RT60w
追加機能マニュアル

このマニュアルでは、RT60wに追加された新機能について説明しています。ユーザーズマニュアルと併せてお読みください。

目次

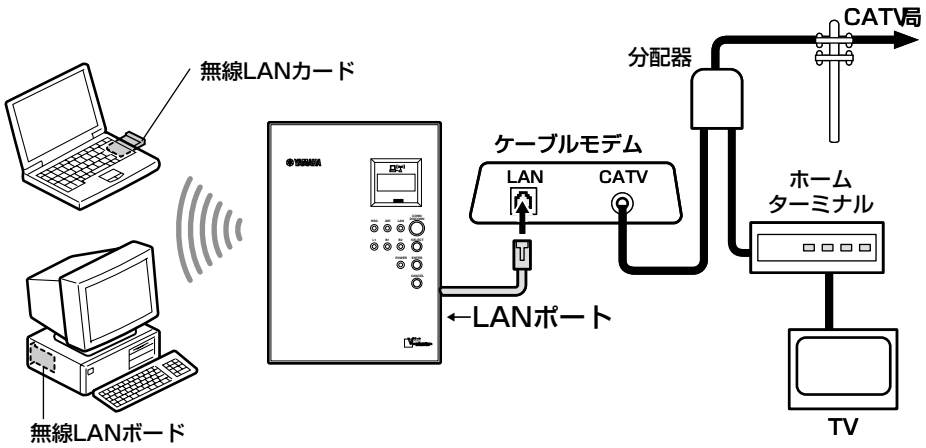
第１章
CATV/ADSLの接続

この章では、RT60wでCATV/ADSLに接続する時の基本的な操作や知っておいてほしい知識について説明しています。使い始める前に、ご一読ください。

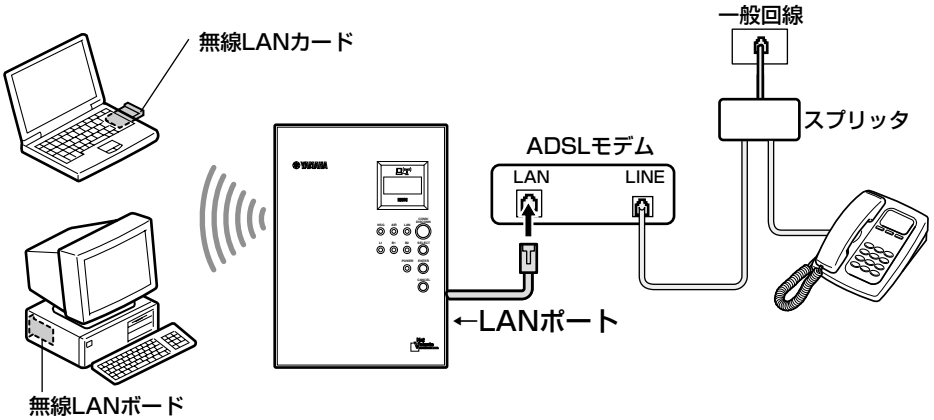
1.1 CATV/ADSLの接続

CATV 接続や ADSL 接続、フレッツ・ADSL 接続での場合は、以下の方法で本機のLANポートにケーブルモデムまたはADSLモデムを接続します。ケーブルモデムやADSLモデムの設置は、業者が行う場合とユーザが行う場合があります。各業者の指示に従って設置してください。

● CATV 接続の場合



● ADSL 接続／フレッツ・ADSL 接続の場合



⚠注意

- CATV または ADSL の場合、本機を CATV アンテナ線や ADSL 用の一般回線に直接接続することはできません。必ず、ケーブルモデムまたは ADSL モデムに接続してください。
- この機能ではRT60wのLANポートはADSL/CATVの回線接続に使用されるため、LAN ポートとパソコンは接続できなくなります。無線 LAN で接続されたパソコンのみがこの機能を使用できます。

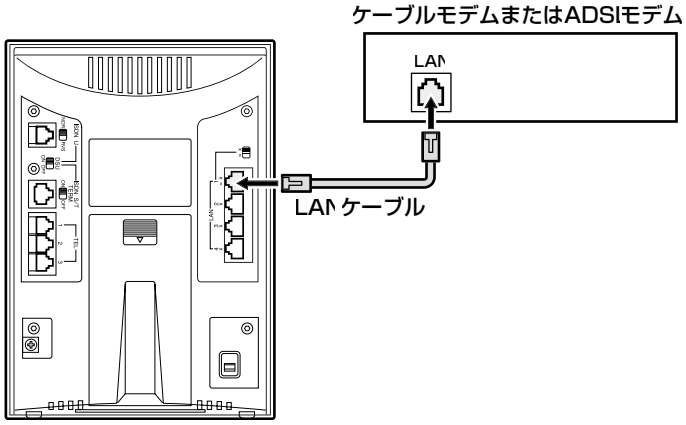
必要なもの

○ LANケーブル　　本機のLANポートは、ケーブルモデムやADSLモデムを接続できます。ケーブルモデムやADSLモデムの種類に合わせてストレートタイプまたはクロスタイプのLANケーブルをご用意ください。（ケーブルモデムやADSLモデムに付属している場合もあります。）

MEMO
- ケーブルモデムやADSLモデムとパソコンをストレートケーブルで接続するように指示されている場合は、本機のLANポートへの接続もストレートケーブルを使用します。
- ケーブルモデムやADSLモデムとパソコンをクロスケーブルで接続するように指示されている場合は、本機のLANポートへの接続もクロスケーブルを使用します。

接続のしかた

1 ケーブルモデムまたはADSLモデムのLANポートと本機のLAN1ポートをLANケーブルで接続します。L2、3、4ポートには機器を接続しないで下さい。LANスイッチを「Ｉ Ｉ」側にして、LANランプが点灯することを確認してください。



MEMO
- ISDN回線を接続しない場合は、TELポート間の内線通話以外でTELポートにアナログ機器（電話機、FAX、モデムなど）を接続して使うことはできません。

2 無線LANの設定をまだ行っていない場合は、設定してください。（→スタートマニュアル「第2.8節　無線LANに接続する」）

1.2　CATV、PPPoE方式以外のADSL接続を設定する

PPPoE方式以外のADSLでインターネットに接続する場合は、本機の「かんたん設定ページ」を開いて、CATV/ADSLの接続先を設定します。
フレッツ・ADSLなどPPPoE方式のADSL接続の場合は、「1.3　ADSL接続を設定する」をご覧ください。

⚠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と、パソコンのダイヤルアップネットワーク設定（TA接続利用時）の両方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、ご使用ください。（→「第２章　ファイアウォール機能の使いかた」）

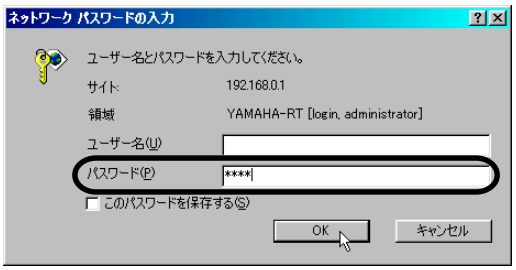
ここではWindows 98とInternet Explorer 5.5の画面を例に説明しています。他のOSの場合、画面表示が多少異なりますが、操作は同じです。「RT60wパソコンセットアップ」で引き続き設定する場合は、手順３から始めてください。

1 POWERスイッチをオンにします。

2 無線LANに接続している1台のパソコンでブラウザを開き、アドレス入力欄に“http://192.168.0.1/”を入力して、［enter］キーを押します。
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。

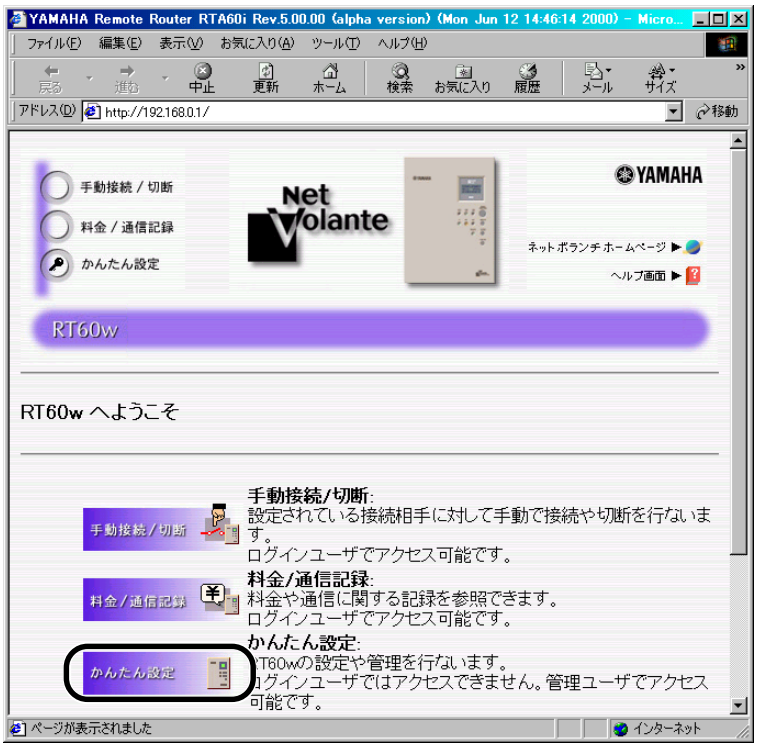
「ネットワーク パスワードの入力」ウィンドウが表示されます。

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、［OK］ボタンを押します。

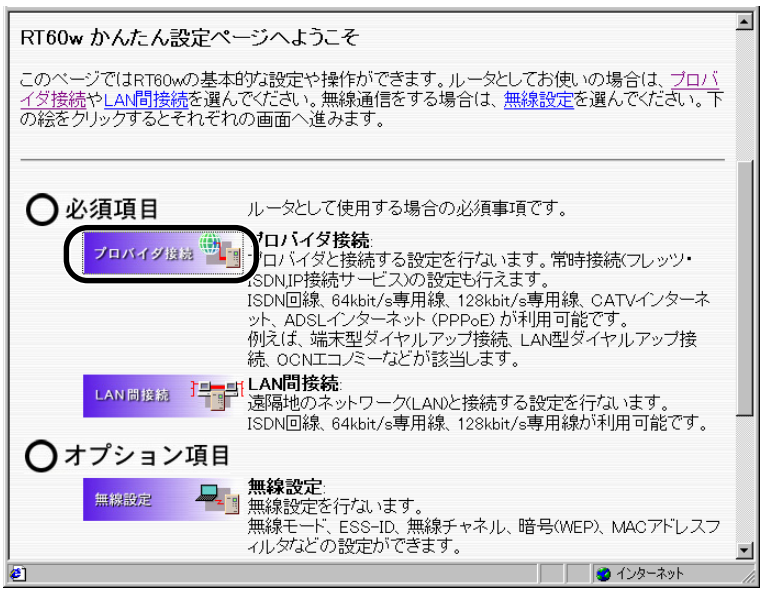


「RT60wへようこそ」ページが表示されます。

4 ［かんたん設定］を押します。

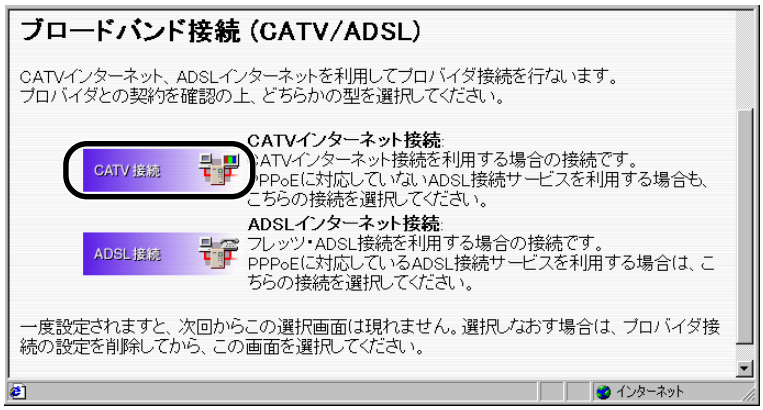


5 ［プロバイダ接続］を押します。

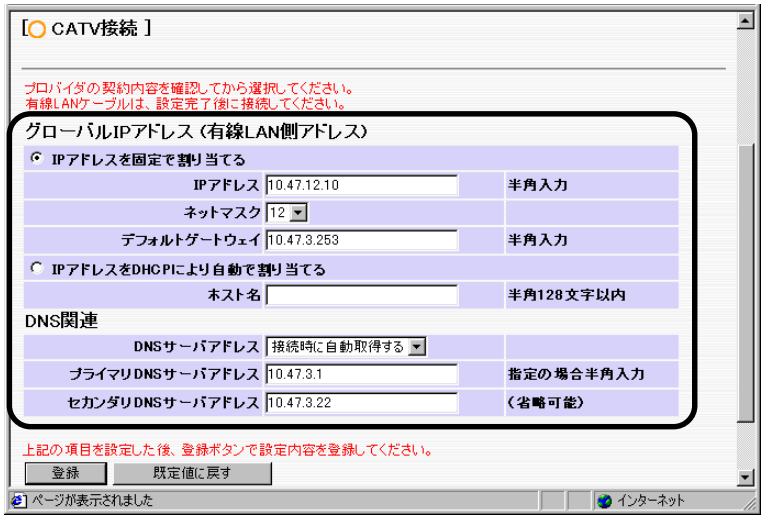


「RT60w プロバイダ接続の接続形態選択」ページが表示されます。

6 [ブロードバンド接続 CATV/ADSL)]の［CATV 接続］を押します。



7 プロバイダまたはCATV業者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します。



グローバルIPアドレス： ［IPアドレスを固定で割り当てる］ ［IPアドレスをDCHPにより自動で割り当てる］	LANポートに割り当てるIPアドレスの取得方法を選択します。 自動取得となっている場合に選択してください。 プロバイダまたはCATV業者からIPアドレスが指定されている場合に選択してください。
IPアドレスの指定：	IPアドレスをプロバイダまたはCATV業者から指定されている場合に入力してください。
ネットマスク：	ネットマスクをプロバイダまたはCATV業者から指定されている場合に入力してください。
デフォルトゲートウェイアドレス：	デフォルトゲートウェイをプロバイダまたはCATV業者から指定されている場合に入力してください。

DNS サーバアドレス： ［IP アドレスを指定する］ ［接続時に自動取得する］	DNS サーバアドレスの取得方法を選択します。 プロバイダまたは CATV 業者から DNS サーバアドレスが指定されている場合に選択してください。 プロバイダまたは CATV 業者から 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択してください。
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てください。
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てください。（省略可）

⚠注意

・RT60w は工場出荷状態で無線 LAN 側のネットワークアドレスとして 192.168.0.0/24を使用します。有線LAN側のネットワークアドレスと無線 LAN 側のネットワークアドレスが同じ場合は、ルータの IP アドレスを変更することで無線 LAN 側のネットワークアドレスを変更します。（→ユーザーズマニュアル 「7.5 ルータのIPアドレスを変更する」）

8 入力し終わったら、［登録］ボタンを押します。
メッセージに従ってボタンを押すと接続先が登録されます。

⚠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。（→「第２章　ファイアウォール機能の使いかた」）

9 ページ右上の［ネットボランチホームページ］を押します。

インターネットのNetVolanteのホームページが表示されれば、ルータの設定は完了です。

●表示されない場合

接続業者との契約内容と設定が間違っている可能性があります。設定内容をもう一度ご確認ください。（IP アドレス、DNS サーバアドレスなど）

1.3　PPPoE方式のADSL接続を設定する

フレッツ・ADSLなどPPPoE方式を利用したADSLでインターネットに接続する場合は、本機の「かんたん設定ページ」を開いて、ADSLの接続先を設定します。

⚠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と、パソコンのダイヤルアップネットワーク設定（TA接続利用時）の両方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、ご使用ください。（→「第２章　ファイアウォール機能の使いかた」）

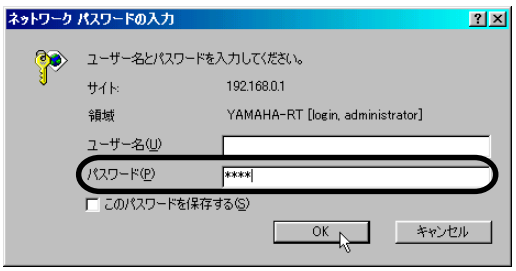
ここではWindows 98とInternet Explorer 5.5の画面を例に説明しています。他のOSの場合、画面表示が多少異なりますが、操作は同じです。「RT60wパソコンセットアップ」で引き続き設定する場合は、手順３から始めてください。

1 POWERスイッチをオンにします。

2 無線LANに接続している１台のパソコンでブラウザを開き、アドレス入力欄に“http://192.168.0.1/”を入力して、［enter］キーを押します。
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。

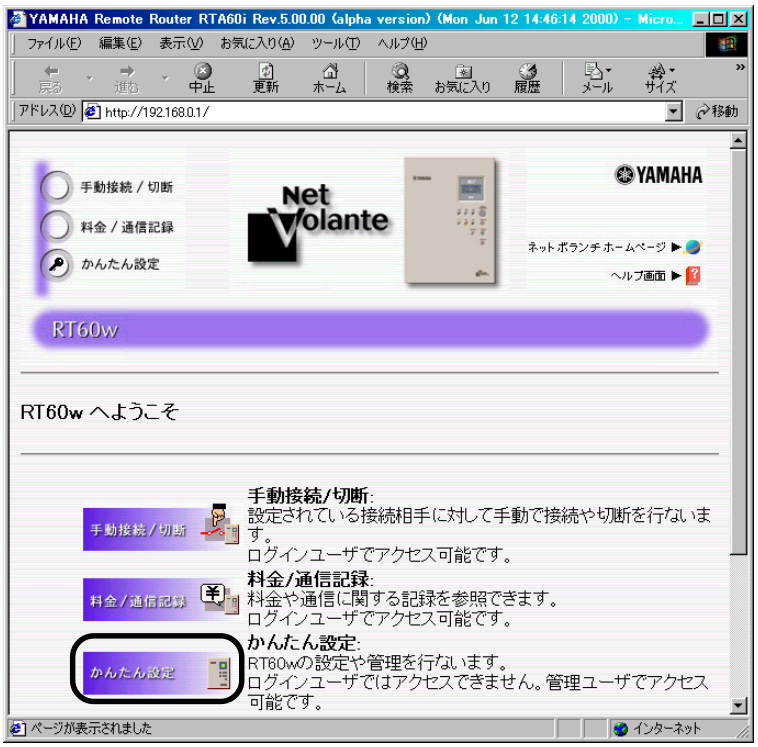
「ネットワーク パスワードの入力」ウィンドウが表示されます。

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、［OK］ボタンを押します。

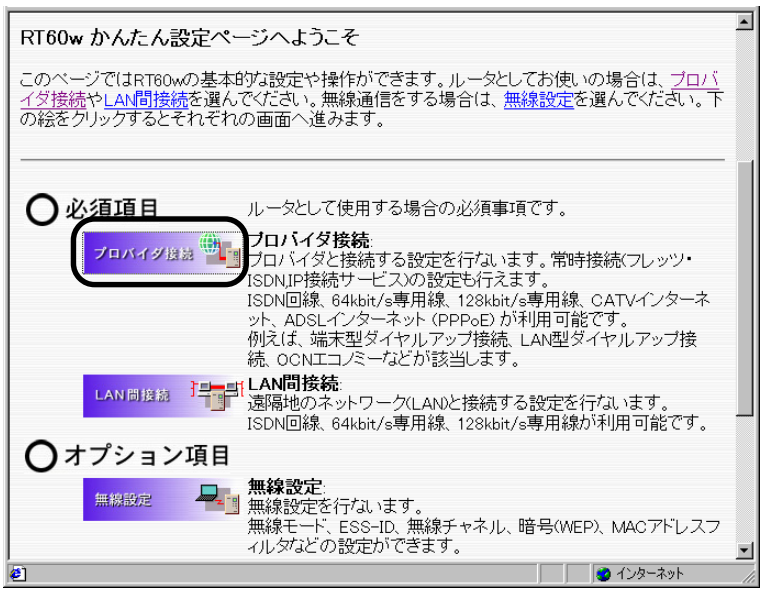


「RT60wへようこそ」ページが表示されます。

4 ［かんたん設定］を押します。

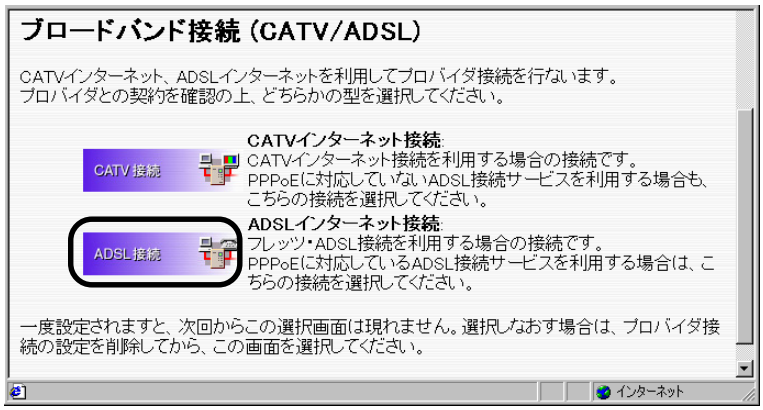


5 ［プロバイダ接続］を押します。

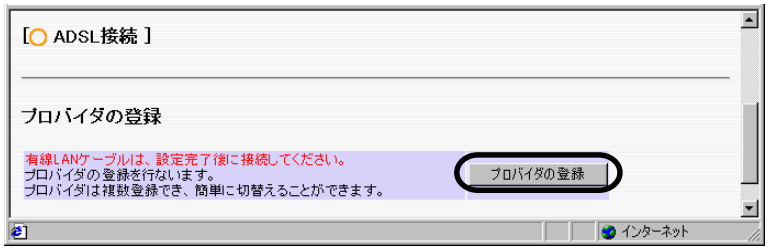


「RT60w プロバイダ接続の接続形態選択」ページが表示されます。

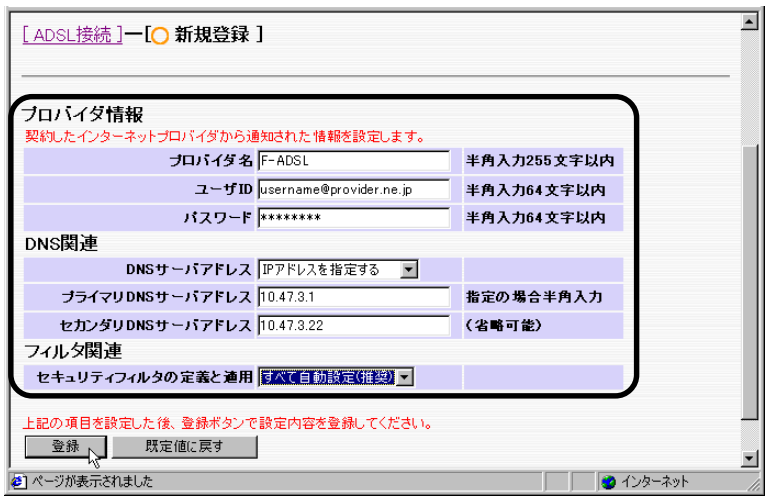
6 [ブロードバンド接続 CATV/ADSL)]の［ADSL 接続］を押します。



7 [プロバイダの登録]を押します。



8 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します。



プロバイダ名：	接続先がわかるような任意の名称を入力してください。
ユーザ ID：	プロバイダから指定されたフレッツ・ADSL 接続用のユーザIDを入力してください。ユーザIDは、必ず書類を確認してください。 例）username@provider.ne.jp username@aaa.provider.ne.jp （サブドメインが付加される場合）
パスワード：	指定されたパスワードまたは自分で変更したパスワードを入力してください。半角英数字で大文字小文字も正確に入力してくだい。
DNS サーバアドレス： ［IP アドレスを指定する］ ［接続時に自動取得する］	DNS サーバアドレスの取得方法を選択します。 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択してください。 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択してください。
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てください。
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てください。（省略可）
セキュリティフィルタの定義と適用: ［すべて自動設定(推奨)］ ［定義のみ自動設定］ ［すべて手動設定］	セキュリティフィルタの設定方法を選択してください。 すべてのフィルタを自動設定します。 フィルタの定義だけを自動設定します。 すべてのフィルタを手動で設定する場合に選択してください。

9 入力し終わったら、［登録］ボタンを押します。
メッセージに従ってボタンを押すと接続先が登録されます。

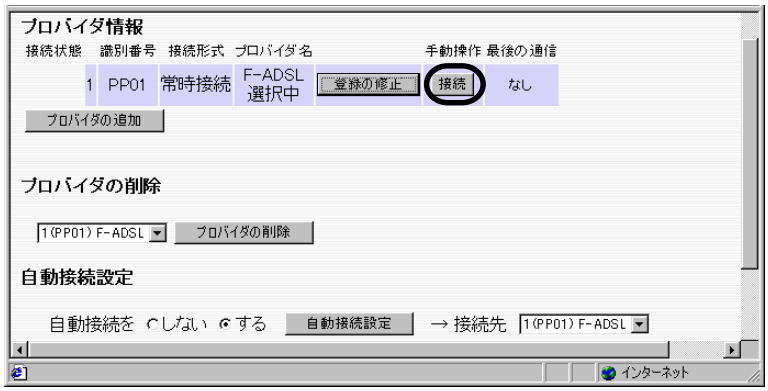
⚠注意

・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。（→ユーザーズマニュアル「第２章　ファイアウォール機能の使いかた」）

MEMO

・設定したパスワードの文字数を隠すため、ページを再表示したときは、パスワード欄が「＊」一つだけの表示となります。

10 登録したプロバイダの［接続］ボタンを押して、手動接続します。



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、以下のことを確認してください。

●失敗した理由が表示された場合

［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］ボタンを押して、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、パスワードを大文字／小文字や全角／半角に注意しながら入力し直してから、もう一度手動接続を行ってください。

11 ページ左上の［ネットボランチホームページ］を押します。

インターネットのNetVolanteのホームページが表示されれば、ルータの設定は完了です。

●表示されない場合

［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］ボタンを押して、一旦接続を切断してから、［登録の修正］ボタンを押して、設定内容をもう一度確認してください。

第２章
ファイアウォール機能の使いかた

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であるフィルタ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ています。設定にはネットワークの知識が必要になるものもありますが、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。
また、より専門的な設定例については、「コマンドリファレンス」やヤマハRTシリーズのホームページ“http://www.rtpro.yamaha.co.jp/”をご覧ください。

2.1　セキュリティ機能について

インターネットに接続すると、世界中のいろいろなホームページを見ることができたり、Eメールが自由に使えたりと、とても便利です。しかし、同時に世界中の危険にさらされていることをも意味します。インターネットに常時接続するときやサーバを公開するときは、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。

⚠注意

・不正アクセスの手段や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、常にリスクがあることをご承知ください。また、常に新しい情報を入手し、自己責任でセキュリティ設定を行うことを強く推奨します。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について

TA/モデムでインターネット接続している場合やサーバを公開している場合は、悪意のある者からパソコンやルータが直接**「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、アドレス変換機能（NAT、IPマスカレード）により比較的安全ですが、誤った設定や設定不足で同様の危険にさらされる場合があります。
もし、ルータ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、フィルタ設定によるセキュリティ（自己防衛）が必要です。

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、特に被害に遭う確率が高くなります。固定アドレスの専用線／ネットワーク型ダイヤルアップ、動的アドレスを使い続けるフレッツ·ISDN／CATV／ADSL／フレッツ·ADSLなどで接続する場合は、十分なセキュリティを設定することをお勧めします。また、ダイヤルアップ接続でもグローバルIPアドレスを割り当てられている間は、同じように被害に遭う可能性があります。同様にセキュリティ設定を行うことをお勧めします。
もちろん、ルータのパスワードを設定しないなどは問題外の行為なので、必ずパスワードを設定したり、ときどきパスワードを変更しながら、ルータをお使いください。

接　続　先	グローバルIPアドレスの種類	危　険　度
端末型ダイヤルアップ接続	動的アドレス	！（接続中危険）
ネットワーク型ダイヤルアップ接続	固定アドレス	！！（接続中危険）
フレッツ·ISDN接続	動的アドレス	！！（長時間接続時危険）
CATV接続、PPPoE方式以外のADSL接続	プライベートアドレスの場合 動的アドレスの場合 固定アドレスの場合	！（CATV内アドレスに対しては危険） ！！（長時間接続時危険） ！！！（常に危険）
フレッツ·ADSLなどPPPoE方式のADSL接続	動的アドレスの場合 固定アドレスの場合	！！（長時間接続時危険） ！！！（常に危険）
専用線接続	固定アドレス	！！！（常に危険）

不正アクセスへの対抗手段について

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

→ 接続を切ったり、グローバルIPアドレスを変えることが、最大の防御です。フレッツ・ISDNやフレッツ・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、接続のたびに動的アドレスを変えることができます。

→ 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である程度防ぐことができます。本機のフィルタ設定で、パケットフィルタリングを行うことが可能です。

→ 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を使って、整合性のないパケットや不審なActiveX、Javaアプレットを通さないことで、かなり防ぐことができます。また、ウィルス検知ソフトと組み合わせて使うことも可能です。しかし、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をインストールする必要があります。

● OS やサーバソフトのセキュリティホールを突いて侵入するもの

→ OS やサーバソフトのバージョンアップや適切な設定・運用を行うことで、かなり防ぐことができます。

●メールの添付ファイルとして侵入するもの

→ ユーザが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ユーザに徹底してもらうことが必要です。また、各パソコンにウィルス検知ソフトをインストールし、ウィルスの早期発見と駆除に勤めることで、被害を最小限にできます。

ルータのフィルタ設定でできること

本機のフィルタ設定では、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することができます。各接続先毎に 100 個ずつのフィルタを設定することが可能です。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ことで、不正なパケットがLAN内に入ることを防げます。
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、ルータで防ぐことはできません。これらのセキュリティに関しては、ウィルス検知ソフト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などを併用してください。

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、次の考えかたを基本にするとよいでしょう。

- **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、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。WWWサーバの公開など、必要がある場合に最小限だけ許可します。
  ただし、ここでいう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で、LAN側からリクエストしたパケットの応答パケットは、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、ホームページデータやEメールの受信は、自由に行えます。

静的フィルタと動的フィルタについて

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**
  一度設定を行うと、データや通信の有無にかかわらず常に有効になるフィルタです。
- **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機能が有効になります。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ようなことができます。

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。

2.2　フィルタを設定する

本機のフィルタ設定は、「かんたん設定ページ」の「フィルタ設定」ページ、またはコンソールコマンドで行います。

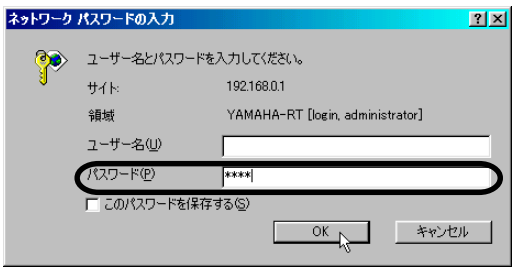
ブラウザで設定する場合

ここではWindows 98とInternet Explorer 5.5の画面を例に説明しています。他のOSの場合、画面表示が多少異なりますが、操作は同じです。「RT60w パソコンセットアップ」で引き続き設定する場合は、手順3から始めてください。

1 無線LANに接続している1台のパソコンでブラウザを開き、アドレス入力欄に“http://192.168.0.1/”を入力して、［enter］キーを押します。
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。

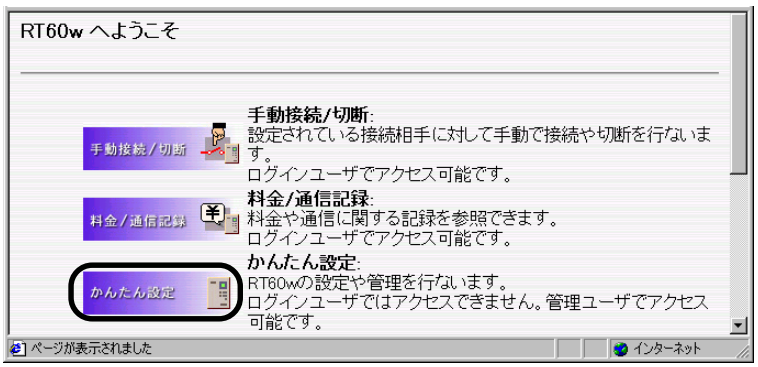
「ネットワーク パスワードの入力」ウィンドウが表示されます。

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、［OK］ボタンを押します。

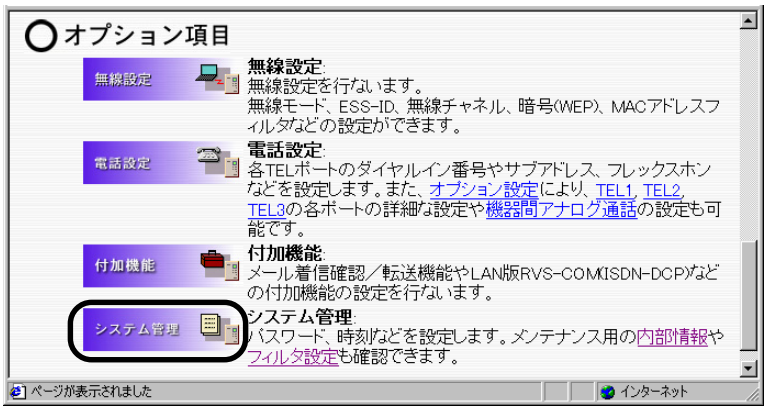


「RT60w へようこそ」ページが表示されます。

3 ［かんたん設定］を押します。



4 ［システム管理］を押します。



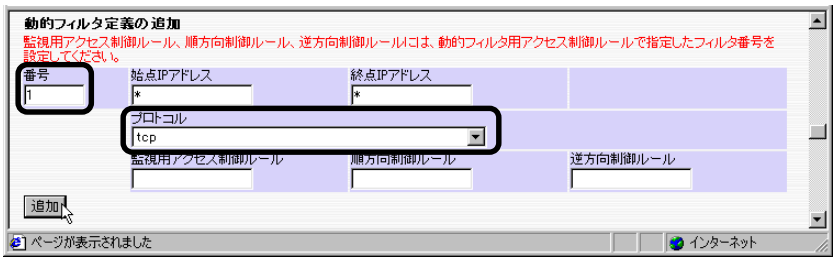
5 ［フィルタ設定］を押します。

動的フィルタの設定例

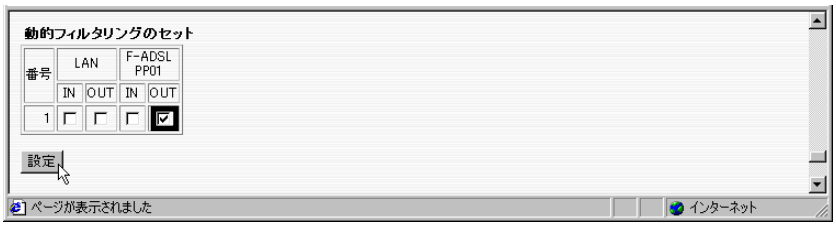
MEMO ・静的フィルタの設定については、ユーザーズマニュアルの「ルータのフィルタ設定変更」（176 ページ）を参照してください。

● tcp に対して動的フィルタを設定する場合の例

6 「動的フィルタ定義の追加」で［フィルタ番号］を入力し、［プロトコル］で tcp を選択し、［追加］ボタンを押します。

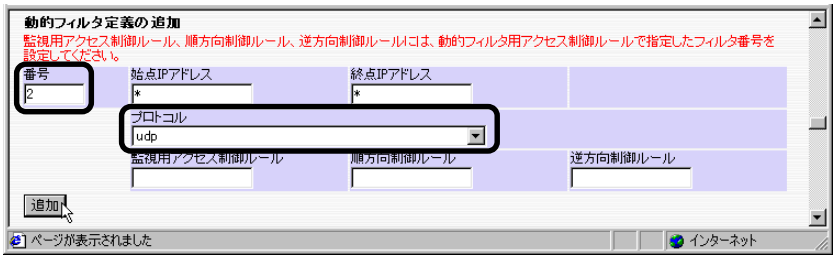


7 「動的フィルタリングのセット」で次のようにチェックし、［設定］ボタンを押します。

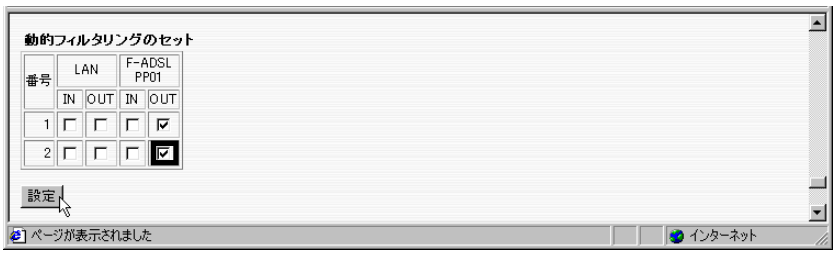


● udp に対して動的フィルタを設定する場合の例

8 「動的フィルタ定義の追加」で［フィルタ番号］を入力し、［プロトコル］で udp を選択し、［追加］ボタンを押します。

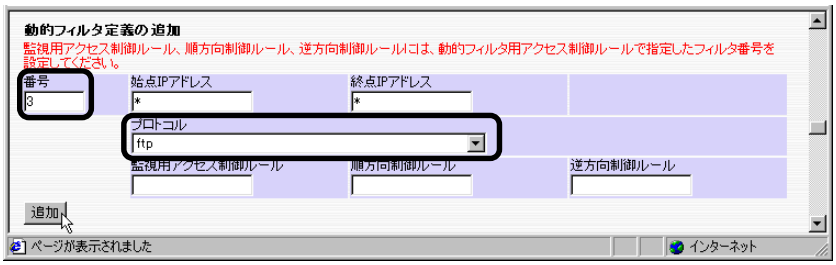


9 「動的フィルタリングのセット」で次のようにチェックし、［設定］ボタンを押します。



● ftp に対して動的フィルタを設定する場合の例

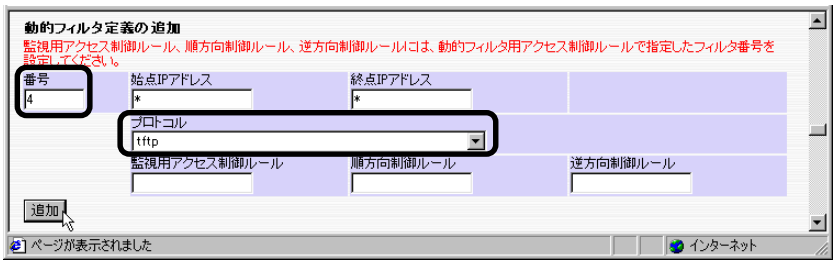
10 「動的フィルタ定義の追加」で［フィルタ番号］を入力し、［プロトコル］で ftp を選択し、［追加］ボタンを押します。



11 「動的フィルタリングのセット」で次のようにチェックし、［設定］ボタンを押します。

● tftp に対して動的フィルタを設定する場合の例

10 「動的フィルタ定義の追加」で［フィルタ番号］を入力し、［プロトコル］で tftp を選択し、［追加］ボタンを押します。



11 「動的フィルタリングのセット」で次のようにチェックし、［設定］ボタンを押します。

全てのプロトコルの動的フィルタを設定した場合の例

全てのプロトコルの動的フィルタを設定した状態の「動的フィルタの設定」と「動的フィルタのセット」の例を以下に示します。

●「動的フィルタの設定」の例

動的フィルタ定義の設定

ブラウザからの設定ではフィルタ番号1～を御使用ください。

番号	始点IPアドレス 監視用アクセス制御ルール	終点IPアドレス 順方向制御ルール	プロトコル 逆方向制御ルール
1	* -	* -	tcp -
2	* -	* -	udp -
3	* -	* -	ftp -
4	* -	* -	tftp -
5	* -	* -	domain -
6	* -	* -	www -
7	* -	* -	smtp -
8	* -	* -	pop3 -
9	* -	* -	telnet -

ページが表示されました　インターネット

●「動的フィルタのセット」の例

動的フィルタリングのセット

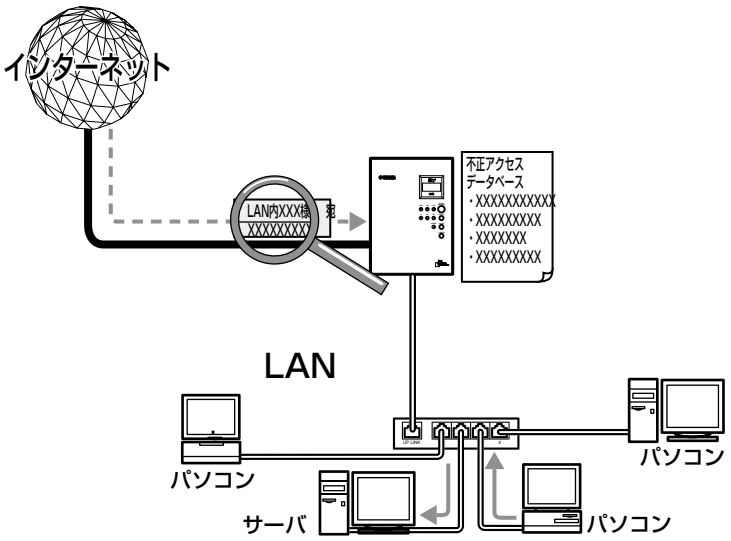
番号	LAN		F-ADSL PP01	
	IN	OUT	IN	OUT
1	☐	☐	☐	☑
2	☐	☐	☐	☑
3	☐	☐	☐	☑
4	☐	☐	☐	☑
5	☐	☐	☐	☑
6	☐	☐	☐	☑
7	☐	☐	☐	☑
8	☐	☐	☐	☑
9	☐	☐	☐	☑

設定

ページが表示されました　インターネット

2.3　不正アクセス検知機能について

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知し、ユーザに警告する機能です。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したり、破棄することができます。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。



⚠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。また検知された場合に、それが必ず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、ご使用ください。
- 本機能は各インタフェース、入出力に適用可能ですが、適用数が多くなると、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。

2.4 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「フィルタ設定」ページで行います。インタフェース毎に、検知するパケットの方向や検知時の処理方法を設定することができます。

MEMO

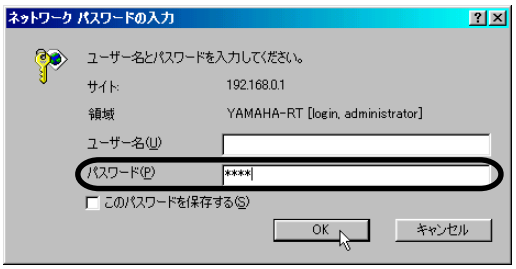
・不正アクセス検知機能を有効にした場合、工場出荷状態では侵入検知の際にブザーを鳴らします。鳴らしたくないときは、［システム管理］の［ブザー設定］で変更することができます。

ここではWindows 98とInternet Explorer 5.5の画面を例に説明しています。他のOSの場合、画面表示が多少異なりますが、操作は同じです。「RT60w パソコンセットアップ」で引き続き設定する場合は、手順3から始めてください。

1 無線LANに接続している1台のパソコンでブラウザを開き、アドレス入力欄に“http://192.168.0.1/”を入力して、［enter］キーを押します。
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。

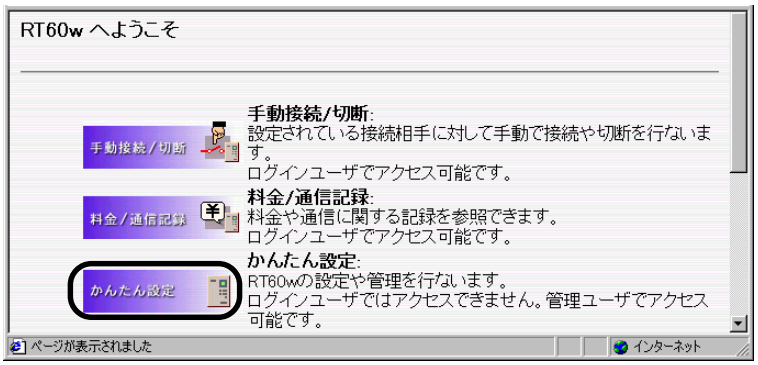
「ネットワーク パスワードの入力」ウィンドウが表示されます。

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、［OK］ボタンを押します。

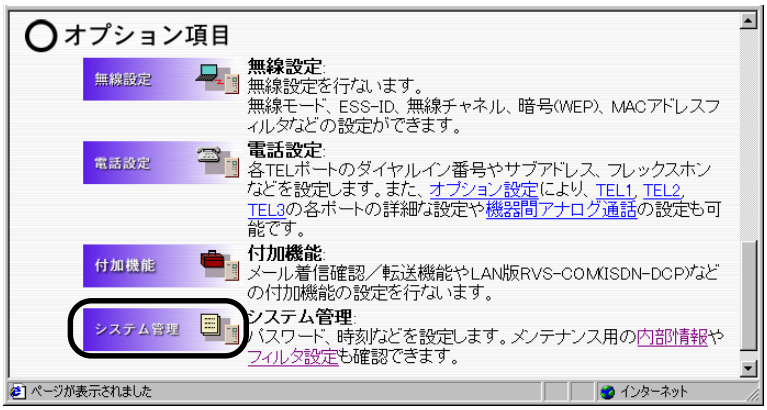


「RT60w へようこそ」ページが表示されます。

3 ［かんたん設定］を押します。

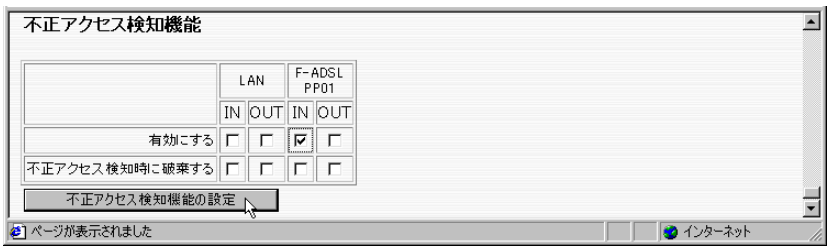


4 [システム管理] を押します。



5 [フィルタ設定] を押します。

6 [不正アクセス検知機能] の各インタフェースの入力/出力方向に対して機能を設定し、[不正アクセス検知機能の設定] ボタンを押します。



IN：	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したときに、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したときに、記録してそのパケットを破棄します。
OUT：	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したときに、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したときに、記録してそのパケットを破棄します。

⚠注意

・本機能は各インタフェース、入出力に適用可能ですが、適用数が多くなりますと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。

MEMO

・不正アクセスの履歴は、ログを参照してください。（→ユーザーズマニュアル「ログ情報の見かた」（218 ページ））