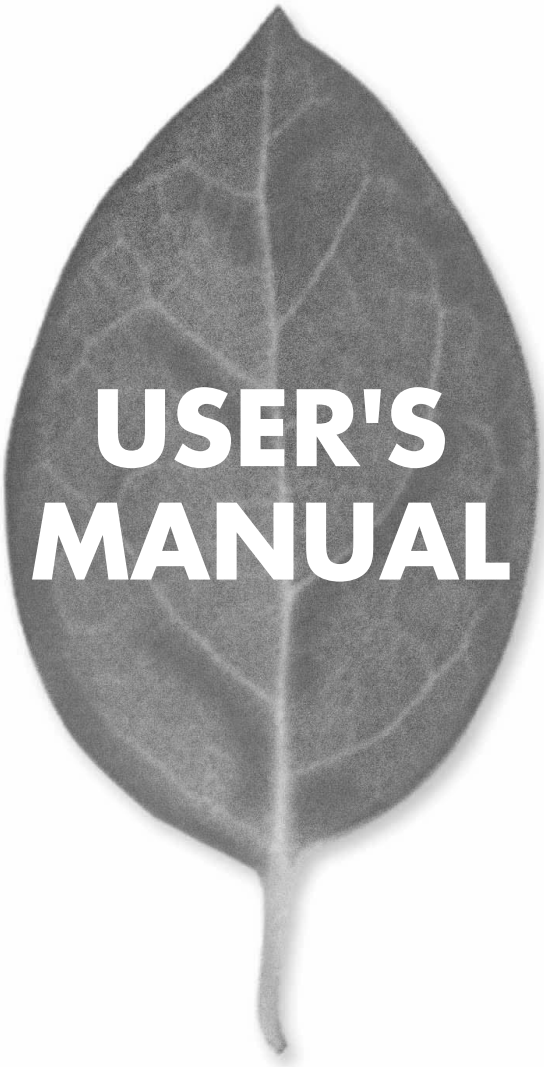


7ポート DMZ ファイアウォール ルータ

BRL-07DMZ

PLANEX COMMUNICATIONS INC.

USER'S MANUAL

7ポート DMZ ファイアウォール ルータ

BRL-07DMZ

本製品を安全にお使いいただくために

⚠警告

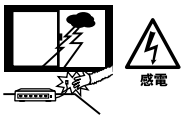
本製品をご利用の際は、以下の注意点を必ずお守りください。これらの事項が守られない場合、感電、火災、故障などにより使用者の重傷または死亡につながるおそれがあります。

分解・改造・修理はダメ！

各部のネジを外したり、カバーを開けたりしないでください。また製品内部の部品を改造・交換しないでください。感電や火災につながるおそれがあります。

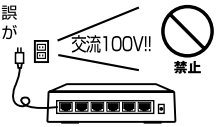
雷のときはさわらないで！

雷が発生している間は、製品各部およびケーブルにさわらないでください。感電するおそれがあります。



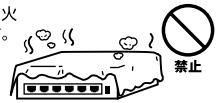
正しい電圧で使用して！

指定の電圧以外で使用すると誤動作や火災につながるおそれがあります。



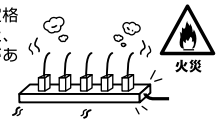
通気口をふさがないで！

内部に熱がこもり、誤動作や火災につながるおそれがあります。



タコ足配線・無理な配線はダメ!

コンセントや電源タップの定格を超えて電気製品を接続すると、発熱し火災につながる危険があります。



電源コードをつけて移動しないで！

本製品を設置・移動する際は、必ず電源コードを前もって抜いておいてください。電源コードを入れたまま移動し、コードが傷つくと誤動作や火災につながるおそれがあります。

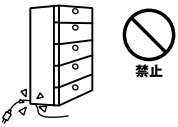
液体・異物は入れないで！

製品内部に液体や異物が入ると、ショートして火災が発生したり、誤動作したりする可能性があります。万一異物や液体が入ってしまった場合は、電源コードをコンセントから外して弊社サポートセンターまでご連絡ください。

電源コードは傷つけないで！

火災・感電につながるおそれがありますので、電源やACアダプタのコードは絶対に加工したり傷つけたりしないでください。また以下の点を守ってコードを傷めないようにしてください。

◇コードの上に物を載せない
◇熱源の側にコードを置かない
◇コードをかじる癖のあるペットは隔離する（かじった部分からショートし発火する危険があります）



設置・保管場所をもう一度確認して！

以下の場所での本製品のご利用や保管は避けてください。これらの場所で設置・保管を行うと誤動作や感電、火災につながる危険があります。

- 本製品が落下する可能性のある不安定な場所
- 高温または多湿の場所（暖房器具の側も含む）
- 急激に温度変化する可能性のある場所（結露のおそれがある所）
- 静電気を帯びやすい場所（絨毯の上も含む）
- 腐食性のガスが発生する場所
- 直射日光のあたる場所
- 振動の激しい場所
- ほこりの多い場所
- 腐食性のガスが発生する場所

◎おねがい

本製品のお手入れ

- 本製品のお手入れは乾いた柔らかい布で行ってください。
- 汚れがひどい場合は、水で薄めた中性洗剤に布を浸し、かたく絞って本製品を拭いてください。また最後に乾いた布で軽く拭いてください。
- 台所用中性洗剤以外は使わないでください。シンナーやベンジン、ワックス、アルコールが入ったものは使用できません。

このマニュアルの構成

本マニュアルは7ポート・ブロードバンドルーター bRoad Lanner BRL-07DMZの概要および使用方法について説明します。本マニュアルの構成は以下のようになっています。

■必ずお読みください

第1章　はじめに
本製品の概要と各部の名称について説明します。必ずお読みください。

■ご使用方法

第2章　ハードウェアの接続
本製品ハードウェアのADSL/ケーブルモデムおよびLANとの接続方法について説明します。必ずお読みください。

第3章　Webブラウザを使った設定の準備
本製品をWebブラウザから設定するためのコンピュータの設定方法について説明します。

第4章　インターネット接続設定
本製品を使って最も簡単にインターネットに接続する方法について説明します。

第5章　詳細設定
本製品のDHCPサーバ機能やローカルサーバ機能等のより詳しい機能の設定の方法について説明します。

第6章　ファイアウォール設定
本製品のファイアウォール設定について説明します。

第7章　その他の機能
本製品の通信状況等を参照する方法や、設定の初期化などについて説明します。

■付録

付録A　トラブルシューティング
「トラブルかな？」と思われる場合の対応方法について説明します。

付録B　TFTPを使用したファームウェアのアップデート
本製品のファームウェアのアップデート方法について説明します。

付録C　デフォルト設定の復帰
本製品を工場出荷時のデフォルト設定に戻す方法について説明します。

付録D　デフォルト設定
本製品の工場出荷時のデフォルト設定について説明します。

付録E　telnet設定
本製品をtelnetを使用して設定する場合の設定メニューについて説明します。

付録F　仕様
本製品の製品仕様です。

●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。

User's Manual　Version 1.0　　No.PMN-01-10-JF-BRL07DMZ

目次

はじめに

1 概要

本製品は、ADSLおよびCATV（ケーブルTV）接続を使用したインターネット接続に対応したブロードバンドルータです。PPPoE接続にも対応しており、NTT東西のフレッツADSLでもご利用できます。NAPT（Network Address Port Translation:ネットワークアドレスポート変換）機能により、1つのIPアドレスを複数のコンピュータで共有し、同時にインターネットにアクセスすることが可能です。

ファイアウォール機能には、Stateful Packet Inspectionを採用する事により、強固なセキュリティ機能を持った、安全な常時接続環境を構築できます。

本製品は、DMZポートを装備しています。複数IPアドレスが割り当てられるサービスにおいて、安全にサーバを公開することができます。

本製品はWEBブラウザまたはtelnetにより、簡単にセットアップすることが可能です。

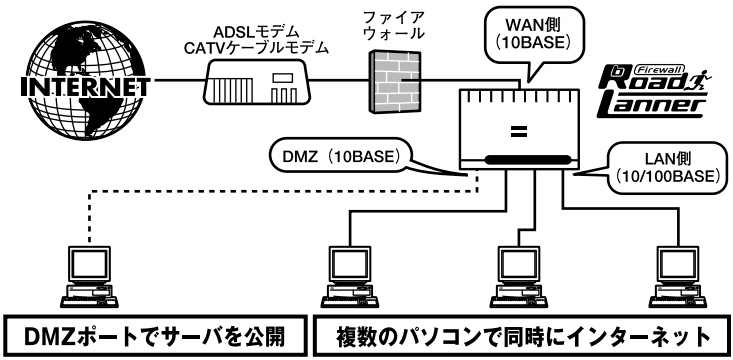


図1-1 bRoad Lanner接続図

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。プロバイダとのご契約内容についてご確認ください。

2 特長

●NAPT機能により1つのIPアドレスを複数のコンピュータで共有可能
●ファイアウォール機能には、Stateful Packet Inspectionを採用
●WAN側に10M RJ-45 ポートを1ポート装備
●LAN側に100M/10M自動認識に対応した7ポートスイッチングハブを内蔵
●WANおよびLANから独立したDMZポートを装備
●WAN側ポートはDHCPクライアントに対応
●LAN側ポートはDHCPサーバに対応（最大253クライアント）
●ローカルサーバ機能により、ローカルネットワーク上のコンピュータにインターネットからアクセス可能
●DMZポートにより複数IPアドレスサービスにおいて安全にサーバの公開が可能
●フィルタ機能を装備、IPアドレス、ポート番号によるアクセス制限が可能
●WAN側の接続方法として通常の接続のほかにPPPoE接続にも対応
●ARMプロセッサによる高速ルーティング
●WEBブラウザから設定可能

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認してください。

●BRL-07DMZ本体
●ACアダプタ
●ストレートタイプLANケーブル（1m）1本
●ショートコード 1本
●ユーザーズマニュアル
●簡単設定マニュアル
●保証書（ユーザーズマニュアルの最後にあります。）

不足品がある場合は、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

■本体上面

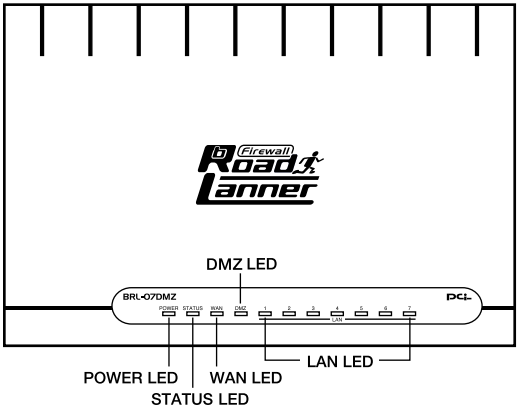


図1-2 BRL-07DMZ本体上面

「POWER LED」
本製品に電源が供給されている場合に点灯します。

「STATUS LED」
本製品がデータの送受信中に点滅します。

「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は点滅します。

「DMZ LED」
DMZ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は点滅します。

「LAN LED」
LAN側ポートのリンクが100Mで確立すると緑色に点灯します。10Mでリンクが確立すると、オレンジ色に点灯します。また、ポートがデータの送受信中は点滅します。

■本体背面

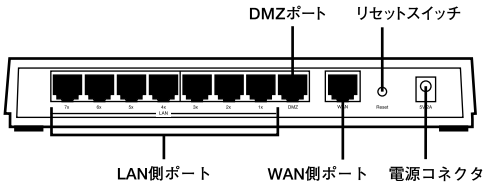


図1-3 BRL-07DMZ本体背面

「LANポート」
本製品をプライベートネットワークと接続するためのRJ-45 LANポートです。

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

「DMZポート」
本製品をDMZネットワークと接続するためのRJ-45 LANポートです。

「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。

「リセットスイッチ」
本製品を再起動する場合に使用します。本製品を再起動する場合はリセットスイッチを1秒間程度（STATUS LEDが点灯するまで）押してください。

■本体裏面

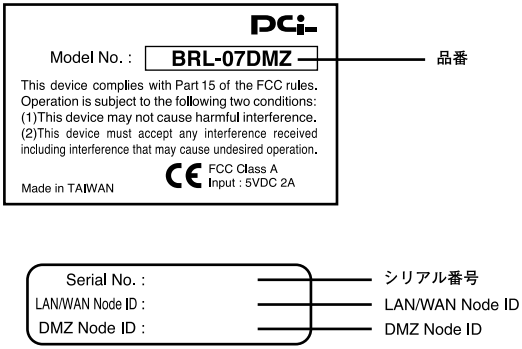


図1-4 BRL-07DMZ本体裏面

「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場合にも必要になります。

「LAN/WAN Node ID」
本製品のLANポートおよびWAN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場合があります。その場合はこのMACアドレスをプロバイダに申請してください。

「DMZ Node ID」
本製品のDMZポートのMACアドレス（物理アドレス）です。

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 95/98/98SE/Me/NT/2000/XPを搭載し、RJ-45 LANポートを装備したコンピュータ

●TCP/IPが利用可能なOS（Mac OS、各種UNIX等）を搭載し、RJ-45 LAN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。

●カテゴリ5以上のLANケーブル

◎ADSL/ケーブルモデム

本製品は、以下のいずれかの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

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、コンピュータとの接続手順について説明します。

1 ADSL/ケーブルモデムとの接続（WAN側ポート）

1. ADSL/ケーブルモデムの電源を切ってください。

2. .本製品付属のLAN用ストレートケーブルもしくは、市販のストレートタイプのLAN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 LANポートを接続してください。

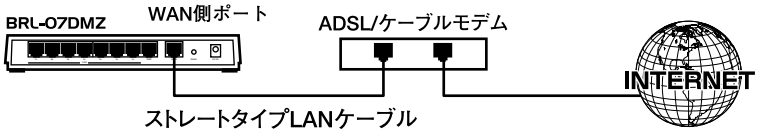


図2-1 ADSL/ケーブルモデムとの接続

注意

ADSL/ケーブルモデムの種類によっては、本製品と接続する際にストレートタイプのLANケーブルでなく、クロスタイプのLANケーブルを必要とするものもあります。ADSL/ケーブルモデム側のRJ-45ポートがMDI-Xの場合はストレートタイプのLANケーブルを、MDIの場合はクロスタイプのLANケーブルをご利用ください。詳細については、お手持ちのADSL/ケーブルモデムのマニュアルを参照してください。

2 ネットワークとの接続（LAN側ポート）

1. ストレートタイプのLANケーブルの一端を本製品のいずれかのLAN側ポートに接続してください。

2. LANケーブルのもう一端をコンピュータのRJ-45 LANポートに接続してください。

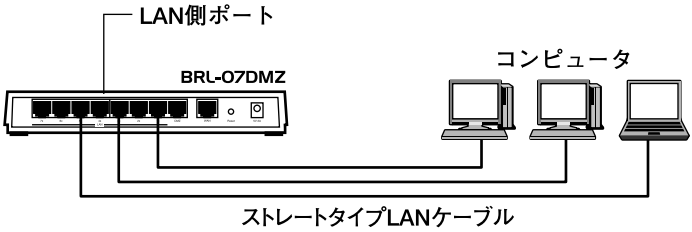


図2-2 ネットワークとの接続

3 DMZネットワークとの接続（DMZポート）

■DMZポートにコンピュータを1台のみ接続する場合

1. ストレートタイプのLANケーブルの一端を本製品のDMZポートに接続してください。

2. LANケーブルのもう一端をコンピュータのRJ-45 LANポートに接続してください。

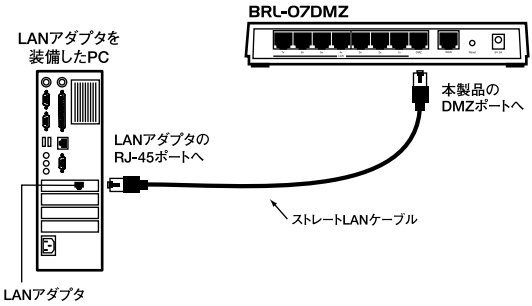


図2-3 DMZポートへのコンピュータの接続

■DMZポートに複数のコンピュータを接続する場合

1. **ストレートタイプのLANケーブルの一端を本製品のDMZポートに接続してください。**

2. **LANケーブルのもう一端をハブのUplink（MDI）ポートに接続してください。（ハブにUplinkポートが無い場合は、クロスタイプのLANケーブルを使用してハブの通常ポートに接続してください。）**

3. **ハブの通常ポート（MDI-X）とコンピュータのRJ-45ポートをストレートタイプのLANケーブルで接続してください。**

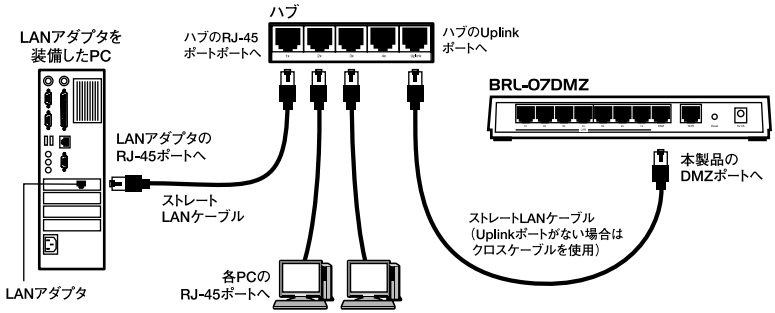


図2-4 DMZポートへの複数コンピュータの接続

4 電源の接続

1. 付属のACアダプタを本製品の電源コネクタに接続してください。

2. ACアダプタをAC100Vコンセントに接続してください。コンセントに直接、ACアダプタを接続できない場合は付属のショートケーブルをご使用ください。

3. ADSL/ケーブルモデムの電源を入れてください。

4. コンピュータの電源を入れてください。

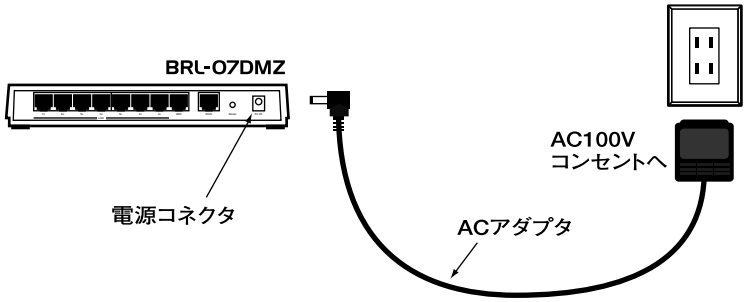


図2-5 電源の接続

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。

5 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 LEDとWAN LEDおよびLAN LEDが点灯します。
これらのLEDが点灯しない場合は以下の点についてご確認ください。

◎POWER LED
●本製品付属のACアダプタを使用していますか？
●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
●LANケーブルの両端はそれぞれ、本製品背面のWAN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？
●LANケーブルの種類（ストレートまたはクロス）は合っていますか？

◎LAN LED
●LANケーブルの両端はそれぞれ、本製品背面のLAN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？
●LANケーブルの種類（ストレートまたはクロス）は合っていますか？

6 本製品のリセット手順

本製品背面にはリセットスイッチが装備されています。何らかの理由で本製品のリセットを行いたい場合は、以下の手順でリセットを行ってください。

1. 本製品に電源が入っていることを確認し、リセットスイッチを約1秒間（STATUS LEDが点灯するまで）押してください。

2. 本製品がリセットされ、再起動します。

> **⚠ 注意**
> *リセットをしても、本製品に保存されている設定は初期化されません。本製品の設定を工場出荷時の状態に初期化したい場合は、「付録C.デフォルト設定の復帰」を参照してください。*

7 電源投入時の自己診断テストについて

本製品は電源投入時、自動的に自己診断テストを実行します。本製品が正常に起動すると、製品上面のSTATUS LEDが5回点滅します。このLEDが5回点滅しない場合は、本製品の故障が考えられます。弊社テクニカルサポートまでご連絡ください。

WEBブラウザを使った設定の準備

本章では本製品をWEBブラウザ経由で設定するための準備から、設定画面にアクセスするまでの手順について説明します。
WEBブラウザを使った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済ませておいてください。

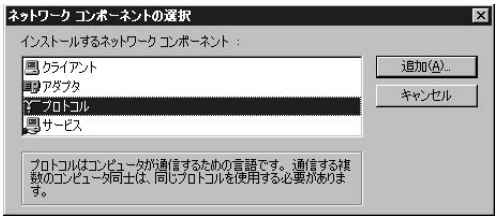
1 コンピュータの設定

■Windows 95/98/98 SE/Me

1. コンピュータにLANアダプタがインストールされ、正常に認識されていることを確認してください。LANアダプタがインストールされていない場合は、LANアダプタのインストールを行ってください。

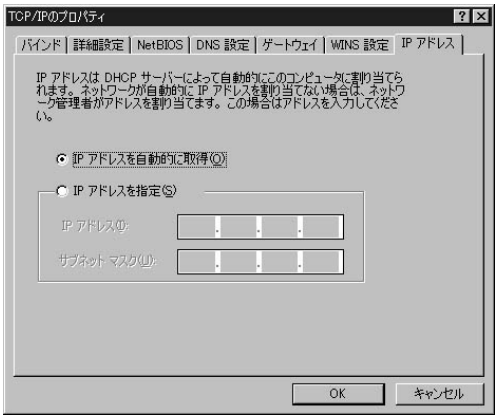
2. コンピュータにTCP/IPプロトコルがインストールされていることを確認します。「スタート」メニューから「設定」→「コントロールパネル」→「ネットワーク」と選択してください。「現在のネットワークコンポーネント」の欄に「TCP/IP」が表示されているか確認してください。インストールされている場合は手順5に進んでください。

3. インストールされていない場合は「追加」ボタンをクリックし、「インストールするネットワークコンポーネント」から「プロトコル」を選択して「追加」ボタンをクリックしてください。



4. ネットワークプロトコルの選択で「製造元」に「Microsoft」を選択し、「ネットワークプロトコル」には「TCP/IP」を選択して「OK」ボタンをクリックしてください。ネットワークのプロパティの画面に戻ります。

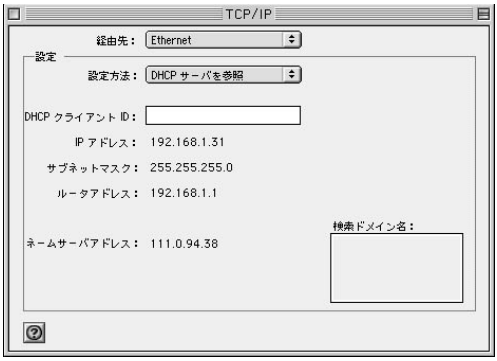
5. 「TCP/IP」を選択し「プロパティ」ボタンをクリックしてください。「TCP/IPのプロパティ」画面が表示されるので、「IPアドレス」タブをクリックしてください。画面内の「IPアドレスを自動的に取得」オプションを選択し、コンピュータを再起動してください。



■Macintosh

1. アップルメニューから「コントロールパネル」→「TCP/IP」と選択してください。

2. TCP/IPの設定ウィンドウの「設定方法」を「DHCPサーバを参照」に設定してください。



3. TCP/IPの設定ウィンドウを閉じて、Macintoshを再起動してください。

■その他のコンピュータまたはOS

ご利用のコンピュータまたはOSのマニュアル及びドキュメントを参照にして、ネットワークプロトコルをTCP/IPに設定してください。IPアドレスはDHCPサーバから取得する設定にしてください。

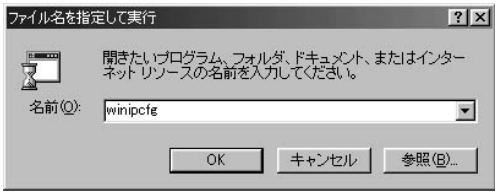
2 コンピュータのIPアドレスの確認

本製品は工場出荷時の状態でDHCPサーバ機能が有効になっています。これにより、接続されているパソコンはIPアドレスを自動的に割り当てられますので、IPアドレスの設定を意識する事なくご利用になれます。ここでは、コンピュータにIPアドレスが正常に割り当てられているか確認する方法について説明します。

■Windows 95/98/98SE/Meパソコンの場合

1. スタートメニューから「ファイル名を指定して実行」を選択します。

2. 「名前」に winipcfg と入力して［OK］ボタンをクリックします。



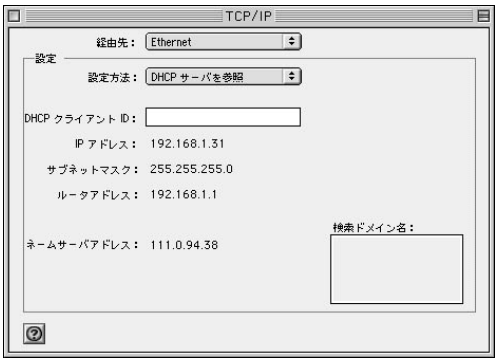
3. IP設定ウィンドウが表示され、現在のIPアドレスが表示されます。本製品が工場出荷時の状態の場合には 192.168.1.xxx（xxxは21～120というIPアドレスが割り振られます。ここでIPアドレスが正常に割り振られていない場合には、本製品とパソコンの接続を確認して、パソコンを再起動させてください。

IPアドレスが正常に取得できていましたら「3-3 WEBブラウザからのアクセス」へ進んでください。正常に取得できていない場合には、各ケーブルの接続を確認してからコンピュータを再起動してください。

■Macintoshパソコンの場合

1. アップルメニューから「コントロールパネル」→「TCP/IP」と選択してください。

2. TCP/IPウィンドウが表示されます。現在のIPアドレスが表示されます。



3. 「IPアドレス」に表示されている値が現在のIPアドレスです。本製品が工場出荷時の状態の場合には 192.168.1.xxx（xxxは21～120）というIPアドレスが割り振られます。ここでIPアドレスが正常に割り振られていない場合には、本製品とパソコンの接続を確認して、パソコンを再起動させてください。

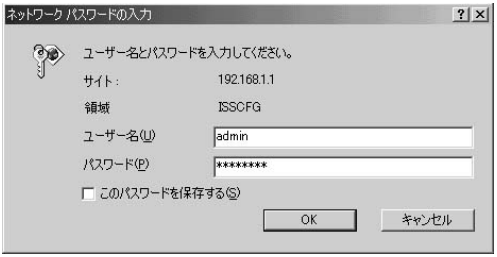
   IPアドレスが正常に取得できていましたら「3-3 WEBブラウザからのアクセス」へ進んでください。正常に取得できていない場合には、各ケーブルの接続を確認してからコンピュータを再起動してください。

3 WEBブラウザからのアクセス

1. コンピュータが起動したら、WEBブラウザを起動してください。

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」）に本製品のデフォルトIPアドレス「192.168.1.1」を入力し、Enterキーを押してください。

3. 本製品にログインするための認証ダイアログボックスが表示されます。デフォルトの管理ユーザー名「admin」と、デフォルトのパスワード「password」を入力して「OK」ボタンをクリックしてください。



4. 本製品のメイン・セットアップメニューが表示されます。

注意

WEB設定画面が表示されない場合は以下の項目を確認してください。

●コンピュータのネットワークアダプタは正常に動作していますか？
→コンピュータまたはネットワークアダプタのマニュアルを参照してネットワーク設定を確認してください。
●コンピュータのTCP/IPの設定が間違っている可能性があります。IPを自動取得（DHCPを使用）する設定にしてください。
●使用しているWEBブラウザで、プロキシが設定されていると設定画面が表示されません。プロキシを使用しない設定にしてください。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。
●お使いのコンピュータがIPアドレスを取得できていない可能性があります。
→3-2 コンピュータのIPアドレスの確認を参照にIPアドレスが正常に取得できているか確認してください。コンピュータがIPアドレスを取得できてない場合は、コンピュータを再起動してください。（デフォルト設定時は 192.168.1.xxx がIPアドレスとして割り当てられます。）

インターネット接続設定

ここでは本製品を利用してインターネットへ接続するための設定方法について説明します。

1 インターネット設定

1. **WEBブラウザで設定画面を開きます。**

2. **ブラウザ画面左側のメニューから、[インターネット設定] の文字をクリックしてください。[インターネット設定] ページが表示されます。**

3. ご利用のインターネット接続サービスのタイプを選択します。ブラウザ画面上部のメニューバーに2つの選択肢が表示されます。ご利用のインターネット接続サービスを選択してください。

◎PPPoE設定
NTT東日本/NTT西日本の「フレッツ・ADSL」、「Bフレッツ」や東京めたりっく通信の「G-One（Single）」サービス、名古屋めたりっく通信の「Home」サービス等のPPPoEプロトコルを使用したインターネット接続サービスをご利用の場合はこちらを選択してください。

◎CATV設定
CATVインターネット接続サービスや、「Yahoo! BB」等のPPPoEプロトコルを使用しないADSL接続サービスをご利用の場合はこちらを選択してください。 また、IPアドレスの取得にDHCPを使用するサービスの場合も、こちらから設定を行ってください。

2 PPPoE設定

[PPPoE設定] では、PPPoE方式を採用したインターネットサービスをご利用の場合の設定を行います。

> **⚠ 注意**
> ***PPPoE接続ではないADSLインターネット接続サービスの場合は、[CATV設定] から設定を行ってください。***

1. **[インターネット設定] ページの上部メニューバーから [PPPoE設定] を選択します。[PPPoE設定] ページが表示されます。表示される設定項目に必要な情報を入力します。**

◎ユーザ名

プロバイダから指定されたPPPoE接続ユーザ名を、正確に入力してください。「フレッツ・ADSL」、「Bフレッツ」の場合は“ @ ”(アットマーク) 以下も入力します。(工場出荷時の状態では空欄に設定されています。)

例：pci011@planexbrl.ne.jp

注意

最大63文字の半角英数字を入力可能です。大文字・小文字の違いに注意して入力してください。PPPoE接続ユーザ名はメールアカウント名などと異なる場合があります。（工場出荷時の状態では空欄に設定されています。）

◎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、正確に入力してください。セキュリティのため、この欄に入力した文字は“＊”（アスタリスク）表示されます。

例：rY0Co%Mtu

注意

最大31文字の半角英数字を入力可能です。大文字・小文字の違いに注意して入力してください。PPPoE接続パスワードはメールパスワードなどと異なる場合があります。

◎サービス名

プロバイダから指定されたPPPoEサービス名を、正確に入力してください。特に指定されていない場合は入力する必要はありません。（工場出荷時の状態では空欄に設定されています。）

例：PPPServ

注意

最大63文字の半角英数字を入力可能です。大文字・小文字の違いに注意して入力してください。

◎自動接続

パソコン上でWEBブラウザを起動した場合など、LAN側のパソコンからのインターネット接続要求に応じて自動的にインターネット接続したい場合は、「有効」に設定してください。定額のインターネット接続サービスの場合は「有効」に設定することをお勧めします。（工場出荷時の状態では「有効」に設定されています。）

注意

「無効」に設定した場合は、［診断ツール］ - ［PPPoE診断］ページで手動接続しなければなりません。

◎自動切断までの時間
PPPoEでインターネットに接続中、通信が無い状態が続いた場合に 自動的にPPPoE接続を切断するまでの時間を分単位で指定します。"0 ～ 120"の範囲で指定できます。自動切断したくない場合は、この欄に"0"を入力してください。(工場出荷時の状態では「120」に設定されています。)

例：3

◎IPアドレス自動取得
IPアドレスがプロバイダから自動的に割り当てられる場合は「する」、IPアドレスが固定で割り当てられている場合は「しない」を選択します。「しない」に設定した場合は次の「固定IPアドレス」も設定してください。(工場出荷時の状態では「有効」に設定されています。)

◎固定IPアドレス
IPアドレスが固定で割り当てられている場合に、プロバイダから指定されたIPアドレスを入力します。複数のグローバルIPアドレスが割り当てられるサービスの場合は、割り当てられたグローバルIPアドレス範囲の中からルータ用に指定されたIPアドレスを入力してください。(工場出荷時の状態では「0.0.0.0 」に設定されています。)

例：172.16.1.10

◎DNSアドレス自動取得
DNSサーバのIPアドレスをプロバイダから自動的に取得する場合は「する」、DNSサーバのIPアドレスが固定で指定されている場合は「しない」を選択します。「しない」に設定した場合は次の「固定DNSアドレス1」および「固定DNSアドレス2」も設定してください。(工場出荷時の状態では「有効」に設定されています。)

◎固定DNSアドレス1
プライマリDNSサーバのIPアドレスがプロバイダから固定で指定されている場合は、プロバイダから指定されたプライマリDNSサーバのIPアドレスを入力します。(工場出荷時の状態では「0.0.0.0」に設定されています。)

例:172.16.1.10

◎固定DNSアドレス2
セカンダリDNSサーバのIPアドレスがプロバイダから固定で指定されている場合は、プロバイダから指定されたプライマリDNSサーバのIPアドレスを入力します。プロバイダからセカンダリDNSサーバのIPアドレスが指定されていない場合は、入力する必要はありません。(工場出荷時の状態では「0.0.0.0」に設定されています。)

例:172.16.1.11

◎MSS(Maximum Segment Size)
MSS(Maximum Segment Size)値を変更します。通常は工場出荷時の設定(1412)を変更する必要はありません。不用意に変更すると、通信ができなくなったり、特定のサイトやアプリケーションが使用できなくなったり、パフォーマンスが低下する等の問題が発生しますので注意してください。

注意
NTT東日本、NTT西日本の「フレッツ・ADSL」、「Bフレッツ」サービスを使用する場合は、MSS値は必ず1414以下の値に設定してください。

2. 入力内容を確認し、正しければ[適用]ボタンをクリックしてください。

3. 画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい]ボタンをクリックしてください。[はい]ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。(再起動には約10秒かかります)

3 PPPoE接続の診断

PPPoE接続の設定が完了したら、実際に正常に接続が行えるかを診断します。

1. ブラウザ画面左側のメニューから「診断ツール」をクリックしてください。「PPPoE診断」ページが表示されます。

2. 「接続」ボタンをクリックしてください。PPPoE接続が開始されます。

3. 接続結果が表示されます。接続結果の最後の行に「Your PPPoE DSL connection is up and running now!」と表示されれば接続は成功です。このメッセージが表示されない場合は、正常に接続できていません。もう一度設定内容に間違いが無いかよく確認してください。

注意

インターネットに正常にアクセス出来ない場合は、付録A「トラブルシューティング」を参照してください。

4 CATV設定

[CATV設定] では、CATV (ケーブルテレビ) インターネット接続サービスや、「Yahoo! BB」等のPPPoE接続を使用しないADSLサービスを使用した場合のインターネット接続の設定と、WAN側ポートのMACアドレスの変更機能について説明します。

注意

PPPoE接続を使用するADSLインターネット接続サービスの場合は、[PPPoE設定] から設定を行ってください。

1. **[インターネット設定] ページの上部メニューバーから [CATV設定] を選択します。[CATV設定] ページが表示されます。表示される設定項目に必要な情報を入力します。**

◎ホスト名

特に必要が無い限り変更する必要はありませんが、ご利用のインターネット接続サービスによっては、ホスト名の設定が必要になります。この場合はプロバイダから指定されたホスト名を入力してください。(工場出荷時の状態では「broadlanner」に設定されています。)

例：Mymachine

◎ドメイン名
特に必要が無い限り設定しません。
ご利用のインターネット接続サービスでドメイン名の設定が必要な場合や、LAN 上でドメイン名を使用している場合は､ここにドメイン名を入力します。この設定を行うと本製品のDHCPサーバ機能によってIPアドレスが自動設定される際に、ドメイン名もパソコンに設定されます。
プロバイダからドメイン名を指定されている場合は、指定されたドメイン名を入力してください。(工場出荷時の状態では空欄に設定されています。)

例：planex.net

◎IPアドレスの設定
プロバイダの、DHCPサーバからIPアドレスを自動的に取得する場合は、「DHCPサーバから自動取得する」を選択してください。プロバイダから、固定のIPアドレスが指定されている場合は、「固定IPアドレスを使用する」を選択して、次のIPアドレス以下の項目について、プロバイダから指定された内容を入力してください。
(工場出荷時の状態では「DHCPサーバから自動取得する」に設定されています。)

◎IPアドレス
IPアドレスが固定で割り当てられる場合は、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。(工場出荷時の状態では「0.0.0.0」に設定されています。)

例：153.16.10.40

◎サブネットマスク
IPアドレスが固定で割り当てられる場合は、プロバイダから指定されたサブネットマスクを入力してください。(工場出荷時の状態では「255.255.255.0 」に設定されています。)

例：255.255.255.240

◎ゲートウェイ
IPアドレスが固定で割り当てられる場合は、プロバイダから指定されたデフォルトゲートウェイを入力してください。（工場出荷時の状態では「0.0.0.0」に設定されています。）

例：153.16.10.36

◎プライマリDNSアドレス
プライマリDNSサーバのIPアドレスがプロバイダから固定で指定されている場合は、プロバイダから指定されたプライマリDNSサーバのIPアドレスを入力します。（工場出荷時の状態では「0.0.0.0」に設定されています。）

例：172.16.1.10

◎セカンダリDNSアドレス
セカンダリDNSサーバのIPアドレスがプロバイダから固定で指定されている場合は、プロバイダから指定されたプライマリDNSサーバのIPアドレスを入力します。プロバイダからセカンダリDNSサーバのIPアドレスが指定されていない場合は、入力する必要はありません。（工場出荷時の状態では「0.0.0.0」に設定されています。）

例：172.16.1.11

◎MACアドレスの変更
本製品のWAN側のMACアドレスに、現在設定を行うためにアクセスしているコンピュータのMACアドレスをコピーする事ができます。これにより、ADSL/ケーブルモデムに接続する機器のMACアドレスの登録が必要なプロバイダの場合に、すでに登録しているコンピュータのMACアドレスをコピーすれば登録の変更をする事無くご利用いただけます。
「コピー」ボタンをクリックすると、現在設定を行うためにアクセスしているパソコンのMACアドレスがWAN側ポートにコピーされます。「元に戻す」ボタンをクリックするとWAN側ポートのMACアドレスが本製品のMACアドレスに戻ります。

2. 入力内容を確認し、正しければ [適用] ボタンをクリックしてください。

3. 画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい] ボタンをクリックしてください。[はい] ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。(再起動には約10秒かかります)

5 ローカルネットワーク設定

ここでは本製品のLAN側ポートのIPアドレスの設定とNAPT（ネットワークアドレスポート変換）の有効/無効の切り替えを行います。
本製品のLAN側ポートのデフォルトIPアドレスは192.168.1.1、デフォルトのサブネットマスクは255.255.255.0です。また、LAN側ネットワークのデフォルトゲートウェイアドレスは本製品のIPアドレス（192.168.1.1）になります。ほとんどの場合、これらの値を変更する必要はありません。

注意

本製品のLAN側ポートのIPアドレスを変更した場合は、変更を有効にするためLAN側ネットワーク上のすべてのコンピュータで、再起動するなどしてIPアドレスを取得しなおしてください。

1. ブラウザ画面左側のメニューから、[ローカルネットワーク設定] の文字をクリックします。メインメニューにローカルネットワーク設定画面が表示されます。各設定項目に必要な情報を入力します。

◎LAN側IPアドレス

本製品LAN側ポートに設定するIPアドレスを入力します。ここに入力するアドレスがLAN側からみた本製品のIPアドレスになります。（工場出荷時の状態では「192.168.1.1 」に設定されています。）

例：192.168.10.1

◎LAN側サブネットマスク
本製品LAN側ポートに接続されたネットワークのサブネットマスクを入力します。(工場出荷時の状態では「255.255.255.0 」に設定されています。)

例:255.255.255.0

◎LAN側デフォルトゲートウェイ
本製品のLAN側ポートに接続されたネットワークのデフォルトゲートウェイ(デフォルトルータ)のIPアドレスを入力します。通常は本製品を経由してインターネットに接続する形になりますので、上記 [LAN側ポートIPアドレス] と同じ値を入力します。(工場出荷時の状態では「192.168.1.1」に設定されています。)

例:192.168.10.1

◎NAPT(ネットワークアドレスポート変換)
本製品のNAPT(ネットワークアドレスポート変換)機能の有効/無効の設定します。有効にする場合は [有効] に、無効にする場合には [無効] に設定します。(工場出荷時の状態では「有効」に設定されています。)

2. **入力内容を確認し、正しければ [適用] ボタンをクリックしてください。**

3. **画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい] ボタンをクリックしてください。[はい] ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。(再起動には約10秒かかります)**

⚠ 注意
IPアドレスを変更した場合は変更を反映させるためLAN側ネットワーク上のすべてのコンピュータを再起動させるなどして、IPアドレスの再取得を行ってください。

詳細設定

ここでは本製品の詳細な設定方法について説明します。

■DHCPサーバ

DHCPサーバ機能を使用すると、LAN側ネットワーク上のコンピュータに自動的にIPアドレスを割り当てることができます。また、特定のコンピュータに対して固定のIPアドレスを割り当てることもできます。DHCPサーバ機能を使用しない場合は、ネットワーク上のすべてのコンピュータにIPアドレスを設定する必要があります。

■ローカルサーバ

ローカルサーバ機能を使用すると、LAN側ネットワーク上のコンピュータを公開することができます。TCPまたはUDPのポート番号ごとにインターネット（WAN）側からの接続要求を転送するコンピュータを指定することができます。

■DMZポート

複数のグローバルIPアドレスが割り当てられるサービスをご使用の場合で、DMZポートに接続したサーバを公開するための設定を行います。

■ルーティング

スタティックルーティングの情報をルーティングテーブルに登録します。

ブラウザ画面左側のメニューから、［詳細設定］の文字をクリックします。メインメニューに［詳細設定］ページが表示されます。

1 DHCPサーバ

ここでは、DHCPサーバ機能の設定を行います。
本製品のDHCPサーバ機能では、LAN側ネットワーク上の各コンピュータに対して、IPアドレス、サブネットマスク、ゲートウェイ、DNSアドレス、WINSサーバアドレスの情報を自動的に割り当てます。

⚠ 注意

●LAN側ネットワーク上にすでにDHCPサーバが存在する場合以外は、本製品のDHCPサーバ機能をご使用になることをおすすめします。
●DHCPサーバの設定変更後は、変更を反映させるためLAN側ネットワーク上のすべてのコンピュータを再起動させるなどして、IPアドレスの再取得を行ってください。

1. **[詳細設定] ページの上部メニューバーから [DHCPサーバ] を選択します。[DHCPサーバ] ページが表示されます。表示される設定項目に必要な情報を入力します。**

◎DHCPサーバ
「有効/無効」から選択してください。この機能を有効にするとLAN 側ポートに接続されたネットワーク上のパソコンに対して、本製品が自動的にIPアドレスを割り当てます。有効にする場合は以下の項目も設定してください。（工場出荷時の状態では「有効」に設定されています。）

◎プライマリDNSアドレス
プロバイダから指定されたDNSサーバのIPアドレスを入力してください。（工場出荷時の状態では「0.0.0.0 」に設定されています。）

例：172.16.1.10

◎セカンダリDNSアドレス
プロバイダからセカンダリ（バックアップ）DNSサーバのIPアドレスも指定されている場合は入力してください。（工場出荷時の状態では「0.0.0.0 」に設定されています。）

例：172.16.1.11

◎WINSサーバアドレス
LAN側ポートに接続されたネットワーク上にWINSサーバがある場合はそのIPアドレスを入力します。（工場出荷時の状態では「0.0.0.0 」に設定されています。）

例：172.16.1.20

2. 入力内容を確認し、正しければ［適用］ボタンをクリックしてください。

3. 画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

●IPアドレス割り当て範囲の設定

[DHCPサーバ] ページで [IPアドレス割り当て範囲の設定] をクリックすると、本製品のDHCPサーバ機能により、LAN側ポートに接続されたネットワーク上のパソコンに対して自動的に割り当てられるIPアドレスの範囲がリスト表示されます。

割り当て範囲を削除したい場合は [削除] ボタンをクリックしてください。(工場出荷時の状態では「192.168.1.21 」～「192.168.1.120 」までのIPアドレス割り当て範囲が設定されています。)

IPアドレスの割り当て範囲を追加したい場合は、[割り当て範囲の追加] をクリックしてください。[IP割当て範囲の追加] ページが表示されます。追加したいIPアドレス範囲の最初のホストアドレスを[割り当て開始IPアドレス] 欄に、最後のホストアドレスを [割り当て終了IPアドレス] 欄に入力して [適用] ボタンをクリックしてください。入力した内容が反映されたページが表示されます。[IPアドレス割当て範囲] は最大で4つまで指定できます。

画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい] ボタンをクリックしてください。[はい] ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。(再起動には約10秒かかります)

●IPアドレスの固定割り当て設定

本製品のDHCPサーバ機能を利用し、なおかつ特定のパソコン（サーバなど）のみ任意のIPアドレスで固定させたい場合に利用します。[DHCPサーバ] ページで [IPアドレスの固定割り当て設定] をクリックすると既に固定IP割り当てを設定している場合はリスト表示されます。

各リストを削除したい場合は [削除] ボタンをクリックしてください。

固定IP割り当てを追加したい場合は、[固定割り当ての追加] をクリックしてください。[固定割り当てIPアドレスの追加] ページが表示されます。固定設定したいIPアドレスを [IPアドレス] 欄に、そのIPアドレスを利用するコンピュータのMACアドレスを [MACアドレス] 欄に入力して、[適用] ボタンをクリックしてください。入力した内容が反映されたページが表示されます。固定IP割り当ては最大16個のクライアントを登録できます。

画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい] ボタンをクリックしてください。[はい] ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

●IPアドレス割り当て状況の表示

現在、本製品のDHCPサーバ機能によりコンピュータに割り当てられているIPアドレスの一覧が表示されます。「コンピュータ（ホスト）名 」にはIPが割り当てられているコンピュータ名が、「割り当てIPアドレス」にはそのコンピュータに割り当てているIPアドレスが表示されます。

2 ローカルサーバ機能

ローカルサーバ機能とは、LAN側ポートに接続されたネットワーク上の任意のコンピュータを、インターネット上から参照可能とする機能です。ローカルサーバ機能では、TCP/UDPのポート番号によって転送先のIPアドレスを指定して設定することができます。

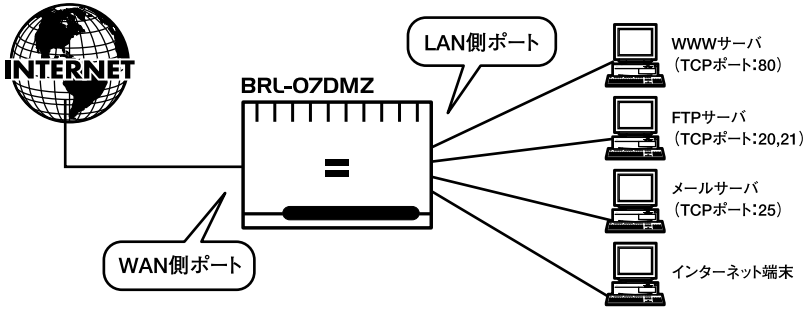


図5-1　ローカルサーバ

注意

本製品のLAN側およびDMZポートに接続したコンピュータから、ローカルサーバにアクセスすることはできません。
ローカルサーバの設定の確認は、WAN側（インターネット）から行って下さい。

1. **[詳細設定] ページの上部メニューバーから [ローカルサーバ] を選択します。[ローカルサーバ] ページが表示されます。表示される設定項目に必要な情報を入力します。**

既にローカルサーバ設定がされている場合は、[ローカルサーバリスト] に各エントリが表示されます。エントリを削除したい場合は [削除] ボタンをクリックしてください。

◎プロトコル
TCPポートを使用したローカルサーバを追加したい場合は [TCP] に、UDPポートを使用したローカルサーバを追加したい場合は [UDP] にします。

◎ポート番号
インターネット上に公開したいポート番号を入力します。[開始] にポート番号範囲の最初のポート番号を入力し、[終了] にポート番号範囲の最後のポート番号を入力します。ポート番号を1個だけ指定したい場合は、[開始] と [終了] に同じポート番号を入力します。
例：HTTP（WEB）サーバを公開する場合は、プロトコルにTCP、開始ポート番号と終了ポート番号に80を入力します。

◎ローカルIPアドレス
上記ポートの転送先パソコンのIPアドレスを入力します。

例：192.168.1.25

入力内容を確認し、正しければ [適用] ボタンをクリックしてください。[ローカルサーバリスト] にエントリが追加されます。[ローカルサーバリスト] は最大32エントリまで登録できます。

3 DMZポート

本製品はDMZポートを装備しています。複数IPアドレスを割り当てられるサービスをご使用の場合DMZポート上でサーバを公開することができます。この場合、WAN→DMZ方向のトラフィックに対してもファイアウォール機能が働くので、より安全にサーバを公開することが可能です。

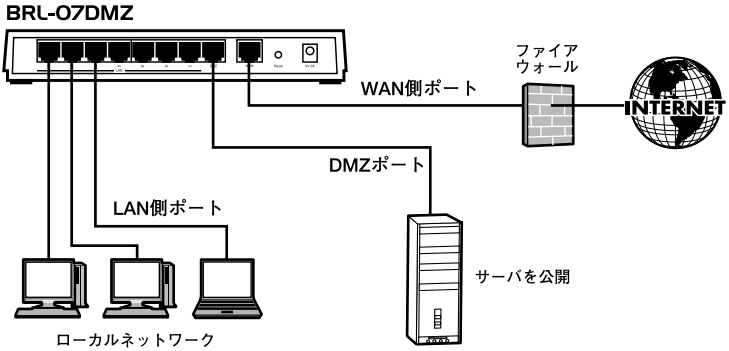


図5-2　DMZネットワーク

[詳細設定] ページの上部メニューバーから　[DMZポート] を選択します。[DMZポート] ページが表示されます。表示される設定項目に必要な情報を入力します。
DMZネットワークには最大で4つのIPアドレス範囲を設定することができます。

◎開始アドレス
DMZネットワークで使用するIPアドレス範囲の開始アドレスを入力してください。

◎終了アドレス
DMZネットワークで使用するIPアドレス範囲の終了アドレスを入力してください。

入力内容を確認し、正しければ［適用］ボタンをクリックしてください。入力した内容が反映されたページが表示されます。
画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

●DMZネットワークの設定例

プロバイダから複数のグローバルIPアドレスが割り当てられる場合、1つのサブネットとして連続したグローバルIPアドレスが割り当てられます。このうち、最初（ネットワークアドレス）と最後（ブロードキャストアドレス）は、システムで予約されておりホスト（コンピュータやサーバ）には使用できません。また、本製品のWAN側ポートで使用するIPアドレスも必要になります。従って、ホストで自由に利用可能なIPアドレスは、（プロバイダから割り当てられたアドレス数－3）個になります。（プロバイダから8個のグローバルIPアドレスが割り当てられている場合は5個が利用可能）

例：プロバイダから153.16.10.40～153.16.10.47（153.16.10.40/29）の8個のグローバルIPアドレスが割り当てられた場合

153.16.10.40 ネットワークアドレス（使用不可）
153.16.10.41 ルータ用（例：本製品WAN側ポート）
153.16.10.42 DMZホスト用（例：プライマリDNSサーバ）
153.16.10.43 DMZホスト用（例：WEBサーバ）
153.16.10.44 DMZホスト用（例：メールサーバ）
153.16.10.45 DMZホスト用（例：FTPサーバ）
153.16.10.46 DMZホスト用（例：その他サーバ）
153.16.10.47 ブロードキャストアドレス（使用不可）

この場合、DMZネットワークで使用可能なIPアドレス範囲は153.16.10.42～153.16.10.46になります。DMZネットワーク設定の［開始アドレス］には153.16.10.42を設定し、[終了アドレス]には153.16.10.46を設定してください。また、本製品のWAN側ポートのIPアドレスには153.16.10.41を固定設定してください。

注意

一般的にルータ（本製品WAN側）に設定するグローバルIPアドレスは、ネットワークアドレスの次のアドレスにします。プロバイダから指定されていない場合は、特に理由がない限りこのアドレスを設定してください。

●DMZホスト（コンピュータやサーバ）の設定
本製品のDMZポートを利用する場合、DMZポートに接続したホスト（パソコンやサーバ）のネットワーク設定は次のようになります。

「IPアドレス」
プロバイダから割り当てられたIPアドレス空間の中からさらに本製品のDMZネットワーク範囲に設定したグローバルIPアドレス

例：153.16.10.42

「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

例：255.255.255.240

「デフォルトゲートウェイ」
割り当てられたIPアドレス範囲の2番目のグローバルIPアドレス（＝本製品WAN側ポートに設定したグローバルIPアドレス）

例：153.16.10.41

4 ルーティング

ここでは、本製品のスタティックルーティングテーブルの参照、スタティックルーティングエントリの追加、RIPの有効/無効の切り替えを行うことができます。

> **注意**
>
> ***ネットワーク上に他にルータが存在しない場合は、スタティックルーティングの設定を行う必要はありません。***
> ***[詳細設定] ページの上部メニューバーから [ルーティング] を選択します。[ルーティング] ページが表示されます。表示される設定項目に必要な情報を入力します。***

既にスタティックルーティング設定がされている場合は、[スタティックルーティング] に各エントリが表示されます。エントリを削除したい場合は [削除] ボタンをクリックしてください。
新たにルーティングテーブルを追加したい場合は、[ルーティングテーブルの追加] をクリックしてください。[スタティックルーティングの追加] ページが表示されます。

◎送信先ネットワーク
パケットの送信先のネットワークアドレスを入力してください。

例：192.168.10.0

◎サブネットマスク
送信先ネットワークのサブネットマスクを入力してください。

例：255.255.255.0

◎ゲートウェイ
送信先ネットワークへ到達するためのゲートウェイ（ルータ）の IPアドレスを入力してください。

例：192.168.1.100

◎メトリック
送信先ネットワークまでのメトリック値を入力してください。

例：1

◎プライベート
「はい」に設定すると、[RIP I&II] が有効の場合でも、このルーティングエントリをRIPで送信しません。

入力内容を確認し、正しければ [適用] ボタンをクリックしてください。[ルーティングテーブル] にエントリが追加されます。[ルーティングテーブル] は最大で5エントリまで登録できます。

◎RIP I&II

本製品はRIP IおよびRIP IIに対応しています。「有効」に設定した場合には、ネットワーク上の他のRIP I/RIP II対応ルータとルーティング情報を交換し、ルーティングテーブルを自動的に更新します。RIPを使用しない場合には「無効」に設定します。

入力内容を確認し、正しければ［適用］ボタンをクリックしてください。
画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

ファイアウォール設定

本製品はネットワークを外部からの不正アクセスや攻撃から保護するため、Stateful Packet Inspectionと呼ばれる技術を採用したファイアウォール機能を内蔵しています。ファイアウォールを通過するネットワークトラフィックに対し、その通過を許可または禁止するためのアクセスルールを設定することができます。アクセスルールはLAN/WAN/DMZの各ネットワーク間のどの方向にも設定することができます。

ブラウザ画面左側のメニューから、[ファイアーウォール設定] の文字をクリックします。メインメニューに [ファイアーウォール設定] ページが表示されます。

以下に各設定メニューの設定内容について説明します。設定変更にあたっては、TCP/IPネットワークについての知識および経験が必要となります。

◎基本設定
本製品に内蔵されているファイアウォール機能の基本設定を変更します。

◎アクセスルール
LAN/WAN/DMZの各ネットワーク間のアクセスルールの設定を行います。本製品はこれらのルールを使ってネットワークトラフィックの送信元IPアドレス、送信先IPアドレスおよび通信ポートを解析し、トラフィックに対してファイアウォールを通過させるか拒否するかの判断をします。

◎URLフィルタ
本製品のファイアウォール機能にはURLフィルタ機能も搭載しています。LAN側ネットワークの全ローカルユーザーに対し、指定されたURLへのアクセスを禁止することが可能です。アクセスを禁止するURLは、最大10個まで登録できます。また、ActiveX、Java、Cookie、Proxyの各サービスについて受け付けるかどうかを設定することができます。

◎E-mail通知
本製品の稼動履歴はイベントログに記録されます。イベントログ内の情報は、セキュリティ上の理由であとで参照が必要となる場合があります。イベントログはWEBブラウザ上からオンラインで参照可能なほか、指定アドレスにE-Mailで送信することも可能です。また内蔵ファイアウォールは、DoS攻撃を検出するたびに自動的に警告メールを管理者に送信します。

◎イベントログ
本製品内に保存されているイベントログを参照します。また、その時点のログをE-Mail通知設定ページ内で登録されているE-Mailアドレスに対して送信することも可能です。またイベントログの消去もここで行います。

1 基本設定

このページでは、ファイアウォール機能の基本設定の変更ができます。本製品のファイアウォール機能には、 Stateful Packet Insepctcionと呼ばれる技術が採用されています。

[ファイアーウォール設定] ページの上部メニューバーから [基本設定] を選択します。[基本設定] ページが表示されます。表示される設定項目に必要な情報を入力します。

◎ファイアウォールを有効にする

本製品のファイアーウォール機能の有効/無効を設定します。ファイアウォール機能はデフォルト設定で有効になっています。ファイアウォール機能を無効にしたい場合は、ファイアウォールを有効にするでいいえを選択してください。(工場出荷時の状態では「有効」に設定されています。)

◎xxx→xxx アクセス初期ルール

LAN/WAN/DMZの各ネットワーク間の基本アクセスルールを設定します。「Forward」に設定した場合には各ネットワーク間のアクセスルールに無いものは転送します。「Discard」に設定した場合には各ネットワーク間のアクセスルールにないものを破棄します。各ネットワーク間のアクセスルールは次の「アクセスルール」で設定します。

◎TCP SYN Flooding攻撃しきい値

ネットワークをSYN Flooding DoS攻撃から守るため、本製品のファイアウォールは、リモート側からの不完全なTCP SYNセッションを1分間に何個まで許可するかを設定することができます。1分間に受信した不完全なTCPセッションがここで設定した数値を超えると、ファイアウォールはSYN Flooding DoS攻撃を受けていると判断します。(工場出荷時の状態では「20」に設定されています。)

◎DoS攻撃検出時の接続拒否時間

何らかのDoS攻撃を感知すると、ファイアウォールは一定時間インターネット側からの新規のTCP/IP接続を拒否し、プライベートネットワークおよび本製品自身を保護します。ここでは接続を拒否する時間を設定します。DoS攻撃検出時に接続拒否する時間を入力してください。(工場出荷時の状態では「5」に設定されています。)

◎NetBIOS接続を許可する

NetBIOS接続では TCP/UDPのポート番号139を使用します。インターネット経由でのNetBIOS接続を許可する場合は、NetBIOS接続を許可するをはいに設定してください。ただしWinNukeなどのDoS攻撃は、このポート番号を使って攻撃を行いますのでご注意ください。セキュリティ上、この設定は外部からのNetBIOS接続が必要な時のみ有効にするようにしてください。(工場出荷時の状態では「いいえ」に設定されています。)

◎マルチキャストパススルー

IPマルチキャストパケットのパススルーを有効にする場合には、「はい」を設定してください。IPマルチキャストパケットのパススルーを無効にする場合には「いいえ」にしてください。(工場出荷時の状態では「いいえ」に設定されています。)

◎IPソースルーティングを許可する

IPソースルーティングを有効にする場合には、「はい」を設定してください。IPソースルーティングを無効にする場合には「いいえ」にしてください。(工場出荷時の状態では「いいえ」に設定されています。)

注意

IPソースルーティングを有効にすると、“ソースアドレス詐称”と呼ばれる手段によるネットワークの侵入の危険があります。特に必要の無い限り「いいえ」に設定することをお勧めします。

◎インターネットからの設定画面へのログイン

WAN側ポートからの設定画面へのアクセスを有効にするか無効にするかの設定です。有効に設定すると、ブラウザ上で本製品のWAN側ポートの IPアドレスを入力することにより、本製品のWEB管理インタフェースにインターネット上からログインできるようになります。(工場出荷時の状態では「無効」に設定されています。)

◎インターネットからのpingへの応答

WAN側のリモートホストからのping (エコー要求) に応答するかどうかを設定することが可能です。本製品の存在をハッカーから隠すため通常は無効に設定することを推奨します。本製品のWAN接続が使用可能かどうかを外部から確認するなどの場合に有効に設定してください。(工場出荷時の状態では「無効」に設定されています。)

入力内容を確認して [適用] ボタンをクリックしてください。入力した内容が反映されたページが表示されます。

画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、[はい] ボタンをクリックしてください。[はい] ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。(再起動には約10秒かかります)

⚠ 注意

●インターネットからの設定画面へのログインおよびインターネットからのpingへの応答の各項目は、セキュリティ上、必要時のみ有効にすることをおすすめします。

●インターネットからの設定画面へのログインを有効にしている状態で、ローカルサーバ機能により WEBサーバを公開する場合は、ポート8080など、ポート80以外のポート番号を使用するようWEBサーバを設定してください。

2 アクセスルール

ここではWAN/LAN/DMZの各ネットワーク間のアクセスルールの設定を行います。本製品のファイアウォール機能はここで設定されたルールに従い、パケットの送信元IPアドレス、送信先IPアドレス、ポート番号を検査し、そのパケットを転送または破棄するかを決定します。

[ファイアウォール設定]ページの上部メニューバーから［アクセスルール］を選択します。アクセスルールの設定を行う、トラフィックの方向を［アクセスルールの方向］から選択して［設定］ボタンをクリックしてください。選択した方向のアクセスルールの設定ページが表示されます。表示される設定項目に必要な情報を入力します。

既に設定したアクセスルールがある場合は、設定されているアクセスルールが表示されます。アクセスルールを削除したい場合は［削除］ボタンをクリックしてください。
新たにアクセスルールを追加したい場合は、各項目を入力してください。

◎プロトコル
TCPポートのフィルタルールを追加したい場合は［TCP］に、UDPポートのフィルタルールを追加したい場合は［UDP］にします。

◎送信元IPアドレス： 開始
フィルタルールを適用したいLAN側の送信元のIPアドレスを入力します。連続したIPアドレスを範囲で指定したい場合は、指定したい範囲の最初のIPアドレスを入力します。

◎送信元IPアドレス： 終了
フィルタルールを適用したいLAN側のIPアドレスを範囲で指定した場合に、指定したい範囲の最後のIPアドレスを入力します。IPアドレスを単独で指定する場合には開始IPアドレスと同じIPアドレスを入力してください。

◎送信先IPアドレス： 開始
フィルタルールを適用したいWAN側の送信先のIPアドレスを入力します。連続したIPアドレスを範囲で指定したい場合は、指定したい範囲の最初のIPアドレスを入力します。

◎送信先IPアドレス： 終了
フィルタルールを適用したいWAN側のIPアドレスを範囲で指定した場合に、指定したい範囲の最後のIPアドレスを入力します。IPアドレスを単独で指定する場合には開始IPアドレスと同じIPアドレスを入力してください。

◎ポート番号： 開始
フィルタルールを適用したいポート番号を入力します。連続したポート番号を範囲で指定したい場合は、指定したい範囲の最初のポート番号を入力します。

◎ポート番号： 終了
フィルタルールを適用したいポート番号を範囲で指定した場合に、指定したい範囲の最後のポート番号を入力します。ポート番号を単独で指定する場合には開始IPアドレスと同じIPアドレスを入力してください。

◎処理
フィルタルールに適合するパケットを通過させたい場合には「Forward」に、フィルタルールに適合するパケットを通過させない場合は「Discard」に設定します。

◎ログ

フィルタルールに適合するパケットを処理した場合に、イベントログに記録を残すか設定します。「On」に設定した場合にはフィルタルールに適合するパケットを処理した時にイベントログに書き込みます。「Off」に設定した場合にはフィルタルールに適合するパケットを処理してもログに記録を残しません。

◎HTTPヘッダの検査（LAN→WANアクセスルールのみ）

ポート番号80（HTTP）を含むフィルタルールを作成する時に、URLフィルタも同時に適用させる場合には、「Yes」に設定してください。URLフィルタを適用させない場合は、「No」に設定しください。ポート番号80（HTTP）を含まない場合は、「N/A」に設定してください。

入力内容を確認して［適用］ボタンをクリックしてください。入力した内容が反映されたページが表示されます。

画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

⚠ 注意

●間違ったルールを作成すると、すべてのファイアウォール機能を無効にしてしまったり、セキュリティホールを開けてしまったり、また、インターネットへのすべてのアクセスを拒否してしまう、などの状態になってしまう場合もあります。ルールの作成/削除には細心の注意をはらい、くれぐれも間違いのないように行ってください。

●フィルタ設定では SYN Flood、Ping of Death、ポートスキャン等の Denial of Service（DoS）攻撃を防ぐことはできません。

3 アクセスルールの設定例

ここでは、アクセスルールの設定例として、DMZポートに接続したWEBサーバ上でhttp（ポート80）のみを公開しその他のポートはすべて遮断する場合の設定例について説明します。

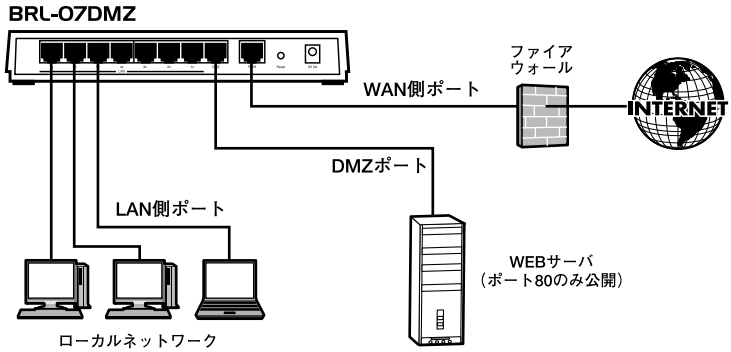


図6-1　DMZポート接続図

［ファイアーウォール設定］ページの上部メニューバーから　［基本設定］を選択します。ファイアウォールの［基本設定］ページが表示されます。［WAN->DMZアクセス初期ルール］を［Discard］に設定して［適用］ボタンをクリックしてください。

次に、［ファイアーウォール設定］ページの上部メニューバーから　［アクセスルール］を選択します。［アクセスルール］ページが表示されます。［アクセスルールの方向］で［WAN->DMZ］を選択して［設定］ボタンをクリックしてください。

［WAN->DMZアクセスルール］の設定ページが表示されます。各設定項目に次のような値を入力して［追加］ボタンをクリックしてください。

プロトコル　　：TCP
送信元IPアドレス：開始 0.0.0.0、終了 0.0.0.0
送信先IPアドレス：開始、終了とも x.x.x.x（DMZネットワーク上のWEBサーバのIPアドレス）
ポート番号　　：開始、終了とも 80
処理　　：Forward
ログ　　：アクセス状況を記録する場合は On

これで、インターネット（WAN）からのDMZネットワークへのアクセスは、WEBサーバのhttp（ポート80）のみが許可されその他のアクセスはすべて遮断されるようになります。

4 URLフィルタ

ここでは、URLフィルタおよびコンテンツフィルタの設定を行います。ここで登録されたURL、IPアドレス、キーワードの含まれるWEBサイトへのLAN側からのアクセスを制限する事が出来ます。

[ファイアーウォール設定]ページの上部メニューバーから [URLフィルタ]を選択します。[URLフィルタ] ページが表示されます。表示される設定項目に必要な情報を入力します。

◎URLフィルタリスト

アクセス制限したいURL、IPアドレス、キーワードのいずれかを入力します。LAN側ネットワーク上のユーザがwww.website.comというWEBサイトへアクセスするのを禁止したい場合は、www.website.comまたはwebsite（キーワード入力）と入力してください。もしwebまたはsiteと入力した場合は、URLにwebまたはsiteを含んだすべてのWEBサイトへのアクセスが禁止されます。

> **注意**
>
> ***URLフィルタを設定した場合には、LAN → WANフィルタにフィルタリングルールが追加されます。追加されたフィルタリングルールを削除しないようにしてください。***

◎コンテンツフィルタ
ActiveX 、Java 、Cookie、Proxyの各サービスについて、受け付けるかどうかを設定できます。受け付けるサービスは「許可」に、拒否するサービスには「拒否」に設定します。

入力内容を確認して［適用］ボタンをクリックしてください。入力した内容が反映されたページが表示されます。
画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

5 E-Mail通知

本製品はE-Mail通知機能を搭載しています。E-Mail通知機能では本製品のイベントログを登録したE-Mailアドレスに送信することができます。また、Denial of Service（DoS）攻撃を検出した場合は、その情報を、登録したE-Mailアドレスに送信します。

［ファイアーウォール設定］ページの上部メニューバーから　［E-Mail通知］を選択します。［E-Mail通知］ページが表示されます。表示される設定項目に必要な情報を入力します。

◎E-Mail通知機能を有効にする

E-Mail通知機能を有効にする場合は「はい」に、無効にする場合には「いいえ」に設定します。

◎E-Mailアドレス

通知先のE-Mailアドレスを入力します。E-Mailアドレスは@を含めて、ドメイン名まで正しく入力してください。

例：myname@planex.co.jp

◎メール（SMTP）サーバアドレス
通知先メールアドレスのメールサーバーを入力します。

例：mail.planex.co.jp

入力内容を確認して［適用］ボタンをクリックしてください。入力した内容が反映されたページが表示されます。
画面左側のメニューから「保存して再起動」をクリックしてください。メッセージが表示されますので、［はい］ボタンをクリックしてください。［はい］ボタンをクリックすると、変更した設定内容が保存され本製品が再起動を開始します。（再起動には約10秒かかります）

注意

- ***プロバイダによっては、メール（SMTP）サーバで外部ネットワークからのメール送信（転送）を禁止していたり、POP before SMTP（メールを送信する前にメールの受信が必要）の制限をしている場合があります。この場合、E-Mail通知機能でメール送信ができないことがあります。これらの制限についてはプロバイダにご確認ください。***
- ***E-Mail通知機能を有効にするには、必ずE-Mailアドレス と メール（SMTP）サーバアドレスの両方を正しく入力してください。***
- ***DoS攻撃を検出した場合は登録したE-Mailアドレスに対して、即座に警告メッセージが送信されます。***
- ***イベントログが送信されると、その時点でそれまでのログ情報は消去されます。***

6 イベントログ

ここでは本製品のイベントログの参照、送信、消去が出来ます。

[ファイアウォール設定] ページの上部メニューバーから　[イベントログ] を選択します。[イベントログ] ページが表示されます。

◎表示の更新
このボタンをクリックすると、表示内容を最新のものに更新します。

◎ログの送信
このボタンをクリックすると、「6-5　E-Mail通知」で設定したE-Mailアドレスにイベントログを送信します。

◎ログの消去
このボタンをクリックすると、ログを消去します。

> **注意**
> ***イベントログがメール送信されると、その時点でそれまでのログ情報は消去されます。イベントログは記録容量の上限に達すると上書きされます。また、本製品を再起動した場合もイベントログは消去されます。***

その他の機能

こ

こでは本製品のその他の機能について説明します。

1 パスワード設定

ここでは本製品の管理ユーザ（admin）のパスワードの設定を行います。セキュリティ上、デフォルトのパスワードから変更してご使用になることをお勧めします。

WEBブラウザの画面左側から、[システム設定] の文字をクリックします。メインメニューに [パスワード設定] ページが表示されます。

◎現在のパスワード

パスワードを変更する場合にはここに現在設定されているパスワードを入力します。セキュリティのため、この欄に文字を入力しても“＊”(アスタリスク) 表示されます。(工場出荷時の状態では「password 」に設定されています。)

◎新しいパスワード

WEBブラウザやTELNET で本製品の設定画面を開く際に必要になる管理者パスアワードを設定します。セキュリティのため、この欄に文字を入力しても“＊”(アスタリスク) 表示されます。

例：PassWord

> **注意**
> *最高8文字の半角英数字を入力可能です。大文字・小文字の違いに注意して入力してください。*

◎パスワードの確認

誤入力防止のため、上記 [管理者パスワード] で入力した文字を再入力してください。セキュリティのため、この欄に文字を入力しても“＊”(アスタリスク) 表示されます。

例：PassWord

> **注意**
> *最高8文字の半角英数字を入力可能です。大文字・小文字の違いに注意して入力してください。*

入力内容を確認して「適用」ボタンをクリックします。次のログイン時よりパスワードが変更されます。

> **注意**
> *パスワードを忘れた場合にも設定画面にアクセスできなくなりますので、忘れないようにしてください。*

2 日付&時間

ここでは本製品に内蔵されている日付と時刻の設定を行います。

[システム設定] ページの上部メニューバーから [日付＆時間] を選択します。[日付と時刻の設定] ページが表示されます。表示される設定項目に必要な情報を入力します。

◎タイムゾーン

タイムゾーンの選択をします。日本国内の場合、タイムゾーンには GMT+09:00 を選択してください。

◎時刻

現在の時刻を入力します。時刻は24時間フォーマットで入力してください。

◎日付

現在の日付を入力します。

◎このコンピュータの日付と時刻を取得

このボタンをクリックすると、現在設定を行うためにアクセスしているコンピュータから現在の日付と時刻を取得できます。

入力内容を確認して「適用」ボタンをクリックします。日付と時刻が変更されます。

注意

再起動を行うと、現在の日付と時刻のデータが消去され、前回設定を行った時点のデータに戻ってしまいます。再起動後、もう一度日付と時刻の設定を行ってください。

3 ステータス表示

ここでは本製品の現在のステータスの表示をします。ステータスには本製品のWAN側ポートの接続状況や、ファームウェアのバージョン等が含まれます。

WEBブラウザの画面左側から、[ステータス表示] の文字をクリックします。メインメニューに [ステータス表示] ページが表示されます。

◎インターネット接続ステータス

現在のWAN側ポートのステータスです。WAN側ポートのIPアドレスをDHCPサーバから取得している場合は、「WAN側IPアドレスを開放」ボタンをクリックするとWAN側のIPアドレスを開放します。「WAN側IPアドレスの再取得」ボタンをクリックするとWAN側IPアドレスの開放と再取得をします。

◎ルータステータス

現在の本製品のファームウェアバージョンとLAN側のステータスです。

［ステータス表示］ページの上部メニューバーから ［アクセス状況］を選択すると、現在のLAN側からWAN側へのアクセス状況が表示されます。

「ローカルIPアドレス」が現在WAN側へアクセスしている端末のIPアドレスです。「アクセス先IPアドレス」がLAN側の端末がアクセスしているWAN側のIPアドレスです。「ポート番号」がその時に使用しているポートになります。

4 診断ツール

ここでは障害発生時に本製品の機能が正常に動作しているか診断することができます。

■PPPoE接続診断

ここではPPPoE接続が正常に行えるかどうかの診断を行います。また、PPPoE接続の設定でサービスオンデマンド（自動接続）および自動切断を無効に設定した場合の手動での接続/切断もここで行います。
ブラウザ画面左側のメニューから、[診断ツール] の文字をクリックします。メインメニューに [PPPoE診断] ページが表示されます。

◎ [接続]

[接続] ボタンをクリックすると現在のPPPoE接続設定を使用してPPPoE接続を開始します。

正常にPPPoE接続が開始されると、接続ログの最後の行に

Your PPPoE DSL connection is up and running now!

と表示されます。Connecting Service Failed等、それ以外のメッセージが表示された場合はPPPoE接続に失敗しています。ケーブル接続や設定に間違いがないか確認してください。

◎ [切断]

[切断] ボタンをクリックするとPPPoE接続を切断し、切断ログを表示します。

■Ping診断

ここではインターネットへの接続を確認するために、pingコマンドを実行することができます。pingコマンドではリモートホスト（コンピュータ）に対して応答要求パケットを送信し、これに対しての応答パケットを受信します。[PPPoE診断] ページの上部メニューバーから [Ping] を選択すると、Pingユーティリティー画面が表示されます。

pingコマンドを実行するにはリモートIPアドレスにリモートホストのIPアドレスを入力してping実行ボタンをクリックしてください。sentとrcvdが同値の結果が表示されていれば、リモートホストへの通信は正常に行えています。Request time outと表示された場合は、リモートホストへ正常に通信が行えていません。

5 保存して再起動

ブラウザ画面左側のメニューから、[保存して再起動] の文字をクリックします。

メインメニューに [保存して再起動] ページが表示されます。

ここで「はい」をクリックすると現在の設定が保存され有効になります。

注意

- ***本製品の設定を変更した場合は変更を反映させるため、必ず［保存して再起動］を実行してください。***
- ***本製品はバッテリーを内蔵していないため、再起動を行うと現在の日付と時刻が前回設定を行った時点のデータに戻ってしまいます。再起動後、もう一度日付と時刻の設定を行ってください。***

6 設定情報の保存/読み込み

ここでは、本製品の設定情報を保存したり、保存した設定情報を読み込ませる事ができます。
ブラウザ画面左側のメニューから、[設定情報の保存/読み込み] の文字をクリックします。メインメニューに [設定情報の保存/読み込み] ページが表示されます。

◎設定情報ファイルの読み込み
ボックスに読み込ませたい設定ファイルをフルパスで指定します。また、[参照] ボタンをクリックするとファイルの選択画面になります。読み込ませたいファイルを選択して [開く] ボタンをクリックしてください。ファイルがフルパスで入力されます。
ファイルを指定したら、[設定情報の読み込み] ボタンをクリックしてください。設定ファイルが読み込まれ、再起動します。

注意

- *設定情報を読み込ませると自動的に再起動します。LAN側IPアドレスやインターネット設定もすべて読み込まれた設定ファイルの情報に変わります。アクセスするコンピュータの設定を読み込ませた設定情報に合わせてください。*
- *本製品のファームウェアのアップデートを行った場合、前のバージョンのファームウェアで保存した設定情報の読み込みはできない場合があります。*

◎設定情報のファイルへの保存

[設定情報の保存] ボタンをクリックしてください。ファイルのダウンロードウィンドウが表示されますので、この「ファイルをディスクに保存する」を選択して、[OK] ボタンをクリックしてください。「保存する場所」と「ファイル名」を指定するウィンドウが開きますので、それぞれ指定して、[保存] ボタンをクリックしてください。設定情報ファイルが保存されます。

7 ファームウェアのアップデート

ここでは本製品のファームウェアのアップデートを行えます。
ブラウザ画面左側のメニューから、[ファームウェアのアップデート] の文字をクリックします。メインメニューに [ファームウェアのアップデート] ページが表示されます。

◎ファームウェアのアップデート
ボックスに読み込ませたいファームウェアをフルパスで指定します。また、[参照] ボタンをクリックするとファイルの選択画面になります。ファームウェアを選択して [開く] ボタンをクリックしてください。ファームウェアがフルパスで入力されます。
ファームウェアを指定したら、[アップデート] ボタンをクリックしてください。ファームウェアが読み込まれ、再起動します。

注意

最新のファームウェア情報につきましては、弊社ホームページ（http://www.planex.co.jp/）をご覧ください。

8 設定の初期化

ブラウザ画面左側のメニューから、[設定の初期化]の文字をクリックします。
メインメニューに [設定の初期化] ページが表示されます。

「はい」をクリックすると本製品の設定を工場出荷時のデフォルト設定に戻します。
デフォルト設定に戻すと、すべての設定が消去されます。

トラブルシューティング

■ POWER LEDが点灯しない

●本製品付属のACアダプタを使用していますか？
●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が点灯しない

●LANケーブルの両端はそれぞれ、本製品背面のWAN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？
●LANケーブルの種類（ストレートまたはクロス）は合っていますか？

■ LAN LEDが点灯しない

●LANケーブルの両端はそれぞれ、本製品背面のLANポートおよびハブ（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？
●ハブ（コンピュータ）の電源は入っていますか？
●LANケーブルの種類（ストレートまたはクロス）は合っていますか？

■ WEB設定画面が表示されない

●コンピュータのネットワークアダプタは正常に動作していますか？コンピュータまたはネットワークアダプタのマニュアルを参照してネットワーク設定を確認してください。
●コンピュータのTCP/IPの設定が間違っている可能性があります。IPを自動取得（DHCPを使用）する設定にしてください。
●使用しているWEBブラウザで、プロキシが設定されていると設定画面が表示されません。プロキシを使用しない設定にしてください。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。

●コンピュータがIPアドレスを取得できていない可能性があります。
→WindowsではDOSプロンプトから、ipconfig コマンドを実行するとIPアドレスが表示されています。Macintoshでは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、IPアドレスの欄にIPが割り振られてるか確認してください。コンピュータがIPアドレスを取得できてない場合は、コンピュータを再起動してください。（デフォルト設定時は192.168.1.xxx がIPアドレスとして割り当てられます。）

■ インターネットにアクセスできない

●WAN側のIP設定が間違っている可能性があります。
→プロバイダから受け取っているIP設定の資料をよく確認し、「第4章」の設定をやり直してください。
●DNSサーバの設定が間違っている可能性があります。
→DHCPサーバ機能を利用されている場合はプロバイダから受け取っているIP設定の資料をよく確認し、「第4章」または「5-1 DHCPサーバ」の設定をやり直してください。
→DHCPサーバ機能を利用していない場合はプロバイダから受け取っているIP設定の資料をよく確認し、コンピュータのDNSサーバ設定を確認してください。
●IPフィルタが設定されていませんか？
→IPフィルタの設定を確認してください。

■ パスワードを忘れてしまった

●本製品の管理者パスワードを忘れてしまい、設定画面にログインできなくなってしまった場合は、「付録C デフォルト設定の復帰」を参照し、本製品を工場出荷時の状態に戻してください。

■ MACアドレスがわからない

●本製品のMACアドレスは本体底面のシールに印刷されています。Node ID： の後の12桁の文字列が本製品のMACアドレスです。

TFTPを使用したファームウェアのアップデート

本製品はWEBブラウザから簡単にアップデートが可能です。通常はWEBブラウザから、ファームウェアのアップデートを行ってください。もし、TFTPを使用してアップデートを行う場合には、ここで説明する手順でアップデートを行ってください。ファームウェアは、弊社ホームページ上（http://www.planex.co.jp/）からダウンロードしてください。

⚠ 注意

アップデートに使用するコンピュータは、必ず本製品のプライベートLAN上に接続してください。また、アップデートに使用する以外のコンピュータおよびWAN側のADSL/ケーブルモデムを外しておいてください。

ファームウェアのファイルをホームページからダウンロードしたら、以下の手順でアップデートを行ってください。

■ Windows NT/2000でのアップデート

1. 本製品のプライベートLAN上に接続したコンピュータで、「スタート」メニューの「プログラム」から「コマンドプロンプト」を実行してください。

2. ダウンロードしたファームウェアファイルをigate17.binというファイル名に変更してから現在のディレクトリにコピーしてください。（プロンプト表示がC:\TEMP＞ の場合は C: のTEMPフォルダにコピーしてください。）

3. コマンドプロンプトで以下のように入力してください。ファームウェアの転送が開始されます。

   tftp 本製品のLAN側IPアドレス get upgrade
   tftp -i 本製品のLAN側IPアドレス put igate17.bin

4. しばらくして、「Transfer Successful」というメッセージが表示されれば、アップデートは成功です。

⚠ 注意

●ファームウェアの書き換え作業中は、STATUS LEDが点滅します。STATUS LEDが点滅している間は、本製品およびコンピュータの電源を絶対に切らないでください。ファームウェアの書き換えに失敗し、復旧不能となる場合があります。

●ファームウェアのアップデートに失敗するとSTATUS LEDが点滅し続けます。この場合は本製品の電源を切ったり、再起動を行ったりせずにもう一度上記手順3のコマンドを実行してみてください。それでもファームウェアのアップデートが成功しない場合は、弊社テクニカルサポートまでご連絡ください。

■ UNIXでのアップデート

1. **ルート（root）でログインしてください。**

2. **ダウンロードしたファームウェアファイルをigate17.binというファイル名に変更してから現在のディレクトリにコピーしてください。**

3. **コマンドプロンプトから以下のコマンドを入力してください。**
   tftp 本製品のLAN側IPアドレス

4. **TFTPプロンプトで以下のコマンドを入力してください。**
   get upgrade
   binary
   put igate17.bin

5. **しばらくして、ファイル転送が終了したらアップデートは完了です。**

6. **TFTPを終了してください。**

⚠ 注意

ファームウェアのアップデートに失敗するとSTATUS LEDが点滅し続けます。この場合は、本製品の電源を切ったり、再起動を行ったりせずにもう一度上記手順4のコマンドを実行してみてください。それでもファームウェアのアップデートが成功しない場合は、弊社テクニカルサポートまでご連絡ください。

■ Macintoshでのアップデート

Macintoshからファームウェアをアップグレードする場合にはMacintosh用TFTPクライアントソフトを利用します。ここでは代表的なMacintosh用TFTPクライアントソフト「MacTFTP Client」を利用した方法を説明します。

以下は「MacTFTP Client」が配布されているホームページアドレスです。ここからソフトウェアをダウンロードしてください。

MacTFTP
http://www.macorchard.com/ftp.html#MacTFTP

1. 「MacTFTP Client」とファームウェアファイルをMacintosh上にダウンロードします。ファームウェアファイルはigate17.binというファイル名に変更してください。

2. 「MacTFTP Client」を起動します。
   (1) [Receive] ボタンをクリックして反転表示させてください。
   (2) [Address] 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。
   (3) [File] ボタンをクリックし、名前欄に「Upgrade」と入力し、[保存] ボタンをクリックしてください。
   (4) [Start] ボタンをクリックしてください。

3. "Tranfer Complete Successfully"と表示されますので、[Reset] ボタンをクリックしてください。
   (1) [Send] ボタンをクリックして反転表示させてください。
   (2) [File] ボタンをクリックしてください。
   ファームウェアファイル (igate17.bin) を指定して開くボタンをクリックしてください。
   (3) [Address] 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。
   (4) [Start] ボタンをクリックしてください。

4. "Transfer Complete Successfully"と表示されます。以上でファームウェアの更新は終了です。

デフォルト設定の復帰

本製品のログインパスワードやIPアドレスを忘れてしまって場合や、不正なIPフィルタを追加してしまったなどの理由で、本製品のWEB設定画面にログインできなくなってしまった場合は、以下の手順で本製品を工場出荷時のデフォルト設定に戻してください。

1. 電源コードを外し本製品の電源を切ってください。
2. 本体背面のリセットスイッチを押したままの状態で、電源ケーブルを接続し電源を入れてください。STATUS LEDが点滅を開始します。
3. そのまま、リセットスイッチを10秒以上押し続けてください。10秒たったらスイッチを離してください。

デフォルト設定

本 製品の工場出荷時のデフォルト設定は以下のようになっています。デフォルト設定の読込みを行った場合も、以下の設定が読込まれます。

項目		設定内容
LAN側	IPアドレス	192.168.1.1
	サブネットマスク	255.255.255.0
DHCPサーバ	DHCPサーバ	有効
	DHCP IP割当て範囲	192.168.1.21～121
	プライマリDNS	0.0.0.0
	セカンダリDNS	0.0.0.0
WAN側	IPアドレス	0.0.0.0
	サブネットマスク	0.0.0.0
	デフォルトゲートウェイ	0.0.0.0
	DHCPクライアント	有効
	PPPoE接続	無効
NAPT機能		有効
パスワード		password
ドメイン名		未設定
ホスト名		broadlanner
ローカルサーバ		なし
DMZポート		なし
ファイアウォール		有効

telnet設定

本 製品をtelnetを使用して設定する場合の設定メニューのメニュー構成について説明します。

注意

telnet設定では、WEBブラウザ設定で行えるすべての設定をサポートしていません。通常の設定はWEBブラウザから行うようにしてください。

＜0.General Information メニュー＞

Administrator Security Setup

Old password	現在のパスワードの入力
New password	新しいパスワードの入力
Retype Password	新しいパスワードの再入力
Authorize MAC Address	MACアドレスによる管理端末のチェック（Yes/No）
Admin's MAC Address	管理端末のMACアドレス

System Setup

LAN IP Address	LAN側IPアドレス
LAN Netmask	LAN側サブネットマスク
Default Gateway	デフォルトゲートウェイ
Domain Name	ドメイン名
Host Name	ホスト名
Service On Demand	PPPoE自動接続（Yes/No）
Network Address Translation	NAPT機能（Yes/No）

＜1.WAN Port Setup＞

Service Type	WAN側サービスタイプの変更
Regular Service Setup	通常接続の設定
PPPoE Sevice Setup	PPPoE接続の設定

＜2.DHCP Server Setup＞

Using DHCP Server .....DHCPサーバの有効/無効
Domain Name Server IP ....プライマリDNSのIPアドレス
Secondary DNS Server IP....セカンダリDNSのIPアドレス
WINS IP.....WINSサーバのIPアドレス
Dynamic-IP Range Setup ...IP割当て範囲の設定
Fixed IP Table Setup .....固定IP割当ての設定
DHCP Leased Table.....DHCP割当中IPリスト

＜3.Local Server Setup＞

Add a New Entry .....ローカルサーバ設定の追加
Delete an Old Entry.....ローカルサーバ設定の削除

＜4.DMZ Port Setup＞

Add a New Range .....DMZネットワークアドレス範囲の追加
Delete an Old Range .....DMZネットワークアドレス範囲の削除

＜5.FireWall Setup＞

Firewall Setup .....ファイアーウォール設定
Firewall Policy Rules .....アクセスルール設定
Date & Time Setting .....日付と時刻の設定
Log Setting.....ログ及びE-Mail通知設定
URL Filter .....URLフィルタ設定
Web Filter .....コンテンツフィルタ設定

＜6.Static Route Setup＞

Add a New Entry .....ルーティング情報の追加
Delete an Old Entry.....ルーティング情報の削除

＜7.Service Diagnostic＞

Connect Service.....PPPoEの接続
Disconnect Service .....PPPoEの切断
PING Host .....pingの実行

＜8.Internet Spy＞

アクセス状況の表示

＜S.Save & Reboot＞

保存して再起動

＜D.Load the default value＞

デフォルト設定の読み込み

＜E.Exit＞

設定画面からのログアウト

仕様

＜準拠する標準＞
IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX

＜ポート＞
LAN : 10BASE-T/100BASE-TX RJ-45 スイッチ × 7ポート
WAN : 10BASE-T RJ-45 × 1ポート
DMZ : 10BASE-T RJ-45 × 1ポート

＜LED＞
POWER、STATUS、WAN、LAN、DMZ

＜入力電源＞
DC 5V、2A

＜消費電力＞
最大10W

＜外形寸法（W×D×H）＞
224.4 × 144.6 × 34 mm

＜重量（本体のみ）＞
424g

＜環境＞
動作温度 0～40℃
動作湿度 35～85%

＜EMI＞
FCC Class A , CE Mark

Memo

Memo

Memo

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。ぜひ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。ユーザー登録を行って戴いたお客様の中から毎月抽選でプレゼントを差し上げております。

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

質問表

技術的なご質問は、この2ページをコピー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：03-5614-1018

送信日：＿＿＿＿＿＿＿＿

会社名			
部署名			
名前			
電　話		FAX	
E-MAIL			

製品名 Product name	7ポート DMZ ファイアウォール ルータ
型番 Product No.	**BRL-07DMZ**
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 ソフトウェア

ネットワークOS	バージョン
OS	バージョン

③ ご使用のプロバイダについて

プロバイダ名	
サービス名	

④ 質問内容

保証規定

プラネックスコミュニケーションズ（株）は、本製品についてご購入日より本保証書に記載の保証期間を設けております。
本製品付属の取扱説明書などに従った正常な使用状態の下で、万一保証期間内に故障・不具合が発生した場合、本保証規定に基づき無償修理・交換対応を行います。
ただし、次のような場合には保証期間内であっても有償修理となります。

1. 本保証書がない場合。
2. 本保証書に、ご購入日・お名前・ご購入代理店印の記入がない場合、または字句が改ざんされている場合。
3. 取扱上の誤り、または不当な改造や修理を原因とする故障及び損傷。
4. ご購入後の輸送・移動・落下による故障及び損傷。
5. 火災、地震、落雷、風水害、ガス害、塩害、異常電圧およびその他の天変地異など、外部に原因がある故障および損傷。
6. 他の機器との接続に起因する故障・損傷。

初期不良交換

保証期間発生日より1ヶ月以内の故障に関しては、初期不良交換サービスの対象となります。
お客様より初期不良である旨申告していただき、弊社がその申告現象を確認した場合に限り、初期不良品として新品と交換いたします。
ただし、検査の結果、動作環境や相性を起因とする不具合であった場合には、初期不良交換サービス対象とはなりません。また、当サービスをご利用頂くには、お買い上げ商品の全ての付属品が揃っていることが条件になります。

◎初期不良・修理の手順（センドバック方式）

弊社は、センドバック方式による初期不良・修理対応を行っております。

1. 本製品に故障・不具合が発生した場合、下記サポートセンターまでご連絡ください。受付番号を発行いたします。
   プラネックスコミュニケーションズ（株）
   サポートセンター　フリーダイヤル 0120-415977
2. 受付番号を明記の上、本製品及び保証書を弊社リペアセンターまでお送りください。
   （誠に勝手ながら、修理品発送の際の送料はお客様のご負担にてお願いいたします。）
3. 当該初期不良・修理品の到着後、初期不良の場合は交換品、修理の場合は修理完了品をお送りいたします。

免責事項

- お客様及び第三者の故意または過失と認められる本製品の故障・不具合の発生につきましては、弊社では一切責任を負いません。
- 本製品の使用及び不具合の発生によって、二次的に発生した損害（事業の中断及び事業利益の損失、記憶装置の内容の変化、消失等）につきましては、弊社では一切責任を負いません。
- 本製品に装着することにより他の機器に生じた故障・損傷について、弊社では本製品以外についての修理費等は一切保証致しません。

※本保証書は日本国内においてのみ有効です。　This warranty is valid only in Japan.

保証書

保証期間 Warranty	西暦　　年　　月　　日より　1　年間		
製品名 Product Name	7ポートDMZ ファイアウォール ルータ		
型番 Product No.	BRL-07DMZ	製造番号 Serial No.	

□個人使用　□法人使用（チェックしてください。）
※ 個人でご使用の場合には、個人名、および住所以降の欄にのみご記入ください。

フリガナ			
会社名			
部署名			
フリガナ			
お名前			
フリガナ			
ご住所	□□□-□□□□ 都道 府県		
TEL		FAX	
メールアドレス			
ご購入 代理店名 ・所在地			

技術的なご質問、バージョンアップ等のお問い合わせは
お気軽に下記へご連絡ください。
なお弊社ホームページにてユーザー登録を行って
いただいていない場合には、
一切のサポートは受けられませんのでご注意ください。

フリーダイヤル：0120-415977
受付時間：月曜日～金曜日（祭日は除く）
10:00～12:00・13:00～17:00
FAX：03-5614-1018
ユーザー登録：http://www.planex.co.jp/user/user.htm

ご質問の受付やドライバのアップデートを
下記Webサイトで行っておりますのでご利用ください。

http://www.planex.co.jp/
E-MAIL:info-planex@planex.co.jp

プラネックスコミュニケーションズ株式会社