フォルダー[UnUSBTA.exe]を使用して、いったんドライバをアンインストールしてから、もう1度ドライバをインストールしてください。

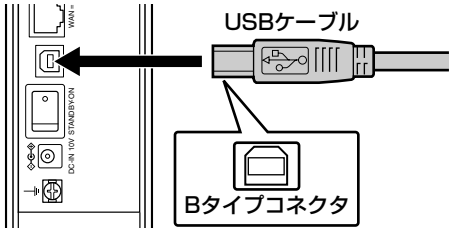
Windows 98SEの場合

Windows 98SEの場合は、USBドライバとモデムのインストールを行います。

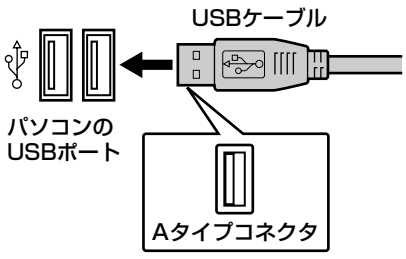
1 **本機とパソコンの電源を入れる。**

2 **パソコンが起動したら、本機に付属のCD-ROMをCD-ROMドライブにセットする。**

3 **本機のUSBポートに、USBケーブルのBタイプ側(四角いコネクタ)を接続する。**



4 **パソコンのUSBポートにUSBケーブルのAタイプ側(平たいコネクタ)を接続する。**



パソコンの画面に、「新しいハードウェアの追加ウィザード」が表示されます。

5 **[次へ]をクリックする。**

6 **[使用中のデバイスに最適なドライバを検索する]を選んでから、[次へ]をクリックする。**

7 **[検索場所の指定]を選んでから[参照]をクリックして、CD-ROMドライブの[USB]フォルダ内にある[WIN9X]フォルダを選び、[OK]をクリックする。**

[検索場所の指定]欄に「D:\USB\WIN9X」と表示されます。CD-ROMドライブ名はお使いのパソコンによって異なります。

8 **[次へ]をクリックする。**

8 ドライバの名称を確認してから、[次へ]をクリックする。

9 表示されたドライバのある場所を確認してから、[次へ]をクリックする。

「D:¥USB¥WIN9X¥YMHUSBTA.INF」になっていない場合は[戻る]をクリックして、選択し直してください。

USBドライバのインストールが始まります。
コピーの途中で「Windows98 Second Edition CD-ROMラベルの付いたディスクを挿入してください」と表示された場合は、Windows98 Second Edition CD-ROMをドライブにセットしてから、[OK]をクリックしてください。

10 USBドライバのコピーが終了したら、[完了]をクリックする。

これで、USBドライバのインストールが完了しました。

続いて新しいハードウェアが検知されて、モデムのインストールが始まります。
手順9でWindows98 Second Edition CD-ROMを入れた場合は、本機に付属のCD-ROMをドライブにセットしてください。

11 [次へ]をクリックする。

12 [使用中のデバイスに最適なドライバを検索する]を選んでから、[次へ]をクリックする。

13 [検索場所の指定]を選んでから[参照]をクリックし、CD-ROMドライブの[USB]フォルダ内の[WIN9X]フォルダを指定して[OK]をクリックする。

[検索場所の指定]に「D:¥USB¥WIN9X」と表示されます。CD-ROMドライブ名はお使いのパソコンによって異なります。

14 [RTW65b USB(Sync)]と表示されていることを確認してから、[次へ]をクリックする。

15 表示されたドライバのある場所を確認してから、[次へ]をクリックする。

「D:¥USB¥WIN9X¥RTW65.INF」になっていない場合は[戻る]をクリックして、選び直してください。

モデムのインストールが始まります。

16 インストールが終了したら、[完了]をクリックする。

これで、モデムのセットアップが完了しました。

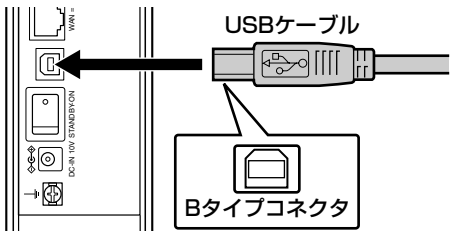
Windows Meの場合

Windows Meの場合は、USBドライバとモデムのインストールを行います。付属のCD-ROMをセットすると、本機用のドライバが自動検索されてインストールされます。

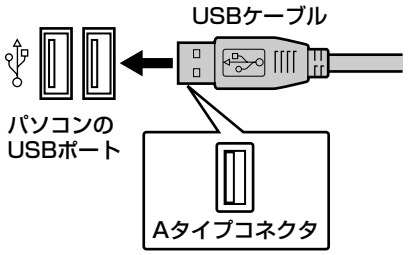
1 本機とパソコンの電源を入れる。

2 パソコンが起動したら、本機に付属のCD-ROMをCD-ROMドライブにセットする。

3 本機のUSBポートにUSBケーブルのBタイプ側(四角いコネクタ)を接続する。



4 パソコンのUSBポートにUSBケーブルのAタイプ側(平たいコネクタ)を接続する。



パソコンの画面に、「新しいハードウェアの追加ウィザード」が表示されます。

5 [適切なドライバを自動的に検索する]を選んでから、[次へ]をクリックする。

6 USBドライバのコピーが終了したら、[完了]をクリックする。

これで、USBドライバのインストールが完了しました。
続いて新しいハードウェアが検出されて、モデムのインストールが始まります。

7 [適切なドライバを自動的に検索する]を選んでから、[次へ]をクリックする。

モデムのインストールが始まります。

8 インストールが終了したら、[完了]をクリックする。

これで、モデムのセットアップが完了しました。

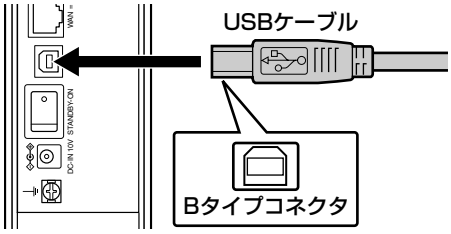
Windows 2000の場合

Windows 2000の場合は、ウィザードに従ってUSBモデムのインストールを行います。

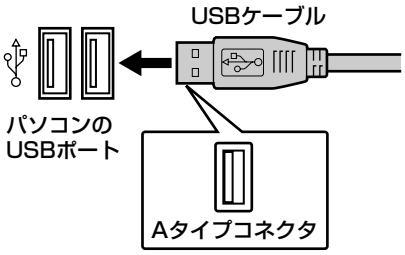
1 本機とパソコンの電源を入れる。

2 パソコンが起動したら、本機に付属のCD-ROMをCD-ROMドライブにセットする。

3 本機のUSBポートにUSBケーブルのBタイプ側(四角いコネクタ)を接続する。

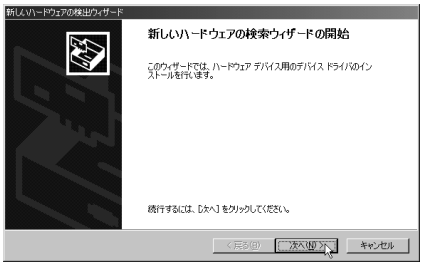


4 パソコンのUSBポートにUSBケーブルのAタイプ側(平たいコネクタ)を接続する。



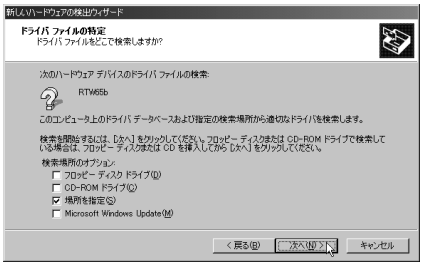
パソコンの画面に、「新しいハードウェアの検出ウィザード」が表示されます。

5 [次へ]をクリックする。

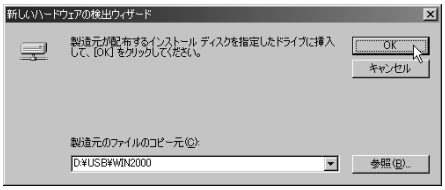


6 **[デバイスに最適なドライバを検索する]を選んでから、[次へ]をクリックする。**

7 **[場所を指定]を選んでから、[次へ]をクリックする。**



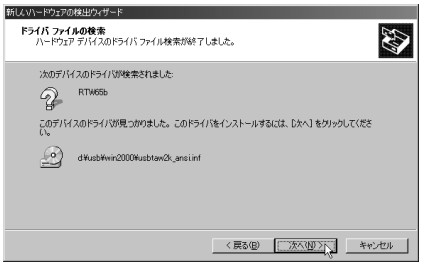
8 **[参照]をクリックしてCD-ROMドライブの[USB]フォルダ内にある[WIN2000]フォルダを選んでから、[OK]をクリックする。**



「製造元のファイルのコピー元」欄に「D:¥USB¥WIN2000」と表示されます。CD-ROMドライブ名はお使いのパソコンによって異なります。

9 **表示されたドライバのある場所を確認してから、[次へ]をクリックする。**

「D:¥USB¥WIN2000¥USBTAW2K.INF」になっていない場合は[戻る]をクリックして、選び直してください。

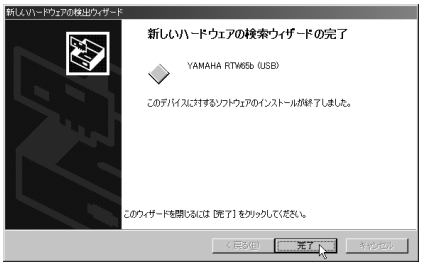


USBドライバのインストールが始まります。

「デジタル署名が見つかりませんでした」というメッセージが表示された場合は

[はい]をクリックしてインストールを続行してください。

10 **USBドライバのコピーが終了したら、[完了]をクリックする。**



これで、USBモデムのセットアップが完了しました。

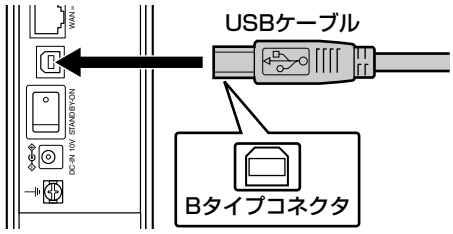
Windows XPの場合

Windows XPの場合は、ウィザードに従ってUSBモデムのインストールを行います。

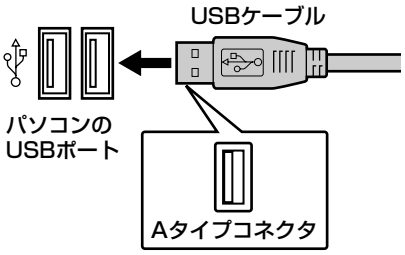
1 **本機とパソコンの電源を入れる。**

2 **パソコンが起動したら、本機に付属のCD-ROMをCD-ROMドライブにセットする。**

3 **本機のUSBポートにUSBケーブルのBタイプ側(四角いコネクタ)を接続する。**

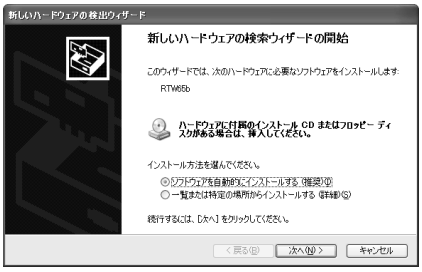


4 **パソコンのUSBポートにUSBケーブルのAタイプ側(平たいコネクタ)を接続する。**



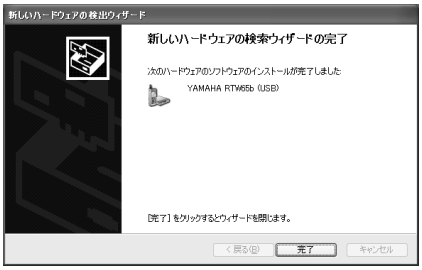
パソコンの画面に、「新しいハードウェアの検出ウィザード」が表示されます。

5 **[ソフトウェアを自動的にインストールする]を選んでから、[次へ]をクリックする。**



USBドライバのインストールが始まります。

6 **USBドライバのコピーが終了したら、[完了]をクリックする。**



これで、USBモデムのセットアップが完了しました。

ヒント

手順5で[ソフトウェアを自動的にインストールする]の代わりに[一覧または特定の場所からインストールする]を選んでインストールする場合は、Windows2000の場合の手順7以降(33ページ)の操作を行ってください。

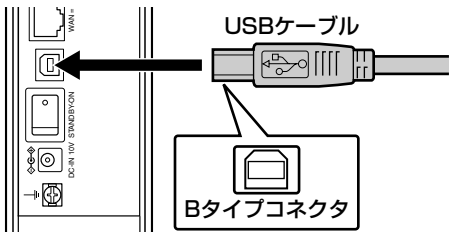
MacOS 9の場合

MacOS 9の場合は、USBケーブルの接続とCCLファイルのインストールを行います。

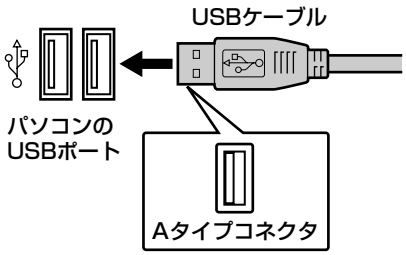
◆ USBケーブルを接続する

1 **本機とパソコンの電源を入れる。**

2 **本機のUSBポートにUSBケーブルのBタイプ側(四角いコネクタ)を接続する。**



3 **パソコンのUSBポートにUSBケーブルのAタイプ側(平たいコネクタ)を接続する。**



これで、USBのセットアップが完了しました。

◆ CCLファイルをインストールする

1 **付属のCD-ROMをCD-ROMドライブにセットする。**

2 **CD-ROMの[CCLファイル]フォルダ内のCCLファイルを、起動ハードディスクの[システムフォルダ]－[機能拡張]－[Modem Scripts]フォルダにコピーする。**

これで、CCLファイルのインストールが完了しました。

USBポートからブロードバンドTA接続する

本機をPPPoE方式ブロードバンドTAとして使う場合は、以下の接続や設定を行ってください。ブロードバンドTA接続は、PPPoE方式の接続でのみ使用できます。

ご注意

- 工場出荷状態では、ブロードバンドTA接続を行うと、現在使用中のルータ接続はいったん切断されます。
- ブロードバンドTA接続中に、本機の設定を保存しないでください。

Windows 98SE/Meの場合

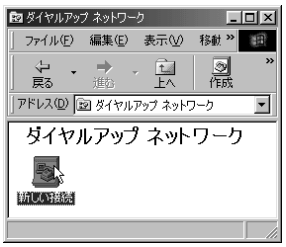
ブロードバンドTA接続するときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

1 **[マイコンピュータ]の[ダイヤルアップ ネットワーク]をダブルクリックする。**

Windows Meの場合は、[コントロールパネル]の[ダイヤルアップ ネットワーク]をダブルクリックします。

2 **[新しい接続]アイコンをダブルクリックする。**

「ダイヤルアップネットワークへようこそ」画面が表示された場合は、[次へ]をクリックします。「所在地情報」画面が表示された場合は、市外局番を入力してください。



3 **[接続名]に「RTW65b-TA」と入力し、[モデムの選択]に[RTW65b USB (Sync)]を選んでから、[次へ]をクリックする。**

4 市外局番は空欄のまま、電話番号に半角英数字で「***#」と入力してから、国番号に[日本(81)]を選んで[次へ]をクリックし、[完了]をクリックする。

「ダイヤルアップ ネットワーク」フォルダ内に、登録したプロバイダ名のアイコンが表示されます。

5 [RTW65b-TA]アイコンを選んでから、[ファイル]メニューから[プロパティ]を選ぶ。

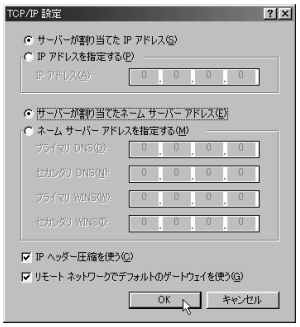
6 [サーバーの種類]タブをクリックする。

Windows Meの場合は、[ネットワーク]タブをクリックします。

7 以下のように設定してから、[TCP/IP設定]をクリックする。

- [詳細オプション]の[ソフトウェア圧縮する]:チェックを外す。
- [使用できるネットワーク　プロトコル]の[NetBEUI]、[IPX/SPX互換]:チェックを外す。
- [TCP/IP]:チェックを付ける。

8 [サーバーが割り当てたネームサーバーアドレス]を選んでから、各ウィンドウの[OK]をクリックしてウィンドウを閉じる。



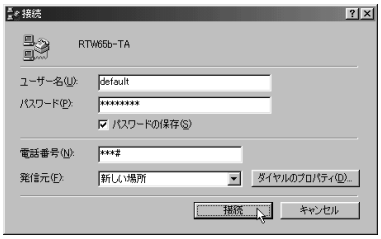
これで、ブロードバンドTA接続の設定が完了しました。

◆ インターネットへ接続する

インターネットへ接続するときは、[RTW65b-TA]アイコンをダブルクリックして、本機のブロードバンドTA機能にダイヤルアップします。

1 **[ダイヤルアップネットワーク]フォルダ内の[RTW65b-TA]アイコンをダブルクリックする。**

2 **プロバイダから入手したユーザー名とパスワードを入力し、[パスワードの保存]をチェックして[接続]をクリックする。**



インターネットに接続すると、接続速度や時間が表示されます。接続中は、WAN LINKランプが点灯します。

ヒント

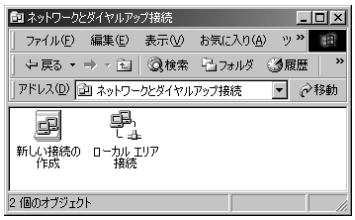
[パスワードの保存]をチェックすると、次回からパスワードの入力が不要になります。ただし、他の人に使われたくないときは、チェックしないでください。

Windows 2000の場合

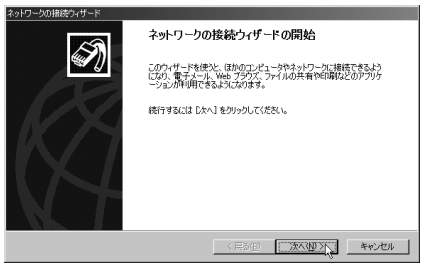
ブロードバンドTA接続するときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

1 **[コントロールパネル]の[ネットワークとダイヤルアップ接続]をダブルクリックする。**

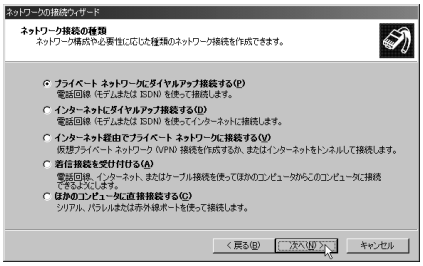
2 **[新しい接続の作成]アイコンをダブルクリックする。**



3 **[次へ]をクリックする。**



4 [プライベートネットワークにダイヤルアップ接続する]を選んでから、[次へ]をクリックする。



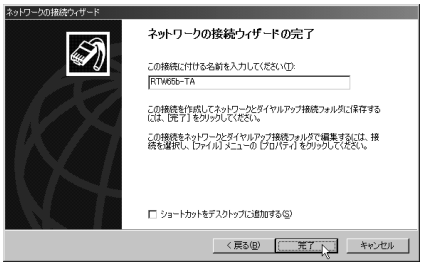
ご注意

「デバイスの選択」画面が表示された場合は、[YAMAHA RTW65b(USB)(COMx)]のみをチェックし、他のデバイスのチェックを外してから[次へ]をクリックします。

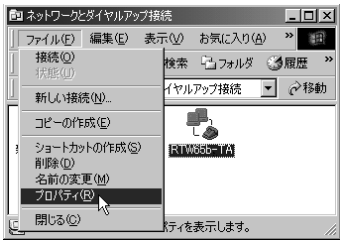
5 電話番号に半角英数字で「***#」と入力してから、[次へ]をクリックする。

6 [すべてのユーザー]を選んでから、[次へ]をクリックする。

7 [接続名]に「RTW65b-TA」と入力してから、[完了]をクリックする。



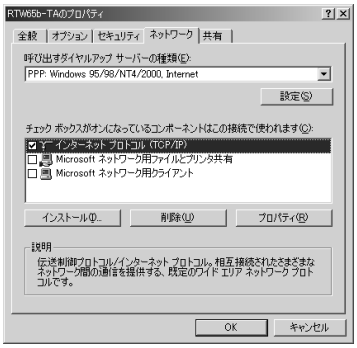
8 [RTW65b-TA]アイコンをクリックして選んでから、[ファイル]メニューから[プロパティ]を選ぶ。



9 [全般]タブをクリックして、[接続の方法]から[YAMAHA RTW65b(USB)(COMX)]を選ぶ。

10 **[ネットワーク]タブをクリックして、以下のように設定してから、[OK]をクリックする。**

- [インターネットプロトコル(TCP/IP)]:チェックを付ける。
- [Microsoftネットワーク用ファイルとプリンタ共有]:チェックを外す。
- [Microsoftネットワーク用クライアント]:チェックを外す。



◆ インターネットへ接続する

インターネットへ接続するときは、[RTW65b-TA]アイコンをダブルクリックして、本機のブロードバンドTA機能にダイヤルアップします。

1 **[ダイヤルアップネットワーク]フォルダ内の[RTW65b-TA]アイコンをダブルクリックする。**

2 **プロバイダから入手したユーザー名とパスワードを入力し、[パスワードの保存]をチェックして[ダイヤル]をクリックする。**

インターネットに接続すると、接続速度や時間が表示されます。接続中は、WAN LINKランプが点灯します。

ヒント

[パスワードの保存]をチェックすると、次回からパスワードの入力が不要になります。ただし、他の人に使われたくないときは、チェックしないでください。

Windows XPの場合

ブロードバンドTA接続するときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

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

2 [ネットワーク接続]をクリックする。

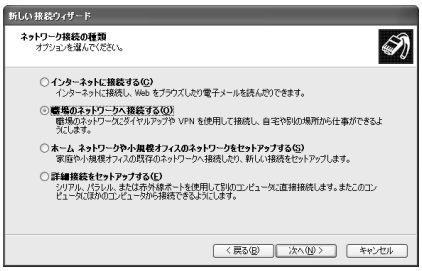
3 [新しい接続を作成する]をクリックする。

「新しい接続ウィザードの開始」画面が表示されます。

「所在地情報」画面が表示された場合は、市外局番を入力してから、[OK]をクリックしてください。

4 [次へ]をクリックする。

5 [職場のネットワークに接続する]を選んでから、[次へ]をクリックする。

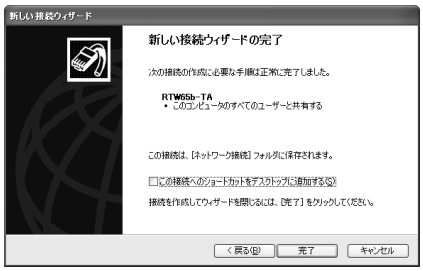


6 [ダイヤルアップ接続]を選んでから、[次へ]をクリックする。

7 [会社名]に「RTW65b-TA」と入力してから、[次へ]をクリックする。

8 電話番号に半角英数字で「***#」と入力してから、[次へ]をクリックする。

9 [完了]をクリックする。



10 [RTW65b-TA]アイコンを選んでから、[この接続の設定を変更する]をクリックする。

11 [全般]タブをクリックして、[接続の方法]から[YAMAHA RTW65b(USB)(COMX)]を選ぶ。

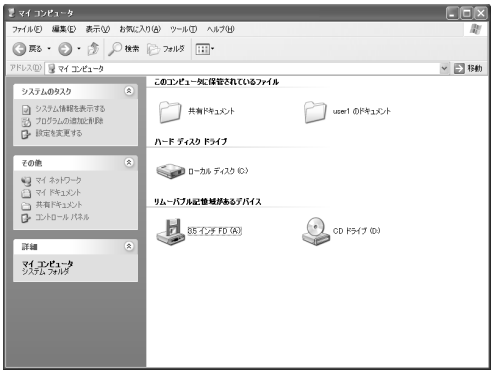
12 [ネットワーク]タブをクリックして、以下のように設定してから、[OK]をクリックする。

- [インターネットプロトコル(TCP/IP)]:チェックを付ける。
- [Microsoftネットワーク用ファイルとプリンタ共有]:チェックを外す。
- [Microsoftネットワーク用クライアント]:チェックを外す。

◆ インターネットへ接続する

インターネットへ接続するときは、[RTW65b-TA]アイコンをダブルクリックして、本機のブロードバンドTA機能にダイヤルアップします。

1 「マイ コンピュータ」画面の[マイ ネットワーク]をクリックする。



2 [ネットワーク接続を表示する]をクリックする。

3 [RTW65b-TA]アイコンを選んでから、[この接続を開始する]をクリックする。

4 プロバイダから入手したユーザー名とパスワードを入力し、[パスワードの保存]をチェックして[ダイヤル]をクリックする。

インターネットに接続すると、接続速度や時間が表示されます。接続中は、WAN LINKランプが点灯します。

ヒント

[パスワードの保存]をチェックすると、次回からパスワードの入力が不要になります。ただし、他の人に使われたくないときは、チェックしないでください。

MacOS 9の場合

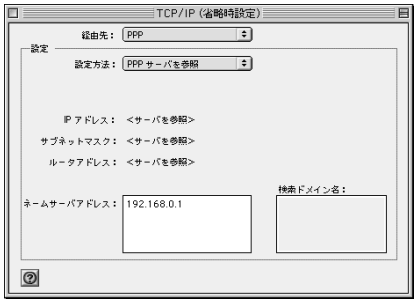
◆ ネットワーク機能を設定する

コントロールパネルの[TCP/IP]と[モデム]を設定します。

1 アップルメニューから[コントロールパネル]－[TCP/IP]を選ぶ。

2 以下のように設定する。

- **経由先**:PPP
- **設定方法**:PPPサーバを参照
- **ネームサーバアドレス**:本機のIPアドレス(工場出荷時は192.168.0.1)

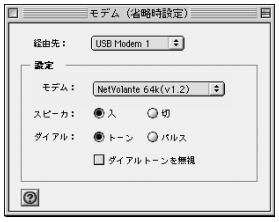


3 設定が終わったら、[ファイル]メニューから[終了]を選ぶ。

4 アップルメニューから[コントロールパネル]－[モデム]を選ぶ。

5 以下のように設定する。

- **経由先**:USB Modem
- **モデム**:NetVolante 64k(v1.2)
- **ダイアル**:トーン



6 設定が終わったら、[ファイル]メニューから[終了]を選ぶ。

◆ダイヤルアップ接続を設定する

1 **アップルメニューから[コントロールパネル]－[リモートアクセス]を選ぶ。**

2 **以下のように設定する。**

- ユーザ ID:プロバイダから入手したユーザー名
- パスワード:プロバイダから入手したパスワード
- パスワードを保存:チェックを付ける。
- 電話番号:半角英数字で「***#」と入力。

3 **設定が終わったら、[ファイル]メニューから[終了]を選ぶ。**

◆ インターネットへ接続する

インターネットへ接続するときは、コントロールパネルの[リモートアクセス]を開いて本機にダイヤルアップ接続します。

1 **アップルメニューから[コントロールパネル]－[リモートアクセス]を選ぶ。**

2 **[接続]をクリックする。**

インターネットに接続すると、接続速度や時間が表示されます。接続中は、WAN LINKランプが点灯します。

ヒント

[リモートアクセス]のエイリアスをシステムフォルダ内の[起動項目]フォルダに入れておくと、Macintoshを起動すると自動的に「リモートアクセス」画面が開くようになります。[接続]をクリックすると、簡単にLANへアクセスできます。

USBポートからLAN接続する（擬似LAN）

本機に内蔵の擬似LAN機能を使うと、USBポートに接続したパソコンも、TCP/IPプロトコルでLANにアクセスできるようになります。LANボードを取り付けられないパソコンを接続するときは、この方法で接続してください。

LANに接続すると、TCP/IPプロトコルのファイルサーバにアクセスできるようになり、ダイヤルアップルータの自動接続機能によるインターネット接続も利用できます。ただし、Windowsのファイル共有やAppleShareのファイル共有は利用できません。

擬似LAN機能を使うときは、以下の接続や設定を行ってください。

Windows 98SE/Meの場合

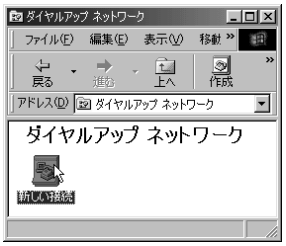
擬似LAN機能を使うときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

1 **[マイコンピュータ]の[ダイヤルアップ ネットワーク]をダブルクリックする。**

Windows Meの場合は、[コントロールパネル]の[ダイヤルアップ ネットワーク]をダブルクリックします。

2 **[新しい接続]アイコンをダブルクリックする。**

「ダイヤルアップネットワークへようこそ」画面が表示された場合は、[次へ]をクリックします。「所在地情報」画面が表示された場合は、市外局番を入力してください。

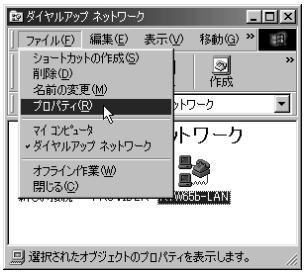


3 **[接続名]に「RTW65b-LAN」と入力し、[モデムの選択]に[RTW65b USB (Sync)]を選んでから、[次へ]をクリックする。**

4 **市外局番は空欄のまま、電話番号に半角英数字で「****」と入力してから、国番号に[日本(81)]を選んで[次へ]をクリックし、[完了]をクリックする。**

「ダイヤルアップ ネットワーク」フォルダ内に、登録したプロバイダ名のアイコンが表示されます。

5 **[RTW65b-LAN]アイコンを選んでから、[ファイル]メニューから[プロパティ]を選ぶ。**

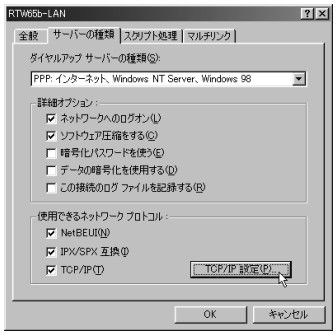


6 **[サーバーの種類]タブをクリックする。**

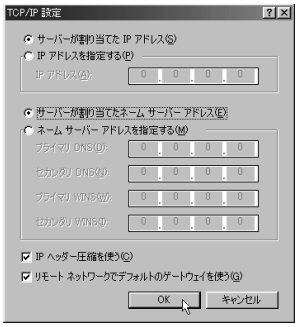
Windows Meの場合は、[ネットワーク]タブをクリックします。

7 **以下のように設定してから、[TCP/IP設定]をクリックする。**

- [詳細オプション]の[ソフトウェア圧縮する]:チェックを外す。
- [使用できるネットワーク　プロトコル]の[NetBEUI]、[IPX/SPX互換]:チェックを外す。
- [TCP/IP]:チェックを付ける。



8 **[サーバーが割り当てたネームサーバーアドレス]を選んでから、各ウィンドウの[OK]をクリックしてウィンドウを閉じる。**



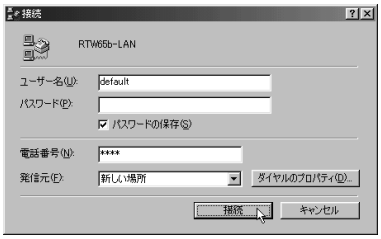
これで、擬似LAN接続の設定が完了しました。

◆ LANに接続する

LANへ接続するときは、[RTW65b-LAN]アイコンをダブルクリックして、本機の擬似LAN機能にダイヤルアップします。

1 **[ダイヤルアップネットワーク]フォルダ内の[RTW65b-LAN]アイコンをダブルクリックする。**

2 **[ユーザー名]に任意の名前を入力し、[パスワード]は空欄、[パスワードの保存]をチェックして[接続]をクリックする。**



本機の擬似LAN機能に接続し、LANにアクセスできるようになります。

ヒント

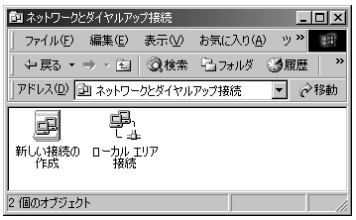
作成した[RTW65b-LAN]アイコンのショートカットをスタートメニューの[スタートアップ]に追加すると、Windowsを起動すると自動的に「RTW65b-LAN」画面が開くようになります。[接続]をクリックすると、簡単にLANにアクセスできます。

Windows 2000の場合

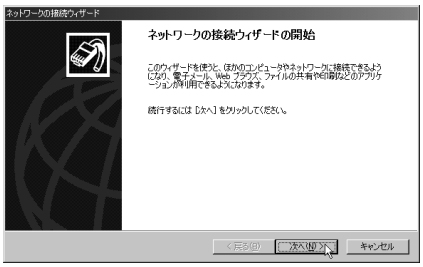
擬似LAN機能を使うときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

1 **[コントロールパネル]の[ネットワークとダイヤルアップ接続]をダブルクリックする。**

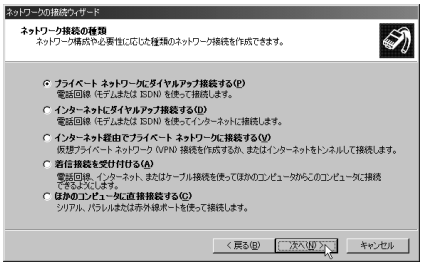
2 **[新しい接続の作成]アイコンをダブルクリックする。**



3 **[次へ]をクリックする。**



4 [プライベートネットワークにダイヤルアップ接続する]を選んでから、[次へ]をクリックする。

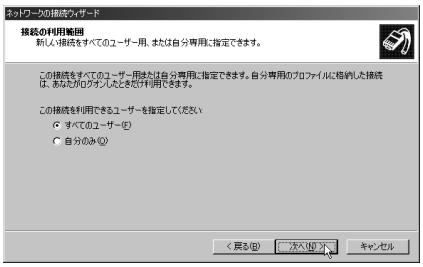


ご注意

「デバイスの選択」画面が表示された場合は、[YAMAHA RTW65b(USB)(COMx)]のみをチェックし、他のデバイスのチェックを外してから[次へ]をクリックします。

5 電話番号に半角英数字で「****」と入力してから、[次へ]をクリックする。

6 [すべてのユーザー]を選んでから、[次へ]をクリックする。



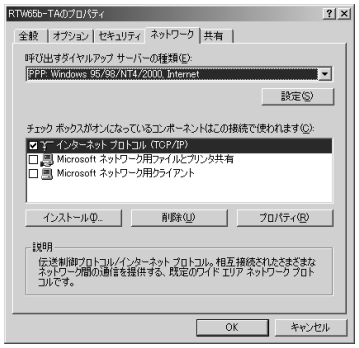
7 [接続名]に「RTW65b-LAN」と入力してから、[完了]をクリックする。

8 [RTW65b-LAN]アイコンをクリックして選んでから、[ファイル]メニューから[プロパティ]を選ぶ。

9 [全般]タブをクリックして、[接続の方法]から[YAMAHA RTW65b(USB)(COMX)]を選ぶ。

10 [ネットワーク]タブをクリックして、以下のように設定してから、[OK]をクリックする。

- [インターネットプロトコル(TCP/IP)]：チェックを付ける。
- [Microsoftネットワーク用ファイルとプリンタ共有]：チェックを外す。
- [Microsoftネットワーク用クライアント]：チェックを外す。

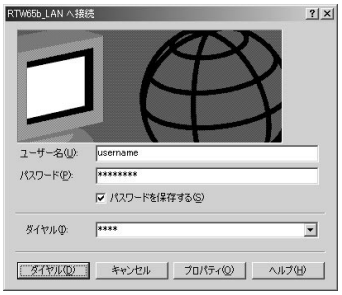


◆ LANへ接続する

LANへ接続するときは、[RTW65b-LAN]アイコンをダブルクリックして、本機の擬似LAN機能にダイヤルアップします。

1 [ダイヤルアップネットワーク]フォルダ内の[RTW65b-LAN]アイコンをダブルクリックする。

2 [ユーザー名]に任意の名前を入力し、[パスワード]は空欄、[パスワードの保存]をチェックして[ダイヤル]をクリックする。



本機の擬似LAN機能に接続し、LANにアクセスできるようになります。

ヒント

作成した[RTW65b-LAN]アイコンのショートカットをスタートメニューの[スタートアップ]に追加すると、Windowsを起動すると自動的に「RTW65b-LAN」画面が開くようになります。[接続]をクリックすると、簡単にLANにアクセスできます。

Windows XPの場合

擬似LAN機能を使うときは、ダイアルアップネットワークのアイコンを作成し、本機へダイアルアップ接続します。

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

2 [ネットワーク接続]をクリックする。

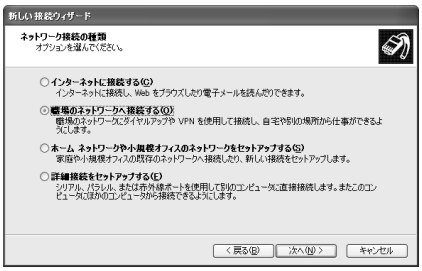
3 [新しい接続を作成する]をクリックする。

「新しい接続ウィザードの開始」画面が表示されます。

「所在地情報」画面が表示された場合は、市外局番を入力してから、[OK]をクリックしてください。

4 [次へ]をクリックする。

5 [職場のネットワークに接続する]を選んでから、[次へ]をクリックする。



6 [ダイヤルアップ接続]を選んでから、[次へ]をクリックする。

7 [会社名]に「RTW65b-LAN」と入力してから、[次へ]をクリックする。

8 電話番号に半角英数字で「****」と入力してから、[次へ]をクリックする。

9 [完了]をクリックする。

10 [RTW65b-LAN]アイコンを選んでから、[この接続の設定を変更する]をクリックする。

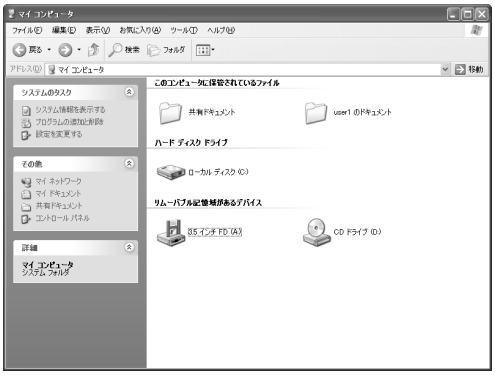
11 [全般]タブをクリックして、[接続の方法]から[YAMAHA RTW65b(USB)(COMX)]を選ぶ。

12 [ネットワーク]タブをクリックして、以下のように設定してから、[OK]をクリックする。

- [インターネットプロトコル(TCP/IP)]:チェックを付ける。
- [Microsoftネットワーク用ファイルとプリンタ共有]:チェックを外す。
- [Microsoftネットワーク用クライアント]:チェックを外す。

◆ LANに接続する

1 「マイ コンピュータ」画面の[マイ ネットワーク]をクリックする。



2 [ネットワーク接続を表示する]をクリックする。

3 [RTW65b-LAN]アイコンを選んでから、[この接続を開始する]をクリックする。

4 [ユーザー名]に任意の名前を入力し、[パスワード]は空欄、[パスワードの保存]をチェックして[ダイヤル]をクリックする。

本機の擬似LAN機能に接続し、LANにアクセスできるようになります。

ヒント

作成した[RTW65b-LAN]アイコンのショートカットをスタートメニューの[スタートアップ]に追加すると、Windowsを起動すると自動的に「RTW65b-LAN」画面が開くようになります。[接続]をクリックすると、簡単にLANにアクセスできます。

MacOS 9の場合

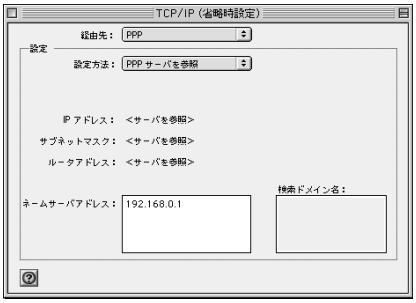
◆ ネットワーク機能を設定する

コントロールパネルの[TCP/IP]と[モデム]を設定します。

1 アップルメニューから[コントロールパネル]－[TCP/IP]を選ぶ。

2 以下のように設定する。

- **経由先**:PPP
- **設定方法**:PPPサーバを参照
- **ネームサーバアドレス**:本機のIPアドレス(工場出荷時は192.168.0.1)



3 設定が終わったら、[ファイル]メニューから[終了]を選ぶ。

4 アップルメニューから[コントロールパネル]－[モデム]を選ぶ。

5 以下のように設定する。

- **経由先**:USB Modem
- **モデム**:NetVolante 64k
- **ダイアル**:トーン

6 設定が終わったら、[ファイル]メニューから[終了]を選ぶ。

◆ダイヤルアップ接続を設定する

1 アップルメニューから[コントロールパネル]－[リモートアクセス]を選ぶ。

2 以下のように設定する。

- ユーザ ID：任意のユーザ名
- パスワード：空欄
- パスワードを保存：チェックを付ける。
- 電話番号：半角英数字で「****」と入力。

3 設定が終わったら、[ファイル]メニューから[終了]を選ぶ。

◆ LANへ接続する

LANへ接続するときは、コントロールパネルの[リモートアクセス]を開いて本機の擬似LAN機能にダイヤルアップ接続します。

1 アップルメニューから[コントロールパネル]－[リモートアクセス]を選ぶ。

2 [接続]をクリックする。

本機の擬似LAN機能にダイヤルアップ接続し、LANにアクセスできるようになります。

ヒント

[リモートアクセス]のエイリアスをシステムフォルダ内の[起動項目]フォルダに入れておくと、Macintoshを起動すると自動的に「リモートアクセス」画面が開くようになります。[接続]をクリックすると、簡単にLANへアクセスできます。

第 5 章
無線 LAN を使う

この章では、本機を利用した無線LANのより高度な活用例を紹介しています。設定にはネットワークの知識が必要になるものもありますが、やりたいことに該当する例を参考にして、本機のルータ機能を十分活用してください。より専門的な設定例については、「設定例集」や「コマンドリファレンス」、ヤマハRTシリーズのホームページ（http://www.rtpro.yamaha.co.jp/）をご覧ください。

本機の無線LAN機能の概要

本機内蔵の無線LANは、電波免許不要の2.4GHz帯周波数を使った無線LANです。本機にはIEEE802.11b規格に準拠した無線アクセスポイント機能が内蔵されており、パソコンに同規格に準拠した無線LANカード（またはボード／アダプタ）を取り付けることで、無線LANを構築できます。

無線LANの主な機能

ご注意

本機の工場出荷状態では、無線LANによる本機へのアクセスが可能になっています。**不正使用を防ぐために、暗号（WEP）を設定することを強くおすすめいたします。**また、無線LANを使用しない場合は、無線モードをオフにしてください。

ESS-ID

無線アクセスポイントを識別するためのグループ名で、同じESS-IDを持つ機器間で通信できます。本機に無線接続をするときは、本機のESS-IDをパソコンの無線LANカード（またはボード／アダプタ）に設定する必要があります。本機の工場出荷値は、本機のLAN側MACアドレスの下6桁が設定されています。

チャネル

IEEE802.11b規格の無線LANで使用する周波数で、14個のチャネルがあります。1～13チャネルが第2世代小電力データ通信システムに、14チャネルが小電力データ通信システムに対応しています。本機の工場出荷値は、チャネル1が設定されています。

ご注意

- 近隣に同じチャネルを使用する無線LANアクセスポイントがあると、別のESS-IDを利用した場合でも、通信速度が低下することがあります。この場合は、異なるチャネルを使用することで干渉を防止し、通信速度を確保してください。
- 各チャネルの周波数が近接しているため、複数のチャネルを使用するときは、3つ以上離れたチャネルをお使いください。
- IEEE802.11bで使用する周波数は移動体識別装置と共用しているため、これらの無線局が付近で運用されている場合は、干渉しないチャネルをお使いください。

WEP

無線LANの通信を暗号化する機能です。WEPを設定すると、無線信号を傍受されても暗号キーなしでは解読することができません。本機のWEPは64bitまたは128bitコードで暗号化しており、それぞれ64bitまたは128bitコードに対応した無線LANカード（またはボード／アダプタ）間で利用できます。

MACアドレスフィルタ

各ネットワーク機器固有のMACアドレスを使って、接続を制限する機能です。MACアドレスフィルタを設定すると特定の機器しか接続できないので、不正な機器によるLANへの侵入を防止することができます。

ご注意

- 本機の無線LANに多くのパソコンを接続すると通信速度が著しく低下します。実用上は、32台以内での利用をおすすめいたします(同時使用可能な無線端末数は、使用環境により減る場合があります)。
- WEPを設定すると、暗号化処理のために通信速度が多少遅くなります。あらかじめご了承ください。
- 64bitコードと128bitコードのWEPを設定した機器を混在して、無線LANを構築することはできません。WEPを設定する場合は、無線LAN全体を64bitまたは128bitコードのいずれかに統一してください

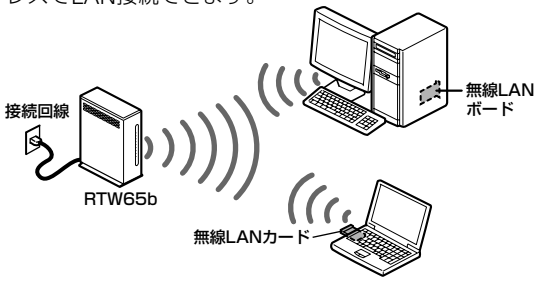
無線LANの利用例

無線LANを使った代表的な接続例を紹介します。

複数のRTW65bを使うと、離れたLANにそれぞれRTW65bを接続してLANどうしを接続できる「無線ブリッジ機能」や、いくつかのRTW65bを有線LANで接続して無線アクセスポイントの自動切り替えにより無線範囲を広げられる「ローミング機能」、さまざまな方法で活用できます。なお、これらの機能はRT60wとの相互接続環境でも使用できます。

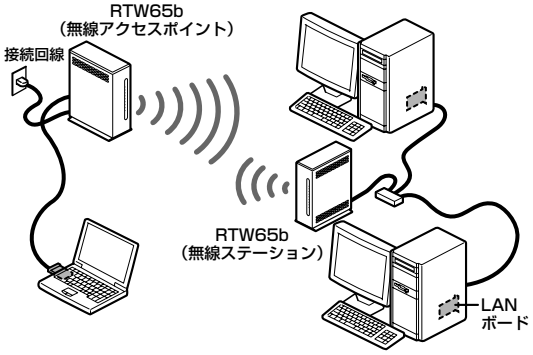
◆ パソコンのみを無線LANに接続する場合

ノートパソコンやデスクトップパソコンを無線でLAN接続できます。別の部屋でも電波の届く範囲なら、ワイヤレスでLAN接続できます。



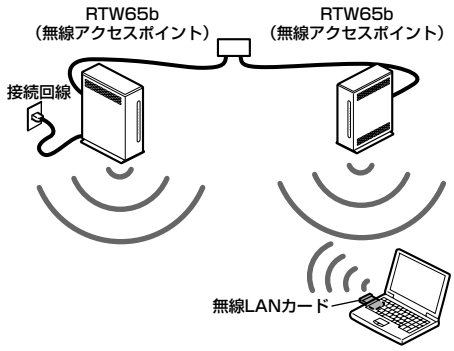
◆ 複数のRTW65bを無線ブリッジ接続する場合

本機に内蔵の「無線ブリッジ接続機能」により、別の部屋や別の階の有線LANでも、それぞれRTW65bを設置することで、ワイヤレスで有線LANどうしを接続することができます。接続できるRTW65bは、合計9台までです。



◆ 複数のRTW65bでローミング接続する場合

本機に内蔵の「ローミング機能」により、LAN上の離れた場所に複数のRTW65bを接続することで、無線LANの届く範囲を広げることができます。無線LAN接続のパソコンが移動している場合でも、電波状態の良いアクセスポイントに自動的に切り替えながら、接続し続けることができます。



無線LANへのアクセスを制限する

本機の無線LANはWEP(暗号化)に加えて、MACアドレスフィルタのセキュリティ機能を内蔵しているため、不正侵入を防ぐことができます。

最小限の設定では、ESS-IDの設定だけでも使えますが、WEP(暗号化)やMACアドレス制限機能を設定して、セキュリティを強化してお使いになることを強くおすすめいたします。

1 **無線LAN接続する機器のMACアドレスを調べる。**

2 **無線LANで接続する、すべての機器の電源を入れる。**

3 **LANに接続している1台のパソコンでWebブラウザを起動して、アドレス入力欄に「http://setup.netvolante.jp/」と半角英字で入力してから、Enterキーを押す。**

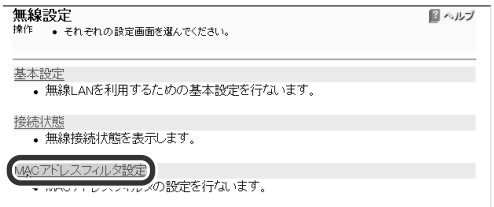
「ネットワーク パスワードの入力」画面が表示されます。

4 **[パスワード]欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

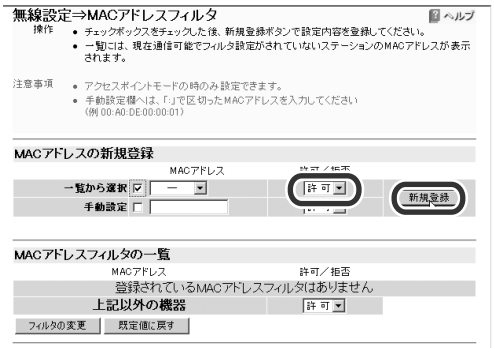
「トップ」画面が表示されます。

5 **[無線設定]をクリックする。**

6 **[MACアドレスフィルタ設定]をクリックする。**



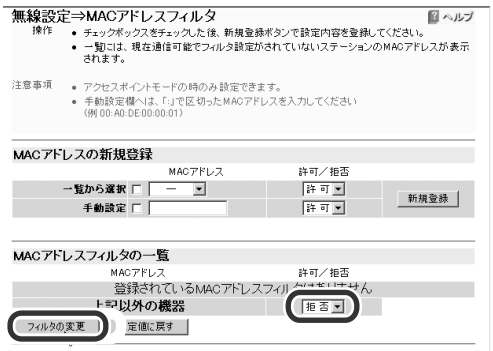
7 **表示されているMACアドレスの各機器について[許可]か[拒否]を選んでから、[新規登録]をクリックする。**



ご注意

MACアドレスフィルタ機能をすでに使用している場合、新しい無線LANカード／ボードに本機のESS-IDを設定すると、「無線設定」画面に[上記以外の機器]と同じ設定(通常は[拒否])で表示されます。使用するときは[許可]を選んでください。

8 **使用する機器をすべて登録したら、[上記以外の機器]で[拒否]を選び、[フィルタの変更]をクリックする。**



MACアドレスフィルタが有効になります。

9 **パソコンから本機の「かんたん設定ページ」を開く。**

開ければ、設定完了です。

無線で複数のRTW65bを接続する

複数のRTW65bを無線で接続するときは、接続回線に接続していないルータの設定を変更します。

設定の変更内容

複数のRTW65bを接続する場合は、使用方法に合わせて次のように設定します。

無線ブリッジ接続の場合

設定項目	回線を接続しているルータ（メインルータ）	その他のルータ（サブルータ）
無線モード	アクセスポイント	ステーション
ESS-ID	同じESS-ID	同じESS-ID
WEP	同じ設定値	同じ設定値
DHCPサービス	サーバ	OFF
IPアドレス	初期値または固定IPアドレス	DHCPクライアントまたは固定IPアドレス

ローミング接続の場合

設定項目	回線を接続しているルータ（メインルータ）	その他のルータ（サブルータ）
無線モード	アクセスポイント	アクセスポイント
ESS-ID	同じESS-ID	同じESS-ID
WEP	同じ設定値	同じ設定値
DHCPサービス	サーバ	OFF
IPアドレス	初期値または固定IPアドレス	DHCPクライアントまたは固定IPアドレス

ご注意

WANポートにCATV用またはADSL用のモデムを接続していないルータでは、WAN LINKランプは点灯しません。回線接続状況は、WANポートを接続回線に接続しているルータのWAN LINKランプで確認してください。

設定を変更する

すでに使用しているRTW65bにあとからRTW65bを無線ステーションルータとして追加設置する場合は、追加するRTW65bのLANポートに接続したパソコンから「かんたん設定ページ」でESS-IDやWEPの設定を行います。

1 **無線アクセスポイントにするメインルータを、LANケーブルでパソコンを接続する。**

2 **メインルータの電源を入れてから、メインルータに接続したパソコンの電源を入れる。**

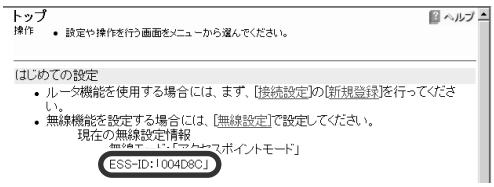
3 **パソコンでWebブラウザを起動して、アドレス入力欄に「http://(メインルータのIPアドレス)/」を入力してから、Enterキーを押す。**

「ネットワーク パスワードの入力」画面が表示されます。

4 **[パスワード]欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

5 **トップページに表示されているESS-ID設定値をメモする。**



6 **追加するサブルータのLANポートに、パソコンをつなぎ変える。**

7 **サブルータの電源を入れてから、サブルータに接続したパソコンを再起動する。**

8 **パソコンでWebブラウザを起動して、アドレス入力欄に「http://(サブルータのIPアドレス)/」を入力してから、Enterキーを押す。**

「ネットワーク パスワードの入力」画面が表示されます。

9 **[パスワード]欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

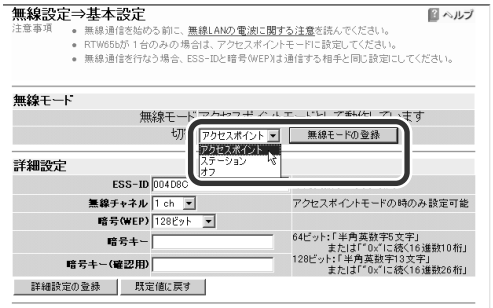
「トップ」画面が表示されます。

10 **[無線設定]をクリックする。**

11 [基本設定]をクリックする。

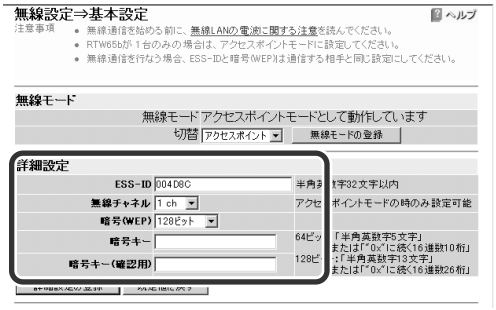
12 無線モードを選んでから、[無線モードの登録]をクリックする。

- **無線ブリッジ接続の場合:**ステーション
- **ローミング接続の場合:**アクセスポイント



13 手順5で確認したメインルータのESS-IDを選ぶ(または入力する)。

メインルータでWEPを使用している場合は、メインルータと同じWEPの設定をしてから、メインルータに設定した暗号キーを入力してください。



ご注意

ESS-ID、WEPの設定が合っていないと、RTW65b間で接続できません。メインルータに設定した値を正確にメモして、必ず同じ値をすべてのサブルータに設定してください。

14 [詳細設定の登録]をクリックする。

15 画面左側の[接続設定]をクリックする。

16 [LAN/WAN設定]をクリックする。

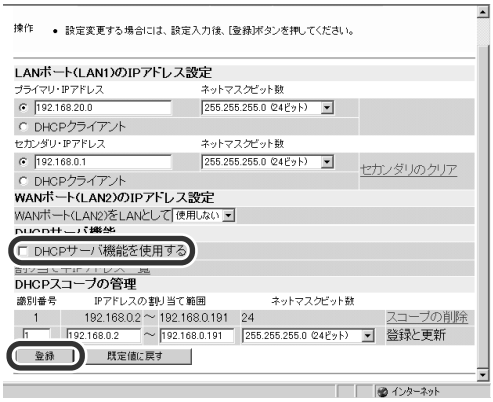
17 サブルータのプライマリ・IPアドレスとネットマスクを設定する。

[DHCPクライアント]を選んだ場合は

サブルータはDHCPサーバからIPアドレスを自動取得します。

変更後のIPアドレスは、メインルータの「かんたん設定ページ」ー「接続設定」ー「LAN/WAN設定」画面の[割り当て中IPアドレス一覧]で、サブルータの底面に記載されているMACアドレスと照らし合わせて確認してください。

18 [DHCPサーバ機能を使用する]のチェックを外してから、[登録]をクリックする。



無線で複数のRTW65bを接続する

ヒント

ローミング接続の場合は、外部HUBを経由してメインルータとサブルータを接続してください。接続には、HUBのポート仕様に合わせて、ストレートケーブルまたはクロスケーブルを使います。

19 パソコンのWebブラウザのアドレス入力欄に「http://(メインルータのIPアドレス)/」を入力してから、Enterキーを押す。

メインルータの「トップ」画面にアクセスできることを確認してください。

アクセスできない場合は

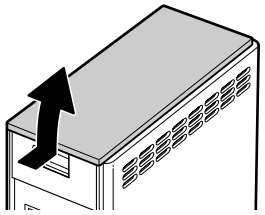
サブルータの設定に誤りがあります。サブルータを工場出荷状態に戻してから、手順6から操作し直してください。

外部アンテナを接続する

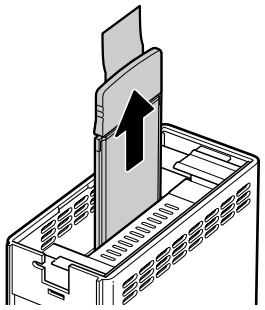
市販の外部アンテナを本機に増設すると、無線LANのカバー範囲を広げたり、データの転送品質を向上させることができます。

1 本機の電源を切る。

2 本機上部のカバーを開く。

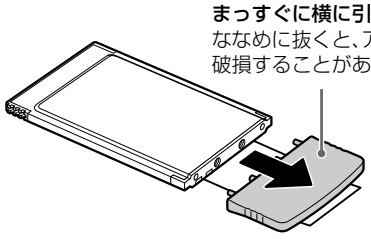


3 内蔵PCカードをまっすぐに引き抜いて、取りはずす。

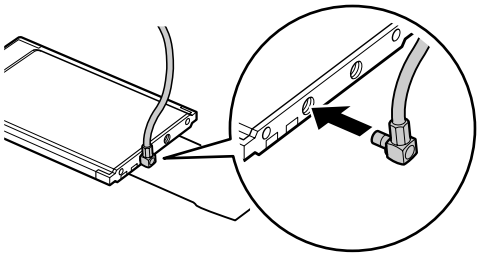


4 PCカードの先端のアンテナを取りはずす。

取りはずした本機付属のアンテナは、なくさないように保管してください。



5 外部アンテナのコネクタを、「カチッ」と音がするまで押し込む。



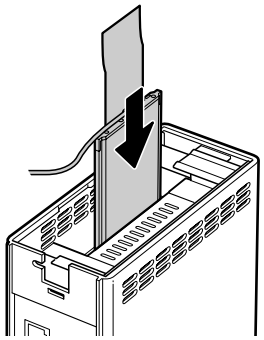
カード上のランプに近い方のコネクタに差し込む。

ヒント

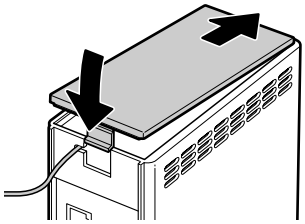
外部アンテナを2本同時に使用することもできます。

6 PCカードを元に戻す。

下図の向きにカードを差し込み、奥まで確実に押し込みます。



7 アンテナ線を筐体のくぼみにあわせて、カバーを閉じる。



8 アンテナを適切な場所に設置する。

◆ 使用アンテナ

- 本機に使用する外部アンテナは、弊社製品をご利用ください。それ以外の製品はご利用いただけません。
- 使用できる外部アンテナについて詳しくは、ネットボランチホームページ(http://NetVolante.jp)をご覧ください。

第 6 章 ファイアウォール機能を使う

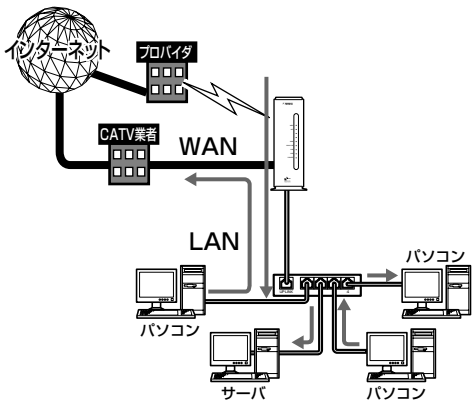
ファイアウォールとは、外部からの不正アクセスを禁止する機能です。この章では、本機のファイアウォール機能を使ったセキュリティ／ルーティング機能や、不正アクセス検知機能について説明します。設定にはネットワークの知識が必要になるものもありますが、該当する例を参考にして、本機の機能を十分活用してください。より専門的な設定例については、「コマンドリファレンス」やヤマハRTシリーズのホームページ（http:/www.rtpro.yamaha.co.jp/）をご覧ください。

本機のファイアウォール機能の概要

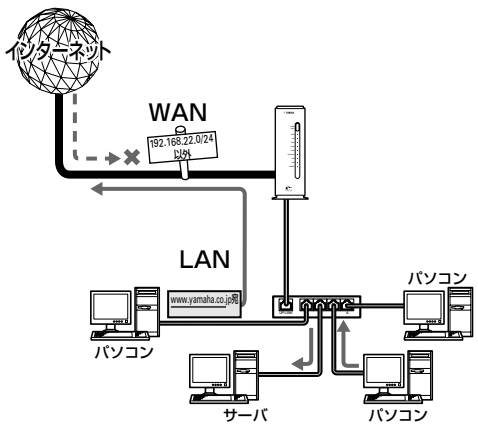
パケット単位のルーティング／セキュリティを設定できます

ネットワークを流れるデータの単位を「パケット」と呼びます。ネットワークに流れているデータは、パケット単位で分割されていて、それぞれが発信元や送信先、データの種類などの情報を持っています。

本来「ルータ」とは、ネットワークを流れるパケットの送信元や送信先、データの種類を監視して、パケットの行き先を制御（ルーティング）する装置のことを呼びます。本機はWANポートとLANポートの間でルーティングを行う機能を持っています。



本機では、パケットの条件を設定して不要な接続を防止したり、パケットの行き先を指定して複数の接続先を使い分けたりすることができます（フィルタ）。フィルタを設定することで、さまざまなルーティングやセキュリティを設定することが可能になります。



セキュリティ対策の必要性について

インターネットに接続すると、世界中のホームページを閲覧したり、世界中の人たちと電子メールで自由に情報を交換したりすることができ、とても便利です。しかし同時に、お使いのパソコンに対する不正アクセスの危険に、世界中からさらされることになります。

特にサーバを公開したりするなど、インターネットに常時接続する環境を導入する場合は、ネットワークの危険についてよくご理解いただいた上で、十分なセキュリティ設定を行うことが必要です。もちろん常時接続する場合以外でも、インターネットに接続している間は、世界中から危険にさらされているという点では同じです。本機の機能を利用して、十分なセキュリティ設定を行ってください。

ご注意

不正アクセスの手段やセキュリティ上の抜け道／穴(セキュリティホール)は、日夜新たに発見されています。本機の機能を含めて、すべての問題を解決できる完璧なセキュリティ対策は存在せず、インターネット接続には常に危険があることをご理解ください。常に新しい情報を入手し、お客様の自己責任でセキュリティ設定を強化することを強くおすすめいたします。

なお、本機を使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。

◆ インターネットからの不正アクセスとは

インターネットに接続している間は、悪意のある者からパソコンやルータがアタック(不正なアクセス)される可能性があります。ルータを介してパソコンを接続している場合は、NATやIPマスカレードといったアドレス変換機能によって比較的安全ですが、設定の誤りや不足によって、同様の危険にさらされる場合があります。

本機の設定を改変されたり、パソコンのシステムやデータを破壊された場合、多大なデータ的被害や金銭的被害に遭うことも十分に考えられます。本機のフィルタを設定するなどのセキュリティ対策を行って、自己防衛してください。

悪意を持った者がアタックを行うときに主な足がかりにするのが、「グローバルIPアドレス」です

同じグローバルIPアドレスを長時間使用している場合は、不正アクセスの被害にあう確率が高くなります。固定アドレス契約接続時に割り当てられた動的アドレスを使い続けるCATV／ADSL／フレッツ･ADSLなどで接続する場合は、十分なセキュリティを設定することをおすすめいたします。

本機のパスワード設定にもご注意ください

パスワードを設定しないで本機を使用することは、ことは、セキュリティ上大変危険です。必ずパスワードを設定するだけでなく、ときどきパスワードを変更して、本機をお使いください。

◆ 接続方法と危険度

接続の種類	グローバルIPアドレスの種類	危険度
CATV接続	プライベートIPアドレスの場合	✘（CATV内アドレスに対して危険）
	動的IPアドレスの場合	✘✘（長時間接続時危険）
	固定IPアドレスの場合	✘✘✘（常に危険）
ADSL接続	動的IPアドレスの場合	✘✘（長時間接続時危険）
	固定IPアドレスの場合	✘✘✘（常に危険）
フレッツ･ADSL接続	動的IPアドレス	✘✘（長時間接続時危険）

不正アクセスに対抗するには

インターネットの不正アクセスは、いくつかの種類に分けられます。それぞれの対抗手段には次のようなものがあります。

◆ 不正なパケットで侵入するもの

- インターネットへの接続を切断したり、グローバルIPアドレスを変更することが、もっとも効果的です。フレッツ·ADSLなどの常時接続でも、本機の自動切断機能を設定することで、接続／切断のたびに動的IPアドレスを変更できます。
- パケットフィルタリング式ファイアウォールで、不要なパケットを通さないことも、ある程度効果があります。パケットフィルタリングは、本機のフィルタ設定で登録できます。
- アプリケーション·ゲートウェイ式ファイアウォールソフトウェアも、整合性のないパケットや不審なActiveX、Javaアプレットをパソコンに受け入れないようにするため、かなり効果があります。ウィルス検知ソフトと組み合わせて使うこともできます。ただしこの場合は、ファイアウォール用サーバを設けて、アプリケーション·ゲートウェイ式ファイアウォールソフトウェアをインストールする必要があります。

◆ OSやサーバソフトウェアのセキュリティホールを突いて侵入するもの

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

◆ 電子メールの添付ファイルとして侵入するもの

添付ファイルを開くことで、感染します。不審な添付ファイルは開かないことを徹底するだけでなく、パソコンにウィルス検知ソフトウェアをインストールして、ウィルスを早期発見／早期駆除することで、被害を最小限に抑えることができます。

本機のフィルタ設定でできること

本機のフィルタ設定では、接続先ごとに100個までのフィルタを設定できます。それぞれのフィルタでパケットの送信元や送信先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないよう設定できます。不正なアクセスに使われやすいパケットや、あり得ないパケットをルータ通過時に破棄するように設定することで、不正なパケットがLAN内に入ることを防ぐことができます。

ただし、高度に偽装したパケットやメールに添付されるウィルス、ActiveX、Javaアプレットなどのように、正規のパケットとして通過するものは、本機のフィルタで防ぐことはできません。ウィルス検知ソフトウェアやアプリケーション·ゲートウェイ式ファイアウォールソフトウェアを併用するようおすすめいたします。

◆ セキュリティを目的としたフィルタ設定の考えかた

フィルタを設定するときは、以下の考えかたを基本にすると良いでしょう。

LAN側からインターネット側へのアクセス(出力方向)は原則許可し、必要に応じて禁止する

LAN側からインターネット側へのアクセスを厳しく規制すると、非常に使いにくいものになり、管理や設定変更に手間がかかります。原則自由とした上で、問題があればその部分だけ制限します。

インターネット側からLAN側へのアクセス(入力方向)は、原則禁止し、必要に応じて許可する

インターネット側からLAN側へのアクセスは、原則禁止して外部からのアクセスを防ぎます。Webサーバの公開など、必要がある場合にのみ最小限だけ許可します。

ご注意

この場合、インターネット側からのアクセスとは、インターネット側からリクエストが始まったパケットのことを指します。LAN側からリクエストしたパケットの応答パケット(例:URLを指定してホームページのデータを要求する)は、該当しません。応答パケットにはACKフラグという識別子が付くので、ホームページのデータや電子メールの受信に制限はありません。

◆ 静的フィルタと動的フィルタ

本機で設定できるフィルタには、次の種類があります。

- **静的フィルタ**：1度設定を行うと、データや通信の有無にかかわらず、常に有効になります。
- **動的フィルタ**：通信状態を監視しながら、必要に応じてフィルタが有効になります。例えば、「通常はインターネットからLANへのデータはすべて禁止にしておき、LAN側からftpのアクセスが発生したときだけ許可する」といった設定ができます。

実際に使用する場合は、それぞれの良いところを併用しながら設定を行います。

◆「かんたん設定ページ」が自動設定するフィルタ

「かんたん設定ページ」では、各設定に応じて自動的にフィルタを適用します。

プロバイダ接続の場合は

フィルタの組み合わせパターンで、7段階のセキュリティレベルを定義しています。

プロバイダの新規登録時に、接続の種類にあわせて以下の設定を自動的に適用します。セキュリティレベルは、必要に応じて後で変更することができます。

- **自動切断を行う設定**：セキュリティレベル3
- **常時接続を行う設定**：セキュリティレベル4または5

LANで運用の場合には

WindowsのNetBIOSによる意図しない発信や、Windowsのセキュリティホールへのアクセスを防ぐフィルタが自動的に適用されます。

ご注意

セキュリティレベルや設定内容は予告なく変更する場合があります。

◆ フィルタ番号の意味

本機のフィルタ機能の番号は、ほぼ無制限に利用できますが、かんたん設定ページでは各接続先毎に100個（0番～99番）ずつ設定できるようにしています。以下に「かんたん設定ページ」の利用する、フィルタ番号の対応を示します。

割当領域	コンソールコマンドのフィルタ番号
LAN/WANポート用割当領域	100000～199999
例）LANポートの静的フィルタ（0～99）	100000～100099
WANポートの静的フィルタ（0～99）	101000～101099
接続先設定用割当領域	200000～299999
例）PP01の静的フィルタ（0～99）	200000～200099
PP02の静的フィルタ（0～99）	201000～201099
：	
PP30の静的フィルタ（0～99）	229000～229099
Anonymousの静的フィルタ（0～99）	232000～232099
フィルタ型ルーティング用割当領域	500000～599999

ご注意

- セキュリティのために、フィルタの設定変更は機能を十分にご理解の上、行ってください。
- フィルタを多く適用すると、処理が複雑になり、インターネットへのアクセス速度が遅くなる場合があります。

セキュリティレベルを変更する

本機の「かんたん設定ページ」では、フィルタを組み合わせた7段階のセキュリティレベルが定義されています。プロバイダの新規登録時に、接続の種類にあわせて自動的にセキュリティレベルが設定されます。設定されたセキュリティレベルは、必要に応じてあとから変更することもできます。

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

「ネットワーク パスワードの入力」画面が表示されます。

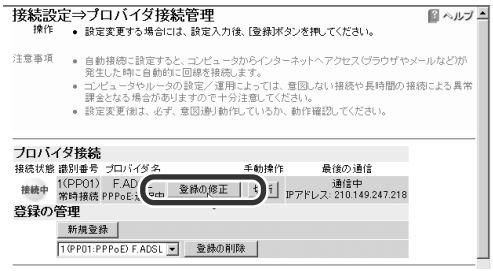
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

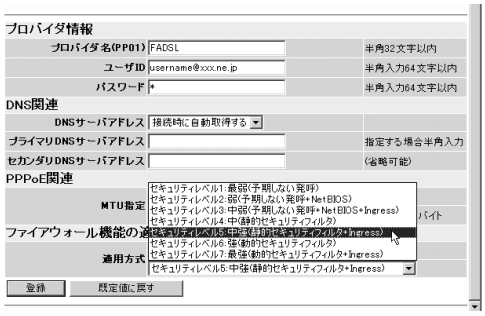
3 **[接続設定]をクリックする。**

4 **[プロバイダ接続管理]をクリックする。**

5 **接続先名の[登録の修正]をクリックする。**



6 **[ファイアウォール機能の適用]の[適用方式]でセキュリティレベルを選んでから、[ファイアウォール機能を適用しなおす]にチェックを付ける。**



ご注意

- セキュリティレベルの数字が大きくなるほど、適用されるフィルタが複雑になり、安全性は高くなります。ただし、パソコンの設定やお使いのソフトウェアによっては、インターネットへのアクセスができなくなったり、制限される場合があります。
- ファイアウォール機能を適用しなおすと、手動設定されたフィルタも含めてすべてのフィルタがいったんクリアされ、新たに設定されます。

7 **[登録]をクリックする。**

セキュリティレベルが選んだレベルに変更されます。

フィルタを設定する

フィルタを設定するには、「かんたん設定ページ」の「ファイアウォール機能」画面またはコンソールコマンドを使用します。

Webブラウザで設定する

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

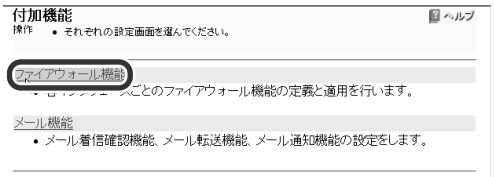
「ネットワーク パスワードの入力」画面が表示されます。

2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

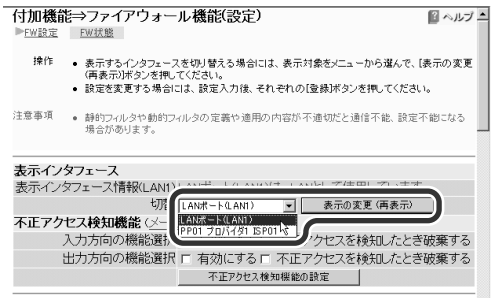
3 **[付加機能]をクリックする。**

4 **[ファイアウォール機能]をクリックする。**



5 **設定する接続先を選んでから、[表示の変更]をクリックする。**

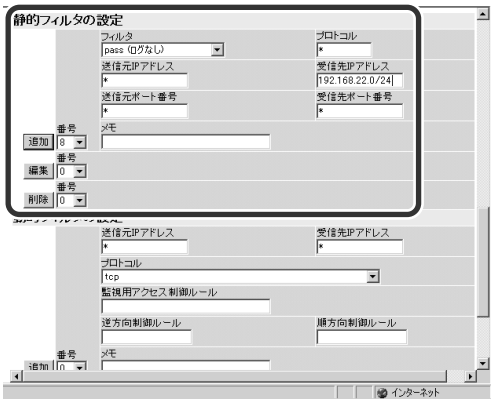
LANポートもひとつの接続先になります。



ご注意

LANを選ぶと、LANポートに接続しているパソコン、およびLANポートに接続しているHUBに接続しているすべてのパソコンが対象になります。

6 **[静的フィルタの設定]でフィルタ番号を選んでから、各設定項目を入力する。**



フィルタ番号

接続先毎に0～99まで使用できます。番号の小さい順に設定内容が優先されます。

フィルタ　処理する方法を選びます。

- **pass(ログなし)**：指定したパケットを通す（記録なし）
- **pass(ログあり)**：指定したパケットを通す（記録あり）
- **reject(ログなし)**：指定したパケットを通さない（記録なし）
- **reject(ログあり)**：指定したパケットを通さない（記録あり）
- **restrict(破棄時ログあり)**：接続中だけ指定したパケットを通し、破棄したパケットの記録を残す
- **restrict(ログなし)**：接続中だけ指定したパケットを通す（記録なし）
- **restrict(ログあり)**：接続中だけ指定したパケットを通す（記録あり）

プロトコル フィルタの対象にするプロトコルを入力します。

例）＊（すべてのプロトコルを指定）
tcp（1つのプロトコルを指定）
tcpfin,tcprst（","で区切って複数指定）

- ＊：すべて
- tcp：TCPパケット
- established：応答TCPパケット（ACKフラグのあるTCPパケット）
- tcpfin：FINフラグのあるTCPパケット
- tcprst：RSTフラグのあるTCPパケット
- udp：UDPパケット
- icmp：ICMPパケット
- icmp-error：エラー通知のためのICMPパケット
- icmp-info：情報通知または診断のためのICMPパケット
- ah：IPsecのahパケット
- esp：IPsecのespパケット

送信元IPアドレス

送信元のIPアドレスを入力します。単独アドレスでもネットワークアドレス（アドレス範囲）でも指定できます。すべての場合は、「＊」を入力します。

例）192.168.0.13（個別のIPアドレスで指定）
192.168.0.0/24（ネットワーク範囲で指定）
192.168.0.20-192.168.0.50（IPアドレス範囲で指定）

送信元ポート

送信元アプリケーションソフトの種類を示すポート番号またはニーモニックを入力します。

例）＊（すべてのポート番号を指定）
137-139（NetBIOS関係のポート番号で指定）
www,pop3,ftp（ニーモニックで指定）

- ＊：すべて
- 23(telnet)：telnet
- 25(smtp)：電子メール（送信）
- 70(gopher)：インターネット情報検索システム
- 79(finger)：機器利用ユーザの情報を調べる機能
- 80(http)：ホームページ閲覧、Webサーバ公開
- 110(pop3)：電子メール（受信）
- 113(ident)：電子メール（ユーザ認証）
- 119(nntp)：ネットワークニュース
- 123(ntp)：ネットワーク時刻合わせ
- 137(netbios_ns)：NetBIOS名前解決
- 138(netbios_dgm)：NetBIOSデータグラム転送
- 139(netbios_ssn)：NetBIOSストリームデータ転送（Windowsファイル共有）
- 194(irc)：インターネット・リレー・チャット
- 443(https)：暗号化されたWebサーバ
- 445(microsoft-ds)：Windows 2000のSMB
- 1723：PPTP（Microsoft VPN Adapter）

受信先IPアドレス

受信先のIPアドレスを入力します。単独アドレスでもネットワークアドレス（アドレス範囲）でも指定できます。すべての場合は、「＊」を入力します。

受信先ポート

受信先アプリケーションソフトの種類を示すポート番号を入力します。すべての場合は、「＊」を入力します。

メモ　設定したフィルタの説明を記入することができます。半角英数字が使用できます。

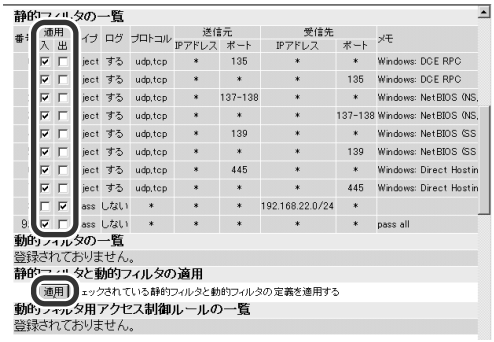
ご注意

フィルタの具体的な設定例については、「フィルタの設定例」(69ページ)をご覧ください。

7 **[追加]をクリックする。**

フィルター一覧に追加されます。

8 **フィルタを設定する方向にチェックを付けてから、[適用]をクリックする。**



適用　対象にするパケットの流れる向きを指定します。

- **入**:接続先から入ってくるパケット
- **出**:接続先へ出て行くパケット

9 **複数のフィルタを設定する場合は、手順5〜7の操作を繰り返す。**

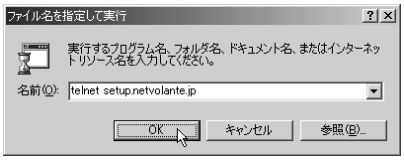
コンソールコマンドで設定する

LANポートに接続しているパソコン、または無線LANで接続しているパソコンからTELNETソフトで本機にログインし、コンソールコマンドを送信して設定します。ここでは、Windows標準のTELNETを使用する場合の操作を説明します。Macintoshではフリーウェアなどをお使いください（MacOS Xでは、MacOS Xに付属のTerminalソフトウェアからTELNETを使用できます）。

1 **[スタート]メニューをクリックして、[ファイル名を指定して実行]をクリックする。**

2 **「telnet setup.netvolante.jp」と入力してから、[OK]をクリックする。**

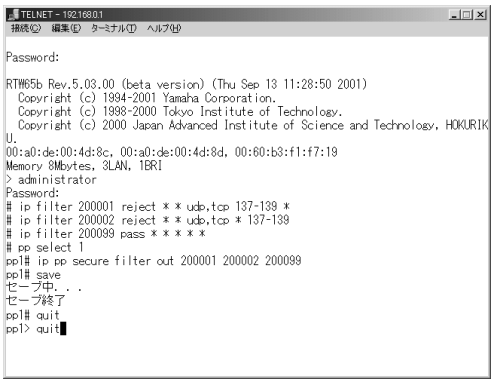
本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開くこともできます。



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

何も表示されなければ一度リターンキーを押します。

「>」の文字が表示されると、コンソールコマンドが入力できます。



ヒント

以下のコマンドを入力してからEnterキーを押すと、説明が表示されます。

- **help**:キー操作の説明が表示されます。
- **show command**:コマンド一覧が表示されます。

4 「administrator」と入力してから、Enterキーを押す。

5 「Password:」と表示されたら、管理パスワードを入力する。

「#」の文字が表示されると、各種ルータコンソールコマンドが入力できます。
コンソールコマンドの種類と働きについて詳しくは、コマンドリファレンスをご覧ください。

6 フィルタコマンドを入力してから、Enterキーを押す。

複数のフィルタを設定する場合は、フィルタコマンド入力操作を繰り返してください。

例：NetBIOSのデータで発信しないようにする設定

```
ip filter 200001 reject * * udp,tcp 137-139 *
```

（全送信元のNetBIOS、TCPとUDPプロトコルのデータを通さない）

```
ip filter 200002 reject * * udp,tcp * 137-139
```

（全送信元のNetBIOS、TCPとUDPプロトコルのデータを通さない）

```
ip filter 200099 pass * * * *
```

（その他の全データを通す）

ご注意

- フィルタの具体的な設定例については、「フィルタの設定例」(69ページ)をご覧ください。
- フィルタコマンド「ip filter」について詳しくは、コマンドリファレンスをご覧ください。

7 フィルタを有効にするコマンドを入力してから、Enterキーを押す。

接続先の方向毎にコマンドを入力してください。

例：プロバイダ（PP01）へ出るパケットに200001、200002、200099のフィルタを有効にする設定

```
pp select 1
```

（接続先を選択）

```
ip pp secure filter out 200001 200002 200099
```

（適用する方向とフィルタ番号を指定）

ご注意

- フィルタの具体的な設定例については、「フィルタの設定例」(69ページ)をご覧ください。
- 「ip pp secure filter」コマンドについては、コマンドリファレンスをご覧ください。

8 設定が終わったら「save」と入力してからEnterキーを押して、設定を本機に保存する。

9 設定を終了するには、「quit」と入力してから、Enterキーを押す。

10 コンソールを終了するには、もう1度「quit」と入力してから、Enterキーを押す。

フィルタの設定例

ここでは、よく使われるフィルタの設定例を紹介します。例を参考に、実際使用している接続先やプライベートIPアドレスに合わせて入力してください。

ここでは、フレッツ·ADSLを例にして説明しています。

フィルタ設定の考えかた

フィルタは「接続先、IN/OUT、始点アドレスの始点ポート／終点アドレスの終点ポート、プロトコル、タイプ」という順序で構成されていますので、「どこから来た(へ行く)、どこから始まるどんなパケットを、どうする」と日本語で考えると、フィルタを作りやすくなります。

例1:プロバイダから来た、すべてのNetBIOS関連のtcpとudpパケットを、通さず記録しない

このフィルタは「PP01 IN * 137-138 tcp,udp reject-nolog」と表現されます。

つまり、「PP01(プロバイダ) IN(から来る) *(すべての) 137-138(NetBIOS関連) tcp,udp(tcpとudpパケット) reject-nolog(通さずに記録しない)」ことになります。

例2:ADSLへ行く、すべてのNetBIOS関連のtcpとudpパケットを、通さず記録する

このフィルタは「wan OUT * 137-138 tcp,udp reject-log」と表現されます。

つまり、「wan(WANポートに接続された回線、この場合はADSL) OUT(へ出ていく) *(すべての) 137-138 (NetBIOS関連) tcp,udp(tcpとudpパケット) reject-log (通さずに記録する)」ことになります。

すこし難しいかもしれませんが、以下の設定例を通してフィルタ設定の考えかたに慣れて、本機のフィルタ機能をぜひ使いこなしてください。

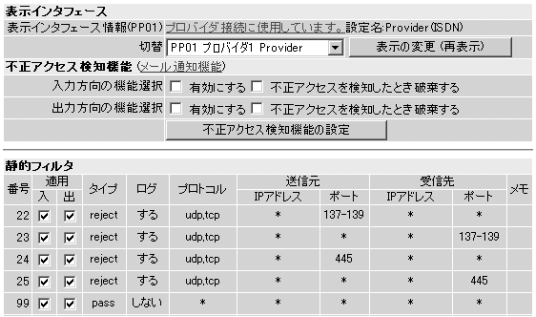
意図しない発信を防ぐフィルタの設定例

◆ 外部からのWIndowsのファイル共有を防ぐ

Windowsのネットワークでは、NetBIOS over TCP/IPプロトコルが使われています。ネットワーク内のNetBIOSパケットにより、自動接続してしまうことがあります。また、Windowsファイル共有やPersonal Webサーバ機能を使っている場合は、接続先側から覗かれてしまう場合もあります。防ぎたい場合は、接続先へNetBIOSパケットが出入りしないようにフィルタを設定します。

NetBIOSパケットを一切通さない設定例

NetBIOS関係のポート137～139に加えて、Windows 2000のファイル共有に使用するSMBプロトコルのポート445を出入り共に通さず、その他を通すように設定します。



コンソールコマンドの場合

```
ip filter 200022 reject-log * * udp,tcp 137-139 *
ip filter 200023 reject-log * * udp,tcp * 137-139
ip filter 200024 reject-log * * udp,tcp 445 *
ip filter 200025 reject-log * * udp,tcp * 445
ip filter 200099 pass-nolog * * * * *
pp select 1
ip pp secure filter in 200022 200023 200024 200025
  200099
ip pp secure filter out 200022 200023 200024 200025
  200099
```

セキュリティの設定例

◆ 特定のパソコンにインターネット接続を禁止する

LAN内の特定のパソコンがインターネットに接続できないようにするには、発信元IPアドレスによるフィルタを設定します。複数のパソコンを指定したい場合は、ネットワーク範囲で設定することができます。不要なパケットを通さないことにより、好ましくない自動接続を防ぐことができます。

ご注意

この設定を使うには、あらかじめLAN内のパソコンに固定プライベートアドレスを設定する必要があります。設定方法については、「パソコンのIPアドレスを管理する」(93ページ)をご覧ください。

コンソールコマンドの場合

```
ip filter 200014 reject-log 192.168.0.22 * * * *
ip filter 200015 reject-log 192.168.0.42-192.168.0.45
  * * * *
ip filter 200099 pass-nolog * * * * *
pp select 1
ip pp secure filter out 200014 200015 200099
```

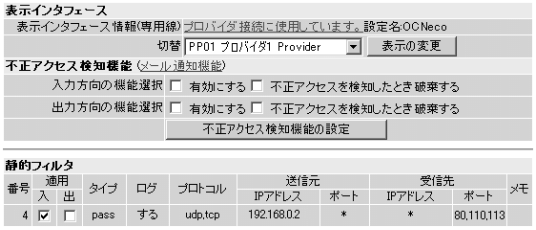
◆ 特定のサーバをインターネットに公開する

LAN内のサーバをインターネットに公開する場合は、送信先IPアドレスによるフィルタを設定します。不要なアクセスを防ぐため、サーバの種類によって公開するポートもあわせて設定してください。

ご注意

サーバを公開するには、その他にもルータやサーバの設定が必要です。設定方法については、「外部にサーバを公開する」(83ページ)をご覧ください。

サーバへのWWWとメールアクセスを通す設定例



コンソールコマンドの場合

```
ip filter 230004 pass-log 192.168.0.2 * udp,tcp *
  80,110,113
pp select 1
ip pp secure filter in 230004
```

◆ 発信元IPアドレス偽装による不正アクセスを防ぐ

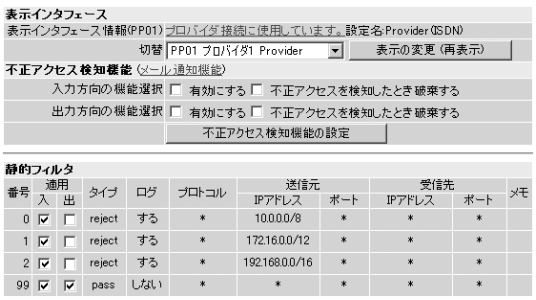
LAN内のプライベートIPアドレスを装って、LANの外から不正アクセスされることがあります。この手法は「ip spoofing攻撃」や「land攻撃」、「smurf攻撃」と呼ばれています。これらの攻撃を回避するには、発信元IPアドレスがプライベートIPアドレスの場合や、自分に割り当てられたグローバルIPアドレスの場合に、パケットを通さないようなフィルタを設定します。

プロバイダ側やWAN側からプライベートIPアドレスでアクセスされることはあり得ませんし、自分のネットワークに割り当てられたグローバルIPアドレスで他からアクセスされることもあり得ませんので、実用上の問題はありません。また、LAN側からプロバイダ側やWAN側へ出るパケットにも設定すると、間違ったパケットがLANの外部に出ることも同時に防ぐことができます。

ご注意

CATV接続の場合など、プロバイダのネットワーク内でプライベートIPアドレスが使われている場合がありますので、そのアドレスは設定しないでください。

固定グローバルIPアドレスを使っていない場合の設定例



コンソールコマンドの場合

```
ip filter 200000 reject-log 10.0.0.0/8 * * * *
ip filter 200001 reject-log 172.16.0.0/12 * * * *
ip filter 200002 reject-log 192.168.0.0/16 * * * *
ip filter 200099 pass-nolog * * * * *
pp select 1
ip pp secure filter in 200000 200001 200002 200099
```

固定グローバルIPアドレスを使っている場合の設定例

ここでは、グローバルIPアドレス(133.176.200.0/28)を割り当てられている場合を例にしています。実際には、ご自分に割り当てられたグローバルIPアドレスを入力してください。

コンソールコマンドの場合

```
ip filter 200000 reject-log 10.0.0.0/8 * * * *
ip filter 200001 reject-log 172.16.0.0/12 * * * *
ip filter 200002 reject-log 192.168.0.0/16 * * * *
ip filter 200003 reject-log 133.176.200.0/28 * * *
  *
ip filter 200098 pass-nolog * 133.176.200.0/28 * *
  *
pp select 1
ip pp secure filter in 200000 200001 200002 200003
  200098
ip filter 200010 reject-log * 10.0.0.0/8 * * *
ip filter 200011 reject-log * 172.16.0.0/12 * * *
ip filter 200012 reject-log * 192.168.0.0/16 * * *
iP filter 200013 reject-log * 133.176.200.0/28 * *
  *
ip filter 200099 pass-nolog 133.176.200.0/28 * * *
  *
pp select 1
ip pp secure filter out 200010 200011 200012 200013
  200099
```

◆ LAN側のネットワークを守る設定例(静的フィルタ)

LAN内のパソコンでインターネット接続を行い、外部からのアクセスを静的フィルタで制限する場合の設定です。接続先設定の入力で制限を行い、出力では制限していません。

ご注意

LAN内に各種サーバを設置したり、UDPを利用する場合は、それぞれの通信を可能にするための静的passフィルタを、入力側に追加して適用する必要があります。より高いセキュリティが必要な場合は、動的フィルタを使用した設定例を参考にしてください。

表示インタフェース

表示インタフェース情報(PP01) プロバイダ接続に使用しています。設定名:Provider(ISDN)

切替 PP01 プロバイダ1 Provider 表示の変更(再表示)

不正アクセス検知機能 (メール通知機能)

入力方向の機能選択 有効にする 不正アクセスを検知したとき破棄する

出力方向の機能選択 有効にする 不正アクセスを検知したとき破棄する

不正アクセス検知機能の設定

静的フィルタ

番号	適用 入	適用 出	タイプ	ログ	プロトコル	送信元 IPアドレス	送信元 ポート	受信先 IPアドレス	受信先 ポート	メモ
3	☑	☐	reject	する	*	192.168.0.0/24	*	*	*	
30	☑	☐	pass	しない	icmp	*	*	192.168.0.0/24	*	
31	☑	☐	pass	しない	established	*	*	192.168.0.0/24	*	
32	☑	☐	pass	しない	tcp	*	*	192.168.0.0/24	113	
33	☑	☐	pass	しない	tcp	*	20	192.168.0.0/24	*	
35	☑	☐	pass	しない	udp	*	53	192.168.0.0/24	*	

コンソールコマンドの場合

```
ip filter 200003 reject 192.168.0.0/24 * * * *
ip filter 200030 pass * 192.168.0.0/24 icmp * *
ip filter 200031 pass * 192.168.0.0/24 established
  * *
ip filter 200032 pass * 192.168.0.0/24 tcp * ident
ip filter 200033 pass * 192.168.0.0/24 tcp ftpdata
  *
ip filter 200035 pass * 192.168.0.0/24 udp domain *
pp select 1
ip pp secure filter in 200003 200030 200031 200032
  200033 200035
```

◆ LAN側のネットワークを守る設定例(静的フィルタ+動的フィルタ)

LAN内のパソコンでインターネット接続を行い、外部からのアクセスを静的フィルタと動的フィルタの両方を組み合わせて制限する場合の設定です。

静的フィルタでは、動的フィルタで制限できないパケットを接続先設定の入力で制限します。動的フィルタでは、接続先設定の出力で制限しています。

ご注意

LAN内に各種サーバを設置する場合は、それぞれの通信を可能にするための静的passフィルタを、入力側に追加して適用する必要があります。

表示インタフェース

表示インタフェース情報(PP01) プロバイダ接続に使用しています。設定名:Provider(ISDN)

切替 PP01 プロバイダ1 Provider 表示の変更(再表示)

不正アクセス検知機能 (メール通知機能)

入力方向の機能選択 有効にする 不正アクセスを検知したとき破棄する

出力方向の機能選択 有効にする 不正アクセスを検知したとき破棄する

不正アクセス検知機能の設定

静的フィルタ

番号	適用 入	適用 出	タイプ	ログ	プロトコル	送信元 IPアドレス	送信元 ポート	受信先 IPアドレス	受信先 ポート	メモ
3	☑	☐	reject	する	*	192.168.0.0/24	*	*	*	
30	☑	☐	pass	しない	icmp	*	*	192.168.0.0/24	*	
32	☑	☐	pass	しない	tcp	*	*	192.168.0.0/24	113	

動的フィルタの一覧

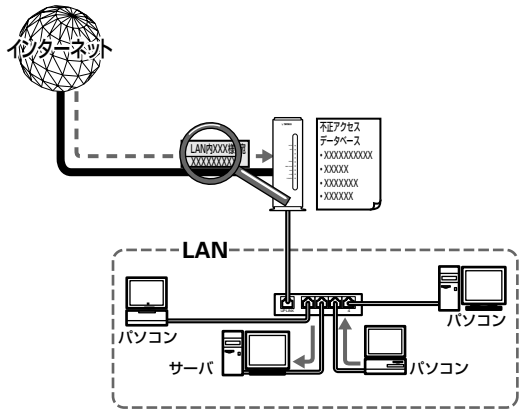
番号	適用 入	適用 出	プロトコル 監視	プロトコル 順方向	プロトコル 逆方向	送信元 IPアドレス	受信先 IPアドレス	メモ
80	☐	☑		ftp		*	*	
98	☐	☑		tcp		*	*	
99	☐	☑		udp		*	*	

コンソールコマンドの場合

```
ip filter 200003 reject 192.168.0.0/24 * * * *
ip filter 200030 pass * 192.168.0.0/24 icmp * *
ip filter 200032 pass * 192.168.0.0/24 tcp * ident
ip filter dynamic 200080 * * ftp
ip filter dynamic 200098 * * tcp
ip filter dynamic 200099 * * udp
pp select 1
ip pp secure filter in 200003 200030 200032
ip pp secure filter out dynamic 200080 200098 200099
```

不正アクセスを検出して警告する

不正アクセス検知機能は、インターネットからの侵入や攻撃などを検出して、警告する機能です。ルータを通過するパケットを、ルータ内の侵入／攻撃パターンのデータベースと比較して、不正アクセスが疑われるパケットを記録／破棄できます。また、この情報を元に不審な発信元やアプリケーションを通さないフィルタを設定することで、よりセキュリティを高めることができます。



ご注意

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

不正アクセス検知機能を設定する

不正アクセス検知機能の設定は、「かんたん設定ページ」の「ファイアウォール機能」画面で行います。インタフェースごとに、検知するパケットの方向や検知時の処理方法を設定できます。

ご注意

- 不正アクセス検知機能を有効にすると、侵入検知の際にブザーが鳴るように工場出荷状態では設定されています。ブザーを鳴らしたくないときは、「かんたん設定ページ」−「システム管理」−「ルータ設定」画面の［ブザー設定］で変更できます。
- 不正アクセス検知機能は各インタフェース、入出力に適用可能ですが、適用数によってはインターネットなどへのアクセス速度が遅くなる場合があります。

1 **Webブラウザを開き、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

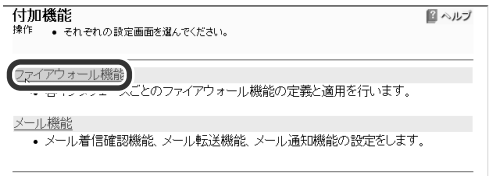
「ネットワーク パスワードの入力」画面が表示されます。

2 **［パスワード］入力欄にルータの管理パスワードを入力してから、［OK］をクリックする。**

「トップ」画面が表示されます。

3 **［付加機能］をクリックする。**

4 **［ファイアウォール機能］をクリックする。**



5 設定する接続先を選んでから、[表示の変更]をクリックする。

通常はインターネットに接続するインタフェース(PPxxやWAN)を選択します。

6 [不正アクセス検知機能]の[入力方向の機能選択]で機能を設定してから、[不正アクセス検知機能の設定]をクリックする。

入力方向の機能選択

インタフェースから入ってくるパケットに対する機能を設定します。

- **有効にする**:不正アクセスを検知すると、記録します。
- **不正アクセスを検知したとき破棄する**:不正アクセスを検知すると、不正アクセス検知履歴に記録してから、そのパケットを破棄します。

出力方向の機能選択

インタフェースへ出ていくパケットに対する機能を設定します。

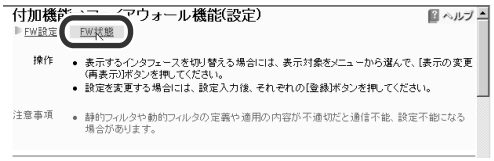
- **有効にする**:不正アクセスを検知すると、記録します。
- **不正アクセスを検知したとき破棄する**:不正アクセスを検知すると、不正アクセス検知履歴に記録してから、そのパケットを破棄します。

不正アクセス検知履歴を確認する

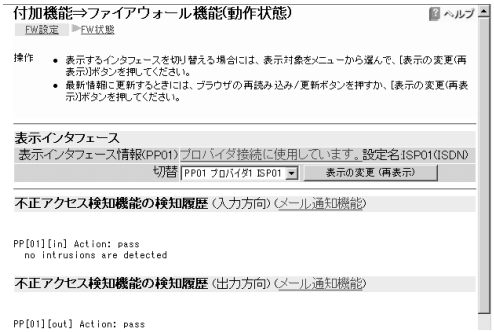
不正アクセス検知履歴は、「かんたん設定ページ」-「ファイアウォール機能」−[FW状態]画面で確認できます。

1 73ページの手順1〜4の操作を行う。

2 [FW状態]をクリックする。



不正アクセスの検知履歴が表示されます。



ご注意

- 不正アクセス検知機能を有効にすると、侵入検知の際にブザーが鳴るように工場出荷状態では設定されています。ブザーを鳴らしたくないときは、「かんたん設定ページ」−「システム管理」−「ルータ設定」画面の[ブザー設定]で変更できます。
- 不正アクセスの手段や侵入/攻撃パターンは、日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入/攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、検知されたパターンが必ずしも重大な不正アクセスであることを判断するものではありません。あくまでセキュリティ管理の目安であることをご理解の上、ご利用ください。

ヒント

不正アクセスを検知した場合に、自動的にメールで知らせるように設定することもできます。外出先からでも不正アクセスがないかどうか監視したいときに便利です。詳しくは「不正アクセス検知をメールで通知する」(26ページ)をご覧ください。

第 7 章
ルータを使いこなす

この章では、本機を使いこなすための活用例を紹介します。設定によってはネットワークの知識が必要になるものもありますが、該当する例を参考にして、本機をご活用ください。より専門的な設定例については、「コマンドリファレンス」、ヤマハRTシリーズのホームページ（http://www.rtpro.yamaha.co.jp/）をご覧ください。

本機へのアクセスを制限する

本機には、本機自体のセキュリティを確保するために、パスワード機能や利用ホスト制限機能を装備しています。これらの機能を利用することで、第三者が不正にルータの設定を変更できないように設定できます。

パスワードには2種類があります

パスワードには「管理パスワード」と「ログインパスワード」の2つの種類があり、以下のような機能の違いがあります。

- **管理パスワード**：すべての画面の設定を閲覧／変更できます。
- **ログインパスワード**：「手動接続と切断」「通信の記録」の設定のみ閲覧／変更できます。

ご注意

本機の「かんたん設定ページ」を最初に開いたときに設定するパスワードは、「管理パスワード」です。また、最初はログインパスワードにも管理パスワードと同じものが設定されます。

パスワードや利用ホスト制限の設定は、「かんたん設定ページ」の「ルータ設定」画面で行います。

1 Webブラウザを起動して、本機の「かんたん設定ページ」を開く。

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

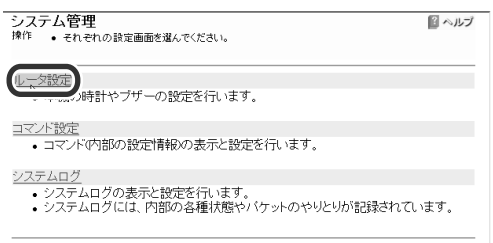
「ネットワーク パスワードの入力」画面が表示されます。

2 [パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。

「トップ」画面が表示されます。

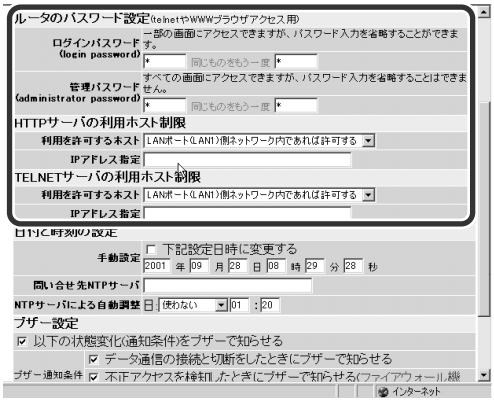
3 画面左側の[システム管理]をクリックする。

4 [ルータ設定]をクリックする。



5 **必要なセキュリティ項目を設定する。**

無線LANの設定項目は、LAN（LAN1）と同様です。



ログインパスワード

一般ユーザ用パスワードを設定します。2つとも同じパスワードを入力してください。

管理者パスワード

ルータ管理者用パスワードを設定します。2つとも同じパスワードを入力してください。

HTTPサーバ利用者制限

Webブラウザで設定できるパソコンを指定します。

- **すべて許可する**：LAN側やWAN側のパソコンすべてに許可します。
- **同一ネットワーク内であれば許可する**：LAN側とWAN側に属するネットワーク内のパソコンにのみ許可します。
- **LANポート（LAN1）側ネットワーク内であれば許可する**：LAN側に属するネットワーク内のパソコンにのみ許可します。
- **WANポート（LAN2）側ネットワーク内であれば許可する**：WAN側に属するネットワーク内のパソコンにのみ許可します。
- **指定したIPアドレスを許可**：指定したIPアドレスのパソコンにのみ許可します。

TELNETサーバ利用者制限

TELNETで設定を変更できるパソコンを指定します。

- **すべて許可する**：LAN側やWAN側のパソコンすべてに許可します。
- **同一ネットワーク内であれば許可する**：LAN側とWAN側に属するネットワーク内のパソコンにのみ許可します。
- **LANポート（LAN1）側ネットワーク内であれば許可する**：LAN側に属するネットワーク内のパソコンにのみ許可します。
- **WANポート（LAN2）側ネットワーク内であれば許可する**：WAN側に属するネットワーク内のパソコンにのみ許可します。
- **すべて許可しない**：TELNETによる設定操作を禁止します。コンソールコマンドや設定してください。
- **指定したIPアドレスを許可**：指定したIPアドレスのパソコンにのみ許可します。

6 **[登録]をクリックする。**

メッセージに従ってボタンをクリックすると、設定が登録されます。

本機のIPアドレスを変更する

すでにプライベートIPアドレスが指定されているLANに本機を導入する場合は、本機のIPアドレスを変更する必要があります。IPアドレスを変更する前に、本機に割り当てるIPアドレスとネットマスクをLANの管理者にお問い合わせください。

ご注意

- グローバルIPアドレスの契約をしていて、LAN内の各パソコンにグローバルIPアドレスを設定している場合は、必ずプロバイダの接続情報を確認してから作業してください。不安なときは、プロバイダまたは電話事業者の技術者にご相談ください。万一間違ったIPアドレスを設定してしまうと、LAN外のホストやネットワークに問題が起きることがあります。
- 管理者がいないときは、LAN内のすべての機器のプライベートIPアドレス設定を調べて、ネットマスクの設定値と、重複しないIPアドレスを決めてください。

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

「ネットワーク パスワードの入力」画面が表示されます。

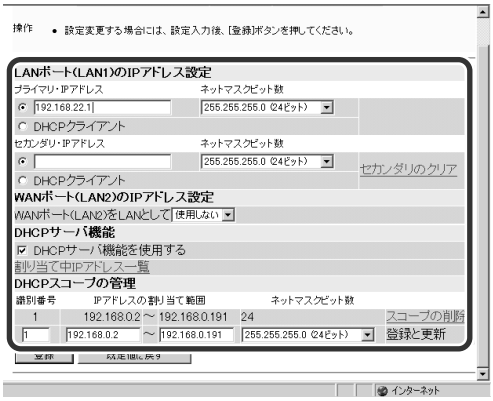
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

3 **[接続設定]をクリックする。**

4 **[LAN/WAN設定]をクリックする。**

5 **[プライマリ・IPアドレス]で本機のIPアドレスとネットマスク、DHCPサーバのIPアドレス割り当て範囲とネットマスクを設定する。**



6 **画面下にある[登録]をクリックする。**

メッセージにしたがってボタンをクリックすると、設定が変更されます。

ご注意

ルータのIPアドレスを変更した場合、LAN上の各パソコンのIPアドレスをリセットする必要があります（98ページ）。

本機の時刻を自動的に合わせる

インターネット上のNTPサーバ(時刻配信サーバ)を利用して、本機の時刻を自動的に合わせることができます。また、NTPサーバを利用して手動で時刻を合わせたり、時刻を直接入力して合わせたりすることもできます。

ご注意

本機のセキュリティ設定によっては、NTPサーバが利用できない場合があります。利用する場合は、セキュリティ設定を変更してください(64ページ)。

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス(工場出荷時は192.168.0.1)を入力して開きます。

「ネットワーク パスワードの入力」画面が表示されます。

2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

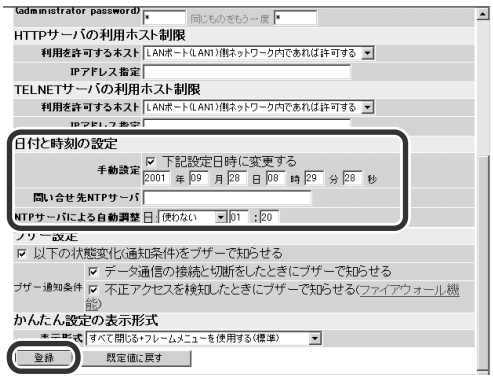
3 **[システム管理]をクリックする。**

4 **[ルータ設定]をクリックする。**

5 **[日付と時刻の設定]で各項目を入力する。**

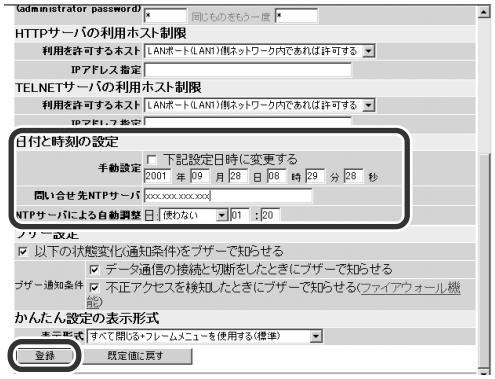
手動で時刻を入力して合わせる場合

[下記設定日時に変更する]にチェックを付けてから、日付と時刻を入力して[登録]をクリックします。



NTPサーバを利用して手動で時刻を合わせる場合

[問い合わせ先NTPサーバ]にNTPサーバのIPアドレスまたはドメイン名を入力してから[登録]をクリックして、さらに[今から更新する]をクリックします。



すぐに時刻が更新されます。

ご注意

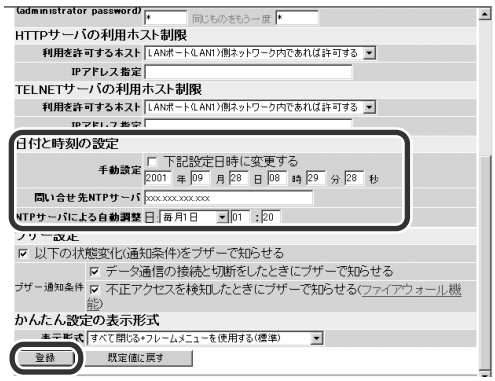
プロバイダの接続設定で「常時接続」を選ぶなどして、ファイアウォール機能のセキュリティレベルが4または5(静的セキュリティフィルタ)に設定されている場合は、NTPサーバからの応答パケットが破棄されてしまうため、時刻を合わせることができません。

この方法で時刻を合わせるときは、プロバイダの接続設定でセキュリティレベルを6または7(動的セキュリティフィルタ)に設定してください。

NTPサーバを利用して定期的に時刻を合わせる場合

[問い合わせ先NTPサーバ]にNTPサーバのIPアドレスまたはドメイン名を入力してから、[登録]をクリックします。

そのあとに[NTPサーバによる自動調整]に更新間隔と時刻を設定してから、[登録]をクリックします。



PPPoEネットワーク型ADSLで接続する

InfoSphere Biz ADSL8サービスなどのように、PPPoEを利用したネットワーク型ADSL接続を利用する場合は、以下の方法で接続します。

回線を接続する

フレッツ·ADSLの場合と同様に接続します。

詳しくは、別冊の「設定マニュアル」の「回線を接続する」(19ページ)をご覧ください。

接続設定を変更する

本機の「かんたん設定ページ」を開いて、PPPoEネットワーク型ADSLの接続先を設定します。

ご注意

- プロバイダ契約を解除または変更した時は、必ず本機の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける可能性が高くなります。十分なセキュリティ設定を行ってから、お使いください。詳しくは「第8章 ファイアウォール機能を使う」(60ページ)をご覧ください。

ここでは、IPマスカレードを使用した設定を、Windows MeとInternet Explorer 5.5の画面を例に説明しています。他の環境の場合、画面表示が多少異なりますが、操作は同じです。

1 本機と設定を行うパソコンだけ電源を入れて、他のパソコンの電源を切る。

ヒント

他のすべてのパソコンを終了できない場合は、本機に1台のパソコンのLANケーブルを直接接続している状態にして、設定を行います。

2 Webブラウザを起動して、本機の「かんたん設定ページ」を開く。

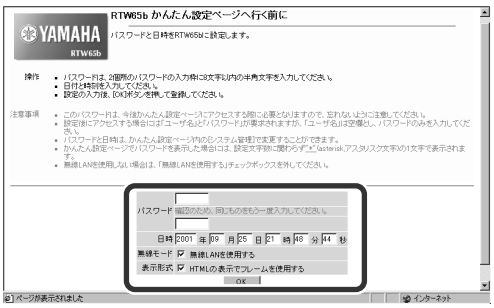
「http://setup.netvolante.jp/」または本機のIPアドレス(工場出荷時は192.168.0.1)を入力して開きます。

初めて開いたときは、「RTW65bかんたん設定ページへ行く前に」が表示されます。2度目以降は、手順4へ進んでください。

ヒント

「RTW65bかんたん設定ページへ行く前に」が表示されないときは、ルータとパソコンの接続や、パソコンの設定を確認してください。詳しくは、別冊の「設定マニュアル」をご覧ください。

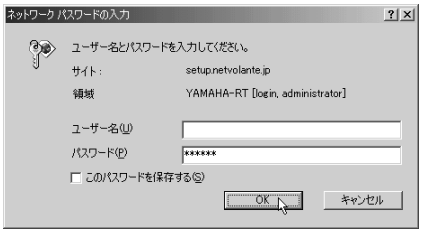
3 ルータの管理パスワードを2つの入力欄に入力してから、日時を設定して[OK]をクリックして、確認のメッセージに従って操作する。



ご注意

- ルータの管理パスワードは、本機の設定を変えるときや情報を見るときに必要になります。プロバイダのパスワードとは別に、大切に管理してください。
- 無線LANを使用しないときは、不正アクセスを防ぐために[無線LANを使用する]のチェックを外してください。

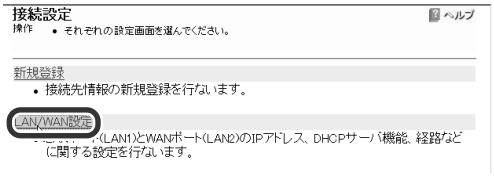
4 [パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。



「トップ」画面が表示されます。

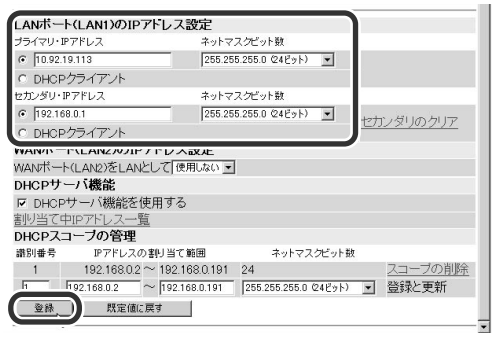
5 [接続設定]をクリックする。

6 [LAN/WAN設定]をクリックする。



7 以下の設定を行ってから、[登録]をクリックする。

- **[LANポート(LAN1)のIPアドレス設定]の[セカンダリ・IPアドレス]**:現在[プライマリ・IPアドレス]に設定されているプライベートIPアドレスとネットマスク(工場出荷時は192.168.0.1/24)を入力する。
- **[プライマリ・IPアドレス]**:プロバイダから割り当てられたIPアドレスの中から、ルータに設定するIPアドレスとネットマスクを入力する。

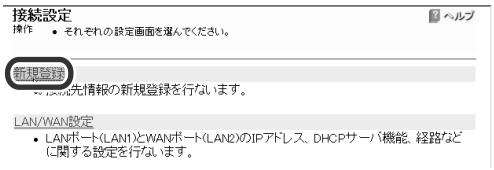


ヒント

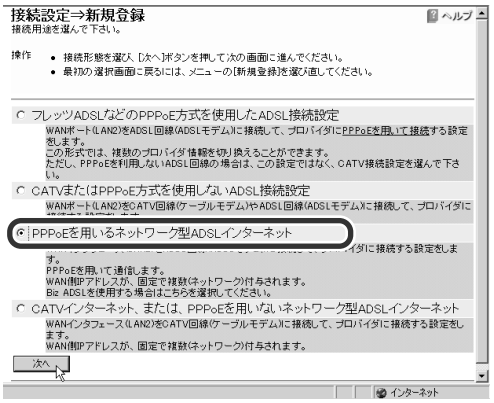
LAN側をプライベートアドレスで利用する場合は、LANポートのIPアドレスの設定を変更する必要はありません。

8 [接続設定]をクリックする。

9 [新規登録]をクリックする。

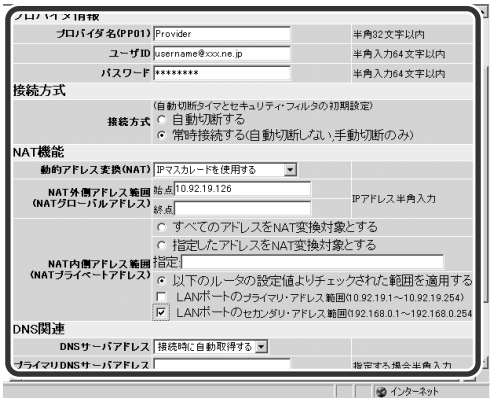


10 [PPPoEを用いるネットワーク型ADSLインターネット]を選んでから、[次へ]をクリックする。



設定入力画面が表示されます。

11 プロバイダの設定情報書類を見ながら、プロバイダ名と各設定項目を入力する。



プロバイダ名

接続先のわかるような名前を入力します。

回線の種類 契約した回線の種類を選びます。

- **64kbit/s**:ディジタルアクセス64などの場合に選びます。
- **128kbit/s**:OCNエコノミーやディジタルアクセス128などの場合に選びます。

動的アドレス変換(NAT)

回線側とLAN側のアドレス変換方法を選びます。

- **NATを使用する:** 回線側とLAN側のアドレスを1対1で変換する場合に選びます。
- **IPマスカレードを使用する:** 回線側とLAN側のアドレスを1対多で変換する場合に選びます。
- **NATとIPマスカレードを併用する:** LAN側の機器にグローバルIPアドレスとプライベートIPアドレスを混在して設定する場合に選びます。
- **使用しない:** アドレス変換機能を使用しない場合に選びます。

NAT外側アドレス範囲

回線側に割り当てる共用グローバルIPアドレスを入力します。

NAT内側アドレス範囲

アドレス変換を行うプライベートIPアドレスの範囲を入力します。

DNSサーバアドレス

DNSサーバアドレスの取得方法を選びます。

- **IPアドレスを指定する:** プロバイダからDNSサーバアドレスが指定されている場合に選びます。
- **接続時に自動取得する:** プロバイダからDNSサーバアドレスが指定されていない場合や、自動取得となっている場合に選びます。

プライマリDNSサーバアドレス

DNSサーバアドレスが指定されている場合に入力します。

セカンダリDNSサーバアドレス

DNSサーバアドレスが2つ指定されている場合に入力します(省略できます)。

ドメイン名 ドメイン名が指定されている場合に入力します(省略できます)。

12 入力し終わったら、[登録]をクリックする。

メッセージにしたがってボタンをクリックすると、接続先が登録されます。

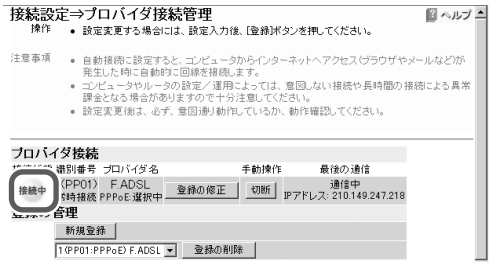
ご注意

インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける可能性が高くなります。十分なセキュリティ設定を行って、ご使用ください。詳しくは「第8章 ファイアウォール機能を使う」(60ページ)をご覧ください。

13 [プロバイダ接続管理]をクリックする。

14 登録したプロバイダの[接続]をクリックして、手動接続してみる。

本機のWAN LINKランプが点灯して左側に「接続中」が表示されたら、正しく設定されています。



接続できない場合は

ユーザIDやパスワードの設定が間違っている可能性があります。

[登録の修正]をクリックして、プロバイダの設定情報書類を見直しながら設定内容を確認したり、パスワードの大文字/小文字や全角/半角に注意して入力し直してから、もう1度手動接続を行ってください。

15 ページ左上の[ネットボランチホームページ]をクリックする。

NetVolanteのホームページが表示されます。

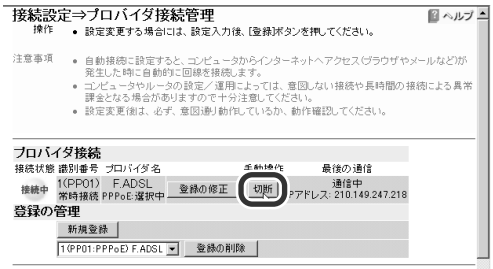
表示されない場合は

DNSサーバアドレスの設定が間違っている可能性があります。

[切断]をクリックしていったん接続を切断してから、[登録の修正]をクリックして、設定内容をもう1度確認してください。

16 **接続できることを確認できたら、Webブラウザの[戻る]をクリックして「プロバイダ接続管理」画面に戻る。**

接続方式で[自動切断する]を選んでいる場合は、登録したプロバイダの[切断]をクリックして手動切断してください。



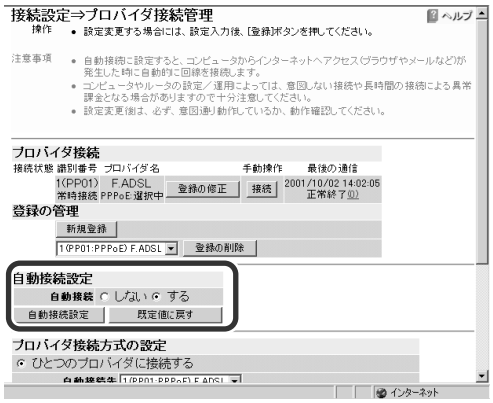
接続方法で[自動切断する]を設定した場合は

手動切断しなくても、一定時間インターネットへアクセスしないと、自動的にプロバイダとの接続が切れます。

ヒント

フレッツ·ADSLは定額料金制なので、発信制限は自動設定されません。

17 **[自動接続設定]が[する]になっていて、[自動接続先]に登録したプロバイダが選ばれていることを確認する。**



これで、PPPoEネットワーク型ADSLの接続設定は完了です。

ルータを正しく認識しないときは

パソコンのIPアドレスをリセットしてください。詳しくは、「IPアドレスをリセットする」(98ページ)をご覧ください。

◆ 使用できるIPアドレスについて

プロバイダから割り当てられたIPアドレスのうち、始めの番号はネットワークアドレス、最後の番号はブロードキャストアドレスに割り当てる規則になっているため、使うことができません。

例えば、「172.16.128.112/28」のIPアドレスを割当てられた場合、割当てられた番号は「172.16.128.112」～「172.16.128.127」の16個ですが、

172.16.128.112＝ネットワークアドレス
172.16.128.113
:
172.16.128.126
172.16.128.127＝ブロードキャストアドレス

になりますので、実際にルータやパソコンに割り当てられる番号は、「172.16.128.113」～「172.16.128.126」の14個となります。

外部にサーバを公開する

インターネットへサーバを公開したい場合は、公開したいサーバに固定プライベートIPアドレスを設定してから、静的IPマスカレードを使用してサーバのIPアドレスとグローバルIPアドレスの関連付けを設定します。

このあとに本機にLAN外からのアクセスを許可するフィルタを設定することで、インターネットからアクセスすることができるようになります。

ご注意

LANの外部にサーバを公開するときは、データを保全するために十分なセキュリティ設定を行ってください。セキュリティ設定が不十分の場合は、双方のLANに接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などにあう可能性があります。

◆ 必要な設定

サーバを公開するためには、次の設定が必要です。

ルータの設定

- 静的IPマスカレードの設定を変更する(83ページ)
- アクセスを許可する設定に変更する(84ページ)

サーバの設定

- パソコンのIPアドレスを設定する(84ページ)
- ファイルサーバソフトの設定を変更する(84ページ)

静的IPマスカレードの設定を変更する

サーバに設定した固定プライベートIPアドレスとサーバに割り当てたグローバルIPアドレスの関連づけを設定します。これにより、インターネット側からサーバのアドレスを指定することができるようになります。

ここでは、LAN内のサーバ(192.168.11.20)にグローバルIPアドレス(10.40.33.114)を割り当てる例を説明します。静的NATの設定は、「かんたん設定ページ」の「ネットワーク型プロバイダ接続」画面で行います。

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス(工場出荷時は192.168.0.1)を入力して開きます。

「ネットワーク パスワードの入力」画面が表示されます。

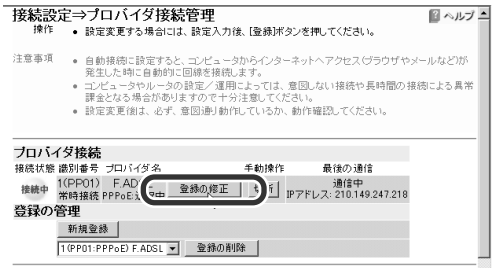
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

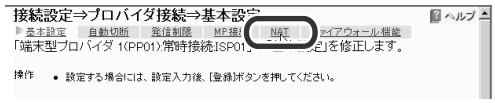
3 **[接続設定]をクリックする。**

4 **[プロバイダ接続管理]をクリックする。**

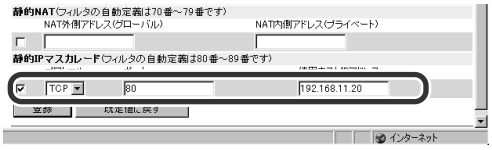
5 **接続先の[登録の修正]をクリックする。**



6 **[NAT]をクリックする。**



7 **[静的IPマスカレード]をチェックしてから、入力欄にプロトコルとポート番号、公開するサーバのプライベートIPアドレスを入力する。**



8 **画面下にある[登録]をクリックする。**

メッセージにしたがってボタンをクリックすると、設定が変更されます。

アクセスを許可する設定に変更する

LAN側で、アクセスを許可するサーバのプライベートIPアドレスや通信プロトコルを設定します。その他のパソコンは、外部からアクセスすることはできないことになります。ここでは、LAN内のサーバ（192.168.11.20）へのアクセスを許可する場合を例に説明します。

1 **83ページの手順1〜2を行い、本機の「かんたん設定ページ」のトップページを開く。**

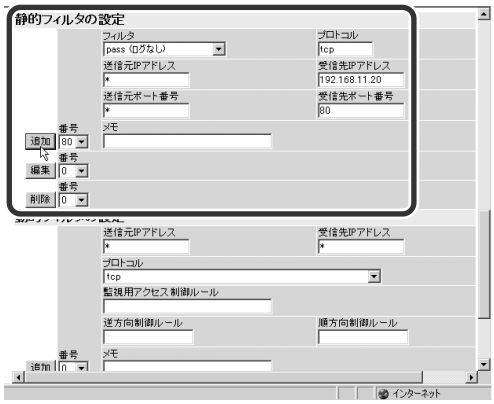
2 **[付加機能]をクリックする。**

3 **[ファイアウォール機能]をクリックする。**

4 **[静的フィルタ設定]で下記の値を入力し、[追加]をクリックする。**

ポート番号などのフィルタの設定について詳しくは、「フィルタを設定する」（65ページ）をご覧ください。

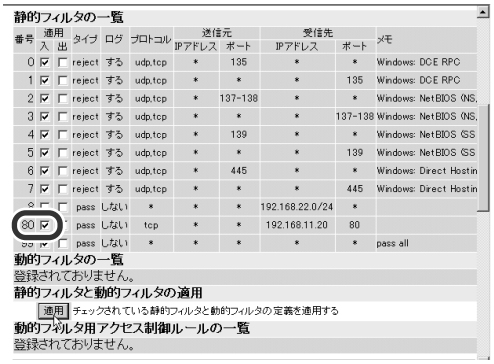
Webサーバを公開する場合の入力例



ご注意

- セキュリティフィルタが適用されている場合は、フィルタ番号80番〜89番にすでに静的IPマスカレード用のフィルタが自動設定されています。
- 公開する相手を限定したい場合は、始点IPアドレスに相手のIPアドレスを指定します。
- ポート番号は利用したいサーバアプリケーションが使用するプロトコルに合わせて変更してください。
- 使用できるフィルタ番号は、各接続先毎に0〜99の100個です。フィルタやプロトコルなどについて詳しくは、「コマンドリファレンス」をご覧ください。

5 **[静的フィルタ設定]で追加したフィルタの[入]をチェックしてから、[適用]をクリックする。**



パソコンのIPアドレスを設定する

外部からのアクセスを許可するサーバまたはパソコンには、固定プライベートIPアドレスを設定します。設定方法について詳しくは、「パソコンのIPアドレスを管理する」（93ページ）をご覧ください。

ファイルサーバソフトの設定を変更する

公開するサーバまたはパソコンにサーバアプリケーションをインストールしてから、公開するフォルダやユーザID、パスワードを設定します。設定の方法については、各ソフトウェアの取扱説明書をご覧ください。

ネットワークゲームやICQ用に設定する

ネットワークゲームやICQなどのグローバルIPアドレスを使ったサービスは、ルータでは正しく動作しない場合があります。この場合は、本機にグローバルIPアドレスとプライベートIPアドレスの関連付け（静的IPマスカレード）の設定を行うことで、問題が解決する場合があります。

ご注意

以下の設定を行っても正しく動作しない場合は、ブロードバンドTA機能で接続してください（35ページ）。

◆ 必要な設定

静的IPマスカレードを設定するためには、次の設定が必要です。

- パソコンのIPアドレスを設定する
- 静的IPマスカレードの設定を変更する

パソコンのIPアドレスを設定する

お互いのLAN上のサーバまたはパソコンで外部からのアクセスを許可するパソコンには、固定プライベートIPアドレスを設定します。設定方法について詳しくは、「パソコンのIPアドレスを管理する」（93ページ）をご覧ください。

静的IPマスカレードの設定を変更する

1台のパソコンの静的マスカレードを設定する場合は、「かんたん設定ページ」の「プロバイダ接続設定」画面で行います。

1 **Webブラウザを起動して、本機の「かんたん設定ページ」を開く。**

「http://setup.netvolante.jp/」または本機のIPアドレス（工場出荷時は192.168.0.1）を入力して開きます。

「ネットワーク パスワードの入力」画面が表示されます。

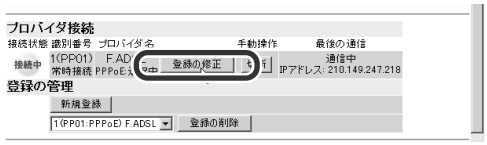
2 **［パスワード］入力欄にルータの管理パスワードを入力してから、［OK］をクリックする。**

「トップ」画面が表示されます。

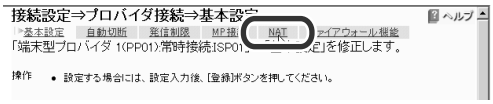
3 **［接続設定］をクリックする。**

4 **［プロバイダ接続管理］をクリックする。**

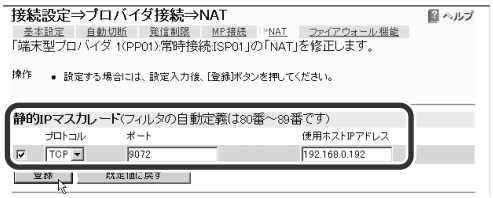
5 **接続先名の右の［登録の修正］をクリックする。**



6 **［NAT］をクリックする。**



7 **［静的IPマスカレード設定］をチェックしてから、プロトコルを選んでポート番号とパソコンのIPアドレスを入力する。**



ご注意

プロトコルやポート番号については、利用するソフトウェアの取扱説明書をご覧ください。

8 **画面下にある［登録］をクリックする。**

メッセージにしたがってボタンをクリックすると、設定が変更されます。

第8章 困ったときは

この章では、本機がうまく動かないときや、トラブルが起きたときの対処方法について説明します。サポート窓口にお問い合わせになる前に、1度お読みください。「つながらない」や「使えない」といった基本的なトラブルについては、一番早い解決方法になるはずです。ネットワークに関連する、より専門的なトラブルや質問については、NetVolanteシリーズのホームページ（http://NetVolante.jp/）をご覧ください。

「困ったな」「故障かな？」と思ったら

本機の症状に応じて、以下のページをご覧ください。

インターネット上のホームページもご覧ください

また、本機に関する最新情報は、インターネットのホームページでも入手できます。設定に関する初歩的な情報からルータの専門的な情報まで、それぞれの目的別に用意していますので、十分ご活用ください。

詳しくは、「本機の最新情報を入手する」（99ページ）をご覧ください。

かんたん設定ページで設定できない

◆ LANランプが点灯しない

HUBやパソコンの電源は入っていますか？

➡ 電源が入っていることを確認してください。

LANポートに機器を正しく接続しても、接続した機器の電源が入っていないときは、本機のLANランプは点灯しません。

正しく接続されていますか？

➡ 本機側、パソコンおよびHUB側共にコネクタをいったん外してから、もう1度カチッとロックするまで差し込んでください。

お使いのケーブルは、LAN用のケーブルですか？

➡ ISDNケーブルのときは取り替えてください。コネクタ形状が全く同じなので注意が必要です。

➡ わからないときは、他のLANケーブルと取り替えてみてください。

◆ かんたん設定ページが開けない

LAN上の他のパソコンやネットワークプリンタは使用できますか？

➡ LANボードやLANカードの設定をやり直して再起動してください。

➡ Windowsの場合は、IPアドレスをリセットしてください(98ページ)。

➡ Macintoshの場合は、「TCP/IP」コントロールパネルの[経由先]を[Ethernet]、[設定方法]を[DHCPサーバを参照]に設定してから、設定を保存してください。

100BASE-TX対応のLANカードを使用していますか？

➡ LANカードを自動認識に設定してください。通信が不安定な場合は、10Mbit/sの半二重に固定してください。

ルータのIPアドレスを変更しましたか？

➡ 本機に設定したIPアドレス「http://(本機のIPアドレス)/」にアクセスしてください。

➡ 本機のIPアドレスを変更した場合は、本機とLANに接続しているすべてのパソコンを再起動してください。再起動または電源を切ることができないときは、パソコンを1台だけ本機に接続し、それ以外のLANケーブルを取り外してから、本機とパソコンの電源を入れてください。

➡ 本機のIPアドレスを変更した場合は、パソコンの設定が同じIPアドレス範囲になっていることを確認してください。また、他の機器とIPアドレスが重なっていないか確認してください。

ルータのURLは合っていますか？

➡ 本機を初めて使うときや工場出荷値にもどした後は、「http://192.168.0.1/」または「http://setup.netvolante.jp/」にアクセスしてください。

ブラウザの接続経路設定はLAN経由になっていますか？

➡ Windows版Internet Explorer5の場合、[インターネットオプション]の[接続]タブでダイヤルアップ接続をする設定になっていると、「かんたん設定ページ」にアクセスできません。[ダイヤルしない]に変更してください。

ブラウザでProxyサーバを使用していますか？

➡ プロキシの設定が正しくないと、「かんたん設定ページ」が表示できなくなります。

- **Internet Explorerの場合:** メニューから[ツール]→[インターネットオプション]→[接続]タブ→[LANの設定]を開き、[プロキシサーバーを使用する]のチェックをはずします。
- **Netscape Navigatorの場合:** メニューから[編集]→[設定]→ カテゴリの[詳細]の[+]をクリック→[プロキシ]を選び[プロキシ]の設定を開き、[インターネットに直接接続する]にチェックを付けます。

Webブラウザを用いて遠隔操作していますか？

➡ IPアドレスによるアクセス制限機能が働いていると、許可されていないホストからのアクセスに対しては、「Error 503 This server is available to members only. I'm sorry, your host is not member.」と表示されます。

「かんたん設定ページ」の[システム管理]－[ルータ設定]－[HTTPサーバの利用ホスト制限]画面で、現在のホストのIPアドレスからの利用が許可されるように設定してください。

◆ かんたん設定ページのパスワードが通らない

「かんたん設定ページ」を一度も開いていませんか？

➡ 「本機の設定を工場出荷状態に戻す」(93ページ)を行ったあと、もう一度、パスワードの設定からやり直してください。パスワードは大文字と小文字も区別しますので、設定したパスワードを間違えないように入力してください。

かんたん設定ページで設定できない

パスワードは設定されていますか？

➡ 本機の設定を行ったルータ管理者にご相談ください。

➡ 設定したパスワードを忘れてしまったときは、「パスワードを忘れてしまった」(92ページ)をご覧ください。

パスワードエラーが表示されますか？

➡ パスワードは、全角／半角や大文字／小文字の違いも区別します。必ず半角の英数字で大文字／小文字も正確に入力してください。

➡ ブラウザ認証情報(ユーザ名、パスワード)が残っていると、それを自動的に送信するため、エラーになります。ユーザ名を削除してからパスワードを入力し直すか、ブラウザをいったん終了してから「かんたん設定ページ」を開き直してください。

◆ 設定内容が元にもどってしまう

プロバイダの設定を行ったときに[登録]をクリックしましたか？

➡「かんたん設定ページ」で設定を変更したときは、必ず[登録]をクリックして設定を保存してください。[登録]をクリックせずに画面を閉じると、設定内容は保存されません。

◆ かんたん設定ページを開く際にWebブラウザにパスワードが保存されない

ネットワークパスワードの入力のダイアログでユーザ名が空欄になっていますか？

➡ 通常はユーザ名は空欄でかまいませんが、Webブラウザによっては、パスワードを保存するためにユーザ名入力が必要な場合があります。この場合は、任意の文字列を入力してください。

インターネットに接続できない

インターネットへ接続できないときは、次の順序で症状を確認して該当する項目の対処を行ってください。

◆ プロバイダに接続できない

お使いのパソコンから「かんたん設定ページ」を開けますか？

➡ パソコンを再起動してください。

➡ Windowsの場合は、IPアドレスをリセットしてください(98ページ)。

本機に自動接続先のプロバイダ情報を登録しましたか？

➡「かんたん設定ページ」で接続するプロバイダの情報を設定してください。

➡「かんたん設定ページ」で自動接続設定をオンにし、接続するプロバイダを選んでください。

◆ プロバイダにはつながっているがホームページが表示されない、または表示が非常に遅い

プロバイダ設定のDNSサーバアドレスは合っていますか？

➡ 本機をルータとして使用している場合は、本機のプロバイダ接続設定にDNSサーバアドレスが設定されているか確認してください。

➡ 本機をルータとして使用している場合は、各パソコンのDNSサーバアドレス設定に本機のIPアドレスを入力してから、パソコンを再起動してください。

➡ WebサーバやDNSサーバが混雑または運休している可能性があります。しばらく時間をおいてから、アクセスし直してください。

プロバイダから与えられたIPアドレスはプライベートアドレスですか？

➡ ファイアウォールなどのセキュリティフィルタを適用している場合は、以下の方法でIngressフィルタの適用を外してください。

- **変更例1:** [プロバイダ接続管理] − [登録の修正]画面で、Ingressフィルタを含まないセキュリティレベルに設定します。
- **変更例2:** ファイアウォール機能の設定で、静的フィルタの 0,1,2,10,11,12の適用を外します。

プロバイダから与えられたIPアドレスとルータに設定されているIPアドレスが重複していませんか？

➡「LAN/WAN設定」画面で、ルータのIPアドレスをプロバイダから与えられたものと重複しないアドレスに変更してください。この場合、ファイアウォール機能は適用し直す必要があります。

PPPoE方式で接続していますか？（PPPoE方式ADSL接続時のみ）

➡ ADSL回線の種類によっては、標準的な設定のままでは、一部のホームページのデータが受信できないか、データの受信が非常に遅くなることがあります。

いったん接続を切断してから、「プロバイダ接続管理」画面のPPPoE方式のプロバイダの［登録の修正］でMTUに1454などの値を設定して、接続し直してください。

回線やプロバイダ、Webサーバが混雑していませんか？

➡ 時間帯などによっては非常に遅くなる場合があります。回線速度に比べて非常に遅い状態が続く場合は、ご利用の回線業者やプロバイダにお問い合わせください。

◆ WAN LINKランプが点灯しない

WANランプは点灯していますか？

➡ 点灯していない場合は、「WANランプが点灯しない」をご覧ください。

PPPoE方式で接続しようとしている場合は、本機で設定したユーザー名やパスワードの設定を確認してください。

◆ WANランプが点灯しない

ADSLモデムやケーブルモデムの電源は入っていますか？

➡ 電源を入れてください。

正しく接続されていますか？

➡ 本機のWANポートおよびADSLモデムやケーブルモデムの電源をいったん外してから、もう1度カチッと音がするまで差し込んでください。

正しいケーブルをお使いですか？

➡ お使いのADSLモデムやケーブルモデムとパソコンを接続するものと同じタイプのケーブルをお使いください。

◆ ルータやPCで、NTPサーバを使った時刻合せができない

NTPサーバのIPアドレスやドメイン名は正しいですか？

➡ 入手したNTPサーバ情報と比較し、正しく設定されていることを確認してください。また、NTPサーバに対してpingを実行し、稼動していることを確認してください。

登録されているNTPサーバへの経路が設定されていますか？

➡ プロバイダ設定や経路設定を確認してください。

セキュリティフィルタが適用されていませんか？

➡ セキュリティフィルタでNTPのポートが制限されている場合は、NTPポートを通す（Pass）フィルタを適用してください。

無線LANがつながらない

無線LANカード(またはボード／アダプタ)は正常ですか？

➡ 無線LANカード(またはボード／アダプタ)の取扱説明書を読んで、正常に動作していることを確認してください。

ESS-ID、WEPの設定は本機とパソコンとで合っていますか？

➡ ルータのESS-ID、WEPの設定値を確認してください。

➡ 各パソコンのESS-ID、WEPの設定値を確認してください。

➡ 本機をリセットして、設定を最初からやり直してください。

チャネルの設定はルータとパソコンとで合っていますか？

➡ 無線LANカード(またはボード／アダプタ)によっては、14チャネルすべてが使えないものがあります。お使いの無線LANカード(またはボード／アダプタ)で使用できるチャネルに合わせて、本機のチャネル設定値を変更してください。

MACアドレス制限機能が設定されていますか？

➡ ルータに接続したいパソコンのMACアドレスを登録してください(55ページ)。

➡ MACアドレス制限機能が不要な場合は、ルータのMACアドレス制限機能を解除してください(55ページ)。

近隣で無線LANアクセスポイント機器を使っていませんか？

➡ 使っている場合や不明な場合は、チャネルを3つ以上離れたチャネルに設定し直してください。

接続確認が取れている無線LANカード(またはボード／アダプタ)を使っていますか？

➡ 使用可能な無線LANカード(またはボード／アダプタ)の最新の情報は、NetVolanteシリーズホームページで確認してください(99ページ)。

本機とパソコンの間に遮蔽物はありませんか？

➡ 本機やパソコンの位置や向きを変えて、電波状態の一番良い位置に設置してください。

➡ 電子レンジなど、電磁波を発生する機器が影響しない位置に本機やパソコンを移動してください。

➡ 外部アンテナを接続してください(58ページ)。

本機の無線モードが[オフ]に設定されていませんか？

➡ 本機の無線モードを[アクセスポイント]または[ステーション]に設定してください。

ブロードバンドTA機能で接続できない

◆ USBランプが点灯しない

本機やパソコン、途中のUSBハブの電源は入っていますか？

➡ USBランプは、本機とパソコンが正常に接続されている時のみ点灯／点滅します。いずれかの電源が入っていないと、点灯しません。

USBコネクタがしっかり接続されていますか？

➡ 不完全な場合はいったん外してから、もう1度コネクタの向きや形状を確認し、奥までしっかりと接続してください。本機側、パソコン側ともに確認してください。

USBケーブルやUSBハブに異常はありませんか？

➡ 別のUSB機器を接続して動作しない場合は、USBケーブルやUSBハブに断線や不具合がある可能性があります。他のUSBケーブルやUSBハブと交換してください。

◆ USBランプが点滅している

通信を行っていますか？

➡ 通信中は、USBランプが不規則に点滅します。これは、正常な動作です。

パソコンは起動していますか？

➡ パソコンの起動中や終了中は、USBランプがゆっくりと点滅します。パソコンが起動し終わるまでお待ちください。

➡ パソコンがサスペンド状態やスリープ状態になっている時はゆっくりと点滅することがあります。

本機が対応しているOSを使っていますか？

➡ USB経由で本機とパソコンを接続して使うには、Windows 98SE/Me/2000/XP、MacOS 9のOSが必要です。Windows 95/98、MacOS 8.6以前の場合は、OSをバージョンアップしてからお使いください。

Windowsパソコンの場合、USBドライバのインストールを途中でキャンセルしましたか？

➡ USBドライバのインストールを途中でキャンセルした場合は、[不明なデバイス]と認識され、USBランプがゆっくり点滅します。[コントロールパネル]－[システム]の[デバイスマネージャ]画面で黄色い ! マークの付いた「不明なデバイス」を削除してからパソコンを再起動して、USBドライバをもう1度インストールしてください(29ページ)。

Windowsパソコンの場合、USBドライバをインストールしましたか？

➡ USBドライバが正常にインストールできなかった場合や操作を間違った場合は、「USB互換デバイス」と誤認識され、USBランプがゆっくり点滅します。付属のUSBアンインストーラを実行してからパソコンを再起動して、USBドライバをもう1度インストールしてください(29ページ)。

Windowsパソコンの場合、USBポートは有効になっていますか？

➡ Windowsでは、USBポートが無効になっていると、USBランプがゆっくり点滅します。[コントロールパネル]－[システム]の[デバイスマネージャ]画面で[ユニバーサル シリアルバス コントローラ]を開き、[～Controller]や[USBルートハブ]に赤い✕マークや黄色い！マークが付いていないことを確認してください。

付いている場合は、パソコンまたはUSBインタフェースボードの取扱説明書に従って問題を解決してから、USBドライバをもう1度インストールしてください。

本機のUSBポートは有効になっていますか？

➡ 本機のUSBポートは、コンソールコマンドで有効/無効を設定することができます。LAN接続したパソコンのTELNETソフトウェアで以下のコンソールコマンドを実行し、本機のUSBポートを有効にしてください。

```
usb use on
save
```

◆ ブロードバンドTAで接続しようとするとエラー(青い画面など)になる

USBケーブルを抜き差ししましたか？

➡ ターミナルソフトやダイヤルアップネットワークソフト、ダイヤルアップサーバを使用中にUSBケーブルを抜き差しすると、Windowsが不安定になってエラーが発生します。パソコンを再起動してください。

本機の電源を入／切しましたか？

➡ ターミナルソフトやダイヤルアップネットワークソフト、ダイヤルアップサーバを使用中に本機の電源をオフにすると、Windowsが不安定になってエラーが発生します。パソコンを再起動してください。

本機をリセットしましたか？

➡ ターミナルソフトやダイヤルアップネットワークソフト、ダイヤルアップサーバを使用中に本機のリセットを行うと、Windowsが不安定になってエラーが発生します。パソコンを再起動してください。

◆ プロバイダにはつながっているが、ホームページが表示されない

ダイヤルアップ設定のDNS(ネームサーバ)のIPアドレスは合っていますか？

➡ Windowsではダイヤルアップネットワークの設定で、DNSサーバのIPアドレスをもう1度確認してください。DNSサーバのIPアドレスは、プロバイダから指定されたものを設定してください。

➡ Windowsではmodemlog.txtを開き、原因を確認してください。

➡ MacintoshではTCP/IPの設定で、DNSサーバのIPアドレスをもう1度確認してください。DNSサーバのIPアドレスはプロバイダから指定されたものを設定してください。

➡ WebサーバやDNSサーバが混雑しているか、または運休している可能性があります。しばらく時間をおいてから、アクセスし直してください。

◆ プロバイダにはつながっているが、動作が不安定になる

オーディオ機器やTA、LANアダプタなど、高い負荷がかかるUSB機器を同時に使用していますか？

➡ USB接続のオーディオ機器やTA、LANアダプタなどを同時に使用すると、高い負荷がかかり、通信が不安定になります。これらの機器とは、同時に使わないでください。

➡ パソコンにUSBのルートが2系統ある場合は、これらのUSB機器を別のUSBポートに接続し直してください。

◆ プロバイダにつながらない

契約している事業者の接続方法はPPPoEに対応していますか？

➡ ブロードバンドTA機能はPPPoEに対応した事業者でのみ利用可能です。PPPoEに対応していないCATV/ADSL事業者ではご利用できません。

ブロードバンドTA機能で接続できない

◆ ブロードバンドTA接続すると、エラー（BUSY）になる

「broadband-ta forced disconnect off」に設定されていませんか？

➡「broadband-ta forced disconnect off」に設定されていると、ルータのADSL接続が優先されます（工場出荷状態では「broadband-ta forced disconnect on」に設定されています）。ブロードバンドTA接続を優先させるには、「かんたん設定ページ」−「システム管理」−「コマンド設定」画面で、以下のコマンドを実行してください。

```
broadband-ta forced disconnect on
```

◆ ルータとブロードバンドTA接続で、同時に別々のプロバイダに接続できない

契約しているADSL事業者（PPPoE方式のみ）は、複数の接続（セッション）をサポートしていますか？

➡ ADSL事業者が複数の接続（セッション）をサポートしていない場合は、ルータとブロードバンドTA接続で、同時に別々のプロバイダに接続できません。ADSL事業者が複数の同時接続をサポートしている場合には、ATコマンドで最大セッション数とコンセントレータ名（半角英数字）を指定してください。

例：2つの同時接続の場合

```
ATS56=2
AT@I/コンセントレータ名/
AT&W（保存）
```

パスワードを忘れてしまった

◆ ログインパスワードを忘れた場合は

管理パスワードでログインしてください。管理パスワードをLANの管理者が管理しているときは、LANの管理者にログインパスワードを再発行してもらいます。

◆ 管理パスワードを忘れた場合は

USBポート経由で接続したパソコンでターミナルソフトウェアを起動して、パスワード「w,lxlma」（ダブリュ、カンマ、エル、エックス、エル、エム、エー）を使ってログインできます。コンソールコマンドについては、「コンソールコマンドで設定する」（19ページ）をご覧ください。

ターミナルソフトウェアの使いかたに慣れていない場合は、「本機の設定を工場出荷状態に戻す」（このページ右側）の説明に従って、本機を工場出荷時の状態に戻してください。

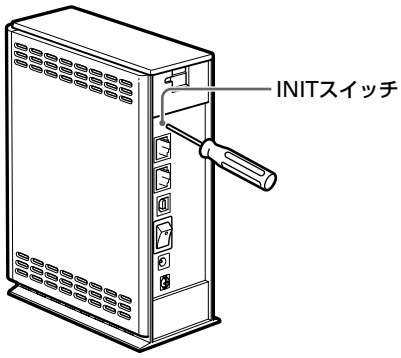
この場合は、それまでに設定した内容はすべて初期化されますので、最初から設定をやり直してください。

本機の設定を工場出荷状態に戻す

本機の設定内容を工場出荷設定に戻したいときは、次の操作を行ってください。

1 **本機の電源を切る。**

2 **INITスイッチを先の細いもので押しながら、電源を入れる。**



現在設定されている内容が、出荷時の設定内容にもどります。
それまでに設定した内容はすべて初期化されますので、最初から設定をやり直してください。

パソコンのIPアドレスを管理する

LANやインターネットへのアクセスができないときは、DHCPサーバによるLAN内IPアドレス自動割り当てで、IPアドレスが重複している場合があります。そのときは、次のような操作を行ってください。

ご注意

固定アドレスで重複している場合は、ネットワーク管理者にお問い合わせください。

現在のIPアドレスを確認する

◆ Windows 95/98/Meの場合

起動ディスクのWindowsフォルダ内にある[Winipcfg.exe]アイコンをダブルクリックして、使用中のLANカード名を選ぶ。

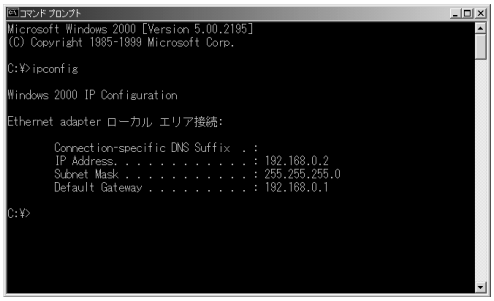
現在パソコンに割り当てられているIPアドレスが表示されます。

◆ Windows 2000/XPの場合

Windows2000の場合を例にして説明していますが、WindowsXPでも操作は同じです。

1 **[スタート]ボタンをクリックして、[プログラム]－[アクセサリ]－「コマンドプロンプト」をクリックする。**

2 **「ipconfig」と入力してから、Enterキーを押す。**

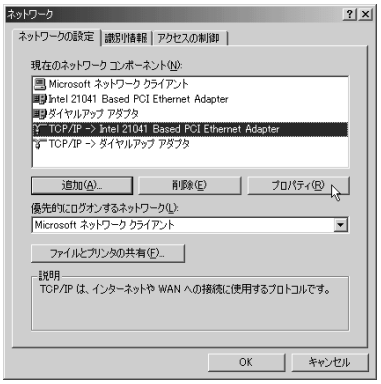


現在パソコンに割り当てられているIPアドレスが表示されます。

IPアドレスを変更する

◆ Windows95/98/Meの場合

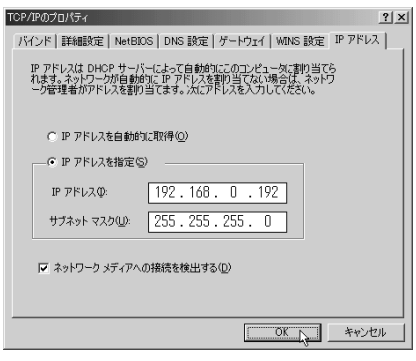
1 [マイコンピュータ]の[コントロールパネル]の[ネットワーク]を開いてから、リストの中の[TCP/IP->(ネットワークカードの名称)]を選び、[プロパティ]をクリックする。



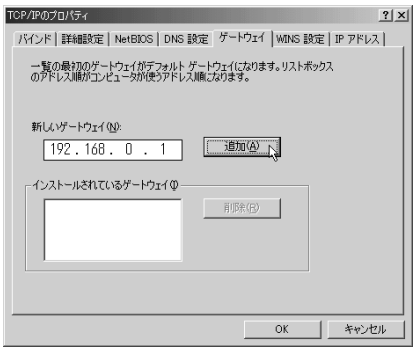
2 [IPアドレス]タブをクリックして、[IPアドレスを指定]を選ぶ。

3 IPアドレスとネットマスク欄に、パソコンに割り当てるIPアドレスとネットマスクを入力する。

本機のIPアドレスが工場出荷状態の場合は、パソコンには192.168.0.192～192.168.0.254の範囲でIPアドレスを設定します。



4 [ゲートウェイ]タブをクリックして、[新しいゲートウェイ]に本機のIPアドレス(工場出荷状態では192.168.0.1)を入力してから、[追加]をクリックする。



5 [DNS設定]タブをクリックしてから、[DNSを使う]を選ぶ。

6 [ホスト名]にWindowsパソコンの名前、[ドメイン]に接続するプロバイダのドメイン名、[DNSサーバーの検索順]に本機のIPアドレス(工場出荷設定では192.168.0.1)を入力してから、[追加]をクリックする。

7 [OK]をクリックして、メッセージに従ってパソコンを再起動する。

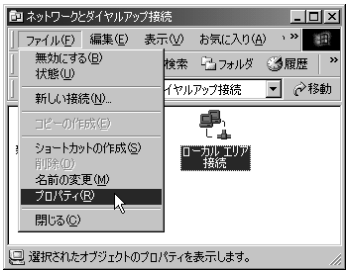
8 LAN上のすべてのWindows95/98/Meパソコンに対して手順1～7の操作を繰り返し、すべてのWindowsパソコンが異なるIPアドレスを持つように設定する。

◆ Windows2000の場合

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

2 [ネットワークとダイヤルアップ接続]をダブルクリックする。

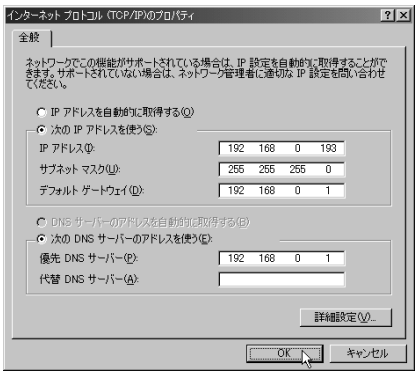
3 本機を接続しているネットワークボード名の[ローカルエリア接続]をクリックして選んでから、[ファイル]メニューから[プロパティ]を選ぶ。



4 リストの[インターネットプロトコル(TCP/IP)]を選んでから、[プロパティ]をクリックする。

5 [次のIPアドレスを使う]を選んでから、[IPアドレス]、[サブネットマスク]、[デフォルトゲートウェイ]にWindowsパソコンに割り当てるIPアドレスとネットマスクを入力する。

- 本機のIPアドレスが工場出荷状態の場合は、パソコンには192.168.0.192～192.168.0.254の範囲でIPアドレスを設定します。
- デフォルトゲートウェイは、本機のIPアドレス(192.168.0.1)を設定します。



6 [次のDNSサーバーのアドレスを使う]を選んでから、[優先DNSサーバー]に本機のIPアドレス(工場出荷設定では192.168.0.1)を入力する。

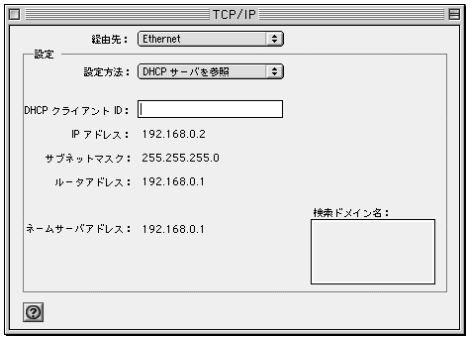
7 [OK]をクリックして、メッセージに従ってパソコンを再起動する。

8 LAN上のすべてのWindows2000パソコンに対して手順1～7の操作を繰り返し、すべてのWindowsパソコンが異なるIPアドレスを持つように設定する。

◆ Mac OSの場合

コントロールパネルの[TCP/IP]を開く。

現在パソコンに割り当てられているIPアドレスが表示されます。



◆ Mac OS Xの場合

1 アップルメニューから[システム環境設定]を選ぶ。

2 [ネットワーク]をクリックする。

現在パソコンに割り当てられているIPアドレスが表示されます。

◆ WindowsXPの場合

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

2 [ネットワークとインターネット接続]をクリックする。

3 [ネットワーク接続]をクリックする。

4 [ローカルエリア接続]のアイコンをクリックする。

5 [この接続の設定を変更する]をクリックする。

6 [インターネットプロトコル(TCP/IP)]を選んでから、[プロパティ]をクリックする。

7 [次のIPアドレスを使う]を選んでから、[IPアドレス]、[サブネットマスク]、[デフォルトゲートウェイ]にWindowsパソコンに割り当てるIPアドレスとネットマスクを入力する。

- 本機のIPアドレスが工場出荷状態の場合は、パソコンには192.168.0.192～192.168.0.254の範囲でIPアドレスを設定します。
- デフォルトゲートウェイは、本機のIPアドレス(192.168.0.1)を設定します。。

8 [次のDNSサーバーのアドレスを使う]を選んでから、[優先DNSサーバー]に本機のIPアドレス(工場出荷設定では192.168.0.1)を入力する。

9 [OK]をクリックして、メッセージに従ってパソコンを再起動する。

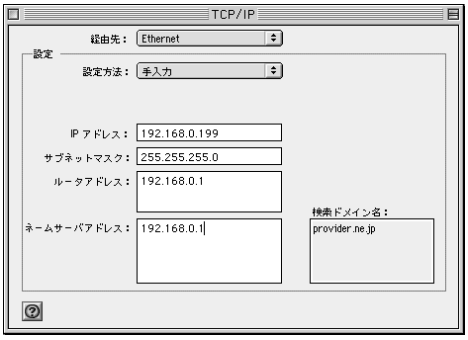
10 LAN上のすべてのWindowsXPパソコンに対して手順1～7の操作を繰り返し、すべてのWindowsパソコンが異なるIPアドレスを持つように設定する。

◆ Mac OSの場合

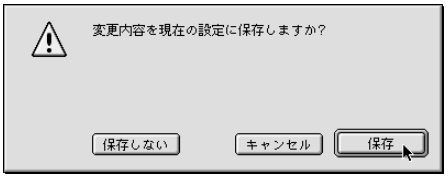
1 アップルメニューから[コントロールパネル]ー[TCP/IP]を選ぶ。

2 以下のように設定してから、ウィンドウを閉じる。

- **経由先:** Ethernet
- **設定方法:** 手入力
- **IPアドレス:** 割り当てるIPアドレス。本機のIPアドレスが工場出荷状態の場合は、パソコンには192.168.0.192～192.168.0.254の範囲でIPアドレスを設定します。
- **サブネットマスク:** ネットマスク
- **ルータアドレス、ネームサーバアドレス:** 本機のIPアドレス(工場出荷設定では192.168.0.1)
- **検索ドメイン名:** 接続するプロバイダのドメイン名



3 確認のダイアログが表示されたら、[保存]をクリックする。



4 LAN上のすべてのMac OSパソコンに対して手順1～3の操作を繰り返し、すべてのMac OSパソコンが異なるIPアドレスを持つように設定する。

◆ Mac OS Xの場合

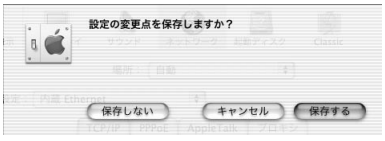
1 アップルメニューから[システム環境設定]を選ぶ。

2 [ネットワーク]をクリックする。

3 以下のように設定してから、ウィンドウを閉じる。

- **経由先**:Ethernet
- **設定方法**:手入力
- **IPアドレス**:割り当てるIPアドレス。本機のIPアドレスが工場出荷状態の場合は、パソコンには192.168.0.192～192.168.0.254の範囲でIPアドレスを設定します。
- **サブネットマスク**:ネットマスク
- **ルータ、ドメインネームサーバ**:本機のIPアドレス(工場出荷設定では192.168.0.1)
- **検索ドメイン名**:接続するプロバイダのドメイン名

4 確認のダイアログが表示されたら、[保存する]をクリックする。



5 LAN上のすべてのMac OS Xパソコンに対して手順1～4の操作を繰り返し、すべてのMac OS Xパソコンが異なるIPアドレスを持つように設定する。

IPアドレスをリセットする

◆ Windows95/98/Meの場合

1 起動ディスクのWindowsフォルダ内にある[Winipcfg.exe]アイコンをダブルクリックする。

2 LANカード名を選び、[解放]をクリックする。

現在パソコンに割り当てられているIPアドレスが表示されます。

3 [書き換え]をクリックする。

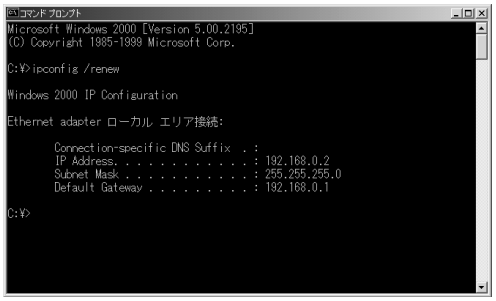
他のパソコンと重複しないプライベートIPアドレスに更新されます。

◆ Windows2000/XPの場合

Windows2000の場合を例にして説明していますが、WindowsXPでも操作は同じです。

1 [スタート]ボタンをクリックして、[プログラム]－[アクセサリ]－「コマンドプロンプト」をクリックする。

2 「ipconfig/renew」と入力してから、Enterキーを押す。



他のパソコンと重複しないプライベートIPアドレスに更新されます。

◆ Mac OS/Mac OS Xの場合

Macintoshを再起動する。

割り当てられていたプライベートIPアドレスがリセットされます。

ヒント

コントロールパネルの［TCP/IP］を開いて経由先を［Ethernet］以外に設定して保存し、もう一度コントロールパネルの［TCP/IP］を開いて経由先を［Ethernet］に設定し直すことで、DHCPサーバから割り当てられたプライベートIPアドレスをリセットすることもできます。

本機の最新情報を入手する

本機に関する最新情報は、インターネットのホームページで入手できます。設定に関する初歩的な情報からルータの専門的な情報まで、それぞれの目的別に用意していますので、十分ご活用ください。

◆ NetVolanteシリーズのホームページ

本機やNetVolanteシリーズに関する最新情報をご覧いただけます。

http://NetVolante.jp/

◆ NetVolanteシリーズでお問い合わせの多い質問（FAQ）

本機やNetVolanteシリーズに関するQ&Aをご覧いただけます。

http://www.rtpro.yamaha.co.jp/RTW65b/FAQ/

◆ NetVolanteシリーズのリビジョンアップ情報

本機やNetVolanteシリーズの最新ファームウェアに関する情報をご覧いただけます。

http://www.rtpro.yamaha.co.jp/RTW65b/RevUpper.html

◆ RTシリーズのホームページ

RTシリーズのルータに関する最新情報やルータの技術情報、高度な利用方法などをご覧いただけます。

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

最新機能を使う（リビジョンアップ）

NetVolanteシリーズのホームページから、本機の機能を管理するプログラム（ファームウェア）をダウンロードして本機に転送することで、本機の最新の機能をご利用いただけます（リビジョンアップ）。

リビジョンアップは次の手順で行います。ここでは、Windows98を例に説明しています。

ご注意

- リビジョンアップを始めたら、完了して本機が再起動するまで絶対に何も操作をしないでください。万一、中断したときは本機が使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- RT-RevUpper（リビジョンアップ・プログラム）をダウンロードするためには、インターネットへの接続が必要です。
- リビジョンアップが完了すると、本機は自動的に再起動されるため、すべての通信が切断されます。
- 工場出荷時に搭載されているファームウェアのリビジョンより古いリビジョンのファームウェアは使用しないでください。

1 パソコンでWebブラウザを起動して、「http://www.rtpro.yamaha.co.jp/RTW65b/RevUpper.html」とアドレス入力欄に入力してから、Enterキーを押す。

本機のリビジョンアップ情報のホームページが表示されます。

2 リビジョンアップの内容をよく読み、お使いのOS用のRT-RevUpper（リビジョンアップ・プログラム）をパソコンにダウンロードする。

WindowsおよびMacintosh以外のOSや、RT-RevUpperが正しく動作しない場合は

tftp用バイナリファイルをダウンロードし、「かんたん設定ページ」の「システム管理」－「コマンド設定」画面のコマンド入力で「tftp host any」を実行してから、tftpソフトウェアを使ってtftp用バイナリファイルを転送してください。

3 ダウンロードしたRT-RevUpper（リビジョンアップ・プログラム）のアイコンをダブルクリックする。

ご注意

RT-RevUpperを開く前に、RTAssistやTELNETなどのルータにアクセスしているプログラムを終了してください。

4 リビジョンアップするルータのIPアドレスを確認してから、［開始］をクリックする。

複数のRTW65bを使用している場合は、リビジョンアップするルータのIPアドレスを選んでください。

指定したIPアドレスを検索し、リビジョンアップ可能なルータの場合は、パスワード入力画面が表示されます。

ご注意

必ずRTW65bのIPアドレスを選んでください。
誤って他機種のIPアドレスを選ぶと、そのルータが使えなくなることがあります。その場合は、持ち込み修理が必要となります。

5 ルータのパスワードを入力してから、［実行］をクリックする。

リビジョンアップが始まります。
リビジョンアップが完了すると、本機は自動的に再起動します。

ご注意

リビジョンアップ中は、絶対にケーブルを抜いたり、本機やパソコンの電源を抜いたりしないでください。ルータが使えなくなり、持ち込み修理が必要となる場合があります。

6 **本機が再起動したら、[終了]をクリックする。**

7 **パソコンでWebブラウザを起動して、本機の「かんたん設定ページ」にアクセスしてリビジョンを確認する。**

リビジョン番号は、「かんたん設定ページ」のタイトルバーやトップ画面、「システム管理」の[コマンド設定]画面、またはRTAssistの[ルータ情報]で確認できます。

サポートとサービス

本機の保証サービスについて

本機や本機の付属品に不良があった場合は、すぐにご購入の販売店へご連絡ください。また、通常のご使用で故障が発生した場合は、保証期間中は無償にて修理いたします。ご購入の販売店またはヤマハサービス窓口へご連絡ください。また保証期間後は、有料にて修理いたします。

なお、保証期間中の修理には、保証書が必要です。ご購入時に「お買い上げ年月日」と「販売店名」の記入をご確認の上、保証書をお受け取りください。保証書がない場合は、保証期間内であっても有料となります。

保証期間：ご購入から1年間

ご質問・お問い合わせについて

本機に関する技術的なご質問やお問い合わせは、下記へご連絡ください。

◆ ネットボランチコールセンター

RTW65b専用サービス窓口
TEL:　03-5715-0350
（土日祝日を除く9時～12時、13時～17時）

◆ 電子メールでのお問い合わせ

- Webお問い合わせページ：
  http://NetVolante.jp/
- メールアドレス：
  support@netvolante.jp

第9章 その他の情報

付録では、CD-ROMに収録されているマニュアルを読むためのソフトウェアのインストール方法や本機の仕様、用語集を収録しています。

Acrobat Readerについて

付属のCD-ROMに収録されているPDF形式の説明書を読むときは、「Acrobat Reader」が必要です。パソコンにインストールされていない場合は、付属のCD-ROMからAcrobat Readerをインストールしてください。

Acrobat Readerをインストールする

◆ Windows 95/98/Me/2000/XPの場合

付属のCD-ROMをパソコンにセットしてから、CD-ROMドライブ内の[Utility]ー[Acrobat]フォルダの[ar500jpn]をダブルクリックする。

インストーラのウィンドウが開いたら画面のメッセージに従い、Acrobat Readerをインストールします。

◆ Macintoshの場合

付属のCD-ROMをパソコンにセットしてから、CD-ROMドライブ内の[ユーティリティ]ー[Adobe Acrobat Reader]フォルダの[Japanese Reader Installer]アイコンをダブルクリックする。

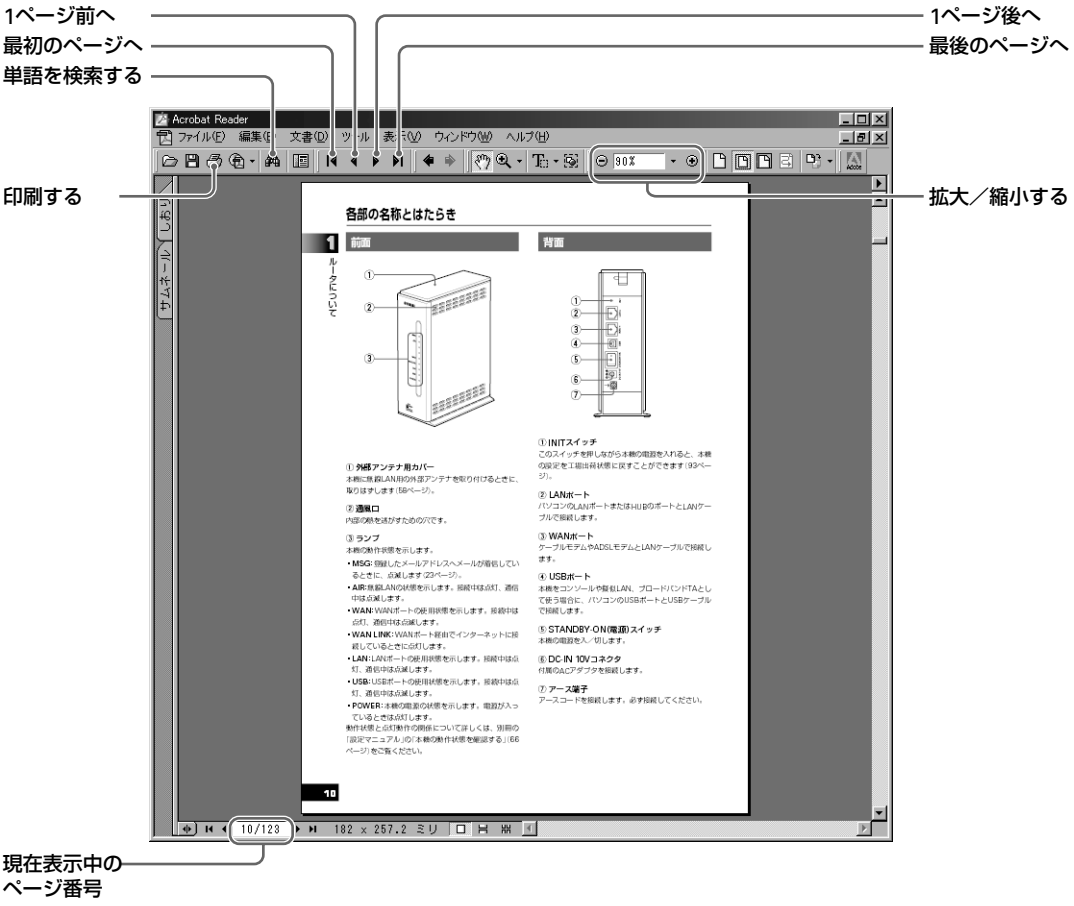
インストーラのウィンドウが開いたら画面のメッセージに従い、Acrobat Readerをインストールします。

Acrobat Readerの使いかた

本機の説明書は、Windows 95/98/Me/2000/XPではCD-ROMの［Manual］フォルダ、MacintoshではCD-ROMの［マニュアル］フォルダ内に収録されています。

PDF形式の説明書のアイコンをダブルクリックすると、「AcrobatReader」ウィンドウに説明書が表示されます。

Acrobat Readerには、次のような機能ボタンがあります。詳しい操作の説明については、Acrobat Readerのヘルプをご覧ください。



主な仕様

外形寸法(幅×高さ×奥行き、突起物を除く):
71 mm×184 mm×137 mm

質量:
本体:700 g
ACアダプタ:560 g

電源:AC100V(50/60Hz)

消費電力:
最大7 W

動作環境条件:
周囲温度 0〜40℃
周囲湿度 15〜85%(結露しないこと)

保管環境条件:
周囲温度 −10〜50℃
周囲湿度 10〜90%(結露しないこと)

LANインタフェース:
イーサネット10/100BASE-TX×1

WANインタフェース:
イーサネット10/100BASE-TX ×1

USBインタフェース:USBシリーズBコネクタ×1

無線インタフェース:
準拠規格:IEEE802.11b(11Mbit/s無線LAN)
RCR STD-33, ARIB STD-T66(小電力データ通信システム)
伝送方式:DS-SS方式単信(半二重)
伝送速度:1、2、5.5、11Mbit/s
周波数範囲:2400〜2497MHz
伝送距離:屋内約25m、屋外約50m(11Mbit/s時)
*伝送距離は遮蔽物や使用環境により短くなる場合があります。

表示機能:
LED×7(MSG、AIR、WAN、WAN LINK、LAN、USB、POWER)

付属品:
ACアダプタ P10V1.2A(1)
USBケーブル(1)
LANケーブル(1)
CD-ROM(1)
各種マニュアル
- はじめにお読みください(1)
- 設定マニュアル(1)
- 活用マニュアル(1)

切断コード一覧

0　通信中または正常切断

1　欠番
存在しない番号に発信した。相手先番号に間違いがある。

2　指定中継網へのルートなし
相手先番号への中継網が存在しないかサービスを提供していない。相手先番号に間違いがある。

3　相手へのルートなし
網が相手先番号へ着信を受け付けない。相手先番号に間違いがある。

6　チャネル利用不可
選択したBチャネルが使用できない。すでに2つのBチャネルが使用されている可能性がある。

16　正常切断

17　着ユーザビジー
発信した相手がすでに他の端末と通信中で通信できない。相手が話中。

18　着ユーザレスポンスなし
発信したが規定時間内に何の反応も返ってこなかった。相手の電源が切れているか、相手先番号が間違っている可能性がある。

19　着ユーザ呼出中／応答なし
発信した相手から呼出(ALERT)による反応があったが、その後規定時間内に応答の反応がなかった。相手先番号が間違っている可能性がある。

20　加入者不在
移動局と無線交信行なえない。相手の携帯電話などの電源が入っていないか圏外にいる。

21　通信拒否
何らかの理由で相手端末が着信を拒否した。ISDN関係のパラメータの不整合がある。相手先番号が間違っている可能性がある。また、相手側が着信可能な設定になっているか確認する。

22　相手加入者番号変更
相手の番号が変更されている。相手先番号に間違いがある。

26　選択されなかったユーザの切断復旧
着信に対して応答したが、他の端末の方が早く応答しており、自端末の応答は選択されなかった。

27 相手端末故障中
相手端末の電源OFFや故障、回線抜けなどにより相手インタフェースの起動不可。通信中に電源をいきなり落した時など。

28 無効番号フォーマット(不完全番号)
相手先番号に間違いがある。

30 状態問合せへの応答
網からの状態問合せに対する応答を示す。

31 その他の正常クラス

34 利用可回線／チャネルなし
利用可能な回線／Bチャネルがない。すでに 2 つのBチャネルが使用されている可能性がある。

38 網故障
網に比較的長時間続きそうな障害が発生した。しばらく使用を見合わせる必要がある。

41 一時的失敗
網に比較的長時間続きそうもない障害が発生した。再発信で接続できる可能性がある。

42 交換機輻輳
網に障害(交換機が高トラフィックで輻輳)が発生した。しばらく使用を見合わせる必要がある。

43 アクセス情報廃棄
網が要求されたアクセス情報を相手に届けることができなかった。しばらく使用を見合わせる必要がある。

44 要求回線／チャネル利用不可
要求した回線／Bチャネルが相手側のインタフェースで提供できない。すでに2つのBチャネルが使用されている可能性がある。

47 その他のリソース使用不可クラス

49 QOS(サービス品質)利用不可
要求されたQOS(Quality Of Service)が提供されない。(RT/RTAでは通常表示されない)

50 要求ファシリティ未契約
要求された付加サービスが提供されない。付加サービスに契約せずに、端末に付加サービスの設定がされている可能性がある。

57 伝達能力不許可
許可していない伝達能力が要求された。(RT/RTAでは通常表示されない)

58 現在利用不可伝達能力
利用不可である伝達能力が要求された。(RT/RTAでは通常表示されない)

63 その他のサービスまたはオプションの利用不可クラス

65 未提供伝達能力指定
サポートしていない伝達能力が要求された。(RT/RTAでは通常表示されない)

66 未提供チャネル種別指定
サポートしていないチャネル種別が要求された。(RT/RTAでは通常表示されない)

69 未提供ファシリティ要求
提供していない付加サービスが要求された。(RT/RTAでは通常表示されない)

70 制限ディジタル情報伝達能力のみ可能
非制限デジタルを要求されたが、制限ディジタルのみサポートしている(RT/RTAでは通常表示されない)

79 その他のサービスまたはオプションの未提供クラス

81 無効呼番号使用
使用中のものと異なる呼番号のメッセージを受信した。(RT/RTAでは通常表示されない)

82 無効チャネル番号使用
使用できないチャネル番号を要求した。(RT/RTAでは通常表示されない)

83 指定された中断呼識別番号未使用
中断された呼と異なる呼番号で再開しようとした。(RT/RTAでは通常表示されない)

84 中断呼識別番号使用中
再開の可能性がある呼に対して中断を要求した。(RT/RTAでは通常表示されない)

85 中断呼なし
再開の可能性のある呼以外の呼に対して再開を要求した。(RT/RTAでは通常表示されない)

86 指定中断呼切断復旧済
すでに切断した呼に対して再開を要求した。(RT/RTAでは通常表示されない)

88 端末属性不一致
端末属性が一致しない端末に発信した。またはそのような端末からの着信を受け取った。
相手先番号が間違っている可能性がある。例えば、自側が同期PPPで相手側がアナログモデムの場合のように、双方での端末属性の設定に不一致がある。

91 無効中継網選択
誤ったフォーマットの中継網識別を受信した相手先番号が間違っている可能性がある。

95 その他の無効メッセージクラス

96 必須情報要素不足
必要な情報要素が不足していた。不正な相手からの着信を受け取った。(RT/RTAでは通常表示されない)

97 メッセージ種別未定義または未提供
認識できないメッセージを受信した。不正な相手からの着信を受け取った。(RT/RTAでは通常表示されない)

98 呼状態とメッセージ不一致又は、メッセージ種別未定義又は未提供
網との間で状態の不一致が発生した。ルータを再起動する必要がある。

99 情報要素未定義
未定義の情報要素を受信した。(RT/RTAでは通常表示されない)

100 情報要素内容無効
情報要素の内容に誤りがある。(RT/RTAでは通常表示されない)

101 呼状態とメッセージ不一致
網との間で状態の不一致が発生した。ルータを再起動する必要がある。

102 タイマ満了による回復
レイヤ3でのタイムアウトが発生した。

111 その他の手順誤りクラス

127 その他のインタワーキングクラス

112 L2リンクの設定に失敗した
モジュラーケーブルの接続などを確認する必要がある。

545 相手が呼出中のまま応答せずにタイムアウトした
相手先番号が間違っている可能性がある。

548 コールバック手順に成功して相手からコールバックされるのを待っていたがタイムアウトした
相手先番号が間違っている可能性がある。

549 コールバック手順の中でタイムアウトした
相手先番号が間違っている可能性がある。

552 切断タイマ(isdn disconnect time)による切断
正常切断。

553 出力切断タイマ(isdn disconnect output time)による切断
正常切断。

554 入力切断タイマ(isdn disconnect input time)による切断
正常切断。

556 Fast Data 切断タイマ(isdn fast disconnect time)による切断
正常切断。

557 強制切断タイマ(isdn forced disconnect time)による切断
正常切断。

769 コールバックの応答がなかった
コールバック手順での問題。相手先番号が間違っている可能性がある。

770 コールバックの応答に失敗した
コールバック手順での問題。相手先番号が間違っている可能性がある。

772 回線コネクタ抜けにより発信失敗

774 再発信禁止条件により発信失敗
しばらくしてから再発信すれば接続できる。

780 累積課金による発信制限により発信失敗
通信履歴などで「意図しない接続」が行なわれていないことを確認後累積課金情報をクリアする。

781 累積接続時間による発信制限により発信失敗
通信履歴などで「意図しない接続」が行なわれていないことを確認後累積接続時間情報をクリアする。

782 累積発信回数による発信制限により発信失敗
通信履歴などで「意図しない接続」が行なわれていないことを確認後累積発信回数情報をクリアする。

783 AC電源断により発信失敗
バックアップ電池による動作中のため、発信できなかった。

848 PPPoE接続でサーバによりサービスを拒否された
要求したサービスがサーバにより拒否された。(RT/RTAでは表示されない)

849 PPPoE接続でサーバによりサービスを拒否された
サーバが高トラフィックで輻輳している可能性がある。

850 PPPoE接続で回復不能なエラーが発生した
ログに表示された理由のエラーが発生した。

851 PPPoE接続でPADIタイムアウト
接続先にサーバが存在しない。または、サーバまでの区間の回線状態が良くない可能性がある。

852 PPPoE接続でPADRタイムアウト
サーバまでの区間の回線状態が良くない可能性がある。

1025 PIAFS接続でネゴシエーション失敗
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある(相手と本機の間で、PIAFSの起動方式が一致していない可能性がある)。

1026 PIAFS接続でRTFが範囲を超えている
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある。

1027 PIAFS接続でT001タイムアウト
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある(相手と本機の間で、PIAFSの起動方式が一致していない可能性がある)。

1028 PIAFS接続でT002タイムアウト
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある(相手と本機の間で、PIAFSの起動方式が一致していない可能性がある)。

1029 PIAFS接続でT003タイムアウト
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある(相手と本機の間で、PIAFSの起動方式が一致していない可能性がある)。

1030 PIAFS接続でT101タイムアウト
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある。

1031 PIAFS接続でリンク解放受付K回送出済
相手がPIAFSに対応していないか、または無線区間を含む回線状態が良くない可能性がある。

1281 PPP手順においてLCPタイムアウト
設定誤りの可能性がある。

1282 PPP手順においてIPCPタイムアウト
設定誤りの可能性がある。

1296 コールバックによる接続が拒否された
設定誤りの可能性がある。

1297 相手による認証が拒否された
設定誤りの可能性がある。

1298 自分が認証を拒否した
設定誤りの可能性がある。

1299 相手の認証に失敗した
設定誤りの可能性がある。

1300 相手に認証させるのに失敗した
設定誤りの可能性がある。

1301 相手に認証させるのに失敗した回数が多すぎるため発信できない
設定誤りの可能性がある。

1302 相手の認証でタイムアウトした
設定誤りの可能性がある。

1303 相手に認証させるのにタイムアウトした
設定誤りの可能性がある。

1304 MPに失敗した回数が多すぎるため発信できない
設定誤りの可能性がある。

Webブラウザ設定ページ項目一覧

一般ユーザ用ページ

トップページ

手動接続と切断	• プロバイダ接続
通信の記録	• メール着信数 • メール転送履歴 • 通信履歴

管理者用ページ

[接続設定]

*の項目は、設定が登録されている場合に表示されます。

新規登録	• フレッツ·ADSLなどのPPPoEを使用したADSL接続設定 • CATVまたはPPPoEを使用しないADSL接続設定 • PPPoEを用いるネットワーク型ADSLインターネット • CATVインターネット、または、PPPoEを使用しないネットワーク型ADSLインターネット
プロバイダ接続管理*	• プロバイダ接続 • 登録の管理 • 自動接続設定 • プロバイダへの接続方式
LAN/WAN設定	• 基本設定 LANポート(LAN1)のIPアドレス設定 WANポート(LAN2)のIPアドレス設定 DHCPサーバ機能 DHCPスコープの管理 • 経路設定

[無線設定]

基本設定	• 無線モード • 詳細設定
接続状態	• 現在通信しているステーションのMACアドレス一覧
MACアドレスフィルタ設定	• MACアドレスの新規登録 • MACアドレスフィルタの一覧

[付加機能]

ファイアウォール機能	• FW設定 表示インタフェース 不正アクセス検知機能 静的フィルタの一覧 動的フィルタの一覧 静的フィルタと動的フィルタの適用 動的フィルタ用アクセス制御ルールの一覧 静的フィルタの設定 動的フィルタの設定 動的フィルタ用アクセス制御ルールの設定 • FW状態 表示インタフェース 不正アクセス検知機能の侵入履歴 動的フィルタの動作状態
メール機能	• メール着信確認とメール転送機能（メールサーバの登録） • メール通知機能

[システム管理]

ルータ設定	• ルータのパスワード設定 • HTTPサーバの利用ホスト制限 • TELNETサーバの利用ホスト制限 • 日付と時刻の設定 • ブザーの設定 • かんたん設定ページの表示形式
コマンド設定	• 表示スタイルの変更 • Config表示 • コマンド入力 • HTTPまたはTELNETによるアクセス
システムログ	• 表示スタイルの変更 • Syslog表示 • Syslog設定

ATコマンド一覧

ご注意

本機では有効でないコマンドもあります。

ATコマンド

A　着信に対して応答

実行例:

ATA

D　指定された相手に発信

実行例:

ATD031234567(03-123-4567へダイヤルする)

ATD031234567;(03-123-4567へのダイヤルを準備し、コマンドモードへ)

ATD031234567/123(03-123-4567、サブアドレス123へダイヤル)

ATDR031234567/123(03-123-4567/123 へコールバック要求する)

ATDN(再ダイヤルする)

ATDS=3(短縮3 番へダイヤルする)

E　コマンド入力に対するエコーの有無の指定

設定例:

ATE0(入力されたコマンドをエコーバックしない)

ATE1(入力されたコマンドをエコーバックする、工場出荷設定)

H　切断復旧処理の起動

実行例:ATH

I　製品情報等の表示

実行例:

ATI0(製品名を表示する)

ATI1(ファームウェアのリビジョンを表示する)

ATI2(製造メーカ名を表示する)

ATI3(診断情報等を表示する)

O　オンラインコマンドモードからオンラインデータ状態への遷移

実行例:ATO

Q　コマンド入力に対する応答の有無の指定

設定例:

ATQ0(入力されたコマンドに対する応答あり、工場出荷設定)

ATQ1(入力されたコマンドに対する応答なし)

S　S レジスタの値の表示

実行例:

ATS30?(Sレジスタ30の値の表示)

Sレジスタについて詳しくは、「Sレジスタの詳細」(113ページ)をご覧ください。

S　S レジスタの値の設定

設定例:

ATS30=0(Sレジスタ30の値を0に設定)

Sレジスタについて詳しくは、「Sレジスタの詳細」(113ページ)をご覧ください。

V　リザルトコードと情報テキストの表示フォーマットの指定

設定例:

ATV0(数字形式(numeric form)で出力)

ATV1(文字形式(verbose form)で出力、工場出荷設定)

数字形式／文字形式の対応について詳しくは、リザルトコードセット表をご覧ください。

W　CONNECTの通信速度の指定

設定例:

ATW0(通信速度表示にはDTE速度を使用)

ATW2(通信速度表示には回線速度を使用(工場出荷設定)

X　CONNECTの通信速度表示とトーン検出の指定

設定例:

ATX0(通信速度表示なし、BT検出なし、DT検出なし)

ATX1(通信速度表示あり、BT検出なし、DT検出なし、工場出荷設定)

ATX2(通信速度表示あり、BT検出なし、DT検出あり)

ATX3(通信速度表示あり、BT検出あり、DT検出なし)

ATX4(通信速度表示あり、BT検出あり、DT検出あり)

詳しくはリザルトコードセット表をご覧ください。

Z　シリアルポートのリセットとユーザプロファイルの読み出し

実行例:ATZ

&C CD信号線の制御

設定例:

AT&C0(常時ON)

AT&C1(リモートDTEのRS信号(=受信キャリア)に応じて変化、工場出荷設定)

&D DTR信号のONからOFFへの変化に対する処理

設定例:

AT&D0(何もしない)

AT&D1(オンラインモードならばコマンドモードに遷移)

AT&D2(回線切断、工場出荷設定)

AT&D3(回線切断、シリアルポートのリセット)

&F 工場出荷設定に戻す

実行例:AT&F

&K DTEフロー制御

設定例:

AT&K0(なし)

AT&K1(RS/CSフロー制御、工場出荷設定)

AT&K2(XON/XOFFフロー制御)

&N CI信号線の制御

設定例:

AT&N0(着信中にON、工場出荷設定)

AT&N1(着信から通信終了までON)

AT&N2(着信中にON(1秒)とOFF(2秒)の繰り返し)

&Q 発信時のプロトコル選択

設定例:AT&Q1(非同期/同期PPP、工場出荷設定)

&R コンソールコマンド入力状態へ移行

実行例:AT&R

&S DSR 信号線の制御

設定例:

AT&S0(常時ON、工場出荷設定)

AT&S2(リモートDTEのDTR信号に応じて変化)

&V 現在のパラメータ内容の表示

設定例:AT&V(現在のパラメータとSレジスタの内容の表示)

&W 現在のパラメータをユーザプロファイルへ保存

実行例:AT&W

&Z 短縮番号の登録

短縮番号は0から9まで使用できます。

設定例:

AT&Z2=031234567(03-123-4567を短縮2番に登録)

AT&Z9=031234567/12(03-123-4567/12を短縮9番に登録

&Z 短縮番号の表示

実行例:

AT&Z(0～9の全ての登録番号表示)

AT&Z5(登録番号5の表示)

&Z 短縮番号の削除

短縮番号は0から9まで使用できます。

実行例:AT&Z3=(登録番号3の削除)

$A 直前の通信料金の取り出し

実行例:AT$A

$B 累積通信料金表示

実行例:AT$B

$C 直前の通信の切断コードの取り出し

実行例:AT$C

$D 累積通信料金の初期化

実行例:AT$D

$G グローバル着信の有無

設定例:

AT$G0(グローバル着信しない)

AT$G1(グローバル着信する、工場出荷設定)

$H 着信時におけるHLC による通信可能性確認の有無

設定例:

AT$H0(HLCが異なる端末からの着信は受け付けない)

AT$H1(HLCが異なる端末からの着信も受け付ける、工場出荷設定)

$I 自己アドレス登録時のサブアドレスなし着信の扱いの設定

設定例:

AT$I0(着信しない)

AT$I1(着信する、工場出荷設定)

$L 着信時のリザルトコードRING の表示形式

設定例:

AT$L0(発信アドレス情報なし、工場出荷設定)

AT$L1(発信アドレス情報あり)

$M MP機能使用の設定

設定例:

AT$M0(MP機能は使用不可、工場出荷設定)

AT$M1(MP機能は使用可)

$N スループットBODの設定

設定例:

AT$N0(スループットBODを使用しない、工場出荷設定)

AT$N1(スループットBODを 使用する)

$P 発信者番号通知の有無

設定例:

AT$P0(発信者番号を通知しない)

AT$P1(発信者番号を通知する、工場出荷設定)

$R コールバックの有無

設定例:

AT$R0(コールバック用の着信を受け付けない、工場出荷設定)

AT$R1(コールバック用の着信を受け付ける)

$S 識別着信の有無

設定例:

AT$S0(識別着信しない、工場出荷設定)

AT$S1(登録番号と一致時にその着信を拒否)

AT$S2(登録番号と一致時にその着信を許可)

AT$S5(番号通知のない着信を全て拒否)

$V 非同期/同期PPP変換での制御キャラクタの2バイト文字変換

設定例:

AT$V0(制御キャラクタを2バイト文字に変換しない、工場出荷設定)

AT$V1(制御キャラクタを2バイト文字に変換する)

$W識別番号の登録

識別番号は0から99まで使用できます。

設定例:

AT$W2=031234567(識別番号2を03-123-4567に登録)

AT$W6=031234567/2(識別番号6を03-123-4567/2に登録)

$W識別番号の表示

識別番号は0から99まで使用できます。

実行例:

AT$W2(識別番号2を表示)

AT$W(0〜99 の全ての登録番号表示)

$W識別番号の削除

識別番号は0から99まで使用できます。

実行例:AT$W2=(識別番号2を削除)

$Z 自己アドレスの登録

設定例:

AT$Z=031234567(自己アドレス03-123-4567)

AT$Z=031234567/9(自己アドレス03-123-4567/9)

$Z 自己アドレスの表示

実行例:AT$Z

$Z 自己アドレスの削除

実行例:AT$Z=

@A 擬似LAN接続用のダイヤル番号の登録

設定例:

AT@A=123456789*#

AT@A=****(工場出荷設定)

@A 擬似LAN接続用のダイヤル番号の表示

実行例:AT@A

@A 擬似LAN接続用のダイヤル番号の削除

実行例:AT@A=

@B擬似LAN接続時のIPアドレスの登録

設定例:

AT@B192.168.0.240(擬似LAN接続用のIPアドレス192.168.0.240)

AT@B0.0.0.0(DHCP 使用、工場出荷設定)

@Cデフォルトのコンソールモードの設定

起動時とログインタイマのタイムアウト時、ここで設定されているモードになります。

設定例:

AT@C0(コンソール)

AT@C1(ATコマンド、工場出荷設定)

@D DTE速度未検出時のデフォルトDTE速度の指定

設定例:

AT@D0(DTE使用不可)

AT@D1(2400bit/s)

AT@D2(4800bit/s)

AT@D3(9600bit/s)

AT@D4(19200bit/s)

AT@D5(38400bit/s)

AT@D6(57600bit/s)

AT@D7(115200bit/s、工場出荷設定)

AT@D8(230400bit/s)

@F TAでの着信の許可／不許可の指定

設定例:

AT@F0(TAで着信しない)

AT@F1(TA で着信する、工場出荷設定)

@G MP時のCHAP認証のユーザ名とパスワードの設定

ユーザ名とパスワードは32文字以内で設定できます。ユーザ名やパスワード文字列の中に「/」が含まれる場合は、「=」や「?」等の文字を区切子として使用してください。

設定例:

AT@G/RTW65b/himitsu/(ユーザ名RTW65b、パスワードhimitsu)

AT@G?RTW65b?(/123)?(ユーザ名RTW65b、パスワード(/123))

@H ブロードバンドTA接続用のダイヤル番号の設定

実行例:AT@H=***#

@H ブロードバンドTA接続用のダイヤル番号の表示

実行例:AT@H

@H ブロードバンドTA接続用のダイヤル番号の削除

実行例:AT@H=

@I ブロードバンドTA接続時におけるアクセスコンセントレータ名の設定

AT@Iの直後の文字を区切子として、アクセスコンセントレータ名を半角英数字64文字以内で設定できます。

Sレジスタの詳細

番号	設定範囲	内容
0	0 1〜255 1回	自動応答なし 指定回数の呼び出し後に自動応答 (工場出荷設定)
1	0〜255 0回	呼出カウント(注:設定不可) (工場出荷設定)
2	0〜127 43	エスケープシーケンスを構成する文字(コード) (工場出荷設定)
3	0〜127 13	復帰文字(終端文字コード) (工場出荷設定)
4	0〜127 10	改行文字コード (工場出荷設定)
5	0〜127 8	後退文字(編集文字コード) (工場出荷設定)
7	1〜50 30秒	発信時相手応答待ち時間(注:総合ディジタル通信端末等の接続の技術的条件第4条) (工場出荷設定)
10	0 〜255 0秒	キャリア断許容時間(0.1秒単位) (注:キャリア=同期パターン/同期フラグ) (工場出荷設定)
12	0 〜255 50x20m秒	エスケープシーケンスガードタイム(20m秒単位) (工場出荷設定)
20	1〜100 70%	スループットBODで2Bチャネル目の接続を始める回線の負荷率(回線速度に対する%値)。ATS20を越える負荷がATS21回繰り返さると2Bチャネル目を接続。 (工場出荷設定)
21	1 〜100 1回	スループットBODで2Bチャネル目の接続を始める回線の負荷率の回数。ATS20を越える負荷がATS21回繰り返されると2Bチャネル目を接続。 (工場出荷設定)

番号	設定範囲	内容
22	1～50	スループットBODで2Bチャネル目の切断を始める回線の負荷率(回線速度に対する%値)。ATS22を下回る負荷がATS23回繰り返されると2Bチャネル目を切断。
	30%	(工場出荷設定)
23	1～100	スループットBODで2Bチャネル目の切断を始める回線の負荷率の回数。ATS22を下回る負荷がATS23回繰り返されると2Bチャネル目を切断。
	2回	(工場出荷設定)
30	0	自動切断しない
	1～30	指定時間内にデータ送受信がなければ切断
	10分	(工場出荷設定;擬似LAN接続では無効)
42	0 ～255	現在のDTE-TA間速度とプロトコル(設定不可)
43	0 ～255	現在のTA-TA 間速度とプロトコル(設定不可)
50	1	ブロードバンドTAでLAN1を使用
	2	ブロードバンドTAでLAN2を使用
		(工場出荷設定)
51	1～10	PADIパケットの再送時間の初期値再送ごとに2倍の時間を設定
	3	(工場出荷設定)
52	1～10	PADIパケットの最大再送回数
	5	(工場出荷設定)
53	1～10	PADRパケットの再送時間の初期値再送ごとに2倍の時間を設定
	3	(工場出荷設定)
54	1～10	PADRパケットの最大再送回数
	5	(工場出荷設定)
55	0	TCPパケットのMSSを制限しない
	1	MSSをMTUの値に応じて制限する
	1240～1452	MSSオプション値
	0	(工場出荷設定)

番号	設定範囲	内容
56	1～2	契約しているPPPoE事業者の最大セッション数
	1	(工場出荷設定)
64	0	データポート用の呼にHLCなし
	1～127	データポート用の呼にHLCあり(コード)
	0	(工場出荷設定)(注:JT-Q931HLCの高位レイヤ特性識別)
96	1～255	コールバック起動側での着信監視タイマ
	60秒	(工場出荷設定)
97	0	コールバック被起動側ですぐ折り返し
	1～15	コールバック被起動側で折り返すまでの待ち時間
	0秒	(工場出荷設定)
102	0	呼び出ししない
	1	i･ナンバーのポート番号1
	2	i･ナンバーのポート番号2
	3	i･ナンバーのポート番号1と2
	4	i･ナンバーのポート番号3
	5	i･ナンバーのポート番号1と3
	6	i･ナンバーのポート番号2と3
	7	i･ナンバーの全てのポート番号
		(工場出荷状態)

SレジスタのS64の設定値の設定範囲は、10進数で0から127までの全ての整数です。その中で決められているものだけを以下の表で示します。

10進数	16進数	意味
1	01	電話
4	04	G2/3FAX
33	21	G4FAX
49	31	テレテックス
50	32	ビデオテックス
53	35	テレックス
56	38	メッセージハンドリングシステム(MHS)
65	41	OSIアプリケーション

リザルトコードの詳細

数字形式、文字形式のリザルトコードセットによる違いを表に示します。

○:表示される、−:表示されない

数字形式	文字形式	ATX0	ATX1	ATX2	ATX3	ATX4
0	OK	○	○	○	○	○
1	CONNECT	○	−	−	−	−
2	RING*	○	○	○	○	○
3	NO CARRIER	○	○	○	○	○
4	ERROR	○	○	○	○	○
6	NO DIALTONE	−	−	○	−	○
7	BUSY	−	−	○	○	○
10	CONNECT 2400	−	○	○	○	○
11	CONNECT 4800	−	○	○	○	○
12	CONNECT 9600	−	○	○	○	○
13	CONNECT 19200	−	○	○	○	○
14	CONNECT 38400	−	○	○	○	○
15	CONNECT 57600	−	○	○	○	○
16	CONNECT 64000	−	○	○	○	○
17	CONNECT 115200	−	○	○	○	○
18	CONNECT 128000	−	○	○	○	○
19	CONNECT 230400	−	○	○	○	○

* AT$L0に設定すると、文字形式でのRING表示の後ろの発信番号を省略できます。

用語解説

10BASE-T
イーサネットの規格の一つで、ツイストペアケーブルを用いた、10Mbit/sの速度のものを表します。本機のLANポートは10BASE-T/100BASE-TX対応です。

100BASE-TX
イーサネットの規格の一つで、ツイストペアケーブルを用いた、100Mbit/sの速度のものを表します。本機のLANポートは10BASE-T/100BASE-TX対応です。

APOP
メールサーバからメールを受信するために使用するPOP3プロトコルの認証において、パスワードを暗号化してやりとりする方式です。

ATコマンド
米国Hayes社が開発したモデムの制御コマンドです。コマンドがすべて「AT」で始まるのが特徴です。

Acrobat
アドビ·システムズ社が開発した、コンピュータ上で文書を電子的に取り扱うことのできるツールです。Acrobatが取り扱う文書はPDFファイルと呼ばれ、文書閲覧用ソフトであるAcrobat Readerで自由に閲覧することができます。

BIOS
パソコンのハードウェアの設定を行うことができる、もっとも基本的なソフトです。

CHAP
PPPでのユーザ認証の方式の一つです。CHAPではパスワードを回線上に流さないので、たとえ回線を盗聴されてもパスワードが盗まれないという特徴があります。

DCE
コンピュータとモデムやTAを使った通信システムの中で、モデムやTAのことを総称してDCEと呼びます。

DHCP
コンピュータが起動するためのさまざまな情報をコンピュータ自体には持たず、サーバからネットワーク経由で受け取るためのプロトコルです。

DIN
DINとはドイツ工業規格(日本のJISに相当)するものですが、DINで規定されているコネクタのことをDINコネクタと呼ぶことがあります。MacintoshのモデムプリンタポートにはDIN9pinコネクタが使われています。

DNS
インターネットで用いられる名前空間をドメインという階層で分散管理するためのシステムのことです。インターネットで用いられる名前には、ホスト名、メールサーバ名、ネームサーバ名、IPアドレスなどの種類があります。DNSを使うことでホスト名をIPアドレスに効率的に変換することができます。

DTE
コンピュータとモデムやTAを使った通信システムの中で、コンピュータのことを総称してDTEと呼びます。

ESS-ID
各無線LANのネットワークを識別するためのグループ名です。

FTP
ファイルをさまざまなコンピュータ間で転送するためのプロトコルです。FTPサービスを提供する側をFTPサーバ、FTPサービスを利用する側をFTPクライアントと呼びます。

HTML
ドキュメント記述言語であり、通常の文章の中にタグを埋め込んでいく方式をとります。他のドキュメントへのリンクを持つことができるのが最大の特長で、それゆえに「ハイパーテキスト」と呼ばれることがあります。WWWページを記述する言語として広く利用されています。

HUB
10BASE-Tや100BASE-TXのポートを多数持ち、その間で通信を可能にする装置のことです。

ICQ
ネットワーク上のパソコン間で簡単にメッセージをやりとりできるインスタントメッセージングソフトのことです。インターネットでも簡単に利用できます。ICQの名前の由来は「I seek you」と読めるから、ということだそうです。

IDS(Intruder Detection System)
ネットワーク上を流れるパケットを分析し、不正アクセスを検知して管理者に通報するシステムのことです。

Ingressフィルタリング

ルータやファイアウォールなどで、確実に不要なパケットを事前にフィルタで破棄することです。例えば、LANと同じ発信元のIPアドレスのパケットは外部(WAN)からは受信しないという前提で外部からのパケットを制限します。本機では、プロバイダ接続設定を行なったときにプライベートIPアドレスとLAN側に設定しているIPアドレスに関するIngressフィルタを自動適用します。ネットワーク環境に合った設定で運用することが重要です。

Internet Explorer

Windows やMacOSに標準でついてくるブラウザソフトのことです。

IP

インターネットで使用されるプロトコルです。IPを中心にして、その上位にはアプリケーション寄りのプロトコルが、下位には通信回線寄りのプロトコルが積み重なることで全体としてインターネットを構築しています。

IPX/SPX

ノベル社のネットワークOS、NetWareのために開発されたプロトコルです。

IPアドレス

インターネットでそれぞれのコンピュータを識別するためにつけられるアドレスです。

IPマスカレード

NATの中でも特にTCPやUDPのポート番号を変換することにより、1つのIPアドレスで複数のホストを動作させる技術のことです。

LAN

屋内に限定するなど、比較的狭い範囲でコンピュータを接続するネットワークのことです。

MACアドレス

ネットワーク上の識別番号です。各ネットワーク機器に固有の番号が設定されています。

NAT

IPパケットのIPアドレスなどを途中のルータで書き換える技術のことです。グローバルIPアドレスの世界であるインターネットとプライベートIPアドレス空間との間で通信できるようにすることができます。

NetBEUI

Windowsで使われるネットワークプロトコルです。

NTP

ネットワーク上でコンピュータの時計をあわせるためのプロトコルです。多くのプロバイダはNTPサーバを動作させているので、そこに時間合わせをさせるようにすると、コンピュータの時計を正確な時刻に保てます。

OutlookExpress

WindowsやMacOSに標準でついてくるメールソフトです。

PAP

PPPでのユーザ認証の方式の一つです。PAPではパスワードがそのままの形で回線上に流れます。

PDF

→Acrobat

POP3

メールサーバからメールを受信するためのプロトコルです。

PPPoE

Ethernet上で、PPP接続を行うためのプロトコルです。接続先を選択したり、接続の時にユーザ認証を行うことでダイヤルアップ接続と同じように接続を行うことができます。

PPTP

LAN上の特定の機器間でPPPパケットを通すためのプロトコルです。本機にこの機能に対応しており、LAN上のWindowsパソコンから本機をTAとして使用することができます。

TA

ISDNに対応していない装置をISDNに接続するための装置のことです。一般に、単にTAと言った場合には、RS-232Cのデータ用シリアルポート経由でパソコンをISDNに接続するための装置のことを言います。TAにはその他に、電話機やモデムなどのアナログ回線用端末を接続するためのアナログTAがあります。本機はUSBポート接続のブロードバンドTA機能を内蔵しています。

TCP
IPの上で、データが確実に相手に届くことを保証するためにあるプロトコルのことです。多くのアプリケーションはTCP上に構築されています。

TCP/IP
インターネットで使用されるプロトコル全体の総称です。

TELNET
他のコンピュータを遠隔操作するためのプロトコルです。本機もTELNETにより遠隔操作することができます。

TFTP
ファイル転送プロトコルの一種で、FTPに比べて簡単な仕組みで実現されています。本機のファームウェアのリビジョンアップにはTFTPを利用しています。

UDP
IPに、アプリケーションを識別するためにポート番号を指定する機能を付け加えるプロトコルです。

UPLINK
HUBを、より上位のHUBに接続するためのポートのことです。

URL
WWWページのアドレスなどを記述したもののことです。例として、以下のようなものになります。

http://www.rtpro.yamaha.co.jp/RT/FAQ/index.html
（プロトコル名://ホスト名.一般的にはファイル名）

USB
プラグ＆プレイに対応したシリアルバス規格です。本機には、1つのUSBポートを装備しています。

WAN
LANよりも広い範囲でコンピュータを接続するネットワークです。離れた場所のLAN同士をつなぐネットワークを指す場合もあります。

WEP（暗号化機能）
無線LANの通信を暗号化して送受信する機能です。無線LAN通信の盗聴を防止できます。本機は64ビットまたは128ビットキーで暗号化しています。

WWW
HTML文書を蓄えるWWWサーバと、HTML文書を表示する能力を持つWWWブラウザの間でHTTPを用いてHTML文書を転送するシステムのことです。

WWWブラウザ
→ブラウザ

アクセスポイント（無線）
有線LANやISDN回線と無線LANをつなぐ機能を持った装置です。本機には無線アクセスポイントが内蔵されています。

アクティブデスクトップ
Windowsで画面全体の表示にWWWを利用したもののことです。画面がWWWと連係しており、登録されたWWWサイトへのアクセスが簡単に行えます。

イーサネット
LANで使われる、ケーブルまで含んだネットワークプロトコルのことです。使用されるケーブルや通信速度などで10BASE-2、10BASE-5、10BASE-T、100BASE-TXなどの種類があります。

インターネット
世界中のコンピュータをIPを使って接続したネットワークのことです。

回線速度
通信回線が流すことのできるデータの転送速度のことです。例えば、ISDNのBチャネルは64kbit/s、イーサネットの10BASE-Tは10Mbit/sです。

管理パスワード
本機の設定を行うために必要なパスワードです。

擬似LAN
USBポートに接続したパソコンから本機にダイヤルアップすることにより、本機のLANポートに接続されているLANにアクセスできる機能です。LANポートを持たないパソコンでもLANにアクセスすることができます。

ゲートウェイ
→ルータ

コンソール
本機では、TELNETなどでログインしてコマンドを入力できる画面のことをいいます。

コントロールパネル
Windowsのいろいろな設定を行うためのフォルダです。「マイコンピュータ」の中にあります。

サーバ
ネットワーク上でいろいろなサービスを提供するコンピュータのことです。WWWサーバ、DHCPサーバ、FTPサーバ、ネームサーバ、メールサーバなどがあります。

終端抵抗
→ターミネータ

スタティック(静的)フィルタ
固定的に動作するフィルタです。一度設定するとフィルタが常時有効になります。

ステーション(無線)
RTW65bをどうしを無線で接続する場合のクライアント側のRTW65bのことです。

静的IPマスカレード
IPマスカレードを利用する時には、外部からのアクセスができなくなりますが、静的IPマスカレードを利用すると外部からのアクセスをできるように設定できます。

静的フィルタ
→スタティックフィルタ

専用線
特定の相手と、常に通信できるようになっている回線のことです。利用するためにはNTTなどの通信事業者に申し込みます。

ダイナミック(動的)フィルタ
通信状態を監視しながら、必要に応じてフィルタを有効にします。

動的フィルタ
→ダイナミックフィルタ

ドメイン名
インターネット上の組織名をあらわす名前のことです。例えば、「yamaha.co.jp」はドメイン名です。DNSで利用されます。

認証
接続相手を確認することです。パスワードを確認するのがもっとも一般的な方法で、PPPではPAPやCHAPを使ってパスワードを確認します。

ネットマスク
IPアドレスと論理積をとるとネットワークアドレスが得られるようなビット列のことをいいます。ネットマスクは最上位ビットから連続して1が続き、あるところから最下位ビットまで0が続く形なので、最上位ビットから1が続いている長さでネットマスクを表すことができます。これをネットマスク長といいます。本機の設定では、ネットマスクはすべてネットマスク長で設定します。ネットマスクの設定を間違えるとまったく通信できなくなってしまうことがあるので注意が必要です。

ネットワークアドレス
ネットワークを識別するためのIPアドレスです。あるネットワークに所属するホストのIPアドレスはすべて、上位部分はネットワークアドレスと一緒でなくてはいけません。

ネットワークゲーム
ネットワークを用いて不特定の相手や遠隔地の相手と対戦することのできるゲームのことです。インターネットの普及とともにネットワークゲームが愛好されるようになってきています。

ネームサーバ
DNSで、名前とIPアドレスなどの変換を行うためのサーバです。ネームサーバだけは名前で指定できないので、必ずIPアドレスで指定しなくてはいけません。

パケット
IPで取り扱うデータの1単位のことです。IPではすべてのデータはパケットという単位で扱われます。パケットはデータグラムと呼ばれることもあります。

ファームウェア
本機に内蔵されていて、本機の動作を制御するソフトのことです。ファームウェアをネットボランチホームページからダウンロードし本機をリビジョンアップすることで、購入後でも最新の機能を利用することができます。

ファイアウォール(firewall、防火壁)
外部ネットワークからの不正アクセスを防ぐ機能／装置です。

フィルタ
ルータはパケットを転送する時に、パケットの内容によっては転送せずに捨ててしまう機能のことです。フィルタを適切に設定することで外部からの侵入を阻止したり、必要のない発信を止めたりすることができます。

ブラウザ
WWWサーバからHTML文書を入手し、表示する機能を持ったソフトのことです。代表的なものには、Internet ExplorerやNetscape Communicatorがあります。

ブリッジ
パケットのIPアドレスをチェックせず、他のネットワークにすべて転送する装置です。

ブロードキャスト
ネットワーク全体のホストへパケットを送信することです。そのようなことができるアドレスをブロードキャストアドレスと呼びます。

プロトコル
通信を行う時の規約のことです。

プロバイダ
インターネットサービスプロバイダの略で、インターネットへの接続サービスを提供する業者のことです。接続に必要なアクセスポイントの整備や、インターネットで必要なIPアドレスの取得代行サービスなどを行います。

ホスト
IPでは、ホストはIP的に接続されているすべてのコンピュータのことを指します。

ポート番号
TCPやUDPでアプリケーションを識別するための番号です。例えば、WWWはTCPの80番、メールはTCPの25番です。サービスを提供するサーバ側のポート番号はアプリケーションによって決まっていますが、そこに接続にいくクライアント側のポート番号はその時々によって変わります。

ホームページ
WWWサイトの一番入口のページを指します。

無線ブリッジ
本機やRT60wどうしを、無線で接続する機能です。複数の無線LANをひとつのLANとして管理できます。

メールサーバ
メールを送信したり、受信したメールを蓄えておくサーバのことです。

リビジョン
本機に内蔵されるファームウェアの版のことです。バージョンともいいます。新しいリビジョンのファームウェアを本機に送り込むことをリビジョンアップといいます。

ルータ
パケットのIPアドレスに基づいて適切な方向へパケットを転送する機能を持つ装置のことです。ゲートウェイともいいます。

ログ
装置の状態や動作の記録を時間順に記録したものです。

ログアウト
装置へのアクセスを終わることです。

ログイン
TELNETなどで装置へのアクセスを始めることです。

ログインパスワード
本機にログインするためのパスワードです。設定を行うことはできませんが、接続状態やログを見ることができます。

ローミング(無線)
複数の無線アクセスポイントを有線LANで接続することで、アクセスポイントを自動的に切り替える機能です。無線LANでアクセスできる範囲が広がりますので、複数階にまたがるような大きなオフィスを移動しながら、インターネットにアクセスしたいときに便利です。

索引

英数字

五十音順

ア行

カ行

サ行

タ行

ナ行

ハ行

マ行

ラ行

ヤマハ株式会社

●ネットボランチコールセンター
RTW65b専用サービス窓口
TEL: 03-5715-0350
土日祝日を除く9時～12時、13時～17時

●電子メールでのお問い合わせ
Webお問い合わせページ： http://NetVolante.jp/
メールアドレス： support@netvolante.jp

V838460