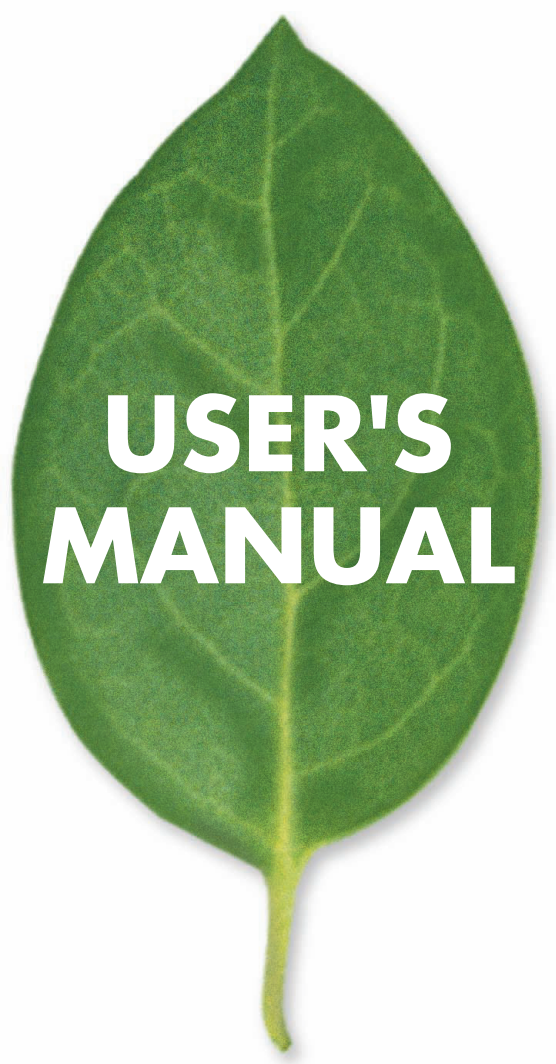


ハイスピード無線ブロードバンドルータ

BLW-04FMG

PLANEX COMMUNICATIONS INC.

USER'S MANUAL

ハイスピード無線ブロードバンドルータ

BLW-04FMG

使用前に必ずお読みください

■本書の目的

本製品をお買い上げいただき誠にありがとうございます。本書は、本製品を正しくお使いいただくための手引きです。必要なときにいつでもご覧いただくために、大切に保管していただきますようお願いいたします。

■ご注意

- 本製品の故障・誤作動・不具合・通信不良、停電・落雷などの外的要因、第3者による妨害行為などの要因によって、通信機会を逃したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねます。
- 通信内容や保持情報の漏洩、改ざん、破壊などによる経済的・精神的損害につきましては、当社は一切その責任を負いかねます。
- 本製品は、一般家庭や小規模事業所におけるブロードバンド環境下での利用を前提にしています。物理的・論理的に規模の大きなネットワークや、一般的ではない環境または目的で本製品を使用した場合、正常に動作しない可能性があります。
- 本製品パッケージ等に記載されている性能値（スループット）は、当社試験環境下での参考測定値であり、お客様環境下での性能を保証するものではありません。また、バージョンアップ等により予告無く性能が上下することがあります。
- ハードウェア、ソフトウェア、外観に関しては、将来予告なく変更されることがあります。
- 本製品内部のソフトウェア（ファームウエア）更新ファイル公開を通じた修正や機能追加は、お客様サービスの一環として随時提供しているものです。内容や提供時期に関しての保証は一切ありません。
- 一般的に、インターネットなどの公衆網の利用に際しては、通信事業者との契約が必要になります。
- 通信事業者によっては公衆網に接続可能な端末台数を制限、あるいは台数に応じた料金を設定している場合があります。通信事業者との契約内容をご確認ください。
- 輸送費、設定、調整、設置工事などは、お客様負担となります。
- 本製品は日本国内仕様であるため、別途定める保証規定は日本国内でのみ有効です。

■著作権等

●マニュアル内の表記について

本マニュアル内では製品の名称を本製品と表記します。区別が必要な場合は製品型番で表記します。
本マニュアルにおける記載内容は、将来予告なく変更されることがあります。

User's Manual Version 1.1 No.PMN-05-10-NW-BLW04FMG

■無線LAN製品ご使用時におけるセキュリティに関するご注意

（お客様の権利（プライバシー保護）に関する重要な事項です！）

無線LANでは、LANケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由にLAN接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

・通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、IDやパスワード又はクレジットカード番号等の個人情報、メールの内容等の通信内容を盗み見られる可能性があります。

・不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、個人情報や機密情報を取り出す（情報漏洩）、特定の人物になりすまして通信し、不正な情報を流す（なりすまし）、傍受した通信内容を書き換えて発信する（改ざん）、コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）等の行為をされてしまう可能性があります。

本来、無線LANカードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線LAN製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

無線LAN機器は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。
従って、お客様がセキュリティ問題発生の可能性を少なくするためには、無線LANカードや無線LANアクセスポイントをご使用になる前に、必ず無線LAN機器のセキュリティに関する全ての設定をマニュアルにしたがって行ってください。
なお、無線LANの仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解の上、ご使用下さい。
セキュリティの設定などについて、お客様ご自分で対処できない場合には、弊社サポートセンターまでお問い合わせ下さい。

セキュリティ対策を施さず、あるいは、無線LANの仕様上やむを得ない事情によりセキュリティの問題が発生してしまった場合、弊社ではこれによって生じた損害に対する責任を負いかねます。
弊社では、お客様がセキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

目次

第5章 詳細設定

第6章 無線設定

付録A ネットワークQ&A

付録B 仕様

ユーザー登録について

弊社へのお問い合わせ

質問表

はじめに

1 概要

本製品は、ADSL FTTHおよびCATV（ケーブルTV）接続を使ったインターネット接続に対応した高性能ブロードバンドルータです。
ブロードバンド環境向けの便利な機能を満載していますのであらゆるニーズに対応しています。

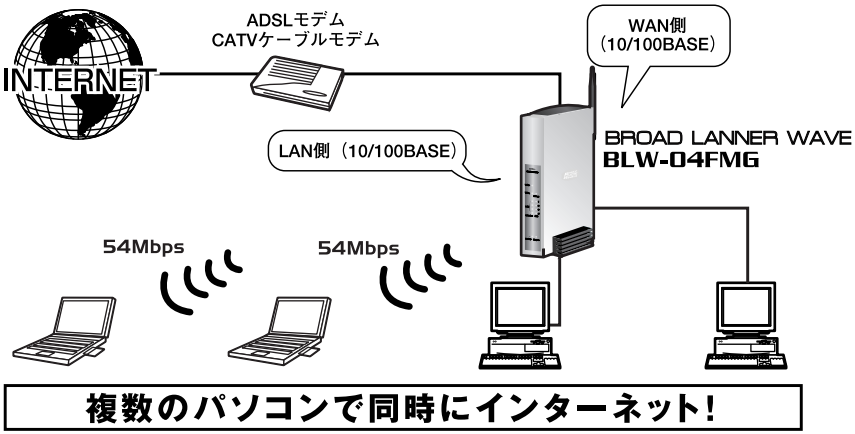


図1-1　BROAD LANNER WAVE接続図

注意

プロバイダによっては本製品のようなルータの使用や複数のコンピュータからのアクセスを制限している場合もあります。プロバイダとの契約内容についてご確認ください。

2 特長

●MIPS 32bitプロセッサによる超高速ルーティング
●WAN側に100BASE-TX/10BASE-T自動認識対応RJ-45 STPポート×1装備
●LAN側に100BASE-TX/10BASE-T自動認識、Auto MDI/MDIXに対応した4ポートスイッチングハブを内蔵しているので、ケーブルの結線方向（ストレート・クロス）がどちらでもご利用できます。

●NAPT機能［P.77〜］
1つのIPアドレスを複数PCで同時ブロードバンド利用が可能。

●DHCPクライアント機能［P.53〜］
IPアドレスの自動割り当て(DHCP)に対応しているプロバイダに対応しています。（各種CATVやYahoo!BBなど）ブロードバンド接続に必要なIP設定が自動的に行われますので設定も最小限で済みます。

●PPPoEクライアント機能［P.41〜］
PPPoEというプロトコルを採用しているプロバイダにも対応しています。（フレッツ・ADSLやBフレッツなど）これまで接続ツールで個別にネット接続していた事を本製品がまとめて担当するので接続しているPCは接続管理を気にすることなく複数台同時にネット利用ができます。

●PPPoEマルチセッション機能［P.45〜］
異なる2つのPPPoE接続相手先への同時接続が可能なPPPoEマルチセッションに対応しています。

●複数グローバルIPアドレス対応（DMZネットワーク）［P.62〜］
複数のグローバルIPアドレスが提供されるブロードバンドサービスについてDMZネットワーク/NAT&スルー機能を使うと、本製品のLAN側にグローバルIPアドレスホストとプライベートアドレスホストを共存させることができます。

●複数グローバルIPアドレス対応（NAPT）［P.77〜］
NAPT機能を使うと、1個以上のグローバルIPアドレスを、LAN側のプライベートIPアドレスホストに1対1で関連付けることもできます。

●サーバ公開、ネットワークゲーム対応（NAPT・静的マスカレード）［P.79〜］
インターネットサーバの公開やNAT経由では使えない多くのアプリケーション/サービス（ゲームなど）を利用することができます。

●不正通信や攻撃からの防御（SPI/攻撃検知）［P.92〜］
これらの機能を有効にすることで、本製品を経由する通信状況をリアルタイムで把握しつつ不正なパケットや攻撃を遮断することができます。

●不要な通信を完全遮断（静的フィルタ）［P.87〜］
フィルタリングルールを個別設定することでインターネット側からの不正な通信、LAN側からの不要な通信を遮断することができます。

●通信状態の把握（ログ機能）[P.96～]

本製品の状態は、syslogサーバへのログ出力、ログメール送信、WWWブラウザ設定画面でのログ表示、の3種類の方法で把握することができます。

●Windows / MSN Messenger 対応（UPnP機能）

Universal Plug and Play Internet Gateway Device v1.0に準拠し、Windows MSN MessengerなどのUPnP対応アプリケーションを簡単に利用することができます。

●ダイナミックDNSサービス対応 [P.98～]

本製品は3つのダイナミックDNSサービス（MyDNS.JP、Dynamic DO!.JP、DynDNS）に対応し、IPアドレス更新を自動的におこなうことができます。

●ローカルルータとしても利用可能（NAPT無効/スタティックルーティング機能）[P.77～、P.86～]

NAPT機能を無効にすることで、異なるIPネットワーク間のルーティングも可能です。

●DHCPサーバ機能 [P.70～]

本製品に接続するパソコンに対するIP設定（IPアドレス割り当てなど）を自動化し、面倒な作業をすることなくネットワークとの通信をおこなうことができます。

●LAN側端末同士の通信を遮断（ポートベースVLAN機能）[P.95～]

ＬＡＮ同士の通信をポートごとに切り分けることができるので、LAN内の他ユーザからのデータ覗き見によるプライバシー侵害・情報漏洩や、LAN内で拡散していくウィルス/ワーム、LAN側のパソコン等を踏み台にしたさらなる攻撃などを未然に防ぐことができます。

●機能追加/修正（ファームウェア更新/新ファームウェアお知らせ機能）[P.100～]

弊社ホームページにて公開されるファイルに更新することで、本製品の機能を決定付ける内部ソフトウェア（ファームウェア）を更新することができます。また更新情報を本製品が自動的に確認しメールでの通知がおこなえます。

●初心者にもわかりやすいかんたん設定（WWWブラウザ設定）

本製品の設定はすべてWWWブラウザを使ったホームページ形式の設定画面上でおこなえます。

●設定内容のセーブとロード [P.101～]

本製品に設定した内容をファイルとして保存することができます。保存したデータは再度本製品に書き込むことができますので、バックアップに便利です。

●無線機能

本製品はIEEE802.11g/IEEE802.11bに対応しており、最大54Mbpsの高速な無線通信をおこなうことができます。

3 梱包内容の確認

パッケージに以下の付属品が含まれていることを確かめてください。

- ●BLW-04FMG本体
- ●専用ACアダプタ
- ●縦置き用スタンド
- ●ツイストペアケーブル（ストレートタイプ：1m）1本
- ●ショートコード1本
- ●ユーザーズマニュアル CD-ROM
- ●スタートガイド
- ●保証書/安全に関する説明書

付属品が足りないときは､販売店または弊社テクニカルサポートまでご連絡ください。

4 各部の名称

■本体前面

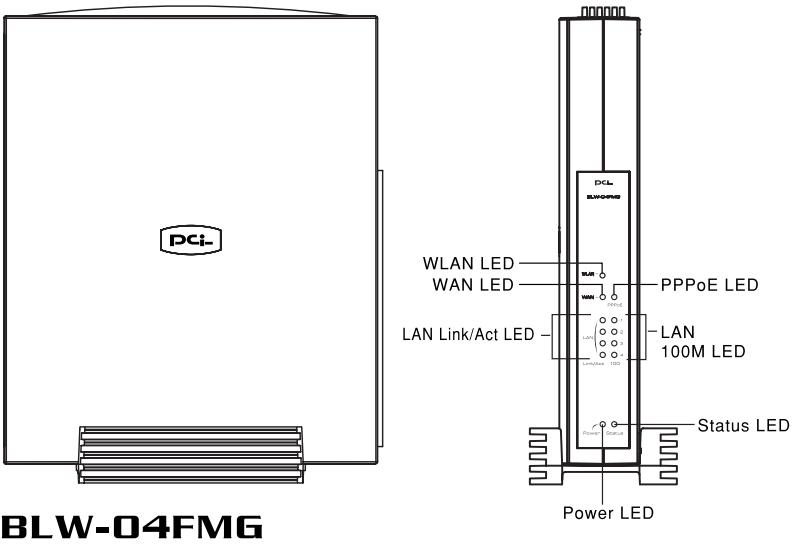


図1-2 BLW-04FMG本体前面

「Power LED」
本製品に電源が供給されているときに点灯します。

「Status LED」
本製品の起動時とエラー発生時に点灯します。

「LAN Link/Act LED」
LAN側ポートのリンクが確立しているときに点灯します。また、ポートがデータの送受信中には点滅します。

「LAN 100M LED」
ポートのリンクが、100Mで確立しているときに点灯します。

「WAN LED」
WAN側ポートのリンクが確立しているときに点灯します。また、ポートがデータの送受信中には点滅します。

「PPPoE LED」
WAN側ポートでPPPoE接続が確立しているときに点灯します。

「WLAN LED」
本製品の無線機能が有効時に点灯します。データ送受信時は点滅します。

■本体背面

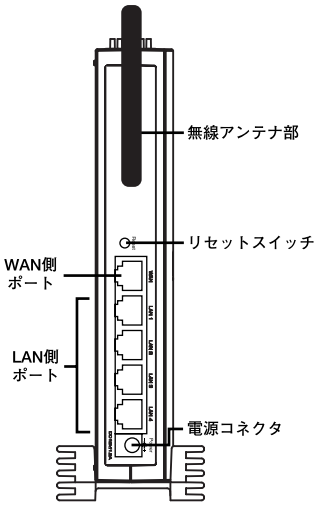


図1-3 BLW-04FMG本体背面

「WAN側ポート」
本製品をADSLまたはケーブルモデムと接続するためのRJ-45 STPポートです。

「LAN側ポート」
本製品にコンピュータを直接接続するためのRJ-45 STPポートです。

「リセットスイッチ」
本製品を再起動するときや、本製品の設定を工場出荷時の状態に戻すときに使います。

「電源コネクタ」
付属のACアダプタを接続するための電源コネクタです。

「無線アンテナ部」
自由な角度にできるので、無線の感度が悪い時は調整することができます。

■本体裏面

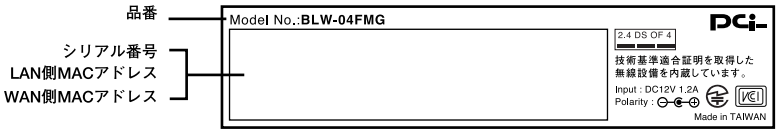


図1-4 BLW-04FMG本体裏面

「品番」
本製品の製品型番です。

「シリアル番号」
本製品のシリアルナンバーです。製品外箱に記載されているものと同じ番号です。ユーザ登録時に必要となります。また、製品故障時などにサポートを受けるときにも必要になります。

「LAN側MACアドレス」
本製品のLAN側ポートのMACアドレス（物理アドレス）です。

「WAN側MACアドレス」
本製品のWAN側ポートのMACアドレス（物理アドレス）です。プロバイダによってはADSL/ケーブルモデムに接続する機器のMACアドレスの申請が必要なことがあります。そのときはこのWAN側ポートのMACアドレスをプロバイダに申請してください。

5 対応機器

■コンピュータ機器

本製品は、以下のいずれかのコンピュータに対応しています。

●Windows 95/98/Me、NT3.51/NT4.0、Windows 2000、Windows XPを搭載し、Ethernet（RJ-45）ポートを装備したコンピュータ

●TCP/IPが利用できるOS（Mac OS、各種UNIXなど）を搭載し、Ethernet（RJ-45）ポートを装備したコンピュータ

■ネットワーク機器

本製品では、以下のネットワーク機器が必要となります。

●ツイストペアケーブル（本製品に接続するコンピュータの台数分）

■ADSL/ケーブルモデム

本製品は、以下のADSL/ケーブルモデムに対応しています。

●RJ-45（LAN）ポートを装備した外付ADSLモデム

●RJ-45（LAN）ポートを装備した外付ケーブルモデム

■WEB設定について

本製品の設定に使用するWWWブラウザは、Java Scriptやスタイルシートに対応している必要があります。また、Netscape Navigator、Mozilla、Operaで設定画面を表示させた場合、表示が多少乱れることがあります。セキュリティホールの問題もありますので、できる限り最新版のブラウザをお使いください。Internet Explorer バージョン6.0以上を推奨します。

6 設定の初期化

IPアドレスやパスワードを忘れてしまったときや、間違った設定をしてしまい設定画面にアクセスできなくなったときなどに設定の初期化が必要になることがあります。

注意

設定の初期化を行うと、LAN側/WAN側ポートの設定や、フィルタ設定等すべての設定が初期化されます。初期化を実行する前に、本当に初期化を行っても問題がないかを確認してください。また予期せぬエラーを避けるために本製品に接続しているケーブルを予めポートから外しておくことを推奨します。

本製品の設定の初期化は、以下の手順で行ってください。

1. 本製品の電源がONの状態で、インターネット接続を切断していることを確認します。
（WEB設定画面「アカウント管理」項目の状態で切断されていればOKです。切断方法については、4章「インターネット接続設定」をご参照ください。）

2. 本製品背面のリセットスイッチを先のとがったペンなどで押します。

3. 20秒間セットスイッチを押したままにしてください。
（この間にStatusランプが点灯し初期化がおこなわれます）

4. Statusランプが点灯したらリセットスイッチを離します。初期化が行われます。
Statusランプが消灯した時点で初期化完了となります。

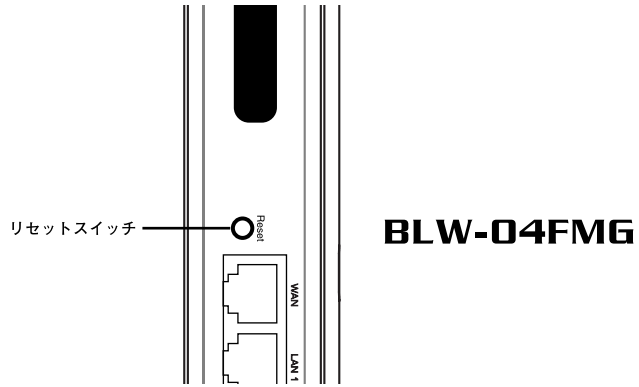


図1-5　リセットスイッチ

ハードウェアの接続

本章では、本製品とADSL/ケーブルモデム等、コンピュータとの接続手順について説明します。

1 設置場所について

本製品を設置する際には必ず以下の点をお守りくださいますようお願いします。

●湿気の多い場所に設置しないでください。
●チリやほこりの多い場所には設置しないでください。
●直射日光のあたる場所や温度の高い場所には設置しないでください。
●内部に熱がこもる原因となりますので、周囲にはなるべく空間を空けてください。

注意

通風口にほこりなどがたまると内部に熱がこもる原因となります。定期的に点検を行い、ほこりがたまっているようでしたら掃除機等でほこりを取り除くようにしてください。

2 設置

本製品は、デスクトップ上などの平らな場所に設置して使ってください。

■縦置きする場合

本体を付属の縦置き用スタンドに図のようにセットしてください。

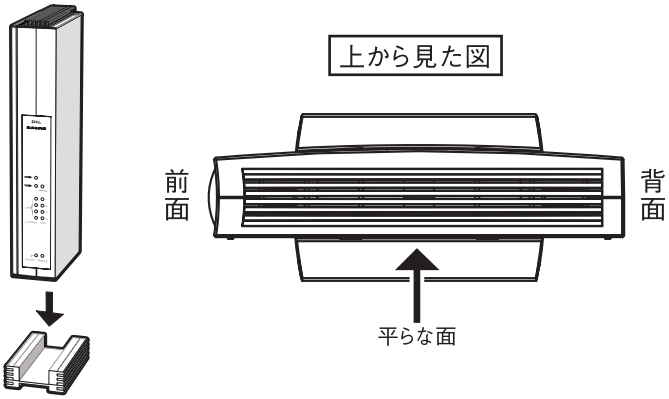


図2-1　本体縦置き

■横置きする場合

図のように本体の平らな面が下になるように設置して下さい。

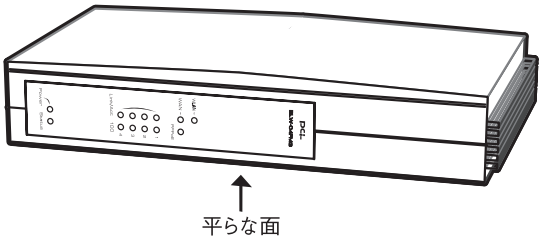


図2-2　本体横置き

3 WAN側ポートにADSL/ケーブルモデムを接続する

1. ADSL/ケーブルモデムの電源を切ってください。
電源スイッチがないタイプはコンセントからACアダプタを引き抜いてください。

2. 本製品付属のツイストペアケーブルで、本製品背面のWAN側ポートとADSL/ケーブルモデムのRJ-45ポートを接続します。
＊RJ-45ポート　モデムによっては「LAN」「Ethernet」などと表記されていることもあります。

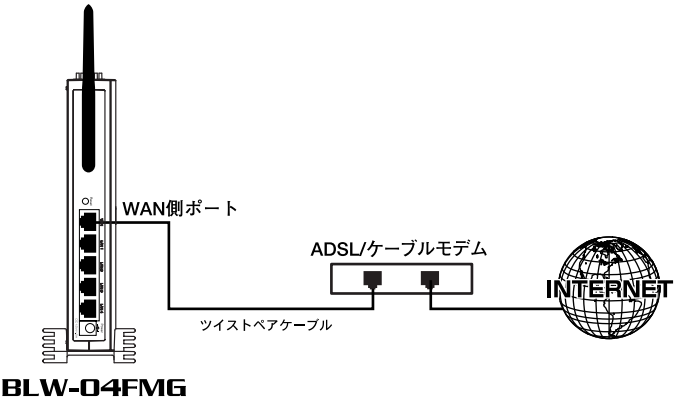


図2-3　ADSL/ケーブルモデムとの接続

注意

本製品のWAN側ポートはMDIポートになっています。また、本製品付属のツイストペアケーブルはストレートタイプです。ご利用になっているADSL/ケーブルモデムのポートがMDIポートのときはクロスオーバタイプのツイストペアケーブルを使用してください。

4 LAN側ポートへのコンピュータの接続

1. ツイストペアケーブルの一端を本製品のLAN 側ポートに接続します。本製品のLAN 側ポートは結線のタイプを自動認識するAuto MDI/MDI - X に対応しています。コンピュータを接続するツイストペアケーブルはストレートタイプ、クロスオーバタイプのどちらでも使用できます。

2. ツイストペアケーブルのもう一端をコンピュータのRJ-45 ポートに接続します。
このとき、ケーブルのコネクタがポートの奥までしっかりささっているか確認してください。

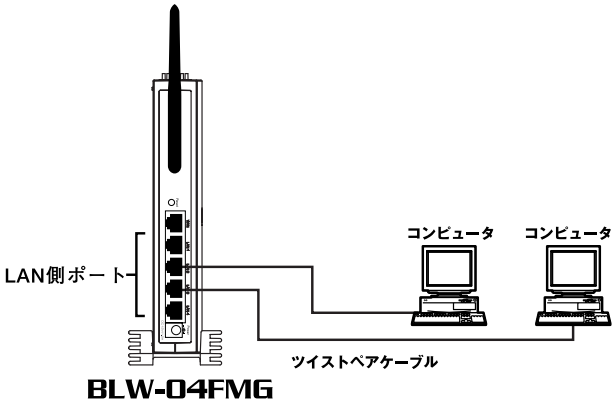


図2-4　コンピュータとの接続

5 電源の接続

1. ADSL/ケーブルモデムの電源を入れます。
2. 付属のACアダプタを本製品の電源コネクタに接続します。
3. ACアダプタをAC100Vコンセントに接続します。スペースの問題でACアダプタをコンセントに直接接続できないときは付属のショートコードをお使いください。
4. コンピュータの電源を入れてください。
5. 次項の接続の確認に進んでください。

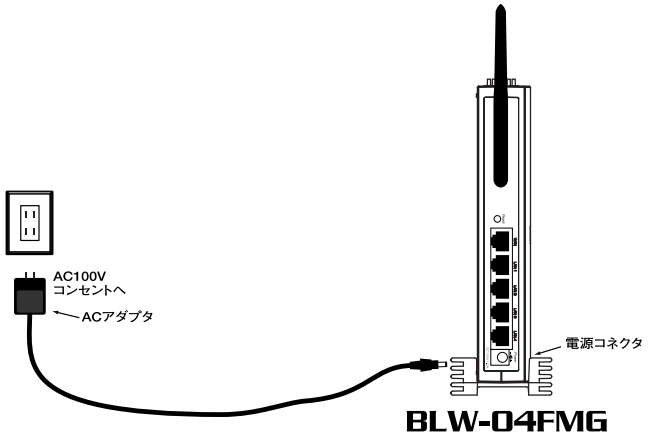


図2-5　電源の接続

注意

ACアダプタは必ず付属のものを使用してください。付属以外のACアダプタの使用は、製品の故障、誤動作等の原因となります。付属以外のACアダプタを使用した場合の故障は保証の範囲外となります。

6 接続の確認

これまでの接続を行い本製品の電源を入れると本製品のPOWER、WAN、LAN Link/Actの各LED が点灯します。これらのLEDが点灯しないときは以下の点についてお確かめください。

◎POWER LED

・本製品付属のACアダプタを使っていますか？
・ACアダプタが本製品背面の電源コネクタにしっかりと接続されていますか？
・ACアダプタはAC100Vコンセントにしっかりと接続されていますか？

◎WAN LED

・ツイストペアケーブルの両端はそれぞれ、本製品背面のWAN側ポートおよびADSL/ケーブルモデムのRJ-45ポートにしっかりと接続されていますか？
・ADSL/ケーブルモデムの電源は入っていますか？
・使用しているツイストペアケーブルのタイプは間違っていませんか？

◎LAN Link/Act LED

・ツイストペアケーブルの両端はそれぞれ、本製品背面のLAN側ポートおよびコンピュータのRJ-45ポートにしっかりと接続されていますか？
・コンピュータの電源は入っていますか？

◎WLAN LED

・しばらく様子を見てください。それでも点灯しない場合は弊社テクニカルサポートまでご連絡ください。

コンピュータの設定

本章では本製品を使ったインターネットへのアクセスとWEBブラウザから設定するために必要なコンピュータの設定手順について説明します。コンピュータの設定を開始する前に、第2章「ハードウェアの接続」を参照して本製品とADSL/ケーブルモデム、コンピュータの接続を完了させておいてください。

ご利用のOSに応じて次のページをご覧ください。

○ WindowsXP Professional （32bit ）及びHomeEdition の場合
⇒3-1. ネットワーク設定（windowsXP）へ

○ Windows 2000 の場合
⇒3-3. ネットワーク設定（Windows 2000）へ

○ Windows 98（SecondEdition 含む）/Meの場合
⇒3-5. ネットワーク設定（Windows 98/Me）へ

○ Macintosh（Mac OS9）の場合
⇒3-7. ネットワーク設定（Mac OS9）へ

○ Macintosh（Mac OS X）の場合
⇒3-8. ネットワーク設定（Mac OS X）へ

メモ

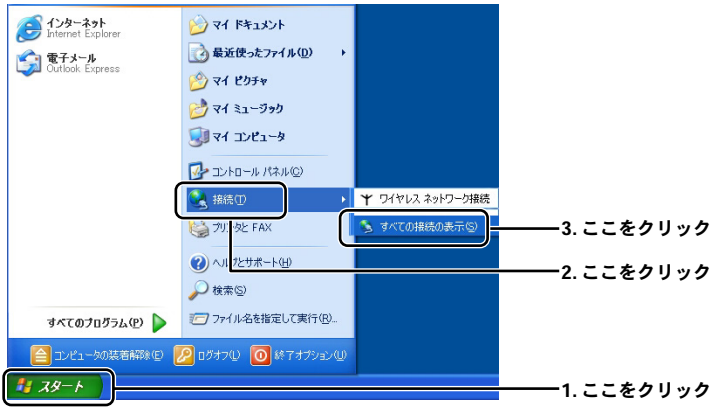
作業を始める前にコンピュータにLANアダプタが装着され、正常に認識されていることを確かめてください。LANアダプタが装着されていないときは、LANアダプタの追加導入を行ってください。

弊社ではPCIバス接続型のLANアダプタ「FW-110TX」をはじめ、ノートパソコンなどに便利なPCカードタイプの「FNW-3700-TX」などいろいろな形態のLANアダプタを取り扱っています。是非ご参考ください。

1 ネットワーク設定（Windows XP）

1.「スタート」ボタンから「接続」内の「すべての接続の表示」を選択します。

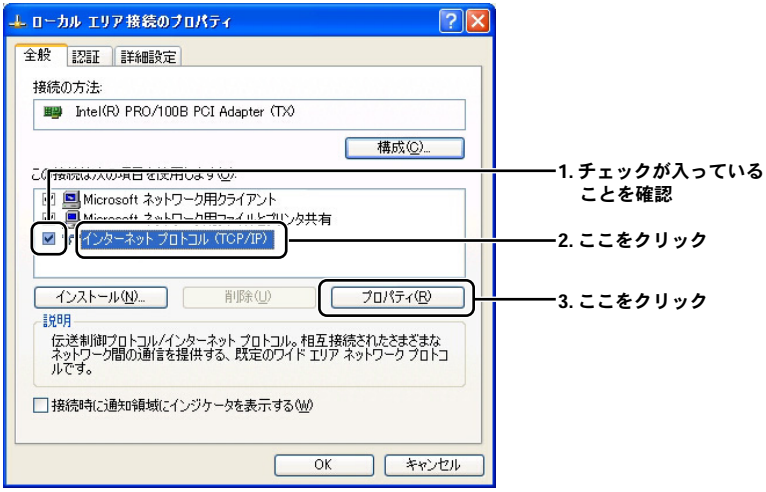
＊Windows クラシックスタイルの場合は「スタート」から「設定」内の「ネットワーク接続」を選択します。



2.「ローカルエリア接続のプロパティ」ウィンドウを開きます。

＊「ローカルエリア接続」アイコンが複数ある場合は本製品と接続している機器のアイコンを選択してください。

3.「インターネットプロトコル（TCP/IP）」を選択して設定画面を開きます。



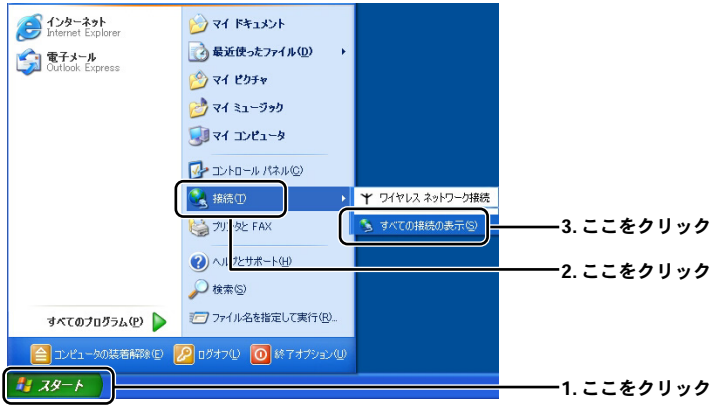
4.「全般」にある各項目を以下のように設定確認します。

5. 設定を終了します。
「ローカルエリア接続のプロパティ」ウィンドウの「OK」をクリックします。
ネットワークの設定は終了です。

2 IPアドレスの確認方法（Windows XP）

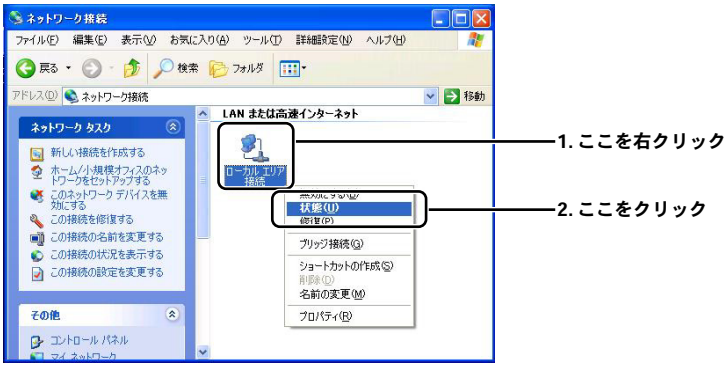
1.「スタート」から「接続」内の「すべての接続の表示」を選択します。

＊Windows クラシックスタイルの場合は「スタート」から「設定」内の「ネットワーク接続」を選択します。



2.「ローカルエリア接続のプロパティ」ウィンドウを開きます。

＊「ローカルエリア接続」アイコンが複数ある場合は本製品と接続している機器のアイコンを選択してください。



3.「ローカルエリア接続の状態」が開きます。
「ローカルエリア接続の状態」の「サポート」タブを選択します。

4.IPアドレスなどアドレス情報を確認します。

「192.168.1.xxx」になっていることを確認します

＊工場出荷時設定の場合

接続先になる本製品の「LAN設定」にあわせた表示になっていることを確認します。

5.「閉じる」をクリックしてIPアドレスの確認を終了します。

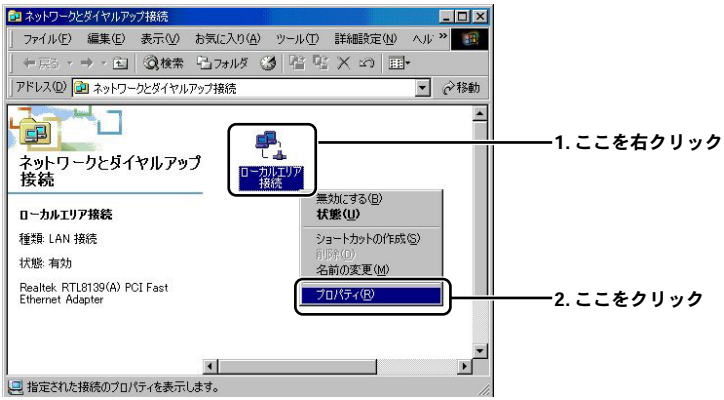
> **メモ**
>
> ***IPアドレスが0.0.0.0や169.254.***.***という様な表示になっている場合には、一旦コンピュータを再起動してみてください。***

3 ネットワーク設定（Windows 2000）

1. 「スタート」から「設定」内の「ネットワークとダイヤルアップ接続」を選びます。

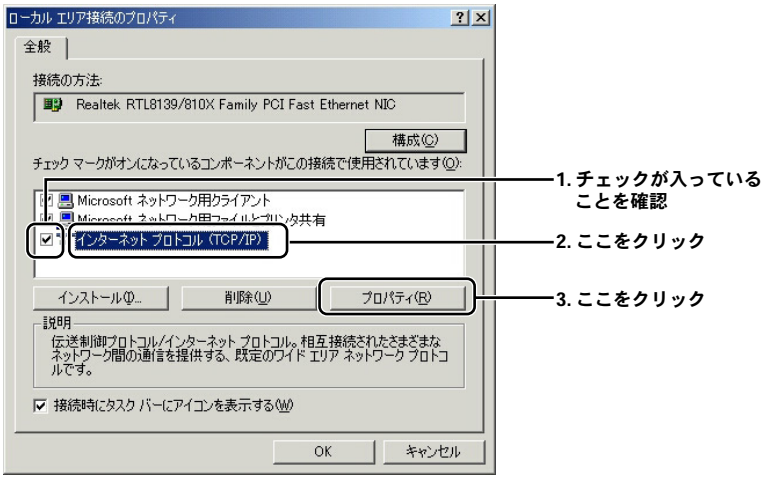
2. 「ローカルエリア接続」アイコンを右クリックし、表示されるメニューから「プロパティ」を選びます。

＊「ローカルエリア接続」アイコンが複数ある場合は本製品と接続している機器のアイコンを選択してください。

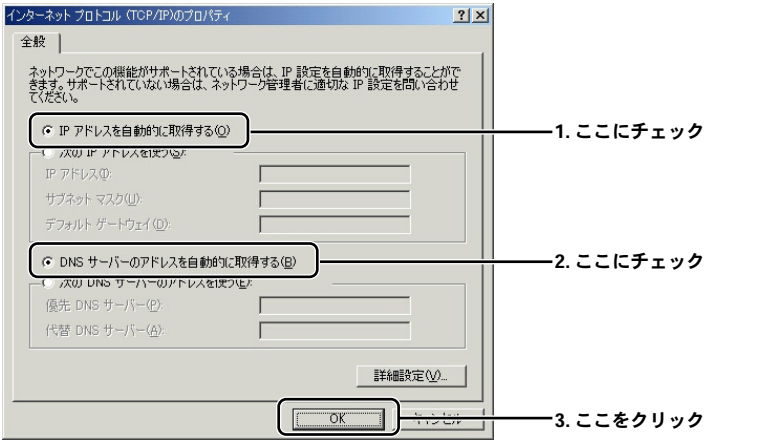


3.「ローカルエリア接続のプロパティ」に「インターネットプロトコル（TCP/IP）」が表示されているか確認して「プロパティ」を開きます。

＊もしもない場合は、「F1」キーを押してwindows標準ヘルプのキーワードから「TCP/IPをインストールする」を検索して御参照ください。



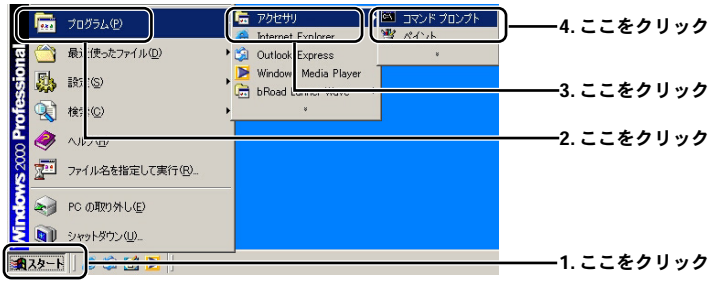
4.「全般」内の各項目の設定を確認します。



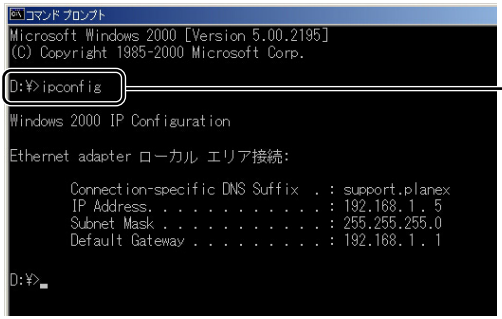
5.「ローカルエリア接続のプロパティ」の画面に戻るのでこれを閉じてください。ネットワークの設定を終了します。

4 IPアドレスの確認方法（Windows 2000）

1.「スタート」から「プログラム」内の「アクセサリ」より「コマンドプロンプト」を選びます。



2.「コマンドプロンプト」画面内で「ipconfig 」（半角英数字）と入力して「Enter キー」を押します。表示されたアドレス情報を確認します。



接続先になる本製品の「LAN設定」にあわせた表示になっていることを確認

例：「192.168.1.xxx」（「ｘｘｘ」は任意の数字になります。）

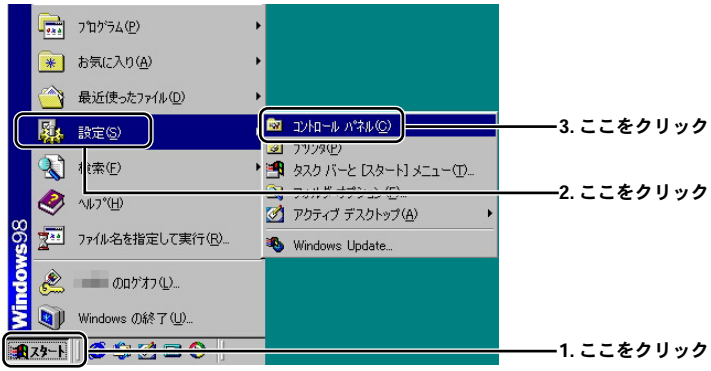
＊工場出荷時設定の場合

メモ

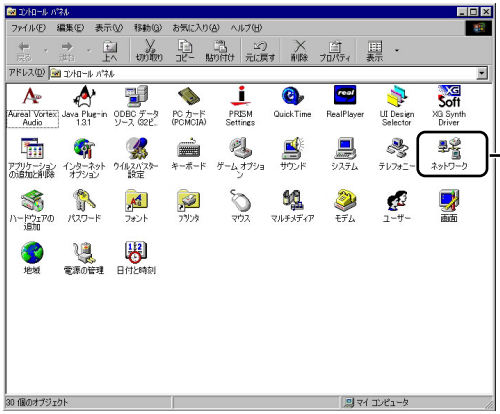
IPアドレスが0.0.0.0や169.254..***という様な表示になっている場合には、「コマンドプロンプト」画面内で「ipconfig /release」（半角英数字）と入力して「Enter」キーを押します。その状態でコンピュータの再起動をしてください。***

5 ネットワーク設定（Windows 98/Me）

1.「スタート」から「設定」内の「コントロールパネル」を選びます。

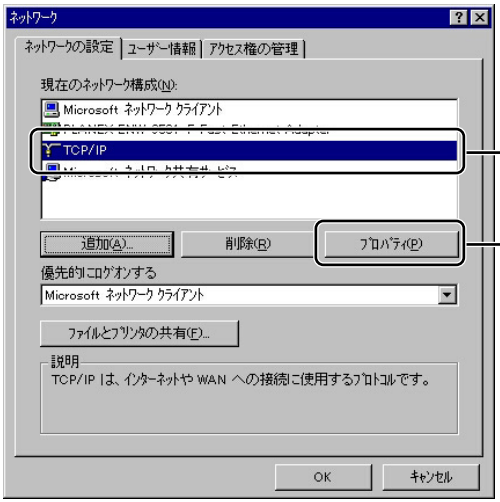


2.「コントロールパネル」一覧から「ネットワーク」を開きます。

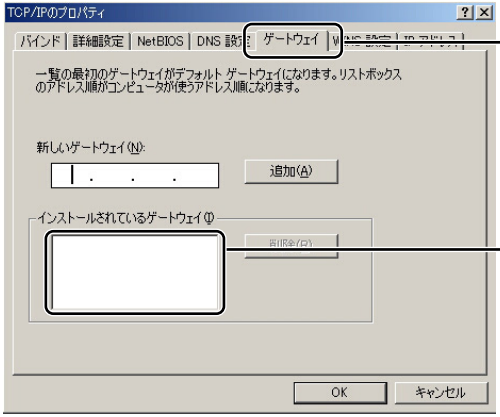


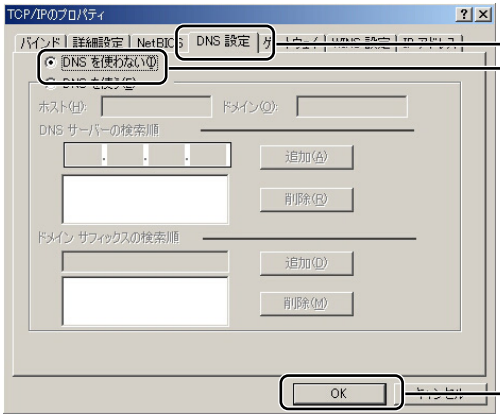
3.「現在のネットワーク構成」の欄に「TCP/IP」が表示されているか確かめてください。

＊もし、ない場合は「F1」キーを押してwindowsヘルプのキーワードから「ネットワークプロトコルをインストールする」を検索して御参照ください。



4.「TCP/IP のプロパティ」内の各項目の確認をおこないます。





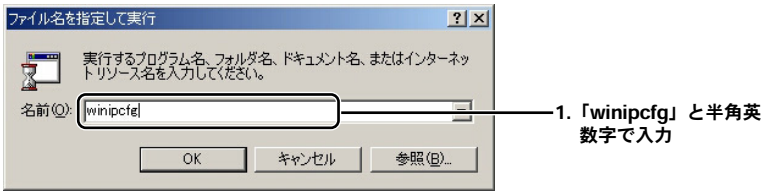
5. 設定を完了させてコンピュータを再起動します。

＊自動的に再起動がかからない場合には手動で再起動をかけます。

6 IPアドレスの確認方法（Windows 98/Me）

1.「スタート」から「ファイル名を指定して実行」を選びます。

2.「名前」欄に「winipcfg 」（半角英数字）と入力します。



3.「IP 設定」内でIP アドレスを確認します。

接続先になる本製品の「LAN設定」にあわせた表示になっていることを確認します。

例：「192.168.1.xxx」（「ｘｘｘ」は任意の数字になります。）

＊工場出荷時設定の場合

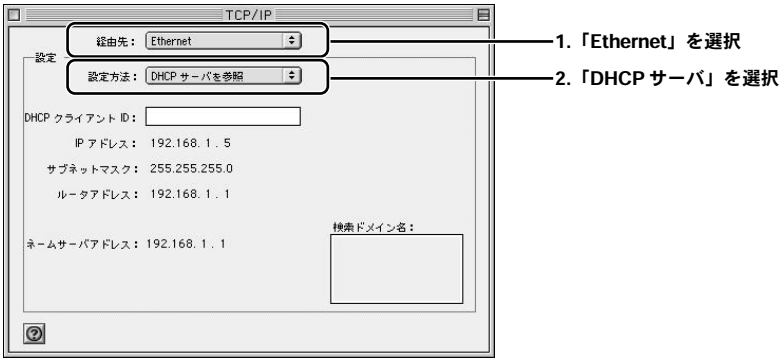
メモ

IPアドレスが0.0.0.0や169.254..***という様な表示になっている場合には、「IP 設定」画面内で「すべて解放」ボタンを押してから「OK」ボタンを押します。その状態でコンピュータを再起動してください。***

7 ネットワーク設定（Mac OS9）

1. アップルメニューから「コントロールパネル」→「TCP/IP」を順に選択します。

2. TCP/IPの設定ウィンドウが表示されますので、プルダウンメニューから以下を選択します。



3. TCP/IPの設定ウィンドウを閉じて、Macintoshを再起動します。

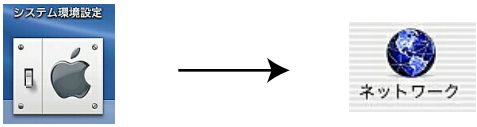
4. 起動が完了したら再度「TCP/IPの設定ウィンドウ」を表示してIPアドレス「192.168.1.XXX」になっていることを確認します。
（XXXは任意の数字になります）
ウインドウを閉じてネットワークの設定を終了します。

8 ネットワーク設定（Mac OSX）

1. Dockにある［システム環境設定］を開きます。

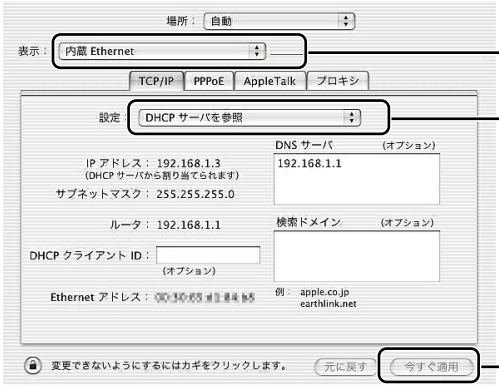
＊もし、Dockに該当のアイコンがない場合は、「アップルメニュー」→「システム環境設定」を選択してください。

2.「システム環境設定」の「ネットワーク」アイコンをクリックしてネットワーク設定項目を開きます。



ダブルクリック　　ダブルクリック

3.「ネットワーク設定」項目を以下の通り設定します。



1.「内蔵 Ethernet」を選択

2.「DHCP サーバ」を選択

3. ここをクリック

4. 再度、「TCP/IPの設定ウィンドウ」を表示してIPアドレス「192.168.1.X」になっていることを確認します。（Xは1以外の任意の数字です）
ウインドウを閉じてネットワークの設定を終了します。

注意

本製品をご使用になる以前に、MacPCから直接PPPoE接続を行っていた場合、MacのPPPoE設定を無効にする必要があります。「システム環境設定」→「内蔵 Ethernet」→「PPPoE」項目を表示して「PPPoEを使って接続する」に入っているチェックを外してください。

インターネット接続設定

本章では本製品のインターネットへの接続手順について説明します。ここでは、必要最小限の設定だけで、本製品を経由したインターネットへのアクセスを行えるようになります。インターネット接続設定を開始する前に、第2章「ハードウェアの接続」および第3章「コンピュータの設定」を済ませておいてください。本製品をより詳細に設定したいときは、第5章「詳細設定」を参照してください。

1 インターネット接続方法の確認

本製品は通常接続（固定IPアドレス）、通常接続（DHCPクライアント）、PPPoE接続の3つの接続方式をサポートしています。
本製品のインターネット接続の設定は、お客様が契約しているプロバイダとのサービス内容によって異なります。次の中からお客様のプロバイダとの契約内容にあった接続方法を選択して、本製品の設定を行ってください。また、契約プロバイダより案内されている接続設定情報を予め確認しておいてください。

■PPPoE接続
NTT東日本株式会社/NTT西日本株式会社の「フレッツ・ADSL」および「Bフレッツ」などで採用されているPPPoEプロトコルを使う接続方法です。接続にはユーザ名（アカウント名）とパスワードが必要です。
→次項「4-2 PPPoE接続の設定」に進んでください。

■DHCP接続
多くのケーブルテレビインターネット接続サービスや、ヤフー株式会社の「Yahoo! BB」などのサービスで採用されている、DHCP プロトコルを使ってIPアドレスが自動に割り当てられる方法です。
→次項「4-4 通常接続の設定」に進んでください。

■固定IPアドレス接続

IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバアドレスなどのアドレス情報があらかじめプロバイダから割り当てられるサービスでの接続方法です。

→次項「4-4 通常接続の設定」に進んでください。

注意

・本製品を@NetHomeまたは、ZAQでご使用になるときは、@NetHomeまたは、ZAQへのルータ使用の登録が必要です。(2003年10月現在)

・それぞれの接続方式は排他選択であり、2つの接続方式を同時利用することはできません。ご利用のブロードバンドサービスに適した接続方式を選択してください。

2 PPPoE接続の設定

注意

・ブラウザでプロキシを使用する設定がされていると設定画面が表示されません。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」→「LANの設定」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。プロキシを使用しないように設定するか、もしくはプロキシの詳細設定画面で「次で始まるドメイン（アドレス）にはプロキシを使用しない」の欄に本製品のLAN側ポートのIPアドレスを入力してください。

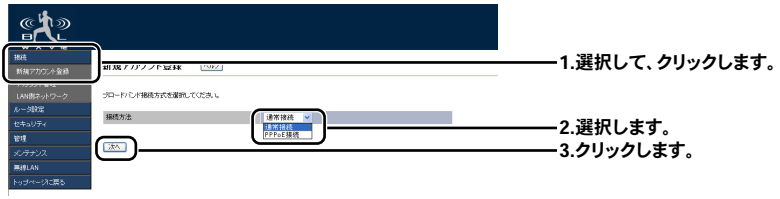
・PPPoE接続の場合、本製品が接続処理を行うのでプロバイダから配布されるPPPoE接続ソフトウェアは必要ありません。インストールしてある場合は、アンインストールするか、そのソフトの自動接続機能を無効にしてください。

1. コンピュータが起動したら、WEBブラウザを起動します。

2. WEBブラウザのURLを入力する欄（Netscape では「場所」、Internet Explorerでは「アドレス」）に本製品のIPアドレス（デフォルト値は「192.168.1.1」）を入力し、Enterキーを押します。

3. 設定画面にログインするためのログイン画面が表示されます。
工場出荷時のパスワードは「password」です。パスワード欄に「password」と入力して、「OK」ボタンをクリックします。

4. 本製品の設定画面が表示されます。
メニューバーから「接続」→「新規アカウント登録」をクリックします。
接続方式を「PPPoE接続」を選択して、「次へ」をクリックします。



5. 「PPPoE接続設定」画面が表示されます。
以下の項目を入力します。

「アカウント名［任意］」
このPPPoE接続アカウントに、自由に名前を付けることができます。
契約プロバイダ名など、他のアカウントと区別できる（重複しない）わかりやすい名前を入力してください。
ここで設定した名前は「ルータ設定」や「セキュリティ」項目でも利用されます。
⇒**設定範囲**　　半角英数字 1～32文字まで　初期値 なし

「PPPoEユーザ名」
プロバイダから指定されたPPPoE接続ユーザ名を入力します。
フレッツ・ADSLやBフレッツの場合は、@（アットマーク） 以下も正確に入力する必要があります。大文字・小文字は別の文字として扱われることや、数字の0（ゼロ）と英字のO（オー）の違いなどに注意してください。
⇒**設定範囲**　　半角文字 1～64文字まで　初期値 なし

「PPPoEパスワード」
プロバイダから指定されたPPPoE接続パスワードを入力します。
大文字・小文字は別の文字として扱われることや、数字の0（ゼロ）と英字のO（オー）の違いなどに注意してください。ここに入力した値は、セキュリティのため＊（アスタリスク）表示されます。
⇒設定範囲　　半角英数 1〜64文字まで　初期値 なし

「PPPoEパスワード再入力」
入力間違い防止のため、PPPoEパスワードを再度入力してください。
⇒設定範囲　　半角英数 1〜64文字まで、初期値 なし

「PPPoEサービス名」
プロバイダからPPPoE接続サービス名を指定された場合のみ入力します。
通常は指定がない限り入力しないでください。
⇒設定範囲　　半角文字 0〜64文字まで、初期値 なし

「PPP認証方式」
PPPoE接続時の認証方法を決定します。
接続相手にあわせる・CHAP・PAP の3つから選択します。
通常は「接続相手にあわせる」のままで構いません。
⇒初期値　　接続相手にあわせる
・接続相手にあわせる［推奨］
PPPoE接続相手先から提示された認証方式に本製品が従います
・CHAP
CHAP方式でユーザ認証を行います
・PAP
PAP方式でユーザ認証を行います

「WAN側IPアドレス設定方法」
WAN側IPアドレスの設定方法を「自動取得/固定設定」の2つから選択します。
プロバイダから指定がない場合は「自動取得」となります。
⇒初期値　　自動取得
・自動取得
PPPoE接続時に、プロバイダからIPアドレスを自動的に取得する場合
・固定設定
プロバイダから特定のIPアドレスが割り当てられている場合

「固定WAN側IPアドレス」
＜WAN側IPアドレス設定方法＞で「固定設定」を選択した場合に、プロバイダから指定されたIPアドレスを入力してください。
「自動取得」を選択した場合は、入力する必要はありません。
⇒設定範囲　　半角数字 1.0.0.1〜223.255.255.254

「DNSサーバアドレス設定方法」
DNSサーバのIPアドレスをどうやって設定するかを決定します。
自動取得・固定設定 のいずれかを選択します。
⇒初期値　　自動取得
・自動取得　　PPPoE接続時に自動取得する場合
・固定設定　　特定のDNSサーバを利用したい場合

「プライマリ・セカンダリDNSサーバアドレス」
＜DNSサーバアドレス設定方法＞で「固定設定」を選択した場合に、利用するDNSサーバのIPアドレスを入力します。
「自動取得」を選択した場合は、入力する必要はありません。
⇒設定範囲　　半角数字 1.0.0.1〜223.255.255.254

「MSS サイズ」
PPPoE接続におけるMSS値を入力します（MSS ＝ MTU - 40）。利用しているブロードバンドサービスによってはMSS値の上限が制限されていることがありますので注意してください。また、フレッツ・ADSL、Bフレッツの最大MSS値は、1414byteとされています。
⇒設定範囲　　半角数字 536〜1452、初期値 1412

6. 画面最下部にある「設定」ボタンをクリックし再起動後、4章「5.アカウント管理」に進んでください。

DMZネットワークを設定する必要がある場合は、4章「6.DMZネットワーク」を参照してください。

3 PPPoEマルチセッション

■PPPoEマルチセッションとは

本製品は、同時に複数のPPPoE接続相手先との通信が可能なPPPoEマルチセッションに対応しています。これは1つのWANアクセス機器（ブロードバンドルータなど）が、複数のPPPoEアカウントを使ってそれぞれ異なるネットワークに接続できる機能です。本製品は、最大2つのPPPoEセッションに同時接続することができます。（最大PPPoE 2セッションサポート）

NTT東日本、NTT西日本のフレッツ・ADSLやBフレッツがこれに対応しています。その他のPPPoE接続ブロードバンドサービスに関しては、サービス事業者に確認してください。また、一つのアカウントで2つ以上のPPPoEセッションを確立することはできません。一般的な運用形態として、一つをプロバイダから提供されているアカウント、もう一つはフレッツスクウェアから提供されているアカウントを併用することが挙げられます。これにより、通常のインターネット接続を利用しつつ、同時にフレッツスクウェアとの通信も可能となります。

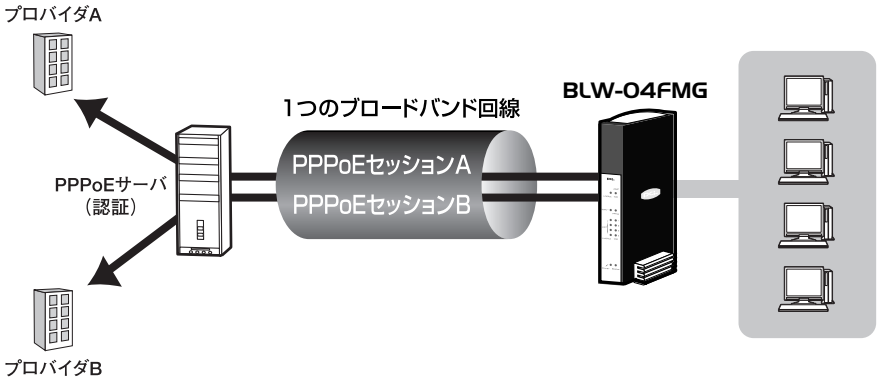


図4-1　PPPoEマルチセッション構成図

■本製品におけるPPPoEマルチセッションの利用方法

1台のブロードバンドルータを利用してPPPoEマルチセッションを行う際、ルーティングの問題が発生します。たとえば1台のブロードバンドルータが、2つのPPPoEアカウントを利用して2つのPPPoEセッションを確立している場合、LAN側からのパケットをどちらのセッションに転送するかというルーティングポリシーは、接続先のネットワークがどんなネットワークなのかを知らないブロードバンドルータが自動で判別できることではなく、ユーザ自身が決めなければなりません。本製品は、ポリシールーティングという考え方を導入し、送信先IPアドレスだけでなく、以下のようにプロトコル、送信元IPアドレス、送信先ポート番号、送信元ポート番号といった、詳細なパラメータをユーザが指定し、柔軟なルーティングポリシーを設定できるようにしています。
→5章「4. ポリシールーティング」

具体的には、本製品に設定された2つのPPPoEアカウントのうち、主に利用したいPPPoEアカウントを「プライマリセッション」、特定用途に使いたいPPPoEアカウントを「セカンダリセッション」とします。そしてユーザ自身が設定したポリシールートに基づき、ポリシールートに一致しないトラフィックは（デフォルトルートとして機能する）プライマリセッションへ、ポリシールートに一致したトラフィックは指定されたインターフェイス（この場合はセカンダリセッション）に転送します。

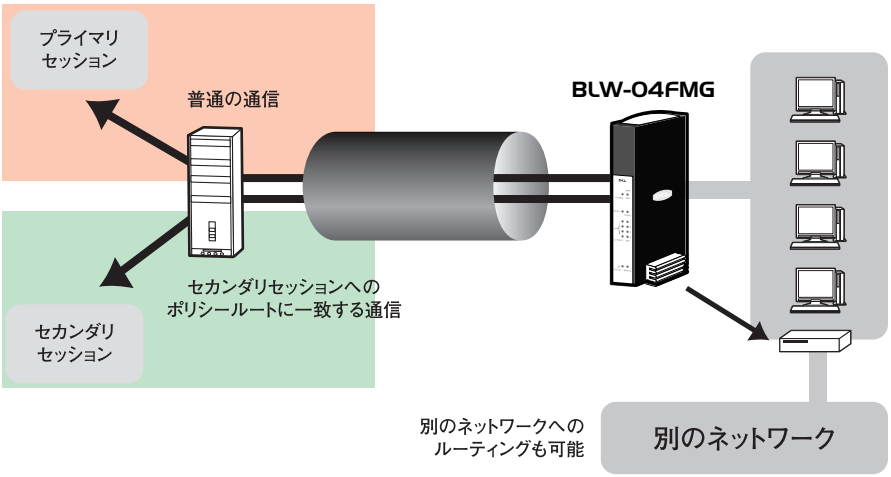


図4-2　ポリシールーティング

■PPPoEマルチセッションとDNS ルーティング

本製品ではポリシールーティングにより柔軟なPPPoEマルチセッション利用を実現していますが、たとえば「このURLとの通信はセカンダリセッションを利用したい」という場合、宛先として設定できるパラメータが送信先IPアドレスだけだと、URLを使ってアクセスしているサーバのIPアドレスを、ユーザが一つ一つ調べて入力しなければならなくなります。万が一それでもいい場合でも、特定ホストに割り当てられているIPアドレスは変更される可能性があり、変更されたら再度入力しなおさなければなりません。また、「planex.co.jp」ドメイン管理下のすべてのサイト（www.planex.co.jp や ftp.planex.co.jpなど）との通信でセカンダリセッションを利用する、といった指定は事実上不可能です。

これに対して本製品は、DNSルーティングという考え方を導入し、ポリシールーティングと同じように、「指定されたDNS問い合わせ（アドレス解決）を、指定されたインターフェイス（セカンダリセッション）の指定されたDNSサーバ（セカンダリセッション上のDNSサーバ）に転送する」という機能を持ちます。
→5章「5. DNSルーティング」

ここで注意すべき点は、ポリシールーティングとDNSルーティングは基本的に別個の機能として働くことです。すなわち、「www.planex.co.jpのDNS問い合わせはセカンダリセッションのDNSサーバに転送する」と設定しただけでは、DNS問い合わせ自身はセカンダリセッション上のDNSサーバで解決しますが、アドレス解決後の「www.planex.co.jp」宛の通信トラフィックはデフォルトルートであるプライマリセッションに転送されてしまいます。
「www.planex.co.jp」宛のDNS問い合わせだけでなく、アドレス解決後の「www.planex.co.jp」宛の通信も、セカンダリセッションを利用したい場合は、DNSルーティングとポリシールーティングの連携を設定しなければなりません。

具体的には、ポリシールーティングの設定において、「宛先」に送信先IPアドレスを入力する代わりに、DNSルーティングのID番号を入力します。この設定を行うことで本製品は、LAN側ホストからの「www.planex.co.jp」のDNS問い合わせ（アドレス解決）をセカンダリセッション上のDNSサーバに転送し、DNSサーバからの回答（www.planex.co.jp のIPアドレス）を問い合わせたLAN側ホストに教えるだけでなく、当該ポリシールートの送信先IPアドレスとして一時的に記憶します。その後、LAN側ホストから「www.planex.co.jp」のIPアドレス宛の通信が来ると、記憶しているIPアドレスと照合し、セカンダリセッションに転送します。
さらに注意点として、DNS問い合わせを転送するという性格上、DNSルーティングを利用するためには、LAN側ホストが本製品のProxy DNS機能を利用する必要があります。すなわち、LAN側ホストのIP設定を本製品のDHCPサーバ機能によって自動構成するか、もしくは本製品のLAN側IPアドレスをLAN側ホストのDNSサーバアドレスとして手動登録しておく必要があります。

■具体的なPPPoEマルチセッションの利用例

プロバイダのPPPoEアカウントを1個しか持っていなくても、フレッツ・ADSLやBフレッツのユーザならば、ブロードバンドコンテンツサイトである**フレッツ・スクウェアのPPPoEアカウント**を無料で利用することができます。
ここでは、フレッツ・スクウェアを例に挙げて、PPPoEマルチセッションの設定例を解説します。

下記は2003年9月現在の情報です。フレッツ・スクウェアの接続方法は、変更される時があります。
フレッツ・スクウェアの接続方法の詳細は、NTT東日本、NTT西日本の情報もあわせて参照ください。

○**NTT東日本：http://flets.com/**
○**NTT西日本：http://www.ntt-west.co.jp/flets/**

1. まず、通常のインターネット通信で利用するプロバイダのPPPoEアカウントを登録します。

2. 次に、フレッツ・スクウェアのPPPoEアカウントを登録します。

●フレッツ・スクウェア（NTT東日本）の場合
アカウント名　　：この接続アカウントに任意の名前を付けます
PPPoEユーザ名　：guest@flets
PPPoEパスワード：guest
その他　　：デフォルト設定のまま

●フレッツ・スクウェア（NTT西日本）の場合
アカウント名　　：この接続アカウントに任意の名前を付けます
PPPoEユーザ名　：flets@flets
PPPoEパスワード：flets
その他　　：デフォルト設定のまま

3. ［アカウント管理］で以下のように設定し、画面最下部にある「設定」ボタンをクリックします。

「接続方式の選択」
「PPPoE接続」を選択します。

「PPPoEアカウントリスト」
「セッション」欄で、通常のインターネット通信で利用するプロバイダのPPPoEアカウントを「プライマリ」
フレッツ・スクウェアのアカウントを「セカンダリ」に設定します。

4. 再起動後、「ルータ設定」→「ＤＮＳルーティング」をクリックして「ＤＮＳルーティング」設定画面を表示させます。
「ＤＮＳルートの追加」をクリックして、以下の通りDNSルートを登録します。

ＤＮＳルートID	32
送信元アドレス	＊（すべて）
クエリタイプ	すべて　または　a
DNSクエリ	.flets
インターフェース	（セカンダリセッションのアカウント名を選択します）
DNSサーバアドレス	空欄

5. 続いて、「ルータ設定」→［ポリシールーティング］をクリックして「ポリシールーティング」設定画面の設定を表示させます。
「ポリシールーティング」をクリックして、以下の通りポリシールートを登録します。

ポリシールートID	32
プロトコル	＊（すべて）
宛先	DNSルートID
宛先IPアドレス	32　（DNSルーティングで設定したルートを指定します）
またはDNSルートID	
送信先ポート	空欄
送信元IPアドレス	＊（すべて）
送信元ポート	空欄
ゲートウェイ	空欄
インターフェース	（セカンダリセッションのアカウント名を選択します）

6. ［LAN側ネットワーク］で、Proxy DNSが「有効」であることを確認してください。
LAN側ホストが本製品のDHCPサーバ機能を利用していない場合は、LAN側ホストのDNSサーバアドレス設定を、本製品のLAN側IPアドレスにしておいてください。以上で設定は終了です。

7. ブラウザから「http://www.flets」にアクセスして接続を確認してください。

注意

▼PPPoEマルチセッションの注意事項

・PPPoEマルチセッションを利用する場合は、必ず本製品のProxy DNS機能を利用することが前提となります。

・パソコンにある「DNSキャッシュ」という仕組みにより、本製品の設定が正常に行われていても意図した動作が行われない場合があります。その場合は、本製品とパソコンの再起動を行ってみてください。

4 通常接続の設定

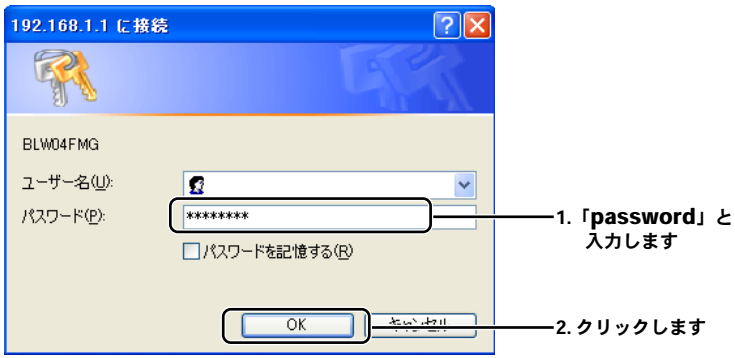
DHCP接続の場合は、「DHCPクライアント機能」→「**有効**」を目安に設定してください。
固定IP接続の場合は、「DHCPクライアント機能」→「**無効**」を目安に設定してください。

> **注意**
>
> ***・ブラウザでプロキシを使用する設定がされていると設定画面が表示されません。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」→「LANの設定」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。プロキシを使用しないように設定するか、もしくはプロキシの詳細設定画面で「次で始まるドメイン（アドレス）にはプロキシを使用しない」の欄に本製品のLAN側ポートのIPアドレスを入力してください。***

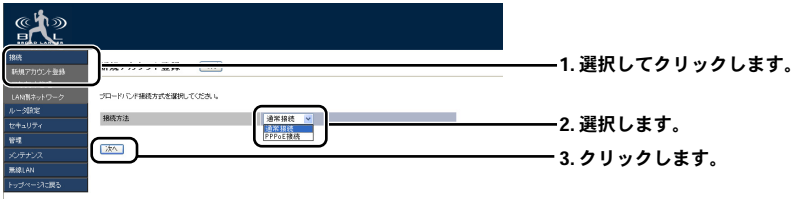
1. コンピュータが起動したら、WEBブラウザを起動します。

2. WEBブラウザのURLを入力する欄（Netscape では「場所」、Internet Explorerでは「アドレス」）に本製品のIPアドレス（デフォルト値は「192.168.1.1」）を入力し、Enterキーを押します。

3. 設定画面にログインするためのログイン画面が表示されます。
工場出荷時のパスワードは「password」です。パスワード欄に「password」と入力して、「OK」ボタンをクリックします。



4. 本製品の設定画面が表示されます。
メニューバーから「接続」→「新規アカウント登録」をクリックします。
接続方式に「通常接続」を選択して、「次へ」をクリックします。



5. 「通常接続設定」画面が表示されます。
以下の項目を入力します。

「アカウント名［任意］」
このPPPoE接続アカウントに、自由に名前を付けることができます。
契約プロバイダ名など、他のアカウントと区別できる（重複しない）わかりやすい名前を入力してください。
ここで設定した名前は「ルータ設定」や「セキュリティ」項目でも利用されます。
⇒設定範囲　　半角英数字 1～32文字まで　初期値 なし

「DHCPクライアント機能」
DHCPクライアント機能の動作を決定します。
⇒初期値　　有効
・有効
接続時に、プロバイダのDHCPサーバからIPアドレスが自動的に割り当てられる場合（Yahoo!BBなどDHCP接続方式を取っているプロバイダと接続する場合に使用します）
・無効
プロバイダから特定のIPアドレスが固定的に割り当てられている場合や個別のネットーワを構成する際に使用します

「DHCPクライアントID（ホスト名）」
＜DHCPクライアント機能＞で「有効」を選択した場合、ご利用のブロードバンドサービスによってはDHCPクライアントID（ホスト名）の設定が必要なことがあります。プロバイダから指定されているときのみ入力してください。指定されていない場合はデフォルトのままか空欄にします。＜DHCPクライアント機能＞で「無効」を選択した場合は、設定する必要はありません。
⇒設定範囲　　半角英数字 0〜64文字まで、初期値 brl04fmg

「WAN IPアドレス」
＜DHCPクライアント機能＞で「無効」を選択した場合に、プロバイダから固定的に割り当てられているIPアドレスを入力してください。これが本製品のWAN側ポートのIPアドレスになります。＜DHCPクライアント機能＞で「有効」を選択した場合は、プロバイダのDHCPサーバから自動的にIPアドレスが割り当てられるため入力する必要はありません。
⇒設定範囲　　半角数字 1.0.0.1〜223.255.255.254

「WANサブネットマスク」
＜DHCPクライアント機能＞で「無効」を選択した場合に、プロバイダから指定されているサブネットマスクを入力してください。これが本製品のWAN側ネットワークのネットマスクになります。＜DHCPクライアント機能＞で「有効」を選択した場合は、プロバイダのDHCPサーバから自動的にサブネットマスクが割り当てられるため入力する必要はありません。
⇒設定範囲　　半角数字 255.0.0.0〜255.255.255.252

「WANデフォルトゲートウェイ」
＜DHCPクライアント機能＞で「無効」を選択した場合に、プロバイダから指定されているデフォルトゲートウェイまたはデフォルトルート（ルータ）のIPアドレスを入力してください。これが本製品のWAN側ネットワークのデフォルトゲートウェイになります。＜DHCPクライアント機能＞で「有効」を選択した場合は、プロバイダのDHCPサーバから自動的にデフォルトゲートウェイが割り当てられるため入力する必要はありません。
⇒設定範囲　　半角数字 1.0.0.1〜223.255.255.254

「DNSサーバアドレス設定方法」
DNSサーバのIPアドレスをどうやって設定するかを決定します。
自動取得・固定設定 のいずれかを選択します。
⇒初期値　　自動取得
・自動取得
＜DHCPクライアント機能＞「有効」選択時、DNSサーバのIPアドレスも、プロバイダから自動取得する場合。＜DHCPクライアント機能＞で「無効」を選択した場合は、これを選択してはいけません
・固定設定
＜DHCPクライアント機能＞で「無効」を選択した場合は必ずこれを選択します。＜DHCPクライアント機能＞で「有効」を選択した場合で、プロバイダのDNSサーバではなく特定のDNSサーバを利用したい場合も、これを選択します

「プライマリ・セカンダリDNSサーバアドレス」
＜DNSサーバアドレス設定方法＞で「固定設定」を選択した場合に、利用するDNSサーバのIPアドレスを入力します。
「自動取得」を選択した場合は、入力する必要はありません
⇒設定範囲　　半角数字 1.0.0.1～223.255.255.254

6. 画面最下部にある「設定」ボタンをクリックし再起動後、4章「5.アカウント管理」に進んでください。

DMZネットワークを設定する必要がある場合は、4章「6.DMZネットワーク」を参照して設定を行ってください。

注意

・プロバイダから「ドメイン名」の指定がある場合は、4章「7.LAN側ネットワーク」をご参照ください。
・本製品を@NetHomeでご使用になるときは、@NetHomeへのルータ使用の登録をしたうえで、「ホスト名」欄に@NetHomeから指定されたサブドメイン名を設定してください。
・プロバイダによってはインターネットに接続するPCのMACアドレスの登録が必要なことがあります。すでにPCのMACアドレスが登録されているときは5章「9.管理者設定・WAN側MACアドレス」を参照して設定を行ってください。

5 アカウント管理

本製品は、登録されている1つの通常接続アカウントと最高2つのPPPoE接続アカウントを管理できます。また、同時に各アカウントの状態確認ができます。

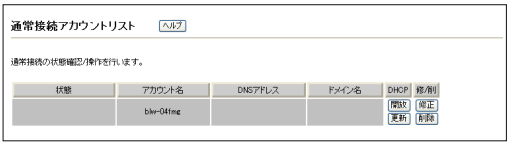
1. メニューバーから「接続」→「アカウント管理」をクリックします。
「アカウント管理」画面が表示されます。

●接続アカウント管理

「接続方式の選択」
通常接続とPPPoE接続のどちらを利用するかのいずれかを選択します。利用するアカウントが既に設定されていることを確認してから、適切な方式を選択してください。(本製品は、通常接続とPPPoE接続を同時に実現することはできません。)
⇒初期値　　通常接続

・通常接続
既に設定してある通常接続アカウントを使って、インターネットに接続する場合
・PPPoE接続
既に設定してあるPPPoE接続アカウントを使って、インターネットに接続する場合

●通常接続アカウントリスト



「状態」
通常接続アカウントの現在の状態を表示します。状態を表す表示には以下の6種類があります。

Disabled
通常接続が無効の状態

Link Down
本製品のWAN側ポートの物理的または電気的リンクが確立されていない状態

Connect ［IPAddress Subnetmask Defaultgateway］
本製品のWAN IPアドレスが固定設定されており、WAN側ポートの物理的・電気的リンクが確立されている状態
［ ］内はそれぞれ、WAN IPアドレス、WANサブネットマスク、WANデフォルトゲートウェイ

Connected ［IPAddress Subnetmask Defaultgateway DHCPTime］
本製品のDHCPクライアント機能が有効かつDHCPサーバからWAN IPアドレスを正常に取得できている状態
［ ］内はそれぞれ、WAN IPアドレス、WANサブネットマスク、WANデフォルトゲートウェイ、DHCPリースの残り時間（分）

DHCP offering
本製品のDHCPクライアント機能が有効であるが、DHCPサーバからWAN IPアドレスを取得できていない状態

DHCP Released
本製品のDHCPクライアント機能が有効であるが、以下のボタンによりDHCPサーバにIPアドレスを返却している状態

「アカウント名」
「通常接続設定」で、通常接続アカウントに付けた名前を表示します。

「DNSアドレス」
DHCPサーバから自動取得した、または固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを示します。

「ドメイン名」
DHCPサーバから自動取得した、または［LAN側ネットワーク］で手動設定したドメイン名を示します。

「DHCP」
DHCPクライアント機能で取得したWAN側IPアドレスの更新や開放を行います。

・「開放」
このボタンを押すと、DHCPサーバにWAN側IPアドレスを返上します。
WAN側IPアドレスが取得済みの時のみ、押すことができます

・「更新」
このボタンを押すと、DHCPサーバからWAN側IPアドレスを自動取得します。WAN側IPアドレスが未取得の時のみ、押すことができます

＊通常は、DHCPサーバからIPアドレスなどを自動取得していますが、上手く取得できていない場合にこの「開放」・「更新」をクリックすることで、手動更新を行えます。

「修/削」
該通常接続アカウントを、修正または削除します。「修正」ボタンを押すと、アカウント修正画面に移ります。

●PPPoE接続アカウントリスト

「状態」
当該PPPoE接続アカウントの現在の状態を表示します。状態を表す表示には以下の13種類があります。

Disabled
PPPoE接続が無効の状態

Link Down
本製品のWAN側ポートの物理的または電気的リンクが確立されていない状態

Connected ［IPAddress ServerAddress mm-dd:hh:mm:ss］
正常にPPPoE接続が確立されている状態。[ ] 内はWAN IPアドレス、PPPサーバIPアドレス、接続成功した月日時分秒を示します

Disconnected ［mm-dd:hh:mm:ss］
PPPoE接続を切断した後の状態。[ ] 内は切断した月日時分秒を示します

In the PPPoE Sequence
PPPoE接続シーケンスを実行している状態

PPPoE:Service-Name-Error
［PPPoE接続設定］ で設定してあるPPPoEサービス名が、PPPoEサーバに拒否された状態

PPPoE:AC-System-Error
PPPoEサーバ上でエラーが発生した状態

PPPoE:Generic-Error
エラーが発生した場合

PPPoE:PADI-Timeout
PPPoEサーバが発見できていない状態

PPPoE:LCP-Timeout
LCPタイムアウト。設定が間違っているか、本製品では接続できない特殊なサービスである可能性があります

PPPoE:IPCP-Timeout
IPCPタイムアウト。設定が間違っている可能性があります

PPPoE:Authentication-Failed
PPP認証に失敗した場合。設定が間違っている可能性があります

PPPoE:Authentication-Timeout
PPP認証タイムアウト。設定が間違っている可能性があります

「アカウント名」
［PPPoE接続設定］で、当該PPPoE接続アカウントに付けた名前を示します。

「DNSアドレス」
PPPoEサーバから自動取得した、または固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを示します。

「セッション」
PPPoEマルチセッション機能の動作として、それぞれのセッション用に異なる2つのPPPoEアカウントを割り当てることができます。ここでは、それぞれのアカウントをどちらのセッションで利用するか決定します。実際に通信を行うにはこれらを適切に選択する必要があります。
⇒初期値　　無効

・無効
単にアカウント情報を保持しておくだけで、実際の接続には利用しません
・プライマリ
常に1つのPPPoEアカウントを「プライマリ」に設定してください。これが主に利用する接続になります
・セカンダリ
通常のブロードバンド通信は「プライマリ」に設定したPPPoEアカウントを利用します。一方、[ポリシールーティング] で、セカンダリセッションを転送先インターフェイスに設定したポリシールートに一致する通信は、「セカンダリ」に設定したPPPoEアカウントを利用します。さらに、[DNSルーティング] で、セカンダリセッションを転送先インターフェイスに設定したDNSルートに一致するDNSクエリも、「セカンダリ」に設定したPPPoEアカウントを利用します。補助的なアカウントをこれに設定してください

「接続」
当該PPPoEアカウントの接続動作を決定します。
⇒初期値　　自動
・自動
LAN側ネットワークからインターネットへ向かう通信が検出された時のみ、当該PPPoEアカウントへの接続動作を開始します。一旦接続に成功した後は、「切断」ボタンが押された場合、＜アイドルタイム＞が経過した場合、公衆網側から切断された場合、PPPoEサーバが検出されなくなった場合に、切断動作を行います
・常時
セッション・キープ・アライブ機能です。再起動後や電源投入後、すぐに当該PPPoEアカウントへの接続動作を開始し、成功するまで試行します。一旦接続に成功した後は、「切断」ボタンが押された場合、公衆網側から切断された場合、PPPoEサーバが検出されなくなった場合に、切断動作を行いますが、切断完了後すぐに接続動作を再開します。すなわち、当該PPPoEアカウントへの接続を常に維持しようとします。＜アイドルタイム＞の値は無視されます
・手動
「接続」ボタンが押された時のみ、当該PPPoEアカウントへの接続動作を開始します。一旦接続に成功した後は、「切断」ボタンが押された場合、＜アイドルタイム＞が経過した場合、公衆網側から切断された場合、PPPoEサーバが検出されなくなった場合に、切断動作を行います

「アイドルタイム」
当該PPPoEアカウントへの接続中、ここに指定した時間（分）、WAN側とLAN側との通信が検出されない場合、自動的に切断動作を行います。この処理を行いたくない場合は「0」を入力してください。
⇒設定範囲　　半角数字 0〜999分、初期値 20分

「操作」
手動操作によるPPPoE接続や切断を行います。接続したい時は「接続」ボタン、切断したい時は「切断」ボタンを押してください。
ただし、＜接続＞が「常時」に設定されている場合、手動切断直後に自動的に再接続動作を行います。

「修/削」
当該PPPoE接続アカウントを、修正または削除します。修正する場合は「修正」ボタン、削除する場合は「削除」ボタンを押してください。

「PPP-Echo-Request送出間隔」
本製品はPPPoE接続中、PPPサーバに対してPPP-Echo-Requestを送出し、それに対する応答パケット（PPP-Echo-Reply）を確認することで、PPPセッションの状況を監視します。ここではそのPPP-Echo-requestの送出間隔（秒）を決定します。
⇒設定範囲　　半角数字 10〜300秒、初期値 60秒

「PPP-Echo-Requestリトライ回数」
上記＜PPP-Echo-Request送出間隔＞でPPP-Echo-Requestを送出し、連続何回PPPサーバから応答がない場合に切断と判断し接続動作を行うかを決定します。
⇒設定範囲　　半角数字 1〜99回、初期値 6回

2. いずれかの設定を変更した場合は、画面の一番下の「設定」のボタンをクリックして設定の保存をしてください。

注意

・セカンダリセッションへの接続は、1つの物理回線で2つ以上のPPPoEセッションを利用可能なブロードバンドサービス（フレッツ・ADSL、Bフレッツなど）に限定されます。それ以外の場合は、絶対にセカンダリセッションを設定しないでください。

・極端に短いPPP-Echo-Request送出間隔や極端に少ないPPP-Echo-Requestリトライ回数を設定すると、PPPoEセッションの切断と再接続が頻繁に発生します。必要がない限りこれらの値は変更しないでください。

・WAN側IPアドレスを自動取得するPPPoEブロードバンドサービス（動的なIPアドレス）の場合、PPPoE接続アカウントリストの＜接続＞で「常時」を選択することは、WAN側IPアドレスが一定であることを保証するものではありません。単に切断されたことを検出し、自動的に再接続動作を行うだけです。WAN側IPアドレスは接続する度に変わる可能性があります。

・設定項目を再確認した上でインターネットに接続出来ない場合は、「付録A ネットワークQ&A」を参照してみてください。

6 DMZネットワーク

本製品は、DMZネットワーク機能を有し、NAPTによるプライベートホスト通信と、公開サーバなどのグローバルホスト通信を同時に実現することができます。DMZとLANはそれぞれ論理的別セグメントであり、各セグメントのセキュリティポリシーも分けることができて、またセグメント間の通信を細かく制御・制限することで、より高いセキュリティを保つことができます。
DMZネットワーク上には、グローバルIPアドレスホストを設置します。また、プライベートネットワークのNAPT用グローバルIPアドレスだけでなく、DMZネットワークに設置するサーバのグローバルIPアドレスも必要です。したがって、プロバイダから複数のグローバルIPアドレスを割り当てられているサービスの場合のみ、DMZネットワーク機能を利用することができます。

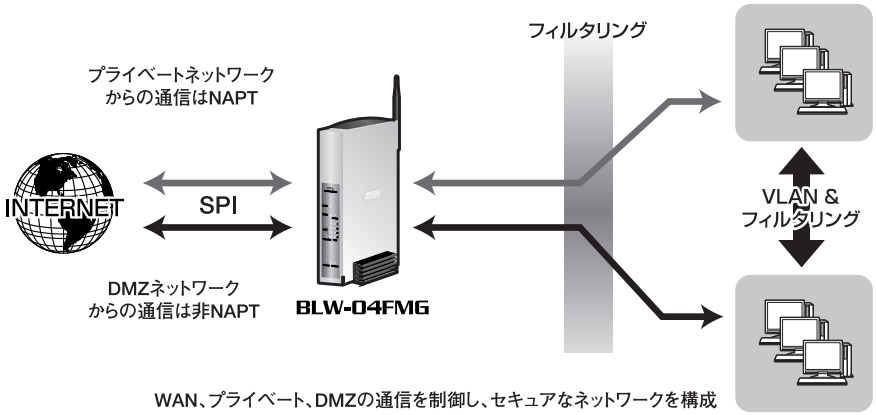


図4-3　DMZ構成図

今回は以下の複数グローバルIPを使ってDMZネットワークの設定方法を解説します。

＜例＞

割り当てアドレス	**153.16.10.8 ～ 153.16.10.15 までのグローバル IP アドレス**
ネットマスク	**255.255.255.248**
プレフィックス長	**29bit**
ネットワークアドレス	**153.16.10.8**
ブロードキャストアドレス	**153.16.10.15**
プロバイダから指定された デフォルトゲートウェイアドレス	**153.16.10.14**

1. 本製品のWANポート設定を行います。
「アカウント管理」から該当のアカウント項目「修正」をクリックします。

2. 以下事項を追記設定します。

＜通常接続の場合＞
「DHCPクライアント機能」
「無効」を選択します。

「WAN IPアドレス」
本製品自身に割り当てられるグローバルIPアドレスで、プライベートホストのNAPTにも利用されます。
割り当てアドレスのネットワークアドレスとブロードキャストアドレスは使用できません。
割り当て範囲であれば、いずれでも問題はありませんが、慣習的にネットワークアドレスの次のアドレスを選択します。
⇒設定例　　153.16.10.9

「WANサブネットマスク」
プロバイダから指定されたサブネットマスクをそのまま入力します。
⇒設定例　　255.255.255.248

「WANデフォルトゲートウェイ」
プロバイダから指定されたデフォルトゲートウェイをそのまま設定します。
ここで指定したIPアドレスは、他の用途に利用することはできません。
⇒設定例　　153.16.10.14

「DNSサーバアドレス」
プロバイダから指定されたDNSサーバIPアドレスまたは、（プライマリ・セカンダリ）自分で運営しているDNSサーバのIPアドレスを入力します。

＜PPPoEアカウントの場合＞
「WAN側IPアドレス設定方法」
「固定設定」を選択します。

「WAN側固定IPアドレス」
本製品自身に割り当てられるグローバルIPアドレスで、プライベートホストのNAPTにも利用されます。
割り当てアドレスのネットワークアドレスとブロードキャストアドレスは使用できません。割り当て範囲であれば、いずれでも問題はありませんが、慣習的にネットワークアドレスの次のアドレスを選択します。
⇒設定例　　153.16.10.9

「DNSサーバアドレス設定方法」
「固定設定」を選択します。

「DNSアドレス」
プロバイダから指定されたDNSサーバIPアドレスまたは、（プライマリ・セカンダリ）自分で運営しているDNSサーバのIPアドレスを入力します。

「DNZネットワークサブネットマスク」
プロバイダから指定されたサブネットマスクをそのまま入力します。
⇒設定例　　255.255.255.248

3. 上記入力内容を確認して、「設定」ボタンをクリックしてください。

4. 再度、「アカウント管理」から該当のアカウント項目「修正」をクリックして「DMZネットワークの追加」を行います。
DMZネットワークテーブルに、LAN側に設置するグローバルIPアドレスホストで利用する、グローバルIPアドレス範囲を設定します。ネットワークアドレスとブロードキャストアドレスは必ず除外してください。また、上記で設定したWAN IPアドレス、WANデフォルトゲートウェイも除外します。
最高4範囲まで設定することができますが、本製品の処理負荷を軽減するために、実際に利用するグローバルIPアドレス範囲のみ設定するようにしてください。設定例では、153.16.10.10 ～ 153.16.10.13とします。

5. 次に、グローバルIPアドレスホストが本製品のLAN側に位置し、インターネット通信をするために、本製品のLAN側ポートがこれらのグローバルIPアドレスホストにとってのデフォルトゲートウェイとなる必要があります。
「接続」→「LAN側ネットワーク」を開きます。

6. 下記の追加設定を行ってください。

「セカンダリLANモード」
LAN側のグローバルIPアドレスホストのためのデフォルトゲートウェイとして機能するのが、本製品LANポートが持つ2つの論理IPインターフェイスのうちの、セカンダリLANインターフェイスです。ここではセカンダリLANモードとして、「DMZネットワークのゲートウェイアドレス」を選択します。

「セカンダリLAN IPアドレス」
LAN側のグローバルIPアドレスホストのためのデフォルトゲートウェイアドレスを決定します。基本的に、ネットワークアドレスやブロードキャストアドレス以外で、且つこれまでの設定で利用していないグローバルIPアドレスの中から1つを選びます。ただし、本製品のひとつの特徴としてグローバルIPアドレスの節約のため、既に上記で設定した「WAN IPアドレス」と同じグローバルIPアドレスを、LAN側グローバルデフォルトゲートウェイアドレスとして再利用することができます。設定例では、153.16.10.9となります。

「セカンダリLANサブネットマスク」
設定しないでください。(0.0.0.0 のままにしておきます)

7. DMZネットワークに関する本製品への設定は以上です。
あとは、LAN側に設置するグローバルIPアドレスホストそれぞれに、以下のようなネットワーク設定を行います。

・DMZネットワーク範囲内のグローバルIPアドレスを自IPアドレスとして割り当て
設定例では153.16.10.10 ～ 153.16.10.13 までのグローバルIPアドレス
・サブネットマスクを設定
設定例では255.255.255.248

・デフォルトゲートウェイアドレスを設定
設定例では153.16.10.9

・利用するDNSサーバのIPアドレスを設定

以上でDMZネットワークの設定は終了です。

注意

・*DMZネットワーク範囲が1個のIPアドレスの場合は、「最初のIPアドレス」と「最後のIPアドレス」を同じにしてください。*
＜最初のIPアドレス＞は常に＜最後のIPアドレス＞より小さいか、同じアドレスにしてください。

・*DMZネットワーク範囲には、本製品自身が持つNAPT用WAN側IPアドレスや、ネットワークアドレス・ブロードキャストアドレスが含まれないように注意してください。*

・*DMZネットワークテーブルで設定するグローバルIPアドレス範囲は、実際に利用する（実際にDMZセグメントに設置する）グローバルIPアドレスのみ設定してください。余分に（DMZセグメントに存在しない）グローバルIPアドレスを設定していると、インターネット側からそのIPアドレス宛にホスト/バックドア探索パケットや攻撃パケットなどが来る度に、本製品がDMZセグメントへ向けて無意味なarpをブロードキャスト送信することになります。*

・*セカンダリLANおよびDMZネットワーク上のホストは、本製品のUPnP機能を利用することはできません。*

・*DMZネットワーク上のホストから本製品の設定画面にアクセスしたい場合は、WWWブラウザでセカンダリLAN IPアドレスにアクセスしてください。*

・*DMZネットワーク利用時、セカンダリLAN IPアドレスは、Proxy DNSとして機能しません。したがってDMZネットワーク上のホストのIP設定では、DNSサーバアドレスを直接指定する必要があります。*

・*DMZネットワーク上のホストは、インターネット上から直接参照可能な状態になります。セキュリティを確保するには、フィルタなどを設定してください。静的フィルタなどの設定では「lan1」がDMZネットワーク（セカンダリLAN）のことを示します。*

・*lan0 ←→lan1間の通信はデフォルトで禁止されているので、DMZネットワークに設置したグローバルIP端末とローカル端末間の通信を行う場合には静的フィルタでlan0 ←→lan1間の通過フィルタルールを追加設定してください。*

・*DMZ端末に対するフィルタの設定は「アカウント <-->lan1」に対して行ってください。*

・*マルチNAT機能を利用する場合、DMZネットワークの設定は不要です。*

・*DMZネットワークのマスク長は28bit以上に設定してください。*

7 LAN側ネットワーク

本製品のLAN側ネットワークに関して説明します。

本製品のLAN側ポートは、最大で2個のIPアドレスを持つことができます。
しかし、DMZネットワークを利用している場合や、本製品のLAN側に2つのIPネットワーク（サブネット）を設置している場合を除き、通常はLAN側IPアドレスを1個だけ設定して利用します。主に利用するLAN側IPアドレスを本製品では「プライマリLAN IPアドレス」、このIPアドレスが属するLAN側IPネットワーク（サブネット）を「プライマリLANネットワーク」と呼びます。プライマリLAN IPアドレスは本製品の設定を行う際に用いるほか、プライマリLANネットワーク上のホストからみたゲートウェイアドレスとしても利用されます。

セカンダリLANを使用する状況は以下を想定しています。

●DMZネットワーク（通常接続/PPPoE接続）を利用する場合
DMZネットワークを利用する場合、セカンダリLANを利用します。すなわち、DMZネットワークとセカンダリLANネットワークは同じネットワークであることを意味します。この時、セカンダリLAN IPアドレスは、DMZネットワーク上のホストから見たゲートウェイアドレスとなります。
NAPT機能が有効の場合、DMZネットワーク（セカンダリLANネットワーク）の通信はNAPT処理されません。プライマリLANネットワークからWAN側への通信のみNAPT処理されます。NAPT機能が無効の場合は、DMZネットワーク（セカンダリLANネットワーク）の通信、プライマリLANネットワークの通信ともにNAPT処理されません。

●LAN側に2つのネットワークを設置する場合（NAPT有効時）
一般的なブロードバンドルータは、1個のLAN側ネットワークしか配置できませんが、本製品は2個のIPネットワークをLAN側に配置することが可能です。NAPT機能が有効の場合、プライマリLANネットワークからWAN側への通信、セカンダリLANネットワークからWAN側への通信ともにNAPT処理が行われます。NAPT機能が無効の場合は、どちらもNAPT処理されません。

⚠ 注意

・DMZネットワーク利用時、DMZネットワーク（セカンダリLANネットワーク）のサブネットと、WAN側ネットワークのサブネットは、完全に一致するにもかかわらず、本製品の異なるインターフェイス上に位置することになります。DMZネットワーク（セカンダリLANネットワーク）上のホストしか利用せず、NAPTを前提としたプライベートIPホストをLAN側に設置しない場合でも、プライマリLAN IPアドレスは設定しておく必要があります（工場出荷時の設定値のままで可）。ただし、NAPT機能を無効化することは可能です。

・セカンダリLANおよびDMZネットワーク上のホストは、本製品のUPnP機能を利用することはできません。

・セカンダリLANネットワーク（DMZネットワーク）上のホストから本製品の設定画面にアクセスしたい場合は、WWWブラウザでセカンダリLAN IPアドレスにアクセスしてください。

・DMZネットワーク利用時、セカンダリLAN IPアドレスは、Proxy DNSとして機能しません。したがってDMZネットワーク上のホストのIP設定では、DNSサーバアドレスを直接指定する必要があります。ただしDMZネットワーク機能を利用していない場合のセカンダリLAN IPアドレスは、Proxy DNSとして機能します。

・本製品のDHCPサーバ機能で配布できるIPアドレスは、プライマリLANネットワークのIPアドレスだけです。セカンダリLANネットワークのIPアドレスを配布することはできません。

・セカンダリLAN（DMZネットワーク）と、プライマリLANの2つのIPネットワーク間のルーティングは、デフォルトで禁止（静的フィルタ項目に何も設定されていない）状態になります。このルーティングを行いたい場合は、静的フィルタ設定で、「lan0 -> lan1」「lan1 -> lan0」の両方向で、pass（通過させる）ルールを設定してください。ただし、この設定を行った場合、プライマリLANも安全性が若干低下しますので、通過許可するパケットを、必要なものだけに制限する方法をお勧めします。

●LAN側ネットワーク設定

1. メニューバーから「接続」→「LAN側ネットワーク」をクリックします。「LAN側ネットワーク」設定画面が表示されます。

2. 以下の設定項目を入力します。

「プライマリLAN IPアドレス」
LAN側ポートのプライマリLAN IPアドレスを入力します。このアドレスがLAN側から見た本製品のIPアドレスになります。
⇒設定範囲　　半角数字 1.0.0.1～223.255.255.254
初期値 192.168.1.1

「プライマリLANサブネットマスク」
プライマリLAN LANネットワークのサブネットマスクを入力します。
⇒設定範囲　　半角数字 255.0.0.0～255.255.255.252
初期値 255.255.255.0

「セカンダリLANモード」
そのセカンダリLANネットワークの利用形態を決定します。
⇒初期値　　無効
・無効
セカンダリLANを利用しません。通常はこれを選択します
・有効
2つめのLAN側ネットワークを設置する場合、「有効」を選択します

以下の＜セカンダリLAN IPアドレス＞と＜セカンダリLANサブネットマスク＞も入力してください。

「DMZネットワークのゲートウェイアドレス」
セカンダリLANをDMZネットワーク上のホスト群にとっての（デフォルト）ゲートウェイIPアドレスとして利用します。

以下の＜セカンダリLAN IPアドレス＞と＜セカンダリLANサブネットマスク＞に入力する必要はありません。

「セカンダリLAN IPアドレス」
＜セカンダリLANモード＞で、「有効」または「DMZネットワークのゲートウェイアドレス」を選択した場合に、セカンダリLANのIPアドレスを入力します。ここに入力するアドレスがセカンダリLANネットワークから見た本製品のIPアドレスになります。
⇒設定範囲　　半角数字 1.0.0.1～223.255.255.254

「セカンダリLANサブネットマスク」
＜セカンダリLANモード＞で、「有効」を選択した場合に、セカンダリLANネットワークのサブネットマスクを入力します。
⇒設定範囲　　半角数字 255.0.0.0～255.255.255.252

「DHCPサーバ機能［プライマリLANのみ］」
DHCPサーバ機能の動作を決定します。
⇒初期値 有効

・有効
LAN側ネットワーク（プライマリLANのみ）にDHCPサーバ機能を提供します
・無効
DHCPサーバ機能を提供しません。LAN側ネットワーク上のすべての端末は、手動でIP設定を行う必要があります

「DHCPリース状況の表示」
本製品のDHCPサーバ機能から割り当てられてたIPアドレスの状況を表示します。

「LANデフォルトゲートウェイ」
＜DHCPサーバ機能＞で「有効」を選択した場合に、LAN側ネットワーク上のDHCPクライアントに配布されるデフォルトゲートウェイのIPアドレスを入力します。一般的に、LAN側ネットワークのデフォルトゲートウェイは本製品になりますので、本製品のプライマリLAN IPアドレスを入力してください。異なるIPアドレスを指定すると、インターネット通信できなくなります。
⇒設定範囲　　半角数字 1.0.0.1～223.255.255.254
初期値 192.168.1.1

「WINSサーバIPアドレス」
＜DHCPサーバ機能＞でLAN側ネットワーク上のDHCPクライアントに配布するWINSサーバのIPアドレスを入力します。
通常は使用しません。
⇒設定範囲　　半角数字 1.0.0.1～223.255.255.254

「ドメイン名」
＜DHCPサーバ機能＞でLAN側ネットワーク上のDHCPクライアントに配布するドメイン名を入力します。ドメイン名は、不完全な名前の解決に用いられるDNSサフィックスとして各端末上で利用されます。
⇒設定範囲　　半角英数字 0～63文字

「DHCPリース時間」
＜DHCPサーバ機能＞でLAN側ネットワーク上のDHCPクライアントに配布するIP設定のリース期間（時間）を入力します。
⇒設定範囲　　半角数字 1～999999時間、初期値 72時間

「無期限リース」
DHCPサーバ機能により、LAN側ネットワーク上のDHCPクライアントに配布されるIP設定のリース期間を無限にしたい場合のみ、チェックを入れてください。上記＜DHCPリース時間＞の値は無視されます。＜DHCPサーバ機能＞で「無効」を選択した場合は、設定する必要はありません。

「Proxy DNS機能［DNSルーティング利用時必須］」
プロバイダのDNSサーバに代わって、本製品があたかもDNSサーバとして振舞う、Proxy DNS機能の動作を決定します。
LAN側ネットワークに対し、Proxy DNS機能を提供します。
DNSルーティングやPPPoEマルチセッション利用時は必ず「有効」にしてください。
⇒初期値　　有効

「Universal Plug and Play機能」
LAN側ネットワークに対するUPnP機能の動作を決定します。
これが「有効」の場合、プライマリLANネットワーク上のホストに対し、UPnP機能（Internet Gateway Device version1.0）を提供します。
⇒初期値　　有効

3. DHCPスコープまたはDHCP固定IPアドレスを設定する必要がある場合は、次に進んでください。

特にそれらを設定する必要がなければ、画面一番下の「設定」ボタンをクリックして作業を終了します。

●DHCPスコープテーブル
本製品のDHCPサーバの割り当てIPアドレス範囲が表示されます。

1. DHCPスコープテーブルでは、何番から何番までのIPアドレスをDHCPサーバ機能によりLAN側ホストに割り当てるかを表示します。
DHCPスコープは、最高4範囲まで設定することができます。
⇒設定範囲　　1～254　初期値　192.168.1.20～192.168.1.50

「最初のIPアドレス」
既に設定されているDHCPスコープの、最初のIPアドレスを表示します。

「最後のIPアドレス」
既に設定されているDHCPスコープの、最後のIPアドレスを表示します。

「修/削」
既に設定されているDHCPスコープを、修正または削除します。修正する場合は修正ボタンを、削除する場合は削除ボタンをクリックしてください。

2. DHCPスコープの設定が完了している場合は、画面一番下の「設定」ボタンをクリックしてください。

●DHCPスコープの追加

最高4つまでDHCPスコープを追加することができます。

1.「DHCPスコープの追加」ボタンをクリックします。

「最初のIPアドレス」
設定したいDHCPスコープの、最初のIPアドレス（ aaa.bbb.ccc.ddd 形式でdddの値）を入力してください。

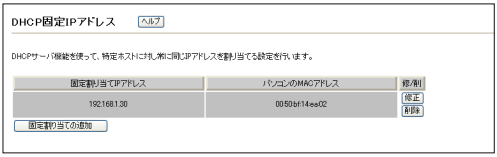
「最後のIPアドレス」
設定したいDHCPスコープの、最後のIPアドレス（ aaa.bbb.ccc.ddd 形式でdddの値）を入力してください。

2. 画面一番下の「設定」ボタンをクリックすると、[LAN側ネットワーク] に戻りますので再度、画面一番下の設定ボタンをクリックしてください。

注意

・クラスCサブネット（255）を越えるDHCPスコープは設定できません。
・<最初のIPアドレス>は常に<最後のIPアドレス>より小さくしてください。
・DHCPスコープ範囲には、本製品自身が持つプライマリLAN IPアドレスや、ネットワークアドレス・ブロードキャストアドレスが含まれないように注意してください。

●DHCP固定IPアドレステーブル



DHCPサーバ機能では、MACアドレスを指定することで、特定の端末にあらかじめ決めておいたIPアドレスを割り当てることができます。ここでは、MACアドレスとIPアドレスの組み合わせを表示します。

1. DHCP固定IPアドレステーブルでは、どのMACアドレスのホストに、何番のIPアドレスを割り当てるかを表示します。DHCP固定IPアドレスは、最高16組み合わせ設定することができます。
⇒初期値　　なし

「固定割り当てIPアドレス」
既に設定されているMACアドレスとIPアドレスの組み合わせのうち、MACアドレスを表示します。

「パソコンのMACアドレス」
既に設定されているMACアドレスとIPアドレスの組み合わせのうち、IPアドレスを表示します。

「修/削」
既に設定されているMACアドレスとIPアドレスの組み合わせを、修正または削除します。修正する場合はボタンを、削除する場合はボタンをクリックしてください。

2. DHCP固定IPアドレスの設定が完了している場合は、画面一番下の「設定」ボタンをクリックしてください。
DHCP固定IPアドレスを追加する場合は、以下の項目に進んでください。

●DHCP固定IPアドレスの追加

1.「DHCPスコープの追加」ボタンをクリックします。

「固定割り当てIPアドレス」
設定したいMACアドレスとIPアドレスの組み合わせのうち、IPアドレス（aaa.bbb.ccc.ddd 形式でdddの値）を入力してください。

「パソコンのMACアドレス」
設定したいMACアドレスとIPアドレスの組み合わせのうち、MACアドレスを入力してください。

2. 画面一番下の「設定」ボタンをクリックすると、［LAN側ネットワーク］に戻ります。再度画面一番下のボタンをクリックしてください。

注意

・＜固定割り当てIPアドレス＞には、本製品自身が持つプライマリLAN IPアドレスや、ネットワークアドレス・ブロードキャストアドレスを設定しないでください。
・＜パソコンのMACアドレス＞には、特殊な予約MACアドレスである「00:00:00:00:00:00」や「ff:ff:ff:ff:ff:ff」を設定しないでください。

詳細設定

本章では本製品の各機能の概要について説明します。設定項目の詳細についてはWEB設定画面の各項目ごとに「ヘルプ」を用意していますのでそちらをご参照ください。

注意

・WEBブラウザから本製品にアクセスするには、フレーム表示に対応したブラウザをご利用になる必要があります。Netscape 6.0以降またはMicrosoft Internet Explorer 5.0以降のご利用を推奨します。

・ブラウザでプロキシを使う設定になっていると設定画面が表示されません。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」→「LANの設定」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。プロキシを使わない設定にするか、もしくはプロキシの詳細設定画面で「次で始まるドメイン（アドレス）にはプロキシを使用しない」の欄に本製品のLAN側ポートのIPアドレスを入力します。

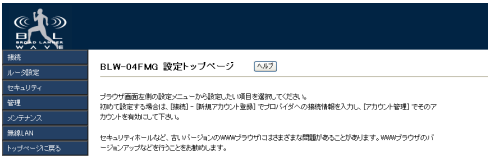
1 設定画面を開く

1. コンピュータが起動したら、WEBブラウザを起動します。

2. WEBブラウザのURLを入力する欄（Netscape では「場所」、Internet Explorerでは「アドレス」）に本製品のLAN側ポートのIPアドレスを入力し、Enterキーを押します。工場出荷時や本製品の初期化後のLAN側ポートのIPアドレスは「192.168.1.1」です。

3. 設定画面にログインするためのパスワード入力画面が表示されます。パスワード欄にパスワードを入力して、「OK」ボタンをクリックします。工場出荷時や本製品の初期化後のパスワードは「password」です。

4. 本製品の設定画面が表示されます。



2 NAPT

●NAPTとは？

主にIPアドレスの共有を実現するため、送信元IPアドレスと送信元ポート番号の変換を行う機能をNAPTと呼びます。本製品のようなNAPTルータは、LAN側からのパケットをWAN側（インターネット上）の送信先に転送する際、送信元IPアドレスと送信元ポート番号の変換を行います。応答パケットが帰ってきたら、以前に行った変換の履歴を元に、LAN側に転送します。また、この機能を「無効」にするとアドレス/ポート変換を行わないでルーティングを行います。こういったローカルルータとしての使用も可能です。

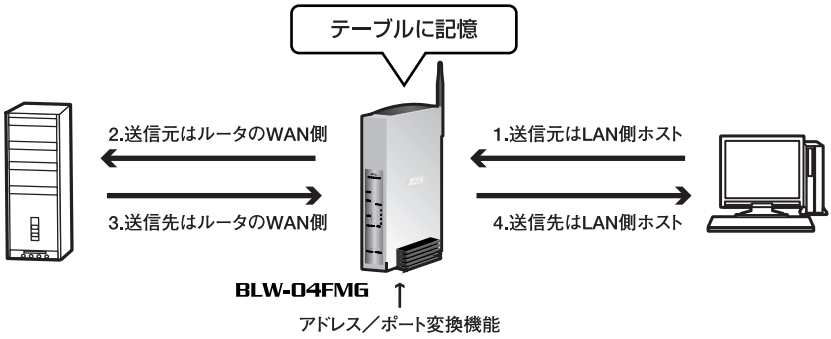


図5-1

●NAPT非対応アプリケーションサポート

NAPT機能は、IPパケットのヘッダ情報である送信元IPアドレス/送信先IPアドレスや、tcp, udpヘッダの送信元ポート/送信先ポートを変換します。こうした性格上、tcpでもudpでもないVPN（PPTP, L2TP, IPsec）、2つのtcpコネクションを利用するFTP、UDPストリーミング（RTP/UDP, MMS/UDP）などを利用するアプリケーションには通常のNAPTルータでは対応できません。

これに対し本製品はこれらのプロトコルパケットに特殊な処理を行うことで、NAPT配下のLAN側プライベートIPアドレスホストのためのVPNパススルー、FTP転送や、UDPストリーミングをサポートします。

●FTP制御ポート
FTPコントロールセッションで使用するTCPポート番号を入力します。

●VPNパススルー機能
VPNパススルー機能を有効にすると、本製品LAN側VPNノードとWAN側VPNノードとの間のVPN通信が可能になります。

・LAN側にPPTPクライアントを設置する場合
本製品のPPTPパススルー機能を有効にしてください。本製品はマルチPPTPパススルーに対応していますので、LAN側に複数のPPTPクライアントを設置する場合でも、PPTPパススルー機能を有効にするだけで利用できます。

・LAN側にPPTPサーバを設置する場合
本製品のPPTPパススルー機能を有効にし、さらに静的マスカレード設定で、tcpポート1723番宛てのトラフィックをLAN側PPTPサーバに転送する設定を行ってください。LAN側に設置可能なPPTPサーバ数は1台のみサポートします。

・LAN側にL2TPクライアントを設置する場合
本製品のL2TPパススルー機能を有効にしてください。本製品はマルチL2TPパススルーに対応していますので、LAN側に複数のL2TPクライアントを設置する場合でも、L2TPパススルー機能を有効にするだけで利用できます。

・LAN側にL2TPサーバを設置する場合
本製品のL2TPパススルー機能を有効にし、さらに静的マスカレード設定で、udpポート1701番宛てのトラフィックをLAN側にL2TPサーバに転送する設定をおこなってください。LAN側に設置可能なL2TPサーバ数は1台のみサポートします。

・LAN側にIPsecノードを設置する場合
本製品のIPsecパススルー機能を有効にし、さらに静的マスカレード設定で、プロトコル「＊（すべて）」のトラフィックをLAN側Psecノードに転送する設定を行ってください。LAN側に設置できるIPsecノード数は1台のみサポートします。

⚠ 注意

- ***VPNパススルー機能が必要になるのは、本製品のNAPT配下にLAN側VPNノードを設置する場合のみです。複数グローバルIPアドレスサービスで、DMZネットワーク機能を利用したLAN側DMZホスト（グローバルIPホスト）がVPNを利用する場合は、本製品への設定は特に必要ありません。***
- ***IPsecパススルー機能では、静的マスカレードを設定せずにLAN側IPsecノードからVPNトンネルを開始する場合に限り、複数のLAN側IPsecノードによる複数のIPsecトンネルをサポートします。ただしIPsecでは、切断されたIPsecトンネルの再接続などの際に、WAN側IPsecノードからトンネル接続が開始されることもあるため、原則的に、LAN側に設置できるIPsecノード数は1台のみ、かつ静的マスカレード設定が必要となります。***
- ***IPsecパススルー機能がサポートするのは、IPsecトンネリングモードのみです。トランスポートモードはサポートしません。***

3 静的マスカレード

●静的マスカレードとは？

LAN側にインターネットサーバを公開したい場合などで、WAN側から開始される通信がある場合、NAPTの変換履歴がないために、NAPTルータはWAN側から来たトラフィックを破棄してしまいます。

あらかじめWAN側から開始されるトラフィックのポート番号が判明している場合に、そのポートにきた通信を特定のLAN側ホストに転送するように設定しておくことで意図したLAN側ホストと通信させることが可能となります。

さらにポート番号が不明の場合でも、WAN側から開始されNAPTテーブルに該当しなかったトラフィックのLAN側転送先ホストを、あらかじめ決めておくことも可能です。本製品ではこれらの機能をまとめて静的マスカレードと呼びます（NAPTルータ製品の中には、これらを「ローカルサーバ機能」、「バーチャルサーバ機能」、「DMZホスト機能」などと呼称しているものもあります）。この機能を使えば、WAN側IPアドレスのtcp 80番ポートに来たトラフィックを、LAN側のWWWサーバ（プライベートIP）に転送するといったことができます（WWWサーバの公開）。

静的IPマスカレード機能：

本製品のWAN側IPアドレス宛にくる転送先LAN側ホストが不明なパケットのうち、特定のプロトコル/ポートのパケットを予め設定したローカルIPアドレスのホストあてに転送する機能です。ポート公開を必要最小限にすることで、セキュリティ的なリスクを少なくすることができます。

マルチNAT機能：

本製品のWAN側IPアドレス宛にくる転送先LAN側ホストが不明なパケットのうち、すべてのパケットを予め設定したローカルIPアドレスのホストあてに転送する機能です。アプリケーションで使用するプロトコル/ポートが不明な場合はとりあえずマルチNAT機能を使用します。

複数グローバルIP接続の場合、それぞれのグローバルIPアドレスをローカルIPアドレスと1対1で指定することもできます。

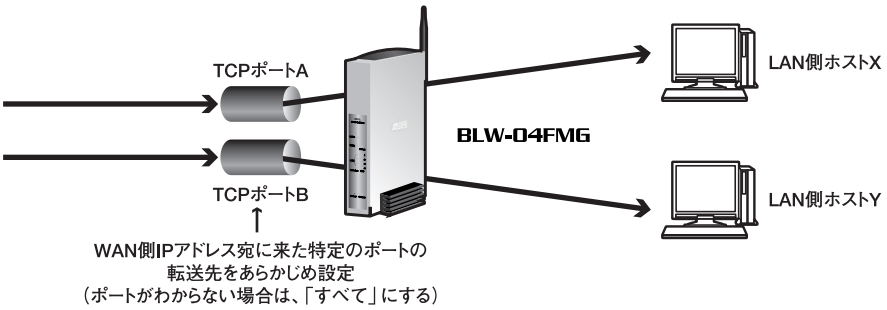
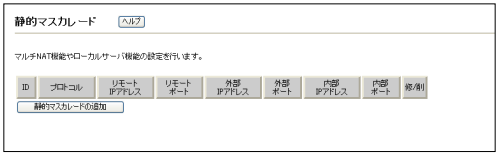


図5-2



注意

静的マスカレードの転送先LAN側ホストは、設定されたポートを通して、インターネットから直接参照可能な状態になります。セキュリティを確保するにはフィルタなどを設定してください。
WAN側からのすべてのトラフィックを指定したLAN側ホストに転送したい場合（他社製低価格ブロードバンドルータにおいて「バーチャルコンピュータ」や「仮想DMZ」などと呼称されている機能）、静的マスカレードの追加の際のプロトコル選択で「＊（すべて）」を選択してください。
プロトコル選択で「＊（すべて）」を指定した場合でも、すべてのトラフィックが設定されたLAN側ホストのみに転送されるわけではなく、通常の動的NAPTテーブル（履歴）に一致しなかったトラフィックのみが静的マスカレード転送の対象になります。したがって、他のLAN側ホストによる通常のNAPT通信も同時に行うことができます。
LAN側のFTPサーバをインターネットに公開する場合は、tcpポート21番宛てのトラフィックをLAN側FTPサーバに転送する静的マスカレード設定を行ってください。本製品はFTP pasv/port両方の転送方式をサポートしており、データコネクションポートのマスカレードが必要な場合、本製品が自動的にポートを空けるため、データコネクション用の静的マスカレードは不要です。ただし、WAN側からLAN側FTPサーバへのアクセスには、できるかぎりportモードを利用してください。

4 ポリシールーティング

●ポリシールティングとは？

本製品はスタティックルーティングやダイナミックルーティングに加え、ポリシールーティングという考え方を導入し、送信先IPアドレスだけでなくプロトコル、送信元IPアドレス、送信先ポート番号、送信元ポート番号といった、詳細なパラメータを経路判断項目として取り上げることができます。これらを指定し、柔軟なルーティングポリシーを設定できるようになります。

「ポリシールートID」

最高32個のポリシールートを設定することができます。これはスタティックルーティングやダイナミックルーティングで言うところのメトリックの代替として働くものです。対象トラフィックが複数のポリシールート間で重複する場合、ID番号が小さいポリシールートが優先されます。

「プロトコル」

プロトコルに関係なくすべて、icmp、tcp、udpを選択可能です。

「送信先IPアドレス」

特定の送信先IPアドレスだけでなく、サブネット単位（プレフィックス長指定）、IPアドレス範囲、IPアドレスの列挙でも指定することができます。

「送信先ポート」

tcpやudpの場合は、送信先ポート番号も指定可能です。特定のポート番号だけでなく、ポート範囲、ポートの列挙でも指定することができます。

「送信元IPアドレス」

特定の送信元IPアドレスだけでなく、サブネット単位（プレフィックス長指定）、IPアドレス範囲、IPアドレスの列挙でも指定することができます。

「送信元ポート」
tcpやudpの場合は、送信元ポート番号も指定可能です。特定のポート番号だけでなく、ポート範囲、ポートの列挙でも指定することができます。

「ゲートウェイ」
基本的にPPPoEインターフェイス側に転送したいポリシールートの場合は設定しません。
通常接続でWAN側デフォルトゲートウェイ以外のWAN側ルータに転送したい場合は、ここに転送先ゲートウェイアドレスを設定してください。
また、LANインターフェイス側に転送したいポリシールートの場合も、ここに転送先ゲートウェイアドレスを設定してください。

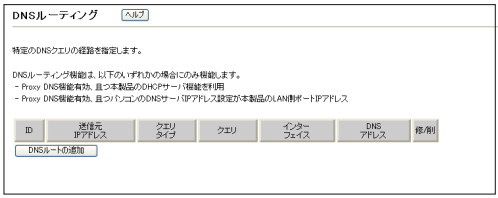
「インターフェイス」
上記パラメータで指定したトラフィックを出力するインターフェイスを指定します。「lan0」はプライマリLANネットワーク、「lan1」はセカンダリLANネットワークまたはDMZネットワークのインターフェイスを意味します。
PPPoEマルチセッションでのルーティングの場合は、主にセカンダリセッションのアカウント名を選択することになります。

5 DNSルーティング

●DNSルーティングとは？

本製品は、DNSルーティングという考え方を導入し、ポリシールーティングと同じように、「指定されたDNS問い合わせを、指定されたインターフェイスの、指定されたDNSサーバに転送する」という機能を持ちます。

DNSルーティングの機能は、主にPPPoEセカンダリセッションへのDNS問い合わせ転送と、ポリシールーティングとの連携によるセカンダリセッションへのルーティングを目的に実装しています。ただし、この機能を応用することで、特定のDNS問い合わせだけをLAN側に設置した自前のDNSサーバに転送したり、インターネット上の特定のDNSサーバに転送したりすることももちろん可能です。



「ID」

最高32個のDNSルートを設定することができます。IDが小さいDNSルートが優先されることに注意してください。

「送信元IPアドレス」

DNSルートを利用するLAN側ホストを限定したい場合は入力します。特に限定しない場合は「＊」を入力します。

「DNSクエリタイプ」

DNSクエリタイプを選択します。特に特殊な用途でない限り、すべて（ptr以外）を選択します。

「DNSクエリ」

どのようなURLにアクセスするかを決定します。DNSクエリタイプでptrを選択した場合を除き、ホスト名やドメイン名を入力します。ptrを選択した場合は、IPアドレスを入力します。

「インターフェイス」
転送先のDNSサーバがWAN側にある場合はそのアカウント名、プライマリLAN側にある場合は「lan0」、セカンダリLAN側にある場合は「lan1」を選択します。

「DNSアドレス」
セカンダリセッションのデフォルトDNSサーバなど、そのインターフェイス上のデフォルト（本製品自身が知っている）DNSサーバアドレスを利用する場合は入力する必要はありません。本製品が知らないDNSサーバを利用する場合は必ず入力します。

注意

・PPPoEマルチセッションを利用する場合やDNSルーティングを利用する場合は、必ずProxy DNS機能を利用してください。
Proxy DNS機能は、プライマリLANネットワークだけでなく、セカンダリLANネットワーク（DMZ除く）に対しても機能します。したがって、プライマリLANネットワーク上のホストのDNSサーバアドレスはプライマリLAN IPアドレス、セカンダリLANネットワーク上のホストのDNSサーバアドレスはセカンダリLAN IPアドレスになります。

・セカンダリLANがDMZネットワークである（DMZネットワークを利用している）場合、セカンダリLAN IPアドレスはProxy DNSとして機能しません。したがって、DMZネットワーク上のホストは、DNSルーティング機能を利用することはできません。

・本製品のDHCPサーバ機能はプライマリLANネットワークのみ有効です。したがってセカンダリLANネットワーク上のホストのIPアドレス設定、DNSサーバアドレス設定は手動で行う必要があります。

・DNSルーティングとポリシールーティングの連携を使ってPPPoEマルチセッションを利用する場合、本製品は、当該DNSルートに基づいたDNS問い合わせの転送を行い、さらにそれにより解決されたIPアドレスをポリシールートの送信先IPアドレスとして一時的にルーティングテーブルに追加します。ここで追加されるルートは一時的なものであり、本製品の電源断・再起動・ファームウェア更新作業などを行うと消去されてしまいます。
一方、パソコンには「DNSキャッシュ」という仕組みがあり、解決後のIPアドレスをパソコン内に保存（キャッシュ）しておくことで、同じDNS問い合わせを極力減らすようになっています。
快適にPPPoEマルチセッションを行っていても、本製品の電源入れ直し・再起動・ファームウェア更新作業などを行うと、本製品に記憶されていたアドレスが消去されるにもかかわらず、パソコンにはDNSキャッシュが存在することになり、正常なPPPoEマルチセッションが行えない状態になります。（これは、DNSルーティングとポリシールーティングの連携を使っている場合にのみ発生します。）
こうした現象を防ぐには、本製品の電源入れ直し・再起動・ファームウェア更新作業などの後、起動していたパソコンで以下の作業を行ってください。

・Windows XP/2003/2000/NT4.0/NT3.51の場合
コマンドプロンプト上で以下のコマンドを実行する。またはパソコンを再起動する。
ipconfig /flushdns

・その他のOSの場合
パソコンを再起動する。

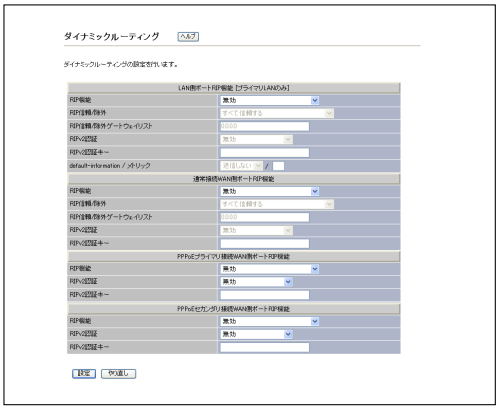
6 ルーティング

●ダイナミックルーティング

本製品では、LAN側ポート（プライマリLAN）と通常接続時のWAN側ポート、PPPoEプライマリセッション時のWAN側ポート、PPPoEセカンダリセッション時のWAN側ポートのRIP機能設定が行えます。

RIP（Routing Information Protocol）またはRIPv2を利用して、他のルータからの経路情報の受信（Listen）や、他のルータ（RIP Listener）に対する経路情報の広告（Advertise）を行う場合は、RIP機能を利用します。

RIPv2の認証機構を利用する場合は、RIPv2認証機能とRIPv2認証キーを設定してください。RIPv2認証キーを設定すると、RIP受信の際には受信RIPv2パケットのうち一致する認証キーを持つものだけを信頼し、RIP広告の際には本製品からの経路情報広告パケットに認証キーが埋め込まれます。

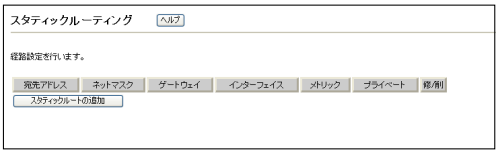


注意

RIPv2の認証機構は、権限（キー）を持たない近隣ゲートウェイによるルーティングテーブルの破壊を防止するためにあります。しかし、RIPv2パケット中のキーデータやルート情報は暗号化されているわけではなく平文で送受信されるため、完全ではありません。
RIPv2の認証機構を利用した場合、本製品は、設定されたRIPv2認証キーと一致しないRIP広告を無視します。したがって、ルート情報を交換したい近隣ルータにも同一キーを設定する必要があります。
通常、PPPoE接続ではRIPは使用しません。

●スタティックルーティング

本製品に対し、新たに経路（ルート）を追加したい場合には、スタティックルーティング機能を利用します。本製品には最大30のスタティックルートを設定することができ、任意のスタティックルートをRIP機能によって広告することも可能です。
ここではスタティックルーティングの一覧を「スタティックルーティングテーブル」、個別のスタティックルーティングのエントリを「（スタティック）ルート」と呼びます。



注意

・スタティックルーティング/ダイナミックルーティングの利用には、以下のような注意事項があります。

・通常のブロードバンド利用では、特に必要の無い限りスタティックルーティング機能やダイナミックルーティング機能を設定する必要はありません。また、スタティックルーティングは本製品の経路情報（ルーティングテーブル）に直接影響がある機能ですので慎重に設定を行ってください。

・本製品のWAN側ポート（インターフェイス）は、常にデフォルトルートとなっています。したがって特に必要の無い限り、WAN側に存在するネットワークへの経路をスタティックルートとして登録する必要はありません。WAN側に存在するネットワークへの経路をRIP広告（[プライベート]を「No」にする場合）したい場合などに限り、WAN側に存在するネットワークへの経路をスタティックルートとして登録してください。

・RIPv1とRIPv2を同時に利用することはできません。どちらか一方のみ利用することができます。

・RIPv2では、マルチキャストのみサポートします。RIPv2ブロードキャストパケットの広告/受信はサポートしていません。

・RIPv2認証で「Hexキー認証」を設定する場合、RIPv2の認証機構では最高16オクテットの認証文字列が許可されていますので、キーデータ1オクテットずつを16進表記、最高32個の数字を空白なしで入力してください。奇数個では正常に動作しません。また、16文字より少ないキーを設定すると、設定画面上で0（padding）が表示されます。
default-information広告機能は通常設定する必要はありません。LAN側にフローティングスタティックルーティングをサポートするルータがある場合など、本製品からのdefault-informationの広告が必要な場合に限り設定してください。
default-information広告機能では、宛先ネットワーク 0.0.0.0/0、ゲートウェイ 0.0.0.0（自ルータ）の経路を広告します。メトリックは2から15までの任意の数字を入力してください。

7 静的フィルタ

●静的フィルタとは？

静的フィルタとは、本製品に入ってくるパケットのヘッダ情報を元に、あらかじめ決めたルールにしたがってそのパケットを処理（通過させる・破棄する）する機能です。本製品は各WAN接続、プライマリLAN（lan0）、セカンダリLAN（lan1）間のそれぞれの方向で静的フィルタを設定することができます（10方向）。

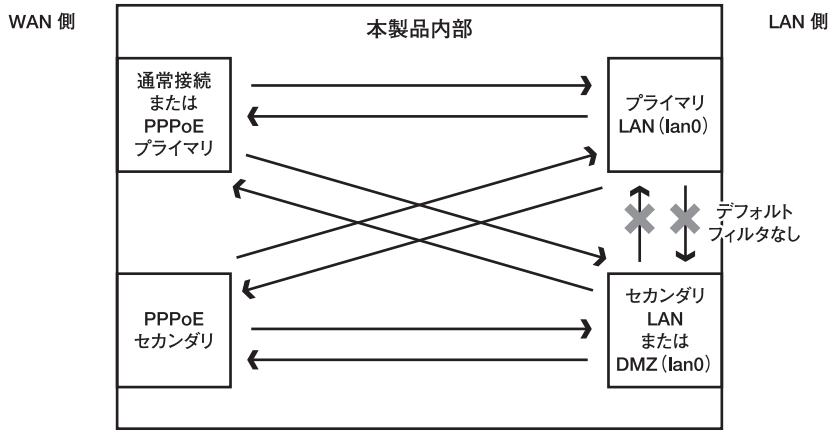


図5-3

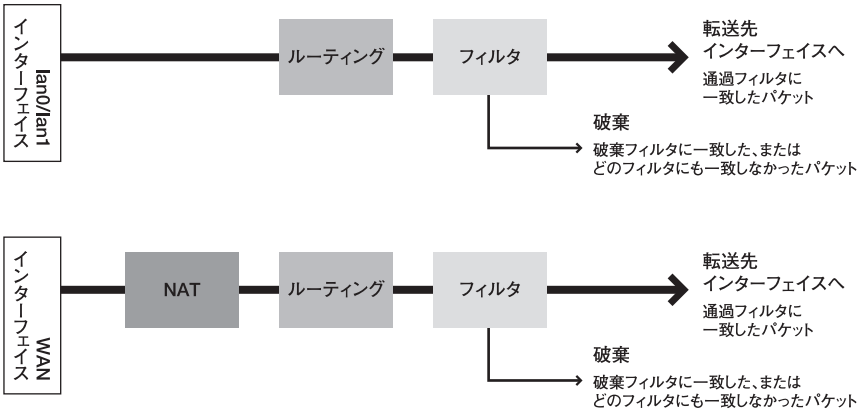


図5-4

●実際の動作

本製品内部で静的フィルタが機能する部分は、ルーティング（ポリシールーティングも含む）の後です。ただしNAPT機能が有効の場合にWAN側から入ってくるパケットに関しては、NAPT - ルーティング - 静的フィルタの順となります。したがって、NAPT有効時のフィルタは、NAPT変換前（LAN側からのパケット）またはNAPT変換後（WAN側からのパケット）のヘッダ情報を念頭において、フィルタを作成する必要があります。

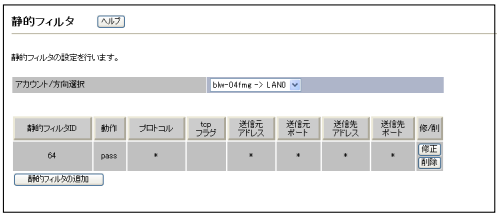
●設定例

ここでは、LAN側からWAN側へのtcpとudp両方の135番から139番までのフィルタを例に、静的フィルタ設定を順を追って説明します。（これらはWindowsのNetBIOSで利用されるポートで、主にLAN内での通信に使われます。）

1. 設定画面を開きます。

2. サイドメニューから、「セキュリティ」-「静的フィルタ」をクリックします。

3. 静的フィルタ設定画面が表示されます。



4.「アカウント/方向選択」で設定したいフィルタが対象とするパケットの方向を選択します。
ここではLANからWANへ出て行くパケットが対象ですので、「lan0 ->アカウント名」を選択します。

5.［静的フィルタの追加］ボタンをクリックします。

6.「静的フィルタ追加/修正」画面が表示されるので以下の各項目を入力します。

「静的フィルタID」
設定したい静的フィルタのエントリに、番号を付けます。適当な番号を選んでください。

「動作」
「破棄」を選択します。

「プロトコル」
設定したい静的フィルタはtcp/udp両方が対象ですので、「tcp&udp」を選択します。

「tcpフラグチェック」
tcpのフラグチェックは不要ですので、「tcpフラグチェックしない」を選択します。

「送信元IPアドレス」
必要ならば送信元となるLAN側のIPアドレスを入力しますが、ここでは特に送信元は限定しませんので、「＊」を入力します。

「送信元ポート」
特に限定しませんので、「＊」を選択します。

「送信先IPアドレス」
特に限定しませんので、「＊」を入力します。

「送信先ポート」
送信先ポートとして、「135-139」と入力します。

7. 入力内容を確認して「設定」ボタンをクリックして、設定を終了します。

8 ダイナミックフィルタ

●ダイナミックフィルタとは

静的フィルタは、あくまでも静的なものです。通過を指定したフィルタは常に対象パケットを通過させ、破棄を指定したフィルタは常に対象パケットを破棄します。これに対しダイナミックフィルタは、「指定したパケットが検出された時に、指定されたパケットを通す」という動作をします。このきっかけになるフィルタを「トリガ」、トリガによって通過を許可されるフィルタを「アクション」と呼びます。

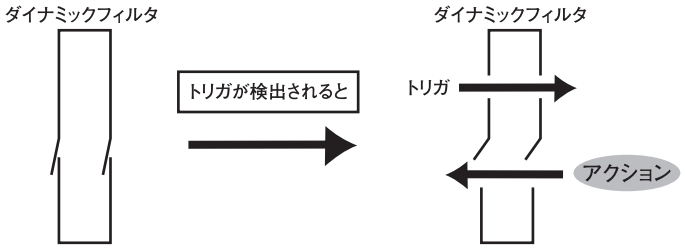


図5-5

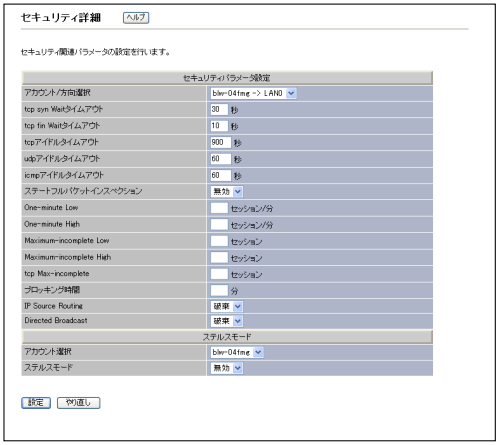
注意

ダイナミックフィルタ機能を利用には、以下の注意事項があります。

- ***ダイナミックフィルタは、静的フィルタより常に優先されます。したがってたとえ重複する静的フィルタが存在していたとしてもトリガ対象パケットは常に通過しトリガ検出時にアクション対象パケットは通過します。***
- ***NAPT有効時にWAN側からLAN側へのトリガを設定するには、同じ内容の静的マスカレードを設定しない限り、トリガ対象パケットはNAPTを超えることができません。必ず設定してください。***
- ***NAPT有効時に、WAN側からLAN側へのアクションを設定する場所は、静的マスカレードを設定する必要はありません。***

9 セキュリティ詳細

「セキュリティ詳細」では、パケットの転送や破棄に関連する本製品の詳細なパラメータの設定を行います。
通常の使用では特に変更する必要はありません。



●ステートフルパケットインスペクションとは

本製品のステートフルパケットインスペクション機能では、本製品を通過するそれぞれのコネクションをリアルタイムで監視し、その状態をステートテーブルに一時的に記憶するとともに、次に来るパケットを予測します。実際に来たパケットがその予測と一致する場合は通過を許可し、一致しない場合は破棄しすることで、単純なパケットフィルタより厳しいファイアウォール機能を実現しています。

tcp通信の場合

tcpコネクションの通信の場合、本製品は各コネクションの、送信元IPアドレス、送信先IPアドレス、送信元ポート、送信先ポート、tcpフラグ、tcpシーケンス番号、tcpコネクション状態、FTPの場合はftp dataの状態、をステートテーブルに記憶し、これらの状態情報から推測される受信パケットと、実際の受信パケットのタイプが異なる場合、そのパケットを不正なものと判断し破棄します。

コネクションレス型通信の場合
通信の状態という概念が存在しない、udpやicmpのようなコネクションレス型通信の場合でも、本製品は仮想的なコネクションと位置付け、送信元IPアドレス、送信先IPアドレス、送信元ポート、送信先ポート、icmpの場合はシーケンス番号、などをステートテーブルに記憶し、これらの状態情報から推測される受信パケットと、実際の受信パケットのタイプが異なる場合、そのパケットを不正なものと判断し破棄します。

さらに本製品のステートフルパケットインスペクション機能は、half-openセッション（establish状態に移行していないtcpセッションや、一定時間応答パケットが検出されないudp仮想セッション）の総数を監視しており、half-openセッション数が設定値を超えた場合、新規セッション要求が設定値を超えた場合、同一送信先IPアドレスに対するtcp halh-openセッション数が設定値を超えた場合などに、既存のhalf-openセッションの削除を行ったり、新規tcpセッション要求を拒否したりすることができます。

●攻撃検知機能
ステートフルパケットインスペクション機能に加え、本製品はインターネット側からの攻撃パケットやスキャンパケットを検出し、そのパケットを破棄した上で、syslogやE-mailログを介してユーザに警告を発することができます。

・攻撃通知一覧
「Ping of Death」「TearDrop / Bonk / Boink」「Syn flood」「Icmp flood」「LAND attack」「smurf」「異常tcpパケット」
「IP Spoofing」「Syn Fin scan」「Fin Stealth scan」「Vecna scan」「Nmap Xmas scan」「Full Xmas scan」「Null scan」

注意

・ステートフルパケットインスペクションを利用するためには、［セキュリティ詳細］で［ステートフルパケットインスペクション］を「有効」にする必要があります。

・攻撃検知機能は、常に有効になっています。本製品への設定は特に必要ありません。

・検知した攻撃パケットや異常なパケットは、自動的に破棄されます。検知したことをログ出力したい場合は、syslog機能またはE-mailログ機能を利用してください。

・本製品のステートフルパケットインスペクションや攻撃検知機能は、必ずしもすべての攻撃パケットや異常なパケットを検出することができるわけではありません。

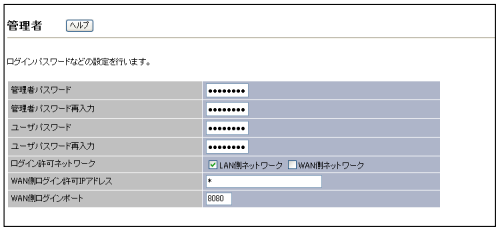
・不特定多数との通信を行うようなP2P（peer to peer）ネットワークアプリケーションを長時間利用する場合や、非常に多くのアクセスがあるインターネットサーバを静的マスカレードやDMZネットワーク機能で公開する場合、SPI機能が有効では、一定数以上の新規セッションが阻害されることがあります。このような場合はSPI機能を無効にしてください。

10 管理者設定・WAN側MACアドレス

「管理者」の項目では、本製品設定画面へのアクセスに関する設定を行います。

●管理者

本製品へのログインパスワードやログイン許可範囲などを設定します。



●WWWサービス制限

インターネットサイト上のActive X、Java、Cookie、Proxyに関し、LAN側ホストより利用を制限することができます。

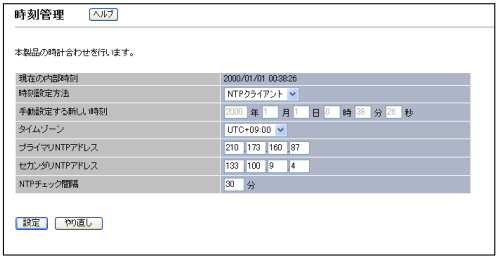
●MACアドレス

本製品のWAN側ポートMACアドレスの確認/変更を行います。
通常は変更する必要はありませんが、プロバイダによってはインターネットに接続するコンピュータのMACアドレスを事前に登録するタイプのものがあります。この場合、登録しているMACアドレスを本製品に設定することで解消することができます。

＊本製品のMACアドレスは、本体底面に表記されています。

11 時刻設定

［時刻管理］では、ログ機能などで用いる、本製品内部時計の時刻合わせに関する設定を行います。



5 詳細設定

注意

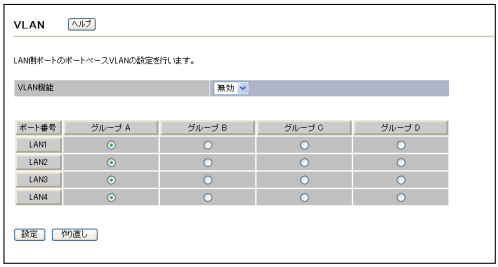
・工場出荷時値のNTPサーバ「210.173.160.87」は、独立行政法人通信総合研究所とNTT、IIJ、インターネットマルチフィードが公開している試行サービスのNTPサーバ「ntp3.jst.mfeed.ad.jp」です。
（参考：http://www.jst.mfeed.ad.jp/）

・工場出荷時値のNTPサーバ「133.100.9.4」は、福岡大学情報工学科情報アーキテクチャ部門が公開しているNTPサーバ「drake.nc.fukuoka-u.ac.jp」です。
（参考：http://www.fukuoka-u.ac.jp/）

・公開NTPサーバサービスは、利用者責任でご利用ください。サービスの停止、欠陥、及びそれらが原因となり発生した損失については、弊社およびサービス提供者は一切責任を負いません。

12 VLAN

本製品のLAN側スイッチングハブはポートベースVLAN機能を持っています。これは相互通信を許可するポート間でグループを作り、異なるグループとの通信を完全に遮断する機能です。本製品のLAN側ポートは最高4つのVLANグループに分割できます（4グループの場合は全ポート独立）。



注意

LAN側ポートをVLANで分割してもそれぞれのポートに接続されたホストと本製品との通信は可能です。したがって、VLANでLANポート間通信を遮断しつつ、ブロードバンド接続を行うことができます。

VLANで遮断していても、本製品のルーティングによりプライマリLANネットワークとセカンダリLAN（DMZ）ネットワークのルーティングは潜在的に可能です（デフォルトでは通過フィルタを設定していないので不可）。完全に遮断したい場合は、lan0とlan1間のフィルタが何も設定されていないことを確認しておいてください。フィルタエントリが存在しない場合、すべてのパケットは破棄されます。

13 ログ

［ログ］では、ログ機能を使った本製品の状態確認に関する設定を行います。
ログ機能により本製品の状態は、以下の3種類の方法で把握することができます。

・syslog機能
syslogとは、syslogメッセージ（ログ）をネットワーク上に設置されているsyslogデーモン（サーバ）に対して出力する機能です。syslogデーモン側でファイルを保存しておくことができ、長期間のログ収集に適しています。
本製品のsyslog機能を利用するためには、別途syslogデーモン（サーバ）を用意することが必要です。
（フリーソフトウェアも公開されています）

・メールによるログ配信機能
本製品では、指定したアドレスへのメールによるログ配信も可能です。ログ配信には毎日決まった時間に行う、DoS攻撃検出時、メモリー杯時に配信する、から選択できます。

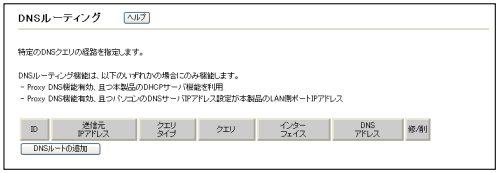
・設定画面でのログ表示
ブラウザ設定画面上でログを確認することができます。

ログ情報は、以下5種類の情報が出力されます。
・PPPoE接続関連情報
・DHCP接続関連情報
・NTP関連
・DNS関連
・フィルタリング関連

14 モニタ

●セッションモニタ

［セッションモニタ］では、NAPTの状態を確認できます。（設定を必要とする項目はありません）



「アクティブNAPTセッション数」

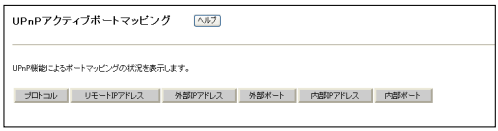
このページを開いた時点でのNAPTテーブルにより管理されている、NAPTセッションの数を表示します。多ければ多いほど、本製品の全体的なパフォーマンスは低下します。

「アクティブダイナミックフィルタ数」

このページを開いた時点で、アクションが発動しているダイナミックフィルタの数を表示します。

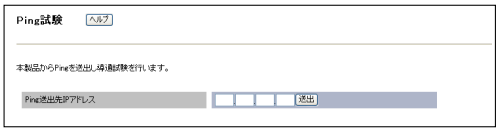
●UPnPアクティブポートマッピング

UPnPを使って、Control Point（パソコン上のUPnPソフトなど）からの要求により動的に追加されたポートマッピングの状態を表示します。



●Ping試験

本製品から特定のIPアドレスに対して、Pingを送信し、その応答を確認することができます。



15 ダイナミックDNS

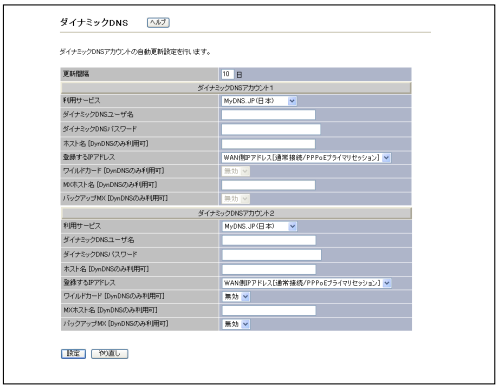
●ダイナミックDNSとは？

通常のブロードバンドサービスは、接続の度にWAN側グローバルIPアドレスが変化（動的IPアドレス割り当て）してしまいます。これではせっかくインターネットサーバなどを公開しても、そのサーバにアクセスしたい人たちが最新のIPアドレスを知っておく必要があり、不特定多数への情報発信には適しません。

この問題を解消するひとつの手段として、複数のサービス事業者から提供されているダイナミックDNSサービスを利用します。ダイナミックDNSサービスユーザは自分専用のドメイン名（ホスト名）を持つことができ、そのアドレス解決をサービス事業者のDNSサービスが請け負います。

たとえば、「BLW-04FMG.dyndns.org（仮）」というドメイン名を取得していると仮定します。

本製品は、WAN側グローバルIPアドレスに変更が発生すると、このダイナミックDNSアカウントの登録IPアドレス更新処理を自動的にDNSサービスへ行います。これにより、公開するURL「http://BLW-04FMG.dyndns.org」は常に、本製品のWAN側グローバルIPアドレスと関連しているので、ユーザはこのURLに問い合わせを行えば、公開されているサーバにアクセスできるようになります。



●対応ダイナミックDNSサービス
本製品のダイナミックDNSアカウント更新機能が対応するサービスは、次の3つのサービスです。

・MyDNS.JP
株式会社ウェブコミュニケーションズ（BiG-NET）が運営しているダイナミックDNSサービス（無料）です。サービスの詳細は、http://www.mydns.jp/ を参照してください。

・DynamicDO!.jp
フルカワ・システム・デザインが運営しているダイナミックDNSサービス（無料）です。サービスの詳細は、http://ddo.jp/ をご覧ください。

・DynDNS.org
Dynamic DNS Network Services, LLCが運営している、国内外を問わず最も有名なダイナミックDNSサービス（無料）です。サービスの詳細は、http://www.dyndns.org/ をご覧ください。

⚠ 注意

・本製品のダイナミックDNSアカウント更新機能は、以下のタイミングでに、設定されているダイナミックDNSアカウントの登録IPアドレスを更新します。
通常接続（DHCPクライアント）の場合、WAN側DHCPサーバからIPアドレスを取得した時
通常接続（固定IPアドレス）の場合、WAN側ポートのリンクが確立された時
PPPoE接続の場合、IPCPでIPアドレスを取得した場合
同一WAN側IPアドレスの利用期間が［更新間隔］で設定された日数に達した時
・ダイナミックDNSアカウント更新機能を設定、または設定変更した後は、［アカウント管理］画面上でインターネット接続を一旦切断し、再度接続してください。PPPoE接続の場合は［切断］-［接続］、DHCP接続の場合は［開放］-［更新］を行います。
ほとんどすべての無料ダイナミックDNSサービスでは、最後の更新から長期間（3週間程度）経過すると、そのダイナミックDNSアカウントが無効または削除されます。これを防ぐため、［更新間隔］設定では、最後のダイナミックDNSアカウント更新から指定した期間（日単位）、WAN側ポートIPアドレスが変化しなかった場合に、再度同じIPアドレスでダイナミックDNSアカウントを更新します。ただし、ダイナミックDNSサービスによっては、頻繁な更新を拒否することがありますので、［更新間隔］には10日前後の値を設定してください。

16 ファームウェアの更新・設定情報の保存

［更新/設定情報］では、ファームウェアの更新、設定情報の保存と読み込み、設定の初期化などを行います。

●ファームウェア更新

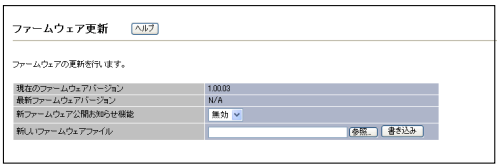
現在のファームウェアバージョンの確認、公開されているファームウェアバージョンの確認、ファームウェアの更新を行います。

・新ファームウェア公開お知らせメール機能

新ファームウェア公開お知らせ機能を利用すると、本製品向けの新しいファームウェアが公開された時に、設定されたメールアドレス宛にお知らせメールが届きます。1日に1回、本製品が弊社サーバにアクセスし、そのとき公開されている最新のファームウェアバージョンを取得します。そのバージョン番号が本製品のファームウェアより新しい場合、本製品自身が設定されたメールアドレス宛（ログ機能の「送信先メールアドレス」）にお知らせメールを送信します。

・ファームウェア更新

本製品を制御しているファームウェアについて、機能追加や仕様変更などの目的で弊社ホームページ上で改良版ファームウェアが公開されます。これをダウンロードして、この「ファームウェアの更新」機能と使ってアップデートすることで本製品の機能追加などがなされます。



注意

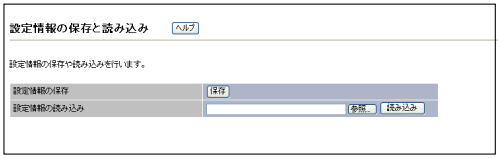
・本製品は1日に1回、最新ファームウェアバージョンをチェックします。
チェックのタイミングによっては、新ファームウェア公開後最長で2日程度経過してから、<最新ファームウェアバージョン>が更新されます。
ファームウェアの書き換えの際しては、ファームウェアファイルに添付されている「リリースノート」、「アップデート手順書」、「ソフトウェア使用許諾契約書」などの文書をよく読んでください。

・ファームウェア書き換え中、本製品のStatus LEDが赤色に点滅し続け、書き換え終了後、自動的に再起動します。完了するまでに40秒から60秒ほど時間がかかりますが、その間不要な操作は行わないでください。
ファームウェアの書き換え作業中、本製品およびコンピュータの電源を切ったり、ネットワークケーブルを抜いたりしないでください。
ファームウェアの書き換えが正常に終了したにもかかわらず、正常な通信が行えない場合は、1章「6. 設定の初期化」を参照し、リセットスイッチを使って本製品の設定を初期状態に戻したあと、再度設定を行ってください。

・ファームウェアの書き換えを行った後も、基本的に以前の設定内容は保持されたままの状態で新しい更新が適用されます。
ただし、より安全を期すために、ファームウェアの書き換え後、WWWブラウザ設定画面上、またはリセットスイッチを使って、一旦本製品の設定を初期化し、再度設定し直すことをお勧めします。

●設定情報の保存と読み込み

現在の設定を保存したり、保存しておいた設定ファイルを読み込んだりします。

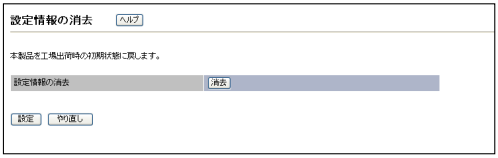


注意

設定情報ファイルには、それを保存したときの本製品のLAN側IPアドレスや、WWW設定画面ログインパスワードも格納されています。以前保存した設定情報ファイルを読み込むと、LAN側IPアドレスやログインパスワードも設定情報ファイルの内容に基づいて書き換わりますので注意してください。
異なるファームウェアバージョン間では、設定情報ファイルは互換性を持ちません。

●設定情報の消去

現在の設定を完全に消去し、工場出荷時の状態に初期化します。



注意

製品の設定を消去すると、本製品のLAN側IPアドレスが［192.168.1.1］に初期化されることに注意してください。
LAN側ホストがDHCPクライアントである場合は、LAN側ホストを再起動するなどして、本製品のDHCPサーバ機能からIPアドレスを取得し直す必要があります。LAN側ホストのIPアドレスを固定設定していた場合は、LAN側ホストのIP設定を変更する必要があります。

無線設定

本章では本製品の無線LANアクセスポイント機能を使用する方法について説明します。

1 無線LANアクセスポイントについて

本製品は無線ネットワークと既存の有線部イーサネットネットワークとを接続にするためのアクセスポイントとして機能します。
本製品を使用することで既存のイーサネットネットワーク資産を利用した無線ネットワークをシームレスに構築することが可能です。本製品はIEEE802.11およびIEEE802.11b/gに準拠し、伝送速度は54/48/36/24/18/12/11/9/6/5.5/2/1Mbpsに対応しています。
またSSIDやWEP、MACアドレスフィルタリングなどに加え、SSID隠蔽モードを使用することで、第三者からの無断接続を防ぎ堅牢なセキュリティを保つことができます。

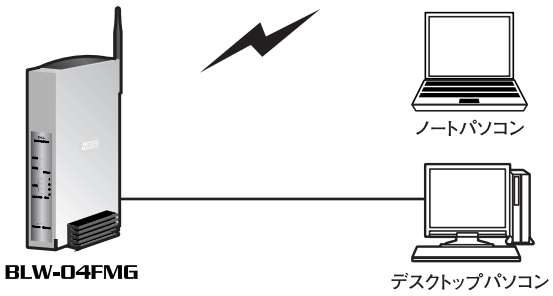


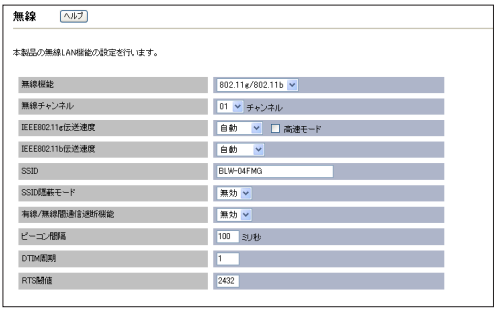
図6-1

2 無線設定

本製品の無線設定について説明します。
無線設定を行うにはWEB設定画面左側のメニューから「無線LAN」－「無線」をクリックします。

●無線

無線設定を行う画面が表示されます。本製品の基本的な無線通信の設定を行います。



「無線機能」

本製品は、無線LAN規格IEEE802.11b/IEEE802.11gに対応しています。
通常は「802.11g/802.11b」モードを使うことで11g/11bの両方の無線通信を同時に行うことができます。11g方式しか使用しない場合は「802.11g（54Mbps）」を選択し、11b方式しか使用しない場合は「802.11b（11Mbs）」を選択してください。
無線機能を使用しない場合は「無効」を選択してください。

「無線チャンネル」

無線機能で使用するチャンネルを1～13までで選択してください。

「IEEE802.11g伝送速度」
802.11gで使用する伝送速度を54/48/36/24/18/12/9/6Mbps、自動から選択します。
自動を選択することで、電波状況に応じて常に最適な伝送速度が自動的に設定されます。（自動を推奨）

「IEEE802.11b伝送速度」
802.11bで使用する伝送速度を11/5.5/2/1Mbps、自動から選択します。
自動を選択することで、電波状況に応じて常に最適な伝送速度が自動的に設定されます。（自動を推奨）

「SSID」
無線LANアクセスポイントを識別するための名前になります。
SSIDを設定する事により無線LANグループが作成され、同じSSIDをもつ無線クライアントのみが本製品と通信を行う事ができます。

「SSID隠蔽モード」
SSIDを隠す（公開しない）ことにより、他の無線クライアントがAP検索やサイトサーベイを行っても本製品を検知できません。これにより、SSIDを予め知ってる人だけが本製品と通信ができ、第三者からの無断接続を防ぎます。

「有線/無線間通信遮断機能」
有線クライアントと無線クライアント間の通信を遮断します。

「ビーコン間隔」
本製品から送信するビーコンの間隔を設定します。

「DTIM値」
本製品から送信されるビーコンにDTIMを含める周期を設定します。

「RTS閾値」
RTS閾値で指定したサイズ以上のパケットを送信するときに、RTS（送信要求）パケットを送信します。多くのクライアントが一つのアクセスポイントに集中した場合、相互に認識されない状態（かくれ端末）になる事があります。この場合は、RTS閾値を小さくする事で改善されます。

●暗号化-WEP

本製品のWEP設定を行います。

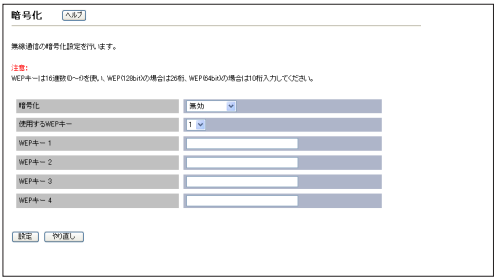
WEP機能は無線通信を暗号化することで、暗号化の設定が一致しない無線クライアントや暗号化されてない無線クライアントとの接続を防ぎます。

暗号化を行う場合は、本製品と通信する全ての無線クライアントに同様の設定を行ってください。

WPAで暗号化する方法は、「暗号化－WPA」を参照してください。

ご注意：

セキュリティの無効は、無線LANの通信傍受、不正利用、情報漏洩、データの改ざんなどが行える非常に危険な状態となり、ネットワーク全体の安全性が損なわれる恐れがあります。お客さまの利益を守るためにも、セキュリティは必ず設定してご利用ください。



「暗号化」

＜無効＞　　暗号化を行いません。

＜WEP（64bit）＞　　64bitのWEPによる暗号化を行います。

＜WEP（128bit）＞　　128bitのWEPによる暗号化を行います。

「使用するWEPキー」

暗号化の際に使用するデフォルトキーを選択します。

暗号化を行う場合は、本製品と無線クライアントの"使用するWEPキー"の番号とその番号の"WEPキー"を一致させるよう注意してください。

「WEPキー１～４」

暗号化でWEP（64bit）またはWEP（128bit）を選択した場合に、暗号化で使用するWEPキーを入力します。4つのWEPキー欄全てに任意の16進数を入力します。

＜暗号化でWEP（128bit）を選択した場合＞

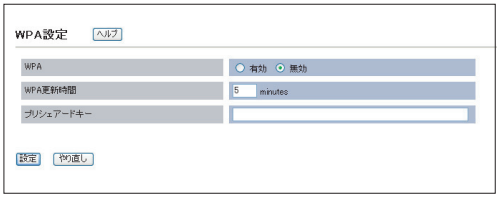
16進数（0～9、A～F）で26桁のWEPキーを入力します。

＜暗号化でWEP（64bit）を選択した場合＞

16進数（0～9、A～F）で10桁のWEPキーを入力します。

● 暗号化－WPA

WPA暗号化設定を行います。本製品は、プリシェアードキーを設定するPSK方式に対応しています。
一定時間ごとにキーを更新して通信します。
WPAで暗号化するときは、WPA設定を選びます。
※WPA設定と、暗号化-WEP設定は、同時に有効にすることはできません。



「WPA」
「有効」、または「無効」を選びます。WPAでの暗号化を有効にします。

「WPA更新時間」
キー更新の間隔を設定します。単位は分です。

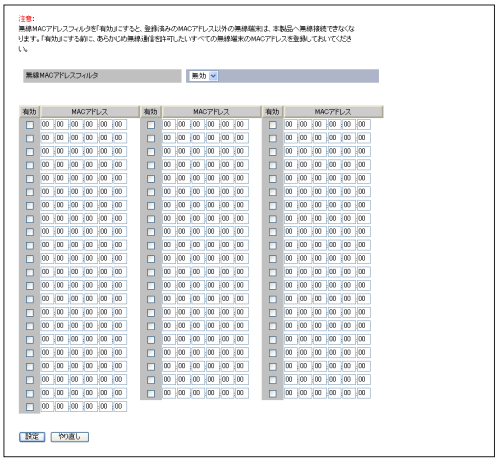
「プリシェアードキー」
プリシェアードキーを設定します。このキーによって認証します。

	入力可能文字	入力可能文字数
ASCII	半角英数文字	8～63
HEX（16進法）	0～9、a～f、A～F	64

以上で無線設定は終了です。
入力内容を確認し、間違いがなければ「設定」ボタンをクリックしてください。
画面の指示に従って進んでください、再起動のメッセージが表示されましたら「OK」ボタンをクリックし再起動します。
設定は再起動後、有効になります。

3 無線MACアドレスフィルタリング

本製品の無線通信で使用するMACアドレスフィルタリングを設定します。
無線MACアドレスフィルタリングを行うにはWEB設定画面左側のメニューから「無線LAN」－「無線MACアドレスフィルタリング」をクリックします。
本製品の無線MACアドレスフィルタリングは無線クライアントのみ有効です。



本製品に無線MACアドレスフィルタリングを登録すると、登録済みのMACアドレス以外の無線クライアントは本製品に無線接続できなくなります。

「無線MACアドレスフィルタリング」
＜無効＞　　無線MACアドレスフィルタリングを無効にします。
＜有効＞　　無線MACアドレスフィルタリングを有効にします。

「MACアドレス」
無線MACアドレスフィルタリングを有効にしたときに、無線通信を許可したい、全ての無線クライアントのMACアドレスを登録してください。

「有効」
登録したMACアドレスフィルタリングを有効にするとき、チェックボックスにチェックを入れます。MACアドレスを登録していても、このチェックが外れている場合はそのMACアドレスを持つ無線クライアントは本製品と通信ができません。

以上で無線MACアドレスフィルタリングの設定は終了です。
入力内容を確認し、間違いが無ければ「設定」ボタンをクリックしてください。
画面の指示に従って進んでください、再起動のメッセージが表示されましたら「OK」ボタンをクリックし再起動します。
設定は再起動後、有効になります。

ネットワークQ&A

1 ブロードバンドルータの色々な「?」について

インターネットの急速な普及により、ブロードバンドルータ（以下、ＢＢルータ）を使用する場面が増えてきました。特に多く寄せられる、LAN全般や弊社製品を使用する際にぶつかる疑問点についていくつかまとめてみました。
ネットワークはよく解らない…という方は是非ご一読ください。弊社製品に対する理解を深められることでしょう。

Q BBルータの設定は接続するコンピュータに対して全部で行うのですか？

A　いいえ

複数台接続している環境であっても、いずれか1台のコンピュータからBBルータの設定を行うだけで完了します。

補足

設定作業を行った1台でBBルータを介してインターネットにアクセスできるようになっていれば、その時点でBBルータの設定は完了したことになります。他のコンピュータから同じように設定を行う必要はありません。
例えば、2台のコンピュータのうち、1台はインターネットにアクセスできるが、もう1台はアクセスできないという場合は、BBルータではなくコンピュータ側に問題があることが考えられます。

Q インターネットに接続できないのに、どうやって設定画面にアクセスするんですか？

A インターネットへの接続と関係なく設定画面にアクセスできます。

設定画面はBBルータの中にあります。BBルータの中に設定用のホームページが存在しアクセスすることで、BBルータの設定を行っているのです。
ですから、BBルータがインターネット（モデム）につながっていなくてもコンピュータは設定画面にアクセスすることができるのです。

Q「ブラウザ」ってなんですか？

A インターネット上のホームページ等を見るためのソフトです。

「インターネットエクスプローラ」や「ネットスケープ」等が代表的なソフトになります。

補足

BBルータのマニュアルでは「インターネットエクスプローラ」の画面が使われているので「ネットスケープではどうやって設定するんですか？」という質問も寄せられますが、例えば「yahoo」のホームページが「インターネットエクスプローラ」でも「ネットスケープ」でも見ることができるように、BBルータの設定画面も問題なく「ネットスケープ」で表示することができます。

Q IPアドレスってなんですか？

A TCP/IPプロトコルを使ったネットワークにおいて、コンピュータごとに割り当てられる個別の数字のことを言います。

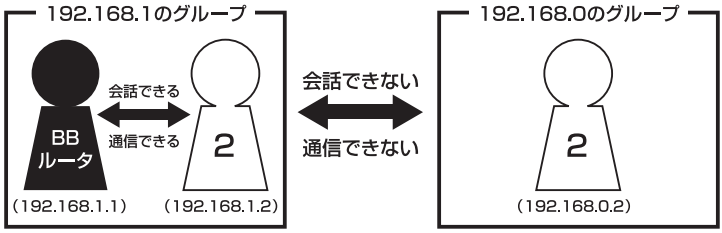
数字がちょっと変わるだけでアクセスできなくなったりする厄介なイメージがあると思いますが、簡単に考えるなら「学校のクラスと出席番号」に置き換えて考えると判り易いかと思います。

例えばA君とB君とC君がいて、A君とB君は「1-1」組でC君が「1-2」組の場合、A君とB君は同じ教室なのでいつでも話をすることができますが、C君は教室が別なのでA君達とは会えません。IPアドレスもほとんどそれと同じような理屈になっています。

実際のIPアドレスで例えるなら、BBルータのIPアドレスは出荷時には「192.168.1.1」というIPアドレスが設定されています。これは、BBルータ君は「192.168.1」組の出席番号「1」番という意味になります。このBBルータ君と話をするにはコンピュータも「192.168.1」組に入らないと教室が別になるので話ができません。

BBルータにアクセスするコンピュータのIPアドレスが「192.168.1.2」であれば「192.168.1」組の出席番号「2」番になるので、そのコンピュータはBBルータ君と話をすることができます。
もしコンピュータのIPアドレスが「192.168.0.2」だと、そのコンピュータは「192.168.0」組になるためBBルータ君とは教室が別になり、BBルータ君と話をすることができません。

つまり、BBルータにアクセスするにはコンピュータのIPアドレスが「192.168.1.**」という数字でなくてはならないのです。



上記の説明で「出席番号が同じになるとどうなるの？」という疑問を持った方もいると思います。
もし同じ出席番号の人が同じ教室に2人いたら混乱しますね？ ネットワークもそれと同じで、IPアドレスは重複してはいけないようになっています。
同じ番号のコンピュータが存在した場合、「その番号を使っている人が他にいますよ」という内容の警告メッセージがコンピュータ上に表示されます。

ここまで読んでいただいた方はもうお判りだと思いますが、IPアドレス「AA.BB.CC.DD」の3つ目（CC）までがネットワークのグループを表していて、最後の数字（DD）がコンピュータごとに設定される個別の数字ということになります。

補足

厳密にはもっと色々なルールがあるのですが、BBルータの設定画面にアクセスするには少なくとも上記レベルのルールが判っていれば、トラブルに遭った時の対処や問題の切り分けに役立つと思います。

2 設定画面

ここではBBルータの設定画面にうまくアクセスできない場合の主な確認点及び確認方法をまとめました。ご利用のコンピュータに該当する項目がないかチェックしてください。

Q 設定画面にアクセスできないのですが?

A LANランプ、IPアドレス、プロキシ、セキュリティソフトそれぞれの項目が正しく設定されていないとアクセスできません。もう一度設定を確認してみてください。
また、BBルータとの通信が正常に行われていない可能性もあります。これはpingというコマンドを使って確認することができます。

確認!

LANランプ

LANランプは点灯していますか?

コンピュータが接続されて正常に通信ができる状態になると「LINK」と言われるランプが点灯します。
BBルータには「LAN」「Link/Act」「LAN LINK」等の名称で呼ばれるランプがついていますので、そのランプが点灯しているか確認してください。(詳しくはマニュアル第1章 4の「各部の名称」をご覧ください)。

・点灯しない場合
ランプが点灯していない場合、BBルータとコンピュータは通信できる状態になっていませんので、設定画面にもアクセスできません。
いくつか原因は考えられますが、まずはケーブルを交換してみてください。
正常にランプが点灯しているポートで使用中の、他のケーブルを使って接続してみてください。
ケーブル交換の後、正常にランプが点灯するようであれば、交換前に使用していたケーブルに問題がある(断線やクロスケーブルなど)ということになります。

確認!

IPアドレス

IPアドレスが正しく取得できていますか?

アクセスできない場合は、取得しているIPアドレスを確認してください。
BBルータには「192.168.1.1」というIPアドレスが出荷時に設定されており、BBルータにアクセスするにはコンピュータが「192.168.1.**」というIPアドレスを取得している必要があります(最後の「**」には任意の数字が入ります)。
異なるIPアドレス(210.119.**.**等)を取得している場合はBBルータの設定画面にはアクセスできません。

・確認方法
主なOSでの確認方法は以下のようになりますので、取得しているIPアドレスの確認を行ってください。

Windows 95/98/MEの場合:
1.「スタート」→「ファイル名を指定して実行」を選択、「名前」→「WINIPCFG」と入力→「OK」をクリックしてください。

2.「IP設定」というウインドウが開きますので「アダプタアドレス」の上をご使用のLANカードに変更してください。

3.「IPアドレス」に「192.168.1.**」という数字が表示されることをご確認ください(**には任意の数字が入ります)。

Windows 2000/XPの場合:
1.「スタート」→「プログラム」→「アクセサリ」を開き、「コマンドプロンプト」を選択してください。

2.キーの入力待ちになりましたら「IPCONFIG」と入力し、Enterキーを押してください。

3.「IPアドレス」に「192.168.1.**」という数字が表示されることをご確認ください(**には任意の数字が入ります)。

Macintoshの場合:
1.アップルメニューから「コントロールパネル」→「TCP/IP」を開いてください。

2.「IPアドレス」に「192.168.1.**」という数字が表示されることをご確認ください(**には任意の数字が入ります)。

・まったく違うIPアドレスを取得している場合（Windowsのみ）

確認したIPアドレスが「192.168.1.**」ではなく、まったく違うIPアドレスを取得している場合、以下の方法で取得しているIPアドレスを開放して、再度IPアドレスを取得しなおすことができます。

Windows 95/98/MEの場合：

1.「スタート」→「ファイル名を指定して実行」を選択、「名前」→「WINIPCFG」と入力→「OK」をクリックしてください。

2.「IP設定」というウインドウが開きますので「アダプタアドレス」の上をご使用のLANカードに変更→「すべて開放」ボタンをクリックしてください。

3.「IPアドレス」が「0.0.0.0」になったのを確認してから「すべて書き換え」ボタンをクリックしてください。

4.「IPアドレス」に「192.168.1.**」という数字が表示されていれば正しく取得できたことになります（**には任意の数字が入ります）。

Windows 2000/XPの場合：

1.「スタート」→「プログラム」→「アクセサリ」を開き、「コマンドプロンプト」を選択してください。

2.キーの入力待ちになりましたら「IPCONFIG /RELEASE」と入力し、Enterキーを押してください。

3.再度「IPCONFIG / RENEW」と入力し、Enterキーを押してください。

4.「IPアドレス」に「192.168.1.**」という数字が表示されていれば、正しく取得できたことになります（**には任意の数字が入ります）。

確認!

ping

BBルータと正常に通信していますか？

・接続確認方法（Windowsのみ）
BBルータと通信できているかどうかは「ping」というコマンドで確認することができます。

Windows 95/98の場合：
1.「スタート」→「プログラム」→「MS-DOSプロンプト」を選択、「MS-DOSプロンプト」のウインドウが開きます。

2.ウインドウが開くとカーソルが点滅してコマンドの入力待ちになりますので「ping 192.168.1.1」と入力して、最後にEnterキーを押してください。

3.「Pinging 192.168.1.1 with・・・」というメッセージに続いて、その後連続4回同じメッセージが表示されると思います。
「Reply from　192.168.1.1・・・」というメッセージが返ってきていれば正常です。

Windows MEの場合：
1.「スタート」→「プログラム」→「アクセサリ」→「MS-DOSプロンプト」を選択、「MS-DOSプロンプト」のウインドウが開きます。

2.ウインドウが開くとカーソルが点滅してコマンドの入力待ちになりますので「ping 192.168.1.1」と入力して、最後にEnterキーを押してください。

3.「Pinging 192.168.1.1 with・・・」というメッセージに続いて、その後連続4回同じメッセージが表示されると思います。「Reply from　192.168.1.1・・・」というメッセージが返ってきていれば正常です。

Windows 2000/XPの場合：
1.「スタート」→「プログラム」→「アクセサリ」→「コマンドプロンプト」を選択、「コマンドプロンプト」のウインドウが開きます。

2.ウインドウが開くとカーソルが点滅してコマンドの入力待ちになりますので「ping 192.168.1.1」と入力して、最後にEnterキーを押してください。

3.「Pinging 192.168.1.1 with・・・」というメッセージに続いて、その後連続4回同じメッセージが表示されると思います。「Reply from　192.168.1.1・・・」というメッセージが返ってきていれば正常です。

・応答が「Request Timed Out」になる

「ping 192.168.1.1」と実行した時「Request Timed Out」と表示される場合は、IPアドレスが正しく取得できていないか、コンピュータのLANアダプタが正常に動作していない可能性が考えられます。

1. IPアドレスが正しく取得できているか確認してください。「IPアドレスが正しく取得できているか」に確認方法が記載されています。

2. LANアダプタが正常に動作しているか確認してください。確認方法はモデムに直接接続してインターネットにアクセスできれば正常です。

確認!

ブラウザのプロキシ（PROXY）設定

不要な設定をしていませんか？

ブラウザのプロキシになんらかの設定が行われていると、アドレスに指定された所に接続する前に、プロキシで設定した所に接続しようとしてしまうため、設定画面にアクセスできない場合があります。その場合は以下のような手順でプロキシの設定を解除してください。

インターネットエクスプローラの場合（5.0以降）：

1.メニューの「ツール」→「インターネットオプション」を選んでください。

2.「接続」タブをクリック→「LANの設定」ボタンをクリックしてください。

3.「自動設定」と「プロキシサーバ」のチェックボックスでチェックされている項目がありましたら、全ての項目のチェックを外してください。

4.「OK」ボタンをクリック→「ローカルエリアネットワークの設定」ウインドウを閉じてください。

5.再度「OK」ボタンをクリック→「インターネットオプション」ウインドウを閉じてください。

6.一度インターネットエクスプローラを終了させてから再度起動し、再度BBルータの設定画面にアクセスできるか試してください。

ネットスケープの場合：
1.メニューの「編集」→「設定」を選択してください。

2.「詳細」→「プロキシ」を選択、「インターネットに直接接続する」をチェックしてください。

3.「OK」ボタンをクリック→ウインドウを閉じてください。

4.一度ネットスケープを終了させてから再度起動し、再度BBルータの設定画面にアクセスできるか試してください。

セキュリティ関連ソフトの影響

ウイルスバスターやノートンアンチウイルス等、最近のウイルスチェックソフトには簡易ファイヤウォールという機能を搭載した物が増えています。

ファイヤウォールはアクセス許可をしていないIPアドレスからのパケット(通信)を遮断したりする機能です。

有効になっていると稀にBBルータとの接続時にファイヤウォール機能が働いて設定画面がうまく表示されない事や、設定内容を保存するとエラーになること等があります。
ウイルスチェックソフトやインターネットセキュリティソフトをご使用になられている場合は、それらのソフトを停止させてみてください。停止方法が判らない場合は、各ソフトウエアのマニュアルをご覧ください。

3 インターネットにアクセスできない

ここではBBルータの設定を行ってもインターネットへのアクセスができない場合の、主な確認点及び確認方法をまとめました。
接続方法別にまとめてありますので該当する項目がないかチェックしてください。
設定画面にアクセスができない場合は、112ページ「設定画面にアクセスできないのですが？」をご覧ください。

共通項目　事前確認編

どの接続方法にも共通する、最初に確認すべき点です。

Q 設定画面ではすべて正しく設定できたのですが、なぜインターネットにアクセスできないのでしょうか？

A BBルータが正しく接続されていないと通信が行われないので、インターネットにはアクセスできません。以下を確認してください。

確認!

WANランプ

WANランプは点灯していますか？

BBルータとモデムを接続して正常に通信ができる状態になると、BBルータの「WAN」のランプが点灯します。

・点灯しない場合

「WAN」のランプが点灯しない場合は、モデムと正常に接続していないことを表しますので、その状態ではインターネットに接続することができません。

本製品は「AutoMDI/MDI-X」に対応しているので、ケーブルの種類（ストレート/クロス）の違いは関係なくなります。
ポートにケーブルのコネクタが正しく挿さっているか再度確認してください。
それでも、点灯しない場合は使用しているLANケーブルを変えてみる必要があります。

接続設定フレッツ編

ここではNTT提供のフレッツ・ADSL、Bフレッツ等のようなフレッツ接続ツールを利用してインターネットにアクセスする場合の、インターネット接続に関する主な確認点をまとめました。
接続ツール等を使わない場合は117ページ「接続設定ケーブルTV、Yahoo!BB編」をご覧ください。

Q インターネットへの接続や切断はどうするの？

A BBルータが回線の状態を検知し、自動的に接続・切断を行います。

NTT「フレッツ」を利用されているほとんどの方が、NTTのフレッツ接続ツールを使ってインターネットに接続し､アクセスをやめる時は切断処理をしていたと思いますが、「BBルータを使う場合はどうやって接続するの？」という疑問をもたれる方もいると思います。

BBルータ使用の場合、コンピュータがインターネットへ接続しようとすると、そのコンピュータはBBルータに接続のための信号を送信します。
BBルータはその信号を受信すると、回線が切断状態の時には自動的に接続を開始します。そして、一定時間インターネットへの接続が発生しない場合、自動的に切断を行うようになっています。

つまり、ユーザーは接続や切断を意識することなく、インターネットへアクセスできるのです。

注意

上記の動作は出荷時の設定で使用した場合になります。設定内容によっては上記のような動作にならない場合もありますのでご注意ください。

Q 今までフレッツ接続ツールを使っていたのですが、BBルータを設置した場合にインターネット接続する時の確認点はなんですか?

A ユーザID、パスワード、PPPoE設定・接続、接続ツールなどです。

確認!

ユーザID、パスワード

ユーザIDとパスワードに間違いはないですか？

フレッツ接続の場合、接続のためにユーザーID（ログインID）とパスワード（ログインパスワード）をBBルータに設定しますが、その入力を間違えると正常に接続できません。
入力ミスは意外と多く、再度入力し直すと接続できることが度々ありますので、入力した内容に間違いがないか、今一度確認してください。
「1（いち）」⇔「l（エル）」、「0（ゼロ）」⇔「O（オー）」の間違いなど。

フレッツの場合は「@」以降の入力が必須です

フレッツ・ADSLやBフレッツの場合は、ユーザID（ログインID）やパスワード（ログインパスワード）の入力が必須です。
特に注意すべき点として、ユーザIDの設定ではご利用になるプロバイダごとに、ユーザIDの後ろに「@****.ne.jp」というような設定入力が必要です。

プロバイダからの接続資料にはユーザIDの表記で「@」以降の部分が記載されていない場合もあります。
その場合はNTTからのフレッツ接続資料の中に、プロバイダ別のドメイン名リストがありますので、そちらで「@」以降の表記をご確認ください。

確認!

PPPoE設定

PPPoE接続の結果を確認してください。

BBルータにより確認方法が異なってくるため詳細は割愛しますが、PPPoEの接続設定の後には接続確認が大抵の場合行われます。
「接続診断」という機能を持ったBBルータの場合は、その機能を使って接続結果が良好かどうかを確認してください。
設定の最後で自動的に接続し、その結果を画面上に表示するタイプのBBルータの場合、接続に成功したというメッセージが表示されるか確認してください。

・接続テストの結果、接続できなかったという場合

「PADI-TIMEOUT」や「サーバからの応答 NG」等になる時は、PPPoE設定の「ユーザID」の設定が正しくても接続できないことがあります。
その場合、モデム・BBルータ・コンピュータの電源をそれぞれ切り、電源を切ったままの状態で30～60分ほどそのままにしておいてください。
30～60分ほど経過しましたらモデム→BBルータ→コンピュータの順番に電源を入れてください。

確認!

フレッツ接続ツール

フレッツ接続ツールは使いません

BBルータを使用する場合は本編冒頭の「インターネットへの接続や切断はどうするの？」にも書きましたように、フレッツ接続ツールは使用しません。
もし現在、BBルータの設定後にフレッツ接続ツールを起動してインターネットへの接続をしている場合は、フレッツ接続ツールは使用せずにブラウザを起動して、インターネットに接続できるか確認してください。
正しく接続設定が行われていれば、フレッツ接続ツールを使用しないで接続できます。

・PPPoE接続だけど接続ツールを使わない場合の設定は？

ADSL回線でPPPoE接続だが、モデムにコンピュータを接続してインターネットにアクセスする際、接続ツール等を使用しないという場合は、ご利用のモデムにBBルータ機能がついている可能性が考えられます。その場合は「PPPoE接続」ではありませんので、次項の「アッカやイー・アクセスをご利用の場合」を参考に設定を行ってください。

ルータ機能付きモデムをご利用の場合

プロバイダから提供されているモデムにルータ機能がついている場合、複数のコンピュータで利用するときは、ハブがあればアクセスできるため本来BBルータは必要ありません。
しかし、どうしてもBBルータを使用したいという場合は、BBルータのIPアドレスを変更することで利用可能になります。
*BBルータのIPアドレスは本冊子の冒頭でも触れているように「192.168.1.1」になります。もし、ご利用のモデムも同じく「192.168.1.1」というIPアドレスを持っていて、しかも設定画面にアクセスした時にモデムの設定が行えるようだと、BBルータのWAN側とLAN側が同じようなアドレス（192.168.1.**）になってしまい、BBルータが混乱して正常な動作ができなくなります。*
*ハブではなくBBルータを使用したい場合はBBルータのLAN側のIPアドレスを、「192.168.2.**」等のようにWAN側のIPとは別のアドレスに変更すれば、接続できるようになります。*
このような場合、ルータは2段構成となります。そのため仕様想定外の動作をする可能性があります。予めご理解のうえでご使用ください。

接続設定ケーブルTV、Yahoo!BB編

Q ケーブルTVインターネットやYahoo!BBを利用した場合に、インターネット接続する時の確認点はなんですか?

A IPアドレスの取得、ケーブルTVインターネットの場合はケーブルの接続方法にもご注意ください。

IPアドレスの取得

・ケーブルTVやYahoo!BBをご利用の場合

ケーブルTVやYahoo!BBを利用する場合は「通常接続（DHCP接続）」という方式で接続を行います。
各BBルータのマニュアルをご覧いただくと判るかと思いますが、この場合設定らしい設定はほとんど必要ありません。
インターネットに接続するには、BBルータがプロバイダからIPアドレスを取得しなければいけませんので、BBルータのWAN側ポートにIPアドレスが表示されているか確認してください。
確認方法はBBルータによって画面が異なりますので詳細は割愛しますが、「ステータス表示」や「アカウント管理」の画面で確認することができます。

ケーブルの接続

・WAN側ポートにIPアドレスが割り当てられない時

ケーブルTV等を利用したPPPoE以外のインターネット接続方法の場合、BBルータを接続する前まではコンピュータをモデムに接続して利用していることが多いと思います。
ケーブルをモデムから外してそのままBBルータに接続してしまうと、本来BBルータに割り当てられるはずのIPアドレスをコンピュータが持ったままになってしまい、BBルータがモデムからIPアドレスを正しく取得できないことがあります。
その場合はコンピュータを再度モデムに接続しなおしていただき、一度コンピュータを終了させる処理を行ってください。
モデム接続後にコンピュータを終了させれば、通常は取得したIPアドレスは開放されます。コンピュータの電源が切れたらモデムとBBルータを接続し、モデム→BBルータ→コンピュータの順番に電源を入れてください。

・それでも接続できない場合

モデムにコンピュータを接続した後、一旦終了させてからモデムとBBルータを接続し、電源を入れなおしてもインターネットに接続できない場合は、モデム・BBルータ・コンピュータの電源をそれぞれ切り、電源を切ったままの状態で60分ほどそのままにしておいてください。

モデムを含めた全ての機器の電源を長時間切ることによって、プロバイダ側のサーバが記憶している情報が削除されて、初めて接続した時のような状態で接続することができます。60分ほど経過しましたらモデム→BBルータ→コンピュータの順番に電源を入れてください。

共通項目　最終確認編

どの接続方法にも共通する、最後に確認すべき点です。

Q 事前確認、接続設定と確認して問題がなかったのですが、それでもアクセスできません。ほかに確認点はありますか?

A コンピュータのIPアドレスが自動取得である事と、DNSサーバアドレスの設定を再確認してください。

確認!

自動取得

コンピュータのIPアドレスは自動取得になっていますか?

コンピュータのIPアドレスを手動で設定する場合、正しく設定されていないと設定画面にはアクセスできてもインターネットにアクセスできないことがあります。
手動設定の場合の注意点は次ページ「IPアドレスを手動で設定する場合の注意点は?」を参照していただき、コンピュータのIPアドレスが正しく自動取得になっているか、マニュアルを再度確認してください。

確認!

DNSサーバアドレス

IPアドレスでホームページにアクセスしてみてください。

ブラウザのアドレスに「http://210.197.75.205」と入力してEnterキーを押していただき、弊社（プラネックス）のホームページが表示されるか確認してください。
「http://210.197.75.205」だとアクセスできて「http://www.planex.co.jp」だとアクセスできない場合は、DNSサーバアドレスが正しく設定できていない可能性が考えられます。次ページ「IPアドレスを手動で設定する場合の注意点は?」を参考に設定を行ってください。

4 その他　よくあるお問い合わせについて

ここでは、多数寄せられる質問について、いくつかまとめてみました。

Q IPアドレスを手動で設定する場合の注意点は？

A IPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバアドレスが正しく設定されているか再確認してください。

IPアドレスの基本的なルールは冒頭の「IPアドレスってなんですか？」の中で触れていますが、設定画面にアクセスする場合に必要な最低限の説明だけなので、インターネットに接続する場合の設定については不十分になっています。手動でIPアドレスを設定する場合の注意点は以下のようになります。

IPアドレス：
IPアドレスの設定については110ページ「IPアドレスってなんですか？」をご覧ください。

サブネットマスク：
通常は「255.255.255.0」と指定してください。

デフォルトゲートウエイ：
（MacOSでは「ルータアドレス」と言います）
BBルータのIPアドレスが入ります。出荷時の設定は「192.168.1.1」になります。ここが正しく設定されていないとインターネットには接続できません。

DNSサーバアドレス：
（MacOSでは「ネームサーバアドレス」と言います）
ご利用になっているプロバイダのDNSサーバアドレスを入力してください。
BBルータによっては「デフォルトゲートウエイ」と同じIPアドレスで問題ない場合もありますが、判らない場合はプロバイダ指定のDNSサーバアドレスを設定するのが確実です。
ここが正しく設定されていないと「www.planex.co.jp」という名前（ドメイン名）でホームページにアクセスできなくなります。

Q BBルータに接続しているコンピュータ同士の通信ができません。

A pingを打って通信確認ができれば、BBルータの問題ではありません。OS側の設定の問題だと思われます。

インターネットへの接続は問題ないのに、コンピュータ同士のファイル共有等ができないという問い合わせも良く寄せられます。コンピュータ同士のLAN接続について、基本的にBBルータは関与しておりません。

BBルータの通信確認

コンピュータ同士が本当にアクセスできていないのか確認する方法として、112ページ「設定画面にアクセスできないのですが？」の中に、取得しているIPアドレスを確認する方法と、指定のIPアドレスにpingを打つ方法を紹介していますので、そちらを参考にそれぞれのコンピュータが取得しているIPアドレスを確認して、相手のコンピュータに対してpingを打ってみてください。

「Reply from・・・」が帰ってくればコンピュータ同士の接続は問題なくできていることになりますので、ファイル共有等ができないのはBBルータの問題ではなくOS側の設定の問題ということになります。

OS側の要因

pingの結果が「Request timed out」だったり、pingが通っても接続できない場合に考えられる一つの要因として、ファイヤウォールソフトの存在が挙げられます。ウイルスチェックソフトやインターネットセキュリティのソフトには、簡易ファイヤウォール機能を有している物があります。

使用しているコンピュータにそれらのソフトをインストールしている場合、ファイヤウォールが有効になっていると、たとえ自宅の中の同じネットワーク上のコンピュータであっても、ファイヤウォールから見ると第三者がそのコンピュータにアクセスしているように映るため、アクセスされないように遮断してしまいます。

該当するようなソフトを利用されている場合は、それらのソフトを停止させた状態で再度pingコマンドを打ち、通信状態を確認してみてください。

停止させるとpingが通るような場合は、それらソフトのファイヤウォールに他のコンピュータのIPアドレスを設定し、信頼するコンピュータとして認識させることで、ファイヤウォールを有効にしながらファイル共有ができるようになります。

Q コンピュータの電源をOFFにしたのに、BBルータのLANのランプがついたままですが故障でしょうか？

A 故障ではありません。「Wake On Lan」機能によるものです。

最近のLANアダプタには「Wake On Lan（以下WOL）」という、他のコンピュータから電源をON/OFF操作するための機能がついている物が多くなっています。
「WOL」に対応したLANアダプタでその機能が有効になっている場合、電源ONの信号を受信できるように待機状態になっている必要があるため、コンピュータ自体の電源はOFFになっていても、LANアダプタはBBルータのハブとLINKした（LANのランプが点灯した）状態になります。つまりBBルータ側ではどうすることもできません。
消えるようにするには「WOL」の機能をOFFにする必要がありますので、ご使用のLANアダプタのメーカーか、あるいは標準でコンピュータに搭載されているLANアダプタの場合はコンピュータメーカーに機能を無効にする手順をお問い合わせください。

仕様

準拠する標準	無線LAN	IEEE802.11b、IEEE802.11g
		ARIB STD-T66
	LAN 側	IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX
	WAN 側	IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX
伝送速度	LAN 側	10/100Mbps
	WAN 側	10/100Mbps
ポート	LAN 側	10BASE-T/100BASE-TX RJ-45 ×4 ポート（Auto MDI/MDI-X）
	WAN 側	10BASE-T/100BASE-TX RJ-45 ×1 ポート
ネットワークケーブル		10BASE-T カテゴリ3 以上ツイストペアケーブル（100m）
		100BASE-TX カテゴリ5 以上ツイストペアケーブル（100m）
LED		Power 、Status 、LAN Link/Act 、LAN 100M 、WAN 、PPPoE、WLAN
入力電源		DC12V 、1.2A
消費電力		最大8.2W
外形寸法（本体のみ）		180（W）×150（H）×29.3（D） mm
重量（本体のみ）		525g
環境		動作温度0～40 ℃、動作湿度35～85 %
EMI		VCCI　Class B

ユーザー登録について

この度は弊社製品をお買い上げいただき誠にありがとうございます。弊社では製品をお買い上げいただいたお客様にユーザー登録をお願いしております。ユーザー登録を行っていただいたお客様には新製品情報、バージョンアップ情報、キャンペーン情報等さまざまな情報を提供させていただきます。また、製品の故障等でユーザーサポートをお受けになるにはお客様のユーザー登録が必要となります。ユーザー登録の際は、ホームページ掲載の「個人情報保護方針について」をご確認後、ユーザー登録を行ってくださいますようお願いいたします。

ユーザー登録は下記弊社インターネットホームページ上で受け付けております。

http://www.planex.co.jp/user/

弊社へのお問い合わせ

■弊社製品の追加購入

弊社製品のご購入は、販売店様またはPLANEXダイレクトまで。
ケーブル1本からレイヤ3スイッチまで、お客様が探しているものが見つかります。

〈PLANEX DIRECT〉
http://direct.planex.co.jp/

■製品に関するお問い合わせ

製品購入前のご相談や、ご質問は弊社専任アドバイザーにお任せください。
ネットワーク導入やシステム構築・拡張など、お客様のお手伝いをいたします。

〈ご質問/お見積もりフォーム〉
http://www.planex.co.jp/lan.shtml

■技術的なお問い合わせ・修理に関するお問い合わせ

製品購入後のご質問は、弊社サポートセンターまでお問い合わせください。
豊富な知識をもったサポート技術者が、お客様の問題を解決いたします。

〈お問い合わせフォーム〉
http://www.planex.co.jp/support/techform/
受付：24時間
〈電話〉
フリーダイヤル：0120-415977
受付：月～金曜日、10～12時、13～17時
＊祝祭日および弊社規定の休業日を除く
〈FAX〉
ファクス番号：03-5766-1615
受付：24時間

◇お問い合わせ前のお願い

サポートを円滑に行うため、お問い合わせ前に以下のものをご用意ください。
お客様のご協力お願いいたします。

・弊社製品の製品型番とシリアルナンバー
・ご利用のコンピュータの型番とオペレーティングシステム名（Windows XP/Meなど）
・ご利用のネットワークの環境（回線の種類やインターネットサービスプロバイダ名など）
・ご質問内容（現在の状態、症状など。エラーメッセージが表示されている場合はその詳細を書きとめてください）

■その他

その他のお問い合わせ先は、弊社ホームページからお確かめください。

プラネックスコミュニケーションズ
http://www.planex.co.jp/

質問表

技術的なご質問は、この2ページをプリントして必要事項をご記入の上、下記FAX番号へお送りください。

プラネックスコミュニケーションズ テクニカルサポート担当 行

FAX：03-5766-1615

送信日：＿＿＿＿＿＿＿＿

会社名			
部署名			
名前			
電　話		FAX	
E-MAIL			

製品名 Product name	**ハイスピート無線ブロードバンドルータ**
型番 Product No.	**BLW-04FMG**
製造番号 Serial No.	

① ご使用のコンピュータについて

メーカー	
型番	

② OS

OS	バージョン

③ 質問内容

プラネックスコミュニケーションズ株式会社