



reference manual
リファレンスマニュアル

第二版



はじめに

本取扱説明書の目的

本製品をお買い上げいただき誠に有難うございます。本取扱説明書「BA5000 Pro リファレンスマニュアル」は、本製品を使ったインターネット接続設定の詳細をご説明する資料です。必要なときにいつでもご覧いただくために、本取扱説明書が入ったCD-ROMは大切に保管していただきますようお願いいたします。

内容の変更について

本取扱説明書は製品出荷時点の機能について説明しています。ご購入後、ファームウェアの更新などで設定項目の増加や内容の変更が起こる恐れがあります。あらかじめご了承ください。

最新版の取扱説明書は、インターネット経由でダウンロードすることも可能です。

BAシリーズ製品情報ホームページ

<http://www.ntt-me.co.jp/bar/>

商標について

- ・ MS、Microsoft、Windowsは、米国Microsoft Corporationの登録商標です。
 - ・ Macintoshは、アップルコンピュータ社の登録商標です。
 - ・ Ethernetは、富士ゼロックス社の登録商標です。
 - ・ BA5000 Proは、株式会社エヌ・ティ・ティ エムイーの商標です。
- その他の商品名、会社名は、各社の商標または登録商標です。

その他

- ・ 本取扱説明書をご覧いただく前に、「BA5000 Proマニュアル 接続編」をよく読んでおいてください。
- ・ 製品に関する免責事項、取扱注意事項、表記・略称、記号は、紙媒体の「BA5000 Proマニュアル 接続編」に準じます。

目次

はじめに 1

1. PPPoE接続	3
1.1 PPPoE接続とは	4
1.2 PPPoE接続の種類	5
1.3 一般的なPPPoE接続設定	7
1.4 unnumbered PPPoE接続 (DMZネットワーク設定)	12
1.5 PPPoEマルチセッション接続設定	18
1.6 PPPoE接続の状況確認	25
2. 通常接続	27
2.1 通常接続設定の種類	28
2.2 固定IPアドレス通常接続設定	30
2.3 複数固定IPアドレス通常接続設定	32
2.4 通常接続の状況確認	35
3. NAT	37
3.1 NAT機能	38
3.2 サーバ公開/ゲームの利用 (マルチNAT)	41
3.3 サーバ公開/ゲームの利用 (ローカルサーバ)	44
3.4 Universal Plug and Play	48
3.5 H.323NAT	55
3.6 VPNパススルー	56
4. スタティックルーティングとダイナミックルーティング	58
4.1 スタティックルーティング	59
4.2 ダイナミックルーティング	61
5. セキュリティ	62
5.1 ファイアウォール機能	63
5.2 静的フィルタ	64
5.3 ステートフルパケットインスペクション	68
5.4 攻撃検知	69
6. 管理	73
6.1 設定画面へのログイン制限	74
6.2 時刻制限	76
7. 状態の確認	78
7.1 ログ機能	79
7.2 モニタ機能	81
8. その他	82
8.1 MACアドレスの変更	83
8.2 WWWサービス制限	84
8.3 Pingによる導通確認	86
9. ファームウェアと設定情報	87
9.1 ファームウェアの更新	88
9.2 設定情報の保存と読み込み	89
9.3 設定情報の消去 (設定画面経由)	90
9.4 設定情報の消去 (外部から)	91
10. その他	93
10.1 IP設定とMACアドレスの確認	94
10.2 メール送受信に時間がかかる場合	97
10.3 NetBIOSフィルタ	98
10.4 トラブルシューティング	99

第1章



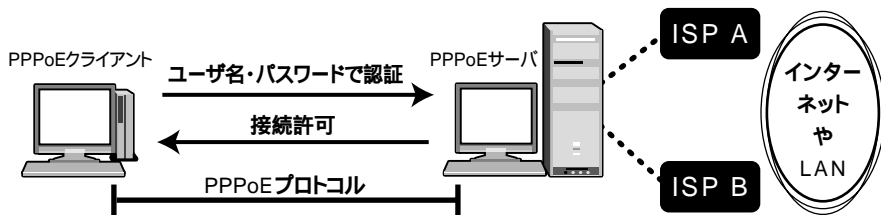
PPPoE接続

「フレッツ・ADSL」や「Bフレッツ」で使用されているPPPoEと、それに関連する本製品の設定を説明します。

1. PPPoEとは



PPPoEとは、ダイヤルアップ接続(PPP接続)のように、利用者のユーザ名、パスワードを使った接続をEthernet上で行う仕組みです。



利点

- ・利用者を認証することで、利用者の限定、課金、サービスの差別化、セキュリティなどを実現する。
- ・複数のPPPoE接続先プロバイダが同一ネットワークに存在する場合、利用者はユーザ名とパスワードを使ってプロバイダを切り替えることができる。
- ・ADSLモデムのインストールが簡単である。
- ・同時に複数のPPPoEセッションを利用することも可能。

PPPoE接続に必要なもの

- ・1台のパソコンだけでブロードバンド接続する場合
「フレッツ接続ツール」などのPPPoEクライアントソフトウェア、Windows XPなどのOS標準のPPPoEクライアント機能、またはPPPoEクライアント機能対応ブロードバンドルータ
- ・複数のパソコンでブロードバンド接続する場合
PPPoEクライアント機能対応ブロードバンドルータ。



注意

ブロードバンドルータを使ったPPPoEブロードバンド接続を行う場合、「フレッツ接続ツール」などのPPPoEクライアントソフトウェアは、削除しておいてください。

2.PPPoE接続の種類



現在のブロードバンド環境で利用されているPPPoE接続は、いくつかに分類することができます。

利用可能なIPアドレス(PPPoE 1セッションあたり)

・一般的なPPPoE接続

ユーザ名とパスワードの認証後、1個のIPアドレスがプロバイダから割り当てられるサービス。多くの個人向けのPPPoEブロードバンドサービスはこのタイプです。

・ unnumbered接続 (LAN型接続)

ユーザ名とパスワードの認証後、複数のIPアドレスがプロバイダから割り当てられるサービス。一部の法人向けのPPPoEブロードバンドサービスがこのタイプを採用しています。本取扱説明書では、1個のPPPoEアカウントで、複数の連続したIPアドレス(1サブネット)を提供し、上位ネットワークとunnumbered接続するサービスを、「unnumbered接続サービス」としております。その他のサービスでは機能しない場合がありますのでご注意ください。

- unnumbered接続サービス例-

OCN ADSLアクセス IP8/IP16 「フレッツ」プラン

OCN 光アクセス IP8/IP16 「Bフレッツ」プラン

IJ DSL/Fサービス (1/16C, 1/32C, 1/64C)

IJ FiberAccess/Fサービス (1/16C, 1/32C, 1/64C)

InfoSphere Biz ADSL8、 Biz ADSL16

InfoSphere Biz Hikari8、 Biz Hikari16

NTT-ME エンタープライズADSL8/16

NTT-ME エンタープライズBF8

同時セッション数(1ブロードバンド回線あたり)

・シングルセッション

1つのブロードバンド回線で、1セッションしか同時に利用できないサービス。多くの個人向けPPPoEサービスはこのタイプです。

・マルチセッション

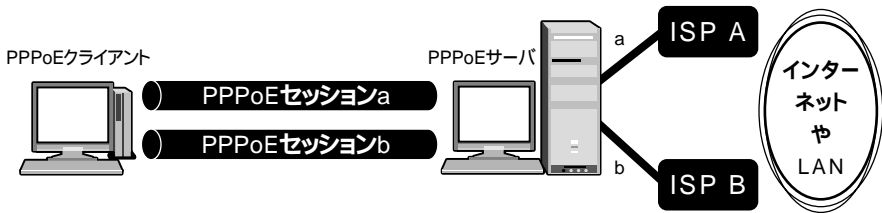
1つのブロードバンド回線で、同時に2セッション以上のPPPoEが利用できるサービス。「Bフレッツ」はこのタイプです。

マルチセッションをサポートするブロードバンドサービスの利用方法は、以下の2つがあります。

複数のPPPoEクライアント機器(パソコンやルータ)を使って、それぞれ異なるプロバイダに接続する。

PPPoEマルチセッションに対応した1台のルータを使って、それぞれのセッションを同時に使い分ける。

本製品は、PPPoEマルチセッション(最高2セッション)に対応しています。



接続設定ページ

一般的なPPPoE接続

「1-3. 一般的なPPPoE接続設定」のページへ

unnumbered接続

「1-4. unnumbered PPPoE接続(DMZネットワーク設定)」のページへ

マルチセッション

「1-5. マルチセッション設定」のページへ

3.一般的なPPPoE接続設定



ユーザ名とパスワードの認証後、1個のIPアドレスがプロバイダから割り当てられるサービスをご利用の場合の設定方法を説明します。

[接続設定] - [新規登録] ページ

PPPoE接続アカウントを新規登録します。

新規登録**接続方法**

「PPPoE接続」を選択し、「次へ」ボタンを押します。

[PPPoE接続設定] ページが表示されます。

[PPPoE接続設定] ページ

PPPoE接続アカウントを登録します。

PPPoE接続設定**アカウント名 [任意]**

この接続設定に、任意の名前を付けることができます。プロバイダ名などを入力して下さい。

設定可能な文字：半角英数字、最高32文字まで

PPPoEユーザ名

プロバイダから指定されたPPPoE接続ユーザ名を正確に入力してください。「フレッツ・ADSL」や「Bフレッツ」の場合は、“@”（アットマーク）以下も入力します。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード

プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード再入力

入力間違い防止のためもう一度、プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

PPPoEサービス名

プロバイダからPPPoE接続サービス名を指定された場合のみ、正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPP認証方式

PPP認証方式を設定します。通常は「接続相手にあわせる」を選択してください。

WAN側IPアドレス設定方法

自動取得： PPP認証中に、プロバイダからIPアドレスを自動的に取得する場合。プロバイダから特にIPアドレスを指定されていない場合もこれを選択してください。

固定設定： IPアドレスが固定で指定されている場合。

固定WAN側IPアドレス

[WAN側IPアドレス設定方法] で「固定設定」を選択した場合に、プロバイダから指定されたIPアドレスを入力してください。

DNSサーバアドレス設定方法

自動取得： [WAN側IPアドレス設定方法] で「自動取得」を選択した際に、DNSサーバのIPアドレスも同時に自動取得する場合。

固定設定： DNSサーバのIPアドレスを固定設定する場合や、[WAN側IPアドレス設定方法] で「固定設定」を選択した場合。

プライマリDNSサーバアドレス

[DNSサーバアドレス設定方法] で「固定設定」を選択した場合に、プロバイダから指定された1個目のDNSサーバのIPアドレスを入力します。

セカンダリDNSサーバアドレス

[DNSサーバアドレス設定方法] で「固定設定」を選択した場合に、プロバイダから指定された2個目のDNSサーバのIPアドレスを入力します。

MSSサイズ

MSS(Maximum Segment Size) 値を調整します。通常、MSS値はMTU値から40を引いた値になります。MSS値は特に必要がない限り絶対に変更しないで下さい。

工場出荷時値： 1412byte

WAN側ポートRIP機能

WAN側ポートのRIP機能を設定します。通常のインターネット接続ではRIPを使用しませんので「無効」を選択してください。

無効： RIP機能を利用しない場合。

受信のみ： 外部からのRIP受信のみ行う場合。

送信のみ： 外部へのRIP送信のみ行う場合。

送受信： RIP送受信を行う場合。



注意

- ・ PPPoEユーザ名、PPPoEパスワード、PPPoEサービス名では、大文字・小文字は別の文字として扱われます。
- ・ PPPoEサービス名は、一般的なインターネット接続サービス名称とは異なります。「フレッツ・ADSL」では入力しないで下さい。

DMZネットワーク設定
ここは設定しないで下さい。

[設定]ボタンをクリックしてください

変更した設定内容が保存され、再起動完了後に[アカウント管理]ページが表示されます。

[接続設定]-[アカウント管理]ページ

新規登録したPPPoEアカウントは、そのままでは使えないため、アカウント管理ページで有効にする必要があります。

接続アカウント管理

接続方式の選択

「PPPoE接続」を選択します。

通常接続アカウントリスト

ここは操作しないで下さい。

PPPoE接続アカウントリスト

PPPoE接続アカウントでの接続状態表示や操作を行います。[アカウント名]欄で、先ほど登録したPPPoEアカウントを探し、以下の設定を行ってください。

状態

現在の接続状態が表示されます。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

自動取得した、あるいは固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

セッション

本製品は、最大4個のPPPoEアカウントを記憶することができます。先ほど登録したPPPoEアカウントで「プライマリ1」または「プライマリ2」を選択してください。

プライマリ1	常に1つのPPPoEアカウントをプライマリ1に設定してください。このPPPoEアカウントが主に使用するPPPoE接続になります。
プライマリ2	プライマリ1のバックアップ用アカウントです。プライマリ1に設定したアカウントでの接続に失敗すると、本製品はプライマリ2に設定したアカウントでPPPoE接続を試みます。さらに続けてプライマリ2でも接続失敗した場合はプライマリ1での接続と、どちらかのアカウントで接続が成功するまで繰り返します。(参照:キープ・アライブ)
セカンダリ1、セカンダリ2	2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。絶対に選択しないで下さい。
無効	単に設定情報を記憶しておくだけです。実際のPPPoE接続には利用しません。

アイドルタイム

ここに指定した時間、インターネットとの通信がない場合、自動的にPPPoE接続を切断します。自動切断を行いたくない場合は“0”を入力してください。ただし、以下の[キープ・アライブ]を「有効」に設定すると、自動切断機能は無効になります。

工場出荷時値：20分 設定可能範囲：0～999分

キープ・アライブ

セッション・キープアライブ機能です。これが有効にされたPPPoE接続アカウントへの接続が開始されると、その後は常にそのアカウントへの接続を維持しようとします。

不安定なxDSL回線などで、意図しない切断が発生しても、切断されたことを検知し、再接続します。

キープアライブ機能の状態	動作
プライマリ1 = 無効 プライマリ2 = (登録なし)	以下の[プライマリセッション接続トリガ]に基づいた接続開始を行います。
プライマリ1 = 有効 プライマリ2 = 有効または無効	電源投入直後からプライマリ1への接続を開始します。接続失敗した場合や、意図しない切断の場合も、常にプライマリ1への再接続を成功するまで行います。プライマリ2への接続は行われません。

操作

手動によるPPPoE接続または切断を行います。ただし、「プライマリ1」と「プライマリ2」に同時接続することはできません。

修削

選択したアカウントの修正または削除を行います。

プライマリセッション接続トリガ

自動接続： LAN側ネットワークからインターネットへの通信要求が検出されると「プライマリ1」への接続動作を開始します。

手動接続： 本設定画面上で[接続]ボタンを押さない限り接続しません。

セカンダリセッション接続トリガ

2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。ここを設定する必要はありません。

PPP-Echo-Request送出間隔/リトライ回数

「キープ・アライブ」機能では、PPPoEサーバに対してPPP-Echo-Requestを送出し、それに対する応答パケット(PPP-Echo-Reply)を確認することで、PPPoEセッションを監視します。

ここでは、PPP-Echo-Requestの間隔と、“連続何回”PPPoEサーバから応答がない場合に「切断」と判断し、再接続動作を開始するかを設定します。

PPP-Echo-Request送出間隔： 工場出荷時値：60秒、設定可能範囲：10～300秒

PPP-Echo-Requestリトライ回数： 工場出荷時値：6回、設定可能範囲：1～99回

One Point!

不安定なADSL回線をご利用の場合、極端に短い送出間隔や少ないリトライ回数を設定すると、頻繁にPPPoEセッションの切断と再接続が繰り返されてしまいます。必要がない限りこの値は変更しないで下さい。

セカンダリセッション接続ルール

2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。ここを設定する必要はありません。

[設定]ボタンをクリックしてください

変更した設定内容が保存されます。再起動完了後設定したPPPoEアカウントへの接続が使用可能になります。

4.unnumbered PPPoE接続(DMZネットワーク設定)

Trying

ユーザ名とパスワードの認証後、複数のIPアドレスがプロバイダから割り当てられる、unnumbered PPPoE接続サービスをご利用の場合の設定方法を説明します。

確認事項

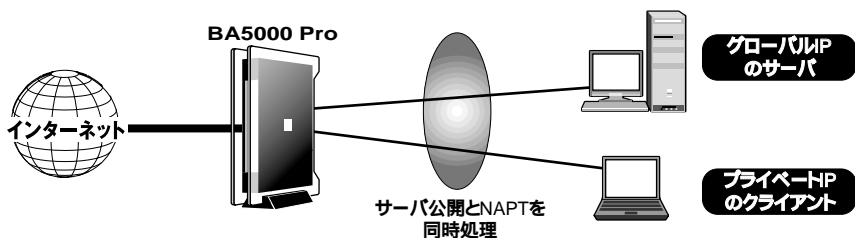
IPアドレスの割り当て方法

割り当てられる連続したグローバルIPアドレスのうち、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、一般的にホストに使用しません。また、本製品に対するグローバルIPアドレスの割り当てでも必要になります。

本製品に割り当てられるグローバルIPアドレスは、プロバイダの指示に従ってください。

DMZネットワーク機能

本製品のDMZネットワーク機能を利用すると、グローバルIPアドレスホスト(パソコン)を本製品のLAN側に設置することができます。通常のNAPTルータとしても動作しますので、プライベートIPアドレスを持つパソコンも同時にインターネット接続可能です(NAT&スルー)。



注意

- ・ LAN側ポートにグローバルIPアドレスホストを直接置くことができるDMZネットワーク機能は、1対1のNAT変換を行うマルチNAT機能とは異なります。ご注意ください。
- ・ DMZネットワーク機能を利用して本製品のLAN側に接続されたグローバルIPアドレスホストは、インターネットから直接参照可能な状態になります。

DMZネットワークを利用する際のパソコンの設定

・グローバルIPホスト

IPアドレス : 割り当てられたグローバルIPのうち、ネットワークアドレス、ブロードキャストアドレス、本製品WAN側IPアドレス以外のアドレス

サブネットマスク : グローバルIP8個の場合は「255.255.255.248」、16個の場合は「255.255.255.240」。

デフォルトゲートウェイ : 本製品WAN側IPアドレス

・プライベートIPホスト

変更の必要はありません。

[接続設定] - [新規登録] ページ

unnumbered PPPoE接続アカウントを新規登録します。

新規登録

接続方法

「PPPoE接続」を選択し、「次へ」ボタンを押します。

[PPPoE接続設定]ページが表示されます。

[PPPoE接続設定] ページ

PPPoE接続アカウントを登録します。

PPPoE接続設定

アカウント名 [任意]

この接続設定に、任意の名前を付けることができます。プロバイダ名などを入力して下さい。

設定可能な文字：半角英数字、最高32文字まで

PPPoEユーザ名

プロバイダから指定されたPPPoE接続ユーザ名を正確に入力してください。「フレッツ・ADSL」や「Bフレッツ」の場合は、“@”(アットマーク)以下も入力します。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード

プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード再入力

入力間違い防止のためもう一度、プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

PPPoEサービス名

プロバイダからPPPoE接続サービス名を指定された場合のみ、正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPP認証方式

PPP認証方式を設定します。通常は「接続相手にあわせる」を選択してください。

WAN側IPアドレス設定方法

固定設定： IPアドレスが固定で指定されている場合。通常、unnumbered PPPoE接続では固定IPアドレスを使用しますのでこれを選択してください。

自動取得： PPP認証中に、プロバイダからIPアドレスを自動的に取得する場合。

固定WAN側IPアドレス

[WAN側IPアドレス設定方法]で「固定設定」を選択した場合に、プロバイダの指示に従い、本製品WAN側ポートに設定するグローバルIPアドレスを入力してください。特に指示がない場合は、割り当てグローバルIPアドレス範囲の2番目のアドレスを入力してください。

DNSサーバアドレス設定方法

固定設定： DNSサーバのIPアドレスを固定設定する場合や、[WAN側IPアドレス設定方法]で「固定設定」を選択した場合。

自動取得： [WAN側IPアドレス設定方法]で「自動取得」を選択した際に、DNSサーバのIPアドレスも同時に自動取得する場合。

プライマリDNSサーバアドレス

[DNSサーバアドレス設定方法]で「固定設定」を選択した場合に、プロバイダから指定された、または自分で運営している1個目のDNSサーバのIPアドレスを入力します。

セカンダリDNSサーバアドレス

[DNSサーバアドレス設定方法]で「固定設定」を選択した場合に、プロバイダから指定された、または自分で運営している2個目のDNSサーバのIPアドレスを入力します。

MSSサイズ

MSS (Maximum Segment Size) 値を調整します。通常、MSS値はMTU値から40を引いた値になります。

MSS値は特に必要がない限り絶対に変更しないで下さい。

工場出荷時値：1412byte

WAN側ポートRIP機能

WAN側ポートのRIP機能を設定します。通常のインターネット接続ではRIPを使用しませんので「無効」を選択してください。

無効： RIP機能を利用しない場合。

受信のみ： 外部からのRIP受信のみ行う場合。

送信のみ： 外部へのRIP送信のみ行う場合。

送受信： RIP送受信を行う場合。



注意

- ・ PPPoEユーザ名、PPPoEパスワード、PPPoEサービス名は、大文字・小文字は別の文字として扱われます。
- ・ PPPoEサービス名は、一般的なインターネット接続サービス名称とは異なります。「フレッツ・ADSL」では入力しないで下さい。

DMZネットワーク設定

ここでは、利用可能なグローバルIPアドレスのうち、何番から何番までのグローバルIPアドレス範囲をLAN側に設置するかを設定・表示します。最高4個のグローバルIPアドレス範囲を設定可能です。

最初のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最初のグローバルIPアドレスを表示します。

最後のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最後のグローバルIPアドレスを表示します。



- ・DMZネットワークに設定するグローバルIPアドレスは、本製品WAN側ポートのアドレスと重複しないようにしてください。
- ・DMZネットワーク設定は、グローバルIPアドレスのホストのLAN側への設置を可能にする機能です。複数のグローバルIPアドレスは使用するが、LAN側にグローバルIPアドレスホストを置きたくない場合は、[マルチNAT設定]を行ってください。マルチNAT機能を利用すると、グローバルIPアドレスとプライベートIPアドレスの1対1の変換を行います。

[設定]ボタンをクリックしてください

変更した設定内容が保存され、再起動完了後に[アカウント管理]ページが表示されます。

[接続設定] - [アカウント管理] ページ

新規登録したunnumbered PPPoEアカウントは、そのままでは使えないため、アカウント管理ページで有効にする必要があります。

接続アカウント管理

接続方式の選択

「PPPoE接続」を選択します。

通常接続アカウントリスト

ここは操作しないで下さい。

PPPoE接続アカウントリスト

PPPoE接続アカウントでの接続状態表示や操作を行います。[アカウント名]欄で、先ほど登録したunnumbered PPPoEアカウントを探し、以下の設定を行ってください。

状態

現在の接続状態が表示されます。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

自動取得した、あるいは固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

セッション

本製品は、最大4個のPPPoEアカウントを保持することができます。先ほど登録したunnumbered PPPoEアカウントで、「プライマリ1」を選択してください。

プライマリ1	常に1つのPPPoEアカウントをプライマリ1に設定してください。このPPPoEアカウントが主に使用するPPPoE接続になります。
プライマリ2	プライマリ1のバックアップ用アカウントです。プライマリ1に設定したアカウントでの接続に失敗すると、本製品はプライマリ2に設定したアカウントでPPPoE接続を試みます。さらに続けてプライマリ2でも接続失敗した場合はプライマリ1での接続と、どちらかのアカウントで接続が成功するまで繰り返します。(参照:キープ・アライブ)
セカンダリ1	2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。
セカンダリ2	セカンダリ1のバックアップ用アカウントです。セカンダリ1に設定したアカウントでの接続に失敗すると、本製品はセカンダリ2に設定したアカウントでPPPoE接続を試みます。さらに続けてセカンダリ2でも接続失敗した場合はセカンダリ1での接続と、どちらかのアカウントで接続が成功するまで繰り返します。(参照:キープ・アライブ)
無効	単に設定情報を記憶しておくだけです。実際のPPPoE接続には利用しません。

アイドルタイム

ここに指定した時間、インターネットとの通信がない場合、自動的にPPPoE接続を切断します。自動切断を行いたくない場合は「0」を入力してください。ただし、以下の[キープ・アライブ]を「有効」に設定すると、自動切断機能は無効になります。

工場出荷時値:20分 設定可能範囲:0-999分

キープ・アライブ

セッション・キープアライブ機能です。これが有効にされたPPPoE接続アカウントへの接続が開始されると、その後は常にそのアカウントへの接続を維持しようとします。

不安定なxDSL回線などで、意図しない切断が発生しても、切断されたことを検知し、再接続します。

キープアライブ機能の状態	動作
プライマリ1 = 無効 プライマリ2 = (登録なし)	以下の[プライマリセッション接続トリガ]に基づいた接続開始を行います。
プライマリ1 = 有効 プライマリ2 = 有効または無効	電源投入直後からプライマリ1への接続を開始します。接続失敗した場合や、意図しない切断の場合も、常にプライマリ1への再接続を成功するまで行います。プライマリ2への接続は行われません。

操作

手動によるPPPoE接続または切断を行います。ただし、「プライマリ 1」と「プライマリ 2」、または「セカンダリ 1」と「セカンダリ 2」に同時接続することはできません。

修/削

選択したアカウントの修正または削除を行います。

プライマリセッション接続トリガ

自動接続： LAN側ネットワークからインターネットへの通信要求が検出されると「プライマリ 1」への接続動作を開始します。

手動接続： 本設定画面上で[接続]ボタンを押さない限り接続しません。

セカンダリセッション接続トリガ

2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。unnumbered PPPoE接続アカウントの設定の場合、考慮する必要はありません。

PPP-Echo-Request送出間隔/リトライ回数

「キープ・アライブ」機能では、PPPoEサーバに対してPPP-Echo-Requestを送出し、それに対する応答パケット (PPP-Echo-Reply)を確認することで、PPPoEセッションを監視します。

ここでは、PPP-Echo-Requestの間隔と、"連続何回"PPPoEサーバから応答がない場合に「切断」と判断し、再接続動作を開始するかを設定します。

PPP-Echo-Request送出間隔：工場出荷時値：60秒、設定可能範囲：10～300秒

PPP-Echo-Requestリトライ回数：工場出荷時値：6回、設定可能範囲：1～99回

One Point!

不安定なADSL回線をご利用の場合、極端に短い送出間隔や少ないリトライ回数を設定すると、頻繁にPPPoEセッションの切断と再接続が繰り返されてしまいます。必要がない限りこの値は変更しないで下さい。

セカンダリセッション接続ルール

2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。unnumbered PPPoE接続アカウントの設定の場合、考慮する必要はありません。

[設定]ボタンをクリックしてください

変更した設定内容が保存されます。再起動完了後、設定したunnumbered PPPoEアカウントへの接続が使用可能になります。

5.PPPoEマルチセッション接続設定

Trying

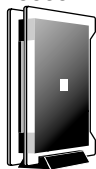
1つのブロードバンド回線で、同時に2セッション以上のPPPoEが利用できる、PPPoEマルチセッションサービスをご利用の場合の設定方法を説明します。

PPPoEマルチセッション機能

PPPoEマルチセッションの動作

- 本製品は最高2つのPPPoEセッションを同時処理することができます。
- 本製品を使って2つのPPPoEセッションに同時に接続する場合、“どの”PPPoE接続アカウントで、“どのような”通信をやり取りするかを決定しなければなりません。このような通信の“振り分け”にはさまざまな考え方がありますが、本製品は以下のようなルールに基づいて振り分けを行います。
LAN側からWAN側へのパケットのうち、指定した条件に一致するパケットとその応答パケットを、「セカンダリセッション」に設定したPPPoE接続アカウントを使って通信します。
その条件を「セカンダリセッション接続ルール」と呼びます。
セカンダリセッション接続ルールには、「送信元IPアドレス」、「送信先IPアドレスまたはホスト名」、「プロトコル」、「送信先ポート」を指定できます。
セカンダリセッション接続ルールに一致しない通信はすべて、「プライマリセッション」に設定したPPPoE接続アカウントを使って通信します。
- セカンダリセッション接続ルールで、「送信先ポート」の指定ができないため、セカンダリセッションのPPPoE接続アカウントにマルチNAT機能や静的マスカレード機能を適用しての、ネットワークゲームやインターネットサーバの公開は、ほぼ不可能です。

BA5000 Pro



条件に一致する通信

セカンダリセッション
の接続先

条件に一致しない通信

プライマリセッション
の接続先

セカンダリセッションへの接続は、2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。それ以外の場合は、絶対に[セカンダリセッション接続ルール]を設定しないで下さい。

セカンダリセッションを利用する場合は、[接続設定]-[LAN設定]のProxy DNSを必ず有効にして下さい。この場合、LAN側ホストから見たDNSサーバは、本製品LAN側IPアドレスになります。

[接続設定] - [新規登録] ページ

PPPoEマルチセッションを利用するため、セカンダリセッションとして利用したいIPPPoE接続アカウントを新規登録します。あらかじめプライマリセッション用のPPPoE接続アカウントを登録しておいてください。

新規登録

接続方法

「PPPoE接続」を選択し、「次へ」ボタンを押します。

[PPPoE接続設定] ページが表示されます。

[PPPoE接続設定] ページ

PPPoE接続アカウントを登録します。

PPPoE接続設定

アカウント名[任意]

この接続設定に、任意の名前を付けることができます。プロバイダ名などを入力して下さい。

設定可能な文字：半角英数字、最高32文字まで

PPPoEユーザ名

プロバイダから指定されたPPPoE接続ユーザ名を正確に入力してください。「フレッツ・ADSL」や「Bフレッツ」の場合は、“@”(アットマーク)以下も入力します。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード

プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPPoEパスワード再入力

入力間違い防止のためもう一度、プロバイダから指定されたPPPoE接続パスワードを正確に入力してください。

PPPoEサービス名

プロバイダからPPPoE接続サービス名を指定された場合のみ、正確に入力してください。

設定可能な文字：半角英数字、最高64文字まで

PPP認証方式

PPP認証方式を設定します。通常は「接続相手にあわせる」を選択してください。

WAN側IPアドレス設定方法

自動取得： PPP認証中に、プロバイダからIPアドレスを自動的に取得する場合。プロバイダから特にIPアドレスを指定されていない場合もこれを選択してください。

固定設定： IPアドレスが固定で指定されている場合。

固定WAN側IPアドレス

[WAN側IPアドレス設定方法] で「固定設定」を選択した場合に、プロバイダから指定されたIPアドレスを入力してください。

DNSサーバアドレス設定方法

固定設定：DNSサーバのIPアドレスを固定設定する場合や、[WAN側IPアドレス設定方法]で「固定設定」を選択した場合。

自動取得：[WAN側IPアドレス設定方法]で「自動取得」を選択した際に、DNSサーバのIPアドレスも同時に自動取得する場合。

プライマリDNSサーバアドレス

[DNSサーバアドレス設定方法]で「固定設定」を選択した場合に、プロバイダから指定された1個目のDNSサーバのIPアドレスを入力します。

セカンダリDNSサーバアドレス

[DNSサーバアドレス設定方法]で「固定設定」を選択した場合に、プロバイダから指定された2個目のDNSサーバのIPアドレスを入力します。

MSSサイズ

MSS (Maximum Segment Size) 値を調整します。通常、MSS値はMTU値から40を引いた値になります。

MSS値は特に必要がない限り絶対に変更しないで下さい。

工場出荷時値：1412byte

WAN側ポートRIP機能

WAN側ポートのRIP機能を設定します。通常のインターネット接続ではRIPを使用しませんので「無効」を選択してください。

無効：RIP機能を利用しない場合。

受信のみ：外部からのRIP受信のみ行う場合。

送信のみ：外部へのRIP送信のみ行う場合。

送受信：RIP送受信を行う場合。



注意

- ・ PPPoEユーザ名、PPPoEパスワード、PPPoEサービス名は、大文字・小文字は別の文字として扱われます。
- ・ PPPoEサービス名は、一般的なインターネット接続サービス名称とは異なります。「フレッツ・ADSL」では入力しないで下さい。

DMZネットワーク設定

ここでは、利用可能なグローバルIPアドレスのうち、何番から何番までのグローバルIPアドレス範囲をLAN側に設置するかを設定・表示します。最高4個のグローバルIPアドレス範囲を設定可能です。

最初のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最初のグローバルIPアドレスを表示します。

最後のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最後のグローバルIPアドレスを表示します。



注意

DMZネットワークに設定するグローバルIPアドレスは、本製品WAN側ポートのアドレスと重複しないようにしてください。

[設定] ボタンをクリックしてください。変更した設定内容が保存され、再起動完了後に**[アカウント管理]** ページが表示されます。

[接続設定]-[アカウント管理]ページ

新規登録したPPPoEアカウントは、そのままでは使えないため、アカウント管理ページで有効にする必要があります。

接続アカウント管理

接続方式の選択

「PPPoE接続」を選択します。

通常接続アカウントリスト

ここは操作しないで下さい。

PPPoE接続アカウントリスト

PPPoE接続アカウントでの接続状態表示や操作を行います。[アカウント名]欄で、先ほど登録したPPPoE接続アカウントを探し、以下の設定を行ってください。

状態

現在の接続状態が表示されます。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

自動取得した、あるいは固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

セッション

本製品は、最大4個のPPPoEアカウントを保持することができます。いずれかひとつのPPPoEアカウントを「プライマリ1」にし、その他を「セカンダリ1/2」や「プライマリ2」に設定してください。

プライマリ1	常に1つのPPPoEアカウントをプライマリ1に設定してください。このPPPoEアカウントが主に使用するPPPoE接続になります。
プライマリ2	プライマリ1のバックアップ用アカウントです。プライマリ1に設定したアカウントでの接続に失敗すると、本製品はプライマリ2に設定したアカウントでPPPoE接続を試みます。さらに続けてプライマリ2でも接続失敗した場合はプライマリ1での接続と、どちらかのアカウントで接続が成功するまで繰り返します。(参照:キープ・アライブ)
セカンダリ1	2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。
セカンダリ2	セカンダリ1のバックアップ用アカウントです。セカンダリ1に設定したアカウントでの接続に失敗すると、本製品はセカンダリ2に設定したアカウントでPPPoE接続を試みます。さらに続けてセカンダリ2でも接続失敗した場合はセカンダリ1での接続と、どちらかのアカウントで接続が成功するまで繰り返します。(参照:キープ・アライブ)
無効	単に設定情報を記憶しておくだけです。実際のPPPoE接続には利用しません。

アイドルタイム

ここに指定した時間、インターネットとの通信がない場合、自動的にPPPoE接続を切断します。自動切断を行いたくない場合は「0」を入力してください。ただし、以下の[キープ・アライブ]を「有効」に設定すると、自動切断機能は無効になります。

工場出荷時値:20分 設定可能範囲:0~999分

キープ・アライブ

セッション・キープアライブ機能です。これが有効にされたPPPoE接続アカウントへの接続が開始されると、その後は常にそのアカウントへの接続を維持しようとします。

不安定なxDSL回線などで、意図しない切断が発生しても、切断されたことを検知し、再接続します。

キープアライブ機能の状態	動作
プライマリ1 = 無効 プライマリ2 = (登録なし)	以下の[プライマリセッション接続トリガ]に基づいた接続開始を行います。
プライマリ1 = 有効 プライマリ2 = 有効または無効	電源投入直後からプライマリ1への接続を開始します。接続失敗した場合や、意図しない切断の場合も、常にプライマリ1への再接続を成功するまで行います。プライマリ2への接続は行われません。

操作

手動によるPPPoE接続または切断を行います。ただし、「プライマリ1」と「プライマリ2」、または「セカンダリ1」と「セカンダリ2」に同時接続することはできません。

修削

選択したアカウントの修正または削除を行います。

プライマリセッション接続トリガ

自動接続： LAN側ネットワークからインターネットへの通信要求が検出されると「プライマリ 1」への接続動作を開始します。

手動接続： 本設定画面上で[接続]ボタンを押さない限り、プライマリセッションに接続しません。

セカンダリセッション接続トリガ

自動接続： セカンダリセッション接続ルールに一致する、LAN側ネットワークからインターネットへの通信要求が検出されると「セカンダリ 1」への接続動作を開始します。

手動接続： 本設定画面上で[接続]ボタンを押さない限り、セカンダリセッションに接続しません。

PPP-Echo-Request送出間隔/リトライ回数

「キープ・アライブ」機能では、PPPoEサーバに対してPPP-Echo-Requestを送出し、それに対する応答パケット (PPP-Echo-Reply)を確認することで、PPPoEセッションを監視します。

ここでは、PPP-Echo-Requestの間隔と、“連続何回”PPPoEサーバから応答がない場合に「切断」と判断し、再接続動作を開始するかを設定します。

PPP-Echo-Request送出間隔：工場出荷時値：60秒、設定可能範囲：10～300秒

PPP-Echo-Requestリトライ回数：工場出荷時値：6回、設定可能範囲：1～99回

One Point!

不安定なADSL回線をご利用の場合、極端に短い送出間隔や少ないリトライ回数を設定すると、頻繁にPPPoEセッションの切断と再接続が繰り返されてしまいます。必要がない限りこの値は変更しないで下さい。

セカンダリセッション接続ルール

LAN側からインターネットへの、以下で指定するすべての条件に一致する通信が検出された場合、その通信はセカンダリセッションを利用します。それ以外の通信はプライマリセッションを利用します。

送信元IPアドレス

LAN側からインターネットへのパケットの送信元IPアドレス、すなわち、LAN側のどのIPアドレスのパソコンがセカンダリセッションを利用するかを設定します。アドレスの指定方法は以下のとおりです。

送信元IPアドレス例	説明
*	すべてのIPアドレス
192.168.1.3	特定のホスト・アドレス
192.168.1.0/24	ネットワーク・アドレス(24ビットマスク)
192.168.1.3-192.168.1.33	範囲指定 スペース無しでハイフン“-”区切り
192.168.1.3,192.168.0.8	列挙指定 スペース無しでコンマ“,”区切り
(何も指定せず)	このルールは無視する。

送信先IPアドレスまたはホスト名

LAN側からインターネットへのパケットの送信先IPアドレスまたはホスト名、すなわち、インターネット上のどのホストへの通信がセカンダリセッションを利用するかを設定します。

インターネット上のホストのIPアドレス、または“www.ntt-me.co.jp”などのホスト名の、いずれか一方を設定してください。IPアドレスの指定方法は上の送信元アドレス例を参照してください。

ホスト名例	説明
.jp	トップレベルドメインのみ指定。 日本(jp)サイトすべて。
.co.jp	セカンダリレベルドメインまで指定。 最後に“ .co.jp ”が付くサイトすべて。
www.ntt-me.co.jp	「www.ntt-me.co.jp」のみ。
.www.ntt-me.co.jp	「host1.www.ntt-me.co.jp」や「host2.www.ntt-me.co.jp」。 「www.ntt-me.co.jp」には該当しない。 上の例と“ . ”(ドット)の有無による違いに注意。
www.*.co.jp	ワイルドカード使用。
(何も指定せず)	このルールは無視する。

プロトコル/送信先ポート

LAN側からインターネットへのパケットのプロトコルと送信先ポート、すなわち、どのようなインターネットサービスでセカンダリセッションを利用するかを設定します。

例: WWWページを閲覧するのにセカンダリセッションを利用する場合は、プロトコルに「tcp」、送信先ポートに「80」を設定。

送信元ポート例	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“-”区切り
80,8080	列挙指定 スペース無しでコンマ“,”区切り



注意

セカンダリセッションへの接続は、2つのPPPoEセッションを同時に使用できるサービスにおいてのみ利用することができます。また、Proxy DNS機能(LAN設定)を必ず利用して下さい。

[設定]ボタンをクリックしてください

変更した内容が保存されます。再起動完了後、設定したプライマリセッションやセカンダリセッションへの接続が使用可能になります。

6.PPPoE接続の状況確認



現在のPPPoEの接続状況は、本製品WWW設定画面で確認することができます。

[接続設定] - [アカウント管理] ページ

PPPoE接続アカウントリスト

これまでに登録したPPPoE接続アカウントがリスト表示されます。

状態

現在の接続状態が表示されます。表示される内容の意味は以下のとおりです。

メッセージ	内容
Disabled	PPPoE接続が無効。
Link Down	WAN側ポートの物理リンクが確立されていない状態。 WAN側ポートにケーブルが挿されていない場合。 クロス/ストレート結線が間違っている場合。 WAN側ポートと接続している機器の電源が入っていない場合など。
Connect (yyyy:mm:dd:hh:mm:ss wan-ip pppserver-ip)	正常にPPPoE接続できている状態。yyyy:mm:dd:hh:mm:ss は接続した時刻、wan-ip はWAN側ポートのIPアドレス、pppserver-ip はPPPoEサーバのIPアドレスを示します。
Disconnect(yyyy:mm:dd:hh:mm:ss)	正常にPPPoE接続を切断している状態。() 内は切断した時刻を示します。
In the PPPoE Sequence	PPPoEシーケンス中の状態。
PPPoE:Service-Name-Error	設定してあるPPPoEサービス名がPPPoEサーバにより拒否された状態。
PPPoE:AC-System-Error	PPPoEサーバから拒否された状態
PPPoE:Generic-Error	PPPoEシーケンス中に不明なエラーが発生した場合。
PPPoE:PADI-Timeout	PADIタイムアウト
PPPoE:PADR-Timeout	PADRタイムアウト
PPPoE:LCP-Timeout	LCPタイムアウト。設定が間違っている可能性があります。
PPPoE:IPCP-Timeout	IPCPタイムアウト。設定が間違っている可能性があります。
PPPoE:Authentication-Failed	PPP認証に失敗した場合。設定が間違っている可能性があります。
PPPoE:Authentication-Timeout	PPP認証に失敗した場合。設定が間違っている可能性があります。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

自動取得した、あるいは固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

操作

手動によるPPPoE接続または切断を行います。ただし、「プライマリ1」と「プライマリ2」、「セカンダリ1」と「セカンダリ2」に同時接続することはできません。

修/削

選択したアカウントの修正または削除を行います。

One Point!

設定を変更する場合は、[設定]ボタンをクリックしてください。

第2章



通常接続

「Yahoo! BB」や通常のCATVインターネットでの本製品の設定を説明します。

1.通常接続設定の種類



PPPoEではない、一般的なEthernet接続サービスを説明します。

IPを使った通信に必要なパラメータ

Ethernet上でのIP(TCP/IP)を使ったネットワーク通信では、各ホスト(パソコンやルータ)が、以下のパラメータを保持している必要があります。

・IPアドレス

IPプロトコル上で、各ホストを特定するための番号です。ドットノテーション(xxx.xxx.xxx.xxx)形式で表示されます。

・サブネットマスク

サブネットとは、IPネットワークで効率的な通信を実現するためにネットワークを分割した単位です。そしてIPアドレスを持つホストがどこのサブネットに存在するかを判断する番号を、サブネットマスクといいます。ドットノテーション(xxx.xxx.xxx.xxx)形式で表示されます。

・デフォルトゲートウェイ

自分のルーティングテーブルに載っていないIPアドレス、すなわち、どこに存在するかわからない相手へのデータ送信時に、転送を依頼する相手のIPアドレスです。外部ネットワークへの出口となるホストのアドレスになります。一般的にはルータがこの役割を担います。ドットノテーション(xxx.xxx.xxx.xxx)形式で表示されます。

さらに通常のブロードバンド通信では、以下のパラメータも保持している必要があります。

・DNSサーバアドレス

「www.ntt-me.co.jp」などのホスト名をもとに、そのホストのIPアドレスを教えてくれるサーバをDNSサーバといいます。DNSの仕組みがあるおかげで、直感的なホスト名を使用することができるようになっています。

通常接続設定の種類

・固定IPアドレスサービス

IPアドレスなどの通信に必要なパラメータが、プロバイダから固定的に割り当てられているサービスです。常に同じパラメータを使用することができます。

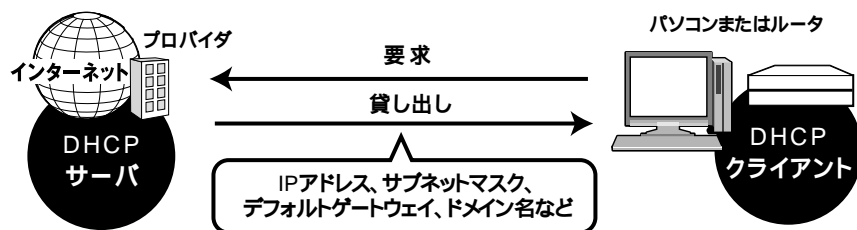
・複数固定IPアドレスサービス

固定IPアドレスサービスの中でも、複数のIPアドレスが割り当てられるサービスです。

・動的IPアドレスサービス

DHCPを利用して、ネットワークに接続した時点で、IPアドレスなどのパラメータを自動的に取得するサービスです。接続するたびに異なるIPアドレスになる可能性があります。

IPアドレスを教えてくれるホスト(プロバイダ側)をDHCPサーバ、DHCPサーバからIPアドレスを自動取得するホスト(ユーザ側)をDHCPクライアントといいます。



接続設定ページ

- ・動的IPアドレスサービス
- ・固定IPアドレスサービス
- ・複数固定IPアドレスサービス

付属の「BA5000 Proマニュアル 接続編」を参照してください。
「2-2. 固定IPアドレス通常接続設定」のページへ
「2-3. 複数固定IPアドレス通常接続設定」のページへ

2. 固定IPアドレス通常接続設定



CATVインターネットなどの一般的なEthernet接続サービスで、固定IPアドレスを利用できる場合の設定方法を説明します。

[接続設定] - [新規登録] ページ

新規登録

接続方法

「通常接続」を選択し、「次へ」ボタンを押します。

[通常接続設定] ページが表示されます。

[通常接続設定] ページ

通常接続アカウントを登録します。

アカウント名 [任意]

この接続設定に、任意の名前を付けることができます。プロバイダ名などを入力して下さい。

設定可能な文字：半角英数字、最高32文字まで

DHCPクライアント機能

無効 : DHCPクライアント機能を無効にし、IPアドレスを固定設定します。これを選択してください。

有効 : プロバイダからIPアドレスが自動的に割り当てられる場合。(本製品のDHCPクライアント機能を有効にする場合)

DHCPクライアントID (ホスト名)

入力する必要はありません。

WAN IPアドレス

プロバイダから割り当てられた固定IPアドレスを入力します。

WAN サブネットマスク

プロバイダから割り当てられたサブネットマスクを入力します。

WAN デフォルトゲートウェイ

プロバイダから割り当てられたデフォルトゲートウェイのIPアドレスを入力します。

DNSサーバアドレス設定方法

無効 : DHCPクライアント機能を利用せず、DNSサーバアドレスも固定設定するため、これを選択します。

有効 : DHCPクライアント機能で「有効」を選択した場合。

プライマリDNSサーバアドレス

プロバイダから割り当てられたプライマリDNSサーバのIPアドレス、または自分が運営しているプライマリDNSサーバのIPアドレスを入力します。

セカンダリDNSサーバアドレス
プロバイダから割り当てられたセカンダリDNSサーバのIPアドレス、または自分が運営しているセカンダリDNSサーバのIPアドレスを入力します。セカンダリDNSサーバがない場合は入力する必要はありません。

WAN側ポートRIP機能
無効 : RIP機能を利用しない場合。通常はこれを選択してください。
受信のみ : 外部からのRIP受信のみ行う場合。
送信のみ : 外部へのRIP送信のみ行う場合。
送受信 : RIP送受信を行う場合。

DMZネットワーク設定
プロバイダから割り当てられるIPアドレスが1個の場合、DMZネットワークテーブルは絶対に設定しないで下さい。複数のグローバルIPアドレスが利用可能な通常接続サービスの場合のみ、DMZネットワークテーブルを設定可能です。

[設定]ボタンをクリックしてください

変更した設定内容が保存され、[アカウント管理]ページが表示されます。

[接続設定] - [アカウント管理] ページ

新規登録した通常接続アカウントは、そのままでは使えないため、アカウント管理のページで有効にする必要があります。

接続アカウント管理
接続方式の選択
「通常接続」を選択します。

通常接続アカウントリスト
通常接続アカウントでの接続状態表示や操作を行います。
状態
現在の接続状態が表示されます。

アカウント名
設定したアカウントの名前を表示します。

DNSアドレス
固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

ドメイン名
ドメイン名を表示します。ドメイン名の設定は、[LAN設定]で行います。

DHCP
DHCPクライアント機能を使用しないため、ここは関係ありません。

修正
この通常接続アカウントの修正または削除を行います。

このページでは、特に設定する項目はありません。

3.複数固定IPアドレス通常接続設定



CATVインターネットなど、一般的なEthernet接続サービスで固定IPアドレスを利用できる場合で、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ている場合の設定方法を説明します。

[接続設定] - [新規登録] ページ

新規登録

接続方法

「通常接続」を選択し、「次へ」ボタンを押します。

[通常接続設定] ページが表示されます。

[通常接続設定] ページ

通常接続アカウントを登録します。

アカウント名 [任意]

この接続設定に、任意の名前を付けることができます。プロバイダ名などを入力して下さい。

設定可能な文字：半角英数字、最高32文字まで

DHCPクライアント機能

無効 : DHCPクライアント機能を無効にし、IPアドレスを固定設定します。これを選択してください。

有効 : プロバイダからIPアドレスが自動的に割り当てられる場合。(本製品のDHCPクライアント機能を有効にする場合)

DHCPクライアントID (ホスト名)

入力する必要はありません。

WAN IPアドレス

プロバイダから割り当てられた固定IPアドレスを入力します。

WAN サブネットマスク

プロバイダから割り当てられたサブネットマスクを入力します。

WAN デフォルトゲートウェイ

プロバイダから割り当てられたデフォルトゲートウェイのIPアドレスを入力します。

DNSサーバアドレス設定方法

無効 : DHCPクライアント機能を利用せず、DNSサーバアドレスも固定設定するため、これを選択します。

有効 : DHCPクライアント機能で「有効」を選択した場合。

プライマリDNSサーバアドレス

プロバイダから割り当てられたプライマリDNSサーバのIPアドレス、または自分が運営しているプライマリDNSサーバのIPアドレスを入力します。

セカンダリDNSサーバアドレス

プロバイダから割り当てられたセカンダリDNSサーバのIPアドレス、または自分が運営しているセカンダリDNSサーバのIPアドレスを入力します。

WAN側ポートRIP機能

無効 : RIP機能を利用しない場合。通常はこれを選択してください。

受信のみ : 外部からのRIP受信のみ行う場合。

送信のみ : 外部へのRIP送信のみ行う場合。

送受信 : RIP送受信を行う場合。

DMZネットワーク設定

ここでは、利用可能なグローバルIPアドレスのうち、何番から何番までのグローバルIPアドレスホストをLAN側に設置するかを設定・表示します。最高4個のグローバルIPアドレス範囲を設定可能です。

最初のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最初のグローバルIPアドレスを表示します。

最後のIPアドレス

LAN側で利用したいグローバルIPアドレス範囲の、最後のグローバルIPアドレスを表示します。



- ・DMZネットワークに設定するグローバルIPアドレスは、本製品WAN側ポートのアドレスと重複しないようにしてください。
- ・DMZネットワーク設定は、グローバルIPアドレスのホストのLAN側への設置を可能にする機能です。複数のグローバルIPアドレスは使用するが、LAN側にグローバルIPアドレスホストを置きたくない場合は、[マルチNAT設定]を行ってください。マルチNAT機能を利用すると、グローバルIPアドレスとプライベートIPアドレスの1対1の変換を行います。

[設定]ボタンをクリックしてください

変更した設定内容が保存され、[アカウント管理]ページが表示されます。

[接続設定] - [アカウント管理] ページ

新規登録した通常接続アカウントは、そのままでは使えないため、アカウント管理ページで有効にする必要があります。

接続アカウント管理

接続方式の選択

「通常接続」を選択します。

通常接続アカウントリスト

通常接続アカウントでの接続状態表示や操作を行います。

状態

現在の接続状態が表示されます。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

ドメイン名

ドメイン名を表示します。ドメイン名の設定は、[LAN設定]で行います。

DHCP

DHCPクライアント機能を使用しないため、ここは関係ありません。

修正

この通常接続アカウントの修正または削除を行います。

このページでは、特に設定する項目はありません。

DMZネットワークを利用する際のパソコンの設定**・グローバルIPホスト**

IPアドレス : 割り当てられたグローバルIPのうち、ネットワークアドレス、ブロードキャストアドレス、本製品WAN側IPアドレス以外のアドレス

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

デフォルトゲートウェイ : プロバイダから指定されたデフォルトゲートウェイ

・プライベートIPホスト

変更の必要はありません。

4.通常接続の状況確認



現在の通常接続の状況は、本製品WWW設定画面で確認することができます。

[接続設定] - [アカウント管理] ページ

通常接続アカウントリスト

登録した通常接続アカウントがリスト表示されます。

状態

現在の接続状態が表示されます。表示される内容の意味は以下のとおりです。

メッセージ	内容
Disabled	通常接続が無効。
Link Down	WAN側ポートの物理リンクが確立されていない状態。 WAN側ポートにケーブルが挿されていない場合。 クロス/ストレート結線が間違っている場合。 WAN側ポートと接続している機器の電源が入っていない場合など。
Connect	IPアドレスを固定設定しており、物理リンクが確立されている状態
Connect [wan-ip : subnetmask : gateway-ip dhcp-time]	DHCPクライアント機能を有効にしており、正常にIPアドレスを取得できている状態。wan-ip はWAN側IPアドレス、subnetmask はサブネットマスク、gateway-ip はデフォルトゲートウェイのIPアドレス、dhcp-time はDHCPリースの残り時間を示します。
DHCP Offering	DHCPクライアント機能を有効にしている、まだIPアドレスを正常に取得できていない状態。

アカウント名

設定したアカウントの名前を表示します。

DNSアドレス

DHCPで取得した、あるいは固定設定しているプライマリDNSサーバとセカンダリDNSサーバのIPアドレスを表示します。

ドメイン名

ドメイン名を表示します。

DHCP

DHCPクライアント機能を有効にしている場合、取得したWAN側IPアドレスの更新や開放を行います。固定IPアドレスの場合は関係ありません。「開放」「更新」の順でボタンを押してください。

「開放」ボタン： プロバイダのDHCPサーバにIPアドレスを返上します。

「更新」ボタン： プロバイダのDHCPサーバからIPアドレスを自動取得します。

修正

この通常接続アカウントの修正または削除を行います。

このページでは、特に設定する項目はありません。

第3章



NAPT

アドレス変換機能や静的マスカレードの設定を説明します。

1.NAPT機能

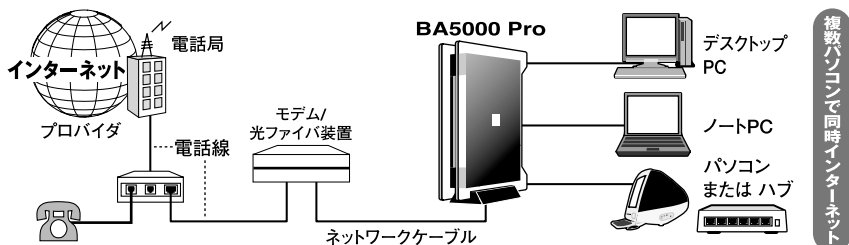


NAPT機能に関する説明をします。

NAPT

本製品はネットワークアドレス変換（NAPT）機能に対応しています。

NAPT機能では、プロバイダから割り当てられるグローバルIPアドレスと、LAN側のプライベートIPアドレスの変換を行い、グローバルIPアドレスが1個しか割り当てられないブロードバンドサービスでも、複数台のパソコンでの同時通信を実現します。



NAPT機能は、以下のように動作します。

LAN側のパソコンがインターネット側への通信要求パケットをルータのLAN側ポートへ送る。

（送信元IPアドレスはパソコンのプライベートIPアドレス）

ルータは、このパケットの送信元IPアドレスなどを、WAN側ポートのアドレスに書き換えた後、そのパケットをインターネット側へ送り出し、その記録を保持する。

この応答パケットが、インターネット側からルータのWAN側ポートへ到達する。

（送信元IPアドレスはルータのグローバルIPアドレス）

ルータはこの記録から、それがどのパソコンへの通信かを判断し、そのパソコンへ送る。

（送信元IPアドレスはパソコンのプライベートIPアドレス）

NAPT機能を無効にした場合

本製品はNAPT機能を無効にすることもできます。NAPT機能を無効にした場合は、以下のことに注意してください。

- ・ 通常のブロードバンドサービスでNAPT機能を無効にすると、複数台のパソコンの同時インターネット接続はできなくなります。
- ・ NAPT機能を無効にすると、WAN側ネットワーク LAN側ネットワーク間のルーティングを行います。
- ・ たくさんのネットワークへのルーティングを可能にするには、以下のいずれかの設定を行ってください。
本製品に対して、スタティックルートを設定する。
RIP機能を利用できる場合は、WAN側またはLAN側でRIP機能を有効にする。

NAPT機能の制限と静的マスカレード機能

Webサイトの閲覧など、LAN側のパソコンからインターネット側への通信要求パケットから始まる一連の通信はNAPT機能で対応できます。しかし、ルータにとって転送先ホストが不明なため、WAN側からLAN側への通信要求パケットから始まる通信は、通常のNAPT機能では対応できません。

例1 LAN側にインターネットサーバを設置する場合

例2 ネットワークゲームをプレイする場合。

このような場合、WAN側からの特定の通信の転送先LAN側ホストをあらかじめ設定しておく、静的マスカレード機能を利用することで、問題を回避することができます。

静的マスカレード機能の種類

本製品で設定できる静的マスカレードには、以下の2種類があります。

・マルチNAT機能

グローバルIPアドレス1個のサービスの場合

本製品のWAN側IPアドレス宛てに来る、転送先LAN側ホストが不明のパケットを、設定したプライベートIPアドレスホストに転送します。

複数グローバルIPアドレスのサービスの場合

を行うことができるほか、本製品のWAN側IPアドレス以外のグローバルIPアドレス宛てに来るすべてのパケットを、それぞれのグローバルIPアドレスごとに設定したプライベートIPアドレスホストに転送することもできます。

・ローカルサーバ機能

グローバルIPアドレス1個のサービスの場合

本製品のWAN側IPアドレス宛てに来る、転送先LAN側ホストが不明のパケットうち、特定のポートのポートのパケットを、設定したプライベートIPアドレスホストに転送します。

複数グローバルIPアドレスのサービスの場合

を行うことができるほか、本製品のWAN側IPアドレス以外のグローバルIPアドレス宛てに来る、特定のアドレス/ポートのポートのパケットを、設定したプライベートIPアドレスホストに転送することもできます。



- ・マルチNAT機能の転送先に設定したプライベートIPアドレスホストは、インターネットから直接参照可能になります。
- ・ローカルサーバ機能の転送先に設定したプライベートIPアドレスホストは、設定したポートを通じてインターネットから直接参照可能になります。

接続設定ページ

- ・マルチNAT機能を使う場合
- ・ローカルサーバ機能を使う場合
- ・UPnP機能を利用する場合
- ・H.323インターネット電話を使いたい場合
- ・VPNを使いたい場合

- 「3-2.サーバ公開/ゲームの利用(マルチNAT)」のページへ
- 「3-3.サーバ公開/ゲームの利用(ローカルサーバ)」のページへ
- 「3-4.Universal Plug and Play」のページへ
- 「3-5.H.323NAT」のページへ
- 「3-6.VPNパススルー」のページへ

2.サーバ公開/ゲームの利用(マルチNAT)



静的マスカレードのマルチNAT機能を使って、インターネットサーバの公開やネットワークゲームの利用を可能にする方法を説明します。



注意

- ・マルチNAT機能の転送先に設定したプライベートIPアドレスホストは、インターネットから直接参照可能になります。特定のプロトコル/ポートのパケットで設定したい場合は、「サーバ公開/ゲームの利用(ローカルサーバ)」のページを参照してください。

[ルータ設定] - [NAPT] ページ

NAPT設定

アカウント選択

どのアカウントの接続で、インターネットサーバ公開やネットワークゲームをやりたいか選択します。ここで選択した接続アカウントでマルチNAT機能を設定することになります。

静的マスカレードテーブル

現在設定してある、静的マスカレード設定の表示・操作を行います。

ID

静的マスカレードのID番号を示します。小さい番号の静的マスカレールドルールが優先されます。

プロトコル

インターネットからLAN側への通信を許可するプロトコルを表示します。

* (すべて): インターネットからLAN側への通信のうち、LAN側転送先がわからないすべてのパケットが対象になります。

- icmp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- tcp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- udp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- tcp&udp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。

外部IPアドレス

マルチNATで、インターネットからLAN側への通信を許可する際の、インターネット側から見た送信先IPアドレス(公開するIPアドレス)を表示します。

グローバルIPアドレス1個のサービスの場合	WAN側ポートIPアドレス
複数グローバルIPアドレスのサービスで本製品のWAN側IPアドレスで公開する場合	WAN側ポートIPアドレス
複数グローバルIPアドレスのサービスで本製品のWAN側IPアドレス以外で公開する場合	本製品のWAN側IPアドレス以外のグローバルIPアドレス (プロバイダから割り当てられたもの)

外部ポート

マルチNATでは関係ありません。

内部IPアドレス

上記、[外部IPアドレス]宛てのパケットが、本製品のWAN側ポートに送られてきた場合に、それが転送されるべきLAN側ホストのIPアドレスを表示します。ここに表示されたIPアドレスのホストが、公開インターネットサーバまたはネットワークゲームをプレイするパソコンになります。

内部ポート

マルチNATでは関係ありません。

修正/削除

選択した静的マスカレードの修正または削除を行います。

静的マスカレードの追加

静的マスカレードの追加を行います。

[静的マスカレードの追加/修正]ページが表示されます。

[静的マスカレードの追加/修正] ページ

静的マスカレードの追加を行います。

静的マスカレードの追加

ID

静的マスカレードのID番号を入力します。小さい番号の静的マスカレードルールが優先されます。

設定可能範囲: 1 ~ 32

プロトコル

インターネットからLAN側への通信を許可するプロトコルを選択します。

* (すべて): インターネットからLAN側への通信のうち、LAN側転送先がわからないすべてのパケットが対象になります。マルチNAT機能を利用する場合はこれを選択してください。

- icmp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- tcp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- udp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。
- tcp&udp : 「3-3. サーバ公開/ゲームの利用(ローカルサーバ)」のページ参照。

外部IPアドレス

マルチNATで、インターネットからLAN側への通信を許可する際の、インターネット側から見た送信先IPアドレス(公開するIPアドレス)を選択します。

グローバルIPアドレス1個のサービスの場合	「WAN側ポートIPアドレス」を選択
複数グローバルIPアドレスのサービスで本製品のWAN側IPアドレスで公開する場合	「WAN側ポートIPアドレス」を選択
複数グローバルIPアドレスのサービスで本製品のWAN側IPアドレス以外で公開する場合	「指定」を選択

外部IPアドレス入力

[外部IPアドレス]で「指定」を選択した場合のみ、インターネットに公開したいグローバルIPアドレス(本製品WAN側ポート以外)を入力します。

外部ポート

マルチNATでは関係ありません。

内部IPアドレス

上記、[外部IPアドレス]宛てのパケットが、本製品のWAN側ポートに送られてきた場合に、それが転送されるべきLAN側ホストのIPアドレスを入力します。ここに入力されたIPアドレスのホストが、公開インターネットサーバまたはネットワークゲームをプレイするパソコンになります。

内部ポート

マルチNATでは関係ありません。

内部ポート指定

マルチNATでは関係ありません。

[設定] ボタンをクリックしてください

設定した静的マスカレードが追加されます。

3.サーバ公開/ゲームの利用(ローカルサーバ)



静的マスカレードのローカルサーバ機能を使って、インターネットサーバの公開やネットワークゲームの利用を可能にする方法を説明します。



注意

ローカルサーバ機能では、インターネット側からの特定のプロトコル/ポートのパケットのLAN側転送先ホストを設定します。利用したいサーバやゲームが使用するプロトコル/ポートが不明な場合や、すべてのパケットで設定したい場合は、「サーバ公開/ゲームの利用(マルチNAT)」のページを参照してください。ローカルサーバ機能の転送先のプライベートIPアドレスホストは、設定したプロトコル/ポートを通じてインターネットから直接参照可能になります。

[ルータ設定] - [NAPT] ページ

NAPT設定

アカウント選択

どのアカウントの接続で、インターネットサーバ公開やネットワークゲームをやりたいか選択します。ここで選択した接続アカウントでマルチNAT機能を設定することになります。

静的マスカレードテーブル

現在設定してある、静的マスカレード設定の表示・操作を行います。

ID

静的マスカレードのID番号を表示します。小さい番号の静的マスカレードルールが優先されます。

プロトコル

インターネットからLAN側への通信を許可するプロトコルを表示します。

- * (すべて) : インターネットからLAN側への通信のうち、LAN側転送先がわからないすべてのパケットが対象になります。ローカルサーバ機能では選択しません。
- icmp : インターネットからLAN側への通信のうち、LAN側転送先のわからないicmpパケット(Pingなど)が対象になります。
- tcp : インターネットからLAN側への通信のうち、以下の[外部ポート]に示されたtcpパケットが対象になります。
- udp : インターネットからLAN側への通信のうち、以下の[外部ポート]に示されたudpパケットが対象になります。
- tcp&udp : インターネットからLAN側への通信のうち、以下の[外部ポート]に示されたtcpパケットとudpパケットが対象になります。

外部IPアドレス

ローカルサーバ機能で、インターネットからLAN側への通信を許可する際の、インターネット側から見た送信先IPアドレス(公開するIPアドレス)を表示します。

グローバルIPアドレス1個のサービスの場合	WAN側ポートIPアドレス
複数グローバルIPアドレスのサービスで 本製品のWAN側IPアドレスで公開する場合	WAN側ポートIPアドレス
複数グローバルIPアドレスのサービスで 本製品のWAN側IPアドレス以外で公開する場合	本製品のWAN側IPアドレス以外のグローバルIPアドレス (プロバイダから割り当てられたもの)

外部ポート

ローカルサーバ機能で、インターネットからLAN側への通信を許可する際の、インターネット側から見た送信先ポート(公開するポート)を表示します。

内部IPアドレス

上記、[外部IPアドレス]宛てのパケットが、本製品のWAN側ポートに送られてきた場合に、それが転送されるべきLAN側ホストのIPアドレスを表示します。ここに表示されたIPアドレスのホストが、公開インターネットサーバまたはネットワークゲームをプレイするパソコンになります。

内部ポート

ローカルサーバ機能で、インターネットからLAN側への通信を許可する際の、LAN側ホストの待ち受けポートを表示します。通常は[外部ポート]と同じになります。

修正/削除

選択した静的マスカレードの修正または削除を行います。

静的マスカレードの追加

静的マスカレードの追加を行います。

[静的マスカレードの追加/修正]ページが表示されます。

[静的マスカレードの追加/修正] ページ

静的マスカレードの追加を行います。

静的マスカレードの追加

ID

静的マスカレードのID番号を入力します。小さい番号の静的マスカレードルールが優先されます。
設定可能範囲：1～32

プロトコル

インターネットからLAN側への通信を許可するプロトコルを選択します。

* (すべて) : インターネットからLAN側への通信のうち、LAN側転送先がわからないすべてのパケットが対象になります。ローカルサーバ機能では選択しません。

- icmp : インターネットからLAN側への通信のうち、LAN側転送先のわからないicmpパケット (Pingなど) が対象になります。
- tcp : インターネットからLAN側への通信のうち、以下の[外部ポート]で指定したtcpパケットが対象になります。
- udp : インターネットからLAN側への通信のうち、以下の[外部ポート]で指定したudpパケットが対象になります。
- tcp&udp : インターネットからLAN側への通信のうち、以下の[外部ポート]で指定したtcpパケットとudpパケットが対象になります。

外部IPアドレス

マルチNATで、インターネットからLAN側への通信を許可する際の、インターネット側から見た送信先IPアドレス(公開するIPアドレス)を選択します。

グローバルIPアドレス1個のサービスの場合	「WAN側ポートIPアドレス」を選択
複数グローバルIPアドレスのサービスで 本製品のWAN側IPアドレスで公開する場合	「WAN側ポートIPアドレス」を選択
複数グローバルIPアドレスのサービスで 本製品のWAN側IPアドレス以外で公開する場合	「指定」を選択

外部IPアドレス入力

[外部IPアドレス]で「指定」を選択した場合に、インターネットに公開したいグローバルIPアドレス(本製品WAN側ポート以外)を入力します。

外部ポート

[プロトコル]欄で、tcp、udpまたはtcp&udpを選択している場合に、インターネット側から見た送信先ポート番号（公開ポート番号）を入力します。ネットワークゲームや公開サーバで利用するプロトコルのポート番号を入力してください。

IPアドレスの指定方法は上の送信元アドレス例を参照してください。

例：WWWサーバを公開するには、プロトコルに「tcp」、送信先ポートに「80」を設定。

送信元ポート例	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“-”区切り
80,8080	列挙指定 スペース無しでコンマ“,”区切り

内部IPアドレス

上記、[外部IPアドレス]宛てのパケットが、本製品のWAN側ポートに送られてきた場合に、それが転送されるべきLAN側ホストのIPアドレスを入力します。ここに入力されたIPアドレスのホストが、公開インターネットサーバまたはネットワークゲームをプレイするパソコンになります。

内部ポート

[プロトコル]欄で、tcp、udpまたはtcp&udpを選択している場合に、[内部IPアドレス]で指定されたパソコンが、そのパケットを受け入れるポート番号を選択します。通常は「外部ポート番号と同じ」にしてください。WAN側の待ち受けポートと、転送先（LAN上）のパソコンの待ち受けポートを異なる番号にしたい場合のみ、「指定」を選択して以下の[内部ポート指定]欄に入力してください。

内部ポート指定

[内部ポート]欄で、「指定」を選択している場合に、ここに転送先（LAN上）のパソコンの待ち受けポートを入力してください。ポートの指定方法は、上の外部ポート例を参照して下さい。

[設定]ボタンをクリックしてください

設定した静的マスカレードが追加されます。

4. Universal Plug and Play



本製品はUniversal Plug and Play(UPnP)機能を実装しています。この機能を利用すると、UPnPに対応したアプリケーションを簡単に利用することができます。

UPnPを利用できるOS

本製品のUPnP機能を利用するには、UPnP対応OSが必要です。平成14年6月現在、標準でUPnPに対応しているOSは以下の通りです。

- ・ Windows XP
- ・ Windows Me

UPnPを利用できるアプリケーション

UPnPを利用した通信を実現するためには、OSのサポートだけでなくアプリケーション側の対応も必要です。平成14年6月現在のUPnP対応アプリケーションは以下の通りです。

- ・ Windows Messenger version 4.6以上

Windows XPに標準搭載されているインスタントメッセージングソフト(IM)です。インターネットを使ったテレビ電話(ビデオチャット)などが可能です。

- ・ MSN Messenger version 4.6以上

Windows 95/98/Me/2000と、Windows NT 4.0以上で利用することができるインスタントメッセージングソフト(IM)です。インターネット電話(音声チャット)などが可能です。ただし、UPnPを利用できるのはWindows Meに限定されます。

利用できるMessengerの機能

本製品のUPnP機能により利用可能になるWindows Messenger、MSN Messengerの機能は以下の通りです。

	Windows Messenger	MSN Messenger
インスタントメッセージ		
音声チャット		
ビデオチャット		機能なし
電話をかける(.NET Voice Services)		
ファイルの送受信		
アプリケーション共有		機能なし
ホワイトボード		機能なし
リモートアシスタンス		機能なし
複数のMessenger端末利用		



注意

- ・音声チャットには、音声入力/出力のためのマイク/スピーカ、またはヘッドセットが必要です。
- ・ビデオチャットには、マイク/スピーカまたはヘッドセットと、映像入力を行うためのカメラ(USB接続カメラなど)が必要です。
- ・音声チャットやビデオチャットは、パソコン同士でしか利用できませんが、「電話をかける」(.NET Voice Services)では、NTT一般公衆回線(03-xxxx-xxxxなど)に電話をかけることができます。ただしこの機能を利用するためには、.NET Voice Servicesプロバイダとの契約が必要です。
- ・Windows Updateのすべての更新を適用することを推奨します。
- ・複数固定IPアドレスサービスの場合に、本製品のDMZネットワーク機能を利用し、LAN側に設置しているグローバルIPホストでWindows MessengerやMSN Messengerを使う場合は、本製品のUPnP機能を有効にする必要はありません。
- ・ご利用のブロードバンドサービスによっては、ユーザに対してプライベートIPアドレスを割り当てる場合があります。このような場合、Messengerの各機能は利用できないことがあります。
- ・Windows 95/98/Me/2000やWindows NT 4.0以上で、MSN MessengerやNetMeetingを利用するためには、「3-5. サーバ公開/ゲームの利用(マルチNAT)」を参照してください。ただし、一部の機能を利用できない場合があります。
- ・UPnPという仕組みは、家庭内LANなどの小規模ネットワークでのプラグアンドプレイ環境実現を目的としています。また、ブロードキャストやマルチキャストを多用するため、帯域の利用効率は良くありません。したがって中規模以上のネットワークでのUPnP利用は推奨しません。

Windows XPでの準備

Windows Messengerのバージョンの確認

Windows Messenger version 4.6以降をインストールしてあるかどうか確認してください。Windows Messengerのバージョンは、Windows Messengerのメニューから、[ヘルプ] - [Windows Messengerのバージョン情報] で確認することができます。Windows Messengerのバージョンが4.6より古い場合は、Windows Updateからダウンロードインストールすることが出来ます。



Windows Messengerのオーディオに関するアップデート

Windows Messengerのオーディオに関するアップデートが適用されているかどうか確認します。Windows Updateを実行し、更新の一覧に「Windows Messengerのオーディオに関するアップデート」が表示される場合は、それを選択してインストールしてください。

UPnPサポートのインストール

- 1 [ネットワーク接続]を開き、メニューの[詳細設定] - [オプションネットワークコンポーネント]をクリックします。



- 2 [コンポーネント]欄の[ネットワークサービス]を反転表示させ、[詳細]ボタンをクリックします。



- 3 [ネットワークサービスのサブコンポーネント]欄の[ユニバーサルプラグアンドプレイ]にチェックが入っているかどうか確認します。入っていない場合は、チェックを入れて[OK]ボタンをクリックし、画面の指示に従ってください。この際、Windows XPのCD-ROMを要求される場合があります。



Windows Meでの準備

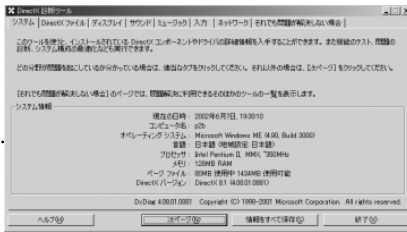
MSN Messengerのバージョンの確認

MSN Messenger version 4.6以降をインストールしてあるかどうか確認してください。MSN Messengerのバージョンは、MSN Messengerのメニューから、[ヘルプ] - [MSN Messengerのバージョン情報] で確認することができます。



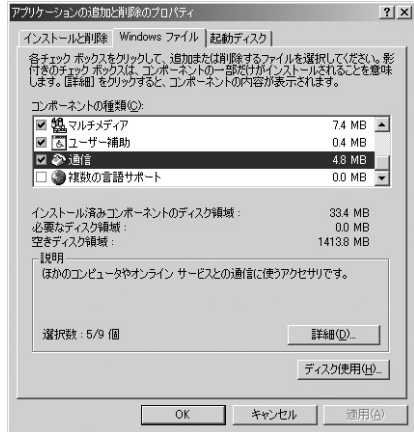
DirectXのバージョンの確認

DirectX8.1以降をインストールしてあるかどうか確認してください。DirectXのバージョンは、[ファイル名を指定して実行] で「dxdiag」を実行することで確認することができます。DirectXのバージョンが8.1より古い場合は、Windows Updateからダウンロードインストールすることができます。

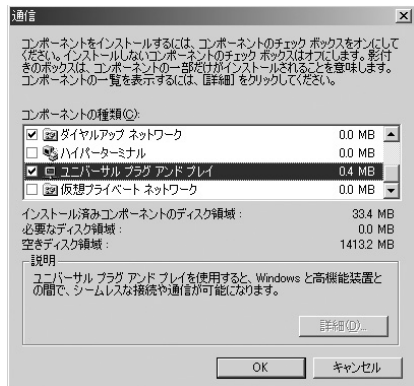


UPnPサポートのインストール

- 1 [コントロールパネル] を開き、[アプリケーションの追加と削除] を実行し、[アプリケーションの追加と削除のプロパティ] から、[Windowsファイル] タブをクリックします。



- 2 [コンポーネントの種類] 欄の [通信] を反転表示させ、[詳細] ボタンをクリックし、[コンポーネントの種類] 欄の [ユニバーサルプラグアンドプレイ] にチェックが入っているかどうか確認します。入っていない場合は、チェックを入れて [OK] ボタンをクリックし、画面の指示に従ってください。この際、Windows MeのCD-ROMを要求される場合があります。



本製品のUPnP機能の設定

本製品は工場出荷時にUPnP機能が有効に設定されています。UPnP機能が有効に設定されているかどうかは以下の手順で確認することができます。

1 WWWブラウザで設定画面を開きます。

2 メニューバーから、[接続設定] - [LAN設定] の文字をクリックします
[LAN設定] ページが表示されます。



[LAN設定]

Universal Plug and Play機能

UPnP機能を設定します。以下のオプションを選択した後、[設定] ボタンを押してください。
有効：UPnP機能を利用します。
無効：UPnP機能を利用しません。

UPnP機能の利用 (Windows XPの場合)

マイネットワーク画面

1 Windows XP上の[マイネットワーク]画面に、[BA5000 Pro Broadband Router]というアイコンが表示されます。



2 [BA5000 Pro Broadband Router]アイコンを右クリックし、コンテキストメニューから [プロパティ] をクリックすると、本製品のプロパティが表示されます。



3 [BA5000 Pro Broadband Router]アイコンをダブルクリックすると、本製品の設定画面が表示されます。

ネットワーク接続画面

- 1 Windows XP上の[ネットワーク接続]画面に、現在設定されている接続アカウントが、「BA5000Pro 上の xxxx (xxxxはアカウント名) として表示されます。



- 2 「BA5000Pro 上の xxxx」アイコンを右クリックし、コンテキストメニューから[プロパティ]をクリックすると、その接続のプロパティが表示されます。



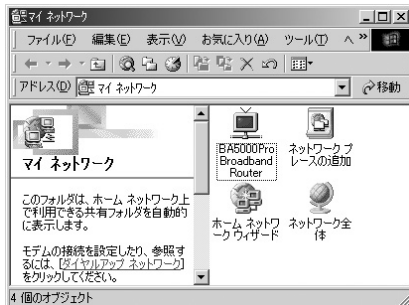
- 3 [接続時に通知領域にインジケータを表示する]にチェックを入れると、ブロードバンド接続中にタスクバー上の通知領域に接続アイコンが表示されます。



UPnP機能の利用 (Windows Meの場合)

マイネットワーク画面

- 1 Windows Me上の [マイネットワーク] 画面に、[BA5000 Pro Broadband Router] というアイコンが表示されます。



- 2 [BA5000 Pro Broadband Router] アイコンを右クリックし、コンテキストメニューから [プロパティ] をクリックすると、本製品のプロパティが表示されます。



- 3 [BA5000 Pro Broadband Router] アイコンをダブルクリックすると、本製品の設定画面が表示されます。

Windows Messenger、MSN Messengerの利用方法

本製品のUPnP機能を有効にしている場合、Windows Messenger、MSN Messengerの利用のための特別な設定は必要ありません。



本製品は、H.323v2プロトコルを使用する音声電話端末/ソフトウェアでの音声通信のルーティングに対応しています。ここではその音声通信を利用するための本製品の設定方法を説明します。



注意

- ・本製品が対応するのは、H.323v2プロトコルを使用した音声通信ですが、H.323v2端末/ソフトウェアはメーカー間で実装が異なります。したがって、すべてのH.323v2通信をサポートするわけではありませんのであらかじめご了承ください。対応サービスは順次弊社ホームページに掲載します。
- ・1個のグローバルIPアドレスサービスの場合、H.323v2通信を利用できるプライベートIPホスト数は1台です。マルチNAT機能を設定します。
- ・複数グローバルIPアドレスサービスで、マルチNAT機能を使っている場合は、マルチNAT機能で設定したプライベートIPホストでH.323v2通信を利用可能です。
- ・複数グローバルIPアドレスサービスで、DMZネットワーク機能を使っている場合は、DMZネットワークに設定したグローバルIPアドレスホストですべてのH.323v2通信を利用可能です。

本製品の設定方法

- ・1個のグローバルIPアドレスサービスの場合
「3-2. サーバ公開/ゲームの利用(マルチNAT)」のページを参照して同じように設定してください。
- ・複数グローバルIPアドレスサービス
マルチNAT機能、またはDMZネットワーク機能を設定してください。DMZネットワーク機能をすでに設定している場合は、他の設定は特に必要ありません。

6.VPNパススルー



本製品は、LAN側に設置したVPN端末とインターネット上のVPN端末間の、VPN通信をサポートします。(VPNパススルー)



注意

- ・対応するVPNプロトコルは、PPTP、L2TP、IPsecです。
- ・1個のグローバルIPアドレスサービスの場合、上記VPNサービスを利用できるプライベートIPホスト数は1台です。マルチNAT機能を設定します。
- ・複数グローバルIPアドレスサービスで、マルチNAT機能を使っている場合は、マルチNAT機能で設定したプライベートIPホストで上記VPNサービスを利用可能です。
- ・複数グローバルIPアドレスサービスで、DMZネットワーク機能を使っている場合は、DMZネットワークに設定したグローバルIPアドレスホストですべてのVPNサービスを利用可能です。その他の設定は特に必要ありません。

本製品の設定方法(マルチNAT機能を利用する場合)

[ルータ設定] - [NAPT] ページ

NAPT設定

アカウント選択

どのアカウントの接続で、VPN通信を利用したいか選択します。

PPTPパススルー機能

有効: NAPT機能が有効の際に、LAN側パソコンでPPTPプロトコルを利用する場合。

無効: 利用しない場合。

L2TPパススルー機能

有効: NAPT機能が有効の際に、LAN側パソコンでL2TPプロトコルを利用する場合。

無効: 利用しない場合。

IPsecパススルー機能

有効: NAPT機能が有効の際に、LAN側パソコンでIPsecプロトコルを利用する場合。

無効: 利用しない場合。

静的マスカレードテーブル

- ・1個のグローバルIPアドレスサービスの場合

「3-2. サーバ公開/ゲームの利用(マルチNAT)」のページを参照して同様に設定してください。

- ・複数グローバルIPアドレスサービス

マルチNAT機能、またはDMZネットワーク機能を設定してください。DMZネットワーク機能をすでに設定している場合は、他の設定は特に必要ありません。

[設定]ボタンをクリックしてください。

設定した静的マスカレードが追加され、本製品が再起動します。

第4章



スタティックルーティングと ダイナミックルーティング

スタティックルーティングとダイナミックの設定を説明します。

1.スタティックルーティング



本製品は、静的な経路情報(スタティックルート)の設定を行うことができます。



注意

- ・宛先ネットワークが存在しなくなった場合、経路上のルータに障害が発生した場合や、間違った経路情報を設定した場合、正常な通信が行われなくなりますので注意してください。
- ・通常のブロードバンドインターネットでは、スタティックルートの設定は不要です。トラブルの原因となりますので特に必要のない限りスタティックルートは設定しないで下さい。

[ルータ設定] - [ルーティング] ページ

スタティックルートテーブル

設定可能経路数 : 16経路

宛先アドレス

宛先ネットワークまたはIPアドレスを表示します。

ネットマスク

宛先アドレス (ネットワーク) のネットマスクを表示します。

ゲートウェイ

宛先アドレス(ネットワーク) へ到達するための、ゲートウェイ(ネクストホップルータ) のIPアドレスを表示します。

メトリック

宛先ネットワーク(ネットワーク) までのディスタンス(ホップ数) を表示します。

プライベート

"Yes" : RIP機能を有効にしている場合でも、この経路情報をRIP送信しません。

"No" : RIP機能を有効にしている場合、この経路情報をRIP送信します。

修正

選択した経路情報を修正します。

削除

選択した経路情報を削除します。

スタティックルートの追加

スタティックルートの追加を行います。

[スタティックルートの追加/修正] ページが表示されます。

[スタティックルートの追加/修正]ページ

スタティックルートの追加を行います。

スタティックルートの追加/修正

宛先アドレス

宛先ネットワークまたはIPアドレスを入力します。

ネットマスク

宛先アドレス (ネットワーク) のネットマスクを入力します。

ゲートウェイ

宛先アドレス (ネットワーク) へ到達するための、ゲートウェイ (ネクストホップルータ) のIPアドレスを入力します。

メトリック

宛先ネットワーク (ネットワーク) までのディスタンス (ホップ数) を入力します。

最大メトリック数 : 15

プライベート

"Yes" : RIP機能を有効にしている場合でも、この経路情報をRIP送信しません。

"No" : RIP機能を有効にしている場合、この経路情報をRIP送信します。

[設定] ボタンをクリックしてください

設定したスタティックルートが追加されます。

4

2. ダイナミックルーティング



本製品はRIPv2をサポートします。近隣のルータが同じくRIPv2をサポートする場合、本製品のダイナミックルーティング機能を使って、経路情報の交換を行うことができます。



注意

- ・本製品はWAN側、LAN側それぞれ別に、ダイナミックルーティング機能の有効/無効を設定することができます。以下では、LAN側のダイナミックルーティング機能の設定方法を説明します。
- ・WAN側のダイナミックルーティング機能の設定は、接続アカウントの設定画面で設定してください。

[ルータ設定] - [ルーティング] ページ

ルーティング設定

LAN側RIP

LAN側ネットワークに対する、本製品のRIP機能の動作を設定します。

- “無効” : LAN側RIP機能を無効にする場合。通常はこれを選択してください。
- “受信のみ” : LAN側ネットワーク上のRIP対応機器から、経路情報の受信のみを行います。本製品が保持するルーティング情報は送信されません。
- “送信のみ” : LAN側ネットワーク上のRIP対応機器に対して、本製品が保持する経路情報を送信します。受信は行いません。
- “送受信” : LAN側ネットワーク上のRIP対応機器と本製品とで、経路情報のやり取りを行います。

[設定] ボタンをクリックしてください

本製品が再起動します。

第5章



セキュリティ

本製品のファイアウォール機能を説明します。

1.ファイアウォール機能



常時外部と通信可能な状態になるブロードバンド環境では、セキュリティを確保することが重要です。ここでは本製品のファイアウォール機能を説明します。

本製品がサポートするファイアウォール機能

・静的フィルタ

パケットのヘッダ情報に基づいたルールにより、入力パケットの通過/破棄を行います。

・ステートフルパケットインスペクション

各々の通信状態(IPアドレスやシーケンス番号)を記憶し、次に来るべきパケットを予測します。受信パケットとその予測を比較・検査した結果、不正なパケットと判断された場合は破棄されます。ヘッダ情報に基づいたパケットの選別のみが行わない、静的なパケットフィルタリングと比較して、より安全なインターネット通信が可能です。

・攻撃検知機能

ネットワーク上のホストに対して高負荷を与える、DoS(Denial of Service: サービス拒否攻撃)などの攻撃を検知し、そのパケットを破棄した上でログに記録します。

・不完全なセッションの増加防止

不完全なセッションの数を把握し、不完全セッションの増加を防ぎます。

付加機能

上記ファイアウォール機能を補完するものとして、本製品は以下のような機能を持ちます。

・ログ機能

syslogデーモン(サーバ)へのsyslogメッセージ送信、ログメール送信、WWWブラウザなどの画面で、本製品の状態を把握することができます。また、攻撃検知機能によりネットワーク攻撃が検知された場合は、管理者に対するログメール通知も可能です。



注意

- ・本製品のファイアウォール機能は、“より安全な”ブロードバンド環境を提供するものです。インターネットからのすべての不正侵入、攻撃に対処することはできませんので、あらかじめご了承ください。
- ・本製品のファイアウォール機能では、ウィルスやワームなどを防御することはできません。また、LAN内での不正行為や攻撃も防御することはできません。あらかじめご了承ください。

2. 静的フィルタ

Trying

パケットのヘッダ情報に基づいたルールにより、パケットの通過/破棄を行います。WAN LAN、LAN WANの2方向のパケットに対してフィルタを適用することができます。



注意

静的フィルタでは、本製品に入ってきたすべてのパケットを、ここで設定したすべてのフィルタと照らし合わせ、そのパケットの通過/破棄を決定します。そのため、設定したフィルタ数が多いほど動作が遅くなる可能性があります。あらかじめご了承ください。

[セキュリティ]-[フィルタ]ページ

フィルタ

フィルタを設定する接続アカウントとフィルタ方向を選択します。

アカウント/方向選択

これまでに設定してある接続アカウントと方向の組み合わせから選択可能です。設定したい、接続アカウントと方向を選択してください。

静的フィルタテーブル

上の[アカウント方向選択]で選択した接続アカウント/方向で、設定してある静的フィルタを表示します。
最大フィルタ数: 64フィルタ(接続アカウント/方向ごと)

ID

静的フィルタのID番号を表示します。小さい番号のフィルタが優先されます。

動作

そのフィルタに該当するパケットが検出された場合の、本製品の処理動作を表示します。

- 通過 : そのフィルタに該当するパケットを通過させます。
- 通過(ログ) : そのフィルタに該当するパケットを通過させ、なおかつその記録をログに残します。
- 破棄 : そのフィルタに該当するパケットを破棄します。
- 破棄(ログ) : そのフィルタに該当するパケットを破棄し、なおかつその記録をログに残します。



注意

多くのフィルタでログ記録を指定した場合や、ログ記録を指定したフィルタに該当するパケットが多い場合、大量のログが生成されることにより本製品の動作が遅くなる、ログ内容が頻繁に書き換わるなどの弊害が発生します。ログ記録するフィルタは極力少なくしてください。

プロトコル

フィルタの対象となるプロトコルを表示します。tcp、udp、tcp&udpの場合は、以下の[フラグ]や[ポート]も関係します。

- * (すべて) : すべてのパケットが対象になります。
- icmp : icmpパケット(pingなど)が対象になります。
- tcp : tcpパケットが対象になります。
- udp : udpパケットが対象になります。
- tcp&udp : tcpとudpパケットが対象になります。

tcpフラグ

上の[プロトコル]欄が「tcp」または「tcp&udp」の場合、ここに示されたすべてのtcpフラグを持つパケットがフィルタの対象になります。指定が無い場合は、フラグの状態は関係ありません。

送信元IPアドレス

フィルタの対象となる送信元IPアドレスを表示します。

送信元IPアドレス例	説明
*	すべてのIPアドレス
19.16.1.3	特定のホスト・アドレス
19.16.1.0/24	ネットワーク・アドレス(24ビットマスク)
19.16.1.3-19.16.1.33	範囲指定 スペース無しでハイフン“ - ”区切り
19.16.1.3,19.16.1.8	列挙指定 スペース無しでコンマ“ , ”区切り

送信元ポート

上の[プロトコル]欄で、「tcp」、「udp」または「tcp&udp」が表示されている場合に、フィルタの対象となる送信元ポートを表示します。

送信元ポート例	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“ - ”区切り
80,8080	列挙指定 スペース無しでコンマ“ , ”区切り

送信先IPアドレス

フィルタの対象となる送信先IPアドレスを表示します。表示形式は送信元IPアドレスと同様です。

送信先ポート

上の[プロトコル]欄で、「tcp」、「udp」または「tcp&udp」が表示されている場合に、フィルタの対象となる送信先ポートを表示します。表示形式は送信元ポートと同様です。

修/削

選択した静的フィルタを修正または削除します。

静的フィルタの追加

静的フィルタの追加を行います。

[静的フィルタの追加/修正]ページが表示されます。

[静的フィルタの追加/修正] ページ

静的フィルタの追加を行います。

静的フィルタの追加/修正

ID

静的フィルタのID番号を入力します。小さい番号のフィルタが優先されますので注意してください。また、既に設定してあるフィルタと同じ番号は使わないで下さい。

動作

そのフィルタに該当するパケットが検出された場合の、本製品の処理動作を選択します。

通過 : そのフィルタに該当するパケットを通過させます。

通過(ログ) : そのフィルタに該当するパケットを通過させ、なおかつその記録をログに残します。

破棄 : そのフィルタに該当するパケットを破棄します。

破棄(ログ) : そのフィルタに該当するパケットを破棄し、なおかつその記録をログに残します。



注意

- ・多くのフィルタでログ記録を指定した場合や、ログ記録を指定したフィルタに該当するパケットが多い場合、大量のログが生成されることにより本製品の動作が遅くなる、ログ内容が頻繁に書き換わるなどの弊害が発生します。ログ記録するフィルタは極力少なくしてください。
- ・異なる接続アカウント/方向や、間違ったフィルタを設定すると、通信に支障をきたす場合があります。フィルタの設定は十分注意して行ってください。

プロトコル

フィルタの対象となるプロトコルを選択します。tcp、udp、tcp&udpの場合は、以下の[フラグ]や[ポート]も関係します。

* (すべて) : すべてのパケットが対象になります。

icmp : icmpパケット(pingなど)が対象になります。

tcp : tcpパケットが対象になります。

udp : udpパケットが対象になります。

tcp&udp : tcpとudpパケットが対象になります。

tcpフラグ

上の[プロトコル]欄が「tcp」または「tcp&udp」の場合、ここで選択したすべてのtcpフラグを持つパケットがフィルタの対象になります。指定が無い場合は、フラグの状態は関係ありません。

送信元IPアドレス

フィルタの対象となる送信元IPアドレスを入力します。

送信元IPアドレス例	説明
*	すべてのIPアドレス
19.16.1.3	特定のホスト・アドレス
19.16.1.0/24	ネットワーク・アドレス(24ビットマスク)
19.16.1.3-19.16.1.33	範囲指定 スペース無しでハイフン“ - ”区切り
19.16.1.3,19.16.1.8	列挙指定 スペース無しでコンマ“ , ”区切り

送信元ポート

上の[プロトコル]欄で、「tcp」、「udp」または「tcp&udp」が表示されている場合に、フィルタの対象となる送信元ポートを入力します。

送信元ポート例	説明
*	すべてのポート
80	特定のポート
80-110	範囲指定 スペース無しでハイフン“ - ”区切り
80,8080	列挙指定 スペース無しでコンマ“ , ”区切り

送信先IPアドレス

フィルタの対象となる送信先IPアドレスを入力します。IPアドレスの指定方法は、送信元IPアドレス例を参照して下さい。

送信先ポート

上の[プロトコル]欄で、「tcp」、「udp」または「tcp&udp」が表示されている場合に、フィルタの対象となる送信先IPポートを入力します。ポートの指定方法は、送信元ポート例を参照して下さい。

[設定]ボタンをクリックしてください

設定した静的フィルタが追加されます。

3.ステートフルパケットインスペクション



ステートフルパケットインスペクション機能を有効にすると、本製品は各々の通信状態（IPアドレスやシーケンス番号）を記憶し、次に来るべきパケットを予測します。受信パケットとその予測を比較・検査した結果、不正なパケットと判断された場合は破棄されます。

ヘッダ情報に基づいたパケットの選別のみしか行わない、静的なパケットフィルタリングと比較して、より安全なインターネット通信が可能です。

本製品のステートフルパケットインスペクションの動作

・TCP通信の場合

ステートフルパケットインスペクションが有効の場合、本製品はTCPセッションの状態、すなわち、送信元IPアドレス、送信先IPアドレス、送信元ポート番号、送信先ポート番号、TCPコネクション状態、シーケンス番号、FTP dataの状態などを記憶しています。これらの状態保存情報から予測される受信パケットと、実際にきたパケットのタイプが異なる場合、不正なものと判断され破棄されます。

・UDP/ICMPの場合

UDPやICMPはコネクションレス型の通信のため状態という概念がありませんが、本製品はNATテーブルの情報に基づいて受信パケットを予測し、実際にきたパケットのタイプと異なる場合、不正なものと判断され破棄されます。

[セキュリティ] - [フィルタ] ページ

ステートフルパケットインスペクションを設定します。

フィルタ

ステートフルパケットインスペクションを設定する接続アカウントとフィルタ方向を選択します。

アカウント/方向選択

これまでに設定してある接続アカウントと方向の組み合わせから選択可能です。ステートフルパケットインスペクションを設定したい、接続アカウントと方向を選択してください。

ステートフルパケットインスペクション

有効：ステートフルパケットインスペクション機能を有効にします。

無効：ステートフルパケットインスペクションを無効にします。

[設定] ボタンをクリックしてください

本製品が再起動します。

One Point!

- ・ステートフルパケットインスペクションを有効にすると、攻撃検知機能も有効になります。
- ・ステートフルパケットインスペクションや、攻撃検知機能のログ生成により、本製品の動作が遅くなる、ログ内容が頻繁に書き換わるなどの弊害が発生する可能性があります。

4. 攻撃検知



ステートフルパケットインスペクション機能を有効にすると、本製品はDoS (Denial of Service) などのインターネット側からの攻撃を検出し、適切な防御を行います。また、不完全なセッションの増加を防ぐ機能も備えています。

本製品で検知できるネットワーク攻撃

本製品はインターネット側からの以下のような攻撃を検知し、防御をするとともにログへの記録を行います。

・Ping of Death

攻撃対象ホストに対して、規格外の巨大な(65536byte以上)Pingを送りつける攻撃です。攻撃対象ホストのシステムダウンを引き起こします。

・TearDrop / Bonk / Boink

攻撃対象ホストに対して、同一内容、またはフラグメントオフセット値が重複する(フラグメント・オーバーラップ)IPフラグメントパケットを連続して大量に送りつける攻撃です。IPフラグメント再構成時に問題を引き起こし、攻撃対象ホストのシステムダウンを引き起こします。

・SYN flood

TCP/IP通信では通常、3ウェイハンドシェイクと呼ばれる手順で、コネクションが確立(established)されます。SYN floodでは攻撃対象ホストに対して、存在しない送信元IPアドレスを持つSYNパケットを連続して大量に送りつける攻撃です。攻撃対象ホストが返すSYN + ACKへの応答が無いため、SYN_RCVD状態のまま資源(メモリなど)を消費してしまい、攻撃対象ホストのシステムダウンを引き起こします。

・LAND

攻撃対象ホストに対して、送信元と送信先が同じSYNパケットを連続して大量に送りつける攻撃です。攻撃対象ホストの無限ループやシステムダウンを引き起こします。

・smurf

攻撃者は、送信先IPアドレスがブロードキャストアドレスであるPing(ICMP Echo Request)を特定のネットワーク送ります。受け取ったネットワークの全ホストは、その送信元IPアドレスに対して応答(ICMP Echo Reply)を送信します。ここで送信元IPアドレスが偽造されていると、大量のICMP Echo Replyが攻撃対象ホストに送信されてしまいます。

・IP Spoofing

送信元IPアドレスのなりすまし(偽造)で、応答パケットの誤配信を招く、SYN floodやLAND、smurfなど多くの攻撃に使用される手法です。

・Port scan

Port scanは、特定のホストでどのようなポートが開いているかを走査する手法です。これ自体は攻撃ではありませんが、攻撃や進入の前段階に行われることが多いのも事実です。

・Code Red

マイクロソフトのInternet Information Server(IIS)の脆弱性を狙うワームです。Web内容の改竄やほかのIISへの感染を行います。

[セキュリティ]-[フィルタ]ページ

攻撃検知機能を設定します。

フィルタ

アカウント/方向選択

これまでに設定してある接続アカウントと方向の組み合わせから選択可能です。攻撃検知機能を設定したい、接続アカウントと方向を選択してください。

ステートフルパケットインスペクション

有効：ステートフルパケットインスペクション機能を有効にします。攻撃検知機能を利用したい場合は、これを選択してください。

無効：ステートフルパケットインスペクションを無効にします。

tcpコネクションタイムアウト

接続要求(syn)パケットから、established状態に移行するまでのタイムアウト時間を指定します。この時間を経過してもestablished状態に移行してないtcpセッションは破棄されます。

工場出荷時値：30秒、設定可能範囲：1～9999秒

tcp finタイムアウト

fin-exchange検出後のセッションタイムアウト時間を指定します。fin-exchange検出後、この時間を経過した場合、そのtcpセッションは破棄されます。

工場出荷時値：1分、設定可能範囲：1～99分

tcpアイドルタイムアウト

tcpセッションのアイドルタイムアウト時間を指定します。この時間、tcpセッションで通信が検出されなかった場合、そのセッションは破棄されます。

工場出荷時値：60分、設定可能範囲：1～99分

udpアイドルタイムアウト

udpセッションのアイドルタイムアウト時間を指定します。この時間、udpセッションで通信が検出されなかった場合、そのセッションは破棄されます。

工場出荷時値：1分、設定可能範囲：1～99分

icmpアイドルタイムアウト

icmpセッションのアイドルタイムアウト時間を指定します。この時間、icmpセッションで通信が検出されなかった場合、そのセッションは破棄されます。

工場出荷時値：1分、設定可能範囲：1～99分

one-minute high

1分間の新規セッションの最大値を指定します。本製品は1分間ごとの新規セッション数を検査し、この値以上になると新規セッションを拒否します。

工場出荷時値：100、設定可能範囲：1～999

max-incomplete high

1 分間の新規half-openセッションの最大値を指定します。本製品は 1 分間ごとのhalf-openセッション数を検査し、この値以上になると新規セッションを拒否します。

工場出荷時値：100、設定可能範囲：1～999

tcp half-openセッション：tcpの3ウェイハンドシェイクが完了しておらず、established状態に移行していないtcpセッションを意味します。

udp half-openセッション：応答パケットが検出されていない状態のudpセッションを意味します。

tcp max-incomplete high

同じ送信先IPアドレスを持つ新規tcpセッションを拒否する、同じ送信先IPアドレスを持つtcp half-openセッション数(1分間のhalf-openセッション数)を指定します。本製品は1分間ごとのtcp half-openセッション数を検査します。この値以上になると、同じ送信先IPアドレスを持つ新規TCPセッションを拒否します。

工場出荷時値：10、設定可能範囲：1～250

ブロッキング

[tcp Max-incomplete high]が指定した値以上になった場合に、一定時間同じ送信先IPアドレスを持つ新規セッションを受け付けるかどうかを選択します。

有効： 同じ送信先IPアドレスを持つ新規tcp half-openセッションを、以下の[ブロッキング時間]の間受け付けません。また、それ以前の同じ送信先IPアドレスを持つtcp half-openセッションは、すべて破棄されます。連続して繰り返されがちな攻撃を防御する場合や、インターネット公開サーバの負荷を軽減する目的で使用してください。

無効： [tcp max-incomplete high] に従った動作のみ行います。

ブロッキング時間

同じ送信先IPアドレスを持つ新規tcp half-openセッションを拒否する時間を分単位で指定します。連続して繰り返されがちな攻撃を防御する目的の場合は長めの時間を、インターネット公開サーバの負荷を軽減する目的の場合は短めの時間を指定してください。

工場出荷時値：1分、設定可能範囲：1-999



あまり長い時間を指定するとインターネット通信に支障が生じてしまう可能性があります。

IP Source Routing

インターネット側からの、“source-route”オプション付きパケットの取り扱いを指定します。始点経路制御により、指定された経路を通るこのパケットは攻撃に使用される恐れがあります。

許可： インターネット側からの、“source-route”オプション付きパケットの通過を許可します。

破棄： インターネット側からの、“source-route”オプション付きパケットの通過を破棄します。

Directed-broadcast

インターネット側からの、Directed-broadcastパケットの取り扱いを指定します。

許可： インターネット側からの、Directed-broadcastパケットの通過を許可します。

破棄： インターネット側からの、Directed-broadcastパケットの通過を破棄します。

ステルスモード

インターネット側から本製品のWAN側ポートに対する、icmp要求（pingなど）への動作を指定します。

有効： icmp要求（pingなど）を無視します。応答もしませんので、pingなどによる攻撃先の存在確認から逃れることができます。

無効： icmp要求（pingなど）に応答します。



注意

- ・ [tcpコネクションタイムアウト] [tcp finタイムアウト] [tcpアイドルタイムアウト] [udpアイドルタイムアウト] [icmpアイドルタイムアウト] [one-minute high] [max-incomplete high] [tcp max-incomplete high] [ブロッキング時間]で、不適切な値を設定すると、通信に支障をきたす可能性があります。必要がない限り絶対に工場出荷時の設定を変更しないで下さい。
- ・ ステルスモードが働くのは本製品WAN側ポートIPアドレスのみです。また、静的マスカレードやマルチNAT設定で、本製品WAN側ポート宛でのicmpや特定ポートパケットをLAN側ホストに転送する設定を行っている場合、icmpやそのポート宛でのパケットも転送されます。それに応答するかどうかは転送先ホストによります。

[設定] ボタンをクリックしてください

設定が保存され、本製品が再起動します。

第6章



管理

本製品のWWW設定画面へのアクセス制限や時刻設定を説明します。

1. 設定画面へのログイン制限



本製品を設定できる管理者を制限する方法を説明します。

設定画面へのログインを制限する目的

本製品には、ブロードバンドアクセスに関する情報やセキュリティ関係の設定が保存されます。これらが不適切に変更されると、ブロードバンド接続に支障をきたすほか、セキュリティ面からも好ましくありません。そこで本製品は、WWWブラウザ設定画面へのログインを制限する方法として以下の2つの設定を行うことができます。

・パスワード制限

WWWブラウザ設定画面を表示する際に要求されるパスワードを設定可能です。パスワードには以下の2種類があります。

管理者パスワード

本製品の設定画面へのログインと、全設定の閲覧・変更・保存が可能なパスワードです。

工場出荷時値：password、設定可能な文字：半角英数字、5文字以上8文字以内

ユーザパスワード

本製品の設定画面へのログインと、全設定の閲覧が可能なパスワードです。ただし、設定の変更・保存はできません。

工場出荷時値：users、設定可能な文字：半角英数字、5文字以上8文字以内

・ログイン許可端末制限

本製品の設定を行うことができるホストを、本製品のLAN側ネットワークのホストにするか、WAN側ネットワークのホストにするかを選択します。さらに、設定可能なホストのIPアドレスを設定することもできます。

[管理設定] - [管理者設定] ページ

設定画面へのアクセス制限機能を設定します。

管理者設定

管理者パスワード

管理者パスワードを変更します。セキュリティのため、ここに入力された値は“*”表示されます。

工場出荷時値：password、設定可能な文字：半角英数字5文字以上8文字以内

管理者パスワード再入力

設定ミスを防ぐため、上の[管理者パスワード]で入力したパスワードを再度そのまま入力します。

工場出荷時値：password、設定可能な文字：半角英数字5文字以上8文字以内

ユーザパスワード

ユーザパスワードを変更します。セキュリティのため、ここに入力された値は“*”表示されます。

工場出荷時値：users、設定可能な文字：半角英数字5文字以上8文字以内

ユーザパスワード再入力

設定ミスを防ぐため、上の[ユーザパスワード]で入力したパスワードを再度そのまま入力します。

工場出荷時値：users、設定可能な文字：半角英数字5文字以上8文字以内

ログイン許可ネットワーク
WAN側LAN側、どちらのネットワークからの設定画面ログインを許可するかどうかを設定します。
工場出荷時値：LAN側ネットワーク

ログイン許可IPアドレス
[ログイン許可ネットワーク]で許可したネットワーク上の、どのIPアドレスのホストからの設定画面ログインを許可するか入力します。ここに入力したホスト以外からの設定画面ログインはできません。
工場出荷時値：*

送信元IPアドレス例	説明
*	すべてのIPアドレス
19.16.1.3	特定のホスト・アドレス
19.16.1.0/24	ネットワーク・アドレス(24ビットマスク)
19.16.1.3-19.16.1.33	範囲指定 スペース無しでハイフン“-”区切り
19.16.1.3,19.16.1.8	列挙指定 スペース無しでコンマ“,”区切り



- ・パスワード欄では、大文字と小文字は別の文字として認識されます。
- ・変更したパスワードは忘れないようにしてください。
- ・特に必要の無い限り、WAN側ネットワークからの設定画面ログインは許可しないで下さい。
- ・「ログイン許可IPアドレス」には、通常「*」（すべて）」を入力しておいてください。「*」（すべて）以外を設定する際は、ログインを許可したいすべてのホストのIPアドレスを入力してください。例えばLAN側、WAN側双方からのログインを許可しても、LAN側のホストのIPアドレスを入力しない限り、LAN側パソコンからのログインはできません。

[設定]ボタンをクリックしてください

本製品が再起動します。再起動後は設定したパスワードでログインしてください。

2.時刻設定



ログ機能などで利用する、本製品の内部時計の時刻を合わせます。

[管理設定] - [時刻設定] ページ

時計の時刻を変更します。

時刻設定

現在の内部時刻

このページ開いた時点の、本製品に記憶されている内部時刻を表示します。

時刻設定方法

時刻設定を自動で行うか、手入力するかを選択します。

工場出荷時値：NTPクライアント

NTPクライアント：NTP(Network Time Protocol)を使い、ネットワーク上のNTPサーバに対する時刻情報問い合わせを行い、内部時刻を調整します。

手動：手動で時刻を設定します。以下の[新しい時刻]欄に現在の正しい時刻を入力してください。

新しい時刻

[時刻設定方法]で「手動」を選択した場合に、現在の正しい時刻を入力します。

タイムゾーン

[時刻設定方法]で「NTPクライアント」を選択した場合に選択します。タイムゾーンとは、そのパソコンが設置されている地域の標準時が、世界標準時と何時間のずれがあるかを示すものです。本製品は日本国内で使用するため、必ず「GMT+09:00」にしてください。

プライマリNTPアドレス

[時刻設定方法]で「NTPクライアント」を選択した場合に、本製品が時刻問い合わせするネットワーク上のNTPサーバアドレスを入力します。

工場出荷時値：210.173.160.87

セカンダリNTPアドレス

[時刻設定方法]で「NTPクライアント」を選択した場合に、本製品が時刻問い合わせするネットワーク上のセカンダリNTPサーバアドレスを入力します。プライマリNTPサーバへの時刻問い合わせに失敗した場合、このサーバに問い合わせず。

工場出荷時値：133.100.9.4

チェック間隔

[時刻設定方法]で「NTPクライアント」を選択した場合に、本製品がネットワーク上のNTPサーバに対して時刻問い合わせする間隔(分単位)を入力します。

工場出荷時値：30分

One Point!

短い間隔で時刻問い合わせると、無駄なネットワークトラフィックが増えてしまいます。



- ・工場出荷時値のNTPサーバ「210.173.160.87」は、独立行政法人通信総合研究所とNTT、IJJ、インターネットマルチフィードが公開している試行サービスのNTPサーバ「ntp3.jst.mfeed.ad.jp」です。(参考：<http://www.jst.mfeed.ad.jp/>)
- ・工場出荷時値のNTPサーバ「133.100.9.4」は、福岡大学情報工学科情報アーキテクチャ部門が公開しているNTPサーバ「drake.nc.fukuoka-u.ac.jp」です。(参考：<http://www.fukuoka-u.ac.jp/>)
- ・上記NTPサーバ公開サービスは、利用者責任でご利用ください。サービスの停止、欠陥、欠陥及びそれらが原因となり発生した損失については、当社およびサービス提供者は一切責任を負いません。
- ・本製品の内部時刻にはずれが生じます。あらかじめご了承ください。
- ・本製品には、時刻情報保持のための電池がなく、NTPサーバ機能もありません。

[設定]ボタンをクリックしてください

本製品が再起動します。

第7章



状態の確認

ログによる情報収集やモニタ機能を説明します。

1. ログ機能



ログ機能を設定します。

本製品のログ機能

本製品は、syslog機能、メールによるログ配信機能、設定画面でのログ表示の、3種類のログ機能で状態を確認することができます。ここではログ出力に関する設定を行います。

・syslog

syslogとは、syslogメッセージ(ログ)を、ネットワーク上に存在するsyslogデーモン(サーバ)に出力する機能です。syslogデーモン側でファイル保存しておくことができ、長期間のログ収集に適しています。本製品のsyslog機能を利用するためには、ネットワーク上にsyslogデーモン(サーバ)が必要です。

Unix系OSの場合 : syslogdをお使いください。

Windows系OSの場合 : Vectorなどの、フリーウェア/シェアウェアサイトで検索してください。ただし、ISDNダイヤルアップルータに特化したソフトウェアは正常に動作しないことがあります。

MAC OSの場合 : Mac NetLoggerなどをお使いください。

(参考 : <http://www.versiontracker.com/moreinfo.fcgi?id=2517>)

[メンテナンス]-[ログ]ページ

ログ機能を設定します。

ログ設定

syslogレベル

syslogメッセージとして出力する情報の種類を選択します。通常は「info」のみチェックしてください。

工場出荷時 : infoのみ



注意

「notice」や「debug」レベルにチェックを入れたると、場合によっては大量のログが生成されることがあり、無駄なトラフィックや本製品の動作が遅くなるなどの弊害が発生します。

syslogサーバIPアドレス

syslogメッセージの送信先になる、syslogデーモン(サーバ)のIPアドレスを入力します。

smtpサーバIPアドレス

本製品はメールによるログ配信も可能です。メールによるログ配信を行う場合は、メールサーバ(SMTP)のIPアドレスを入力してください。ホスト名入力はできません。

宛先メールアドレス

メールによるログ配信を行う場合、宛先メールアドレス(To:)を入力してください。このメールアドレスにログメールが送信されます。

例 : hoge@ntt-me.co.jp

送信元メールアドレス

メールによるログ配信を行う場合、そのメールの送信元メールアドレス(From:)を入力してください。ネットワーク管理者のメールアドレスなどを推奨します。

ログメールの件名

メールによるログ配信を行う場合、そのメールの件名(Subject:)を入力してください。

設定可能な文字: 半角英数字

例: ba5000pro log

ログメール送信トリガ

どのタイミングでログメールを送信するか設定します。以下のオプションから選択してください。

・DoS攻撃検出時

[フィルタ]設定画面で[ステートフルパケットインスペクション]を「有効」にしている状態で、本製品がDoS攻撃を検出した時に、ログメールを送信します。

・メモリー一杯時

ログ情報は本製品のメモリ上に記憶されます。ログが溜まり、メモリに余裕が無くなった時に、ログメール送信します。

・毎日

毎日決まった時間に、ログメールを送信します。送信時刻も入力してください

ログ内容表示

現在のログ内容を表示します。

ログ内容消去

現在本製品のメモリに記憶されているログを消去します。

ログメール送信

メールログを手動で送信します。



注意

ログが溜まりメモリに余裕が無くなった場合、ログ内容は上書きされます。

[設定]ボタンをクリックしてください

本製品が再起動します。

2. モニタ機能



現在の本製品内部の、NAPTセッション(NATテーブル)の状況表示です。

**注意**

たくさんのセッションが存在する場合、この画面に表示しきれない、あるいはセッションモニタページの表示が途中で途切れることがあります。

[メンテナンス] - [モニタ] ページ

NAPTセッションを表示します。

セッションモニタ**送信元IPアドレス**

そのセッションの送信元IPアドレスを示します。

送信元ポート

そのセッションの送信元ポートを示します。

NAPT後のポート

そのセッションのNAPT変換後のポートを示します。

送信先IPアドレス

そのセッションの送信先IPアドレスを示します。

送信先ポート

そのセッションの送信先ポートを示します。

ここでは、特に設定する項目はありません。

第8章



その他

その他の機能について説明します。

1. MACアドレスの変更



本製品WAN側ポートのMACアドレスを表示・変更します。

WAN側ポートMACアドレス変更が必要な理由

通常接続のプロバイダの中には、ケーブルモデムなどに直接接続する機器（パソコンなど）のMACアドレスを申請しないとインターネット接続できないことがあり、それまでケーブルモデムに接続していたパソコンからルータに付け替えると、ブロードバンド通信できなくなってしまいます。

本製品はこのような場合に備え、WAN側ポートのMACアドレス変更が可能です。既にプロバイダに申請しているMACアドレスに変更することで、プロバイダに対して新たに申請し直す必要がなく、すぐにブロードバンド接続することが可能になります。

[管理設定] - [管理者設定] ページ

ログ機能を設定します。

MACアドレス設定

WAN側ポートMACアドレス

現在のWAN側ポートMACアドレスを表示します。変更したい場合は書き換えてください。



注意

- ・特に必要の無い限りMACアドレスの変更は行わないで下さい。
- ・「00:00:00:00:00:00」や「ff:ff:ff:ff:ff:ff」などの特殊なアドレスは入力できません。また、本製品LAN側ポートのMACアドレスや、本製品WAN側ポートと同一セグメント上のホストと同じMACアドレスを入力しないで下さい。

[設定] ボタンをクリックしてください

本製品が再起動します。

2.WWWサービス制限



WWWが実現するサービスの中には便利な機能の反面、多少の危険性を伴うものがあります。より安全なインターネット通信を実現するために、必要がないサービスを利用できなくすることもセキュリティを高める方法です。

本製品で制限できるWWWサービス

・ActiveX

Webサーバからダウンロードしたプログラムをクライアントで実行することで、インタラクティブな動的コンテンツやデータベース運用などを実現する仕組みです。システムにダメージを与えるコードが含まれている可能性があります。

・Java

ActiveXと同様に、プログラムをWebページに埋め込む目的で使用されています。システムにダメージを与えるコードが含まれている可能性があります。

・Cookie

インターネット上での匿名性を重視する場合は、Cookieをブロックします。Cookieとは、Webサイトを訪問した際に、サーバがクライアントのハードディスクに書き込み・検索する、小さな情報ファイルです。ユーザ情報を記憶しておき、面倒な入力作業なしでその人のためのページを表示する目的などに使われます。

・Proxy

インターネット上にあるWeb Proxyを利用できなくします。コンテンツフィルタなどを使用している場合に有効にしてください。



注意

- ・通常のインターネット通信に支障をきたす恐れがあります。いずれも便利な機能ですのでよく考えて設定してください。また、WWWサービス制限を設定した後に利用できなくなった安全なWebサイトがある場合は、制限を解除してください。
- ・Cookieをブロックすると、WebサーバによるCookieの設定や検索が不可能になり、会員ページなどが利用できなくなります。また、JavaScript経由のCookieはブロックできません。
- ・これらの制限はWWWブラウザの詳細設定でも可能です。パソコンごとに制限を変えたい場合は、各パソコンのWWWブラウザで設定してください。
- ・WWWサービス制限機能を有効にすると、本製品の処理が遅くなる可能性があります。

[管理設定] - [管理者設定] ページ

WWWサービス制限を設定します。

WWWサービス制限

制限する機能

ここで選択したWWWサービスは、LAN側ホストで利用できなくなります。

工場出荷時設定：(選択なし)

[設定] ボタンをクリックしてください

本製品が再起動します。

3.Pingによる導通確認



本製品から特定のIPアドレス宛てに、Ping(ICMP Echo Request)を送出することができます。導通確認に用いてください。

[メンテナンス] - [更新/設定情報] ページ

Pingを送出します。

Ping試験

Ping送出先IPアドレス

本製品から送出したいPing送出先IPアドレスを入力し、[送出]ボタンをクリックします。結果は設定画面に表示されます。

ここでは、特に設定する項目はありません。

第9章



ファームウェアと設定情報

ファームウェアの更新と設定情報保存、本製品のリセットの方法を説明します。

1.ファームウェアの更新



本製品はファームウェアを更新することで、機能追加や不具合修正などの変更を行うことができます。



警告

- ・ファームウェアを更新すると、それまでの設定内容が工場出荷時状態に初期化される場合があります。詳細は各ファームウェアファイルに付属の「readme」を参照してください。
- ・アップグレード作業はお客様自身の責任で行ってください。アップグレード作業を起因とする故障・誤作動・不具合・通信不良や、通信などの機会を逃したために生じた損害などの純粹経済損失につきましては、当社は一切その責任を負いかねますのであらかじめご了承ください。
- ・アップグレード作業中は、ネットワーク上の機器の電源やケーブルを抜かないでください。また、アップグレード作業中は不必要なキーボード操作などは行わないでください。ファームウェアの書き込みに失敗することがあります。
- ・必ずLAN側ポートに接続されたネットワーク上のコンピュータを使って、アップグレードしてください。WAN側ポートからはアップグレードすることはできません。
- ・ファームウェアの更新を行う場合は、あらかじめBAシリーズ製品情報ページから、現在のファームウェアバージョンより新しいファームウェアバイナリファイルをダウンロードしておいてください。
- ・ファームウェアの更新には数十秒ほど時間がかかります。更新中に、本製品の電源を落としたり、ネットワークケーブルをコネクタから外したりしないで下さい。本製品が破壊される可能性があります。

[メンテナンス] - [更新/設定情報] ページ

ファームウェア更新

現在のファームウェアバージョン

現在の本製品のファームウェアバージョンを表示します。

新しいファームウェアファイル

ファームウェアを書き換えます。[参照]ボタンを押して、パソコンに保存しておいたファームウェアファイル(xxx.bin)を選択してから、[アップグレード]ボタンを押してください。

2. 設定情報の保存と読み込み



本製品の設定情報をパソコンにファイルとして保存、または以前保存した設定情報を本製品に書き込みます。



警告

- ・ファームウェアを更新すると、更新以前の設定情報ファイルを読み込めない場合があります。詳細は各ファームウェアファイルに付属の「readme」を参照してください。
- ・設定情報を読み込むと、ログインパスワードやLAN側ポートIPアドレスも、その設定情報を保存した時点のものに置き換わります。設定画面にアクセスするIPアドレスやパスワードが変わることもありますので注意してください。
- ・設定情報の読み込みには数十秒ほど時間がかかります。読み込み中に、本製品の電源を落としたり、ネットワークケーブルをコネクタから外したりしないで下さい。本製品が破壊される可能性があります。

[メンテナンス]-[更新/設定情報]ページ

設定情報の保存と読み込み

設定情報の保存

[保存]ボタンを押すと、現在の設定内容をパソコンにファイルとして保存することができます。

設定情報の読み込み

以前保存した設定情報を読み込む場合は、「参照」ボタンを押して設定情報ファイル名を選択し、「読み込み」ボタンを押してください。

3. 設定情報の消去(設定画面経由)



間違った設定を保存してしまった場合や、すべての設定情報を消去したい場合など、本製品を工場出荷時の状態に戻したいときも、WWWブラウザの設定画面から簡単に行うことができます。



注意

- ・設定内容の消去を行うと、それまでに設定した内容が消去され、工場出荷時状態に初期化されます。再度設定しなおす際に備えて、重要な情報はメモをとっておいてください。
- ・設定情報の消去を行った場合は、再度適切な設定を行ってください。

[メンテナンス] - [更新/設定情報] ページ

設定情報の消去

設定情報の消去

設定情報を消去して工場出荷時の状態に戻す場合は、[消去]ボタンを押してください。

4. 設定情報の消去(外部から)



間違った設定を保存した場合など、本製品の設定画面にログインできなくなることがあります。このような場合は、本製品付属CD-ROM内の初期化ユーティリティを使って、本製品を工場出荷時の状態に戻すことができます。



注意

- ・ 設定内容の消去を行うと、それまでに設定した内容が消去され、工場出荷時状態に初期化されます。再度設定しなおす際に備えて、重要な情報はメモをとっておいてください。
- ・ 設定情報の消去を行った場合は、再度適切な設定を行ってください。
- ・ 必要がない限り、設定情報の消去は行わないで下さい。

ユーティリティの内容と目的

・ Windows用初期化ユーティリティ

Windows/パソコンにインストールして、本製品を工場出荷時の状態にします。

対応OS : Windows 95/98/Me/XP/2000/NT

・ Mac用初期化ユーティリティ

Macintosh/パソコンにインストールして、本製品を工場出荷時の状態にします。

対応OS : Mac OS 8.x/9.x/10.x

Windows/パソコンで初期化ユーティリティを使う

1 リファレンスマニュアル/ユーティリティ CD-ROMを、CD-ROMドライブに挿入してください。

CD-ROMが自動再生され初期画面が表示されます。

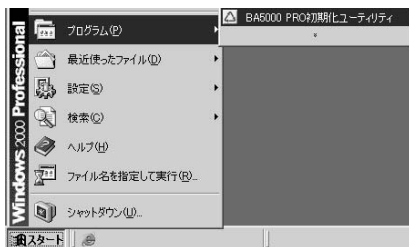
CD-ROMが自動再生されなかった場合は、3を参照してください。

2 初期画面の案内にしたがって、Windows用初期化ユーティリティセットアップファイルを、パソコンのハードディスクにダウンロードします。

ファイル名：
b5prst10.exe (バージョン1.0の場合)



3 ダウンロードしたファイルをダブルクリックし、インストールを開始します。案内にしたがってインストール作業を進めてください。CD-ROMが自動再生されなかった場合は、CD-ROMドライブ内の[Utility] - [Win] フォルダの、「b5prst10.exe」をダブルクリックしてください。インストールが完了すると、スタートメニューの[プログラム]に、「BA5000 Pro初期化ユーティリティ」が登録されます。



4 パソコンと本製品のLAN側ポートがネットワークケーブルで正しく接続されており、本製品の電源が入っていることを確認します。

5 「BA5000Pro初期化ユーティリティ」を起動してください。本製品を工場出荷時の設定に戻したい場合は、[初期化を実行]ボタンをクリックします。



6 本製品が初期化されます。

アンインストール方法
「BA5000Pro初期化ユーティリティ」をアンインストールする場合は、[コントロールパネル] - [アプリケーションの追加と削除] から行ってください。

MacOS で初期化ユーティリティを使う

1 リファレンスマニュアル/ユーティリティ CD-ROMを、CD-ROMドライブに挿入してください。

2 CD-ROMドライブ内のmenu.htmlを開き、画面の案内に従って下さい。

第10章



その他

1.IP設定とMACアドレスの確認



本製品を利用してブロードバンド接続するためには、正しいIP設定をパソコンに施す必要があります。ここでは、パソコンのIP設定とMACアドレスの確認を行います。

また、本製品のDHCPサーバ機能を利用している場合は、IPアドレスここで更新することも可能です。

パソコンのIP設定の確認項目

・IPアドレス

パソコンのIPアドレスが、本製品のLAN側IPアドレスや他のパソコンと重複していないか、ネットワークアドレスやブロードキャストになっていないか確認します。

・サブネットマスク

本製品と同じサブネットマスクになっている必要があります。

・デフォルトゲートウェイ

通常、本製品のLAN側IPアドレスになっている必要があります。

・DNSサーバIPアドレス

本製品のProxyDNS機能を利用している場合

DNSサーバIPアドレスが、本製品のLAN側IPアドレスになっている必要があります。

ProxyDNS機能を利用していない場合

プロバイダのDNSサーバIPアドレスになっている必要があります。

・DHCPサーバ

本製品のDHCPサーバを利用している場合、DHCPサーバIPアドレスが、本製品のLAN側IPアドレスになっている必要があります。

・ドメイン名

ドメイン名設定が必要なプロバイダの場合、パソコンが所属するドメインも指定されたドメイン名になっている必要があります。

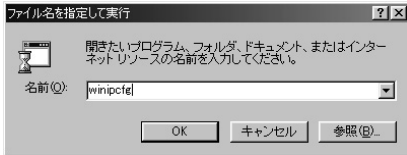
One Point!

DHCPサーバ機能、ProxyDNS機能、ドメイン名設定については、「BA5000 Proマニュアル 接続編」を参照してください。

Windows 95/98/Meの場合

1 スタートメニューから、[ファイル名を指定して実行]をクリックしてください。[ファイル名を指定して実行]ダイアログボックスが表示されます。

2 [名前(O):]欄に、「winipcfg」と入力して [OK]ボタンをクリックします。



[IP設定]画面が表示されます。

3 一番上のリストボックスから、使用しているLANアダプタを選択した後、[詳細]ボタンをクリックします。そのパソコンのIP設定の詳細とMACアドレス(アダプタアドレス)が表示されますので確認してください。



One Point!

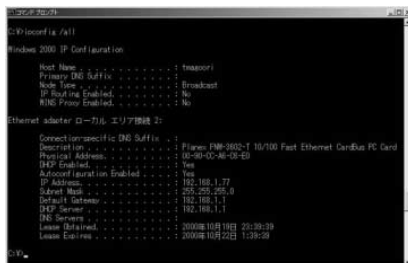
DHCPサーバ機能を利用している場合

本製品のDHCPサーバ機能を利用している場合は、ここでIP設定を更新することができます。[開放]ボタンをクリックして、IPアドレスを返上した後、[更新]ボタンをクリックしてください。[更新]ボタンをクリックすると、本製品のDHCPサーバからIP設定を取得しなおします。

Windows 2000/NT/XPの場合

- 1 コマンドプロンプトから、以下のコマンドを実行します。
ipconfig /all

- 2 そのパソコンのIP設定の詳細が表示されます。「Ethernet adapter」の後に続く接続名が、本製品を利用する接続名であることを確認の上、IP設定内容とMACアドレス(Physical Address)を見ます。



```
Windows 2000 IP Configuration:

Host Name . . . . . : msasoft
Primary DNS Suffix . . . . . :
Node Name . . . . . :
NetBIOS Over LAN Card . . . . . :
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter ローカル エリア接続 2:

Connection-specific DNS Suffix . . . :
Description . . . . . : Planex PAM-3602-T 10/100 Fast Ethernet Card
Physical Address . . . . . : 80-40-0C-9E-09-E9
DHCP Enabled . . . . . : Yes
Autotunneling Enabled . . . . . : Yes
IP Address . . . . . : 192.168.1.77
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . :
Lease Expires . . . . . : 2008/10/11 20:28:30
Lease Expires . . . . . : 2008/10/11 20:28:30
```

One Point!

DHCPサーバ機能を利用している場合

本製品のDHCPサーバ機能を利用している場合は、ここでIP設定を更新することができます。以下のコマンドを実行してください。

- ipconfig /release : DHCPサーバへIPアドレスを返します。
- ipconfig /renew : 本製品のDHCPサーバからIP設定を取得しなおします。

2. メール送受信に時間がかかる場合

Trying

本製品を利用してブロードバンド通信している際、メールの送受信に時間がかかるケースがあります。このような現象への対処方法を説明します。

メールの送受信に時間がかかる理由

メールサーバによっては、メールクライアント側のホストに対しident(tcp 113番)というプロトコルを使って、クライアントの存在確認をするものがあります。このようなメールサーバでident要求がタイムアウトするまでメールの送受信を受けつけない仕様になっている場合、本製品はidentを破棄しますので、メールの送受信に時間がかかることになります。

解決方法

ローカルサーバ機能で、tcp 113番をLAN側ホストに転送する設定を行ってください。またはマルチNAT機能で転送先が不明なすべてのWAN側からの通信をLAN側ホストに転送する設定を行ってください。

One Point!

- ・転送先のLAN側ホストは、実在するホストであればどれでもかまいません。
- ・不具合が起こる同じメールサーバを複数パソコンで利用している場合は、1日の中で稼働時間がもっとも長いホストに転送する設定を行ってください。

3.NetBIOSフィルタ



Windowsネットワークにおいて、攻撃に利用されがちなNetBIOS関係のポートを以下に示します。一般的に、インターネット上では利用しないサービスですので、LAN WAN方向、WAN LAN方向の両方のフィルタを設定することをお勧めします。

プロトコル	ポート	用途
tcp/udp	135	DCE準拠RPC
udp	137	NetBIOS名前解決
udp	138	データグラム転送
tcp	139	ストリームデータ転送
tcp/udp	445	SMB Direct Hosting

4.トラブルシューティング

Power LEDが点灯しない。
専用ACアダプタは正しく接続されていますか？
電源ケーブルにキズやねじれはありませんか？
Status LEDが長時間点滅を繰り返す。
電源を再投入しても同じ症状が出る場合は、故障の可能性があります。BAサポートセンターまでご連絡ください。
WAN Link LEDが点灯しない。
WAN側ポートとxDSL/ケーブルモデム/FTTH装置は、ネットワークケーブルで正しく接続されていますか？
xDSL/ケーブルモデム/FTTH装置の電源は入っていますか？
WAN側ポートUplinkスイッチを切り替えてみてください。
ネットワークケーブルにキズやねじれはありませんか？
LAN Link LEDが点灯しない。
LAN側ポートとパソコンは、ネットワークケーブルで正しく接続されていますか？
パソコンの電源は入っていますか？
ネットワークケーブルにキズやねじれはありませんか？
WWW設定画面にアクセスできない。表示がおかしい。
WWWブラウザのリロードボタンで再度アクセスしてみてください。
[アカウント管理]、[モニタ]画面、[フィルタ]画面は、表示に若干時間がかかります。
WWWブラウザのプロキシ設定を解除してください。
JavaScriptとFrame表示に対応したWWWブラウザを使用してください。
パソコンやLAN側ポートと、IPアドレスが重複するホストはありませんか？
パソコンのIP設定を確認してください。(参考:「10.1 IP設定とMACアドレスの確認」ページ)
パソコンを再起動してみてください。
本製品のDHCPサーバ機能を利用している場合、IP設定を更新してみてください。(参考:「10.1 IP設定とMACアドレスの確認」ページ)
ログインパスワードは、大文字・小文字を区別して正しく入力していますか？
ログインパスワードを変更していませんか？
ネットワークやIPアドレスで、設定画面へのログイン制限を有効にしていないですか？この場合、許可されたネットワークの、許可されたホストからしかログインできません。(参考:「6.1 設定画面へのログイン制限」)
インターネットに接続できない。(通常接続)
もう一度通常接続設定を確認してください。
[アカウント管理]画面 - [接続方式の選択]は「通常接続」になっていますか？
パソコンのIP設定を確認してください。(参考:「10.1 IP設定とMACアドレスの確認」ページ)
DHCPサーバ有効の場合、IP設定を更新してみてください。(参考:「10.1 IP設定とMACアドレスの確認」ページ)
DHCPサーバ無効/ProxyDNS無効の場合、すべてのパソコンのDNS設定をプロバイダ指定のDNSサーバにする必要があります。
DHCPサーバ無効/ProxyDNS有効の場合、すべてのパソコンのDNS設定を本製品LAN側IPアドレスにする必要があります。
間違ったフィルタを設定していませんか？
プロバイダからドメイン名やホスト名を指定されている場合は、本製品に設定してください。
インターネットに接続できない。(PPPoE接続)
もう一度PPPoE接続設定を確認してください。
[アカウント管理]画面 - [接続方式の選択]は「PPPoE接続」になっていますか？
[アカウント管理]画面 - [PPPoEアカウントリスト]で、利用したいPPPoEアカウントに「プライマリ1」を設定していますか？
セカンダリセッションも利用している場合は、[アカウント管理]画面 - [セカンダリセッション接続ルール]を再確認してください。
PPPoEユーザ名とPPPoEパスワードは、大文字・小文字を区別して正しく入力していますか？
DHCPサーバ有効の場合、IP設定を更新してみてください。(参考:「10.1 IP設定とMACアドレスの確認」ページ)
DHCPサーバ無効/ProxyDNS無効の場合、すべてのパソコンのDNS設定をプロバイダ指定のDNSサーバにする必要があります。
DHCPサーバ無効/ProxyDNS有効の場合、すべてのパソコンのDNS設定を本製品LAN側IPアドレスにする必要があります。
セカンダリセッションも利用する場合は、ProxyDNSを有効にしてください。DHCPサーバが無効の場合は、すべてのパソコンのDNS設定も本製品LAN側IPアドレスにする必要があります。
間違ったフィルタを設定していませんか？
特定のネットワークソフトウェア/ゲームが利用できない。
そのソフトを利用するパソコンに対する、マルチNATがローカルサーバ機能を設定してください。(参照:3.2「サーバ公開/ゲームの利用(マルチNAT)」)
マルチNATやローカルサーバ機能を利用して、一部のネットワークソフトウェア・ネットワークゲームは機能しません。
メールの送受信に時間がかかる。
「10.2 メール送受信に時間がかかる場合」を参照してください。

株式会社 エヌ・ティ・ティ エムイー