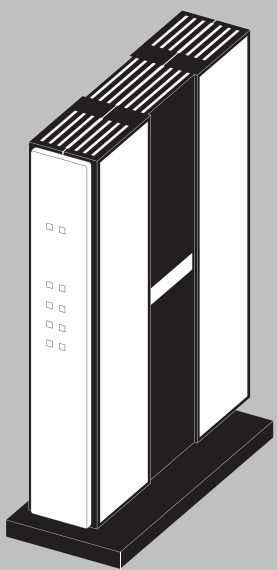
NTT-ME

MN8300

高速ブロードバンドルータ
マニュアル

このたびは、MN8300 をお買い上げいただき、まことにありがとうございます。

- 本書では MN8300 をご導入いただく際の設置や接続の方法、設定の方法等について説明しています。MN8300 を正しくお使いいただき、十分にご活用いただくためにも、必ずお読みいただくようお願いいたします。
- お読みになったあとも、本商品のそばなどいつも手もとに置いてお使いください。



第 2 版

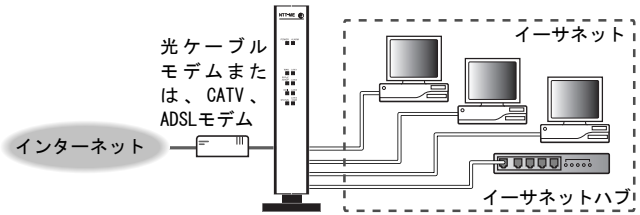
特　長

1. 光アクセスサービス、ADSL/CATV サービス対応

光アクセスサービス、ADSL/CATV サービスに対応しています。また PPPoE 接続方式にも対応しています。

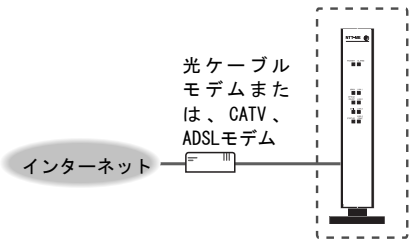
2. 余裕のスループット 100Mbps

高スループットで快適なインターネット接続環境がご利用できます。



3. PPPoE マルチセッション対応

1 つのブロードバンド回線で、同時に最大 8 セッションの PPPoE 接続が利用できます。また、複数のプロバイダへの同時接続が可能です。フレッツ®・スクウェアなどにも対応しています。



4. UPnP(Universal Plug and Play)対応

MSN® Messenger Ver.5.0/6.1 以降、Windows Messenger Ver.4.7 以降の音声／ビデオチャットなどのアプリケーションを簡単な設定でご利用いただくことができます。また、PPPoE サブセッションに対しても UPnP 対応しています。

5. LAN 型 PPPoE 接続対応

複数のグローバル IP アドレスを取得して LAN 内で利用する接続形態に対応しています。また、通信回線側に IP アドレスを割り当てないアンナンバード方式にも対応しています。

6. DMZ ポート搭載

LAN4 ポートを DMZ ポートとして利用できます。GapNAT/マルチ GapNAT 利用時にグローバル IP アドレスの割り当てられるセグメントを DMZ ポート（LAN4）に固定できます。これにより、DMZ ポートを LAN ポートと切り離し、外部からの接続をすべて DMZ ポートに転送することで高いセキュリティ環境を構築することができます。

7. GapNAT/マルチ GapNAT 機能搭載

プロバイダから割り当てられたグローバル IP アドレスを LAN 側の端末に割り当てることができます。グローバル IP アドレス端末とプライベートアドレス端末の混在ネットワークが簡単に構築できます。サーバ公開やネットワーク対戦ゲームに便利です。また、マルチ GapNAT では 8/16/32 個のグローバル IP アドレスに対応できます。

8. 多彩なセキュリティ機能搭載

「ステルスモード」、「ステートフル・パケット・インスペクション」、「パケットフィルタリング（ワンタッチフィルタ）」、「NAT＋IP マスカレード（ワンタッチ NAT）」、「DMZ」などルータとしての充実したセキュリティ機能を搭載しています。

9. ダイナミック DNS 対応

固定のグローバルアドレスを持っていない場合でも、ダイナミック DNS 機能を利用することで、公開サーバに自分のドメイン名を使って、外部からアクセスすることができます。

10. PPTP、L2TP、IPsec パススルー対応

LAN 側のネットワークと WAN 側のネットワークで VPN(Virtual Private Network)通信をサポートします。PPTP、L2TP、IPsec を利用した VPN を構築することができます。

11. シンプル WWW 設定

設定は、WWW ブラウザの設定画面に入力するだけの簡単設定です。
「ユーザ ID」、「パスワード」、「フレッツ・スクウェア使用の有無」などを入力するだけで、プリセットされた設定内容が自動的に設定される「おまかせ設定」と、機能ごとに詳細な設定が可能な「詳細設定」の 2 つのモードで設定が可能です。

【商標／登録商標について】

- 「フレッツ」は東日本電信電話株式会社と西日本電信電話株式会社の登録商標です。
- Netscape Navigator は、米国およびその他の諸国の Netscape Communications Corporation 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。
- Mac、Macintosh、MacTCP は、米国アップルコンピューター社の米国およびその他の国における登録商標または商標です。
- Microsoft、MSN、Windows、Windows NT、DirectX および Xbox は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- インテルは、アメリカ合衆国およびその他の国における Intel Corporation またはその子会社の登録商標です。
- GapNAT は住友電気工業株式会社の商標です。
- その他記載の会社名・商品名等は、各会社の商標または登録商標です。
- 本製品の OS には、米国 Wind River Systems, Inc.の VxWorks を採用しています。本製品に搭載されているソフトウェアのリバースエジニアリング、コピー、転売、改造を行うことを禁止します。
- This product includes software developed by the Apache Software Foundation (http://www.apache.org/).Copyright (C) 1993-2002 by Darren Reed.
  Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory.
  Funded under Grant P41-RR02188 by the National Institutes of Health.
  Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.
  Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002 Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000,2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

【略称について】

- Windows®95 の正式名称は、Microsoft®Windows®95 Operating System です。（以下 Windows 95）
- Windows®98 の正式名称は、Microsoft®Windows®98 Operating System です。（以下 Windows 98）
- Windows®Me の正式名称は、Microsoft®Windows®Millennium Edition Operating System です。（以下 Windows Me）
- Windows®2000 の正式名称は、Microsoft®Windows®2000 Professional または Microsoft® Windows®2000 Server です。（以下 Windows 2000）
- Windows®XP の正式名称は、Microsoft®Windows®XP Professional または Microsoft®Windows® XP Home Edition です。（以下 Windows XP）
- Windows NT®、Windows NT®4.0 の正式名称は、Microsoft®Windows NT®Workstation Operating System Version 4.0 および Microsoft®Windows NT®Server Network Operating System Version4.0 です。（以下 Windows NT4.0）
- Microsoft Corporation のガイドラインにしたがって画面写真を使用しています。
- 本書では光ケーブルモデム、ADSL モデム、または CATV モデムのことをモデムと呼んでいます。
- Windows/MSN®Messenger の正式名称は Windows Messenger と MSN®Messenger です。本書では Windows Messenger のみを有する機能について説明する場合でも Windows/MSN®Messenger と表記していますが、Windows Messenger と MSN®Messenger では、バージョンによって有する機能が異なりますのでご注意ください。
- UPnP™は、Universal Plug and Play の略称です。
- IGD とは、UPnP フォーラムで定義された Internet Gateway Device を意味します。

目　次

1 ご使用の前に

安全にお使いいただくために

⚠	警告	この表示の欄は、「死亡または重傷などを負う可能性が想定される」内容です。
⚠	注意	この表示の欄は、「傷害を負う可能性または物的損害のみが発生する可能性が想定される」内容です。
注意	お願い	この表示を無視して、誤った取り扱いをすると、本商品の本来の性能を発揮できなかったり、機能停止を招く内容を示しています。
Memo	お知らせ	この表示は、本商品を取り扱ううえでの注意事項を示しています。

⚠ 警告

- **ACアダプタのコードやプラグを破損しないでください。**
  ACアダプタのコードやプラグを傷つけたり、加工したり、熱器具に近づけたり、無理に曲げたり、ねじったり、引っ張ったり、重い物を載せたり、束ねたりしないでください。
  ACアダプタのコードやプラグを傷んだまま使用すると、感電・ショート・火災の原因になります。
- **ACアダプタのプラグのほこりなどは定期的にとってください。**
  プラグにほこりなどがたまると、湿気などで絶縁不良となり、火災の原因になります。ACアダプタをコンセントから抜き、乾いた布でふいてください。
- **ぬれた手でACアダプタの抜き差しはしないでください。**
  感電の原因になります。
- **ACアダプタのプラグは根元まで確実に差し込んでください。**
  差し込みが不完全だと、感電や発熱による火災の原因になります。傷んだプラグ・ゆるんだコンセントは使用しないでください。
- **コンセントや配線器具の定格を超える使いかたや、交流100V 以外での使用はしないでください。**
  たこ足配線などで、定格を超えると、発熱による火災の原因になります。
- **専用のACアダプタ（極性統一プラグ）以外は使わないでください。**
  専用以外のACアダプタを使用すると、電圧や＋－の極性が異なっていることがあるため、発煙・火災のおそれがあります。
- **ACアダプタを抜き差しするときは本体（金属でない部分）を持ってください。**
  感電の原因になります。
- **心臓ペースメーカーの装着部位から22cm以上離してください。**
  電波によりペースメーカーの作動に影響を与える場合があります。
- **自動ドア、火災報知器などの自動制御機器の近くには設置しないでください。**
  本機器からの電波が自動制御機器に影響を及ぼすことがあり、誤動作による事故の原因になります。

⚠ 警告

- **医用電気機器の近くでの設置や使用をしないでください。**
  手術室、集中治療室、CCU※等には持ち込まないでください。本機器からの電波が、医用電気機器に影響を及ぼすことがあり、誤動作による事故の原因になります。
  ※CCUとは、冠状動脈疾患監視病室の略称です。
- **本機器や、ACアダプタをぬらさないでください。**
  近くに花びん、コップなどを置かないでください。発火・感電の原因になります。ぬらした場合は、ACアダプタを抜いて技術サポートセンターへご連絡ください。
- **本機器やACアダプタから煙・異臭・異音が出たり、落下などにより破損したときは使用を中止してください。**
  そのまま使用すると、火災や感電の原因になります。ACアダプタを抜いて技術サポートセンターへご連絡ください。
- **本機器内部や、ジャック、ポートにクリップやピンなどの金属物や異物を入れないでください。**
  火災・感電の原因になります。
- **本機器を分解したり、修理・改造をしないでください。**
  故障したり、火災・感電の原因になります。
- **落下させたり、強い衝撃を加えないでください。**
  故障やけがの原因になることがあります。
- **雷が鳴ったら本機器やACアダプタに触れないでください。**
  感電の原因になります。落雷などのおそれがあるときは、必ずACアダプタをコンセントから抜いて、ご使用を控えてください。場合によっては感電や故障のおそれがあります。

⚠ 注意

- **水平でない場所や振動の激しい場所には設置しないでください。**
  落下により、けがの原因になることがあります。
- **火気を近づけないでください。**
  火災の原因になることがあります。
- **水、湿気、ほこり、油煙などの多い場所（調理台や加湿器のそばなど）に設置しないでください。**
  故障や感電・ショートの原因になることがあります。
- **通気孔をふさぐような設置はしないでください。**
  熱がこもり、火災や故障の原因になります。
- **ケーブルを曲げたり落としたり、強い衝撃を与えたりしないでください。**
  故障・変形・破損や感電の原因になることがあります。
- **ケーブルを引っぱったり、コネクタ部に無理な力を加えないでください。**
  損傷や感電の原因になることがあります。

正しくお使いいただくために

使用・設置場所について

⚠ 注意

● 長時間直射日光の当たるところや、冷・暖房器の近くなどに設置しないでください。（変形・変色または故障・誤動作の原因になります。）
● 本機器は、涼しくて湿気が少なく、なるべく温度が一定の場所に設置してください。 動作温度：5℃～40℃ 動作湿度：5%～85% （結露しないこと）

ご使用について

⚠ 注意

● ジャック、ポートに触れないでください。（故障の原因になります。）
● 隣接して使用しているラジオやテレビから2m以上離してくださいまた、同一コンセントでご使用の場合は、コンセントを別にしてください。（ラジオやテレビに雑音が入ることがあります。）
● 長時間使用しないときや、お手入れするときは、必ず電源プラグをコンセントから抜いてください。（漏電・感電の原因になることがあります。）

日頃のお手入れについて

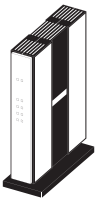
⚠ 注意

- ベンジンやシンナー、研磨剤などを使って本機器を拭かないでください。柔らかい乾いた布をお使いください。（本機器が変形・変色することがあります。）
- 隣接して使用しているラジオやテレビから 2m 以上離してください。また、同一コンセントでご使用の場合は、コンセントを別にしてください。（ラジオやテレビに雑音が入ることがあります。）

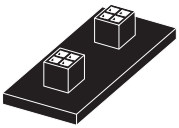
- 本機器は日本国内用です。国外での使用に対するサービスは致しかねます。
  This product is designed for use in Japan.
  NTT-ME cannot provide service for this product if used outside Japan.
- 本機器の故障・誤作動・不具合・通信不良、あるいは停電、落雷などの外的要因によって、通信などの機会を逃したために生じた損害などの純粋経済損失につきましては、当社は責任を負えない場合もございますのであらかじめご了承ください。
- 通信内容の漏洩による経済的・精神的損害につきましては、当社は責任を負えない場合もございますので、あらかじめご了承ください。
- 本機器は、プロバイダから付与されるインターネットアクセスアカウント1つで、複数端末からのインターネットアクセスを実現する機能を搭載しています。ただし、プロバイダによってはインターネットにアクセス可能な端末台数を制限、あるいは台数によって別途追加料金を設定している場合があります。本機器をインターネットアクセスに用いる際は、ご契約プロバイダとの約款の範囲内でのご利用をお願いいたします。
- この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。
-
- 本書の内容は、将来予告なしに変更する場合があります。
-

本体と付属品の確認

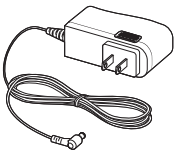
ご使用いただく前に、次の付属品がそろっているか確認してください。
万一、不足の品がありましたら、お手数ですがお買い上げの販売店または技術サポートセンターまでご連絡ください。



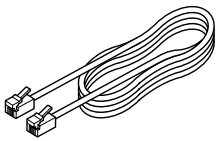
□MN8300
本体　1 台



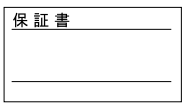
□スタンド　1 個



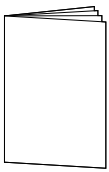
□AC アダプタ　1 個



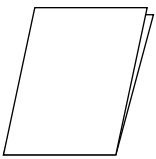
□LAN ケーブル 1 本
（ストレート カテゴリ 5 長さ：約 2m）



□保証書　1 部



□マニュアル（本書）1 冊



□インターネット接続ガイド　1 枚

[奨励パソコン環境]

本機器の設置には、下記のパソコンやソフトウェアを準備してください。

	Windowsパソコン	Macintoshパソコン
インタフェース	イーサネットインタフェース イーサネットケーブル	イーサネットインタフェース イーサネットケーブル
メモリ	16MB以上	16MB以上
プロトコル	TCP/IPプロトコルが実装されていること	Open Transport 1.3 以降が実装されていること
WWWブラウザ	Internet Explorer 5.0以降、または、Netscape Navigator 6.2以降	Internet Explorer 5.0以降、または、Netscape Navigator 6.2以降

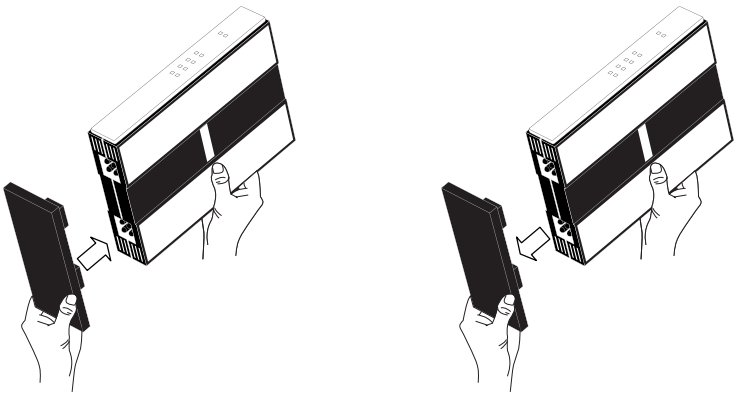
Memo Macintosh パソコンで Internet Explorer を使用している場合、入力した文字がテキストボックスの左側に隠れることがあります。

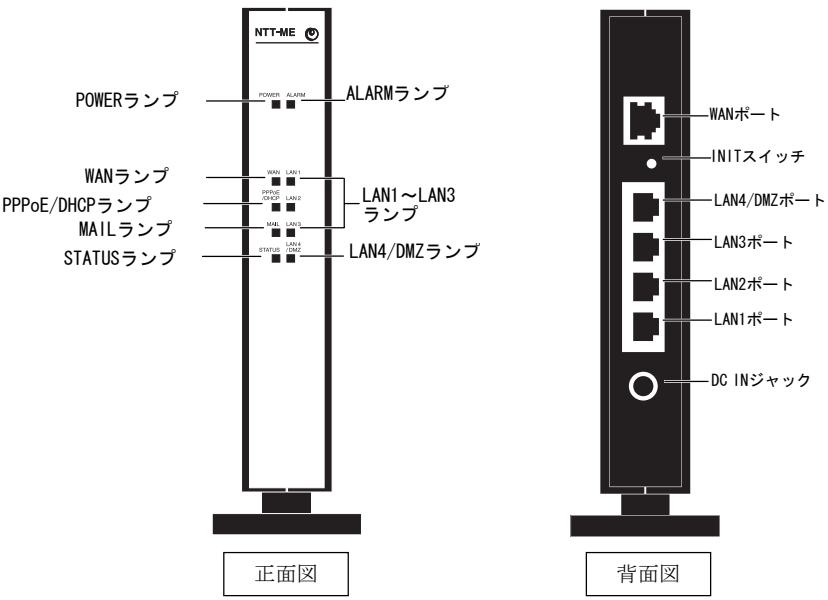
Memo Windows パソコンで Internet Explorer バージョン 5.5 を使用している場合、ブラウザの戻るボタンでは、設定内容が正しく表示されないことがあります。バージョン 6.0 以降の使用をお勧めします。

各部の名称

スタンドの取り付け／取り外し

スタンドを取り付けるときは、スタンドのロック部を本体の穴に合わせ、確実に挿入してください。スタンドを取り外すときは、スタンドを矢印の方向に引いてください。





正面図　　背面図

ランプ表示

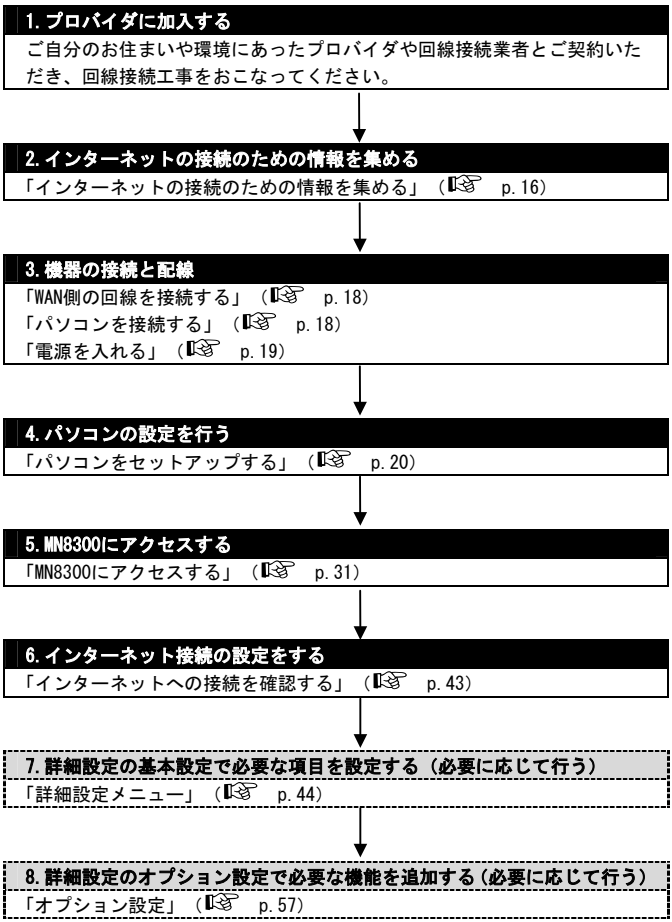
ランプ表示

ランプ	点灯色	表示内容
POWER	 緑	電源が入っています。
ALARM	 赤（点滅）	障害時に点滅します。
WAN	 緑	ADSLモデム、光ケーブルモデムなどに接続しています。
	 緑（点滅）	WAN回線接続後の点滅は、データ通信をしています。
PPPoE/DHCP	 緑	PPPリンク確立状態、またはDHCPでIPアドレス取得済みです。
	 緑（点滅）	DHCPでIPアドレスを要求中です。
	 赤（点滅）	PPPリンク確立中です。
	 橙（点滅）	PPP認証実行中です。認証に失敗すると赤色または橙色に点滅します。DHCP使用の場合には橙色表示はありません。
	消　灯	PPPoEもDHCPも使用されていません。
MAIL	 緑（点滅）	新着メールがメールサーバに着信しています。（ただし、メール着信通知設定を行っている場合）
STATUS	 緑	現状、運用中は点灯しません。（将来の拡張機能用です。）
LAN1～LAN3	 緑	ハブまたはパソコンに接続されています。
	 緑（点滅）	WAN回線接続後の点滅は、データ通信をしています。
LAN4/DMZ	 緑	非DMZポートとして設定され、ハブまたパソコンなどに接続してます。
	 緑（点滅）	LAN4回線接続後の点滅は、非DMZポートとして設定され、データ通信をしています。
	 橙	DMZポートとして設定され、ハブまたはパソコンなどに接続しています。
	 橙（点滅）	DMZポートとして設定され、データ通信をしています。

インターネットへの接続手順と情報の収集

インターネットへの接続手順

本機器を使ってインターネットに接続する流れを図で説明します。この手順に従って接続や設定をおこなってください。



インターネットの接続のための情報を集める

本機器を設置する前に、以下のものがそろっていることをご確認ください。

- TCP/IP を実装している Windows パソコンまたは Macintosh パソコン
- CATV/ADSL/光アクセスサービス用モデム

  Memo　モデムによっては、最初に接続されていたネットワーク機器の MAC アドレスを記憶し、それ以外のネットワーク機器と接続できなくなる機種があります。この場合は、一度モデムの電源を切り、しばらくしてから再度電源を入れてください。

  Memo　モデムによっては、数時間から 1 日程度電源を切る必要がある場合があります。

  Memo　プロバイダによっては、モデムの電源を切ることを禁止している場合があります。問題がないことを確認のうえ、作業をおこなってください。
- インターネット接続に関するアカウント情報（プロバイダから通知されています。）

■ インターネット接続に関するアカウント情報を集める

インターネットへの接続方法は、プロバイダによって異なります。接続方法は、大きく次の 4 種類に分けられます。

- PPPoE（Point to Point Protocol over Ethernet）接続（端末型）
- PPPoE 接続（LAN 型）
- DHCP 接続（DHCP サーバを使ったインターネット接続）
- 固定 IP 接続（IP アドレス固定のインターネット接続）

インターネット接続に関するアカウント情報を参照のうえ、適切な接続方法をご確認ください。インターネットへの接続方法がどれに該当するかわからない場合は、ご契約のプロバイダにお問い合わせください。

■ プロバイダからのアカウント情報をメモしてください。

① PPPoE(Point to Point Protocol over Ethernet)接続（端末型）
光ケーブル、ADSL を使ってインターネットに接続する一般的な接続方法です。B フレッツ、フレッツ・ADSL などで採用されています。端末型の場合は、1 つの IP アドレスをプロバイダから取得し、インターネットに接続します。ユーザーID とパスワードの入力が必要になります。また、PPPoE 接続サービス名、PPPoE 接続サーバ名、DNS サーバアドレスの入力が必要になる場合があります。プロバイダから送付されるアカウント情報を確認し、必要事項をメモしてください。

ユーザーID		パスワード	
PPPoE接続サービス名		PPPoE接続サーバ名	
DNSサーバアドレス（プライマリ）	. . .	DNSサーバアドレス（セカンダリ）	. . .

② PPPoE 接続（LAN 型）

PPPoE 接続で複数の IP アドレスがプロバイダから与えられる場合の接続方式です。入力事項は、PPPoE 接続（端末型）と同じですが、プロバイダから割り当てられた IP アドレスのうちの 1 つを本機器本体の IP アドレスとして指定し、下記にメモしてください。

ユーザーID		パスワード	
PPPoE接続サービス名		PPPoE接続サーバ名	. . .
DNSサーバアドレス（プライマリ）	. . .	DNSサーバアドレス（セカンダリ）	. . .
ルータ用グローバルIPアドレス	. . .		

③ DHCP 接続（DHCP サーバを使ったインターネット接続）

プロバイダのサーバが IP アドレスを自動で割り当て、接続します。ホスト名※、DNS サーバアドレスの入力が必要になる場合があります。プロバイダから送付されるアカウント情報を確認し、下記にメモしてください。

ホスト名		WAN側 MACアドレス	
DNSサーバアドレス（プライマリ）	. . .	DNSサーバアドレス（セカンダリ）	. . .

※「ホスト名」は、プロバイダによっては「コンピュータ名入力欄に入力する ID」と指示されている場合があります。

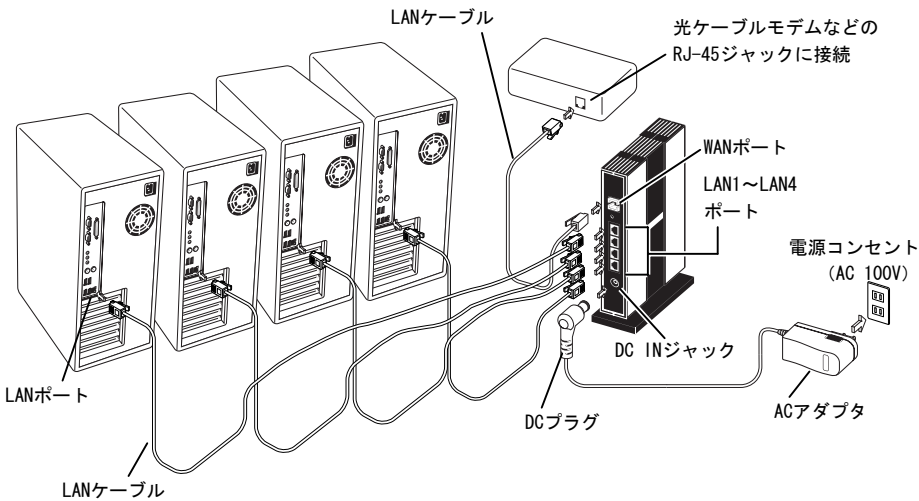
④ 固定 IP 接続（IP アドレス固定のインターネット接続）

プロバイダから、IP アドレスを固定に設定するように指示されている場合は、WAN 側 IP アドレス/マスク長、デフォルトゲートウェイアドレス、DNS サーバアドレスの入力が必要になります。プロバイダから送付されるアカウント情報を確認し、必要事項をメモしてください。

WAN側IPアドレス/マスク長	. . .	デフォルトゲートウェイアドレス	. . .
DNSサーバアドレス（プライマリ）	. . .	DNSサーバアドレス（セカンダリ）	. . .

2 インターネットへの接続

機器の接続と配線



WAN 側の回線を接続する

光ケーブルモデムまたは CATV、ADSL モデムを使用して接続してください。
※接続する前に光ケーブルモデムまたは CATV、ADSL モデムなどをご用意ください。

① 付属の LAN ケーブル(カテゴリ 5 仕様)を光ケーブルモデムなどの RJ-45 ポートに差し込みます。

② LAN ケーブルのもう一方を本機器の WAN ポートに差し込みます。

パソコンを接続する

パソコンと本機器を接続してください。
LAN ポートを搭載したパソコンに、LAN ケーブルを接続してください。

① パソコンの電源を切ります。

② LAN ケーブル（カテゴリ 5 仕様）を本機器の LAN1～LAN4 ポートのいずれかに差し込みます。

③ LAN ケーブルのもう一方をパソコンの LAN ポートに差し込みます。

Memo LAN1～LAN4 ポートは、極性に関係なく接続できます。本機器が極性の切り替えを自動でおこないます。

電源を入れる

すべての機器を接続したら、次の手順に従って、電源を入れてください。
パソコンやイーサネットハブを含め、すべての機器の電源が入っていないことを事前に確認してください。

① ACアダプタのDCプラグを本機器のDC INジャックに差し込み、ACアダプタをコンセントに差し込みます。

⚠ 警告
専用のACアダプタ（極性統一プラグ）以外は使わない 専用以外のACアダプタは、電圧や＋－の極性が異なっていることがあるため、発煙・火災のおそれがあり、危険です。

② イーサネットハブがLAN1～LAN4ポートに接続されている場合は、イーサネットハブの電源を入れます。

③ 本機器に接続されているパソコンの電源を入れます。

Memo 本機器のPOWERランプが緑色に点灯していることと、接続しているネットワークに対応したランプ（WAN、LAN）が緑色に点灯していることを確認してください（☞ p.14）。ランプが消えていたり、ALARMランプが赤色に点灯、点滅となっているときは「トラブルシューティング」（☞ p.172）を参照してください。

パソコンをセットアップする

機器の接続（☞ p. 18）が終わったら、本機器を使用してインターネットに接続ができるようにパソコンの TCP/IP の設定をおこないます。本機器の DHCP サーバ機能を使うと、LAN 側のパソコンの TCP/IP の設定を自動化できます。ここでは本機器の DHCP サーバ機能を使った場合のパソコンの設定を説明します。

次の手順に従って、本機器に接続しているすべてのパソコンを設定してください。

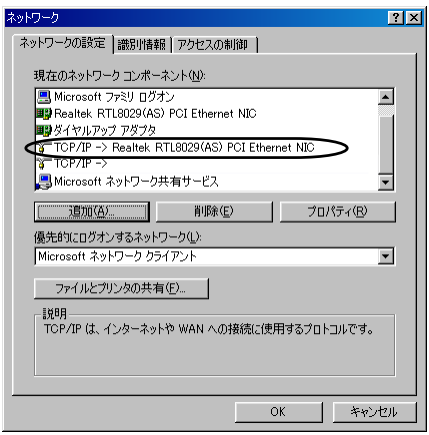
Windows 95/98/Meの場合

次の手順に従って、パソコンごとに IP アドレスを設定してください。

① [スタート]ボタンをクリックし、 設定 を選び、コントロールパネル をクリックしてください。

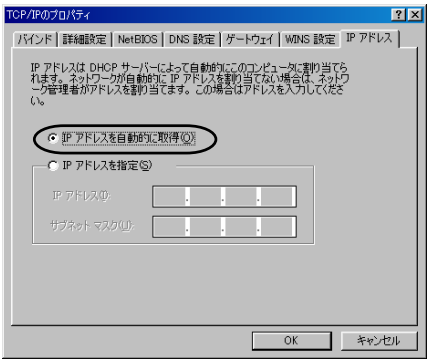
② 「ネットワーク」アイコンをダブルクリックしてください。 Windows Me を使っていて ネットワーク アイコンが見つからない場合は、「すべてのコントロールパネルのオプションを表示する」をクリックしてください。

③ 本機器に接続しているネットワークカードに対応した TCP/IP を選び、ネットワークダイアログボックス の プロパティ をクリックしてください。

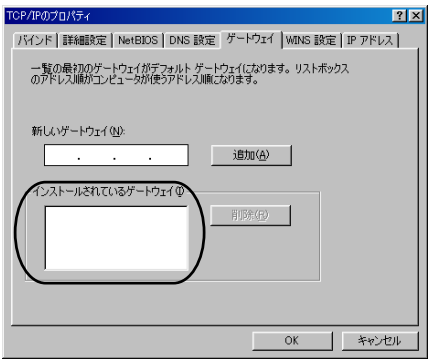


※画面はWindows Meの例です。

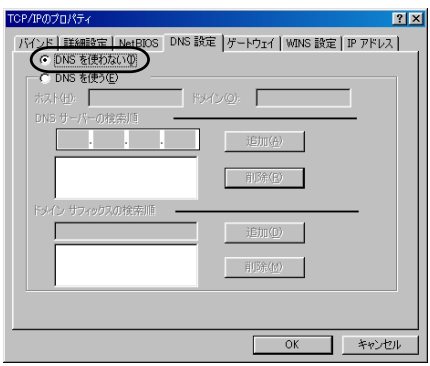
④ IP アドレスタブ をクリックし、「IP アドレスを自動的に取得」を選択してください。



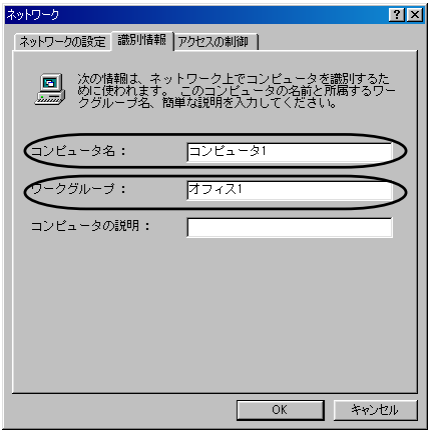
⑤ ゲートウェイタブ をクリックし、インストールされているゲートウェイ の入力欄に何も入力されていないことを確認してください。入力されていた場合は、入力されている IP アドレスを選択し、削除 をクリックします。



⑥ DNS 設定タブ をクリックし、「DNS を使わない」を選び、OK をクリックします。

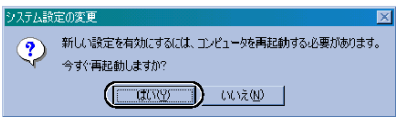


⑦ 識別情報 タブをクリックし、「コンピュータ名およびワークグループ」入力欄に名前を入力してください。「コンピュータ名」はネットワーク上でパソコンを識別するためにつけます。 任意の名前 をつけてかまいませんが、他のパソコンと同じ名前はつけないでください。「ワークグループ」は、ネットワーク上でどのパソコンをどのグループに所属させるかを決めるための名前です。ネットワークで通信したいパソコンには、同じ「ワークグループ」を入力してください。



⑧ OK をクリックし、 システム設定の変更 ダイアログボックスを表示します。

⑨ はい をクリックし、パソコンを再起動します。パソコンに本機器から IP アドレスが割り当てられます。同様に、本機器に接続している他のパソコンを設定してください。



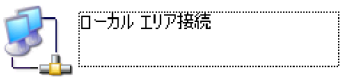
Memo 設定を確認するには、「MN8300 にアクセスする」（☞ p.31）を参照してください。

Windows XP/2000 の場合

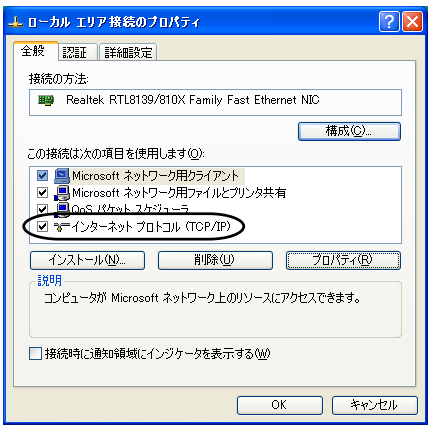
次の手順に従って、パソコンごとに IP アドレスを設定してください。
画面は Windows XP(Home Edition)の例です。

① [スタート]メニューの マイコンピュータ から マイネットワーク を選び、ネットワーク接続を表示 するを選択してください。Windows 2000 の場合は、「マイネットワーク」アイコンを右クリックし、「プロパティ」を選択してください。

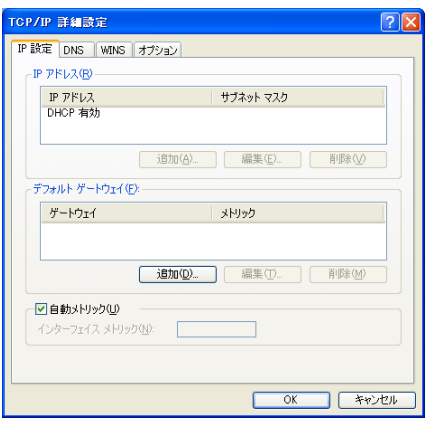
② 本機器に接続している「ローカルエリア接続」アイコンを右クリックし、「プロパティ」を選択してください。



③ 「インターネットプロトコル(TCP/IP)」を選び、プロパティ をクリックしてください。

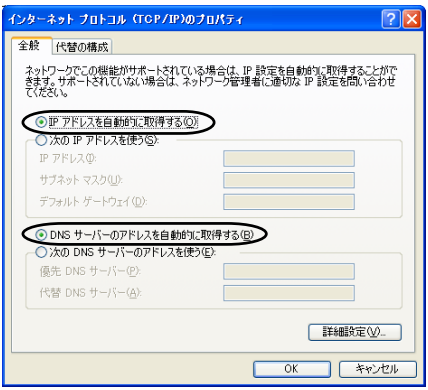


④ 詳細設定... をクリックしてください。右の画面が表示されます。



⑤　「デフォルトゲートウェイ」の入力欄に何も入力されていないことを確認し、OK をクリックしてください。入力されていた場合は、入力されている IP アドレスを選択し、削除 をクリックしてください。

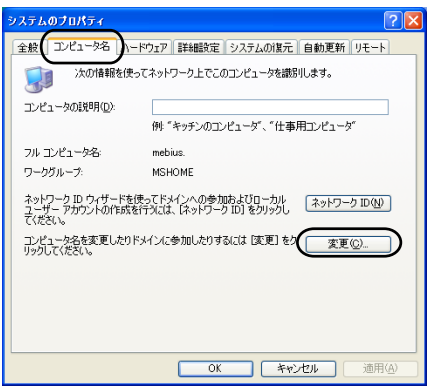
⑥　「IP アドレスを自動的に取得する」を選び、「DNS サーバーのアドレスを自動的に取得する」を選び、OK をクリックしてください。



⑦　閉じる をクリックし、「ローカルエリア接続のプロパティ」のウィンドウを閉じる Windows 2000 の場合は、OK をクリックし、「ローカルエリア接続」のプロパティのウィンドウを閉じてください。

⑧　スタート メニューから マイコンピュータ を表示させた状態で右クリックし、プロパティ を選ぶ Windows 2000 の場合は、「マイコンピュータ」アイコンを右クリックし、プロパティ を選んでください。

⑨　コンピュータ名 タブをクリックし、変更... をクリックしてください。Windows 2000 の場合は、 ネットワーク ID タブをクリックし、プロパティ をクリックしてください。



⑩ 「コンピュータ名」と「ワークグループ」入力欄に名前を入力してください。「コンピュータ名」はネットワーク上でパソコンを識別するためにつけます。任意の名前をつけてかまいませんが、他のパソコンと同じ名前はつけないでください。「ワークグループ」は、ネットワーク上でどのパソコンをどのグループに所属させるかを決めるための名前です。ネットワークで通信したいパソコンには、同じ「ワークグループ」を入力してください。

⑪ 必要に応じて複数回 OK をクリックし、「システムのプロパティ」を閉じてください。

⑫ はい をクリックして、パソコンを再起動してください。パソコンに本機器から IP アドレスが割り当てられます。同様に、本機器に接続している他のパソコンを設定してください。

Memo 本機器の設定を確認するには、「MN8300 にアクセスする」（☞ p.31）を参照してください。

Windows NT 4.0の場合

次の手順に従って、パソコンごとに IP アドレスを設定してください。

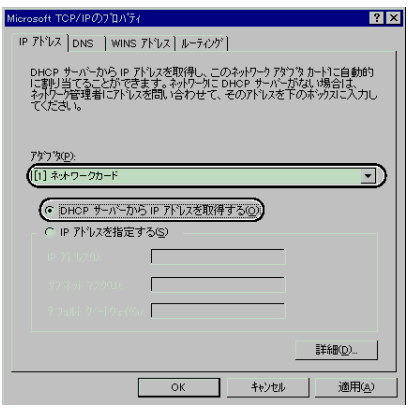
① [スタート]ボタンをクリックし、 設定 を選び、コントロールパネル をクリックしてください。

② 「ネットワーク」アイコンをダブルクリックしてください。

③ プロトコルタブ をクリックし、「TCP/IP プロトコル」を選び、 プロパティ をクリックしてください。

④ TCP/IP のプロパティ ダイアログボックスで、IP アドレスタブ をクリックしてください。

⑤ 本機器に接続しているネットワークカードを「アダプタ」コンボボックスから選び、「DHCP サーバーから IP アドレスを取得する」を選択してください。



⑥ デフォルトゲートウェイ の入力欄に何も入力されていないことを確認してください。

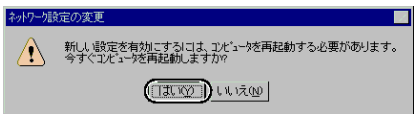
⑦ OK をクリックしてください。

⑧ 識別 タブをクリックしてください。

⑨ 必要に応じてを 変更 クリックし、「コンピュータ名」と「ワークグループ」入力欄に名前を入力してください。「コンピュータ名」はネットワーク上でパソコンを識別するためにつけます。 任意の名前 をつけてかまいませんが、他のパソコンと同じ名前はつけないでください。「ワークグループ」は、ネットワーク上でどのパソコンをどのグループに所属させるかを決めるための名前です。ネットワークで通信したいパソコンには、同じ「ワークグループ」を入力してください。

⑩ 閉じる をクリックしてください。

⑪ はい をクリックして、パソコンを再起動してください。パソコンに本機器から IP アドレスが割り当てられます。同様に、本機器に接続している他のパソコンを設定してください。



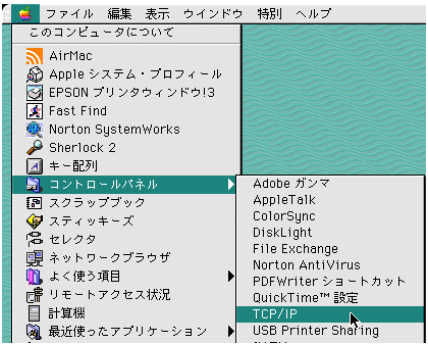
Memo 本機器の設定を確認するには、「MN8300 にアクセスする」（☞ p.31）を参照してください。

Mac OS 8.1～9.2の場合

次の手順は、Mac OS 9.2 operating system software を使った場合です。Mac OS のバージョンによっては若干操作方法が異なる場合があります。パソコンごとに IP アドレスを設定してください。

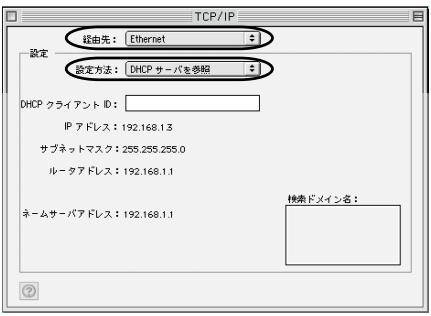
① アップルメニューから コントロールパネル を選択してください。

② コントロールパネル メニューから TCP/IP を選択してください。

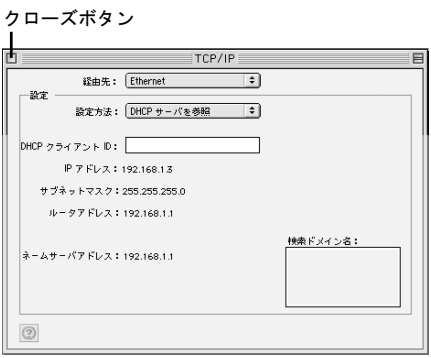


③ 経由先 ポップアップメニューから Ethernet を選択してください。

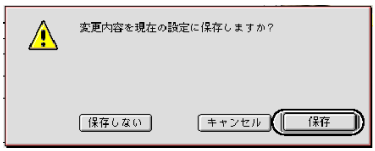
④ 設定方法 ポップアップメニューから DHCP サーバを参照 を選択してください。



⑤ クローズボタン をクリックしてください。



⑥ 保存 をクリックしてください。



⑦ パソコンを再起動してください。
パソコンに本機器から IP アドレスが割り当てられます。同様に、本機器に接続している他のパソコンを設定してください。

Memo 本機器の設定を確認するには、「MN8300 にアクセスする」（☞ p.31）を参照してください。

Mac OS X (10.1～10.2)の場合

次の手順に従って、パソコンごとに IP アドレスを設定してください。次の手順は、Mac OS 10.1 を使った場合です。Mac OS のバージョンによっては若干操作方法が異なる場合があります。パソコンごとに IP アドレスを設定してください。

① [アップル]メニューから システム環境設定 を選ぶシステム環境設定画面が表示されます。

② 「ネットワーク」アイコンをクリックしてください。

③ 表示 ポップアップメニューから 内蔵 Ethernet を選択してください。

④ TCP/IP の 設定 ポップアップメニューから DHCP サーバを参照 を選び、必要に応じて 今すぐ適用 をクリックしてください。

⑤ クローズボタンをクリックしてください。

Memo 本機器の設定を確認するには、「MN8300 にアクセスする」（☞ p.31）を参照してください。

MN8300を設定する

MN8300にアクセスする

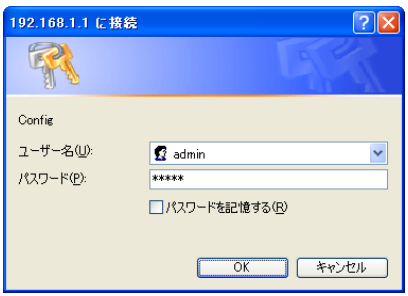
本機器の設定ページは「おまかせ設定」と「詳細設定」の 2 つに分かれています。「おまかせ設定」は、「接続モード」、「ユーザ ID」、「パスワード」、「フレッツ・スクウェア使用の有無」と、必要に応じて「DNS サーバアドレス」を入力すれば自動設定します。「詳細設定」は、機能ごとに詳細な設定が可能です。本機器の設定を行うには、以下の手順で本機器へログインし設定ページを表示させます。

① WWW ブラウザを起動し、本機器のアドレス「http://192.168.1.1/（工場出荷時設定）」を指定します。

注意 WWW ブラウザの設定で JavaScript の使用を無効にしている場合は、有効にしてください。

注意 本機器へのアクセスはプロキシサーバを経由してはできません。
「WWW ブラウザの設定」（☞ p.157）を参照して、WWW ブラウザの設定を変更してください。

② 192.168.1.1 に接続画面が表示されます。「ユーザー名」および「パスワード」に「admin」と入力し（工場出荷時設定）、OK をクリックします。



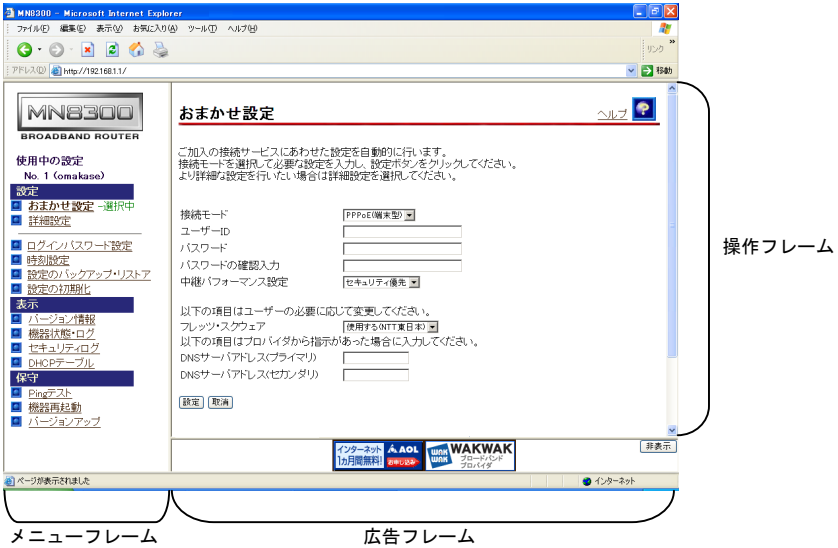
Memo 「ユーザー名：admin」、「パスワード：admin」は工場出荷時の設定です。

Memo 本機器の WWW 設定画面上で、ユーザー名およびパスワードを変更することができます。詳細は、「ログインパスワードの設定」（☞ p.85）を参照してください。セキュリティ面で工場出荷時初期値からの変更をお勧めします。

Memo 前回設定した IP アドレスやパスワードがわからなくなって本機器にアクセスできない場合は、「一時的に工場出荷時設定で起動する」（☞ p.156）を参照してください。

Memo ここで入力する「ユーザー名」および「パスワード」は、プロバイダから割り当てられた「ユーザー名」、「パスワード」ではありません。

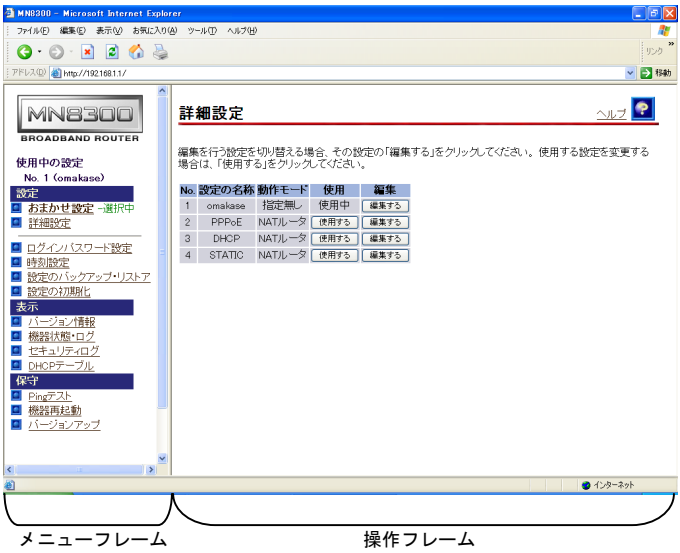
③　本機器の設定ページおまかせ設定画面が表示されます。



詳細設定ページを表示したいときは、以下の手順で表示します。
設定ページの画面は、メニューフレーム、操作フレーム、および広告フレームに分かれており、メニューフレームから設定・表示・保守の各メニューを選択すると操作フレームに設定ページや関連情報が表示されます。

Memo　操作フレーム右上の?マークや項目をクリックすると、それぞれの説明が表示されます。
Memo　広告フレーム内にあるを　非表示　をクリックすると、広告フレームを非表示にできます。

④　メニューフレームから詳細設定をクリックします。



Memo　上の図は、広告フレームを非表示にした状態です。本書では、特に断りがない限り、広告フレームが非表示の画面を使用します。

インターネット接続の設定をする

本機器をインターネットに接続するための接続方法は、次の 4 種類に分けられます。※

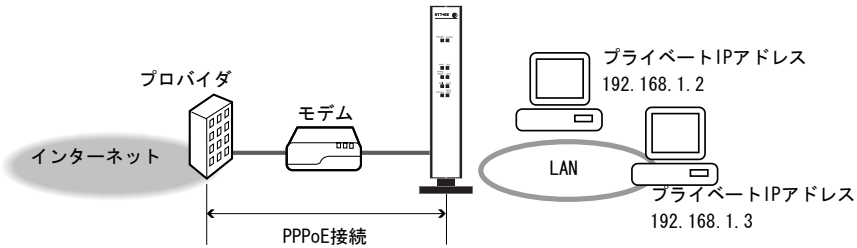
- PPPoE（端末型）接続（☞ p.35）
- PPPoE（LAN 型）接続（☞ p.37）
- DHCP 接続(DHCP サーバを使ったインターネット接続)（☞ p.39）
- 固定 IP 接続(IP アドレス固定のインターネット接続)（☞ p.41）

「インターネットへの接続手順と情報の収集」（☞ p. 15）を参照して、本機器をインターネットに接続してください。

※インターネットの接続方法が、DHCP 接続、固定 IP 接続、PPPoE 接続（端末型）、PPPoE 接続（LAN 型）のどれに該当するかなど、サービス内容や契約内容についての詳細は、ご契約のプロバイダにお問い合わせください。

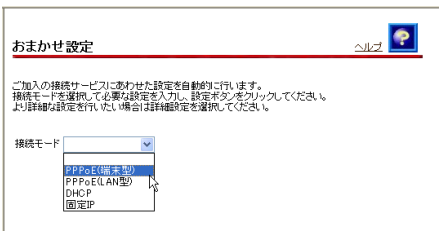
■ PPPoE 接続（端末型）の場合

PPPoE 接続（端末型）の設定は、次の手順に従ってください。

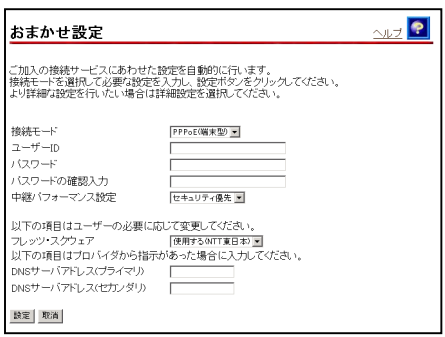


① メニューフレームから おまかせ設定 を選択してください。

② 接続モードから「PPPoE（端末型）」を選択してください。PPPoE 接続（端末型）モードの設定画面が表示されます。



③ [ユーザ ID]、[パスワード]、[パスワードの確認入力]（パスワードと同一文字）を入力します。通常に使用する場合は、[中継パフォーマンス設定]から「セキュリティ優先」を選択します。フレッツ・スクウェアを使用する場合は[フレッツ・スクウェア]から「使用する（NTT 東日本）」、「使用する（NTT 西日本）」を選択します。また、プロバイダから指定がある場合は[DNS サーバアドレス（プライマリ）]、[DNS サーバアドレス（セカンダリ）]を入力します。「インターネットへの接続手順と情報の収集」（☞ p. 15）を参照してください。元の設定に戻すには、 取消 をクリックしてください。



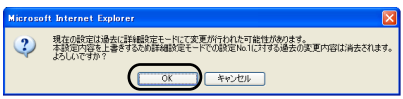
注意 「フレッツ・スクウェア」は、B フレッツまたはフレッツ・ADSL 以外では利用できません。

Memo 「中継パフォーマンス」は、ステートフル・パケット・インスペクションなどのセキュリティを確保した上で利用するモード（セキュリティ優先モード）と、セキュリティ機能をすべて外した状態で中継性能を重視するモード（スループット優先モード）があります。通常は「セキュリティ優先モード」を選択してください。

Memo 「フレッツ・スクウェア」を「使用する」に設定すると、PPPoE 接続先設定のサブセッション 1 に「フレッツ・スクウェア」が自動的に登録され、PPPoE 自動接続が「常にする」となります。詳細は「接続先設定（PPPoE 接続モードのみ）」（☞ p.53）を参照してください。

④ 設定値の入力を終えたら、 設定 をクリックしてください。

⑤ 設定 No.1 に対する上書き確認メッセージが表示されるので、 OK をクリックすると、本機器が自動的に再起動します。



⑥ LAN 上に接続されたすべてのパソコンを再起動してください。

⑦ 本機器本体前面の[PPPoE/DHCP]ランプが緑色に点灯していることを確認してください。

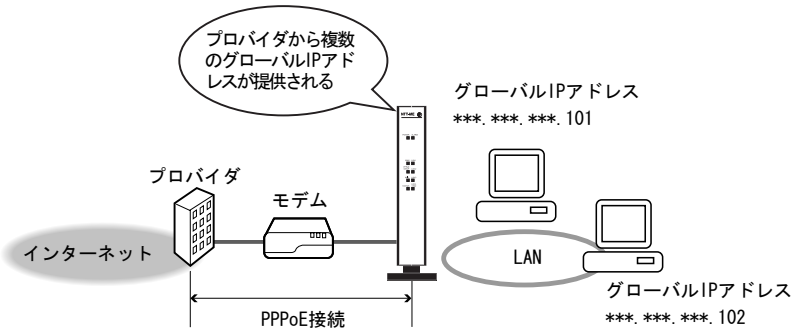
⑧ LAN 側に接続しているすべてのパソコンから、インターネットへのアクセスを確認してください。

注意 利用するプロバイダから指示がある場合、PPP 設定の認証方式を変更してください。変更は「接続先設定（PPPoE 接続モードのみ）」で行います（☞ p.53）

注意 利用するプロバイダから指示がある場合、MTU 値を変更してください。指示がない場合は工場出荷時設定（1500）です。変更は「接続先設定（PPPoE 接続モードのみ）」で行います。（☞ p.53）

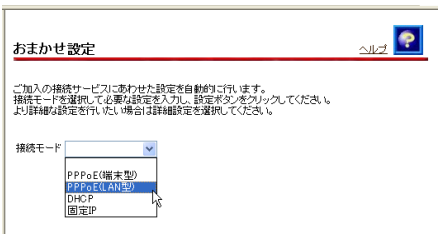
■ PPPoE 接続（LAN 型）の場合

PPPoE 接続（LAN 型）は、複数のグローバル IP アドレスをプロバイダから提供される接続形態です。PPPoE 接続（LAN 型）の設定は、次の手順に従ってください。

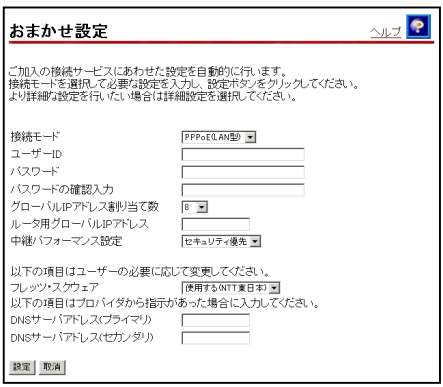


① メニューフレームから おまかせ設定 を選択してください。

② 接続モードから、「PPPoE（LAN 型）」を選択してください。PPPoE 接続（LAN 型）モードの設定画面が表示されます。



③ [ユーザ ID]、[パスワード]、[パスワードの確認入力]（パスワードと同一文字）を入力します。[グローバル IP アドレス割り当て数]には、プロバイダから割り当てられた数を「8」、「16」、「32」から選択します。
通常に使用する場合は、[中継パフォーマンス設定]から「セキュリティ優先」を選択します。
フレッツ・スクウェアを使用する場合は[フレッツ・スクウェア]から「使用する（NTT 東日本）」、「使用する（NTT 西日本）」を選択します。また、プロバイダから指示がある場合は[DNS サーバアドレス（プライマリ）]、[DNS サーバアドレス（セカンダリ）]を入力します。「インターネットへの接続手順と情報の収集」（☞ p. 15）を参照してください。



注意 「フレッツ・スクウェア」は、B フレッツまたはフレッツ・ADSL 以外では利用できません。

Memo 「中継パフォーマンス」は、ステートフル・パケット・インスペクションなどのセキュリティを確保した上で利用するモード（セキュリティ優先モード）と、セキュリティ機能をすべて外した状態で中継性能を重視するモード（スループット優先モード）があります。通常は「セキュリティ優先モード」を選択してください。

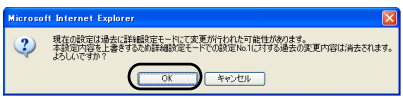
Memo 「フレッツ・スクウェア」を「使用する」に設定すると、PPPoE 接続先設定のサブセッション 1 に「フレッツ・スクウェア」が自動的に登録され、PPPoE 自動接続が「常にする」となります。詳細は接続先設定（PPPoE 接続モードのみ）（☞ p.53）を参照してください。

- ルータ本体の IP アドレスについて
  プロバイダから割り当てられたグローバル IP アドレスの 1 つを ルータ本体の IP アドレス に入力し、指定されたネットマスクを入力してください。ルータから WAN 側に直接送信するときに、この IP アドレスを送信元 IP アドレスとして使います。

④ 元の設定に戻すには、取消 をクリックしてください。

⑤ 設定値の入力を終えたら、 設定 をクリックしてください。

⑥ 設定 No.1 に対する上書き確認メッセージが表示されるので、 OK をクリックすると、本機器が自動的に再起動します。



⑦ LAN 上に接続されたすべてのパソコンを再起動してください。

⑧ 本機器本体前面の PPPoE/DHCP ランプが緑色に点灯していることを確認してください。

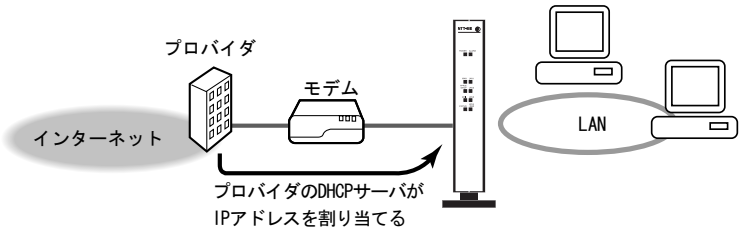
⑨ LAN 側に接続しているすべてのパソコンから、インターネットへのアクセスを確認してください。

Memo パソコンにグローバル IP アドレスを固定設定します。「パソコンの IP アドレスを固定するには」（☞ p.160）を参照してください。

Memo パソコンにプライベート IP アドレスを固定設定して、静的 NAT アドレス変換を利用してグローバル IP アドレスを設定する。「パソコンの IP アドレスを固定するには」（☞ p.160）、および「（GapNAT 通過）・NAT アドレス変換設定（ワンタッチ NAT 設定）」（☞ p.60）を参照してください。

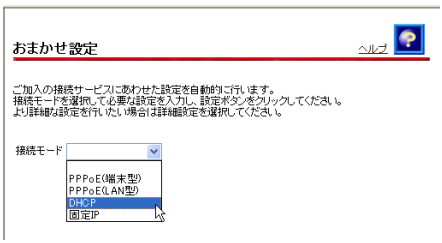
■ DHCP 接続(DHCP サーバを使ったインターネット接続)の場合

DHCP 接続(IP アドレスを自動的にプロバイダから割り当ててもらう)は、次の手順に従ってください。本機器は NAT ルータとして設定されます。



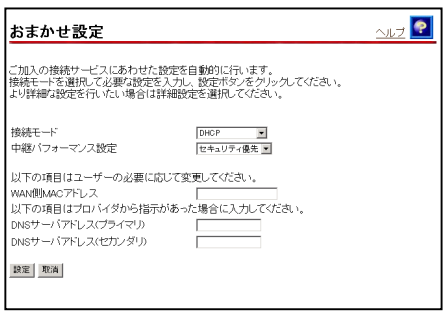
① メニューフレームから、おまかせ設定 を選択してください。

② 接続モードから「DHCP」を選択してください。
DHCP 接続モードの設定画面が表示されます。



③ 通常に使用する場合は、[中継パフォーマンス設定]から「セキュリティ優先」を選択します。
プロバイダから指定がある場合は、[WAN 側 MAC アドレス]※、[DNS サーバアドレス(プライマリ)]、[DNS サーバアドレス(セカンダリ)]を入力してください。「インターネットへの接続手順と情報の収集」(☞ p.15)を参照してください。元の設定に戻すには、 取消 をクリックしてください。

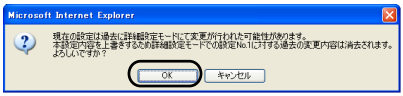
※[WAN 側 MAC アドレス]は、プロバイダによっては固定の値を申請している場合があります。



Memo 「中継パフォーマンス」は、ステートフル・パケット・インスペクションなどのセキュリティを確保した上で利用するモード(セキュリティ優先モード)と、セキュリティ機能をすべて外した状態で中継性能を重視するモード(スループット優先モード)があります。通常は「セキュリティ優先モード」を選択してください。

④　設定値の入力を終えたら、 設定 をクリックしてください。

⑤　設定 No.1 に対する上書き確認メッセージが表示されるので、 OK をクリックすると、本機器が自動的に再起動します。



⑥　LAN 上に接続されたすべてのパソコンを再起動してください。

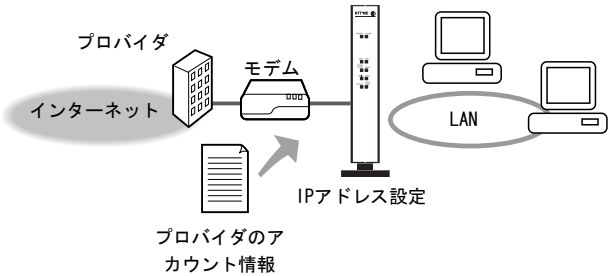
⑦　本機器本体前面の PPPoE/DHCP ランプが緑色に点灯していることを確認してください。

※[詳細設定]ページのメニューフレームから 機器状態・ログ をクリックして状態を確認してください。 機器状態・ログ について詳細は「機器状態・ログ」（☞ p.74）を参照してください。

⑧　LAN 側に接続しているすべてのパソコンから、インターネットへのアクセスを確認してください。

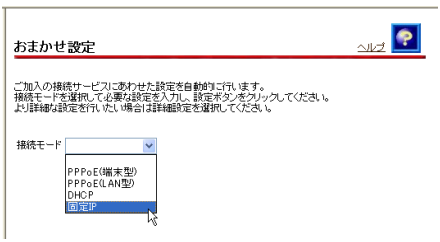
■ 固定 IP 接続(IP アドレス固定のインターネット接続)の場合

プロバイダからのアカウント情報に IP アドレスやゲートウェイアドレスなどの値を入力するように指示がある場合は、本機器にこれらの値を入力する必要があります。

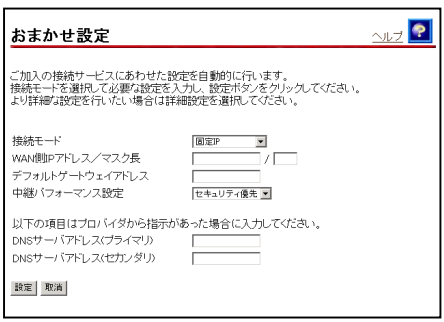


① メニューフレームから、おまかせ設定 を選択してください。

② 接続モードから、「固定 IP」を選択してください。固定 IP 接続モードの設定画面が表示されます。



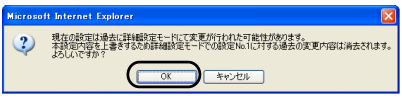
③ [WAN 側 IP アドレス/マスク長]、[デフォルトゲートウェイアドレス]、[DNS サーバアドレス（プライマリ）]、[DNS サーバアドレス（セカンダリ）]を入力してください。
通常に使用する場合は、[中継パフォーマンス設定]から「セキュリティ優先」を選択します。
「インターネットへの接続手順と情報の収集」（☞ p.15）を参照してください。元の設定に戻すには、 取消 をクリックしてください。



Memo　「中継パフォーマンス」は、ステートフル・パケット・インスペクションなどのセキュリティを確保した上で利用するモード（セキュリティ優先モード）と、セキュリティ機能をすべて外した状態で中継性能を重視するモード（スループット優先モード）があります。通常は「セキュリティ優先モード」を選択してください。

④　設定値の入力を終えたら、 設定 をクリックしてください。

⑤　設定 No.1 に対する上書き確認メッセージが表示されるので、 OK をクリックすると、本機器が自動的に再起動します。



⑥　LAN 上に接続されたすべてのパソコンを再起動してください。

⑦　LAN 側に接続しているすべてのパソコンから、インターネットへのアクセスを確認してください。

インターネットへの接続を確認する

■ 接続の確認

インターネットに接続するための設定が終わったら、インターネットの WWW サイトにアクセスしてください。WWW サイトが表示されたら、インターネットに接続されたことになります。

① WWW ブラウザを起動してください。

② WWW ブラウザのアドレスバーに http://192.168.1.1/を入力して、WWW 設定画面にアクセスしてください。

③ 詳細情報メニューから機器状態・ログをクリックして、設定した接続、またはセッションが「確立」になっているか確認してください。（☞ p.74 ページ）

④ WWW ブラウザのアドレスバーに WWW サイトのアドレス（例 http://www.ntt-me.co.jp/）を入力してください。WWW サイトが表示されます。

■ WWW サイトが表示されなかった場合（詳細は 174 ページを参照してください。）

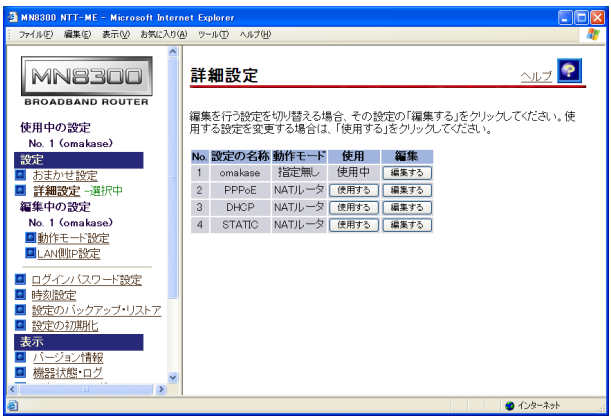
- パソコンを再起動してください。
- WWW サイトのアドレスが WWW ブラウザのアドレスバーに正しく入力されているか、確認してください。
- 「MN8300 にアクセスする」（☞ p.31）をおこなったか、確認してください。
- 本機器とモデムとの接続を確認してください。
- パソコン、本機器、その他の機器の電源を適切な順番で入れたか、確認してください。詳細は、「電源を入れる」（☞ p.19）を参照してください。
- プロバイダから受け取ったインターネットへの接続に関するアカウント情報を確認してください。設定値を入力する必要があれば、「インターネット接続の設定をする」（☞ p.34）を参照し、本機器に設定値を入力してください。

3 MN8300の詳細設定について

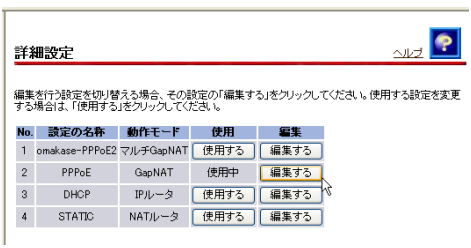
詳細設定メニュー

通常のインターネット・アクセスサービスを利用するには「おまかせ設定」だけで行えますが、PPPoE マルチセッションやセキュリティなどの拡張機能を使用したい場合には詳細設定メニューで必要な項目を設定します。
本機器では「おまかせ設定」、「PPPoE」、「DHCP」、「STATIC」（固定 IP）用に計 4 種類の設定を保存しておくことができ、必要に応じて設定を切り替えることができます。

① **メニューフレームより詳細設定をクリックしてください。操作フレームに設定の選択画面が表示されます。**

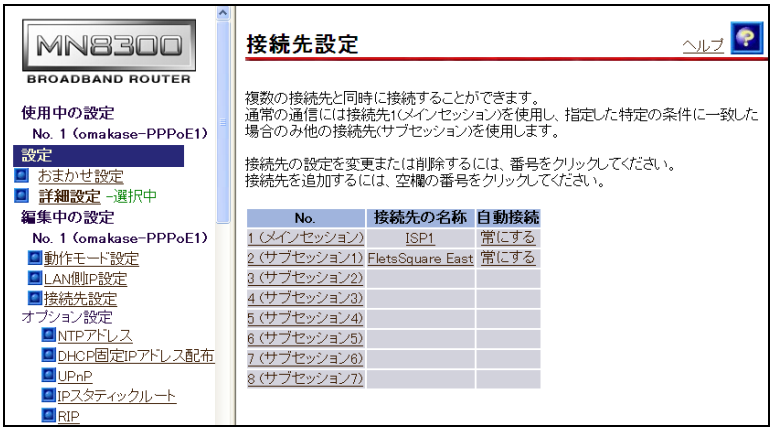


② 編集したい行の 編集する をクリックしてください。

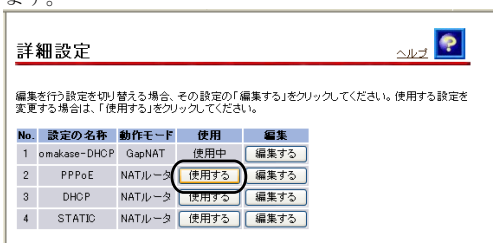


Memo おまかせ設定に拡張機能を付加したい場合は No.1 の"omakase-XXX"の 編集する をクリックします。新規に設定する場合には接続モード（No.2 [PPPoE]、No.3 [DHCP]、No.4 [STATIC]）に応じた行の 編集する をクリックします。

操作フレームには基本設定項目、オプション設定項目とセキュリティ設定項目のメニューが表示されます。各設定項目は選択した接続モードに応じて適応する項目のみが表示されます。
まずは、基本設定の各項目について確認しながら設定作業を行い、次に必要に応じてオプション設定・セキュリティ設定を行ってください。※以下の画面は PPPoE の場合の例です。



すべての編集が完了したら、該当する行の 使用する をクリックしますと、設定の変更が行われます。



詳細設定メニューには以下のようなメニューが用意されています。

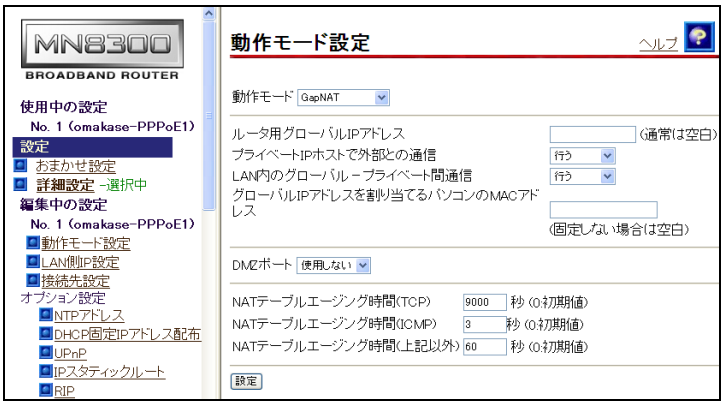
基本設定	
動作モード設定	本機器の動作モードを「NATルータ」、「IPルータ」、「GapNAT」、「マルチGapNAT」から選択します。 ＊GapNAT/マルチGapNATについては、「GapNATとDMZホストの構築」（☞ p.119）の項を参照してください。
LAN側IP設定	LAN側のアドレス設定等に関する項目を設定します。
接続先設定	PPPoEに関する各種設定を行います。また、PPPoEマルチセッションで接続する接続先の詳細情報も設定します。 ＊PPPoE接続モード選択時にのみ表示されます。
WAN側DHCP設定	WAN側とDHCPで交換する情報を設定します。 ＊DHCP接続モード選択時にのみ表示されます。
WAN側IP設定	WAN側のIPアドレス設定情報を入力します。 ＊固定IP接続モード選択時にのみ表示されます。
オプション設定	
NTPアドレス設定	NTPによって本機器の時刻設定を行う場合に設定します。
DHCP固定IPアドレス	DHCPサーバを利用して、LAN側にある端末に対してIPアドレスを自動設定する場合でも、MACアドレスを指定することで、固定のIPアドレスを付与できます。最大16台まで設定できます。
UPnP設定	UPnPに関する詳細設定を行う場合に設定します。 ＊IPルータでの利用時は表示されません。
IPスタティックルート	IPルーティング情報を登録する場合に設定します。
RIP設定	動的ルーティングであるRIPを起動させる場合に設定します。 ＊NATルータ、IPルータでの利用時のみ表示されます。
NATアドレス変換	NATテーブルのアドレス変換情報を固定的に変更したい場合に設定します。 ＊NATルータでの利用時に表示されます。
GapNAT通過・NATアドレス変換	NATテーブルのアドレス変換情報を固定的に変更したい場合に設定します。 ＊GapNAT、マルチGapNATでの利用時に表示されます。
GapNAT通過	外部から開始されたグローバルIPアドレス宛の通信のうち、LAN側に通過させるものを、プロトコルおよびTCP/UDPポート番号を指定して制限することができます。 ＊固定IP接続モードでGapNAT、マルチGapNATを利用する場合にのみ表示されます。
NATアドレス・ポート変換	NATテーブルの変換情報をポート番号情報まで含めて固定的に変更したい場合に設定します。 ＊IPルータでの利用時は表示されません。
ダイナミックDNS設定	ダイナミックDNSサイトを登録する場合に設定します。
メール着信通知設定	定期的にメールサーバにアクセスし、本体前面のMAILランプで新着メールの到達をお知らせする場合に設定します。
syslogサーバ設定	外部syslogサーバを利用する場合に設定します。

セキュリティ設定	
アクセス制限（ステルス）	本機器の設定画面等へのアクセスを制限します。
SPI設定	ステートフル・パケット・インスペクション機能の使用を変更します。 ＊IPルータでの利用時はSPIを利用できませんので、このメニューは表示されません。
IPフィルタ設定	IPパケットフィルタリングを行う条件を追加、変更します。ワンタッチフィルタ設定も可能です。
不正アクセス検知設定	WAN側から本機器に対してアタック等の不正アクセスがかけられた場合に、ログ・syslogに不正アクセスを通知する条件を設定します。

基本設定

動作モードの設定

動作モード設定では本機器の動作モードを「NAT ルータ」、「IP ルータ」、「GapNAT」、「マルチ GapNAT」から選択します。
データ入力欄に設定する内容がない場合は空欄のままにしてください。
プロバイダへの接続モードに応じて設定できる動作モード、設定項目が異なります。
※画面は動作モードを GapNAT とした場合の例です。



動作モード	設定項目	内容
NATルータ	NATテーブルエージング時間（TCP）	NATテーブルからTCPセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったTCPセッションについてはNATテーブルから削除されます。本設定値が適用されるのは、TCPセッションのうち確立中のもののみで、未確立や切断後のものについては自動的に適切なエージング時間が選択されます。
	NATテーブルエージング時間（ICMP）	NATテーブルからICMPセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
	NATテーブルエージング時間（上記以外）	NATテーブルから上記以外のセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
IPルータ	なし	動作モード以外設定項目なし。
GapNAT ※1	ルータ用グローバルアドレス	GapNATで本機器のLAN側に設定されるグローバルIPアドレスを変更したい場合に設定します。通常は入力の必要はありません。
	プライベートIPホストで外部との通信	GapNAT機能で割り当てられたグローバルIPアドレス以外のプライベートIPアドレスをもつLAN側端末とWANとの通信を制御します。「行う」、「行わない」から選択します。
	LAN内のグローバル・プライベート間通信	GapNAT機能で割り当てられたグローバルIPアドレスをもつLAN側端末と、それ以外のプライベートIPアドレスをもつLAN側端末との通信を制御します。「行う」、「行わない」から選択します。
	グローバルIPアドレスを割り当てるパソコンのMACアドレス	GapNAT機能でグローバルIPアドレスを割り当てるLAN側端末をMACアドレスで固定することができます。固定しない場合は空欄のままとしてください。 MACアドレスの入力方法は2桁づつハイフンかコロンで区切って入力するか、区切りなしで12桁を入力します。 例： 02-23-45-67-89-01 02:23:45:67:89:01 0223454678901 パソコンのMACアドレスを確認するには、「パソコンのIPアドレスやMACアドレスを確認するには」（☞ p.169）を参照してください。
	DMZポート	「使用する」を選択した場合、グローバルIPアドレスをもつDMZホストをLAN4/DMZポートにくくりつけることができます。本設定を行うと、GapNATでグローバルIPアドレスが割り当てられる端末はLAN4ポートに限定されます。「使用しない」を選択した場合はGapNATでグローバルIPアドレスが割り当てられる端末は任意のLANポートに接続できます。

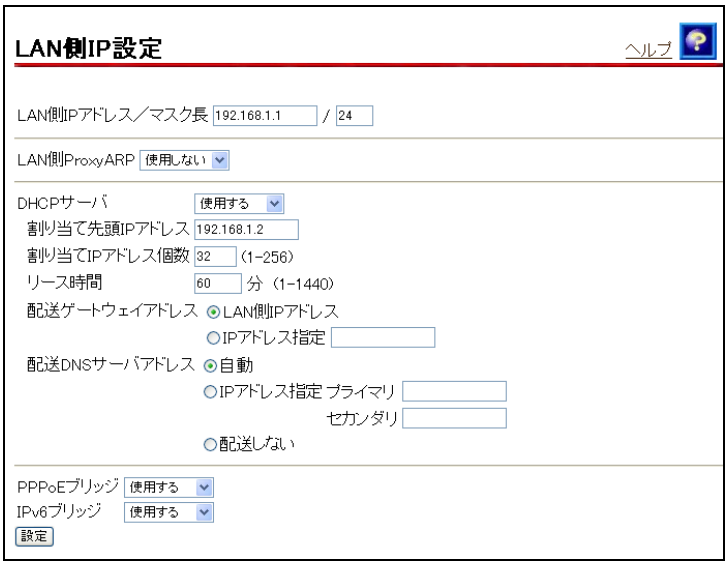
動作モード	設定項目	内容
GapNAT ※1	NATテーブルエージング時間（TCP以外）	NATテーブルからTCP以外のセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
	NATテーブルエージング時間（ICMP）	NATテーブルからICMPセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
	NATテーブルエージング時間（上記以外）	NATテーブルから上記以外のセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
マルチGapNAT ※2	グローバルIPアドレス割り当て数	プロバイダから割り当てられたグルーバルIPアドレスの個数を「8」、「16」、「32」から選んでください。
	ルータ用グローバルアドレス	マルチGapNATで本機器のLAN側に設定されるグローバルIPアドレスを指定したい場合に設定します。通常はプロバイダから割り当てられた連続したアドレスの範囲から、最小のもの・最大のもの以外の値を設定してください。
	プライベートIPホストで外部との通信	マルチGapNAT機能で割り当てられたグローバルIPアドレス以外のプライベートIPアドレスをもつLAN側端末とWANとの通信を制御します。「行う」、「行わない」から選択します。
	LAN内のグローバル・プライベート間通信	マルチGapNAT機能で割り当てられたグローバルIPアドレスをもつLAN側端末と、それ以外のプライベートIPアドレスをもつLAN側端末との通信を制御します。「行う」、「行わない」から選択します。
	NATテーブルエージング時間（TCP）	NATテーブルからTCPセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったTCPセッションについてはNATテーブルから削除されます。本設定値が適用されるのは、TCPセッションのうち確立中のもののみで、未確立や切断後のものについては自動的に適切なエージング時間が選択されます。
	NATテーブルエージング時間（ICMP）	NATテーブルからICMPセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。
	NATテーブルエージング時間（上記以外）	NATテーブルから上記以外のセッションを削除するまでの時間を1～65535秒の範囲で指定してください。ここで指定した時間以上通信がなかったセッションについてはNATテーブルから削除されます。

※1：GapNAT の詳細については「GapNAT と DMZ ホストの構築」（☞ p.119）を参照してください。

※2：DHCP 接続モードではマルチ GapNAT 動作モードは選択できません。マルチ GapNAT の詳細については「GapNAT と DMZ ホストの構築」（☞ p.119）を参照してください。

LAN側IP設定

本機器の LAN 側に設定するプライベートアドレスまたは固定 IP 接続でプロバイダから情報と、LAN 側パソコンに IP アドレスを割り当てる DHCP サーバの情報を設定します。
また、PPPoE ブリッジ機能の設定を行います。



※画面は動作モードを NAT ルータ、GapNAT、マルチ GapNAT とした場合の例です。

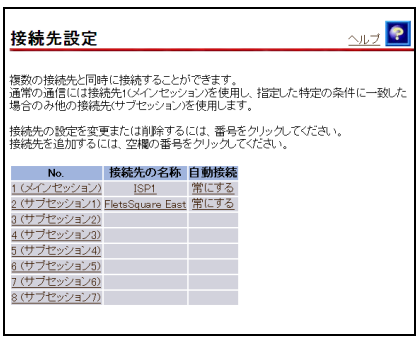
設定項目	内容
LAN側IPアドレス／マスク長	本機器のLAN側に設定するIPアドレスとマスク長を登録します。IPアドレスとマスク長はスーパネットに対応いています。
LAN側ProxyARP	LAN側でARPの代理応答を「使用する」、「使用しない」から選択します。通常は「使用しない」とします。
DHCPサーバ	LAN内のパソコン等にDHCPでアドレスを割り当てる場合に「使用する」を設定します。DHCPサーバ機能を非活性にするには「使わない」と設定してください。
割り当て先頭IPアドレス	DHCPサーバを「使用する」場合に有効。 DHCPで割り当てる最小のIPアドレスを設定します。
割り当てIPアドレス個数	DHCPサーバを「使用する」場合に有効。 LAN側のパソコンにIPアドレスを割り当てるために確保する個数を設定します。最大256個です、
リース時間	DHCPサーバを「使用する」場合に有効。 DHCPで割り当てるIPアドレスのリース時間を1 ～1440分までの範囲で設定します。パソコンを継続的に使用する場合は、自動的に再リースされます。
配送ゲートウェイアドレス	DHCPサーバを「使用する」場合に有効。 パソコンに配送するゲートウェイアドレスです。本機器以外のネットワーク機器を標準のゲートウェイとして使用する場合は[IPアドレス指定]を選択し、IPアドレスを入力してください。
配送DNSサーバアドレス	パソコンに配送するDNSサーバアドレスです。[自動]・[IPアドレス指定]・[配送しない]から選択してください。 [自動]： プロバイダからPPPによりDNSサーバアドレスを取得するよう指示があった場合に選択します。この場合、DNS サーバアドレスとしてLAN側IPアドレスが配送されます（本機器はDNS Proxyとなり、DNSパケットをDNSサーバに転送します）。 [IPアドレス指定]： プロバイダからDNSサーバアドレスを指示されている場合に選択し、該当のプライマリDNSサーバとセカンダリDNSサーバのIP アドレスを入力します。 [配送しない]： パソコン側でDNSサーバアドレスを指定したい場合やDNSサーバアドレスを設定しない場合に選択します。
PPPoEブリッジ	編集中の接続モードがPPPoEの場合に表示されます。 LAN側にPPPoEクライアント端末が存在した場合、その端末が送信するPPPoEパケットをブリッジングしてWAN側に中継させることができます。 「使用する」、「使用しない」から選択できます。
IPv6ブリッジ	編集中の接続モードがPPPoEの場合に表示されます。 LAN側にIPv6クライアント端末が存在した場合、その端末が送信するIPv6パケットをブリッジングして中継させることができます。 「使用する」、「使用しない」から選択できます。

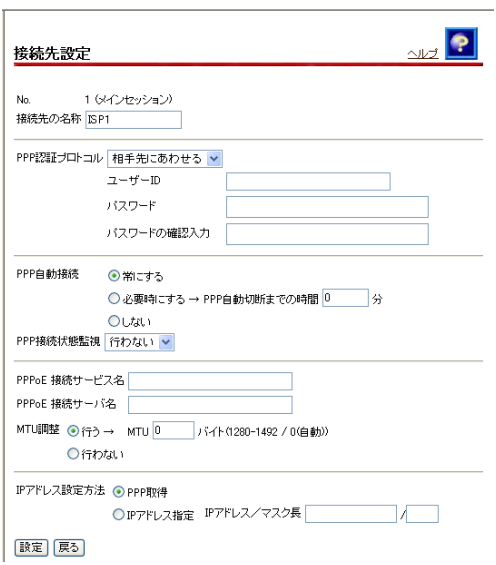
接続先設定（PPPoE接続モードのみ）

本機器のプロバイダ接続モードが「PPPoE 接続（端末型）」または「PPPoE 接続（LAN 型）」の場合に表示されます。PPPoE 接続に関する設定項目と PPPoE サブセッションの定義・接続ルールについての情報を設定します。メインセッションは 1 つ、サブセッションは最大 7 つ登録することができます。

ここではメインセッションとサブセッションに共通の設定項目を示します。サブセッション接続ルールについては、「PPPoE マルチセッションを使用するには」（☞ p. 98）を参照してください。

① NO.1 の（メインセッション）をクリックしてください。



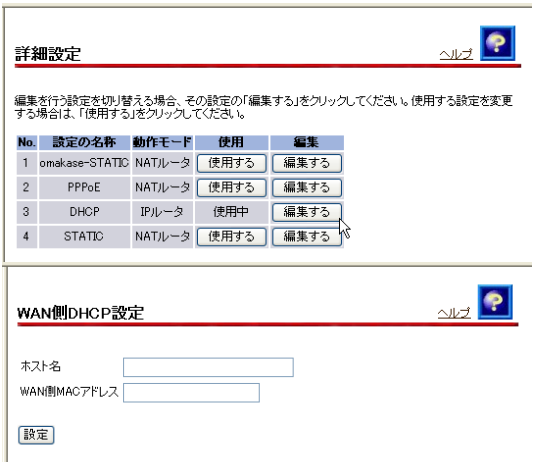


設定項目	内容
接続先の名称	接続先を識別するためにわかりやすい名称を登録します。入力は半角英数字および記号（一部の記号を除く）を使用できます。半角カナや漢字は使用できません。また、文字数は16文字以内です
PPP認証プロトコル	認証プロトコルを「認証なし」、「相手先にあわせる」、「PAP」、「CHAP」の中から選択します。 ※プロバイダから特に指定が無い場合は「相手先にあわせる」を選択してください。プロバイダから指示があった場合は、その指示に従ってください。
ユーザーID	PPPサーバに送信するユーザーIDを入力します。一般にユーザーIDは契約したプロバイダから提供されます。
パスワード	PPPサーバに送信するパスワードを入力します。一般にパスワードはユーザーIDとともに契約したプロバイダから提供されます。
パスワードの確認入力	確認のため、パスワードを再度入力します。
PPP自動接続	プロバイダとのPPP接続を自動的に行うか否かを選択します。 [常にする]： WAN側リンク確立時にPPPを自動接続します。また、何らかの理由でPPPが切断された場合も自動的に再接続します。通常は[常にする]を選択してください。 [必要時にする]： インターネットへのアクセスを開始する時点でプロバイダと自動的に接続します。[必要時にする]を選択した場合は「PPP自動切断までの時間（分）」を入力します。 [しない]： PPPによるプロバイダとの接続を手動で行います。この場合、PPPの接続はメニューフレームの[PPP切断／接続]を選択して行ってください。
PPP状態監視	PPPの接続状態を監視するか否かを選択します。 [行う]： PPPのLCP Echoという機能を使用していてPPPの接続が保持されているかどうかを確認します。5分ごとに確認を行い、3回連続で保持されていないと判定した場合に、PPPの切断を行います。 [行わない]： PPPの接続状態の監視は行いません。
PPPoE接続サービス名	PPPoEの接続先のサービス名を入力します。 ※設定については、契約したプロバイダの指示に従ってください。特に指示がない場合は空欄としてください。
PPPoE接続サーバ名	PPPoEを使用する場合に、接続先のサーバ名を入力します。 ※設定については、契約したプロバイダの指示に従ってください。特に指示がない場合は空欄としてください。
MTU調整	「行う」、「行わない」から選択します。 「行う」を選択した場合、0(自動調整)または1280-1492の固定値を選択してください。「行わない」を選択した場合、MTUは1500固定となります。

設定項目	内容
IPアドレス設定方法	WAN側のIPアドレスの設定方法を選択します。 [PPP取得]： プロバイダから特に指定が無い場合は[PPP取得]を選択してください。 [IPアドレス指定]： WAN側のIPアドレスを指定する場合は[IPアドレス指定]をチェックして、IPアドレスとマスク長を入力してください。 [Unnumbered]： （IPルータモード時のみ表示）固定IPアドレス利用時にプロバイダからWAN側のIPアドレスの指定が無い場合は[Unnumbered]、ルータID番号「LAN」を選択してください。

WAN側DHCP設定（DHCP接続モードのみ）

DHCP 接続モードを選択した場合にのみ表示されるメニューです。
ホスト名と WAN 側 MAC アドレスを入力してください。



- ホスト名はプロバイダから特に指定がある場合に入力します。プロバイダによってはデバイス名と呼ぶ場合もあり、また、パソコンのコンピュータ名入力欄に入力する ID と指示されている場合もあります。
- WAN 側 MAC アドレスは、利用するプロバイダから指定された場合に限り、本機器の WAN 側 MAC アドレスを変更することができます。（CATV などで固定の MAC アドレスしかプロバイダ側がサポートしない場合）

注意 **プロバイダが指定されていない場合には空欄としてください。**

WAN側IP設定（固定IP接続モードのみ）

固定 IP（Static）接続モードを選択した場合にのみ表示される画面です。動作モードが「NAT ルータ」、「IP ルータ」、「GapNAT」の場合にのみ表示されます。プロバイダから割り当てられたグローバルアドレスのうち、本機器の WAN 側に設定する IP アドレスを「IP アドレス／マスク長」の形式で入力してください。「GapNAT」の場合のみ、接続先 IP アドレスとして、WAN 側のインタフェースで本装置と通信する相手の IP アドレスを入力してください。

オプション設定

NTPアドレス設定

本機器の内部ログ情報などで使用している時刻を、NTP サーバを登録することで自動であわせることができます。NTP 優先サーバと代替サーバの IP アドレスを入力してください。

Memo NTP サーバを登録しない場合、「時刻の設定」（☞ p.86）で現在時刻を設定してください。本機器は内部時計にてログ情報等に時刻を表示します。ただし、電源供給がなくなると、時刻を忘れます。また、長時間運用していますと誤差が生じることがありますので、定期的に時刻合わせを行うようにしてください。

Memo 時刻の設定はログ情報にのみ使用されていますので、時刻誤差が他の機能に影響を及ぼすようなことはありません。

Memo NTP サーバ「210.173.160.87」は、独立行政法人通信総合研究所と NTT、IIJ、インターネットマルチフィードが公開している試行サービスの NTP サーバ「ntp3.jst.mfeed.ad.jp」です。
（参考：http://www.jst.mfeed.ad.jp/）
NTP サーバ「133.100.9.4」は、福岡大学情報工学科情報アーキテクチャ部門が公開している NTP サーバ「drake.nc.fukuoka-u.ac.jp」です。（参考：http://www.fukuoka-u.ac.jp/）
※公開 NTP サーバサービスは、利用者責任でご利用ください。サービスの停止、欠陥、及びそれらが原因となり発生した損失については、当社およびサービス提供者は一切責任を負いません。

DHCP固定IPアドレス配布設定

DHCP サーバが配布する IP アドレスを固定したい端末の MAC アドレスを設定します。固定したい IP アドレスの右横にある「MAC アドレス」欄に、その IP アドレスを配布する端末の MAC アドレスを入力します。入力後、 設定 ボタンをクリックすると、固定 IP アドレスの配布設定は完了です。

Memo 最大 16 件まで設定可能です。

Memo MAC アドレスの確認方法は、「パソコンの IP アドレスや MAC アドレスを確認するには」（☞ p.169）を参照してください。

注意 17 件目以降の設定は無効になります。

注意 割り当て IP アドレス個数の変更により、設定していた IP アドレスが割り当て IP アドレスの範囲外になった場合は、その設定は無効になります。

UPnP設定

本機器では UPnP IGD（Internet Gateway Device）機能をサポートしています。本機器の工場出荷時では UPnP 機能は利用可能な状態となっています。ここでは UPnP NAT 情報の自動消去や UPnP を利用するパソコンを限定することができます。
使用する UPnP 端末が多く、短時間に本機器の内部 UPnP NAT テーブルを消費するような場合に本設定が必要です。

Memo 本機器では本設定の必要のないことの目安として、LAN 側で同時に使用する UPnP 対応パソコンの上限数を 10 台以下としています。

Memo 本機器の動作モードが IP ルータの場合は、UPnP 機能は動作しません。オプション設定メニューにも本設定は表示されません。

設定項目	内容
UPnPを「使用する」	UPnP機能を動作させます。「使用しない」とすれば機能を停止します。
UPnP優先接続先	フレッツ・コミュニケーションを使う場合に、フレッツ・コミュニケーションの接続先設定を登録しているセッションを選択します。
UPnP NAT設定情報の自動消去	UPnP端末が起動されてUPnP NAT情報が登録された時刻から、ここで指定した時間を経過した場合にUPnP NAT情報を強制的に消去します。UPnP NAT情報が使用中の場合は消去を行わずに期間の延長をします。 「行わない」：初期値です。 「1時間後に行う」、「2時間後に行う」、「4時間後に行う」、「6時間後に行う」、「12時間後に行う」、「24時間後に行う」 から選択します。
UPnPの使用を許可するIPアドレス	UPnPを受け付けるLAN側端末のIPアドレスを10件まで登録できます。1件でも登録されると、登録外端末からのUPnP要求は受け付けません。

Memo UPnP 機能の詳細については、「UPnP 機能と Windows/MSN Messenger」（☞ p.142）を参照してください。

Memo フレッツ・コミュニケーションは、NTT 西日本が提供しているフレッツユーザー同士の映像通信サービスです。詳細については、「フレッツ・コミュニケーションを利用する」（☞ p.117）、および以下の WWW サイトを参照してください。
URL：http://www.ntt-west.co.jp/flets/fc/

注意 「UPnP 優先接続先」で、フレッツ・コミュニケーションの接続先設定を登録しているセッションを選択すると、他の UPnP 機能が利用できなくなります。

IPスタティックルート設定

既存LANに本機器を接続する場合にルーティング設定が必要になることがあります。「IPスタティックルート」はスタティックにIPルーティングテーブルの内容を設定するもので、最大32個まで設定が可能です。

設定項目	内容
宛先アドレス／マスク長	宛先（サブ）ネットワークアドレスをIPアドレスとそれに対応するマスク長の組合せで設定します。
ゲートウェイアドレス	宛先へのゲートウェイアドレスを設定します。
ホップカウント	本機器でRIPを使用する場合のみ意味を持ちます。宛先ネットワークまでのホップ数を1～15までの範囲で設定してください。

・ デフォルトルートを設定する場合は、以下の値を入力してください。

宛先ネットワークアドレス： 0.0.0.0/0

ゲートウェイアドレス： 接続先ルータのアドレス

ポップカウント： 13

RIP設定

本機器の動作モードを「NATルータ」または「IPルータ」とした場合に、RIP機能が利用できます。（ただし、固定IP接続モードでは利用できません。）RIP機能は動的にルーティング情報を交換するもので、LAN側にはRIP対応のルータか端末が必要です。

・ 設定項目は[LAN側RIP設定]で以下の4つから選択します。

- ルーティング情報の送受信を行わない。（RIP非活性）
- ルーティング情報の受信を行う。
- ルーティング情報の送信を行う。
- ルーティング情報の送受信を行う。

（GapNAT通過）・NATアドレス変換設定（ワンタッチNAT設定）

本機器の動作モードを「NAT ルータ」「GapNAT」または「マルチ GapNAT」として使用する場合は、IP アドレスの変換と同時に自動的に TCP/UDP ポート番号の変換を行います。特別なプロトコルを使用している場合や外部から LAN 上の WWW サーバに対してアクセスを許可したい場合等には自動変換を止め、変換方法を指定する必要があります。

パケット中継時にポート番号の変換を行わない場合は、「NAT アドレス変換設定」にて設定します。（最大 64 件まで設定可能）ここで登録したポート番号を持つパケットについては IP アドレスの変換のみが行われます。
パケットが持つポート番号を別の番号に固定的に変換する場合は、次項の「NAT アドレス・ポート変換設定」（☞ p.63）を参照し設定してください。
よく使われる設定についてはワンタッチ設定を用意しています。ワンタッチ設定は接続先 1（メインセッション）に対して有効です。

注意 **本機器の動作モードが「GapNAT」または「マルチ GapNAT」の場合は GapNAT でグローバルアドレスが割り当てられた端末と接続先 1 との間の通信に対して有効となります。**

注意 **ワンタッチ設定を利用する場合は、事前に「IP フィルタの設定」の[外部装置から開始される TCP セッションを遮断]のチェックを外して設定してください。**

◆ [WWW サーバを外部に公開する]
LAN 側で外部に公開する WWW サーバの IP アドレスの設定が必要です。（NAT アドレス変換テーブルの No.1 が使用されます。）

◆ [FTP サーバを外部に公開する]
LAN 側で外部に公開する FTP サーバの IP アドレスの設定が必要です。（NAT アドレス変換テーブルの No.2 と No.3 が使用されます。）

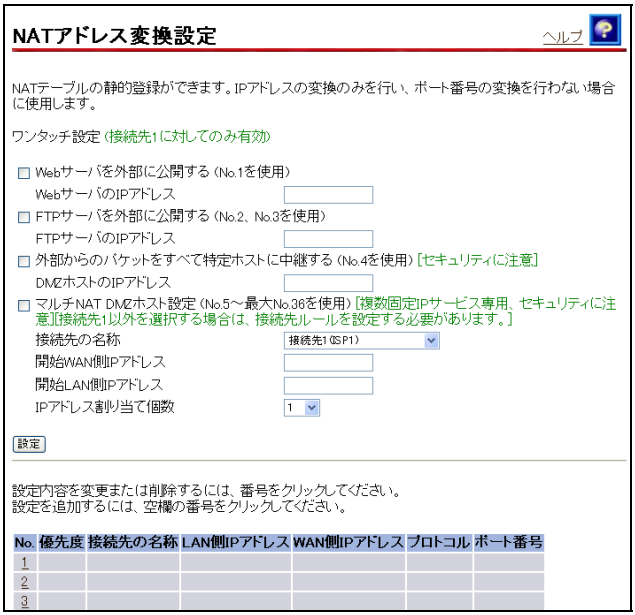
◆ [外部からのパケットをすべて特定ホストに中継する]
LAN 側に設置する DMZ ホストの IP アドレスの設定が必要です。（NAT アドレス変換テーブルの No.4 が使用されます。）

◆ [マルチ NAT DMZ ホスト設定]
複数のグローバル IP アドレスを保持しているときに使用します。入力した IP アドレスおよび割り当て個数に基づき、マルチ NAT 設定を行います。（NAT アドレス変換テーブルの No.5 が使用されます。）

注意 **[外部からのパケットをすべて特定ホストに中継する]設定を行うと、LAN 側に接続した他のパソコンはインターネットへのアクセスができなくなります。**

注意 **DMZ ホストを構築する場合は、[外部からのパケットを全て特定ホストに中継する]にチェックして、[DMZ ホストの IP アドレス]に DMZ ホストに割り当てる IP アドレスを入力してください。**

注意 **外部からのパケットをすべて中継するため、NAT 機能によるセキュリティの効果はなくなります。外部からの不正アクセスには十分ご注意ください。**



個別に設定内容を見たい場合や変更したい場合は表形式で表されている NAT アドレス変換テーブルの[No.（1～64）]をクリックし、設定画面を表示させます。
追加したい場合は未登録の No を選択してください。
設定が終えたら、 設定 をクリックします。

設定項目	内容
優先度	この条件の優先度を0～99までの範囲で設定します。各条件はこの値の小さい順に評価され、最初に合致した条件だけがNATの動作に反映されます。「0」を指定した場合、設定は無効になります。複数の条件に同じ優先度を指定することはできませんが、例外として「0」だけは同時に複数指定することができます。
接続先の名称	この設定を適用するWAN側接続先を接続先1～8から選択します。
LAN側IPアドレス	適用するLAN側パソコンのIPアドレスを設定します。
WAN側IPアドレス	NAT変換後のWAN側でのIPアドレスを設定します。通常は[自分のWAN側IPアドレス]を選択してください。
プロトコル	WAN側に公開したいアプリケーションが使用するプロトコルを指定します。プロトコルを指定する場合は、「TCP」、「UDP」、「TCPとUDP両方」、「ICMP」、「GRE」、「全プロトコル(共有)」、「全プロトコル(占有)」のいずれかを選択してください。「TCP」、「UDP」、「TCPとUDP両方」を選択した場合はポート番号の指定も行ってください。全てのプロトコルについて通過を許可する場合で、LAN側IPアドレスで指定した以外の端末を使って外部との通信を行う時は全プロトコル(共有)を、行わない時は全プロトコル(占有)を選択してください。 「全プロトコル」を選択した場合は、すべてのプロトコルが変換対象となります。また、「TCPとUDP両方」については、すべてのポートを指定した場合と同様となります。セキュリティを十分に考慮して設定してください。
ポート番号	中継時に変換しないポート番号の範囲を入力します。最小値と最大値を「-（ハイフン）」で区切って設定してください。また、変換しないポート番号が1つの場合は、最小値と最大値に同じ値を入力してください。

注意 NAT アドレス変換設定の設定、変更、削除を行った時点で設定した内容が動作に反映されるため、その時点で通信しているセッションが遮断されることがあります。

Memo NAT ルータで使用時に正常動作しない通信対戦ゲーム等の通信アプリケーションの中には、本設定によりアプリケーションが使用するポート番号を変換しないように設定することで正常動作するものがあります。

Memo LAN 側に PPTP サーバを設置する場合は、プロトコル「TCP」・ポート番号「1723-1723」の設定が必要となります。

Memo LAN 側に IPsec サーバを設置する場合は、プロトコル「UDP」・ポート番号「500-500」の設定が必要となります。

NATアドレス・ポート変換設定

本機器の LAN 側に接続された端末上のアプリケーションを WAN 側に公開するなど、端末上のアプリケーションと本機器の WAN 側の well-known な TCP/UDP ポートを関係付けるために NAT アドレス・ポート変換を静的に設定します。
最大登録件数は 64 件で、優先度の高いものから順に処理されます。
本設定と NAT アドレス変換との違いは、NAT アドレス変換が IP アドレスを変換するだけでポート番号を変換しないのに対し、本設定はポート番号も同時に変換する点です。例えば、LAN 側に接続された 2 台の端末で同時に telnet サーバ(TCP/23 番ポート)を WAN 側に公開する必要がある場合、NAT アドレス変換ではアプリケーションのポート番号が重複するため、このような設定はできませんが、本設定では一方を WAN 側の 2023 番ポート、他方を 3023 番ポートに割り当てることができます。なお、本設定は NAT アドレス変換の設定よりも優先して処理されます。

設定内容を変更または削除するには、番号をクリックしてください。
設定を追加するには、空欄の番号をクリックしてください。

設定項目	内容
優先度	この条件の優先度を0～99までの範囲で設定します。各条件はこの値の小さい順に処理され、最初に合致した条件だけがNATの動作に反映されます。「0」を指定した場合、設定は無効になります。複数の条件に同じ優先度を指定することはできませんが、例外として「0」だけは同時に複数指定することができます。
接続先の名称	この設定を適用するWAN側接続先を接続先1～8から選択します。
LAN側IPアドレス	適用するLAN側パソコンのIPアドレスを設定します。
WAN側IPアドレス	NAT変換後のWAN側でのIPアドレスを設定します。通常は[自分のWAN側IPアドレス]を選択してください。
プロトコル	WAN側に公開したいアプリケーションが使用するプロトコルを指定します。プロトコルを指定する場合は、「TCP」、「UDP」、「TCPとUDP両方」のいずれかを選択してください。
LAN側ポート番号	NATを使用するアプリケーションがLAN側端末上で使用するポート番号を設定します。また、一部のアプリケーションについてはポート名で指定することも可能です。
WAN側ポート番号	WAN側において公開アプリケーションが使用するポート番号を設定します。WAN側からはこのポート番号を指定してLAN側端末上で実行中のアプリケーションにアクセスすることができます。

注意 NAT アドレス変換設定の設定、変更、削除を行った時点で設定した内容が動作に反映されるため、その時点で通信しているセッションが遮断されることがあります。

Memo LAN 側ポート番号と WAN 側ポート番号に同じポート番号を設定した場合は、「NAT アドレス変換設定」で設定した場合と同様に動作しますが、本設定は、「NAT アドレス変換設定」の設定内容よりも優先して処理されます。

ダイナミックDNS設定

ダイナミック DNS（DDNS）サービスプロバイダが提供する DNS サーバに、割り当てを受けたドメイン名に自分の IP アドレスを登録・更新する機能です。最大 2 つまでの DDNS プロバイダの IP アドレスを登録できます。
現在サポートしている DDNS サービスは以下の 4 つです。

- miniDNS.net
- Dynamic Do!.jp
- MyDNS.jp
- DynDNS

通知のタイミングは、(1)PPP がリンクアップし IP アドレスが変わった場合、(2)自動更新間隔で設定した時間が経過した場合、(3)本設定画面の設定ボタンを押した場合、に IP アドレスを通知します。本設定は IP アドレスの更新のみを行うため、ホスト名などの登録は各 DDNS 登録サイトにてあらかじめ行っておく必要があります。また、サイトによっては通知した IP が有効になるまで 3～4 日程度かかる場合があります。

設定項目	内容
登録サイト名	上記DDNSサービスから選択
更新IPアドレス	接続先1～8いずれかのIPアドレス
登録ホスト名	プロバイダから指定されたホスト名
登録ユーザーID	ダイナミックDNS登録時に通知されたユーザIDです。miniDNS.jp使用の場合"Login ID"として通知されたもの、Dynamic Do!.jp 使用の場合"登録ドメイン"として通知されたものを入力してください。
登録パスワード	プロバイダから指定されたパスワード
登録パスワードの確認入力	登録パスワードと同じ値を入力してください。
通知間隔	IPアドレスの更新を自動通知させたい時間を分単位で入力してください。設定ボタンを押した時点で更新が通知されますので、自動更新は設定ボタンを押した時点から設定した時間経過する度に自動的に更新通知をおこないます。 「0」を設定した場合はIPアドレスの更新を通知しません。
WildCardを「使用する」	WildCard機能を使うか使わないかを指定します。dynDNSのみこの値が反映されます。
MailExchangerを「使用する」	MailExchanger機能を使うか使わないかを指定します。使用する場合はメールアドレス欄に希望の値を入力してください。dynDNSのみこの値が反映されます。
メールアドレス	MailExchanger機能を使う場合に希望するメールアドレスを入力します。dynDNSのみこの値が反映されます。
Backup MXを「使用する」	MailExchanger機能を使う場合にBackup MXを使うか使わないかを指定します。dynDNSのみこの値が反映されます。

メール着信通知設定

登録したメールサーバに定期的に新着メールの到着を確認し、メール着信が確認された場合は本機器の前面パネルの MAIL ランプでお知らせする機能です。認証タイプは“標準”（POP）と“APOP”に対応しています。
メールサーバとユーザーID の組合せは最大 4 件まで登録できます。No をクリックして設定してください。
送信者フィルタを登録すると、From 行にマッチしたメールだけの着信を確認することができます。送信者フィルタは 8 件まで登録可能です。

注意 送信者フィルタはメールサーバに貯まったメールのうち最新の 100 件分のみを対象としています。

設定項目	内容
メールサーバ名	メールサーバの名前またはIPアドレスを入力してください。
認証タイプ	メールサーバに対する認証タイプを指定してください。 「標準」、「APOP」から選択します。
ユーザーID	メールアカウントのユーザーIDを入力してください。
パスワード	メールアカウントのパスワードを入力してください。
パスワードの確認入力	パスワードと同じ値を入力してください。
着信確認	メールのチェックを行う間隔を「5分」、「10分」、「30分」、「1時間」、「行わない」から選択してください。
送信者フィルタ1～8	送信者フィルタに相手のメールアドレスの一部または全部を指定して、特定の相手からのメールが着信したときのみMAILランプを点滅させるように設定できます。各フィルタのどれかひとつの条件に一致した場合に有効となります。

syslogサーバ設定

本機器が保持している「機器状態ログ」と「セキュリティログ」を指定の syslog サーバに転送する機能です。LAN 側で syslog サーバを設置している場合に利用できます。
登録できるサーバは 1 台のみです。

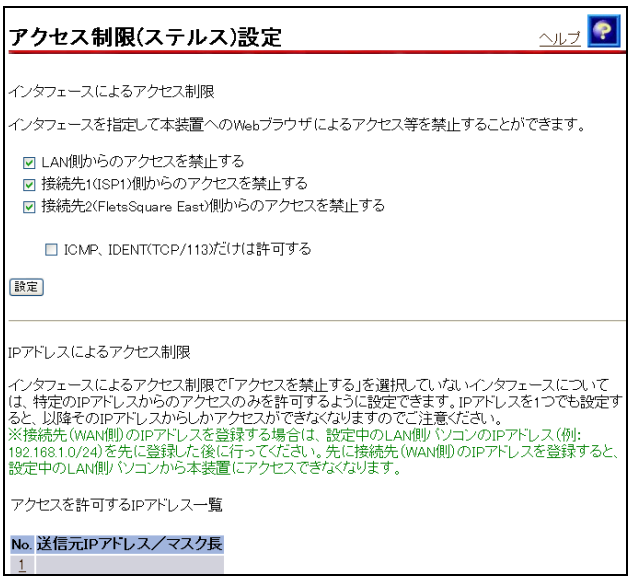
設定項目	内容
syslogサーバ名	syslogサーバの名前またはIPアドレスを入力してください。
イベントログの通知 「使用する」	本機器が保持する「機器状態ログ」の転送を行います。
セキュリティログの通知 「使用する」	本機器が保持する「セキュリティログ」の転送を行います。

セキュリティ設定

アクセス制限（ステルス）設定

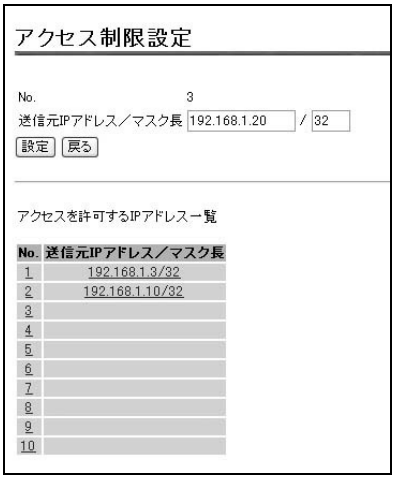
本機器に対する WWW でのアクセスを「インタフェースによる制限」と「IP アドレスによる制限」を設定することができます。

注意　「インタフェースによる制限」は「IP アドレスによる制限」よりも優先します。



「インタフェース指定による制限」は WAN 側（接続先を複数設定している場合には各接続先が対象）と LAN 側の各々についてアクセスの禁止を設定します。ICMP（Ping 等）や IDENT（TCP/113 ポート）のみのアクセスを例外的に許可することもできます。
すべてのインタフェースからのアクセスを禁止することはできません。

「IP アドレス指定による制限」は 1 件でも登録された場合、登録 IP アドレスからのアクセスしか受け付けません。たとえば、本機器の設定ページを編集する管理者を 2 名に限定したい場合、その管理者が使用するパソコンの IP アドレスを登録してください。
1 件も登録されていない場合は、すべての送信元からのアクセスを許可します。



Memo 送信元 IP アドレス／マスク長の入力
登録する IP アドレスをアドレスとマスク長で入力しますので、たとえば、IP アドレスの下 1 バイトを特定しない場合は、192.168.1.0／24 のように指定することもできます。

注意 WAN 側から特定の IP アドレスからのアクセスを許し、LAN 側から自由にアクセスしたい場合は、IP アドレス指定により、WAN 側の特定 IP アドレスとともに、LAN 側ネットワークアドレス（ex.192.168.1.0/24）の 2 件を登録してください。

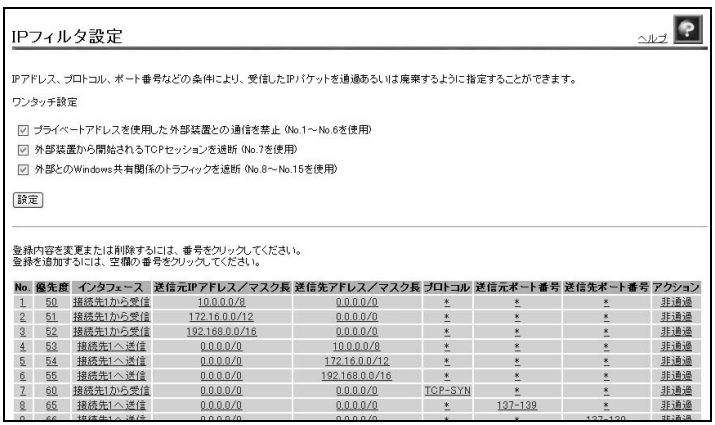
注意 アクセス制限（ステルス）設定を行った後、設定ページにアクセスできなくなった場合は、「一時的に工場出荷時設定で起動する」（☞ p156）を参照してください。

SPI(ステートフル・パケット・インスペクション)設定

本機器の動作モードが「NAT ルータ」、「GapNAT」、「マルチ GapNAT」の場合に、ステートフル・パケット・インスペクション機能を利用することができます。
SPI 機能を使用することにより、WAN 側と LAN 側でパケット中継を行っているとき、LAN 側から WAN 側への送信パケットとそれに対応する WAN 側からの受信パケットとの整合性を検査して、不正なパケットを破棄することができます。
設定は「ステートフル・パケット・インスペクション機能」を「使用する」、「使用しない」です。

IPフィルタ設定（ワンタッチ設定）

IP アドレス、プロトコル、ポート番号の条件を指定することより、受信した IP パケットを通過あるいは廃棄することができます。条件を適切に設定（最大 128 個まで設定可能）することにより、特定のサービスやホスト間の通信を禁止するための簡易ファイアウォールを構築することができます。優先度の小さい順からフィルタリングの処理が行われます。



本画面では、よくあるフィルタ条件をワンタッチで設定できるワンタッチ設定があります。これは接続先 1（メインセッション）へのアクセスに対して有効です。

◆ **［プライベートアドレスを使用した外部装置との通信を禁止］**
インターネット上には、プライベートアドレス（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）を持った端末装置は通常存在しません。この項目を選択することにより、発信元アドレスをプライベートアドレスにして発信元を確認できないようにした（なりすまし）端末装置からの不正なアクセスを防止します。

注意 **プライベートアドレスを利用して運営するサイトに接続する場合はチェックをはずしてください。**

◆ [外部装置から開始される TCP セッションを遮断]

WWW 参照、FTP 等の TCP セッションを外部から開始されて、LAN 側のパソコンを不正に操作される可能性があります。この項目を選択することにより、インターネット側の不特定ユーザから TCP でアクセスされることを防止します。

注意 「NAT アドレス変換」のワンタッチ設定を利用する場合は、このチェックを外してください。

注意 ftp クライアントをポートモード（アクティブモード）で使用する場合は、このチェックを外してください。

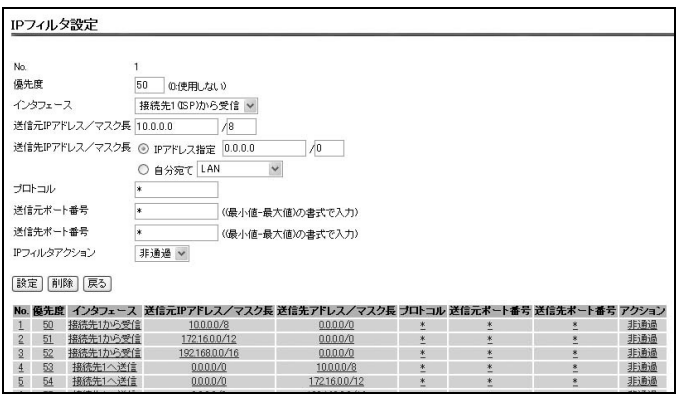
◆ [外部との Windows 共有関係のトラフィックを遮断]

Windows の共有を行った場合、不特定のユーザから自分のパソコンのファイルを参照、変更される可能性があります。この項目を選択することにより、外部装置との間で Windows 共有が行われなくなります。

個別に設定内容を見たい場合や変更したい場合は表形式で表されているフィルタ条件の No.（1～128） をクリックし、設定画面を表示させます。

追加したい場合は未登録の No を選択してください。

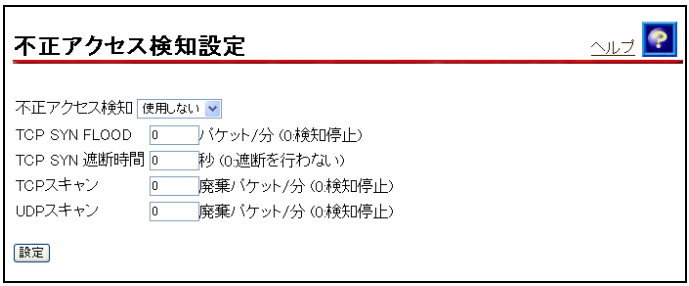
設定が終えたら、 設定 をクリックします。



設定項目	内容
No	エントリNoです。あらかじめ1から128番までが用意されています。既に登録されているものを編集した場合はその内容が上書きされます。
優先度	この条件の優先度を0～128までの範囲で設定します。各条件はこの値の小さい順に評価され、最初に合致した条件だけがIPフィルタの動作に反映されます。 「0」を指定した場合、設定は無効になります。また、値が小さいほど優先度は高くなります。複数の条件に同じ優先度を指定することはできませんが、例外として「0」だけは同時に複数指定することができます。
インタフェース	インタフェースに関するフィルタリング条件です。インタフェースの種類としてはLAN側あるいはWAN側を選択することができます。さらに、各インタフェースについて、そこから受信する場合とそこへ送信する場合を選択することができます。
送信元IPアドレス／マスク長	パケットの送信元IPアドレスに関するフィルタリング条件です。この値を指定する場合は、IPアドレスとマスク長の組合せで入力してください。例えば、163.221.74.0/24と指定すると、163.221.74.0～163.221.74.255がフィルタリングの対象となります。なお、全ての送信元IPアドレスをフィルタリング対象にする場合は、0.0.0.0/0を指定します。
送信先IPアドレス／マスク長	パケットの送信先IPアドレスに関するフィルタリング条件です。IPアドレスを指定する場合は、IPアドレスとマスク長の組合せで入力してください。なお、全ての送信先IPアドレスをフィルタリング対象にする場合は、0.0.0.0/0を指定します。
プロトコル	パケットのプロトコルタイプに関するフィルタリング条件です。この値を指定する場合は、1以上255以下の数値、あるいは、予約済の名前を入力してください。予約済の名前としては、*, TCP, TCP-SYN, TCP-FIN, UDP, ICMPが用意されています。大文字、小文字の区別はありません。なお、*が指定された場合は、全てのプロトコルがフィルタリング対象になります。
送信元ポート番号	パケットのTCPおよびUDPの送信元ポート番号に関するフィルタリング条件です。この値を指定する場合は、1以上65535以下の数値を入力してください。また、数値と"-"(ハイフン)を組合せて範囲を指定することもできます。さらに、予約済みの名前でポート番号を指定することもできます。予約済みの名前としては、*, ftp, ftpdata, smtp, WWW, pop3, sunrpc, nntp, ntp, login, pptp, domain, routeが用意されています。大文字、小文字の区別はされません。なお、*を指定した場合は、全ての送信元ポート番号がフィルタリング対象になります。
送信先ポート番号	パケットのTCPおよびUDPの送信先ポート番号に関するフィルタリング条件です。この値を指定する場合は、1以上65535以下の数値を入力してください。また、数値と"-"(ハイフン)を組合せて範囲を指定することもできます。さらに、予約済みの名前でポート番号を指定することもできます。予約済みの名前としては、*, ftp, ftpdata, smtp, WWW, pop3, sunrpc, nntp, ntp, login, pptp, domain, routeが用意されています。大文字、小文字の区別はされません。なお、*を指定した場合は、全ての送信先ポート番号がフィルタリング対象になります。
IPフィルタアクション	「通過」が指定された場合は、IPパケットは中継されます。「非通過」が指定された場合は、パケットは破棄されます。

不正アクセス検知設定

本機器の不正アクセス検知機能に関する設定を行います。



設定項目	内容
不正アクセス検知	不正アクセス検知機能を「使用する」「使用しない」のいずれかを選択します。「使用しない」を選択した場合、不正アクセス検知機能の使用を停止できます。
TCP SYN FLOOD	TCP SYN FLOOD攻撃と判定する受信パケット数を1～65535件の範囲で指定します。0を指定した場合は検知を停止します。WAN側からTCP SYNだけのパケットを1分間に設定パケット数以上受信した場合、TCP SYN FLOOD攻撃を受けていると見なし、機器状態・ログ、およびsyslogサーバ（syslog機能が有効な場合）へ保存します。なお正常にTCPセッションが開始されたTCP SYNパケットはTCP SYN FLOOD攻撃としては数えません。
TCP SYN 遮断時間	TCP SYN FLOOD攻撃が検知された場合に、WAN側からのTCP SYN受信を遮断する時間を1～65535秒の範囲で指定します。0を指定した場合はTCP SYN受信を遮断しません。WAN側からのTCP SYN受信が遮断している間、WAN側から開始されるTCPセッションはすべて遮断されますが、LAN側から開始されるTCPセッション、および既に通信しているTCPセッションは遮断されません。
TCPスキャン	TCPスキャン攻撃と判定する廃棄パケット数を1～65535件の範囲で指定します。0を指定した場合は検知を停止します。WAN側からのTCPパケットを1分間に設定パケット数以上廃棄した場合、TCPスキャン攻撃を受けていると見なし、機器状態・ログ、およびsyslogサーバ（syslog機能が有効な場合）へ保存します。
UDPスキャン	UDPスキャン攻撃と判定する廃棄パケット数を1～65535件の範囲で指定します。0を指定した場合は検知を停止します。WAN側からのUDPパケットを1分間に設定パケット数以上廃棄した場合、UDPスキャン攻撃を受けていると見なし、機器状態・ログ、およびsyslogサーバ（syslog機能が有効な場合）へ保存します。

注意 接続を許可するステーションの MAC アドレス一覧に何も設定せずに「使用する」を選択すると、すべての無線 LAN 端末が無線 LAN に接続できなくなりますので、注意してください。

Memo 「無線 LAN 情報」に表示されている、接続中の無線 LAN 端末を、MAC アドレス一覧に登録することができます。

Memo 本機器では IP フィルタで廃棄されたパケットを不正アクセス検知の対象外としています。

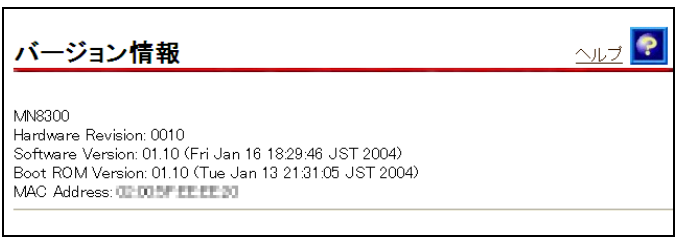
4 MN8300の情報表示について

バージョン情報

本機器のバージョン情報の一覧を表示します。

① メニューフレームより バージョン情報 をクリックします。

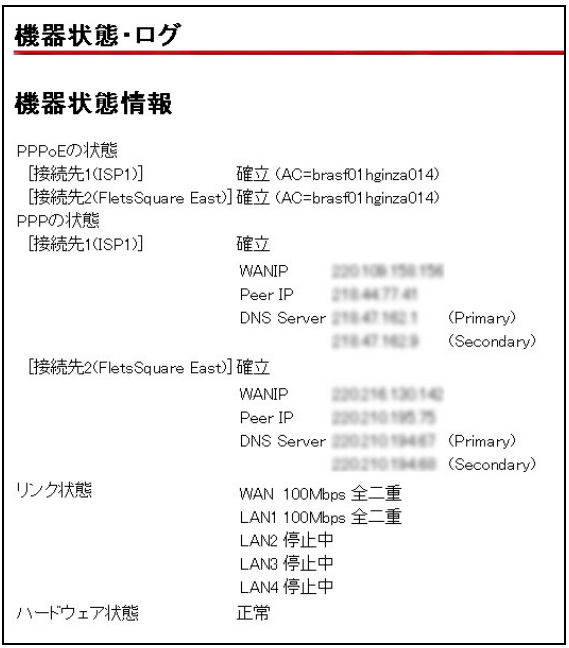
② 操作フレームにバージョン情報画面が表示されます。現在設定されているファームウェアのバージョン情報が表示されます。情報をプリントアウトして保管する場合等にご利用ください。



機器状態・ログ

通信が途切れたとき等、障害の有無を表示します。また、ログの内容を表示し、機器状態の変化について確認できます。

① メニューフレームより 機器状態・ログ をクリックします。
② 操作フレームに機器状態・ログ画面が表示されます。



※画面は PPPoE 接続モードのときの例です。

◆ 機器状態情報

PPP の状態（PPPoE 接続モードのみ表示）

PPP を使用する設定を行っている場合に PPP ネゴシエーションの状態が表示されます。

・確立・・・・・・PPP リンクが確立している

・LCP 中・・・・・リンクレイヤプロトコルのネゴシエーション中

・IPCP 中・・・・・ネットワークレイヤプロトコルのネゴシエーション中

・停止中・・・・・停止している

PPP が確立した場合、あわせて次の情報が表示されます。

・Peer IP・・・・・相手側 IP アドレス

・DNS Server・・・DNS サーバ IP アドレス

PPPoE の状態（PPPoE 接続モードのみ表示）

PPP over Ethernet を使用する設定を行っている場合に、接続の状況が表示されます。

・確立：セッションが確立している

・AC 接続中：AC（PPPoE サーバ）との接続中

・AC 探索中：AC の探索中

・停止中：停止している

「停止中」以外の場合には、次の情報があわせて表示される場合があります。

・AC：サーバ名

・SN：サービス名

LAN リンク状態（PPPoE 接続モードのみ表示）

現在の LAN インタフェースの状態を表示します。

・通信中：接続が確立している

現在の動作モード（10Mbps/100Mbps、全二重/半二重）もあわせて表示されます。

・停止中：停止している（インタフェースダウン）

・異常：何らかの異常が発生し、停止している

DHCP クライアント状態（DHCP 接続モードのみ表示）

DHCP クライアント状態を表示します。
DHCP から IP アドレスなどの情報を取得できている場合は「確立」、DHCP サーバからの応答がない場合は「停止中」と表示されます。

リンク状態（DHCP 接続モード、固定 IP 接続モードのときに表示）

WAN と LAN のインタフェースのリンク状態を表示します。
リンクアップしている場合は、「通信中」と現在の動作モードが表示されます。リンクダウンしている場合は、「停止中」が表示されます。

ハードウェア状態

本機器のハードウェア状態を表示します。

- 正常：ハードウェアに問題がない
- 異常：何らかの異常が検知された

◆ ログ情報

本機器が起動直後からメモリ上に蓄積しているログの内容を最新のものから順に表示します。
ログとともに表示される時間は、絶対時間または機器起動時点を 0 時とする相対時間です。
最大 200 件までのログが蓄積されます。200 件を超えると古いものから順に削除されます。

注意 **絶対時間を表示するには、「時刻の設定」（☞ p.86）または「NTP アドレス設定」（☞ p.57）が必要です。**

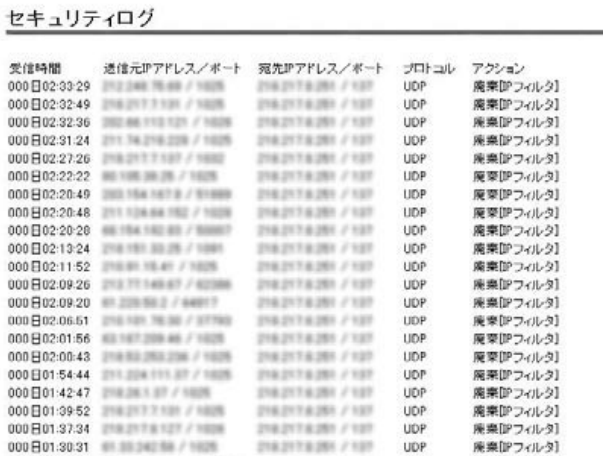
セキュリティログ

本機器が起動直後からメモリ上に蓄積しているセキュリティに関するログの内容を最大200件まで表示します。セキュリティログは以下のようなパケットの受信記録です。

- 外部から受信したパケットのうちIPフィルタ廃棄したパケット
- 外部から受信したパケットのうちNATによって廃棄したパケット
- アクセス制限によって本機器へのアクセスを拒否したパケットログは絶対時刻とともに保存されており、最新のものから順に表示されます。ただし、局側で使用されている装置によっては絶対時刻ではなく機器起動時点を0時とする相対時刻で表示される場合もありますので、時刻設定画面で時刻の設定を行ってください。

注意 「時刻の設定」（☞ p.86）または「NTPアドレス設定」（☞ p.57）での設定を行ってください。

① メニューフレームより セキュリティログ をクリックします。
② 操作フレームにセキュリティログ画面が表示されます。


セキュリティログ

受信時間	送信元IPアドレス／ポート	宛先IPアドレス／ポート	プロトコル	アクション
000日02:33:29	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:32:49	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:32:36	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:31:24	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:27:26	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:22:22	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:20:49	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:20:48	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:20:20	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:13:24	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:11:52	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:09:26	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:09:20	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:06:51	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:01:56	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日02:00:43	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日01:54:44	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日01:42:47	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日01:39:52	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日01:37:34	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]
000日01:30:31	[redacted]	[redacted]	UDP	廃棄[IPフィルタ]

表示される情報は以下の通りです。

1) 受信時刻本機器が該当するパケットを受信した時刻を表示します。

2) 送信元IPアドレス/ポート
該当するパケットのソースアドレスを表示します。プロトコルがTCPもしくはUDPの場合はあわせてポート番号を表示します。

3) 宛先IPアドレス/ポート
該当するパケットのデスティネーションアドレスを表示します。プロトコルがTCPもしくはUDPの場合はあわせてポート番号を表示します。

4) プロトコル
プロトコル番号が TCP/UDP/ICMP の場合のみ、それぞれの文字で表示します。それ以外は番号をそのまま表示させます。

5) アクション
パケットの廃棄原因を表示します。表示メッセージは以下の通りです。

a. 廃棄[IP フィルタ]
受信したパケットが IP フィルタ設定により廃棄された。

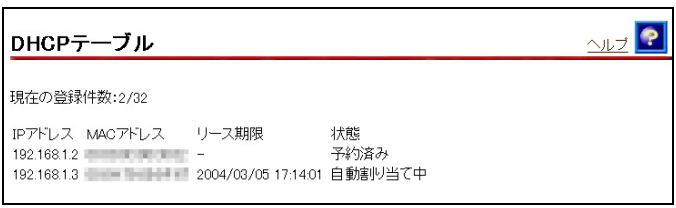
b. 廃棄[NAT]
受信したパケットが NAT 処理(WAN->LAN のエントリがない)により廃棄された。

c. 廃棄[アクセス制限]
受信したパケットがアクセス制限設定により廃棄された。

DHCPテーブル

DHCP が LAN 側の端末に配布した IP アドレスに関する情報を参照できます。
UPnP NAT 設定情報は次の手順で確認できます。

① メニューフレームから DHCP テーブル をクリックします。



[設定画面の各項目の説明]

◆ IP アドレス

DHCP が端末に配布した IP アドレスです。

◆ MAC アドレス

IP アドレスが配布された端末のネットワークインタフェースが持つ MAC アドレスです。

◆ リース期限

配布された IP アドレスの有効期限です。

◆ 状態

IP アドレスの配布状態です。通常は“自動割り当て中”と表示されますが、「DHCP 固定 IP アドレス配布設定」（☞ p.57）で割り当てられた IP アドレスは、“予約済み”と表示されます。

ルーティングテーブル

本機器の設定が DHCP 接続モード・固定 IP 接続モードであり、かつ、動作モードが NAT ルータ・IP ルータモードの場合に表示されるメニューです。
RIP により自動設定されたもの、スタティックルート、および内部の ARP テーブルの内容を表示します。

① メニューフレームより ルーティングテーブル をクリックします。
② 操作フレームにルーティングテーブル画面が表示されます。

GapNAT情報

本機器の動作モードを GapNAT・マルチ GapNAT モードの場合に表示されるメニューです。
グローバル IP アドレス割り当て状況を参照できます。

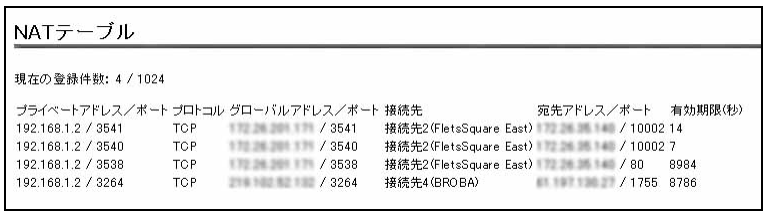
NATテーブル

本機器がアドレス変換に使用している NAT テーブルを参照することができます。自動的に生成されたテーブルと NAT 設定で定義したもののうち、使用しているものが表示されます。

① メニューフレームより NAT テーブル をクリックします。

② 操作フレームに NAT テーブル画面が表示されます。

Memo NAT テーブルは最大 4096 件まで登録できます。


NATテーブル

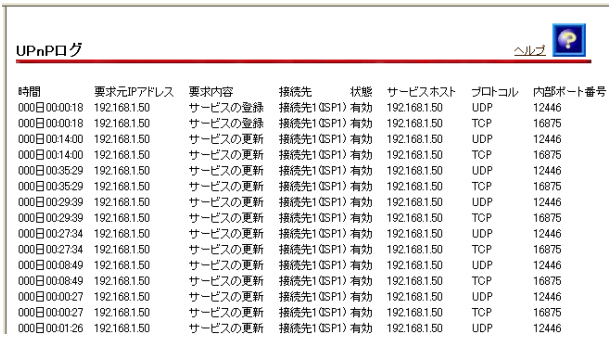
現在の登録件数: 4 / 1024

プライベートアドレス／ポート	プロトコル	グローバルアドレス／ポート	接続先	宛先アドレス／ポート	有効期限(秒)
192.168.1.2 / 3541	TCP	[redacted] / 3541	接続先2(FletsSquare East)	[redacted] / 10002	14
192.168.1.2 / 3540	TCP	[redacted] / 3540	接続先2(FletsSquare East)	[redacted] / 10002	7
192.168.1.2 / 3538	TCP	[redacted] / 3538	接続先2(FletsSquare East)	[redacted] / 80	8984
192.168.1.2 / 3264	TCP	[redacted] / 3264	接続先4(BROBA)	[redacted] / 1755	8786

UPnPログ

UPnP に対応したネットワークアプリケーションソフトウェアが本機器に対して行ったリクエストのログを最新のものから表示します。最大ログ件数は 100 件です。100 件を超えた場合は、古いものから順に消去されます。UPnP ログは以下の手順で確認できます。

① メニューフレームより UPnP ログ をクリックします。


UPnPログ

ヘルプ

時間	要求元IPアドレス	要求内容	接続先	状態	サービスホスト	プロトコル	内部ポート番号
000日00:00:18	192.168.1.50	サービスの登録	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:00:18	192.168.1.50	サービスの登録	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:14:00	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:14:00	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:35:29	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:35:29	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:29:39	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:29:39	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:27:34	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:27:34	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:08:49	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:08:49	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:00:27	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446
000日00:00:27	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	TCP	16875
000日00:01:26	192.168.1.50	サービスの更新	接続先1(ISP1)	有効	192.168.1.50	UDP	12446

［設定画面の各項目の説明］

◆ **時間**

ログは時刻設定を行っていない場合は、機器起動時点を 0 時とする相対時刻で表示されます。

◆ **要求元 IP アドレス**

IP アドレスリクエストを送信した IP アドレスが表示されます。

◆ **要求内容**

リクエストの内容が表示されます。表示内容は次のいずれかの項目です。

● UPnP 用の静的 NAT 設定情報が操作された場合

1）サービスの登録　　UPnP 用静的 NAT 設定情報が新規登録された。
2）サービスの削除　　UPnP 用静的 NAT 設定情報が削除された。
3）サービスの更新　　UPnP 用静的 NAT 設定情報が更新された。
4）サービスの全削除　　UPnP 用静的 NAT 設定情報が WWW から全削除された。
5）登録不可　　UPnP 用静的 NAT 設定情報が最大件数 80 件を超えた。

● PPP 接続／切断要求があった場合

1）PPP 接続要求　　PPP の接続要求があった。
2）PPP 切断要求　　PPP の切断要求があった。

以下の情報は UPnP 用の静的 NAT 情報に対するリクエストがあった場合にだけ表示されます。

◆ **接続先**

登録された UPnP 用の静的 NAT 設定情報の接続先を表示します。

◆ **状態**

登録された UPnP 用の静的 NAT 設定情報の状態を表示します。
以下 2 つの状態を表示します。

1）有効　　登録された UPnP 用の静的 NAT 設定情報は使用される。
2）無効　　登録された UPnP 用の静的 NAT 設定情報は使用されない。

◆ **サービスホスト**

登録された UPnP 用の静的 NAT 設定情報の LAN 側 IP アドレスを表示します。

◆ **プロトコル**

登録された UPnP 用の静的 NAT 設定情報のプロトコルを表示します。TCP もしくは UDP のいずれかを表示します。

◆ **外部ポート番号**

登録された UPnP 用の静的 NAT 設定情報の WAN 側ポート番号を表示します。

◆ **内部ポート番号**

登録された UPnP 用の静的 NAT 設定情報の LAN 側ポート番号を表示します。

◆ **有効期限**

UPnP 用の静的 NAT 設定情報の有効期限を秒数で表示します。Windows/MSN Messenger から設定される静的 NAT 設定情報はすべて“無期限”が指定されます。

UPnP CP（コントロールポイント）テーブル

本機器で認識されたUPnPに対応したネットワークアプリケーションソフトウェアが動作しているパソコンのIPアドレスとMACアドレスを表示します。最大10件が表示されます。

UPnPに対して無通信が続くとOSによって以下の時間経過後に消去されます。

- **Windows Meの場合：約10分**
- **Windows XPの場合：約30分**

また、ARPの有効期限が切れた場合MACアドレスは00:00:00:00:00:00で表示されます。
UPnP CP（コントロールポイント）テーブルは次の手順で確認できます。

① **メニューフレームから UPnP CP テーブル をクリックします。**

UPnP NAT設定情報

UPnP に対応したネットワークアプリケーションソフトウェアが本機器に登録した NAT 設定情報を表示します。最大 128 件まで表示されます。

UPnP NAT 設定情報は次の手順で確認できます。

① メニューフレームから **UPnP NAT 設定情報** をクリックします。

［設定画面の各項目の説明］

◆ **状態**

登録された UPnP 用の静的 NAT 設定情報の状態を表示します。以下 2 つの状態を表示します。

1)有効　　登録された UPnP 用の静的 NAT 設定情報は使用されている。

2)無効　　登録された UPnP 用の静的 NAT 設定情報は使用されていない。

◆ **サービスホスト**

登録された UPnP 用の静的 NAT 設定情報の LAN 側 IP アドレスを表示します。

◆ **接続先**

登録された UPnP 用の静的 NAT 設定情報の接続先を表示します。

◆ **プロトコル**

登録された UPnP 用の静的 NAT 設定情報のプロトコルを表示します。TCP もしくは UDP のいずれかを表示します。

◆ **内部ポート番号**

登録された UPnP 用の静的 NAT 設定情報の LAN 側ポート番号を表示します。

◆ **外部ポート番号**

登録された UPnP 用の静的 NAT 設定情報の WAN 側ポート番号を表示します。

◆ **有効期限**

UPnP 用の静的 NAT 設定情報の有効期限を秒数で表示します。Windows/MSN Messenger から設定される静的 NAT 設定情報はすべて“無制限”が指定されます。

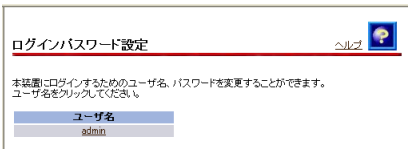
◆ **サービスの説明**

Windows/MSN Messenger 等の UPnP に対応したネットワークアプリケーションソフトウェアによって設定された説明を最大 60 文字で表示します。

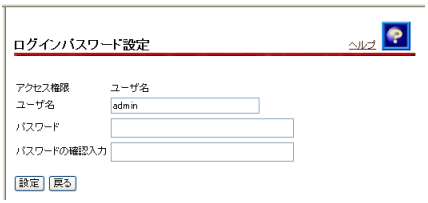
ログインパスワードの設定

セキュリティ上の観点から、運用開始後は以下の手順により「ユーザ名」「パスワード」を変更されることをお勧めします。

① 「詳細設定」ページのメニューフレームより ログインパスワード設定 をクリックしてください。操作フレームにログインパスワード設定画面が表示されます。



② アクセス権限 の「admin」をクリックしてください。一般ユーザ用の設定画面が表示されます。



◆ [ユーザ名]

ユーザー名を入力してください。32 文字以内の半角英数文字が使用できます。（大文字と小文字は区別されます。）

◆ [パスワード]

パスワードに新しいパスワードを入力してください。32 文字以内の半角英数文字が使用できます。(大文字と小文字は区別されます。）尚、入力した文字列はそのまま表示されず、8 文字の“********”に置き替えて表示されます。

◆ [パスワードの確認入力]

パスワードの確認入力に新しいパスワードを再度入力してください。

③ 設定 をクリックし、変更した内容を保存します。次回より、変更した[ユーザ名]、[パスワード]でログインしてください。

注意 設定した[ユーザ名]、[パスワード]を忘れてしまった場合は、[一時的に工場出荷時設定で起動する]（☞ p.156）を参照してログインし、再設定してください。

注意 ここで入力する[ユーザ名]および[パスワード]は、プロバイダから割り当てられた[ユーザ名]と[パスワード]ではありません。本機器にログインするためのものですので任意の文字列を設定してください。

時刻の設定

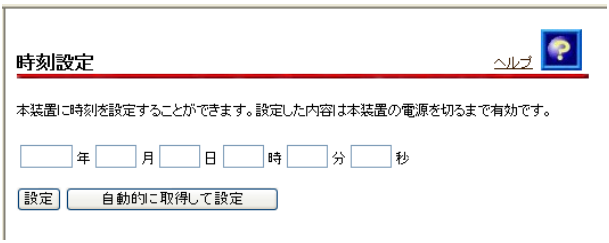
本設定項目で設定した時刻に合わせてログの時間表示をすることができます。

■ 自動設定の場合

本機器の LAN ポートに接続中のパソコンから時刻情報を取得して設定を行ないます。

① メニューフレームから 時刻設定 をクリックします。

② 自動的に取得して設定 をクリックします。



■ 手動設定の場合

手動で日付と時刻を入力して設定します。

① メニューフレームから 時刻設定 をクリックします。

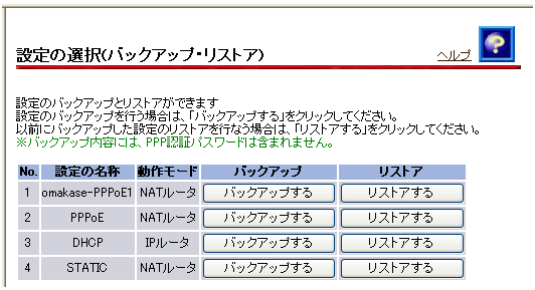
② 日付と時刻を入力します。

③ 設定 をクリックします。

設定のバックアップ・リストア

本機器の各種設定内容は、機器内蔵のフラッシュメモリにユーザ設定として保存されています。本機器のバックアップ機能では、ユーザ設定をテキスト形式でファイルに保存することができます。

① メニューフレームより 設定のバックアップ・リストア をクリックしてください。操作フレームに 設定の選択（バックアップ・リストア）画面が表示されます。

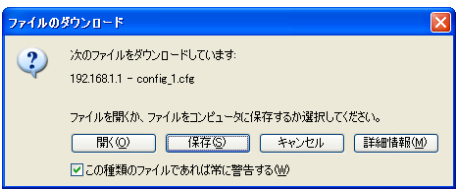


◆ バックアップする

① バックアップを行う場合は、該当する設定の バックアップする をクリックします。

② ファイルのダウンロード画面が表示されます。

③ 保存(S) をクリックして適当なフォルダを指定してバックアップファイルを保存します。

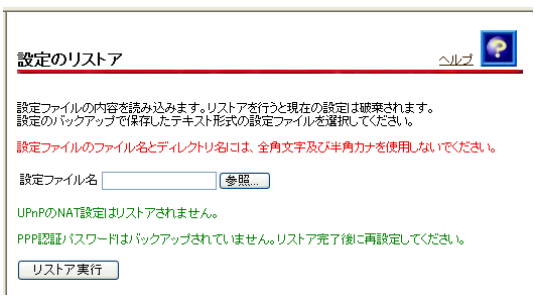


注意 パスワードの設定情報は、バックアップできません。

◆ リストアする

① リストアを行う場合は、該当する設定の リストアする をクリックします。

② 設定のリストア画面が表示されます。



③　[設定ファイル名]で　参照　をクリックし、ファイルの選択画面より、リストアする設定ファイルを選択します。

④　リストア実行　をクリックすると、実行確認のメッセージが表示されます。OK　をクリックすると選択した設定ファイルの内容を上書きし、本機器を再起動します。

注意　パスワードの設定情報は、リストアすることができませんので再設定してください。

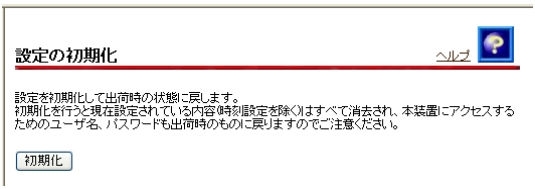
設定を初期化する

本機器の設定内容を初期化（工場出荷時の状態に戻す）する場合は、以下の手順で行ないます。

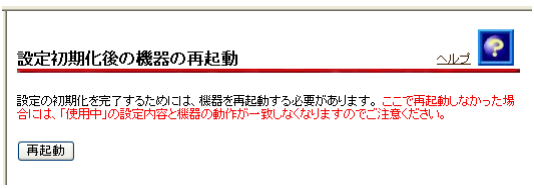
注意 初期化の処理を行うと、「機器状態・ログ」以外の内容はすべて工場出荷時の設定に戻ります。「機器状態・ログ」は、本機器の電源入/切時に初期化されます。必要な設定については、初期化の前にバックアップを行ってください。

① メニューフレームより 設定の初期化 をクリックしてください。操作フレームに設定の初期化画面が表示されます。

② 初期化 をクリックすると設定の初期化が開始します。設定初期化後の機器の再起動画面が表示されます。



③ 再起動 をクリックし、本機器を再起動させます。

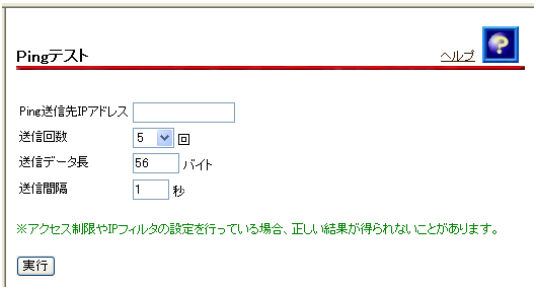


④ 工場出荷時設定で起動します。

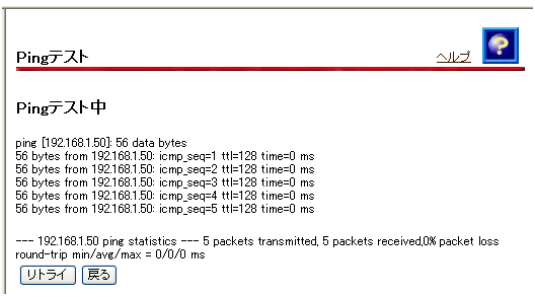
Pingテスト

任意のネットワーク機器との通信が可能かどうかを確認できます。

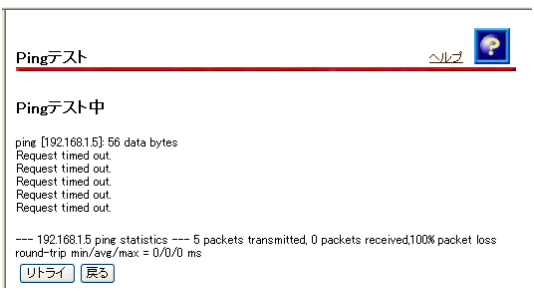
① メニューフレームより Ping テスト をクリックします。操作フレームに Ping テスト画面が表示されます。



② [Ping 送信先 IP アドレス]にプロバイダの DNS サーバ等の IP アドレスを入力し、実行 をクリックします。インターネットへの通信経路が確保されると、以下のような画面が表示されます。



失敗した場合は、以下のような画面が表示されます。再度設定を確認してください。



Ping テスト中は本機器への WWW アクセスはできません。

注意 本機器は、工場出荷時設定で接続先 1 からのアクセス制限（☞ p.67）を行うように設定されています。アクセス制限を解除しないと、回線側からの Ping テストに失敗します。

PPP切断／接続

「PPPoE」を選択している場合は、手動で PPP の接続および切断を行うことができます。PPP 自動接続を行なわない場合は、この機能を使って接続/切断を行ってください。

① メニューフレームより PPP 切断／接続 をクリックします。操作フレームに PPP 切断／接続画面が表示されます。

◆[接続]の場合

① PPP 接続を行う場合は、 接続 をクリックすると相手方ルータと PPP により接続します。

◆[切断]の場合

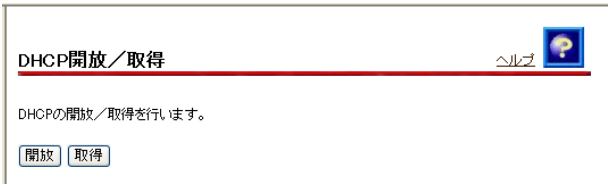
① PPP 接続を切る場合は、 切断 をクリックします。

② PPP の接続状態を確認します。

DHCP開放／取得

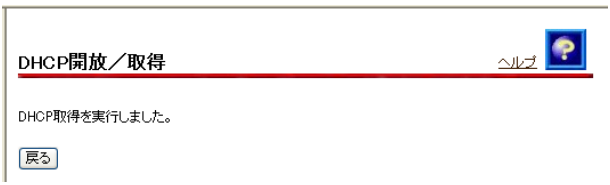
本機器の接続モードが DHCP 接続の場合、WAN 側で取得した IP アドレスを強制的に開放、取得するコマンドです。開放、取得 それぞれのボタンを押下してください。

① メニューフレームより DHCP 開放/取得 をクリックします。操作フレームに DHCP 開放/取得画面が表示されます。



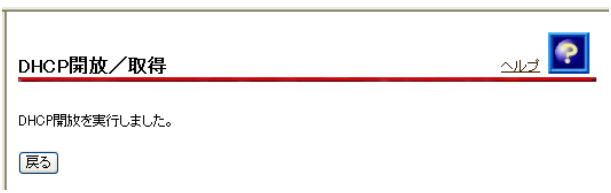
◆取得の場合

① DHCP の取得を行う場合は、 取得 をクリックしてください。WAN 側より IP アドレスを取得します。



◆開放の場合

① DHCP の開放を行う場合は、 開放 をクリックしてください。WAN 側で取得した IP アドレスを開放します。

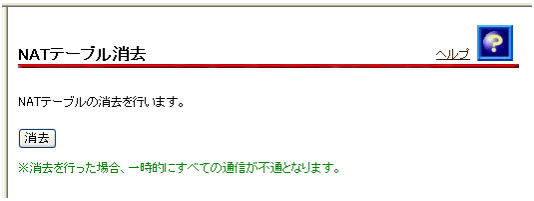


② DHCP の取得状態を確認します。

NATテーブル消去

登録されている NAT テーブルを全て消去することができます。NAT テーブルの登録件数が最大に達し、新たな通信が開始できなくなったときに実行してください。

① メニューフレームより NAT テーブル消去 をクリックします。操作フレームに NAT テーブル消去画面が表示されます。



② 消去 をクリックすると、NAT テーブルの内容を全て消去します。

Memo 現在の NAT テーブル登録件数はメニューフレームの「NAT テーブル」で参照できます。

注意 NAT テーブルを消去した場合、消去前に確立していた全ての通信が一旦無効になります。

UPnP NAT情報消去

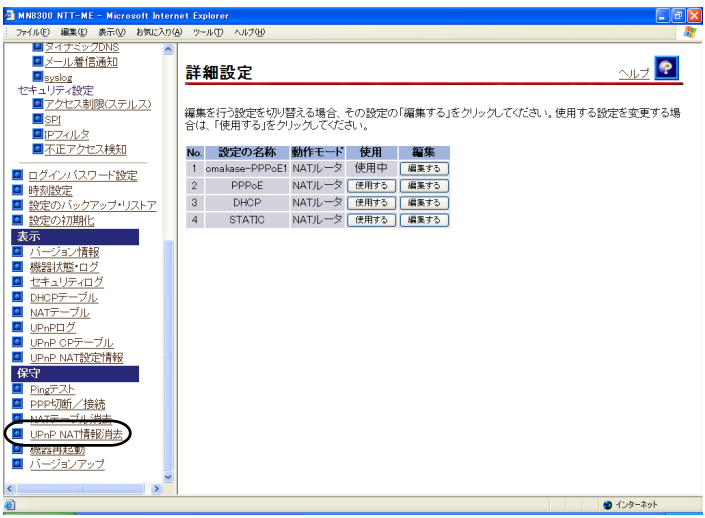
UPnP に対応したネットワークアプリケーションソフトウェアが本機器に登録した NAT 設定情報を強制的に消去するために使用します。 消去 をクリックすると直ちにすべての UPnP 用の NAT 設定情報が消去されます。

注意－ リモートアシスタンスの要求を行った場合、Windows/MSN Messenger を終了しても UPnP NAT 設定情報が残留します。UPnP NAT 設定情報は最大 128 件までしか設定できないので、残留した UPnP NAT 設定情報が蓄積されると正常に Windows/MSN Messenger が利用できなくなることが考えられます。またセキュリティ上の観点からも UPnP NAT 情報消去を実行することをお勧めします。

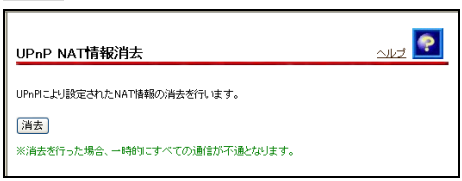
注意－ UPnP NAT 設定情報を消去したとき、一時的にインターネットに対するすべての通信が不通になります。Windows/MSN Messenger を起動している状態で設定変更した場合は、Windows/MSN Messenger を一旦終了してから起動し直してください。Windows/MSN Messenger をサインインし直すだけでは正常に動作しませんのでご注意ください。

UPnP NAT 情報消去は次の手順で行ないます。

① メニューフレームから UPnP NAT 情報消去 をクリックします



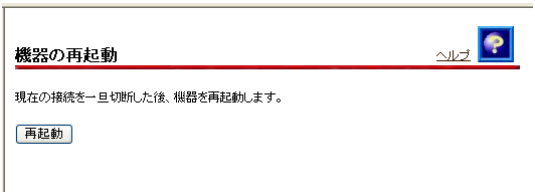
② 消去 をクリックします。



機器の再起動

本機器では、WWW ブラウザの設定画面から機器の再起動を行うことができます。

① メニューフレームより 機器再起動 をクリックします。操作フレームに機器の再起動画面が表示されます。

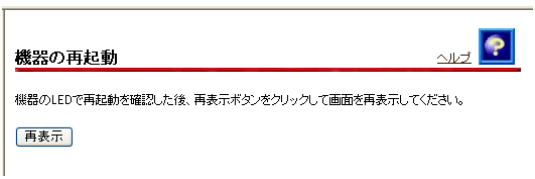


② 再起動 をクリックします。

③ 本機器本体の前面ランプで再起動を確認してください。

Memo 再起動中には WWW ブラウザでの接続はできません。

④ 再起動完了後 再表示 をクリックすると設定ページが表示されます。



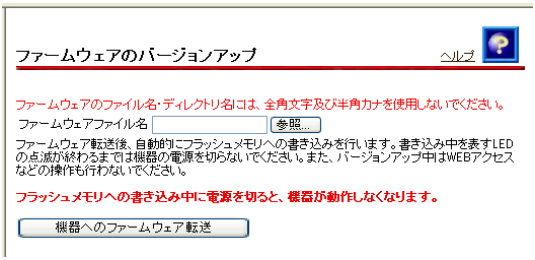
ファームウェアのバージョンアップ

本機器は、NTT-ME のホームページでファームウェアが提供された場合にダウンロードしたファームウェアファイルを用いてバージョンアップすることができます。

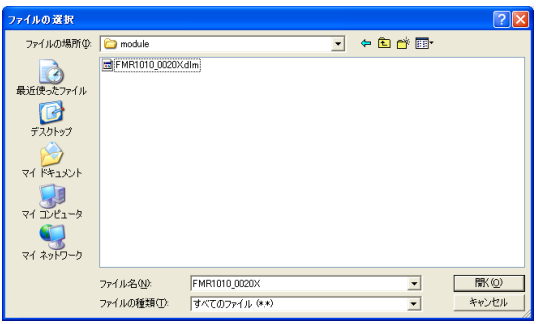
① WWW ブラウザで、http://www.ntt-me.co.jp/mn/mn8300/を開きファームウェアファイルをダウンロードして、パソコン上の適当なフォルダに置きます。

② 保存したファイルをダブルクリックして解凍します。

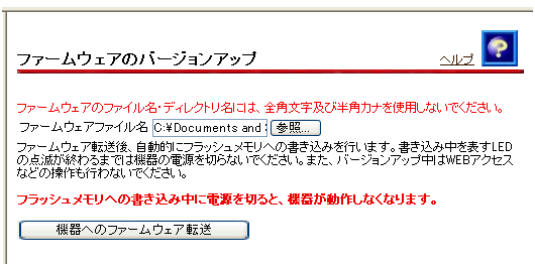
③ メニューフレームより バージョンアップ をクリックします。操作フレームにファームウェアのバージョンアップ画面が表示されます。



④ [ファームウェアファイル名]で 参照 をクリックします。ファイルの選択画面が表示されます。[ファイルの種類]で「すべてのファイル（*.*）」を指定し、手順 1 のファームウェアファイルを選択して 開く(0) をクリックします。

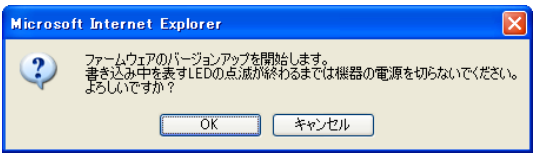


⑤ [ファームウェアファイル名]に選択したファイル名が表示されたら、機器へのファームウェア転送 をクリックします。



⑥ バージョンアップ開始のメッセージが表示されます。

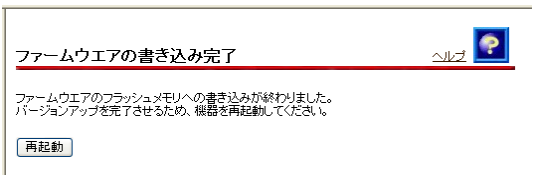
⑦ OK をクリックし、機器へのファームウェア転送およびフラッシュメモリへの書込みを開始します。



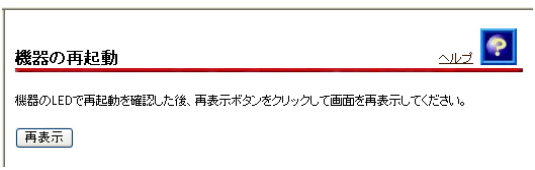
注意 書込み中を示すランプの点滅が終わるまで本機器の電源は切らないでください。フラッシュメモリへの書込み中に電源を切った場合、機器が動作しなくなります。

⑧ ファームウェアの書き込み完了画面が表示されます。

⑨ 再起動 をクリックし、本機器を再起動してください。新しいファームウェアにより動作します。



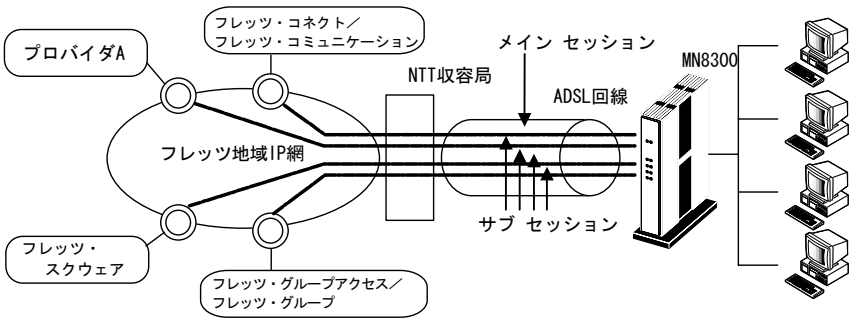
⑩ 本機器本体の前面ランプで再起動の確認後、 再表示 をクリックして画面を再表示させます。



Memo 本機器は、補助記憶装置としてフラッシュメモリを内蔵しています。各種設定やファームウェアの内容は、フラッシュメモリに書き込むことにより電源供給が途切れた場合でもその内容が保持されます。保存されていた設定内容は、バージョンアップ後もそのまま保持されますが、万一の場合に備えて「設定のバックアップ・リストア」（☞ p. 87）を行うことをお勧めします。

PPPoEマルチセッションを使用するには

本機器はPPPoEマルチセッション機能に対応しており、最大8つまでのPPPoEセッションを同時に接続することができます。複数のプロバイダを設定することにより、接続の切り替えをしなくても指定したプロバイダを利用してインターネットへ接続することができます。
NTT東日本エリアでは、Bフレッツで2〜4セッション、フレッツ・ADSLで2セッション、NTT西日本エリアでは、Bフレッツで1〜20セッション、フレッツ・ADSLで1〜5セッションが利用できます。ただし、NTT西日本エリアの場合、利用するセッション数によって申込み、またはフレッツ・プラスの契約が必要になります。（平成16年2月現在）



本機器では、PPPoEマルチセッション機能を使用して、通常のインターネット接続をしたままでフレッツ・スクウェアなどへの接続ができます。

注意 PPPoEマルチセッションを利用するためには、メインセッションに通常のプロバイダ経由のインターネット接続設定が必要です。メインセッションの登録は「インターネット接続の設定をする」（☞ p.34）を参照してください。

注意 PPPoEマルチセッション機能は、Bフレッツまたはフレッツ・ADSL以外では利用できません。

MN8300のPPPoEマルチセッション仕様

本機器では、接続先設定 No.1（接続先 1）をメインセッション、それ以外の接続先をサブセッションと定義します。
本機器のマルチセッション機能は、プロバイダとの接続モードが PPPoE（端末型）または PPPoE（LAN 型）の場合に有効であり、最大 8 セッションまで同時接続が可能です。
なお、サブセッションの動作モード（IP ルータ・NAT ルータ・GapNAT・マルチ GapNAT）は、メインセッションで設定した動作モードと同じになります。

注意 本機器前面の PPPoE/DHCP ランプはメインセッションの状態のみを表示します。

注意 サブセッションの状態を知るためには設定画面の機器状態・ログ画面を参照する必要があります。

注意 GapNAT 通過制限、NAT アドレス変換、NAT アドレス・ポート変換、IP フィルタについてはすべてのセッションについて設定が可能ですが、ワンタッチ設定についてはメインセッションのみが対象となります。

注意 PPPoE マルチセッション機能は本機器の接続モードを PPPoE 接続（端末型）または PPPoE 接続（LAN 型）で設定した場合のみ利用可能です。DHCP 接続、固定 IP 接続モードで設定した場合には有効ではありません。

注意 PPPoE 以外の設定内容を編集した場合、サブセッションの設定メニューは表示されません。

注意 サブセッション経由での PPPoE（LAN 型）接続はできません。

(1) 送信先のサブセッションへの振り分け

送信先の振り分けは以下の方法で行います。
サブセッション毎に接続ルールを設定し、これに従って使用するサブセッションを決定します。
WAN 側へのパケット送信時に各サブセッションに設定された接続ルールを参照し、ルールに合致したサブセッション上に送信が行われます。どのサブセッションの接続ルールにも合致しなかったパケットはメインセッション上に送信されます。

複数のサブセッションの接続ルールに合致する場合は、
サブセッション 1→サブセッション 2→・・・→サブセッション 7 の順番で優先されます。

注意 サブセッション接続ルールは、原則としてそのセッションの PPPoE が接続完了している場合のみ有効となります。

注意 本機器を再起動すると、本機器に LAN 接続したパソコンからフレッツ・スクウェアなどへ正しく接続できない場合があります。これはパソコンがすでに DNS 解決していて、DNS によるセッション振り分けが行われないためです。
本機器を再起動した場合は、必ずパソコンを再起動するか、パソコンの OS またはアプリケーションごとの DNS キャッシュを削除してください。

(2)サブセッション接続ルールの入力規則

サブセッション接続ルールの指定方法は以下の通りです。

ホスト名指定

送信先のホスト名を指定します。たとえば、www.xxx.co.jp と指定すると、www.xxx.co.jp との通信時にこのサブセッションが使用されるようになります。

注意 **IP アドレスを用いた指定方法との併用はできません。**

「,(カンマ)」で区切って入力することで、1 つの接続先に対して、最大 4 つまで指定できます。

ホスト名	入力例	説明
すべて指定	www.xxx.co.jp	www.xxx.co.jp のみ
前方一致指定 [“.”または“*”で終了]	www.xxx. www.xxx.*	“www.xxx” で始まるものすべて
後方一致指定 [“.”または”*”で開始]	.co.jp *.co.jp	“.co.jp”で終わるものすべて
ワイルドカード指定	www.*.co.jp	www.で始まり、”.co.jp”で終わるものすべて

注意 **ホスト名は最大 63 文字までです。**

注意 **“*”は 1 つのみ使用できますが、ホスト名が“.”で始まる場合または“.”で終わる場合は使用できません。**

注意 **ホスト名を指定しない場合は空欄としてください。**

送信先 IP アドレス、送信元 IP アドレス指定

それぞれ 4 個まで指定できます。

IPアドレス	入力例	説明
*	*	すべてのIPアドレス
個別指定	100.1.1.1	100.1.1.1 のみ
範囲指定 [“-“ハイフンで区切る]	100.1.1.2−100.1.1.100	100.1.1.2 から 100.1.1.100 の間のアドレスすべて。

注意 **送信先 IP アドレス、送信元 IP アドレスを指定しない場合は空欄としてください。**

プロトコル&ポート番号指定

プロトコルと TCP/UDP のポート番号を組み合わせて 4 個まで指定できます。

プロトコルは「1 以上 255 以下の数値」、「予約済みの名前（TCP,UDP,ICMP）」、「ワイルドカード（*）」で指定します。
プロトコルが TCP または UDP のものについては「ポート番号」を指定できます。
送信先ポート番号には個別指定、範囲指定、全指定（“*”）が可能であり、範囲指定では最小値と最大値を“-”（ハイフン）でつないで入力します。

注意 **プロトコル&ポート番号指定を指定しない場合は空欄としてください。**

フレッツ・スクウェアを利用する

プロバイダの PPPoE アカウントを 1 個しか持っていなくても、フレッツ・ADSL ユーザならば、ブロードバンドコンテンツサイトであるフレッツ・スクウェアの PPPoE アカウントを無料で利用することができます。
フレッツ・スクウェアは 1 つのセッションを専有するので、PPPoE マルチセッション未対応ルータで接続する場合は、プロバイダとフレッツ・スクウェアの接続をその都度切り替えて利用することになります。
本機器を利用した場合は、プロバイダで 1 つのセッション、フレッツ・スクウェアで 1 つのセッションをそれぞれ専有できるので、接続をその都度切り替える必要がなく、インターネットとフレッツ・スクウェアのコンテンツを同時に利用することが可能となります。
本機器のおまかせ設定を利用すると、これらフレッツ・スクウェアを簡単な操作で利用できます。
以下の設定手順は PPPoE 接続（端末型）モードにおいて、NTT 東日本のフレッツ・スクウェアを利用する手順を示します。

① メニューフレームより おまかせ設定 をクリックして、おまかせ設定画面を表示します。

② 接続モードから 「PPPoE（端末型）」を選択します。

③ 表示画面に、PPPoE の[ユーザーID]、[パスワード]、[パスワードの確認入力]を入力した後、[フレッツ・スクウェア]の項目で、「使用する（NTT 東日本）」か、「使用する（NTT 西日本）」を選択し、設定ボタンをクリックします。

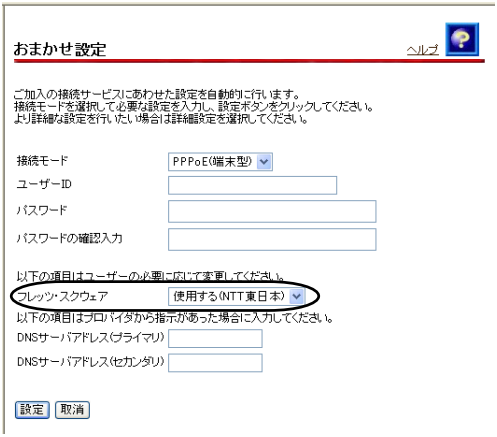
④ 設定変更後の機器の再起動画面が表示されます。

⑤ 再起動をクリックし、本機器を再起動します。

⑥ LAN 内の IP アドレスが変わる可能性がありますので、本機器に接続されているパソコンを再起動します。

⑦ WWW ブラウザで本機器にアクセスします。IP アドレス 「192.168.1.1」、「ユーザー名 ：admin」、「パスワード ：admin（工場出荷時設定の場合）」。

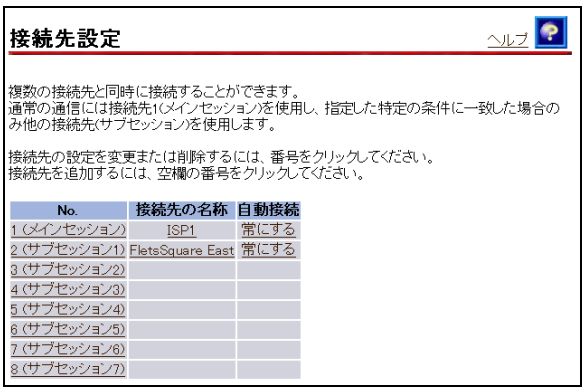
⑧ WWW ブラウザのアドレスに http://www.flets/ を入力してフレッツ・スクウェアのホームページが表示できれば正常にサブセッションが確立されています。



Memo フレッツ・スクウェアに関しては、以下のホームページを参照するか、NTT 東日本、NTT 西日本にお問い合わせください。

NTT 東日本ホームページ　　http://flets.com/

NTT 西日本ホームページ　　http://www.ntt-west.co.jp/flets/



Memo NTT 東日本と NTT 西日本の接続先設定項目の差は以下のとおりです。

フレッツ・スクウェア サービス	接続先の名称（例）	PPP認証プロトコル		接続ルール
		ユーザ名	パスワード	ホスト名
NTT東日本	FletsSquare East	guest@flets	guest	.flets
NTT西日本	FletsSquare West	flets@flets	flets	.flets

フレッツ・グループアクセスまたはフレッツ・グループを利用する

フレッツ・グループアクセス（NTT 東日本がサービス提供）とフレッツ・グループ（NTT 西日本がサービス提供）は、フレッツ・ADSL や B フレッツを利用して低コストでプライベートネットワークを構築できるサービスです。フレッツ・グループアクセスのサービスメニューには最大 10 拠点で利用可能なフレッツ・グループアクセス・ライトと、最大 30 拠点で利用可能なフレッツ・グループアクセス・プロの 2 つがあります（平成 16 年 2 月現在）。また、フレッツ・グループのサービスメニューには最大 10 拠点を、NTT 西日本が構成するグループを一元管理するベーシックメニューと、構成するグループの管理をグループ管理者にお任せするビジネスメニューがあります（平成 16 年 2 月現在）。
ルータを使用してこれらのサービスを利用する場合、LAN 型払い出し方式が利用できるフレッツ・グループアクセス・プロやフレッツ・グループ・ビジネスメニューを選択されることが多いと思います。
ここでは、メインセッションはプロバイダ接続用、サブセッションでフレッツ・グループアクセス・プロ（LAN 型払い出し）を利用するいくつかのシーンを想定して以下に設定例を説明します。サブセッションの動作モードは、メインセッションで設定した動作モードと同じ動作モードになります。フレッツ・グループ・ビジネスメニューにおいても同様の設定例で活用できます。

メインセッション：NAT ルーターサブセッション：NAT ルータ

メインセッション：IP ルーターサブセッション：IP ルータ

設定例は以下の環境を想定して説明します。

- **フレッツでインターネットに接続する。**
- **フレッツ・グループアクセス・プロを利用して 3 拠点でプライベートネットワークを構築する。**

・拠点 1（自分の拠点）

IP アドレス：192.168.10.＊、サブネットマスク：255.255.255.0 で構築

192.168.10.1：ルータ

192.168.10.2～192.168.10.5：フレッツ・グループアクセス端末

・拠点 2

IP アドレス：192.168.20.＊、サブネットマスク：255.255.255.0 で構築

192.168.20.1：ルータ

192.168.20.2～192.168.20.3：フレッツ・グループアクセス端末

・拠点 3

IP アドレス：192.168.30.＊、サブネットマスク：255.255.255.0 で構築

192.168.30.1：ルータ

192.168.30.2～192.168.30.3：フレッツ・グループアクセス端末

Memo フレッツ・グループアクセスまたはフレッツ・グループに関しては、以下のホームページを参照するか、NTT 東日本、NTT 西日本にお問い合わせください。

NTT 東日本ホームページ　http://flets.com/

NTT 西日本ホームページ　http://www.ntt-west.co.jp/flets/

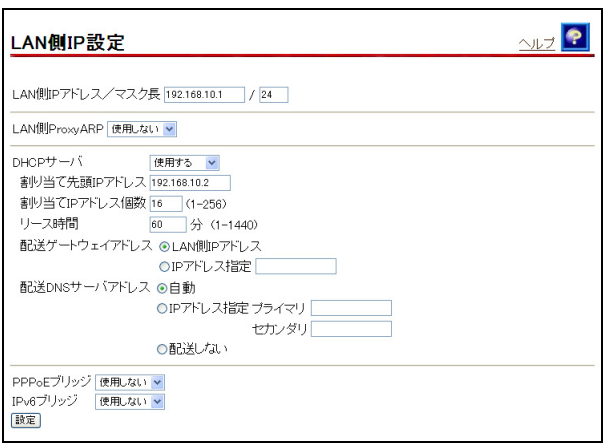
＜Case1＞

◆ メインセッション：プロバイダでインターネット利用

◆ サブセッション：フレッツ・グループアクセス・プロを利用

◆ フレッツ・グループアクセス端末はインターネットも利用

1. おまかせ設定を利用してプロバイダサービスに接続するための設定をします。
2. メニューフレームより詳細設定をクリックして詳細設定画面を表示します。
3. 「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
4. メニューフレームから LAN 側 IP 設定 をクリックして以下を設定します。
   ① [LAN 側 IP アドレス／マスク長]で「192.168.10.1/24」を入力します。
   ② [DHCP サーバ]で「使用する」を選択します。
   ③ [割り当て先頭 IP アドレス]で「192.168.10.2」を入力します。
   ④ [割り当て IP アドレス個数]に必要なアドレス数を入力します。
   ⑤ 設定 をクリックします。
   ⑥ 設定変更後の機器の再起動画面が表示されます。
   ⑦ 再起動 をクリックし、本機器を再起動します。
   ⑧ LAN 内の IP アドレスが変わりますので、本機器に接続されている全てのパソコンを再起動します。

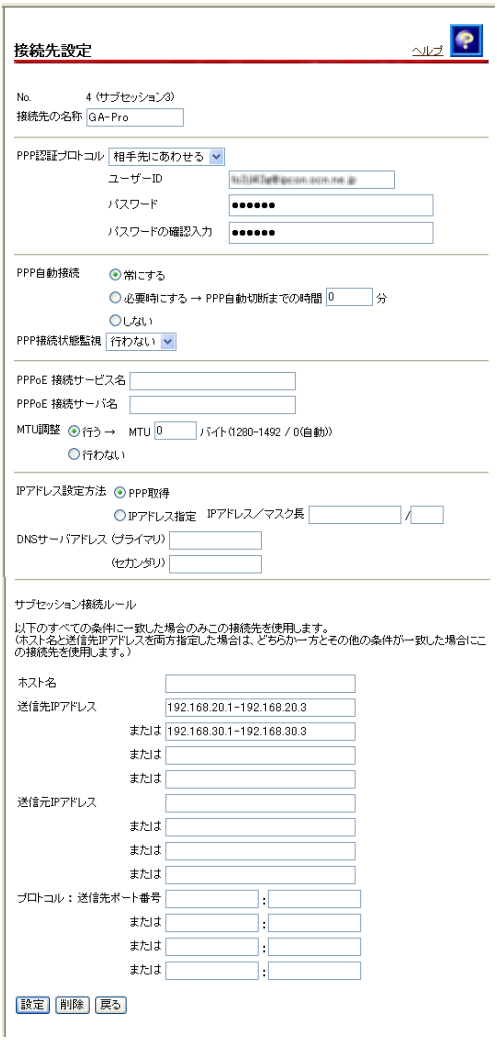


5.WWW ブラウザに本機器の新しい IP アドレス「192.168.10.1」を入力します。
「ユーザ名：admin」、「パスワード：admin」を入力して設定画面を開きます。

6.メニューフレームより 接続先設定 をクリックして以下を設定します。

7.メニューフレームから詳細設定ー「No.1 omakase-PPPoE1」の行の 編集する をクリックします。

① No.4（サブセッション3） をクリックします。
② [接続先の名称]に任意の文字列（例：GA-Pro）を入力します。
③ [ユーザーID]にフレッツ・グループアクセス・プロで割り当てられたユーザ ID を入力します。
④ [パスワード]と[パスワードの確認入力]にフレッツ・グループアクセス・プロで割り当てられたパスワードを入力します。
⑤ [PPP 自動接続]で[常にする]、または[必要時にする]にチェックします。[必要時にする]にチェックした場合は「PPP 自動切断までの時間（分）」を入力します。
⑥ サブセッション接続ルールの[送信先 IP アドレス]で他の拠点の IP アドレスを入力します。（ここでは 192.168.20.1-192.168.20.3 と 192.168.30.1-192.168.30.3 を入力します）
⑦ 設定 をクリックします。
⑧ 機器の再起動画面へ をクリックし、機器の再起動画面で 再起動 をクリックし、本機器を再起動します。
⑨ 本機器の再起動が完了したら 再表示 をクリックします。


接続先設定

ヘルプ

No. 4 (サブセッション3)

接続先の名称 GA-Pro

PPP認証プロトコル 相手先にあわせる

ユーザーID

パスワード ●●●●●●

パスワードの確認入力 ●●●●●●

PPP自動接続 常にする

必要時にする → PPP自動切断までの時間 0 分

しない

PPP接続状態監視 行わない

PPPoE 接続サービス名

PPPoE 接続サーバ名

MTU調整 行う → MTU 0 バイト(1280-1492 / 0(自動))

行わない

IPアドレス設定方法 PPP取得

IPアドレス指定 IPアドレス／マスク長 /

DNSサーバアドレス (プライマリ)

(セカンダリ)

サブセッション接続ルール

以下のすべての条件に一致した場合のみこの接続先を使用します。
(ホスト名と送信先IPアドレスを両方指定した場合は、どちらか一方とその他の条件が一致した場合にこの接続先を使用します。)

ホスト名

送信先IPアドレス 192.168.20.1-192.168.20.3

または 192.168.30.1-192.168.30.3

または

または

送信元IPアドレス

または

または

または

プロトコル：送信先ポート番号 :

または :

または :

または :

設定 削除 戻る

8. メニューフレームより詳細設定－「No.1 omakase-PPPoE1」の行の 編集する をクリックします。

9. メニューフレームから NAT アドレス変換 をクリックして以下を設定します。

① No.1 をクリックします。
② [優先度]に「1」を入力します。
③ [接続先の名称]－「接続先 5(GA-Pro)」を選択します。
④ [LAN 側 IP アドレス]－「192.168.10.2」
⑤ [WAN 側 IP アドレス]で[IP アドレス指定]－「192.168.10.2」を入力します。
⑥ [プロトコル]－「全プロトコル(占有)」を選択します。
⑦ 設定 ボタンをクリックします。
⑧ No.2 をクリックします。
⑨ [優先度]に「2」を入力します。
⑩ [接続先の名称]－「接続先 5(GA-Pro)」を選択します。
⑪ [LAN 側 IP アドレス]－「192.168.10.3」
⑫ [WAN 側 IP アドレス]で[IP アドレス指定]－「192.168.10.3」を入力します。
⑬ [プロトコル]－「全プロトコル(占有)」を選択します。
⑭ 設定 ボタンをクリックします。
⑮ 上記の手順でフレッツ・グループアクセスを利用したいパソコンの IP アドレスをすべて登録します。（最大 64 個まで登録できます。）

これで設定は完了です。

10. Ping コマンドなどを利用して通信テストを実施してください。

Memo その他必要に応じてマニュアルを参照して設定してください。

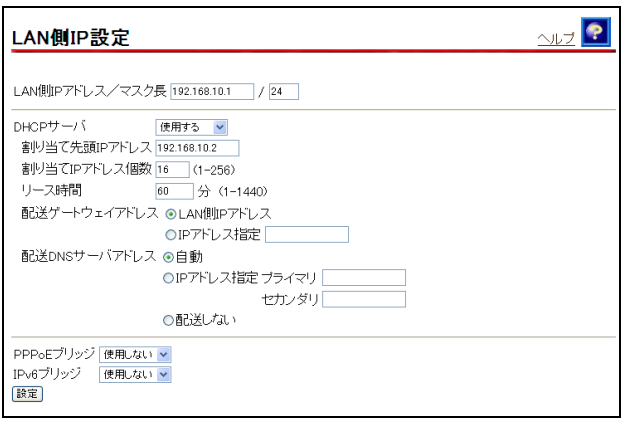
Memo その他の拠点から本機器の設定画面にアクセスするためにはメニューフレームの「アクセス制限（ステルス）」で[接続先＊（接続先の名称）を禁止する]（この例では[接続先 4（GA-Pro）側からのアクセスを禁止する]と表示されます。）のチェックをはずして 設定 してください。

＜Case2＞

- ◆ メインセッション：プロバイダ（複数固定 IP アドレス 8 個のメニュー）をマルチ GapNAT モードで利用
- ◆ サブセッション：フレッツ・グループアクセス・プロを利用
- ◆ フレッツ・グループアクセス端末はインターネットも利用
- ◆ フレッツ・グループアクセス端末（プライベート IP アドレス端末）とマルチ GapNAT 端末間の通信を許可
- ◆ マルチ GapNAT 端末はグローバル IP アドレスを固定設定
- ◆ フレッツ・グループアクセス端末は DHCP で自拠点用プライベート IP アドレスを割り当て

1. おまかせ設定を利用してプロバイダサービスに接続するための設定をします。
2. メニューフレームより詳細設定をクリックして詳細設定画面を表示します。
3. 「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
4. メニューフレームから 動作モード設定 をクリックして以下を設定します。
   - ① [動作モード]で「マルチ GapNAT」を選択します。
   - ② [グローバル IP アドレス割り当て数]で「8」を選択します。
   - ③ [GapNAT 用グローバル IP アドレス]に本機器に割り当てるグローバル IP アドレス（ここでは 100.100.100.1）を入力します。
   - ④ [プライベート IP ホストで外部との通信を]で「行う」を選択します。
   - ⑤ [LAN 内のグローバル IP アドレス-プライベート間通信を]で「行う」を選択します。
   - ⑥ 設定 をクリックします。
   - ⑦ 設定変更後の機器の再起動画面が表示されます。
   - ⑧ 再起動 をクリックし、本機器を再起動します。
   - ⑨ 本機器の再起動が完了したら 再表示 をクリックします。

5. メニューフレームより詳細設定－「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
6. メニューフレームから LAN 側 IP 設定 をクリックして以下を設定します。
   ① [LAN 側 IP アドレス／マスク長]で「192.168.10.1/24」を入力します。
   ② [DHCP サーバ]で「使用する」を選択します。
   ③ [割り当て先頭 IP アドレス]で「192.168.10.2」を入力します。
   ④ 割り当て IP アドレス個数を任意で入力します。
   ⑤ 設定 をクリックします。
   ⑥ 設定変更後の機器の再起動画面が表示されます。
   ⑦ 再起動 をクリックし、本機器を再起動します。
   ⑧ LAN 内の IP アドレスが変わりますので、本機器に接続されている、全てのパソコンを再起動します。



7. WWW ブラウザに本機器の新しい IP アドレス「192.168.10.1」を入力します。
   「ユーザー名：admin」、「パスワード：admin」を入力して設定画面を開きます。
8. 「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
9. メニューフレームより 接続先設定 をクリックして以下を設定します。
   ① No.5（サブセッション 4） をクリックします。
   ② [接続先の名称]に任意の文字列（例：GA-Pro）を入力します。
   ③ [ユーザーID]にフレッツ・グループアクセス・プロで割り当てられたユーザ ID を入力します。

④ [パスワード]と[パスワードの確認入力]にフレッツ・グループアクセス・プロで割り当てられたパスワードを入力します。

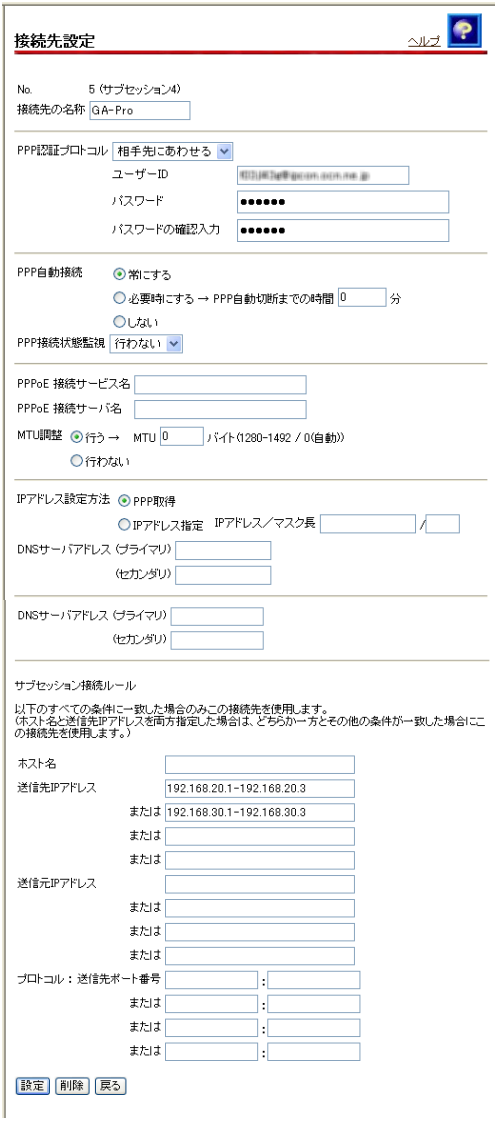
⑤ [PPP 自動接続]で[常にする]、または[必要時にする]にチェックします。
[必要時にする]にチェックした場合は「PPP 自動切断までの時間（分）」を入力します。

⑥ サブセッション接続ルールの[送信先 IP アドレス]で他の拠点の IP アドレスを入力します。
（ここでは 192.168.20.1-192.168.20.3 と 192.168.30.1-192.168.30.3 を入力します）

⑦ 設定 をクリックします。

⑧ 機器の再起動画面へ をクリックし、機器の再起動画面で 再起動 をクリックし、本機器を再起動します。

⑨ 本機器の再起動が完了したら 再表示 をクリックします。



10. 「No.1　omakase-PPPoE1」の行の　編集する　をクリックします。

11. メニューフレームより GapNAT 通過・NAT アドレス変換 をクリックして以下を設定します。

① No.1 をクリックします。

② [優先度]に「1」を入力します。

③ [接続先の名称]－「接続先 5(GA-Pro)」を選択します。

④ [LAN 側 IP アドレス]－「192.168.10.2」

⑤ [WAN 側 IP アドレス]で[IP アドレス指定]－「192.168.10.2」を入力します。

⑥ [プロトコル]－「全プロトコル(占有)」を選択します。

⑦ 設定 ボタンをクリックします。

⑧ No.2 をクリックします。

⑨ [優先度]に「2」を入力します。

⑩ [接続先の名称]－「接続先 5(GA-Pro)」を選択します。

⑪ [LAN 側 IP アドレス]－「192.168.10.3」

⑫ [WAN 側 IP アドレス]で[IP アドレス指定]－「192.168.10.3」を入力します。

⑬ [プロトコル]－「全プロトコル(占有)」を選択します。

⑭ 設定 ボタンをクリックします。

⑮ 上記の手順でフレッツ・グループアクセスを利用したいパソコンの IP アドレスをすべて登録します。（最大 32 個まで登録できます。）

⑯ また GapNAT 端末(グローバル IP アドレス端末)を NAT アドレス変換に設定すればインターネット、フレッツ・グループアクセス両方の利用が可能になります。

これで設定は完了です。

12. Ping コマンドなどを利用して通信テストを実施してください。

Memo マルチ GapNAT での設定方法については、「マルチ GapNAT の設定方法」（☞ p. 134 を併せて参照してください。

Memo サブセッション接続ルールの送信元 IP アドレスに自拠点のフレッツ・グループアクセス端末のプライベート IP アドレスを設定すると、メインセッション経由でインターネットへの接続はできなくなります。

Memo その他必要に応じてマニュアルを参照して設定してください。

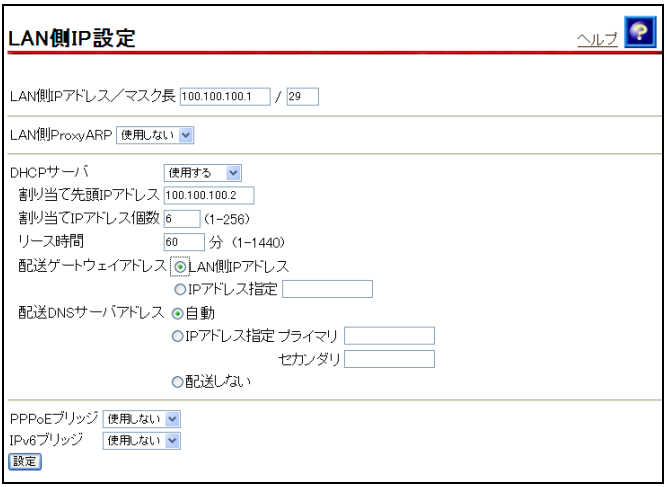
Memo その他の拠点から本機器 の設定画面にアクセスするためにはメニューフレームの アクセス制限（ステルス） で[接続先＊（接続先の名称）を禁止する]（この例では[接続先 5（GA-Pro）側からのアクセスを禁止する]と表示されます。）のチェックをはずして 設定 ボタンをクリックしてください。

＜Case3＞

- ◆ メインセッション：プロバイダ（複数固定 IP アドレス 8 個のメニュー）を IP ルータモードで利用
- ◆ サブセッション：フレッツ・グループアクセス・プロを利用
- ◆ フレッツ・グループアクセス端末でインターネットは利用しない
- ◆ フレッツ・グループアクセス端末（プライベート IP アドレス端末）とグローバル IP アドレス端末間の通信はしない
- ◆ DHCP でグローバル IP アドレスを割り当て
- ◆ フレッツ・グループアクセス端末は固定で自拠点用プライベート IP アドレスを設定

プロバイダはメインセッションで IP ルータモードを利用して設定し、サブセッションでフレッツ・グループアクセスを利用した場合、フレッツ・グループアクセス端末からメインセッション経由でインターネット接続はできません。また、フレッツ・グループアクセス端末（プライベート IP アドレス端末）とグローバル IP アドレス端末間の通信もできません。これらは、Case 2 の例で説明しているマルチ GapNAT モードを利用すれば実現できます。

1. おまかせ設定を利用してプロバイダサービスに接続するための設定をします。
2. メニューフレームより詳細設定をクリックして詳細設定画面を表示します。
3. 「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
4. メニューフレームから 動作モード設定 をクリックし[動作モード]で「IP ルータ」を選択し 設定 をクリックします。
   - ① 設定変更後の機器の再起動画面が表示されます。
   - ② 再起動 をクリックし、本機器を再起動します。
   - ③ 本機器の再起動が完了したら 再表示 をクリックします。
5. メニューフレームから詳細設定－「No.1 omakase-PPPoE1」の行の 編集する をクリックします。
6. メニューフレームで LAN 側 IP 設定 をクリックして以下を設定します。
   - ① [LAN 側 IP アドレス／マスク長]で本機器に割り当てるグローバル IP アドレスとマスク長（ここでは 100.100.100.1/29）を入力します。
   - ② [DHCP サーバ]で「使用する」を選択します。
   - ③ [割り当て先頭 IP アドレス]で端末に割り当てる先頭のグローバル IP アドレス（ここでは 100.100.100.2）を入力します。
   - ④ [割り当て IP アドレス個数]を入力します。（固定 IP アドレス 8 個のメニューの場合は最大 5 個）
   - ⑤ 設定 をクリックします。



⑥ 設定変更後の機器の再起動画面が表示されます。

⑦ 再起動 をクリックし、本機器を再起動します。

⑧ LAN 内の IP アドレスが変わりますので、本機器に接続されている全てのパソコンを再起動します。

7. WWW ブラウザに本機器の新しい IP アドレス「100.100.100.1」を入力します。
「ユーザ名：admin」、「パスワード：admin」を入力して設定画面を開きます。

8. メニューフレームより詳細設定－「No.1 omakase-PPPoE1」の行の 編集する をクリックします。

9. メニューフレームで 接続先設定 をクリックして以下を設定します。

① No.5（サブセッション 4） をクリックします。

② [接続先の名称]に任意の文字列（例：GA-Pro）を入力します。

③ [ユーザーID]にフレッツ・グループアクセスプロで割り当てられたユーザーIDを入力します。

④ [パスワード]と[パスワードの確認入力]にフレッツ・グループアクセス・プロで割り当てられたパスワードを入力します。

⑤ [PPP 自動接続]で[常にする]、または[必要時にする]にチェックします。
[必要時にする]にチェックした場合は「PPP 自動切断までの時間（分）」を入力します。

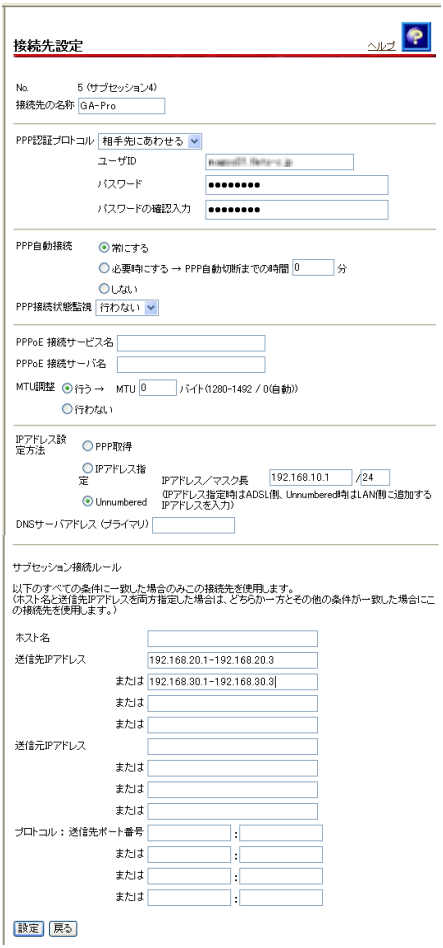
⑥ [IP アドレス設定方法]で[Unnumbered]にチェックし、LAN 側に追加する IP アドレスとマスク長を入力します。（ここでは 192.168.10.1/24）

⑦ サブセッション接続ルールの[送信先 IP アドレス]で他の拠点の IP アドレス（ここでは 192.168.20.1-192.168.20.3 と 192.168.30.1-192.168.30.3 を入力します）

⑧ 設定 をクリックします。

⑨ 機器の再起動画面へ をクリックし、機器の再起動画面で 再起動 をクリックし、本機器を再起動します。

⑩ 本機器の再起動が完了したら 再表示 をクリックします。



10. フレッツ・グループアクセス端末の設定をする。
（ここでは拠点の IP アドレスが「192.168.10.1/24」の場合の設定です。）

① フレッツ・グループアクセスを利用する端末は、パソコンの TCP/IP 設定にフレッツ・グループアクセス拠点用 IP アドレス等を設定する必要があります。

② TCP/IP の設定を開きます。

③ [IP アドレス]：「192.168.10.2」

④ [サブネットマスク]：「255.255.255.0」

⑤ [デフォルトゲートウェイ]：「192.168.10.1」

⑥ [DNS サーバ]：「192.168.10.1」

※複数のパソコンを設定するときは③の IP アドレスをサブネットマスクの範囲で変更してください。

Memo IP ルータモードでの設定方法については、「固定 IP 接続（IP アドレス固定のインターネット接続）の場合」（☞ p.41）の「LAN 側のパソコンにグローバル IP アドレスを直接割り当てる場合（IP ルータとして利用）」を併せて参照してください。

Memo その他必要に応じてマニュアルを参照して設定してください。

Memo その他の拠点から本機器の設定画面にアクセスするためにはメニューフレームの「アクセス制限（ステルス）」で[接続先*（接続先の名称）を禁止する]（この例では[接続先5(GA-Pro)側からのアクセスを禁止する]と表示されます。）のチェックをはずして 設定 をクリックしてください。

フレッツ・コネクトを利用する

フレッツ・コネクトは、NTT 東日本エリアでフレッツ・ADSL、B フレッツを利用している方どうしが、IP テレビ電話で音声・映像・ファイル転送・メッセージ等をやりとりできるサービスです。
本機器では PPPoE マルチセッション機能と UPnP マルチセッション機能を利用して、NTT 東日本が提供するフレッツ・コネクトの「UPnP 対応用ユーティリティソフトウェア」をインストールしたパソコンからインターネットとフレッツ・コネクトを同時に利用することが可能です。
フレッツ・コネクトのサービス提供エリア、料金、利用条件などの最新情報と、本機器の設定方法は以下のホームページを参照してください。

＜フレッツ・コネクト ホームページ＞
⇒ http://flets.com/connect/

＜MN/BA シリーズ　フレッツ・コネクト情報ページ＞
⇒ http://www.ntt-me.co.jp/mn/flets_connect.html

フレッツ・コミュニケーションを利用する

フレッツ・コミュニケーションは、NTT 西日本エリアでフレッツ・ADSL、B フレッツを利用している方どうしが、IP テレビ電話で音声・映像・ファイル転送・メッセージ等をやりとりできるサービスです。
本機器では PPPoE マルチセッション機能と UPnP マルチセッション機能を利用して、NTT 西日本が提供する「フレッツ・コミュニケーションツール」をインストールしたパソコンからインターネットとフレッツ・コミュニケーションを同時に利用することが可能です。
フレッツ・コミュニケーションのサービス提供エリア、料金、利用条件などの最新情報と、本機器の設定方法は以下のホームページを参照してください。

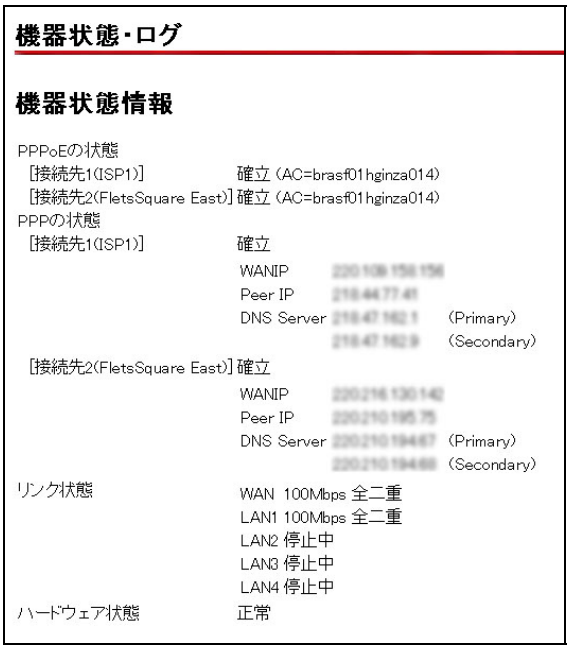
＜フレッツ・コミュニケーション ホームページ＞
⇒ http://www.ntt-west.co.jp/flets/fc/

サブセッションの確立を確認する

本機器前面の状態表示ランプはメインセッションの状態のみを表示しますので、サブセッションの接続が確立したかどうかは設定画面からのみ確認できます。
以下の手順でサブセッションの接続状態を確認します。

1. 詳細設定画面のメニューフレームから 機器状態・ログ をクリックします。

2. 「接続先設定」で設定した設定番号ごとに「接続先＊（接続先の名称）」が表示されます。


機器状態･ログ

機器状態情報

PPPoEの状態
[接続先1(ISP1)] 確立 (AC=brasf01hginza014)
[接続先2(FletsSquare East)] 確立 (AC=brasf01hginza014)
PPPの状態
[接続先1(ISP1)] 確立
WANIP 220.109.159.156
Peer IP 219.44.77.41
DNS Server 219.47.162.1 (Primary)
219.47.162.9 (Secondary)
[接続先2(FletsSquare East)] 確立
WANIP 220.216.130.142
Peer IP 220.210.195.75
DNS Server 220.210.194.67 (Primary)
220.210.194.68 (Secondary)
リンク状態 WAN 100Mbps 全二重
LAN1 100Mbps 全二重
LAN2 停止中
LAN3 停止中
LAN4 停止中
ハードウェア状態 正常

※上記画面はフレッツ・スクウェア（NTT 東日本エリア）をサブセッションで利用した場合の例です。

GapNATとDMZホストの構築

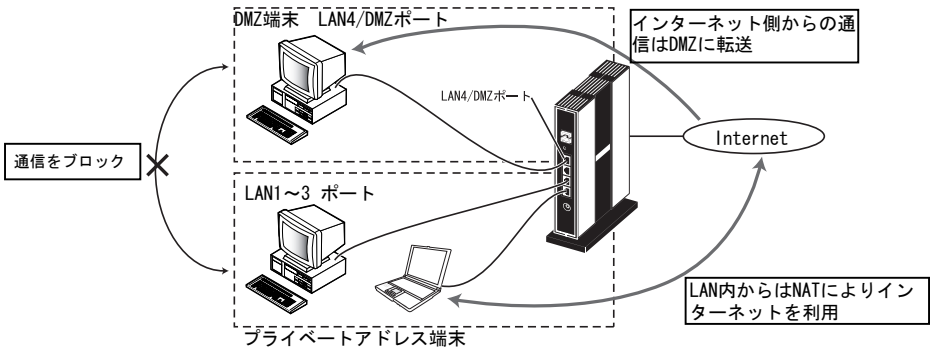
DMZの構築

LAN 内のネットワークと外部ネットワーク間に LAN 内への進入を阻止する目的で設けられるサブネットを DMZ と言います。通常、外部に公開する WWW サーバなどを DMZ に設置します。本機器では GapNAT 機能を利用して、LAN4 ポートを DMZ として運用することができます。DMZ は以下のような概念を持つネットワークです。

Memo インターネット側から開始された通信は、DMZ ネットワークに存在するパソコン(GapNAT 使用時は 1 台、マルチ GapNAT 使用時は複数台)に転送されます。

Memo DMZ ポートと他の LAN とは、相互に通信できません。

Memo LAN 内のパソコンからは、NAT 機能によりインターネットを利用できます。これらの仕組みにより、インターネット側から DMZ へ侵入された場合でも、DMZ と他の LAN との通信は遮断されているため、DMZ 経由で LAN への侵入はできません。これによりインターネット側からの侵入は、DMZ までで食い止めることができ、外部に公開していない他の LAN に存在するパソコンは、侵入者から保護されます。本機器は DMZ に対する通信に関しても、フィルタリングによる制限を設ける簡易的なファイアウォール機能を搭載しているため、更に安全性が高まります。

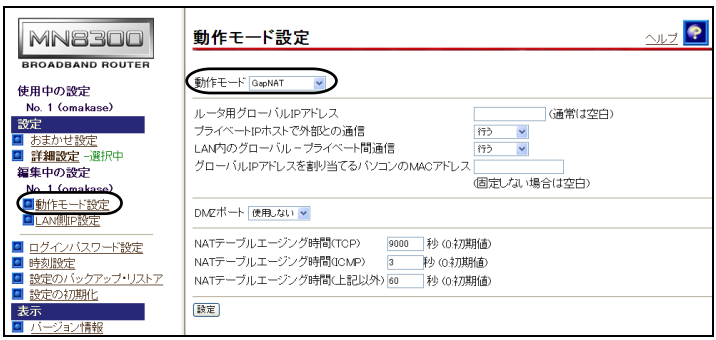


MN8300 では簡単な設定で、上記のような DMZ 環境を構築できます。

GapNAT の場合

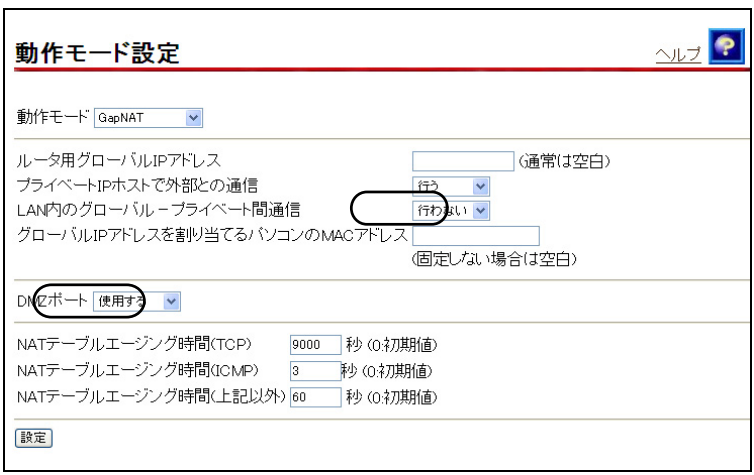
PPPoE 接続（端末型）などのようにグローバル IP アドレスを 1 つ割り当てられているときに DMZ を構築するには、GapNAT を使用します。以下の設定を行ってください。（事前にインターネットへの接続確認を済ませておいてください。）

① 「詳細設定」ページのメニューフレームから 動作モード設定 をクリックし[GapNAT]を選択します。

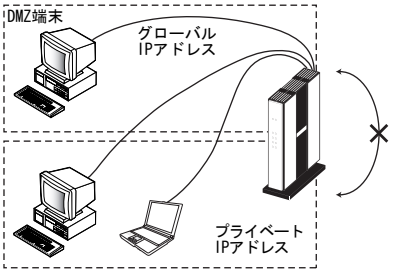


② LAN 内のグローバル-プライベート間通信を[行わない]を選択してください。これにより、DMZ と他の LAN との通信が不可能になります。

③ また、DMZ ポートを[使用する]を選択すれば、DMZ は LAN4 に固定されます。この場合、DMZ ホスト（外部ネットワークに公開したいパソコン）のみを LAN4/DMZ ポートのネットワークに設置してください。



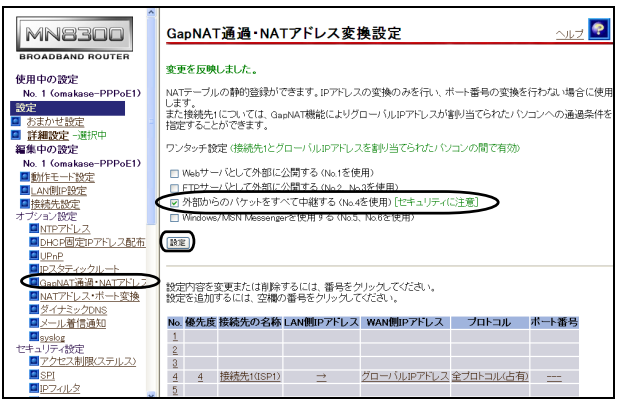
④ 設定 をクリックしてください。



注意 上記手順で[グローバル IP アドレスを割り当てるパソコンの MAC アドレス]を入力していない場合には、グローバル IP アドレスを持つパソコンをシャットダウンした後、初めて起動したパソコンに DHCP でグローバル IP アドレスが割り当てられます。DMZ ポートに複数のパソコンを接続する場合には意図しないパソコンにグローバル IP アドレスが割り当てられることがないように、DMZ ホストとなるパソコンの MAC アドレスを入力してください。「パソコンの IP アドレスや MAC アドレスを確認するには」(☞ p.169)

⑤ メニューフレームから GapNAT 通過・NAT アドレス変換 をクリックします。

⑥ 「外部からのパケットをすべて中継する」にチェックして、 設定 をクリックします。



⑦ メニューフレームから IP フィルタ をクリックし、[プライベートアドレスを使用した外部装置との通信を禁止]にチェックを入れてください。

⑧　さらに[外部装置から開始される TCP セッションを遮断]のチェックをはずします。

Memo　本設定を行った場合、DMZ だけでなく LAN 内からもインターネット上に存在するプライベート IP アドレスのサーバ等にアクセスできなくなります。その結果ビデオサーバ等をプライベート IP アドレスで運用している一部のプロバイダにおいて、それらのサービスを受けることができなくなります。

Memo　本設定により、スプーフィング（なりすまし）による攻撃の一部を遮断できます。

⑨　[外部との Windows 共有関係のトラフィックを遮断]にチェックを入れてください。

Memo　Windows のファイル共有機能(NBT：NetBIOSoverTCP/IP)に対するインターネット側からの攻撃が遮断されます。

⑩　設定 をクリックしてください。設定内容が保存され、動作に反映されます。

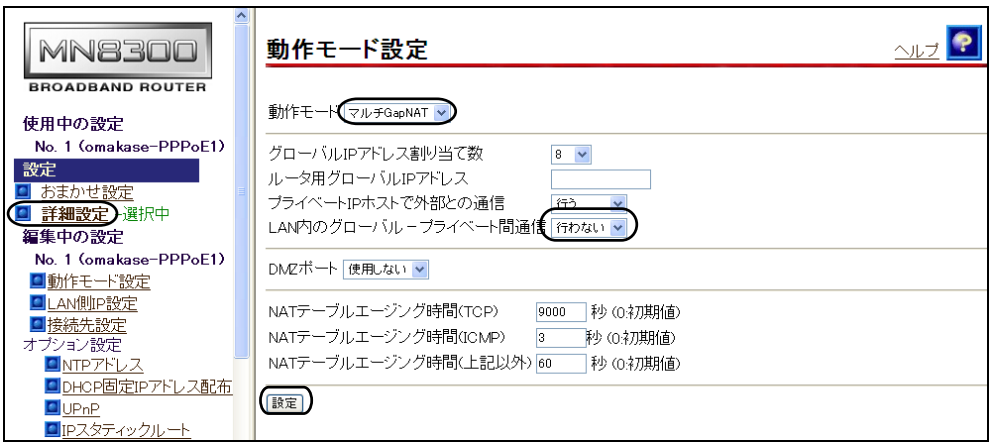
⑪　必要に応じて本書を参照し IP フィルタの設定を行ってください。DMZ 内のパソコンを攻撃から保護するために、IP フィルタ設定を行うことをお勧めします。

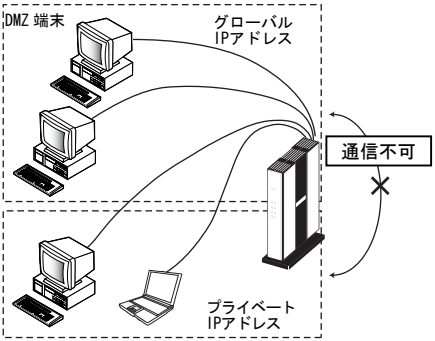
マルチ GapNAT の場合

グローバル IP アドレスを複数割り当てられているときに DMZ を構築するには、マルチ GapNAT を使用します。以下の設定を行ってください。(事前にインターネットへの接続確認を済ませておいてください。)

① 「詳細設定」ページのメニューフレームから 動作モード設定 をクリックし、[マルチ GapNAT]を選択します。

② LAN 内のグローバル-プライベート間通信を[行わない]を選択して 設定 をクリックしてください。これにより、DMZ と他の LAN との通信が不可能になります。





③　メニューフレームの左フレームの IP フィルタ をクリックし、[プライベートアドレスを使用した外部装置との通信を禁止]にチェックを入れてください。

④　さらに[外部装置から開始される TCP セッションを遮断]のチェックをはずします。

注意　本設定を行った場合、DMZ だけでなく LAN 内からもインターネット上に存在するプライベート IP アドレスのサーバ等にアクセスできなくなります。その結果、ビデオサーバ等をプライベート IP アドレスで運用している一部のプロバイダにおいて、それらサービスを受けることができなくなります。

Memo　本設定によりスプーフィング(なりすまし)による攻撃の一部を遮断できます。

⑤　[外部との Windows 共有関係のトラフィックを遮断]にチェックを入れてください。Windows のファイル共有機能(NBT：NetBIOSoverTCP/IP)に対するインターネット側からの攻撃が遮断されます。

⑥　設定 をクリックしてください。設定内容が保存され、動作に反映されます。

⑦　必要に応じて本書を参照しフィルタの設定を行ってください。DMZ 内のパソコンを攻撃から保護するために、フィルタ設定を行うことをお勧めします。

GapNAT（Global Address Proxy with NAT）とは

GapNAT（Global Address Proxy with Network Address Translation）は、従来単純 NAT ルータでは利用不可能であったネットワークミーティングや、一部のインターネット上での対戦型ゲームを、NAT ルータで実現するための機能です。GapNAT を使用した場合は、プロバイダから割り当てられたグローバル IP アドレスを、特定のパソコンに割り当てることにより、NAT ルータがもつ制限から解放することができます。LAN 側に複数パソコンが接続する場合には、本機器に対して最初に DHCP でアドレス取得要求を行ったパソコン、あるいは本機器に MAC アドレス登録を設定したパソコンに対して、グローバル IP アドレスが付与されます。2 台目以降のパソコンには、従来どおり DHCP によりプライベートアドレスが付与されます。

- インターネット側から通信が開始されるアプリケーション:
  NAT を使用している場合には、インターネット側から開始された通信を、LAN 側のどのパソコンに向けて転送すべきかを本機器が判断できないために、結果的には通信を行うことができずアプリケーションが正常に動作しません。
- IP アドレスやポート番号が、独自の方法で通信相手に通知されるアプリケーション:
  プライベート IP アドレスが割り当てられたパソコン上で動作しているアプケーションが、独自の方法で通信相手に IP アドレスを通知しても、通常の NAT 機能では、インターネット上で通用するグローバル IP アドレスに変換できません。このため、LAN 上で使用しているプライベート IP アドレスがそのままインターネット上の通信相手に伝えられてしまいます。結果的に通信相手は、インターネット上に存在しない IP アドレスをもとに通信しようとしてしまうため、通信が継続できなくなります。

GapNAT 機能は、NAT ルータの利点を維持しつつ、LAN 内のパソコンに対して、次の機能を提供します。

- インターネット側から開始された通信を、特定のパソコンに割り振ります。
- パソコン自体にインターネットから認識できる IP アドレスを付けます。
  また GapNAT にはプロバイダから割り当てられるグローバル IP アドレスの個数に応じて、次の 2 つの種類があります。
  - GapNAT（割り当てられるグローバル IP アドレスが 1 つの場合）：
    LAN 内の 1 台のパソコンで、グローバル IP アドレスを使って通信できます。
  - マルチ GapNAT（割り当てられるグローバル IP アドレスが複数の場合）：
    LAN 内の複数のパソコンで、グローバル IP アドレスを使って通信できます。

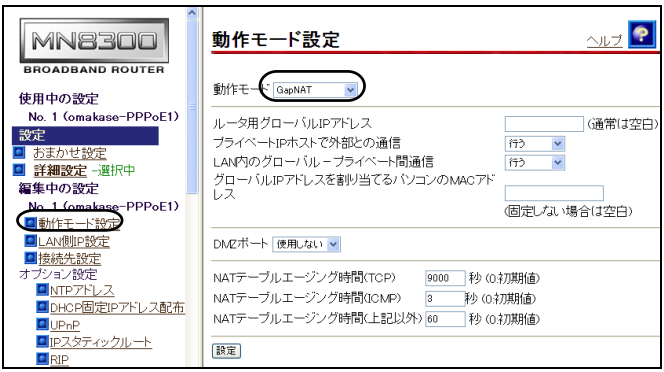
GapNATの設定方法

ここでは初期導入時を想定して説明します。

GapNAT 設定ページの表示

① 詳細設定画面から編集したい設定番号の 編集する をクリックしメニューフレームから 動作モード設定 をクリックします。

② 動作モードで[GapNAT]を選択して 設定 をクリックします。

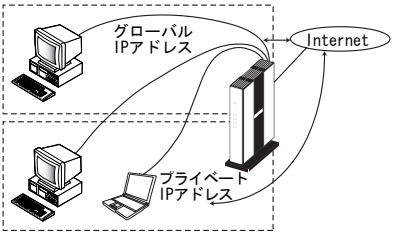


［プライベート IP ホストで外部との通信を行う/行わない］

プライベート IP アドレスが割り当てられたパソコンから、インターネットを利用できるようにするかどうかを選択してください。

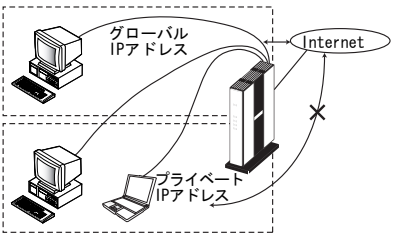
◆ ［行う］を選択した場合：

GapNAT 対象となっているパソコン以外からも、インターネットへのアクセスができます。



◆ ［行わない］を選択した場合：

GapNAT 対象となっているパソコンのみインターネットへのアクセスができます。

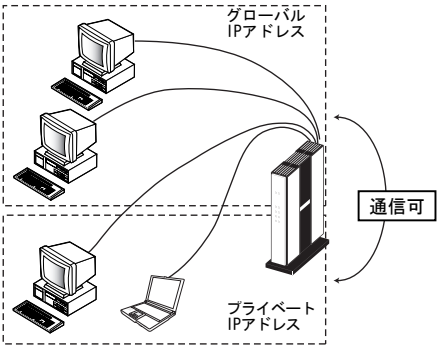


[LAN 内のグローバル-プライベート間通信を行う/行わない]

プライベート IP アドレスと、グローバル IP アドレスが割り当てられたパソコン同士を、相互に通信できるようにするかどうかを選択してください。

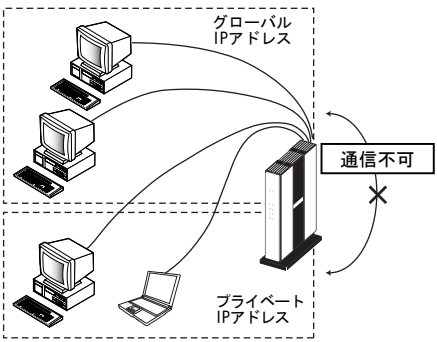
◆ [行う]を選択した場合：

プライベート IP アドレスとグローバル IP アドレスが割り当てられたパソコン同士は、相互に通信を行うことができます。（デフォルト値は[行う]となっています。）



◆ [行わない]を選択した場合：

相互に通信を行うことができません。



Memo　**グローバル-プライベート間通信について**

GapNAT を使用することにより、LAN 内に本機器の WAN 側と同じグローバル IP アドレスが割り当てられたパソコンを 1 台設置することができますが、2 台目以降のパソコンには、LAN 内で使用するプライベート IP アドレスが割り当てられているため、GapNAT 対象とするパソコンと、それ以外のパソコンとではアドレス体系が異なってしまい、そのままでは相互に通信を行うことができません。
本機器では、LAN 側に存在する 2 つのアドレス間をルーティングすることにより、相互に通信することを可能にしています。グローバル IP アドレス端末とプライベート IP アドレス端末間のファイル共有を行いたい場合には、[LAN 内のグローバル-プライベート間通信を行う/行わない]を[行う]と設定します。

[グローバル IP アドレスを割り当てるパソコンの MAC アドレス]

特定のパソコンを常に GapNAT 対象として、グローバル IP アドレスを割り当てたい場合は、該当するパソコンの MAC アドレスを入力してください。次回 IP アドレスが割り当てられる際、入力した MAC アドレスのパソコンに、グローバル IP アドレスが割り当てられます。

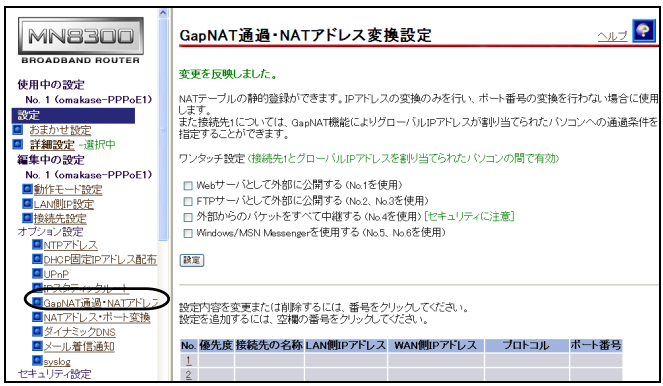
注意　MAC アドレスは、2 桁ずつハイフンかコロンで区切って入力するか、または区切りなしで入力してください。
入力例：02-23-45-67-89-01　01:23:45:67:89:01　012345678901
現在グローバル IP アドレスが割り当てられているパソコンの MAC アドレスは、次の方法で確認することができます。

Memo　MAC アドレスの確認方法は
①本機器起動時にグローバル IP アドレスを割り当てたいパソコンを最初に起動してください。
②Web ブラウザで本機器の設定ページを表示してください。
③メニューから GapNAT 情報 を選択してください。

[GapNAT 通過制限設定]

ここでは LAN 内のグローバル IP アドレスが割り当てられたパソコンに対して、インターネット側からどのような通信を通過させるかを設定してください。初期設定では、インターネット側からのすべてのデータは転送されません。

① 「詳細設定」ページのメニューフレームから GapNAT 通過・NAT アドレス変換 をクリックします。



② 設定したいチェックボックスにチェックして 設定 をクリックします。

GapNAT 機能利用時にワンタッチで以下の内容が設定できます。

・Web サーバとして外部に公開する
・FTP サーバとして外部に公開する
・外部からのパケットをすべて中継する
・Windows/MSN Messenger を使用する

③ GapNAT 通過・NAT アドレス変換画面で[No.1～64]の番号をクリックしてください。

◆ **優先度**：
この条件の優先度を 0～99 までの範囲で設定します。各条件はこの値の小さい順に評価され、最初に合致した条件だけが GapNAT の動作に反映されます。尚、0 を指定した場合、設定は無効になります。
また、値が小さいほど優先度は高くなります。複数の条件に同じ優先度を指定することはできませんが、例外として 0 だけは同時に複数指定することができます。

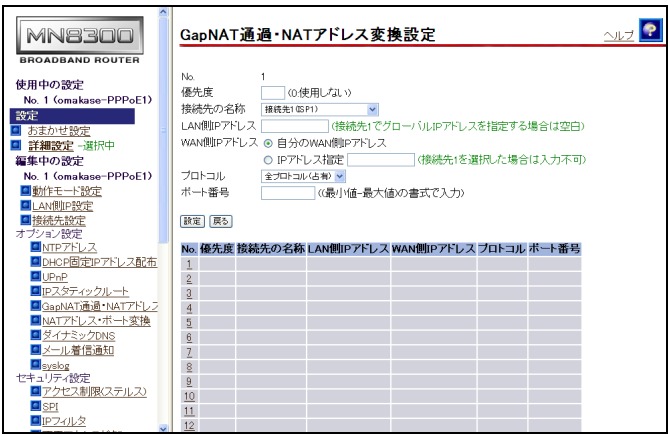
◆ **接続先の名称**：
この設定を適用する接続先を選択します。

◆ **LAN 側 IP アドレス**：
使用する LAN 側パソコンの IP アドレスを設定します。

◆ **WAN 側 IP アドレス**：
変換後の WAN 側 IP アドレスを設定します。通常は[自分の WAN 側 IP アドレス]を選択してください。

◆ **プロトコル**：
変換対象となるプロトコルを選択します。[全プロトコル]を選択した場合は、すべてのプロトコルが変換対象となります。また、[TCP と UDP 両方]については、すべてのポートを指定した場合と同様となります。セキュリティを十分に考慮して設定してください。

◆ **ポート番号**：
ポート番号を入力してください。範囲指定したい場合は、最小値と最大値を「-」（半角ハイフン）でつないでください。



Memo プロトコルに次のいずれかを指定した場合のみ、ポート番号の指定を行ってください。

・TCP・UDP・TCP と UDP の両方

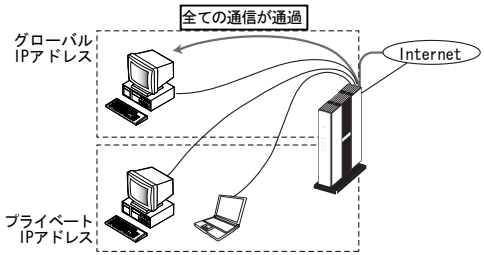
Memo 全てのプロトコルについて通過を許可する場合で、プライベートアドレスを割り当てられたその他のパソコンを使って外部との通信を行う場合は[全プロトコル（共有）]を選んでください。GapNAT 端末だけを利用する場合は[全プロトコル（占有）]を選んでください。

Memo 動作モードで「GapNAT」を選んだ場合に表示される以下設定項目[プライベート IP ホストで外部との通信]と[全プロトコル(共有)]の両方とも使用する(行う）と設定されたときのみプライベート IP アドレスを割り当てられたパソコンが利用できるようになります。

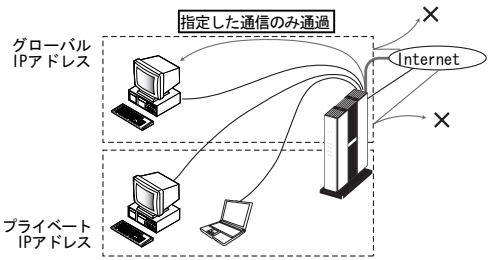
Memo 次のポート番号は名称で入力することができます。ただし、名称で入力した場合は範囲を指定することができません。

20：ftpdata	21：ftp	23：telnet	25：smtp
53：domain	80：www	110：pop	111：sunrpc
119：nntp	123：ntp	513：login	520：route
1723：pptp			

◆ **外部からのすべての通信を通過させる場合**：
インターネット側から開始された通信が、LAN 内のグローバル IP アドレスが割り当てられたパソコンにすべて転送されます。



◆ **常に通過させるプロトコルと TCP/UDP ポート番号を制限する場合**：
インターネット側から開始された通信のうち、あらかじめ指定した通信だけが、LAN 内のグローバル IP アドレスが割り当てられたパソコンに転送されます。



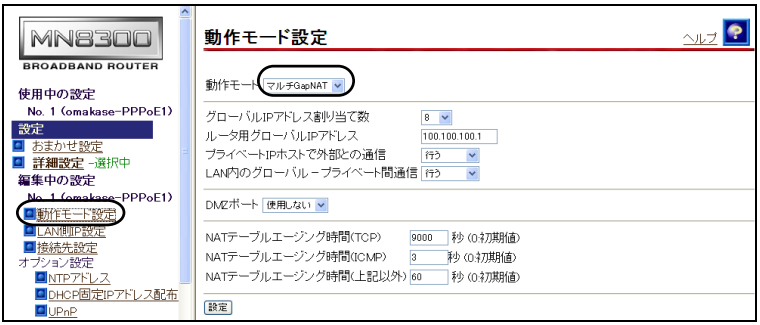
Memo 通過させたい通信を指定しない場合、インターネット側から開始された通信は転送されません。

マルチGapNATの設定方法

ここでは初期導入時を想定して説明します。

① 詳細設定画面から編集したい設定番号の 編集する をクリックし、メニューフレームから 動作モード設定 をクリックします。

② 動作モードで「マルチ GapNAT」を選択します。



[グローバル IP アドレス割り当て数]

① プロバイダから割り当てられたグローバル IP アドレスの個数を「8」・「16」・[32]から選択してください。

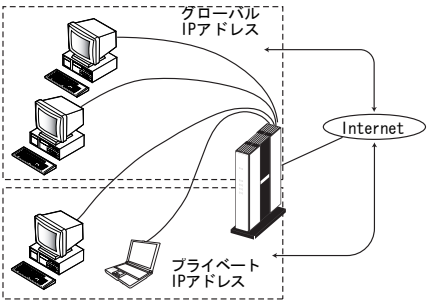
[ルータ用グローバル IP アドレス]

② プロバイダから割り当てられたグローバル IP アドレスのうち、本機器に設定する IP アドレスを入力してください。

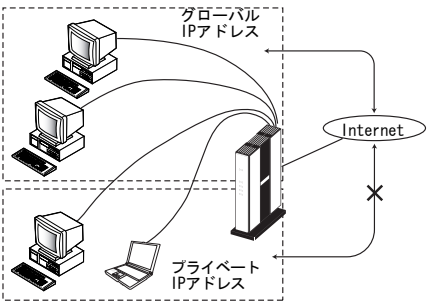
Memo プロバイダから割り当てられた IP アドレスのうち、先頭と末尾はネットワーク名とブロードキャストアドレスとして使用されるため、本機器やパソコンには割り当てることができません。それらの IP アドレスを除外した残りの IP アドレスのうち 1 つを、本機器の LAN 側に割り当てる必要があります。

③　プライベート IP ホストで外部との通信を行う/行わない。プライベート IP アドレスが割り当てられたパソコンからインターネットを利用できるようにするかを選択してください。

◆ [行う]を選択した場合：
マルチ GapNAT 対象となっているパソコン以外からも、インターネットへのアクセスができます。

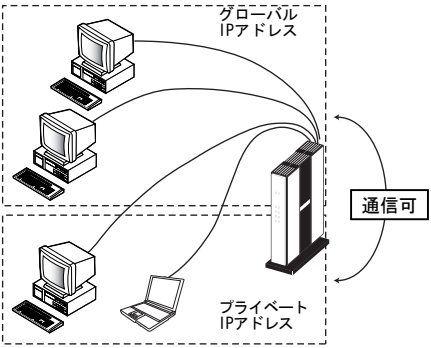


◆ [行わない]を選択した場合：
マルチ GapNAT 対象となっているパソコンのみ、インターネットへのアクセスができます。

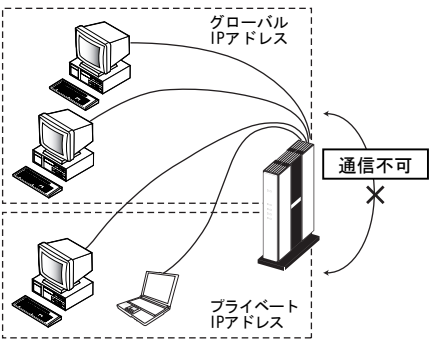


④ LAN 内のグローバル-プライベート間通信をプライベート IP アドレスと、グローバル IP アドレスが割り当てられたパソコン同士が、相互に通信できるようにするかどうかを選択して設定をクリックしてください。

◆ [行う]を選択した場合：
プライベート IP アドレスとグローバル IP アドレスが割り当てられたパソコン同士は、相互に通信を行うことができます。



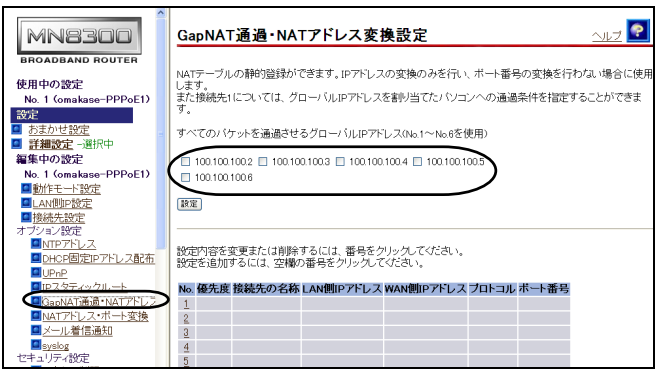
◆ [行わない]を選択した場合：
相互に通信を行うことができません。



[GapNAT 通過設定]

ここでは LAN 内のグローバル IP アドレスが割り当てられたパソコンに対して、インターネット側からどのような通信を通過させるかを設定してください。初期設定では、インターネット側からのすべてのデータは転送されません。

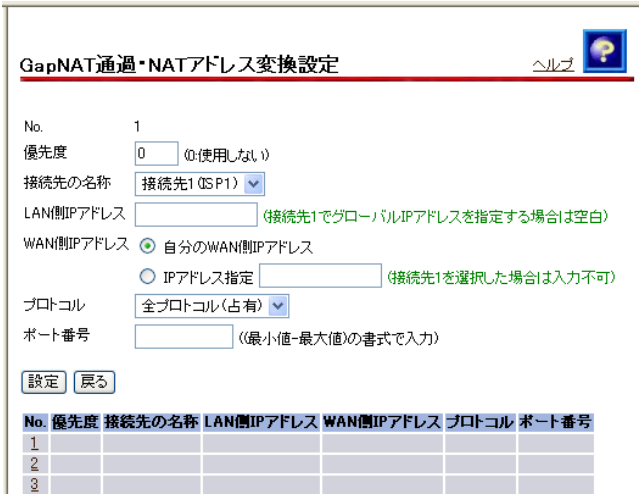
① 「詳細設定」ページのメニューフレームから GapNAT 通過・NAT アドレス変換設定 をクリックします。



② 外部から受信した全てのパケットを通過させるグローバル IP アドレスにチェックして 設定 をクリックします。

Memo 通過させたい通信を指定しない場合、インターネット側から開始された通信は転送されません。

③　通過させるパケットを指定する場合は GapNAT 通過・NAT アドレス変換設定画面で[No.1～64]の番号をクリックしてください。



表の各項目の説明

◆ **優先度**
この条件の優先度を 0～99 までの範囲で設定します。各条件はこの値の小さい順に評価され、最初に合致した条件だけが GapNAT の動作に反映されます。尚、0 を指定した場合、設定は無効になります。また、値が小さいほど優先度は高くなります。複数の条件に同じ優先度を指定することはできませんが、例外として 0 だけは同時に複数指定することができます。

◆ **接続先の名称**
この設定を適用する接続先を選択します。

◆ **LAN 側 IP アドレス**
使用する LAN 側パソコンの IP アドレスを設定します。

◆ **WAN 側 IP アドレス**
変換後の WAN 側 IP アドレスを設定します。グローバル IP アドレスを設定します。グローバル IP アドレスを指定する場合は、[IP アドレス指定]にチェックして IP アドレスを入力してください。

◆ **プロトコル**
変換対象となるプロトコルを選択します。[全プロトコル]を選択した場合は、すべてのプロトコルが変換対象となります。また、[TCP と UDP 両方]については、すべてのポートを指定した場合と同様となります。セキュリティを十分に考慮して設定してください。

◆ **ポート番号**
ポート番号を入力してください。範囲指定したい場合は、最小値と最大値を「-」（半角ハイフン）でつないでください。

Memo　プロトコルに次のいずれかを指定した場合のみポート番号の指定を行ってください。
・TCP・UDP・TCP と UDP の両方

Memo　次のポート番号は名称で入力することができます。ただし、名称で入力した場合は範囲を指定することができません。

20:ftpdata	21:ftp	23:telnet	25:smtp	53:domain
80:www	110:pop	111:sunrpc	119:nntp	123:ntp
513:login	520:route	1723:pptp		

運用の開始

注意　プロバイダから複数の IP アドレスの割り当てを受ける場合、割り当てられた IP アドレスが変動することはないため、マルチ GapNAT にはグローバル IP アドレスを DHCP によって割り当てる機能は搭載していません。それぞれ手動で IP アドレスを設定してください。

① **GapNAT の対象となるパソコンにグローバル IP アドレスを設定してください。**

Memo　設定方法についての詳細は、パソコン、または OS 付属の取扱説明書を参照してください。

② **GapNAT の対象外のパソコンを、すべてシャットダウンしてください。DHCP により割り当てられていたネットワーク設定の内容が、すべて解放されます。**

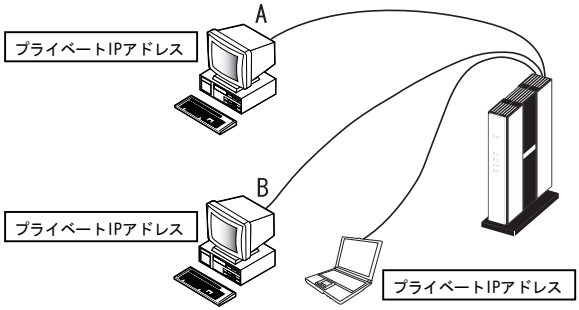
③ **GapNAT の対象外のパソコンを、すべて起動してください。DHCP によりプライベート IP アドレスが、それぞれのパソコンに割り当てられます。**

Memo　本機器の再起動を行った場合は、DHCP のリーステーブルが消去されるため、DHCP によって IP アドレスが配布されているパソコンは、すべてシャットダウンしてください。

GapNAT対象端末の変更方法

次のようなネットワークにおいて、パソコン A に割り当てられているグローバル IP アドレスを、パソコン B に割り当て直す方法について説明します。

Memo マルチ GapNAT を使用している場合は、グローバル IP アドレスを、手動で付け直してください。ここで説明するような手順は不要です。

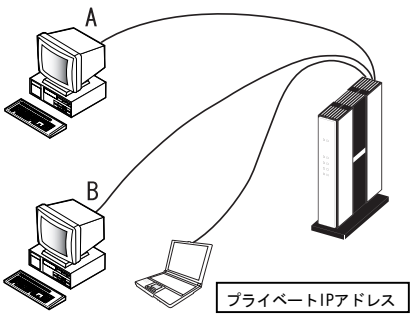


Memo グローバル IP アドレスを割り当てるパソコンの MAC アドレスに、パソコン A の MAC アドレスが設定されている場合は、事前にパソコン B の MAC アドレスに書き換えておいてください。

Memo グローバル IP アドレスを割り当てようとするパソコンは、DHCP で IP アドレスを取得できるように設定しておいてください。

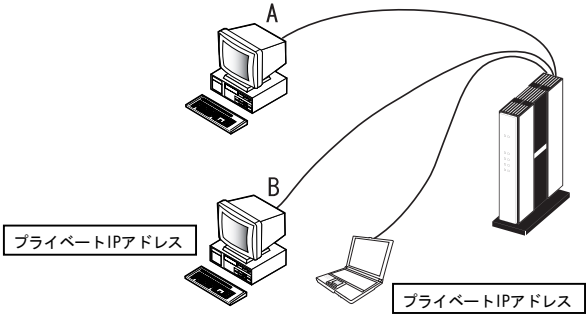
Memo グローバル IP アドレスを割り当てるパソコンを変更するには、DHCP で割り当てられた IP アドレスを解放し、書き換える操作が必要となります。本章の説明に従って、IP アドレスの解放と書き換えを行ってください。

① パソコン A および B 共に IP アドレスを解放してください。パソコン A、B 共に IP アドレスが付けられていない状態になります。



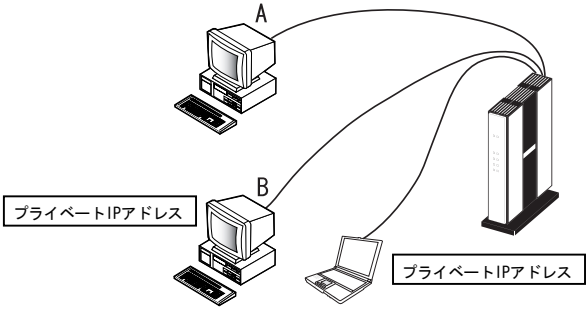
Memo グローバル IP アドレスを割り当てるパソコンを変更する際には、関係するパソコンの IP アドレスを、一旦解放しておく必要があります。

② **パソコン B の IP アドレスを書き換えてください。パソコン B に対して、グローバル IP アドレスが割り当てられます。**



Memo パソコンの設定内容等によっては、動作が不安定になる場合があります。

③ **パソコン A の IP アドレスを書き換えてください。パソコン A に対して、プライベート IP アドレスが割り当てられます。**



以上の操作で GapNAT 対象のパソコンを変更することができます。

Memo GapNAT 対象のパソコンを変更する場合は、DHCP により IP アドレスを取得し直してください。ただし、上位アプリケーションや OS の一部の機能が、IP アドレスの変更を認識できず、パソコンの動作が不安定になる場合があります。念のためにパソコンの再起動を行ってください。再起動を行う場合は、グローバル IP アドレスを割り当てたパソコンが、最初に起動するようにしてください。

Memo 本書では、パソコンの通信用のプロトコルとして、TCP/IP のみがインストールされていることを前提として説明をしています。

UPnP機能とWindows/MSN Messenger

UPnP（Universal Plug and Play）とは

本機器は、UPnP 機能を実装しています。これにより、UPnP に対応したネットワークアプリケーションソフトウェアや UPnP 対応機器の利用が可能になります。本機能は NAT モード、GapNAT モード、マルチ GapNAT モード利用時にメインセッション、サブセッションそれぞれで有効ですが、IP ルータモードでは動作しません。

概要

UPnP IGD（Internet Gateway Device）に準拠し、NAT トラバーサル機能（※）に対応しています。これにより、本機器の LAN ポートに接続した複数台のパソコンから同時に Windows Messenger や MSN Messenger を利用できます。また、Windows/MSN Messenger の利用する機能によって必要だったポート設定が不要となります。

※　NAT トラバーサル機能
ネットワーク認識アプリケーションが、NAT デバイスの配下にあることを検出し、外部 IP アドレスを識別して、NAT の外部ポートからアプリケーションの使用する内部ポートへパケットを転送するポートマッピングを設定できる一連の機能を指します。

UPnP を利用できるパソコン（平成 16 年 2 月現在）

UPnP を利用できるパソコンは、Windows XP と Windows Me です。最大 10 台のパソコンから同時に Windows/MSN Messenger 等の UPnP 対応ネットワークアプリケーションソフトウェアを利用することができますが、利用する機能によっては同時接続可能端末数が 10 台に満たない場合があります。

Memo　Windows/MSN Messenger は、自動的にポートと IP アドレスの割り当て（静的 NAT 設定）を行う仕様です。
使用する静的 NAT テーブル数は利用する Windows/MSN Messenger の機能によって異なります。
従って、Windows/MSN Messenger の利用する機能によっては 10 台未満のクライアントしか同時に接続できない場合があります。

Memo　本機器は UPnP で設定可能な静的 NAT 設定情報は 128 件です。

Memo　Windows/MSN Messenger は本機器のメインセッションでのみ利用可能です。

UPnP 対応ネットワークアプリケーションソフトウェア/UPnP 対応ネットワーク機器

平成 16 年 2 月現在、動作を確認している UPnP 対応のネットワークアプリケーションソフトウェアは以下の通りです。

Windows/MSN Messenger

本機器使用時に、Windows/MSN Messenger で使用できる機能は次の通りです。

（Windows/MSN Messenger 動作確認表）

OS	Windows Me		Windows XP SP1	
Messenger version	MSN Messenger Ver.4.7	MSN Messenger Ver.5.0/6.1	Windows Messenger Ver.4.7	MSN Messenger Ver.5.0/6.1
PC台数	～10台まで	～10台まで	～10台まで	～10台まで
1.インスタントメッセージ	○	○	○	○
2.音声チャット	○	○	○	○
3.ビデオチャット	－	－	○	○
4.電話をかける	○※1	○※1	○※1	○※1
5.ファイル転送	○※1	○※1	○※1	○
6.アプリケーション共有	－	－	○	○
7.ホワイトボード	－	－	○	○
8.リモートアシスタント	－	－	○	○
同一LAN内同士の音声チャット	○	○	○	○
同一LAN内同士のファイル送信	×	×	×	×
同一LAN内同士のビデオチャット	－	－	○	○
同一LAN内同士のアプリケーション共有	－	－	○	○
同一LAN内同士のホワイトボード	－	－	○	○

※UPnP 準拠の機能ではありませんが、本機器独自の機能によって利用可能です。

Memo Windows XP を利用する場合は、「Windows Update」から「Service Pack1」と「重要な更新」の全てをインストールしてください。

Memo Windows Me を利用する場合は、DirectX 8.1 以降のインストールと、「Windows Update」から「重要な更新」の全てをインストールしてください。

フレッツ・コネクト「UPnP 対応用ユーティリティソフトウェア」

NTT 東日本のフレッツ・ADSL 環境で IP テレビ電話機能を実現する「フレッツ・コネクト」の「UPnP 対応用ユーティリティソフト」に対応し、インターネットと、フレッツ・コネクトの同時利用が可能です。
フレッツ・コネクトの利用について「PPPoE マルチセッションを使用するには」（☞ p. 98）を参照してください。
⇒http://flets.com/connect/

Xbox

Xbox を本機器の LAN ポートに接続して、マイクロソフトの提供するオンラインネットワークサービス Xbox *Live* が利用できます。
Xbox *Live* については、下記の URL を参照してください。
⇒http://Xbox.jp/Live/

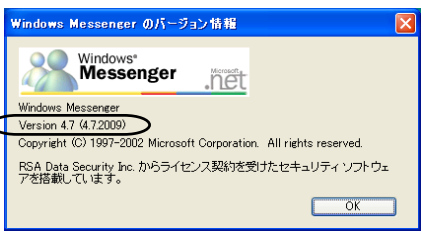
Windows/MSN Messengerを利用するーパソコンの準備

Windows XP の場合

[Windows/MSN Messenger のバージョン確認]

① **Windows/MSN Messenger の[ヘルプ]メニューから「Windows/MSN Messenger のバージョン情報」を選択して Windows/MSN Messenger のバージョンを確認してください。**

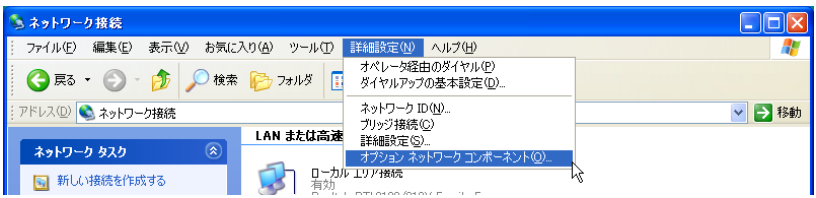
本機器は Windows Messenger 4.7、MSN Messenger 5.0/6.1 で動作確認しています。Windows Messenger 4.7、MSN Messenger 5.0/6.1 より新しいバージョンでの動作確認については、以下のホームページを参照してください。
⇒http://www.ntt-me.co.jp/mn/



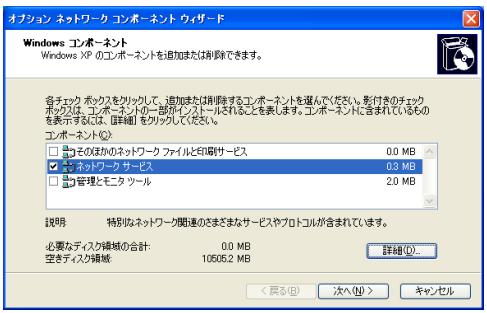
[UPnP の設定]

① [スタート]メニューの マイコンピュータ から マイネットワーク を選び、ネットワーク接続を表示する を選びます。

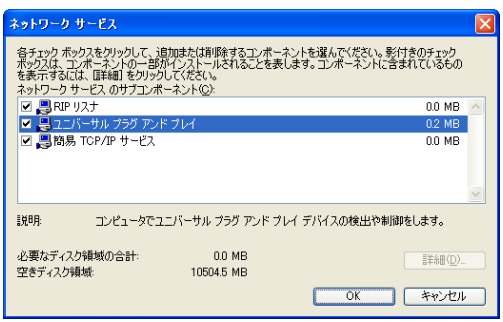
② [詳細設定]メニューから「オプションネットワークコンポーネント」をクリックします。



③ 「ネットワークサービス」を選択して反転表示させ 詳細 をクリックします。



④ ネットワークサービスの画面で「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確認します。チェックされていなければチェックして OK をクリックします。Windows XP の CD-ROM を要求されたときは画面の指示に従って操作してください。



Windows Me の場合

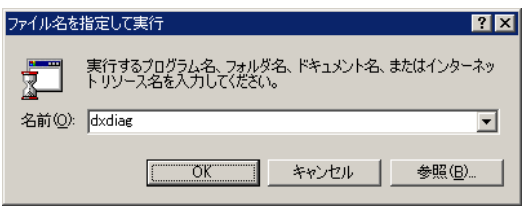
[Windows/MSN Messenger のバージョン確認]

① MSN Messenger の[ヘルプ]メニューから MSN Messenger のバージョン情報 を選択して MSN Messenger のバージョンを確認してください。本機器は MSN Messenger 5.0/6.1 で動作確認しています。
MSN Messenger 5.0/6.1 より新しいバージョンでの動作確認については、以下のホームページを参照してください。⇒http://www.ntt-me.co.jp/mn/

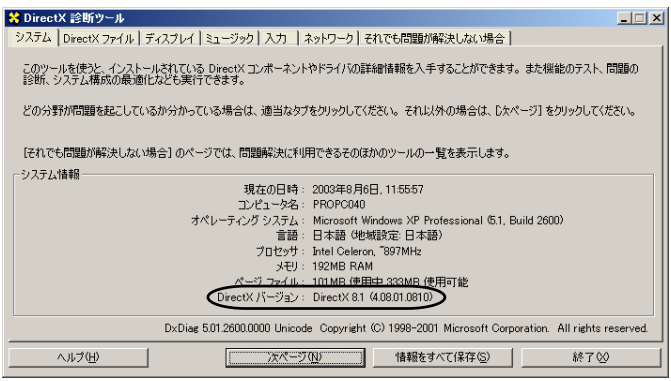
[DirectX のバージョン確認]

① [スタート]メニューの ファイル名を指定して実行 を選択します。

② 名前に「dxdiag」を入力して OK をクリックします。



③ DirectX のバージョンが 8.1 より古い場合はバージョンアップしてください。



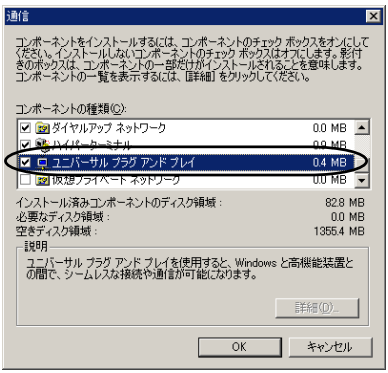
[UPnP の設定]

① [スタート]メニューの 設定 から コントロールパネル を選びます。

② アプリケーションの追加と削除 をダブルクリックして Windows ファイル タブをクリックします。

③ コンポーネントの種類 で「通信」を選択して反転表示させ 詳細 をクリックします。

④ コンポーネントの種類 で「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確認します。チェックされていなければチェックして OK をクリックします。Windows Me の CD-ROM を要求されたときは画面の指示に従って操作してください。



Windows/MSN Messengerを利用する－MN8300の設定

UPnP 対応ネットワークアプリケーションソフトウェア（Windows/MSN Messenger など）を利用する場合の設定

[UPnP 設定]

UPnP は初期設定の状態では本機器の LAN ポートに接続されたパソコンすべてから利用可能になっていますが、オプション設定の「UPnP 設定」（☞ p. 58）で、UPnP NAT 情報の自動消去や UPnP を利用するパソコンを限定することが可能です。UPnP NAT 情報の自動消去、UPnP を利用するパソコンの限定をしない場合には本設定は必要ありません。

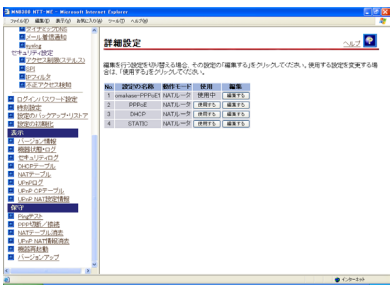
[IP フィルタ設定]

UPnP で Windows/MSN Messenger の「インスタントメッセージ」以外の機能を利用する場合には以下の設定が必要です。

① メニューフレームから詳細設定をクリックします。

② 編集したい No. の 編集する をクリックします。

③ メニューフレームから IP フィルタ をクリックします。



④ [外部装置から開始される TCP セッションを遮断]のチェックを外して 設定 をクリックします。

[GapNAT 通過・NAT アドレス変換設定]

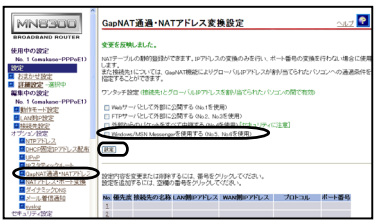
動作モードを「GapNAT」で Windows/MSN Messenger を利用する場合は以下の設定を行ってください。

① メニューフレームから[詳細設定]をクリックします。

② 編集したい No.の 編集する をクリックします。

③ メニューフレームから[GapNAT 通過・NAT アドレス変換]をクリックします。

④ [Windows/MSN Messenger を使用する]にチェックして 設定 をクリックします。



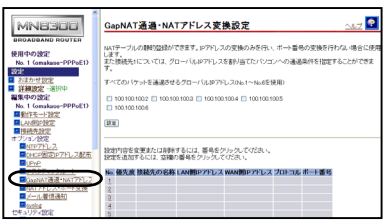
動作モードを「マルチ GapNAT」で Windows/MSN Messenger を利用する場合は以下の設定を行ってください。

① メニューフレームから[詳細設定]をクリックします。

② 編集したい No.の 編集する をクリックします。

③ メニューフレームから[GapNAT 通過・NAT アドレス変換]をクリックします。

④ [No.1～64]の番号をクリックします。



⑤ Windows/MSN Messenger を使用する PC 毎に以下の設定を行います。

優先度	= 1～99
接続先の名称	= [接続先 1 の名称]
LAN 側の IP アドレス	= 空白
WAN 側の IP アドレス	= [Windows/MSN Messenger を使用する PC のグローバル IP アドレス]
プロトコル	= TCP
ポート番号	= 1503

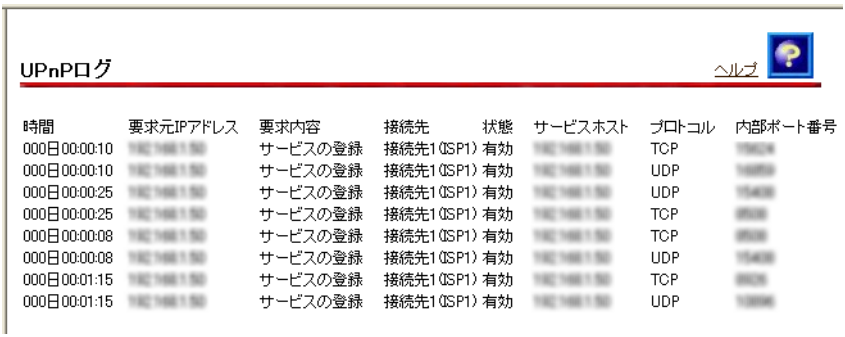
設定の詳細は、p.135～p.136 を参照してください。

UPnP関連情報の表示

[UPnP ログ]

UPnP に対応したネットワークアプリケーションソフトウェアが本機器に対して行ったリクエストのログを最新のものから表示します。最大ログ件数は 100 件です。100 件を超えた場合は古いものから順に消去されます。UPnP ログは以下の手順で確認できます。

① 詳細設定ページのメニューフレームから UPnP ログ をクリックします。



設定画面の各項目の説明

◆ 時間
リクエストを本機器が受け取った時間が表示されます。ログは「時刻の設定」(☞ p. 86) を行っていなければ機器起動時点を 0 時とする相対時刻で表示される場合があります。

◆ 要求元 IP アドレス
IP アドレスリクエストを送信した IP アドレスが表示されます。

◆ 要求内容
リクエストの内容が表示されます。表示内容は次のいずれかの項目です。

・UPnP 用の静的 NAT 設定情報が操作された場合
1) サービスの登録　UPnP 用静的 NAT 設定情報が新規登録された。
2) サービスの削除　UPnP 用静的 NAT 設定情報が削除された。
3) サービスの更新　UPnP 用静的 NAT 設定情報が更新された。
4) サービスの全削除 UPnP 用静的 NAT 設情情報が WWW から全削除された。
5) 登録不可　　UPnP 用静的 NAT 設定情報が最大件数 128 件を超えた。

・PPP 接続／切断要求があった場合
1) PPP 接続要求　　PPP の接続要求があった。
2) PPP 切断要求　　PPP の切断要求があった。

以下の情報は UPnP 用の静的 NAT 情報に対するリクエストがあった場合にだけ表示されます。

- ◆ 接続先対象の接続先を表示します。
- ◆ 状態登録された UPnP 用の静的 NAT 設定情報の状態を表示します。以下 2 つの状態を表示します。
  1) 有効　登録された UPnP 用の静的 NAT 設定情報は使用される。
  2) 無効　登録された UPnP 用の静的 NAT 設定情報は使用されない。
- ◆ サービスホスト登録された UPnP 用の静的 NAT 設定情報の LAN 側 IP アドレスを表示します。
- ◆ プロトコル登録された UPnP 用の静的 NAT 設定情報のプロトコルを表示します。TCP もしくは UDP のいずれかを表示します。
- ◆ 外部ポート番号登録された UPnP 用の静的 NAT 設定情報の WAN 側ポート番号を表示します。
- ◆ 内部ポート番号登録された UPnP 用の静的 NAT 設定情報の LAN 側ポート番号を表示します。
- ◆ 有効期限 UPnP 用の静的 NAT 設定情報の有効期限を秒数で表示します。Windows/MSN Messenger から設定される静的 NAT 設定情報はすべて“無期限”が指定されます。

[UPnP CP（コントロールポイント）テーブル]

本機器で認識された UPnP に対応したネットワークアプリケーションソフトウェアが動作しているパソコンの IP アドレスと MAC アドレスを表示します。最大 10 件が表示されます。
UPnP に対して無通信が続くと OS によって以下の時間経過後に消去されます。
・Windows Me の場合： 約 10 分
・Windows XP の場合： 約 30 分
また、ARP の有効期限が切れた場合 MAC アドレスは 00:00:00:00:00:00 で表示されます。
UPnP CP（コントロールポイント）テーブルは次の手順で確認できます。

① 詳細設定ページのメニューフレームから UPnP CP テーブル をクリックします。

[UPnP NAT 設定情報]

UPnPに対応したネットワークアプリケーションソフトウェアが本機器に登録したNAT設定情報を表示します。最大 128 件まで表示されます。UPnP NAT 設定情報は次の手順で確認できます。

① 詳細設定ページのメニューフレームから UPnP NAT 設定情報 をクリックします。

設定画面の各項目の説明

◆ 状態
登録された UPnP 用の静的 NAT 設定情報の状態を表示します。以下 2 つの状態を表示します。
1) 有効登録された UPnP 用の静的 NAT 設定情報は使用されている。
2) 無効登録された UPnP 用の静的 NAT 設定情報は使用されていない。

◆ サービスホスト
登録された UPnP 用の静的 NAT 設定情報の LAN 側 IP アドレスを表示します。

◆ 接続先
対象の接続先を表示します。

◆ プロトコル
登録された UPnP 用の静的 NAT 設定情報のプロトコルを表示します。TCP もしくは UDP のいずれかを表示します。

◆ 内部ポート番号
登録された UPnP 用の静的 NAT 設定情報の LAN 側ポート番号を表示します。

◆ 外部ポート番号
登録された UPnP 用の静的 NAT 設定情報の WAN 側ポート番号を表示します。

◆ 有効期限
UPnP 用の静的 NAT 設定情報の有効期限を秒数で表示します。Windows/MSN Messenger から設定される静的 NAT 設定情報はすべて “無期限” が指定されます。

◆ サービスの説明
Windows/MSN Messenger 等の UPnP に対応したネットワークアプリケーションソフトウェアによって設定された説明を最大 60 文字で表示します。

[UPnP NAT 情報消去]

UPnPに対応したネットワークアプリケーションソフトウェアが本機器に登録したNAT設定情報を強制的に消去するために使用します。[消去]をクリックすると直ちにすべての UPnP 用の NAT 設定情報が消去されます。

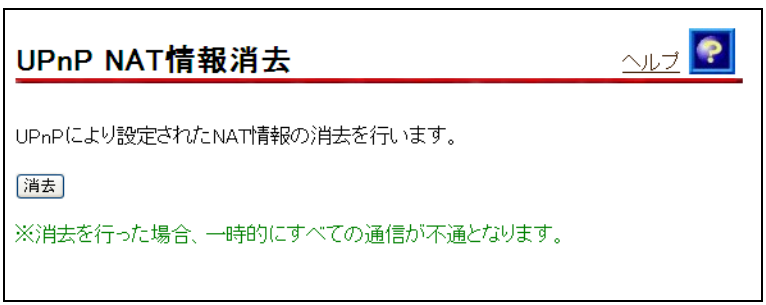
注意 利用する機能によって、Windows/MSN Messenger を終了しても UPnP NAT 設定情報が残留することがあります。UPnP NAT 設定情報は最大 128 件までしか設定できないので、残留した UPnP NAT 設定情報が蓄積されると正常に Windows/MSN Messenger が利用できなくなることが考えられます。またセキュリティ上の観点からも UPnP NAT 情報消去(自動消去)を実行することをお勧めします。

注意 UPnP NAT 設定情報を消去したとき、一時的にインターネットに対するすべての通信が不通になります。Windows/MSN Messenger を起動している状態で設定変更した場合は、Windows/MSN Messenger を一旦終了してから起動し直してください。Windows/MSN Messenger をサインインし直すだけでは正常に動作しませんのでご注意ください。

Memo UPnP 設定画面（☞ p.58）で UPnP NAT 設定情報の自動消去の時間を設定すると、使用中の UPnP NAT 情報以外を自動消去できます。

UPnP NAT 情報消去は次の手順で行います。

① 詳細設定ページのメニューフレームから UPnP NAT 情報消去 をクリックします。



② 消去 をクリックします。

［動作確認情報］

UPnP で Windows/MSN Messenger 等の UPnP に対応したネットワークアプリケーションソフトウェアを利用する場合の動作について、通信する相手の環境によって制約がある場合があります。動作確認情報は以下 URL で随時公開していく予定です。
⇒http://www.ntt-me.co.jp/mn/

その他の注意

- アクセス制限（☞ p.67）
  アクセス制限は UPnP 設定よりも常に優先的に扱われます。LAN 側インタフェースアクセス制限を行った場合、UPnP 機能は使用できなくなります。
- GapNAT 通過・NAT アドレス変換設定（☞ p.60）
  UPnP の NAT 設定情報は、GapNAT 通過・NAT アドレス変換設定よりも常に優先的に扱われます。
- NAT アドレス・ポート変換（☞ p.63）
  UPnP の NAT 設定情報は、NAT アドレス・ポート変換よりも常に優先的に扱われます。
- IP フィルタ（☞ p.69）
  IP フィルタは、UPnP の NAT 設定情報よりも常に優先的に扱われます。
- NAT テーブル消去（☞ p.93）
  NAT テーブル消去を行っても UPnP の NAT 設定情報は消去されません。UPnP の NAT 設定情報の消去には、“UPnP NAT 設定情報消去”を使用してください。ただし、実際に通信に使用されている NAT テーブルはすべて消去されるので、一時的にインターネットに対するすべての通信ができなくなります。
- 構成定義のバックアップ・リストア
  - 構成定義のバックアップを行った場合 UPnP による静的 NAT 設定情報はコメント情報として“#”が先頭についた状態で表示されます。
  - 構成定義のリストアを行った場合 UPnP による静的 NAT 設定情報はリストアできません。“#”が先頭についたままでリストアを行うと UPnP による静的 NAT 設定情報は存在しなかったものとして扱われます。“#”を取り外してリストアを行うとエラーとなります。
- 設定の初期化設定の初期化を実行した場合、UPnP による静的 NAT 情報、UPnP CP テーブルはすべて消去されます。このとき、UPnP ログのログ情報と時刻設定は消去されません。
- 本機器の電源を入/切した場合は、UPnP 静的 NAT 設定情報は保持されます。また、UPnP ログ、UPnP CP テーブルは消去されます。
- LAN 側のネットワーク構成 UPnP 機能は LAN 側と同一のネットワークアドレスからのリクエストに対してのみ有効です。本機器の LAN ポートにその他のルータ等を接続した場合は、そのルータ配下の LAN 上の PC から UPnP 機能を利用することはできません。

VPNパススルーについて

VPN パススルーについて

本機器の動作モードが NAT ルータ、GapNAT、マルチ GapNAT の場合、VPN（仮想プライベートネットワーク）パススルー機能が利用できます。
本機器は VPN パススルーとして、PPTP・IPsec・L2TP に対応しています。
ご利用されている VPN システムに応じた設定を行ってください。

◆ PPTP マルチパススルー
複数の PPTP セッションを NAT ルータでパススルーする機能です。
LAN 側で PPTP クライアントを使用する場合は、特に設定は必要ありません。
LAN 側に PPTP サーバを設置する場合は、「NAT アドレス変換設定」または「GapNAT 通過・NAT アドレス変換設定」にて、TCP ポートの 1723（PPTP）の設定が必要です。

優先度	= 1～99
接続先の名称	= [接続先 1 の名称]
LAN 側の IP アドレス	= [PPTP サーバの IP アドレス]
WAN 側の IP アドレス	= [自分の WAN 側 IP アドレス]
プロトコル	= TCP
ポート番号	= 1723-1723

◆ L2TP パススルー
1 つの L2TP セッションを NAT ルータでパススルーする機能です。
LAN 側で L2TP クライアントを使用する場合は、特に設定は必要ありません。
LAN 側に L2TP サーバを設置する場合は、「NAT アドレス変換設定」または「GapNAT 通過・NAT アドレス変換設定」にて、UDP ポートの 1701（L2TP）の設定が必要です。

優先度	= 1～99
接続先の名称	= [接続先 1 の名称]
LAN 側の IP アドレス	= [L2TP サーバの IP アドレス]
WAN 側の IP アドレス	= [自分の WAN 側 IP アドレス]
プロトコル	= UDP
ポート番号	= 1701-1701

◆ IPsec パススルー
1 つの ESP トンネルモード（AH トンネルモードはサポートしていません）のセッションを NAT ルータでパススルーする機能です。サポートするホストは 1 台だけです。
LAN 側で IPsec クライアントを使用する場合は、特に設定は必要ありません。
LAN 側に IPsec サーバを設置する場合は、「NAT アドレス変換設定」または「GapNAT 通過・NAT アドレス変換設定」にて、UDP ポートの 500（IKE）の NAT アドレス変換が必要になります。

優先度	= 1～99
接続先の名称	= [接続先 1 の名称]
LAN 側の IP アドレス	= [IPsec サーバの IP アドレス]
WAN 側の IP アドレス	= [自分の WAN 側 IP アドレス]
プロトコル	= UDP
ポート番号	= 500-500

7 その他

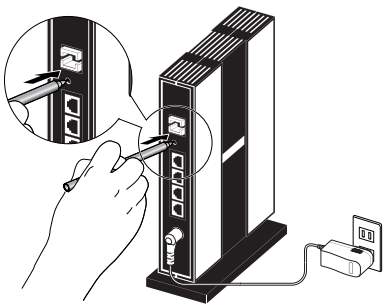
一時的に工場出荷時設定で起動する

MN8300の初期化

本機器には、本体の背面に INIT スイッチがあります。本機器のパスワード（☞ p. 31）を忘れたり、本機器へのアクセスを拒否するような設定をしてしまったときに、またはその他何らかの理由で本機器にアクセスできなくなった場合など、本機器を工場出荷時設定で一時的に起動することにより設定内容の確認や修正を行うことができます

① 本機器の電源を入れます。

② 電源が入っている状態で、本機器背面の INIT スイッチを 3〜4 秒押し続けると、一時的に工場出荷時設定で本機器が起動します。



③ PPPoE/DHCP ランプが緑色→オレンジ色→緑色と 1 秒ごとに点灯していることを確認します。

④ 本機器とパソコンを接続します。（☞ p.18）

⑤ 本機器の設定ページを表示させます。（☞ p.31）

⑥ メニューフレームより詳細設定をクリックし、内容の確認や修正等を行ってください。

⑦ 本機器を再起動します。

⑧ 選択した（確認・修正等を行った）設定内容で起動します。

注意 本機器の DHCP サーバ機能を使うときは、LAN 側のパソコンを再起動してください。

注意 本機器の設定内容を変更することなく再起動するには、WWW 画面の保守・機器再起動を使用するか、電源コンセントから AC アダプタを抜き、その後もう一度差し込みます。

注意 処理後は、必ず本機器を再起動してください。再起動を行なわないと、運用時（本処理前）の設定内容で動作しません。

注意 本処理は、あくまで一時的に工場出荷時の状態で本機器を起動するものであり、設定を初期化するためのものではありません。設定の初期化を行う場合は、「設定を初期化する」（☞ p. 89）を参照してください。

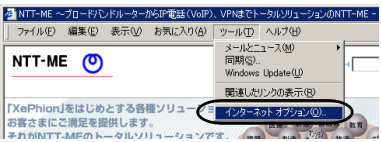
WWWブラウザの設定

プロバイダによっては、プロキシサーバを経由してインターネットに接続する場合があります。本機器の WWW 設定画面は、プロキシサーバを経由してアクセスすることはできません。次の手順に従って WWW ブラウザの設定を変更してください。

Windowsの場合

次の手順は、Internet Explorer 5.5 を使った場合です。

① WWW ブラウザを起動してください。



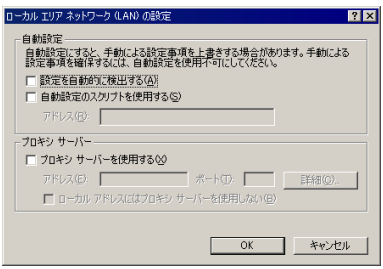
② ツール メニューから インターネットオプション を選択してください。

③ 接続タブ をクリックしてください。

④ LAN の設定 をクリックしてください。

⑤ ローカルエリアネットワーク（LAN）の設定 ダイアログボックスで、「プロキシサーバーを使用する」のチェックボックスがチェックされていないことを確認してください。

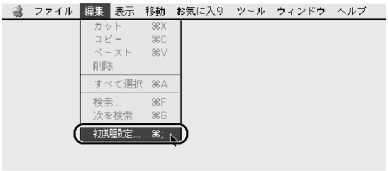
- チェックボックスがチェックされていたら、チェックを外して、 OK をクリックしてください。
- チェックボックスがチェックされていなかったら、 キャンセル をクリックし、設定を終了してください。



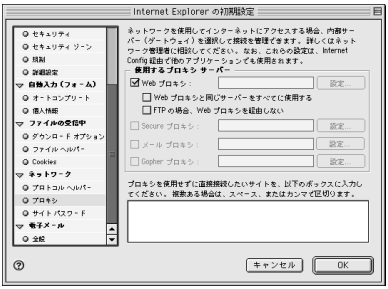
Macintoshの場合

次の手順は、Internet Explorer 5.01 を使った場合です。

① WWW ブラウザを起動してください。



② 編集 メニューから 初期設定 を選択してください。
初期設定 ダイアログボックスが表示されます。



③ リストから プロキシ を選ぶ

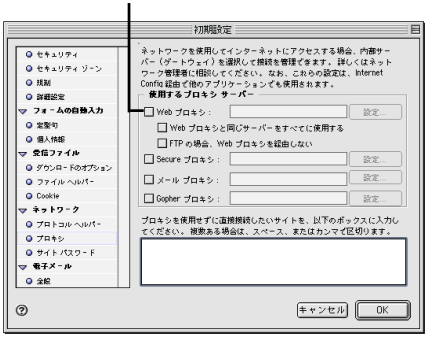
プロキシを選んでください。

④　「Web プロキシ」チェックボックスがチェックされているか確認してください。

- チェックボックスがチェックされていたら、チェックを外して OK をクリックしてください。
- チェックボックスがチェックされていなかったら、設定しないで キャンセル をクリックし、設定を終了してください。

⑤　OK をクリックしてください。

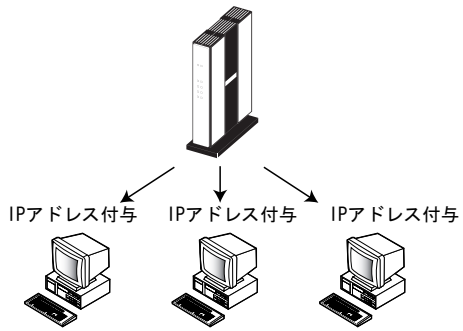
チェックボックスがチェックされていないことを確認してください。



パソコンのIPアドレスを固定するには

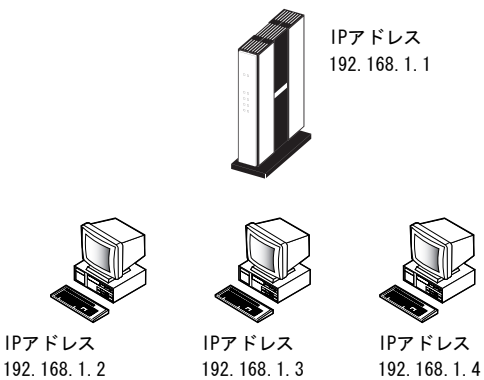
本機器を含めた TCP/IP ネットワークの全てのパソコンには、それぞれ固有の IP アドレスの設定が必要です。本機器では、DHCP サーバ機能を使って、LAN 上の各パソコンに IP アドレスを自動で割り当てることができます。（工場出荷時設定）この場合、本機器が各パソコンに IP アドレスを割り当てたり再割り当てするため、各パソコンの IP アドレスは固定していません。

◆ 本機器が IP アドレスを割り当てるネットワーク（工場出荷時設定）



これに対し、「DHCP 固定 IP アドレス配布設定」（☞ p.57）機能を利用して、最大 16 台まで特定のパソコンの MAC アドレスと割り当てる IP アドレスを設定できます。（17 台目以上は指定した IP アドレス以外の任意の IP アドレスが割り当てられます。）
17 台以上のパソコン等の IP アドレスを固定設定したい場合は、本機器の DHCP サーバ機能を無効にして、LAN 上の各パソコンの IP アドレスを固定することができます。この場合、あらかじめ各パソコンに固有の IP アドレスを設定する必要があります。

◆ IP アドレスが固定されたネットワーク（オプション設定）



各パソコンに固有の IP アドレスを設定した後に、本機器を設定します。「LAN 側 IP 設定」（☞ p.51）を参照し、DHCP サーバ機能を「使用しない」にしてください。各パソコンの設定は、次ページ以降の手順に従ってください。

Windows 95/98/Meの場合

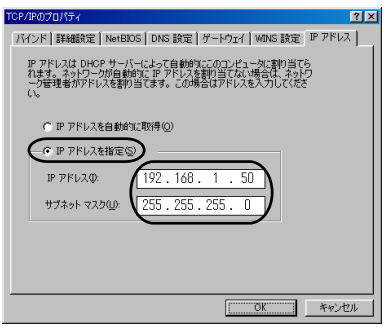
① [スタート]メニューから 設定 を選び、 コントロールパネル をクリックしてください。

② [ネットワーク]アイコンをダブルクリックしてください。
Windows Me で「ネットワーク」アイコンが見つからない場合は、「すべてのコントロールパネルのオプションを表示する」をクリックしてください。

③ ネットワーク ダイアログボックスで、本機器に接続しているネットワークカードに関連した TCP/IP を選び、 プロパティ をクリックしてください。TCP/IP のプロパティ ダイアログボックスが表示されます。

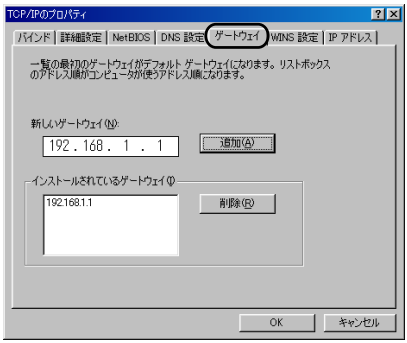
④ TCP/IP のプロパティダイアログボックスで、IP アドレスタブをクリックしてください。

⑤ 「IP アドレスを指定」を選択してください。



⑥ 各パソコンの IP アドレス（例：192.168.1.50）とサブネットマスクを入力してください。サブネットマスクは通常 255.255.255.0 と入力します。本機器の WWW 設定画面にアクセスする場合は、本機器のサブネットマスクと同じ値を入力してください。

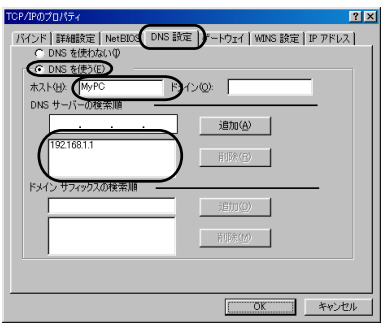
⑦ ゲートウェイタブ をクリックする右の画面が表示されます。



⑧ 192.168.1.1(本機器の工場出荷時設定 IP アドレス）を「新しいゲートウェイ」のアドレス欄に入力し、 追加 をクリックしてください。

⑨ 192.168.1.1 が「インストールされているゲートウェイ」のアドレス欄に入力されていることを確認します。
本機器の IP アドレスを変更する場合は、「インストールされているゲートウェイ」の IP アドレスも変更してください。

⑩ DNS 設定 タブをクリックしてください。

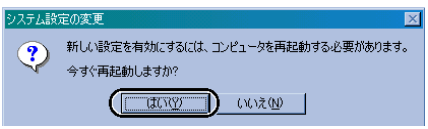


⑪ 「DNS を使う」を選択してください。

⑫ DNS サーバアドレスを「DNS サーバの検索順」のアドレス欄に入力し、 追加 をクリックしてください。

⑬ 任意のホスト名を入力し、 OK をクリックしてください。

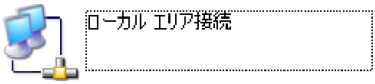
⑭ OK をクリックしてください。
システム設定の変更 ダイアログボックスが表示されます。



⑮ はい をクリックし、パソコンを再起動してください。

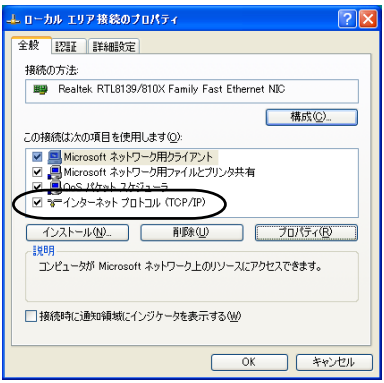
Windows XP/2000の場合

① [スタート]メニューの マイコンピュータ から マイネットワーク を選び、ネットワーク接続を表示する を選択してください。
Windows 2000 の場合は、「マイネットワーク」アイコンを右クリックし、「プロパティ」を選択してください。

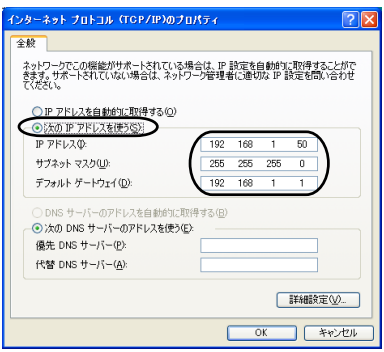


② 本機器が接続されている「ローカルエリア接続」アイコンを右クリックし、プロパティ を選択してください。

③ 「インターネットプロトコル(TCP/IP)」を選び、プロパティ をクリックしてください。



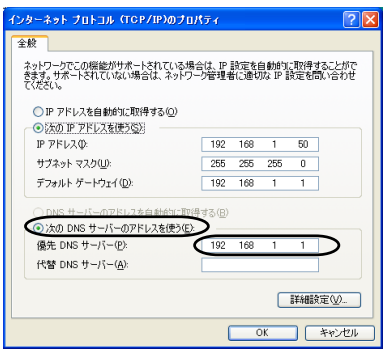
④ 「次の IP アドレスを使う」を選択してください。



⑤　各パソコンの IP アドレス
（例：192.168.1.50）とサブネットマスクを入力し、192.168.1.1（本機器の工場出荷時設定 IP アドレス）を「デフォルトゲートウェイ」の入力欄に入力してください。

サブネットマスクは通常 255.255.255.0 と入力します。本機器の WWW 設定画面にアクセスする場合は、本機器のサブネットマスクと同じ値を入力してください。

⑥　「次の DNS サーバーのアドレスを使う」をクリックしてください。



⑦　「DNSサーバー」のアドレスを入力欄に入力し、
OK をクリックしてください。

⑧　閉じる をクリックしてください。
Windows 2000 の場合は、OK をクリックしてください。

⑨　「ネットワーク接続」のウィンドウを閉じて、パソコンを再起動してください。
Windows 2000 の場合は、「ネットワークとダイヤルアップ接続」のウィンドウを閉じて、パソコンを再起動してください。

Windows NT 4.0の場合

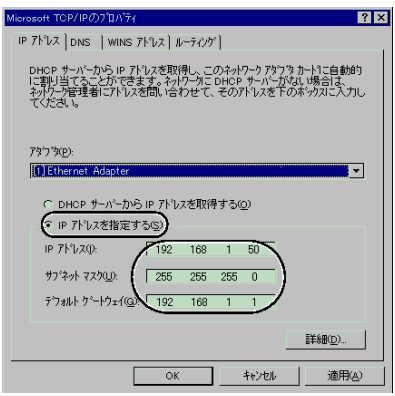
① [スタート]ボタンをクリックし、 設定 を選び、コントロールパネル をクリックしてください。

② 「ネットワーク」アイコンをダブルクリックしてください。

③ プロトコル タブをクリックし、「TCP/IP プロトコル」を選び、 プロパティ をクリックしてください。TCP/IP のプロパティダイアログボックスが表示されます。

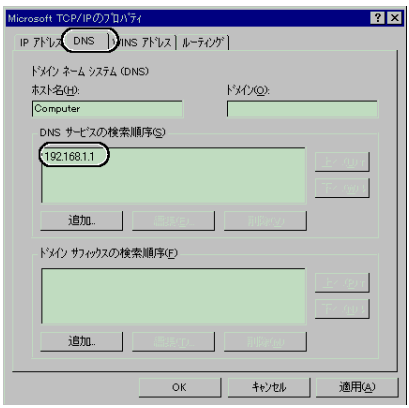
④ TCP/IP のプロパティ ダイアログボックスで、IP アドレスタブ をクリックしてください。

⑤ 「IP アドレスを指定する」を選択してください。



⑥　各パソコンの IP アドレス（例：192.168.1.50）とサブネットマスクを入力し、192.168.1.1（本機器の工場出荷時設定 IP アドレス）を「デフォルトゲートウェイ」の入力欄に入力してください。サブネットマスクは通常 255.255.255.0 と入力します。本機器の WWW 設定画面にアクセスする場合は、本機器のサブネットマスクと同じ値を入力してください。

⑦　DNS タブをクリックしてください。

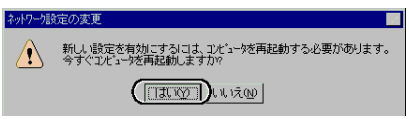


⑧　追加 をクリックし、「DNS サーバ：」入力欄に入力し、追加 をクリックしてください。

⑨　OK をクリックしてください。

⑩　ネットワークダイアログボックスで、OK をクリックしてください。 ネットワーク設定の変更 ダイアログボックスが表示されます。

⑪　はい をクリックし、パソコンを再起動してください。



Mac OS 8.1～9.2の場合

次の手順は、Mac OS 9.2 を使った場合です。Mac OS のバージョンによっては、若干操作方法が異なる場合があります。

① アップルメニューから コントロールパネル を選択してください。

② コントロールパネル メニューから TCP/IP を選択しすると、TCP/IP ダイアログボックスが表示されます。

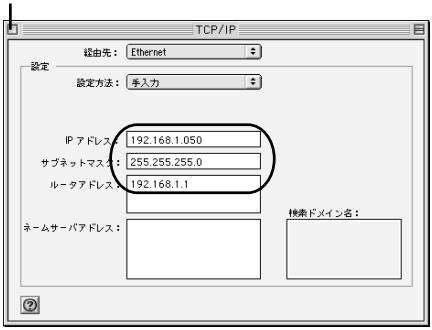
③ 経由先 ポップアップメニューから Ethernet を選択してください。

④ 設定方法 ポップアップメニューから 手入力 を選択してください。

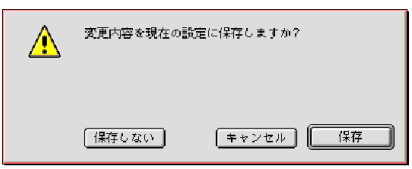
⑤ 入力欄に「IP アドレス」、「サブネットマスク」、「ルータアドレス」、「ネームサーバアドレス」を入力してください。

- サブネットマスクは通常 255.255.255.0 と入力します。本機器の WWW 設定画面にアクセスする場合は、本機器のサブネットマスクと同じ値を入力してください。
- ルータアドレスの入力欄に、192.168.1.1（本機器の工場出荷時設定 IP アドレス）を入力してください。
- 本機器の工場出荷時設定 IP アドレスを変更する場合は、各パソコンのルータアドレスも変更する必要があります。

クローズボタン



⑥ クローズボタンをクリックすると、右のダイアログボックスが表示されます。



⑦ 保存 をクリックしてください。

⑧ パソコンを再起動してください。

Mac OS X（10.1～10.2）の場合

次の手順は、Mac OS 10.1 を使った場合です。Mac OS のバージョンによっては若干操作方法が異なる場合があります。

① アップルメニューから システム環境設定... を選ぶシステム環境設定画面が表示されます。

② 「ネットワーク」アイコンをダブルクリックしてください。

③ 表示 ポップアップメニューから 内蔵 Ethernet 選択してください。

④ TCP/IP の設定 ポップアップメニューから 手入力 を選ぶ

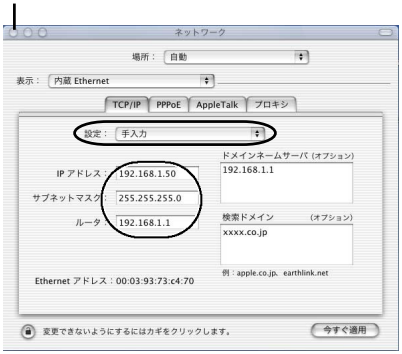
⑤ 入力欄に IP アドレス、サブネットマスク、ルータアドレス、ネームサーバアドレスを入力してください。

- ●サブネットマスクは通常 255.255.255.0 と入力します。本機器の WWW 設定画面にアクセスする場合は、本機器のサブネットマスクと同じ値を入力してください。
- ●ルータアドレスの入力欄に、192.168.1.1（本機器の工場出荷時設定 IP アドレス）を入力してください。
- ●本機器の工場出荷時設定 IP アドレスを変更する場合は、各パソコンのルータアドレスも変更する必要があります。

⑥ クローズボタンをクリックすると右のダイアログボックスが表示されます。

⑦ 保存 するをクリックしてください。

クローズボタン



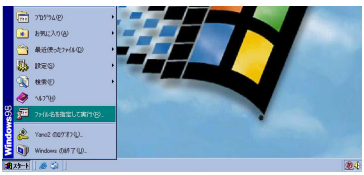
パソコンのIPアドレスやMACアドレスを確認するには

各パソコンから本機器の WWW 設定画面にアクセスできない、またはネットワーク上の他のパソコンと通信できない、などの場合には、各パソコンの IP アドレスの設定に問題がある可能性があります。以下の手順に従って IP アドレスの設定を確認してください。

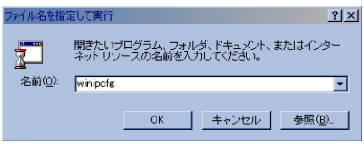
Windows 95/98/Meの場合

以下の手順は、Windows 98 の場合です。

① [スタート]メニューから、 ファイル名を指定して実行 を選択してください。

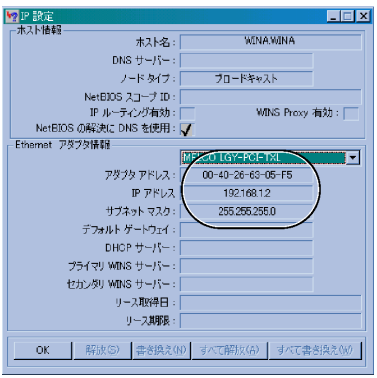


② 「名前欄」に winipcfg と入力し、OK をクリックしてください。



③ IP アドレスを確認したいイーサネットアダプタを選択してください。

④ 詳細 をクリックしてください。
IP アドレス欄 見て、設定されている IP アドレスを確認してください。アダプタアドレス欄 を見て、ネットワークカードの MAC アドレスを確認してください。



Memo 「IP アドレスを自動的に取得する」（☞ p.24）を設定していて、「169.254.XXX.X」などの値が表示された場合は、IP アドレスが正しく取得できていない可能性があります。そのような場合は、次の手順に従って IP アドレスを更新してください。

① 解放 をクリックしてください。
自動取得していた IP アドレスが解放されます。

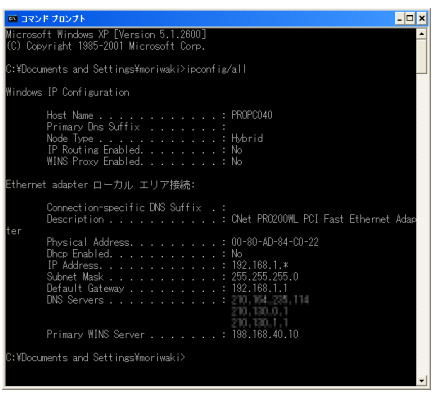
② 書き換え をクリックしてください。
新しい IP アドレスが割り当てられます。

③ OK をクリックしてください。

Windows XP/2000/NT 4.0の場合

① [スタート]メニューから すべてのプログラム 、アクセサリ 、コマンドプロンプト を選ぶ Windows 2000 の場合は、[スタート]メニューからプログラム 、 アクセサリ 、 コマンドプロンプト を選んでください。
Windows NT 4.0 の場合は、[スタート]メニューから プログラム 、 コマンドプロンプト を選んでください。

② コマンドプロンプト の後に ipconfig/all と入力してください。



- ipconfig/renew[アダプタ]について
  DHCP 構成パラメータを更新します。このオプションは DHCP クライアントのパソコンでのみ使用できます。アダプタ名を指定するには、パラメータなしで ipconfig を使ったときに表示されるアダプタ名を入力します。なお、パソコンのネットワークカードが 1 枚の場合は省略します。
- ipconfig/release[アダプタ]について
  現在の DHCP 構成を解除し、パソコンの IP アドレスを無効にします。このオプションは DHCP クライアントのパソコンでのみ使用できます。アダプタ名を指定するには、パラメータなしで ipconfig を使ったときに表示されるアダプタ名を入力します。なお、パソコンのネットワークカードが 1 枚の場合は省略します。

Memo ipconfig コマンドの説明は、コマンドプロンプトの後に ipconfig/?と入力すると表示されます。

8 困ったときには

トラブルシューティング

トラブルが発生した場合には、障害箇所を明確にしてから本章をお読みください。なお、障害箇所の特定には、以下のような手段があります。

- 本機器前面のランプの点灯状況を確認する。
- 本機器へ Ping が可能であるかを確認する。
- プロバイダのアクセスサーバやプロバイダの WWW サーバへ Ping が可能であるかを確認する。
- 著名な WWW サイトへ接続可能であるかを確認する。

現象：POWER ランプが点灯しない

原因：本機器に電源が供給されていない。

▼以下について確認してください

対処：背面の DC IN ジャックと、専用 AC アダプタのプラグがきちんと接続されていますか。

対処：AC アダプタはコンセントに正しく差し込まれていますか。

対処：コンセントに電源が供給されていますか。

対処：本機器付属の専用 AC アダプタを使用していますか。

現象：ALARM ランプが点滅する

原因：本機器の故障

▼以下について確認してください

対処：電源を入れ直しても ALARM ランプが点滅する場合は本装置の故障が考えられますので、技術サポートセンタまでお問い合わせください。なお、通常の電源投入時は ALARM ランプが一時的に点灯／消灯します。

現象：WAN ランプが点灯しない

原因：光モデム、ADSL モデムや CATV モデムとの間での信号が検出できない

▼以下について確認してください

対処：光モデムなどと、LAN ケーブルが正しく接続されていることを確認してください。

対処：光モデムなどの電源が入っていることを確認してください。

現象：PPPoE/DHCP ランプが赤色またはオレンジ色点滅を繰り返す

原因：PPP リンクが確立していない。

▼以下について確認してください

対処：PPP のユーザ ID、パスワードが適切に設定されていますか。ユーザ ID、パスワードについては、プロバイダに確認してください。

対処：プロバイダによって「PPP 認証プロトコル」を[PPP]または[CHAP]に固定しないと接続できない場合があります。「PPP 認証プロトコル」の変更は、「詳細設定」ページのメニューフレームの「接続先設定」で行うことができます。

現象：LAN ランプが点灯しない

▼以下について確認してください

対処：LAN ケーブルが正しく接続されていることを確認してください。

現象：設定内容や状態が分からない

▼以下について確認してください

対処：WWW ブラウザの設定ページで参照してください。

・現在の設定内容 ‥‥‥‥‥：各設定画面

・現在の状態 ‥‥‥‥‥‥‥‥：機器状態・ログ画面

現象：ログインパスワードを忘れた

▼以下について確認してください

対処：工場出荷時のユーザ名は"admin"、パスワードは"admin"です。変更後のパスワードを忘れてしまった場合は、「MN8300 の初期化」（☞ p.156）を参照してください。

現象：IP アドレスを忘れた

▼以下について確認してください

対処：パソコンが DHCP により IP アドレスを自動取得する設定になっている場合、本機器の IP アドレスはデフォルトゲートウェイとして登録されています。デフォルトゲートウェイの IP アドレスは、「パソコンの IP アドレスや MAC アドレスを確認するには」（☞ p.169）を参照してください。

現象：WWW にアクセスできない

▼以下について確認してください

対処：正面の LAN ランプが点灯していますか。

対処：パソコンに適切な IP アドレスが設定されていますか。Windows の場合は、「パソコンの IP アドレスや MAC アドレスを確認するには」（☞ p.169）を参照してください。

対処：本機器の LAN 側に適切な IP アドレスが設定されていますか。

対処：お使いの WWW ブラウザの Proxy 設定は"no proxy"になっていますか。

対処：お使いの WWW ブラウザは JavaScript を使用する設定になっていますか。他、「WWW ブラウザの設定」（☞ p.157）を参照してください。

現象：インターネットにアクセスできない

▼以下について確認してください

対処：正面の LAN ランプは点灯していますか。

対処：PPP を使用している場合は、PPPoE/DHCP ランプが緑色に点灯していますか。

対処：パソコンに適切な IP アドレスが設定されていますか。

対処：本機器と WWW ブラウザ等による通信が可能ですか。

対処：本機器の WWW ブラウザ設定メニューを参照できますか。

対処：本機器の「機器状態情報」において WAN 回線状態が「通信中」となっていますか。または、PPP 状態が「確立」となっていますか。

対処：PPP を使用している場合、本機器に適切な IP アドレスが割り当てられていますか。

対処：以下の設定内容を変更した場合は再度その内容を確認してください。

＊IP スタティックルート設定
＊IP フィルタ（IP ルータ／NAT ルータ）設定
＊NAT 設定（NAT ルータ）
＊アクセス制限（IP ルータ／NAT ルータ／ブリッジ）

対処：設定後、「設定変更後の機器の再起動」が表示されたあとで再起動を行ないましたか。

対処：DNS サーバアドレスを設定していないときは、設定してください。DNS サーバアドレスがわからないときは、プロバイダへお問い合わせください。

対処：設定を変更した場合は、PPP 接続を一旦切断してから PPP 接続し直さないと正常に通信できないことがあります。

対処：ルーティングテーブルにおいて経路情報が適切に設定されていますか（問題があればルーティングテーブルを修正してください）。

対処：トラブルシューティングの他の項目に該当する現象が起きていませんか。

対処：本機器を再起動してください。

対処：パソコンを再起動してください。

対処：本機器をルータとして利用する場合は、「フレッツ接続ツール」や「フレッツマネージャ」、Windows XP の「広帯域ツール」を利用しなくても PPP 接続が可能です。「フレッツ接続ツール」、「フレッツマネージャ」、Windows XP の「広帯域ツール」を利用する場合は、PPPoE 機能を利用する必要があります。PPPoE 機能を利用するには、「LAN 側 IP 設定」(☞ p.51)を参照してください。

お問い合わせ先

■メンテナンスサービスについて

本機器に含まれるソフトウェアが保存されている媒体に不具合があった場合、お買い上げの販売代理店または小売店に返却してください。無償にて新品と交換いたします。なお、不具合品送付にともなう送料は、送り主負担とさせていただきます。

本機器に含まれるハードウェアが購入後 1 年間に通常のご使用において故障した場合、これを保証します。故障品に保証書を添えて、お買い上げの販売代理店または小売店に返却してください。無償にて修理いたします。なお、修理品送付にともなう送料は、送り主負担とさせていただきます。

保証期間でも次のような場合には、有償修理になります。

（1）保証書のご提示がない場合

（2）保証書に機器の製造番号、ご購入日、販売店名の記入がない場合、または字句を書き替えられた場合

（3）接続しているほかの機器に起因して生じた故障、または不当な修理や改造、調整をされた場合

（4）使用上の誤り、または故意・他意に関わらず、ほかの要因による損傷および故障の場合

（5）火災、地震、風水害、落雷、そのほかの天災地変、公害や異常電圧による損傷および故障の場合

（6）購入後の輸送、移動時の落下など、お取り扱いが不適当なため生じた損傷および故障の場合

（7）購入後の取り付け場所の移動、落下などにより生じた損傷および故障の場合

■お問い合わせ先

本機器について技術的なご質問、または製品のアップグレードに関するご質問は、お買い上げの販売代理店、小売店、または技術サポートセンターまでお問い合わせください。

技術サポートセンター

TEL:0570-055-128（NTT 一般電話・携帯電話用）

TEL:03-5675-7956（PHS 及び NTT 以外の電話）

FAX:0570-056-128

9:40～12:00、13:00～18:00(土・日・休日・年末年始は除く）

※通話料はお客様負担となります。
※ナビダイヤル(0570 で始まる電話番号)も通話料のみでご利用いただけます。
※サポートセンタのアナウンスが聞こえた時点から通話料がかかります。
※電話が混雑しているときは、アナウンスが流れた後電話が切れることがあります。
このような場合は、時間をおいて再度お掛け直しください。
※電子メールによるお問い合わせは受け付けておりません。ご了承ください。

■ホームページのご案内

株式会社エヌ・ティ・ティ エムイーのホームページで、製品のサポート情報、最新のファームウェアなどを提供していますので、ご活用ください。

MN8300 ホームページ

株式会社エヌ・ティ・ティ エムイー「MN Information」http://www.ntt-me.co.jp/mn/

MN8300 お問い合わせ用紙

トラブルなどが発生した場合は、このページをコピーして必要事項をご記入の上、175 ページの技術サポートセンターまでFAX してください。
※電子メールによるお問い合わせは受け付けておりません。ご了承ください。

ふりがな 氏名	電話番号 FAX番号
連絡先 〒	
製品お買い上げ日　　年　　月　　日	ファームウェアバージョン　Ver.
製造番号（※本体裏面に記載されています。）	
(1) ご契約のサービスは何ですか。	
[　ADSL・CATV・光ケーブル　]	
(2) トラブルが発生したのはどのポートですか。	
[　LAN ポート関連・WANポート関連・その他（　　）]	
(3) 本機器に接続してご使用のパソコンについて教えてください。	
使用台数 [　　台]	
メーカ名　[　　]	
機種名　[　　]	
ＯＳ　[　DOS・Windows（ 95 / 98 / Me / NT / 2000 / XP ）・ Mac OS（　　）　）	
(4) 通信をおこなっている場合、接続相手先について教えてください。	
接続先 [　プロバイダ　（名称：　　）　・　その他（　　）]	
事業者 [NTT東日本・西日本(Bフレッツ、フレッツ・ADSL)／その他（　　）]	
(5) 発生している症状を詳しく教えてください。	

※エラーが出ている場合はエラー番号、メッセージも記入してください。

製品仕様

■ハードウェア仕様

項目			仕様
CPU			インテル® IXP422 ネットワーク・プロセッサ
メモリ			Flash ROM 4MB／SDRAM 16MB
WAN側インタフェース			
	ポート数		1ポート
	コネクタ形状		8ピンモジュラージャック（RJ-45）
	物理インタフェース		IEEE802.3（10BASE-T）/ IEEE802.3u(100BASE-TX)
	通信速度		10/100Mbps（自動判別）
	全二重/半二重		全二重/半二重（自動判別）
	MDI/MDI-X（ストレート/クロスケーブル）		自動判別
LAN側インタフェース			
	ポート数		4ポート
	コネクタ形状		8ピンモジュラージャック（RJ-45）
	物理インタフェース		IEEE802.3(10BASE-T) / IEEE802.3u(100BASE-TX)
	通信速度		10/100Mbps（自動判別）
	全二重/半二重		全二重/半二重（自動判別）
	MDI/MDI-X（ストレート/クロスケーブル）		自動判別
ユーザインタフェース			
	INITスイッチ（一時初期化用）		押しボタンスイッチ
	状態表示ランプ		
		POWER（グリーン）	通電時点灯
		ALARM（レッド）	機器障害発生時点滅
		WAN（グリーン）	WAN側Ethernetリンク状態表示
		PPPoE/DHCP(グリーン/オレンジ/レッド)	PPPoE/DHCPコネクション状態表示
		LAN1～LAN3（グリーン）	LAN1～3Ethernetリンク状態表示
		LAN4/DMZ（グリーン/オレンジ）	LAN4 Ethernetリンク状態表示 / DMZ設定状態
		MAIL（グリーン）	新着メール着信通知
		STATUS（グリーン）	機器状態表示（将来対応）
その他			
	動作環境	動作温度	5℃～40℃
		動作湿度	5%～85%（ただし、結露しないこと）
		電源電圧	DC12V/1A（専用ACアダプタ使用）
		消費電力	12W以下
	外形寸法	本体のみ	約32(W) × 126(D) × 170(H) [mm]
		縦置き台使用時	約52(W) × 126(D) × 187(H) [mm]
	重量	本体のみ	約360g
		縦置き台	約270g
	電波障害防止		VCCIクラスB
	付属品		専用ACアダプタ、カテゴリ 5UTPケーブル 2.0m、 縦置きスタンド、マニュアル、 インターネット接続ガイド、保証書

用語集

A～Z

10BASE-T
: ネットワーク規格の一種で、電話線コードで使われている“より対線”（Twist Pair Cable）を、ハブにたこ足状に配線してネットワークを構築します。10BASE-T の 10 はデータの伝送速度で 10Mbps で伝送できることを示します。

100BASE-TX
: 100BASE-TX は、伝送速度が 10BASE-T の 10 倍の 100Mbps を実現する規格で、LAN ケーブルにはカテゴリ 5 ケーブルを利用します。コネクタ形状は 10BASE-T と同様 RJ-45 を使用します。

ARP（Address Resolution Protocol）
: ネットワークアドレスをもとに物理アドレスを得るためのプロトコルで、主に IP アドレスから Ethernet アドレス（MAC アドレス）を得るのに使用されます。TCP/IP を実装する機器のほとんどに実装されています。

ARP テーブル
: ARP により得られた IP アドレスと MAC アドレスの対応表を表します。

CATV
: Cable Television の略で、ケーブルテレビのことを示します。最近では、このケーブルテレビの回線を使ってインターネットに接続するサービスを提供する会社が増えてきています。

CHAP（Challenge Handshake Authentication Protocol）
: PPP（Point-to-Point Protocol）接続時に、ユーザ名とパスワードで認証を行う仕組み。RFC1994 で規定されています。プロバイダのアクセスサーバからの要求で認証を行います。PAP（Password Authentication Protocol）と違い、パスワードを暗号化してネットワーク上に送信するため、安全性が高くなります。

DHCP(Dynamic Host Configuration Protocol)
: 各パソコンがネットワークを利用するのに必要な情報をサーバから自動的に取得するプロトコルです。DHCP サーバは、IP ネットワークに関連した情報（IP アドレスの割り当て範囲やデフォルトゲートウェイなど）を保持しており、DHCP クライアントからの要求で、それらの情報を割り当てます。

DHCP サーバ（Dynamic Host Configuration Protocol）
: LAN 内の通信機器の IP アドレスなどのネットワーク設定を自動的に割り当てる機能を持つサーバです。DNS サーバ（Domain Name Service/System）TCP/IP ホスト名から IP アドレス、または IP アドレスから TCP/IP ホスト名を検索するのに用いられるサーバです。

DMZ
: DMZ(De-Militarized Zone)は、一般的にサーバなどを公開するセグメントと一般セグメントを隔離することを意味します。

DNS(Domain Name System)
: ネットワーク環境で使用される IP アドレスは、覚えにくく実用的ではありません。その解決法としてパソコンにわかりやすい名前（ドメイン名）をつけ、IP アドレスに変換して通信が行われます。ドメイン名の例として、“ntt-me.co.jp”などがあります。

DNS サーバ（ドメインネームサーバ、ネームサーバ）
: TCP/IP ホスト名から IP アドレス、または IP アドレスから TCP/IP ホスト名を検索するのに用いられるサーバです。

Ethernet
: Xerox 社などによって開発された LAN 通信方式です。

GapNAT（Global Address Proxy with NAT）

プロバイダから割り当てられたグローバル IP アドレスを、特定のパソコンに割り当てることができる機能です。これにより、従来の NAT ルータによる制限から開放することが可能です。また、グローバル IP アドレスを割り当てられた GapNAT 端末と、プライベート IP アドレスを割り当てられたその他のパソコンが同一 LAN 上で混在する環境を実現します。

IP アドレス

インターネット上のすべてのネットワークインタフェースは、IP アドレスによって識別されます。そのため TCP/IP を使用して通信をおこなうネットワークインタフェースには、固有の IP アドレスが必要です。

IP フィルタ機能

IP アドレスやポート番号などに基づき通信を制限する機能です。簡易ファイアウォールとして使用することも可能です。

IP ホスト

ネットワーク上に置かれている IP 通信装置で、通常はユーザ装置を指します。

IP マスカレード

NAT による IP アドレスの変換だけでなく TCP/UDP のポート番号も変換する機能です。これにより 1 つのグローバル IP アドレスを利用して複数のパソコンが外部と通信することが可能です。

IP ルータ

IP アドレスをもとに転送先を判断し、転送を行うネットワーク機器です。プロバイダと LAN 型接続を行っているときに使用します。一般的には LAN 側にグローバル IP アドレスの割り当てを行い、インターネットと直接通信を行う際に使用します。

LAN（Local Area Network）

会社、組織、学校、工場、ビル、フロア等、ある限定された範囲に敷設されたコンピュータ通信のためのネットワークです。距離、伝送路、トポロジ、プロトコルの明確な定義はないが、一般的には伝送距離が数 m～数十 Km、伝送速度は 1M～数 G ビット／秒程度です。ケーブルや無線等の伝送媒体を複数のコンピュータで共用し、互いに独立した通信を実行できます。

MAC アドレス(Media Access Control)

ネットワークカードに固有の物理アドレスのコードです。ネットワークカードごとに固有のコードが割り当てられています。

MacTCP®

Macintosh で使用される TCP/IP ユーティリティで、設定はコントロールパネルでおこないます。

MTU（Maximum Transfer Unit）

ネットワークを通じて転送可能な最大データ量です。MTU は、ネットワークの種類によって異なります。

NAT（Network Address Translation）

RFC1631 で規定するアドレス変換の方式です。ルータに NAT を搭載することでプライベート IP アドレスとグローバル IP アドレスを変換します。本機器では、さらにポート番号を変換する機能を持つためプロバイダの IP 接続サービスで割り当てられた 1 個の IP アドレスを、LAN 上にある複数台のパソコンで共有できるようになります。この際、IP アドレスとポート番号をもとにした変換テーブルがルータ内に作成され、これを NAT テーブルと呼びます。

NAT ルータ

NAT を使用してプロバイダに接続するルータです。ルータに接続されている複数の端末から送出されるデータは、すべてルータ自身が送出したものとしてインターネットへ送出され、その際の IP アドレスはルータ自身のアドレスが送出元アドレスとなります。インターネットからルータ宛てに受け取ったデータは、本来の行き先端末のアドレスをつけて LAN 内に送出されます。十分なグローバル IP アドレスの割り当てを受けていない場合に多く使用されます。

PAP（Password Authentication Protocol）

PPP（Point-to-Point Protocol）接続時に、ユーザ名とパスワードで認証する仕組みです。RFC1334 で規定する。プロバイダのアクセスサーバが PAP でユーザに認証を要求する。パスワードが暗号化されずに送信されるため、安全性が低いとされています。

Ping

TCP/IP ネットワークにおいて、IP パケットが通信先まで届いているかを調べるために利用される最も基本的なコマンドです。Ping を実行してみて返答があれば途中経路に問題はなく、相手のノードは存在し IP パケットの処理が可能であることが分かります。

POP、POP3（Post Office Protocol version3）

メールクライアントがメールサーバ上に着信したメールをクライアント側に転送する際に用いるプロトコルです。RFC1939 で規定されています。なお、メール送信時には SMTP（SimpleMail Transfer Protocol）を利用します。

PPP（Point-to-Point Protocol）

シリアルラインを使って通信するための物理層／データリンク層プロトコルです。TCP/IP や IPX、その他複数のプロトコルを同じにサポートできます。また、リンク状態（使用しているモデムや回線の状態）に応じた再接続、両端で使用する IP アドレスの自動的なネゴシエーション、認証機能などを持ちます。
公衆回線などを経由して 2 台のパソコンを接続するために開発されたプロトコルです。イーサネット上でユーザ名、パスワードでの認証機能や圧縮機能をサポートするだけでなく、複数のプロトコルを同時にサポートできます。

PPPoE（PPP over Ethernet）

本機器本体ではなく、Ethernet 上に接続したパソコンなどから PPP 接続を行う方式です。Ethernet 上に PPP のフレーム（パケット）を直接のせ、WAN 回線を通じて PPP のアクセスサーバにアクセスします。この場合、本機器は Ethernet のブリッジとして動作します。利点として以下の 3 点が挙げらます。

・本機器での複雑な IP 設定が不要です

・各パソコンから直接インターネットのアクセスサーバに接続するため、NAT 使用時に動作しない電子会議や対戦ゲームなどのアプリケーションを利用できます

・これまでのダイヤルアップ接続と同様に PPP によって認証や課金を行うことができます

PPPoE マルチセッション機能

フレッツ・ADSL、B フレッツなどの複数の PPPoE セッションを利用する際に、複数のプロバイダへ同時接続したり、フレッツ・スクウェアなどのインフォメーションサイトとプロバイダへ同時接続することができます。

PPTP(Point to Point Tunneling Protocol)

インターネット上で VPN を実現するためのプロトコルの 1 つです。PPTP では PPP をベースに、データの暗号化や認証、リンクの確立などの機能を持たせています。現在は Windows XP などに実装されています。

RIP（Routing Information Protocol）

IP ネットワークの経路情報を交換するためのプロトコルで、他のルータとネットワークの経路情報（ルーティングテーブル）をやり取りするのに使用します。

TCP/IP（Transmission Control Protocol/Internet Protocol）

米国防総省の資金援助によるネットワークプロジェクトで開発されたネットワークプロトコルです。インターネットの標準プロトコルであり、現在最も普及しているプロトコルです。ネットワーク層プロトコルは IP で、トランスポート層プロトコルは TCP（Transmission Control Protocol）と UDP（User Data gram）の 2 つです。FTP、SMTP などのアプリケーションは、TCP/IP が利用されています。

UPnP(Universal Plug and Play)

UPnP は、TCP/IP ベースでネットワークデバイスの自動検出や情報交換などをおこなう技術です。UPnP に対応するアプリケーションには、MSN Messenger Ver. 5.0/6.1 以降、Windows Messenger Ver. 4.7 以降などがあります。UPnP Forum によって仕様が策定されています。

URL(Uniform Resource Locator)

インターネット上のリソースを指定する方式です。具体例としては、インターネット上の WWW サイトにアクセスする際に使用する「http://www.ntt-me.co.jp/」のことです。

VPN(Virtual Private Network)

インターネットでデータ通信を行うと、通常はデータの暗号化やユーザ認証などは行われていないため、内容が第三者に盗聴されたり改ざんされたりする恐れがあります。そこで、インターネットにデータを送信する前にデータを暗号化して送信すれば、セキュリティを確保することができます。この暗号化をユーザから透過的におこない、かつユーザ認証によってある特定のユーザだけしかアクセスできないようにすれば、公衆回線網を使っても、専用線接続と同じようなセキュリティを保つことができます。これを VPN（私設仮想回線）といいます。

WAN（Wide Area Network）

建物や敷地を越える遠隔地の間を接続するためのネットワークです。広域網とも呼ばれます。LAN の対比語として多く用いられます。

Web ブラウザ

WWW サーバにアクセスするためのクライアント・プログラムです。Microsoft 社の Internet Explorer や Netscape Communications 社の Netscape Navigator などがあります。

WWW サーバ（World Wide WWW）

画像、動画、音声などをハイパーテキスト形式で蓄積し、情報を提供するファイルサーバです。ハイパーテキスト型情報では、情報内のテキスト文字列（ワード）が別の情報であるテキストやファイル、画像、動画、音声などにリンクしているので、それぞれのワードをマウスでクリックすると、より詳しい情報を抽出することができます。

WWW ブラウザ(World Wide Web)→Web ブラウザ

あ

アクセスルータ

インターネットへアクセスするためのルータです。

インターネット

地球規模でマルチメディア通信ができるネットワークです。インターネットサービスプロバイダがインターネットへの接続サービスをおこなっています。

か

カスケード接続

ハブ同士を接続することです。カスケード接続を行う場合、10BASE-T では 4 段、100BASE-TX では 2 段までという段数制限があるが、スイッチングハブには段数制限はありません。

グローバル IP アドレス

グローバルアドレスとも呼ばれます。NIC（Network Information Center）などの公的機関が割り当てる、インターネット接続時に必要となる IP アドレスの別名です。閉じたネットワーク内部に限り自由に利用できるプライベート IP アドレスが登場したため、反意語としてグローバル IP アドレスと呼ばれるようにりました。

ゲートウェイ

ゲートウェイは、ルーティング情報を交換しネットワークを管理しているコンピュータ（ルータなど）でネットワークの IP パケットの道先案内をします。ローカルネットワーク以外への通信は、デフォルトゲートウェイを介して行われます。

ゲートウェイアドレス

ネットワークにおいて、同一 LAN 上に存在しないノード（物理的、論理的を問わず）や別のネットワークに対するデータ通信を行う場合、ゲートウェイと呼ばれるノード(通常はルータ)へデータを転送します。しかし、どのゲートウェイに送ってよいかが分からない場合はデフォルトゲートウェイという一番代表的なノードへ送ることになる。通常、各ノードにデフォルトゲートウェイだけを設定しておけば、あとはそのデフォルトゲートウェイが適宜ルーティングを行います。

さ

サブネットマスク（Subnet Mask）

IP アドレスからサブネットのネットワークアドレスを求める場合に使用するマスク値のことです。IP アドレスとサブネットマスクの AND をとった結果がサブネットマスクとなります。サブネットマスクは、通常は上位の側から連続してビットを立てた値を用い、たとえば 255.255.255.0 などとしてこれをサブネット長が 24 と表現します。

スイッチングハブ

端末から送られてきたデータを MAC アドレスをベースに解析し、送り先の端末だけにデータを届ける機能を有するハブの 1 つです。

スーパネット

IP アドレスのクラス A マスク長（8 ビット）、クラス B マスク長（16 ビット）、クラス C マスク長（24 ビット）よりも少ないマスク長を設定することをいいます。

スタティックルート

IP ネットワークの経路をあらかじめ手動で決定したものです。

ステートフル・パケット・インスペクション

送出パケットの情報から戻りパケットを予測して、パケットの通過や破棄を決定する動的なパケットフィルタリング方式です。

た

ダウンロード

遠隔地にある装置側からネットワークを使用し、データを自分側に持ってきて保存する作業をいいます。

ドメイン

インターネットやイントラネットのネットワークで、サーバを中心としたネットワークを構成するまとまりを表します。

な

認証プロトコル

PPP プロトコルで認証を行うために用いるプロトコルで PAP、CHAP があります。

ネットマスク

IP アドレスは、ネットワーク ID とホスト ID によって構成されています。ネットワーク ID とホスト ID とを区別するために、ネットマスクがネットワーク ID の長さを判定します。

は

ハブ（HUB）

10BASE-T/100BASE-TX などのケーブルを集配するネットワーク接続機器で、複数の端末を接続する場合に使用します。

パスワード

ファイルやネットワークを利用する際に鍵の役目をする合言葉(文字や数字)です。ネットワークのセキュリティ上、ユーザ識別のためにあらかじめ言葉を登録します。登録されている言葉と一致しない場合は、ファイルやネットワークを利用することができません。

フィルタリング(パケットフィルタリング)

ファイアウォールの一種で、フィルタ機能を用いて、パケットを選択的に IP フォワードする方式のことです。適切に設定すると、不要なパケットが外部に転送されるのを防ぎます。

ファイアウォール

インターネットを利用する際のセキュリティのひとつです。WAN 側から LAN 側への不法な侵入を防ぐ目的で、インターネットとやり取りできるパソコンを制限したり、LAN 側から利用できるインターネットサービスを制限したりします。

ファームウェア

工場出荷時に ROM などにより機器に搭載されているソフトウェアです。本機器ではフラッシュメモリに搭載されており、バージョンアップ時などにはユーザ側で書き替えることができます。

プライベート IP アドレス（Private IP Address）

RFC1597 で規定されており、プライベートアドレスとも呼ばれます。組織内部だけのクローズな環境では、その組織だけで通用する IP アドレスを利用し、インターネットにアクセスする場合だけ本来のユニークなアドレス（グローバルアドレス）を割り当てる方法が一般化しています。プライベートアドレス空間からグローバルアドレス空間（Internet）をアクセスできるようにする仕組みとしては、Proxy や NAT（Network Address Translator）が利用されます。インターネット上へプライベート IP アドレスを持ったパケットを送出することは禁止されています。10.0.0.0～10.225.225.255、172.16.0.0～172.31.255.255、192.168.0.0～192.168.255.255 がプライベートアドレスとして規定されています。

ブリッジ

TCP/IP などのプロトコルに依存しないで中継することができます。通信端末の MAC アドレスを学習し、不要なトラフィックを自動的にフィルタで廃棄します。

プライベート IP アドレスとサブネットマスクの設定値について

インターネットでは使われないネットワーク ID を「プライベート IP アドレス」と呼び、下の表のようにクラス A, クラス B, クラス C の 3 段階に分かれています。LAN の規模に応じてクラスを選び（例えば、20 台くらいまでのパソコンが接続されたネットワークであればクラス C を選ぶ）、そのクラスの IP アドレスの範囲の中で IP アドレスを設定してください。

クラス	サブネットマスク	プライベートIPアドレス （この範囲のアドレスは組織内で自由に設定できる）
クラスA	255.0.0.0	10.0.0.1～10.255.255.254
クラスB	255.255.0.0	172.16.01～172.31.255.254
クラスC	255.255.255.0	192.168.0.1～192.168.255.254

プロキシサーバ

プロキシサーバは、コンピュータとインターネット間のセキュリティを強化したり、キャッシングによって不必要なトラフィックを減らすことで、ネットワーク間のパフォーマンスを向上させるために使用されるサーバです。

ポート番号

TCP/IP、UDP/IP の機能のひとつです。同一サーバやパソコン上で複数のユーザが、または複数のアプリケーションに対して同時にアクセスできる仕組みです。サーバやパソコンは、受信したパケットを受け渡すべき各種インターネットアプリケーションをポート番号によって特定します。たとえば、WWW サーバと FTP サーバを 1 台のサーバ上に構築しても、パケットを受け取った後にポート番号で WWW サーバ宛てなのか FTP サーバ宛てなのかを判断できます。主なアプリケーション用のポート番号は IANA（Internet Assigned Numbers Authority）によって管理され、well-known ポートと呼ばれます。

ポート名

ポート番号につけられた名前です。通常該当するプロトコル名がつけられます。パソコン等の場合、Services ファイルにポート番号とポート名の対応が記載されています。

ホップ数（Hop count）

IP パケットが通過するルータの台数です。メトリックとも呼ばれます。

ら

リンクアップ

リンクとはノード間をつなぐ部分を指し、ノード同士が通信可能な状態になることをリンクアップといいます。

ルータ

IP アドレスにより通信先までの最適な伝送路を探し出してデータの再生中継を行う機器です。LAN を流れるデータのうち、インターネットへ中継すべきデータを判断してデータを転送します。また、インターネットから来たデータの送出先を判断して各端末へ転送します。本機器には、IP ルータと NAT ルータの 2 つのモードがあります。

ルーティングテーブル

ルーティングを行うためにルータが蓄積している経路情報です。あるネットワークに到達するには、隣接したどのルータにパケットを転送するべきかが記載されています。

NTT-ME

技術サポートセンター　TEL:0570-055-128（NTT 一般電話・携帯電話用）
TEL:03-5675-7956（PHS 及び NTT 以外の電話用）
FAX:0570-056-128

株式会社 エヌ・ティ・ティ エムイー
URL http://www.ntt-me.co.jp/

発行日：2004 年 2 月