



# USER'S MANUAL

4ポート ブロードバンド ファイアウォール ルータ

## **BRL-04FW**

**PLANEX COMMUNICATIONS INC.**



# **USER'S MANUAL**

4ポート ブロードバンド ファイアウォール ルータ

**BRL-04FW**

# 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。



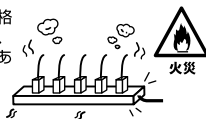
### 正しい電圧で使用して！

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。



### 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。



### 液体・異物はいれないで！

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。



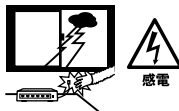
### 設置・保管場所をもう一度確認して！

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

### 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。



### 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。



### 電源コードをつけて移動しないで！

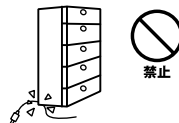
本製品を設置・移動する際は、必ず電源コードを前もって抜いておいてください。電源コードを入れたまま移動し、コードが傷つくと誤動作や火災につながるおそれがあります。



### 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）



### ◎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4ポート・ブロードバンドファイアウォール ルータ bRoad Lanner BRL-04FW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準備

本製品をWebブラウザ経由で設定や、設定が画面にアクセスするまでの手順について説明します。

### 第4章 インターネット設定

本製品を使って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

DHCPサーバ機能、ローカルサーバ機能、バーチャルコンピュータ機能の設定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機能の設定方法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 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。

記載の会社名および製品名は各社の商標または登録商標です。

# 目次

---

本製品を安全にお使いいただくために	2
<b>第1章 はじめに</b>	
1.概要	7
2.特長	8
3.梱包内容の確認	8
4.各部の名称	9
5.対応機器	12
<b>第2章 ハードウェアの接続</b>	
1.ADSL/ケーブルモデムとの接続 (WAN側ポート)	13
2.ネットワークとの接続 (LAN側ポート)	14
3.電源の接続	14
4.接続の確認	15
5.本製品のリセット手順	16
6.電源投入時の自己診断テストについて	16
<b>第3章 Webブラウザを使った設定準備</b>	
1.コンピュータの設定	17
2.コンピュータのIPアドレスの確認	21
3.WWWブラウザからのアクセス	23
<b>第4章 インターネット設定</b>	
1.インターネット設定	25
2.PPPoE設定	27
3.PPPoE複数IP設定	32
4.CATV設定	41
5.ローカルネットワーク設定	51

---

<b>第5章 詳細設定</b> .....	47
1.DHCPサーバ .....	48
2.ローカルサーバ .....	51
3.バーチャルコンピュータ .....	53
4.ルーティング .....	55
<b>第6章 ファイアウォール設定</b> .....	59
1.基本設定 .....	61
2.LAN WANフィルタ .....	64
3.WAN LANフィルタ .....	67
4.URLフィルタ .....	70
5.E-Mail通知 .....	71
6.イベントログ .....	73
<b>第7章 その他の機能</b> .....	
1.パスワード設定 .....	75
2.日付&時間 .....	77
3.ステータス表示 .....	78
4.診断ツール .....	80
5.保存して再起動 .....	82
6.設定情報の保存/読み込み .....	83
7.ファームウェアのアップデート .....	84
8.設定の初期化 .....	85
<b>付属A トラブルシューティング</b> .....	87
<b>付属B TFTPを使用したファームウェアのアップデート</b> .....	91
<b>付属C デフォルト設定の復帰</b> .....	95
<b>付属D デフォルト設定</b> .....	97
<b>付属E telnet設定</b> .....	99
<b>付属F 仕様</b> .....	103





# 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。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。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。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。

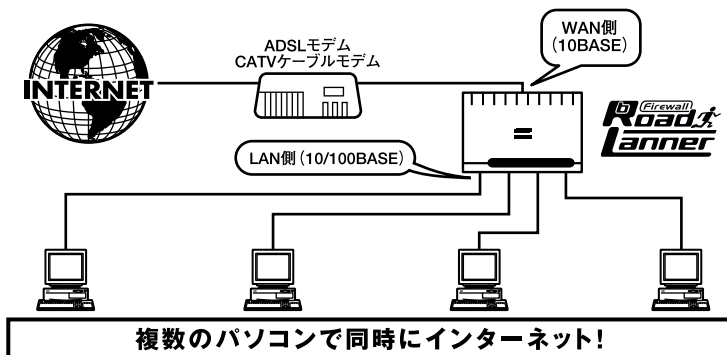


図1-1 bRoad Lanner接続図



### 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4ポートスイッチングハブを内蔵  
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およびバーチャルコンピュータ機能により、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  
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  
マルチNAT機能によりADSLによる複数のグローバルIP接続サービス対応  
ARMプロセッサによる高速ルーティング  
WEBブラウザまたはtelnet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-04FW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  
ユーザズマニュアル  
簡単設定マニュアル  
保証書(ユーザ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

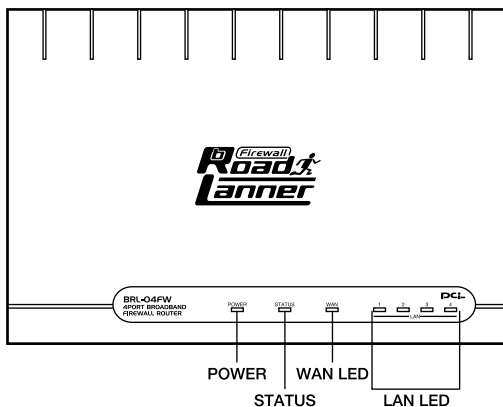


図1-2 BRL-04FW本体上面

#### 「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。

#### 「LAN LED」

LAN側ポートが100Mでリンクが確立すると、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

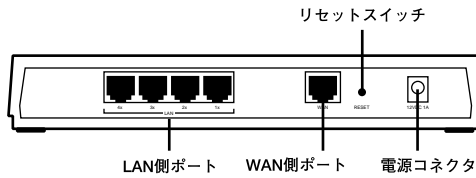


図1-3 BRL-04FW本体背面

## 「LAN側ポート」

本製品をLANと接続するためのRJ-45 LANポートです。

## 「WAN側ポート」

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。

## 「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が点滅を始めるまで)押してください。

## 本体裏面

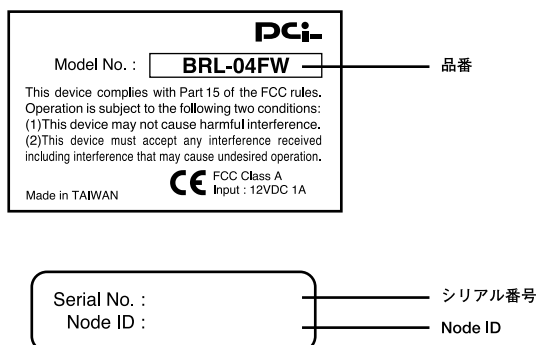


図1-4 BRL-04FW本体裏面

## 「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となります。

## 「Node ID」

本製品の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。

## 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/NT/2000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。

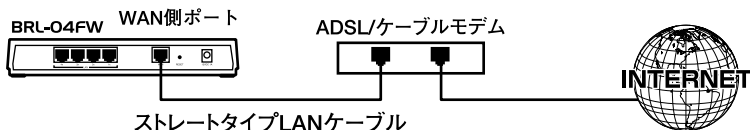


図2-1 ADSL/ケーブルモデムとの接続



### 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。

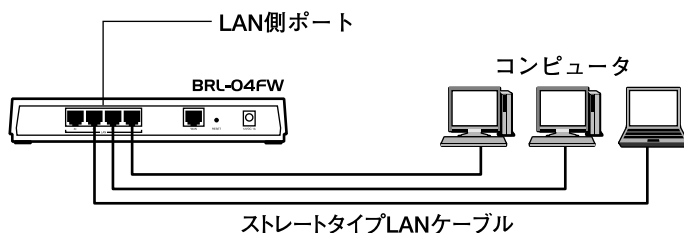


図2-2 ネットワークとの接続

## 3 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。



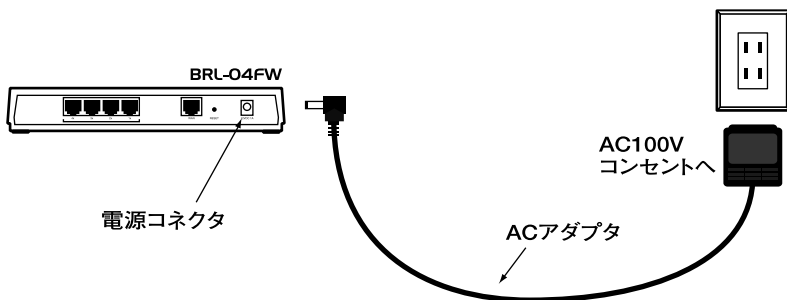


図2-4 電源の接続

**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。

**4****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？

## 5 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。

## 6 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6回点滅します。このLEDが6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

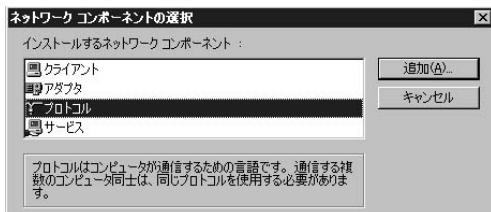
Windows95/98/Me

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。

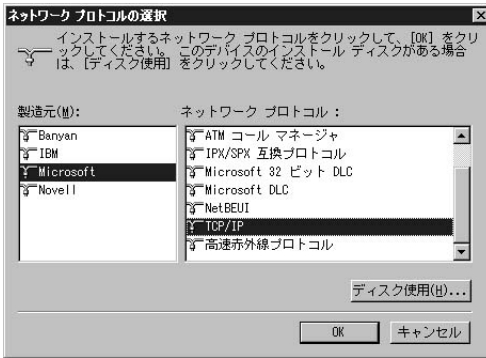
2. コンピュータにTCP/IPプロトコルがインストールされていることを確認します。「スタート」メニューから「設定」「コントロールパネル」「ネットワーク」と選択してください。「現在のネットワークコンポーネント」の欄に「TCP/IP」が表示されているか確認してください。インストールされている場合は手順5に進んでください。



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

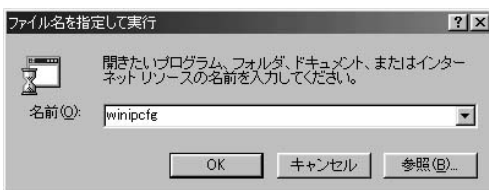
ご利用のコンピュータまたはOSのマニュアル及びドキュメントを参照にして、ネットワークプロトコルをTCP/IPに設定してください。IPアドレスはDHCPサーバから取得する設定にしてください。

## 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。



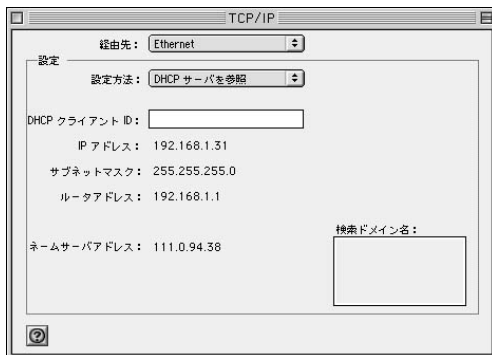
3. IP設定ウィンドウが表示され、現在のIPアドレスが表示されます。bRoadLannerが工場出荷時の状態の場合には 192.168.1.xxx( xxxは21 ~ 120 というIPアドレスが割り振られます。ここでIPアドレスが正常に割り振られていない場合には、bRoadLannerとパソコンの接続を確認して、パソコンを再起動させてください。



IPアドレスが正常に取得できていましたら「3-3 WWW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。



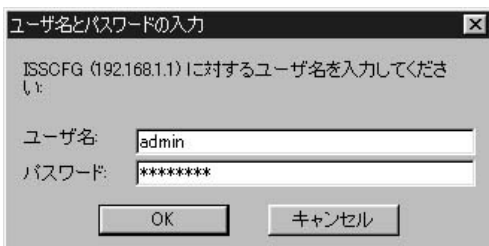
3. 「IPアドレス」に表示されている値が現在のIPアドレスです。bRoadLannerが工場出荷時の状態の場合には 192.168.1.xxx( xxxは21～120) というIPアドレスが割り振られます。ここでIPアドレスが正常に割り振られていない場合には、bRoadLannerとパソコンの接続を確認して、パソコンを再起動させてください。

IPアドレスが正常に取得できていましたら「3-3 WWW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 WWWブラウザからのアクセス

1. コンピュータが起動したら、WWWブラウザを起動してください。
2. WWW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。)

# インターネット設定

こ

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. Webブラウザの画面左側から、[ インターネット設定 ]の文字をクリックします。メインメニューに[ 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。メインメニューに3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。

4

インターネット設定

### PPPoE設定

NTT東日本/NTT西日本の「フレッツ・ADSL」や東京めたりっく通信の「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。

### PPPoE複数IP設定

PPPoE接続で複数のグローバルIPアドレスを使用するLAN型接続のサービスをご利用になる場合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、PPPoEプロトコルを使用しないADSL接続サービス「Yahoo! BB」等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は、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ADSL 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。

また、複数の固定グローバルIP アドレスが割り当てられるPPPoE インターネット接続サービスの場合は、[ PPPoE複数IP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。

bRoed Lanner smart Manager

インターネット設定  
ローカルネットワーク設定  
システム設定  
スチルス表示  
初期ツール  
言語設定  
ファイアウォール設定  
保存して再起動  
設定情報の存在/読み込み  
アップデート  
設定の初期化  
ホーム

注意  
特定のグローバルIPアドレスを使用する、LAN接続のサービスに使用される場合は、PPPoE複数IP設定で設定を行ってください。

PPPoE接続の設定

ユーザ名: [ text ]  
パスワード: [ \*\*\*\* ]  
サービス名: [ text ]  
自動接続:  する  しない  
自動切断までの時間: [ 20 ] 分(0で自動切断なし)  
IPアドレス自動取得:  する  しない  
固定IPアドレス: [ 0 ] [ 0 ] [ 0 ] [ 0 ]  
DNSアドレス自動取得:  する  しない  
固定DNSアドレス1: [ 002 ] [ 002 ] [ 004 ] [ 006 ]  
固定DNSアドレス2: [ 0 ] [ 0 ] [ 0 ] [ 0 ]  
MSS(Maximum Segment Size): [ 412 ]

[ 適用 ] [ クリア ]

ユーザ名  
PPPoE接続を行うためのユーザ名(アカウント名)を入力してください。「フレッツ ADSL」の場合は、単独をきめこみ入力してください。(例: username@home.jp)

パスワード  
ユーザ名に接続するためのパスワードを入力してください。

サービス名  
サービス名が指定されている場合に指定されたサービス名を入力してください。サービス名が指定されていない場合は空欄のままでも構いません。

自動接続  
通信が完了したときに自動でPPPoEの接続を行います。[ 取 ]は通信を中断してください。

自動切断までの時間  
通信が完了したときに、無接続状態がPPPoEを自動で切断します。[ 取 ]は通信を中断してください。

IPアドレス自動取得  
[ 取 ]は設定していただき、[ 取 ]は(イサカ)の固定IPアドレスが指定されている場合は、[ 取 ]は[ 取 ]に設定していただき、[ 取 ]は(イサカ)の固定IPアドレスを入力してください。

DNSアドレス自動取得  
通信が完了したときに、通信が完了したときに(イサカ)の固定DNSアドレスが指定されている場合は、[ 取 ]は[ 取 ]に設定して、その[ 取 ]の固定DNSアドレスに指定されたDNSアドレスを入力してください。

MSS(Maximum Segment Size)  
PPPoE接続時の最大(7)のサイズを設定します。通信が完了したときに1412から変更する必要はありません。また「フレッツ ADSL」の場合は、必ず1412以下の値で入力してください。

## 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。以下のPPPoE サービス名が指定されていない場合は“ @ ”(アットマーク) 以下も入力します。(工場出荷時の状態では「your-name」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ドレス名などと異なる場合があります。

## 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。)

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

従量制の場合などで「無効」に設定した場合は、[アドバンスド設定] - [PPPoE接続の診断] 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」の場合は以下の「ルータ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。  
（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」の場合は以下の「プライマリDNSサーバ」及び「セカンダリDNSサーバ」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、パフォーマンスが著しく落ちますので注意してください。



#### 注意

MSS 値はインターネットスピードのパフォーマンスに影響を与えます。アプリケーションの都合でMSS 値を変更する場合は、そのアプリケーションの許容範囲の最大値を入力してください。



入力内容を確認し、正しければ[適用]ボタンを押してください。  
「設定を保存して再起動します。」メッセージが表示されますので、[はい]  
ボタンを押してください。[はい]ボタンを押すと、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)  
本製品の再起動後にコンピュータを再起動してください。インターネット  
に接続できます。



### 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。PPPoE接続が正常に行われない場合は、「第4章 4.PPPoEの診断」を参照してください。

## 3 PPPoE複数IP設定

[ PPPoE複数IP設定 ]では、PPPoEを使ったインターネット接続サービスで、複数の固定グローバルIPアドレスが利用可能なサービスをご利用の場合の設定を行います。



### 注意

PPPoE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。

また、IPアドレスが1個しか割り当てられない通常のPPPoE採用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。

## 4

## インターネット設定

### 複数グローバルIPアドレスサービスの利点

通常のPPPoEインターネット接続サービスではIPアドレスが1個しか割り当てられません。また、PPPoEでプロバイダに接続した際に空いているIPアドレスが割り当てられますので、接続するごとに毎回違うIPアドレスが割り当てられます。

これに対し、グローバルIPアドレスが固定的に割り当てられていると、常に同じグローバルIPアドレスでインターネットからアクセスできますので、サーバ公開には必須のサービスです。

### PPPoE 複数グローバルIPアドレス接続サービスについて

本マニュアルでは、PPPoE採用ADSLインターネット接続で複数のIPアドレスを提供するサービスを、「PPPoE複数IPアドレスLAN型接続サービス」としております。その他のサービスでは機能しない場合がありますのでご注意ください。

「PPPoE 複数グローバルIPアドレスLAN型接続サービス」はWeb設定画面のみで設定可能です。

## IPアドレスの割り当て方法

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、割り当てられる連続したグローバルIPアドレス空間のうち、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)には使用できません。また、本製品のようなルータに対するIP アドレスも必要になります。従って、お客様のホスト(コンピュータサーバ)で利用可能な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)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 までのグローバル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LAN 側ポート)
- 153.16.10.42 お客様ホスト用(例：プライマリDNS サーバ)
- 153.16.10.43 お客様ホスト用(例：WWW サーバ)
- 153.16.10.44 お客様ホスト用(例：メールサーバ)
- 153.16.10.45 お客様ホスト用(例：FTPサーバ)
- 153.16.10.46 お客様ホスト用(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)



### 注意

一般的にルータ(本製品LAN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で設定してください。

PPPoE複数IPアドレスLAN型接続で、バーチャルコンピュータ機能を利用する場合にはバーチャルコンピュータで登録されたグローバルIPアドレスをLAN側のグローバルIPアドレスとして利用する事は出来ません。

バーチャルコンピュータに登録したグローバルIPアドレスとLAN側のコンピュータ/サーバのIPアドレスと重複しないようにしてください。

## 本製品の機能

本製品の「PPPoE複数IPアドレス LAN型接続」機能を利用すると、プロバイダから割り当てられた複数のグローバルIP アドレスを持つパソコンを、本製品のLAN 側ポートに接続可能になります。さらに、プライベートIP アドレスを持つホスト( パソコン)も接続することができます。

この際、本製品のLAN 側ポートはグローバルIP アドレスとプライベートIP アドレスをそれぞれ1 個、合計2 つのIP アドレスを保持します。また、WAN 側ポートにはIP アドレスは割り当てられておらず、Unnumbered となります。

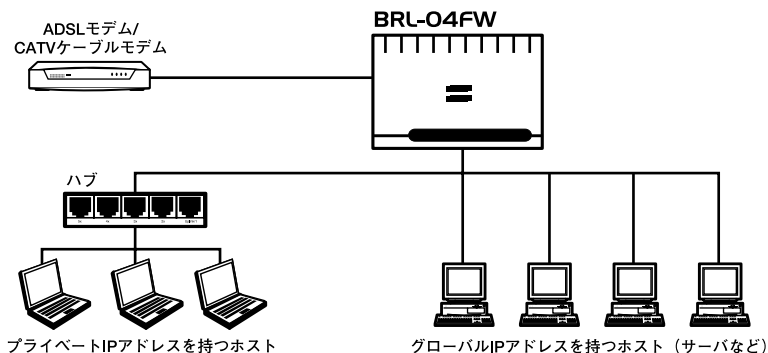


図4-1 PPPoE複数IPアドレス LAN型接続

グローバルIPアドレスネットワーク					
区分	ネットワークアドレス	デフォルトゲートウェイ	各ホストのアドレス	ブロードキャストアドレス	サブネットマスク
IPアドレス	割り当てられたIPアドレス範囲の最初のグローバルIPアドレス	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	ユーザ使用可能なグローバルIPアドレス	割り当てられたIPアドレス範囲の最後のグローバルIPアドレス	プロバイダから指定されたサブネットマスク
例: 153.16.10.40~ 153.16.10.45 の6個のグローバルIPアドレスが割り当てられている場合	153.16.10.40	153.16.10.41	153.16.10.42~ 153.16.10.44	153.16.10.45	255.255.255.240

表4-1 グローバルIPアドレス



### 注意

一般的にルータ(本製品LAN側ポート)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で設定してください。

プライベートIPアドレスネットワーク					
区分	ネットワークアドレス	デフォルトゲートウェイ	各ホストのアドレス	ブロードキャストアドレス	サブネットマスク
IPアドレス	任意のネットワークアドレス	任意のデフォルトゲートウェイ	任意	任意のブロードキャストアドレス	任意のサブネットマスク
例: 19.168.1.0/2.4 プライベートアドレス空間を使用する場合	192.168.1.0	192.168.1.1	192.168.1.2~ 192.168.1.254	192.168.1.255	255.255.255.0

表4-2 プライベートIPアドレス

## ホスト（コンピュータ・サーバ）の設定

本製品の複数グローバルIP アドレスLAN 型接続機能(NAT &スルー)を利用する場合、LAN 側ポートに接続したホスト(パソコン・サーバ)のネットワーク設定は次のようになります。

### グローバルIP アドレスのコンピュータ

<IP アドレス>

プロバイダから割り当てられたIP アドレス空間のうち、利用可能なグローバルIPアドレス(本製品LAN 側ポートに設定するルータアドレスを除く)

例：153.16.10.41

<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LAN側ポートに設定したグローバルIP アドレス)

例：153.16.10.41

## プライベートIP アドレスのコンピュータ(本製品のDHCP サーバ機能 を利用しない場合)

<IP アドレス>

任意のIP アドレス

例：192.168.1.100

<サブネットマスク>

任意のサブネットマスク

例：255.255.255.0

<デフォルトゲートウェイ>

本製品LAN 側ポートに設定したプライベートIP アドレス

例：192.168.1.1

<DNSサーバ>

プロバイダから指定されているDNSサーバアドレス

例：172.16.1.10

## プライベートIP アドレスのコンピュータ(本製品のDHCP サーバ機能 を利用する場合)

各パソコンのDHCPクライアント機能を有効( IPアドレスを自動的に取得する )にするだけで設定完了です。

# 4

## インターネット設定

# 本製品の「PPPoE複数IP設定」の設定方法

1. Webブラウザで設定画面を開きます。

2. [ インターネット設定 ] ページの上部メニューバーから [ PPPoE複数IP設定 ] を選択します。[ PPPoE複数IP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。以下のPPPoE サービス名が指定されていない場合は“ @ ”(アットマーク) 以下も入力します。(工場出荷時の状態では「 your-name 」に設定されています。)

例 : pci0011@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ドレス名などと異なる場合があります。

## 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。)



### 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アドレスなどと異なる場合があります。

例：rY0Co%Mtu

## 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。とく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。)



### 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。

例：PPPServ

## 自動接続

コンピュータ上でWebブラウザを起動した場合など、LAN側のコンピュータ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さ



### 注意

従量制の場合などで「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。

せる場合は、「有効」に設定してください。「PPPoE複数IP設定」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。)



### 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。複数グローバルIP アドレスLAN 型サービスの場合は、“0”を入力して自動切断しないことを推奨します。(工場出荷時の状態では「120」に設定されています。)

例：0

### IPアドレス自動取得

プロバイダからルータのアドレスを指定されている場合は「しない」、指定されていない場合は「する」を入力してください。(工場出荷時の状態では「する」に設定されています。)

### 固定IPアドレス

プロバイダからルータアドレスを指定されている場合はそのアドレス、指定されていない場合は「0.0.0.0」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：153.16.10.41

### 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」の場合は以下の「固定DNSアドレス1」及び「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

## LAN側グローバルIPアドレス

ルータのLAN側ポートで使用するグローバルIPアドレスを入力してください。「固定IPアドレス」と同じアドレスでもかまいません。LAN側でグローバルIPアドレスを使用する機器のデフォルトゲートウェイにはこのアドレスを設定してください。(工場出荷時の状態では「0.0.0.0」に設定されています。)

例：153.16.10.41

## LAN側グローバルサブネットマスク

ルータのLAN側ポートで使用するグローバルIPアドレスを入力してください。上記ルータIPアドレスと同じアドレスでもかまいません。LAN側でグローバルIPアドレスを使用する機器のデフォルトゲートウェイにはこのアドレスを設定してください。(工場出荷時の状態では「0.0.0.0」に設定されています。)

例：255.255.255.240

## MSS(Max Segment Size)

MSS(Max 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、パフォーマンスが著しく落ちますので注意してください。



### 注意

MSS 値はインターネット接続スピードのパフォーマンスに影響を与えます。アプリケーションの都合でMSS 値を変更する場合は、そのアプリケーションの許容範囲の最大値を入力してください。

## 4. 入力内容を確認し、正しければ[適用]ボタンを押してください。

「設定を保存して再起動します。」メッセージが表示されますので、[はい]ボタンを押してください。[はい]ボタンを押すと、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)

## 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、PPPoE接続を使用しないADSLサービス等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アドレスの変更ができます。



### 注意

PPPoE 接続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。

[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。

The screenshot shows the 'bRoad Lanner smart Manager' web interface in a Microsoft Internet Explorer browser. The page title is 'CATV設定'. The main content area contains the following sections:

- 注意**
  - 本製品の設定を実行した場合は、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設定を取崩しおこなって変更を反映してください。
  - MACアドレスの変更を行った場合は、ケーブル/ADSLモデムの電源を一度切ってから、再度電源を入れてください。
- WANポートの設定**
  - ホスト名: [044a]
  - ドメイン名: [ ]
- IPアドレスの設定**
  - IPアドレス: [192] [68] [1] [14]
  - サブネットマスク: [255] [255] [255] [0]
  - ゲートウェイ: [192] [68] [1] [1]
  - プライマリDNSアドレス: [202] [232] [204] [66]
  - セカンダリDNSアドレス: [ ] [ ] [ ] [ ]
- MACアドレスの変更**
  - このコンピュータのMACアドレス: 00:0E:59:28:12:02 [適用]
  - 本製品のMACアドレス: 00:40:01:01:01:01 [元に戻す]
  - [適用] [クリア]
- ホスト名**

プロバイダからホスト名が指定されている場合は、指定されたホスト名を入力してください。詳しくは注意を参照してください。
- ドメイン名**

プロバイダからドメイン名が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。詳しくは注意を参照してください。
- IPアドレスの取得**

プロバイダ、DHCPサーバからIPアドレスを自動取得する場合は、DHCPサーバからの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。
- IPアドレス**

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。
- 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入力してください。
- ゲートウェイ**

プロバイダから指定されたゲートウェイアドレスを入力してください。
- プライマリDNSアドレス**

プロバイダから指定されたDNSプライマリサーバのIPアドレスを入力してください。
- セカンダリDNSアドレス**

プロバイダからDNS上のDNSが指定されている場合は、指定された2番目のDNSアドレスを入力してください。

### 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「brl04fw」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.com

### 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出来ます。

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」ボタンを押すと、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」ボタンを押すと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。

入力内容を確認し、正しければ[適用]ボタンを押してください。

「設定を保存して再起動します。」メッセージが表示されますので、[はい]ボタンを押してください。[はい]ボタンを押すと、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NAT/IPマスカレードの有効/無効の切り替えを行います。

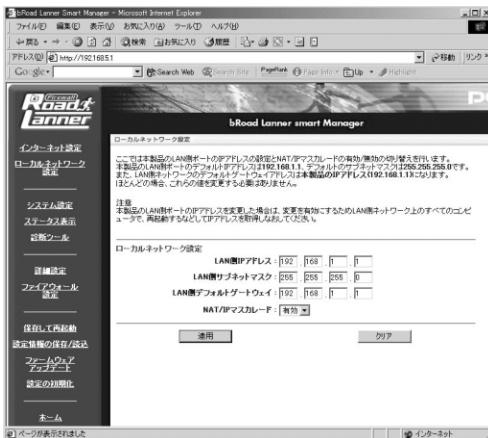
本製品のLAN側ポートのデフォルトIPアドレスは192.168.1.1、デフォルトのサブネットマスクは255.255.255.0です。また、LAN側ネットワークのデフォルトゲートウェイアドレスは本製品のIPアドレス(192.168.1.1)になります。ほとんどの場合、これらの値を変更する必要はありません。



### 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。

Webブラウザの画面左側から、[ 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：192.168.1.1

### 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：192.168.1.1

# 4

## インターネット設定



# 詳細設定

## 詳

細設定では、本製品の以下の機能の設定を行います。

### 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することもできます。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。

### バーチャルコンピュータ

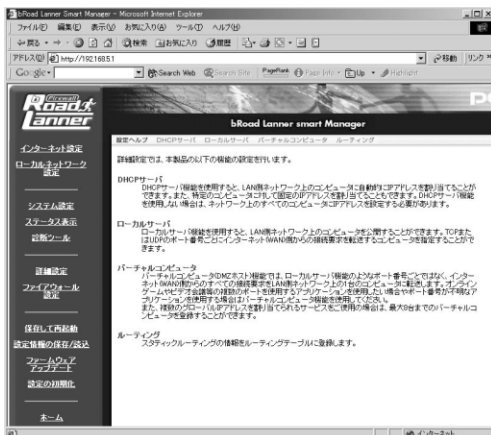
バーチャルコンピュータ(DMZホスト)機能では、ローカルサーバ機能のようなポート番号ごとではなく、インターネット(WAN)側からのすべての接続要求をLAN側ネットワーク上の1台のコンピュータに転送します。オンラインゲームやビデオ会議等の複数のポートを使用するアプリケーションを使用したい場合やポート番号が不明なアプリケーションを使用する場合はバーチャルコンピュータ機能を使用してください。

また、複数のグローバルIPアドレスを割り当てられるサービスをご使用の場合は、最大8台までのバーチャルコンピュータを登録することができます。

## 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。

Webブラウザの画面左側から、[ 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。



# 5 詳細設定

## 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。

[ 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

## IPアドレス割り当て範囲の設定

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ています。この範囲を変更したい場合は[変更]ボタンを、削除したい場合は[削除]ボタンを押してください。(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おり、最高100台のパソコンにIPアドレスを自動的に設定することができます。)

IP アドレスの範囲を追加したい場合は、[割り当て範囲の追加]ボタンを押すと、[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[開始アドレス]欄に、最後のホストアドレスを[終了アドレス]欄に入力して[適用]ボタンを押してください。入力した内容が反映されたページが表示されます。

[IP割当て範囲]は最大で4つの範囲を指定できます。

## 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。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。各リストを変更したい場合は[変更]ボタンを、削除したい場合は[削除]ボタンを押してください。固定IP 割り当てを追加したい場合は、[固定IPの追加]ボタンを押すと[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 アドレスのホストアドレスを[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]ボタンを押してください。入力した内容が反映されたページが表示されます。この設定を行うと、DHCP サーバ機能を利用しているにもかかわらず、特定のパソコンだけ常に同じIP アドレスが割り当てられます。

入力内容を確認し、正しければ[適用]ボタンを押してください。

「設定を保存して再起動します。」メッセージが表示されますので、[ はい ] ボタンを押してください。[ はい ] ボタンを押すと、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)

固定IPでは最大で16個のクライアント登録できます。

### IPアドレス割り当て状況

現在、コンピュータに割り当てている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

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。バーチャルコンピュータ機能が1台のパソコンにすべての通信を転送するのに対して、ローカルサーバ機能では、TCP/UDP ポート番号とIP アドレスの組み合わせを設定することができます

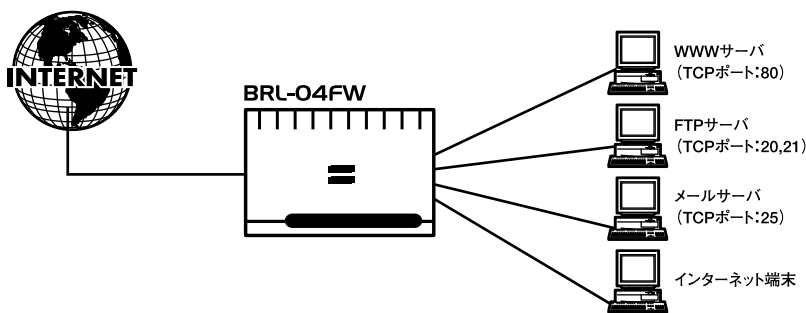
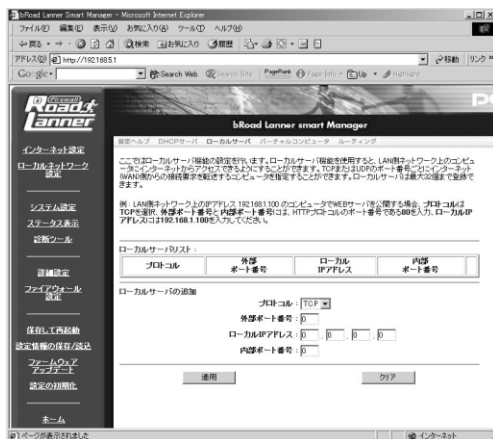


図5-1 ローカルサーバ

[ 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。エントリを変更したい場合は [ 変更 ] ボタンを、エントリを削除したい場合は [ 削除 ] ボタンを押してください。

### プロトコル

TCP ポートを使ったローカルサーバリストを追加したい場合は [ TCP ] に、UDP ポートを使ったローカルサーバリストを追加したい場合は [ UDP ] にします。

### 外部ポート

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。

例：HTTPサーバの場合は、TCP の80 番ポート

### 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

### 内部ポート番号

転送先パソコンでの受信ポート番号を入力します。通常は外部ポートと同じ番号で構いません。

例：HTTPサーバの場合は80番ポート

入力内容を確認し、正しければ[適用]ボタンを押してください。[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 バーチャルコンピュータ

バーチャルコンピュータ機能とは、LAN側の特定のコンピュータをインターネット上からアクセス可能にする機能です。インターネットからの、本製品のWAN側ポートに割り当てられたIPアドレスへのパケットはすべてバーチャルコンピュータに転送されます。通常は、プライベートLAN上のいずれか1台のコンピュータをバーチャルコンピュータとして登録することが可能です。PPPoE複数IPアドレスをご利用の場合には、2台以上のプライベートLAN上のコンピュータをバーチャルコンピュータに登録する事が出来ます。

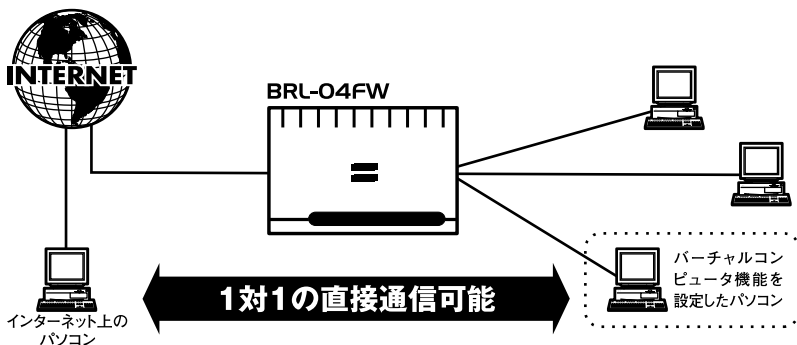
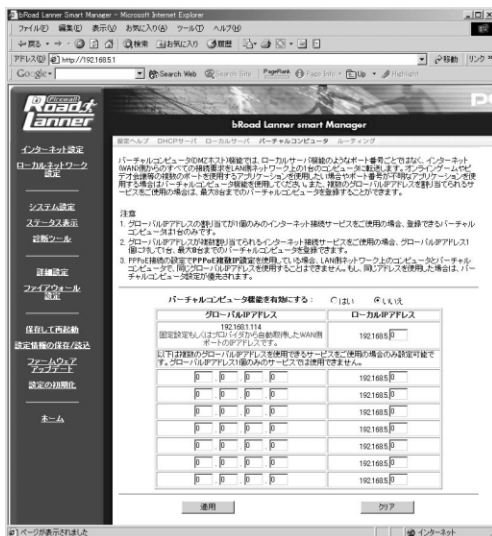


図5-2：バーチャルコンピュータ

[ 詳細設定 ] ページの上部メニューバーから [ バーチャルコンピュータ ] を選択します。[ バーチャルコンピュータ ] 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。



## バーチャルコンピュータ機能を有効にする

「はい/いいえ」から選択してください。「はい」にした場合は以下の[ IP アドレス ] 欄も入力してください。(工場出荷時の状態では「いいえ」に設定されています。)

### グローバルIPアドレス

WAN側のグローバルIPアドレスを登録します。1台目のバーチャルコンピュータのグローバルIPアドレスは、本製品のWAN側のIPアドレスになります。PPPoE複数IPアドレスをご利用の場合は2台目以降にはプロバイダーから割り当てられているグローバルIPアドレスを入力してください。

### ローカルIPアドレス

ローカルLAN側にあるバーチャルコンピュータ機能を利用したいコンピュータのIP アドレスを入力してください。PPPoE複数IPアドレスをご利用の場合は割り当てたグローバルIPアドレス分(最大8台)のコンピュータを登録できます。(工場出荷時の状態では「0.0.0.0」に設定されています。)





## 注意

バーチャルコンピュータ機能を利用するパソコンのIP アドレスは固定しておかなければなりません。  
 PPPoE複数IPアドレスLAN型接続をご利用されている場合には、LAN側のグローバルIPアドレスに登録しているIPアドレスはバーチャルコンピュータで登録するグローバルIPアドレスとして利用する事は出来ません。  
 バーチャルコンピュータに登録したグローバルIPアドレスとLAN側のコンピュータ/サーバのIPアドレスと重複しないようにしてください。

## 4 ルーティング

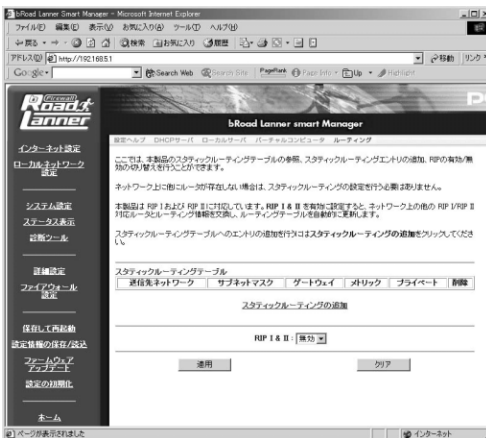
ここでは、本製品のスタティックルーティングテーブルの参照、スタティックルーティングエントリの追加、RIPの有効/無効の切り替えを行うことができます。



## 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]ボタンを押してください。

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]ボタンを押してください。[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]ボタンを押してください。

[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]ボタンを押してください。



# ファイアウォール設定

本

製品はネットワークをハッカーの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。トラフィックはLAN WAN、WAN LANどちらの方向でも制限可能です。

Webブラウザの画面左側から、[ ファイアウォール設定 ]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。

6

ファイアウォール設定

## 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。

### LAN WANフィルタ

LAN WAN方向のネットワークトラフィックへのフィルタの設定を行います。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ます。またトラフィックに対し、ファイアウォールの通行許可を出すかどうかもこれらのルールに基づいて判断します。

### WAN LANフィルタ

WAN LAN方向のネットワークトラフィックへのフィルタの設定を行います。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ます。またトラフィックに対し、ファイアウォールの通行許可を出すかどうかもこれらのルールに基づいて判断します。

### 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 (Help参照) 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いきます。

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 Inspectionと呼ばれる技術が採用されています。

[ファイアウォール設定]ページの上部メニューバーから[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。)

### LAN WAN アクセス初期ルール

LAN側からWAN側へのパケットに対する基本フィルタルールを設定します。「転送」に設定した場合にはLAN側からのWAN側へのパケットのうちフィルタルールに無いものは転送します。「廃棄」に設定した場合にはLAN側からWAN側へのパケットのうちフィルタルールにないものを破棄します。フィルタルールは次の「LAN WANフィルタ」で設定します。(工場出荷時の状態では「転送」に設定されています。)

### TCP SYN Flooding 攻撃しきい値

プライベートネットワークを SYN Flooding DoS 攻撃( Help参照 )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分間の不完全なTCPセッションがこの数値を超えると、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。)

### 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、必要の無い限りは「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응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。)



## 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 LAN→WANフィルタ

ここではLAN側からWAN側へのパケットのフィルタリング設定を行います。ファイアウォールは、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するかどうかを決定します。

デフォルト設定ではファイアウォールは、LAN側からインターネット(WAN)へ送信されるすべてのパケットを許可します。デフォルトの転送ルールは以下のようになります。

1. LAN側からWAN(インターネット)へのすべてのパケットを転送します。
2. WAN側(インターネット)からLANへのすべての接続要求を拒否します。(WAN LANフィルタ参照)

[ファイアウォール設定]ページの上部メニューバーから [LAN WANフィルタ]を選択します。[LAN WAN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。



既にLAN WAN フィルタルールが設定がされている場合は、[ LAN WAN フィルタルール ]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 ]ボタンを押してください。

新たにLAN WAN フィルタ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「転送」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「廃棄」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。「オン」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。「オフ」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

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、「する」に設定して下さい。URLフィルタを適用させない場合は、「しない」に設定して下さい。ポート番号80(HTTP)を含まない場合は、「N/A」に設定して下さい。

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



### 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払い、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 WAN→LANフィルタ

ここではWAN側からLAN側へのパケットのフィルタリング設定を行います。ファイアウォールは、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するかどうかを決定します。

デフォルト設定ではファイアウォールは、インターネット(WAN)からLAN側へのすべてのパケットを拒否します。デフォルトの転送ルールは以下のようになります。

1. LAN側からWAN(インターネット)へのすべてのパケットを転送します。
2. WAN側(インターネット)からLANへのすべての接続要求を拒否します。

[ファイアウォール設定]ページの上部メニューバーから [WAN LANフィルタ]を選択します。[WAN LAN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。

The screenshot shows the 'WAN-LAN フィルタルール' (WAN-LAN Filter Rules) configuration page in the hRoad Lanner smart Manager. The page includes a table of existing rules and a section for creating a new rule.

プロトコル	ポート番号	送信元IPアドレス	送信先IPアドレス	処理	ログ	削除
UDP	80	0.0.0.0	0.0.0.0	Forward	Off	削除

**WAN-LAN フィルタルールの作成**

フィルタルール: [TOP]

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 [0] [0] [0] [0] 終了 [0] [0] [0] [0]

ポート番号: 開始 [0] 終了 [0]

処理: [設定] ログ: [オフ]

## 6

## ファイアウォール設定

既にWAN LAN フィルタルールが設定がされている場合は、[ WAN LAN フィルタルール ]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 ]ボタンを押してください。

新たにWAN LAN フィルタ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WAN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。

#### 送信先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。

#### 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「転送」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「廃棄」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。「オン」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。「オフ」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。

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



### 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。

デフォルト設定では、ポート番号68(DHCP)のパケットを許可するルールが設定されています。WAN側ポートのIPアドレスをDHCPサーバから取得する場合は、このルールを削除しないでください。削除するとDHCPサーバからIPアドレスを取得できなくなります。WAN側ポートのIPアドレスが固定か、またはPPPoE接続を使用する場合は削除してもかまいません。

## 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下さい。

6

ファイアーウォール設定



## コンテンツフィルタ

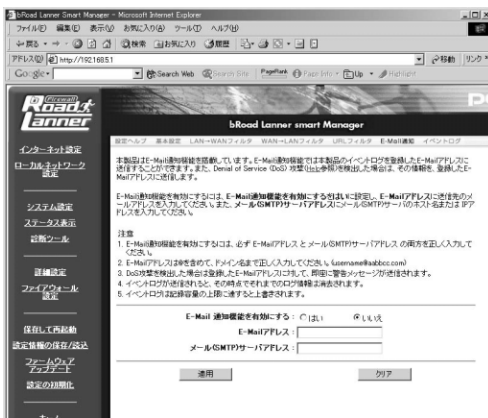
ActiveX、Java、Cookie の各サービスについて、受け付けるかどうかを設定できます。受け付けるサービスは「許可」、拒否するサービスには「拒否」に設定します。

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

## 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。



## 6

## ファイアウォール設定

### 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)

## 6

入力内容を確認して[適用]ボタンを押してください。



### 注意

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。

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。

## 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 [ 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。



### 表示の更新

このボタンを押すと、表示内容を最新のものに更新します。

### ログの送信

このボタンを押すと、「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

このボタンを押すと、ログを消去します。



### 注意

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。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。



# その他の機能

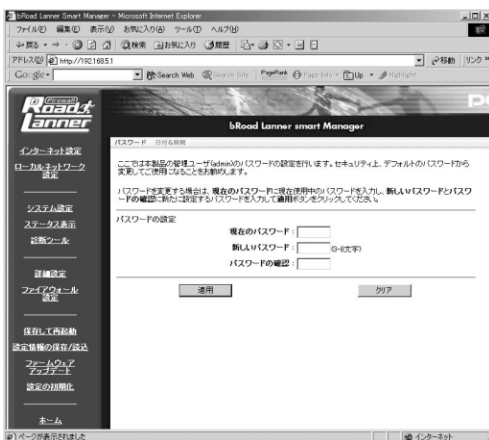
## こ

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。)

## 7

### その他の機能

## 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

最大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

最大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」ボタンを押します。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

このボタンを押すと、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」ボタンを押します。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

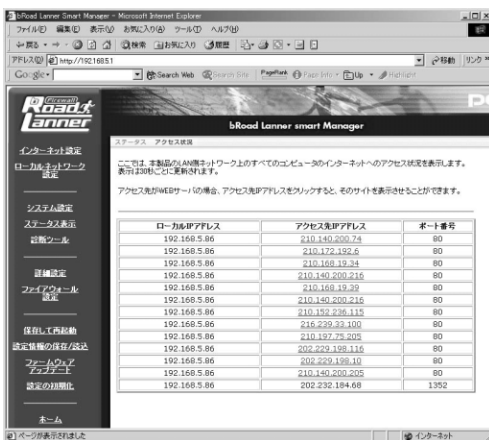
現在のWAN側ポートのステータスです。WAN側ポートのIPアドレスをDHCPサーバから取得している場合は、「WAN側IPアドレスを開放」ボタンを押すとWAN側のIPアドレスを開放します。「WAN側IPアドレスの再取得」ボタンを押すとWAN側IPアドレスの開放と再取得をします。



## 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	アクセス先IPアドレス	ポート番号
192.168.5.86	210.140.200.74	80
192.168.5.86	210.172.192.6	80
192.168.5.86	210.168.19.34	80
192.168.5.86	210.140.200.216	80
192.168.5.86	210.168.13.29	80
192.168.5.86	210.140.200.216	80
192.168.5.86	210.192.236.115	80
192.168.5.86	216.239.33.100	80
192.168.5.86	210.197.75.202	80
192.168.5.86	202.293.199.116	80
192.168.5.86	202.229.199.10	80
192.168.5.86	210.140.200.205	80
192.168.5.86	202.232.184.68	1352

「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為の機能です。

Webブラウザの画面左側から、[ 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。



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/切断もここでを行います。

### 【 接続 】

[ 接続 ]ボタンを押すと現在の設定を読み込んでPPPoE接続を開始します。接続ログの最後の表示が

Connecting Service Successful

Service is running now

と、なっている場合は正常にPPPoE接続が開始された事を表します。

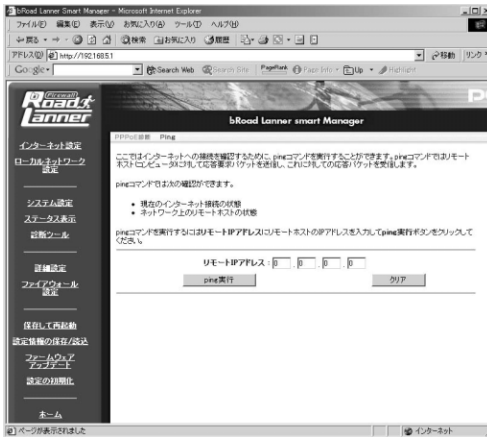
Connecting Service Failed

と、なっている場合はPPPoE接続に失敗した事を表します。接続及び設定の確認してください。

## [ 切断 ]

[ 切断 ] ボタンを押すとPPPoE接続を切断し、切断ログを表示します。

[ 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ユーティリティ画面が表示されます。



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。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

Webブラウザの画面左側から、[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

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。

7

その他の機能

## 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。

Webブラウザの画面左側から、[ 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 ]ボタンを押す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 ]ボタンを押してください。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 ]ボタンを押してください。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。

### 設定情報の保存

[ 設定情報の保存 ] ボタンを押してください。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 ] ボタンを押してください。「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 ] ボタンを押してください。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。

Webブラウザの画面左側から、[ 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 ] ボタンを押す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 ] ボタンを押してください。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 ] ボタンを押してください。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

Webブラウザの画面左側から、[ 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3章」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3章」または「5-1 DHCPサーバ」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。

## インターネット（WAN）からの設定画面へのログインを禁止したい

ローカルサーバ機能を使用して、インターネット（WAN側）からの本製品のWEBおよびtelnet設定画面へのアクセスを禁止することができます。WEBおよびtelnetのポート番号（80、23）をプライベートLAN上で使用していないIPアドレスに割当ててください。

## 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う場合は、「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下さい。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下さい。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。

**<WindowsNT/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(igate14.bin)を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下さい。)
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。  

```
ftfp 本製品のLAN側IPアドレス get upgrade  
ftfp -i 本製品のLAN側IPアドレス put igate14.bin
```
4. しばらくして、「Transfer Succesful」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ランプが点滅します。STATUSランプ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STATUSLED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. 現在のディレクトリにダウンロードしたファームウェアファイル (igate14.bin) を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 igate14.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STATUSLED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(igate14.bin)をMacintosh上にダウンロードします。
2. 「MacTFTP Client」を起動します。
  - (1) [ Receive ]ボタンを押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 ]ボタンを押し、名前欄に「Upgrade」と入力し、保存ボタンを押してください。
  - (4) [ Start ]ボタンを押してください。
3. "Transfer Complete Successfully"と表示されますので、[ Reset ]ボタンを押してください。
  - (1) [ Send ]ボタンを押して反転表示させてください。
  - (2) [ File ]ボタンを押してください。  
ダウンロードしたファームウェアファイル(igate14.bin)を指定して開くボタンを押してください。
  - (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 ]ボタンを押してください。
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たり、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、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。

## C

### デフォルト設定の復帰



# 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み込みを行った場合も、以下の設定が読み込まれます。

D

デフォルト設定

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
	デフォルトゲートウェイ	192.168.1.1
DHCPサーバ	DHCPサーバ	有効
	DHCP IP割当て範囲	192.168.1.21~120
	DHCP固定IP割当て	なし
	プライマリDNS	0.0.0.0
	セカンダリDNS	0.0.0.0
WINSサーバ	0.0.0.0	
WAN側	IPアドレス	0.0.0.0
	サブネットマスク	255.255.255.0
	デフォルトゲートウェイ	0.0.0.0
	サービスタイプ	通常接続
	DHCPクライアント	有効
パスワード	password	
ドメイン名	未設定	
ホスト名	brl04fw	
NAT	有効	
RIP	無効	
ローカルサーバ	なし	
バーチャルコンピュータ	なし	
ルーティングテーブル	なし	



# Telnet設定

**本**

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

## < 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...NAT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 Service Setup.....PPPoE接続の設定

**E**telnet  
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 Host Setup >

- Add a New Entry ……バーチャルコンピュータの設定の追加
- Delete an Old Entry……バーチャルコンピュータの設定の削除

## < 5.FireWall Setup >

- AFireWall Setup ……ファイアーウォール設定
- LAN To WAN Policy Rules …LAN WANフィルタ設定
- WAN To LAN Policy Rules …WAN LANフィルタ設定
- 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の接続テスト
- 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 and 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側：10BASE-T/100BASE-TX RJ-45 スイッチ × 4ポート

WAN側：10BASE-T RJ-45 × 1ポート

< LED >

POWER、STATUS、WAN、LAN

< 入力電源 >

DC 12V、1A

< 消費電力 >

最大12W

< 外形寸法 ( W × D × H ) >

224.4 × 144.6 × 34 mm

< 重量 ( 本体のみ ) >

402g

< 環境 >

動作温度 0 ~ 40

動作湿度 35 ~ 85%

< EMI >

FCC Class A , CE Mark











## 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。

ブ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		F A X	
E-MAIL			

製品名 Product name	4ポート ブロードバンド ファイアウォール ルータ
型番 Product No.	<b>BRL-04FW</b>
製造番号 Serial No.	

### ご使用のコンピュータについて

メーカー	
型番	

### ソフトウェア

ネットワーク OS	バージョン
OS	バージョン





## 保証規定

ブ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となります。

#### 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。

ブ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 <b>1</b> 年間		
製品名 Product Name	4ポート ブロードバンド ファイアウォール ルータ		
型番 Product No.	BRL-04FW	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	<input type="text"/> <input type="text"/> <input type="text"/> - <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> 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](mailto: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**