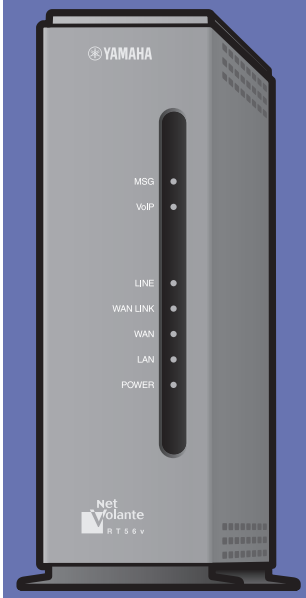
YAMAHA

感 動 を ・ と も に ・ 創 る

RT56v

ブロードバンドVoIPルータ



活用マニュアル

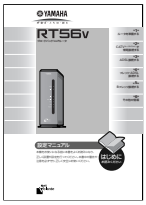
本機をお使いになる前に本書をよくお読みになり、
正しく設置や設定を行ってください。本書中の警告や
注意を必ず守り、正しく安全にお使いください。

Net Volante

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。

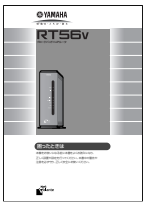
設置のしかたや設定のしかただけでなく、CATV/ADSLなどのブロードバンドルータとしての基本的な使いかたについて説明しています。

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。

電話やブロードバンドルータとしての代表的な使いかたについて、その解説と設定方法を説明しています。

困ったときは



本機のトラブル発生時の対策や、サポート窓口のご案内について、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（122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。契約に違反して本機を使用すると、予想外の料金を請求される場合があります。**

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

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。**

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。

RT56vは「外国為替および外国貿易管理法」に基づいて規制される戦略物資(または役務)に該当します。このため、日本国外への持ち出しには、日本国政府の事前の許可が必要となる場合があります。

詳細な技術情報について

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

目次

第6章 インターネット電話機能を使う

第7章 ルータを使いこなす

第8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

本書ではそれぞれの製品について、以下のように略称で記載しています。

- YAMAHA RT56v：本機
- Microsoft® Windows®：Windows
- Microsoft® Windows 95®：Windows95
- Microsoft® Windows 98®：Windows98
- Microsoft® Windows 98 Second Edition®：Windows98SE
- Microsoft® Windows NT®：WindowsNT
- Microsoft® Windows 2000®：Windows2000
- Microsoft® Windows Millennium Edition®：WindowsMe
- Microsoft® Windows XP® ：WindowsXP
- 10BASE-T（100BASE-TX）ケーブル：LANケーブル

設定例について

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

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。
- “FINAL FANTASY”および“PlayOnline”は、株式会社スクウェアの登録商標または商標です。
- “PlayStation”は株式会社ソニー・コンピュータエンタテインメントの登録商標です。
- 本製品は、RSA Security Inc.のRSA® BSAFE™ WirelessCoreソフトウェアを搭載しております。

RSAはRSA Security Inc.の登録商標です。BSAFEはRSA Security Inc.の米国及びその他の国における登録商標です。

⚠ 警告

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。

- 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アダプタを容易に取り外すことができるような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、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。
- アナログ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

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。

- 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。また、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。
- 本機を修理または移動などの理由により輸送する場合には、必ず本機の設定を保存するようにしてください。

使用上のご注意

- メール確認や転送を設定すると定期的にインターネットへ自動接続を行うので、その度に通信料金やプロバイダ接続料金がかかります。あらかじめご理解いただいた上で、この機能を設定およびご使用ください。
- 自動接続が設定されている場合に、「かんたん設定ページ」の[ネットボランチホームページ]をクリックするとインターネットへ自動接続します。それに伴った通信料金やプロバイダ接続料金がかかりますので、あらかじめご理解いただいた上で、この機能をご使用ください。
- 電話機を使った設定やインターネット電話機能など、本機と電話機間はトーン(プッシュ)で信号がやり取りされます。そのため、停電などによって本機の電源供給が停止すると、トーン(プッシュ)回線用に動作するように設定された電話機がダイヤル回線と直結されることになります。この状態では、お使いの電話機によっては110や119などの緊急電話も含めて、外線通話できない場合があります。

  お使いの電話機にダイヤル／トーン切り換えスイッチがある場合は、「ダイヤル」に切り換えて通話してください。
- TEL1ポート以外のTELポートに接続した電話機で外線通話中に停電が発生すると、停電時はTEL1ポートを優先する仕様のため、TEL1ポートに接続した電話機に外線通話が切り替わります。
- 本機のアナログポートにはモデムあるいはFAXを接続して使用することができますが、インターネット電話機能を使用して通信することはできません。
- 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 はじめに

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。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

ネットボランチ RT56v でできること

本機はCATV／ADSL接続、光ファイバ接続（Bフレッツ）まで、さまざまなインターネット接続方法に対応できるブロードバンドルータです。より高速な回線で接続したいときにも、本機の設定変更のみで対応できます。

ブロードバンド対応

CATVやADSL、光ファイバ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。

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。

インターネット電話機能

通話の相手先もインターネット電話機能を持ったネットボランチシリーズルータを使用している場合には、インターネット経由の会話（インターネット電話）を楽しめます。インターネット経由で通話するため、プロバイダへの通信料以外の通話料金はかかりません。

また、本機はUPnP（ユニバーサル･プラグ･アンド･プレイ）に対応しているため、Windows MessengerやMSN Messengerを利用した音声チャットも楽しめます。

PPTPによる仮想プライベートネットワーク構築

本機はPPTP（Point to Point Tunneling Protocol）に対応しているため、インターネット（ブロードバンド）回線を利用した仮想プライベートネットワーク（VPN）を構築する場合でも、より安全にデータをやり取りできます。

LANとLANをPPTP方式で接続するだけでなく（PPTP-LAN間接続）、外出先からPPTP方式でLANにリモートアクセスでき、便利です。

次のページにつづく▶

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。

かんたん設定

付属のユーティリティソフトウェア「RT56v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「RT56v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。

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。

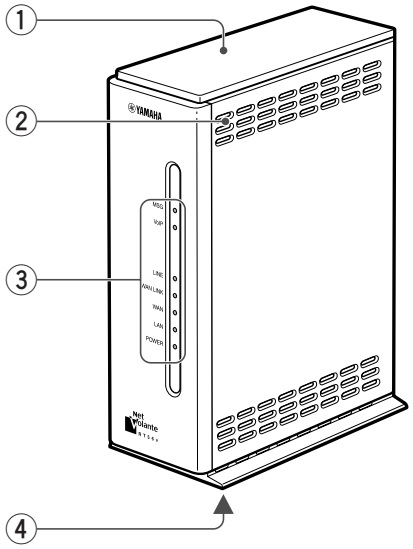
また、ヤマハルータRTシリーズホームページ（http://www.rtpro.yamaha.co.jp/）では、RTシリーズルータを使った高度な活用例や詳しい解説がご覧いただけます。

その他多機能ルータとして便利な機能を装備

- 次世代インターネット・プロトコルの「IPv6」に対応しています。
- TELポートは3ポート装備しているので、今まで使っていた電話やFAX、モデムなどを接続できます。また、Lモードにも対応しています。
- 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。

各部の名称とはたらき

前面



① 上部カバー

DIPスイッチの設定を変更するときは、取り外します。詳しくは「DIPスイッチ」(12ページ)をご覧ください。

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(42ページ)。
- VoIP:インターネット電話機能の使用状態を示します。通話中は点灯、着信時は点滅します。
- LINE:本機に接続した一般回線(アナログ回線)の状態を示します。回線が使用中のときに点灯し、回線が使用されていないとき消灯します。着信時は点滅します。
- WAN LINK:インターネット接続中は点灯します。
- 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。
- 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。
- 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。

④ MACアドレス(底面)

機器固有のネットワーク識別番号です。

前面ランプの点灯状態

◉点灯、 ◎点滅、 ○消灯

MSGランプ

- ◎ プロバイダのメールサーバにメールが到着しています(かんたん設定ページで、メールサーバを登録する必要があります)。

VoIPランプ

- ◉ インターネット電話機能で通話中です。
- ◎ インターネット電話が着信しています。
- ○ インターネット電話機能を使用していません。

LINEランプ

- ◉ 一般回線(アナログ回線)の電話で通話中です。
- ◎ 一般回線(アナログ回線)の電話が着信しています。
- ○ 一般回線(アナログ回線)の電話を使用していません。

WAN LINKランプ

- ◉ インターネットに接続しています。
- ○ インターネットに接続していません。

WANランプ

- ◉ WANが使用可能な状態です。
- ◎ WANポートにデータが流れています。
- ○ WANが使用不可能な状態です。

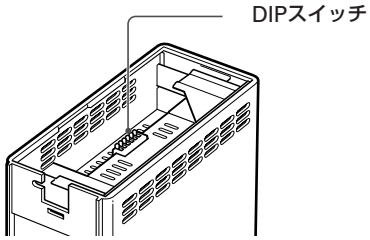
LANランプ

- ◉ LANが使用可能な状態です。
- ◎ LANにデータが流れています。
- ○ LANが使用不可能な状態です。

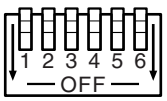
POWERランプ

- ◉ 電源が入っています。
- ○ 電源が切れているか、または停電しています。

DIPスイッチ



本機の上部カバーを取り外すと、DIPスイッチがあります。各スイッチの機能は、以下の通りです。



ご注意

DIPスイッチの設定を変更したら、本機を再起動してください。本機を再起動しないと、変更は反映されません。

スイッチ1

- ON：LAN1ポートのオートネゴシエーションをONにする。
- OFF：LAN1ポートのオートネゴシエーションをOFFにして、10Base Halfに固定する。

スイッチ2

- ON：LAN2ポートのオートネゴシエーションをONにする。
- OFF：LAN2ポートのオートネゴシエーションをOFFにして、10Base Halfに固定する。

スイッチ3

- ON：LAN3ポートのオートネゴシエーションをONにする。
- OFF：LAN3ポートのオートネゴシエーションをOFFにして、10Base Halfに固定する。

スイッチ4

- ON：LAN4ポートのオートネゴシエーションをONにする。
- OFF：LAN4ポートのオートネゴシエーションをOFFにして、10Base Halfに固定する。

スイッチ5

未使用

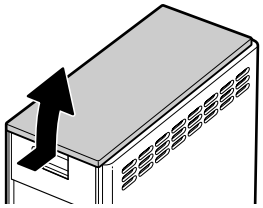
スイッチ6

パスワードを忘れてしまったときに、本機にアクセスするために使用します。詳しくは、「困ったときは」（別冊）の「パスワードを忘れてしまった」（20ページ）をご覧ください。

上部カバーを開ける／閉じる

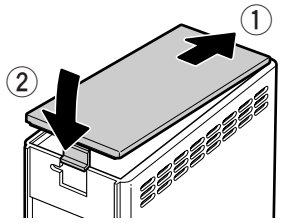
上部カバーを開ける

本機背面のツメの部分を押しながら、カバーを開く。

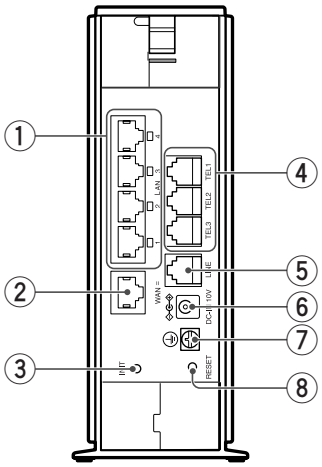


上部カバーを閉じる

本機前面のくぼみにカバーのツメを引っかけてから、「カチッ」と背面のツメが固定されるまでカバーをゆっくり閉じる。



背面



① 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。

② WANポート
ケーブルモデムやADSLモデム、ONUとLANケーブルで接続します。

③ INITスイッチ
このスイッチを押しながらRESETスイッチを押すと、本機の設定を工場出荷状態に戻すことができます。詳しくは、「困ったときは」(別冊)の「本機の設定を工場出荷状態に戻す」(21ページ)をご覧ください。

④ TELポート
電話機やFAXなどのアナログ機器とモジュラーケーブルで接続します。停電時はTEL1ポートのみ使用できます。

⑤ LINEポート
一般回線(アナログ回線)にモジュラーケーブルで接続します。

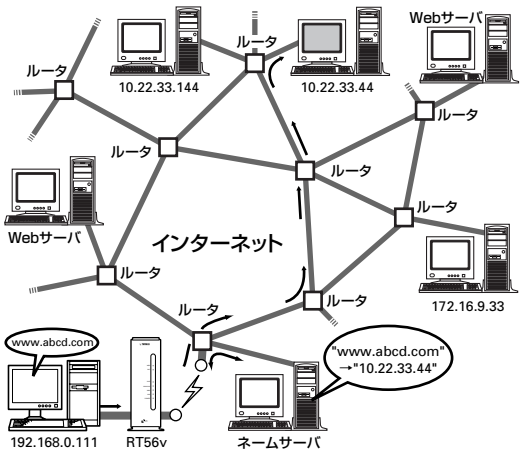
⑥ DC-IN 10Vコネクタ
付属のACアダプタ(P10V1.2A)を接続します。

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。

⑧ RESET(リセット)スイッチ
本機を再起動します。

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。

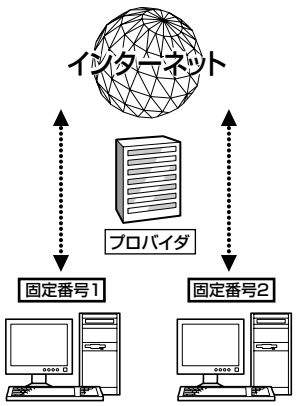
IPアドレスの入手方法は、インターネットへの接続方法によって異なります

CATV／ADSL（PPPoE方式以外）接続、フレッツ・ADSL、Bフレッツなどの　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。

固定IPアドレスサービスを利用する場合は

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。

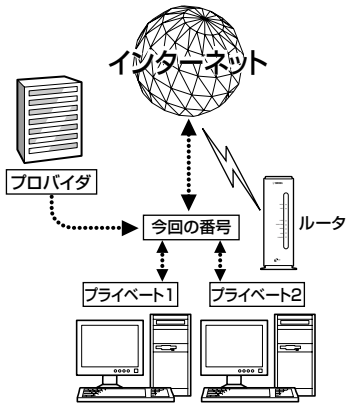


本機などのアドレス変換機能を持ったルータで接続する場合は

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。固定IPアドレスサービス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。CATV／ADSL（PPPoE方式以外）接続、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

ネットワーク型接続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)

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。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

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。

電話機で設定する（18ページ）
本機のTELポートに接続したプッシュボタン式電話機から、本機の電話機能を設定できます。設定は、受話器を上げてダイヤルボタンを押して行います。

パソコンのWebブラウザで設定する（23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。

コンソールコマンドで設定する（27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。

電話機で設定する

TELポートに接続したプッシュボタン式電話機で、本機を設定できます。電話機からは、主に本機の電話機能を設定できます。

設定できる機能と設定値については、「電話機設定機能一覧」(20ページ)をご覧ください。よく使う設定例については、次ページをご覧ください。

ご注意

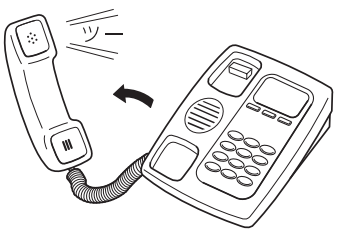
- 電話機から設定するときは、必ず電話機をトーン(プッシュ)に切り替えてから操作してください。パルス(ダイヤル)方式だけでトーンの機能がない電話機からは、設定できません。
- ご利用の回線がダイヤル回線の場合、電話機をトーン(プッシュ)に切り替えると、停電時やアナログ回線に直接電話機を接続したときに電話がかけられなくなります。この場合はお使いの電話機の取扱説明書をご覧になり、電話機の回線種別をダイヤル回線に切り替えてからお使いください。
- 外線電話からは設定できません。
- 電話機から設定すると、設定内容は本機の内蔵メモリに保存されますので、本機の電源を切っても内容は消えません。ただし、IPアドレスとネットマスクは記憶されませんのでご注意ください。

設定のしかた

電話機で「✱、#、機能番号、TELポート番号、設定値」の順でダイヤルしてから # を押すと、本機の電話機能を設定できます。設定できる機能と機能番号について詳しくは、「電話機設定機能一覧」(20ページ)をご覧ください。

ここでは、TEL2ポートにダイヤルイン番号「031-333-2002」を登録する場合を例にして、操作の手順を説明します。

1 受話器を上げる。



発信音が聞こえます。

2 電話機の ✱ と # ボタンを押す。

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 機能番号を押す。

ダイヤルイン番号を設定する場合は、「11」と押します。

4 TELポート番号を押す。

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。TEL2ポートを指定する場合は、「2」を押します。

- ✱ を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。
- TELポート番号が不要な機能は、何も押さずに次の手順へ進んでください。

5 設定値を押す。

ダイヤルイン番号「031-333-2002」を登録するときは、「0313332002」と押します。

6 # を押す。

「ピー」という音が聞こえ、設定が変更されます。

「ピー、ピー」と聞こえるときは

設定内容が適切でなかったり、設定が正常に変更されていません。設定内容を確認してから、手順3から操作し直してください。

7 受話器を置く。

続けて設定するときは、受話器をあげたまま手順3〜6の操作を繰り返します。

設定例

① ダイヤルイン番号を設定する

例:TEL2ポートのダイヤルイン番号を「031-333-2002」にする:

受話器をあげてから、(✱)、(#)、11(機能番号)、2(TEL2ポート)、0313332002、(#) と押す。

② アナログポートを使用制限する

例:TEL2ポートに何も接続しない:

受話器をあげてから、(✱)、(#)、14(機能番号)、2(TEL2ポート)、0(何も接続しない)、(#) と押す。

③ ダイヤルの桁間隔時間を設定する

例:TEL1ポートのダイヤルの桁間隔時間を10秒にする:

受話器をあげてから、(✱)、(#)、41(機能番号)、1(TEL1ポート)、10、(#) と押す。

④ フッキング判定時間を設定する

例:TEL1ポートのフッキング判定時間を1.2秒にする:

受話器をあげてから、(✱)、(#)、42(機能番号)、1(TEL1ポート)、12、(#) と押す。

⑤ 識別着信を設定する

例:031-444-1818からTEL2ポートへの着信を拒否する:

受話器をあげてから、(✱)、(#)、32(機能番号)、2(TEL2ポート)、2、(#) と押す。

そのあとに続けて、33(機能番号)、2(TEL2ポート)、0314441818、(#) と押す。

⑥ ナンバー・ディスプレイ対応に設定する

例:TEL2ポートをナンバー・ディスプレイ対応にする:

受話器をあげてから、(✱)、(#)、39(機能番号)、2(TEL2ポート)、1、(#) と押す。

⑦ Lモードメッセージ到着お知らせ機能の設定

例:Lモードメッセージ到着お知らせ機能を利用する:

受話器をあげてから、(✱)、(#)、86(機能番号)、1(TEL1ポート)、1、(#) と押す。

⑧ パスワードを変更する

例:パスワード「666」を「77」に変更する:

受話器をあげてから、(✱)、(#)、00(機能番号)、666(旧パスワード)、(✱)、77(新パスワード)、(✱)、77(新パスワード確認)、(#) と押す。

⑨ IPアドレスとネットマスクを新規設定する

例:IPアドレスを「192.168.11.1」、ネットマスクを「255.255.255.0」(24ビット)に新規に設定する:

受話器をあげてから、(✱)、(#)、71(機能番号)、192、(✱)、168、(✱)、11、(✱)、1、(#) と押す。

そのあとに続けて、72(機能番号)、255、(✱)、255、(✱)、255、(✱)、0、(#) と押す。

ご注意

- 固定IPアドレスサービス契約時にLANのIPアドレスとしてグローバルIPアドレスを設定する場合は、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相談してください。万一間違ったIPアドレスを設定した場合、LAN外のホストやネットワークにトラブルが起きることがあります。
- IPアドレスを変更するときは、LANの管理者に本機に割り当てるIPアドレスとネットマスクをお問い合わせください。管理者がいないときは、LAN上のすべての機器の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。

電話機設定機能一覧

2桁の機能番号はTELポート（機器）側の設定、3桁の機能番号はLINEポート（回線）側の設定になります。
電話機から設定できる機能の詳細については、コマンドリファレンスをご覧ください。

TELポート（機器）側の設定

機能	機能番号		設定値	初期設定値
TELポートのダイヤル番号設定	11		回線番号またはダイヤルイン番号	番号なし
アナログポート使用制限の設定	14		0=使用しない 1=発信のみ 2=着信のみ 3=発信･着信可能	3
インターネット電話 着信制限の設定	15		0=着信不可 1=自己アドレスのみ着信 2=すべて着信	2
インターネット電話 発信制限の設定	16		0=発信不可 1=発信可	1
即時発信	22		0=使用しない 1=使用する	1
ポーズを判定する時間（秒）	23		1～10	2
識別着信	32		0=しない 1=一致時着信 2=一致時拒否	2
識別着信の番号登録	33	TELポート番号 1=TEL1 2=TEL2 3=TEL3	識別する電話番号	番号なし
優先着信ポート	37		1=優先順位高い 2=優先順位普通 3=優先順位低い	2
着信ベル設定	38		1=パターン1　識別する相手の電話番号 2=パターン2　識別する相手の電話番号	設定なし
ナンバー･ディスプレイ機能	39		0=使用しない 1=ナンバー･ディスプレイのみ使用する 2=ナンバー･ディスプレイとキャッチホン･ディスプレイの両方を使用する	0
ダイヤル桁の間隔設定（秒）	41		1～20	6
フッキング判定時間（1/10秒）	42		5～20	10
フッキング後の操作有効時間（秒）	43		1～9	4
フッキング オンフック無効時間（秒）	44		1～3 0=すべて有効	0
擬似切断信号の設定	45		0=送出しない 1=送出する	1
モデム信号タイプ設定	46		1=タイプ1 2=タイプ2 3=タイプ3	3

機能	機能番号		設定値				初期設定値
送話PADの音量設定	61	TELポート番号 1=TEL1 2=TEL2 3=TEL3	0=PADなし 1=−3dB 2=−6dB 3=−9dB	4=−12dB 5=−15dB 6=−18dB 7=−21dB			0
受話PADの音量設定	62		0=PADなし 1=−3dB 2=−6dB 3=−9dB	4=−12dB 5=−15dB 6=−18dB 7=−21dB			0
DTMF検出レベル	63		0=PADなし 1=−3dB 2=−6dB 3=−9dB 4=−12dB 5=−15dB	6=−18dB 7=−21dB 8=−24dB 9=−27dB 10=−30dB			0
LAN側のルータIPアドレス設定	71		ピリオドごとに＊を入れて、IPアドレスを入力 （例：192.168.0.1の場合は、192＊168＊0＊1）				192＊168＊0＊1
LAN側のネットマスク設定	72		ピリオドごとに＊を入れて、ネットマスクを入力 （例：255.255.255.0の場合は、255＊255＊255＊0）				255＊255＊255＊0
着信時サービス設定	82	TELポート番号 1=TEL1 2=TEL2 3=TEL3	01=ローカルアドレス1 02=ローカルアドレス2 03=ローカルアドレス3 04=ローカルアドレス4 05=ローカルアドレス5	発信端末タイプ ＊=全て	着信サービスタイプ 1= PBダイヤルイン 2= モデムダイヤルイン 3= 無鳴動着信	ダイヤルイン番号	設定なし
擬似ナンバー・リクエスト	83		発番号なし着信 0=拒否 1=許可 2=擬似ナンバーリクエスト	非通知理由 1=公衆電話 2=ユーザによる通知拒否 3=表示圏外 ＊=全て			発番号なし着信 すべて許可
ダイヤル完了ボタン設定	84		0=使用しない 1=使用する				1
再呼出時間設定（秒）	85		10〜180				30
メッセージ到着お知らせ機能	86		0=使用しない 1=使用する				0
アナログポート設定の消去	91		−				−
識別着信の番号削除	92		登録済みの電話番号				−
着信ベルの番号削除	93		着信ベル番号	登録済みの電話番号			−
発着信回数の消去	94		−				−
アナログポート設定の全消去	99		−				−
パスワードの設定	00		（旧パスワード）＊（新パスワード）＊（新パスワード）				−

次のページにつづく▶

LINEポート（回線）側の設定

機能	機能番号	設定値	初期設定値
ダイヤルの種別選択	201	1＝ダイヤル回線（10pps） 2＝ダイヤル回線（20pps） 3＝プッシュ回線	2
ナンバーディスプレイ 着信識別	203	0＝切 1＝自動	1
付加サービス機能設定	204	0＝付加サービスを契約していない回線 1＝付加サービスを契約している回線	0
回線側のポーズ時間設定（秒）	205	1～10	2
フッキング時間設定（1/10秒）	206	3～10	5
受話PADの音量設定	207	0＝PADなし　4＝－12dB 1＝－3dB　5＝－15dB 2＝－6dB　6＝－18dB 3＝－9dB　7＝－21dB	0
送話PADの音量設定	208	0＝PADなし　4＝－12dB 1＝－3dB　5＝－15dB 2＝－6dB　6＝－18dB 3＝－9dB　7＝－21dB	0
LINEポート使用制限の設定	209	0＝LINEポート発信・着信とも禁止 1＝LINEポート発信・着信とも許可	1

Webブラウザから「かんたん設定ページ」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。Webブラウザで設定操作をすると、電話機による設定操作よりも多くの機能を簡単に設定できます。

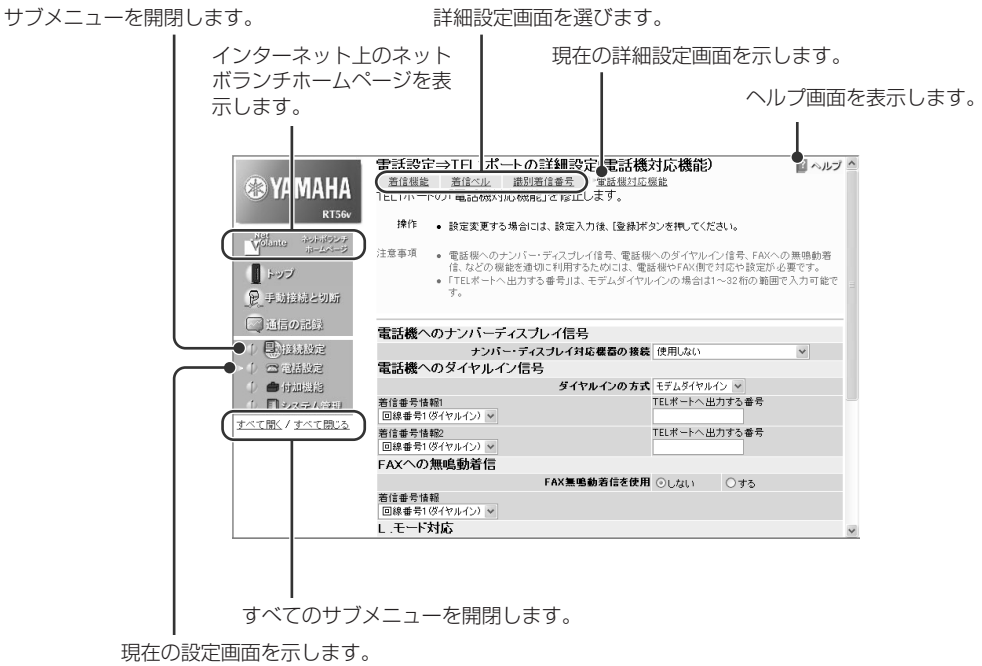
ご注意

「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。

ヒント

- 「かんたん設定ページ」の設定項目については、「『かんたん設定ページ』設定項目一覧」(131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

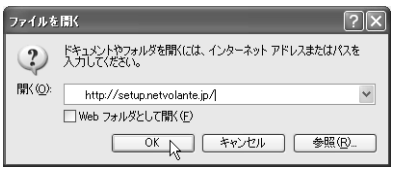
電話機能を設定する場合の例

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。

ご注意

ルータ型ADSLモデムを使用してインターネットに接続している場合など、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。

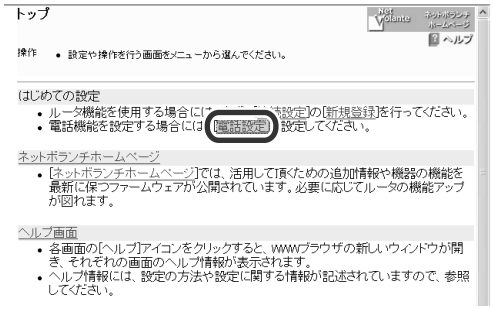
ルータの管理パスワードを設定していない場合は

「RT56vかんたん設定ページへ行く前に」画面が表示されます。ルータの管理パスワードと現在の日時を設定してください。

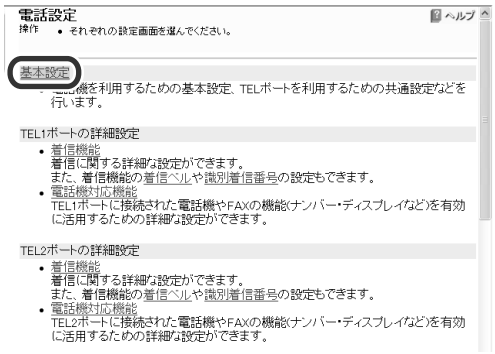
3 **[パスワード]欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

4 **[電話設定]をクリックする。**

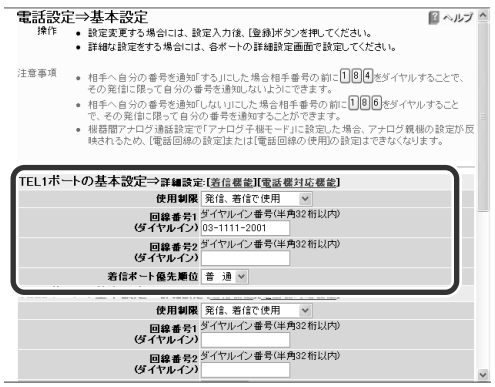


5 **[基本設定]をクリックする。**



6 **ダイヤルイン契約している場合はTELポートに電話番号を設定してから、優先着信ポートや付加サービスなどを選び、[登録]をクリックする。**

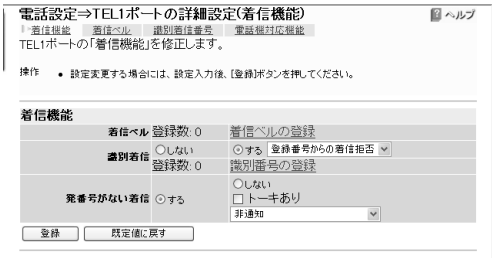
TEL1ポートに契約者番号「03-1111-2001」を登録する場合の例



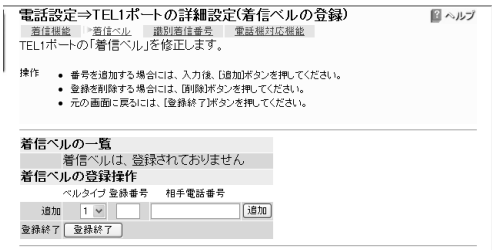
7 **詳しい設定を行う場合には、各ポートごとの[着信機能]や[着信ベル]、[識別着信番号]、[電話機対応機能]をクリックする。**

設定項目について詳しくは、「かんたん設定ページ」のヘルプ画面をご覧ください。

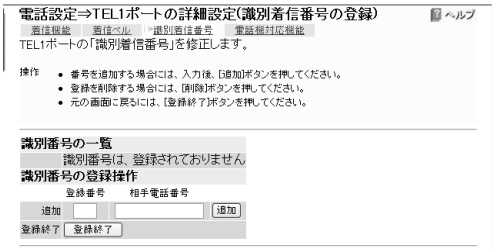
「着信機能」画面



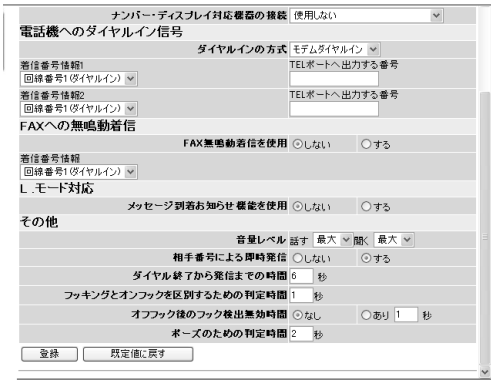
「着信ベル」画面



「識別着信番号」画面



「電話機対応機能」画面



8 **画面入力が終わったら、[登録]をクリックする。**

通信記録を見る場合の例

TELポートや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。

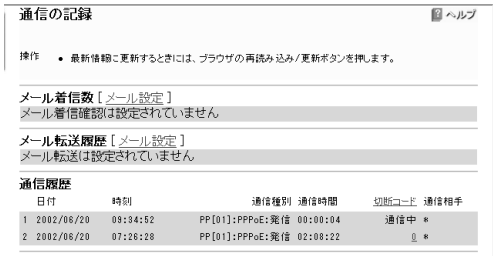
「ネットワーク パスワードの入力」画面が表示されます。

次のページにつづく▶

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。**

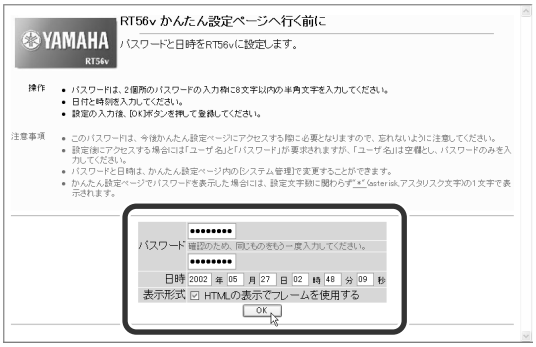
メール着信件数やメール転送件数、通信履歴が表示されます。



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。

特に設定を変更していない場合は、「かんたん設定ページ」を初めて開いたときに入力したパスワードが、「管理パスワード」と「ログインパスワード」の両方に設定されています。



「かんたん設定ページ」を初めて開いたときのパスワード入力画面

「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

- 「管理パスワード」と「ログインパスワード」のどちらかのパスワードだけ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。

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。

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)。

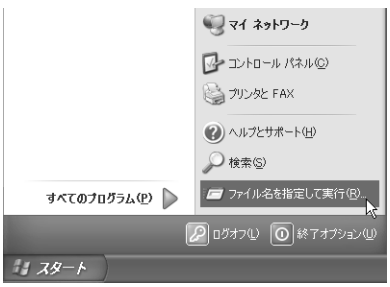
ご注意

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

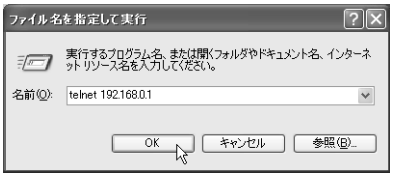
コンソールコマンドの詳細については、コマンドリファレンスをご覧ください。

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。

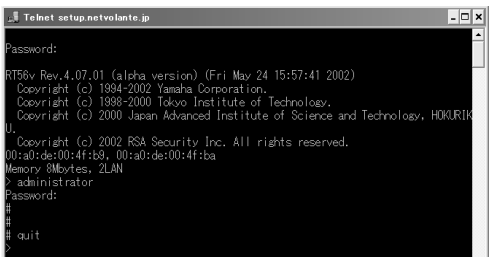
本機のIPアドレスを変更している場合には、「192.168.0.1」のかわりに本機のIPアドレスを入力します。



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。

次のページにつづく▶

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。**

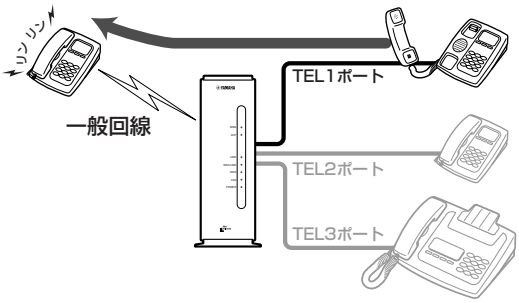
第3章 電話/FAXを使う

この章では、本機を一般回線（アナログ回線）に接続している場合に利用できる電話機能について紹介します。なお、インターネット経由のVoIP通話（インターネット電話機能）については、「第6章 インターネット電話機能を使う」（62ページ）をご覧ください。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

電話をかける

電話機で外線をかけるときは、通常の電話と同じ操作でかけられます。



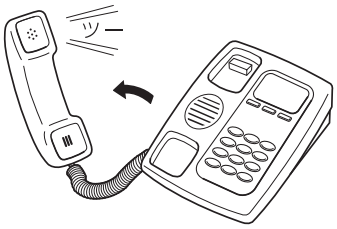
ご注意

- 電話機のダイヤル設定は、できる限り「トーン」（プッシュ）でお使いください。「パルス」の場合は、(*) および (#) の入力ができないため、次のような制限があります。
  - 内線をかけることができません。
  - 電話機からの設定ができません。
- ご利用の回線がダイヤル回線の場合、電話機をトーン（プッシュ）に切り替えると、停電時やアナログ回線に直接電話機を接続したときに電話がかけられなくなります。この場合はお使いの電話機の取扱説明書をご覧になり、電話機の回線種別をダイヤル回線に切り替えてからお使いください。
- 本機の電話機能は、本機を一般回線（アナログ回線）に接続している場合に使用できます。本機を一般回線（アナログ回線）に接続していない場合は、TELポート間の内線通話とインターネット電話、機器間アナログ通話以外、電話をかけられません。

次のページにつづく▶

1 **受話器を上げる。**

発信音が聞こえます。



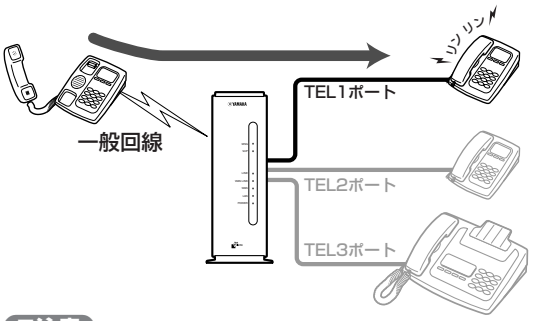
2 **相手の電話番号をダイヤルする。**

呼び出し音が聞こえ、相手が出ると通話できます。

3 **通話が終わったら、受話器を置く。**

電話を受ける

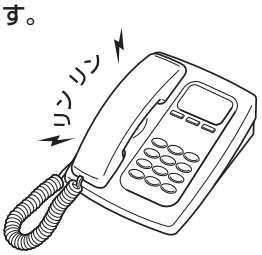
電話がかかってくると、本機のTELポートに接続したアナログ機器から呼び出し音が鳴ります。



ご注意

本機の電話機能は、本機を一般回線（アナログ回線）に接続している場合に使用できます。本機を一般回線（アナログ回線）に接続していない場合は、TELポート間の内線通話とインターネット電話、機器間アナログ通話以外、電話を受けられません。

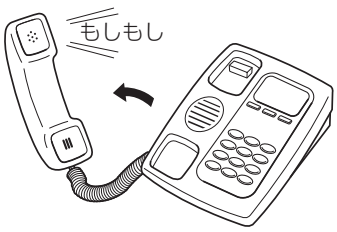
1 **電話がかかってくると、呼び出し音が鳴ります。**



ヒント

ダイヤルインサービスを設定した場合は、設定したTELポートに接続したアナログ機器だけ呼び出し音を鳴らすこともできます。詳しくは、「TELポートごとに使い分ける」（38ページ）をご覧ください。

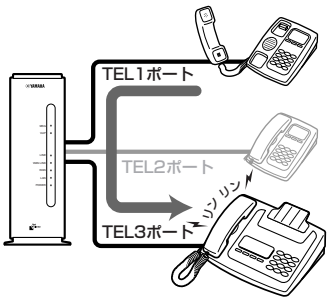
2 **受話器を上げて、通話する。**



3 **通話が終わったら、受話器を置く。**

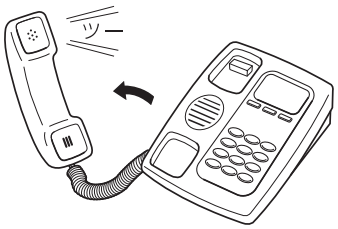
内線電話をかける

TELポートに接続したアナログ機器どうしで、内線通話ができます。アナログ機器の内線番号は、TEL1ポートが[1]、TEL2ポートが[2]、TEL3ポートが[3]となります。



1 **受話器を上げる。**

発信音が聞こえます。



2 **⊛ に続けて、内線番号をダイヤルする。**

- TEL1ポートを呼び出す場合の例:⊛、1
- 全てのポートを呼び出す場合の例:⊛、⊛

指定した内線番号のアナログ機器で呼び出し音が鳴ります。相手が出ると通話できます。

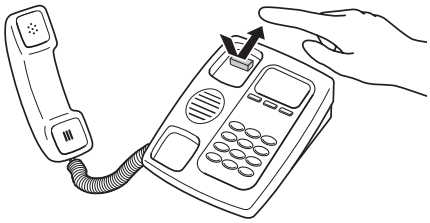
ご注意

- 指定した内線番号の機器が使用中のときは、呼び出し音は鳴りません。
- 機器間アナログ通話機能を利用するときの操作は、「複数のルータ間で通話する(機器間アナログ通話)」(74ページ)をご覧ください。

3 **通話が終わったら、受話器を置く。**

フッキング操作を練習する

フックボタンを押してすぐ放す操作を「フッキング」と呼び、電話を転送したり、着信中に電話を受けたときに通話先を切り替えたりするときに使います。



多機能電話などをお使いのときは、フッキング操作は、キャッチボタン(またはフックボタン、フラッシュボタンなど)を押す操作となります。詳しい操作は、お使いのアナログ電話機の取扱説明書でご確認ください。

ご注意

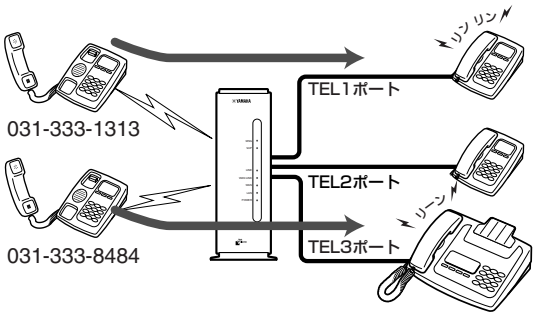
フックボタンを長く(1秒以上)押すと、「オンフック」(受話器を置いた状態)とみなされて電話が切れてしまいます。

ヒント

フッキングと判定する時間は、フッキング判定時間の設定(20ページ)で変更できます。

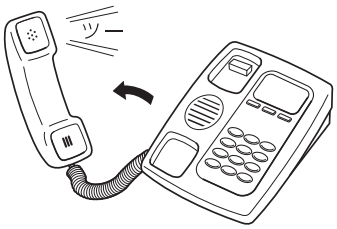
相手によって着信ベル音を変更する

NTTの「ナンバー・ディスプレイサービス」（有料）を契約することで、発信者番号ごとに着信ベル音を変更できます。着信したTELポートごとに、ベル音を2種類から選ぶこともできます。



ここでは、電話機を使って設定する方法を説明します。パソコンを接続している場合は、Webブラウザを使って設定することもできます。

1 **受話器を上げる。**



発信音が聞こえます。

2 **＊と＃を押す。**

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 **ダイヤルボタンを3、8（機能番号38）と押す。**

4 **TELポート番号を指定する。**

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

＊を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

5 **着信ベル音番号を指定する。**

着信ベル音は1と2から選べます。

ご注意

お使いのアナログ機器によっては、着信音が鳴らない場合があります。

6 **発信者番号を押す。**

7 **＃を押す。**

「ピー」という音が聞こえて設定が変更されます。

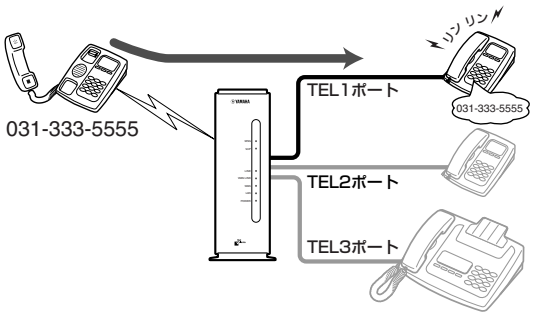
「ピー、ピー」と聞こえるときは

正しく変更されていません。設定内容を確認して、手順3から操作し直してください。

8 **受話器を置く。**

ナンバー・ディスプレイを利用する

ナンバー･ディスプレイは、着信時に発信者の電話番号を表示するサービスです。NTTの「ナンバー･ディスプレイサービス」(有料)を契約することで、電話に出る前に相手の電話番号が確認できます。また、通話中に着信したときも電話番号を表示できるキャッチホン･ディスプレイサービスも利用できます。



ご注意

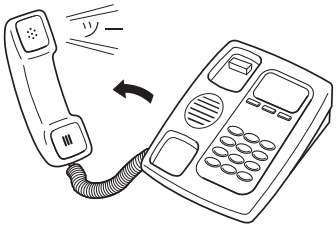
ナンバー･ディスプレイやキャッチホン･ディスプレイを利用するには、ナンバー･ディスプレイやキャッチホン･ディスプレイ対応の電話機やFAXが必要です。

ここでは、電話機を使って設定する方法を説明します。工場出荷設定では「使用しない」になっています。パソコンを接続している場合は、Webブラウザを使って設定することもできます。

ご注意

本設定の前に、お使いの電話機やFAXのナンバー･ディスプレイが利用できる設定になっていることを確認してください。

1 受話器を上げる。



発信音が聞こえます。

2 ⊛ と ⌗ を押す。

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 ダイヤルボタンを3､9(機能番号39)と押す。

4 TELポート番号を指定する。

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

⊛ を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

5 ナンバー･ディスプレイの種類を指定する。

- ナンバー･ディスプレイを使用しない場合:0を押します。
- ナンバー･ディスプレイのみを使用する場合:1を押します。

ご注意

キャッチホン･ディスプレイは、設定に関わりなく接続した電話機で機能します。

6 ⌗ を押す。

「ピー」という音が聞こえて設定が変更されます。

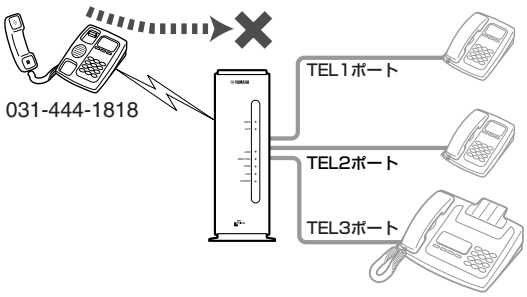
「ピー、ピー」と聞こえるときは

正しく変更されていません。設定内容を確認して、手順3から操作し直してください。

7 受話器を置く。

着信拒否を設定する

NTTの「ナンバー・ディスプレイサービス」（有料）を契約することで、登録した電話番号の着信を拒否したり、登録番号以外の着信を拒否することができる識別着信機能が使用できます。迷惑電話でお困りのときに便利です。

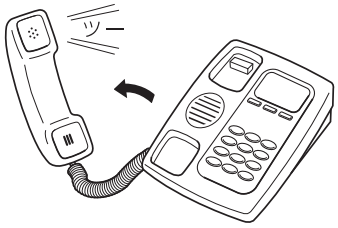


ご注意

- 着信拒否の設定などによって、本機のどのTELポートにも着信できない状態になっている場合は、発信側では着信拒否を示す音ではなく、通常の呼び出し音が鳴り続けます。
  この状態で着信による呼び出しが続いている間（LINEランプが点滅中）は、本機に接続した電話機から一般回線へ発信することはできません。
- TELポートに接続されている電話機のオフフック操作とLINEポートへの着信タイミングによっては、着信拒否設定に関わらず無条件に着信に応答してしまう場合があります。

ここでは、電話機を使って設定する方法を説明します。パソコンを接続している場合は、Webブラウザを使って設定することもできます。

1 受話器を上げる。



発信音が聞こえます。

2 ✱ と # を押す。

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 ダイヤルボタンを3、3（機能番号33）と押す。

4 TELポート番号を指定する。

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

✱ を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

5 拒否したい電話番号をダイヤルする。

6 # を押す。

「ピー」という音が聞こえて設定が変更されます。

「ピー、ピー」と聞こえるときは

正しく変更されていません。設定内容を確認して、手順3から操作し直してください。

7 ダイヤルボタンを3、2（機能番号32）と押す。

8 TELポート番号を指定する。

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

✱ を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

9 着信拒否の種類を指定する。

- 手順5で指定した番号を拒否する場合：2を押します。
- 手順5で指定した番号以外を拒否する場合：1を押します。
- 使用しない場合：0を押します。

10 # を押す。

「ピー」という音が聞こえて設定が変更されます。

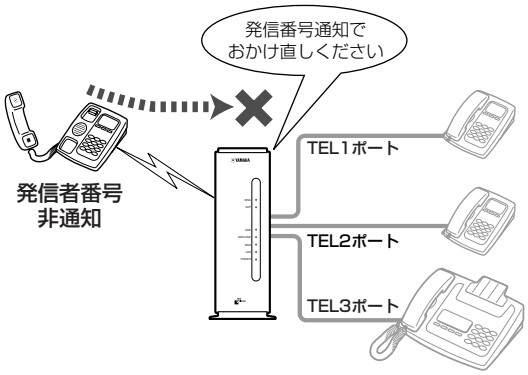
「ピー、ピー」と聞こえるときは

正しく変更されていません。設定内容を確認して、手順7から操作し直してください。

11 受話器を置く。

擬似ナンバー・リクエストを設定する

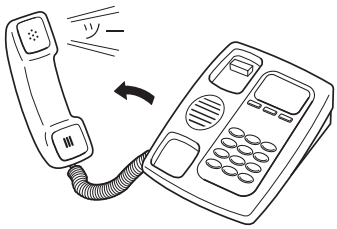
NTTの「ナンバー・ディスプレイサービス」（有料）を契約することで、発信者番号通知がない着信に対して番号を通知してかけ直すよう音声案内（トーキ）を流す擬似ナンバー・リクエスト 機能が使用できます。



ご注意

擬似ナンバー・リクエストを使用すると、発信者側に通話料金がかかります。

1 **受話器を上げる。**



発信音が聞こえます。

2 **(✱) と (#) を押す。**

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 **ダイヤルボタンを8、3（機能番号83）と押す。**

4 **TELポート番号を指定する。**

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

(✱) を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

5 **動作を指定する。**

- 発信者番号情報なし着信を拒否する場合：0を押します。
- 発信者番号情報なし着信を許可する場合：1を押します。
- 擬似ナンバー・リクエストで拒否する場合：2を押します。

6 **擬似ナンバー・リクエストを実行する条件を指定する。**

- 公衆電話からの着信に対して実行する場合：1を押します。
- ユーザによる通知拒否の着信に対して実行する場合：2を押します。
- 表示圏外の着信に対して実行する場合：3を押します。
- すべての着信に対して実行する場合：(✱) を押します。

7 **(#) を押す。**

「ピー」という音が聞こえ、設定が変更されます。

「ピー、ピー」と聞こえるときは

設定内容が適切でなかったり、正常に変更されていません。設定内容を確認して、手順3から操作し直してください。

8 **受話器を置く**

続けて設定するときは、受話器をあげたまま手順3～7の操作を繰り返します。

Lモードの機能を利用する

「Lモード」とは、東日本電信電話株式会社（NTT東日本）および西日本電信電話株式会社（NTT西日本）が提供する、電話機やFAXを使ってメールを送受信したり、情報を検索したりできるサービスです。

Lモード対応電話機やFAXなどのアナログ機器を本機に接続すれば、Lモードのメッセージ到着お知らせサービスを利用できます。

ご注意

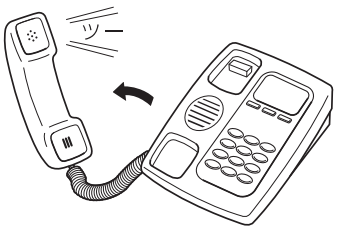
Lモードを利用するには、Lモード対応電話機／FAX以外に、NTT東日本またはNTT西日本との契約が必要です。

本機に接続したLモード対応電話機やFAXからLモードのメッセージ到着お知らせサービスを利用するには、以下の手順で設定を行います。

ご注意

- 設定の前に、お使いの電話機やFAXがＬモード対応製品であることを確認してください。
- 「かんたん設定ページ」の「TELポートの詳細設定（電話機対応機能）」画面の［ダイヤル終了から発信までの時間］の設定値、およびダイヤル桁の間隔設定（機能番号41、20ページ）は、初期設定値（6秒）より短くしないでください。

1 **受話器を上げる。**



発信音が聞こえます。

2 **㊅ と ㊉ を押す。**

発信音が止まり、「ツツー、ツツー」という音が聞こえます。

3 **ダイヤルボタンを8、6（機能番号86）と押す。**

4 **TELポート番号を指定する。**

TELポート番号は、TEL1=1、TEL2=2、TEL3=3です。

㊅ を押すと、設定に使っている電話機が接続されているTELポートが選ばれます。

5 **動作を指定する。**

- メッセージ到着お知らせ機能を使用しない場合：0を押します。
- メッセージ到着お知らせ機能を使用する場合：1を押します。

6 **㊉ を押す。**

「ピー」という音が聞こえ、設定が変更されます。

「ピー、ピー」と聞こえるときは

設定内容が適切でなかったり、正常に変更されていません。設定内容を確認して、手順3から操作し直してください。

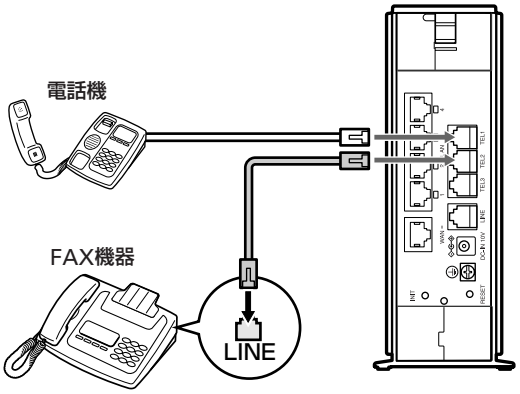
7 **受話器を置く。**

FAX 機器を使う

FAX機器をお持ちの場合は、本機のTELポートに接続して、これまでと同様に使えます。

FAX機器を接続する

FAX機器は、下図のように接続します。



FAX送受信のしかた

今までと同様にFAX機器から送受信できます。詳しい操作方法については、お使いのFAX機器の取扱説明書をご覧ください。

ご注意

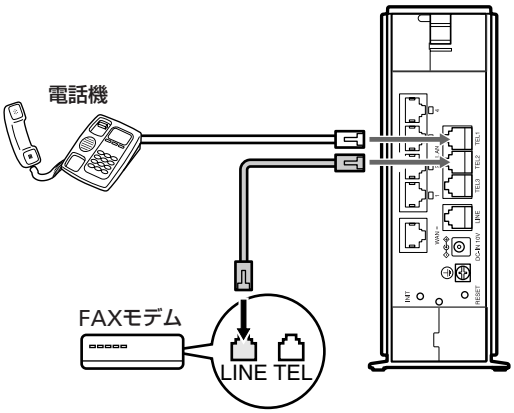
- FAXやモデムでデータの送受信ができないときやエラーが多いときは、「かんたん設定ページ」や電話機からTELポート側の受信や送信の音量レベル(PAD調整)値を徐々に下げて調整してください(21ページ)。
- FAXと電話をTELポートごとに使い分ける場合は、モデム信号方式のダイヤルインサービスへ加入する必要があります(38ページ)。

FAX モデムを使う

FAXモデムをお持ちの場合は、FAXモデムを本機のTELポートに接続して、パソコンでFAXを送受信できます。

FAXモデムを接続する

FAXモデムは、下図のように接続します。



ご注意

FAXモデムの中には、FAXモデムのTELポートにさらに電話機を接続できるものもありますが、この場合モデムに接続した電話機とモデムの着信を使い分けることはできません。FAXモデムや電話機によっては正しく動作しない場合がありますので、本機の別のTELポートに直接接続することをおすすめします。

パソコンの設定について

すでにパソコンでFAXを送受信していた場合は、現在お使いのFAXソフトをそのまま使用できます。詳しい操作方法については、お使いのFAXソフトウェアの取扱説明書をご覧ください。

FAX送受信のしかた

すでにパソコンでFAXを送受信していた場合は、今までと同様にFAXを送受信できます。詳しい操作方法については、お使いのFAXソフトウェアの取扱説明書をご覧ください。

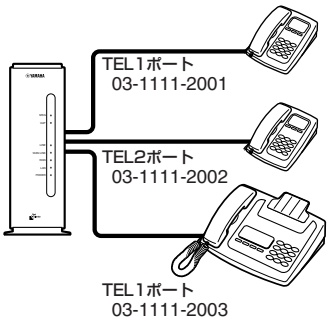
ご注意

FAXやモデムでデータの送受信ができないときやエラーが多いときは、「かんたん設定ページ」または電話機からTELポート側の受信や送信の音量レベル(PAD調整)値を徐々に下げて調整してください(21ページ)。

TEL ポートごとに使い分ける

本機のTELポートに接続したアナログ機器に合わせて、TELポートごとにさまざまな設定を行うことができます。お使いのアナログ機器や付加サービスに応じて設定してください。設定は「かんたん設定ページ」の電話設定画面で行います。

ここでは、図のようにアナログ機器を接続した場合の設定例を紹介します。



ダイヤルインサービスの設定例

ダイヤルインサービスは、契約者回線番号とは別にいくつかの電話番号を追加できるサービスです。ダイヤルイン番号毎に着信条件を設定することにより、機器を指定して電話をかけることができます。

ご注意

アナログ回線のダイヤルインサービスには、以下の2種類があります。

- モデム信号方式のダイヤルインサービス
- PB信号方式のダイヤルインサービス

本機のLINEポート側（一般回線側）は、モデム信号方式のダイヤルインサービスのみ対応しています。PB信号方式のダイヤルインサービスには対応していません。

「電話設定」画面の設定例

ここでは、契約者回線番号「03-1111-2001」をTEL1ポートの電話機、FAX用のダイヤルイン番号「03-1111-2002」をTEL2ポートのFAXで使い分ける例を紹介します。

ご注意

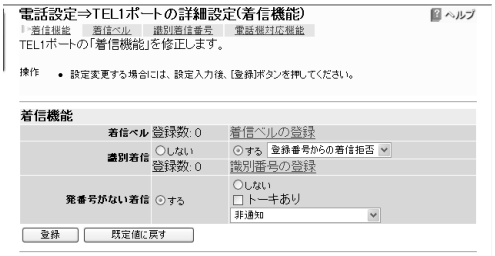
- 各設定項目の詳細については、「かんたん設定ページ」のヘルプ画面をご覧ください。
- ダイヤルイン番号の設定などによって、本機のどのTELポートにも着信できない状態になっている場合は、発信側では着信拒否を示す音ではなく、通常の呼び出し音が鳴り続けます。この状態で着信による呼び出しが続いている間（LINEランプが点滅中）は、本機に接続した電話機から一般回線へ発信することはできません。
- Fネットの1,300Hzの呼出信号に対応しているFAXをお使いの場合、FAX無鳴動着信の項目を設定すると、無音でFAXを自動着信させることができます。なお、本機のLINEポート（一般回線）側は、Fネットの1,300Hzの呼出信号には対応していません。

TELポートごとの設定例

本機の「かんたん設定ページ」を使って、TELポートごとに着信機能や着信ベル音、識別着信番号、電話機対応機能を指定できます。以下の画面は、TEL1ポートの詳細設定画面です。

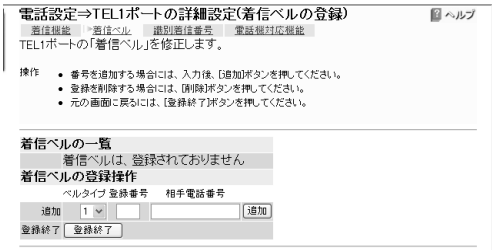
「着信機能」画面

TELポートに着信するときの条件を詳細に設定できます。



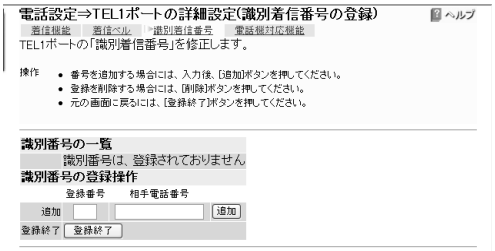
「着信ベル」画面

電話番号によって、着信ベルの種類を指定できます。



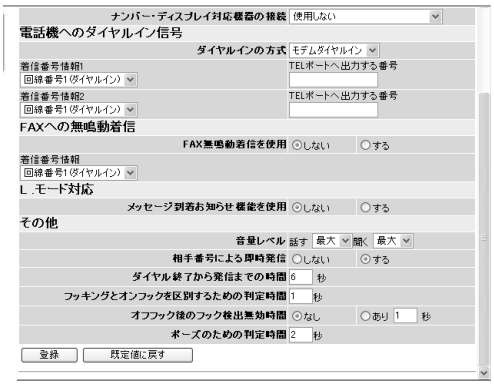
「識別着信番号」画面

友人や家族など、着信時に区別したい相手の電話番号を登録できます。



「電話機対応機能」画面

各種の電話サービスに関する設定や、電話機やFAXを接続する際の条件を詳細に設定できます。



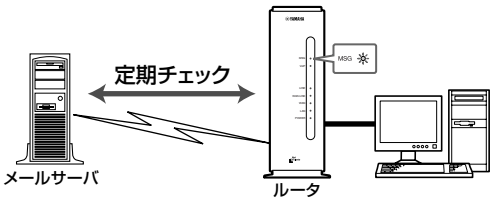
第4章 メール確認／通知機能を使う

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。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

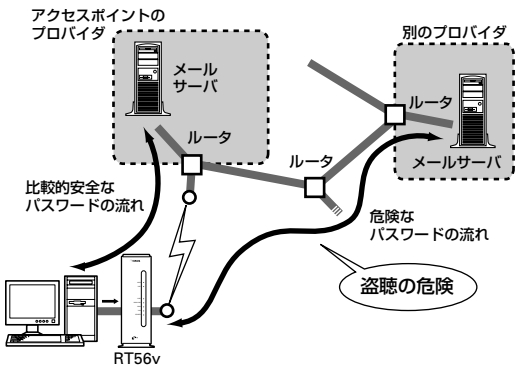
メール着信確認機能とは?

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

- プロバイダと接続中に他のプロバイダ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。

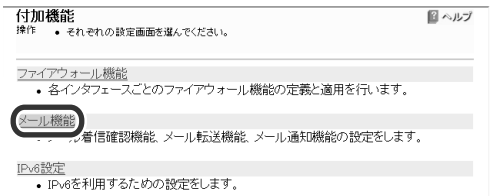
「ネットワーク パスワードの入力」画面が表示されます。

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。**

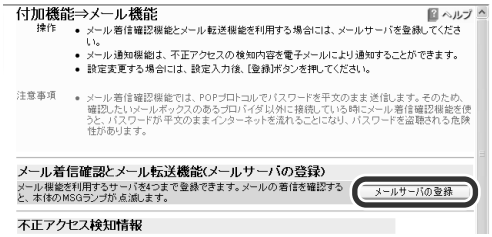
「トップ」画面が表示されます。

3 **画面左側の[付加機能]をクリックする。**

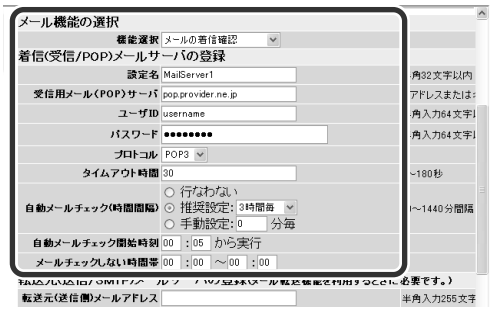
4 **[メール機能]をクリックする。**



5 **[メールサーバの登録]をクリックする。**



6 **確認したいメールアカウントに合わせて、必要な設定をする。**



機能選択　[メールの着信確認]を選びます。

設定名　わかりやすい名前を自由に入力できます（半角英数字で32文字まで）。

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。

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。

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
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
確認しない時間帯を設定します。

次のページにつづく▶

7 **画面下部の[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

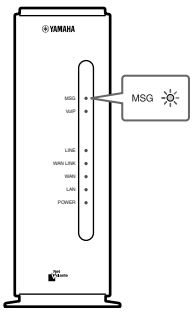
メールが届いていると、本機前面のMSGランプが点滅します。Webブラウザから手動で確認することもできます。

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。

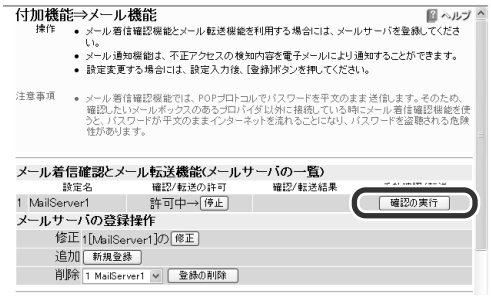
- 「ピカッ」(1回点滅):メールサーバ1にメール着信あり
- 「ピカッピカッ」(2回点滅):メールサーバ2にメール着信あり
- 「ピカッピカッピカッ」(3回点滅):メールサーバ3または4にメール着信あり

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 **41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。**

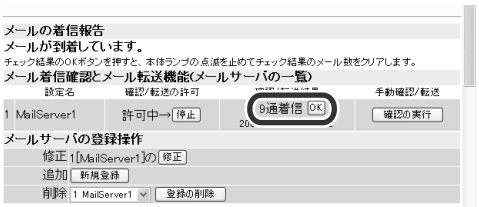


メールサーバに新規メールが届いているかどうか確認されます。確認した結果は、[確認/転送結果]欄に表示されます。

ご注意

プロバイダと接続中に他のプロバイダ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

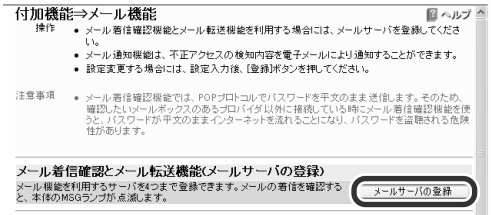
メール着信転送は、着信したメールを登録したメールアドレスへ転送する機能です。転送文字数を設定したり、送信元や題名などの、さまざまな転送条件を設定することもできます。

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。

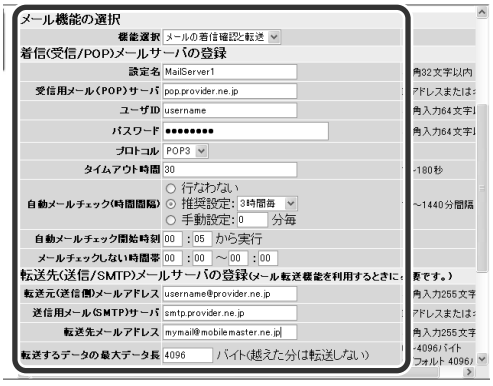
1 **41ページの手順1〜4を行って、本機の「かんたん設定ページ」の「メール機能」画面を開く。**

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、[メールサーバの登録操作]欄の[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。**



次のページにつづく▶

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 画面下部の[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10240バイト)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。

不正アクセス検知をメールで通知する

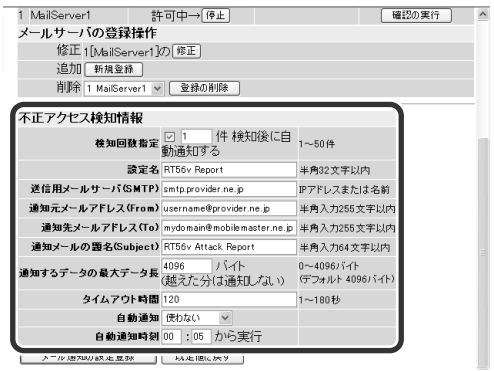
本機のファイアウォール機能(59ページ)で検知した不正アクセス記録を、指定したメールアドレスへ定期的に送信できます。

「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 41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]にチェックを付ける。

3 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。

通知日時指定
通知を送信する日時を指定したいときは、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。

通知メールの題名(Subject)
通知の題名を入力します。

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。

次のページにつづく▶

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。

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。

4 [メール通知の設定登録]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

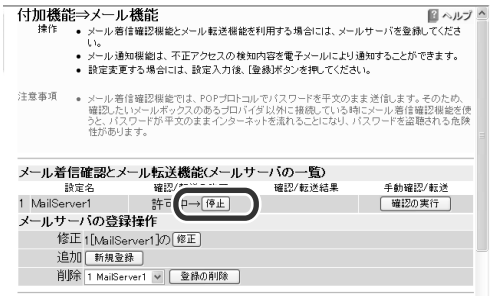
接続先プロバイダは、「プロバイダ接続管理」画面で設定したプロバイダになります。

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 41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。

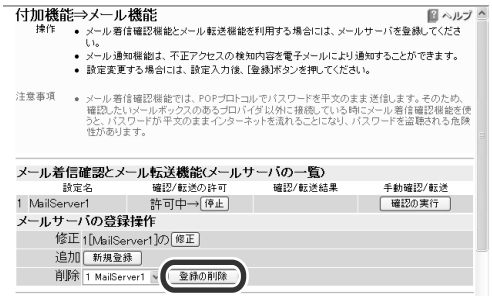
3 他のメールサーバのメールも中止したいときは、手順2の操作を繰り返す。

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 **41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。**

第5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、付属の「コマンドリファレンス」（PDF形式）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。

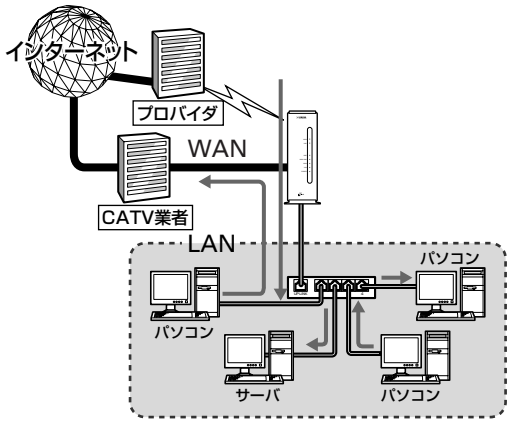
うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

本機のファイアウォール機能の概要

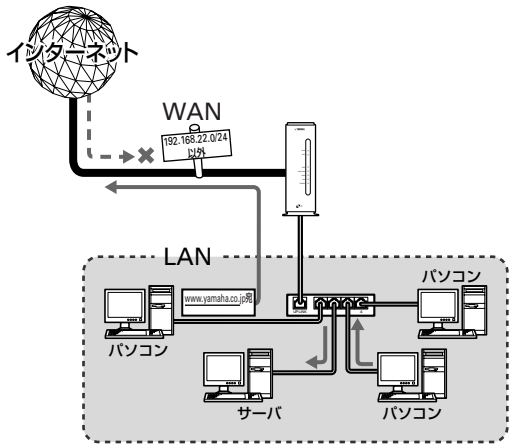
パケット単位のルーティング／セキュリティを設定できます

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自動接続を防止したり、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IPアドレスサービスの利用時やネットワーク型接続、接続時に割り当てられた動的アドレスを使い続けるCATVやADSL、フレッツ･ADSLなどで接続する場合は、十分なセキュリティを設定することをおすすめいたします。

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、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)
ネットワーク型ADSL接続	固定IPアドレス	✘✘✘(常に危険)

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から侵入するもの

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

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6または7

LAN間接続や、リモートアクセスサーバ運用の場合は

Netscape Navigatorを終了する際に、自動的にインターネットへの接続を開始してしまう問題を防ぐフィルタが適用されます。また、Windowsのセキュリティホールに関する定義も自動生成しますので、必要に応じて適用してください。

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)	230000～230099
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。

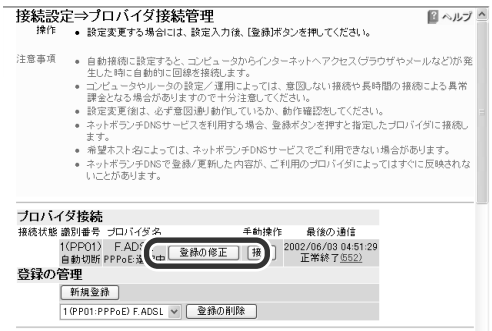
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

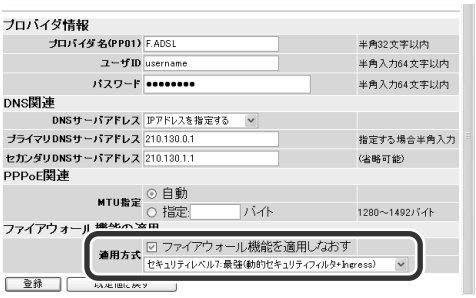
3 **画面左側の[接続設定]をクリックする。**

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。**

選んだセキュリティ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。

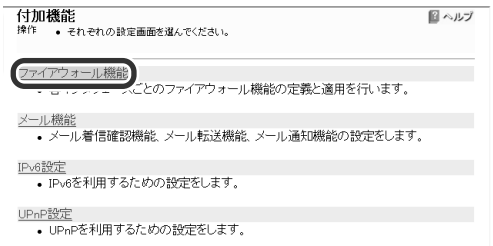
「ネットワーク パスワードの入力」画面が表示されます。

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。

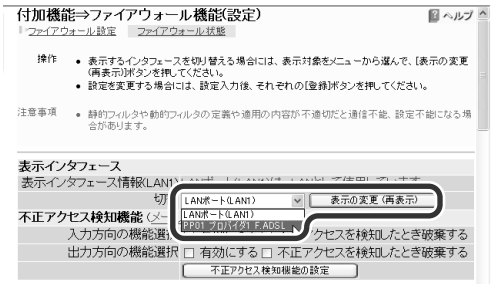
3 **[付加機能]をクリックする。**

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。**

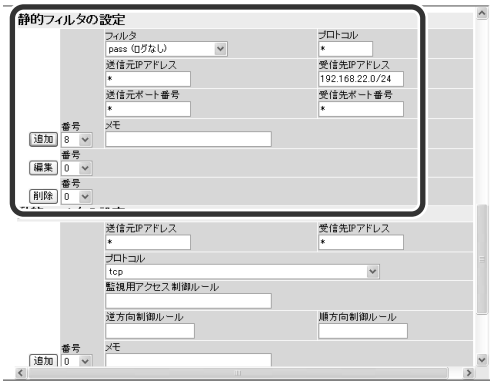
LANポートもひとつの接続先になります。



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」（56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。**

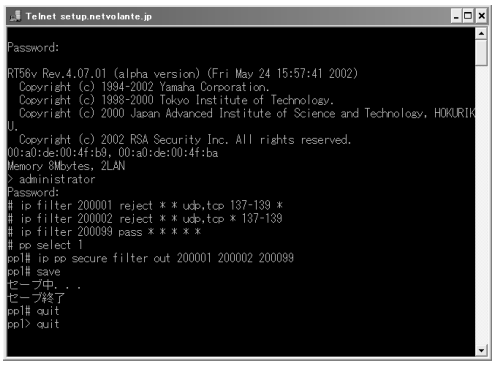
2 **「telnet setup.netvolante.jp」と入力してから、[OK]をクリックする。**

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。

設定例:

NetBIOSのデータで発信しないようにする

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

（どの機器から送信されたものであっても、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
```

（どの機器から送信されたものであっても、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」（次ページ）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。

設定例:

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

```
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」（次ページ）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、下記の接続先条件を例に説明しています。

- PP01：PPPoE を用いるADSL接続

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。

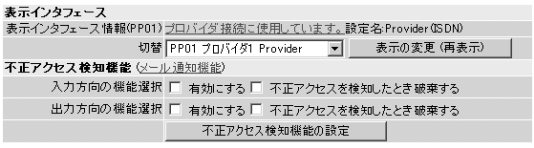
意図しない発信を防ぐフィルタの設定例

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。



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
22	☑	☑	reject	する	udp,tcp	*	137-139	*	*	
23	☑	☑	reject	する	udp,tcp	*	*	*	137-139	
24	☑	☑	reject	する	udp,tcp	*	445	*	*	
25	☑	☑	reject	する	udp,tcp	*	*	*	445	
99	☑	☑	pass	しない	*	*	*	*	*	

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」（124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
```

発信元IPアドレス偽装による不正アクセスを防ぐ

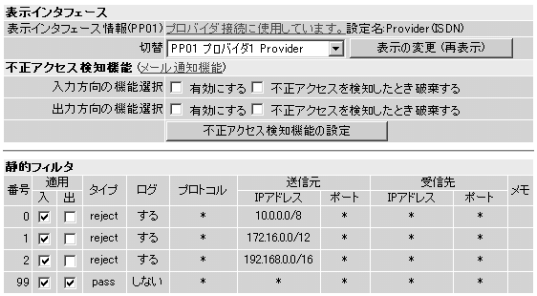
LAN内のプライベートIPアドレスを装って、LANの外から不正アクセスされることがあります。この手法は「ip spoofing攻撃」や「land攻撃」、「smurf攻撃」と呼ばれています。これらの攻撃を回避するには、発信元IPアドレスがプライベートIPアドレスの場合や自分に割り当てられたグローバルIPアドレスの場合に、パケットを通さないようなフィルタを設定します。

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。

プロバイダ接続で固定グローバル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
```

プロバイダ接続で固定グローバル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。

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
```

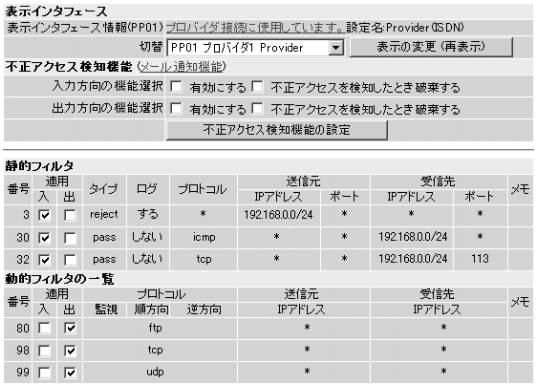
LAN側のネットワークを守る設定例（静的フィルタ+動的フィルタ）

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。

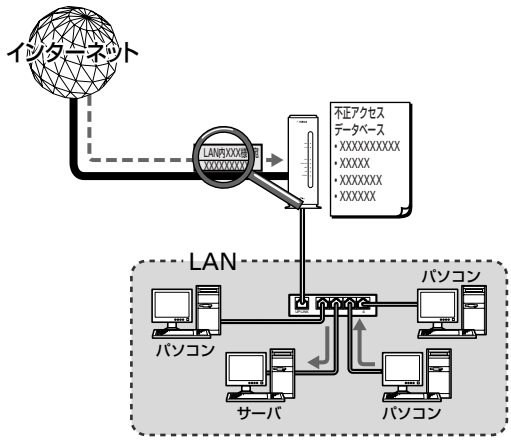


コンソールコマンドの場合

```
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および入出力に適用できますが、適用数によってはインターネットなどへのアクセス速度が遅くなる場合があります。

次のページにつづく▶

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および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。

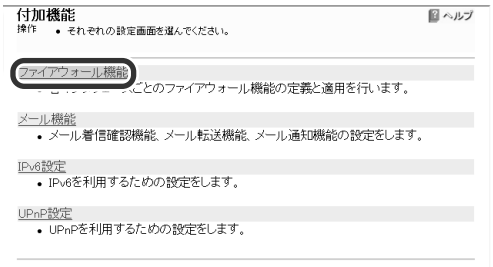
「ネットワーク パスワードの入力」画面が表示されます。

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。

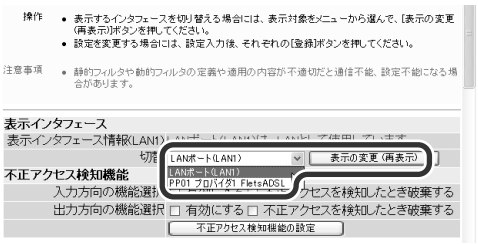
3 **［付加機能］をクリックする。**

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）を選びます。



6 **［不正アクセス検知機能］の［入力方向の機能選択］または［出力方向の機能選択］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。

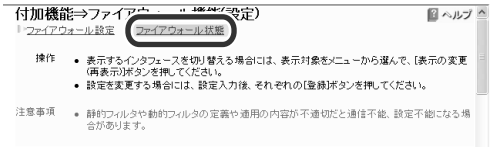
- **有効にする**：不正アクセスを検知すると、記録します。
- **不正アクセスを検知したとき破棄する**：不正アクセスを検知すると、不正アクセス検知履歴に記録してから、そのパケットを破棄します。

不正アクセス検知履歴を確認する

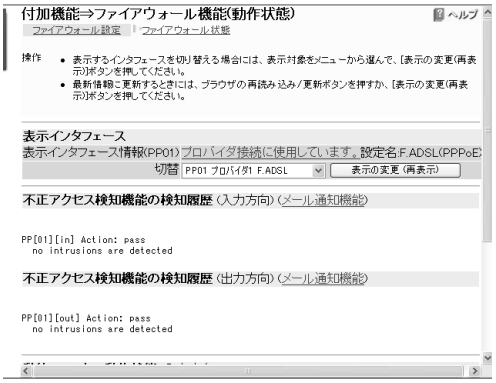
不正アクセス検知履歴は、「かんたん設定ページ」−「付加機能」−「ファイアウォール機能」−［ファイアウォール状態］画面で確認できます。

1 **60ページの手順1〜4の操作を行う。**

2 **［ファイアウォール状態］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」（44ページ）をご覧ください。

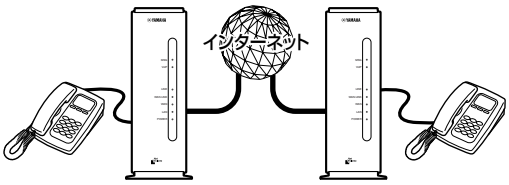
第6章 インターネット電話機能を使う

インターネット電話機能とは、ブロードバンド回線でインターネットに接続している場合に、インターネット経由でRT56vに接続した電話機間で会話できる機能です。その他にも、WindowsパソコンのWindows Messengerなどと音声チャットを楽しんだり、LAN内に設置したRT56v間で内線通話（機器間アナログ通話）を実現することもできます。より専門的な設定例については、付属の「コマンドリファレンス」（PDF形式）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。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

インターネット電話機能とは？

ADSLやCATVなどのブロードバンド回線でインターネットに接続している場合に、インターネット経由でRT56vに接続した電話機間で会話（VoIP通話）できる機能です。電話会社を通さずに通話するため、通常の電話料金はかかりません。



インターネット電話機能ご利用上のご注意

- **インターネット電話機能は、人の生命や高額な財産などを扱うような、高度な信頼性を要求される分野で使用する目的で設計されていません。**本機により発生したトラブルや損失について、当社では一切の責任を負いかねますので、あらかじめご了承ください。
- インターネット経由によるVoIP通話という特性上、インターネット電話機能による通話は第三者によって盗聴される可能性があります。あらかじめご了承ください。
- インターネット電話機能は、ADSLやCATVなどのブロードバンド回線でインターネットに接続している場合のみ利用できます（回線側に最低128kbit/sの帯域が必要です）。
- インターネット電話機能は、プロバイダからグローバルIPアドレスが割り当てられている環境でのみ、利用できます。グローバルIPアドレスとは、下記以外のIPアドレスです。
  - 10.0.0.0～10.255.255.255
  - 172.16.0.0 ～172.31.255.255
  - 192.168.0.0～192.168.255.255

  なお、グローバルIPアドレスが割り当てられていても、ネットワーク型プロバイダ接続でインターネットに接続している場合には、インターネット電話機能を利用できないことがあります。

  また、プライベートIPアドレスの場合でも、LAN内であればインターネット電話機能を利用できます。
- 通話料は無料ですが、インターネットの利用料金（プロバイダ料金および回線料金）が別途かかります。
- インターネット電話機能は、ネットワークが混雑すると、音声が途切れる場合があります。
- インターネット電話では、FAXやモデムは使用できません。

インターネット電話機能のダイヤル方法は?

1.識別番号+通常の電話番号

sipアドレスという仕組みを使って電話番号を「電話ユーザ名」と組み合わせて登録すると、通常の電話と同様に電話をかけられるようになります。

例:電話番号「03-1111-2001」を「sip:rt56v@yamaha.netvolante.jp」というsipアドレスに対応するように登録すると

インターネット電話に対応する識別番号(プレフィックス)をダイヤルしてから03-1111-2001にダイヤルすると、自動的に「sip:rt56v@yamaha.netvolante.jp」宛にインターネット電話をかけます。

したがって、インターネット電話機能を使用する場合は、通話相手がお互いのsipアドレスを知っている必要があります。sipアドレスは、「sip:電話ユーザ名@ホストアドレス」の形式で表されます。

sipアドレスの例

- sip:rt56v@yamaha.netvolante.jp
- sip:rt56v@133.176.200.1
- sip:rt56v@12345678.tel.netvolante.jp

電話ユーザ名は、本機のTELポートごとに任意に設定できます。ホストアドレスをすでに取得している場合はそのアドレスまたはグローバルIPアドレス、ネットボランチDNSサービスで取得した場合は電話アドレスをそれぞれ指定します。

2.ネットボランチ電話番号

ネットボランチDNSサービスを利用すると、8桁のネットボランチ電話番号が割り当てられます。(#)(#)のあとに割り当てられたネットボランチ電話番号をダイヤルすることで、お互いに通話できるようになります。

操作の流れ

インターネット電話機能を利用するには、以下の準備が必要です。

1.インターネット電話を利用できるようにする

工場出荷状態では、インターネット電話は利用しない設定になっています(64ページ)。

2.通話相手を登録する

本機のインターネット電話帳に、インターネット電話での通話相手を登録します(66ページ)。

なお、ネットボランチDNSサービスによって取得した電話番号(ネットボランチ電話番号)へダイヤルする場合は、電話番号をあらかじめ登録する必要はありません。

3.ネットボランチDNSサービスを利用できるようにする(ネットボランチ電話番号を取得する)

インターネット電話を利用するには、通話相手がお互いのグローバルIPアドレスを知っている必要があります。しかし、インターネットに常時接続している場合でも、割り当てられるグローバルIPアドレスは再接続時または時間によって変更される場合があります。

ネットボランチDNSサービスの電話アドレスサービスを利用すると、グローバルIPアドレスが変更されるごとにネットボランチ電話番号の対応付けが行われるようになります。変更されるごとに手動で設定する必要がなくなるので、便利です(67ページ)。

ご注意

ネットボランチDNSサービスをご利用になる前に、必ず「ネットボランチDNSサービスのご利用にあたって」(64ページ)および「ネットボランチDNSサービス利用規約」(100ページ)をご覧ください。

4.インターネット電話で通話する

「かんたん設定ページ」で通話相手を指定してから電話機をダイヤルすると、登録した通話相手につながります。

ネットボランチ電話番号にダイヤルする場合は(#)(#)のあとに番号をダイヤルします。

ネットボランチDNSサービスのご利用にあたって

ネットボランチDNSサービスを利用すると、不特定多数の方から、お使いのルータにアクセスされることが想定されます。そのため、悪意の第三者による不正アクセスにより、損害を受ける場合があります。また、お使いのパソコンを経由して第三者に対して被害を及ぼす可能性もあります。

ネットボランチDNSサービスのご利用にあたっては、お使いのパソコンのセキュリティ対策には、自己責任にて十分ご配慮いただきますようお願いいたします。

DNSの正引き・逆引きについて

ネットボランチDNSサービスでは、登録ホスト名に関しての正引きはできますが、逆引きはできません。逆引きを行うと、登録ホスト名に対するIPアドレスは、接続先のプロバイダで使用しているホスト名になります。

ホスト名・ネットボランチ電話番号の登録および更新について

ご利用中のプロバイダによっては、ホスト名およびネットボランチ電話番号の登録／更新内容がネットボランチDNSサービスにすぐに反映されないことがあります。あらかじめご了承ください。

ホスト名について

登録時の希望ホスト名によっては、ネットボランチDNSサービスでご利用できない場合があります。あらかじめご了承ください。

この場合は、別のホスト名を指定してネットボランチDNSサービスをご利用頂きますようお願いいたします。

インターネット電話を利用できるようにする

ご注意

以下の手順にしたがってインターネット電話を利用できるように設定を変更すると、本機が再起動します。インターネットへの接続が一時中断されますので、ご注意ください。

1 ブロードバンド接続設定を行い、本機を接続状態にする。

プロバイダからグローバルアドレスが割り当てられていることを確認してください。グローバルIPアドレスは、「10.x.x.x」、「172.16.x.x～172.31.x.x」、「192.168.x.x」の3つの範囲以外のIPアドレスです。

ご注意

グローバルアドレスが割り当てられていない場合は、インターネット電話機能を利用できません。

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。

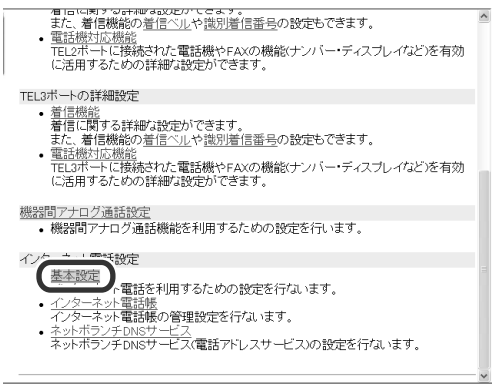
「ネットワーク パスワードの入力」画面が表示されます。

3 [パスワード]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。

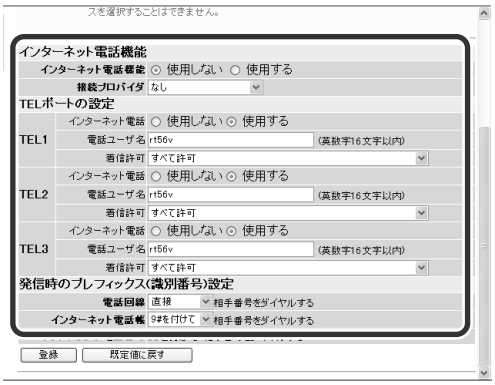
「トップ」画面が表示されます。

4 画面左側の[電話設定]をクリックする。

5 [インターネット電話設定]の[基本設定]をクリックする。



6 必要な設定を行う。



インターネット電話機能

インターネット電話を使うときは[使用する]を選び、使用する接続設定を[接続プロバイダ]から選びます。

TELポートの設定

TELポートごとに、インターネット電話の設定を行います。ポートごとに個別に設定できます。

- **インターネット電話:** インターネット電話を使うときは、[使用する]を選びます。インターネット電話を着信させたくないTELポートの場合は、[使用しない]を選びます。
- **電話ユーザ名:** ここに入力されたユーザ名が発信ユーザ名として使用されます。また、着信許可の設定で「電話ユーザ名が一致した場合に許可」または「電話ユーザ名またはネットボランチ電話番号と一致した場合は許可」に設定している場合は、着信の識別にも使われます。TELポートごとに異なった電話ユーザ名を指定すると、インターネット電話機能の電話番号であるsipアドレスを最大で3つまで使い分けられるため、便利です。
- **着信許可:** インターネット電話が着信したときの動作を選びます。

発信時のプレフィックス(識別番号)設定

- **電話回線:** 一般回線(アナログ回線)で通話したいときに、相手番号前にどのプレフィックスを付けてダイヤルするかを選びます。
- **インターネット電話帳:** インターネット電話帳の相手と通話したいときに、相手番号前にどのプレフィックスを付けてダイヤルするかを選びます。

ご注意

ネットボランチ電話番号の相手と通話するときのプレフィックスは ⑭⑭ に固定されていて、変更することはできません。

ヒント

TELポートごとに異なる電話ユーザ名を設定してから、着信許可を[電話ユーザ名が一致した場合]に設定すると、特定の発信先からのインターネット電話を好みのTELポートに着信するように指定できます。

7 設定が終わったら、[登録]をクリックする。

本機が再起動します。

引き続き通話相手を登録します。「通話相手を登録する」(66ページ)の手順4から操作してください。

通話相手を登録する

本機のインターネット電話帳に、インターネット電話での通話相手を登録します。

ヒント

- インターネット電話帳に通話相手を登録するには、相手のsipアドレス(インターネット電話ユーザ名やIPアドレスまたはホストアドレス)を入力する必要があります。これらの情報は、あらかじめ相手から聞いておくようにしてください。

  sipアドレスについて詳しくは、「インターネット電話機能のダイヤル方法は?」(63ページ)をご覧ください。
- ネットボランチ電話番号を直接ダイヤルする場合は、通話相手をインターネット電話帳に登録する必要はありません。

1 ブロードバンド接続設定を行い、本機を接続状態にする。

プロバイダからグローバルアドレスが割り当てられていることを確認してください。グローバルIPアドレスは、「10.x.x.x」、「172.16.x.x～172.31.x.x」、「192.168.x.x」の3つの範囲以外のIPアドレスです。

ご注意

グローバルアドレスが割り当てられていない場合は、インターネット電話機能を利用できません。

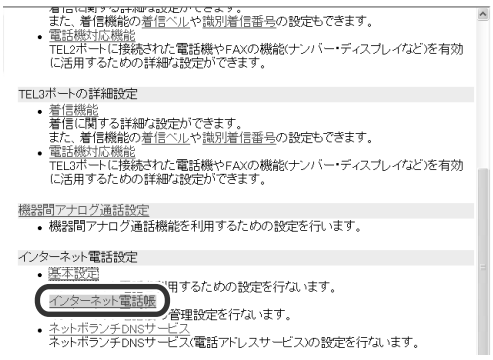
2 Webブラウザを起動して、本機の「かんたん設定ページ」を開く。

3 [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。

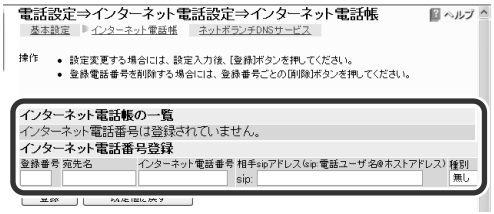
「トップ」画面が表示されます。

4 画面左側の[電話設定]をクリックする。

5 [インターネット電話設定]の[インターネット電話帳]をクリックする。



6 必要な設定を行う。



登録番号 好みの番号を入力します。

宛先名 相手の名前を入力します。

インターネット電話番号

通話相手の電話番号を入力します。あとでわかりやすいように、相手の通常の電話番号をそのまま入力しておくと便利です。

相手sipアドレス

通話相手の電話ユーザ名とホストアドレスを「@」で区切って入力します。

例:rt56v@yamaha.netvolante.jp

電話ユーザ名　ホストアドレス

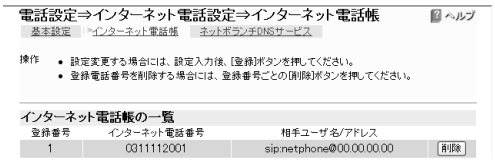
種別 相手がWindowsMessenger(またはMSN Messenger)のときは[登録メンバ]を選び、相手がネットボランチの時は[無し]を選びます。

ご注意

インターネットに常時接続している場合でも、割り当てられるグローバルアドレスは再接続時または時間によって変更される場合があります。
グローバルアドレスを直接設定する場合は、相手のアドレスが変わるごとに再設定が必要となりますので、ご注意ください。

7 設定が終わったら、[登録]をクリックする。

[登録]をクリックしたあとは、画面の指示に従って[追加する]をクリックします。
入力した通話相手先がインターネット電話帳に登録されます。



他の通話相手を続けて登録したいときは、手順6～7を繰り返します。

ネットボランチ電話番号を取得する

ネットボランチDNSサービスを利用すると、通話相手のグローバルIPアドレスが変更されるごとにインターネット電話帳の設定を変更する必要がなくなり、便利です。

ご注意

- ネットボランチ電話番号は、ネットボランチ1台につき1つしか取得できません。
- ネットボランチ電話番号は、それぞれのネットボランチに固有のMACアドレスと組み合わせて登録されています。そのため、すでにネットボランチ電話番号を取得しているネットボランチの設定ファイルを別のネットボランチに適用しても、ネットボランチ電話番号は利用できません。
- ご利用中のプロバイダによっては、ホスト名およびネットボランチ電話番号の登録／更新内容がネットボランチDNSサービスにすぐに反映されないことがあります。あらかじめご了承ください。

ネットボランチDNSサービスの設定をはじめて行う場合は

以下の手順7で[登録]をクリックすると、「ネットボランチDNSサービス利用規約」が表示されます。規約を読んで、同意するときは[利用規約に同意する]、同意しないときは[利用規約に同意しない]をクリックしてください。規約に同意されない場合は、ネットボランチDNSサービスをご利用いただけません。あらかじめご了承ください。

1 ブロードバンド接続設定を行い、本機を接続状態にする。

プロバイダからグローバルアドレスが割り当てられていることを確認してください。グローバルIPアドレスは、「10.x.x.x」、「172.16.x.x～172.31.x.x」、「192.168.x.x」の3つの範囲以外のIPアドレスです。

ご注意

グローバルアドレスが割り当てられていない場合は、インターネット電話機能を利用できません。

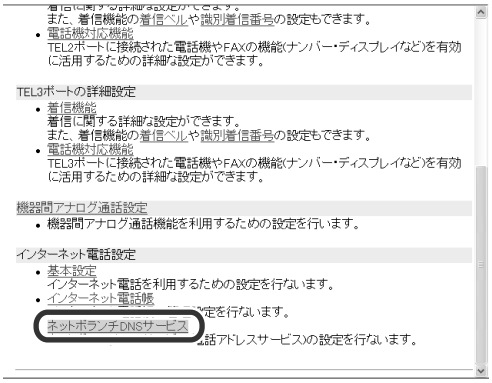
2 Webブラウザを起動して、本機の「かんたん設定ページ」を開く。

3 [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。

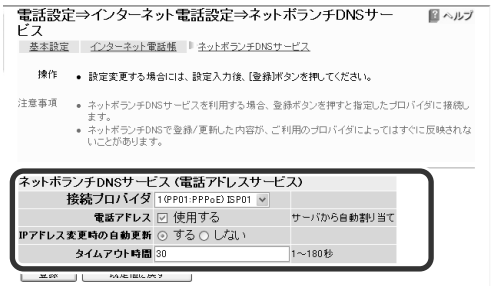
「トップ」画面が表示されます。

4 画面左側の[電話設定]をクリックする。

5 [インターネット電話設定]の[ネットボランチDNSサービス]をクリックする。



6 必要な設定を行う。



接続プロバイダ

ネットボランチDNSサービスを使用する接続プロバイダを選びます。端末型プロバイダ接続のみ利用できます。ネットワーク型プロバイダ接続で接続している場合は、ネットボランチDNSサービスは利用できません。

電話アドレス

ネットボランチDNSサービスを利用するときは、チェックを付けます。電話アドレスは自動的に割り当てられます。

IPアドレス変更時の自動更新

グローバルIPアドレスが変わった場合に、自動的にネットボランチDNSサーバにIPアドレス変更情報を通知したいときは、[する]を選びます。

タイムアウト時間

ネットボランチDNSサービスのタイムアウト時間を、秒で指定します。

7 **設定が終わったら、[登録]をクリックする。**

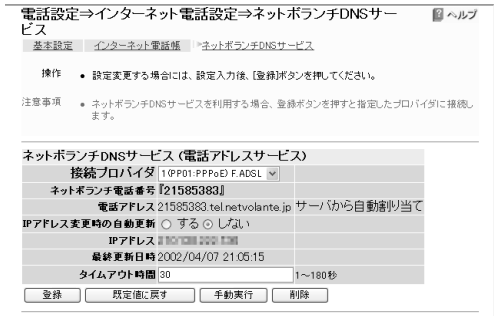
「ネットボランチDNSサービス利用規約」が表示されます。

8 **規約を読んで、同意するときは[利用規約に同意する]、同意しないときは[利用規約に同意しない]をクリックする。**

[利用規約に同意する]をクリックすると、ネットボランチDNSサービスの設定が変更され、電話アドレスの欄にネットボランチDNSサーバから割り当てられたアドレス(ネットボランチ電話番号)が表示されます。

取得できたネットボランチ電話番号をお互い知らせ合うことで、インターネット電話帳へ登録しなくても、インターネット電話をかけあうことができるようになります。

画面の表示例:



接続プロバイダ ネットボランチDNSサービスを使用する接続プロバイダが表示されます。

ネットボランチ電話番号

自分のネットボランチ電話番号が8桁で表示されます。相手先が ㊋、㊋ に続けてこの番号をダイヤルすると、本機につないだ電話機にインターネット電話が着信します。

電話アドレス ネットボランチDNSサービスから割り当てられた電話アドレスが表示されます。

IPアドレス 現在接続中のプロバイダから割り当てられているIPアドレスが表示されます。

最終更新日時 ネットボランチDNSサーバに更新を通知した最終日時が表示されます。

タイムアウト時間

ネットボランチDNSサービスのタイムアウト時間が表示されます。

ヒント

IPアドレス変更時の自動更新(67ページ)で[しない]を選んでいるときにプロバイダから割り当てられたグローバルIPアドレスが変更された場合は、この画面下部の[手動実行]をクリックします。

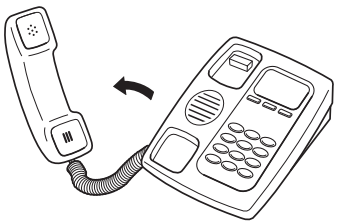
変更されたグローバルIPアドレスが、ネットボランチDNSサーバに通知されます。

インターネット電話で通話する

1 **受話器を上げる。**

発信音が聞こえます。

- **一般回線(アナログ回線)の外線に発信できる場合は:**「ツー」と聞こえます。
- **一般回線(アナログ回線)の外線に発信できない場合は:**「ツ･ツー」と聞こえます。



ご注意

一般回線(アナログ回線)をブロードバンド回線とは別に接続していない場合は、一般回線(アナログ回線)で電話はかけられません。

2 **登録した相手先の電話番号をダイヤルする。**

- **「発信時のプレフィックス(識別番号)設定」で識別用の番号を指定していた場合は:**
  電話番号をダイヤルする前に、識別用の番号(プレフィックス、例:9 (#))をダイヤルしてください。
- **相手のネットボランチ電話番号がわかっている場合は:**
  ネットボランチ電話番号の識別番号(プレフィックス、 (#)(#)) に続けて、番号をダイヤルしてください。

呼び出し音が聞こえ、相手が出ると通話できます。

ダイヤル例:

- **識別用の番号を6 (#) に設定している場合に、電話番号03-1111-2001にダイヤルする**
  6、(#)、0311112001の順にダイヤルします。
- **ネットボランチ電話番号12345678にダイヤルする**
  (#)、(#)、12345678の順にダイヤルします。

接続できないときに一般回線(アナログ回線)を使用して通話する場合は

相手の電話番号を直接ダイヤルしてください(工場出荷状態)。

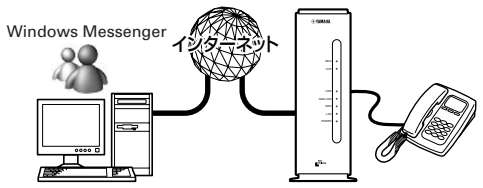
この場合は、通常の電話料金がかかります。

ヒント

ダイヤルした後に (#) を押すと、すぐに発信します。また、何も押さなくてもダイヤル桁の間隔設定で設定された時間(工場出荷時は6秒)を過ぎると、自動的に発信します。
詳しくは「電話機設定機能一覧」(20ページ)をご覧ください。

Windows Messengerと音声チャットする

Windows Messenger（またはMSN Messenger）のバージョン4.6以降と本機に接続した電話機で、インターネット電話機能による通話を楽しめます。相手先がインターネット電話機能に対応していなくても、Windows Messengerに対応したパソコンがあれば、インターネット経由で会話できます。



必要な環境を確認する

インターネット電話機能でWindows Messengerと音声チャットするには、以下の環境や設定が必要です。

- バージョン4.6以降のWindows Messenger（またはMSN Messenger）がパソコンにインストールされている。

  バージョンを確認するには、Windows Messengerの［ヘルプ］メニューから［バージョン情報］を選びます。バージョンが古い場合は、WindowsUpdateなどを使用してバージョンアップしてください。
- Windows Messenger（またはMSN Messenger）でマイクとスピーカーが使用できるように設定されている。
- Windows Messenger（またはMSN Messenger）がインストールされたWindowsパソコンとネットボランチに、それぞれグローバルIPアドレスが割り当てられている。

  通話相手のパソコンがグローバルIPアドレスの割り当てられているUPnP対応ルータ経由でインターネットに接続している場合でも、音声チャットを利用できます。詳しくは「通話相手がUPnP対応ルータ経由でインターネットに接続している場合は」（72ページ）をご覧ください。
- 「インターネット電話機能ご利用上のご注意」（62ページ）も合わせてご確認ください。

ご注意

以下の場合は、Windows MessengerやMSN Messengerによる音声チャットは使用できません。

- CATV接続など、プロバイダから割り当てられるIPアドレスがプライベートIPアドレスの場合
- プロバイダへ接続するために、ルータ型ADSLモデムを介して本機を接続している場合（グローバルIPアドレスが本機のWAN側インタフェースに割り当てられないため）

Windows Messengerの設定を変更する

1 **Windows Messengerを起動する。**

2 **Windows Messengerの［ツール］メニューから［オプション］を選ぶ。**

「オプション」画面が表示されます。

3 **［アカウント］タブをクリックする。**

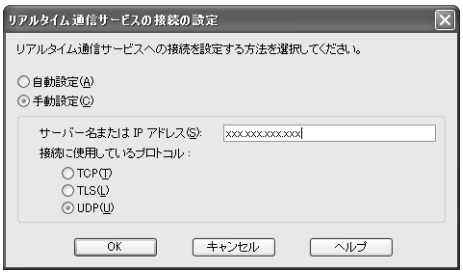
4 **［リアルタイム通信サービスユーザを含める］にチェックを付けてから、「サインイン名」に「適当なユーザ名@自分PCのIPアドレスまたはホスト名」（例：user@192.168.0.1）を入力する。**

5 **「サインイン名」の右側にある、［詳細設定］をクリックする。**

「リアルタイム通信サービスの接続の設定」画面が表示されます。

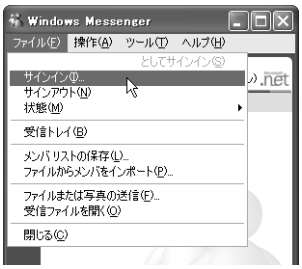
6 **[手動接続]を選んでから以下のように設定し、[OK]をクリックする。**

- **サーバ名またはIPアドレス**：通話したいネットボランチのグローバルIPアドレスまたはホスト名を入力する。
- **接続に使用しているプロトコル**：[UDP]を選ぶ。



7 **[OK]をクリックして、「オプション」画面を閉じる。**

8 **[ファイル]メニューから[サインイン]を選び、Windows Messengerにサインインし直す。**



これでWindows Messenger（またはMSN Messenger）と本機に接続した電話機で通話できるようになります。

ネットボランチの設定を変更する

インターネット電話帳に電話番号と相手のリアルタイム通信サービスに使用するユーザ名を登録します。

- 詳しくは「Windows Messengerの設定を変更する」（前ページ）の手順3、および「通話相手を登録する」（66ページ）をご覧ください。
- [種別]を[登録メンバ]にして設定すると、登録した通話相手が通話できる状態かどうか、「かんたん設定ページ」の「インターネット電話帳」画面でいつでも確認できます。

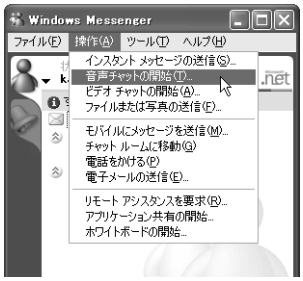
Windows Messengerからネットボランチへ発信する

ご注意

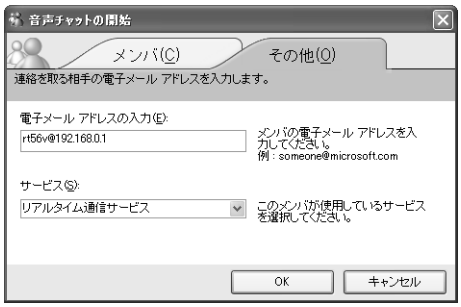
Windows Messengerからネットボランチに発信するには、相手先のネットボランチのグローバルIPアドレスに合わせて、発信する相手ごとにサーバの設定を変更する必要があります。詳しくは、「Windows Messengerの設定を変更する」(70ページ)をご覧ください。

1 Windows Messengerを起動する。

2 [操作]メニューから[音声チャットの開始]を選ぶ。



3 [その他]タブをクリックしてから、「電子メールアドレスの入力」に相手先のネットボランチのsipアドレスを入力し、「サービス」から[リアルタイム通信サービス]を選ぶ。



ヒント

sipアドレスとは、「電話ユーザ名@ネットボランチのグローバルIPアドレスまたはホストアドレス」です。電話ユーザ名は、相手先のネットボランチのインターネット電話機能で各TELポートに設定されているインターネット電話ユーザ名を入力してください。初期設定では、機種名になっています(例:rt56v@192.168.0.1)。

4 [OK]をクリックする。

相手先に発信します。

ネットボランチからWindows Messengerへ発信する

ネットボランチからは、[リアルタイム通信サービスユーザを含める]設定になっているWindows Messengerすべてに対して発信できます。相手先によって設定を変更する必要はありません。

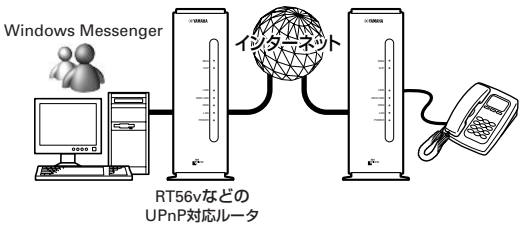
また、相手先がWindows Messengerの[リアルタイム通信サービス]のサーバを発信元のネットボランチに設定している必要はありません。

通常のインターネット電話機能と同様に、識別番号(プレフィックス)に続けて、番号をダイヤルする。

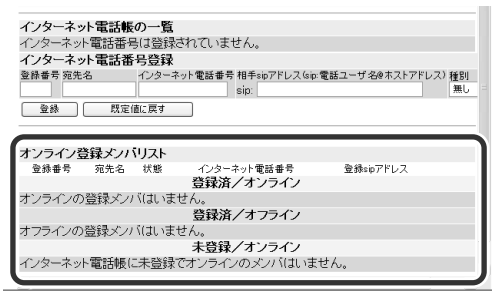
相手先に発信します。

通話相手がUPnP対応ルータ経由でインターネットに接続している場合は

グローバルIPアドレスの割り当てられているUPnP対応ルータ経由で通話相手が接続している場合は、「かんたん設定ページ」で通話相手が通話可能な状態(オンライン)かどうか確認できます。



「通話相手を登録する」(66ページ)の手順1〜5を行って、「インターネット電話帳」画面を表示します。



インターネット電話帳に登録した通話相手が、通話可能な状態(オンライン)かどうか確認できます。

ご注意

- 相手のWindowsMessengerが不正な終了をした場合は、相手が「オンライン」欄に表示されていても通話できないことがあります。
- WindowsMessengerで複数のネットボランチにサインインすることはできません。
- ネットボランチにサインイン中のWindowsMessengerのユーザ同士では、音声チャットはできません。

Windows Messengerとの音声チャットを切断する

ネットボランチ側で通話を止める

電話の受話器を置きます。

Windows Messenger側で通話を止める

[音声チャットの中止]をクリックするか、会話画面を閉じます。

音声チャットが正しく動作しないときは

音声チャットを開始できない場合は

Windows Messengerの通信上の仕様により、音声チャットのための接続に時間がかかることがあります。

また、接続に時間がかかりすぎると、接続されずにそのまま接続処理を中止してしまう場合があります。手順2から操作し直してください。

これまで接続できていた相手と接続できなくなった場合は

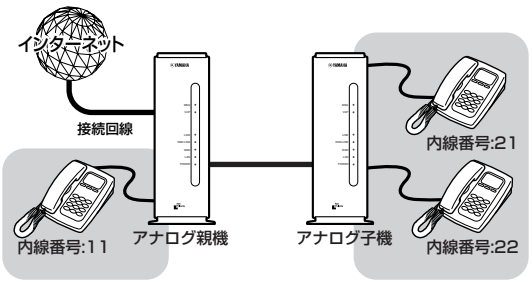
Windows Messengerの終了／起動を繰り返したり、ルータの再起動や回線の切断などによってパソコンとルータでUPnP機能の情報が異なると、正常に接続できなくなることがあります。

この場合は、回線を接続した状態でいったんWindows Messengerをサインアウトしてから、Windows Messengerを再起動します。それでも接続できない場合は、パソコンを再起動してください。

複数のルータ間で通話する（機器間アナログ通話）

本機の「機器間アナログ通話機能」を利用すると、複数のRT56vのTELポートをまとめて管理して、内線通話ができるようになります。また、1台のルータが一般回線（アナログ回線）に接続されていれば、他のルータのTELポートに接続した電話から外線通話をすることもできます。ルータは9台まで接続できます。

複数ルータ間で通話するときは、一般回線（アナログ回線）を接続しているルータにアナログ機器番号1、その他のルータにアナログ機器番号2～9を設定します。



ご注意

- アナログ子機に接続した電話機から機器間アナログ通話機能で外線通話すると、エコー（自分の話した声が遅れて聞こえてくる）が発生します。通話に支障があるような場合は、アナログ親機に接続された電話機で通話してください。
- 機器間アナログ通話機能は、ネットワークが混雑すると、音声が途切れる場合があります。
- アナログ子機にモデムやFAXを接続した場合、ネットワークの混雑状況により通信が途切れることがあります。このような場合はアナログ親機に接続してください。

アナログ子機にするルータの設定を変更する

最初にアナログ子機（一般回線を接続していないルータ）から設定を行います。

1 **Webブラウザを起動して、アナログ子機に設定するルータの「かんたん設定ページ」を開く。**

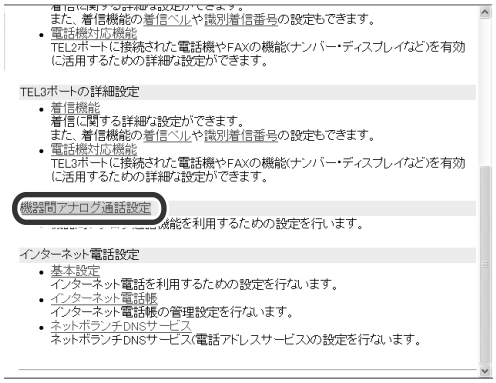
「ネットワーク パスワードの入力」画面が表示されます。

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。

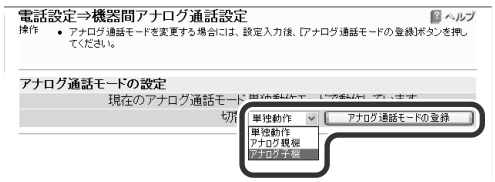
3 **画面左側の［電話設定］をクリックする。**

4 **［機器間アナログ通話設定］をクリックする。**



5 **モード設定で［アナログ子機］を選んでから、［アナログ通話モードの登録］をクリックする。**

メッセージにしたがって操作すると、設定が変更されます。



アナログ親機（一般回線を接続しているルータ）の設定を変更する

アナログ親機（一般回線を接続しているルータ）の設定をした後に、アナログ子機の機器番号を割り当てます。

1 **ブラウザを開き、アナログ親機に設定するルータの「かんたん設定ページ」を開く。**

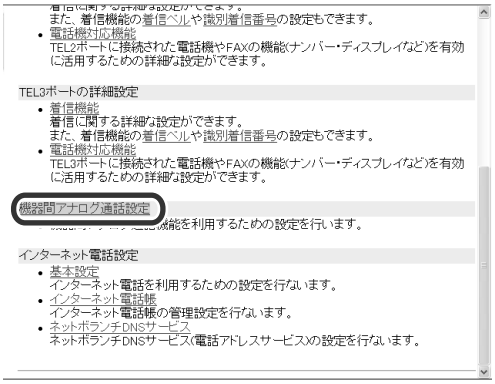
「ネットワーク パスワードの入力」画面が表示されます。

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。

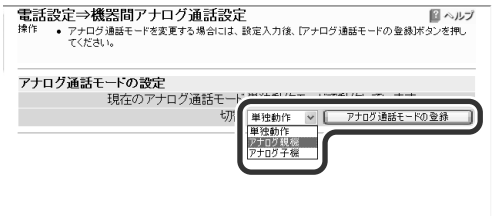
3 **画面左側の［電話設定］をクリックする。**

4 **［機器間アナログ通話設定］をクリックする。**



5 **モード設定で［アナログ親機］を選んでから、［アナログ通話モードの登録］をクリックする。**

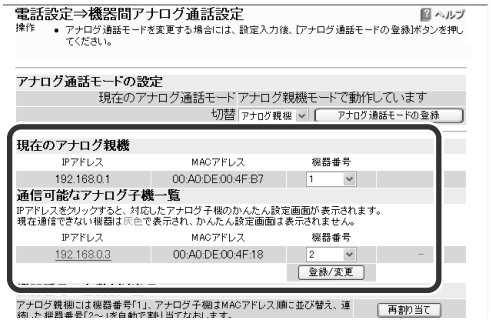
メッセージにしたがって操作すると、設定が変更されます。



アナログ親機の状態や通信可能なアナログ子機一覧が表示されます。

6 **現在のアナログ親機および通信可能なアナログ子機一覧で、アナログ親機と各アナログ子機の機器番号を選んでから、［登録/変更］をクリックする。**

メッセージにしたがって操作すると、設定が変更されます。



ヒント

アナログ親機と各アナログ子機の機器番号は、［再割り当て］をクリックして、自動設定することもできます。

7 **表示された現在のアナログ親機と通信可能なアナログ子機一覧に表示された、MACアドレスと機器番号をメモする。**

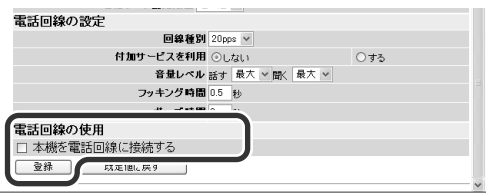
ご注意

アナログ親機と各アナログ子機の機器番号は、内線通話するときに必要になります。

8 **画面左側の［電話設定］をクリックする。**

9 **［基本設定］をクリックする。**

10 **［本機を電話回線に接続する］のチェックを外してから、［登録］をクリックする。**



これで機器間アナログ通話機能の設定は完了です。

ヒント

一般回線が2回線あり、アナログ子機にも一般回線を接続している場合は、アナログ子機側の［本機を電話回線に接続する］のチェックをはずす必要はありません。

通話する

外線にかける

ルータ間の接続の場合も、外線通話のかけかたはルータ1台の場合と同じです。受話器を取ってダイヤルすれば、通話できます。

1 **受話器を上げて、相手の電話番号をダイヤルする。**

呼び出し音が聞こえ、相手が出ると通話できます。

2 **通話が終わったら、受話器を置く。**

内線にかける

ルータ間の接続の場合も、内線通話、外線転送などの機能が使えます。ただし、内線番号は「機器番号＋TELポート番号」に変わります。

1 **受話器を上げて、✱ に続けて内線番号をダイヤルする。**

指定した内線番号のアナログ機器で呼び出し音が鳴ります。相手が出ると通話できます。

- アナログ子機2のTEL2ポートを呼び出す場合は、✱、2、2とダイヤルします。
- アナログ子機3の全TELポートを呼び出す場合は、✱、3、✱ とダイヤルします。
- 全ルータの全TELポートを呼び出す場合は、✱、✱とダイヤルします。

ご注意

指定した内線番号の機器が使用中のときは、呼び出し音は鳴りません。

2 **通話が終わったら、受話器を置く。**

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。

うまく動作しないときは、別冊の「**困ったときは**」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。

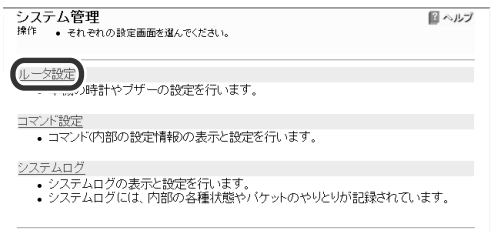
「ネットワーク パスワードの入力」画面が表示されます。

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。

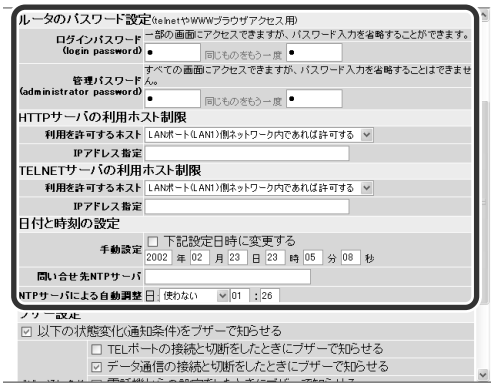
3 画面左側の[システム管理]をクリックする。

4 [ルータ設定]をクリックする。



次のページにつづく▶

5 必要なセキュリティ項目を設定する。



ログインパスワード

一般ユーザ用の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

ルータ管理者用の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ブラウザで本機の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。
- **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で本機の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。Webブラウザや電話機で設定してください。
- **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。

ブザー音の設定を変更する

本機にはブザーが内蔵されており、工場出荷状態ではインターネットへ接続するときと切断するときにブザー音が鳴るように設定されています。ブザー音は、「かんたん設定ページ」の「システム管理」画面で止めたり、鳴らしたりすることができます。

1 **パソコンでWebブラウザを起動して、[ファイル]メニューから[開く]を選ぶ。**

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。

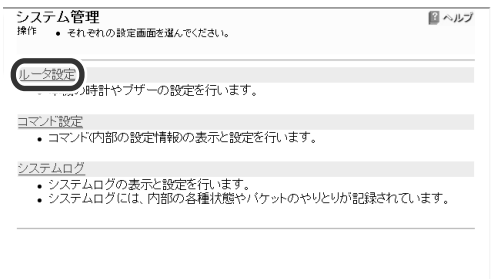
「ネットワーク パスワードの入力」画面が表示されます。

3 **ルータの管理パスワードまたはログイン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。

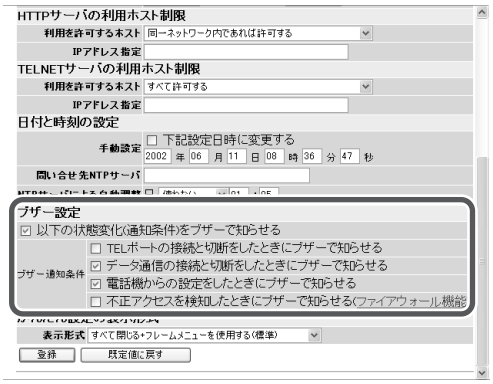
4 **画面左側の[システム管理]をクリックする。**

5 **[ルータ設定]をクリックする。**



6 **ブザー設定でブザー音の動作を設定する。**

設定できる条件は、以下の通りです。



以下の状態変化(通知条件)をブザーで知らせる

ブザー音を止めたいときはチェックを外します。鳴らしたいときはチェックを付けて、条件を選びます。

- **TELポートの接続と切断をしたときにブザーで知らせる**：TELポートに接続した電話機やFAXで発信／着信／切断するたびに、ブザーが鳴ります。
- **データ通信の接続と切断をしたときにブザーで知らせる**：ルータ機能で発信や切断するたびに、ブザーが鳴ります。
- **電話機からの設定をしたときにブザーで知らせる**：TELポートに接続した電話機で設定操作を行うと、ブザーが鳴ります。
- **不正アクセスを検知したときにブザーで知らせる(ファイアウォール機能)**：本機のファイアウォール機能を設定してある場合、不正アクセスを検知した時にブザーが鳴ります。

7 **設定が終わったら、[登録]をクリックする。**

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

- 固定IPアドレスサービスを契約していて、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。

ヒント

パソコンのIPアドレスを変更するには、「パソコンのIPアドレスを管理する」(124ページ)をご覧ください。

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 **画面左側の[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(129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(51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。

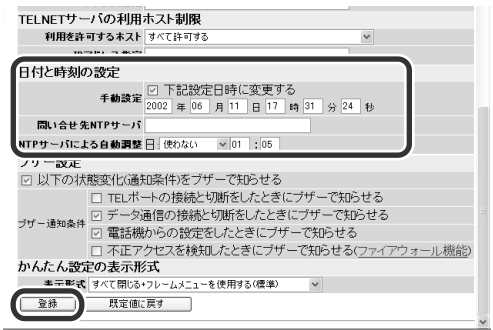
3 [システム管理]をクリックする。

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。

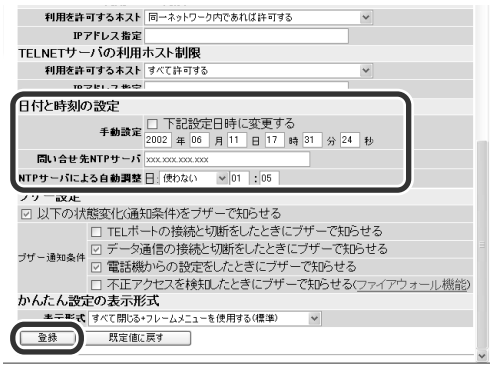
手動で時刻を入力して合わせる場合

[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

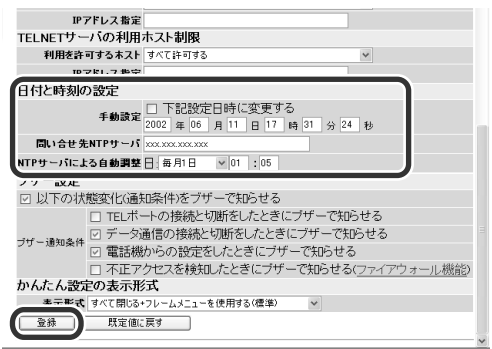
プロバイダの接続設定で「常時接続」を選ぶなどして、ファイアウォール機能のセキュリティレベルが4または5(静的セキュリティフィルタ)に設定されている場合は、NTPサーバからの応答パケットが破棄されてしまうため、時刻を合わせることができません。

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。



本機の設定情報を保存する

プロバイダに接続するために必要な情報や各種の設定情報は、本機の内部で1つの設定ファイル(config)として管理されています。この設定ファイルをパソコンに保存すると、設定のバックアップとして利用したり、設定ファイルをパソコンで編集したりできるので便利です。また、サポート窓口にお問い合わせいただく場合にも、設定ファイルの内容がわかった方がトラブルの早期解決につながることがあります。

ここではWindowsパソコンを使って、テキスト形式で本機の設定情報を保存する操作を例にして説明します。

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。**

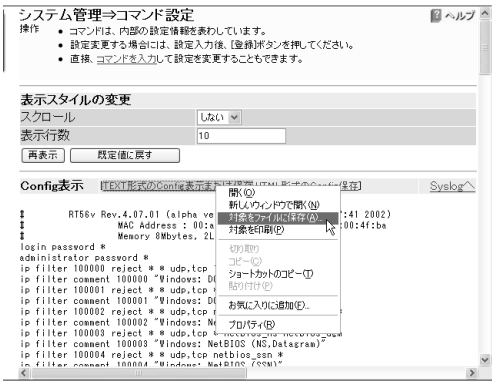
「トップ」画面が表示されます。

4 **画面左側の[システム管理]をクリックする。**

5 **[コマンド設定]をクリックする。**

本機の設定(config)情報が表示されます。

6 **[TEXT形式のconfig表示または保存]を右クリックして、[対象をファイルに保存]を選ぶ。**



7 **好みの保存場所とファイル名を指定してから、[保存]をクリックする。**

本機の設定(config)情報が保存されます。

ヒント

パソコンで編集した設定ファイルを本機に転送したいときは、あらかじめテキスト形式の設定ファイルの内容をクリップボードにコピーしておいてから、「コマンド設定」画面下部にある「コマンド入力」欄に貼り付けます(ペーストします)。

そのあとに[入力]をクリックすると、貼り付けた設定ファイルが本機に転送されます。

ご注意

ネットボランチ電話番号は、それぞれのネットボランチに固有のMACアドレスと組み合わせて登録されています。そのため、すでにネットボランチ電話番号を取得しているネットボランチの設定ファイルを別のネットボランチに適用しても、ネットボランチ電話番号は利用できません。

ネットワークゲームやICQ用に設定を変更する

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、以下の順序で問題を解決してください。

1.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)の設定を行ってみる(83ページ)。

2.DMZホスト機能を利用する(84ページ)。

ヒント

"PlayStation 2"対応のPlayOnline™ およびFINAL FANTASY® XIを使用する場合は、「PlayOnline™対応ネットワークゲーム用に本機の設定を変更する」(85ページ)をご覧ください。

静的IPマスカレード設定で問題を解決する

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」(124ページ)をご覧ください。

静的IPマスカレード設定を変更する

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。

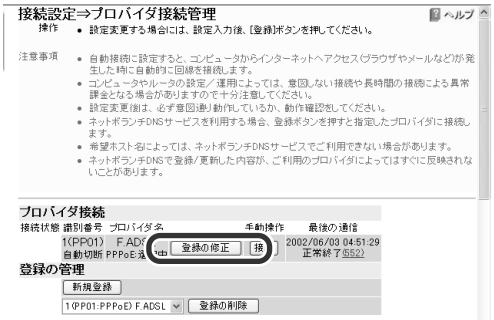
2 [パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。

「トップ」画面が表示されます。

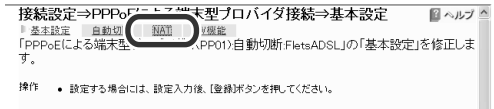
3 [接続設定]をクリックする。

4 [プロバイダ接続管理]をクリックする。

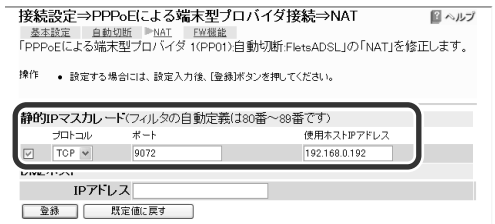
5 接続先名の右の[登録の修正]をクリックする。



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び、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。
- 代表的なソフトウェアについては、「かんたん設定ページ」の「NAT」画面で[ヘルプ]をクリックすると、使用するポート番号などの設定例を確認できます。

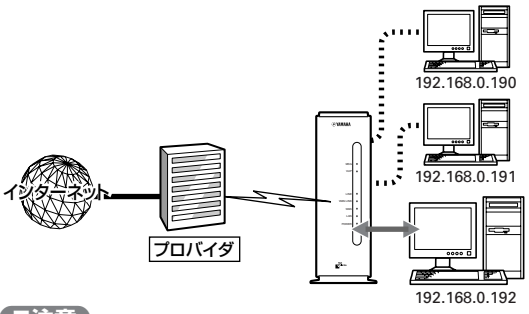
8 画面下にある[登録]をクリックする。

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。

DMZホスト機能を使って問題を解決する

DMZホスト機能を利用することで、本機がNAT/IPマスカレードテーブルに登録されていない宛先へのパケットを受信したときに、設定したIPアドレスのホストに転送するように設定できます。

192.168.0.192をDMZホストとして設定した例



ご注意

- DMZとはDeMilitarized Zone(非武装地帯)の略語です。DMZホスト機能を利用中は、DMZの名の通りパケットがNAT/IPマスカレードテーブルを素通りできるため、外部から意図しない進入、攻撃を受ける可能性があります。
- DMZホスト機能を、同時に複数のパソコンで利用することはできません。

ヒント

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

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
- DMZホストのIPアドレスを指定する

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」(124ページ)をご覧ください。

DMZホストのアドレスを指定する

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。**

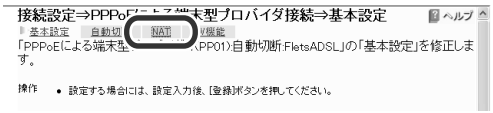
「トップ」画面が表示されます。

3 **[接続設定]をクリックする。**

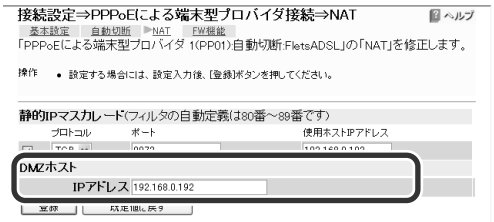
4 **[プロバイダ接続管理]をクリックする。**

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 **「DMZホスト」欄に、DMZホストとして使用したいパソコンの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。

PlayOnline™対応ネットワークゲーム用に本機の設定を変更する

“PlayStation 2”対応のPlayOnline™ およびFINAL FANTASY® XIを使用する場合は、以下の手順で本機の設定を変更してください。

1.ファイアウォール機能の設定を変更する

本機のファイアウォール機能のセキュリティレベルを変更して、ネットワークゲームが正常に動作するかどうか確認します。

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。

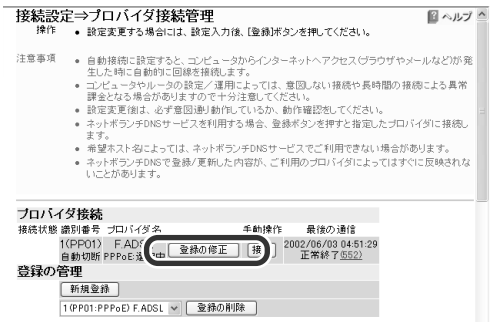
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

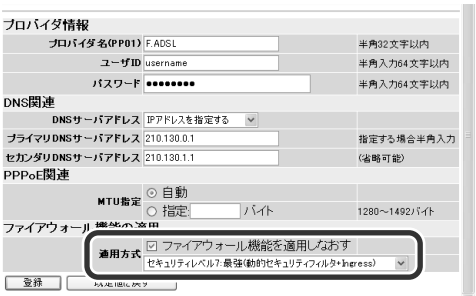
3 **[接続設定]をクリックする。**

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 **「ファイアウォールの適用」欄の[ファイアウォール機能を適用しなおす]にチェックを付けてから、セキュリティレベル6または7を選ぶ。**



7 **[登録]をクリックする。**

ファイアウォール機能のセキュリティレベルが変更されます。

この設定を行ってもネットワークゲームが正常に動作しない場合は

引き続き「2.静的フィルタを追加する」の操作を行ってください。

2.静的フィルタを追加する

PlayOnline™対応ネットワークゲームで使用するポート番号50000～65535（UDPプロトコル）を開放するフィルタを追加します。

ヒント

TCPポートに関しては、セキュリティフィルタの初期状態で内部から外部への通信をすべて通すようになっているので、特別な設定は不要です。

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。**

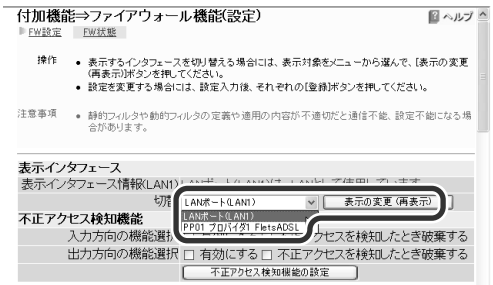
「トップ」画面が表示されます。

3 **画面左側の[付加機能]をクリックする。**

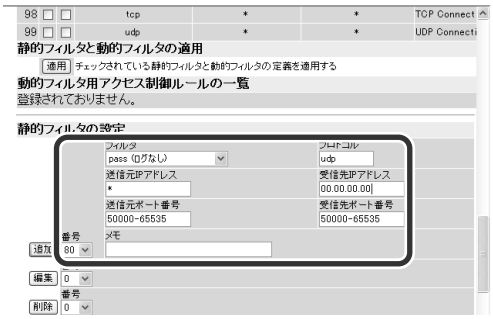
次のページにつづく▶

4 [ファイアウォール機能]をクリックする。

5 [表示インタフェース]で接続に使っているプロバイダを選んでから、[表示の変更(再表示)]をクリックする。



6 「静的フィルタの設定」欄で、以下のような静的フィルタを設定する。



フィルタ　[pass(ログなし)]を選びます。

プロトコル「udp」と半角英字で入力します。

送信元IPアドレス

半角英字で「*」と入力します。

受信先IPアドレス

“PlayStation 2”のIPアドレスを入力します。“PlayStation 2”のIPアドレスが本機のDHCP機能で割り当てられている場合は、「“PlayStation 2”のIPアドレスを確認する」(87ページ)の説明にしたがって確認してください。

送信元ポート番号

半角英数字で「50000-65535」と入力します。

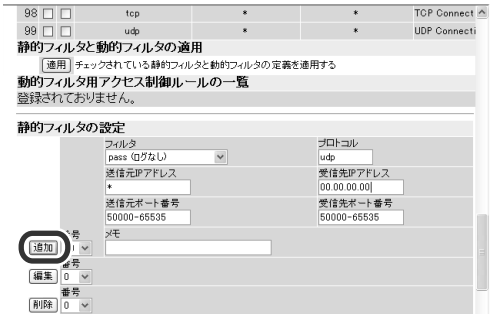
受信先ポート番号

半角英数字で「50000-65535」と入力します。

フィルタ番号

「追加」欄で「80」を選びます。

7 [追加]をクリックする。



8 「静的フィルタの一覧」欄で、追加した静的フィルタ80番の[入]と[出]にそれぞれチェックを付けてから、[適用]をクリックする。

これで必要な静的フィルタの設定は終了です。

“PlayStation 2”のIPアドレスを確認する

“PlayStation 2”のIPアドレスが本機のDHCP機能で割り当てられている場合は、以下の手順でIPアドレスを確認します。

1 **“PlayStation 2”のMACアドレスを調べる。**

“PlayStation 2”で［ネットワーク設定］→［ネットワーク接続設定］→［現在使用中の接続を選択］→［設定を変更］→［ホスト名設定］項目で、“PlayStation 2”のMACアドレスを確認します。確認したMACアドレスは、メモを取っておくことをおすすめします。

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。

「ネットワーク パスワードの入力」画面が表示されます。

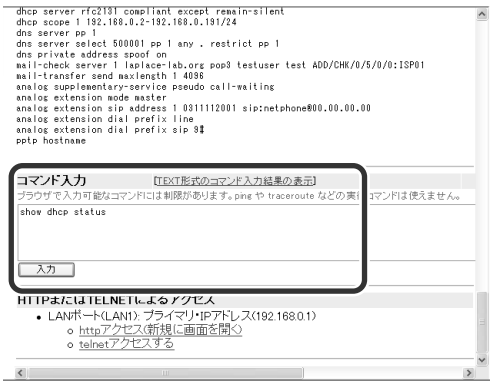
3 **［パスワード］入力欄にルータの管理パスワードを入力してから、［OK］をクリックする。**

「トップ」画面が表示されます。

4 **画面左側の［システム管理］をクリックする。**

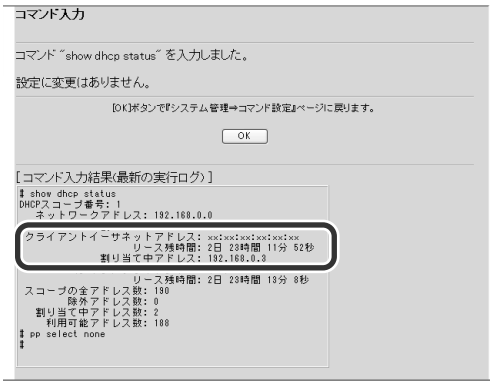
5 **［コマンド設定］をクリックする。**

6 **コマンド入力欄に半角英字で「show dhcp status」と入力してから、［入力］をクリックする。**



「コマンド入力結果」欄に現在のIPアドレス割り当て状況が表示されます。

7 **手順1で調べたMACアドレスが含まれている「クライアントイーサネットアドレス」行を探して、その行の下方にある「割り当て中アドレス」を調べる。**



この「割り当て中アドレス」に記載されているIPアドレスが、“PlayStation 2”のIPアドレスになります。

ヒント

“PlayStation BB Navigator”をお使いの“PlayStation 2”にインストールしている場合は、「UTILITY」→「システム設定」→「本体設定」で、“PlayStation 2”のMACアドレスを確認できます。

自動切断しないように設定する

インターネットに接続している間に、自動切断しない時間範囲を設定できます。

ご注意

- この設定はPPPoE方式でインターネットに接続している場合のみ利用できます。CATVやPPPoE方式以外のADSLで接続している場合は、インターネットに常時接続しています。
- 自動切断しないように設定しても、プロバイダや回線の都合で切断されることがあります。
- 本機の電源を切ると、設定時間内であっても接続が切れます。

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。

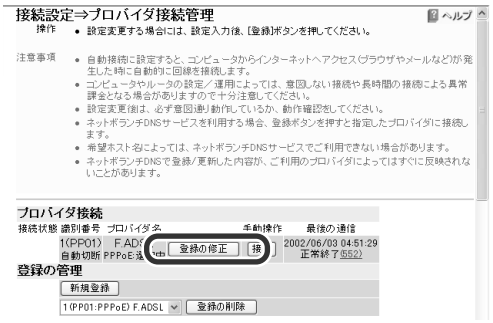
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

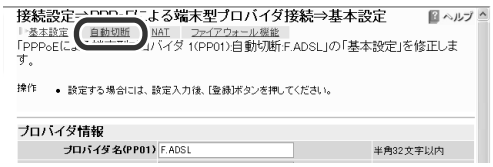
3 **画面左側の[接続設定]をクリックする。**

4 **[プロバイダ接続管理]をクリックする。**

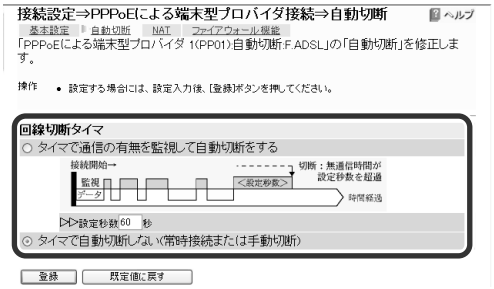
5 **接続先名の右の[登録の修正]をクリックする。**



6 **[自動切断]をクリックする。**



7 **回線接続タイマの動作を選ぶ。**



タイマで通信の有無を監視して自動切断をする

インターネットに一定時間接続していないときは、接続を切断します。この設定を選んだときは、切断するまでの時間を秒単位で指定できます。

タイマで自動切断しない

手動で切断操作を行わない限り、インターネットに常時接続します。

8 **画面下にある[登録]をクリックする。**

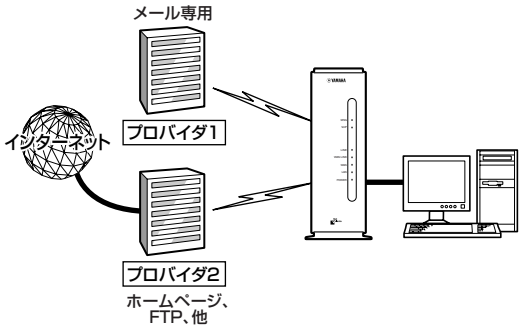
メッセージにしたがってボタンをクリックすると、設定が変更されます。

複数の接続先を使い分ける

複数のプロバイダを登録しておき、おもに使用するプロバイダとメールの確認のためだけにアクセスするプロバイダなど、目的に応じて接続先を使い分けることができます。

メール専用の接続先を使い分ける

メール着信確認機能でプロバイダに直接接続したい場合など、メールとその他のインターネット接続で接続先を使い分けられます。



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。**

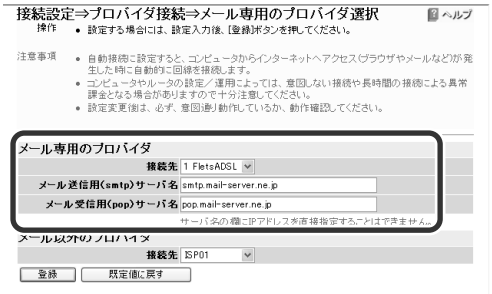
「トップ」画面が表示されます。

3 **画面左側の[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 **[複数のプロバイダに同時接続する]を選び、[メール専用のプロバイダ選択]を選んで[プロバイダへの接続方法の登録(同時接続設定)]をクリックする。**

6 **[メール専用のプロバイダ]の接続先で登録したプロバイダを選んでから、メールサーバ名を設定する。**



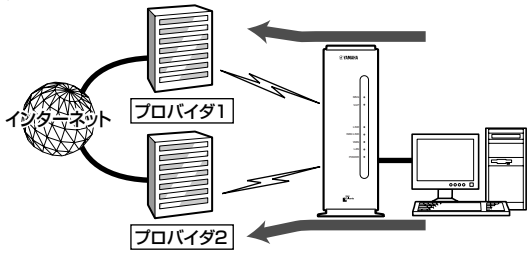
7 **[メール以外のプロバイダ]の接続先で登録したプロバイダを選ぶ。**

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。

パソコンごとに接続先を使い分ける

パソコンごとに、接続するプロバイダを使い分けられます。



この場合は、LAN上のすべてのパソコンのIPアドレスをあらかじめ固定する必要があります。そのあとに、本機の複数プロバイダ選択に関する設定を行います。

各パソコンのIPアドレスを変更する

「パソコンのIPアドレスを管理する」(124ページ)の手順にしたがって、パソコンにIPアドレスを割り当てます。詳しくは、ネットワークの管理者にご相談ください。

本機の設定を変更する

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。**

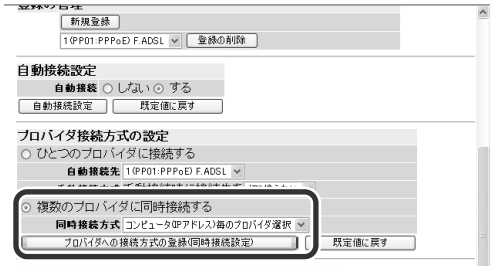
「トップ」画面が表示されます。

3 **画面左側の[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 **以下のように設定してから、[プロバイダへの接続方式の登録(同時接続設定)]をクリックする。**

- **自動接続設定**:する
- **プロバイダ接続方式の設定**:[複数のプロバイダに同時接続する]を選んでから、[コンピュータ(IPアドレス)毎のプロバイダ選択]を選ぶ。



6 **コンピュータのIPアドレスを入力してから、インターネットに接続する際の接続先プロバイダを選ぶ。**

7 **[上記コンピュータ以外の接続先]に、LAN上のその他すべてのコンピュータの接続先プロバイダを設定する。**

8 **メール着信確認機能を使用する場合には、[ルータによるメール着信確認先]でメールサーバのあるプロバイダを選ぶ。**

メールサーバを登録したいときは、[システム管理]画面の[メールサーバの登録]画面で設定してください。

9 **[登録]をクリックして、設定を保存する。**

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。

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。

準備する

フレッツ·ADSLの場合と同様に準備します。

詳しくは、「設定マニュアル」(別冊)の「フレッツ·ADSL接続する」(69〜88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5章 ファイアウォール機能を使う」(47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 XPとInternet Explorer 6.0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。

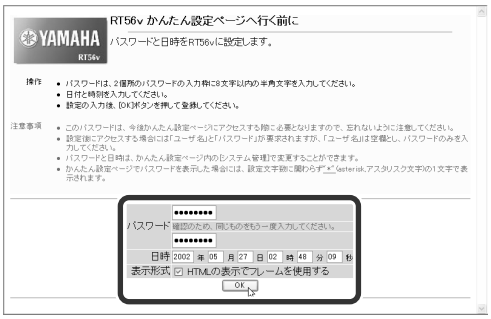
「http://setup.netvolante.jp/」または本機のIPアドレス(工場出荷時は192.168.0.1)を入力して開きます。

初めて開いたときは、「RT56v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

「RT56v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、「設定マニュアル」(別冊)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

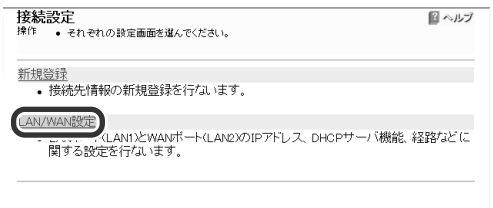
ルータの管理パスワードは、本機の設定を変えるときや情報を見るときに必要になります。プロバイダのパスワードとは別に、大切に管理してください。

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 画面左側の[接続設定]をクリックする。

6 [LAN/WAN設定]をクリックする。



次のページにつづく▶

7 以下の設定を行ってから、[登録]をクリックする。

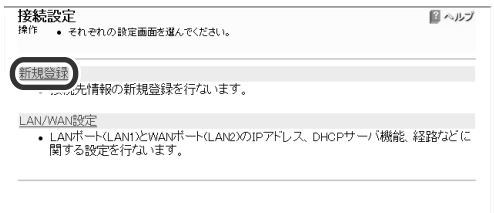
- **[LANポート(LAN1)のIPアドレス設定]の[セカンダリ・IPアドレス]**：現在[プライマリ・IPアドレス]に設定されているプライベートIPアドレスとネットマスク(工場出荷時は192.168.0.1/24)を入力する。
- **[プライマリ・IPアドレス]**：プロバイダから割り当てられたIPアドレスの中から、ルータに設定するIPアドレスとネットマスクを入力する。

ヒント

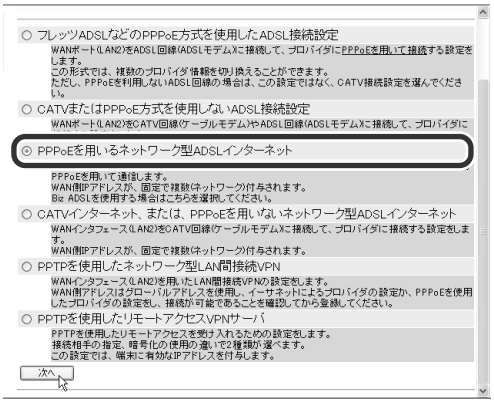
LAN側をプライベートアドレスで利用する場合は、LANポートのIPアドレスの設定を変更する必要はありません。

8 画面左側の[接続設定]をクリックする。

9 [新規登録]をクリックする。

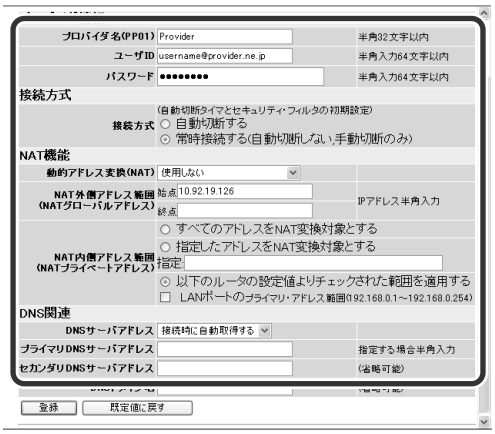


10 [PPPoEを用いるネットワーク型ADSLインターネット]を選んでから、[次へ]をクリックする。



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。

ユーザID ユーザIDを入力します。

パスワード パスワードを入力します。

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5章 ファイアウォール機能を使う」(47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。

画面左側に「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。

次のページにつづく▶

15 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。

NetVolanteのホームページが表示されます。

表示されない場合は

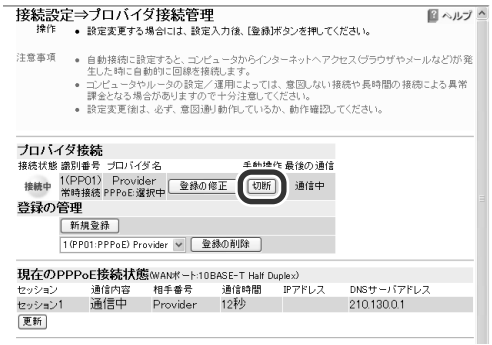
DNSサーバアドレスの設定が間違っている可能性があります。

[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。

これで、PPPoEネットワーク型ADSLの接続設定は完了です。



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

ネットワーク型ADSL接続は定額料金制なので、発信制限は自動設定されません。

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」(129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。

ヒント

ネットボランチDNSサービスを利用することで、固定グローバルIPを取得できない場合でも、サーバを公開して運用できます。詳しくは「ネットボランチDNSサービスを利用する」(98ページ)をご覧ください。

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(95ページ)
- アクセスを許可する設定に変更する(96ページ)

サーバの設定

- パソコンのIPアドレスを設定する(97ページ)
- ファイルサーバソフトの設定を変更する(97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(172.16.128.112)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」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。

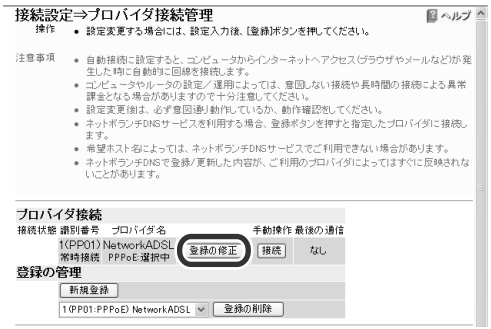
2 [パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。

「トップ」画面が表示されます。

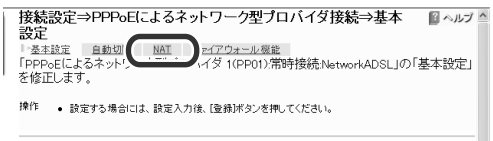
3 画面左側の[接続設定]をクリックする。

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。

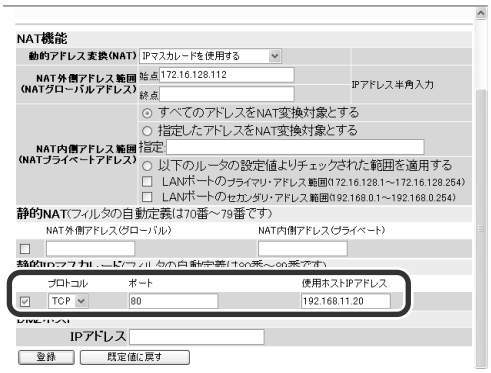


次のページにつづく▶

7 **「静的IPマスカレード」欄のチェックを付けてから、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。**

Webサーバを公開する場合の例:

- プロトコル:TCP
- ポート:80



ご注意

「NAT機能」欄の[動的アドレス変換]で[IPマスカレードを使用する]または[NATとIPマスカレードを併用する]を選んでいない場合は、「静的IPマスカレード」欄が表示されません。

[IPマスカレードを使用する]または[NATとIPマスカレードを併用する]を選んでからNAT外側アドレス範囲(NATグローバルアドレス)を入力して[登録]をクリックすると、「静的IPマスカレード」欄が表示されるようになります。

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

着信側のLANでは、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 **95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。**

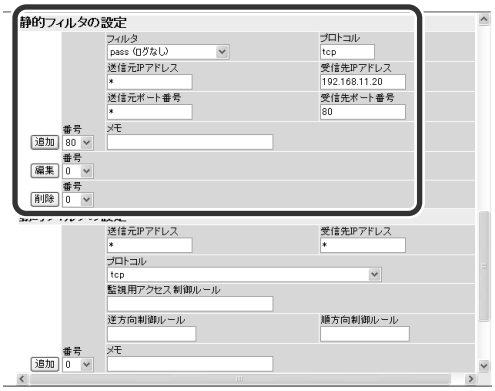
2 **画面左側の[付加機能]をクリックする。**

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」(52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、送信元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。

静的フィルタの一覧

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
0	☑	☐	reject	する	udp,tcp	*	135	*	*	Windows: DCE RPC
1	☑	☐	reject	する	udp,tcp	*	*	*	135	Windows: DCE RPC
2	☑	☐	reject	する	udp,tcp	*	137-138	*	*	Windows: NetBIOS (NS,Dat
3	☑	☐	reject	する	udp,tcp	*	*	*	137-138	Windows: NetBIOS (NS,Dat
4	☑	☐	reject	する	udp,tcp	*	139	*	*	Windows: NetBIOS (SSN)
5	☑	☐	reject	する	udp,tcp	*	*	*	139	Windows: NetBIOS (SSN)
6	☑	☐	reject	する	udp,tcp	*	445	*	*	Windows: Direct Hosting S
7	☑	☐	reject	する	udp,tcp	*	*	*	445	Windows: Direct Hosting S
80	☑	☐	pass	しない	tcp	*	*	192.168.11.20	80	
[illegible]	☐	☐	pass	しない	*	*	*	*	*	pass all

動的フィルタの一覧

登録されておりません。

静的フィルタと動的フィルタの適用

適用 チェックされている静的フィルタと動的フィルタの 定義を適用する

動的フィルタ用アクセス制御ルールの一覧

登録されておりません。

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、「IPアドレスを変更する」(125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

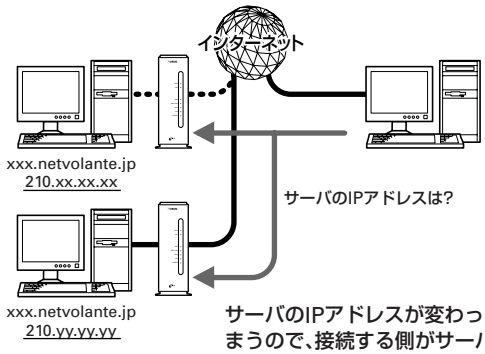
公開するサーバまたはパソコンにサーバアプリケーションをインストールしてから、公開するフォルダやユーザID、パスワードを設定します。設定の方法については、各ソフトウェアの取扱説明書をご覧ください。

ネットボランチ DNS サービスを利用する

ネットボランチDNSサービスとは?

サーバを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、相手のグローバルIPアドレスがわかっている必要があります。

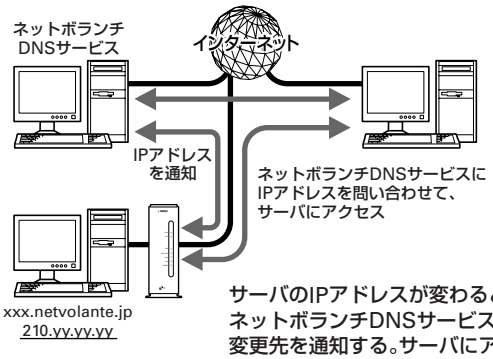
しかし、インターネットに常時接続している場合でも、割り当てられるグローバルIPアドレスは再接続時または時間によって変更される場合があります。そのため、グローバルIPアドレスが固定で割り当てられない接続サービスを利用していると、サーバを構築して公開することは困難でした。



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

ネットボランチDNSサービスを利用すると

グローバルIPアドレスが変更されるごとに(または一定時間おきに)IPアドレスはサーバへ通知されるため、固定のホスト名を持つことができるようになります。したがって、固定IPアドレスサービスを契約していなくても自宅サーバで独自ドメインを使った各種サーバを運用したり、PPTPを利用してVPNを構築して、外部とデータをやり取りしたりできるようになります。



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

ネットボランチDNSサービスで取得できるホスト名

「(ユーザの希望ホスト名).xxx.netvolante.jp」という形式のホスト名を取得できます。「xxx」の部分は、ネットボランチDNSサーバが任意に自動で割り当てます。

ご注意

- ホストアドレスはネットボランチ1台につき1つしか取得できません。
- 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ネットボランチDNSサービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミックDNSサーバに登録することはできません。
- ネットボランチDNSサービスは、プロバイダからグローバルIPアドレスが割り当てられている環境でのみ利用できます。グローバルIPアドレスとは、下記以外のIPアドレスです。
  - 10.0.0.0～10.255.255.255
  - 172.16.0.0 ～172.31.255.255
  - 192.168.0.0～192.168.255.255
- ご利用中のプロバイダによっては、ホスト名およびネットボランチ電話番号の登録／更新内容がネットボランチDNSサービスにすぐに反映されないことがあります。あらかじめご了承ください。

ネットボランチDNSサービスでホストアドレスを取得する

ネットボランチDNSサービスを利用すると、グローバルIPアドレスが変更されるごとに設定を変更する必要がなくなり、便利です。

ご注意

ホストアドレスはネットボランチ1台につき1つしか取得できません。

ネットボランチDNSサービスの設定をはじめて行う場合は

以下の手順7で[登録]をクリックすると、「ネットボランチDNSサービス利用規約」が表示されます。規約を読んで、同意するときは[利用規約に同意する]、同意しないときは[利用規約に同意しない]をクリックしてください。規約に同意されない場合は、ネットボランチDNSサービスをご利用いただけません。あらかじめご了承ください。

1 ブロードバンド接続設定を行い、本機を接続状態にする。

プロバイダからグローバルアドレスが割り当てられていることを確認してください。グローバルIPアドレスは、「10.x.x.x」、「172.16.x.x〜172.31.x.x」、「192.168.x.x」の3つの範囲以外のIPアドレスです。

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。

3 [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。

4 画面左側の[接続設定]をクリックする。

5 [プロバイダ接続管理]をクリックする。

6 必要な設定を行う。

接続プロバイダ

ネットボランチDNSサービスを使用する接続プロバイダを選びます。端末型プロバイダ接続のみ利用できます。ネットワーク型プロバイダ接続で接続している場合は、ネットボランチDNSサービスは利用できません。

ホスト名

希望のホスト名を入力します。ホスト名に使用できるのは、英数字と－(ハイフン)だけです。

ご注意

希望のホスト名が取得できないことがあります。

IPアドレス変更時の自動更新

グローバルIPアドレスが変わった場合に自動的にネットボランチDNSサーバにIPアドレス変更情報を通知したいときは、[する]を選びます。

タイムアウト時間

ネットボランチDNSサービスのタイムアウト時間を秒で指定します。

7 設定が終わったら、[登録]をクリックする。

「ネットボランチDNSサービス利用規約」が表示されます。

次のページにつづく▶

8 規約を読んで、同意するときは［利用規約に同意する］、同意しないときは［利用規約に同意しない］をクリックする。

［利用規約に同意する］をクリックすると、ネットボランチDNSサービスのダイナミックDNSサーバからホストアドレスが割り当てられます。ホストアドレスは「（指定したホスト名）.xxx.netvolante.jp」という形で割り当てられます。「xxx」は、サーバで任意に生成された文字列です。

ホストアドレスを取得できない場合は

- 契約プロバイダによっては、登録／更新してすぐに名前解決ができない場合があります。しばらく時間をおいてから再度試してみてください。
- プロバイダから割り当てられているIPアドレスがグローバルIPアドレスかどうかを確認してください。
- プロバイダの設定で指定したDNSサーバのIPアドレスが正しいかどうか、確認してください。
- ネットボランチDNSサーバのIPアドレスを直接指定してみると問題が解決する場合があります。「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」欄に半角英数字で「netvolante-dns server 211.133.249.145 」と入力してから、［入力］をクリックしてください。

ネットボランチDNSサービス利用規約

ネットボランチDNSサービスを利用するユーザは、以下の利用規約に同意して頂くことが必要です。

1.弊社は本サービスに関連して発生したいかなる損害について、一切の責任を負いません。本サービスの利用は、ユーザ自身の責任で行ってください。

2.弊社は本サービスについて、事前に通知することなくいつでもサービスの条件および内容を変更、停止、中止できるものとします。

3.ユーザは法令に違反する行為、権利侵害、公序良俗に反する行為などを行わないものとします。弊社がユーザとして不適当と判断した場合や、長期にわたりサービスの利用が見られない場合は、登録データ等の変更、削除を行うことがあります。

4.弊社は事前に通知することなく、いつでも本利用規約を変更できるものとします。

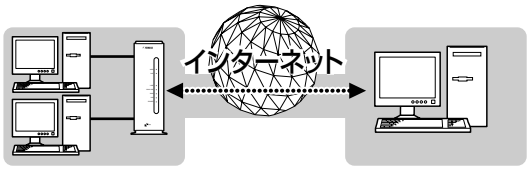
ご注意

- ネットボランチDNSサービスでは、登録ホスト名に関しての正引きはできますが、逆引きはできません。
- ネットボランチDNSサービスに利用することにより、インターネット上の不特定多数ユーザからアクセスされる可能性があります。不正アクセスなどによりルータやパソコンに損害を受けるだけでなく、そのパソコンを経由して他人に損害を与える可能性もあります。ネットボランチDNSサービスのご利用にあたっては、ユーザの自己責任にて十分なセキュリティ対策を行ってください。
- ご利用中のプロバイダによっては、ホスト名およびネットボランチ電話番号の登録／更新内容がネットボランチDNSサービスにすぐに反映されないことがあります。あらかじめご了承ください。

PPTPを利用してリモートアクセスする

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

リモートアクセスをするときは、本機にリモートアクセスユーザのユーザIDやパスワードを登録し、リモートのパソコンにはダイヤルアップ接続の設定を行います。



PPTPを利用して、VPNを構築

ご注意

- ブロードバンド接続した状態でPPTPのトンネル設定を行うため、PPTPを利用したリモートアクセスの設定前にブロードバンド接続の設定が必要です。
- PPTPを利用したリモートアクセスは、プロバイダからグローバルIPアドレスが割り当てられている環境でのみ利用できます。グローバルIPアドレスとは、下記以外のIPアドレスです。
  - 10.0.0.0～10.255.255.255
  - 172.16.0.0 ～172.31.255.255
  - 192.168.0.0～192.168.255.255
- リモートアクセスを利用するときは、データを保全するために十分なセキュリティ設定を行ってください。セキュリティ設定が不十分の場合は、双方のLANに接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などにあう可能性があります。
- 本機のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- Windowsでファイル共有をする場合は、NetBIOS over TCP/IPプロトコルを使用するか、またはWindowsNTサーバを用意する必要があります。
- MacOS8.1以降のMacintoshでファイル共有する場合はAppleShare IPサーバが必要です。なお、MacOS9の場合は、「ファイル共有」コントロールパネルで[TCP/IP接続でファイル共有を可能にする]にチェックを付けることで、AppleShare IPサーバなしでファイル共有できます。

本機で利用できるPPTPについて

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

必要な設定

リモートアクセスするときは、ルータやパソコンに次のような設定が必要です。

ルータの設定

- 接続相手を登録する(102ページ)
- ブロードバンド接続の設定
  - 本機のWAN側にグローバルIPアドレスが割り当てられている必要があります。
  - 動的にWAN側アドレスが割り当てられる端末型接続の場合は、ネットボランチDNSサービス(98ページ)を利用して、使用できるホスト名を取得する必要があります。
  - ネットワーク型接続の場合は、WAN側に割り当てられるグローバルIPアドレスを確認してください。

LAN内サーバまたはパソコンに必要な設定

- 固定IPアドレスを設定する(103ページ)
- ファイルサーバソフトの設定を変更する(103ページ)

リモートアクセスするパソコンの設定

ダイヤルアップ接続設定(104ページ)

接続相手を登録する

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。

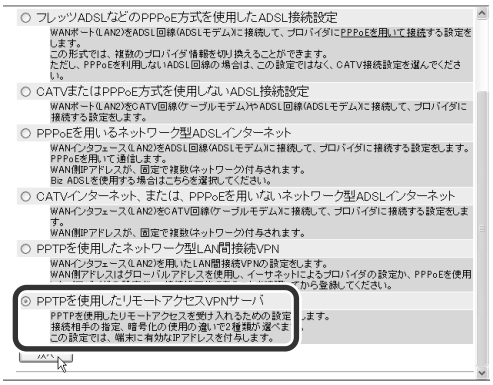
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

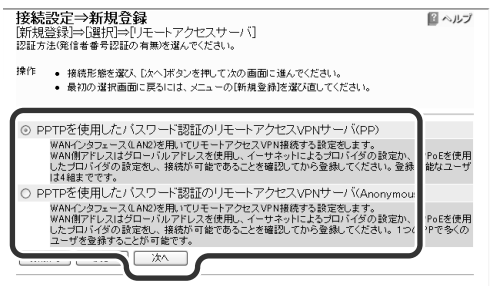
3 **画面左側の[接続設定]をクリックする。**

4 **[新規登録]をクリックする。**

5 **[PPTPを使用したリモートアクセスVPNサーバ]を選んでから、[次へ]をクリックする。**



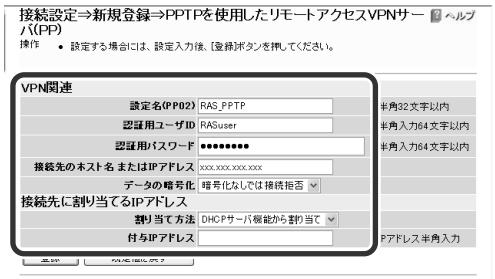
6 **使用したい認証方法を選んでから、[次へ]をクリックする。**



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

7 **必要な設定を行う。**

手順6で[PP]を選んだ場合



設定名(PPxx)

接続先の名前を入力します。

認証用ユーザID

ユーザIDを入力します。

認証用パスワード

パスワードを入力します。

接続先のホスト名またはIPアドレス

PPTPで接続するクライアントPCのIPアドレスまたはホスト名を入力します。

データの暗号化

暗号化なしで接続の要求があったときに、接続を許可するかどうかを選びます。

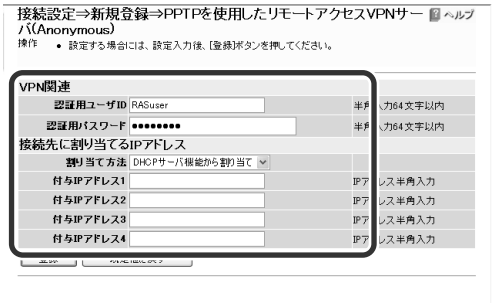
割り当て方法

接続先にIPアドレスをどのように割り当てるかを選びます。接続先に固定IPアドレスを指定する場合は、[固定割り当て]を選んでから、「付与IPアドレス」欄にアドレスを入力します。

ご注意

登録できるユーザ数は最大4つです。PPTPのトンネル接続は、Anonymousで利用しているものも合わせて、同時に4つまでとなります。

手順6で［Anonymous］を選んだ場合



認証用ユーザID

ユーザIDを入力します。

認証用パスワード

パスワードを入力します。

割り当て方法

接続先にIPアドレスをどのように割り当てるかを選びます。接続先に固定IPアドレスを指定する場合は、［固定割り当て］を選んでから、「付与IPアドレス」欄にアドレスを入力します。

ご注意

登録できるユーザ数に制限はありませんが、実際のPPTPのトンネル接続は同時に4つまでとなります。

8 画面下の［登録］をクリックする。

接続相手が登録され、「接続設定」画面に戻ります。

LAN内のサーバやパソコンを設定する

リモートアクセスするには、LAN内のサーバやパソコンにTCP/IPプロトコルでアクセスできるようにするための設定が必要です。

ご注意

- 本機のリモートアクセス機能は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- Windowsでファイル共有をする場合は、NetBIOS over TCP/IPプロトコルを使用するか、またはWindowsNTサーバを用意する必要があります。
- MacOS8.1以降のMacintoshでファイル共有する場合はAppleShare IPサーバが必要です。なお、MacOS9の場合は、「ファイル共有」コントロールパネルで［TCP/IP接続でファイル共有を可能にする］にチェックを付けることで、AppleShare IPサーバなしでファイル共有できます。

サーバやパソコンのIP アドレスを設定する

お互いのLAN上のサーバ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。設定方法については、詳しくは、「IPアドレスを変更する」（125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ファイルサーバソフトやネットワーク共有を設定して、公開するフォルダやユーザID、パスワードを設定します。

リモートアクセスするパソコンの設定を変更する

Windows 98SE/Meの場合

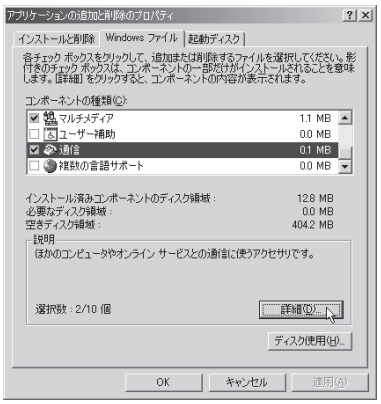
仮想プライベートネットワーク（VPN）をインストールする

PPTPを利用してリモートアクセスするには、Windowsの仮想プライベートネットワークが必要です。インストールされていない場合は、以下の手順でWindowsのCD-ROM（OSインストールCD-ROM）からインストールします。作業を始める前にシステムCD-ROMをご用意ください。

1 **[コントロールパネル]の[アプリケーションの追加と削除]を開き、[Windowsファイル]タブをクリックする。**

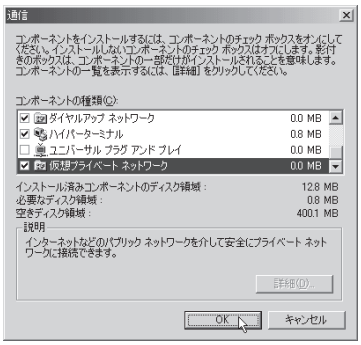
インストール済みのファイルがリストに表示されます。

2 **[通信]をクリックして選んでから、[詳細]をクリックする。**



3 **[仮想プライベートネットワーク]、[ダイヤルアップネットワーク]にチェックが付いていることを確認してから、[OK]をクリックする。**

上記以外の項目にチェックがついていても、問題はありません。



4 **[OK]をクリックする。**

追加機能がインストールされます。
CD-ROMを要求するメッセージが表示された場合は、WindowsのCD-ROMをドライブにセットしてください。

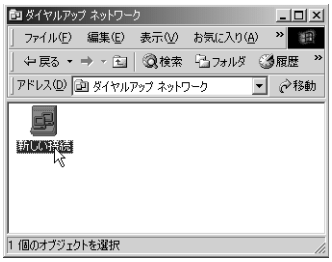
5 **インストールが終わったら、パソコンを再起動する**

再起動後に、仮想プライベートネットワーク機能が使えるようになります。

パソコンのダイヤルアップネットワーク設定を変更する

PPTPを利用してリモートアクセスするには、ダイヤルアップネットワークにリモートアクセスするためのアイコンを作成します。

1 **[マイコンピュータ]の[ダイヤルアップ ネットワーク]をダブルクリックしてから、[新しい接続]アイコンをダブルクリックする。**



[新しい接続]アイコンがない場合には

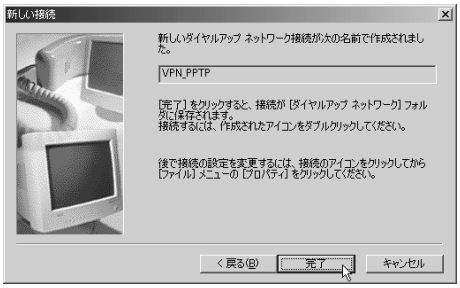
「ダイヤルアップネットワークへようこそ」の画面が表示されるので、[次へ]をクリックします。

2 **「VPN_PPTP」と入力してから、[モデムの選択]から[Microsoft VPN Adapter]を選び、[次へ]をクリックする。**

3 **ネットボランチDNSサービスで取得したホストアドレスまたはRT56vのWAN側IPアドレスを入力してから、[次へ]をクリックする。**

4 **接続名を確認してから、[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リモート接続のアイコンが表示されます。



5 **[VPN_PPTP]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。**

6 **[ネットワーク]タブをクリックする。**

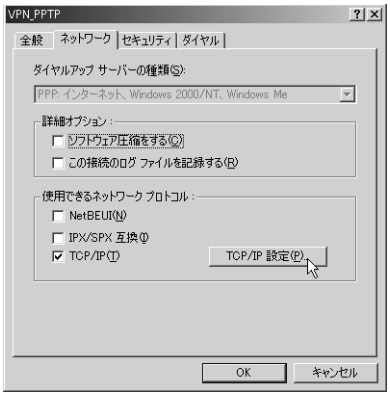
Windows 98SEの場合は[サーバーの種類]タブをクリックします。

次のページにつづく▶

7 以下のように設定する。

Windows Meの場合

- ソフトウェア圧縮をする：チェックを外す。
- NetBEUI、IPX/SPX互換：チェックを外す。
- TCP/IP：チェックを付ける。



Windows 98SEの場合

- ネットワークへのログオン：チェックを付ける。
- ソフトウェア圧縮をする：チェックを外す。
- 暗号化パスワードを使う：チェックを付ける。
- データの暗号化を使用する：RT56vで［暗号化なしでは接続拒否］を選んだ場合は、チェックを付ける。RT56vで［暗号化なしでも接続許可］を選んだ場合は、チェックを外す。
- NetBEUI、IPX/SPX互換：チェックを外す。
- TCP/IP：チェックを付ける。

Windows 98SEの設定は、これで終了です。

8 Windows Meの場合は、［セキュリティ］タブをクリックして以下のように設定を変更してから、［OK］をクリックする。

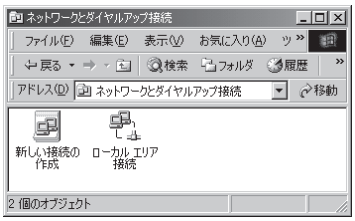
- ネットワークへのログイン：チェックを付ける。
- 暗号化パスワードを使う：チェックを付ける。
- データの暗号化が必要：RT56vで［暗号化なしでは接続拒否］を選んだ場合は、チェックを付ける。RT56vで［暗号化なしでも接続許可］を選んだ場合は、チェックを外す。

これで、PPTPを利用したリモートアクセス接続の設定が完了しました。

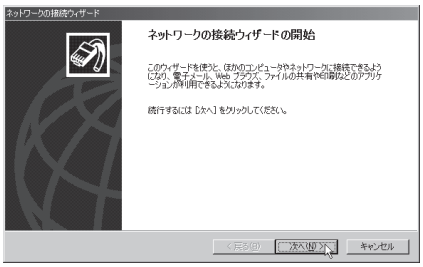
Windows 2000の場合

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。

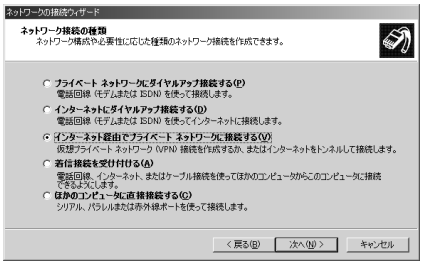
2 [新しい接続の作成]アイコンをダブルクリックする。



3 [次へ]をクリックする。



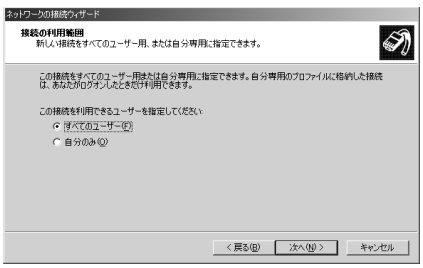
4 [インターネット経由でプライベートネットワークに接続する]を選んでから、[次へ]をクリックする。



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

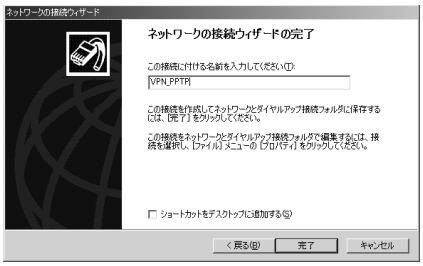
6 ネットボランチDNSサービスで取得したホストアドレスまたはRT56vのWAN側IPアドレスを入力してから、[次へ]をクリックする。

7 [すべてのユーザー]または[自分のみ]を選んでから、[次へ]をクリックする。



次のページにつづく▶

8 [接続名]に「VPN_PPTP」と入力してから、[完了]をクリックする。



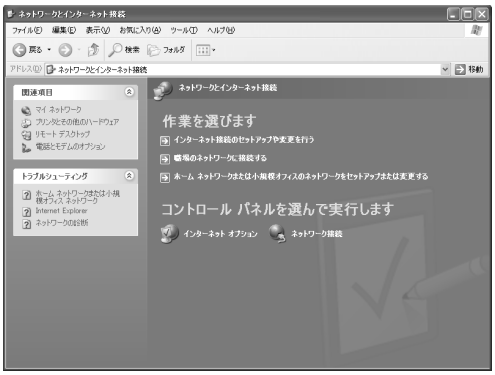
これで、リモートアクセス接続の設定が完了しました。

Windows XPの場合

Windows XPの場合は、ネットワーク機能の設定とダイヤルアップネットワークの設定を行います。

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。

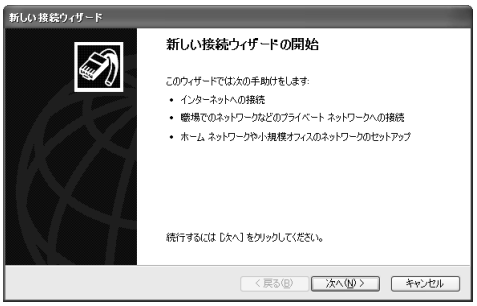


3 [新しい接続を作成する]をクリックする。

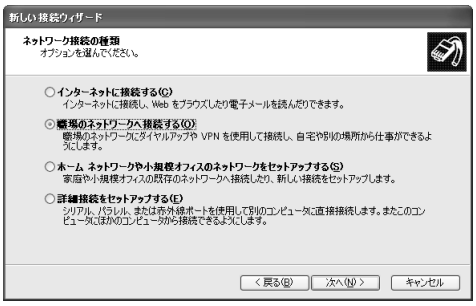
「新しい接続ウィザードの開始」画面が表示されます。

「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。

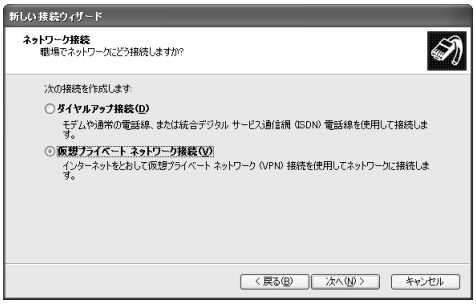
4 [次へ]をクリックする。



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。



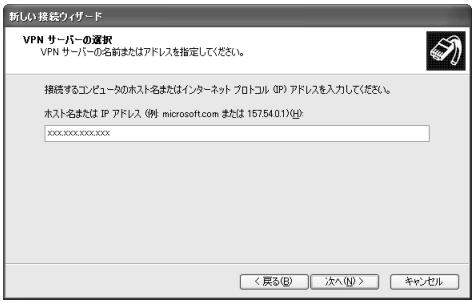
6 [仮想プライベート ネットワーク接続]を選んでから、[次へ]をクリックする。



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

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

9 ネットボランチDNSサービスで取得したホストアドレスまたはRT56vのWAN側IPアドレスを入力してから、[次へ]をクリックする。



10 [完了]をクリックする。

これで、リモートアクセス接続の設定が完了しました。

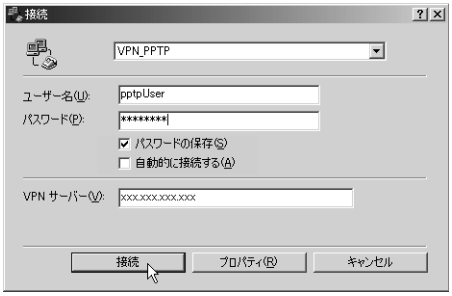
本機へアクセスする

Windows 98SE/Meの場合

1 **ブロードバンド接続設定を行い、本機を接続状態にする。**

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

3 **[接続]をクリックする。**



本機へ接続すると、接続名のウィンドウが表示され、接続速度と接続時間が表示されます。

ご注意

[パスワードの保存]にチェックを付けると、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。チェックしない場合は、接続のたびにパスワード入力が必要になります。

4 **目的に応じたソフトウェアを使って、必要な作業を行う。**

5 **接続を解除するときは、[切断]をクリックする。**

Windows 2000/XPの場合

1 **ブロードバンド接続設定を行い、本機を接続状態にする。**

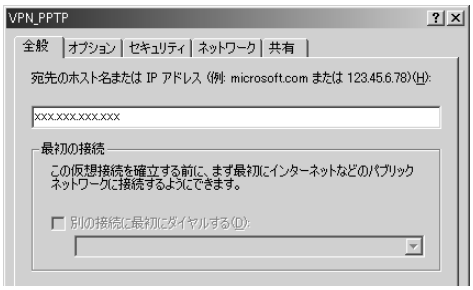
2 **[VPN_PPTP]アイコンをダブルクリックして、接続画面を表示する。**

- **Windows2000の場合:**[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]を開き、[VPN_PPTP]アイコンをダブルクリックする。
- **WindowsXPの場合:**108ページの手順1〜2を行ってから、[VPN_PPTP]アイコンをダブルクリックする。

3 **[ユーザー名]と[パスワード]欄に、102〜103ページの手順7で設定した認証用ユーザIDとパスワードを入力する。**

4 **[プロパティ]をクリックする。**

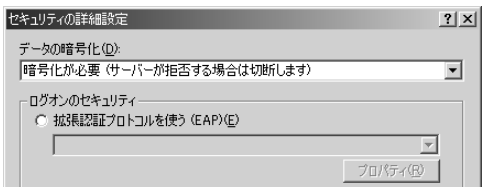
5 **[全般]タブをクリックしてから、[宛先のホスト名またはIPアドレス]欄に、ネットボランチDNSサービスで取得したホストアドレスまたはRT56vのWAN側IPアドレスを入力する。**



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

7 102ページの手順7で行った設定に合わせて、暗号形式を選ぶ。

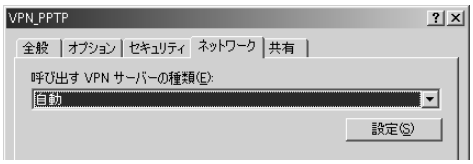
- **RT56vで[暗号化なしでは接続拒否]を選んだ場合:**[暗号化が必要(サーバーが拒否する場合は切断します)]を選びます。
- **RT56vで[暗号化なしでも接続許可]を選んだ場合:**希望する暗号化のレベルを選びます。



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

- [暗号化されていないパスワード(PAP):チェックを外す。
- Shivaパスワード認証プロトコル(SPAP):チェックを外す。
- チャレンジハンドシェイク認証プロトコル(CHAP):チェックを外す。
- Microsoft CHAP(MS-CHAP):チェックを付ける。
- Windows 95サーバーで古いバージョンのMS-CHAPを許可する:チェックを外す。
- Microsoft CHAP Version 2(MS-CHAP v2):チェックを付ける。
- MS-CHAPベースのプロトコルに対してWindowsのログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う:チェックを外す。

9 [ネットワーク]タブをクリックしてから、[呼び出すVPNサーバーの種類](Windows 2000の場合)または[VPNの種類](Windows XPの場合)で「自動」を選び、[設定]をクリックする。



次のページにつづく▶

10 以下のように設定してから、[OK]をクリックする。

- LCP拡張を使う：チェックを外す。
- ソフトウェアによる圧縮を行う：チェックを外す。
- 単一リンク接続に対してマルチリンクをネゴシエートする：チェックを付ける。

11 [VPN_PPTPのプロパティ]画面の[OK]をクリックして、[VPN_PPTPのプロパティ]画面を閉じる。

12 [接続]をクリックする。

本機へのダイヤルアップをはじめます。
接続すると、「ダイヤル アップネットワーク(プロバイダ名)」画面が表示され、接続速度と接続時間が表示されます。

ご注意

[パスワードの保存]にチェックを付けると、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。チェックしない場合は、接続のたびにパスワード入力が必要になります。

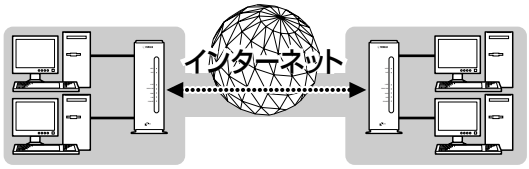
13 目的に応じたソフトウェアを使って、LAN内のパソコンのIPアドレスを指定して作業を行う。

14 接続を解除するときは、[切断]をクリックする。

本機との接続が切れます。

PPTPを利用してVPNを構築する（PPTP-LAN間接続）

RT56vが接続されているLANどうしをインターネット経由でPPPoEまたはCATV接続して、仮想プライベートネットワーク（VPN）を構築できます。PPTPを利用して接続するため、インターネット経由の接続でもセキュリティを保つことができます。



PPTPを利用して、VPNを構築

ADSLなどの通常のブロードバンド回線をそのまま利用してVPNを構築できるため、専用線を導入する場合と比較して、低コストでVPNを実現できます。なお、本機のLAN間接続機能は、TCP/IPプロトコルのサーバソフトウェアに対応しています。

ご注意

- ブロードバンド接続した状態でPPTPのトンネル設定を行うため、PPTP-LAN間接続の設定前にブロードバンド接続の設定が必要です。
- PPTPを利用したLAN間接続は、プロバイダからグローバルIPアドレスが割り当てられている環境でのみ利用できます。グローバルIPアドレスとは、下記以外のIPアドレスです。
  - 10.0.0.0～10.255.255.255
  - 172.16.0.0 ～172.31.255.255
  - 192.168.0.0～192.168.255.255
- 同じネットワークアドレスを設定しているLANどうしのLAN間接続はできません。あらかじめ、どちらかのネットワークアドレスを変更してください。
- LAN間接続を利用するときは、データを保全するために十分なセキュリティ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、破壊の被害を受ける可能性があります。
- 本機のLAN間接続は、WindowsのNetBEUIプロトコルおよびMacOSのAppleTalkプロトコルには対応していません。
- Windowsでファイル共有をする場合は、NetBIOS over TCP/IPプロトコルを使用するか、またはWindowsNTサーバを用意する必要があります。
- MacOS8.1以降のMacintoshでファイル共有する場合はAppleShare IPサーバが必要です。なお、MacOS9の場合は、「ファイル共有」コントロールパネルで［TCP/IP接続でファイル共有を可能にする］にチェックを付けることで、AppleShare IPサーバなしでファイル共有できます。

本機で利用できるPPTPについて

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

PPTPを使用できるように設定する

本機をPPTPサーバ／PPTPクライアントとして動作させるために必要な設定を行います。接続する側のLANに設置したネットボランチはPPTPクライアント、接続される側のLANに設置したネットボランチはPPTPサーバとして設定してください。

1 **ブロードバンド接続設定を行い、本機を接続状態にする。**

プロバイダからグローバルアドレスが割り当てられていることを確認してください。グローバルIPアドレスは、「10.x.x.x」、「172.16.x.x〜172.31.x.x」、「192.168.x.x」の3つの範囲以外のIPアドレスです。

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。

「ネットワーク パスワードの入力」画面が表示されます。

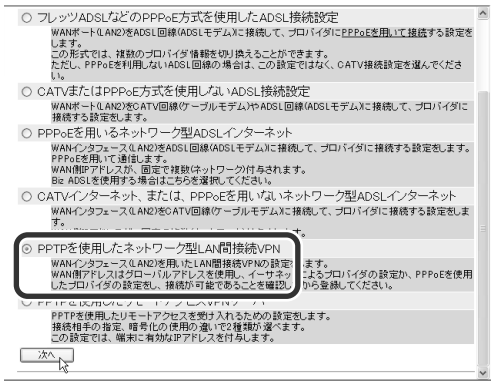
3 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

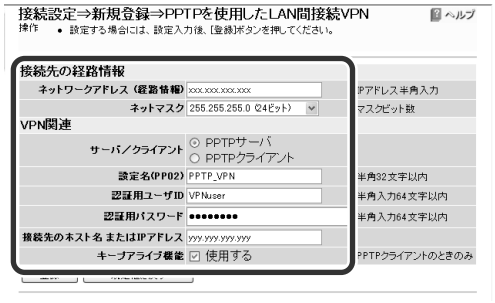
4 **画面左側の[接続設定]をクリックする。**

5 **[新規登録]をクリックする。**

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



7 **必要な設定を行う。**



ネットワークアドレス（経路情報）
接続先のIPアドレスを入力します。

ネットマスク
接続先のネットマスクを選びます。

サーバ／クライアント
RT56vをPPTPサーバとして利用する場合は[PPTPサーバ]、PPTPクライアントとして利用する場合は[PPTPクライアント]を選びます。

設定名　任意の設定名を入力します。

認証用ユーザID
PPTPで接続する際に使用するユーザ名を入力します。

認証用パスワード
PPTPで接続する際に使用するパスワードを入力します。

接続先のホスト名またはIPアドレス
PPTPで接続する相手先機器のホスト名またはIPアドレスを入力します。

キープアライブ
相手に定期的にパケットを送信し、相手から応答がなくなったら自分から切断するように設定するときは、チェックを付けます。

ご注意

PPTPのトンネルは最大で4個まで登録できますが、「かんたん設定ページ」を使って設定する場合は1個のみ登録／管理できます。

10 **画面下の[登録]をクリックする。**

PPTPの設定内容が登録されます。

RT56vをPPTPサーバとして設定した場合は、PPTPサーバとして動作を始めます。

PPTPで接続する

PPTPサーバ／PPTPクライアントに接続します。

ご注意

- PPTPサーバに接続するには、以下の操作を行うネットボランチがPPTPクライアントとして設定されている必要があります。
- PPTPクライアントに接続するには、以下の操作を行うネットボランチがPPTPサーバとして設定されている必要があります。

1 ブロードバンド接続設定を行い、本機を接続状態にする。

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。

「ネットワーク パスワードの入力」画面が表示されます。

3 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。

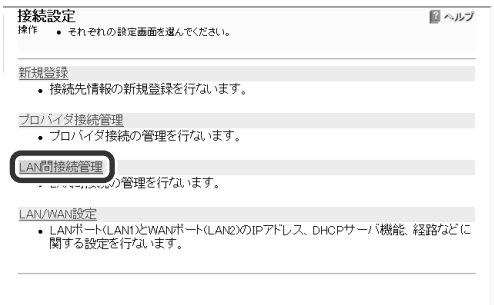
「ネットワーク パスワードの入力」画面が表示されます。

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。

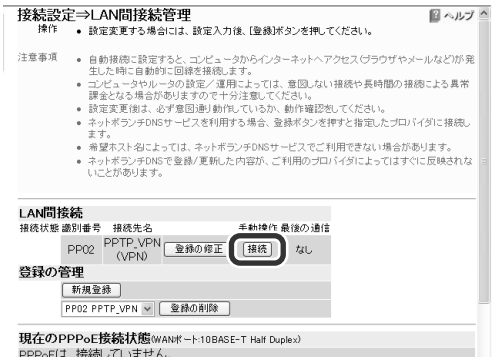
「トップ」画面が表示されます。

5 画面左側の[接続設定]をクリックする。

6 [LAN間接続管理]をクリックする。



7 [接続]をクリックする。



登録したPPTPサーバまたはクライアントに接続して、PPTP-LAN間接続できるようになります。

PPTP-LAN間接続を切断するには

「接続設定」－「LAN間接続管理」画面で、[切断]をクリックします。

ご注意

[切断]をクリックしてもPPTPのセッションが終了するだけで、プロバイダに対するブロードバンド接続は切断されません。

IPv6 環境で使う

本機は次世代インターネット・プロトコルである「IPv6」(Internet Protocol Version 6)に対応しています。本機では従来の「IPv4」に関する機能も継承しているため、既存のネットワークに影響を与えずに、「IPv6」を利用できます。

ご注意

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

IPv6ネットワーク

- エンド―エンドの通信、双方向通信が可能
- 家電製品、自動車、携帯電話機もインターネットに接続できる

IPv4ネットワーク

アドレス不足によりプライベートアドレスを使用している場合、エンド―エンドの通信、双方向通信ができない。

IPv6を導入する前に

IPv6とIPv4のネットの環境を混在させるときのご注意

「IPv6」は、「IPv4」との互換性がないため、それぞれのネットワークが混在するときには、双方を併用するために移行技術(Transition Mechanism)と総称される仕組みが必要になります。また、一般的には、IPv4からIPv6への移行は複数の段階を踏むため、各段階に応じた移行技術が必要になります。

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

プロバイダからの設定情報を確認してください

IPv6接続サービスを契約すると、以下の情報がプロバイダから提供されます。

- プレフィックス(アドレスブロック)
- 接続方法(ネイティブ接続／デュアルスタック接続／トンネル接続)
- トンネルの終端アドレス(トンネル接続の場合)
- 経路制御方法(RIPngを使うか使わないか。特に記載がない場合、RIPngは使用しません。)
- 接続の確認方法(ping6の相手アドレスや、閲覧するWebサイトなど)

Windows XPでIPv6を導入するときは

コマンドプロンプトで、以下のコマンドを入力します。

```
ipv6 install
```

ヒント

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

IPv6を使えるように設定する

設定を始める前に、IPv6で接続する相手(プロバイダ)を登録しておいてください。

ご注意

プロバイダを登録していない場合は、以下の操作を行ってもエラーが発生します。登録していない場合は、接続方法に合わせて「接続設定」−「新規登録」画面で接続先のプロバイダを登録してください。

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。

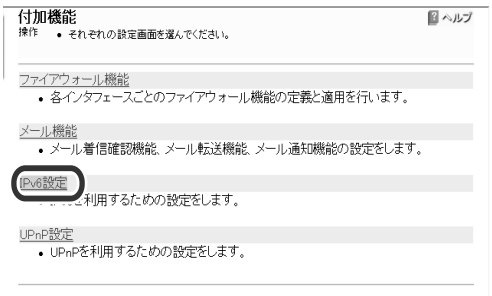
「ネットワーク パスワードの入力」画面が表示されます。

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。**

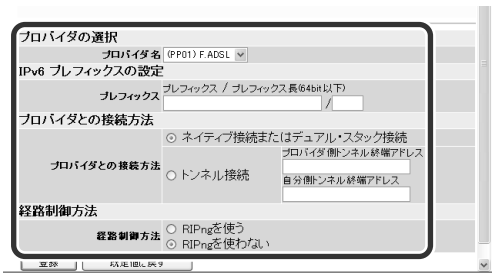
「トップ」画面が表示されます。

3 **画面左側の[付加機能]をクリックする。**

4 **[IPv6設定]をクリックする。**



5 **必要な項目を設定する。**



プロバイダ名

IPv6で接続するプロバイダを選びます。

プレフィックス

プロバイダから指定されたプレフィックス(またはアドレスブロック)を入力します。IPv6のプレフィックス(ネットワーク部)を64ビット以内で指定します。

プレフィックス長(「/」以下の値)は64ビット以下で設定してください。64ビット以上の値を入力すると、入力エラーになります。

プロバイダとの接続方法

プロバイダにIPv6接続する際の、接続方法を指定します。接続方法はプロバイダの提供しているサービスによって決まります。契約内容に合わせて設定してください。

- **ネイティブ接続またはデュアル・スタック接続:** ネットワークをすべてIPv6環境で構築している場合に選びます。IPv6で構築したネットワークにIPv6のパケットを流すため、IPv6環境の機器がIPv4ネットワークにアクセスできなくなりますので、ご注意ください。
- **トンネル接続:** ネットワーク上にIPv4環境の機器が多く存在する場合に選びます。IPv4のネットワーク内部にIPv6用の仮想的なトンネルを設置して、IPv6のパケットをカプセル化してIPv4のネットワーク上に流します。

  この場合、プロバイダから指定されたトンネル終端アドレス(プロバイダ側、自分側)を設定する必要があります。

次のページにつづく▶

経路制御方法

RIPng(動的経路)で経路制御するかどうかを指定します。契約内容に合わせて設定してください。プロバイダの資料に経路制御手法について何も記載されていない場合は、[使わない]を選びます。

- **RIPngを使う**:RIPng(動的経路)で経路制御を行います。
- **RIPngを使わない**:静的経路で経路制御を行います。

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。

IPv6接続を確認する

以下の手順で、IPv6環境が正しく設定されているかどうか確認します。

ヒント

パソコンとRT56vは、LANケーブルで接続した時点で通信可能になります。パソコン側での設定は、特に必要ありません。

1 **LAN側の接続を確認する。**

LANポートに接続されたパソコンから、RT56vのLAN1アドレスにping6を実行します。
返事があれば、正しく設定されています。

ヒント

RT56vのLAN1アドレスは、プレフィックスに「1」をつけたアドレスになります。
例:プレフィックスが「fec0:12ab::/64」の場合

- LAN1アドレスは「fec0:12ab::1/64」になります。
- RT56vのLAN1アドレスにping6を実行するには、「ping6 fec0:12ab::1」とコンソールで入力してから、Enterキーを押します。

2 **LAN側とWAN側の接続を確認する。**

プロバイダへping6を実行したり、専用のWebサイトを閲覧するなど、プロバイダから指定されている確認手順を行います。
これでIPv6環境が利用できるようになりました。

UPnP 機能の動作設定を変更する

UPnP機能とは?

UPnPとは、Univesal Plug and Playの略で、UPnP対応OSがUPnP対応機器を自動的に検出するなどの機能のことです。2002年7月時点でのUPnP対応OSは、WindowsMeおよびWindowsXPのみです。

本機はUPnPに対応しているため、ネットボランチのLAN内にあるパソコンからWindows MessengerやMSN Messengerの音声チャットなどを利用できます。

ご注意

- 本機のUPnP機能は、UPnP Forumで規定されている機能すべてに対応しているわけではありません。
- CATV接続など、プロバイダから割り当てられるIPアドレスがプライベートIPアドレスの場合は、UPnP機能を使用したWindows MessengerやMSN Messengerによる音声チャットは使用できません。
- 「かんたん設定」画面でUPnP機能の設定を行うには、あらかじめ接続プロバイダを登録しておく必要があります
- プロバイダを登録せずにWindows MessengerやMSN MessengerなどのUPnP環境を必要とするソフトウェアを起動すると、ルータとの通信に時間がかかるようになります。この場合は接続プロバイダを登録するか、UPnP機能を停止してください。
- Windows MessengerやMSN Messengerの終了／起動を繰り返したり、ルータの再起動や回線の切断などによってパソコンとルータでUPnP機能の情報が異なると、正常に接続できなくなることがあります。

  この場合は、回線を接続した状態でいったんWindows MessengerやMSN Messengerをサインアウトしてから、Windows MessengerやMSN Messengerを再起動します。それでも接続できない場合は、パソコンを再起動してください。

パソコン側でUPnP機能を使えるか確認する

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

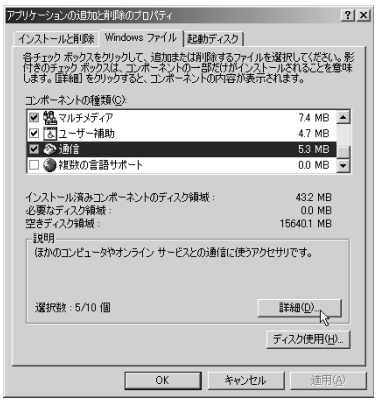
WindowsMeの場合

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

2 **[プログラムの追加と削除]をクリックする。**

3 **[Windowsファイル]タブをクリックする。**

4 **[通信]をクリックして選んでから、[詳細]をクリックする。**



5 **[ユニバーサル プラグ アンドプレイ]にチェックが付いているかどうか確認する。**

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

次のページにつづく▶

6 [ユニバーサル プラグ アンドプレイ]にチェックを付けてから、[OK]をクリックする。

7 [OK]をクリックする。
以後は画面の指示に従って、インストールを行ってください。

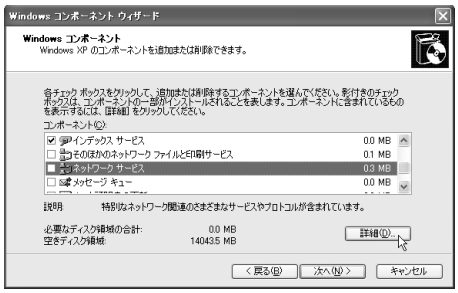
WindowsXPの場合

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

2 [プログラムの追加と削除]をクリックする。

3 画面左側の[Windowsコンポーネントの追加と削除]をクリックする。

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



5 [ユニバーサル プラグ アンドプレイ]にチェックが付いているかどうか確認する。

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

6 [ユニバーサル プラグ アンドプレイ]にチェックを付けてから、[OK]をクリックする。

7 [次へ]をクリックする。
以後は画面の指示に従って、インストールを行ってください。

UPnPを使用しないようにする／設定を変更する

本機のUPnP機能は起動時から動作するため、起動するために特に設定をする必要はありません。ただし、使用環境によっては、UPnP機能がうまく動作しない場合があります。この場合は以下の手順にしたがって、設定を変更してください。

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。

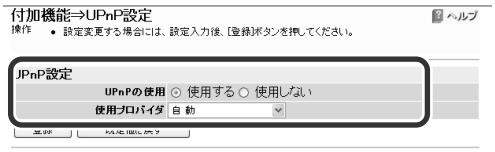
2 **[パスワード]入力欄にルータの管理パスワードを入力してから、[OK]をクリックする。**

「トップ」画面が表示されます。

3 **画面左側の[付加機能]をクリックする。**

4 **[UPnP機能]をクリックする。**

5 **必要な項目を設定する。**



UPnP の使用

UPnP機能を使用する時は、[使用する]を選びます。

使用プロバイダ

UPnP機能を適用するプロバイダを選択します。通常は[自動]（デフォルトゲートウェイのインタフェース）にします。

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。

第8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。

うまく動作しないときは、別冊の「**困ったときは**」をご覧ください。

Acrobat Readerで説明書を読む

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。

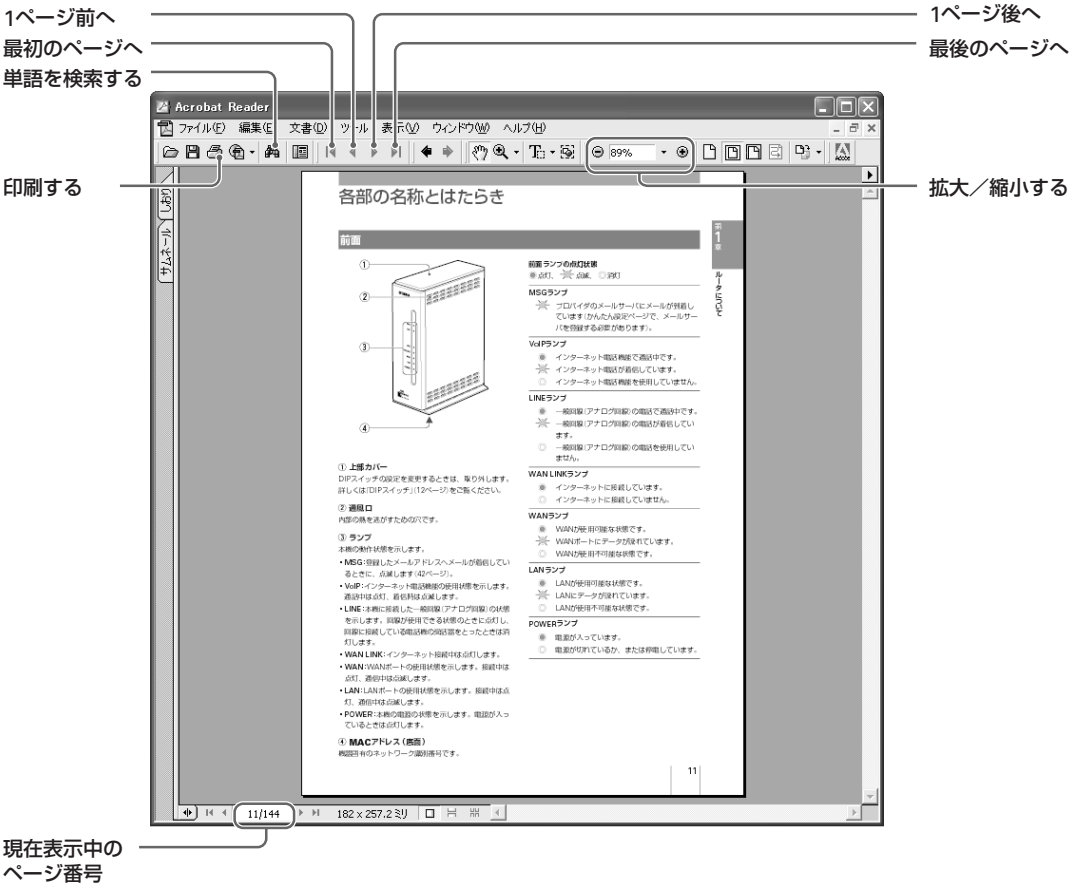
インストーラのウィンドウが開いたら画面のメッセージに従い、Acrobat Readerをインストールします。

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。



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。

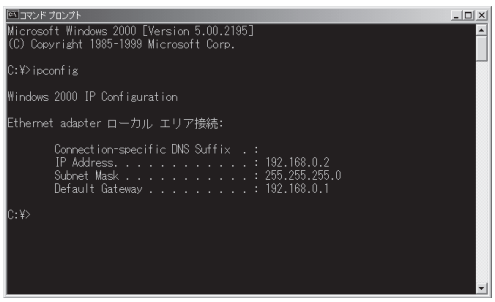
現在パソコンに割り当てられているIPアドレスが表示されます。

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。**

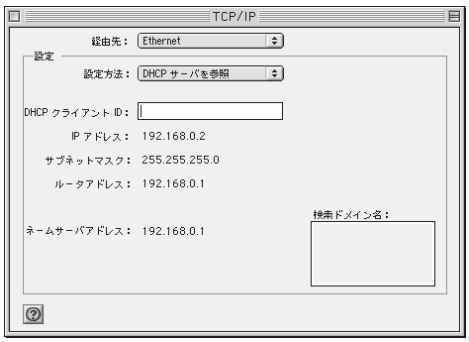


現在パソコンに割り当てられているIPアドレスが表示されます。

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。**

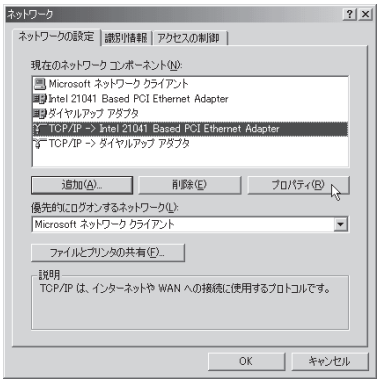
2 **[ネットワーク]をクリックする。**

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。

IPアドレスを変更する

Windows95/98/Meの場合

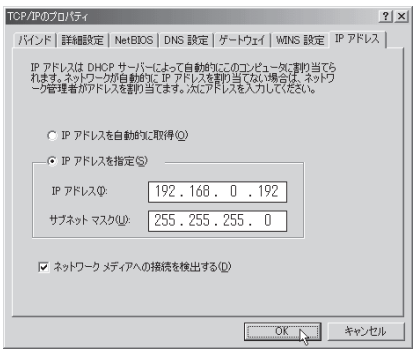
1 [マイコンピュータ]の[コントロールパネル]の[ネットワーク]を開いてから、リストの中の[TCP/IP->(ネットワークカードの名称)]を選び、[プロパティ]をクリックする。



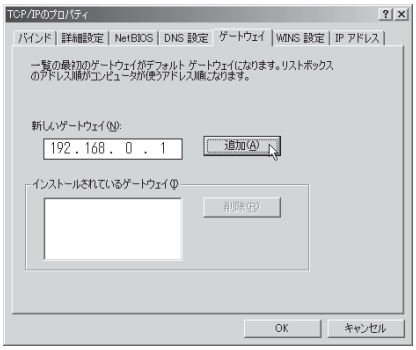
2 [IPアドレス]タブをクリックして、[IPアドレスを指定]を選ぶ。

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。

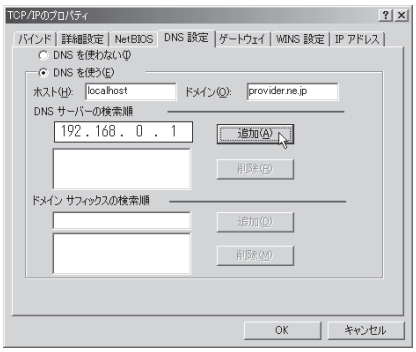


4 [ゲートウェイ]タブをクリックして、[新しいゲートウェイ]に本機のIPアドレス(工場出荷状態では192.168.0.1)を入力してから、[追加]をクリックする。



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。

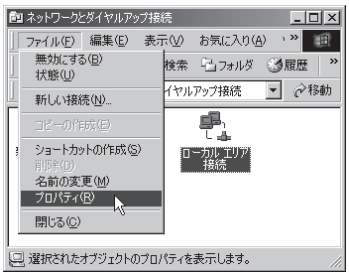
8 LAN上のすべてのWindows95/98/Meパソコンに対して手順1～7の操作を繰り返し、すべてのWindowsパソコンが異なるIPアドレスを持つように設定する。

Windows2000の場合

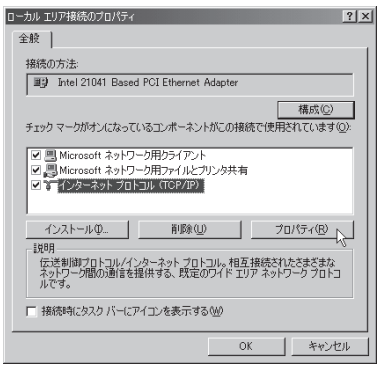
1 [スタート]ボタンをクリックして、[設定]－[コントロール パネル]をクリックする。

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。

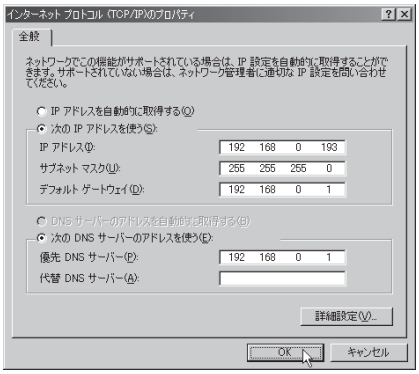


4 リストの[インターネットプロトコル(TCP/IP)]を選んでから、[プロパティ]をクリックする。



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。

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。

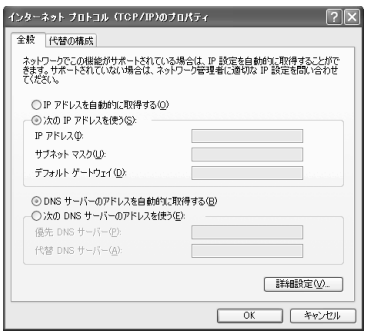
4 [ローカルエリア接続]のアイコンをクリックする。

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。

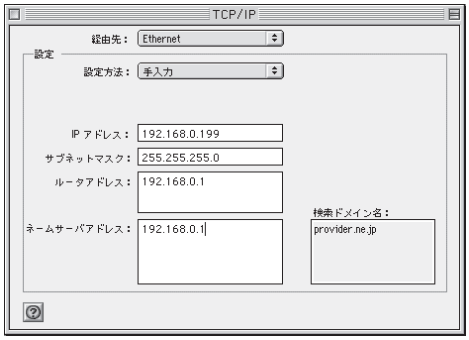
10 LAN上のすべてのWindowsXPパソコンに対して手順1～7の操作を繰り返し、すべてのWindowsパソコンが異なるIPアドレスを持つように設定する。

Mac OSの場合

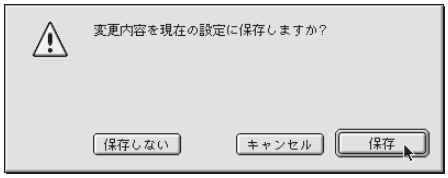
1 アップルメニューから[コントロールパネル]ー[TCP/IP]を選ぶ。

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

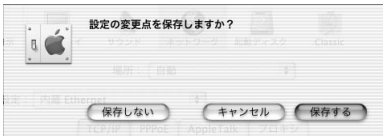
1 アップルメニューから[システム環境設定]を選ぶ。

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。

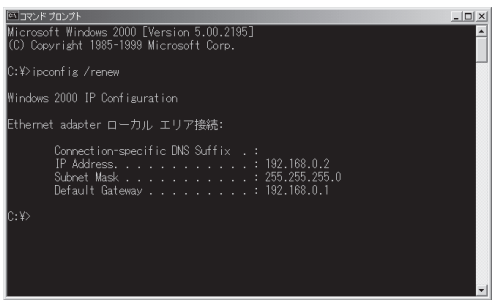
他のパソコンと重複しないプライベートIPアドレスに更新されます。

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。

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:720 g
ACアダプタ:550 g

電源:
AC100V(50/60Hz)

消費電力:
最大10 W
(停電時TEL1ポート使用可)

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)

アナログインタフェース:
2線式(RJ-11)×3(供給電圧−48V)
PB、DP(10PPS, 20PPS)自動認識
線路抵抗 400Ω(電話機込み)

LINE(一般公衆回線)インタフェース:
2線式(RJ-11)×1
PB、DP(10PPS, 20PPS)

LANインタフェース:
イーサネット10/100BASE-TX×4ポート
スイッチングHUB(RJ-45)

WANインタフェース:
イーサネット10/100BASE-TX×1ポート(RJ-45)

表示機能:
LED x 7(MSG、VoIP、LINE、WAN LINK、WAN、
LAN、POWER)

付属品:
ACアダプタ P10V1.2A(1)
LANケーブル(1)
モジュラーケーブル(1)
CD-ROM(1)
各種マニュアル
- 設定マニュアル(1)
- 活用マニュアル(1)
- 困ったときは(1)

「かんたん設定ページ」 設定項目一覧

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 • 現在の接続状態
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を用いないネットワーク型ADSLインターネット • PPTPを使用したネットワーク型LAN間接続VPN • PPTPを使用したリモートアクセスVPNサーバ
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の設定 • ネットボランチDNSサービス（ホストアドレスサービス） • 現在の接続状態
LAN間接続管理*	• LAN間接続 • 登録の管理 • 現在の回線接続状態
リモートアクセス管理*	• リモートアクセスVPNサーバ（PP） • リモートアクセスVPNサーバ（Anonymous） • 登録の管理 • 現在の回線接続状態
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

[電話設定]

基本設定	• TEL1ポート • TEL2ポート • TEL3ポート • 電話回線の設定 • 電話回線の利用
TEL1ポートの詳細	• 着信機能 • 着信ベル • 識別着信番号 • 電話機対応機能
TEL2ポートの詳細	• 着信機能 • 着信ベル • 識別着信番号 • 電話機対応機能
TEL3ポートの詳細	• 着信機能 • 着信ベル • 識別着信番号 • 電話機対応機能
機器間アナログ通話設定	• アナログ通話モードの設定
インターネット電話設定	• 基本設定 • インターネット電話帳 • ネットボランチDNSサービス

[付加機能]

ファイアウォール機能	• ファイアウォール設定 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 • ファイアウォール状態 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
IPv6設定	• プロバイダの選択 • IPv6プレフィックスの設定 • プロバイダとの接続方法 • 経路制御方法
UPnP設定	• UPnP設定

[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

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。

config
プロバイダに接続するために必要な情報や各種の設定情報を、1つの設定ファイル(config)としてまとめたものです。

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。

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。

DP
電話で発信する時に、電話機から電話局に送信する信号の一種です。

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。Web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。

IPv4／IPv6
IPv6は現在のインターネットにおけるアドレスの不足や経路制御の複雑さを解決する新しい通信方式で、Internet Protocol Version 6の略語です。IPv6を用いると、すべての機器を固有のアドレスによって識別できるようになるため、双方向の通信が可能になります。なお、従来の通信方式はIPv4（Internet Protocol version 4）と呼ばれます。IPv4とIPv6の間には互換性はありません。

IPv6 over IPv4トンネリング／IPv4 over IPv6トンネリング
IPv6 over IPv4トンネリングとは、IPv4ネットワークを経由してIPv6ネットワークを接続するためのプロトコルです。IPv6への移行の初期においては、IPv4ネットワークの中にIPv6ネットワークが点在する環境となるため、IPv6 over IPv4トンネリングが重要になります。

IPv4 over IPv6トンネリングは、IPv6ネットワークを経由してIPv4ネットワークを接続するためのプロトコルです。IPv6ネットワークで隔てられたIPv4ネットワークを接続する場合に使用します。

Lモード
NTT東日本およびNTT西日本が提供する、電話機やFAXを使ってメールを送受信したり、情報を検索したりできるサービスです。

Lモード対応電話機やFAXなどのアナログ機器を本機に接続すれば、Lモードのメッセージ到着お知らせサービスを利用できます。

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。

PB
電話機が電話をかける時に、ダイヤルボタンに応じて発する音のことです。いわゆる「ピポパ」です。

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。

PPP
ISDNなどの通信回線上で、IP通信を行うための下回りを担当するプロトコルです。データの圧縮を行ったり、接続の時には相手を確認するユーザ認証を行うことで、知らない相手からの接続を拒否するような機能を持っています。

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。

RIPng
IPv4で広く用いられているRIPを、IPv6に対応させた経路制御プロトコルです。 RIPngは、IPv6における基本的な経路制御プロトコルとして扱われます。

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。

UPnP
Univesal Plug and Playの略で、TCP/IPを元にしたプロトコルです。UPnP対応OSからはネットワーク内のUPnP対応機器を自動的に検出できるため、設定の手間を削減できます。

URL
Web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://ホストアドレス/一般的にはファイル名）

VoIP
Voice over IPの略で、IPネットワーク上で音声通話をするための技術です。ネットボランチでは、インターネットを経由して通話を行うインターネット電話機能と、LAN内で内線通話を行う機器間アナログ通話機能でこの技術を利用しています。

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。

Webブラウザ
→ブラウザ

WWW
World Wide Webの略語です。HTML文書を蓄えるWebサーバと、HTML文書を表示する能力を持つWeb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。

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。

オフフック
電話機の受話器を持ち上げた状態のことです。

オンフック
電話機の受話器を置いた状態のことです。オンフックの時、電話は切れています。

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。

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。

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。

識別着信
電話番号を登録し、その電話番号から電話がかかってきた時に着信するかどうかを指定できる機能です。登録した番号からの着信は受け取らなかったり、反対に登録した番号からの着信だけができるようにしたりすることができます。

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。

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

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。

ダイヤルイン
1本の回線に複数の電話番号を割り当てることです。ダイヤルインを利用するには、NTTなどの通信事業者に申し込みます。

ダイヤルトーン
電話で、受話器を上げた時にツーと聞こえる音です。電話機のダイヤルはダイヤルトーンが聞こえてから回し始めます。

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。

トーン回線
アナログの電話回線で、PBにより発信できる回線のことです。

トンネル
ネットワーク上に仮想の専用通路を設けるための技術です。パケットの暗号化などによってデータ内容を隠蔽して、セキュリティを高めます。主にインターネット上の仮想プライベートネットワーク(VPN)を構築する際の専用通路を指しますが、IPv4ネットワークを経由してIPv6ネットワークを接続するためのプロトコルのことを指す場合もあります。
→IPv6 over IPv4トンネリング

ナンバー・ディスプレイ
オンフック時に着信があったとき、どこから着信したかを通知してくれる機能のことです。

ナンバー・リクエスト
ナンバー･ディスプレイの付加サービスの1つで、番号非通知でかかってきた電話に対して、かけなおすように音声案内(トーキ)を流す機能のことです。本機ではNTTと契約しなくともナンバー･リクエストの動作を擬似的に再現する、擬似ナンバー･リクエスト機能に対応しています。

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。

パルス回線
アナログの電話回線で、DPの回数で発信する電話番号を指定する回線のことです。

ビジートーン
電話で、相手が話中などの時に聞こえる音「ツー、ツー」です。

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。

フッキング
電話機のフックスイッチ(受話器を置くところにあるスイッチ)をポンと押してすぐ離す操作のことです。最近の電話機ではフックスイッチとは別にフッキングするためのボタンが用意されていることもあります。フッキングはフレックスホンの操作を行う時などに使います。

ブラウザ
Web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
Webサイトの一番入口のページを指します。

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。

モデム
パソコンのシリアルポートやモデムポートに接続して、アナログ回線経由で通信を行うための装置です。

優先着信
同じ電話番号で複数のTELポートに着信する場合、指定したTELポートを先に鳴らす機能です。

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。

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
RT56v専用サービス窓口
TEL―03-5715-0350
ADSLルータ専用お客様窓口
TEL―03-5715-3575
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

V953370

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