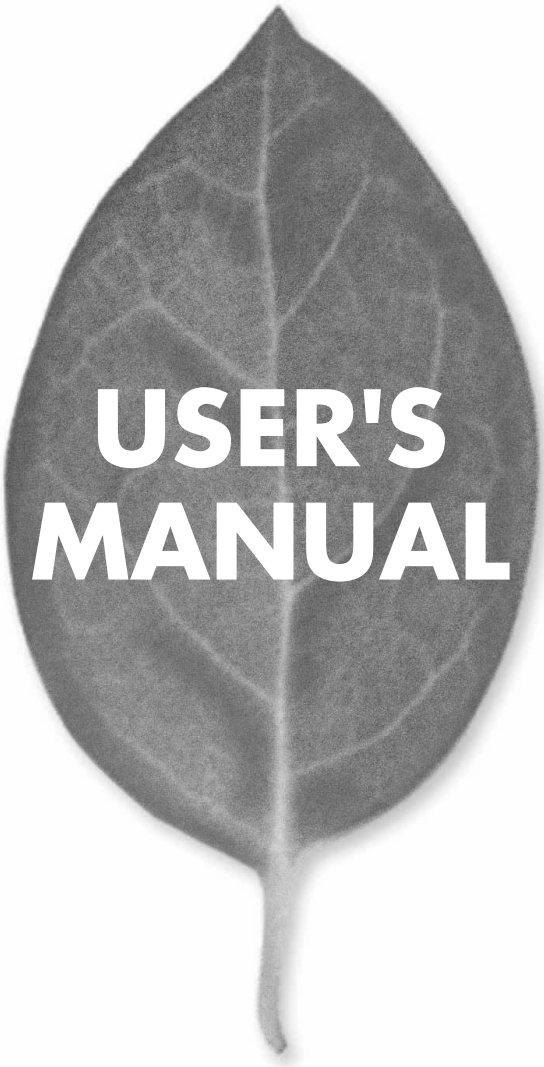


VPN 4ポート ブロードバンド ルータ

BLV-04D

PLANEX COMMUNICATIONS INC.

USER'S MANUAL

VPN 4ポート ブロードバンド ルータ

BLV-04D

本製品を安全にお使いいただくために

⚠警告

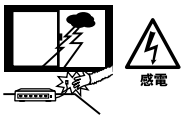
本製品をご利用の際は、以下の注意点を必ずお守りください。これらの事項が守られない場合、感電、火災、故障などにより使用者の重傷または死亡につながるおそれがあります。

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。

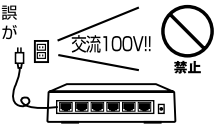
雷のときはさわらないで！

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。



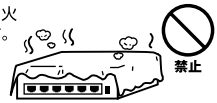
正しい電圧で使用して！

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。



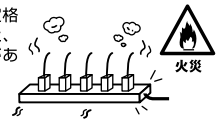
通気口をふさがないで！

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。

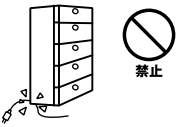
液体・異物は入れないで！

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VPN 4ポート ブロードバンドルータ bRoad Lanner BLV-04D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　コンピュータの設定
本製品を使用したインターネットへのアクセスと本製品のWEBブラウザからの設定に必要な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
本製品のインターネットへの接続設定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　VPNゲートウェイ設定
本製品のVPNゲートウェイ機能の設定の方法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　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C　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-02-11-YT-BLV-04D

目次

はじめに

1 概要

本製品は、ADSLおよびCATV（ケーブルTV）接続を使っ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。NAT/IPマスカレード（NAPT）機能によって、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できます。
また、VPNゲートウェイ機能を搭載しており、簡単にインターネット経由のVPN（バーチャルプライベートネットワーク）を構築することができます。さらにDMZ専用ポートを装備し、LAN側ローカルネットワークへの不正アクセスを防いだ状態で安全にサーバを公開することができます。本製品はWEBブラウザによって、簡単にセットアップできます。

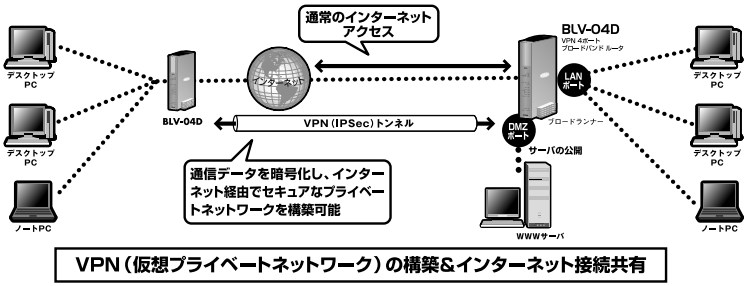


図1-1　bRoad Lanner接続図

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

●MIPS 32bitプロセッサによる高速ルーティング
●ADSL、CATV接続などのWAN回線に対応
●NAT/IPマスカレード機能によって1つのIPアドレスを複数のコンピュータで共有できます
●WAN側に100BASE-TX/10BASE-T自動認識に対応したRJ-45 STPポートを1ポート装備
●LAN側に100BASE-TX/10BASE-T自動認識、Auto MDI/MDI-Xに対応した4ポートスイッチングハブを内蔵
●DMZ側に100BASE-TX/10BASE-T自動認識に対応したRJ-45 STPポートを1ポート装備
●ハードウェア処理による高速VPN（IPSec）ゲートウェイ機能を搭載（最大70拠点まで接続することができます）
●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クライアントまで割り当てることができます）
●DNSリレー機能に対応
●ローカルサーバ機能によってTCP/UDPプロトコルのポート番号ごとに、LAN側のコンピュータにインターネットからアクセスできます
●バーチャルコンピュータ機能によって、LAN側のコンピュータにインターネットからアクセスできます
●ファイアウォール機能を装備、インターネットからの攻撃を検出し防御します
●フィルタ機能を装備、LAN側コンピュータのインターネットへのアクセスを制限できます
●WAN側の接続方法は、通常接続のほかPPPoE接続に対応しています
●複数のグローバルIPアドレスを使用するUnnumbered接続に対応
●LAN側ポートは最高4グループまでのポートベースVLAN機能に対応
●ログ機能に対応、記録したログはE-MailおよびSyslogサーバに送信可能
●WEBブラウザから設定できます
●UPnP（ユニバーサルプラグアンドプレイ）機能に対応
●Dynamic DNS（dyndns.org）サービスに対応

3 梱包内容の確認

パッケージに以下の付属品が含まれていることを確かめてください。

●BLV-04D本体
●ACアダプタ
●縦置き用スタンド
●ツイストペアケーブル（ストレートタイプ：1m）1本
●ショートコード1本
●このユーザーズマニュアル
●保証書（ユーザーズマニュアルの最後にあります）

不足品があるときは、販売店または弊社テクニカルサポートまでご連絡ください。

4 各部の名称

■本体前面

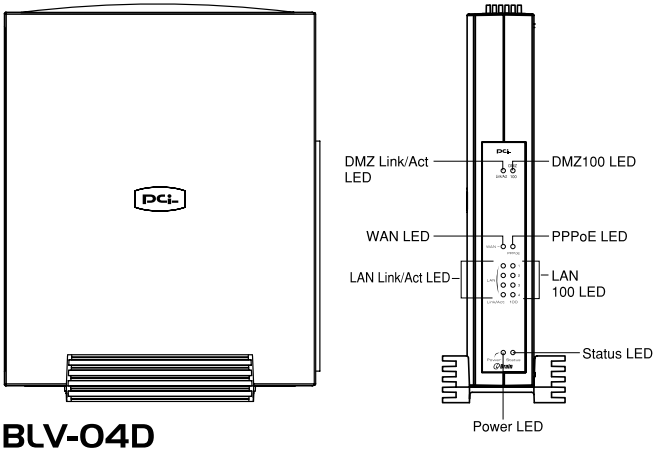


図1-2　BLV-04D本体前面

「Power LED」
本製品に電源が供給されているときに点灯します。
「Status LED」
本製品の起動時とエラー発生時に点灯します。
「LAN Link/Act LED」
LAN側ポートのリンクが確立しているときに点灯します。また、ポートがデータの送受信中には点滅します。
「LAN 100 LED」
ポートのリンクが、100Mで確立しているときに点灯します。
「WAN LED」
WAN側ポートのリンクが確立しているときに点灯します。また、ポートがデータの送受信中には点滅します。
「PPPoE LED」
WAN側ポートでPPPoE接続が確立しているときに点灯します。
「DMZ Link/Act LED」
DMZ側ポートのリンクが確立しているときに点灯します。また、ポートがデータの送受信中には点滅します。
「DMZ 100 LED」
DMZポートのリンクが、100Mで確立しているときに点灯します。

■本体背面

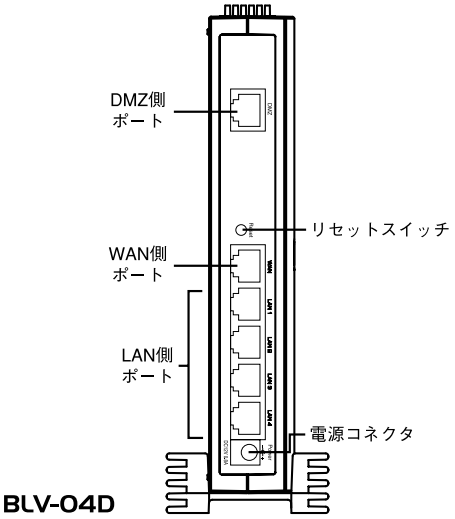


図1-3　BLV-04D本体背面

「WAN側ポート」
本製品をADSLまたはケーブルモデムと接続するためのRJ-45 STPポートです。
「LAN側ポート」
本製品にコンピュータを接続するためのRJ-45 STPポートです。
「DMZ側ポート」
本製品にDMZ機能により外部に公開するコンピュータを接続するための RJ-45 STPポートです。
「リセットスイッチ」
本製品を再起動するときや、本製品の設定を工場出荷時の状態に戻すときに使います。
「電源コネクタ」
付属のACアダプタを接続するための電源コネクタです。

■本体裏面

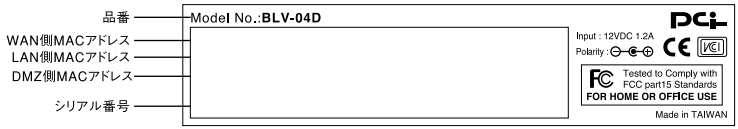


図1-4　BLV-04D本体裏面

「品番」
本製品の製品型番です。
「シリアル番号」
本製品のシリアルナンバーです。製品外箱に記載されているものと同じ番号です。ユーザ登録時に必要となります。また、製品故障時などにサポートを受けるときにも必要になります。
「LAN側MACアドレス」
本製品のLAN側ポートのMACアドレス（物理アドレス）です。
「WAN側MACアドレス」
本製品のWAN側ポートのMACアドレス（物理アドレス）です。プロバイダによってはADSL/ケーブルモデムに接続する機器のMACアドレスの申請が必要なことがあります。そのときはこのWAN側ポートのMACアドレスをプロバイダに申請してください。
「DMZ側MACアドレス」
本製品のDMZ側ポートの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/Me、Windows 2000、Windows XPを搭載し、Ethernet（RJ-45）ポートを装備したコンピュータ

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

■ネットワーク機器

本製品では、以下のネットワーク機器が必要となります。

●ツイストペアケーブル（本製品に接続するコンピュータの台数分）

■ADSL/ケーブルモデム

本製品は、以下のADSL/ケーブルモデムに対応しています。

●RJ-45（LAN）ポートを装備した外付ADSLモデム

●RJ-45（LAN）ポートを装備した外付ケーブルモデム

6 設定の初期化

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

> **注意**
>
> ***設定の初期化を行うと、LAN側/WAN側ポートの設定やフィルタ設定、VPN設定などすべての設定が初期化されます。初期化を実行する前に、本当に初期化を行っても問題がないかを確認してください。***

1. **本製品の電源をOFFにしてください。**
2. **本製品背面のリセットスイッチを先のとがったペンなどで押したまま電源をONにしてください。**
3. **約20秒間リセットスイッチを押したままにしてください。**
4. **リセットスイッチを離します。本製品のすべての設定が初期化されます。**

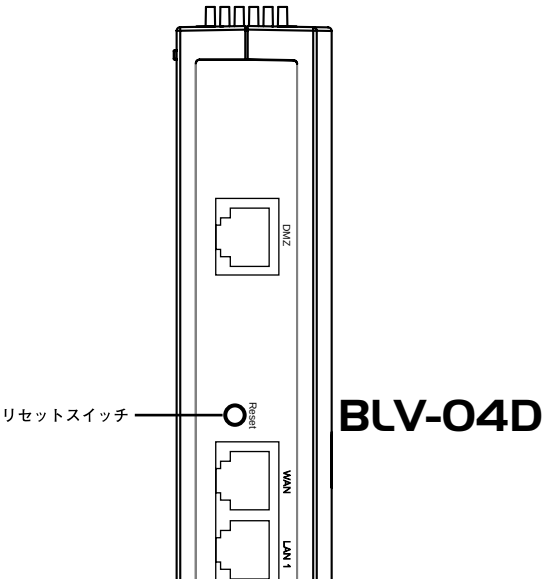


図1-5　リセットスイッチ

ハードウェアの接続

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

1 設置場所について

本製品を設置する際には必ず以下の点をお守りくださいますようお願いします。

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

⚠ 注意

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

2 設置

本製品は、デスクトップ上などの平らな場所に設置して使ってください。

■縦置きする場合

本体を付属の縦置き用スタンドに図のようにセットしてください。

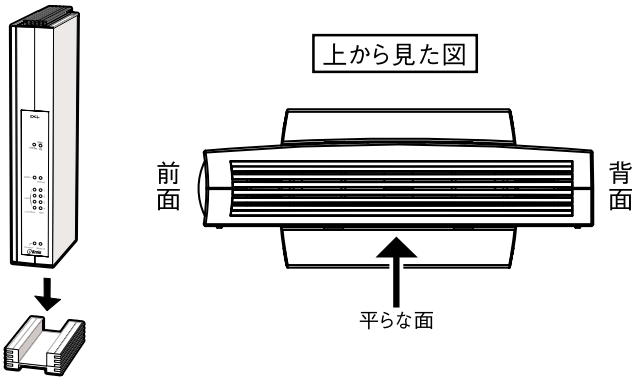


図2-1 縦置き

■横置きする場合

図のように本体の平らな面が下になるように設置してください。

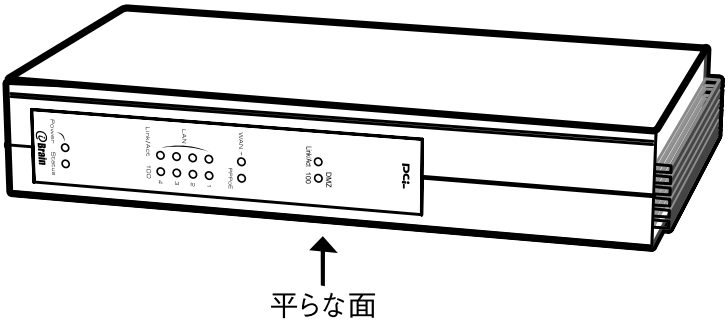


図2-2 横置き

3 WAN側ポートにADSL/ケーブルモデムを接続する

1. ADSL/ケーブルモデムの電源を切ってください。

2. 本製品付属のツイストペアケーブルで、本製品背面のWAN側ポートとADSL/ケーブルモデムのRJ-45ポートを接続します。

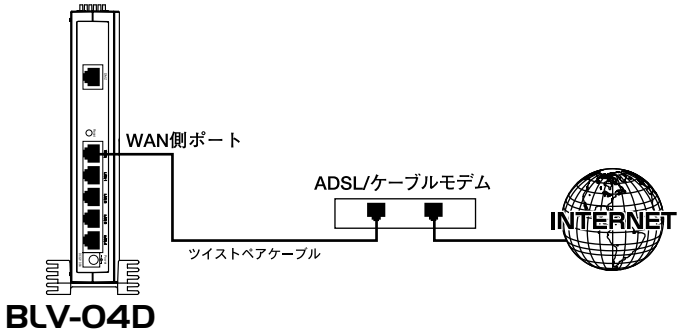


図2-3　ADSL/ケーブルモデムとの接続

注意

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

4 LAN側ポートへのコンピュータの接続

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

2. ツイストペアケーブルのもう一端をコンピュータのRJ-45ポートに接続します。

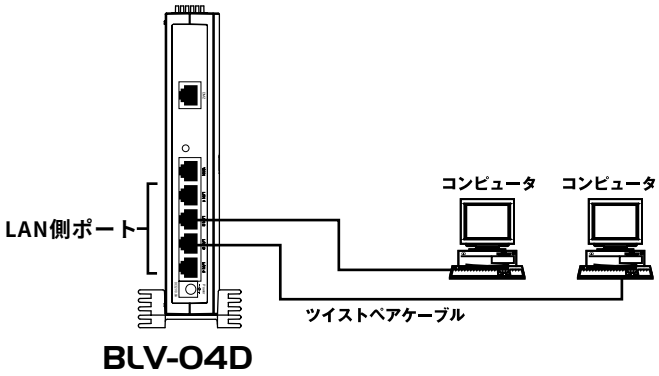


図2-4　コンピュータを接続

5 電源の接続

1. ADSL/ケーブルモデムの電源を入れます。
2. 付属のACアダプタを本製品の電源コネクタに接続します。
3. ACアダプタをAC100Vコンセントに接続します。スペースの問題でACアダプタをコンセントに直接接続できないときは付属のショートコードをお使いください。
4. コンピュータの電源を入れてください。
5. 20ページの接続の確認に進んでください。

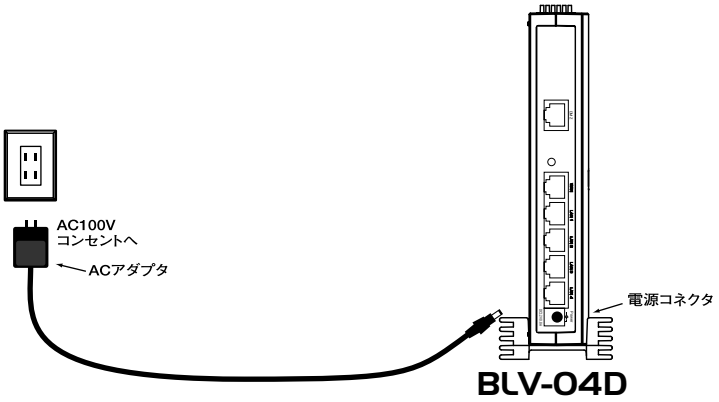


図2-5　電源の接続

注意

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

6 接続の確認

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

◎POWER LED

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

◎WAN LED

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

◎LAN Link/Act LED

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

コンピュータの設定

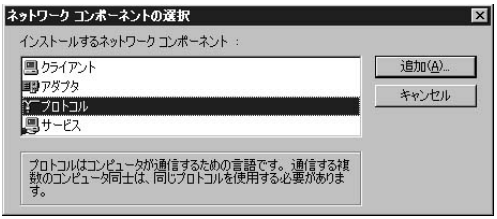
本章では本製品を使ったインターネットへのアクセスとWEBブラウザから設定するために必要なコンピュータの設定手順について説明します。コンピュータの設定を開始する前に、第2章「ハードウェアの接続」を参照して本製品とADSL/ケーブルモデム、コンピュータの接続を完了させておいてください。

1 Windows 95/98/Me

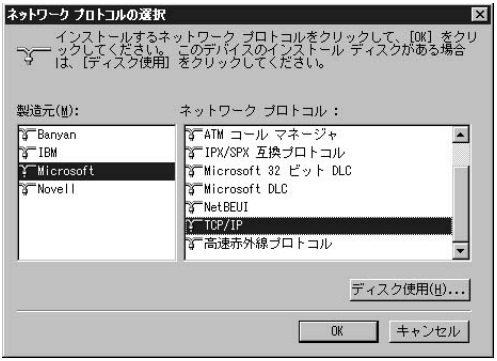
1. コンピュータにネットワークアダプタがインストールされ、正常に認識されていることを確かめてください。ネットワークアダプタがインストールされていないときは、ネットワークアダプタのインストールを行ってください。

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かめます。「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」と選択します。「現在のネットワーク構成」の欄に「TCP/IP」が表示されているか確かめてください。インストールされているときは手順5に進んでください。

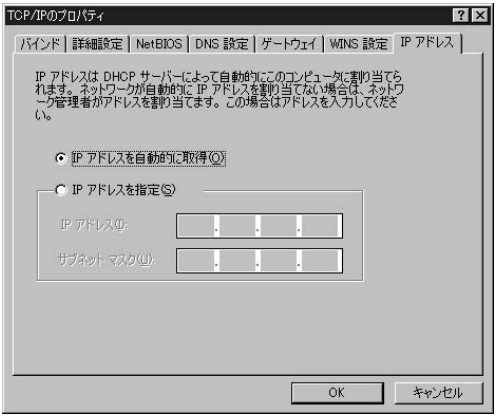
3. **インストールされていないときは「追加」ボタンをクリックし、「インストールするネットワークコンポーネント」から「プロトコル」を選択して「追加」ボタンをクリックします。**



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ます。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ます。「TCP/IPのプロパティ」画面が表示されるので、「IPアドレス」タブをクリックします。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ます。**

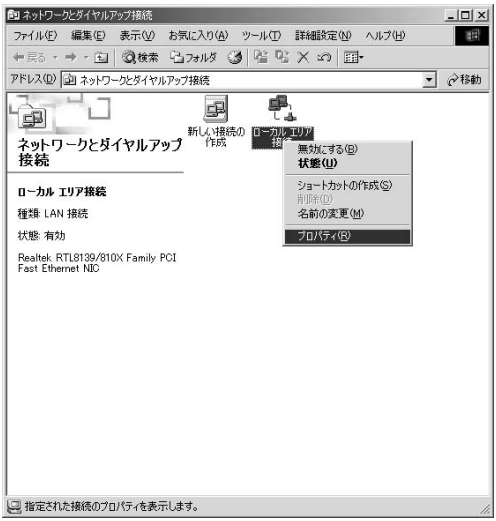


2 Windows 2000

1. コンピュータにネットワーク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かめてください。ネットワークアダプタがインストールされていないときは、ネットワークアダプタのインストールを行ってください。

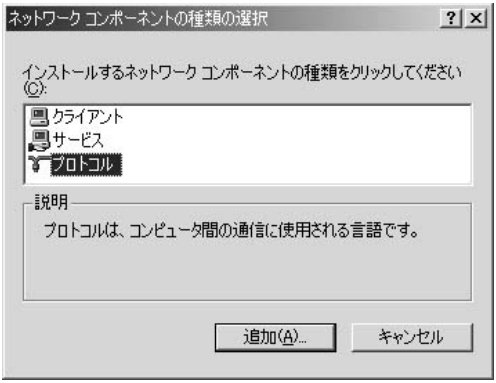
2. コンピュータにTCP/IPプロトコルがインストールされていることを確かめます。「スタート」メニューから「設定」→「コントロールパネル」→「ネットワークとダイアルアップ接続」と選択します。

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

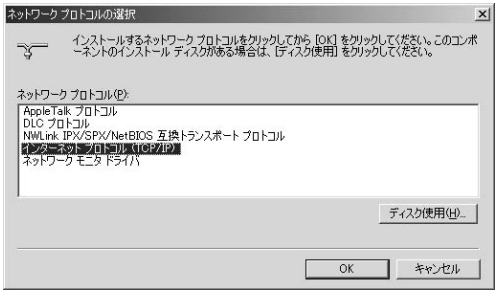


4. **「ローカルエリア接続のプロパティ」に「インターネットプロトコル(TCP/IP)」が表示されているか確かめてください。インストールされているときは手順7に進んでください。**

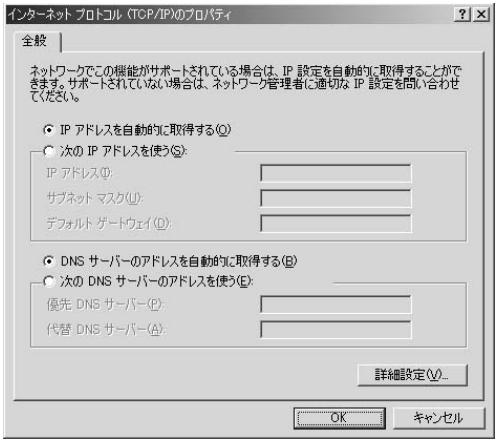
5. **インストールされていないときは「インストール」ボタンをクリックし、「ネットワークコンポーネントの種類の選択」から「プロトコル」を選択して「追加」ボタンをクリックします。**



6.「ネットワークプロトコルの選択」で「インターネットプロトコル（TCP/IP）」を選択して「OK」ボタンをクリックします。ローカルエリア接続のプロパティの画面に戻ります。



7.「インターネットプロトコル（TCP/IP）」を選択し「プロパティ」ボタンをクリックします。「インターネットプロトコル（TCP/IP） のプロパティ」画面が表示されるので、「IP アドレスを自動的に取得する」と「DNSサーバーのアドレスを自動的に取得する」の2つのオプションを選択し「OK」ボタンをクリックします。

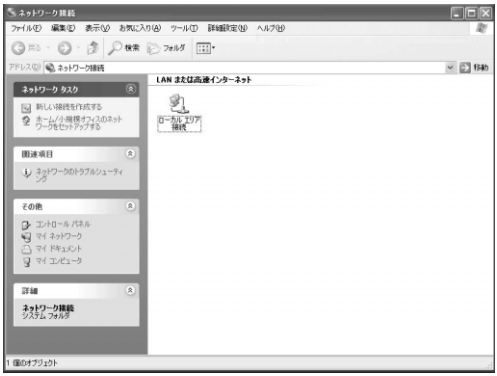


8.「ローカルエリア接続のプロパティ」の画面に戻るのでこれを閉じてください。

3 Windows XP

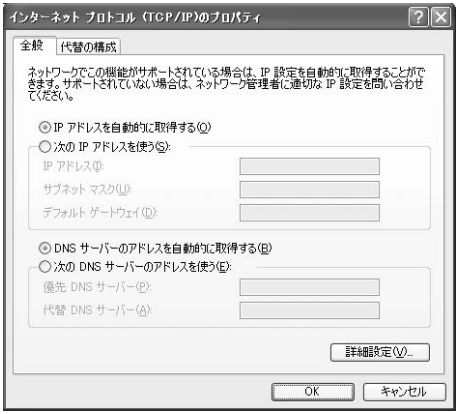
1. コンピュータにLANアダプタがインストールされ、正常に認識されていることを確かめてください。LANアダプタがインストールされていないときは、LANアダプタのインストールを行ってください。

2. コンピュータでTCP/IPプロトコルが有効になっていることを確かめます。「スタート」メニューを開き、「マイコンピュータ」を選択します。表示された「マイコンピュータ」ウィンドウの左側の「その他」の中にある「マイネットワーク」を右クリックし、メニューから「プロパティ」を選択します。「ネットワーク接続」ウィンドウが表示されます。



3. 「ローカルエリア接続」アイコンを右クリックして表示されるメニューから「プロパティ」を選択します。「ローカルエリア接続のプロパティ」ウィンドウが表示されます。「この接続は次の項目を使用します」の欄の「インターネットプロトコル（TCP/IP）」の左側のチェックボックスがチェックされているか確かめてください。チェックされていないときはチェックします。

4. 「インターネットプロトコル（TCP/IP）」を選択し「プロパティ」ボタンをクリックします。「インターネットプロトコル（TCP/IP）のプロパティ」画面が表示されるので、「全般」タブをクリックします。画面内の「IPアドレスを自動的に取得する」と「DNSサーバのアドレスを自動的に取得する」のオプションを選択し、「OK」ボタンをクリックします。

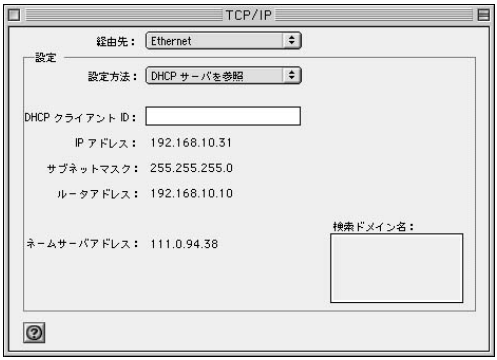


5. 「ローカルエリア接続のプロパティ」ウィンドウに戻ったら、「閉じる」ボタンをクリックします。

4 Macintosh

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

2. TCP/IPの設定ウィンドウの「設定方法」を「DHCPサーバを参照」に設定します。



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

インターネット接続設定

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

1 インターネット接続方法の確認

本製品のインターネット接続の設定は、お客様が契約しているプロバイダとのサービス内容によって異なります。
次の中からお客様のプロバイダとの契約内容にあった接続方法を選択して、本製品の設定を行ってください。

■PPPoE接続

NTT東日本株式会社/NTT西日本株式会社の「フレッツ・ADSL」および「Bフレッツ」や、東京めたりっく通信株式会社の「G-One（旧Single）」サービスなどで採用されている、PPPoEプロトコルを使う接続方法です。接続にはユーザ名（アカウント名）とパスワードが必要です。
→33ページの「4-2 PPPoE接続の設定」に進んでください。

■DHCP接続

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

→39ページの「4-3 DHCP接続の設定」に進んでください。

■固定IPアドレス接続

プロバイダから固定のIPアドレスが割り当てられるサービスでの接続方法です。

→44ページの「4-4 固定IP接続の設定」に進んでください。

注意

本製品をJ-COM@NetHomeまたはJ-COM・ZAQでご使用になるときは、J-COM@NetHomeまたはJ-COM・ZAQへの、ルータ使用の登録が必要です。（2002年8月現在）

2 PPPoE接続の設定

⚠ 注意

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

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

1. **コンピュータが起動したら、WEBブラウザを起動します。**

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

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

4. **本製品の設定画面が表示されます。画面左側のメニューから「簡単インターネット設定」をクリックします。**

5. **「簡単インターネット設定」画面が表示されます。「次へ ＞」をクリックします。**

6. WAN設定画面が表示されるので「PPPoE接続」を選択して「次へ」ボタンをクリックします。

7. PPPoE接続の設定画面が表示されます。次の項目を入力して「次へ >」ボタンをクリックします。

「接続ユーザ名」
プロバイダから指定されたPPPoE接続のユーザ名（アカウント名）を入力します。

「接続パスワード」
プロバイダから指定されたPPPoE接続のパスワードを入力します。

「サービス名」
通常は空欄ままでかまいません。プロバイダからサービス名の指定があるときのみ、指定されたサービス名を入力してください。

「自動接続」
「有効にする」をチェックすると、PPPoE接続が切断されているときにLAN側からインターネットへの通信が発生すると自動でPPPoE接続をします。

「自動切断」
「有効にする」をチェックすると、設定した時間、インターネットへの通信がない状態が続くとPPPoE接続を自動切断します。自動切断を無効に設定するとセッションキープアライブ機能が働くようになります。この場合、本製品の起動時やPPPoE接続が切断されたときに自動的に再接続を行います。設定可能な範囲は 1〜99（分）です。

「MSS（Maximum Segment Size ）」
PPPoE接続時のMSS（Maximum Segment Size ）値を変更します。通常は工場出荷時の設定「1414」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低下したりするので注意してください。設定可能な範囲は 536〜1452 です。MSS値に40を加えた値がMTU値になります。

注意
NTT 東日本株式会社/NTT 西日本株式会社の「フレッツ・ADSL 」「B フレッツ」のときは、必ず「1414 」以下の値でご使用ください。

8. IPアドレスの設定画面が表示されます。通常、PPPoE接続では「自動取得」を選択します。固定のIPアドレスが割り当てられるPPPoE接続サービスの場合は、「固定IPアドレス割り当て」を選択して、次の項目を入力します。入力が終わったら「次へ ＞」ボタンをクリックします。

「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、一般的には、割り当てられたグローバルIPアドレスの中から2番目のIPアドレスを設定します。詳しくは第5章「15.DMZ機能による複数グローバルIPアドレス接続の設定」を参照してください。

「サブネットマスク」
グローバルIPアドレスが1個のみ割り当てられるサービスをご利用の場合は、空欄のままでかまいません。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利用の場合は、プロバイダから割り当てられているサブネットマスクを入力します。

「DNSアドレス」
プロバイダから指定されたDNSサーバアドレスを入力します。DNSアドレスの指定がない場合は空欄のままでかまいません。

9. **設定終了の画面が表示されます。「インターネット接続のテストを行う」をチェックして「完了」ボタンをクリックします。**
これまでの設定を保存し、インターネットに接続できるか確認を行います。「テスト結果」欄にテストの結果が表示されるので確認してください。

PPPoE接続が成功したら、「閉じる」ボタンをクリックしてください。

PPPoE接続が成功しないときは、ユーザ名、パスワードなどの設定に間違いがないか確かめてください。

注意

プロバイダから配布されるPPPoE接続ソフトウェアをコンピュータにインストールする必要はありません。インストールしてある場合は、アンインストールするか、そのソフトの自動接続機能を無効にしてください。

3 DHCP接続の設定

⚠ 注意

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

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

1. コンピュータが起動したら、WEBブラウザを起動します。

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

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

4. **本製品の設定画面が表示されます。画面左側のメニューから「簡単インターネット設定」をクリックします。**

5. **「簡単インターネット設定」画面が表示されます。「次へ ＞」をクリックします。**

6. **WAN設定画面が表示されるので「通常接続」を選択して「次へ」ボタンをクリックします。**

7. **ホスト名、ドメイン名、MACアドレスの設定画面が表示されます。通常は変更の必要はありません。これらの項目についてプロバイダから指定があるときだけ変更してください。入力が終わったら「次へ ＞」ボタンをクリックします。**

「ホスト名」
プロバイダから指定されたホスト名を入力します。指定がないときは変更の必要はありません。

「ドメイン名」
プロバイダから指定されたドメイン名を入力します。指定がないときは空欄のままでかまいません。

「MACアドレス」
本製品の現在のWAN側ポートのMACアドレスが表示されます。プロバイダによってはインターネットに接続するPCのMACアドレスの登録が必要なことがあります。すでにPCのMACアドレスを登録しているときは登録済みのMACアドレスに変更することにより、プロバイダへの登録変更をすることなくご利用いただけます。

「出荷時設定」
本製品のWAN側ポートのMACアドレスを出荷時の設定に戻します。

「このPCからコピー」
本製品のWAN側ポートのMACアドレスに、現在設定するためにアクセスしているPCのMACアドレスをコピーできます。

注意
本製品をJ-COM@NetHomeでご使用になるときは、J-COM@NetHomeへのルータ使用の登録をしたうえで、「ホスト名」欄にJ-COM@NetHomeから指定されたコンピュータ名を設定してください。

8. IPアドレスの設定画面が表示されます。「自動取得」を選択し、「次へ ＞」ボタンをクリックします。

9. 設定終了の画面が表示されます。「インターネット接続のテストを行う」をチェックして「完了」ボタンをクリックします。
これまでの設定を保存し、インターネットに接続できるか確認を行います。「テスト結果」欄にテストの結果が表示されるので確認してください。
接続が成功したら、「閉じる」ボタンをクリックしてください。
接続が成功しないときは、ホスト名、ドメイン名などの設定に間違いがないか確かめてください。

4 固定IP接続の設定

⚠ 注意

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

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

1. コンピュータが起動したら、WEBブラウザを起動します。

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

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

4. 本製品の設定画面が表示されます。画面左側のメニューから「簡単インターネット設定」をクリックします。

5. 「簡単インターネット設定」画面が表示されます。「次へ ＞」をクリックします。

6. **WAN設定画面が表示されるので「通常接続」を選択して「次へ」ボタンをクリックします。**

7. **ホスト名、ドメイン名、MACアドレスの設定画面が表示されます。通常は変更の必要はありません。これらの項目についてプロバイダから指定があるときだけ変更してください。入力が終わったら「次へ ＞」ボタンをクリックします。**

「ホスト名」
プロバイダから指定されたホスト名を入力します。指定がないときは変更の必要はありません。

「ドメイン名」
プロバイダから指定されたドメイン名を入力します。指定がないときは空欄のままでかまいません。

「MACアドレス」
本製品の現在のWAN側ポートのMACアドレスが表示されます。プロバイダによってはインターネットに接続するPCのMACアドレスの登録が必要なことがあります。すでにPCのMACアドレスを登録しているときは登録済みのMACアドレスに変更することにより、プロバイダへの登録変更をすることなくご利用いただけます。

「出荷時設定」
本製品のWAN側ポートのMACアドレスを出荷時の設定に戻します。

「このPCからコピー」
本製品のWAN側ポートのMACアドレスに、現在設定するためにアクセスしているPCのMACアドレスをコピーできます。

8. **IPアドレスの設定画面が表示されます。「固定IPアドレス割り当て」を選択して、次の項目を入力します。入力が終わったら「次へ >」ボタンをクリックします。**

「IPアドレス」
プロバイダから指定されたIPアドレスを入力します。

「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ます。

「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ます。

「DNSアドレス」
プロバイダから指定されたDNSサーバアドレスを入力します。

9. **設定終了の画面が表示されます。「インターネット接続のテストを行う」をチェックして「完了」ボタンをクリックします。**
これまでの設定を保存し、インターネットに接続できるか確認を行います。
「テスト結果」欄にテストの結果が表示されるので確認してください。
接続が成功したら、「閉じる」ボタンをクリックしてください。
接続が成功しないときは、ホスト名、ドメイン名などの設定に間違いがないか確かめてください。

詳細設定

ここでは、WEBブラウザを使用して本製品の各機能の詳細な設定を行う手順を説明します。

⚠ 注意

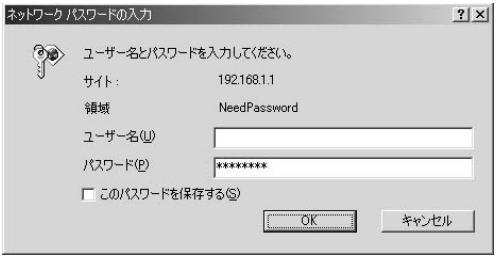
・WEBブラウザから本製品にアクセスするには、フレーム表示に対応したブラウザをご利用になる必要があります。Netscape 6.0以降またはMicrosoft Internet Explorer 5.0以降のご利用を推奨します。
・ブラウザでプロキシを使う設定になっていると設定画面が表示されません。Internet Explorerでは「表示（ツール）」→「インターネットオプション」→「接続」→「LANの設定」、Netscapeでは「編集」→「設定」→「詳細」にプロキシの設定項目があります。プロキシを使わない設定にするか、もしくはプロキシの詳細設定画面で「次で始まるドメイン（アドレス）にはプロキシを使用しない」の欄に本製品のLAN側ポートのIPアドレスを入力します。

1 設定画面を開く

本製品の設定画面には以下の手順でアクセスしてください。

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

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



4. 本製品の設定画面が表示されます。

2 管理者パスワードの設定

本製品の管理者パスワードは工場出荷時は「password」に設定されています。本製品のご利用に際してはセキュリティ上、管理者パスワードの変更を推奨します。管理者パスワードを変更するには、画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「パスワード設定」をクリックします。

「新しいパスワード」
新しいパスワードを入力します。パスワードの最大長は半角文字で9文字です。

「新しいパスワードの確認」
確認のため新しいパスワードをもう一度入力します。

設定が終了したら、「設定」ボタンをクリックします。

3 LANポートの設定

本製品のLANポートのIPアドレス設定とDHCPサーバ機能の設定を行います。LANポートを設定するには、画面左側のメインメニューから「ローカルネットワーク設定」をクリックします。

5 詳細設定

「IPアドレス」
LAN側ポートに設定するIPアドレスを入力します。デフォルトでは「192.168.1.1」に設定されています。

「サブネットマスク」
LAN側ポートのサブネットマスクです。デフォルトでは「255.255.255.0」に設定されています。

「DHCPサーバ」
DHCPサーバ機能を使うと、LAN側のコンピュータに自動でIPアドレスが割り当てられます。これにより、LAN側ネットワークのコンピュータにIPアドレスを手動で設定する必要がなくなります。
DHCPサーバ機能を使うときは「有効にする」をチェックします。DHCPサーバ機能を使わないときは「有効にする」のチェックを外します。

「割り当て開始IPアドレス」
DHCPサーバ機能によって、割り当てるIPアドレス範囲の開始アドレスを設定します。「.」（ドット）で区切られた4つの数字の内の最後の1つを入力します。例えば「192.168.1.200」を設定するときは「200」を入力します。

「割り当て終了IPアドレス」
DHCPサーバ機能によって、割り当てるIPアドレス範囲の終了アドレスを設定します。

設定が終了したら「設定」ボタンをクリックします。

●DHCPサーバによる固定IPアドレス割り当て

本製品のDHCPサーバからLAN側の特定のコンピュータに対して、常に固定のIPアドレスを割り当てるには、「PCデータベース」機能から設定をします。詳細は「5-4 PCデータベースの作成」を参照してください。

⚠ 注意

1.DHCPサーバで割り当てるIPアドレス範囲には本製品のLAN側ポートのIPアドレスが含まれないように設定してください。
2.DHCPサーバ機能を使用しないときは、LAN 側ネットワーク上のすべてのコンピュータのIPアドレスを手動で設定してください。

4 PCデータベースの作成

本製品のLAN側ポートに接続されているコンピュータのデータベース「PCデータベース」を作成します。PCデータベースは本製品の以下の機能で使用します。これらの機能を使用するときは、あらかじめPCデータベースの作成を行ってください。

●PCデータベースを使用する機能

- DHCPサーバによる固定IPアドレスの割り当て
- ローカルサーバ機能
- バーチャルコンピュータ機能
- 特殊アプリケーション機能
- アクセス制限機能

PCデータベースの設定をするには、画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「PCデータベース」をクリックします。

画面左側の「PCリスト」欄には、PCデータベースに登録されているコンピュータが表示されます。本製品のDHCPサーバ機能でIPアドレスを自動取得しているコンピュータは自動的にPCデータベースに登録されます。

●コンピュータの追加

IPアドレスを固定設定しているコンピュータをPCデータベースに登録するには、「コンピュータ名」に登録するコンピュータの名前と、「IPアドレス」欄にコンピュータのIPアドレスを入力して、「< 追加」ボタンをクリックします。IPアドレスは「.」（ドット）で区切られた4つの数字の内の最後の1つを入力します。例えば「192.168.1.200」を設定するときは「200」を入力します。

●コンピュータの削除

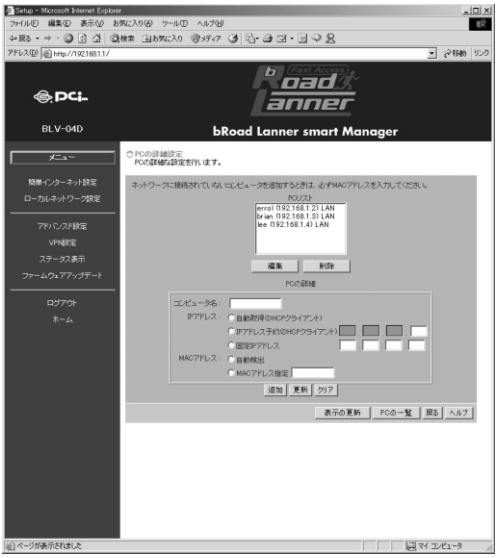
「PCリスト」から削除するコンピュータを選択して、「削除」ボタンをクリックします。

●PCデータベースの一覧表示

「PCの一覧」ボタンをクリックするとPCデータベースに登録されているコンピュータを一覧表示します。

●コンピュータの詳細設定

PCデータベースに登録されているコンピュータの詳細設定を行います。



「編集」ボタン

すでに登録してあるコンピュータの設定を変更するには、PCリストからコンピュータを選択して、「編集」ボタンをクリックします。

「削除」ボタン

すでに登録してあるコンピュータを削除するには、PCリストからコンピュータを選択して、「削除」ボタンをクリックします。

「コンピュータ名」

コンピュータ名を入力します。

「IPアドレス」

IPアドレスの割り当て方法を選択します。本製品のDHCPサーバ機能からIPアドレスを割り当てるときは「自動取得」を選択します。DHCPサーバ機能から固定のIPアドレスを割り当てるときは「IPアドレス予約」を選択して、割り当てるIPアドレスを入力します。IPアドレスは「.」（ドット）で区切られた4つの数字の内の最後の1つを入力します。例えば「192.168.1.200」を設定するときは「200」を入力します。DHCPサーバ機能を使用しないで固定のIPアドレスを設定しているときは「固定設定」を選択して固定設定するIPアドレスを入力します。

「MACアドレス」
コンピュータのMACアドレスを設定します。MACアドレスを自動検出するときは「自動検出」を選択します。MACアドレスを直接入力するときは「MACアドレス指定」選択して、コンピュータのMACアドレスを入力します。MACアドレスは16進数（0 - 9、a - f)、12桁で入力してください。（例：0090cc11aa22）

「追加」ボタン
入力した内容でコンピュータを登録するには、「追加」ボタンをクリックします。

「更新」ボタン
入力した内容でコンピュータの設定を更新するには。「更新」ボタンをクリックします。

「PCの一覧」ボタン
PCデータベースに登録されているコンピュータを一覧表示します。

5 ローカルサーバ機能

ローカルサーバ機能とは、LAN側に接続したコンピュータ上で動作しているサーバ（アプリケーション）にインターネット（WAN）側からアクセスできる機能です。ローカルサーバ機能では、あらかじめ定義されているアプリケーションごとに転送先のLAN側コンピュータのローカルIPアドレスを設定できます。ローカルサーバ機能の設定をするには、あらかじめ転送先のコンピュータをPCデータベースに登録しておく必要があります。
ローカルサーバ機能を設定するには、画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「ローカルサーバ」をクリックします。

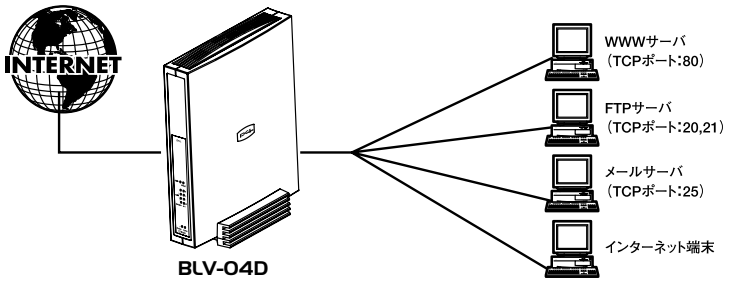


図5-1　ローカルサーバ

「登録済みのサーバ」
登録されているローカルサーバが表示されます。登録済みのローカルサーバの設定を変更するには、設定を変更するサーバをリストから選択してください。「サーバの設定」に選択したサーバの設定状況が表示されます。あらかじめ次のサーバ（アプリケーション）が登録されています。

登録済みのサーバ：WEB（HTTP）、FTP（Data/Control）、E-Mail（POP3/SMTP）、DNS、Telnet

登録済みのサーバにないサービスを公開するときは、IPフィルタリングルールで公開するサービスの設定を行います。詳細については「5-10 IPフィルタリング」を参照してください。

「有効にする」
サーバを有効にするときはチェックします。サーバを無効にするときはチェックを外します。

「ローカルPC」
インターネット側からのアクセスを転送（公開）するLAN側のコンピュータをリストから選択します。転送先に指定するコンピュータはあらかじめPCデータベースに登録しておいてください。

◎例：WEBサーバの公開

LAN側のコンピュータでWEBサーバを公開するときは、あらかじめ「PCデータベース」の設定で公開するコンピュータを登録しておきます。その次にローカルサーバの設定で「登録済みのサーバ」から「Web」を選択し、「ローカルPC」欄で公開するコンピュータを選択します。「有効にする」欄をチェックして「設定」ボタンをクリックします。
設定したWEBサーバにインターネットからアクセスするには、WEBブラウザのアドレス（URL）入力欄に本製品のWAN側ポートのIPアドレスを入力します。

6 バーチャルコンピュータ機能

バーチャルコンピュータ機能とは、LAN側のコンピュータにインターネット（WAN）側からアクセスする機能で、DMZ（DeMilitarized Zone）とよばれることもあります。バーチャルコンピュータを設定すると、インターネットからの本製品WAN側ポートのグローバルIPアドレスへ送られてくる不明なパケットはすべて設定したバーチャルコンピュータに転送されます。バーチャルコンピュータの設定をするには、あらかじめ転送先のコンピュータをPCデータベースに登録しておく必要があります。

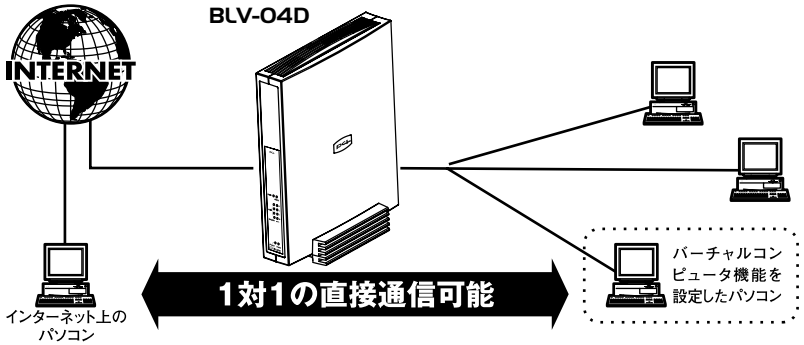


図5-2 バーチャルコンピュータ機能

バーチャルコンピュータを設定するには、画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「バーチャルコンピュータ」をクリックします。

注意

バーチャルコンピュータ機能を有効にすると、バーチャルコンピュータに設定したコンピュータに対してセキュリティが無効な状態になります。バーチャルコンピュータ機能は、必要時以外は無効にしておくことを推奨します。

「バーチャルコンピュータ」

バーチャルコンピュータ機能を使うときは「有効にする」をチェックし、転送先の（公開する）コンピュータを右側のリストから選択します。転送先に指定するコンピュータはあらかじめPCデータベースに登録しておいてください。バーチャルコンピュータ機能を使わないときはチェックを外します。

設定が終了したら「設定」ボタンをクリックします。

7 特殊アプリケーション

特殊アプリケーション機能とは、アプリケーションで使用する送信パケットと受信パケットでプロトコルとポート番号が異なるため、NAPT（IPマスカレード）環境では使用できないアプリケーションを使用できるようにする機能です。特殊アプリケーション機能の設定をするには、あらかじめアプリケーションを使用するLAN側のコンピュータをPCデータベースに登録しておく必要があります。
特殊アプリケーション機能を設定するには、画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「バーチャルコンピュータ」をクリックします。

「アプリケーション名」
使用するアプリケーションを選択します。登録されていないアプリケーションを使用するときは、「アプリケーションの追加」ボタンをクリックしてアプリケーションの追加を行います。
「アプリケーションを使用するPC」
アプリケーションを使用するコンピュータを右側のリストから選択します。使用するコンピュータはあらかじめPCデータベースに登録しておいてください。

設定が終了したら「設定」ボタンをクリックします。

●特殊アプリケーションの追加

特殊アプリケーションの追加を行うには、「アプリケーションの追加」ボタンをクリックしてください。特殊アプリケーションの追加画面が表示されます。特殊アプリケーションの追加を行うにはアプリケーションで使用するプロトコルとポート番号を調べておく必要があります。特殊アプリケーションは6個まで登録できます。

注意

ここで追加した特殊アプリケーションは、特殊アプリケーションリストには表示されません。また、アプリケーションを使用するコンピュータを指定する必要もありません。

「アプリケーション名」
追加するアプリケーションのアプリケーション名を入力してください。有効にするときはアプリケーション名の前のチェックボックスをチェックしてください。

「送信パケット」
アプリケーションの送信パケットで使用する、「プロトコル」と「開始ポート」番号、「終了ポート」番号を入力します。

「受信パケット」
アプリケーションの受信パケットで使用する、「プロトコル」と「開始ポート」番号、「終了ポート」番号を入力します。

設定が終了したら「設定」ボタンをクリックします。

8 アクセス制限

本製品は、LAN側のコンピュータのグループごとにWEB参照やE-mailの使用などの特定のインターネットサービスを曜日や時間を指定して制限することが可能です。アクセス制限の設定をするには、コンピュータのグループを編集するためにアクセス制限するLAN側のコンピュータをPCデータベースに登録しておく必要があります。

フィルタ機能の設定を行うには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「アクセス制限」をクリックしてください。

●グループの編集

アクセス制限はコンピュータのグループごとに設定します。グループには「Group1」から「Group4」と「Everyone」の5つがあります。アクセス制限を行うコンピュータが何れかのグループに参加するよう設定します。「Group1」から「Group4」のどのグループにも参加していないコンピュータは自動的に「Everyone」に参加することになります。グループのメンバを編集するにはLAN側のコンピュータをPCデータベースに登録しておく必要があります。

メンバの編集を行うグループを選択して「メンバの編集」ボタンをクリックします。選択したグループのメンバ編集画面が表示されます。

「グループのメンバ（PC）」

グループに参加しているコンピュータが表示されます。メンバから削除するには、削除するコンピュータを選択して「削除 >」ボタンをクリックします。

「その他のPC」

グループに参加していないコンピュータが表示されます。メンバに追加するには、追加するコンピュータを選択して「< 追加」ボタンをクリックします。

設定が終了したら「設定」ボタンをクリックします。

●グループのアクセス制限の設定

「グループを選択」
アクセス制限の設定をするグループを選択します。

「アクセス制限」
アクセス制限の種類を選択します。アクセス制限をしないときは「なし」を選択します。すべてのサービスの使用を制限するときは「すべてのサービス」を選択します。特定のサービスのみ使用を制限するときは「選択したサービス」を選択し、下記の「制限するサービスを選択」の欄で使用を禁止するサービスを選択します。

「スケジュール」
何曜日の何時から何時までのように、スケジュールを決めてサービスの使用を制限するときは「あり」を選択します。スケジュールを決めずに常にサービスの使用を制限するときは「なし」を選択します。スケジュールの設定方法についてはこの後で説明します。

「制限するサービスを選択」
使用を制限するサービスを選択します。リストにないサービスを追加するときは「サービスリストの編集」ボタンをクリックします。

「アクセス制限ログの表示」
アクセス制限の動作記録を表示します。

「アクセス制限ログのクリア」
アクセス制限の動作記録を消去します。

設定が終了したら「設定」ボタンをクリックします。

●スケジュールの設定

スケジュールの設定は曜日ごとに何時から何時までという形でアクセス制限する時間を入力します。各曜日2つまで時間を設定できます。時間は24時間表記で入力してください。1日中制限を行うときはその曜日の「Session1」の欄に「00：00 - 24：00」と入力します。1日中制限を行わないときはその曜日のすべての欄を空欄にします。

設定が終了したら「設定」ボタンをクリックします。

●サービスリストの編集

「登録されているサービス」
登録されているサービスの一覧が表示されます。ユーザが追加したサービスにはサービス名の前に「*」（アスタリスク）が表示されます。追加したサービスを削除するときは、削除するサービスを選択して「削除」ボタンをクリックします。初期登録されているサービスは削除できません。

「サービス名」
追加するサービスの名前を入力します。

「プロトコル」
追加するサービスで使用しているプロトコルを「TCP」、「UDP」、「TCP&UDP」、「ICMP」から選択します。

「開始ポート」
プロトコルで「TCP」、「UDP」、「TCP&UDP」を選択したときはサービスで使用しているポート範囲の開始ポート番号を入力します。

「終了ポート」
プロトコルで「TCP」、「UDP」、「TCP&UDP」を選択したときはサービスで使用しているポート範囲の終了ポート番号を入力します。

「ICMPタイプ」
プロトコルで「ICMP」を選択したときは、ICMPのタイプを入力します。

設定が終了したら「設定」ボタンをクリックします。

9 URLフィルタ

URLフィルタ機能では、LAN側のコンピュータからの登録されたURLへのアクセスを制限する事ができます。
ファイアウォール機能を設定するには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「URLフィルタ」をクリックします。

「URLフィルタ」
ここをチェックするとURLフィルタが有効になります。URLフィルタを無効にするにはチェックを外してください。
「URLフィルタの設定」ボタン
URLフィルタの設定をするときにクリックします。

●URLフィルタの設定

アクセスを制限するURLの登録をします。アクセスを制限したいWEBサイトのURL 、IPアドレス、キーワードのいずれかを入力します。
例えば、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。

「削除」ボタン
フィルタを削除したいときは、削除したいフィルタをフィルタリストから選択してこのボタンをクリックします。
「すべて削除」ボタン
すべてのフィルタを削除したいときはこのボタンをクリックします。
「フィルタの追加」
追加したいフィルタのURL、IPアドレス、キーワードの何れかを入力して「追加」ボタンをクリックします。

> **注意**
> ***URLを入力するときは、http：// の部分は入力しないでください。***

10 IPフィルタリング

IPフィルタリングでは、IPアドレスやポート番号を指定して、特定の通信を遮断したり、または特定の通信のみをLAN側に転送しサーバを公開することができます。IPフィルタリング機能を設定するには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「IPフィルタリング」をクリックします。

> **注意**
>
> ***IPフィルタルールに間違ったルールを設定すると通信が一切できなくなることがあります。ルールの追加は十分注意して行ってください。***

「フィルタの方向」
フィルタルールは各ポート間の通信の方向ごとに設定できます。フィルタの表示/追加を行う方向を選択します。

「フィルタエントリ」
各フィルタエントリには次の情報が表示されます。ルールは表示されている順に適用されます。

「ルール名」
ルールの名前が表示されます。

「送信元」
このルールが適用される送信元IPアドレスが表示されます。

「送信先」
このルールが適用される送信先IPアドレスが表示されます。

「動作」
ルールが適用されたときの動作 ”Forward”（転送） または ”Block”（破棄） が表示されます。

●ルールの追加/編集

ルールの追加をするときは「追加」ボタンをクリックします。
登録済みのルールを編集するときは、リストから編集するルールを選択して「編集」ボタンをクリックします。
IPフィルタルールの設定画面が表示されます。

「ルール名」

このルールに付ける名前を入力します。任意の名前を設定できます。

「ルールの方向」

ルールは各方向ごとに設定できます。追加するルールの方向を選択します。

「送信元IPアドレス」

このルールを適用する、送信元IPアドレスを設定します。
IPアドレスは次の方法で指定できます。

- Any　：すべての送信元IPアドレスがこのルールの対象になります。
- 1個のアドレス　：1個のIPアドレスを指定します。「開始IPアドレス」欄に対象となるIPアドレスを入力します。
- アドレス範囲指定　：IPアドレスを範囲で指定します。対象となるIPアドレス範囲の最初のIPアドレスを「開始IPアドレス」欄に、最後のIPアドレスを「終了IPアドレス」欄に入力します。

・サブネット指定　：IPアドレスをサブネットで指定します。対象となるサブネットのネットワークアドレスを「開始IPアドレス」欄に、サブネットマスクを「サブネットマスク」欄に入力します。

「送信先IPアドレス」
このルールを適用する、送信先IPアドレスを設定します。IPアドレスは次の方法で指定できます。

・Any　：すべての送信先IPアドレスがこのルールの対象になります。
・1個のアドレス　：1個のIPアドレスを指定します。「開始IPアドレス」欄に対象となるIPアドレスを入力します。
・アドレス範囲指定　：IPアドレスを範囲で指定します。対象となるIPアドレス範囲の最初のIPアドレスを「開始IPアドレス」欄に、最後のIPアドレスを「終了IPアドレス」欄に入力します。
・サブネット指定　：IPアドレスをサブネットで指定します。対象となるサブネットのネットワークアドレスを「開始IPアドレス」欄に、サブネットマスクを「サブネットマスク」欄に入力します。

「サービスリスト」
このルールを適用するサービスを選択します。サービスリストに適用したいサービスが無いときは、「サービスリストの編集」ボタンをクリックして、サービスを追加します。

「動作」
このルールに合致したときの動作を設定します。
・転送　：このルールに合致したパケットを転送します。
・破棄　：このルールに合致したパケットを破棄します。

「ログ」
IPフィルタログへの記録の方法を設定します。
・すべて記録　：ルールに合致した場合も、ルールに合致しない場合もログに記録します。
・記録しない　：一切ログに記録しません。
・ルールに合致したときは記録　：ルールに合致した場合だけログに記録します。
・ルールに合致しないときは記録　：ルールに合致しなかった場合だけログに記録します。

●ルールの移動

ルールを移動することによりルールが適用される順番を変更することができます。ルールの位置を移動するには次の2つの方法があります。

・移動するルールを選択して、リストの右側にある上下の矢印ボタンをクリックします。移動を適用するには「OK」ボタンをクリックします。移動をキャンセルするときは「CANCEL」ボタンをクリックします。
・移動するルールを選択して ” 移動 ” ボタンをクリックすると、移動先の位置を入力するダイアログボックスが表示されるので、移動先を番号で入力します。

●ルールの削除

登録済みのルールを削除するときは、リストから削除するルールを選択して「削除」ボタンをクリックします。

●IPフィルタログの表示

「ログの表示」ボタンをクリックすると、IPフィルタの動作状況のログが表示されます。

●ルールの一覧表示

「ルールの一覧」ボタンをクリックすると、現在登録されているすべてのルールが表示されます。

●IPフィルタリングルールによるローカルサーバ公開の設定

ローカルサーバ機能に登録されていないサービスを公開するときは、IPフィルタリングに転送ルールを追加します。

各項目をそれぞれ次のように設定します。

「ルール名」
任意のルール名を入力します。

「ルール方向」
「WAN⇒LAN」を選択します。

「送信元IPアドレス」
通常は、アドレス指定には「Any」を選択します。特定のIPアドレスからのアクセスのみ許可するときは、アクセスを許可したいIPアドレスを設定します。

「サービスリスト」
公開するサービスを選択します。リストに公開するサービスがないときは「サービスリストの編集」ボタンをクリックして、サービスを追加します。

「動作」
「転送」を選択します。

「ログ」
任意のログ方法を選択します。

11 ファイアウォール設定

本製品はSPI（Statefull Packet Inspection）方式のファイアウォール機能を装備しており、DoS（Denial of Service）攻撃の検出ができます。インターネット（WAN）側からの次の攻撃を検出し、これを遮断します。

検出できる攻撃：「IP Spoofing」「Land Attack」「Ping of Death」「Zero Length IP」「Smurf Attack」「UDP Port Loopback」「Snork Attack」「TCP null scan」「TCP Syn flood」

検出した攻撃は、ログに記録することができます。また、記録したログはE-MailとSyslogで送信することができます。

ファイアウォール機能を設定するには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「セキュリティ」をクリックします。

「ファイアウォール機能」
ファイアウォール機能を使うときは「DoS（Denial of Service）攻撃検出を有効にする」をチェックし、次の「WAN側回線速度」を設定します。ファイアウォール機能を使わないときはチェックを外します。DoS攻撃の検出とともにSPI方式のファイアウォール機能も有効になります。

「WAN側回線速度」
ファイアウォール機能を使用するときに、WAN側の回線の速度を設定します。

「WAN（インターネット）からのpingに応答する」
この項目をチェックすると、WAN（インターネット）からのpingに応答します。チェックを外すとpingに応答しません。pingは攻撃の前段階として、攻撃対象となるホストの検出に使用されることがあります。よりセキュリティを高めるためにはチェックを外しておくことを推奨します。

設定が終了したら「設定」ボタンをクリックします。

12 VPNパススルー設定

本製品はLAN-WAN間でVPNパケットをパススルーすることができます。パススルー可能なVPNプロトコルは、IPsec、PPTP、L2TP の3種類です。VPNパススルーの設定をするには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「セキュリティ」をクリックします。

「IPsecパススルー有効」
この項目をチェックするとIPsecプロトコルを使用したVPNパケットのパススルー機能が有効になります。無効にしたいときはチェックを外します。
「PPTPパススルー有効」
この項目をチェックするとPPTPプロトコルを使用したVPNパケットのパススルー機能が有効になります。無効にしたいときはチェックを外します。
「L2TPパススルー有効」
この項目をチェックするとL2TPプロトコルを使用したVPNパケットのパススルー機能が有効になります。無効にしたいときはチェックを外します。

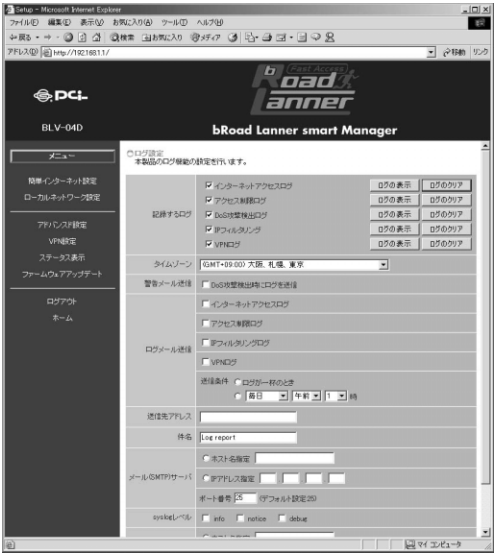
設定が終了したら「設定」ボタンをクリックします。

注意

・VPNパススルー機能はVPNゲートウェイ機能とは異なります。VPNパススルー機能を使用して、実際にVPNでの通信を行うにはVPNサーバやVPNクライアントなどの機能に対応した機器やソフトウェアなどが必要です。
・LAN側にVPNサーバを設置する場合は、VPNサーバをバーチャルコンピュータに設定してください。

13 ログ機能の設定

本製品はLAN側コンピュータからのインターネットアクセスやアクセス制限、DoS攻撃検出などの状況をログに記録することができます。また、記録したログはE-Mail送信やsyslogサーバに送信することもできます。
ログ機能の設定をするには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「ログ」をクリックします。



「記録するログ」
記録するログの種類を選択します。「インターネットアクセスログ」はLAN側のコンピュータからのインターネットへのアクセスを記録します。「アクセス制限ログ」はアクセス制限機能の動作状況を記録します。「DoS攻撃検出ログ」はDoS攻撃の検出を記録します。「IPフィルタリング」はIPフィルタリングの動作状況を記録します。「VPN動作ログ」はVPNゲートウェイ機能の動作状況を記録します。

「ログの表示」ボタン
ログを表示します。

「ログのクリア」ボタン
ログを消去します。

「タイムゾーン」
ログに時刻を記録ときに適用するタイムゾーンを選択します。日本の場合、「(GMT＋09：00）大阪、札幌、東京」を選択します。

「警告メール送信」
DoS攻撃検出ログが有効で、DoS攻撃を検出したときにDoS攻撃検出ログをメール送信するかどうかを設定します。DoS攻撃検出ログをメール送信するときは「送信先アドレス」などの各項目を正しく設定してください。

「ログメール送信」
DoS攻撃検出以外のログについてメール送信するかどうかを設定します。メール送信するときは「送信条件」と「送信先アドレス」などの各項目を正しく設定してください。

「送信先アドレス」
メールの送信先アドレスを入力します。メールアドレスは「@（アットマーク)」以降も含めて正しく入力してください。

「件名」
送信メールの件名を入力します。

「メール（SMTP）サーバ」
送信先のメール（SMTP）サーバのアドレスをホスト名またはIPアドレスで入力します。

「ポート番号」
メール送信に使用するポート番号を入力します。通常はデフォルト値の「25」から変更する必要はありません。

「syslogレベル」
syslogサーバに送信するsyslogメッセージのレベルを設定します。送信するsyslogレベルをチェックします。syslogメッセージの送信を行わないときはすべてのチェックを外します。

「syslogサーバ」
syslogメッセージを送信するsyslogサーバをIPアドレスまたはホスト名で入力します。

設定が終了したら「設定」ボタンをクリックします。

14 UPnP（ユニバーサルプラグアンドプレイ）

本製品はUPnP（ユニバーサルプラグアンドプレイ）に対応しています。UPnP機能の設定をするには、画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「UPnP」をクリックします。

「UPnP」
この項目をチェックするとUPnP機能が有効になります。UPnP機能を無効にするときはチェックを外します。

「UPnP経由で設定を変更できる」
この項目をチェックするとUPnPプロトコル経由での本製品の設定の変更ができるようになります。

「UPnP経由でインターネットアクセスを無効にできる」
この項目をチェックするとUPnPプロトコル経由での本製品のインターネット接続を無効にできるようになります。

設定が終了したら「設定」ボタンをクリックします。

注意

UPnPからの設定変更は通常のWEBブラウザからの設定と違い、パスワードが必要ありません。このためLAN側に多数のユーザが接続している環境などでは、UPnP経由での設定変更とインターネットアクセス無効の設定はチェックしないで使用することを推奨します。

15 ルーティング設定

本製品はダイナミックルーティングプロトコルとしてRIP（Ver.1）に対応しています。また、スタティックルーティングを追加することができます。ルーティングの設定をするには、設定画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「ルーティング」をクリックします。

「RIP」
この項目をチェックするとRIP（Ver.1）が有効になります。RIPを有効にすると、ネットワーク上の他のRIP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を無効にするときはチェックを外してください。

設定が終了したら「設定」ボタンをクリックします。

●スタティックルーティングエントリの追加/修正

「スタティックルーティングテーブル」には、登録されたスタティックルーティングのエントリが表示されます。
スタティックルーティングを追加するときは、次の各項目を入力して「追加」ボタンをクリックします。登録済みのエントリを修正するときは、スタティックルーティングテーブルから修正するエントリを選択し、次の各項目を変更して「更新」ボタンをクリックします。エントリを削除するときは削除するエントリを選択して「削除」ボタンをクリックします。
スタティックルーティングエントリの最大登録数は20です。

「送信先アドレス」
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。

「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。

「ゲートウェイアドレス」
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。

「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。

●ルーティングテーブルの表示

「ルーティングテーブルの表示」ボタンをクリックすると、スタティックルーティングも含めた、すべてのルーティングテーブルが表示されます。

16 DMZ機能による複数グローバルIPアドレス接続の設定

本製品はDMZネットワーク機能を装備しています。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利用のときは、DMZ機能によりサーバを公開することができます。

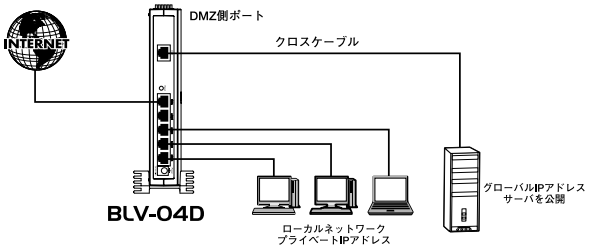


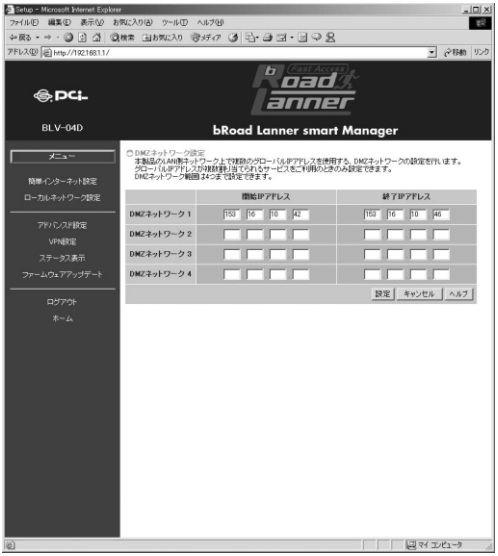
図5-3 DMZネットワーク

DMZネットワーク機能でグローバルIPアドレスを使用して公開するサーバはDMZポートに接続します。DMZポートにサーバを直接接続するときは、クロスタイプのLANケーブルを使用します。

DMZネットワークの設定をするには、設定画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「DMZネットワーク」をクリックします。

画面に設定済みのDMZネットワーク範囲がリスト表示されます。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。

DMZネットワーク範囲の設定をするには、DMZネットワーク範囲の最初のIPアドレスを「開始IPアドレス」欄に、最後のIPアドレスを「終了IPアドレス」欄に入力して「設定」ボタンをクリックします。



●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IP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。
・LAN側ポートの設定は変更しないでください。LAN側ポートにグローバルIPアドレスを設定すると正常に動作しません。

●ＤＭＺホスト（コンピュータやサーバ）の設定

本製品のDMZネットワーク機能を利用する場合、DMZネットワークに接続するホスト（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アドレスの中で、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

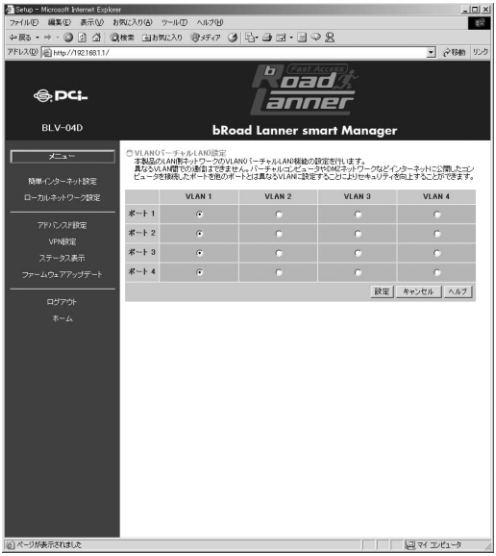
■デフォルトゲートウェイ

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

17 VLAN（バーチャルLAN）

本製品のLAN側ポートは最高4グループのポートベースVLANに対応しています。VLAN設定をすると異なるVLANグループ間では通信ができなくなります。バーチャルコンピュータ機能を使用してインターネットに公開するコンピュータを接続したポートを他のポートとは異なるVLANグループに設定することによりセキュリティを向上することができます。工場出荷時の状態ではすべてのポートがVLANグループ1に参加しています。
VLANの設定をするには、設定画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「VLAN（バーチャルLAN）」をクリックします。



各ポートごとに参加するVLANグループを選択してください。各ポートは1つのVLANグループに参加することができます。

設定が終了したら「設定」ボタンをクリックします。

18 MACアドレスの変更

本製品のWAN側ポートのMACアドレスを変更します。通常はMACアドレスを変更する必要はありません。プロバイダによってはインターネットに接続するコンピュータのMACアドレスの登録が必要なことがあります。すでにコンピュータのMACアドレスを登録しているときは登録済みのMACアドレスに変更することにより、プロバイダへの登録変更をすることなくご利用いただけます。

MACアドレスの変更をするには、設定画面左側のメインメニューから「アドバンスド設定」をクリックし、表示されるアドバンスド設定メニューから「MACアドレス」をクリックします。

「MACアドレス」
本製品の現在のWAN側ポートのMACアドレスが表示されます。

「出荷時設定」
本製品のWAN側ポートのMACアドレスを出荷時の設定に戻します。

「このPCからコピー」
本製品のWAN側ポートのMACアドレスに、現在設定するためにアクセスしているコンピュータのMACアドレスをコピーできます。

設定が終了したら「設定」ボタンをクリックします。

19 リモート管理設定

本製品のインターネット（WAN）からの設定画面へのログイン許可の設定を行います。設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「リモート管理」をクリックします。

「リモート管理」
この項目をチェックするとインターネット（WAN）側からの設定画面へのログインを許可します。この項目は必要なとき以外はセキュリティ上、チェックしないことを推奨します。

「ポート番号」
インターネット（WAN）側から設定画面へアクセスするときのポート番号を設定します。

設定が終了したら「保存」ボタンをクリックします。

インターネット側から、本製品の設定画面にアクセスするときはブラウザのアドレスを入力する欄に次のように入力してください。

http：//WAN側IPアドレス：ポート番号/

20 Dynamic DNS設定

本製品はwww.dyndns.orgにより提供されているDynamic DNSサービスに対応しています。dyndns.orgに登録してあるユーザ名、パスワード、ドメイン名の情報を本製品に設定しておくことにより、自動的に登録内容の更新を行います。
DynamicDNSの設定をするには、設定画面左側のメインメニューの「アドバンスド設定」をクリックして表示されるアドバンスド設定メニューから「Dynamic DNS」をクリックします。

注意

設定をする前に http：//www.dyndns.org/ にアクセスしてドメイン名の登録を行ってください。

「ユーザ名」
dyndns.orgに登録したユーザ名を入力します。

「パスワード」
dyndns.orgに登録したパスワードを入力します。

「ドメイン名」
dyndns.orgに登録したドメイン名を入力します。

設定が終了したら「設定」ボタンをクリックします。

21 ステータス表示

ステータス表示画面では、本製品のWAN側ポートの接続状況、LAN側ポートの設定、ファームウェアのバージョンなどの情報を表示と、DHCPによるWAN側IPアドレスの開放/更新、PPPoE接続の手動接続/切断の操作ができます。
ステータス画面を表示するには、メインメニューから「ステータス表示」をクリックします。

WAN側ポートのステータスの「詳細」ボタンをクリックすると、さらに詳細なステータスが表示されます。

「解放/更新」ボタン
WAN側ポートの接続方法がDHCP接続のときにIPアドレスの解放/更新をします。

「接続」ボタン
WAN側ポートの接続方法がPPPoE接続のときにPPPoEの接続処理をします。

「切断」ボタン
WAN側ポートの接続方法がPPPoE接続のときにPPPoEの切断処理をします。

22 ファームウェアのアップデート

本製品はWEBブラウザからファームウェアのアップデートができます。

ファームウェアをアップデートするときは、設定画面左側のメインメニューの「ファームウェアアップデート」をクリックします。

「パスワード」
本製品の管理者パスワードを入力します。

「ファームウェアファイル」
ファームウェアファイルをフルパスで入力します。または「参照」ボタンをクリックしてファームウェアファイルを選択します。
ファームウェアファイルを選択したら、「アップデート」ボタンをクリックします。ファームウェアが読み込まれ本製品が再起動します。

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。

VPNゲートウェイ設定

本章では、本製品のVPN（IPSec）ゲートウェイ機能について説明します。

1 VPNゲートウェイ機能について

VPN（仮想プライベートネットワーク）とは、インターネット経由で遠隔地の拠点間を仮想的なプライベートネットワークのように接続する機能です。本製品のVPNゲートウェイ機能では、VPNのプロトコルとしてIPSecに対応しています。IPSecを使用したVPNには、トンネルモードとトランスポートモードがありますが、本製品はトンネルモードのIPSecに対応しています。

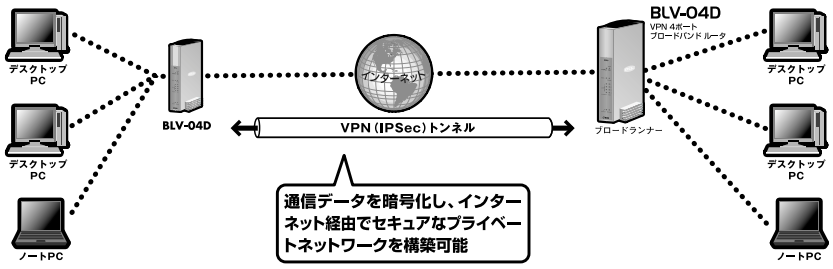


図6-1 VPN

本製品は、IPSecの鍵交換方法として手動設定と IKE（Internet Key Exchange）による自動設定に対応しています。
その他、本製品のVPNゲートウェイ機能では次のプロトコル、アルゴリズムに対応しています。

認証方式	RSA Signature（公開鍵方式） Pre-shared key（共通鍵方式）
ハッシュアルゴリズム	MD5、SHA-1
暗号化アルゴリズム	DES、3DES
鍵交換モード	Main Mode、Aggressive Mode
Diffie-Hellman Group	Group1（768bit） Group2（1024bit）

表6-1 IPSecプロトコル/アルゴリズム

2 VPNポリシーの設定

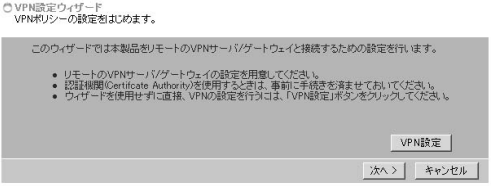
VPNによる通信を行うには、鍵交換の方法や暗号化のアルゴリズム、VPN通信を適用するローカルおよびリモート側のIPアドレスなどの情報を定義した、VPNポリシーを設定します。
VPNポリシーの設定は、WEB設定画面の左側のメニューから「VPN設定」を選択して表示される「VPN設定メニュー」から「VPNポリシー」を選択します。

画面には設定済みのVPNポリシーが表示されます。VPNポリシーは先に表示されているものから順に適用されます。VPNポリシーの最大登録数は70個です。本製品は同時に最大70拠点との接続が可能です。

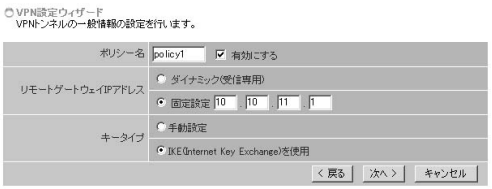
●VPNポリシーの追加

1. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

2. 「次へ ＞」ボタンをクリックしてください。ここで「VPN設定」ボタンをクリックするとウィザードを使用せずに直接ポリシーの設定をすることができます。



3. このポリシーの一般情報を設定します。次の項目を入力して「次へ ＞」ボタンをクリックします。



「ポリシー名」

このVPNポリシーの名前を設定します。任意の名前を入力できます。登録するVPNポリシーをすぐに有効するときは「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」

リモート側のVPNゲートウェイのIPアドレスを設定します。「ダイナミック」を選択すると、このルータは受信専用となります。「固定設定」を選択したときは、リモート側のVPNゲートウェイのIPアドレスを入力します。

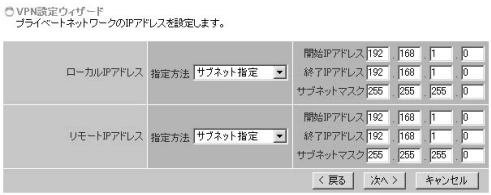
「キータイプ」

キー設定の種類を設定します。キーを手動設定するときは「手動設定」を選択します。IKEプロトコルを使用してキーを自動設定するときは「IKE（Internet Key Exchange）を使用する」を選択します。

注意

「リモートゲートウェイIPアドレス」で「ダイナミック」を設定できるポリシーは1つのみです。複数のポリシーで「ダイナミック」設定をすることはできません。

4. このポリシーを適用する、ローカルIPアドレスとリモートIPアドレスを設定します。次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」

このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。IPアドレスの指定には次の方法があります。

- すべて　：すべてのローカルIPアドレスを指定します。
- 1個のアドレス　：1個のIPアドレス（ホスト）を指定します。「開始IPアドレス」にホストのIPアドレスを入力します。
- アドレス範囲指定　：IPアドレスを範囲で指定します。「開始IPアドレス」と「終了IPアドレス」にIPアドレス範囲を入力します。
- サブネット指定　：IPアドレスをサブネットで指定します。「開始IPアドレス」にネットワークアドレスを入力し、「サブネットマスク」にサブネットマスクを入力します。

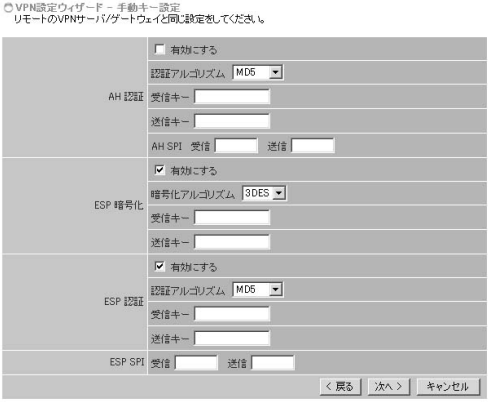
「リモートIPアドレス」

このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。IPアドレスの指定には次の方法があります。

- 1個のアドレス　：1個のIPアドレス（ホスト）を指定します。「開始IPアドレス」にホストのIPアドレスを入力します。
- アドレス範囲指定　：IPアドレスを範囲で指定します。「開始IPアドレス」と「終了IPアドレス」にIPアドレス範囲を入力します。
- サブネット指定　：IPアドレスをサブネットで指定します。「開始IPアドレス」にネットワークアドレスを入力し、「サブネットマスク」にサブネットマスクを入力します。

5. キーの設定をします。手順3で選択したキーの種類により設定内容が異なります。次の項目を入力して「次へ ＞」ボタンをクリックします。

■キーを手動設定する場合



「AH認証」

AH認証を行うかどうかを設定します。AH認証を行うときは「有効にする」をチェックして、「認証アルゴリズム」、「送信キー」、「受信キー」、「AH SPI」を設定します。

「送信キー」、「受信キー」はASCII文字列もしくは16進数（0-9、A-F）で入力します。「認証アルゴリズム」に「MD5」を選択したときは、32桁の16進数または16文字のASCII文字列で入力します。「認証アルゴリズム」に「SHA-1」を選択したときは、40桁の16進数または20文字のASCII文字列で入力します。ここで設定した「送信キー」をリモート側の「受信キー」に設定します。また、ここで設定した「受信キー」をリモート側の「送信キー」に設定します。

「AH SPI」は4桁以上の数字で入力します。ここで設定した「受信 SPI」をリモート側の「送信 SPI」に設定します。また、ここで設定した「送信 SPI」をリモート側の「受信 SPI」に設定します。

「ESP暗号化」

ESP暗号化を行うかどうかを設定します。ESP暗号化を行うときは「有効にする」をチェックして、「暗号化アルゴリズム」、「送信キー」、「受信キー」を設定します。

「送信キー」、「受信キー」はASCII文字列もしくは16進数（0-9、A-F）で入力します。「暗号化」に「DES」を選択したときは、16桁の16進数または8文字のASCII文字列で入力します。「暗号化アルゴリズム」に「3DES」を選択したときは、48桁の16進数または24文字のASCII文字列で入力します。ここで設定した「送信キー」をリモート側の「受信キー」に設定します。また、ここで設定した「受信キー」をリモート側の「送信キー」に設定します。

「ESP認証」

ESP認証を行うかどうかを設定します。通常「ESP暗号化」を有効にするときは「ESP認証」も有効にします。ESP認証を行うときは「有効にする」をチェックして、「認証アルゴリズム」、「送信キー」、「受信キー」を設定します。

「送信キー」、「受信キー」はASCII文字列もしくは16進数（0-9、A-F）で入力します。「認証アルゴリズム」に「MD5」を選択したときは、32桁の16進数または16文字のASCII文字列で入力します。「認証アルゴリズム」に「SHA-1」を選択したときは、40桁の16進数または20文字のASCII文字列で入力します。ここで設定した「送信キー」をリモート側の「受信キー」に設定します。また、ここで設定した「受信キー」をリモート側の「送信キー」に設定します。

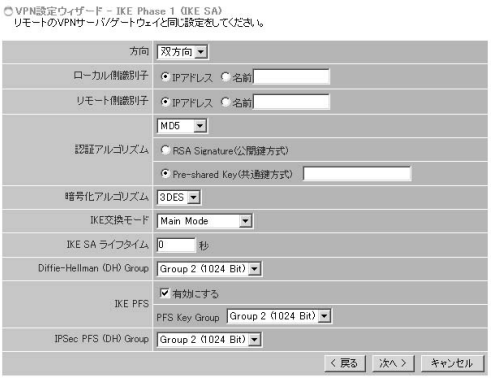
「ESP SPI」

「ESP暗号化」および「ESP認証」を有効にしたときだけ「ESP SPI」を設定します。「ESP SPI」は4桁以上の数字で入力します。ここで設定した「受信 SPI」をリモート側の「送信 SPI」に設定します。また、ここで設定した「送信 SPI」をリモート側の「受信 SPI」に設定します。

■キーをIKEにより自動設定する場合

IKEによるキー設定では「PHASE-1」と「PHASE-2」の2つの設定が必要です。

A.IKE PHASE-1



「方向」

接続の方向を設定します。「受信側」を選択するとリモート側のVPNゲートウェイからの接続に対して応答する側（レスポンダ）となります。こちらからリモート側への接続を開始することはありません。「送信側」を選択するとリモート側のVPNゲートウェイへの接続を開始する側（イニシエータ）となります。リモート側からの接続への応答は行いません。「双方向」を選択するとリモート側からの接続への応答、リモート側への接続の開始の両方の動作を行います。

「ローカル側識別子」

ローカル側（この）ルータの識別子を設定します。「IPアドレス」を選択すると識別子にIPアドレスを使用します。「名前」を選択したときはこのルータの名前（ホスト名など）を入力します。ここで設定した識別子をリモート側のVPNゲートウェイの「リモート側識別子」に設定します。

「リモート側識別子」

リモート側ルータの識別子を設定します。「IPアドレス」を選択すると識別子にIPアドレスを使用します。「名前」を選択したときはこのルータの名前（ホスト名など）を入力します。ここで設定した識別子をリモート側のVPNゲートウェイの「ローカル側識別子」に設定します。

「認証アルゴリズム」
認証アルゴリズムと鍵方式を設定します。「認証アルゴリズム」を「MD5」または「SHA-1」から選択します。「鍵方式」を「RSA Signature（公開鍵方式）」または「Pre-shared key（共通鍵方式）」から選択します。「RSA Signature（公開鍵方式）」を選択したときは、接続する両端で認証局（CA）による証明書が必要です。「Pre-shared key（共通鍵方式）」を選択したときは、128文字以内のキー文字列を入力します。認証アルゴリズムと鍵方式はリモート側にも同じ設定をします。

「暗号化アルゴリズム」
暗号化アルゴリズムを「DES」または「3DES」から選択します。「3DES」を使用したほうが、よりセキュリティが高くなります。リモート側にも同じ設定をしてください。

「IKE交換モード」
IKE交換モードを「Main Mode」または「Aggressive Mode」から選択します。「Main Mode」では、通信が確立するまでIDを隠蔽します。より安全ですが、通信を開始するまでに時間がかかります。「Aggressive Mode」では、IDの隠蔽は行いませんが、より早く通信を開始することができます。リモート側にも同じ設定をしてください。

「IKE SA ライフタイム」
IKE SAのキーの有効期間を秒単位で設定します。例えば8時間を設定するときは「28800」を入力します。

「Diffie-Hellman （DH） Group」
Diffie-Hellman鍵交換アルゴリズムで使用するパラメータを「Group 1（768Bit）」または「Group 2（1024Bit）」から選択します。リモート側にも同じ設定をしてください。

「IKE PFS」
IKE SA Phase2においてPFS（Perfect Forward Secrecy）を使用するか設定します。PFSを使用したほうが、よりセキュリティが高くなります。リモート側にも同じ設定をしてください。「Disable」を選択するとPFSを使用しません。PFSを使用するときは「Group 1（768Bit）」または「Group 2（1024Bit）」を選択します。

「IPSec PFS」
IPSec SAにおいてPFS（Perfect Forward Secrecy）を使用するか設定します。PFSを使用したほうが、よりセキュリティが高くなります。リモート側にも同じ設定をしてください。「Disable」を選択するとPFSを使用しません。PFSを使用するときは「Group 1（768Bit）」または「Group 2（1024Bit）」を選択します。

B.IKE PHASE-2

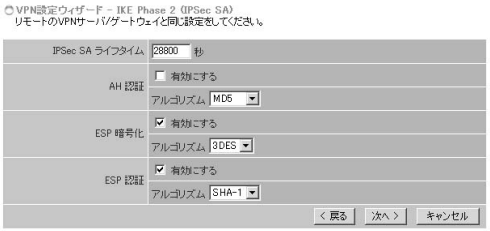
「IKE SA ライフタイム」
IKE SAのキーの有効期間を秒単位で設定します。例えば8時間を設定するときは「28800」を入力します。

「AH認証」
AH認証を行うかどうかを設定します。AH認証を行うときは「有効にする」をチェックして、「アルゴリズム」を「MD5」または「SHA-1」から選択します。

「ESP暗号化」
ESP暗号化を行うかどうかを設定します。ESP暗号化を行うときは「有効にする」をチェックして、「アルゴリズム」を「DES」または「3DES」から選択します。

「ESP認証」
ESP認証を行うかどうかを設定します。通常「ESP暗号化」を有効にするときは「ESP認証」も有効にします。ESP認証を行うときは「有効にする」をチェックして、「アルゴリズム」を「MD5」または「SHA-1」から選択します。

6. これでポリシーの設定は完了です。「完了」ボタンをクリックします。



●VPNポリシーの編集
既存のVPNポリシーの設定を変更するときは、変更するVPNポリシーを選択して「更新」ボタンをクリックします。

●VPNポリシーの有効/無効の切り替え
既存のVPNポリシーの有効/無効の切り替えをするときは、変更するVPNポリシーを選択して「有効/無効」ボタンをクリックします。

●VPNポリシーのコピー
既存のVPNポリシーをコピーして新たにVPNポリシーを作成するときは、元のVPNポリシーを選択して「コピー」ボタンをクリックします。

●VPNポリシーの削除
既存のVPNポリシーを削除するときは、削除するVPNポリシーを選択して「削除」ボタンをクリックします。

●VPNポリシーの移動
VPNポリシーは登録順に適用されます。既存のVPNポリシーの順番を変更する方法には次の2つがあります。

A.変更するVPNポリシーを選択して「移動」ボタンをクリックします。移動先を入力するダイアログボックスが表示されるので移動先を番号で入力します。

B.変更するVPNポリシーを選択して右側の上下の矢印ボタンをクリックします。移動した結果を保存する時は「OK」ボタンをクリックします。移動をキャンセルするときは「CANCEL」ボタンをクリックします。

3 手動鍵設定での設定例

ここでは鍵を手動設定するときの設定について説明します。
例として、次のようなVPNネットワークを構築します。

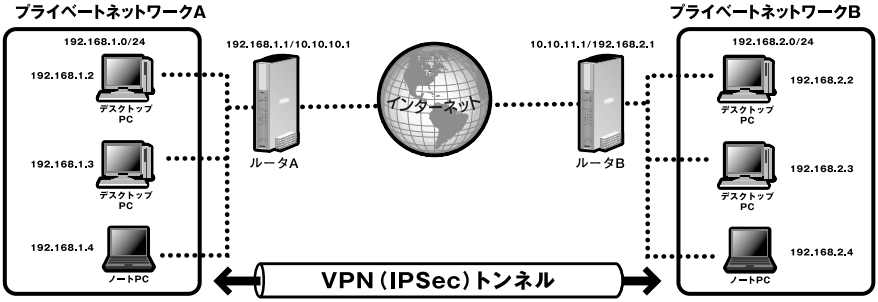


図6-2 ネットワーク例

項目	ルータA	ルータB
キータイプ	手動設定	手動設定
AH認証	なし	なし
ESP暗号化	3DES	3DES
ESP認証	SHA-1	SHA-1
ESP暗号化キー	RouterA01234567890123456	RouterB01234567890123456
認証キー	RouterA0123456789012	RouterB0123456789012
ESP SPI	10000	10001

表6-2 VPNポリシー

●ルータAの設定

VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。

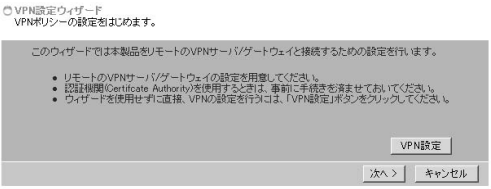
1. **本製品のWEB設定画面にログインしてください。**

2. **設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。**

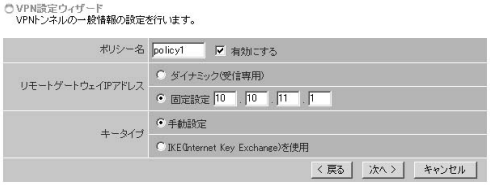
3. **VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。**

4. **VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。**

5. **「次へ ＞」ボタンをクリックしてください。**



6. 次の項目を入力して「次へ ＞」ボタンをクリックします。

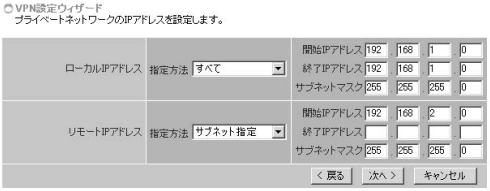


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータBのIPアドレス「10.10.11.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「手動設定」を選択します。

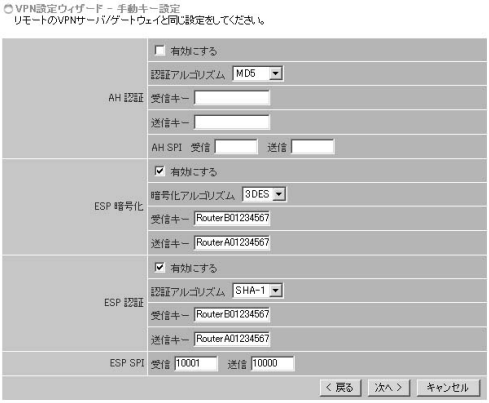
7. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークBのアドレス「192.168.2.0」と「サブネットマスク」に「255.255.255.0」を設定します。

8. **次の項目を入力して「次へ >」ボタンをクリックします。**



「AH認証」

AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」

ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「暗号化アルゴリズム」には「3DES」を選択します。「受信キー」には「RouterB01234567890123456」を入力します。「送信キー」には「RouterA01234567890123456」を入力します。

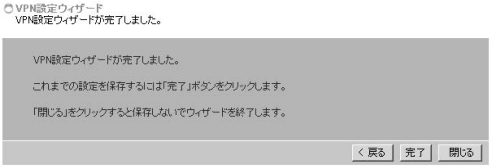
「ESP認証」

ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「認証アルゴリズム」には「SHA-1」を選択します。「受信キー」には「RouterB0123456789012」を入力します。「送信キー」には「RouterA0123456789012」を入力します。

「ESP SPI」

ESP暗号化およびESP認証を有効にするときはESP SPIを設定します。ここでは「受信キー」には「10001」を入力します。「送信キー」には「10000」を入力します。

9. 以上でルータAの設定は完了です。「完了」ボタンをクリックします。

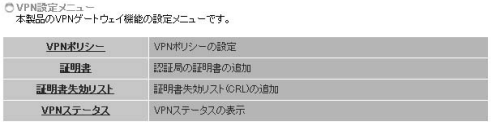


●ルータBの設定

VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。

1. 本製品のWEB設定画面にログインしてください。

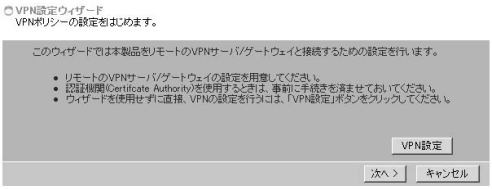
2. 設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。



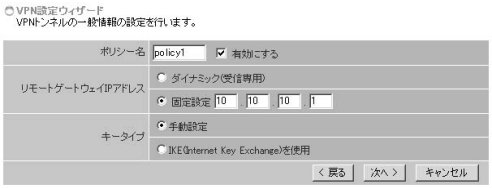
3. VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

4. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

5.「次へ ＞」ボタンをクリックしてください。



6. 次の項目を入力して「次へ ＞」ボタンをクリックします。

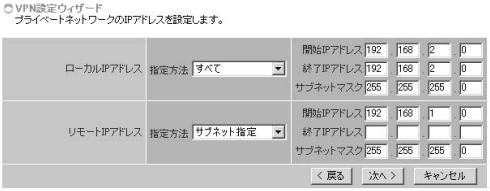


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータAのIPアドレス「10.10.10.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「手動設定」を選択します。

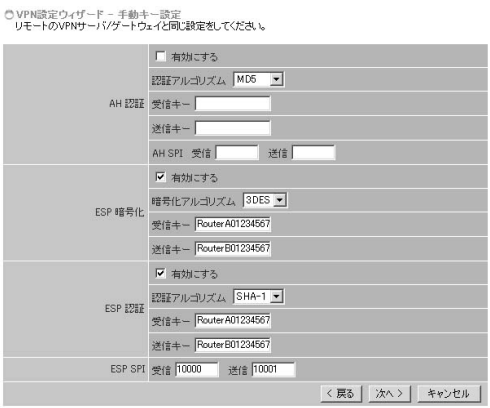
7. 次の項目を入力して「次へ >」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークAのアドレス「192.168.1.0」と「サブネットマスク」に「255.255.255.0」を設定します。

8. 次の項目を入力して「次へ >」ボタンをクリックします。



「AH認証」
AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」

ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「暗号化アルゴリズム」には「3DES」を選択します。「受信キー」には「RouterA01234567890123456」を入力します。「送信キー」には「RouterB01234567890123456」を入力します。

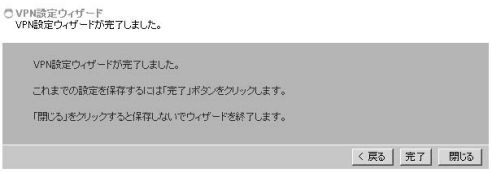
「ESP認証」

ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「認証アルゴリズム」には「SHA-1」を選択します。「受信キー」には「RouterA0123456789012」を入力します。「送信キー」には「RouterB0123456789012」を入力します。

「ESP SPI」

ESP暗号化およびESP認証を有効にするときはESP SPIを設定します。ここでは「受信キー」には「10000」を入力します。「送信キー」には「10001」を入力します。

9. **以上でルータBの設定は完了です。「完了」ボタンをクリックします。**



4 IKEによる自動鍵設定での設定例

ここではIKE（Internet Key Exchange）により自動設定するときの設定について説明します。
例として、次のようなVPNネットワークを構築します。

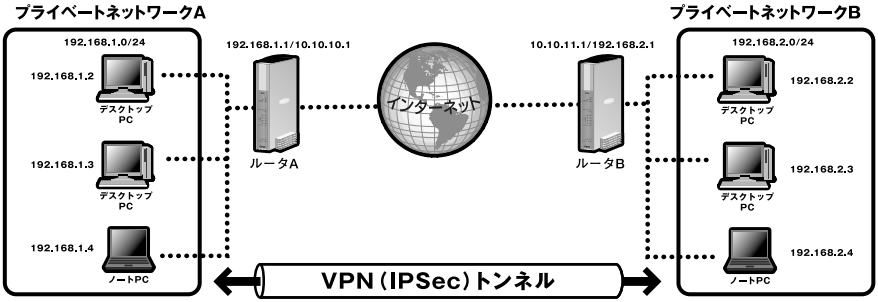


図6-3 ネットワーク例

項目	ルータA	ルータB
キータイプ	IKE	IKE
方向	双方向	双方向
IKE認証	SHA-1	SHA-1
鍵方式	Pre-shared Key	Pre-shared Key
キー	0123456789	0123456789
IKE交換モード	Main Mode	Main Mode
Diffie-Hellman group	Group2	Group2
IKE PFS	Group2	Group2
IPSec PFS	Group2	Group2
AH認証	なし	なし
ESP暗号化	3DES	3DES
ESP認証	SHA-1	SHA-1

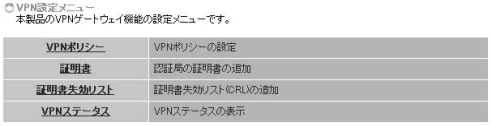
表6-3 VPNポリシー

●ルータAの設定

VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。

1. 本製品のWEB設定画面にログインしてください。

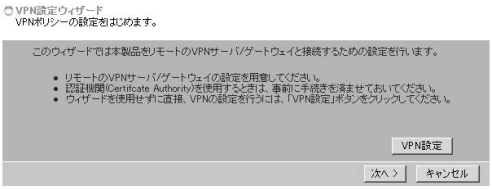
2. 設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。



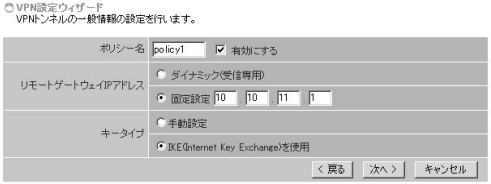
3. VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

4. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

5.「次へ ＞」ボタンをクリックしてください。



6. 次の項目を入力して「次へ ＞」ボタンをクリックします。

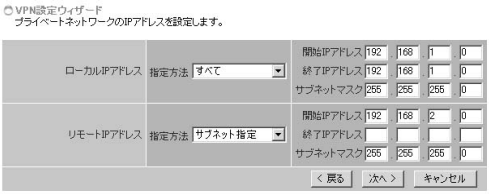


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータBのIPアドレス「10.10.11.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「IKE（Internet Key Exchange）を使用」を選択します。

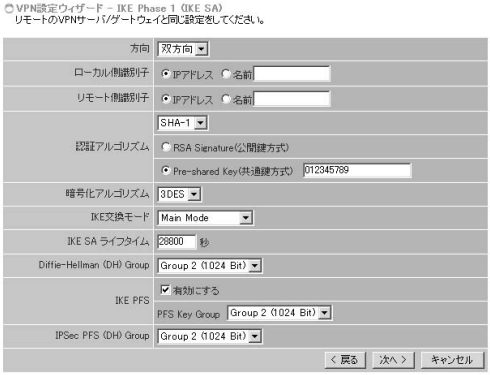
7. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークBのアドレス「192.168.2.0」と「サブネットマスク」に「255.255.255.0」を設定します。

8. IKE Phase-1の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。



「方向」
ここでは「双方向」を選択します。

「ローカル側識別子」
ここでは「IPアドレス」を選択します。

「リモート側識別子」
ここでは「IPアドレス」を選択します。

「認証アルゴリズム」
認証アルゴリズムを設定します。ここでは「認証アルゴリズム」には「SHA-1」を選択します。鍵方式には「Pre-shared Key（共通鍵方式）」を選択します。キー文字列には「0123456789」を入力します。

「暗号化アルゴリズム」
ここでは「3DES」を選択します。

「IKE交換モード」
ここでは「Main Mode」を選択します。

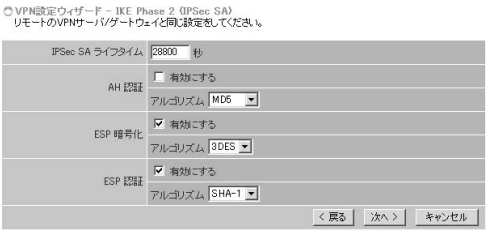
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「Diffie-Hellman（DH）Group」
ここでは「Group 2（1024bit)」を選択します。

「IKE PFS」
ここではIKE PFSを有効にします。「有効にする」をチェックして、「PFS Key Group」には「Group 2（1024bit)」を選択します。

「IPSec PFS（DH）Group」
ここではIPSec PFSを有効にします。Key Groupには「Group 2（1024bit)」を選択します。

9. **IKE Phase-2の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「AH認証」
AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」
ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「アルゴリズム」には「3DES」を選択します。

「ESP認証」
ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「アルゴリズム」には「SHA-1」を選択します。

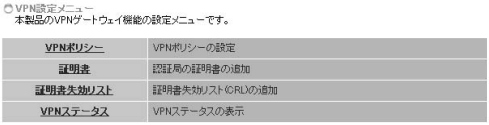
10. **以上でルータAの設定は完了です。「完了」ボタンをクリックします。**

●ルータBの設定

VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。

1. 本製品のWEB設定画面にログインしてください。

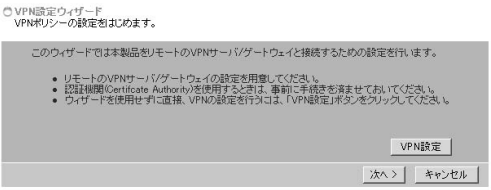
2. 設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。



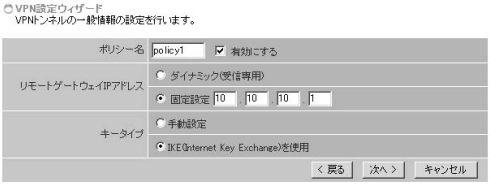
3. VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

4. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

5.「次へ ＞」ボタンをクリックしてください。



6. 次の項目を入力して「次へ ＞」ボタンをクリックします。

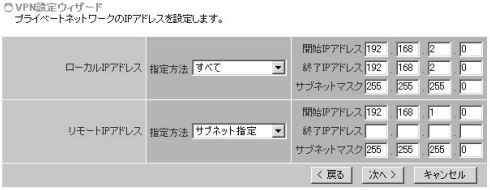


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータBのIPアドレス「10.10.10.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「IKE（Internet Key Exchange）を使用」を選択します。

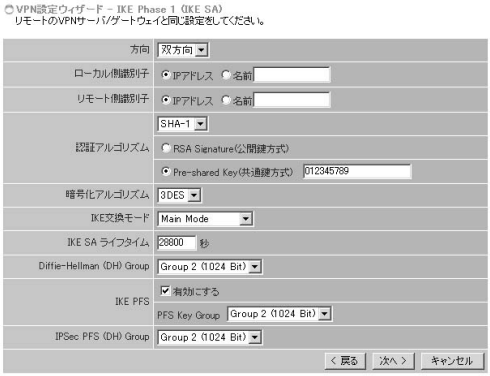
7. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークBのアドレス「192.168.1.0」と「サブネットマスク」に「255.255.255.0」を設定します。

8. **IKE Phase-1の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「方向」
ここでは「双方向」を選択します。

「ローカル側識別子」
ここでは「IPアドレス」を選択します。

「リモート側識別子」
ここでは「IPアドレス」を選択します。

「認証アルゴリズム」
認証アルゴリズムを設定します。ここでは「認証アルゴリズム」には「SHA-1」を選択します。鍵方式には「Pre-shared Key（共通鍵方式）」を選択します。キー文字列には「0123456789」を入力します。

「暗号化アルゴリズム」
ここでは「3DES」を選択します。

「IKE交換モード」
ここでは「Main Mode」を選択します。

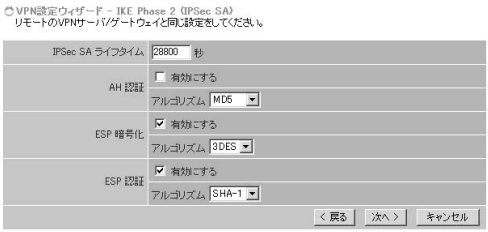
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「Diffie-Hellman（DH）Group」
ここでは「Group 2（1024bit）」を選択します。

「IKE PFS」
ここではIKE PFSを有効にします。「有効にする」をチェックして、「PFS Key Group」には「Group 2（1024bit）」を選択します。

「IPSec PFS（DH）Group」
ここではIPSec PFSを有効にします。Key Groupには「Group 2（1024bit）」を選択します。

9. **IKE Phase-2の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

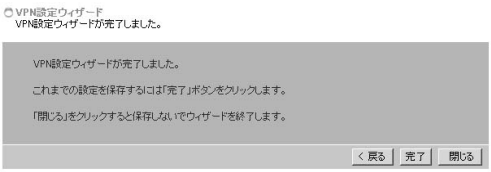
「AH認証」
AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」
ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「アルゴリズム」には「3DES」を選択します。

「ESP認証」

ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「アルゴリズム」には「SHA-1」を選択します。

10. **以上でルータBの設定は完了です。「完了」ボタンをクリックします。**



5 Windows2000/XPとの接続例

ここではWindows2000/XPとVPN接続するときの設定について説明します。
例として、次のようなVPNネットワークを構築します。

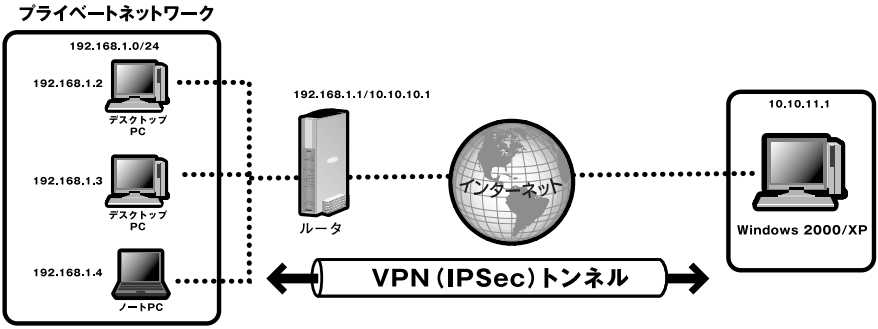


図6-4 ネットワーク例

項目	ルータ	Windows2000/XP
キータイプ	IKE	IKE
方向	双方向	双方向
IKE認証	SHA-1	SHA-1
鍵方式	Pre-shared Key	Pre-shared Key
キー	0123456789	0123456789
IKE交換モード	Main Mode	Main Mode
Diffie-Hellman group	Group1	Group1
IKE PFS	使用しない	使用しない
IPSec PFS	使用しない	使用しない
AH認証	なし	なし
ESP暗号化	DES	DES
ESP認証	MD5	MD5

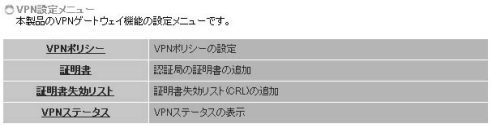
表6-4 VPNポリシー

●ルータの設定

VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。

1. 本製品のWEB設定画面にログインしてください。

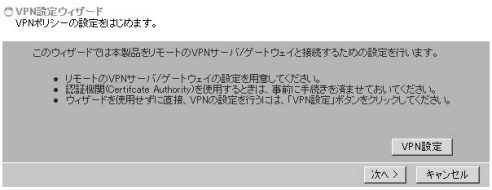
2. 設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。



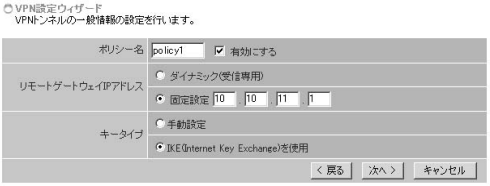
3. VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

4. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

5.「次へ ＞」ボタンをクリックしてください。



6. 次の項目を入力して「次へ ＞」ボタンをクリックします。

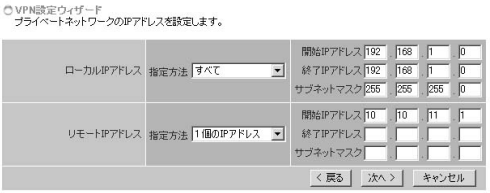


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、Windows2000/XP PCのIPアドレス「10.10.11.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「IKE（Internet Key Exchange）を使用」を選択します。

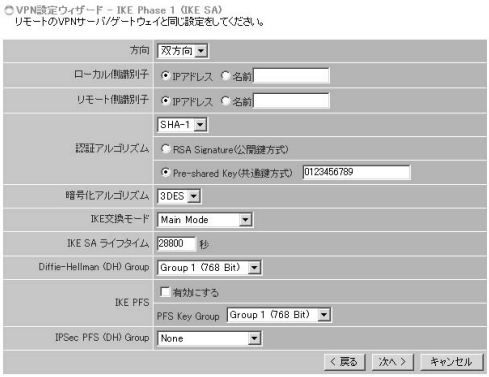
7. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、Windows2000/XP PCのIPアドレスを指定するので「1個のIPアドレス」を選択し、「開始IPアドレス」にWindows2000/XP PCのアドレス「10.10.11.1」を設定します。

8. **IKE Phase-1の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「方向」
ここでは「双方向」を選択します。

「ローカル側識別子」
ここでは「IPアドレス」を選択します。

「リモート側識別子」
ここでは「IPアドレス」を選択します。

「認証アルゴリズム」
認証アルゴリズムを設定します。ここでは「認証アルゴリズム」には「SHA-1」を選択します。鍵方式には「Pre-shared Key（共通鍵方式）」を選択します。キー文字列には「0123456789」を入力します。

「暗号化アルゴリズム」
ここでは「3DES」を選択します。

「IKE交換モード」
ここでは「Main Mode」を選択します。

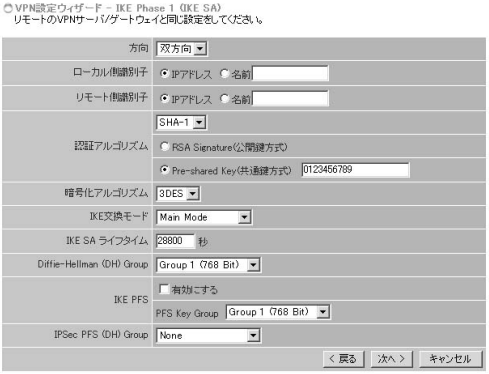
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「Diffie-Hellman（DH）Group」
ここでは「Group 1（768bit)」を選択します。

「IKE PFS」
ここではIKE PFSは使用しません。「有効にする」のチェックを外します。

「IPSec PFS（DH）Group」
ここではIPSec PFSは使用しません。「None」を選択します。

9. **IKE Phase-2の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「AH認証」

AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」

ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「アルゴリズム」には「DES」を選択します。

「ESP認証」

ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「アルゴリズム」には「MD5」を選択します。

10. **以上でルータの設定は完了です。「完了」ボタンをクリックします。**

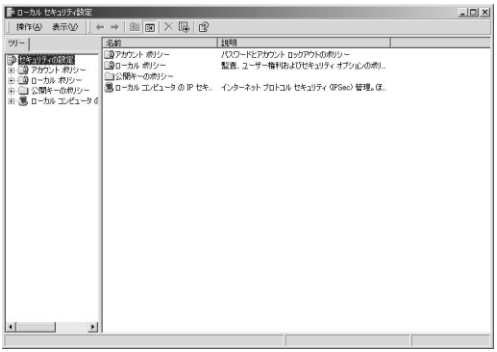
●Windows2000/XPの設定

Windows2000/XPのコンピュータは、あらかじめインターネットに問題なくアクセスできることを確認しておいてください。

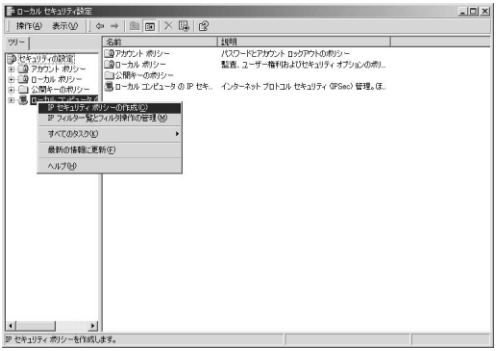
1. **「スタート」メニューの「設定」から「コントロールパネル」を選択します。**

2. **「コントロールパネル」から「管理ツール」を開きます。**

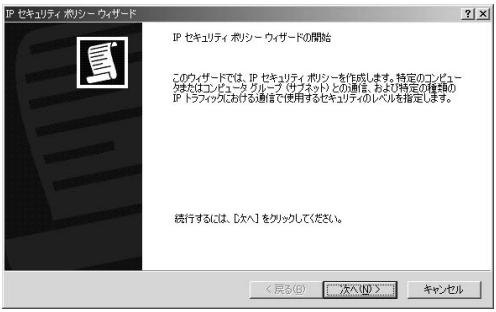
3. **「管理ツール」から「ローカルセキュリティポリシー」を起動します。**



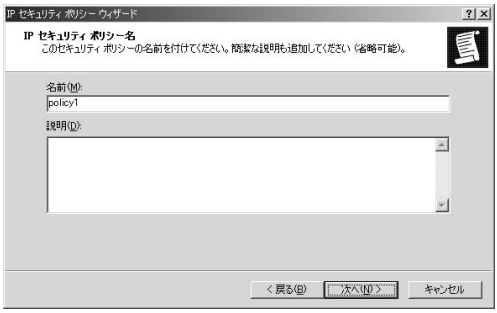
4. **「ローカルセキュリティ設定」画面の「ローカルコンピュータのIPセキュリティポリシー」を右クリックして表示されるメニューから「IPセキュリティポリシーの作成」を選択します。**



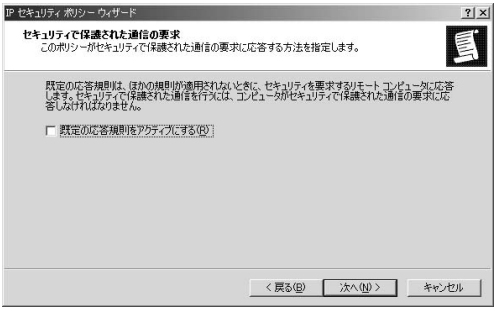
5.「次へ」をクリックします。



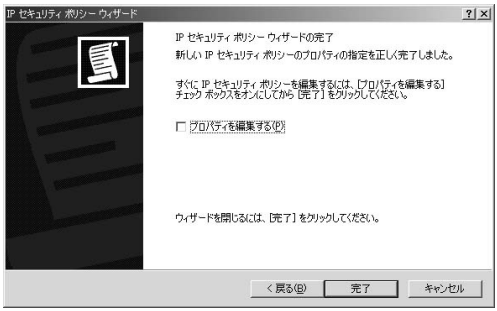
6.「名前」の欄に任意のポリシー名を入力して、「次へ」をクリックします。ここでは例として「policy1」と入力します。



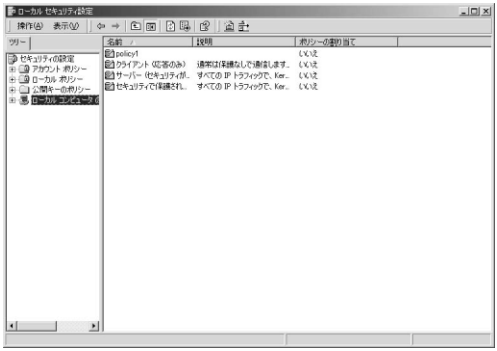
7.「規定の応答規則をアクティブにする」からチェックを外して、「次へ」をクリックします。



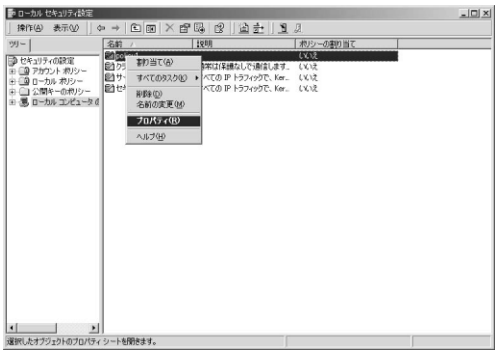
8.「プロパティを編集する」からチェックを外して、「完了」をクリックします。



9.「ローカルセキュリティ設定」画面で「ローカルコンピュータのIPセキュリティポリシー」クリックすると、作成したポリシーがリストに表示されます。



10. 作成したポリシーを右クリックして表示されるメニューから、「プロパティ」を選択します。



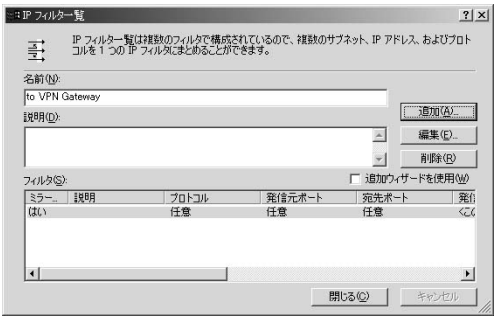
11. **ポリシーの設定画面が表示されます。ポリシーには送信用と受信用の2つのフィルタを追加する必要があります。最初に送信用のフィルタを作成します。「追加ウィザードを使用」のチェックを外してから「追加」をクリックします。**

9. **「追加」をクリックします。**

13. 「名前」の欄にフィルタの名前を入力します。ここでは、送信用のフィルタであることがわかるように、例として「to VPN Gateway」と入力します。「追加ウィザードを使用」からチェックを外してから「追加」をクリックします。

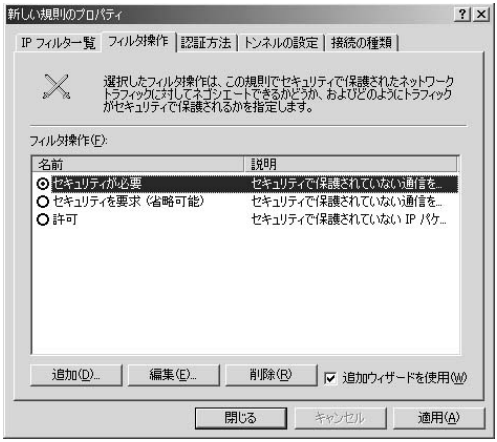
14. 「発信元アドレス」には「このコンピュータのIPアドレス」を選択します。「宛先アドレス」には、ルータ側のローカルネットワークのアドレスを入力します。ここでは「特定のIPサブネット」を選択し、「IPアドレス」には「192.168.1.0」、「サブネットマスク」には「255.255.255.0」を入力します。「ミラー化」の項目をチェックして「OK」をクリックします。

15.「IPフィルター一覧」画面に戻るので「閉じる」をクリックします。

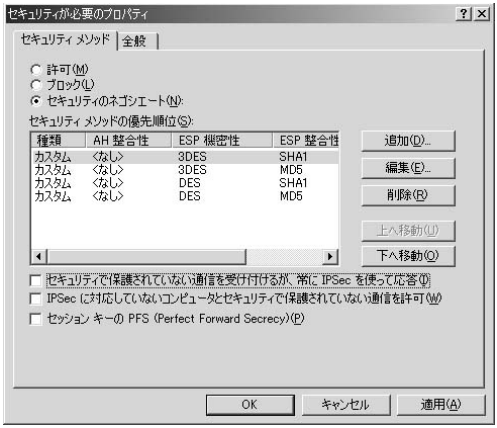


16.「新しい規則のプロパティ」画面に戻ります。追加したフィルタ「to VPN Gateway」を選択して「フィルタ操作」タブを選択します。

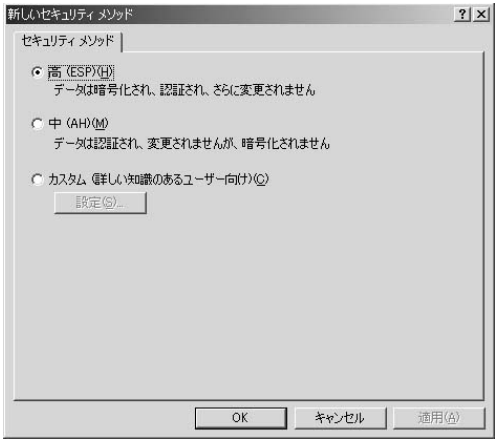
17.「セキュリティが必要」を選択して「編集」をクリックします。



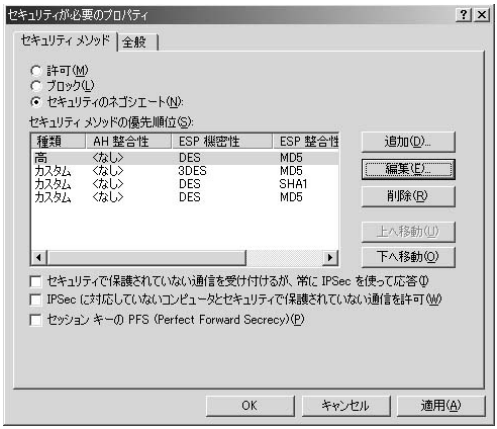
18.「セキュリティのネゴシエート」を選択し、「セキュリティで保護されていない通信を受け付けるが、常にIPsecを使って応答」からチェックを外します。登録されているセキュリティメソッドの中で一番上に表示されているメソッドを選択して「編集」をクリックします。



19.「セキュリティメソッド」で「高（ESP)」を選択して、「OK」をクリックします。



20.「セキュリティが必要のプロパティ」画面に戻るので「OK」をクリックします。

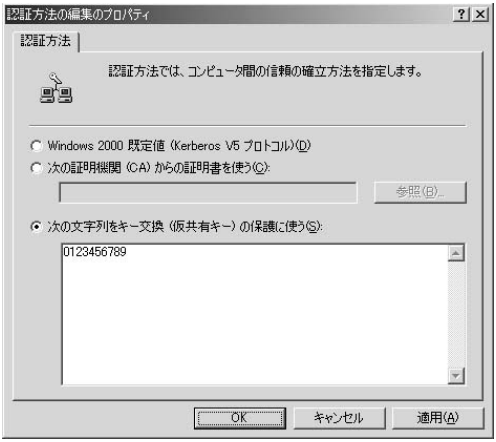


21.「新しい規則のプロパティ」画面に戻るので「トンネルの設定」タブを選択します。

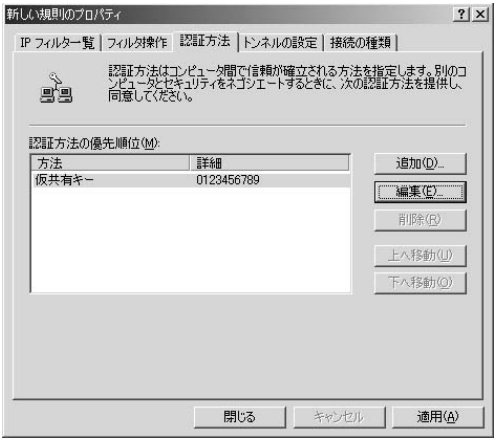
22.「次のIPアドレスでトンネルエンドポイントを指定する」を選択します。IPアドレスにはリモート側のWAN側IPアドレスを入力します。ここでは例としてルータのWAN側IPアドレス「10.10.10.1」を入力します。

23.「認証方法」タブを選択して、「編集」をクリックします。

24.「次の文字列をキー変換（仮共有キー）の保護に使う」を選択して、Pre-shared Keyを入力して「OK」をクリックします。ここでは例として「0123456789」を入力します。



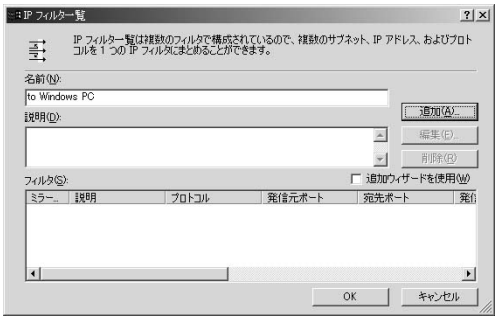
25.「閉じる」をクリックします。



26. 送信用のフィルタが追加されます。次に受信用のフィルタを追加します。「追加」をクリックします。

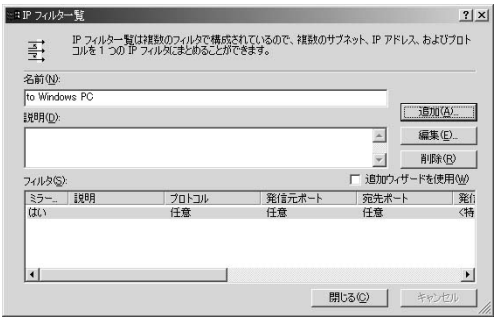
27.「追加」をクリックします。

28. 「名前」の欄にフィルタの名前を入力します。ここでは、受信用のフィルタであることがわかるように、例として「to Windows PC」と入力します。「追加ウィザードを使用」からチェックを外してから「追加」をクリックします。



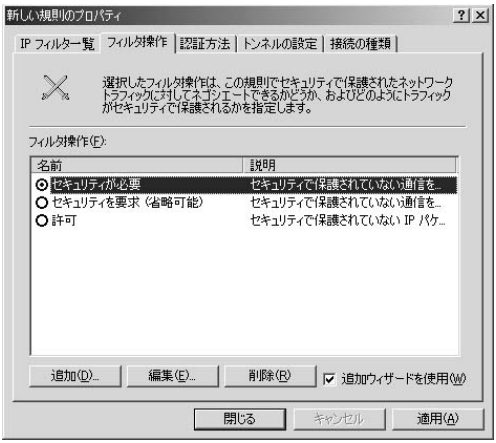
29. 「発信元アドレス」には、ルータ側のローカルネットワークのアドレスを入力します。ここでは「特定のIPサブネット」を選択し、「IPアドレス」には「192.168.1.0」、「サブネットマスク」には「255.255.255.0」を入力します。「発信元アドレス」には「このコンピュータのIPアドレス」を選択します。「ミラー化」の項目をチェックして「OK」をクリックします。

30.「IPフィルター一覧」画面に戻るので「閉じる」をクリックします。

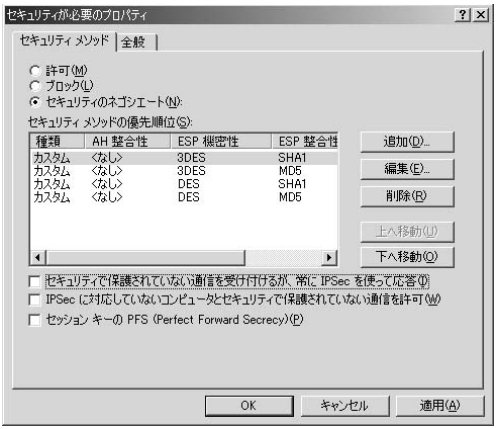


31.「新しい規則のプロパティ」画面に戻ります。追加したフィルタ「to Windows PC」を選択して「フィルタ操作」タブを選択します。

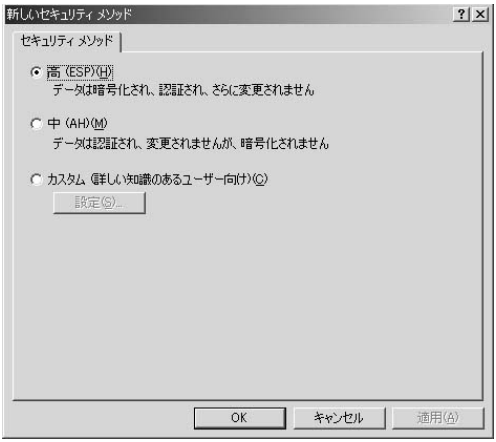
32.「セキュリティが必要」を選択して「編集」をクリックします。



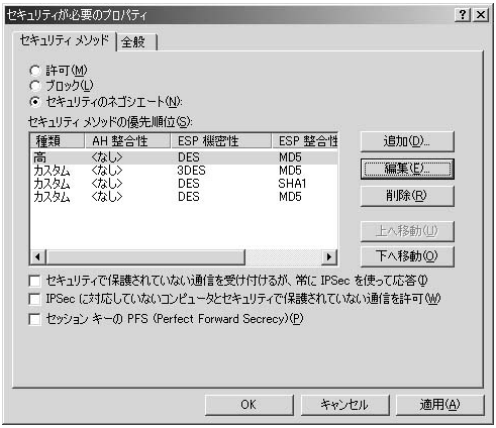
33.「セキュリティのネゴシエート」を選択して、「セキュリティで保護されていない通信を受け付けるが、常にIPsecを使って応答」からチェックを外します。登録されているセキュリティメソッドの中で一番上に表示されているメソッドを選択して「編集」をクリックします。



34.「セキュリティメソッド」で「高（ESP）」を選択して、「OK」をクリックします。



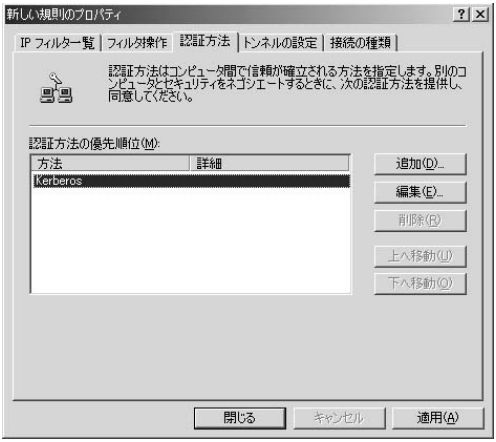
35.「セキュリティが必要のプロパティ」画面に戻るので「OK」をクリックします。



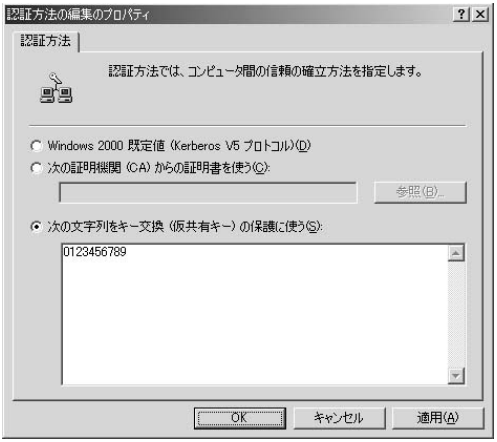
36.「新しい規則のプロパティ」画面に戻るので「トンネルの設定」タブを選択します。

37.「次のIPアドレスでトンネルエンドポイントを指定する」を選択します。IPアドレスにはこのコンピュータのIPアドレスを入力します。ここでは例として「10.10.11.1」を入力します。

38.「認証方法」タブを選択します。「編集」をクリックします。



39.「次の文字列をキー変換（仮共有キー）の保護に使う」を選択して、Pre-shared Keyを入力して「OK」をクリックします。ここでは例として「0123456789」を入力します。

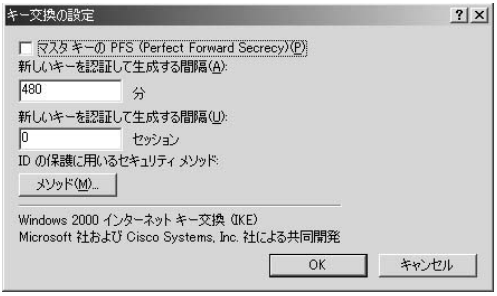


40.「閉じる」をクリックします。

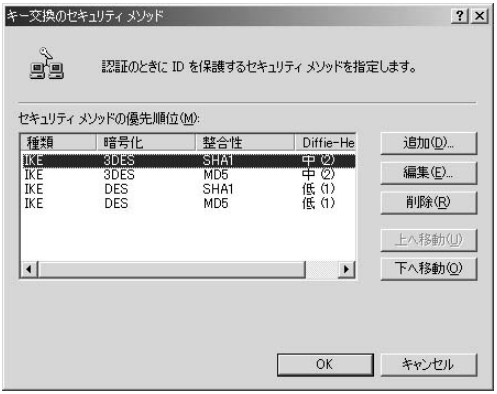
41. 受信用のフィルタが追加されます。「全般」タブを選択します。

42.「詳細」をクリックします。

43.「メソッド」をクリックします。



44. 登録されているセキュリティメソッドの中から一番上に登録されているメソッドを選択して、「編集」をクリックします。



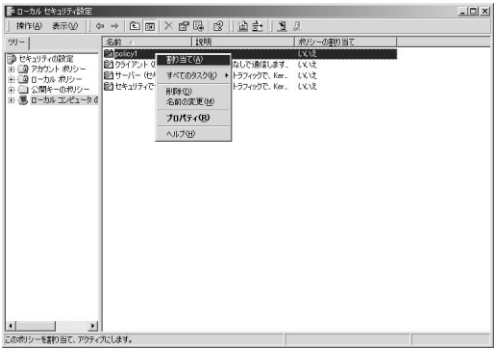
45.「整合性アルゴリズム」には「SHA1」、「暗号化アルゴリズム」には「3DES」、「Diffie-Hellman グループ」には「低（1）」を選択して、「OK」をクリックします。

46.「キー交換のセキュリティメソッド」の画面に戻るので「OK」をクリックします。

47.「キー交換の設定」の画面に戻るので「OK」をクリックします。

48.「policy1のプロパティ」の画面に戻るので「閉じる」をクリックします。

49. ポリシーの登録は終了です。「セキュリティの設定」画面に戻るので、登録されたポリシー（policy1）を右クリックして表示されるメニューから、「割り当て」を選択します。



50. 以上でWindows2000/XPの設定は完了です。

6 認証局（CA）を使用した設定例

ここではIKE（Internet Key Exchange）により自動設定し、さらに鍵方式としてRSA Signature（公開鍵方式）を使用するときの証明書の登録とルータの設定について説明します。
例として、次のようなVPNネットワークを構築します。

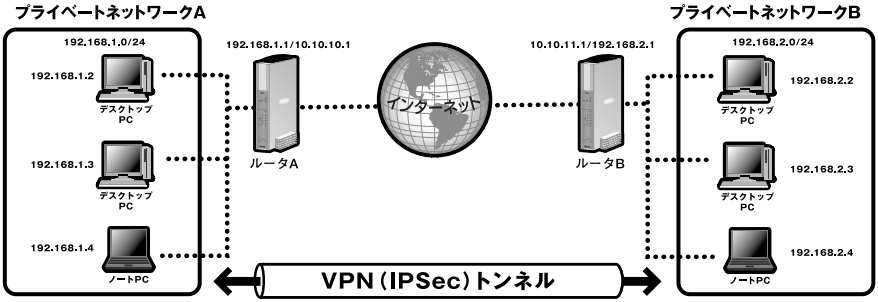


図6-5 ネットワーク例

項目	ルータA	ルータB
キータイプ	IKE	IKE
方向	双方向	双方向
IKE認証	SHA-1	SHA-1
鍵方式	RSA Signature	RSA Signature
キー	0123456789	0123456789
IKE交換モード	Main Mode	Main Mode
Diffie-Hellman group	Group2	Group2
IKE PFS	Group2	Group2
IPSec PFS	Group2	Group2
AH認証	なし	なし
ESP暗号化	3DES	3DES
ESP認証	SHA-1	SHA-1

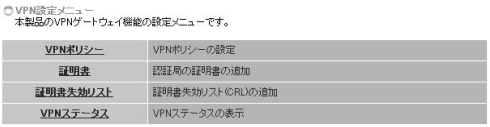
表6-5 VPNポリシー

●ルータAの設定

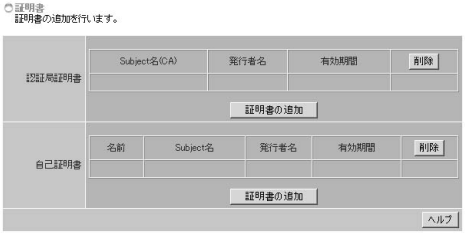
VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。また、認証許可からの証明書ファイルを用意しておいてください。

1. **本製品のWEB設定画面にログインしてください。**

2. **設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。**



3. **最初に認証局（CA）証明書を追加します。VPN設定メニューから「証明書」をクリックしてください。証明書設定画面が表示されます。**



4. **認証局証明書を追加します。認証局証明書はリモート側のルータの証明書の正当性を確認するときに使用します。認証局証明書欄の「証明書の追加」ボタンをクリックします。**

5. 認証局証明書の追加画面が表示されます。参照ボタンをクリックして、あらかじめ用意しておいた証明書ファイルを選択してください。「アップロード」ボタンをクリックすると証明書ファイルが読み込まれ認証局証明書が追加されます。

6. 次に自己証明書の追加をします。証明書設定画面の自己証明書欄の「証明書の追加」ボタンをクリックします。

7. 自己証明書の発行を要求するのに必要なデータを設定します。次の項目を入力して「次へ >」ボタンをクリックします。

「名前」

証明書の名前を入力します。任意の名前を入力してかまいません。ここでは「RouterA」と入力します。

「所持者（Subject）名」

証明書の所持者の名前になります。一般的に会社名や所属名などを入力します。ここでは「PLANEX」と入力します。

「ハッシュアルゴリズム」
ハッシュアルゴリズムを「MD5」、「SHA1」から選択します。ここでは「MD5」を選択します。

「署名アルゴリズム」
署名アルゴリズムを「DSS」、「RSA」から選択します。ここでは「RSA」を選択します。

「キーの長さ」
キーの長さを「512」、「1024」、「2048」から選択します。ここでは「1024」を選択します。

8. **前の手順で入力されたデータを元に公開鍵データが作成されます。表示された公開鍵データをコピーして認証局に証明書を要求します。認証局から証明書ファイルを受け取ったら「次へ ＞」ボタンをクリックします。**

注意

●認証局への証明書の要求手続きは使用する認証局により異なります。使用する認証局からの指示に従ってください。
●認証局への証明書の要求手続きは、必ず別のブラウザ画面を開いてから行ってください。

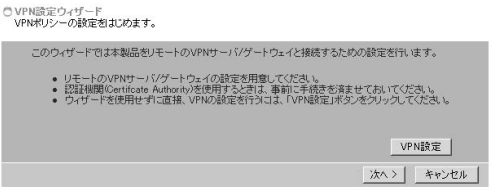
9. 認証局から受け取った自己証明書を追加します。参照ボタンをクリックして、自己証明書ファイルを選択してください。「アップロード」ボタンをクリックすると自己証明書ファイルが読み込まれます。

10. 自己証明書が追加されます。

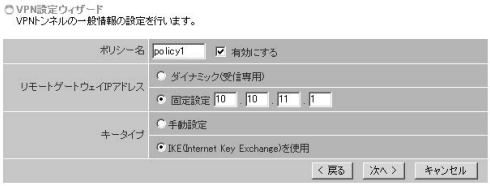
11. VPNポリシーの設定をします。VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

12. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

13.「次へ >」ボタンをクリックしてください。



14. 次の項目を入力して「次へ ＞」ボタンをクリックします。

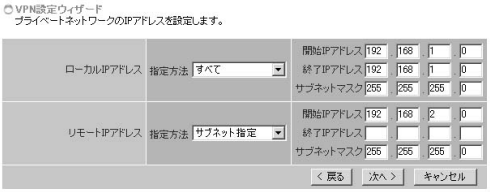


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータBのIPアドレス「10.10.11.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「IKE（Internet Key Exchange）を使用」を選択します。

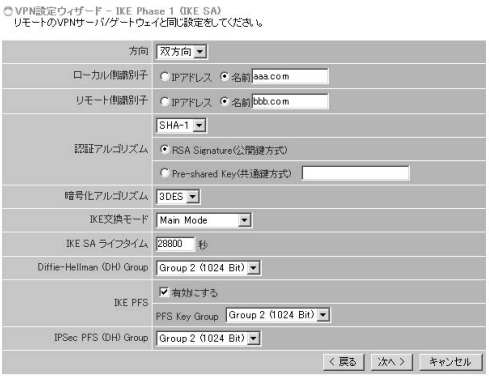
15. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークBのアドレス「192.168.2.0」と「サブネットマスク」に「255.255.255.0」を設定します。

16. IKE Phase-1の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。



「方向」
ここでは「双方向」を選択します。

「ローカル側識別子」
ここでは「名前」を選択し、このルータのホスト名を入力します。

「リモート側識別子」
ここでは「名前」を選択し、リモート側のルータのホスト名を入力します。

「認証アルゴリズム」
認証アルゴリズムを設定します。ここでは「認証アルゴリズム」には「SHA-1」を選択します。鍵方式には「RSA Signature（公開鍵方式）」を選択します。

「暗号化アルゴリズム」
ここでは「3DES」を選択します。

「IKE交換モード」
ここでは「Main Mode」を選択します。

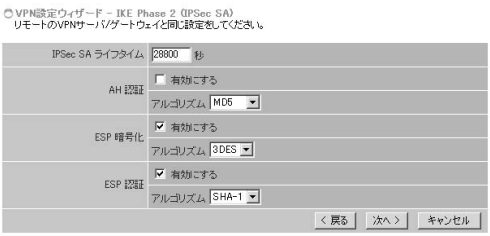
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「Diffie-Hellman（DH）Group」
ここでは「Group 2（1024bit)」を選択します。

「IKE PFS」
ここではIKE PFSを有効にします。「有効にする」をチェックして、「PFS Key Group」には「Group 2（1024bit)」を選択します。

「IPSec PFS（DH）Group」
ここではIPSec PFSを有効にします。Key Groupには「Group 2（1024bit)」を選択します。

17. **IKE Phase-2の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



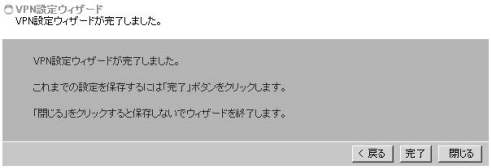
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「AH認証」
AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

「ESP暗号化」
ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「アルゴリズム」には「3DES」を選択します。

「ESP認証」
ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「アルゴリズム」には「SHA-1」を選択します。

18. 以上でルータAの設定は完了です。「完了」ボタンをクリックします。

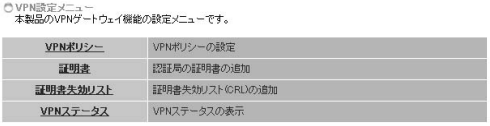


●ルータBの設定

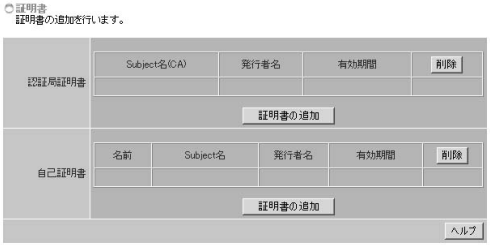
VPNゲートウェイの設定を始める前に、あらかじめインターネット接続のための設定をして、インターネットに問題なくアクセスできることを確認しておいてください。また、認証許可からの証明書ファイルを用意しておいてください。

1. 本製品のWEB設定画面にログインしてください。

2. 設定画面左側のメニューから「VPN設定」をクリックしてください。VPN設定メニューが表示されます。



3. 最初に認証局（CA）証明書を追加します。VPN設定メニューから「証明書」をクリックしてください。証明書設定画面が表示されます。



4. 認証局証明書を追加します。認証局証明書はリモート側のルータの証明書の正当性を確認するときに使用します。認証局証明書欄の「証明書の追加」ボタンをクリックします。

5. 認証局証明書の追加画面が表示されます。参照ボタンをクリックして、あらかじめ用意しておいた証明書ファイルを選択してください。「アップロード」ボタンをクリックすると証明書ファイルが読み込まれ認証局証明書が追加されます。

6. 次に自己証明書の追加をします。証明書設定画面の自己証明書欄の「証明書の追加」ボタンをクリックします。

7. 自己証明書の発行を要求するのに必要なデータを設定します。次の項目を入力して「次へ ＞」ボタンをクリックします。

「名前」
証明書の名前を入力します。任意の名前を入力してかまいません。ここでは「RouterB」と入力します。

「所持者（Subject）名」
証明書の所持者の名前になります。一般的に会社名や所属名などを入力します。ここでは「PLANEX」と入力します。

「ハッシュアルゴリズム」
ハッシュアルゴリズムを「MD5」、「SHA1」から選択します。ここでは「MD5」を選択します。

「署名アルゴリズム」
署名アルゴリズムを「DSS」、「RSA」から選択します。ここでは「RSA」を選択します。

「キーの長さ」
キーの長さを「512」、「1024」、「2048」から選択します。ここでは「1024」を選択します。

8. **前の手順で入力されたデータを元に公開鍵データが作成されます。表示された公開鍵データをコピーして認証局に証明書を要求します。認証局から証明書ファイルを受け取ったら「次へ ＞」ボタンをクリックします。**

注意

●認証局への証明書の要求手続きは使用する認証局により異なります。使用する認証局からの指示に従ってください。
●認証局への証明書の要求手続きは、必ず別のブラウザ画面を開いてから行ってください。

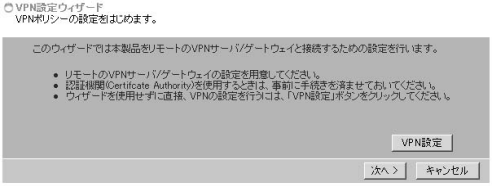
9. 認証局から受け取った自己証明書を追加します。参照ボタンをクリックして、自己証明書ファイルを選択してください。「アップロード」ボタンをクリックすると自己証明書ファイルが読み込まれます。

10. 自己証明書が追加されます。

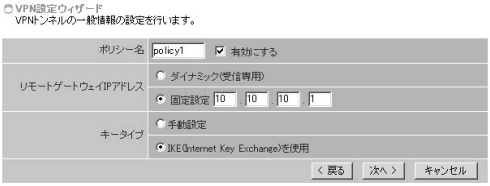
11. VPNポリシーの設定をします。VPN設定メニューから「VPNポリシー」をクリックしてください。VPNポリシー設定画面が表示されます。

12. VPNポリシー設定画面で「追加」ボタンをクリックしてください。VPNポリシー設定ウィザードが開始されます。

13.「次へ ＞」ボタンをクリックしてください。



14. 次の項目を入力して「次へ ＞」ボタンをクリックします。

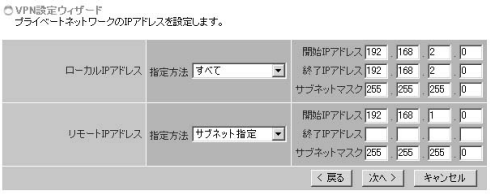


「ポリシー名」
このVPNポリシーの名前を設定します。ここでは「policy1」と入力し、「有効にする」をチェックします。

「リモートゲートウェイIPアドレス」
リモート側のVPNゲートウェイのIPアドレスを設定します。ここでは、「固定設定」を選択して、ルータAのIPアドレス「10.10.10.1」を入力します。

「キータイプ」
キー設定の種類を設定します。ここでは、「IKE（Internet Key Exchange）を使用」を選択します。

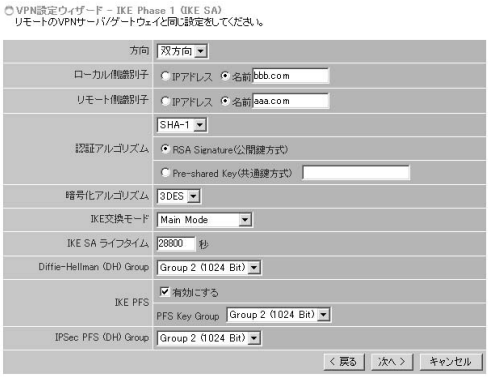
15. 次の項目を入力して「次へ ＞」ボタンをクリックします。



「ローカルIPアドレス」
このポリシーを適用する、ローカルネットワークのIPアドレスを設定します。ここでは、「すべて」を選択します。

「リモートIPアドレス」
このポリシーを適用する、リモート側ネットワークのIPアドレスを設定します。ここでは、「サブネット指定」を選択し、「開始IPアドレス」にプライベートネットワークAのアドレス「192.168.1.0」と「サブネットマスク」に「255.255.255.0」を設定します。

16. **IKE Phase-1の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「方向」
ここでは「双方向」を選択します。

「ローカル側識別子」
ここでは「名前」を選択し、このルータのホスト名を入力します。

「リモート側識別子」
ここでは「名前」を選択し、リモート側のルータのホスト名を入力します。

「認証アルゴリズム」
認証アルゴリズムを設定します。ここでは「認証アルゴリズム」には「SHA-1」を選択します。鍵方式には「RSA Signature（公開鍵方式)」を選択します。

「暗号化アルゴリズム」
ここでは「3DES」を選択します。

「IKE交換モード」
ここでは「Main Mode」を選択します。

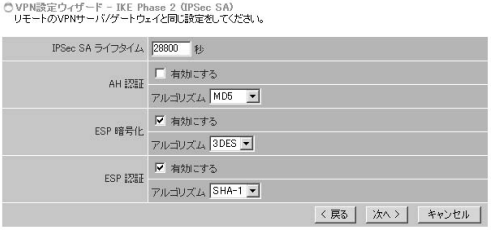
「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「Diffie-Hellman（DH）Group」
ここでは「Group 2（1024bit）」を選択します。

「IKE PFS」
ここではIKE PFSを有効にします。「有効にする」をチェックして、「PFS Key Group」には「Group 2（1024bit）」を選択します。

「IPSec PFS（DH）Group」
ここではIPSec PFSを有効にします。Key Groupには「Group 2（1024bit）」を選択します。

17. **IKE Phase-2の設定をします。次の項目を入力して「次へ ＞」ボタンをクリックします。**



「IKE SA ライフタイム」
ここでは「28800」（8時間）を入力します。

「AH認証」
AH認証を行うかどうかを設定します。ここではAH認証は使用しません。「有効にする」のチェックを外します。

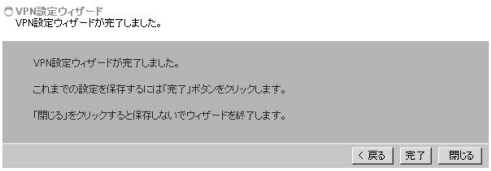
「ESP暗号化」

ESP暗号化を行うかどうかを設定します。ここではESP暗号化を行います。「有効にする」をチェックします。「アルゴリズム」には「3DES」を選択します。

「ESP認証」

ESP認証を行うかどうかを設定します。通常ESP暗号化を有効にするときはESP認証も有効にします。ここではESP認証を行います。「有効にする」をチェックします。「アルゴリズム」には「SHA-1」を選択します。

18. **以上でルータBの設定は完了です。「完了」ボタンをクリックします。**



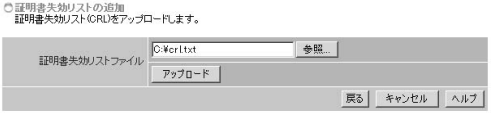
7 証明書失効リスト（CRL）の登録

認証局から発行される証明書失効リスト（CRL）の登録を行うには、設定画面左側のメニューの「VPN設定」をクリックして表示されるVPN設定メニューから「証明書失効リスト」をクリックします。

登録されている証明書失効リストが表示されます。

●証明書失効リストの追加

「CRLの追加」ボタンをクリックします。



「参照」ボタンをクリックして、認証局から発行された証明書失効リストファイルを選択して。「アップロード」ボタンをクリックします。証明書失効リストが追加されます。

●証明書失効リストの削除

登録されている証明書失効リストを削除するには、削除する証明書失効リストを選択して「削除」ボタンをクリックします。

8 VPNステータスの表示

VPNステータスの表示では、現在接続されているVPNセッションが表示されます。

「表示の更新」ボタンをクリックすると表示が更新されます。
「ログの表示」ボタンをクリックするとVPNログが表示されます。

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アダプタをお使いになっていますか？
●ACアダプタが本製品背面の電源コネクタにしっかりと接続されていますか？

■ WAN LEDが点灯しない

●ツイストペアケーブルの両端はそれぞれ、本製品背面のWAN側ポートおよびADSL/ケーブルモデムのRJ-45ポートにしっかりと接続されていますか？
●ADSL/ケーブルモデムの電源は入っていますか？
●LANケーブルの種類は間違っていませんか？
●ADSL/ケーブルモデムにMDI/MDI-Xの切り替えスイッチがある場合は切り替えてみてください。

■ LAN Link/Act LEDが点灯しない

●ツイストペアケーブルの両端はそれぞれ、本製品背面のLAN側ポートおよびハブまたはコンピュータの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？

■ DMZ Link/Actが点灯しない

●ツイストペアケーブルの両端はそれぞれ、本製品背面のDMZ側ポートおよびハブまたはコンピュータのRJ-45ポートにしっかりと接続されていますか？
●ハブまたはコンピュータの電源は入っていますか？
●LANケーブルの種類は間違っていませんか？
●本製品のDMZ側ポートはMDIタイプになっています。コンピュータを直接接続するときはクロスタイプのLANケーブルを使用してください。

■ 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かめてください。

●コンピュータのTCP/IPの設定に間違いがあることも考えられます。IPを自動取得（DHCPサーバでの設定）する設定にします。

●お使いになっている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。プロキシを使わない設定にします。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ことも考えられます。→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かめてください。コンピュータがIPアドレスを取得できてないときは、コンピュータを再起動します。（デフォルト設定時は192.168.1.xxx がIPアドレスに割り当てられます。）

■ インターネットにアクセスできない

●WAN側のIP設定に間違いがあることも考えられます。
→プロバイダから受け取っているIP設定の資料をよく確かめ、「第4章 インターネット接続設定」をやり直します。

●PPPoE接続の場合は、ユーザ名の設定で@（アットマーク）以降が正しく設定されているか、入力したパスワードに間違いがないか確認してください。

●DNSサーバの設定に間違いがあることも考えられます。
→DHCPサーバ機能を利用されているとき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かめ、「第4章 インターネット接続設定」をやり直します。
→DHCPサーバ機能を利用していないとき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かめ、コンピュータのDNSサーバ設定を確かめてください。

●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かめてください。

■ IPアドレス、または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ときは、「1-6 設定の初期化」を参照し、IPアドレス、またはパスワードを工場出荷時の状態に戻します。

■ 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。MACアドレスはLAN側ポートとWAN側ポートで異なりますので注意してください。プロバイダへMACアドレスの申請が必要なときはWAN側ポートのMACアドレスを申請してください。または、本製品のMACアドレス変更機能をお使いください。

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
	デフォルトゲートウェイ	192.168.1.1
DHCPサーバ	DHCPサーバー	有効
	DHCP　IP割当て範囲	192.168.1.2～100
	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
WAN側	IPアドレス	0.0.0.0
	サブネッットマスク	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
管理者ログイン許可ネットワーク		LAN側のみ
ドメイン名		未設定
ホスト名		サーバ名
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
ステートフルパケットインスペクション		無効
URLフィルタ		なし
UPnP機能		有効
VLAN		全ポート グループ1
VPNゲートウェイ		未設定

仕様

項目	説明
品名	VPN 4ポート ブロードバンド ルータ
型番	BLV-04D
準拠する標準	LAN側IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX WAN側IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX DMZ側IEEE802.3 10BASE-T、IEEE802.3u 100BASE-TX
伝送速度	LAN側10/100Mbps WAN側10/100Mbps DMZ側10/100Mbps
ポート	LAN側10BASE-T/100BASE-TX RJ-45×4ポート（Auto MDI/MDI-X） WAN側10BASE-T/100BASE-TX RJ-45×1ポート（MDI） DMZ側10BASE-T/100BASE-TX RJ-45×1ポート（MDI）
ネットワークケーブル	10BASE-T カテゴリ3以上ツイストペアケーブル（最大100m） 100BASE-TX カテゴリ5以上ツイストペアケーブル（最大100m）
LED	Power、Status、LAN Link/Act、LAN 100、WAN、 PPPoE、DMZ Link/Act、DMZ 100
VPNゲートウェイ	IPSec 最大トンネル数:70 IPSecプロトコル:MD5、SHA-1、DES、3DES、IKE
入力電源	DC12V、1200mA
消費電力	最大9.0W
外形寸法（W×D×H）	180 ×150 × 29.3mm
重量（本体のみ）	589g
環境	動作温度0～40℃、動作湿度35～85％
EMI	VCCI Class B、FCC Class B、CE

Memo

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/

弊社へのお問い合わせ

■弊社製品の追加購入

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

〈PCIダイレクト〉
http://direct.planex.co.jp/

■製品に関するお問い合わせ

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

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

■技術的なお問い合わせ・修理に関するお問い合わせ

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

〈お問い合わせフォーム〉
http://www.planex.co.jp/support/techform/
受付：24時間
〈電話〉
フリーダイヤル：0120-415977
受付：月～金曜日、10～12時、13～17時
＊祝祭日および弊社規定の休業日を除く
〈FAX〉
ファクス番号：03-5614-1018
受付：24時間

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

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

■その他

その他のお問い合わせ先は、弊社ホームページからお確かめください。

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

質問表

技術的なご質問は、この2ページを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	VPN 4ポート ブロードバンド ルータ
型番 Product No.	**BLV-04D**
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 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・修理依頼の手順（センドバック方式）

弊社では、センドバック（先に修理依頼品をお送りいただき、弊社より修理完了品をご返却する）方式による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、弊社サポートセンターまでご連絡ください。お送り先をご案内させていただきます。

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　　FAX・03-5614-1018
Web・http://www.planex.co.jp/support/repair/

2.ご案内に従って、修理依頼品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、リペアセンターへお送りいただく際の送料はお客様のご負担でお願いいたします。）

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。

保 証 書

●弊社の保証規定を必ずご覧下さい●

保証期間 Warranty	西暦　　年　　月　　日 より 1年間
製品名 Product name	VPN 4ポート ブロードバンド ルータ
型番 Product No.	**BLV-04D**
製造番号 Serial No.	

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	

※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.

プラネックスコミュニケーションズ株式会社

プラネックスコミュニケーションズ株式会社