高速ＶＰＮアクセスルータ
MR504DV

取扱説明書

詳細設定編

OMRON

1. はじめに

このたびは、オムロン高速VPNアクセスルータMR504DVをお買い上げいただき、ありがとうございます。
本製品は、さまざまな機能を備え、ブロードバンド回線を十分に活用していただくための多機能高速VPNアクセスルータです。
本取扱説明書は、本製品を高度な設定でご利用になる場合に参照してください。

■本取扱説明書の内容について
本取扱説明書では、ブラウザを使った場合の設定画面の説明を、メニュー順に説明しています。

- クイック設定
  ルータ設定画面のクイック設定から操作できる設定画面の説明をします。
  - 『6-1.ブロードバンドで接続』(P.25)
    PPPoEおよびIPアドレスの設定方法について説明します。
  - 『6-2.管理コマンド・設定』(P.41)
    本製品の再起動、設定の消去、ユーザ・パスワードの変更、アクセス制御、ファームウェア更新、および設定メンテナンスの操作方法について説明します。
  - 『6-3.切断／接続状況』(P.51)
    PPTPおよびPPPoEの切断や接続状況の表示について説明します。
  - 『6-4.情報表示』(P.55)
    設定やIP経路、ログ、WAN状況、UPnP状況、IPSec状況、IPv6アドレス、IPv6経路、SNMP情報など本製品の情報表示の仕方について説明します。
  - 『6-5.その他』(P.62)
    オンラインヘルプの表示方法について説明します。
- 詳細設定
  ルータ設定画面の詳細設定から操作できる設定画面の説明をします。
  - 『7-1.接続／相手先登録』(P.66)
    PPPoEおよびPPTPの相手先を、詳しい設定を指定して登録する方法について説明します。
  - 『7-2.本体設定』(P.74)
    本体の名称や時刻など、システムに関する設定方法について説明します
  - 『7-3.ルータ設定』(P.76)
    WAN設定や、LAN設定の設定方法について説明します。
  - 『7-4.セキュリティ設定』(P.84)
    ファイアウォール設定、ログ通知設定、セキュリティオプション(VPNパススルー、ステルスモード、SPI設定)、インターネットアクセス制御、アプリケーション設定、MACアドレスフィルタ設定、および証明書の設定について説明します。
  - 『7-5.VPN(IPSec)設定』(P.107)
    VPNポリシーの設定について説明します。
  - 『7-6.IPv6設定』(P.124)
    IPv6の設定および表示について説明します。
  - 『7-7.NAT設定』(P.131)
    NATを使用したアドレスマッピングの設定について説明します。
  - 『7-8.UPnP設定』(P.134)
    UPnP設定について説明します。
  - 『7-9.ダイナミックDNS設定』(P.135)
    DDNS設定について説明します。
  - 『7-10.SNMP設定』(P.136)
    SNMP設定について説明します。
  - 『7-11.管理コマンド・設定』(P.139)
    本製品の再起動、設定の消去、ユーザ・パスワードの変更、アクセス制御、ファームウェア更新、および設定メンテナンスの操作方法について説明します。

- 『7-12.切断／接続状況』(P.143)
  PPTPおよびPPPoEの切断や接続状況の表示について説明します。
- 『7-13.情報表示』(P.144)
  設定やIP経路、ログ、WAN状況、UPnP状況、IPSec状況、IPv6アドレス、IPv6経路、SNMP情報など本製品の情報表示の仕方について説明します。
- 『7-14.その他』(P.148)
  オンラインヘルプの表示方法について説明します。

取扱説明書について

(1)本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。

(2)本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。

(3)本取扱説明書の内容については、万全を期して作成いたしましたが、万一ご不審な点やご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点がございましたら、当社までご連絡ください。

(4)本取扱説明書内で指示されている内容には、必ず従ってください。

(5)本取扱説明書の瑕疵(誤記等)により発生した障害、損害についての保証の範囲は、本製品の修理、交換、または同等機能の製品との代替交換に限ります。

2. この取扱説明書について

表記について

- **Windows 98SEは、“Windows 98”として表記します。**
  本取扱説明書では、Windows 98とWindows 98SE（Second Edition）は、ともに“Windows 98”と表記しています。
- **メニュー名、画面名、アイコン名、ボタン名、タブ名、項目名：[ ]で囲んで表記します。**
  （例）[OK]をクリックしてください。
- **参照する章のタイトル：『』で囲んで表記します。**
  （例）『設置・配線する』を参照してください。
- **メニューの選択：[メインメニュー名]－[サブメニュー名]と表記します。**
  （例）[スタート]－[コントロールパネル]をクリックしてください。
- **パソコンのキーボードのキーは＜ ＞で囲んで表記します。**
  <Enter>キーを押します。
- **操作方法の補足説明として次のようなイラストを使用しています。**


大切

このイラストがついている文章では、ハードウェアやソフトウェアへの損害を防止するために、守っていただきたいことを記載しています。

補足

このイラストがついてる文章では、設定、操作時に役立つ一般情報や補足情報を記載しています。

- **各画面の操作方法の説明に、次のような表記を使用しています。**

① … **表示されている画面での操作の順番を示します。**
②
・
・
・
①→②→③とお進みください。

クリック … **マウスの左側を1回押してください。**

ダブルクリック … **マウスの左側を2回押してください。**

右クリック … **マウスの右側を1回押してください。**

選択 … 複数ある項目の中から該当する項目を選択します。選択するには、マウスの左側を1回押してください。

確認 … 表示内容が本文のとおり正しく表示されているか確認してください。

入力 … 本文のとおり、キーボードより文字または英数字を入力してください。

チェックいれる
チェックしない … マウスの左側を 1 回押すことでチェックをいれる／しないが指定できます。

☑、◉ … チェックいれる、の状態

☐、○ … チェックしない、の状態

画面表示について

表示画面は、操作説明の一例として掲載しているものです。お客様のパソコン画面に表示される画面とは異なる場合もあります。あらかじめご了承ください。

商標について

Microsoft、Windowsは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
本取扱説明書では、以下のように表記します。

- Microsoft® Windows® Server 2003 operating systemは、Windows Server 2003と表記します。
- Microsoft® Windows® XP Home Edition operating system およびMicrosoft® Windows® XP Professional operating systemは、Windows XPと表記します。
- Microsoft® Windows® Millennium Edition operating systemは、Windows Meと表記します。
- Microsoft® Windows® 98 operating systemは、Windows 98と表記します。
- Microsoft® Windows® 95 operating systemは、Windows 95と表記します。
- Microsoft® Windows® 2000 Professional operating systemおよびMicrosoft® Windows® 2000 Server operating systemは、Windows 2000と表記します。
- Microsoft® Windows NT® Workstation operating system version4.0およびMicrosoft® Windows NT® Server operating system version4.0は、Windows NT 4.0と表記します。

Apple、Macintosh、Mac OSは、米国Apple Computer, Inc.の米国およびその他の国における商標または登録商標です。
Adobe、およびReaderは、Adobe Systems Incorporated（アドビシステムズ社）の商標または登録商標です。
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。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。

本文中の各社の登録商標または商標には、TM、®マークは表示しておりません。

3. 利用目的別早見表

PPPoEマルチセッションを設定したい

プロバイダを複数契約している場合、フレッツ・スクウェアを利用したい場合などは、PPPoEマルチセッションを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPPoE設定：サブ1～6（登録番号2～15のPPPoE登録）	P.25	P.66

グローバルIPアドレスをパソコンに割り当てたい
グローバルIP8/16を利用した設定をしたい
アンナンバード設定をしたい

パソコンにグローバルIPアドレスを割り当てる場合は、LAN型接続で相手先を登録する必要があります。この場合、ルータにはグローバルIPアドレスを割り当てずにパソコンにだけ割り当てる方式（アンナンバード接続）で設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPPoE（LAN型接続方式）の登録	-	P.66
LAN側IPアドレスの設定	-	P.79

フレッツ・グループアクセスライト（端末型）を使用したい

フレッツ・グループアクセスライト（端末型）で使用する場合は、PPPoEの設定が必要になります。また、複数台の端末を接続するときは、VPNの設定も必要になります。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPPoE設定：サブ1～6（登録番号2～15のPPPoE登録）	P.25	P.66
VPNポリシーの設定	-	P.108

フレッツ・グループアクセスプロ（LAN型）を使用したい

フレッツ・グループアクセスプロ（LAN型）で使用する場合は、PPPoEの設定が必要になります。また、複数台の端末を接続するときは、アンナンバードの設定も必要になります。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPPoE（LAN型接続方式）の登録	P.25	P.66
LAN側IPアドレスの設定	-	P.79

フレッツ・オフィスを使用したい

フレッツ・オフィスを使用する場合は、PPPoEの設定が必要になります。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPPoE設定：サブ1～6（登録番号2～15のPPPoE登録）	P.25	P.66

FLET'S.NetなどIPv6環境に接続したい

IPv6環境に接続する場合には、本製品のIPv6を設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
IPv6設定	-	P.124

VPN(IPSec)接続したい

VPN接続する場合は、VPNポリシー設定を行います。

必要な設定	参照ページ	
	クイック設定	詳細設定
VPNポリシー設定	-	P.108

VPN接続にPPTPを使用したい

PPTPを使ってVPN接続したい場合は、PPTP接続方式の相手先を登録します。

必要な設定	参照ページ	
	クイック設定	詳細設定
PPTPの登録	-	P.66

VPNを使用して拠点間通信をしたい

VPN接続する場合は、経由するセンタルータのVPNポリシー設定でローカルIPアドレス、リモートIPアドレス両方を「全て」に設定します。また、各拠点ルータのVPNポリシー設定で、利モートIPアドレスを「全て」に設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
VPNポリシー設定 センタ側ルータでは、ローカルIPアドレス、リモートIPアドレスの両方を「全て」に設定 拠点側ルータでは、利モードIPアドレスを「全て」に設定	-	P.108

アドレス体系を変えずにVPNを導入したい

既存のローカルIPアドレスを変更せずに、同じサブネットを使用したネットワークにVPN接続したい場合は、VPNポリシー設定でNAT+VPNを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
VPNポリシー設定:NAT+VPN	-	P.108
NATアドレスマッピングの登録	-	P.131

各機能の設定・参照・制限をユーザごとに設定したい

本製品の設定操作の権限をユーザごとに設定することができます。

必要な設定	参照ページ	
	クイック設定	詳細設定
アクセス制限設定	P.45	P.140

ルータの状態をSNMPで監視したい

SNMPマネージャを使用してルータの状態を監視したい場合は、SNMPを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
SNMP設定	-	P.136

SYSLOGをサーバに転送したい

SYSLOGをLAN上のサーバなどに転送して管理したい場合は、SYSLOGサーバ転送オプションを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
SYSLOGサーバ転送オプション	-	P.88

ファイアウォールを設定したい

LAN内のパソコンにグローバルIPアドレスを割り当てられている場合など、外部からの攻撃が考えられる場合は、ファイアウォールを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
ファイアウォール設定	-	P.84

インターネットアクセスを制御したい

LAN内のパソコンからのインターネットアクセスを制御したい場合は、インターネットアクセス制御を設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
インターネットアクセス制御設定	-	P.93

サーバを立てたい
仮想サーバの設定をしたい

LAN上のパソコンに設置したWebサーバやFTPサーバを公開したい場合は、NATを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
NAT設定	-	P.131
ファイアウォール設定	-	P.84

時間を設定したい

本製品の日付と時刻は手動設定またはNTPサーバを利用して設定できます。

必要な設定	参照ページ	
	クイック設定	詳細設定
日付と時刻の設定	-	P.74

ダイナミックDNSを使用したい

ダイナミックDNSを使用したい場合は、ダイナミックDNSを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
ダイナミックDNS設定	-	P.135

IP電話(VoIPアダプタ)を使用したい

IP電話サービスを使用したい場合は、UPnPを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
UPnP設定	-	P.134

ネットワークアプリケーションを利用したい

ネットワークゲームを利用する場合、アプリケーション登録とポート開放の設定が必要になることがあります。

必要な設定	参照ページ	
	クイック設定	詳細設定
アプリケーション設定	-	P.96
ファイアウォール設定	-	P.84
NAT設定	-	P.131

各種Messengerを使用するための設定をしたい

MessengerなどUPnPを利用したアプリケーションを使用したい場合は、UPnPを設定します。

必要な設定	参照ページ	
	クイック設定	詳細設定
UPnP設定	-	P.134

4. 目次

5. ルータ設定画面の表示

ルータの設定は、お使いのパソコンからブラウザを使ってルータの設定画面を表示し設定します。

5-1. ルータ設定の画面の表示

＊ Windows XPの画面を参照してご説明しております。

ブラウザは、以下のものを使用してください。手順は各OS共通です。
Windows　：Internet Explorer 5.5以降またはNetscape Navigator 7.0以降
Macintosh　：Internet Explorer 5.0以降またはNetscape Navigator 7.0以降

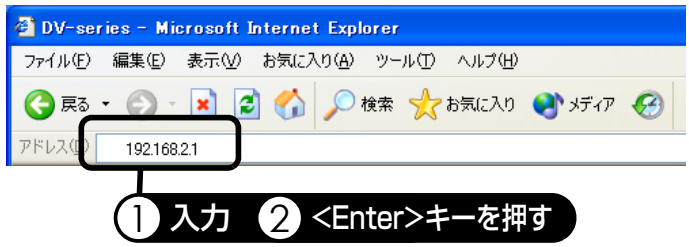
1. **[スタート]－[インターネット]をクリックします。**

＊ Windows XP以外のOSの場合、デスクトップ上にある[Internet Explorer]アイコンをダブルクリックしてください。

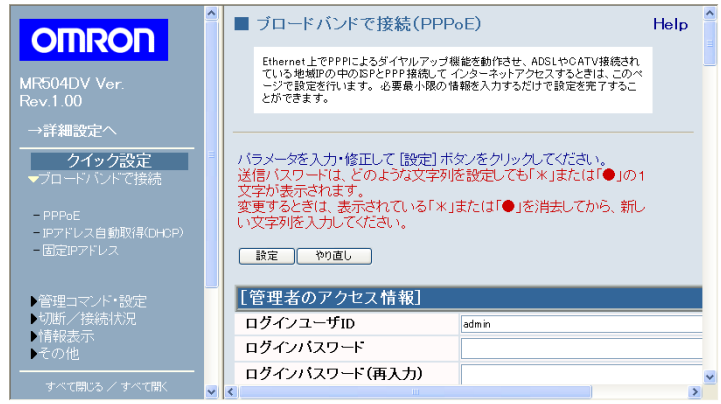
2. **アドレス欄に、本製品のIPアドレス「192.168.2.1」を入力し<Enter>キーを押します。**

＊ Macintoshの場合は<return>キーを押します。

＊ 初期設定のIPアドレスは、「192.168.2.1」です。すでに本製品のIPアドレスを変更している場合は、変更後のIPアドレスを入力してください。



3. 初期画面が表示されます。



補足

- 本製品のIPアドレス「192.168.2.1」を入力後、初期画面が表示されるまでに数分かかる場合があります。
- 初期画面が表示されない場合は、『9.困ったときには』(P.154) を参照してください。

引き続き、『5-2.ルータの設定』(P.15)へ進んでください。

大切

- パスワードにより、アクセスできるユーザを限定するログイン管理機能があります。設定方法は、『6-1-1.PPPoE』(P.25) または『6-2-3.ユーザ・パスワード変更』(P.43) を参照してください。

5-2. ルータの設定

ここでは、クイック設定を利用して接続先を設定する方法について説明します。
必要な設定は、接続しているモデムの種類や契約しているプロバイダによって異なります。以下の表を参照し、必要な設定の手順説明へお進みください。

ADSLモデムをご使用の場合		
	Bフレッツ（FTTH）、フレッツ・ADSL等（PPPoE）をご契約の場合	手順1『PPPoEメインの設定』（P.16）
	Yahoo!BB、一部FTTH サービス等（DHCP）をご契約の場合	手順1『IP アドレスの設定（YahooBB、一部FTTHサービス等（DHCP）、CATVの場合）』（P.18）
ケーブルモデムをご使用の場合		
	CATV（ケーブルテレビ）をご契約の場合	手順1『IP アドレスの設定（YahooBB、一部FTTHサービス等（DHCP）、CATVの場合）』（P.18）(*1)

*1　CATV（ケーブルテレビ）をご契約の場合、プロバイダからホスト名、ドメイン名、MAC アドレスなどが指定されることがあります。これらの設定が必要な場合は、以下を参照し設定してください。

ホスト名：詳細設定画面→［ルータ設定］→［WAN］→［DHCPクライアントID］
ドメイン名：詳細設定画面→［ルータ設定］→［LAN］→［ドメイン名］
MACアドレス：詳細設定画面→［ルータ設定］→［WAN］→［MACアドレス］

設定方法については、『7-3-1.WAN』（P.76）および『7-3-2.LAN』（P.79）を参照してください。

大切

- Bフレッツやフレッツ・ADSLなどのPPPoE方式のADSL、FTTH接続サービスをご利用の場合は、PPPoE接続用のソフトが起動していないことを確認してください。（常駐ソフトとしてスタートアップのショートカットアイコンにPPPoE接続用のソフトが入っている場合は終了させてください。）

補足

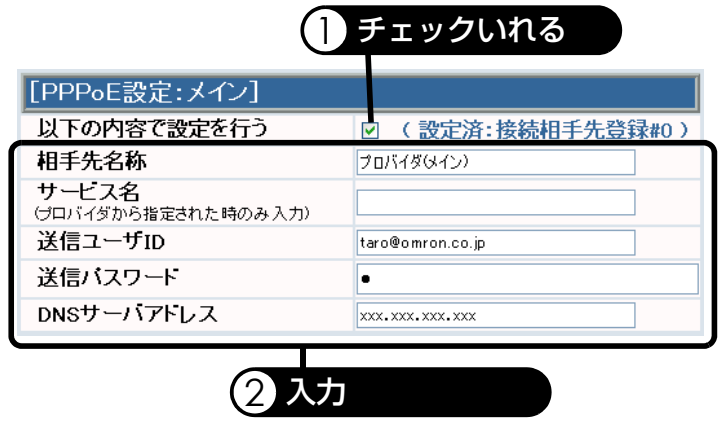
- インターネットに接続する接続情報は、ご契約されているプロバイダやサービスの内容により異なります。ご契約のADSL接続サービスの情報を用意して設定を行ってください。
- クイック設定で PPPoE 相手先の登録を行った場合、端末型接続（ルータの WAN のみにグローバルIPアドレスが割り当てられLAN側のパソコンではプライベートアドレスを利用する接続形態）でPPPoE を登録します。LAN型接続（ルータおよびLAN側のパソコンにグローバルIPアドレスを割り当てる場合）を利用したい場合は、詳細設定画面の［接続／相手先登録］からPPPoEの登録を行ってください。詳細設定画面の［接続／相手先登録］からの登録方法については、『7-1.接続／相手先登録』（P.66）を参照してください。
- PPPoE マルチセッションおよびPPTP による接続もサポートしております。PPPoE マルチセッションおよびPPTPによる設定方法については、『7-1.接続／相手先登録』（P.66）を参照してください。

手順　PPPoEメインの設定

PPPoEメインの設定では、Bフレッツ(FTTH)、フレッツ・ADSL等、PPPoEを使用してインターネットに接続する場合に、プロバイダから指定された接続情報を設定します。

1. **ルータ設定画面の右側のページを下にスクロールし、[PPPoE設定:メイン]を表示します。**

2. **[以下の内容で設定を行う]欄をチェックし、各項目を入力します。**

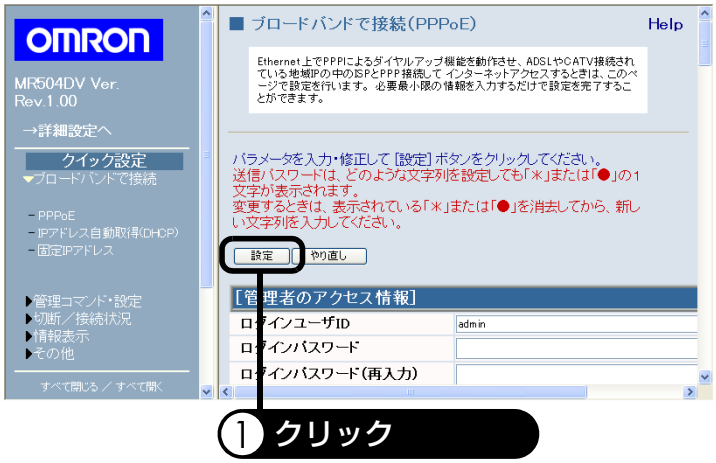


項目	説明
相手先名称	設定した相手先がどこであるかを特定するための名称を入力します。任意の名称を入力できます。 初期値:プロバイダ(メイン)
サービス名	プロバイダから指定されたサービス名がある場合に、指定されたサービス名を入力します。指定がない場合は、入力しないでください。
送信ユーザID	プロバイダから指定されたユーザID(アカウント／ログインID／認証IDともいう)を入力します。 例:taro@omron.co.jp ＊　送信ユーザIDは@を含むドメインネームをすべて入力してください。 ＊　大文字・小文字を間違えないように入力してください。
送信パスワード	プロバイダから指定されたパスワードを(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk ＊　大文字・小文字を間違えないように入力してください。 ＊　入力時「●」または「＊」で表示されます。設定後は1文字で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。指定がない場合は、入力しないでください。

補足

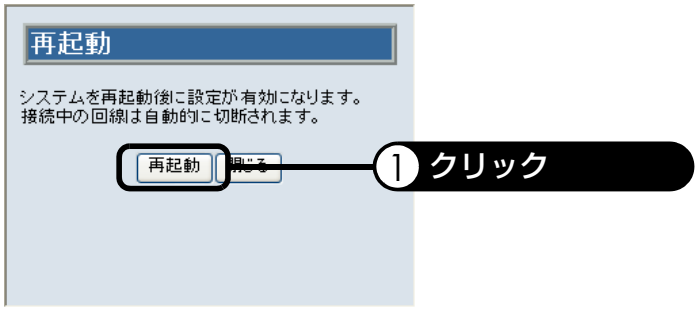
- クイック設定でPPPoEを設定した場合、接続モードは自動接続に設定されます。自動接続では、LANからの接続要求時に自動的に接続します。
  接続モードは、自動接続以外にも常時接続や手動接続を設定することもできます。設定方法については、『7-1.接続／相手先登録』(P.66)を参照してください。

3. ページを一番上までスクロールし、[設定]をクリックします。



4. 再起動画面が表示されるので、[再起動]をクリックします。

・ システムを再起動します。再起動中は、[状態]ランプが点灯します。システムの再起動を完了すると、[状態]ランプの点灯が消え、再起動画面を自動的に閉じます。



PPPoEメインの設定は以上です。
引き続き、『IPアドレスの設定(YahooBB、一部FTTHサービス等(DHCP)、CATVの場合)』(P.18)へお進みください。

手順　IPアドレスの設定(YahooBB、一部FTTHサービス等(DHCP)、CATVの場合)

IPアドレスの設定は、プロバイダからグローバルIPアドレスが指定されているか、指定されていないかによって、設定方法が異なります。

IPアドレスが指定されていない場合

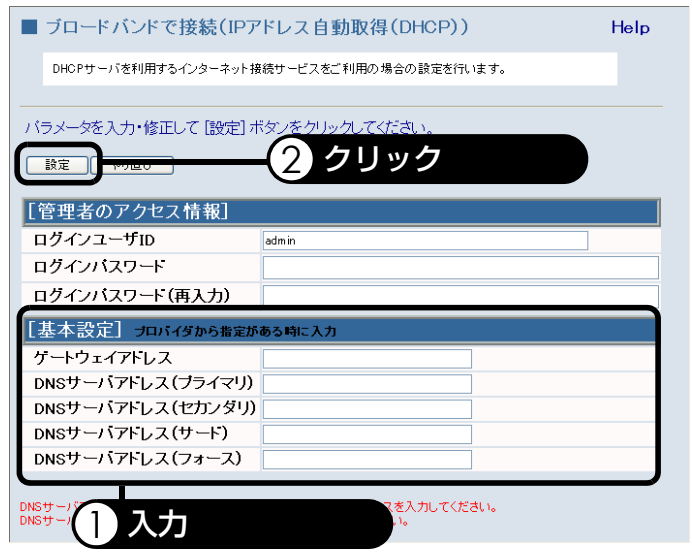
大切

- PPPoE の設定がある場合は、『6-2-2. 設定の消去』(P.42)を参照し、すべてのルータ接続相手先情報を消去してください。

1. [ブロードバンドで接続]の[IPアドレス自動取得(DHCP)]をクリックします。

2. 必要に応じて[基本設定]の項目を入力し、[設定]をクリックします。

＊ [基本設定]の入力は、プロバイダから指定がある項目のみ入力してください。プロバイダから指定がない場合は、何も入力せずに[設定]をクリックしてください。

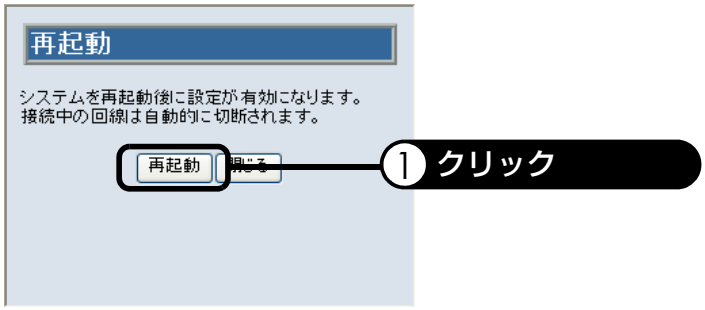


項目	説明
ゲートウェイアドレス	プロバイダから指定されたゲートウェイ(ゲートウェイアドレス／デフォルトゲートウェイともいう)がある場合に、指定されたゲートウェイを入力します。

項目	説明
DNSサーバアドレス （プライマリ） （セカンダリ） （サード） （フォース）	プロバイダから指定されたそれぞれ（プライマリ、セカンダリ、サード、フォース）のDNSサーバアドレスがある場合に、指定されたDNSサーバアドレスをそれぞれ入力します。

3. **再起動画面が表示されるので、[再起動]をクリックします。**

・ システムを再起動します。再起動中は、[状態]ランプが点灯します。システムの再起動を完了すると、[状態]ランプの点灯が消え、再起動画面を自動的に閉じます。

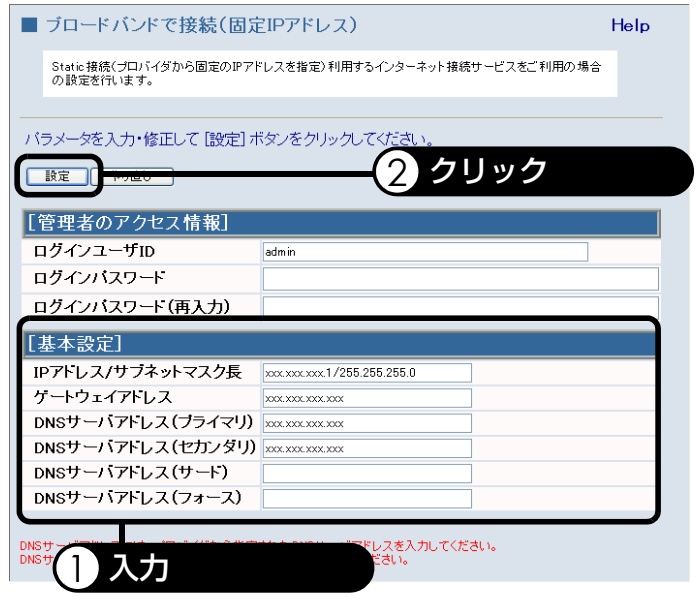


IPアドレスの設定は以上です。
引き続き、『5-3.ホームページを見る』(P.22)へお進みください。

IPアドレスが指定されている場合

1. **[ブロードバンドで接続]の[固定IPアドレス]をクリックします。**

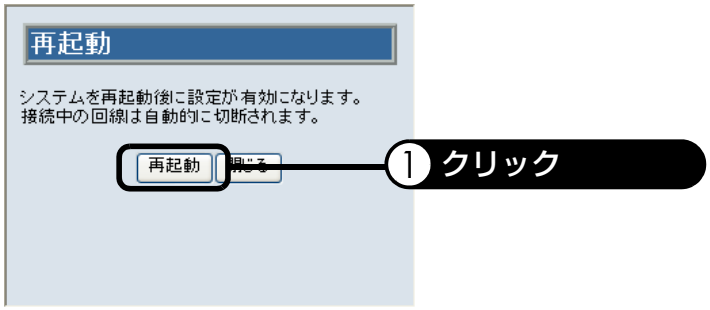
2. 必要に応じて[基本設定]の項目を入力し、[設定]をクリックします。



項目	説明
IPアドレス／ サブネットマスク長	プロバイダから指定されたIPアドレスおよびサブネットマスクを「IPアドレス/サブネットマスク」のフォーマットで入力します。 例：xxx.xxx.xxx.1/255.255.255.0 ＊ 入力したサブネットマスクは、設定を適用すると、「/24」のような入力したサブネットマスクを示すビット数に変換されます。 ＊ 「255.255.255.0」などサブネットマスクを入力する代わりに、サブネットマスクを表すビット数を入力することもできます。 例：xxx.xxx.xxx.1/24
ゲートウェイアドレス	プロバイダから指定されたゲートウェイ（ゲートウェイアドレス／デフォルトゲートウェイともいう）がある場合に、指定されたゲートウェイを入力します。
DNSサーバアドレス （プライマリ） （セカンダリ） （サード） （フォース）	プロバイダから指定されたそれぞれ（プライマリ、セカンダリ、サード、フォース）のDNSサーバアドレスがある場合に、指定されたDNSサーバアドレスをそれぞれ入力します。

3. **再起動画面が表示されるので、[再起動]をクリックします。**

・システムを再起動します。再起動中は、[状態]ランプが点灯します。システムの再起動を完了すると、[状態]ランプの点灯が消え、再起動画面を自動的に閉じます。



IPアドレスの設定は以上です。
引き続き、『5-3.ホームページを見る』(P.22)へお進みください。

5-2-1. ファイアウォールについて

本製品ではファイアウォール機能(SPI)が初期状態で設定してあるので、そのままご使用いただけます*。さらに詳細な設定をする場合は、『7-4. セキュリティ設定』(P.84)を参照してください。

＊ プロバイダから指定された固定IPアドレス(グローバルIPアドレス)を本製品に接続されたパソコンに割り当てた場合、グローバルIPアドレスを割り当てたパソコンは、インターネットに対して全てのポートがデフォルトの状態では常に閉じた状態になっています。また、本製品にはファイアウォール機能(SPI)が初期状態で設定されています。しかし、すべての外部攻撃からの保護を保証するものではありませんので、万一に備えて、不正侵入を防止するためのセキュリティソフトウェアを個々のパソコンにインストールしておくことをお勧めします。

5-3. ホームページを見る

1. アドレス欄に、半角文字で「http://www.omron.co.jp/ped-j/」と入力し、<Enter>キーを押します。
Macintoshの方は<Return>キーを押します。

補足

- ホームページが表示されない場合は、『9. 困ったときには』の『4. ホームページが表示されない』(P.156) を参照してください。

2. 終了するときは、ブラウザを閉じてください。

6. クイック設定

クイック設定画面では、必要最小限の情報を入力するだけでルータをインターネットに接続することができます。
ブラウザでルータ設定画面を表示すると、クイック設定画面が表示されます。

クイック設定画面には、以下のメニューがあります。設定したいメニューをクリックすると各設定画面が表示されるので、必要に応じて設定を行ってください。

メニュー		説明	参照ページ
ブロードバンドで接続			
	PPPoE	PPPoEの設定を行います。また、PPPoEの接続・切断を操作することができます。	P.25
	IPアドレス自動取得(DHCP)	ルータWAN側のIPアドレスをDHCPを使って設定します。	P.36
	固定IPアドレス	ルータWAN側のIPアドレスを固定IPアドレスで設定します。	P.38
管理コマンド・設定			
	再起動	ルータを再起動します。	P.41
	設定の消去	ルータの設定を各項目別にリセットすることができます。	P.42
	ユーザ・パスワード変更	ルータ設定画面を表示するためのユーザID・パスワードを設定します。	P.43
	アクセス権限	ルータ設定画面のアクセス権限を設定します。	P.45
	ファームウェア更新	ルータのファームウェアを更新します。	P.48
	設定メンテナンス	設定ファイルを直接編集して、ルータの設定を変更したり、設定情報をファイルに保存できます。	P.49
切断／接続状況			
	PPTP	PPTP回線の切断を操作します。また、接続状況を表示することができます。	P.51
	PPPoE	PPPoE回線の切断を操作します。また、接続状況を表示することができます。	P.53
情報表示			
	設定	設定情報を表示します。	P.55
	IP経路	IP経路情報を表示します。	P.55
	ログ	ログを表示または消去します。	P.56
	WAN状況	WANの設定状況を表示します。	P.57
	UPnP状況	UPnPの設定状況を表示します。	P.58
	IPSec状況	IPSecの設定状況を表示します。	P.59
	IPv6アドレス	IPv6アドレスの一覧を表示します。	P.60

メニュー		説明	参照ページ
	IPv6経路	IPv6経路情報を表示します。	P.60
	SNMP情報	SNMP情報を表示します。	P.61
その他			
	オンラインヘルプ	オンラインヘルプを表示します。	P.62

6-1. ブロードバンドで接続

補足

- 設定手順については、『5-2.　ルータの設定』(P.15) を参照してください。ここでは、画面の説明や各設定項目の詳しい説明について記載しています。
- インターネットに接続する接続情報は、ご契約されているプロバイダやサービスの内容により異なります。ご契約のADSL接続サービスの情報を用意して設定を行ってください。

6-1-1. PPPoE

Ethernet上でPPPによるダイヤルアップ機能を動作させ、ADSLやCATV接続されている地域IPの中のISPとPPP接続してインターネットアクセスするときは、このページで設定を行います。必要最小限の情報を入力するだけで設定を完了することができます。また、PPPoEの接続／切断を操作することができます。

大切

- Bフレッツやフレッツ・ADSLなどのPPPoE方式のADSL、FTTH接続サービスをご利用の場合は、PPPoE接続用のソフトが起動していないことを確認してください。(常駐ソフトとしてスタートアップのショートカットアイコンにPPPoE接続用のソフトが入っている場合は終了させてください。)

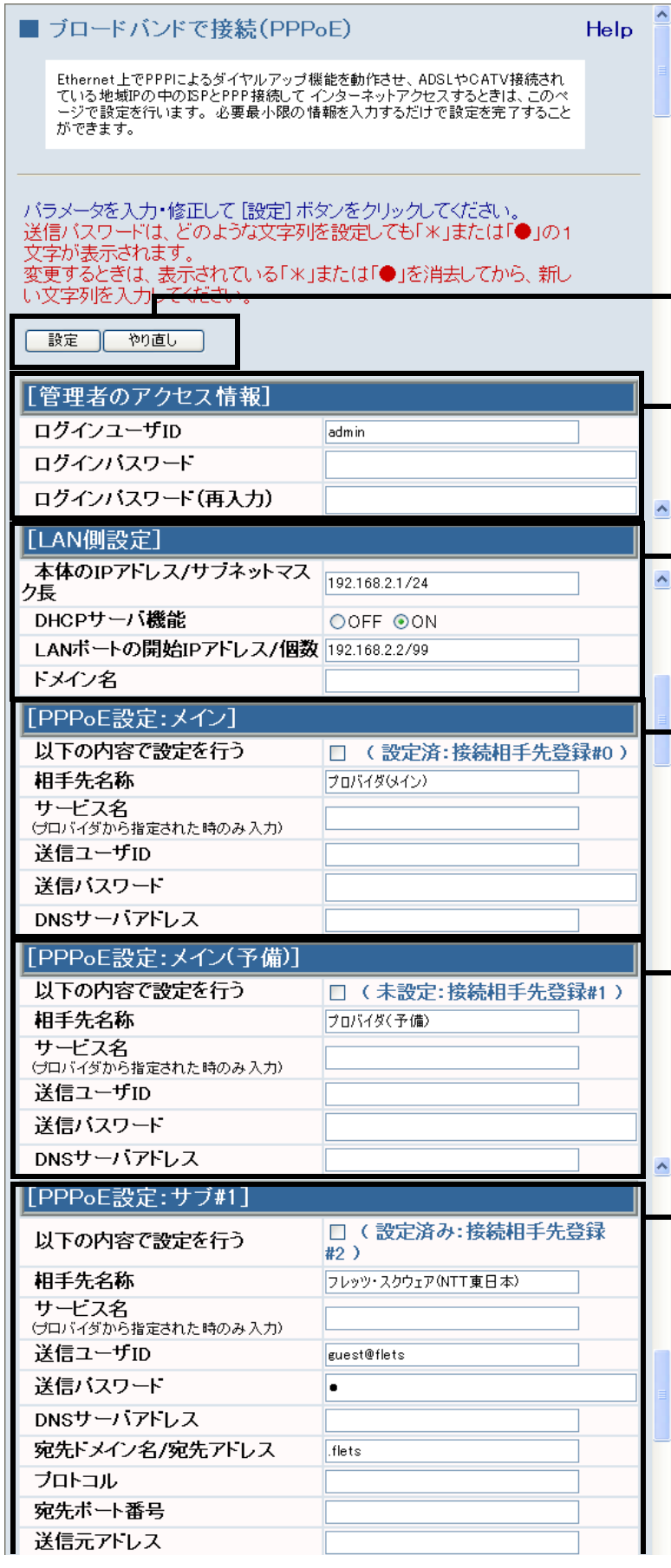
補足

- [PPPoE 設定：メイン] にマルチセッション選択ルールを設定したい場合、各相手先の接続切断モードを設定したい場合、PPTP接続方式の相手先を登録したい場合は、詳細設定画面の [接続／相手先登録] で登録を行ってください。
  詳細設定画面の [接続／相手先登録] からの相手先の登録については、『7-1.接続／相手先登録』(P.66) を参照してください。
- クイック設定で PPPoE 相手先の登録を行った場合、端末型接続(ルータの WAN のみにグローバルIPアドレスが割り当てられLAN側のパソコンではプライベートアドレスを利用する接続形態)でPPPoEを登録します。LAN型接続(ルータおよびLAN側のパソコンにグローバルIPアドレスを割り当てる場合)を利用したい場合は、詳細設定画面の [接続／相手先登録] からPPPoEの登録を行ってください。
- 詳細設定画面の [接続／相手先登録] からの相手先の登録については、『7-1.　接続／相手先登録』(P.66) を参照してください。

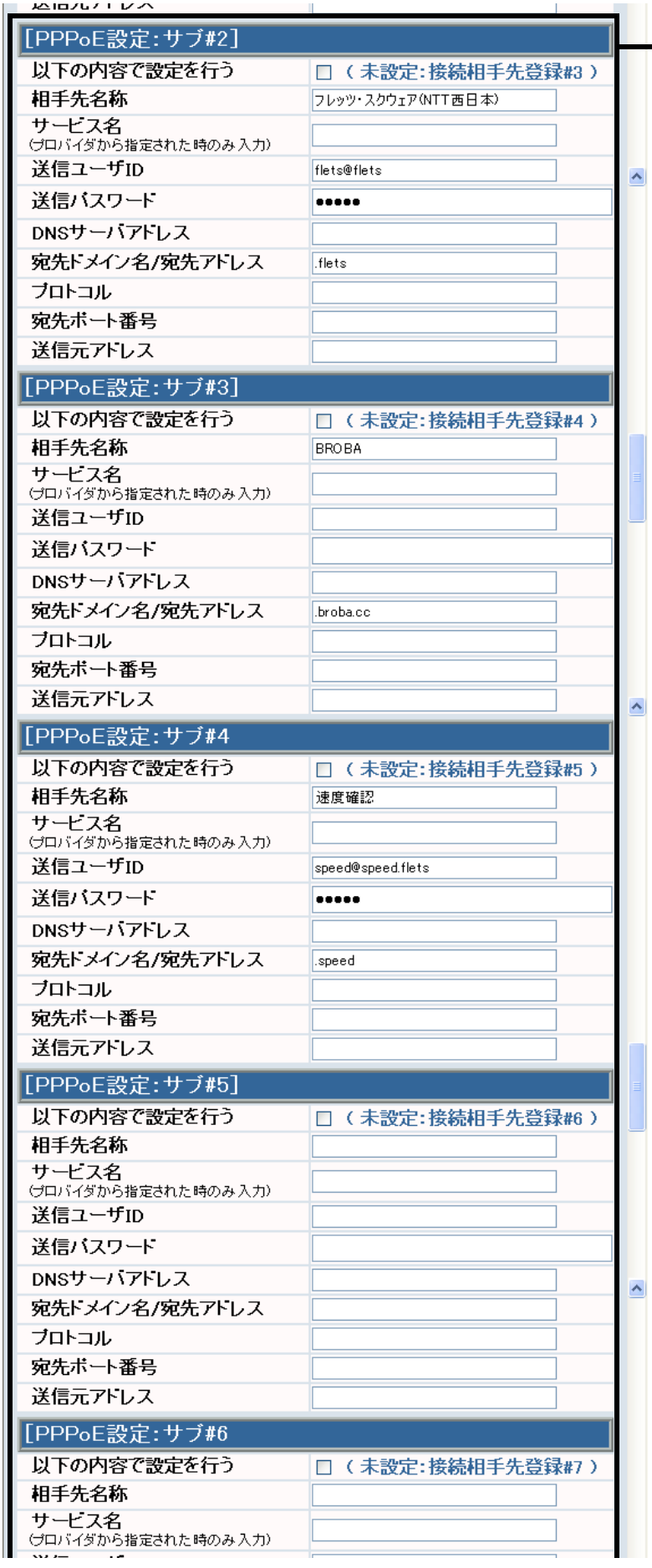
表示方法

1. [ブロードバンドで接続]→[PPPoE]の順にクリックします。
   ・ 詳細設定画面を表示している場合は、[→クイック設定へ] をクリックしてから、上記メニューをクリックします。

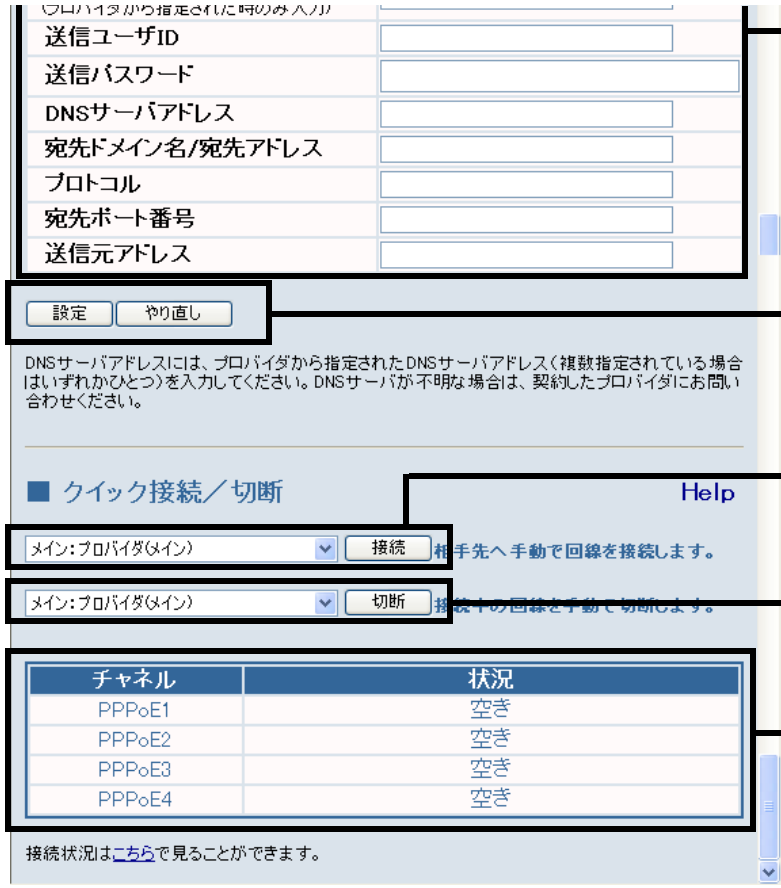
設定画面の説明



1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。(P.28)
2. 管理者のアクセス情報：ルータ設定画面の管理者ユーザ名およびパスワードを設定します。(P.28)
3. LAN側設定：LANポートの情報を設定します。(P.29)
4. PPPoE設定:メイン：通常接続する相手先を登録します。登録番号#0の相手先として登録されます。(P.29)
5. PPPoE設定:メイン(予備)：[PPPoE設定:メイン]で設定した相手先に接続できない場合に接続する相手先を登録します。(P.30)
6. PPPoE設定:サブ#1～6：PPPoEマルチセッションを設定したい場合は、これらに各相手先の情報を登録します。登録番号#2～#7として登録されます。(P.30)



6. PPPoE設定:サブ#1～6：PPPoEマルチセッションを設定したい場合は、これらに各相手先の情報を登録します。登録番号#2～#7として登録されます。(P.30)



6. PPPoE設定:サブ#1～6：PPPoEマルチセッションを設定したい場合は、これらに各相手先の情報を登録します。登録番号#2～#7として登録されます。(P.30)

1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。(P.28)

7. クイック接続：PPPoE接続を操作します。(P.35)

8. クイック切断：PPPoE接続の切断を操作します。(P.35)

9. チャンネル一覧：各PPPoEチャンネルの接続状況を表示します。(P.35)

1. 設定／やり直し　：　各設定項目で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。「LAN側設定」「PPPoE設定」を変更した場合は、クリックすると、再起動画面が表示されるので、[再起動]をクリックして本製品を再起動します。再起動を開始すると、[状態]ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態]ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 管理者のアクセス情報　：　ルータ設定画面の管理者ユーザ名およびパスワードを設定します。

項目	説明
ログインユーザ名 (初期値:admin)	ルータ設定画面にアクセスするための管理者用ログインユーザ名を入力します。ただし、ログインパスワードを設定していない場合はアクセス制御を無効にします。
ログインパスワード (初期値:なし)	ルータ設定画面にアクセスするための管理者用ログインパスワードを設定します。設定すると、ルータ設定画面にアクセスしたときに、ユーザ名とパスワードの入力画面が表示されるようになります。
ログインパスワード(再入力)	[ログインパスワード]欄に入力したパスワード再入力します。

補足

- 「管理者のアクセス情報」では、管理者用のユーザ名およびパスワードのみを変更することができます。各ユーザのユーザ名およびパスワードを設定または変更したい場合は、『6-2-3. ユーザ・パスワード変更』(P.43)を参照してください。

3. LAN側設定　　：LANポートの情報を設定します。

項目	説明
本体のIPアドレス／ サブネットマスク長 (初期値:192.168.2.1/24)	本体LAN側のIPアドレスおよびサブネットマスクを「IPアドレス/サブネットマスク」のフォーマットで入力します。 例:192.168.2.1/255.255.255.0 入力したサブネットマスクは、設定を適用すると、「/24」のような入力したサブネットマスクを示すビット数に変換されます。 「255.255.255.0」などサブネットマスクを入力する代わりに、サブネットマスクを表すビット数を入力することもできます。 例:192.168.2.1/24
DHCPサーバ機能 (初期値:ON)	DHCPサーバ機能を「OFF」にするか「ON」にするかを選択します。 「ON」にした場合、[LANポートの開始IPアドレス／個数]欄に入力した設定に従って、LANポートに接続されているパソコンにDHCP機能を使ってIPアドレスを割り当てます。
LANポートの開始IPアドレス／ 個数 (初期値:192.168.2.2/99)	DHCP機能を「ON」にした場合に、LANポートに接続されているパソコンに割り当てる開始IPアドレスおよび個数を「開始IPアドレス/個数」のフォーマットで入力します。
ドメイン名	CATV(ケーブルテレビ)をご契約の場合に、プロバイダからドメイン名の指定がある場合は、指定されたドメイン名を入力します。

4. PPPoE設定:メイン　　：通常接続する相手先を登録します。登録番号 #0 の相手先として登録されます。

項目	説明
以下の内容で設定を行う	設定を変更した場合にチェックします。チェックしていない場合は、以下の項目を変更し[設定]をクリックしても、設定は保存されません。
相手先名称 (初期値:プロバイダ(メイン))	設定した相手先がどこであるかを特定するための名称を入力します。任意の名称を入力できます。
サービス名	プロバイダから指定されたサービス名がある場合に、指定されたサービス名を入力します。指定がない場合は、入力しないでください。
送信ユーザID	プロバイダから指定されたユーザID(アカウント／ログインID／認証IDともいう)を入力します。 例:taro@omron.co.jp 送信ユーザIDは@を含むドメインネームをすべて入力してください。 大文字・小文字を間違えないように入力してください。
送信パスワード	プロバイダから指定されたパスワード(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk 大文字・小文字を間違えないように入力してください。 入力時「●」または「＊」で表示されます。設定後は1文字で表示されます。

項目	説明
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。

補足

- クイック設定でPPPoEを設定した場合、接続モードは自動接続に設定されます。自動接続では、LANからの接続要求時に自動的に接続します。
  接続モードは、自動接続以外にも常時接続や手動接続を設定することもできます。設定方法については『7-1.接続／相手先登録』(P.66)を参照してください。

5. PPPoE設定:メイン(予備)　:　[PPPoE 設定:メイン]で設定した相手先に接続できない場合に接続する相手先を登録します。

項目	説明
以下の内容で設定を行う	設定を変更した場合にチェックします。チェックしていない場合は、以下の項目を変更し[設定]をクリックしても、設定は保存されません。
相手先名称 (初期値:プロバイダ(メイン))	設定した相手先がどこであるかを特定するための名称を入力します。任意の名称を入力できます。
サービス名	プロバイダから指定されたサービス名がある場合に、指定されたサービス名を入力します。指定がない場合は、入力しないでください。
送信ユーザID	プロバイダから指定されたユーザID(アカウント／ログインID／認証IDともいう)を入力します。 例:taro@omron.co.jp 送信ユーザIDは@を含むドメインネームをすべて入力してください。 大文字・小文字を間違えないように入力してください。
送信パスワード	プロバイダから指定されたパスワード(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk 大文字・小文字を間違えないように入力してください。 入力時「●」または「＊」で表示されます。設定後は1文字で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。

6. PPPoE設定:サブ＃1～6　:　PPPoE マルチセッションを設定したい場合は、これらに各相手先の情報を登録します。登録番号#2～#7として登録されます。

項目	説明
以下の内容で設定を行う	設定を変更した場合にチェックします。チェックしていない場合は、以下の項目を変更し[設定]をクリックしても、設定は保存されません。
相手先名称	設定した相手先がどこであるかを特定するための名称を入力します。任意の名称を入力できます。
サービス名	プロバイダから指定されたサービス名がある場合に、指定されたサービス名を入力します。指定がない場合は、入力しないでください。

項目	説明
送信ユーザID	プロバイダから指定されたユーザID(アカウント／ログインID／認証IDともいう)を入力します。 例:taro@omron.co.jp 送信ユーザIDは@を含むドメインネームをすべて入力してください。 大文字・小文字を間違えないように入力してください。
送信パスワード	プロバイダから指定されたパスワード(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk 大文字・小文字を間違えないように入力してください。 入力時「●」または「＊」の1文字で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。
宛先ドメイン名／宛先アドレス	接続する宛先ドメイン名(ただし「http://」およびディレクトリは除く)またはIPアドレスを入力して、マルチセッション選択ルールを設定します。複数のドメイン名またはアドレスを指定したい場合は、カンマ(,)で区切って入力します。登録できるアドレスは最大4個です。ただし、この項目欄ではドメイン名とアドレスを併用して設定することはできません。ドメイン名とアドレスを併用して設定したい場合は、詳細設定の相手先登録画面のオプション欄で設定します。 →『7-1-1.相手先登録』(P.67) 指定したドメイン名またはURLアドレスにLAN側のパソコンからアクセス要求が送られてきた場合に、この相手先を使用してインターネットにアクセスするようになります。
プロトコル	通信に使用するプロトコルを入力して、マルチセッション選択ルールを設定します。ニーモニック(esp, gre, icmp, ipencap, tcp, udp)またはプロトコル番号で入力します。例えば、Webにアクセスするときに使用する相手先に設定する場合は、「tcp」と入力します。 空欄または「＊」を入力した場合は、すべてのプロトコルが対象となります。「＊」を入力して設定した場合は、再登録時には空欄で表示されます。
宛先ポート番号	通信に使用するポート番号を入力して、マルチセッション選択ルールを設定します。ニーモニックまたはポート番号で入力します。例えば、Webにアクセスするときに使用する相手先に設定する場合は、「80」と入力します。空欄または「＊」を入力した場合は、すべてのポート番号が対象となります。「＊」を入力して設定した場合は、再登録時には空欄で表示されます。
送信元アドレス	この接続を利用するPCのローカルIPアドレスを入力して、マルチセッション選択ルールを設定します。IPアドレスの範囲を指定したい場合は、ハイフン(-)で区切って入力します。また、スラッシュ(/)で区切って、サブネットマスク長を指定することもできます。

補足

宛先ドメイン名／宛先アドレスについて

- [宛先ドメイン名／宛先アドレス]欄には、ドメイン名とアドレスを併用して入力することはできません。ドメイン名とアドレスを併用してマルチセッション選択ルールを設定したい場合は、詳細設定画面から相手先の登録を行います。→『7-1-1.相手先登録』(P.67)
- IPアドレスの場合、ハイフンで区切ってアドレスの範囲を指定することもできます。
  例：xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyyy
- 空欄または＊を入力した場合は、すべての宛先が対象となります。

例：ホスト名の指定	接続対象となる宛先
.jp	最後に.jpがつくサイトすべて
.co.jp	最後に.co.jpがつくサイトすべて
.www.omron.co.jp	最後に.www.omron.co.jpがつくサイトすべて (host.www.omron.co.jp, host2.www.omron.co.jpなど。 ただし、www.omron.co.jpは対象外。)
www.omron.co.jp	www.omron.co.jpのみ(先頭に「.」がない場合)

- AutoDNS機能がOFFになっている場合は、宛先とドメイン名を指定しても無効になります。AutoDNS機能をONにしたい場合は、『7-3-2.LAN』(P.79)を参照してください。

補足

PPPoEセッションキープアライブ機能について

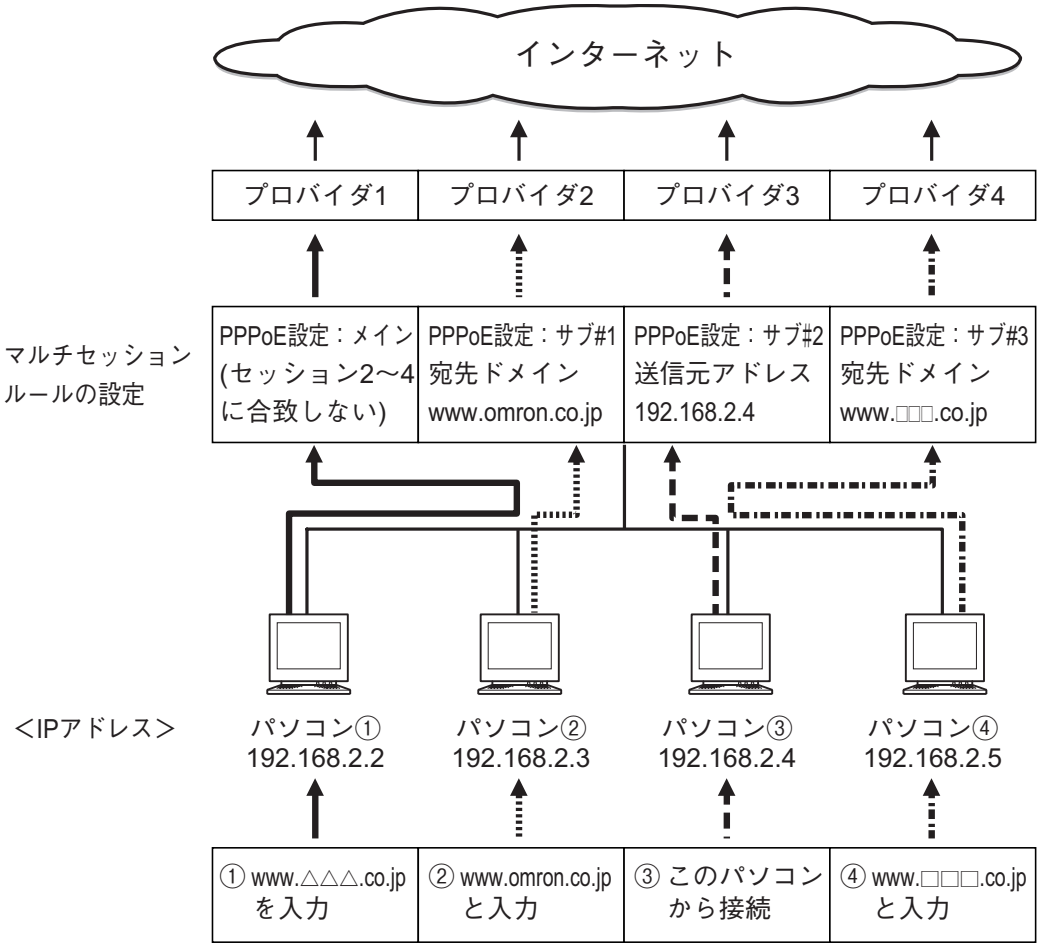
- PPPoE セッションキープアライブ機能を使うと、PPPoE 接続が何らかの理由で切断された場合に、自動で定期的に再接続を試みます。初期設定では、この機能はOFFになっています。PPPoEセッションキープアライブ機能を有効にしたい場合は、詳細設定画面の[接続／相手先登録]から、PPPoEの登録を行ってください。設定方法については、『7-1.接続／相手先登録』(P.66)を参照してください。

補足

マルチセッション選択ルールの設定について

マルチセッション選択ルールを指定することで、どのような場合にどの接続を使用するかを設定し相手先を使い分けることができます。

例えば、以下図のように動作します。



① パソコン①からブラウザに www. △△△ .co.jp と入力した場合、どのマルチセッション選択ルールにも合致しないため、セッション1のプロバイダで接続されます。

② パソコン②から www.omron.co.jp と入力した場合、サブ＃１のマルチセッション選択ルールと合致したため、サブ＃1のプロバイダで接続されます。

③ IP アドレスが「192.168.2.4」のパソコン③からインターネットに接続する場合、サブ＃２のマルチセッション選択ルールと合致したため、サブ＃2のプロバイダで接続されます。

④ パソコン④からブラウザにwww.□□□.co.jpと入力した場合、サブ＃3のマルチセッション選択ルールと合致したため、サブ＃3のプロバイダで接続されます。

補足

フレッツ・スクウェアを設定する場合

通常接続するメインのプロバイダとしか契約していない場合でも、Bフレッツまたはフレッツ・ADSLユーザであれば、フレッツ・スクウェアに無料で接続できます。
フレッツ・スクウェアに接続するための設定は、あらかじめ[PPPoE設定:サブ#1](NTT東日本)および[PPPoE設定:サブ#2](NTT西日本)に入力されています。これらの[以下の内容で設定を行う]をチェックし[設定]をクリックするか、必要に応じて他のサブ設定欄に以下の内容を設定します。

設定例

相手先名称	:	「フレッツ・スクウェア」
サービス名	:	空欄
送信ユーザID	:	NTT東日本の場合…「guest@flets」 NTT西日本の場合…「flets@flets」
送信パスワード	:	NTT東日本の場合…「guest」(*1) NTT西日本の場合…「flets」(*1)
DNSサーバアドレス	:	空欄
宛先ドメイン名／宛先アドレス	:	NTT東日本の場合…「.flets」 NTT西日本の場合…「flets」
プロトコル	:	空欄
宛先ポート番号	:	空欄
送信元アドレス	:	空欄

設定完了後、フレッツ・スクウェアにアクセスする場合はブラウザのアドレス欄に「http://www.flets/」と入力し、<Enter>キーを押してください。フレッツ・スクウェアのページが表示されます。

*1　フレッツ・スクウェアのユーザID、パスワードは、2005年7月現在の内容です。

補足

BROBAを設定する場合

BROBAに接続するには、別途NTTとの契約が必要になります。BROBAを契約している場合、通常のインターネット経由でもBROBAをご利用いただけますが、本製品を使って独立したセッションを確立することで、より高品質のコンテンツが利用可能になります。
BROBAに接続するための基本的な設定は、あらかじめ[PPPoE設定:サブ#3]に入力されています。ただし、送信ユーザIDや送信パスワードは、BROBAを契約後に指示されますので、これらの情報はそれぞれ入力する必要があります。

設定例

相手先名称	:	「BROBA」
サービス名	:	空欄
送信ユーザID	:	BROBAから指示されたユーザID「xxxxx@broba.cc」
送信パスワード	:	BROBAから指示されたパスワード
DNSサーバアドレス	:	空欄
宛先ドメイン名／宛先アドレス	:	「.broba.cc」
プロトコル	:	空欄
宛先ポート番号	:	空欄
送信元アドレス	:	空欄

設定完了後、BROBAにアクセスする場合はブラウザのアドレス欄に「http://www.broba.cc/」と入力し、<Enter>キーを押してください。BROBAのページが表示されます。

7. クイック接続　　：PPPoE接続を操作します。

項目	説明
ドロップダウンメニュー	接続するPPPoE接続を選択します。
[接続]	クリックすると、ドロップダウンメニューで選択したPPPoE相手先に接続します。

8. クイック切断　　：PPPoE接続の切断を操作します。

項目	説明
ドロップダウンメニュー	接続を切断するPPPoE接続を選択します。
[切断]	クリックすると、ドロップダウンメニューで選択したPPPoE相手先を切断します。

9. チャンネル一覧　　：各PPPoEチャンネルの接続状況を表示します。

項目	説明
チャンネル	PPPoEのチャンネル一覧を表示します。本製品では、同時に4つのPPPoEを接続することができます。
状態	それぞれのチャンネルが空き状態にあるか接続状態にあるかを表示します。

6-1-2. IPアドレス自動取得(DHCP)

DHCPサーバを利用するインターネット接続サービスをご利用の場合(プロバイダから固定IPアドレスの指定がない場合)は、このページでDHCPの設定を行います。

大切

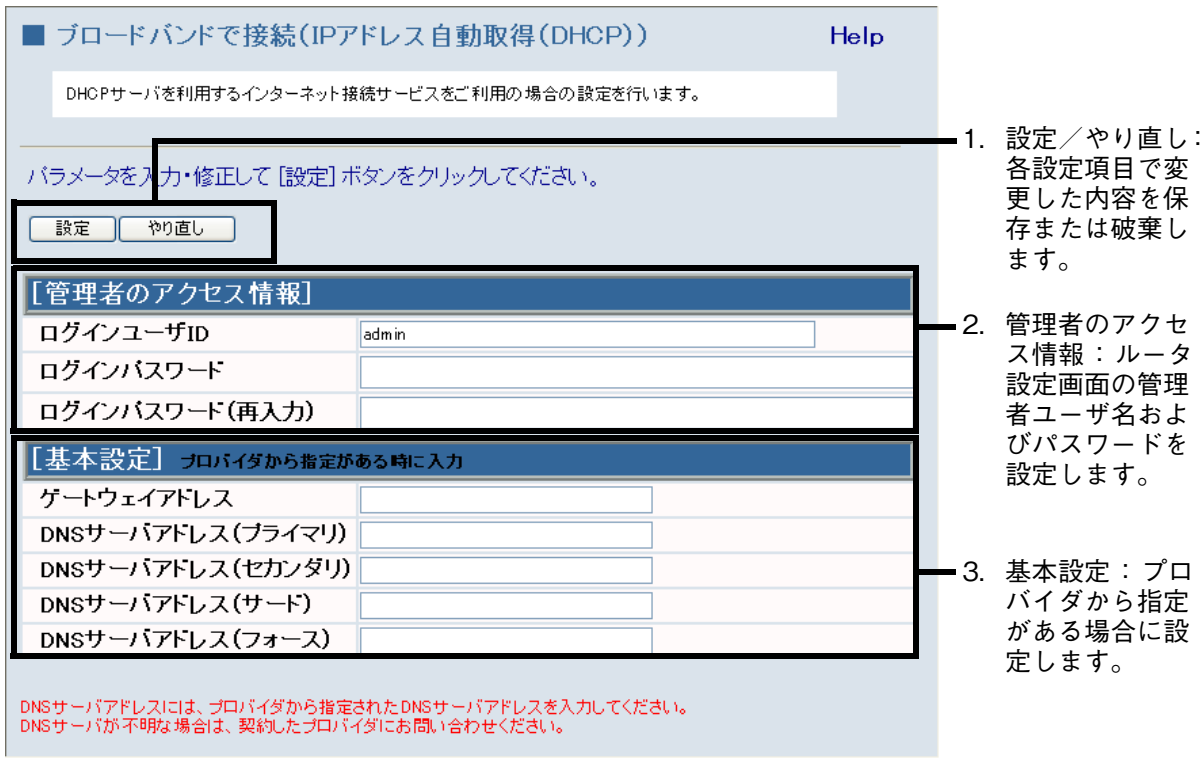
- PPPoE の設定がある場合は、『7-11-2. 設定の消去』(P.139) を参照し、相手先登録情報を消去してください。

表示方法

1. **[ブロードバンドで接続]→[IPアドレス自動取得(DHCP)]の順にクリックします。**

・ 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。

設定画面の説明



1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。
2. 管理者のアクセス情報：ルータ設定画面の管理者ユーザ名およびパスワードを設定します。
3. 基本設定：プロバイダから指定がある場合に設定します。

1. 設定／やり直し　：各設定項目で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動] をクリックして本製品を再起動します。再起動を開始すると、[状態] ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態] ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度 [設定] をクリックして有効になった内容はクリアされません。

2. 管理者のアクセス情報　：ルータ設定画面の管理者ユーザ名およびパスワードを設定します。

項目	説明
ログインユーザ名 (初期値:admin)	ルータ設定画面にアクセスするための管理者用ログインユーザ名を入力します。ただし、ログインパスワードを設定していない場合はアクセス制御を無効にします。
ログインパスワード (初期値:なし)	ルータ設定画面にアクセスするための管理者用ログインパスワードを設定します。設定すると、ルータ設定画面にアクセスしたときに、ユーザ名とパスワードの入力画面が表示されるようになります。
ログインパスワード(再入力)	[ログインパスワード]欄に入力したパスワード再入力します。

補足

- 「管理者のアクセス情報」では、管理者用のユーザ名およびパスワードのみを変更することができます。各ユーザのユーザ名およびパスワードを設定または変更したい場合は、『6-2-3. ユーザ・パスワード変更』(P.43) を参照してください。

3. 基本設定　：プロバイダから指定がある場合に設定します。

項目	説明
ゲートウェイアドレス	プロバイダから指定されたゲートウェイ(ゲートウェイアドレス、デフォルトゲートウェイともいう)がある場合に、指定されたゲートウェイを入力します。
DNSサーバアドレス (プライマリ) (セカンダリ) (サード) (フォース)	プロバイダから指定されたそれぞれ(プライマリ、セカンダリ、サード、フォース)のDNSサーバアドレスがある場合に、指定されたDNSサーバアドレスをそれぞれ入力します。

6-1-3. 固定IPアドレス

プロバイダから固定IPアドレスの指示がある場合は、このページで固定IPアドレスの設定を行います。

大切

- PPPoE の設定がある場合は、『7-11-2. 設定の消去』(P.139) を参照し、相手先登録情報を消去してください。

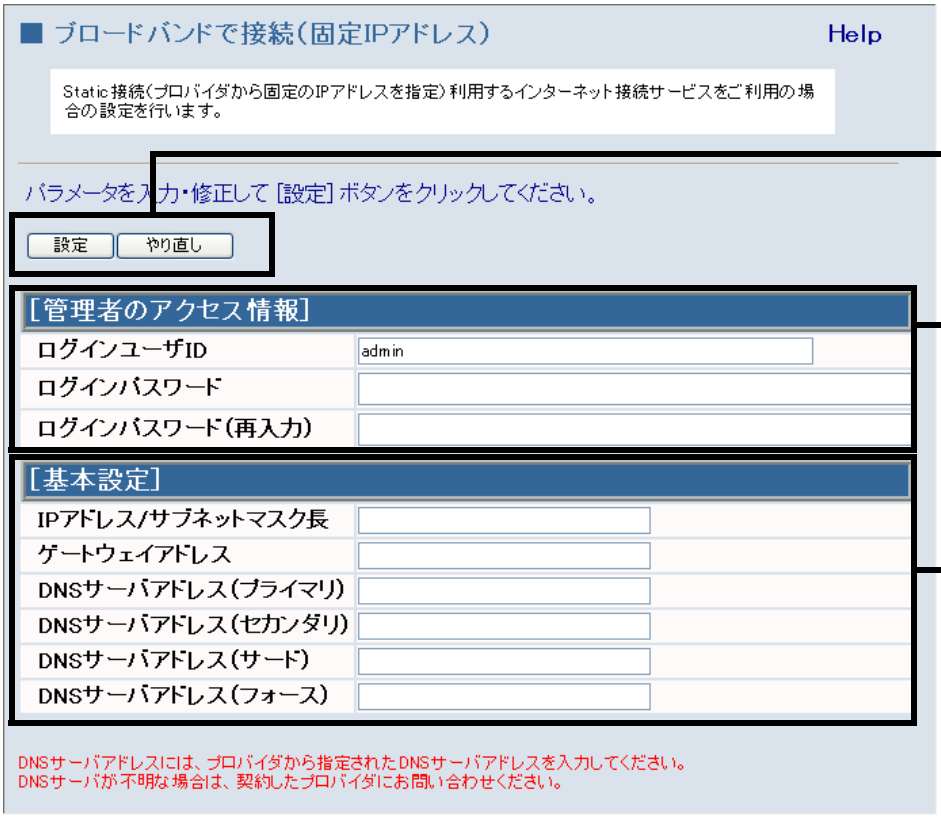
補足

- アンナンバードの設定をしたい場合は、プロバイダから支給された固定 IP アドレスを WAN 側IPアドレスではなくLAN側IPアドレスとして設定する必要があります。この場合は、詳細設定画面の [接続／相手先登録] からLAN型接続にて相手先を登録し、詳細設定画面の [ルータ設定] ー [LAN] にてプロバイダから支給された固定IPアドレスを設定します。設定方法については、『7-1.接続／相手先登録』(P.66) および『7-3-2.LAN』(P.79) を参照してください。
- 複数プロバイダと契約していて、プロバイダからそれぞれ異なる固定IPアドレスが支給されている場合、詳細設定画面の [接続／相手先登録] から相手先を登録するときにWAN側のグローバルIPアドレスを [オプション] 欄で相手先ごとに設定します。設定方法については、『7-1.接続／相手先登録』(P.66) を参照してください。

表示方法

1. **[ブロードバンドで接続]→[固定IPアドレス]の順にクリックします。**
   ・ 詳細設定画面を表示している場合は、[→クイック設定へ] をクリックしてから、上記メニューをクリックします。

設定画面の説明



1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。
2. 管理者のアクセス情報：ルータ設定画面の管理者ユーザ名およびパスワードを設定します。
3. 基本設定：プロバイダから指定された情報を設定します。

1. 設定／やり直し　：各設定項目で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動] をクリックして本製品を再起動します。再起動を開始すると、[状態] ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態] ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度 [設定] をクリックして有効になった内容はクリアされません。

2. 管理者のアクセス情報　：ルータ設定画面の管理者ユーザ名およびパスワードを設定します。

項目	説明
ログインユーザ名 (初期値:admin)	ルータ設定画面にアクセスするための管理者用ログインユーザ名を入力します。ただし、ログインパスワードを設定していない場合はアクセス制御を無効にします。
ログインパスワード (初期値:なし)	ルータ設定画面にアクセスするための管理者用ログインパスワードを設定します。設定すると、ルータ設定画面にアクセスしたときに、ユーザ名とパスワードの入力画面が表示されるようになります。
ログインパスワード(再入力)	[ログインパスワード] 欄に入力したパスワード再入力します。

補足

- 「管理者のアクセス情報」では、管理者用のユーザ名およびパスワードのみを変更することができます。各ユーザのユーザ名およびパスワードを設定または変更したい場合は、『6-2-3. ユーザ・パスワード変更』(P.43)を参照してください。

3. 基本設定　　：プロバイダから指定された情報を設定します。

項目	説明
IPアドレス／ サブネットマスク長	プロバイダから指定されたIPアドレスおよびサブネットマスクを「IPアドレス/サブネットマスク」のフォーマットで入力します。 例：xxx.xxx.xxx.1/255.255.255.0 入力したサブネットマスクは、設定を適用すると、「/24」のような入力したサブネットマスクを示すビット数に変換されます。 「255.255.255.0」などサブネットマスクを入力する代わりに、サブネットマスクを表すビット数を入力することもできます。 例：xxx.xxx.xxx.1/24
ゲートウェイアドレス	プロバイダから指定されたゲートウェイ(ゲートウェイアドレス、デフォルトゲートウェイともいう)がある場合に、指定されたゲートウェイを入力します。
DNSサーバアドレス (プライマリ) (セカンダリ) (サード) (フォース)	プロバイダから指定されたそれぞれ(プライマリ、セカンダリ、サード、フォース)のDNSサーバアドレスがある場合に、指定されたDNSサーバアドレスをそれぞれ入力します。

6-2. 管理コマンド・設定

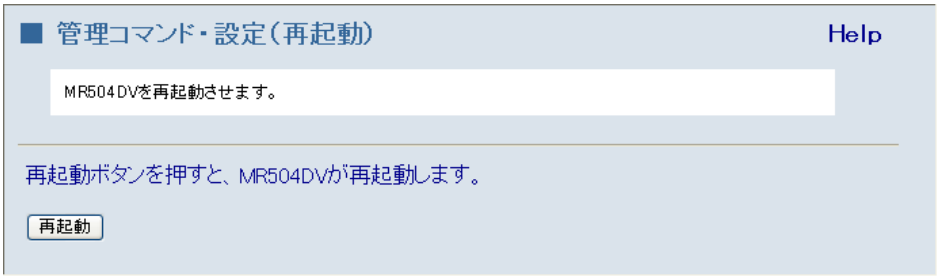
6-2-1. 再起動

本製品を再起動します。本製品の設定を変更し、再起動画面で[再起動]をクリックした場合と同じように、このページで本製品の再起動を手動で操作することができます。

表示方法

1. **[管理コマンド・設定]→[再起動]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[再起動]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
[再起動]	クリックすると本製品を再起動します。再起動を開始すると、[状態]ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態]ランプが消えます。

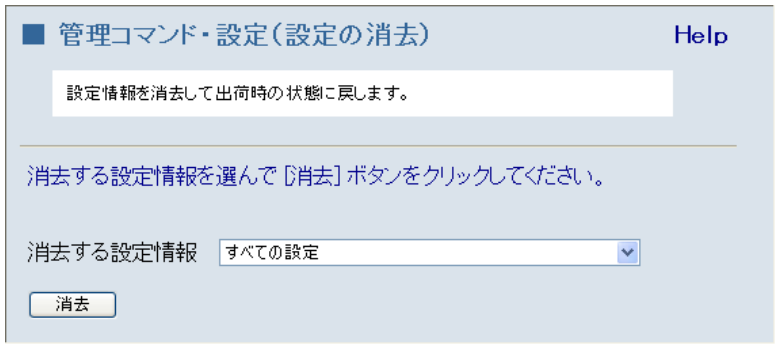
6-2-2. 設定の消去

本製品の設定を消去して、出荷時の設定に戻します。
全設定を出荷時の設定に戻すか、または希望の項目を選択して、その項目だけを出荷時の設定に戻すこともできます。

表示方法

1. **[管理コマンド・設定]→[設定の消去]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[設定の消去]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
消去する設定情報	出荷時の設定に戻したい設定項目を選択します。すべての設定を出荷時の設定に戻したい場合は、「すべての設定」を選択します。
[消去]	クリックすると、[消去する設定情報]で選択した設定情報を出荷時の設定に戻します。クリックすると、再起動画面が表示されるので、[再起動]をクリックして本製品を再起動します。再起動を開始すると、[状態]ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態]ランプが消えます。

6-2-3. ユーザ・パスワード変更

ルータ設定画面にアクセスするためのユーザIDおよびパスワードを設定します。ブロードバンドや専用線でインターネットに常時接続する場合は、外部からの侵入を防ぐために設定することをお勧めします。
本製品では、管理者用のユーザID・パスワードを１つ、またユーザ用のユーザID・パスワードを３つまで設定することができます。

補足

- 管理者用のユーザ ID およびパスワードの設定は、[ブロードバンドで接続]の[PPPoE]、[IPアドレス自動取得(DHCP)]、[固定IPアドレス]のページでも設定することができます。

表示方法

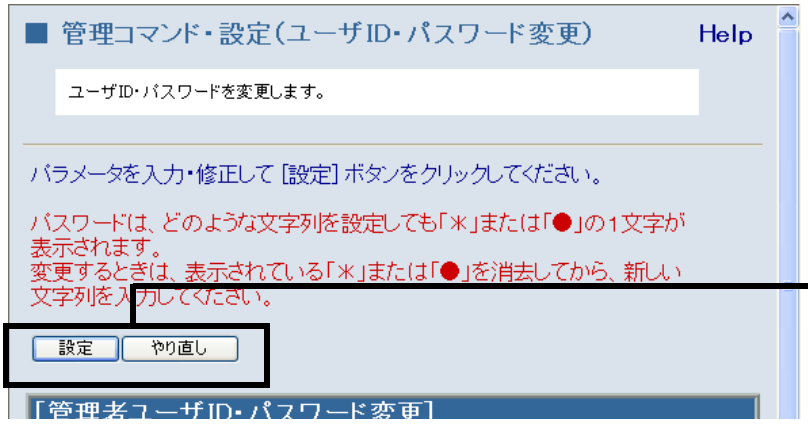
1. **[管理コマンド・設定]→[ユーザ・パスワード変更]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[ユーザ・パスワード変更]をクリックしても同様の画面が表示されます。

設定画面の説明

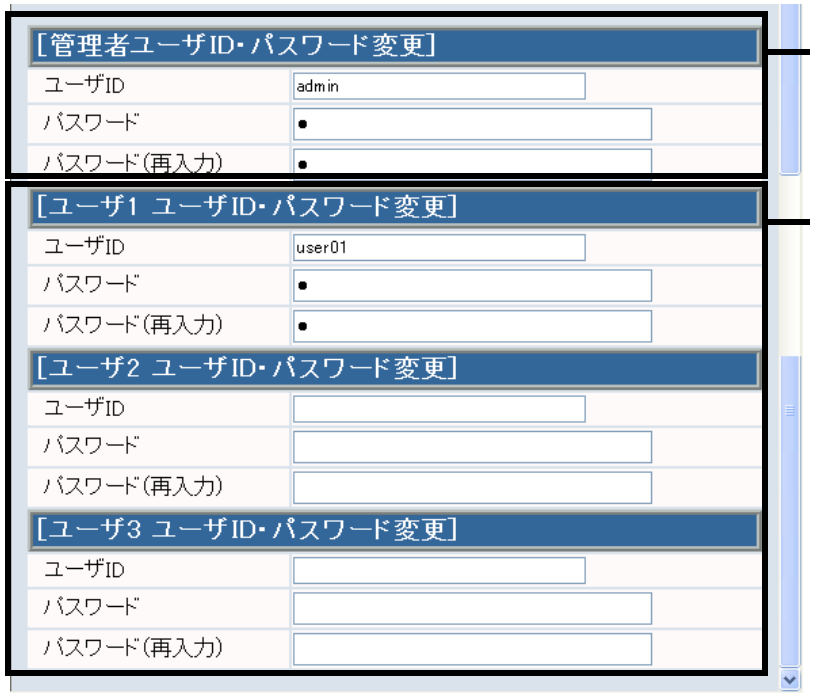
補足

管理者、ユーザの各制限について

- 管理者でログインした場合は、管理者用およびユーザ用のログイン ID およびパスワードすべての設定を変更することができます。ユーザ用のユーザIDでログインした場合は、ログインに使用したユーザIDおよびパスワードの設定のみ変更することができます。
- ユーザ用のユーザIDおよびパスワードを設定した場合は、『6-2-4.アクセス権限』(P.45)を参照して、設定したユーザのアクセス制限を設定してください。アクセス制限を設定していない場合は、ユーザID・パスワードを設定してもルータ設定画面にアクセスすることができません。
- 管理者、ユーザを切り替えてログインする場合は、ブラウザの再起動が必要です。



1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。



2. 管理者ユーザID・パスワード変更：管理者用のユーザIDおよびパスワードを設定します。管理者でログインした場合のみ表示されます。

3. ユーザ1～3 ユーザID・パスワード変更：ユーザ用のユーザIDおよびパスワードを設定します。管理者でログインした場合は、ユーザ1～ユーザ3すべてのユーザID・パスワードの設定欄が表示されます。ユーザ用ユーザIDでログインした場合は、自分のユーザID・パスワードのみ表示されます。

1. 設定／やり直し　：　各設定項目で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 管理者ユーザID・パスワード変更　：　管理者用のユーザ ID およびパスワードを設定します。管理者でログインした場合のみ表示されます。

項目	説明
ユーザID (初期値:admin)	管理者用ログインユーザ名を入力します。ただし、ログインパスワードを設定していない場合はアクセス制御を無効にします。
パスワード (初期値:なし)	管理者用ログインパスワードを設定します。設定すると、ルータ設定画面にアクセスしたときに、ユーザ名とパスワードの入力画面が表示されるようになります。
パスワード(再入力)	[パスワード]欄に入力したパスワード再入力します。

3. ユーザ1～3 ユーザID・パスワード変更：　ユーザ用のユーザ ID およびパスワードを設定します。管理者でログインした場合は、ユーザ１～ユーザ３すべてのユーザID・パスワードの設定欄が表示されます。ユーザ用ユーザIDでログインした場合は、自分のユーザID・パスワードのみ表示されます。

項目	説明
ユーザID	ユーザ1～ユーザ3用ログインユーザ名を入力します。
パスワード	ルータ設定画面にアクセスするためのログインパスワードを設定します。
パスワード(再入力)	[パスワード]欄に入力したパスワード再入力します。

6-2-4. アクセス権限

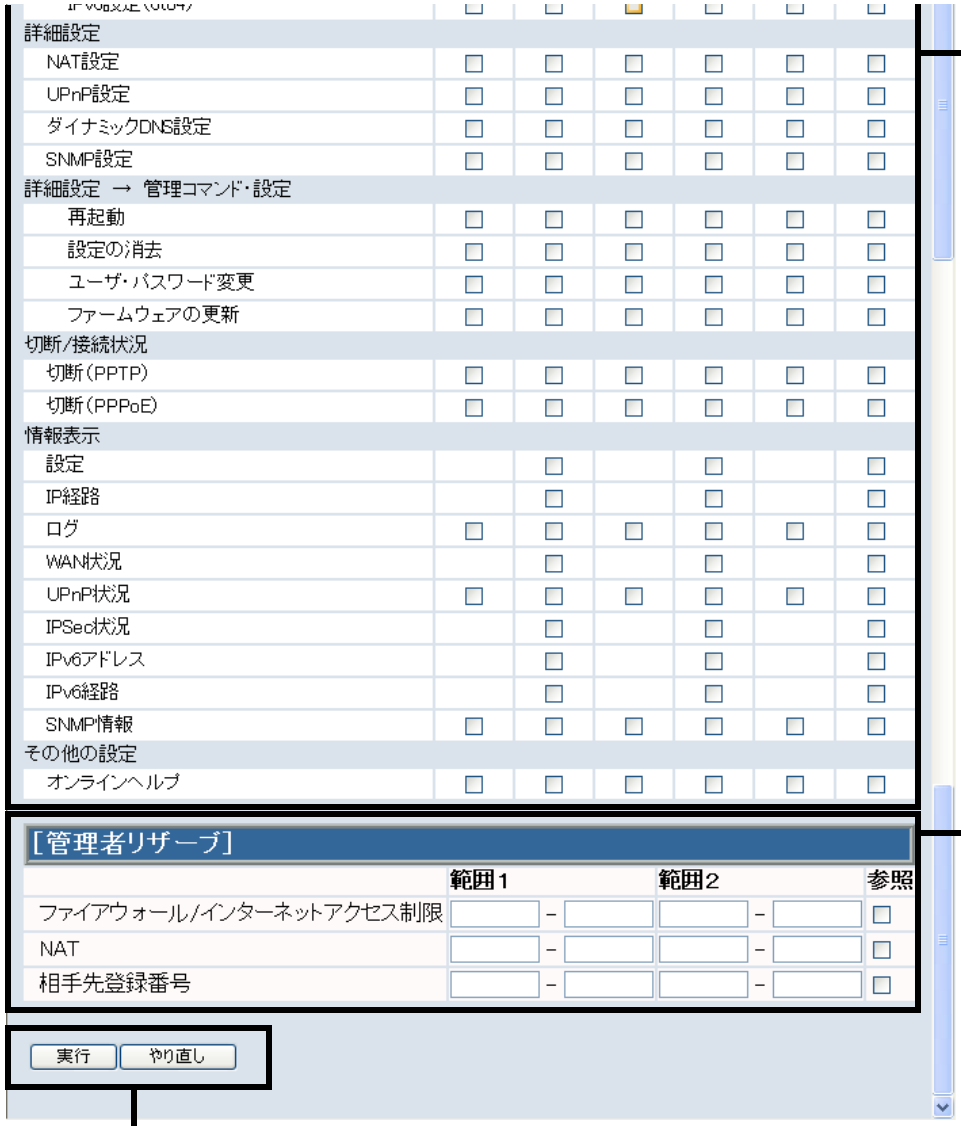
ルータ設定画面のアクセス権限をユーザごとに設定します。管理者でログインした場合またはユーザID・パスワードが設定されていない場合のみ表示されます。

表示方法

1. [管理コマンド・設定]→[アクセス権限]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[アクセス権限]をクリックしても同様の画面が表示されます。

設定画面の説明

1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。
2. 設定ページ・ユーザー覧：変更または参照を許可する設定画面を各ユーザごとに設定します。



2. 設定ページ・ユーザ一覧：変更または参照を許可する設定画面を各ユーザごとに設定します。

3. 管理者リザーブ：ファイアウォール、インターネットアクセス制御、NAT、相手先登録で登録(設定)した番号で、管理者のみが設定／変更可能な番号を設定します。

1. 設定／やり直し：各設定項目で変更した内容を保存または破棄します。

1. 設定／やり直し　　：　各設定項目で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	変更した内容を破棄し、変更前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 設定ページ・ユーザ一覧　　：　変更または参照を許可する設定画面を各ユーザごとに設定します。

項目	説明
変更	設定の変更を許可する設定画面のチェックボックスをチェックします。[全ページ]項目の変更チェックボックスをチェックすると、すべての設定画面の変更チェックボックスにチェックが入ります。

項目	説明
参照	参照のみを許可する設定画面のチェックボックスをチェックします。[全ページ]項目にある参照チェックボックスをチェックすると、すべての設定画面の参照チェックボックスにチェックが入ります。

3. 管理者リザーブ　：　ファイアウォール、インターネットアクセス制御、NAT、相手先登録で登録(設定)した番号で、管理者のみが設定／変更可能な番号を設定します。

項目	説明
ファイアウォール／ インターネットアクセス制御	管理者のみが登録可能なファイアウォール・インターネットアクセス制御の登録番号の範囲を入力します。 各ユーザに設定内容の参照を許可する場合は、[参照]チェックボックスをチェックします。
NAT	管理者のみが登録可能なNATの登録番号の範囲を入力します。 各ユーザに設定内容の参照を許可する場合は、[参照]チェックボックスをチェックします。
接続先番号	管理者のみが登録可能な相手先の登録番号の範囲を入力します。 各ユーザに設定内容の参照を許可する場合は、[参照]チェックボックスをチェックします。

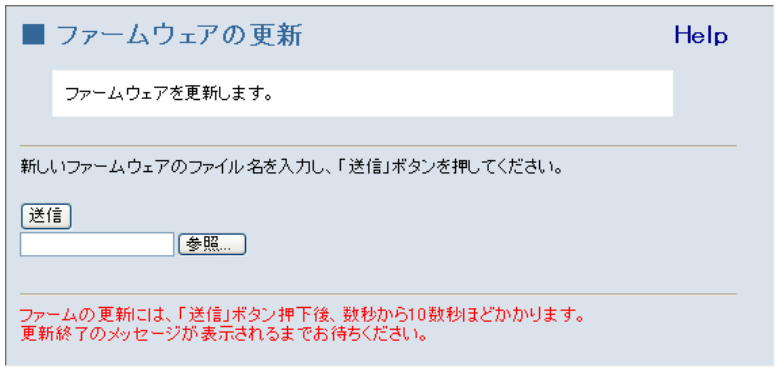
6-2-5. ファームウェア更新

新しいファームウェアが公開された場合は、このページを使ってファームウェアを更新することができます。

表示方法

1. **[管理コマンド・設定]→[ファームウェア更新]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[ファームウェア更新]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
[送信]	[参照]欄で選択したファームウェアを本製品に送信します。ファームウェアの送信には数秒から10数秒ほどかかることがあります。
[参照]	クリックすると、ファイルの選択画面が表示されるので、本製品にアップロードするファームウェアのファイルを選択します。

6-2-6. 設定メンテナンス

このメニューをクリックすると、設定メンテナンス画面が別ウィンドウで表示されます。
設定メンテナンス画面では、直接設定ファイルを編集して、本製品の設定を変更することができます。
また、設定をHTML形式やテキスト形式にして、ファイルに保存することができます。HTML形式で保存したファイルを読み込むことで設定を復元することができます。

大切

- 誤った設定を入力した場合、本製品が正常に動作しなくなることがあります。設定の入力方法がわからない場合は、絶対に変更しないでください。誤って設定を保存してしまった場合は、本製品の背面にある[リセット]ボタンを長押しして、出荷時の設定に戻して再度本製品の設定をやり直してください。

補足

設定をHTML形式で保存する／HTML形式で保存したファイルを読み込む

設定をHTML形式で保存するには、設定メンテナンス画面を表示した状態で、ブラウザの[ファイル]－[名前を付けて保存]で保存します。
保存したHTMLファイルから設定を復元したい場合は、保存したHTMLファイルをダブルクリックしてブラウザで開き、[設定]をクリックします。(ただし、設定メンテナンス画面をHTML保存した後に、本製品のLAN側IPアドレスが変更されていた場合は、HTMLファイルから設定を復元することはできません。)
保存したファイルの読み込みが完了すると、自動的に再起動のページが表示されますので、[再起動]をクリックして本製品を再起動してください。

設定をテキスト形式で保存する／テキスト形式で保存したファイルを読み込む

設定をテキスト形式で保存するには、設定メンテナンス画面に表示された設定情報をコピーし、メモ帳などにペーストしてテキストファイルとして保存します。
保存したテキストファイルから設定を復元したい場合は、設定メンテナンス画面を表示し、保存したテキストファイルから設定情報をコピーして、設定メンテナンス画面にペーストし、[設定]をクリックします。
保存したファイルの読み込みが完了すると、自動的に再起動のページが表示されますので、[再起動]をクリックして本製品を再起動してください。

表示方法

1. **[管理コマンド・設定]→[設定メンテナンス]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[管理コマンド・設定]→[設定メンテナンス]をクリックしても同様の画面が表示されます。

設定画面の説明

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動]をクリックして本製品を再起動します。再起動を開始すると、[状態]ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態]ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。
入力欄	現在の設定がコマンド形式で表示されます。必要に応じて設定を変更することができます。コマンドによる設定方法については、『コマンド一覧』を参照してください。

6-3. 切断／接続状況

6-3-1. PPTP

手動でPPTP回線を切断します。また、PPTP回線の接続状況を確認することができます。
本製品ではPPTPを最大2回線同時に接続することができます。

表示方法

1. [切断／接続状況]→[PPTP]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[切断／接続状況]→[PPTP]をクリックしても同様の画面が表示されます。

設定画面の説明

1. 切断(PPTP)：PPTPチャンネルの切断を操作します。

2. 接続状況(PPTP)：PPTPチャンネルの接続状況を表示します。

1. 切断(PPTP)　　：PPTPチャンネルの切断を操作します。

項目	説明
切断するチャンネル	切断するPPTPチャンネルを選択します。
[切断]	クリックすると[切断するチャンネル]で選択したPPTPチャンネルを切断します。

2. 接続状況(PPTP)　　：PPTPチャンネルの接続状況を表示します。

項目	説明
接続状況	チャンネルが接続中であるか空きになっているかを表示します。
接続時刻	接続を開始した時刻を表示します。
接続モード	相手先と接続しているモードを表示します。「端末型」か「LAN型」いずれかを表示します。
リンクプロトコル	接続に使用されているプロトコルを表示します。
相手先ルータアドレス	相手先のルータのIPアドレスを表示します。
相手先DNSサーバアドレス	相手先のDNSサーバアドレスを表示します。
無通信時間／自動切断時間(秒)	通信されていない時間と、自動切断するまでの時間を秒単位で表示します。
経過時間／最大接続時間(分)	接続を開始してから経過した時間と、設定されている最大接続時間を分単位で表示します。
割り当てIPアドレス	端末型接続時に割り当てられるグローバルIPアドレスを表示します。

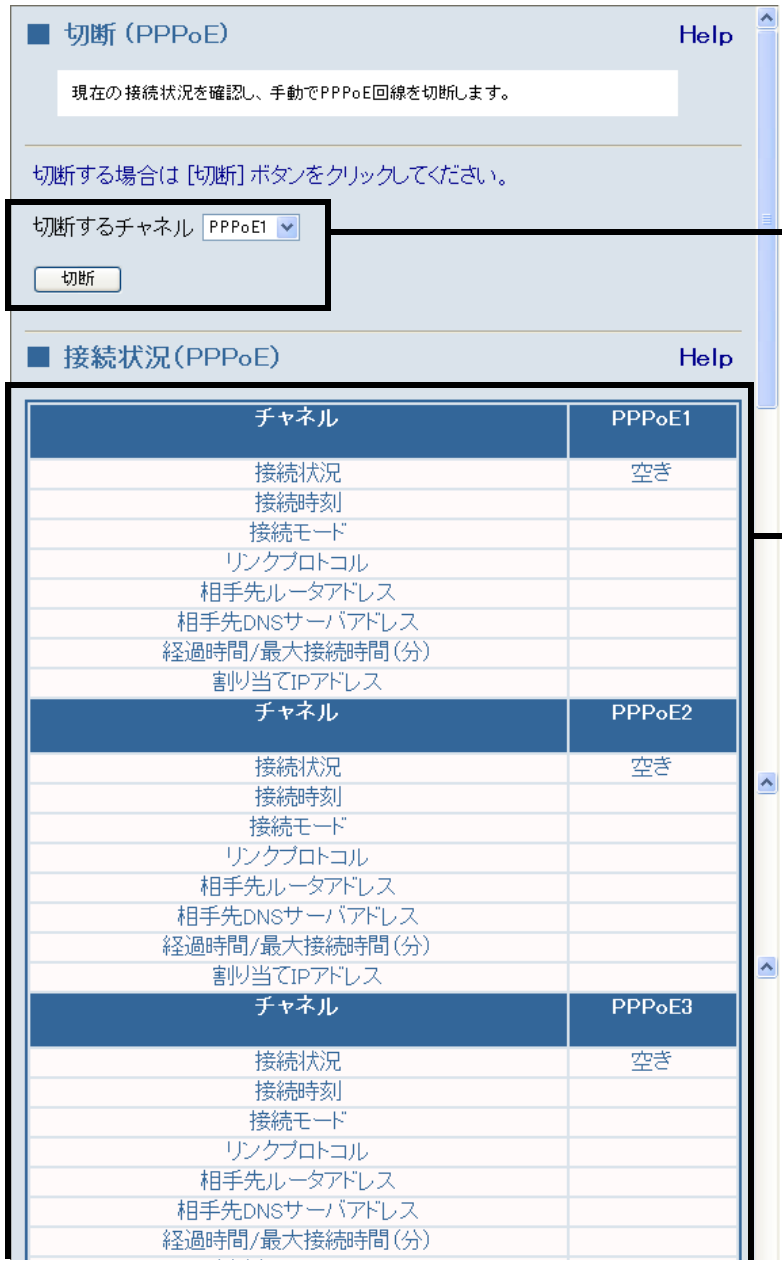
6-3-2. PPPoE

手動でPPPoE回線を切断します。また、PPPoE回線の接続状況を確認することができます。
本製品ではPPPoEを最大4回線同時に接続することができます。

表示方法

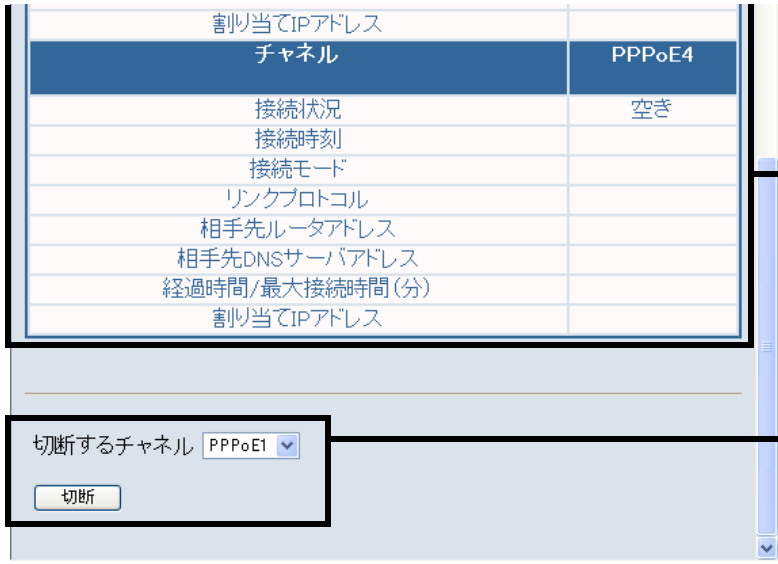
1. [切断／接続状況]→[PPPoE]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[切断／接続状況]→[PPPoE]をクリックしても同様の画面が表示されます。

設定画面の説明



1. 切断（PPPoE）：PPPoEチャンネルの切断を操作します。

2. 接続状況（PPPoE）：PPPoEチャンネルの接続状況を表示します。



1. 切断(PPPoE)　　：PPPoEチャンネルの切断を操作します。

項目	説明
切断するチャンネル	切断するPPPoEチャンネルを選択します。
[切断]	クリックすると[切断するチャンネル]で選択したPPPoEチャンネルを切断します。

2. 接続状況(PPPoE)　　：PPPoEチャンネルの接続状況を表示します。

項目	説明
接続状況	チャンネルが接続中であるか空きになっているかを表示します。
接続時刻	接続を開始した時刻を表示します。
接続モード	相手先と接続しているモードを表示します。「端末型」か「LAN型」いずれかを表示します。
リンクプロトコル	接続に使用されているプロトコルを表示します。
相手先ルータアドレス	相手先のルータのIPアドレスを表示します。
相手先DNSサーバアドレス	相手先のDNSサーバアドレスを表示します。
無通信時間／自動切断時間(秒)	通信されていない時間と、自動切断するまでの時間を秒単位で表示します。
経過時間／最大接続時間(分)	接続を開始してから経過した時間と、設定されている最大接続時間を分単位で表示します。
割り当てIPアドレス	端末型接続時に割り当てられるグローバルIPアドレスを表示します。

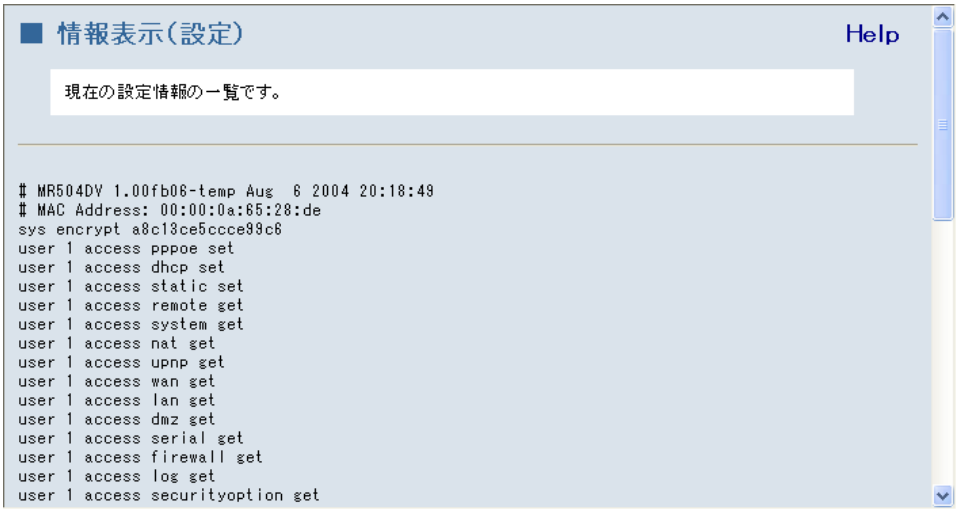
6-4. 情報表示

6-4-1. 設定

設定情報を表示します。

表示方法

1. [情報表示]→[設定]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[設定]をクリックしても同様の画面が表示されます。

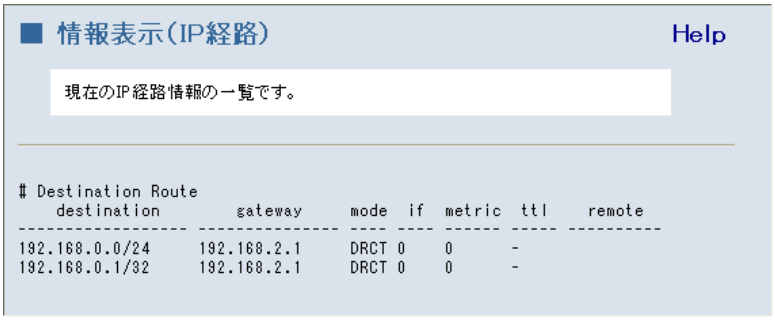


6-4-2. IP経路

現在のIP経路情報を表示します。

表示方法

1. [情報表示]→[IP経路]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[IP経路]をクリックしても同様の画面が表示されます。



6-4-3. ログ

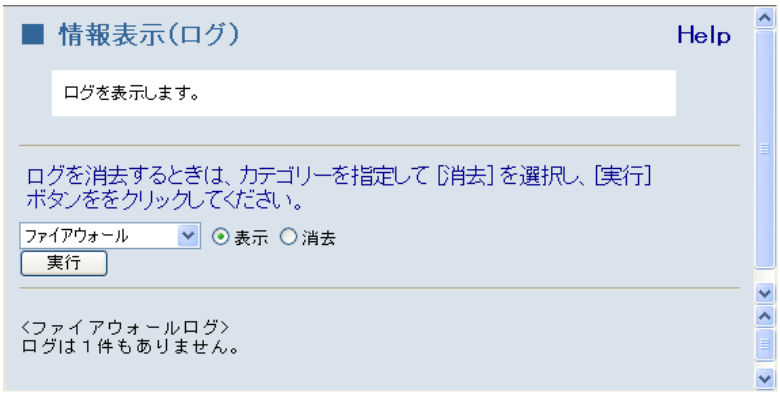
ログの表示および消去を操作します。以下のログを表示または消去することができます。

- DoS攻撃防御
- ファイアウォール
- インターネットアクセス
- アクセスコントロール
- VPN
- 全て

表示方法

1. **[情報表示]→[ログ]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[ログ]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
ドロップダウンメニュー	表示または消去したいログのカテゴリーを選択します。「全て」を選択すると、全てのログを表示または消去することができます。
表示／消去	ドロップダウンメニューで選択したカテゴリーのログを表示するか、消去するかを選択します。
[実行]	[表示]を選択した場合は、ドロップダウンメニューで選択したカテゴリーのログを画面下に表示します。 [消去]を選択した場合は、ドロップダウンメニューで選択したカテゴリーのログを消去します。

6-4-4. WAN状況

現在のWANの接続状況を表示します。

表示方法

1. [情報表示]→[WAN状況]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[WAN状況]をクリックしても同様の画面が表示されます。

設定画面の説明

項目	説明
MACアドレス	WANポートのMACアドレスを表示します。
IPアドレス	接続時に割り当てられるWANポートのIPアドレスを表示します。
サブネットマスク	接続時に割り当てられるサブネットマスクを表示します。
デフォルトゲート	接続時に割り当てられるゲートウェイのIPアドレスを表示します。
DNSサーバアドレス	接続時に割り当てられるDNSサーバのIPアドレスを表示します。
ドメイン名	接続時に割り当てられるドメイン名が表示されます。

補足

- 表示されるのは[IPアドレス取得]または[固定IPアドレス]に設定している場合です。[PPPoE]で設定している場合、画面下の「PPPoEの接続状況はこちらで見ることができます。」にて確認できます。

6-4-5. UPnP状況

UPnPの設定情報やMessengerなどによる通信で要求されたポートマッピングの情報を確認できます。また、ポートマッピングの情報を消去することができます。

補足

- 本製品の電源を入れ直した場合や本製品を再起動した場合は、ポートマッピング情報は自動的に消去されます。

表示方法

1. [情報表示]→[UPnP状況]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[UPnP状況]をクリックしても同様の画面が表示されます。

設定画面の説明

項目	説明
[消去]	クリックすると、ポートマッピング情報を消去します。
UPnP機能	UPnP機能がON/OFFを表示します。
自動削除設定	UPnPのNAT情報を自動的に削除する時間を表示します。「自動削除しない」が表示されている場合は、NAT情報の自動的削除機能は無効になっていることを示します。自動的削除機能の設定は、詳細設定画面の[UPnP設定]で設定できます。→『7-8.UPnP設定』(P.134)
ポートマッピングテーブル	Messengerなどによる通信で要求されたポートマッピング情報を表示します。[消去]をクリックした場合、本製品の電源を入れ直した場合、または本製品を再起動した場合は、情報をすべて消去します。

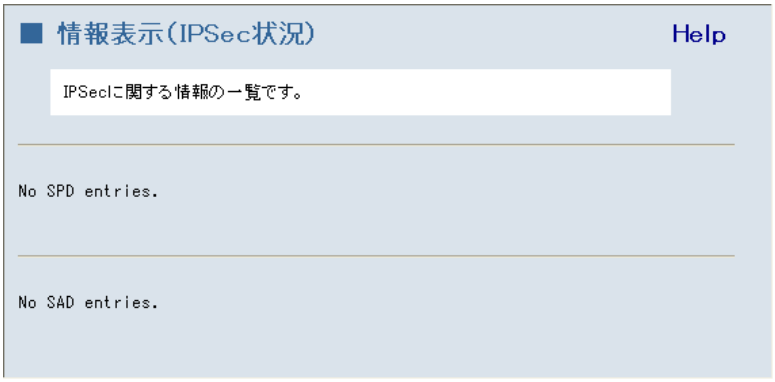
6-4-6. IPSec状況

IPSecに関する情報を表示します。

表示方法

1. [情報表示]→[IPSec状況]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[IPSec状況]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
SPDエントリ	画面上段には、SPD(Security Policy Database)エントリの情報を表示します。現在登録しているIPSecポリシーで有効になっている情報を表示します。
SADエントリ	画面下段には、SAD(Security Association Database)エントリの情報を表示します。現在実際に使用しているIPSecSA情報を表示します。

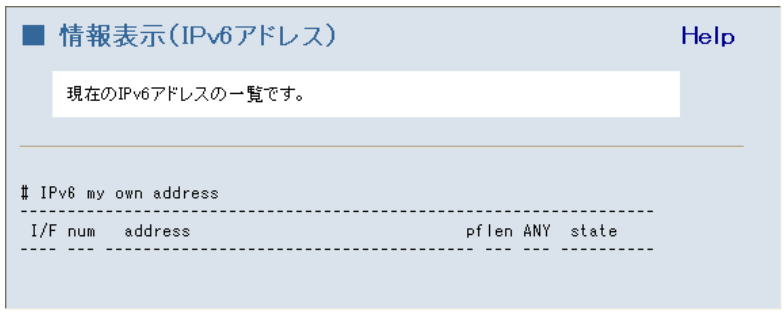
6-4-7. IPv6アドレス

IPv6アドレスの一覧を表示します。

表示方法

1. [情報表示]→[IPv6アドレス]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[IPv6アドレス]をクリックしても同様の画面が表示されます。

設定画面の説明



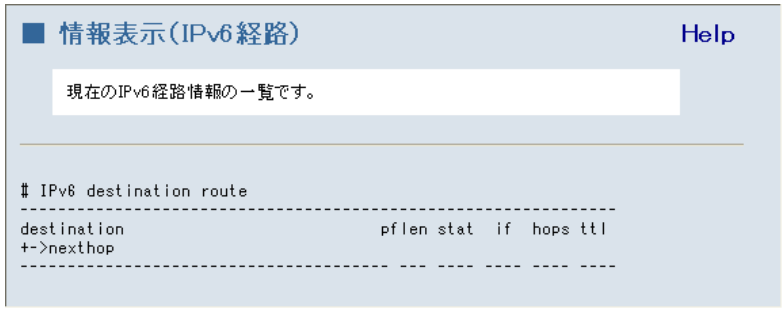
6-4-8. IPv6経路

現在のIPv6経路情報を表示します。

表示方法

1. [情報表示]→[IPv6経路]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[IPv6経路]をクリックしても同様の画面が表示されます。

設定画面の説明



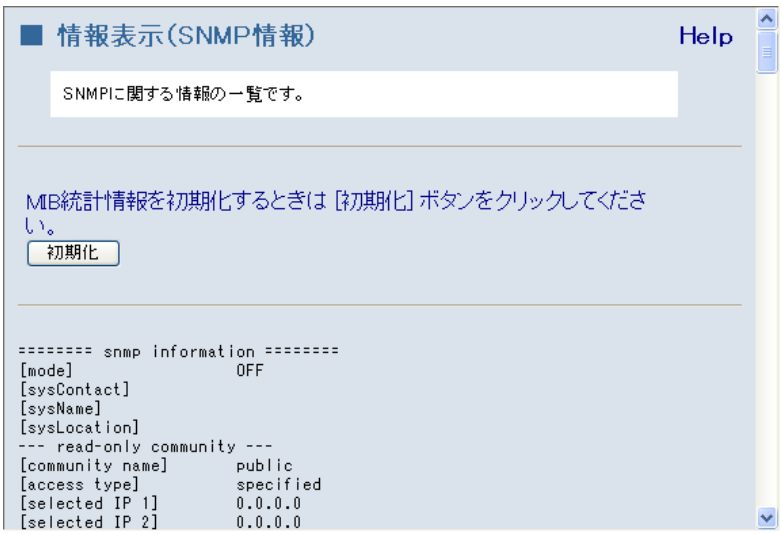
6-4-9. SNMP情報

SNMPに関する情報を表示します。

表示方法

1. [情報表示]→[SNMP情報]の順にクリックします。
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[情報表示]→[SNMP情報]をクリックしても同様の画面が表示されます。

設定画面の説明



項目	説明
[初期化]	クリックすると、MIB統計上を初期化し出荷時の設定に戻します。
SNMP情報	SNMP情報およびMIB情報を表示します。

6-5. その他

6-5-1. オンラインヘルプ

オンラインヘルプを表示します。

補足

- 各設定ページにある[Help]をクリックしても、オンラインヘルプを表示することができます。

表示方法

1. **[その他]→[オンラインヘルプ]の順にクリックします。**
   - 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
   - 詳細設定画面の[その他]→[オンラインヘルプ]をクリックしてもオンラインヘルプを表示することができます。

7. 詳細設定

さらに詳しい設定をしたい場合は、詳細設定画面にて設定を行います。

詳細設定画面には、以下のメニューがあります。設定したいメニューをクリックすると各設定画面が表示されるので、必要に応じて設定を行ってください。

メニュー		説明	参照ページ
接続／相手先登録		相手先の登録や接続、消去を操作します。また、PPTP接続方式の相手先を登録したい場合もこのメニューから相手先の登録を行います。	P.66
本体設定		本体名称や時間設定、およびNTPサーバを設定します。	P.74
ルータ設定			
	WAN	WANポート情報を設定を行います。	P.76
	LAN	LANポートの設定を行います。	P.79
	DMZ	DMZポートの設定を行います。	P.83
	コンソールポート	この機能は本装置では対応していません。	-
セキュリティ設定			
	ファイアウォール	ファイアウォールを設定します。	P.84
	ログ	ログの出力レベルや取得オプション、SYSLOGサーバの転送オプションを設定します。	P.88
	セキュリティオプション	VPNパススルーやステルスモード、SPIを設定します。	P.90
	インターネットアクセス制御	インターネットへのアクセス制御を設定します。	P.93
	アプリケーション	アプリケーションの登録・編集・消去を操作します。	P.96
	スケジュール	スケジュールの登録を行います。	P.98
	MACアドレスフィルタ	MACアドレスフィルタを設定します。	P.100
	URLフィルタ	URLフィルタを設定します	P.102
	証明書(https)	HTTPS用の証明書をインストールします。	P.104
VPN(IPSec)設定			
	VPNポリシー	VPNポリシーを設定します。	P.108
	証明書(IPSec)	IPSec用の証明書をインストールします。	P.121

メニュー		説明	参照ページ
IPv6設定			
	共通	インターフェースを除くIPv6パラメータを設定します。	P.124
	インターフェース	IPv6で使用するインターフェースを設定します。	P.126
	6to4	6to4リレールータを設定します。	P.130
NAT設定		NATアドレスマッピングを設定します。	P.131
UPnP設定		UPnPを設定します。	P.134
ダイナミックDNS設定		DDNSを設定します。	P.135
SNMP設定		SNMPを設定します。	P.136
管理コマンド・設定			
	再起動	ルータを再起動します。	P.139
	設定の消去	ルータの設定を各項目別にリセットすることができます。	P.139
	ユーザ・パスワード変更	ルータ設定画面を表示するためのユーザID・パスワードを設定します。	P.140
	アクセス制御	ルータ設定画面のアクセス権限を設定します。	P.140
	ファームウェア更新	ルータのファームウェアを更新します。	P.141
	設定メンテナンス	設定ファイルを直接編集して、ルータの設定を変更したり、設定情報をファイルに保存できます。	P.141
切断／接続状況			
	PPTP	PPTP回線の切断を操作します。また、接続状況を表示することができます。	P.143
	PPPoE	PPPoE回線の切断を操作します。また、接続状況を表示することができます。	P.143
情報表示			
	設定	設定情報を表示します。	P.144
	IP経路	IP経路情報を表示します。	P.144
	ログ	ログを表示または消去します。	P.145
	WAN状況	WANの設定状況を表示します。	P.145
	UPnP状況	UPnPの設定状況を表示します。	P.146
	IPSec状況	IPSecの設定状況を表示します。	P.146
	IPv6アドレス	IPv6アドレスの一覧を表示します。	P.147
	IPv6経路	IPv6経路情報を表示します。	P.147
	SNMP情報	SNMP情報を表示します。	P.147

メニュー	説明	参照ページ
その他		
オンラインヘルプ	オンラインヘルプを表示します。	P.148

7-1. 接続／相手先登録

詳しい相手先の情報を登録または登録内容の変更をしたい場合、登録された相手先への手動接続や消去を操作したい場合は、このページで行います。また、PPTP接続方式の相手先を登録したい場合も、このページで登録を行います。相手先の登録は、最大16個まで登録できます。

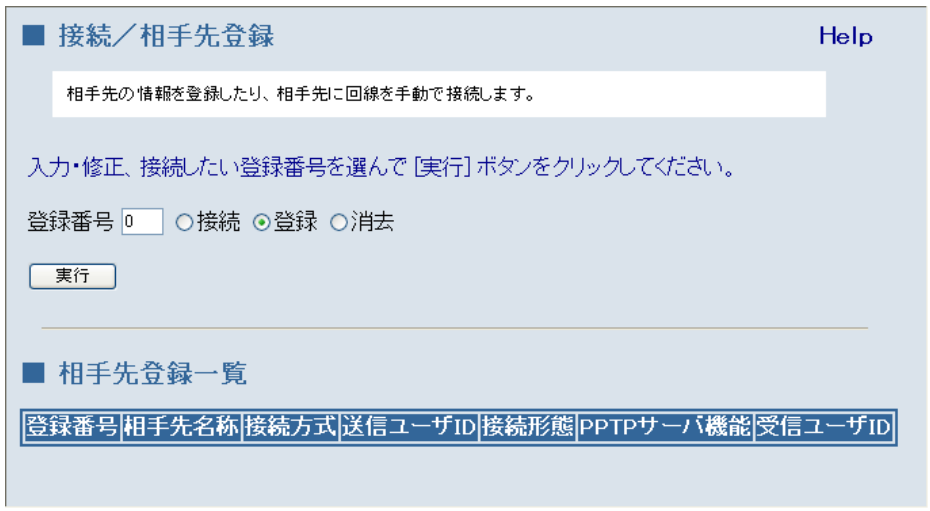
補足

- PPPoE 接続方式の相手先を詳細な設定を省いて簡単に設定したい場合は、クイック設定画面の［ブロードバンドで接続］→［PPPoE］の設定で相手先の登録を行ってください。→『6-1-1.PPPoE』（P.25）

表示方法

1. ［→詳細設定へ］をクリックして詳細設定画面を表示し、［接続／相手先登録］をクリックします。

設定画面の説明

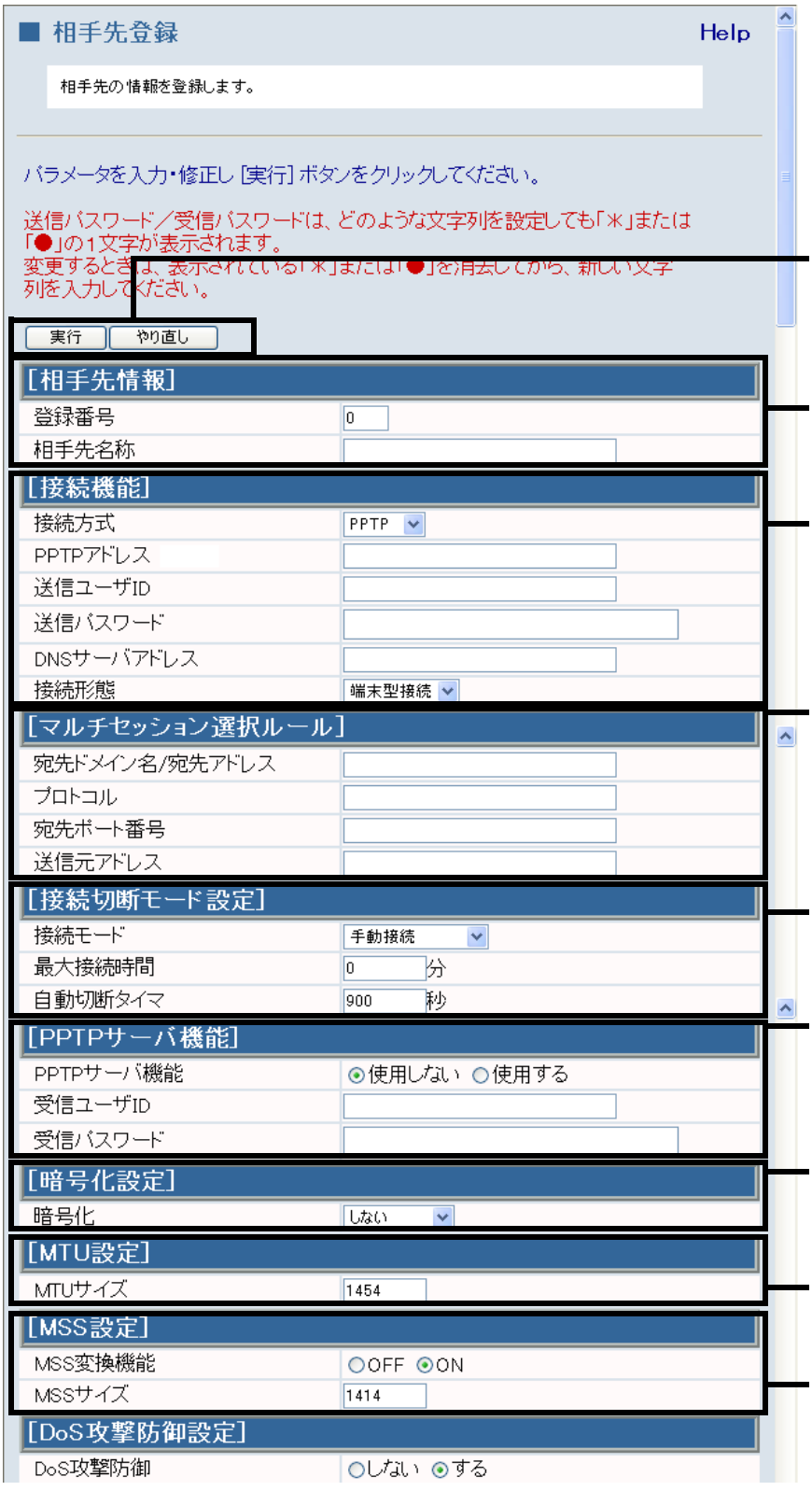


項目	説明
登録番号	接続、登録、または消去したい相手先の登録番号を入力します。0～15まで登録できます。
接続／登録／消去	● ［登録番号］欄に入力した相手先に手動接続する場合は［接続］を選択します。 ● ［登録番号］欄に入力した番号で相手先を登録したい場合、または［登録番号］欄に入力した相手先の設定情報を変更したい場合は、［登録］を選択します。 ● ［登録番号］欄に入力した相手先の設定情報を消去したい場合は［消去］を選択します。
［実行］	［登録番号］欄に入力した相手先の接続、登録、または消去を実行します。［登録］を選択し［実行］をクリックした場合は、相手先登録画面が表示されます。相手先登録画面の設定方法については、『7-1-1.相手先登録』（P.67）を参照してください。
相手先登録一覧	現在登録されている相手先一覧を表示します。

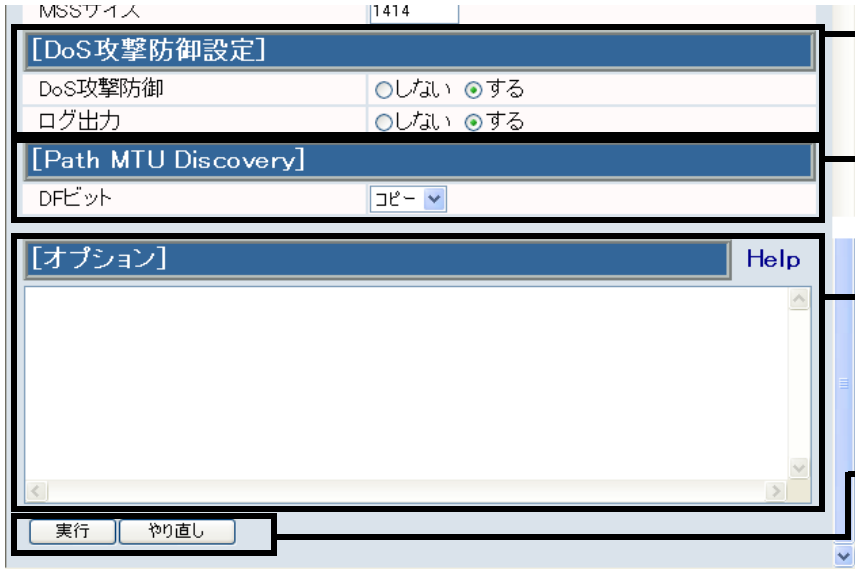
7-1-1. 相手先登録

接続／相手先登録画面で[登録]を選択し[実行]をクリックすると、相手先登録画面が表示されます。相手先登録画面では、詳しい相手先情報を設定することができます。

設定画面の説明



1. 実行／やり直し：各設定項目で変更した内容を保存または破棄します。(P.68)
2. 相手先情報：相手先の登録番号および名称を設定します。(P.68)
3. 接続機能：接続方式や、プロバイダから指示された情報を入力します。(P.68)
4. マルチセッション選択ルール：接続条件により接続する相手先を使い分けたい場合には、マルチセッション選択ルールを設定します。(P.70)
5. 接続切断モード設定：接続切断モードを設定します。(P.71)
6. PPTPサーバ機能：PPTPサーバ機能を使用する場合に設定します。(P.72)
7. 暗号化設定：PPTP通信のデータを暗号化するかどうかを設定します。(P.72)
8. MTU設定：送信可能なデータの最大値を設定します。(P.72)
9. MSS設定：PPPoE接続時に、MSS変換を使用するかどうかを設定します。(P.72)



10. DoS攻撃防御設定：DoS攻撃防御設定を使用するかどうかを設定します。(P.73)
11. Path MTU Discovery：Path MTU DiscoveryのDFビットモードを設定します。(P.73)
12. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。(P.73)
1. 実行／やり直し：各設定項目で変更した内容を保存または破棄します。(P.68)

1. 実行／やり直し　：　各設定項目で変更した内容を保存または破棄します。

項目	説明
[実行]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[実行]をクリックして有効になった内容はクリアされません。

2. 相手先情報　：　相手先の登録番号および名称を設定します。

項目	説明
登録番号	登録番号を入力します。あらかじめ、接続／相手先登録画面の[登録番号]欄で入力した登録番号が表示されているので、変更する必要はありません。ただし、設定した登録番号とは別の登録番号で登録したい場合は、登録番号を変更します。0～15まで入力できます。
相手先名称	設定した相手先がどこであるかを特定するための名称を入力します。漢字、ひらがな、英数字を使って、任意の名称を入力できます。

3. 接続機能　：　接続方式や、プロバイダから指示された情報を入力します。

項目	説明
接続方式	PPPoEを利用した相手先を登録する場合は「PPPoE」を選択します。 PPTPを利用した相手先を登録する場合は「PPTP」を選択します。
PPTPアドレス	[接続方式]欄で[PPTP]を選択した場合に、PPTPサーバのIPアドレスを入力します。 [接続方式]欄で[PPPoE]を選択した場合は、入力する必要はありません。
送信ユーザID	プロバイダから指定されたユーザID(アカウント／ログインID／認証IDともいう)を入力します。 例：taro@omron.co.jp 送信ユーザIDは@を含むドメインネームをすべて入力してください。 大文字・小文字を間違えないように入力してください。

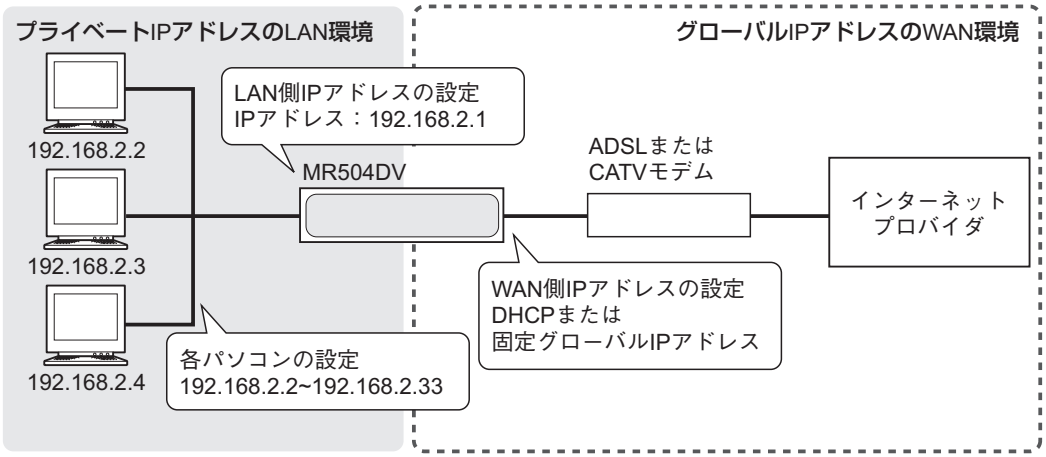
項目	説明
送信パスワード	プロバイダから指定されたパスワード(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk 大文字・小文字を間違えないように入力してください。 入力時「●」または「＊」で表示されます。設定後は1文字で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。
接続形態	LAN側に接続されたパソコンではプライベートIPアドレスを使用しWAN側のIPアドレスにのみグローバルIPアドレスを利用する場合は[端末型接続]を選択します。 LAN側に接続されたパソコンにもグローバルIPアドレスを使用する場合は、[LAN型接続]を選択します。

補足

端末型接続とLAN型接続について

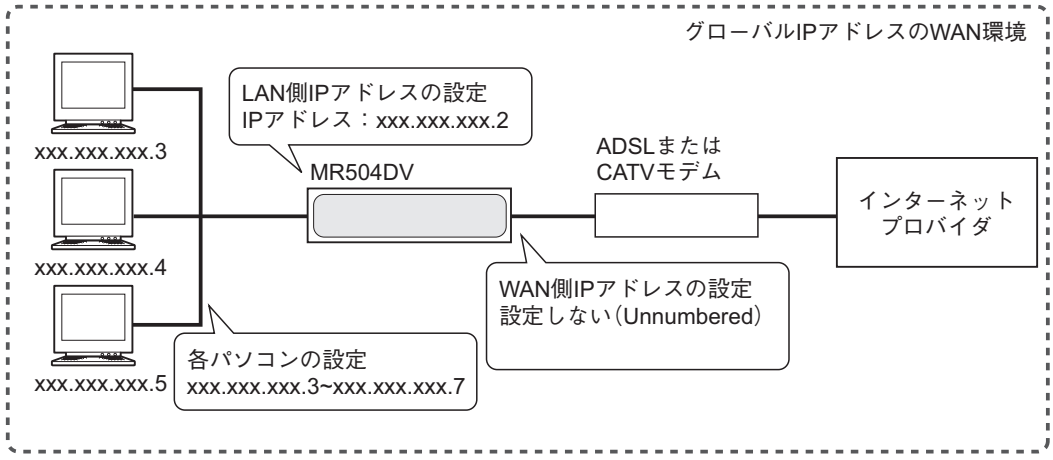
端末型接続を利用するか、LAN型接続を利用するかは、プロバイダから複数のグローバルIPアドレスを割り当てられているかいないかによって決まります。

端末型接続の例



プロバイダから割り当てられるグローバルIPアドレスが1つのみの場合は、端末型接続を選択します。この場合、LAN側のパソコンにはプライベートIPアドレスを割り当てます。それぞれのパソコンは、本製品WAN側に設定されたグローバルIPアドレスを使用し、インターネットに接続することができます。本製品は、あらかじめプライベートIPアドレスをLAN側に接続したパソコンに割り当てるように設定しているため、LAN側の設定を変更する必要はありません。ただし、既存のLAN環境で使用しているプライベートIPアドレスがある場合は、本製品LAN側のIPアドレスの設定を変更する必要があります。

LAN型接続の例（アンナンバード）



IP8/IP16サービスなど、プロバイダから複数のグローバルIPアドレスが割り当てられている場合は、LAN型接続を選択します。LAN型接続では、通常、本製品WAN側のIPアドレスは設定せずにLAN側のIPアドレスを設定します（アンナンバード設定）。
例えば、IP8サービスの場合は、プロバイダから8つのグローバルIPアドレスが割り当てられます。この場合、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、最初と最後のグローバルIPアドレスは使用できないため、本製品LAN側には2番目のグローバルIPアドレスを、LAN側に接続されたパソコンには3番目から7番目までのグローバルIPアドレスを使用します。
IP8やIP16サービスをご利用の場合のLAN設定については、『7-3-2.LAN』（P.79）を参照してください。

4. マルチセッション選択ルール ： 接続条件により接続する相手先を使い分けたい場合には、マルチセッション選択ルールを設定します。

項目	説明
宛先ドメイン名／宛先アドレス	接続する宛先ドメイン名（ただし「http://」およびディレクトリは除く）またはIPアドレスを入力して、マルチセッション選択ルールを設定します。複数のドメイン名またはアドレスを指定したい場合は、カンマ（ , ）で区切って入力します。登録できるアドレスは最大4個です。ただし、この項目欄ではドメイン名とアドレスを併用して設定することはできません。ドメイン名とアドレスを併用して設定したい場合は、[オプション]欄で設定します。 指定したドメイン名またはURLアドレスにLAN側のパソコンからアクセス要求が送られてきた場合に、この相手先を使用してインターネットにアクセスするようになります。
プロトコル	通信に使用するプロトコルを入力して、マルチセッション選択ルールを設定します。ニーモニック（esp, gre, icmp, ipencap, tcp, udp）またはプロトコル番号で入力します。例えば、Webにアクセスするときに使用する相手先に設定する場合は、「tcp」と入力します。 空欄または「＊」を入力した場合は、すべてのプロトコルが対象となります。「＊」を入力して設定した場合は、再登録時には空欄で表示されます。
宛先ポート番号	通信に使用するポート番号を入力して、マルチセッション選択ルールを設定します。ニーモニックまたはポート番号で入力します。例えば、Webにアクセスするときに使用する相手先に設定する場合は、「80」と入力します。空欄または「＊」を入力した場合は、すべてのポート番号が対象となります。「＊」を入力して設定した場合は、再登録時には空欄で表示されます。

項目	説明
送信元アドレス	この接続を利用するパソコンのローカルIPアドレスを入力して、マルチセッション選択ルールを設定します。IPアドレスの範囲を指定したい場合は、ハイフン(-)で区切って入力します。また、スラッシュ(/)で区切って、サブネットマスク長を指定することもできます。

補足

宛先ドメイン名／宛先アドレスについて

- [宛先ドメイン名／宛先アドレス]欄には、ドメイン名とアドレスを併用して入力することはできません。ドメイン名とアドレスを併用してマルチセッション選択ルールを設定したい場合は、[宛先ドメイン名／宛先アドレス]欄にドメイン名を入力し、アドレスはオプション欄にコマンドで入力します。
- IPアドレスの場合、ハイフンで区切ってアドレスの範囲を指定することもできます。
  例：xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyyy
- 空欄または＊を入力した場合は、すべての宛先が対象となります。

例：ホスト名の指定	接続対象となる宛先
.jp	最後に.jpがつくサイトすべて
.co.jp	最後に.co.jpがつくサイトすべて
.www.omron.co.jp	最後に.www.omron.co.jpがつくサイトすべて (host.www.omron.co.jp, host2.www.omron.co.jpなど。 ただし、www.omron.co.jpは対象外。)
www.omron.co.jp	www.omron.co.jpのみ(先頭に「.」がない場合)

- AutoDNS機能がOFFになっている場合は、宛先とドメイン名を指定しても無効になります。AutoDNS機能をONにしたい場合は、『7-3-2.LAN』(P.79)を参照してください。

補足

マルチセッション選択ルールの設定について

- マルチセッション選択ルールの詳しい説明については、『マルチセッション選択ルールの設定について』(P.33)を参照してください。
- マルチセッション選択ルールを使用して、フレッツ・スクウェアを設定する場合、またはBROBA を設定したい場合は、『フレッツ・スクウェアを設定する場合』（P.34）および『BROBA を設定する場合』（P.34）を参照してください。

5. 接続切断モード設定　　：接続切断モードを設定します。

項目	説明
接続モード	● 常時接続するよう設定する場合は、[常時接続]を選択します。 ● ブラウザでインターネットへアクセスしたときに自動的に接続するよう設定する場合は、[自動接続(メイン)]または[自動接続(サブ)]を選択します。[自動接続(メイン)]を設定した相手先を優先的に使用するようになりますが、マルチセッション選択ルールなどを設定したサブの相手先を自動接続するようにしたい場合は、「自動接続(サブ)]を選択します。 ● 手動接続するよう設定する場合は、[手動接続]を選択します。
最大接続時間	接続を保持する最大の時間を分単位で設定します。通信中であっても、接続してから設定した時間が経過した場合は自動的に接続を切断するようになります。最大接続時間を無効にしたいばあいは「0」を入力します。
自動切断タイマ	一定時間通信が行われなかった場合に、自動的に接続を切断する時間を秒単位で入力します。

6. PPTPサーバ機能　　：PPTPサーバ機能を使用する場合に設定します。

項目	説明
PPTPサーバ機能	PPTP接続において相手先の環境から接続要求があった場合にユーザIDとパスワード認証を行う場合は、[使用する]を選択します。 [使用する]を選択した場合は、[受信ユーザID]および[受信パスワード]を設定します。
受信ユーザID	[PPTPサーバ機能]で[使用する]を選択した場合に、相手先からのPPTP接続を許可するユーザIDを入力します。
受信パスワード	[PPTPサーバ機能]で[使用する]を選択した場合に、相手先からのPPTP接続を許可するパスワードを入力します。

7. 暗号化設定　　：PPTP通信のデータを暗号化するかどうかを設定します。

項目	説明
暗号化	PPTP通信中のデータを暗号化しない場合は、「しない」を選択します。 PPTP通信中のデータを暗号化する場合は、暗号化形式を選択します。 以下の暗号化形式を選択できます。 ● MPPE-40：MPPE（鍵長40bit）でPPTP暗号化通信を行います。 ● MPPE-128：MPPE（鍵長 128bit）で PPTP 暗号化通信を行います。 ● MPPE-any：相手先の設定に従って、MPPE（鍵長40bit）またはMPPE（鍵長128bit）でPPTP暗号化通信を行います。

8. MTU設定　　：送信可能なデータの最大値を設定します。

項目	説明
MTUサイズ	540～1500の範囲で1通信で送信可能なデータの最大値を入力します。MTUサイズは相手先によって通常以下のように設定します。 PPPoE　　：1454 PPPoE以外　：1500

補足

- MTUサイズは[ルータ設定]－[WAN]にて設定することもできます。
  [ルータ設定]－[WAN]で設定したMTUサイズは、WANポートの初期設定値となります。
  [ルータ設定]－[WAN]で設定したMTUサイズより大きいMTUサイズを相手先登録にて設定した場合は、[ルータ設定]－[WAN]で設定したMTUサイズを適用します。

9. MSS設定　　：PPPoE接続時に、MSS変換を使用するかどうかを設定します。

項目	説明
MSS変換機能	MSS変換機能をONにするかOFFにするかを選択します。 MSS変換機能をONにした場合、TCPによる通信で受信可能なセグメントサイズの最大値を変更することができます。MSS値を変更しないと利用できないネットワークゲームやサーバと通信したい場合は、MMS変換機能をONにします。ONにした場合は、[MSSサイズ]欄でMSSの最大値を入力します。

項目	説明
MSSサイズ	MSS変換機能をONにした場合に、通信可能なMSS最大値を入力します。MSSサイズは、MTUサイズから-40した値より大きいサイズを指定することはできません。(MSSサイズ< MTUサイズ-40) 例えば、MTUサイズが「1454」だった場合、MSSサイズに指定できる最大値は「1414」になります。

10. DoS攻撃防御設定　：DoS攻撃防御設定を使用するかどうかを設定します。

項目	説明
DoS攻撃防御	DoS攻撃防御を使用するかどうかを選択します。
ログ出力	DoS攻撃防御を使用する場合に、DoS攻撃防御ログを出力するかどうかを選択します。

11. Path MTU Discovery　：Path MTU DiscoveryのDFビットモードを設定します。

項目	説明
DFビット	DFビットのモードを設定します。 ● [コピー]を選択すると、DFビットをそのままPPPoEトンネルの外側にコピーします。 ● [クリア]を選択すると、PPPoEトンネルの外側のDFビットを0にします。 ● [セット]を選択すると、PPPoEトンネルの外側のDFビットを1にします。

12. オプション　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
入力欄	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。このオプション欄では以下の設定を入力することができます。 ● IPアドレスネゴシエーション ● DNSサーバアドレスネゴシエーション ● 相手先ルータアドレス ● WAN側IPアドレス ● PPPoEサービス名 ● PPPoEサーバ名 ● LCPエコーチェック ● セッションキープアライブ機能 ● セッションキープアライブ拡張機能 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

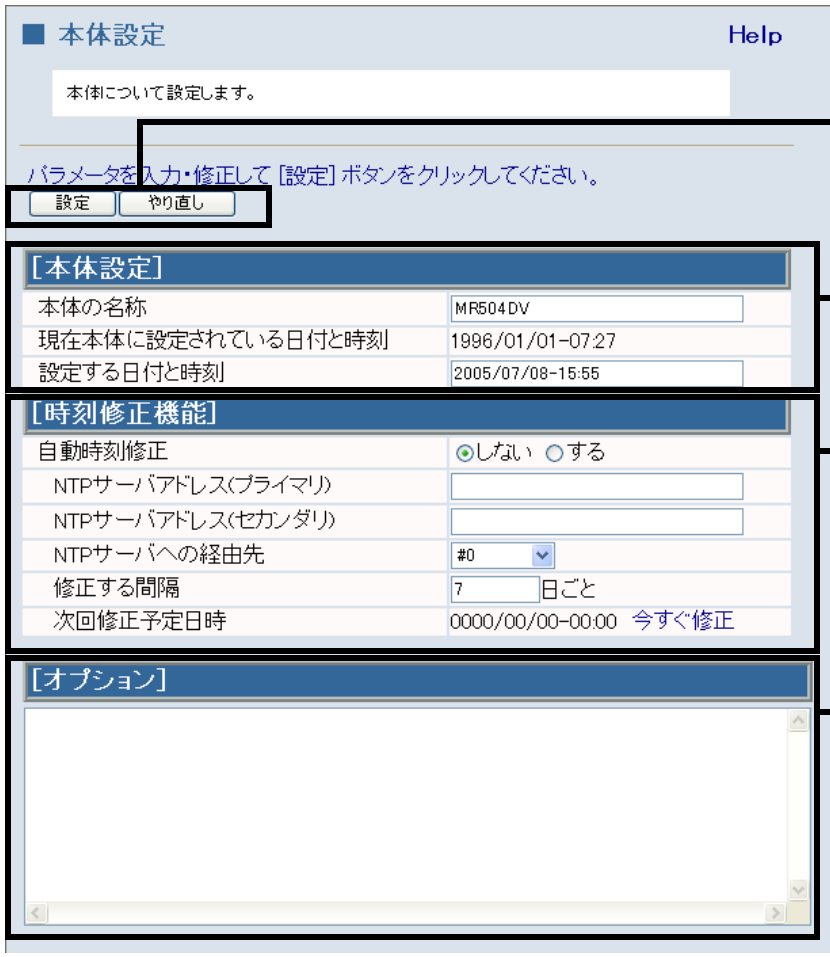
7-2. 本体設定

本体名称や時間設定、NTPサーバの設定を行います。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[本体設定]をクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。
2. 本体設定：本体名称および日付と時刻を設定します。
3. 時刻修正機能：NTPサーバを使った時刻修正機能を設定します。
4. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。

1. 設定／やり直し　　：　各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 本体設定　　：本体名称および日付と時刻を設定します。

項目	説明
本体の名称	本体の名称を入力します。英数字のみ入力可能です。設定した名称は、ルータ設定画面の左側上部に表示されます。
現在本体に設定されている日付と時刻	現在本製品に設定されている日付と時刻を表示します。
設定する日付と時刻	[現在本体に設定されている日付と時刻]が間違っている場合は、この欄に正しい日付と時刻を入力します。入力する日付と時間は、「YYYY/MM/DD-HH:MM」の書式で入力してください。 年　月　日　時　分

3. 時刻修正機能　　：NTPサーバを使った時刻修正機能を設定します。

項目	説明
自動時刻修正	NTPサーバを使用して定期的に日付と時間の修正を行う場合は、[する]を選択します。[する]を選択した場合は、[NTPサーバアドレス(プライマリ)][NTPサーバへの経由先][修正する間隔]を設定してください。
NTPサーバアドレス(プライマリ)	時間修正を問い合わせるNTPサーバのIPアドレスを入力します。
NTPサーバアドレス(セカンダリ)	[NTPサーバアドレス(プライマリ)]に接続できなかった場合に、時間修正を問い合わせるNTPサーバのIPアドレスを入力します。
NTPサーバへの経由先	PPPoE接続を介してインターネット上のNTPサーバに時間修正の問い合わせをする場合は、利用するPPPoE相手先の登録番号を選択します。 PPPoEを使用していないプロバイダを介してインターネット上のNTPサーバに時間修正の問い合わせをする場合、またはLAN内のNTPサーバに時間修正の問い合わせをする場合は、[Ethernet]を選択します。
修正する間隔	NTPサーバに時間修正を問い合わせる間隔を日数で入力します。
次回修正予定日時	次回NTPサーバに時間修正の問い合わせる日時を表示します。今すぐ時間修正の問い合わせたい場合は、[今すぐ修正]をクリックします。

4. オプション　　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
入力欄	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

7-3. ルータ設定

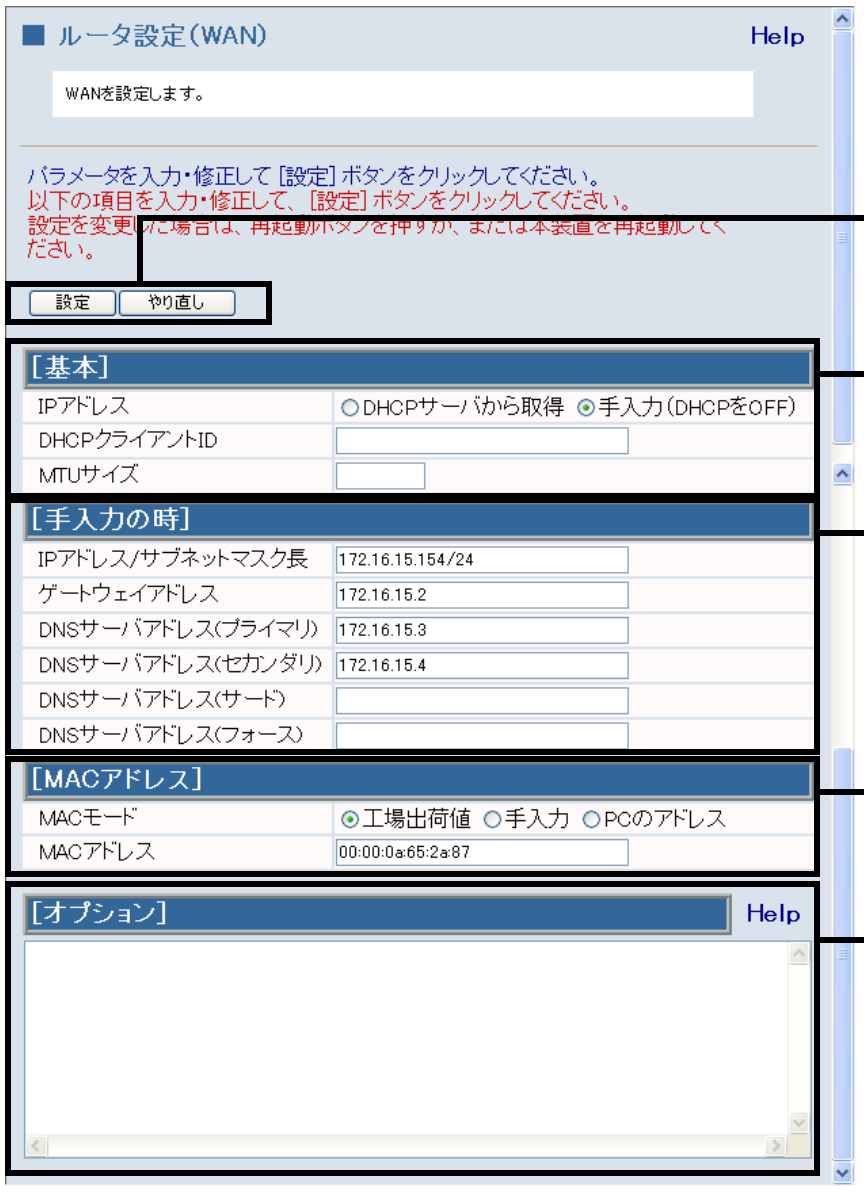
7-3-1. WAN

WANを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[ルータ設定]→[WAN]の順にクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。
2. 基本：WANのIPアドレスをDHCPを使って割り当てる場合に設定します。
3. 手入力の時：WANのIPアドレスをプロバイダから指示された固定IPアドレスで割り当てる場合に設定します。
4. MACアドレス：本製品のMACアドレスを変更する必要がある場合に設定します。
5. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。

1. 設定／やり直し　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動] をクリックして本製品を再起動します。再起動を開始すると、[状態] ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態] ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度 [設定] をクリックして有効になった内容はクリアされません。

2. 基本　：WANのIPアドレスをDHCPを使って割り当てる場合に設定します。

項目	説明
IPアドレス	WAN側のIPアドレスをプロバイダのDHCPから取得するか、固定グローバルIPアドレスを入力するかを選択します。 プロバイダからIPアドレスの指定がない場合は、[DHCPサーバから取得] を選択します。 プロバイダから固定のグローバルIPアドレスが指定されている場合は、[手入力(DHCPをOFF)] を選択します。
DHCPクライアントID	IPアドレスをプロバイダのDHCPから取得する場合に、プロバイダからDHCPクライアントID(ホスト名)の指定がある場合は、そのIDを入力します。指定されていない場合は、空欄のままにしてください。
MTUサイズ	540～1500の範囲で1通信で送信可能なデータの最大値を入力します。 本製品では初期設定として1500 byteのMTUサイズが設定されています。1500 byteでは通信できない場合は、この欄にMTUサイズを入力します。 また、MTUサイズは相手先ごとに設定することもできます。相手先ごとにMTUサイズを指定したい場合は、この欄は空欄のままにし、相手先登録にてMTUサイズを指定します。この欄でMTUサイズを指定した場合、指定したサイズ以上のMTUサイズを相手先登録にて設定しても、この欄で設定したMTUサイズを適用します。

3. 手入力の時　：WANのIPアドレスをプロバイダから指示された固定IPアドレスで割り当てる場合に設定します。

項目	説明
IPアドレス／サブネットマスク長	[IPアドレス] 欄で [手入力(DHCPをOFF)] を選択した場合は、プロバイダから指定されたIPアドレスおよびサブネットマスクを「IPアドレス/サブネットマスク」のフォーマットで入力します。 例:xxx.xxx.xxx.1/255.255.255.0 入力したサブネットマスクは、設定を適用すると、「/24」のような入力したサブネットマスクを示すビット数に変換されます。 「255.255.255.0」などサブネットマスクを入力する代わりに、サブネットマスクを表すビット数を入力することもできます。 例:xxx.xxx.xxx.1/24
ゲートウェイアドレス	プロバイダから指定されたゲートウェイ(ゲートウェイアドレス、デフォルトゲートウェイともいう)がある場合に、指定されたゲートウェイを入力します。
DNSサーバアドレス (プライマリ) (セカンダリ) (サード) (フォース)	プロバイダから指定されたそれぞれ(プライマリ、セカンダリ、サード、フォース)のDNSサーバアドレスがある場合に、指定されたDNSサーバアドレスをそれぞれ入力します。

4. MACアドレス　　：本製品のMACアドレスを変更する必要がある場合に設定します。

項目	説明
MACモード	本製品のMACアドレスの設定方法を選択します。 ● 本製品に初期値として割り当てられたMACアドレスを使用する場合は、[工場出荷値]を選択します。プロバイダからMACアドレスの指定がない場合は、[工場出荷値]を選択してください。 ● プロバイダから指定された MAC アドレスがある場合は、[手入力]を選択します。この場合は、[MACアドレス]欄にて指定されたMACアドレスを入力します。 ● 以前パソコンを直接CATVモデムなどに接続し、パソコンのMACアドレスでプロバイダへの接続認証を行っていた場合は、[PCのアドレス]を選択します。[PCのアドレス]を選択した場合は、設定の変更を操作したパソコンのMACアドレスをルータのMACアドレスとして設定します。
MACアドレス	[MACモード]で[手入力]を選択した場合に、本機に設定するMACアドレスを入力します。それ以外の場合は、変更しないでください。

5. オプション　　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
オプション	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。このオプション欄では以下の設定を入力することができます。 ● LAN型接続モード設定 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

7-3-2. LAN

LANを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[ルータ設定]→[LAN]の順にクリックします。

設定画面の説明

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.80)
2. 基本：LAN側の基本設定を行います。(P.80)
3. DHCPサーバ：本製品をDHCPサーバとして使用する場合に設定します。(P.80)
4. AutoDNS：接続したプロバイダごとのDNSサーバアドレスを自動的に検出するようにしたい場合に設定します。(P.81)
5. リモートアクセスサーバ：本製品にPPTPにて遠隔地からアクセスできるように設定します。(P.81)
6. Path MTU Discovery：Path MTU Discovery機能を設定します。(P.82)
7. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。(P.82)

1. 設定／やり直し　　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動] をクリックして本製品を再起動します。再起動を開始すると、[状態] ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態] ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度 [設定] をクリックして有効になった内容はクリアされません。

2. 基本　　：LAN側の基本設定を行います。

項目	説明
本体のIPアドレス／ サブネットマスク長	MR504DVのIPアドレスおよびサブネットマスクを「IPアドレス/サブネットマスク」のフォーマットで入力します。アンナンバードを設定する場合は、プロバイダから指定されたIPアドレス(2番目)を入力します。 例：xxx.xxx.xxx.1/255.255.255.0 入力したサブネットマスクは、設定を適用すると、「/24」のような入力したサブネットマスクを示すビット数に変換されます。 「255.255.255.0」などサブネットマスクを入力する代わりに、サブネットマスクを表すビット数を入力することもできます。 例：xxx.xxx.xxx.1/24
ブロードキャストアドレス	● ブロードキャストアドレスが「0」の LAN 上で、すべてのパソコンにパケットを送信する場合は [全て0] を選択します。 ● ブロードキャストアドレスが「1」(10進数で255)のLAN上で、すべてのパソコンにパケットを送信する場合は [全て1] を選択します。 ● ブロードキャストアドレスが「0」の LAN 上で、サブネット内のパソコンのみにパケットを送信する場合は [サブネット+全て0] を選択します。 ● ブロードキャストアドレスが「1」の LAN 上で、サブネット内のパソコンのみにパケットを送信する場合は [サブネット+全て1] を選択します。
RIP送受信モード	● RIP パケットの送受信を行う場合は、[送信と受信を行う] を選択します。 ● RIP パケットの送受信を行わない場合は、[送信も受信も行わない] を選択します。 ● RIP パケットの受信のみ行う場合は、[受信のみ行う] を選択します。 ● RIP パケットの送信のみ行う場合は、[送信のみ行う] を選択します。
MTUサイズ	540～1500の範囲で1パケットで送信可能なデータの最大値を入力します。 本製品では初期設定として1500 byteのMTUサイズが設定されています。1500 byteでは通信できない場合は、この欄にMTUサイズを入力します。

3. DHCPサーバ　　：本製品をDHCPサーバとして使用する場合に設定します。

項目	説明
DHCPサーバ機能	DHCPサーバ機能をONにするかOFFにするかを選択します。

項目	説明
開始IPアドレス／個数	DHCPサーバ機能をONにした場合に、LANに接続されたパソコンにDHCPを使って割り当てるIPアドレスと個数を「IPアドレス/個数」の書式で入力します。 例:192.168.2.2～192.168.2.33を割り当てる場合 192.168.2.2/32
ドメイン名	CATV(ケーブルテレビ)をご契約の場合に、プロバイダからドメイン名の指定がある場合は、指定されたドメイン名を入力します。
リース時間	DHCPサーバ機能によってパソコンに割り当てたIPアドレスの有効期限を時間単位で入力します。ここに入力された時間が経過すると、パソコンに割り当てたIPアドレスを再割付します。
WINSサーバアドレス（プライマリ）	DHCPサーバ機能を使ってパソコンに割り当てるプライマリWINSサーバのIPアドレスを入力します。
WINSサーバアドレス（セカンダリ）	DHCPサーバ機能を使ってパソコンに割り当てるセカンダリWINSサーバのIPアドレスを入力します。

4. AutoDNS　：接続したプロバイダごとのDNSサーバアドレスを自動的に検出するようにしたい場合に設定します。

項目	説明
AutoDNS機能	AutoDNS機能をONにするかOFFにするかを選択します。 AutoDNS機能をONにすると、異なるプロバイダに接続するたびにDNSサーバアドレスを検出することができるようになります。
LAN側DNSサーバアドレス（プライマリ）	● AutoDNS機能をONにしLANにDNSサーバがある場合には、パソコンからドメイン名解決要求を転送するプライマリDNSサーバのIPアドレスを入力します。 ● AutoDNS機能をOFFにしDHCPサーバ機能をONにしている場合は、LAN上またはプロバイダのプライマリDNSサーバのIPアドレスを入力します。
LAN側DNSサーバアドレス（セカンダリ）	● AutoDNS機能をONにしLANにDNSサーバがある場合には、パソコンからドメイン名解決要求を転送するセカンダリDNSサーバのIPアドレスを入力します。 ● AutoDNS機能をOFFにしDHCPサーバ機能をONにしている場合は、LAN上またはプロバイダのセカンダリDNSサーバのIPアドレスを入力します。

5. リモートアクセスサーバ　：本製品にPPTPにて遠隔地からアクセスできるように設定します。

項目	説明
リモートアクセスサーバ機能	リモートアクセスサーバ機能をONにするかOFFにするかを選択します。ONにした場合は、[リモートIPアドレス1]～[リモートIPアドレス2]欄に必要に応じて設定します。
リモートIPアドレス1～2	リモートアクセスサーバ機能をONにした場合に、リモートアクセスするパソコンに割り当てるIPアドレスを入力します。(*1)

*1　本製品と同じサブネットのIPアドレスを設定する必要があります。

6. Path MTU Discovery　：Path MTU Discovery機能を設定します。

項目	説明
Path MTU Discovery機能	Path MTU Discovery機能をONにするかOFFにするかを選択します。Path MTU Discovery機能をONにすると、通信経路によって最適なパケットサイズを検知して通信を行います。

7. オプション　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
オプション	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。このオプション欄では以下の設定を入力することができます。 ● DHCPスタティック設定 ● 簡易DNS設定 ● IP経路情報の追加 ● ソース経路情報の登録 ● IPフィルタの設定 ● NATテーブルの登録(*1) ● NAT使用時ブロードキャストパケット転送 ● Directed-Broadcast [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

*1　NATテーブル(NATアドレスマッピング)の登録は、詳細設定画面の[NAT設定]で設定することもできます。

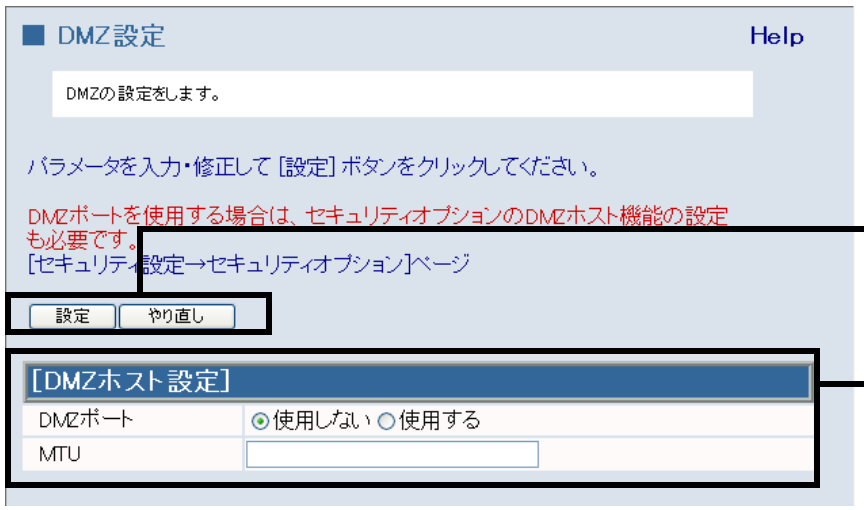
7-3-3. DMZ

DMZを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[ルータ設定]→[DMZ]の順にクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。
2. DMZホスト設定：DMZ設定を行います。

1. 設定／やり直し　　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。クリックすると、再起動画面が表示されるので、[再起動]をクリックして本製品を再起動します。再起動を開始すると、[状態]ランプが点灯するので、再起動が完了するまで数秒間待ちます。再起動が完了すると、[状態]ランプが消えます。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。

2. DMZホスト設定　　：DMZ設定を行います。

項目	説明
DMZポート	DMZを使用するかしないかを選択します。(*1)
MTU	540～1500の範囲で1パケットで送信可能なデータの最大値を入力します。

*1　DMZポートを使用する場合は、上記に加えて、詳細設定画面の[セキュリティ設定]－[セキュリティオプション]の[DMZホストアドレス]欄で、DMZポートで使用するアドレスを登録してください。また、[ルータ設定]－[LAN]の[オプション]欄、または[管理コマンド・設定]－[設定メンテナンス]にて以下のコマンドを追加してください。
- 全てのプロトコルを透過させる受信用フィルタを追加する
  例）ip filter 1 pass in * xxx.xxx.xxx.xxx * wanany
  （xxx.xxx.xxx.xxxには、DMZホストアドレスを指定）

7-4. セキュリティ設定

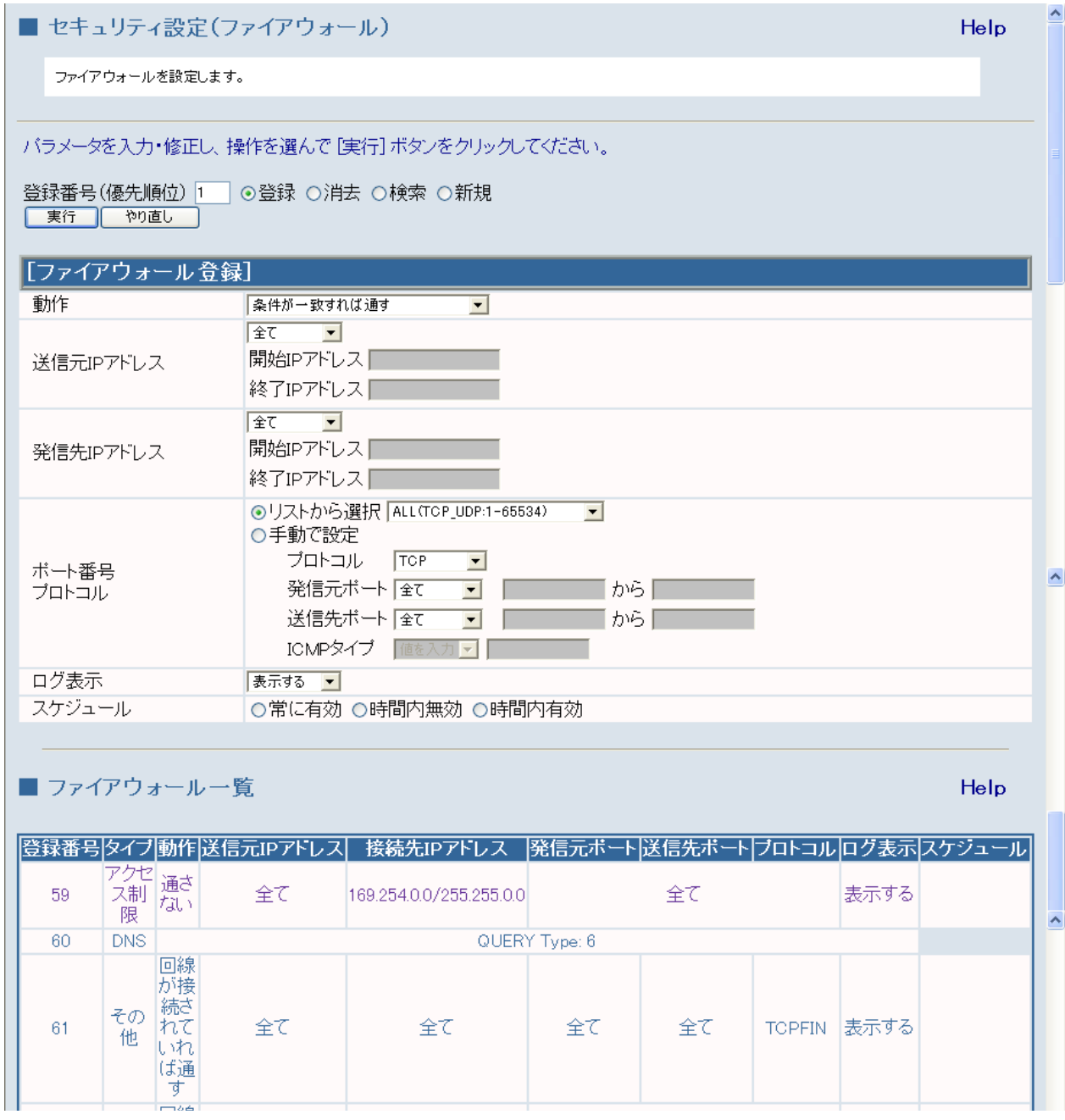
7-4-1. ファイアウォール

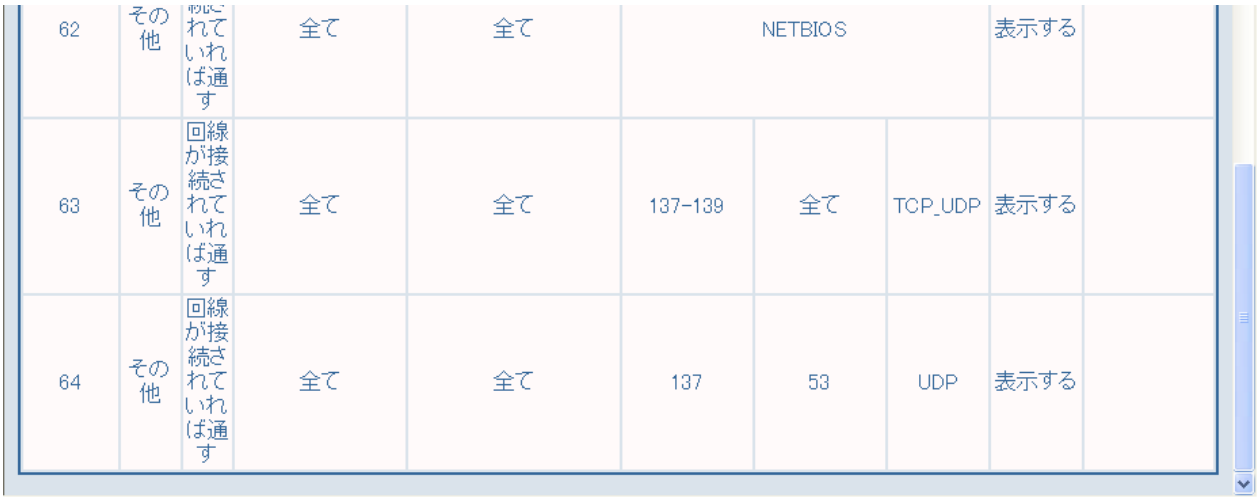
ファイアウォールを設定し、WAN→LANのテーブルを作成します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[ファイアウォール]の順にクリックします。

設定画面の説明





62	その他	線が接続されていれば通す	全て	全て	NETBIOS			表示する	
63	その他	回線が接続されていれば通す	全て	全て	137-139	全て	TCP_UDP	表示する	
64	その他	回線が接続されていれば通す	全て	全て	137	53	UDP	表示する	

項目	説明
登録番号(優先順位)	登録、検索、消去したいファイアウォールの登録番号を入力します。1～64まで登録できます。
登録／消去／検索／新規	実行する操作を選択します。 ● [登録]を選択し[実行]をクリックした場合は、[ファイアウォール登録]にて設定した内容を[登録番号(優先順位)]に入力した番号で登録します。 ● [消去]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のファイアウォール設定を消去します。 ● [検索]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のファイアウォール設定内容が[ファイアウォール登録]に表示されます。すでに登録済みのファイアウォール設定を変更したい場合に便利です。 ● [新規]を選択し[実行]をクリックした場合は、[ファイアウォール登録]にて設定した内容を、優先順位の高い未登録の登録番号で登録します。
[実行]	クリックすると、[登録]／[消去]／[検索]／[新規]で選択した操作を実行します。
[やり直し]	クリックすると、[ファイアウォール設定]にて変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[実行]をクリックして有効になった内容はクリアされません。
動作	ファイアウォールを登録する場合に、ファイアウォールの動作を選択します。 ● 設定した内容と一致する通信を許可する場合は[条件が一致すれば通す]を選択します。 ● 設定した内容と一致する通信を許可しない場合は[条件が一致すれば通さない]を選択します。 ● 設定した内容と一致する通信を回線が接続されているときのみ許可する場合は[回線が接続されている場合だけ通す]を選択します。

項目	説明
送信元IPアドレス	送信元IPアドレスの条件を設定します。 ● すべての送信元IPアドレスを条件として登録する場合は、ドロップダウンメニューで[全て]を選択します。 ● 送信元IPアドレスの条件をIPアドレスで範囲指定したい場合は、ドロップダウンメニューで[範囲指定]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● 送信元IPアドレスの条件を固定のIPアドレスで指定したい場合は、ドロップダウンメニューで[個別]を選択します。この場合、[開始IPアドレス]欄に指定するIPアドレスを入力します。 ● 送信元IPアドレスの条件をIPアドレスとサブネットマスクで指定したい場合は、ドロップダウンメニューで[ネットワーク]を選択します。この場合、[開始IPアドレス]欄にIPアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。
発信先IPアドレス	発信先IPアドレスの条件を設定します。 ● すべての発信先IPアドレスを条件として登録する場合は、ドロップダウンメニューで[全て]を選択します。 ● 発信先IPアドレスの条件をIPアドレスで範囲指定したい場合は、ドロップダウンメニューで[範囲指定]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● 発信先IPアドレスの条件を固定のIPアドレスで指定したい場合は、ドロップダウンメニューで[個別]を選択します。この場合、[開始IPアドレス]欄に指定するIPアドレスを入力します。 ● 発信先IPアドレスの条件をIPアドレスとサブネットマスクで指定したい場合は、ドロップダウンメニューで[ネットワーク]を選択します。この場合、[開始IPアドレス]欄にIPアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>ポート番号
プロトコル</td><td colspan="2">ポート番号／プロトコルの条件を設定します。
● 特定のプロトコルが使用するポート番号をすべて条件に設定したい場合は、[リストから選択] ドロップダウンメニューで条件に指定するプロトコルを選択します。
● プロトコルやポート番号を手動で詳しく条件を設定したい場合は、[手動で設定] を選択します。この場合、[プロトコル]、[発信元ポート]、[送信先ポート]、[ICMPタイプ] で条件を設定します。</td></tr>
<tr><td></td><td>項目</td><td>説明</td></tr>
<tr><td></td><td>プロトコル</td><td>条件に指定するプロトコルの種類を選択します。</td></tr>
<tr><td></td><td>発信元ポート</td><td>発信元ポートを指定する条件を選択します。選択したプロトコルが使用するすべてのポート番号を条件として設定する場合は、ドロップダウンメニューで [全て] を選択します。特定の範囲のポート番号を指定したい場合は、ドロップダウンメニューで [範囲指定] を選択し、右側欄にそれぞれ開始ポート番号と終了ポート番号を入力します。固定のポート番号のみを条件として設定したい場合は、ドロップダウンメニューで [個別] を選択し右側欄にポート番号を入力します。</td></tr>
<tr><td></td><td>通信先ポート</td><td>送信先ポートを指定する条件を選択します。選択したプロトコルが使用するすべてのポート番号を条件として設定する場合は、ドロップダウンメニューで [全て] を選択します。特定の範囲のポート番号を指定したい場合は、ドロップダウンメニューで [範囲指定] を選択し、右側欄にそれぞれ開始ポート番号と終了ポート番号を入力します。固定のポート番号のみを条件として設定したい場合は、ドロップダウンメニューで [個別] を選択し右側欄にポート番号を入力します。</td></tr>
<tr><td></td><td>ICMPタイプ</td><td>[プロトコル] 欄で [ICMP] を選択した場合に、ICMP タイプの条件を設定します。すべてのICMP タイプを条件に設定する場合は、[全て] を選択します。ICMP タイプを指定したい場合は、[値を入力] を選択し、右側欄にICMPタイプを入力します。</td></tr>
<tr><td>ログ表示</td><td colspan="2">設定したファイアウォールの条件に一致する通信が行われた場合に、ファイアウォールログに表示するかどうかを選択します。</td></tr>
<tr><td>スケジュール</td><td colspan="2">ファイアウォールのスケジュールを設定します。
● 登録するファイアウォールを常に有効にする場合は、[常に有効] を選択します。
● 登録するファイアウォールを、指定した時間だけ無効にする場合は [時間内無効] を選択します。時間内無効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内無効] を選択しても [常に有効] になります。(→P.98)
● 登録するファイアウォールを、指定した時間だけ有効にする場合は [時間内有効] を選択します。時間内有効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内有効] を選択しても [常に有効] になります。(→P.98)</td></tr>
<tr><td>ファイアウォール一覧</td><td colspan="2">登録されているファイアウォール一覧を表示します。</td></tr>
</table>

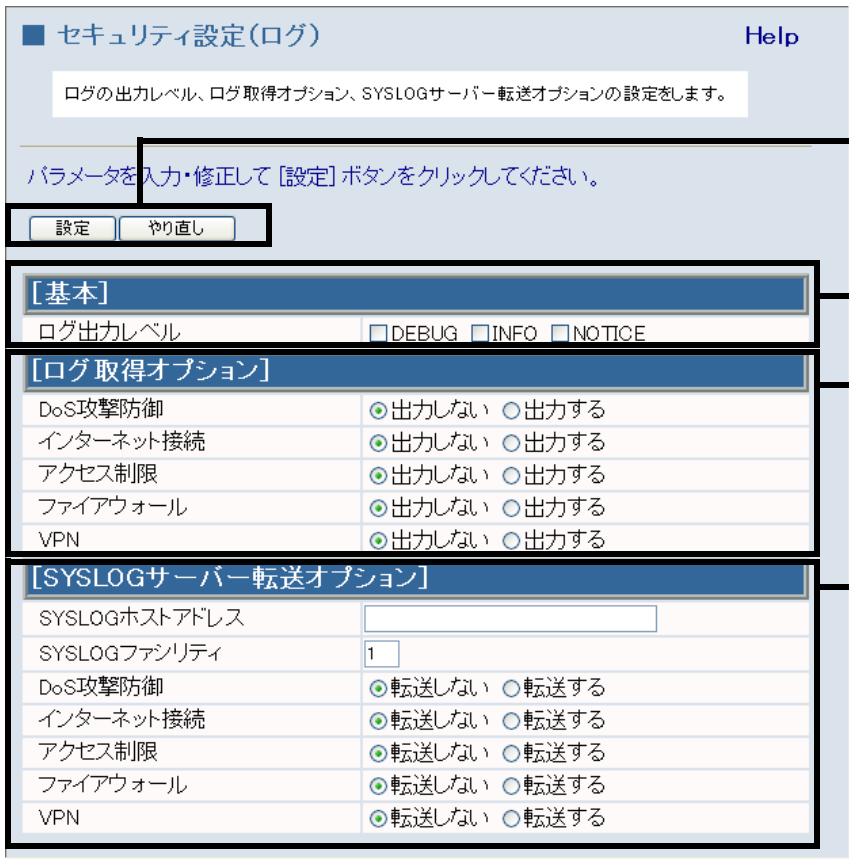
7-4-2. ログ

ログ出力やSYSLOGサーバ転送機能を設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[ログ]の順にクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。
2. 基本：ログ出力レベルを設定します。
3. ログ取得オプション：ログに出力するイベントを設定します。
4. SYSLOGサーバ転送オプション：ログをSYSLOGサーバに転送する場合に設定します。

1. 設定／やり直し　　：　各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 基本　　：ログ出力レベルを設定します。

項目	説明
ログ出力レベル	ログに出力するステータスレベルを選択します。複数選択することができます。NOTICE→INFO→DEBUGの順にログ出力レベルが高くなります。ログ出力レベルが高くなると、その分CPUに負担がかかり、処理が遅くなります。

3. ログ取得オプション　　：ログに出力するイベントを設定します。

項目	説明
DoS攻撃防御	DoS攻撃防御をログに出力するかどうかを選択します。
インターネット接続	インターネット接続をログに出力するかどうかを選択します。
アクセス制御	アクセス制御をログに出力するかどうかを選択します。
ファイアウォール	ファイアウォールをログに出力するかどうかを選択します。
VPN	VPN接続をログに出力するかどうかを選択します。

4. SYSLOGサーバ転送オプション　：ログをSYSLOGサーバに転送する場合に設定します。

項目	説明
SYSLOGホストアドレス	SYSLOGサーバのIPアドレスを入力します。
SYSLOGファシリティ	SYSLOGを転送する際のファシリティコード番号を入力します。通常は「1」を指定します。
DoS攻撃防御	DoS攻撃防御ログをSYSLOGサーバに転送するかしないかを選択します。
インターネット接続	インターネット接続ログをSYSLOGサーバに転送するかしないかを選択します。
アクセス制御	アクセス制御ログをSYSLOGサーバに転送するかしないかを選択します。
ファイアウォール	ファイアウォールログをSYSLOGサーバに転送するかしないかを選択します。
VPN	VPNログをSYSLOGサーバに転送するかしないかを選択します。

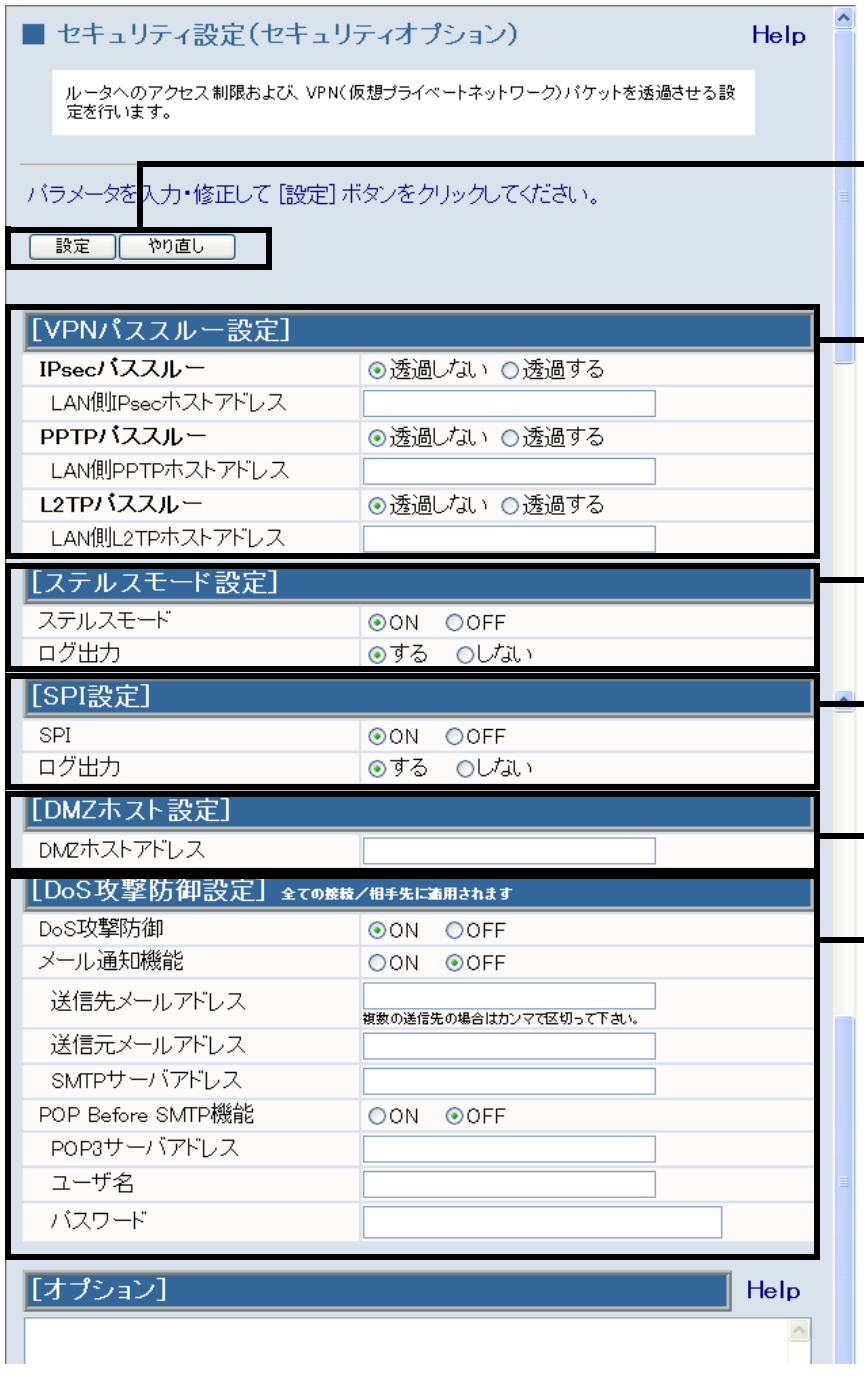
7-4-3. セキュリティオプション

ルータへのアクセス制御およびVPN(仮想プライベートネットワーク)パケットを透過させる設定を行います。

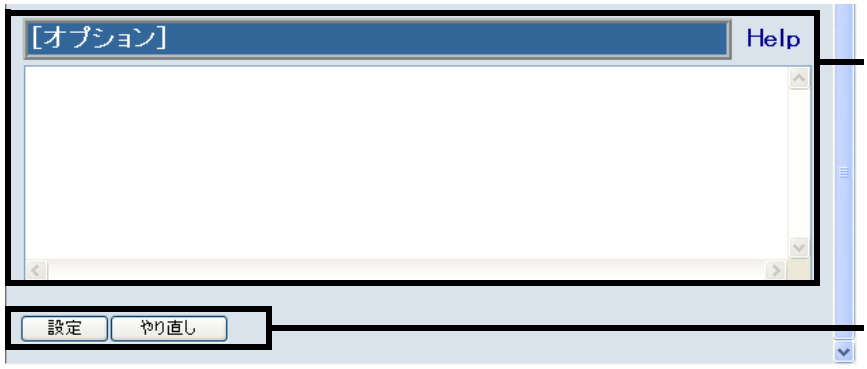
表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[セキュリティオプション]の順にクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。
2. VPNパススルー設定：VPNのパケットをWAN側へ透過させる設定を行います。
3. ステルスモード設定：ステルスモードを設定します。
4. SPI設定：SPIを使用して受信パケットを監視するかどうかを設定します。
5. DMZホスト設定：DMZホストを設定します。
6. DoS攻撃防御設定：DoS攻撃防御を有効にするかどうかを設定します。



7. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。

1. 設定／やり直し　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. VPNパススルー設定　：VPNのパケットをWAN側へ透過させる設定を行います。

項目	説明
IPSecパススルー	IPSecのパケットを透過するかどうかを選択します。
LAN側IPSecホストアドレス	特定のパソコンのみでIPSec通信する場合に、IPSec通信を行うパソコンのIPアドレスを入力します。LAN内にIPSecサーバを設置する場合は、必ずサーバのIPアドレスを入力してください。
PPTPパススルー	PPTPのパケットを透過するかどうかを選択します。
LAN側PPTPホストアドレス	特定のパソコンのみでPPTP通信する場合に、PPTP通信を行うパソコンのIPアドレスを入力します。LAN内にPPTPサーバを設置する場合は、必ずサーバのIPアドレスを入力してください。
L2TPパススルー	L2TPのパケットを透過するかどうかを選択します。
LAN側L2TPホストアドレス	特定のパソコンのみでL2TP通信する場合に、L2TP通信を行うパソコンのIPアドレスを入力します。LAN内にL2TPサーバを設置する場合は、必ずサーバのIPアドレスを入力してください。

3. ステルスモード設定　：ステルスモードを設定します。

項目	説明
ステルスモード	ステルスモードをONにするかOFFにするかを選択します。 ステルスモードをONにした場合、WAN側からのPINGコマンドに応答しなくなります。また、WAN側にICMPエラーやTCPリセット（ポート番号113を除く）を返さなくなります。
ログ出力	ステルスモードにより応答を破棄したパケットのログをSYSLOGサーバに出力するかどうかを選択します。

4. SPI設定　　：SPIを使用して受信パケットを監視するかどうかを設定します。

項目	説明
SPI	SPI機能をONにするかOFFにするかを選択します。 SPI機能をONにした場合、受信パケットをチェックして不正な受信パケットを破棄します。
ログ出力	SPIにより破棄したパケットのログをSYSLOGサーバに出力するかどうかを選択します。

5. DMZホスト設定　　：DMZホストを設定します。

項目	説明
DMZホストアドレス	DMZポートに接続するパソコンのIPアドレスを入力します。IPアドレスを指定すると、指定したIPアドレス以外のパソコンをDMZポートに接続しても通信できなくなります。

6. DoS攻撃防御設定　　：DoS攻撃防御を有効にするかどうかを設定します。

項目	説明
DoS攻撃防御	DoS攻撃防御をONにするかOFFにするかを選択します。 ONにすると、すべての接続に対してDoS攻撃防御を有効にします。
メール通知機能	メール通知機能をONにするかOFFにするかを選択します。 ONにすると、DoS攻撃防御を行うごとに、指定したメールアドレスに通知メッセージを送信します。 ONを選択した場合は、[送信先メールアドレス] [送信元メールアドレス] [SMTPサーバアドレス] を入力してください。
送信先メールアドレス	通知メッセージを送信するメールアドレスを入力します。複数のメールアドレスを入力したい場合は、カンマ(,)で区切って入力します。
送信元メールアドレス	通知メッセージの送信元メールアドレスを入力します。
SMTPサーバアドレス	通知メッセージを送信するときに使用するSMTPサーバのIPアドレスを入力します。
POP Before SMTP機能	POP Before SMTP機能をONにするかOFFにするかを選択します。 ONにすると、SMTPでメール通知を送信する前に、指定したPOP3サーバに問い合わせてユーザ名およびパスワードの認証を行います。 ONにした場合は、[POP3サーバアドレス] [ユーザ名] [パスワード] を入力します。
POP3サーバアドレス	POP Before SMTP機能でユーザ名およびパスワードの認証を行うPOP3サーバのIPアドレスを入力します。
ユーザ名	POP Before SMTP機能の認証に使用するユーザ名を入力します。
パスワード	POP Before SMTP機能の認証に使用するパスワードを入力します。

7. オプション　　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
オプション	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

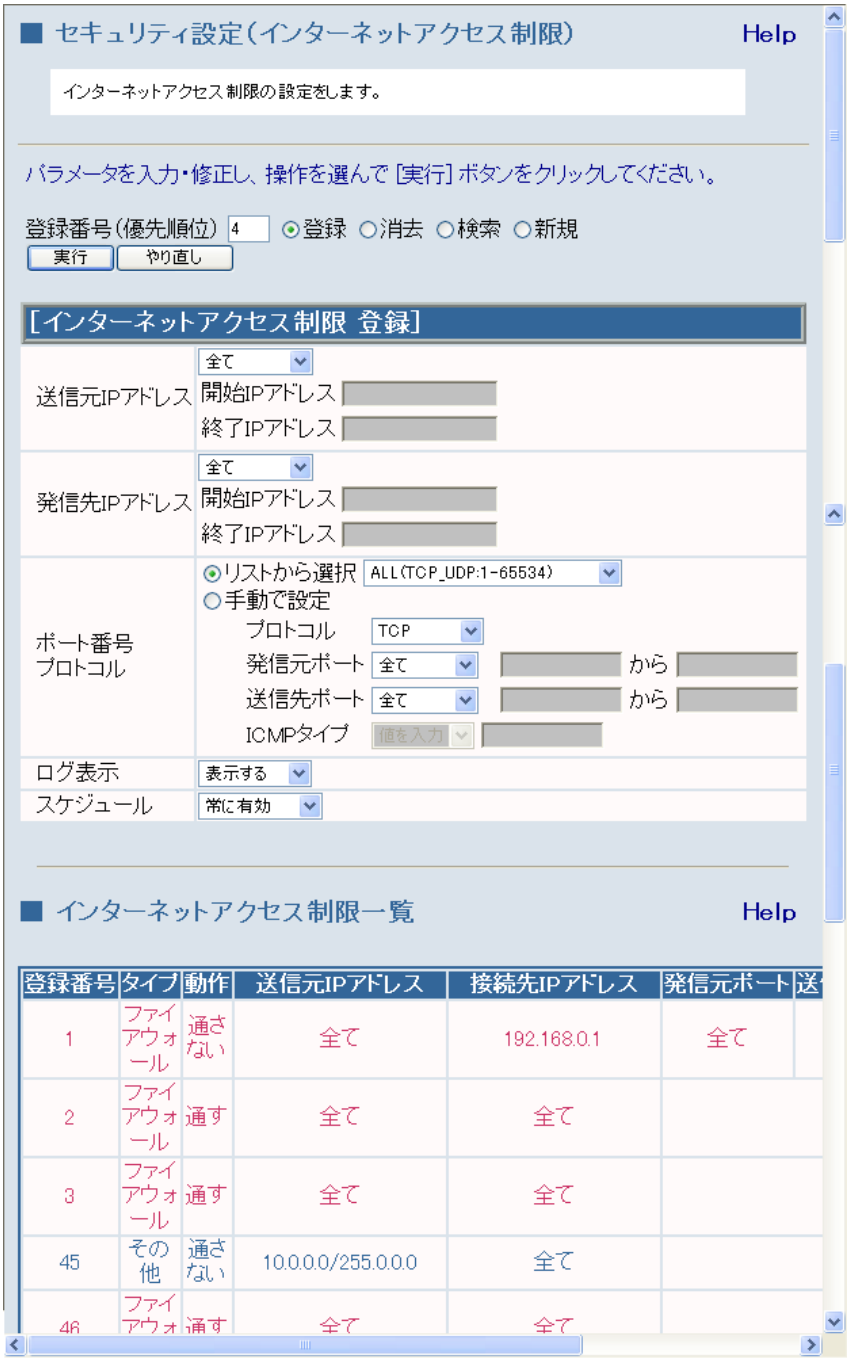
7-4-4. インターネットアクセス制御

インターネットアクセス制御を設定し、LAN→WANのテーブルを作成します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[インターネットアクセス制御]の順にクリックします。

設定画面の説明



項目	説明
登録番号(優先順位)	登録、検索、または消去したいインターネットアクセス制御の登録番号を入力します。登録する場合は、1～64まで登録できます。
登録／消去／検索／新規	実行する操作を選択します。 ● [登録]を選択し[実行]をクリックした場合は、[インターネットアクセス制御登録]にて設定した内容を[登録番号(優先順位)]に入力した番号で登録します。 ● [消去]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のインターネットアクセス制御設定を消去します。 ● [検索]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のインターネットアクセス制御設定内容が[インターネットアクセス制御登録]に表示されます。すでに登録済みのインターネットアクセス制御設定を変更したい場合に便利です。 ● [新規]を選択し[実行]をクリックした場合は、[インターネットアクセス制御登録]にて設定した内容を、優先順位の高い未登録の登録番号で登録します。
[実行]	クリックすると、[登録]／[消去]／[検索]／[新規]で選択した操作を実行します。
[やり直し]	クリックすると、[インターネットアクセス制御登録]にて変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[実行]をクリックして有効になった内容はクリアされません。
送信元IPアドレス	送信元IPアドレスの条件を設定します。 ● すべての送信元IPアドレスを条件として登録する場合は、ドロップダウンメニューで[全て]を選択します。 ● 送信元IPアドレスの条件をIPアドレスで範囲指定したい場合は、ドロップダウンメニューで[範囲指定]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● 送信元IPアドレスの条件を固定のIPアドレスで指定したい場合は、ドロップダウンメニューで[個別]を選択します。この場合、[開始IPアドレス]欄に指定するIPアドレスを入力します。 ● 送信元IPアドレスの条件をIPアドレスとサブネットマスクで指定したい場合は、ドロップダウンメニューで[ネットワーク]を選択します。この場合、[開始IPアドレス]欄にIPアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。
発信先IPアドレス	発信先IPアドレスの条件を設定します。 ● すべての発信先IPアドレスを条件として登録する場合は、ドロップダウンメニューで[全て]を選択します。 ● 発信先IPアドレスの条件をIPアドレスで範囲指定したい場合は、ドロップダウンメニューで[範囲指定]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● 発信先IPアドレスの条件を固定のIPアドレスで指定したい場合は、ドロップダウンメニューで[個別]を選択します。この場合、[開始IPアドレス]欄に指定するIPアドレスを入力します。 ● 発信先IPアドレスの条件をIPアドレスとサブネットマスクで指定したい場合は、ドロップダウンメニューで[ネットワーク]を選択します。この場合、[開始IPアドレス]欄にIPアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。

<table>
<tr><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>ポート番号
プロトコル</td><td colspan="2">ポート番号／プロトコルの条件を設定します。
● 特定のプロトコルが使用するポート番号をすべて条件に設定したい場合は、[リストから選択] ドロップダウンメニューで条件に指定するプロトコルを選択します。
● プロトコルやポート番号を手動で詳しく条件を設定したい場合は、[手動で設定] を選択します。この場合、[プロトコル]、[発信元ポート]、[送信先ポート]、[ICMPタイプ] で条件を設定します。</td></tr>
<tr><td></td><td>項目</td><td>説明</td></tr>
<tr><td></td><td>プロトコル</td><td>条件に指定するプロトコルの種類を選択します。</td></tr>
<tr><td></td><td>発信元ポート</td><td>発信元ポートを指定する条件を選択します。選択したプロトコルが使用するすべてのポート番号を条件として設定する場合は、ドロップダウンメニューで [全て] を選択します。特定の範囲のポート番号を指定したい場合は、ドロップダウンメニューで [範囲指定] を選択し、右側欄にそれぞれ開始ポート番号と終了ポート番号を入力します。固定のポート番号のみを条件として設定したい場合は、ドロップダウンメニューで [個別] を選択し右側欄にポート番号を入力します。</td></tr>
<tr><td></td><td>送信先ポート</td><td>送信先ポートを指定する条件を選択します。選択したプロトコルが使用するすべてのポート番号を条件として設定する場合は、ドロップダウンメニューで [全て] を選択します。特定の範囲のポート番号を指定したい場合は、ドロップダウンメニューで [範囲指定] を選択し、右側欄にそれぞれ開始ポート番号と終了ポート番号を入力します。固定のポート番号のみを条件として設定したい場合は、ドロップダウンメニューで [個別] を選択し右側欄にポート番号を入力します。</td></tr>
<tr><td></td><td>ICMPタイプ</td><td>[プロトコル] 欄で [ICMP] を選択した場合に、ICMP タイプの条件を設定します。すべてのICMP タイプを条件に設定する場合は、[全て] を選択します。ICMP タイプを指定したい場合は、[値を入力] を選択し、右側欄にICMPタイプを入力します。</td></tr>
<tr><td>ログ表示</td><td colspan="2">設定したインターネットアクセス制御の条件に一致する通信が行われた場合に、インターネットアクセス制御ログに表示するかどうかを選択します。</td></tr>
<tr><td>スケジュール</td><td colspan="2">インターネットアクセス制御のスケジュールを設定します。
● 登録するインターネットアクセス制御を常に有効にする場合は、[常に有効] を選択します。
● 登録するインターネットアクセス制御を、指定した時間だけ無効にする場合は [時間内無効] を選択します。時間内無効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内無効] を選択しても [常に有効] になります。
(→P.98)
● 登録するインターネットアクセス制御を、指定した時間だけ有効にする場合は [時間内有効] を選択します。時間内有効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内有効] を選択しても [常に有効] になります。
(→P.98)</td></tr>
<tr><td>インターネットアクセス制御一覧</td><td colspan="2">登録されているインターネットアクセス制御一覧を表示します。</td></tr>
</table>

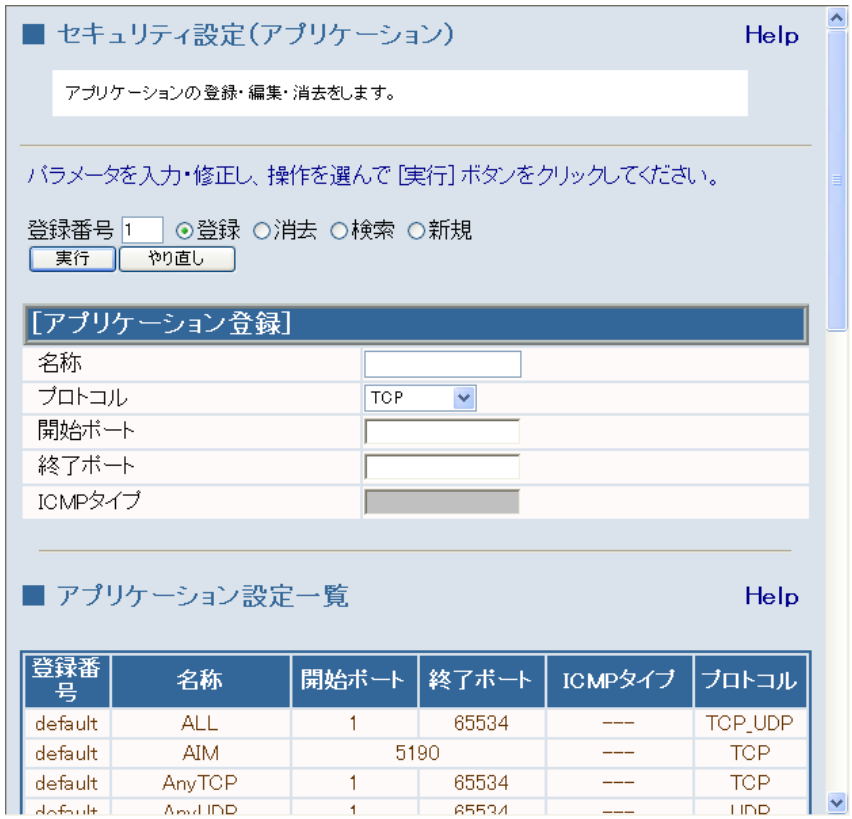
7-4-5. アプリケーション

アプリケーションの登録、編集、消去を行います。
ネットワークゲームなどを利用する場合は、アプリケーション設定とポート開放の設定が必要になる場合があります。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[アプリケーション]の順にクリックします。

設定画面の説明



項目	説明
登録番号	登録、検索、または消去したい相手先の登録番号を入力します。[登録]を選択している場合は、すでに登録されているアプリケーション設定の登録番号またはその次の空き番号のみ入力できます。(最大64個)

項目	説明
登録／消去／検索／新規	実行する操作を選択します。 ● [登録]を選択し[実行]をクリックした場合は、[アプリケーション登録]にて設定した内容を[登録番号]に入力した番号で登録します。 ● [消去]を選択し[実行]をクリックした場合は、[登録番号]に入力した番号のアプリケーション設定を消去します。 ● [検索]を選択し[実行]をクリックした場合は、[登録番号]に入力した番号のアプリケーション設定内容が[アプリケーション登録]に表示されます。すでに登録済みのアプリケーション設定を変更したい場合に便利です。 ● [新規]を選択し[実行]をクリックした場合は、[アプリケーション登録]にて設定した内容を、優先順位の高い未登録の登録番号で登録します。
[実行]	クリックすると、[登録]／[消去]／[検索]／[新規]で選択した操作を実行します。
[やり直し]	クリックすると、[アプリケーション登録]にて変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[実行]をクリックして有効になった内容はクリアされません。
名称	アプリケーション設定の名称を入力します。
プロトコル	アプリケーションで通信に使用するプロトコルを選択します。
開始ポート	アプリケーションが使用するポート番号で先頭のポート番号を入力します。使用するポート番号が1つの場合は、そのポート番号を入力します。
終了ポート	アプリケーションが使用するポート番号で最後のポート番号を入力します。使用するポート番号が1つの場合は、[開始ポート]欄に入力したポート番号と同じものを入力します。
ICMPタイプ	[プロトコル]欄で[ICMP]を選択した場合は、サーバソフトが使用するICMPタイプを入力します。
アプリケーション設定一覧	登録されているアプリケーション設定一覧を表示します。

7-4-6. スケジュール

ファイアウォール、インターネットアクセス制御、URL フィルタ、MAC アドレスフィルタのスケジュールを設定します。

補足

- スケジュール設定画面では、スケジュール機能の有効／無効および各曜日ごとのスケジュールの登録／削除を操作することができます。登録したスケジュールをどのように適用するかは、ファイアウォール、インターネットアクセス制御、URL フィルタ、MAC アドレスフィルタ、それぞれを登録するときに設定します。
  →『7-4-1. ファイアウォール』（P.84）
  →『7-4-4. インターネットアクセス制御』（P.93）
  →『7-4-7.MAC アドレスフィルタ』（P.100）
  →『7-4-8.URL フィルタ』（P.102）

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[スケジュール]の順にクリックします。

設定画面の説明

1. スケジュール設定：スケジュール機能を設定します。

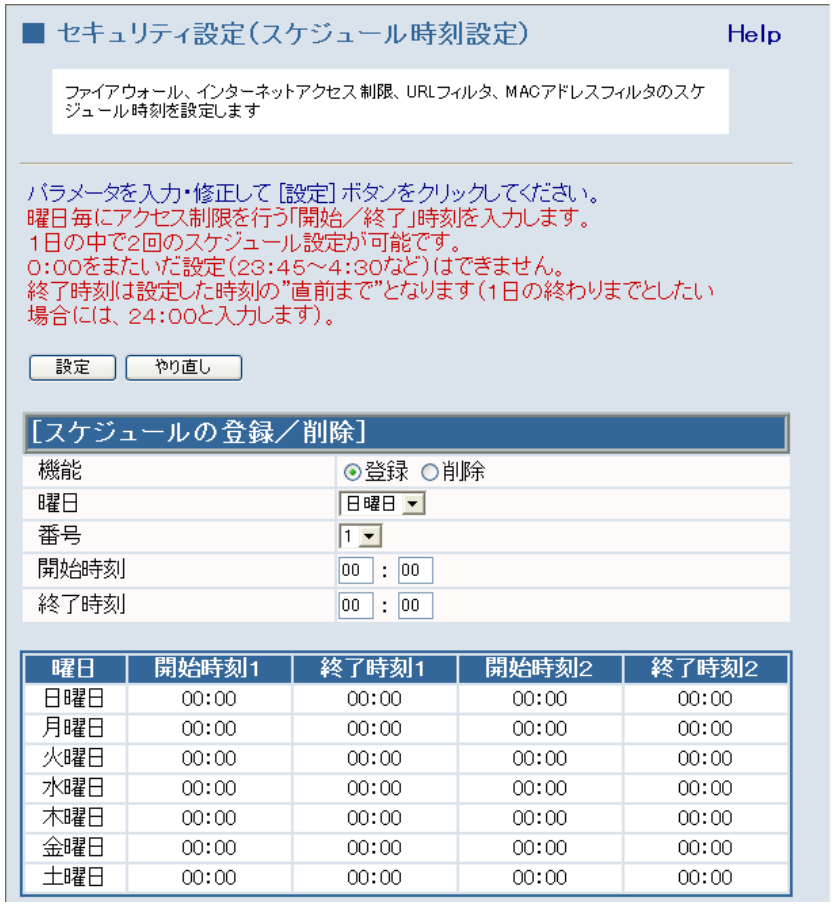
2. スケジュールの登録：「※スケジュール時刻の登録、削除をするときはここをクリック」をクリックすると、スケジュール時刻設定画面が表示されます。このリンクからスケジュール時刻の登録および消去を行います。

1. スケジュール設定　　：スケジュール機能を設定します。

項目	説明
［設定］	クリックすると、変更した内容を保存します。

項目	説明
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。
スケジュール機能	スケジュール機能をONにするかOFFにするかを選択します。

2. スケジュールの登録　：「※スケジュール時刻の登録、削除をするときはここをクリック」をクリックすると、スケジュール時刻設定画面が表示されます。このリンクからスケジュール時刻の登録および消去を行います。



項目	説明
[設定]	[機能]欄で[登録]を選択している場合は、クリックすると、指定した設定で登録を行います。 [機能]欄で[削除]を選択している場合は、クリックすると、指定したスケジュールを削除します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。
機能	スケジュールを登録するかまたは削除するかを選択します。
曜日	スケジュールを登録する曜日を選択します。
番号	スケジュールの番号を選択します。各曜日ごとに２つまでスケジュールを登録することができます。
開始時刻	開始時刻を入力します。
終了時刻	終了時刻を入力します。

7-4-7. MACアドレスフィルタ

MACアドレスフィルタで通過させるMACアドレスを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[MACアドレスフィルタ]の順にクリックします。

設定画面の説明

1. MACアドレスフィルタ設定：MACアドレスフィルタ機能を設定します。

2. MACアドレスの登録：「※MACアドレスの登録、削除をするときはここをクリック」をクリックするとMACアドレス設定画面が表示されます。このリンクからMACアドレスの登録および消去を行います。

1. MACアドレスフィルタ設定　：　MACアドレスフィルタ機能を設定します。

項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。
MACアドレスフィルタ機能	MACアドレスフィルタ機能をONにするかOFFにするかを選択します。 ※ MACアドレスフィルタ機能をONにした場合、一覧に登録されたMACアドレスのパソコンからしか本製品に接続できなくなります。MACアドレスフィルタ機能をONにする前に、本製品に接続されているパソコンのMACアドレスを登録してください。登録せずにMACアドレスフィルタ機能をONにすると、ルータ設定画面にアクセスできなくなってしまいます。

2. MACアドレスの登録　：「※ MAC アドレスの登録、削除をするときはここをクリック」をクリックするとMAC アドレス設定画面が表示されます。このリンクからMACアドレスの登録および消去を行います。

項目	説明
[設定]	[機能] 欄で [登録] を選択している場合は、クリックすると、選択した登録番号およびMACアドレスで登録を行います。 [機能] 欄で [削除] を選択している場合は、クリックすると、選択した登録番号のMACアドレスを削除します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度 [設定] をクリックして有効になった内容はクリアされません。
機能	MACアドレスを登録するかまたは削除するかを選択します。
登録番号	登録または削除する登録番号を選択します。
MACアドレス	[機能] 欄で [登録] を選択した場合に、登録するMAC アドレスを入力します。
スケジュール	MACアドレスフィルタのスケジュールを設定します。 ● 登録するMAC アドレスフィルタを常に有効にする場合は、[常に有効] を選択します。 ● 登録する MAC アドレスフィルタを、指定した時間だけ無効にする場合は [時間内無効] を選択します。時間内無効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内無効] を選択しても [常に有効] になります。(→P.98) ● 登録する MAC アドレスフィルタを、指定した時間だけ有効にする場合は [時間内有効] を選択します。時間内有効にした場合は、[セキュリティ設定] の [スケジュール設定] で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内有効] を選択しても [常に有効] になります。(→P.98)

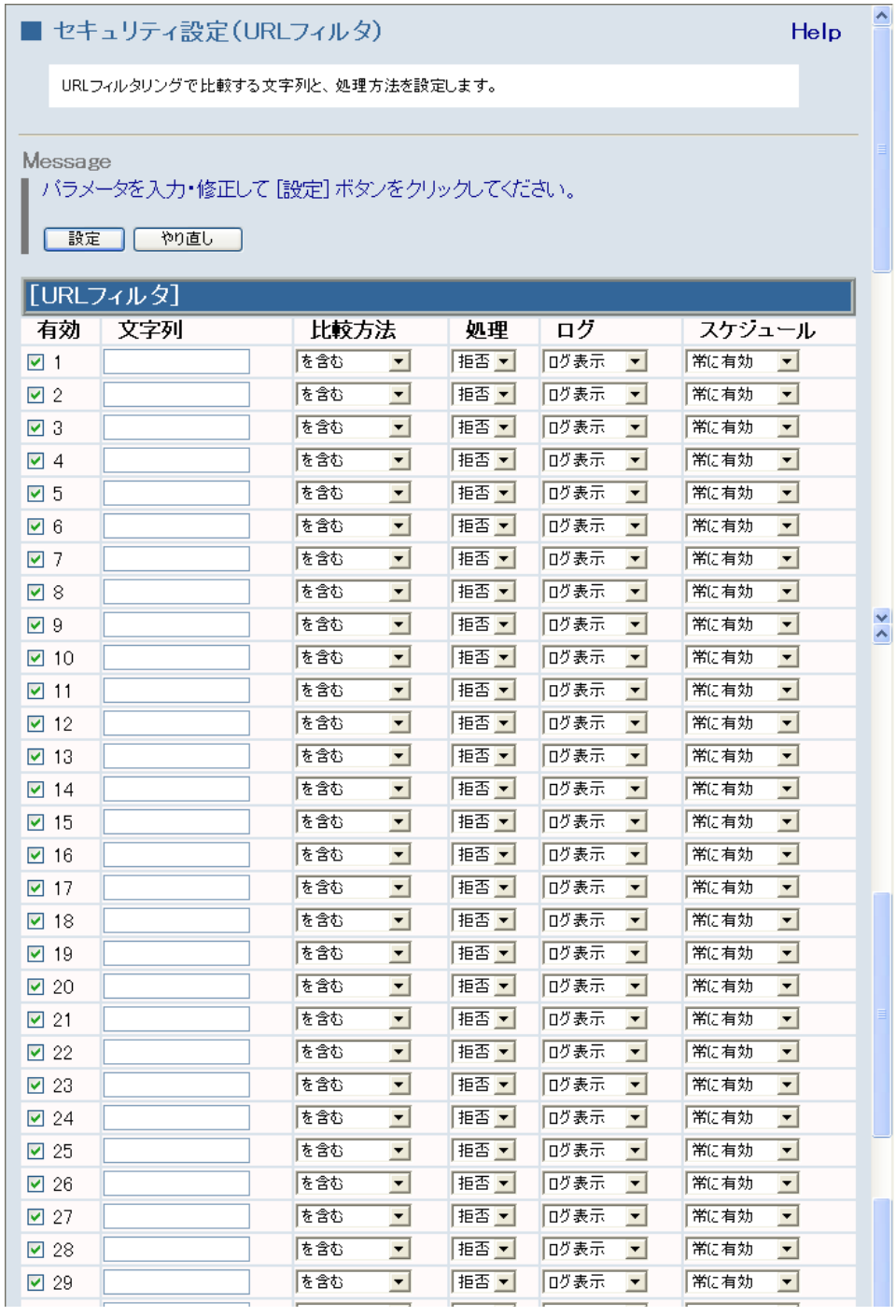
7-4-8. URLフィルタ

URLフィルタリングで比較する文字列と処理方法を設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[URLフィルタ]の順にクリックします。

設定画面の説明



項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。
有効	URLフィルタリングを有効にする設定のチェックボックスをチェックします。
文字列	比較する文字列を入力します。
比較方法	[文字列]欄に入力した文字列をどのように比較するかを選択します。
処理	[文字列]欄および[比較方法]欄で設定した条件と一致する場合に、通信を拒否するか通過させるかを選択します。
ログ	指定したURLフィルタリングの条件でアクセスがあった場合に、ログに表示するかどうかを選択します。
スケジュール	URLフィルタのスケジュールを設定します。 ● 登録するURLフィルタを常に有効にする場合は、[常に有効]を選択します。 ● 登録するURLフィルタを、指定した時間だけ無効にする場合は、[時間内無効]を選択します。時間内無効にした場合は、[セキュリティ設定]の[スケジュール設定]で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内無効]を選択しても[常に有効]になります。(→P.98) ● 登録するURLフィルタを、指定した時間だけ有効にする場合は、[時間内有効]を選択します。時間内有効にした場合は、[セキュリティ設定]の[スケジュール設定]で、スケジュールを設定します。ただし、スケジュール設定が無効になっている場合は、[時間内有効]を選択しても[常に有効]になります。(→P.98)
上記の条件に一致しなかったもの	1～31の設定で指定した条件に一致しない場合の処理およびログ表示を設定します。

7-4-9. 証明書(https)

HTTPS通信用の証明書をインストールします。

補足

証明書のインストール手順

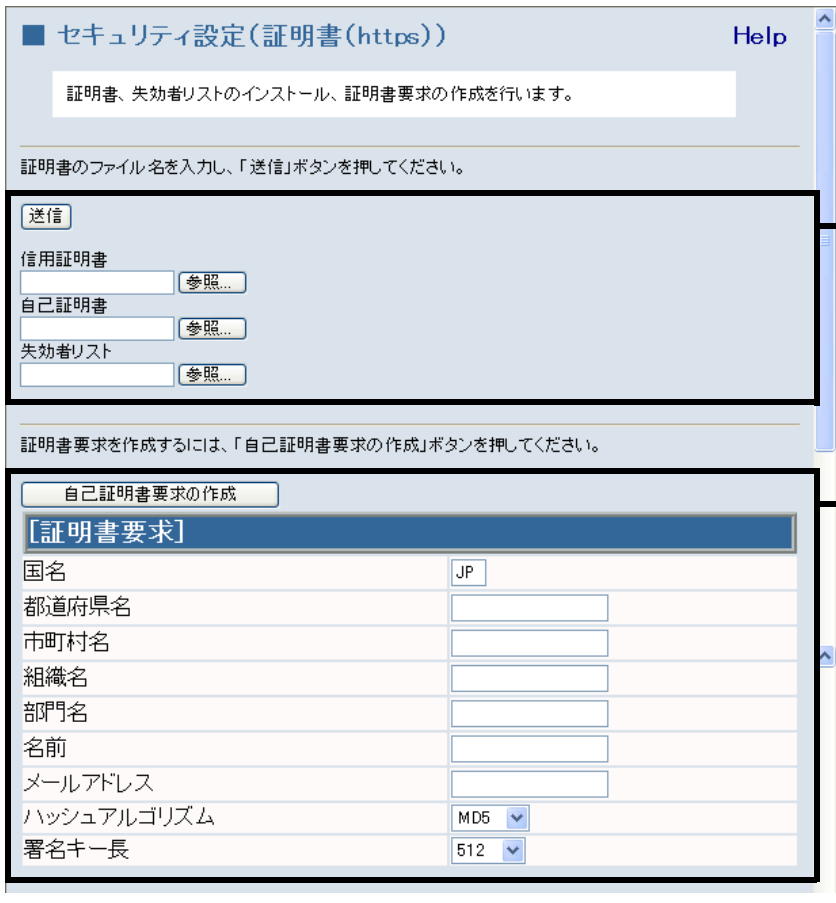
証明書のインストールは、以下の手順で行います。

1. CA(証明機関)から信用証明書ファイルを入手します。
2. [信用証明書]欄で入手した信用証明書ファイルを参照し、[送信]をクリックします。
3. [証明書要求]欄の各項目を入力し、[自己証明書要求の作成]をクリックして、自己証明書要求用の仮キーを表示します。
4. 表示された仮キーをコピーし、CA(証明機関)のホームページにアクセスし、コピーした仮キーを使用して自己証明書ファイルを入手します。
5. [自己証明書]欄で入手した自己証明書ファイルを参照し、[送信]をクリックします。

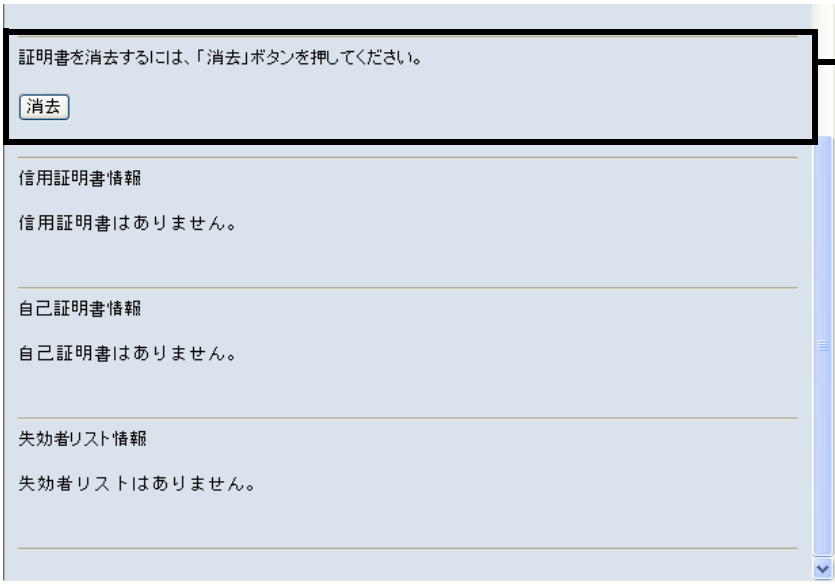
表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[セキュリティ設定]→[証明書(https)]の順にクリックします。

設定画面の説明



1. 証明書のインストール:信用証明書、自己証明書、失効者リストをインストールします。
2. 自己証明書要求：自己証明書要求用の署名キーを作成します。



3. 証明書の消去：証明書を消去します。

1. 証明書のインストール　　：　信用証明書、自己証明書、失効者リストをインストールします。

項目	説明
[送信]	クリックすると、[信用証明書] [自己証明書] [失効者リスト] で参照したファイルをインストールします。クリックする前にインストールしたいファイルを各欄で参照してください。
信用証明書	認証局(CA)から発行された信用証明書をインストールする場合は、[参照] をクリックして発行された証明書ファイルを選択します。
自己証明書	作成した自己証明書をインストールする場合は、[参照] をクリックして証明書ファイルを選択します。
失効者リスト	失効者リストをインストールする場合は、[参照] をクリックして失効者リストに追加する証明書ファイルを選択します。 秘密鍵の安全性が損なわれた場合などに、有効期限前に証明書を失効させたい場合は、失効させたい証明書ファイルを選択して、失効者リストに追加します。

2. 自己証明書要求　　：　自己証明書要求用の署名キーを作成します。

項目	説明
[自己証明書要求の作成]	クリックすると、[証明書要求] 欄で設定した内容で、自己証明書要求用の仮キーを表示します。
国名	国名を2桁のコードで入力します。あらかじめ「JP」が入力されているので、通常変更する必要はありません。
都道府県名	都道府県名を入力します。
市町村名	市町村名を入力します。
組織名	組織名を入力します。任意の名称を入力できます。
部門名	部門名を入力します。任意の名称を入力できます。
名前	名前を入力します。任意の名称を入力できます。
メールアドレス	メールアドレスを入力します。
ハッシュアルゴリズム	ハッシュアルゴリズムを選択します。

項目	説明
署名キー長	署名キー長を選択します。大きい数値ほど、セキュリティが高くなります。

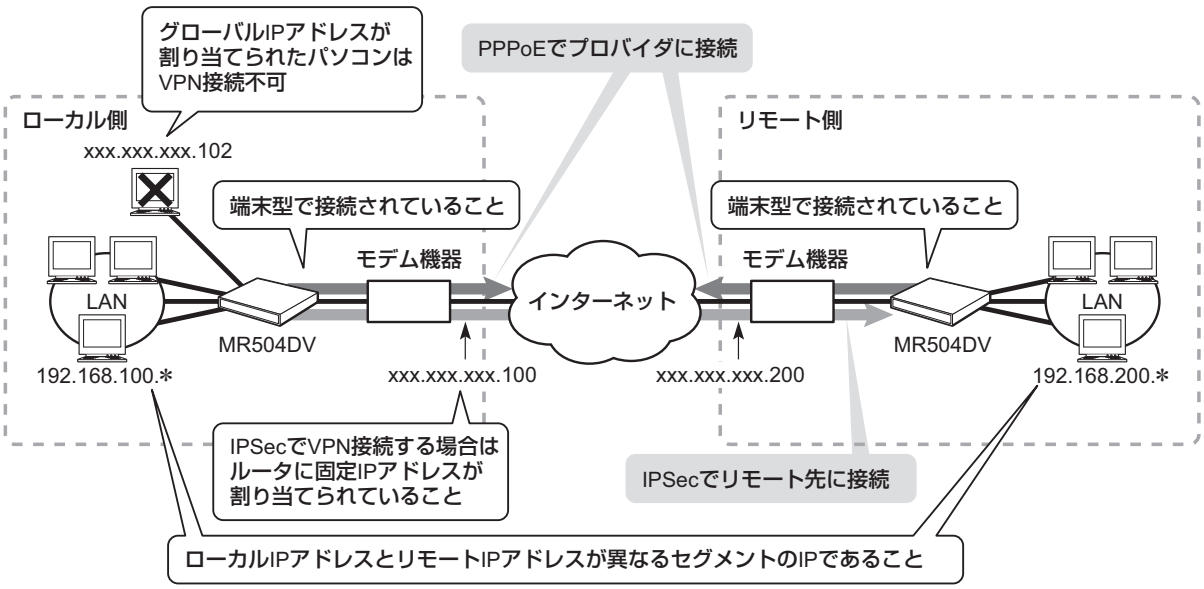
3. 証明書の消去　　：証明書を消去します。

項目	説明
[消去]	クリックすると、インストールしたすべての証明書を消去します。

7-5. VPN(IPSec)設定

VPN(バーチャル・プライベート・ネットワーク)はインターネットのような公共通信ネットワークを介してセキュリティを高めるために、考案された仕組みです。
本製品では、VPN接続としてIPSecトンネリングクライアント機能を搭載しそれぞれの拠点で固定グローバルIPの場合に、最大50トンネルの同時接続が可能です。
また本製品ではIPSec、PPTP、L2TPの各パススルーモードをサポートしています。パススルー設定は、本取扱説明書『7-4-3.セキュリティオプション』(P.90)を参照してください。

以下の図は、VPN接続の例とVPN接続する際の必要項目を説明しています。



大切

IPSecトンネリングクライアント機能を利用する上での注意点は以下になります。

- IPSec接続する互いのネットワークは違うセグメントで接続してください。
- IPSec接続させる互いのネットワークのインターネット網との接続IPアドレスは双方動的IPアドレスでは、使用できません。片側は固定である必要があります。
- 本製品は、最大50トンネルの同時接続が可能ですが、動的IPアドレスは50トンネルのうち1トンネルに限ります。
- トンネルの両端のネットワークは、双方ともにネットワーク数は 1 つに限ります。複数のネットワークは対象になりません。
- 本製品のローカルネットワークアドレスは、NAPT/NAT 変換されたプライベートアドレスに限定されます。アンナンバード接続により使用するパソコンはIPSec接続の対象にはなりません。
- トンネル内のパケットに対して、フィルタリングはできません。
- IPSec 接続する接続先の指定は IP アドレスで設定します。ドメインでの指定はできません。

7-5-1. VPNポリシー

リモート先のVPNサーバおよびゲートウェイへのVPN(IPSecクライアント機能)接続を設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[VPN(IPSec)設定]→[VPNポリシー]の順にクリックします。

設定画面の説明

1. 基本設定：IPSec機能を設定します。
2. VPNポリシーの登録：VPNポリシーとの登録を操作します。

1. 基本設定　　：　IPSec機能を設定します。

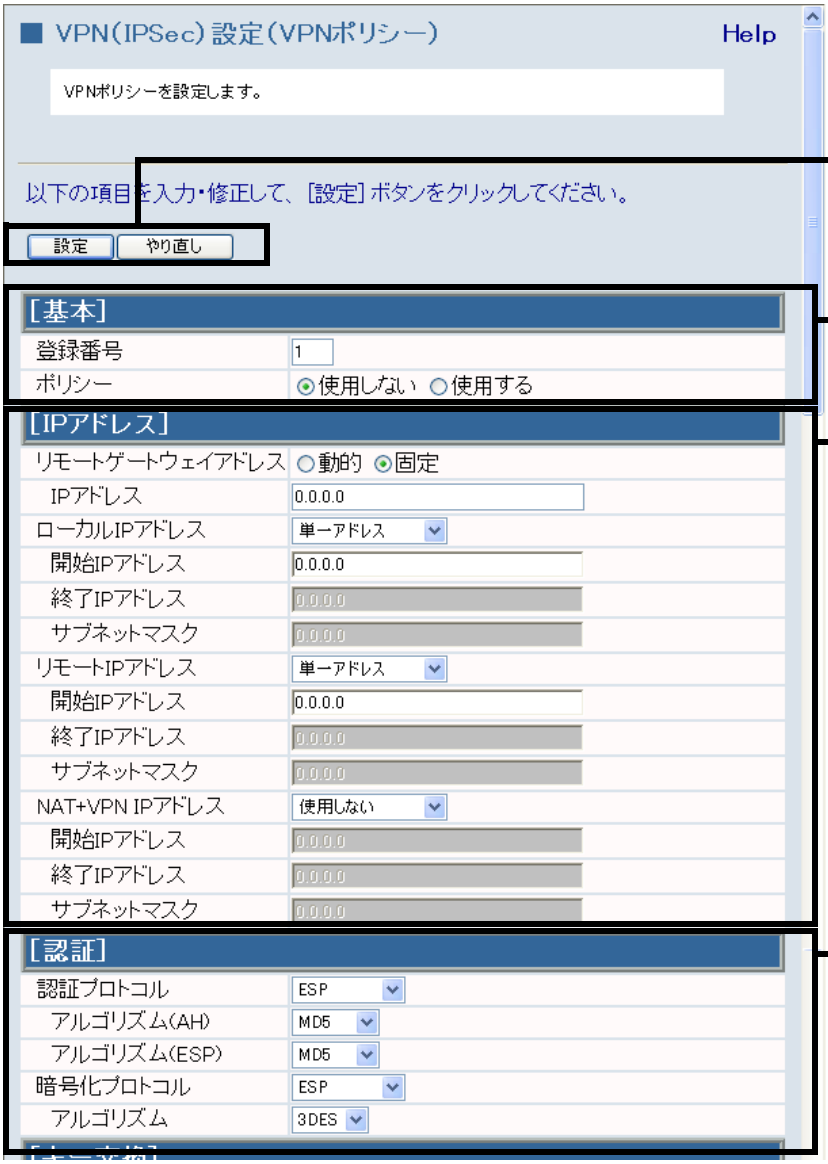
項目	説明
[実行]	クリックすると、基本設定で設定した内容を保存します。
IPSec機能	IPSec機能を使用するかしないかを選択します。 IPSec機能を使用すると、VPN接続間でデータを暗号化して送受信することができます。

2. VPNポリシーの登録　　：　VPNポリシーとの登録を操作します。

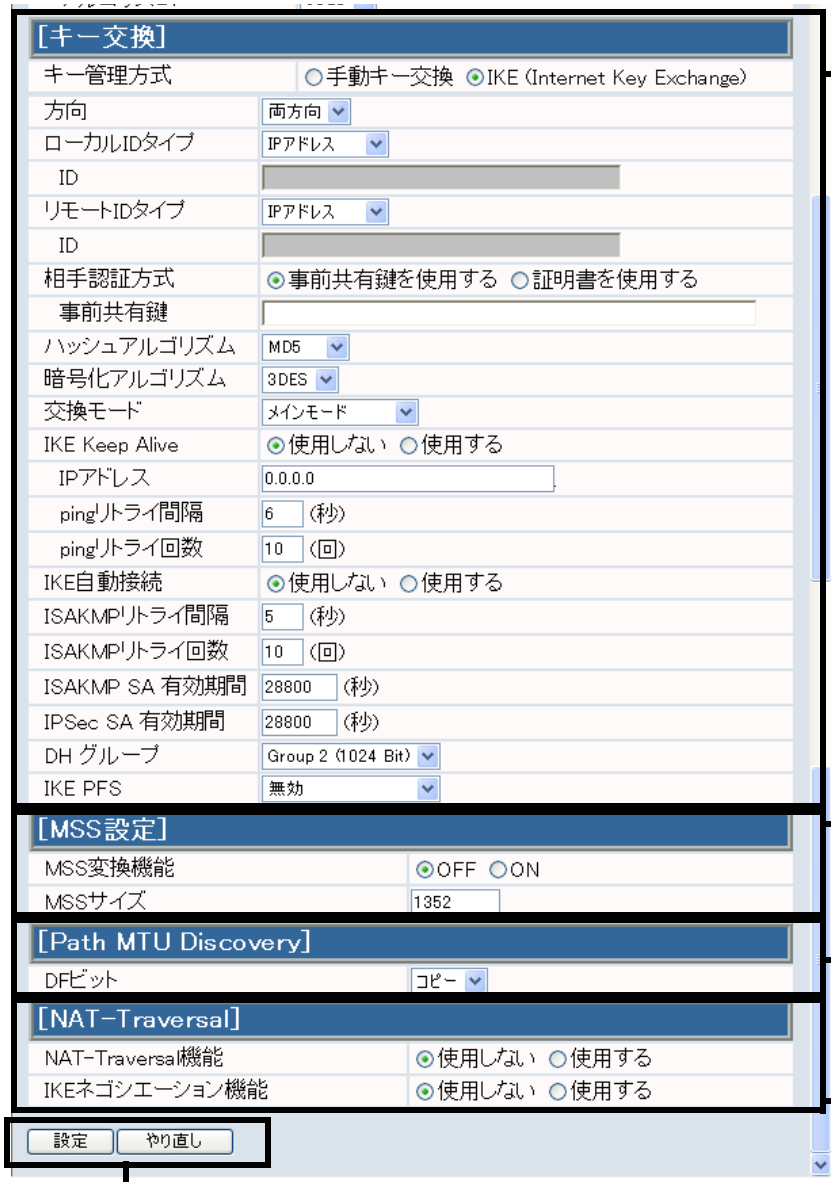
項目	説明
登録番号	VPNポリシーを登録または消去したいVPNポリシーの登録番号を入力します。1～50まで入力することができます。

項目	説明
登録／消去	● [登録番号]欄で入力した登録番号の VPN ポリシー設定の登録または登録内容の変更をしたい場合は、[登録] を選択します。 ● [登録番号]欄で入力した登録番号の VPN ポリシー設定を消去したい場合は、[消去] を選択します。
[実行]	● [登録] を選択して [実行] をクリックした場合は、[登録番号]欄で入力した登録番号のVPNポリシー設定を登録または変更します。この場合、クリックすると、VPNポリシー設定の登録画面が表示されます。VPNポリシー設定画面の詳細については『VPNポリシー設定の登録画面の説明』(P.109) を参照してください。 ● [消去] を選択して [実行] をクリックした場合は、[登録番号]欄で入力した登録番号のVPNポリシー設定を消去します。

VPNポリシー設定の登録画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.110)
2. 基本：VPNポリシーの基本情報を設定します。(P.111)
3. IPアドレス：VPN接続するローカルIPアドレスおよびリモートIPアドレスを設定します。(P.111)
4. 認証：認証方式を設定します。(P.115)



5. キー交換：キー交換を設定します。[キー管理方式]で[手動キー交換]または[IKE(Internet Key Exchange)]を選択したかによって、設定項目が変わります。(P.115)

6. MSS設定：MSS変換を使用するかどうかを設定します。(P.120)

7. Path MTU Discovery：Path MTU DiscoveryのDFビットモードを設定します。(P.120)

8. NAT-Traversal：NAT-Traversal機能を設定します。(P.120)

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.110)

1. 設定／やり直し　　：　各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。

大切

- [IPSec 機能]を[使用する]の状態で設定を変更した場合、設定変更が有効になりません。一度[IPSec機能]を[使用しない]に設定するか、本製品を再起動してください。

2. 基本　　：VPNポリシーの基本情報を設定します。

項目	説明
登録番号	登録番号を入力します。あらかじめ、前の画面の[登録番号]欄で入力した登録番号が表示されているので、変更する必要はありません。ただし、設定した登録番号とは別の登録番号で登録したい場合は、登録番号を変更します。1～50まで入力できます。
ポリシー	登録するポリシーを使用するかしないかを選択します。[使用しない]に設定した場合は、登録してもVPN接続されません。

3. IPアドレス　　：VPN接続するローカルIPアドレスおよびリモートIPアドレスを設定します。

項目	説明
リモートゲートウェイアドレス	● VPN 接続する相手(リモート先)のグローバル IP アドレスが固定グローバルIPアドレスではない場合は[動的]を選択します。 ● VPN 接続する相手(リモート先)のグローバル IP アドレスが固定グローバルIPアドレスの場合は[固定]を選択します。[固定]を選択した場合は、[IPアドレス]欄にリモートゲートウェイIPアドレスを入力します。
IPアドレス	[リモートゲートウェイアドレス]で[固定]を選択した場合に、VPN接続する相手(リモート先)のグローバルIPアドレスを入力します。
ローカルIPアドレス	VPN接続を許可するローカルIPアドレスを設定します。 ● すべてのローカルIPアドレスのパソコンからVPN接続を許可する場合は、ドロップダウンメニューで[全て]を選択します。 お使いのルータをVPN拠点通信用のセンター側ルータとして利用する場合は、[全て]を選択します。(『VPN拠点間通信を利用する場合』(P.113)) ● 単一のローカルIPアドレスのパソコンのみVPN接続を許可する場合は、ドロップダウンメニューで[単一アドレス]を選択します。この場合、[開始IPアドレス]欄にVPN接続を許可する端末のIPアドレスを入力します。 ● 範囲指定したローカルIPアドレスのパソコンからのみVPN接続を許可する場合は、ドロップダウンメニューで[範囲アドレス]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● IP アドレスとサブネットマスクで指定したローカル IP アドレスのパソコンからのみVPN接続を許可する場合は、ドロップダウンメニューで[サブネットアドレス]を選択します。この場合、[開始IPアドレス]欄にネットワークアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。

項目	説明
リモートIPアドレス	[リモートゲートウェイアドレス]欄で[固定]を選択した場合に、リモート先のIPアドレスを設定します。 ● リモート先のすべてのパソコンからVPN接続する場合は、ドロップダウンメニューで[全て]を選択します。 VPN拠点通信を利用する場合は、[全て]を選択します。(『VPN拠点間通信を利用する場合』(P.113)) ● リモート先の単一のパソコンにのみVPN接続する場合は、ドロップダウンメニューで[単一アドレス]を選択します。この場合、[開始IPアドレス]欄にVPN接続するリモート先のパソコンに設定されたIPアドレスを入力します。 ● 範囲指定したIPアドレスのパソコンにのみVPN接続する場合は、ドロップダウンメニューで[範囲アドレス]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● IPアドレスとサブネットマスクで指定したIPアドレスのパソコンにのみVPN接続する場合は、ドロップダウンメニューで[サブネットアドレス]を選択します。この場合、[開始IPアドレス]欄にネットワークアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。
NAT+VPN IPアドレス	NAT+VPN接続を許可するローカルIPアドレスを設定します。 IPアドレスが同じネットワークに同時にVPN接続する場合は、NAT+VPN 機能を使用します。(NAT+VPN 機能については、『NAT+VPN機能とは』(P.114)を参照してください。) ● すべてのNAT仮想IPアドレスのパソコンからVPN接続を許可する場合は、ドロップダウンメニューで[全て]を選択します。 ● 単一のNAT仮想IPアドレスのパソコンのみVPN接続を許可する場合は、ドロップダウンメニューで[単一アドレス]を選択します。この場合、[開始IPアドレス]欄にVPN接続を許可する端末の仮想IPアドレスを入力します。 ● 範囲指定したNAT仮想IPアドレスのパソコンからのみVPN接続を許可する場合は、ドロップダウンメニューで[範囲アドレス]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● IPアドレスとサブネットマスクで指定したNAT仮想IPアドレスのパソコンからのみVPN接続を許可する場合は、ドロップダウンメニューで[サブネットアドレス]を選択します。この場合、[開始IPアドレス]欄にネットワークアドレスを、[サブネットマスク]欄にサブネットマスクを入力します。 ● NAT+VPN 接続を使用しない場合は、ドロップダウンメニューで[使用しない]を選択します。

大切

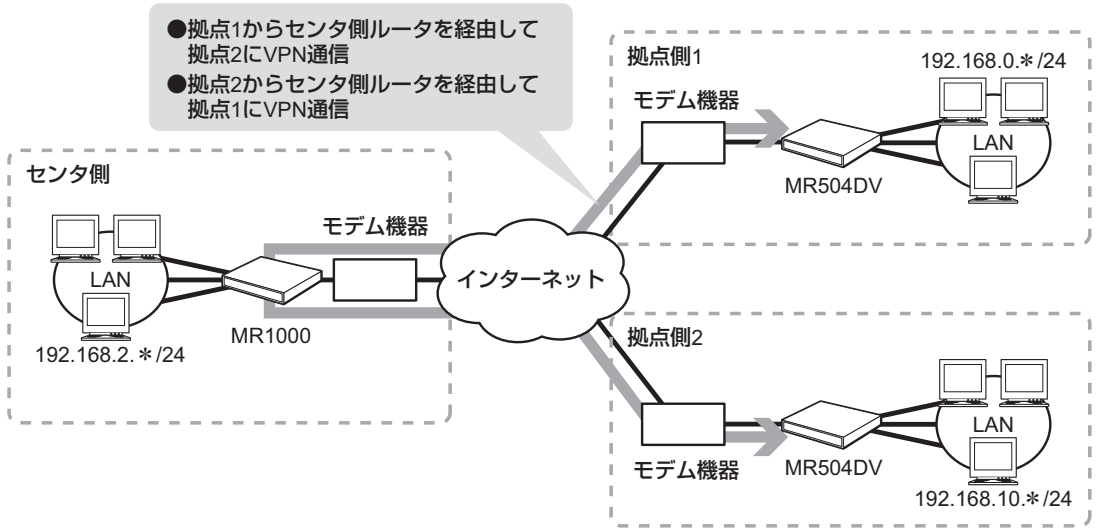
● [リモートゲートウェイアドレス] に [動的] が設定された VPN ポリシーを複数登録することはできますが、同時に 2 つ以上接続することはできません。

補足

VPN拠点間通信を利用する場合

VPN接続のセンタを介して拠点間でVPN接続し、データをやりとりすることができます。

VPN拠点間通信の例



上記の例では、それぞれのルータにおいて、以下のように設定します。

センタ側ルータ「MR1000」の設定(*1)

- ローカルIPアドレス:「全て」
- リモートIPアドレス:「全て」

拠点1ルータ設定

- ローカルIPアドレス:「192.168.0.0/24」
- リモートIPアドレス:「全て」

拠点2ルータ設定

- ローカルIPアドレス:「192.168.10.0/24」
- リモートIPアドレス:「全て」

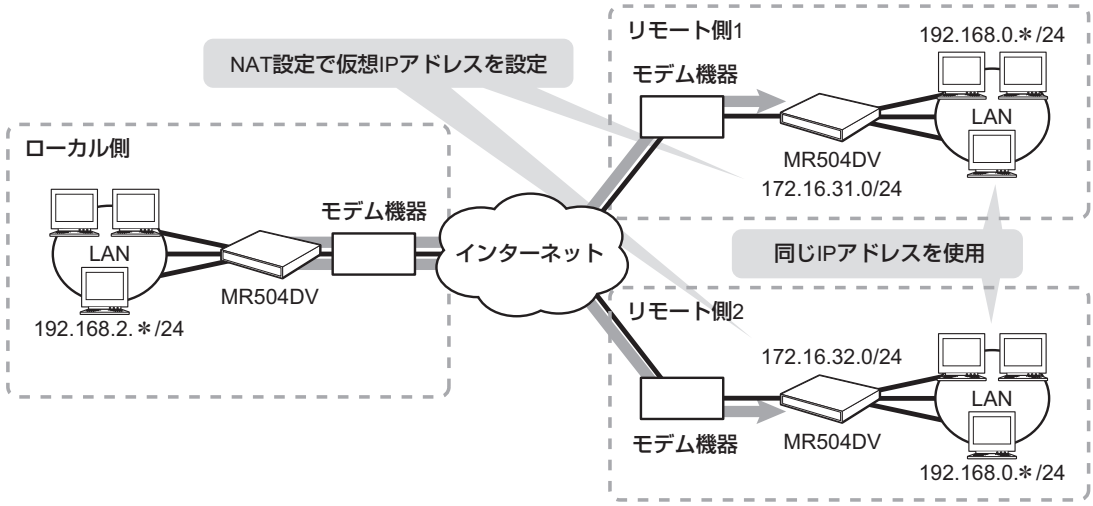
*1　センタ側ルータは、VPN ポリシーの設定として、ローカル IP アドレス、リモート IP アドレスともに「全て」を設定できる必要があります。

補足

NAT+VPN機能とは

リモート先のネットワークアドレスが他のリモート先のネットワークアドレスと同じ場合は、NAT+VPN機能を使用してIPSec接続することができます。
(注)NAT+VPN機能は、ローカル側とリモート側が別ネットワークアドレス体系であることが条件となります。同一ネットワークアドレス体系の場合は、NAT+VPN機能を使用しても、正しくVPN接続できません。

NAT+VPNの例



NAT+VPN機能を使用する場合は、NAT設定でネットワークの仮想IPアドレスを設定します。VPN接続する際は、NATで設定した仮想IPアドレスをリモート先のIPアドレスとして使用します。
上記の例では、それぞれのルータにおいて、以下のように設定します。

ローカル側ルータの設定

- メインモードのとき
  「172.16.31.0/24」および「172.16.32.0/24」をリモートIPアドレスとしたVPNポリシーを登録する
- アグレッシブモードのとき
  リモートIPアドレスの設定は不要

リモート側1ルータ設定

- NAT設定で以下のように設定(*1)
  - プライベートIPアドレス: 192.168.0.1-192.168.0.254
  - グローバルIPアドレス: 172.16.31.1-172.16.31.254
  - インターフェース: ipsec1
- VPNポリシーで以下のように設定
  - ローカルIPアドレス: 192.168.0.0/24
  - リモートIPアドレス: 192.168.2.0/24
  - NAT+VPN IPアドレス: 172.16.31.0/24

リモート側2ルータ設定

- NAT設定で以下のように設定(*1)
  - プライベートIPアドレス: 192.168.0.1-192.168.0.254
  - グローバルIPアドレス: 172.16.32.1-172.16.32.254
  - インターフェース: ipsec1
- VPNポリシーで以下のように設定
  - ローカルIPアドレス: 192.168.0.0/24
  - リモートIPアドレス: 192.168.2.0/24
  - NAT+VPN IPアドレス: 172.16.32.0/24

*1 NAT設定については、『7-7.NAT設定』(P.131)を参照してください。

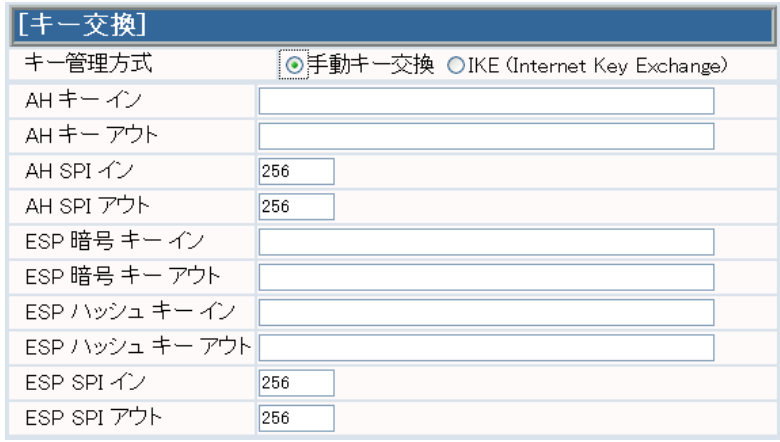
4. 認証　　：認証方式を設定します。

項目	説明
認証プロトコル	認証に使用するプロトコルを選択します。 ● 認証をしない場合は、[使用しない]を選択します。 ● ESPハッシュを使用する場合は、[ESP]を選択します。 ● AHハッシュを使用する場合は、[AH]を選択します。
アルゴリズム(AH)	[認証プロトコル]欄で[AH]を選択した場合に、AHハッシュのアルゴリズムを選択します。
アルゴリズム(ESP)	[認証プロトコル]欄で[ESP]を選択した場合に、ESPハッシュのアルゴリズムを選択します。
暗号化プロトコル	ESP暗号を使用するかどうかを選択します。
アルゴリズム	[暗号化プロトコル]欄で[ESP]を選択した場合に、ESP暗号のアルゴリズムを選択します。 [認証プロトコル]欄で[AH]を選択している場合はアルゴリズムに[NULL]を設定することはできません。[NULL]を選択すると、設定が正しくないため、設定を保存することができません。

5. キー交換　　：キー交換を設定します。[キー管理方式]で[手動キー交換]または[IKE(Internet Key Exchange)]を選択したかによって、設定項目が変わります。

項目	説明
キー管理方式	キー管理方式を選択します。[手動キー交換]または[IKE(Internet Key Exchange)]を選択したかによって、設定項目が変わります。 ● 手動で設定したキーを使用する場合は[手動キー交換]を選択します。ただし、[リモートゲートウェイアドレス]欄で[動的]が選択されている場合は、[手動キー交換]を選択することはできません。→『手動キー交換を選択した場合』(P.116) ● IKE(Internet Key Exchange)を使用する場合は[IKE(Internet Key Exchange)]を選択します。→『IKE(Internet Key Exchange)を選択した場合』(P.118)

手動キー交換を選択した場合



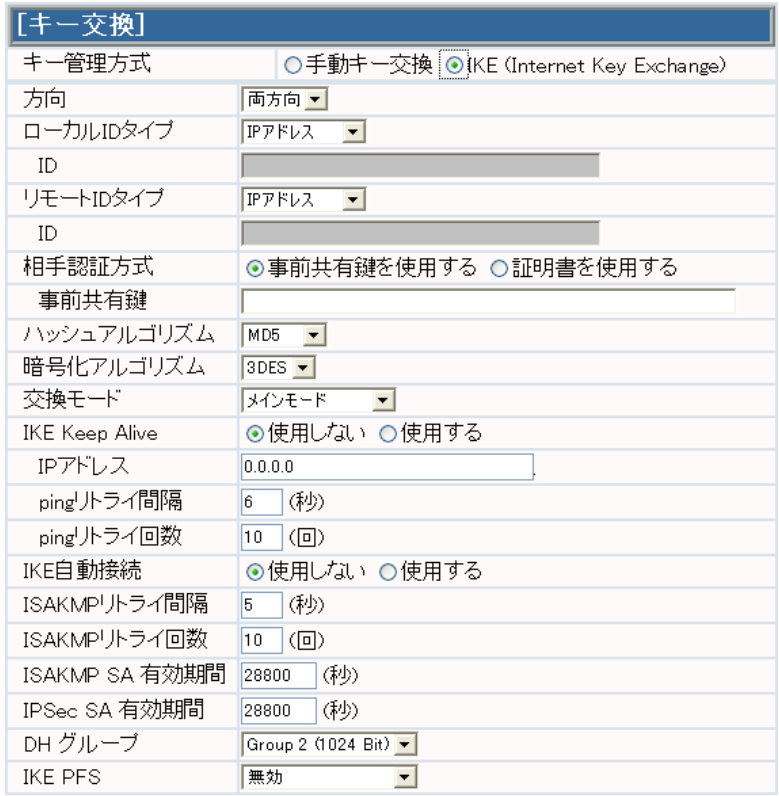
項目	説明
AHキーイン	[認証プロトコル]欄で[AH]を選択した場合に、AHハッシュに使用するInboud側のキーを入力します。[認証プロトコル]欄で[ESP]を選択している場合は、入力する必要はありません。 ● [アルゴリズム(AH)]欄で[MD5]を選択した場合は、32文字(半角英数字)でキーを入力します。 ● [アルゴリズム(AH)]欄で[SHA-1]を選択した場合は、40文字(半角英数字)でキーを入力します。
AHキーアウト	[認証プロトコル]欄で[AH]を選択した場合に、AHハッシュに使用するOutboud側のキーを入力します。[認証プロトコル]欄で[ESP]を選択している場合は、入力する必要はありません。 ● [アルゴリズム(AH)]欄で[MD5]を選択した場合は、32文字(半角英数字)でキーを入力します。 ● [アルゴリズム(AH)]欄で[SHA-1]を選択した場合は、40文字(半角英数字)でキーを入力します。
AH SPIイン	[認証プロトコル]欄で[AH]を選択した場合に、VPN機器が送信するセキュリティポリシーインデックス(SPI)の数値(4桁～8桁)を入力します。[AH SPIアウト]に入力する数値とは異なる数値を指定する必要があります。 [認証プロトコル]欄で[ESP]を選択している場合は、入力する必要はありません。
AH SPIアウト	[認証プロトコル]欄で[AH]を選択した場合に、VPN機器が送信するセキュリティポリシーインデックス(SPI)の数値(4桁～8桁)を入力します。[AH SPIイン]に入力する数値とは異なる数値を指定する必要があります。 [認証プロトコル]欄で[ESP]を選択している場合は、入力する必要はありません。
ESP暗号化キーイン	[暗号化プロトコル]欄で[ESP]を選択した場合に、ESP暗号化に使用するInboud側のキーを入力します。[暗号化プロトコル]欄で[使用しない]を選択している場合は、入力する必要はありません。 ● [暗号化プロトコル]欄下の[アルゴリズム]欄で[DES]を選択した場合は、16文字(半角英数字)でキーを入力します。 ● [暗号化プロトコル]欄下の[アルゴリズム]欄で[3DES]を選択した場合は、48文字(半角英数字)でキーを入力します。

項目	説明
ESP暗号化キーアウト	[暗号化プロトコル]欄で[ESP]を選択した場合に、ESP暗号化に使用するOutboud側のキーを入力します。[暗号化プロトコル]欄で[使用しない]を選択している場合は、入力する必要はありません。 ● [暗号化プロトコル]欄下の[アルゴリズム]欄で[DES]を選択した場合は、16文字(半角英数字)でキーを入力します。 ● [暗号化プロトコル]欄下の[アルゴリズム]欄で[3DES]を選択した場合は、48文字(半角英数字)でキーを入力します。
ESPハッシュキーイン	[認証プロトコル]欄で[ESP]を選択した場合に、ESPハッシュに使用するInboud側のキーを入力します。[認証プロトコル]欄で[AH]を選択している場合は、入力する必要はありません。 ● [アルゴリズム(ESP)]欄で[MD5]を選択した場合は、32文字(半角英数字)でキーを入力します。 ● [アルゴリズム(ESP)]欄で[SHA-1]を選択した場合は、40文字(半角英数字)でキーを入力します。
ESPハッシュキーアウト	[認証プロトコル]欄で[ESP]を選択した場合に、ESPハッシュに使用するOutboud側のキーを入力します。[認証プロトコル]欄で[AH]を選択している場合は、入力する必要はありません。 ● [アルゴリズム(EPS)]欄で[MD5]を選択した場合は、32文字(半角英数字)でキーを入力します。 ● [アルゴリズム(EPS)]欄で[SHA-1]を選択した場合は、40文字(半角英数字)でキーを入力します。
ESP SPIイン	[認証プロトコル]欄で[ESP]を選択した場合に、VPN機器が送信するセキュリティポリシーインデックス(SPI)の数値(4桁～8桁)を入力します。[ESP SPIアウト]に入力する数値とは異なる数値を指定する必要があります。 [認証プロトコル]欄で[AH]を選択している場合は、入力する必要はありません。
ESP SPIアウト	[認証プロトコル]欄で[ESP]を選択した場合に、VPN機器が送信するセキュリティポリシーインデックス(SPI)の数値(4桁～8桁)を入力します。[ESP SPIイン]に入力する数値とは異なる数値を指定する必要があります。 [認証プロトコル]欄で[AH]を選択している場合は、入力する必要はありません。

大切

- [キー交換]欄の設定は、接続するリモート先の VPN ポリシー設定と整合性がとれている必要があります。
- キー交換の設定を手動キーで設定する場合、それぞれのイン／アウトキーとSPIイン／アウトの値は、リモート先の VPN ポリシー設定と逆に設定する必要があります。

IKE(Internet Key Exchange)を選択した場合



項目	説明
方向	暗号キーのネゴシエーションを開始する方向を[起動者][応答者][両方向]から選択します。 [起動者]または[応答者]を選択した場合、相手側は自分の設定とは異なる[起動者]または[応答者]を選択してください。 [リモートゲートウェイアドレス]欄で[動的]を選択した場合は、[応答者]として設定されます。
ローカルIDタイプ	ローカルIPタイプを選択します。 ● 本製品のWAN側IPアドレスを使って認証を行う場合は[IPアドレス]を選択します。 ● [FQDN]または[USER FQDN]を選択した場合は、[ID]欄に認証に使用する文字を入力します。
ID	[ローカルIPタイプ]欄にて[FQDN]または[USER FQDN]を選択した場合は、この欄に認証に使用する文字を、最大32文字まで入力できます。
リモートIDタイプ	リモートIDタイプを選択します。 ● リモート先のWAN側IPアドレスを使って認証を行う場合は[IPアドレス]を選択します。 ● [FQDN]または[USER FQDN]を選択した場合は、[ID]欄に認証に使用する文字を入力します。
ID	[リモートIDタイプ]欄にて[FQDN]または[USER FQDN]を選択した場合は、この欄に認証に使用する文字を最大32文字まで入力できます。
相手認証方式	事前共有鍵か証明書を使用するか選択します。 証明書を使用する場合は、証明書(IPSec)の登録が必要となります。 →『7-5-2.証明書(IPSec)』(P.121)

項目	説明
事前共有鍵	[相手認証方式]欄で[事前共有鍵を使用する]を選択した場合に、最大49文字(半角英数字)で事前共有キーを入力します。リモート先で設定する事前共有キーと同じキーを入力する必要があります。
ハッシュアルゴリズム	ハッシュアルゴリズムを選択します。
暗号化アルゴリズム	暗号化アルゴリズムを選択します。
交換モード	IKEの交換モードを選択します。[リモートゲートウェイアドレス]欄で[動的]が選択されている場合は、[アグレッシブモード]として設定されます。 ● セキュリティよりもスピードを重視したい場合は、[メインモード]を選択します。ただし、[ローカルIDタイプ]欄と[リモートIDタイプ]欄両方で[IPアドレス]による認証を選択している場合のみ選択できます。 ● スピードよりもセキュリティを重視したい場合は、[アグレッシブモード]を選択します。
IKE Keep Alive	IKEキープアライブ機能を使用するかどうかを選択します。 IKEキープアライブ機能を使用すると、VPN接続が切断された場合に、自動的に再接続を行います。 IKE Keep Aliveを使用しPPPoEで接続する場合は、PPPoE登録時に[接続モード]を[常時接続]に設定してください。
IPアドレス	[IKE Keep Alive]欄で[使用する]を選択した場合に、VPN接続が切断されたかどうかを調べるためPINGを送信するIPアドレスを入力します。通常、リモート先のローカルIPアドレスを入力します。
pingリトライ間隔	[IKE Keep Alive]欄で[使用する]を選択した場合に、PINGを送信する間隔を秒単位で入力します。1～100まで入力できます。
pingリトライ回数	[IKE Keep Alive]欄で[使用する]を選択した場合に、PINGを送信する回数を入力します。1～100まで入力できます。ここで指定した回数PINGを送信しても応答がない場合に、IPSecが切断されたと認識します。
IKE自動接続	IKE自動接続機能を使用するかどうかを選択します。 IKE自動接続機能を使用すると、ルータ起動時に、自動的にIPSec接続を行います。
ISAKMPリトライ間隔	認証に失敗した場合に、認証を再送信する間隔を秒単位で入力します。1～100まで入力できます。
ISAKMPリトライ回数	認証に失敗した場合に、認証を再送信する回数を入力します。0～50まで入力できます。「0」を入力した場合は、一度認証に失敗するとそのままVPN接続を停止します。
ISAKMP SA有効期間	ISAKMPによる認証の有効期限を秒単位で入力します。1～9999999まで入力できます。認証に成功してから指定した秒数を経過すると、再認証を行います。
IPSec SA有効期間	IPSec SAによる認証の有効期限を秒単位で入力します。 1～9999999まで入力できます。認証に成功してから指定した秒数を経過すると、再認証を行います。
DHグループ	Diffie-Hellman鍵交換アルゴリズムを使用するグループを選択します。リモート先のDHグループの設定と同じグループを設定する必要があります。数値が大きいほどセキュリティが高くなるので、リモート先で[Group 2(1024 Bit)]が設定可能な場合は、[Group 2(1024 Bit)]を選択します。

項目	説明
IKE PFS	PFSを使用するかどうかを選択します。リモート先のIKE PFS設定と同じグループを設定する必要があります。 PFSを使用すると、暗号化を強化することができます。数値が大きいほどセキュリティが高くなるので、リモート先で[Group 2(1024 Bit)]が設定可能な場合は、[Group 2(1024 Bit)]を選択します。

6. MSS設定　　：MSS変換を使用するかどうかを設定します。

項目	説明
MSS変換機能	MSS変換機能をONにするかOFFにするかを選択します。 MSS変換機能をONにした場合、TCPによる通信で受信可能なセグメントサイズの最大値を変更することができます。MSS値を変更しないと利用できないサーバと通信したい場合は、MMS変換機能をONにします。ONにした場合は、[MSSサイズ]欄でMSSの最大値を入力します。
MSSサイズ	MSS変換機能をONにした場合に、通信可能なMSS最大値を入力します。MSSサイズは、MTUサイズから-40した値より大きいサイズを指定することはできません。(MSSサイズ< MTUサイズ-40) 例えば、MTUサイズが「1454」だった場合、MSSサイズに指定できる最大値は「1414」になります。

7. Path MTU Discovery　　：Path MTU DiscoveryのDFビットモードを設定します。

項目	説明
DFビット	DFビットのモードを設定します。 ● [コピー]を選択すると、DFビットをそのままIPSecトンネルの外側にコピーします。 ● [クリア]を選択すると、IPSecトンネルの外側のDFビットを0にします。 ● [セット]を選択すると、IPSecトンネルの外側のDFビットを1にします。

8. NAT-Traversal　　：NAT-Traversal機能を設定します。

項目	説明
NAT-Traversal機能	NAT-Traversal機能を使用するかどうかを選択します。 NAT環境においてVPN接続を利用したい場合は[使用する]に設定します。
IKEネゴシエーション機能	NAT環境においてVPN接続する場合に、IKEネゴシエーション機能を使用するかどうかを選択します。 VPN接続時に、相手先がNAT-Traversalに対応しているかどうかを確認するために使用します。また、途中経路でNATによるアドレス・ポート番号の変換が行われたかどうかを判断します。なお、この機能は相手先が本製品の場合のみ使用可能となります。

7-5-2. 証明書(IPSec)

IPSec通信用の証明書をインストールします。

補足

証明書のインストール手順

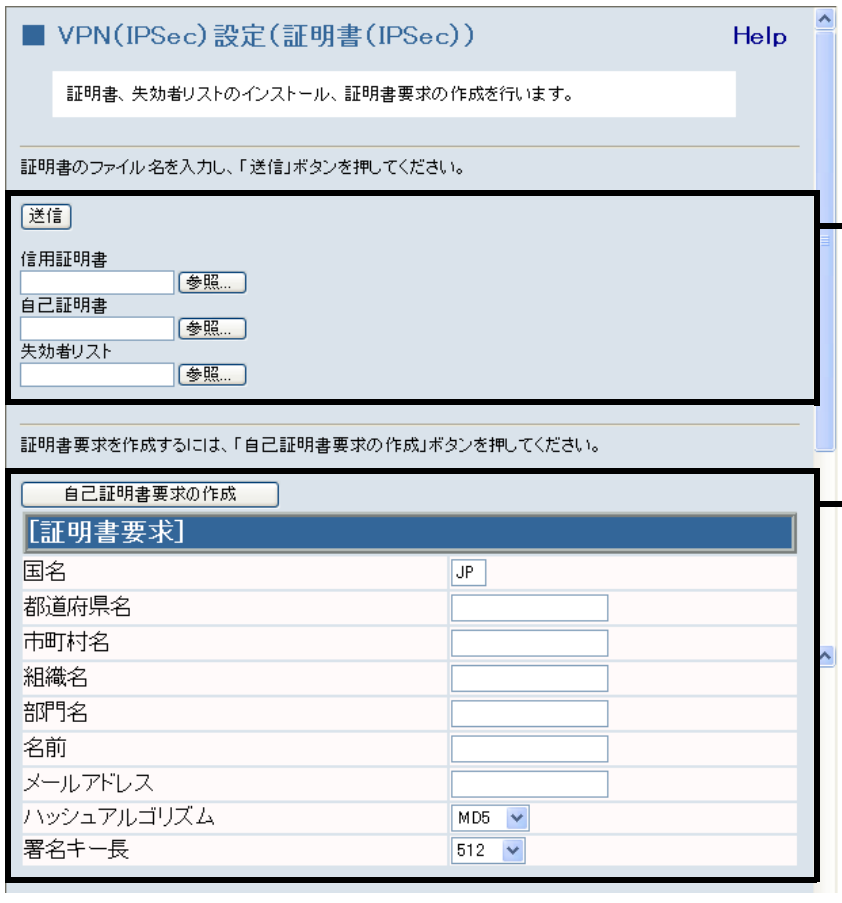
証明書のインストールは、以下の手順で行います。

1. CA(証明機関)から信用証明書ファイルを入手します。
2. [信用証明書]欄で入手した信用証明書ファイルを参照し、[送信]をクリックします。
3. [証明書要求]欄の各項目を入力し、[自己証明書要求の作成]をクリックして、自己証明書要求用の仮キーを表示します。
4. 表示された仮キーをコピーし、CA(証明機関)のホームページにアクセスし、コピーした仮キーを使用して自己証明書ファイルを入手します。
5. [自己証明書]欄で入手した自己証明書ファイルを参照し、[送信]をクリックします。

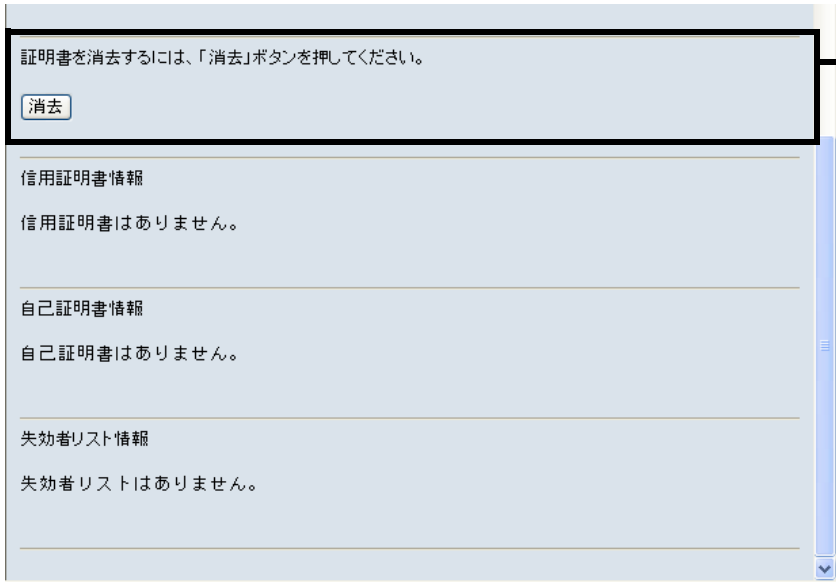
表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[VPN(IPSec)設定]→[証明書(IPSec)]の順にクリックします。

設定画面の説明



1. 証明書のインストール:信用証明書、自己証明書、失効者リストをインストールします。
2. 自己証明書要求：自己証明書要求用の署名キーを作成します。



3. 証明書の消去：証明書を消去します。

1. 証明書のインストール　　：　信用証明書、自己証明書、失効者リストをインストールします。

項目	説明
[送信]	クリックすると、[信用証明書] [自己証明書] [失効者リスト] で参照したファイルをインストールします。クリックする前にインストールしたいファイルを各欄で参照してください。
信用証明書	認証局(CA)から発行された信用証明書をインストールする場合は、[参照] をクリックして発行された証明書ファイルを選択します。
自己証明書	作成した自己証明書をインストールする場合は、[参照] をクリックして証明書ファイルを選択します。
失効者リスト	失効者リストをインストールする場合は、[参照] をクリックして失効者リストに追加する証明書ファイルを選択します。 秘密鍵の安全性が損なわれた場合などに、有効期限前に証明書を失効させたい場合は、失効させたい証明書ファイルを選択して、失効者リストに追加します。

2. 自己証明書要求　　：　自己証明書要求用の署名キーを作成します。

項目	説明
[自己証明書要求の作成]	クリックすると、[証明書要求] 欄で設定した内容で、自己証明書要求用の仮キーを表示します。
国名	国名を2桁のコードで入力します。あらかじめ「JP」が入力されているので、通常変更する必要はありません。
都道府県名	都道府県名を入力します。
市町村名	市町村名を入力します。
組織名	組織名を入力します。任意の名称を入力できます。
部門名	部門名を入力します。任意の名称を入力できます。
名前	名前を入力します。任意の名称を入力できます。
メールアドレス	メールアドレスを入力します。
ハッシュアルゴリズム	ハッシュアルゴリズムを選択します。

項目	説明
署名キー長	署名キー長を選択します。大きい数値ほど、セキュリティが高くなります。

3. 証明書の消去　　：証明書を消去します。

項目	説明
[消去]	クリックすると、インストールしたすべての証明書を消去します。

7-6. IPv6設定

本製品はIPv6に対応しています。
FLET'S.Netなど、IPv6を利用したネットワークに接続する場合に設定します。

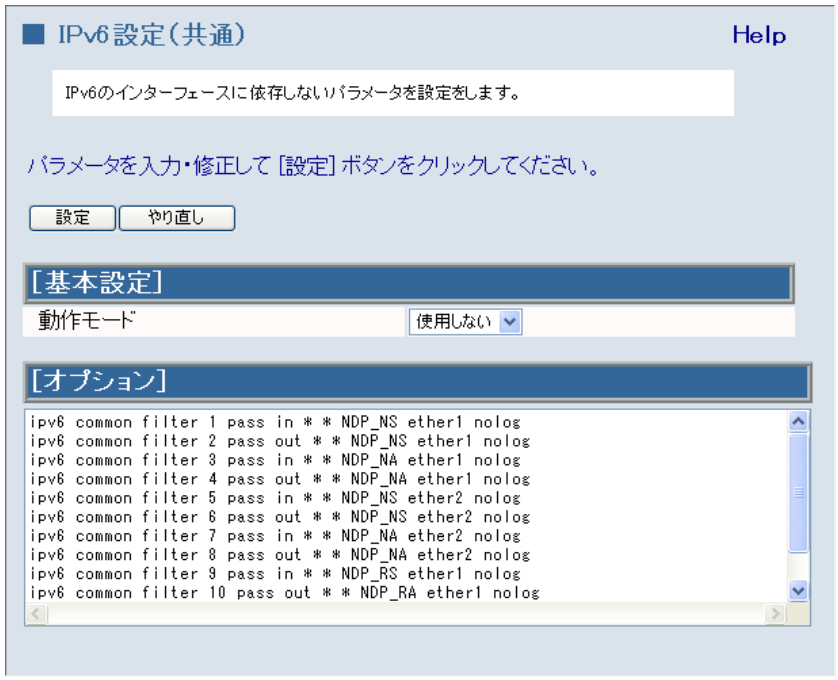
7-6-1. 共通

インターフェースに依存しないIPv6パラメータを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[IPv6設定]→[共通]の順にクリックします。

設定画面の説明



項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。
動作モード	IPv6の動作方法を選択します。 ● IPv6を使用する場合は、[使用する]を選択します。 ● IPv6による通信を透過しWAN↔LAN間をパススルーさせる(IPv6ブリッジ機能)場合は、[パススルー]を選択します。 ● IPv6を使用しない場合は、[使用しない]を選択します。

項目	説明
オプション	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

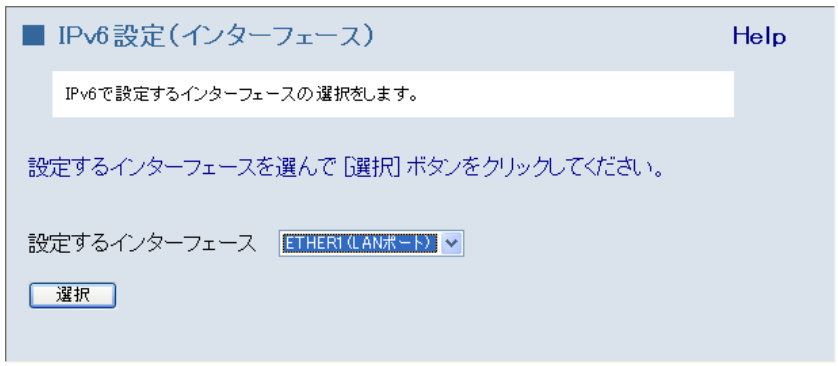
7-6-2. インターフェース

各インターフェースのIPv6パラメータを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[IPv6設定]→[インターフェース]の順にクリックします。

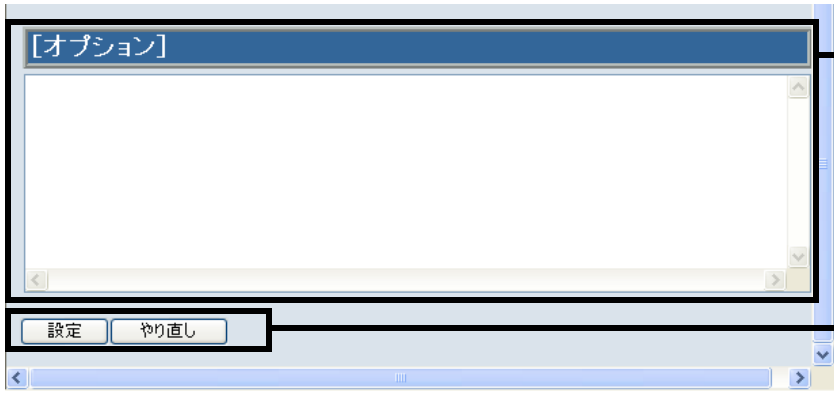
設定画面の説明



項目	説明
設定するインターフェース	IPv6を設定するインターフェースを選択します。
[選択]	クリックすると、「設定するインターフェース」で選択したインターフェースのIPv6設定画面が表示されます。

IPv6(インターフェース)画面の設定

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.128)
2. 基本：IPv6の基本情報を設定します。(P.128)
3. IPv6アドレス／プレフィックス1～5：各プレフィックスを設定します。(P.128)



4. オプション：上記項目で指定できない設定を、コマンドを入力して設定することができます。(P.129)

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.128)

1. 設定／やり直し　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 基本　：IPv6の基本情報を設定します。

項目	説明
登録インターフェース	選択したインターフェース名が表示されます。
インターフェースID	インターフェースIDを入力します。 インターフェースIDは、16進数を使用して16ビットごとにコロン(:)で区切り、16桁で入力します。 他機器で設定されているインターフェースIDは使用できません。 例:2001:db8:7654:3210
RA送信	RA(ルータ広報メッセージ:Router Advertisement Message)を送信する場合は[する]を選択します。 初期値:しない

3. IPv6アドレス／プレフィックス1~5：各プレフィックスを設定します。

項目	説明
IPv6アドレス／プレフィックス長	IPアドレスとプレフィックス長を設定します。 プレフィックス長は、48以上64以下で設定します。 例:2001:db8:7654:3210::1/64
アドレスタイプ	IPv6のアドレスタイプを設定します。 ● [ユニキャストアドレス(手動設定)]を選択すると、「インターフェースID」に入力した値をIPv6インターフェースIDとして設定します。 ● [ユニキャストアドレス(EUI-64 使用)]を選択すると、MAC アドレスがIPv6インターフェースIDとして設定されます。 ● 同じIPv6アドレスを他機器に設定し、それぞれ近くにいる同様のIPv6アドレスが設定された装置にアクセスするようにする場合は、「エニーキャストアドレス」を選択します。

項目	説明
プレフィックスの推奨有効時間	プレフィックスの推奨有効時間を設定します。 無期限にする場合は、[無期限] を選択します。 時間指定する場合は、[時間指定] を選択し、0～4294967294秒の間で時間を指定します。 初期値:604800
プレフィックスの最終有効時間	プレフィックスの最終有効時間を設定します。設定した時間を経過すると、指定したIPv6アドレスは無効になります。 無期限にする場合は、[無期限] を選択します。 時間指定する場合は、[時間指定] を選択し、0～4294967294秒の間で時間を指定します。 初期値:2592000
プレフィックスのフラグ	● 「on-link」では、プレフィックスのLフラグ(on-link flag)を立てる場合はチェックします。 ● 「自動設定」では、プレフィックスのAフラグ(Autonomous address-configuration flag)を立てる場合はチェックします。

4. オプション　：上記項目で指定できない設定を、コマンドを入力して設定することができます。

項目	説明
オプション	画面上の項目で設定できない内容を設定する必要がある場合に、コマンドをこの欄に入力します。 [オプション]欄で指定できる設定の詳細については、『コマンド一覧』を参照してください。

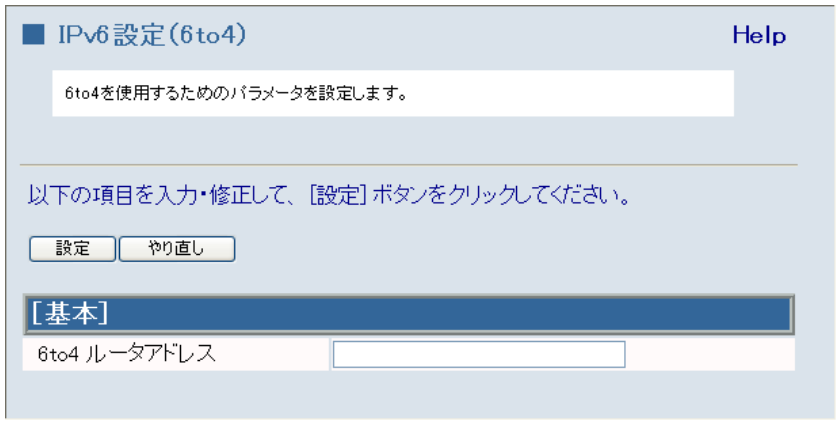
7-6-3. 6to4

6to4機能を設定します。
本製品を介して、IPv6を使用したサイトなどに接続する場合に設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[IPv6設定]→[6to4]の順にクリックします。

設定画面の説明



項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。
6to4ルータアドレス	相手側ルータのIPアドレスまたはドメイン名を入力します。

7-7. NAT設定

WAN側に割り当てられたグローバルIPアドレスとLAN側のパソコンのIPアドレスをマッピングし、インターネットからLAN内のパソコンにアクセスできるように設定します。

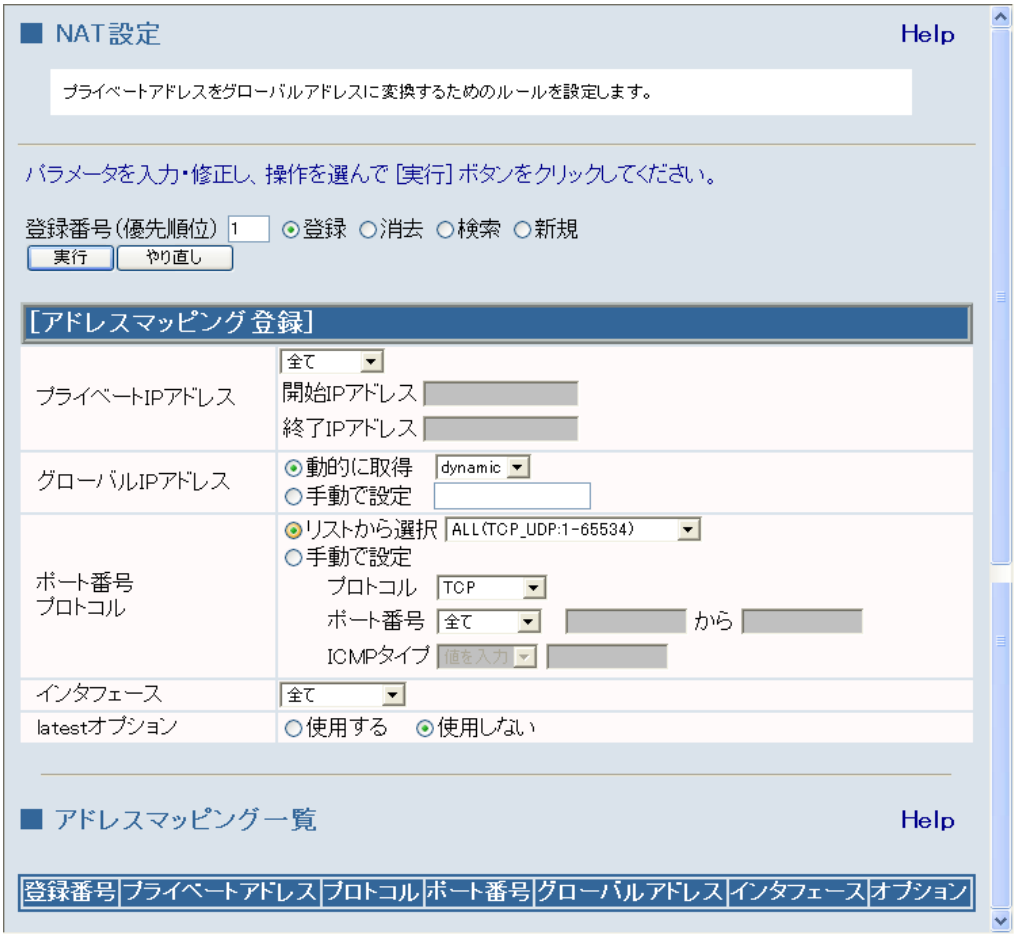
補足

- 本製品は出荷時の設定で、WAN側のグローバルIPアドレスをLAN側のパソコンで共有しインターネットに接続できるようにするNAPT機能をサポートしております。したがってNATを設定しなくても、LAN側に接続されたパソコンから本製品を介してインターネットに接続することが可能です。NATの設定は、インターネット側からLAN内のプライベートIPアドレスが設定されたパソコンに接続できるようにしたい場合や、LAN内のFTPサーバをインターネットに公開したい場合、Webサーバを公開したい場合、特定の受信パケットをLAN内のパソコンで受信できるようにしたい場合などに設定します。
- NAT/NAPT を使ってアドレス変換できる数は最大 128 件まで登録できます。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[NAT設定]をクリックします。

設定画面の説明



項目	説明
登録番号(優先順位)	登録、検索、または消去したいアドレスマッピングの登録番号を入力します。1～128まで登録できます。
登録／消去／検索／新規	実行する操作を選択します。 ● [登録]を選択し[実行]をクリックした場合は、[アドレスマッピング登録]にて設定した内容を[登録番号(優先順位)]に入力した番号で登録します。 ● [消去]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のアドレスマッピング設定を消去します。 ● [検索]を選択し[実行]をクリックした場合は、[登録番号(優先順位)]に入力した番号のアドレスマッピング設定を[アドレスマッピング登録]に反映します。すでに登録済みのアドレスマッピング設定を変更したい場合に便利です。 ● [新規]を選択し[実行]をクリックした場合は、[アドレスマッピング登録]にて設定した内容を、優先順位の高い未登録の登録番号で登録します。
[実行]	クリックすると、[登録]／[消去]／[検索]／[新規]で選択した操作を実行します。
[やり直し]	クリックすると、[アドレスマッピング登録]にて変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[実行]をクリックして有効になった内容はクリアされません。
プライベートIPアドレス	グローバルIPアドレスに割り当てるプライベートIPアドレスを設定します。 ● すべてのプライベートIPアドレスをグローバルIPアドレスに割り当てる場合は、ドロップダウンメニューで[全て]を選択します。 ● グローバルIPアドレスに割り当てるプライベートIPアドレスを範囲指定したい場合は、ドロップダウンメニューで[範囲指定]を選択します。この場合、[開始IPアドレス]と[終了IPアドレス]欄にそれぞれIPアドレスを入力します。 ● グローバルIPアドレスに割り当てるプライベートIPアドレスを固定のIPアドレスで指定したい場合は、ドロップダウンメニューで[個別]を選択します。この場合、[開始IPアドレス]欄に指定するIPアドレスを入力します。
グローバルIPアドレス	プライベートIPアドレスを割り当てるグローバルIPアドレスを設定します。 ● 本製品のWAN側グローバルIPアドレスが動的な場合は[動的に取得]を選択します。[動的に取得]を選択した場合、[dynamic] [ipcp] [dhcp]からグローバルIPアドレスを取得する方法を選択します。 PPPoE／PPTPなど相手先に適用される場合は[ipcp]を、WANポートに適用される場合は[dhcp]を、相手先およびWANポート全ての相手先に適用される場合は[dynamic]を選択します。 ● 割り当てるグローバルIPアドレスが固定の場合は、[手動で設定]を選択します。[手動で設定]を選択した場合、右欄に固定のグローバルIPアドレスを入力します。通常は、本製品WAN側に割り当てられた固定グローバルIPアドレスを入力します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>ポート番号
プロトコル</td><td>通信を許可するポート番号／プロトコルを設定します。
● 特定のプロトコルが使用するポート番号をすべて許可する場合は、[リストから選択] ドロップダウンメニューで条件に指定するプロトコルを選択します。
● 通信を許可するプロトコルやポート番号を手動で詳しく設定したい場合は、[手動で設定] を選択します。この場合、[プロトコル]、[ポート番号]、[ICMPタイプ] で条件を設定します。
<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>プロトコル</td><td>通信を許可するプロトコルの種類を選択します。</td></tr>
<tr><td>ポート番号</td><td>通信を許可するポート番号を設定します。選択したプロトコルが使用するすべてのポート番号を条件として設定する場合は、ドロップダウンメニューで [全て] を選択します。特定の範囲のポート番号を指定したい場合は、ドロップダウンメニューで [範囲指定] を選択し、右側欄にそれぞれ開始ポート番号と終了ポート番号を入力します。固定のポート番号のみを条件として設定したい場合は、ドロップダウンメニューで [個別] を選択し右側欄にポート番号を入力します。</td></tr>
<tr><td>ICMPタイプ</td><td>[プロトコル] 欄で [ICMP] を選択した場合に、通信を許可するICMP タイプを設定します。すべてのICMPタイプ許可する場合は、[全て] を選択します。ICMP タイプを指定したい場合は、[値を入力] を選択し、右側欄にICMPタイプを入力します。</td></tr>
</table></td></tr>
<tr><td>インターフェース</td><td>設定したアドレスマッピングを適用する相手先を選択します。指定したプライベートIPアドレスのパソコンからインターネットアクセスの要求があった場合に、指定した相手先を使用してインターネットに通信します。</td></tr>
<tr><td>latestオプション</td><td>プライベートIPアドレスの範囲が指定されている場合に、インターネット側から受信したパケットを最後にインターネット通信したパソコンに転送するかどうかを設定します。LAN内の特定のパソコンをインターネットからアクセスできるようにする場合には、[使用する] を選択します。
latestオプションを使用しない場合は、外部からのアクセスはすべて拒否します。</td></tr>
</table>

大切

- latest オプションを有効にすると、設定されているプロトコルおよびポート番号に対して、インターネットからのアクセスが可能な状態になります。latest オプションは、FTPサーバやWebサーバなど外部からのアクセスを許可する場合だけ設定するようにしてください。

7-8. UPnP設定

UPnP（Universal Plug and Play）の設定を行います。
同時に複数台のパソコンでWindows Messengerを使用したい場合や、NTT東日本およびNTT西日本が提供するVoIPアダプタを使用したIP電話サービスを使用したい場合に設定します。

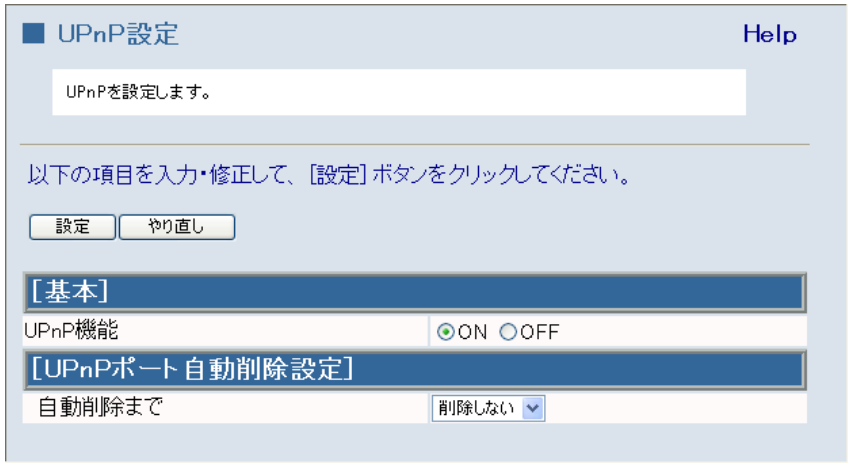
補足

- UPnPを利用してパソコン（Windows XP/Me/98）からWindows Messengerなどを使用するには、パソコンのUPnP機能も設定する必要があります。なお、Windows 2000/NT 4.0/95はUPnP機能を搭載していないため利用できません。
- VoIPアダプタを利用される場合は、本製品の［UPnP機能］をONにしてください。

表示方法

1. ［→詳細設定へ］をクリックして詳細設定画面を表示し、［UPnP設定］をクリックします。

設定画面の説明



項目	説明
［設定］	クリックすると、変更した内容を保存します。
［やり直し］	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度［設定］をクリックして有効になった内容はクリアされません。
UPnP機能	UPnP機能をONにするかOFFにするかを選択します。
自動削除まで	UPnP対応アプリケーションにより登録されたNAT情報を削除するかどうかを選択します。 削除する場合は、UPnP対応アプリケーションを終了してから、NAT情報を自動的に削除するまでの時間を選択します。

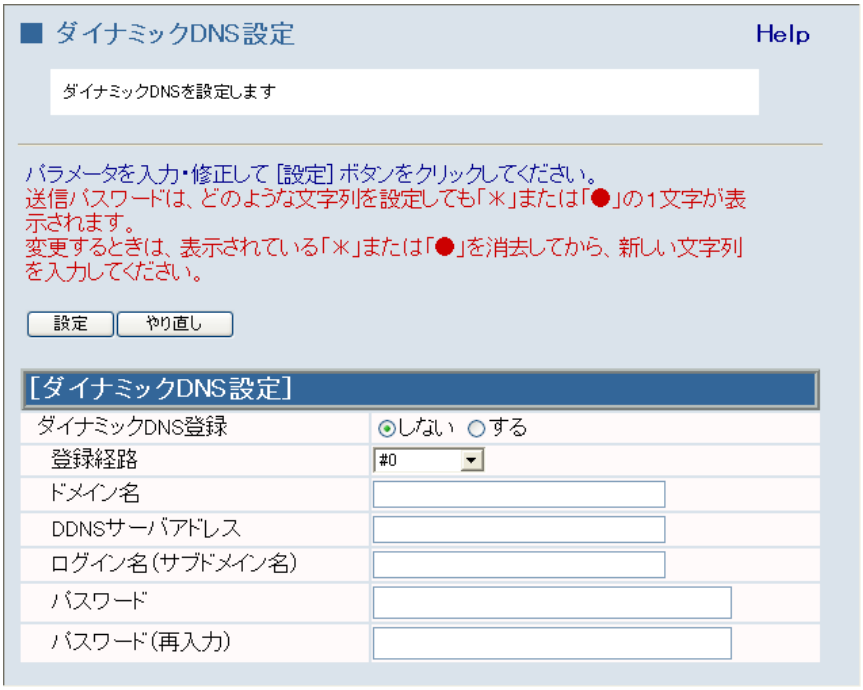
7-9. ダイナミックDNS設定

DDNSを設定します。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[ダイナミックDNS設定]をクリックします。

設定画面の説明



項目	説明
[設定]	クリックすると、変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。ただし、一度[設定]をクリックして有効になった内容はクリアされません。
ダイナミックDNS登録	DDNS登録をするかどうかを選択します。
登録経路	DDNS登録を行う際に使用する相手先の登録番号を選択します。
ドメイン名	DDNS登録するドメイン名を入力します。
DDNSサーバアドレス	ドメイン名を登録するDDNSサーバのIPアドレスを入力します。
ログイン名(サブドメイン名)	DDNSサーバにアクセスするためのログイン名を入力します。
パスワード	DDNSサーバにアクセスするためのパスワードを入力します。
パスワード(再入力)	[パスワード]欄に入力したパスワードを再入力します。

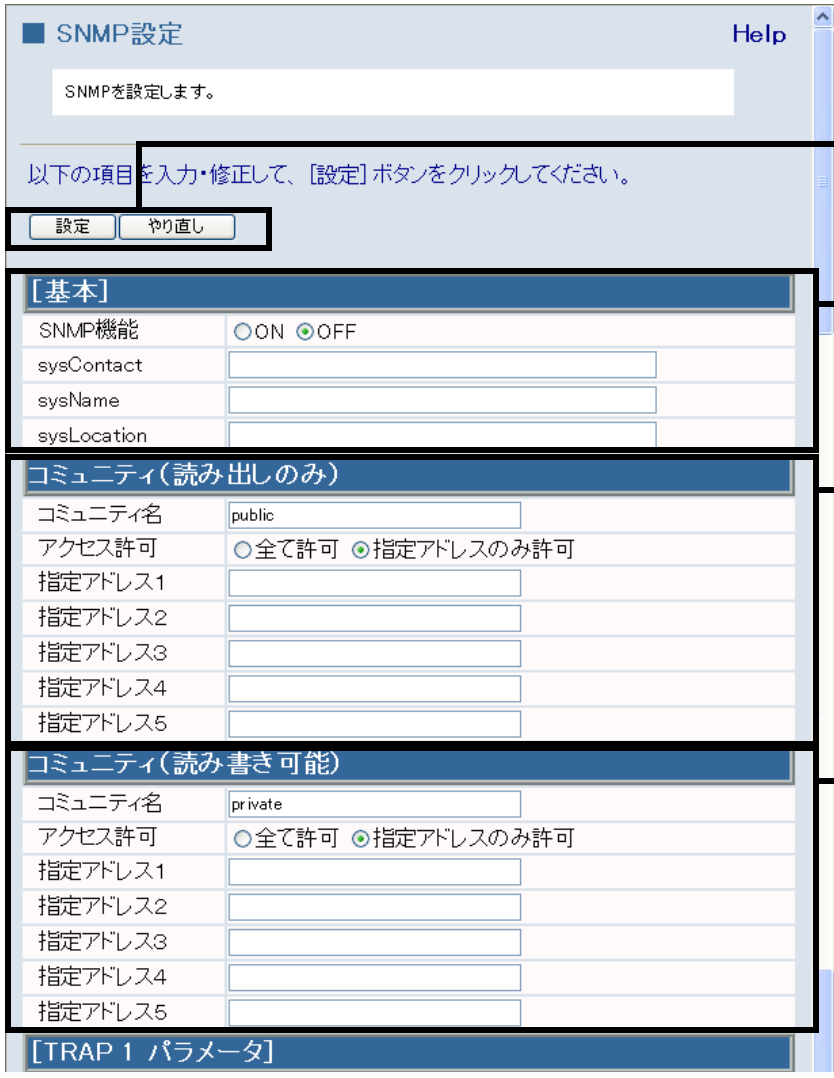
7-10. SNMP設定

SNMPエージェント機能を設定します。
外部のSNMPマネージャを使用して、本製品のルータ情報(MIB情報)を取得したい場合に設定します。
本製品では最大2つのSNMPマネージャへSNMPトラップを送信することができます。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[SNMP設定]をクリックします。

設定画面の説明



1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.137)
2. 基本：SNMPの基本情報を設定します。(P.137)
3. コミュニティ(読み出しのみ)：読み出し専用のコミュニティを設定します。(P.137)
4. コミュニティ(読み書き可能)：読み書き可能なコミュニティを設定します。(P.138)

5. TRAP1/2パラメータ：SNMPトラップを送信先を設定します。最大2つまで指定できます。(P.138)

1. 設定／やり直し：各設定で変更した内容を保存または破棄します。(P.137)

1. 設定／やり直し　：各設定で変更した内容を保存または破棄します。

項目	説明
[設定]	変更した内容を保存します。
[やり直し]	クリックすると、変更した内容をクリアし設定入力前の状態に戻します。だだし、一度[設定]をクリックして有効になった内容はクリアされません。

2. 基本　：SNMPの基本情報を設定します。

項目	説明
SNMP機能	SNMP機能を使用するかどうかを選択します。
sysContact	管理者の名前や連絡先を入力します。 1～255文字のASCII文字列で入力します。
sysName	機器の名称などを入力します。 1～255文字のASCII文字列で入力します。
sysLocation	機器の設置場所などを入力します。 1～255文字のASCII文字列で入力します。

3. コミュニティ(読み出しのみ)　：読み出し専用のコミュニティを設定します。

項目	説明
コミュニティ名	読み出し専用のコミュニティ名を入力します。 1～32文字の半角英数字で入力します。 初期値:public

項目	説明
アクセス許可	読み出しを許可するエージェントを制限するかどうかを設定します。 ● すべてのエージェントへ読み出しを許可する場合は[全て許可]を選択します。 ● 指定した IP アドレスのエージェントへのみ読み出しを許可する場合は、[指定アドレスのみ許可]を選択します。これを選択した場合は、「指定アドレス1～5」に指定するIPアドレスを入力します。
指定アドレス1～5	「アクセス許可」で[指定アドレスのみ許可]を選択した場合に、読み出しを許可するエージェントのIPアドレスを入力します。最大５つまで指定することができます。

4. コミュニティ(読み書き可能) : 読み書き可能なコミュニティを設定します。

項目	説明
コミュニティ名	読み書き専用のコミュニティ名を入力します。 1～32文字の半角英数字で入力します。 初期値:private
アクセス許可	読み書きを許可するエージェントを制限するかどうかを設定します。 ● すべてのエージェントへ読み書きを許可する場合は[全て許可]を選択します。 ● 指定した IP アドレスのエージェントへのみ読み書きを許可する場合は、[指定アドレスのみ許可]を選択します。これを選択した場合は、「指定アドレス1～5」に指定するIPアドレスを入力します。
指定アドレス1～5	「アクセス許可」で[指定アドレスのみ許可]を選択した場合に、読み書きを許可するエージェントのIPアドレスを入力します。最大５つまで指定することができます。

5. TRAP1/2パラメータ : SNMPトラップを送信先を設定します。最大2つまで指定できます。

項目	説明
コミュニティ名	SNMPトラップを送信するコミュニティ名を入力します。 1～32文字の半角英数字で入力します。
trap送信先IP	SNMPトラップを送信するホストのIPアドレスを入力します。
inform	informを送信するかどうかを選択します。
start	start トラップ(再起動時に送信するトラップ)を送信するかどうかを選択します。
link-down	link-downトラップ(WAN側が遮断されたときに送信するトラップ)を送信するかどうかを選択します。 PPPoE接続している場合は、遮断されたときにlink-down トラップが送信されます。DHCP の場合は、DHCP アドレスを解放したときにlink-downトラップが送信されます。
link-up	link-upトラップ(WAN側が接続されたときに送信するトラップ)を送信するかどうかを選択します。 PPPoE接続している場合は、接続されたときにlink-up トラップが送信されます。DHCPの場合は、DHCPアドレスを取得したときにlink-upトラップが送信されます。
authfail	authfail トラップ(指定されたコミュニティでの認証失敗時に送信するトラップ)を送信するかどうかを選択します。

7-11. 管理コマンド・設定

7-11-1. 再起動

本製品を再起動します。本製品の設定を変更し、再起動画面で[再起動]をクリックした場合と同じように、このページで本製品の再起動を手動で操作することができます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[管理コマンド・設定]→[再起動]の順にクリックします。**
   - クイック設定画面の[管理コマンド・設定]→[再起動]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[再起動]をクリックした場合と同様です。画面説明については、『6-2-1.再起動』(P.41)を参照してください。

7-11-2. 設定の消去

本製品の設定を消去して、出荷時の設定に戻します。
全設定を出荷時の設定に戻すか、または希望の項目を選択して、その項目だけを出荷時の設定に戻すこともできます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[管理コマンド・設定]→[設定の消去]の順にクリックします。**
   - クイック設定画面の[管理コマンド・設定]→[設定の消去]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[設定の消去]をクリックした場合と同様です。画面説明については、『6-2-2.設定の消去』(P.42)を参照してください。

7-11-3. ユーザ・パスワード変更

ルータ設定画面にアクセスするためのユーザIDおよびパスワードを設定します。ブロードバンドや専用線でインターネットに常時接続する場合は、外部からの侵入を防ぐために設定することをお勧めします。
本製品では、管理者用のユーザID・パスワードを１つ、またユーザ用のユーザID・パスワードを3つまで設定することができます。

補足

- 管理者用のユーザ ID およびパスワードの設定は、[ブロードバンドで接続]の[PPPoE]、[IPアドレス自動取得(DHCP)]、[固定IPアドレス]のページでも設定することができます。

表示方法

1. [→詳細設定へ]をクリックして詳細設定画面を表示し、[管理コマンド・設定]→[ユーザ・パスワード変更]の順にクリックします。

・ クイック設定画面の[管理コマンド・設定]→[ユーザ・パスワード変更]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[ユーザ・パスワード変更]をクリックした場合と同様です。画面説明については、『6-2-3.ユーザ・パスワード変更』(P.43)を参照してください。

7-11-4. アクセス権限

ルータ設定画面のアクセス権限をユーザごとに設定します。管理者でログインした場合またはユーザID・パスワードが設定されていない場合のみ表示されます。

表示方法

1. [管理コマンド・設定]→[アクセス権限]の順にクリックします。

・ クイック設定画面の[管理コマンド・設定]→[アクセス権限]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[アクセス権限]をクリックした場合と同様です。画面説明については、『6-2-4.アクセス権限』(P.45)を参照してください。

7-11-5. ファームウェア更新

新しいファームウェアが公開された場合は、このページを使ってファームウェアを更新することができます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[管理コマンド・設定]→[ファームウェア更新]の順にクリックします。**
   - クイック設定画面の[管理コマンド・設定]→[ファームウェア更新]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[ファームウェア更新]をクリックした場合と同様です。画面説明については、『6-2-5. ファームウェア更新』(P.48)を参照してください。

7-11-6. 設定メンテナンス

このメニューをクリックすると、設定メンテナンス画面が別ウィンドウで表示されます。
設定メンテナンス画面では、直接設定ファイルを編集して、本製品の設定を変更することができます。
また、設定をHTML形式やテキスト形式にして、ファイルに保存することができます。HTML形式で保存したファイルを読み込むことで設定を復元することができます。


大切

- 誤った設定を入力した場合、本製品が正常に動作しなくなることがあります。設定の入力方法がわからない場合は、絶対に変更しないでください。誤って設定を保存してしまった場合は、本製品の背面にある［リセット］ボタンを長押しして、出荷時の設定に戻して再度本製品の設定をやり直してください。

補足

設定をHTML形式で保存する／HTML形式で保存したファイルを読み込む

設定をHTML形式で保存するには、設定メンテナンス画面を表示した状態で、ブラウザの[ファイル]－[名前を付けて保存]で保存します。
保存したHTMLファイルから設定を復元したい場合は、保存したHTMLファイルをダブルクリックしてブラウザで開き、[設定]をクリックします。(ただし、設定メンテナンス画面をHTML保存した後に、本製品のLAN側IPアドレスが変更されていた場合は、HTMLファイルから設定を復元することはできません。)
保存したファイルの読み込みが完了すると、自動的に再起動のページが表示されますので、[再起動]をクリックして本製品を再起動してください。

設定をテキスト形式で保存する／テキスト形式で保存したファイルを読み込む

設定をテキスト形式で保存するには、設定メンテナンス画面に表示された設定情報をコピーし、メモ帳などにペーストしてテキストファイルとして保存します。
保存したテキストファイルから設定を復元したい場合は、設定メンテナンス画面を表示し、保存したテキストファイルから設定情報をコピーして、設定メンテナンス画面にペーストし、[設定]をクリックします。
保存したファイルの読み込みが完了すると、自動的に再起動のページが表示されますので、[再起動]をクリックして本製品を再起動してください。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[管理コマンド・設定]→[設定メンテナンス]の順にクリックします。**
   - クイック設定画面の[管理コマンド・設定]→[設定メンテナンス]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[管理コマンド・設定]→[設定メンテナンス]をクリックした場合と同様です。画面説明については、『6-2-6. 設定メンテナンス』(P.49)を参照してください。

7-12. 切断／接続状況

7-12-1. PPTP

手動でPPTP回線を切断します。また、PPTP回線の接続状況を確認することができます。
本製品ではPPTPを最大2回線同時に接続することができます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[切断／接続状況]→[PPTP]の順にクリックします。**
   - クイック設定画面の[切断／接続状況]→[PPTP]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[切断／接続状況]→[PPTP]をクリックした場合と同様です。画面説明については、『6-3-1.PPTP』(P.51)を参照してください。

7-12-2. PPPoE

手動でPPPoE回線を切断します。また、PPPoE回線の接続状況を確認することができます。
本製品ではPPPoEを最大4回線同時に接続することができます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[切断／接続状況]→[PPPoE]の順にクリックします。**
   - クイック設定画面の[切断／接続状況]→[PPPoE]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[切断／接続状況]→[PPPoE]をクリックした場合と同様です。画面説明については、『6-3-2.PPPoE』(P.53)を参照してください。

7-13. 情報表示

7-13-1. 設定

設定情報を表示します。

表示方法

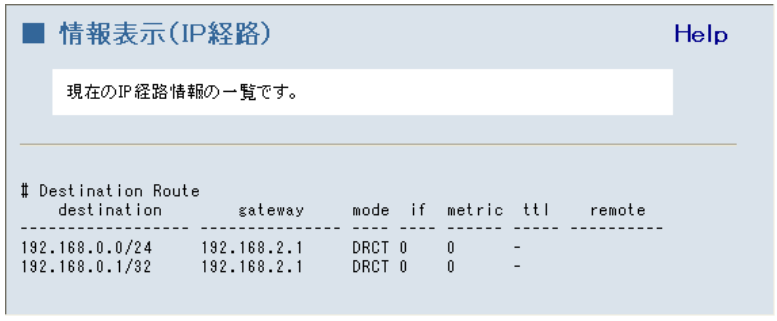
1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[設定]の順にクリックします。**
   - クイック設定画面の[情報表示]→[設定]をクリックしても同様の画面が表示されます。

7-13-2. IP経路

現在のIP経路情報を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[IP経路]の順にクリックします。**
   - クイック設定画面の[情報表示]→[IP経路]をクリックしても同様の画面が表示されます。



7-13-3. ログ

ログの表示および消去を操作します。以下のログを表示または消去することができます。

- DoS攻撃防御
- ファイアウォール
- インターネットアクセス
- アクセスコントロール
- VPN
- 全て

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[ログ]の順にクリックします。**
   - クイック設定画面の[情報表示]→[ログ]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の[情報表示]→[ログ]をクリックした場合と同様です。画面説明については、『6-4-3.ログ』(P.56)を参照してください。

7-13-4. WAN状況

現在のWANの接続状況を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[WAN状況]の順にクリックします。**
   - クイック設定画面の[情報表示]→[WAN状況]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[WAN状況]をクリックした場合と同様です。画面説明については、『6-4-4.WAN状況』(P.57)を参照してください。

7-13-5. UPnP状況

UPnPの設定情報やMessengerなどによる通信で要求されたポートマッピングの情報を確認できます。また、ポートマッピングの情報を消去することができます。

補足

- 本製品の電源を入れ直した場合や本製品を再起動した場合は、ポートマッピング情報は自動的に消去されます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[UPnP状況]の順にクリックします。**
   - クイック設定画面の[情報表示]→[UPnP状況]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[UPnP状況]をクリックした場合と同様です。画面説明については、『6-4-5.UPnP状況』(P.58)を参照してください。

7-13-6. IPSec状況

IPSecに関する情報を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[IPSec状況]の順にクリックします。**
   - クイック設定画面の[情報表示]→[IPSec状況]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[IPSec状況]をクリックした場合と同様です。画面説明については、『6-4-6.IPSec状況』(P.59)を参照してください。

7-13-7. IPv6アドレス

IPv6アドレスの一覧を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[IPv6アドレス]の順にクリックします。**
   - クイック設定画面の[情報表示]→[IPv6アドレス]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[IPv6アドレス]をクリックした場合と同様です。画面説明については、『6-4-7.IPv6アドレス』(P.60)を参照してください。

7-13-8. IPv6経路

現在のIPv6経路情報を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[IPv6経路]の順にクリックします。**
   - クイック設定画面の[情報表示]→[IPv6経路]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[IPv6経路]をクリックした場合と同様です。画面説明については、『6-4-8.IPv6経路』(P.60)を参照してください。

7-13-9. SNMP情報

SNMPに関する情報を表示します。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[情報表示]→[SNMP情報]の順にクリックします。**
   - クイック設定画面の[情報表示]→[SNMP情報]をクリックしても同様の画面が表示されます。

設定画面の説明

表示される画面は、クイック設定画面の、[情報表示]→[SNMP情報]をクリックした場合と同様です。画面説明については、『6-4-9.SNMP情報』(P.61)を参照してください。

7-14. その他

7-14-1. オンラインヘルプ

オンラインヘルプを表示します。

補足

- 各設定ページにある［Help］をクリックしても、オンラインヘルプを表示することができます。

表示方法

1. **[→詳細設定へ]をクリックして詳細設定画面を表示し、[その他]→[オンラインヘルプ]の順にクリックします。**
   - クイック設定画面の[その他]→[オンラインヘルプ]をクリックしてもオンラインヘルプを表示することができます。

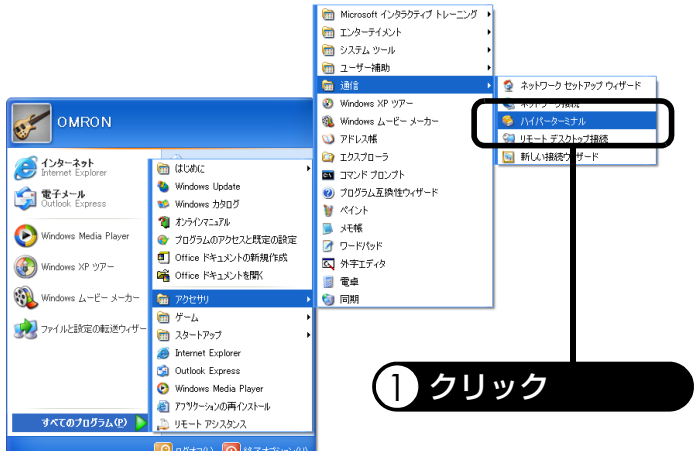
8. コマンドを使った設定方法

本製品では、telnetプログラムやコマンドプロンプトを使って設定することができます。
この章では、ハイパーターミナルやコマンドプロンプトで本機に接続するまでの手順を説明します。コマンドを使った本製品の設定方法については、『コマンド一覧』を参照してください。

8-1. ハイパーターミナルを使った設定方法

＊　Windows XPの画面を参照してご説明しております。

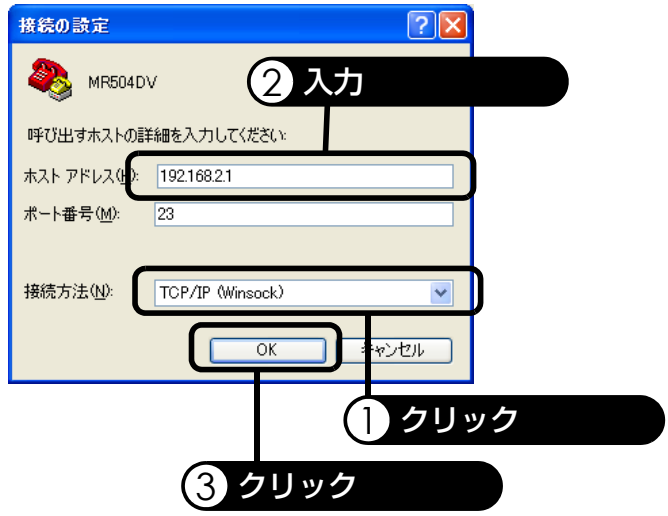
1. [スタート]－[すべてのプログラム]－[アクセサリ]－[通信]－[ハイパーターミナル]の順にクリックします。



2. 接続の設定画面が表示されるので、[名前]欄に任意の接続名を入力し、[OK]をクリックします。

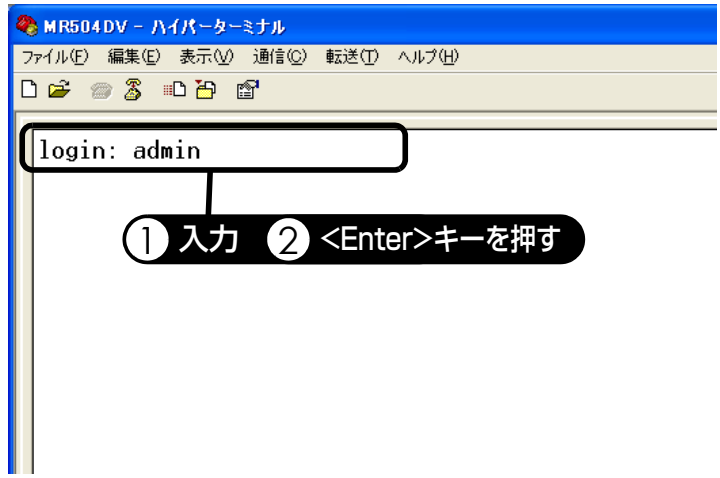
3. **[接続方法]欄で[TCP/IP (Winsock)]を選択し、[ホストアドレス]欄に「192.168.2.1」を入力して、[OK]をクリックします。**

・ ルータのIPアドレスをすでに変更していた場合は、[ホストアドレス]欄にはルータのIPアドレスを入力してください。
・ [ポート番号]欄にはあらかじめ「23」が入力された状態になっています。そのまま変更しないでください。



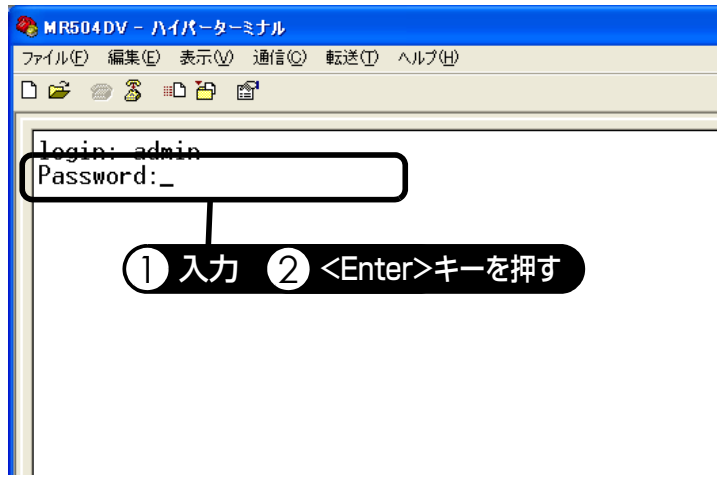
4. **ハイパーターミナル画面が表示され、「login:」が画面に表示されます。**
管理者用ユーザIDを入力し、<Enter>キーを押します。

・ 出荷時の設定では、管理者用ユーザIDは「admin」です。



5. **管理者用パスワードが設定されている場合は、「Password:」が画面に表示されます。**
設定したパスワードを入力し、<Enter>キーを押します。

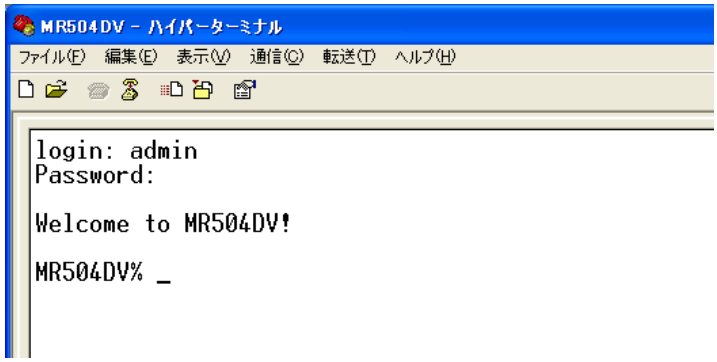
・ 出荷時の設定では、パスワードは設定されていません。パスワードを設定していない場合は、「Password:」を表示せずに、そのままログインします。



補足

- パスワードを入力しても、カーソル位置には何も表示しません。パスワードを入力する際には、正しいキーを押していることを確認しながら入力してください。

6. ログインに成功すると、「Welcome to MR504DV!」が表示されます。

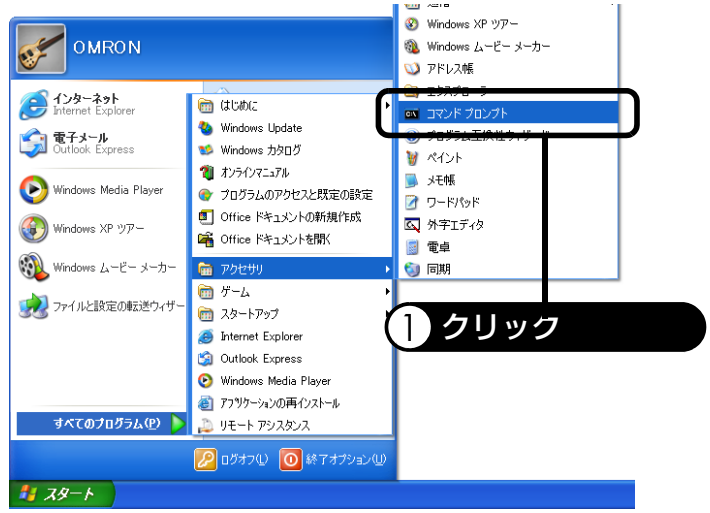


以上でログインは完了です。

8-2. コマンドプロンプトを使った設定方法

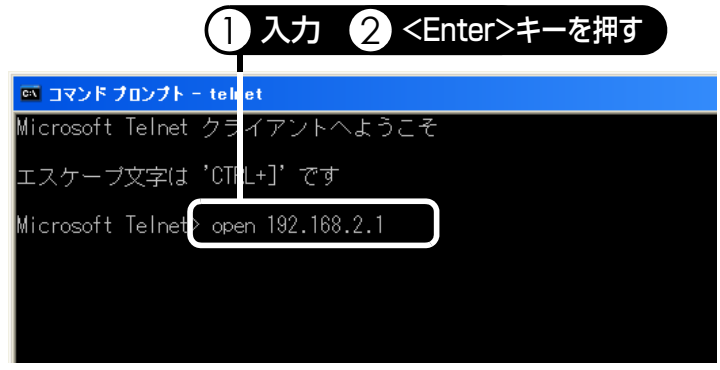
＊　Windows XPの画面を参照してご説明しております。

1. [スタート]－[すべてのプログラム]－[アクセサリ]－[コマンドプロンプト]の順にクリックします。

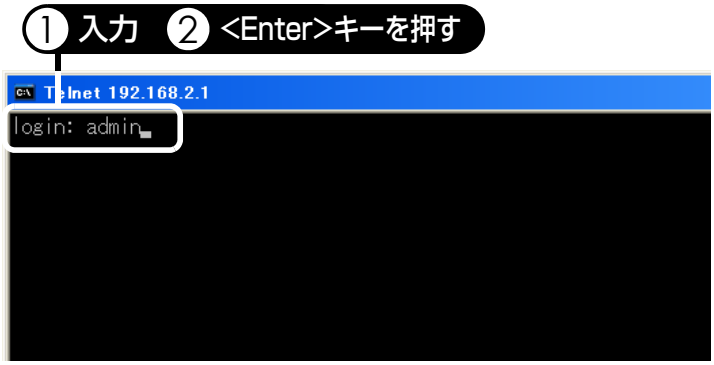


2. コマンドプロンプトが起動したら、「telnet」と入力し、<Enter>キーを押します。

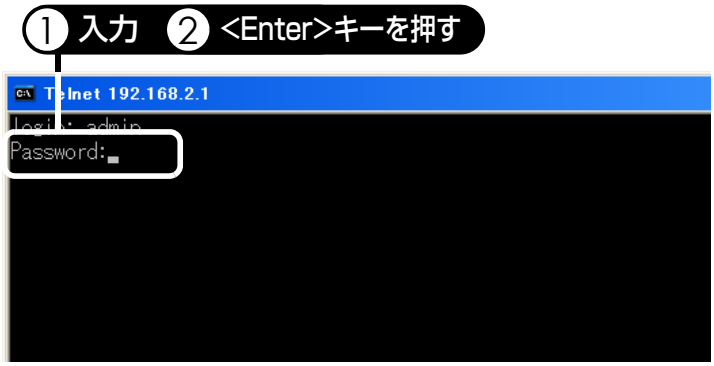
3. 「Microsoft Telnet>」が表示されたら、「open 192.168.2.1」と入力し、<Enter>キーを押します。
   - ルータのIPアドレスをすでに変更していた場合は、「192.168.2.1」の代わりにルータのIPアドレスを入力してください。



4. 「login:」が画面に表示されます。
管理者用ユーザIDを入力し、<Enter>キーを押します。
・ 出荷時の設定では、管理者用ユーザIDは「admin」です。



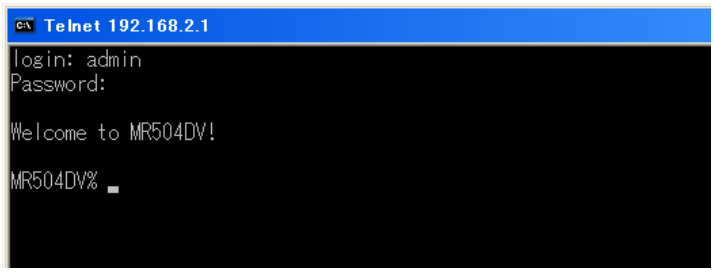
5. 管理者用パスワードが設定されている場合は、「Password:」が画面に表示されます。
設定したパスワードを入力し、<Enter>キーを押します。
・ 出荷時の設定では、パスワードは設定されていません。パスワードを設定していない場合は、「Password:」を表示せずに、そのままログインします。



補足

- パスワードを入力しても、カーソル位置には何も表示しません。パスワードを入力する際には、正しいキーを押していることを確認しながら入力してください。

6. ログインに成功すると、「Welcome to MR504DV!」が表示されます。



以上でログインは完了です。

9. 困ったときには

本製品の動作やインターネット接続に問題がある場合の対策や各種要望などについて説明します。本章に記載されている対策でも解決されない場合は、当社カスタマサポートセンタ（TEL：0120−77−4717）へお問い合わせください。

1. ACアダプタを電源コネクタに接続しても、[電源]ランプが点灯しない

対策1 本製品に同梱されているACアダプタを使用していることを確認してください。

対策2 電源プラグがコンセントに正しく接続されていることを確認してください。

対策3 ACアダプタがコンセントに正しく接続されていることを確認してください。
また、別のコンセントにACアダプタを接続していただき、[電源]ランプが点灯するかご確認ください。

対策1～3を実施しても[電源]ランプが点灯しない場合は、本製品が故障しています。本書巻末の「修理依頼票」を利用して、当社周辺機器修理センタへ修理依頼をしてください。『12.修理・問い合わせ』（P.165）を参照してください。

2. 初期画面が表示されない

LANポートに接続している場合

対策1 ルータの電源が入っていることを確認してください。
電源が入っている場合には、[電源]ランプが緑色に点灯します。

対策2 LANケーブルがルータに正しく接続されていること、およびLANケーブルがパソコンに正しく接続されていることを確認してください。
ルータの電源が入っていて、LANケーブルでパソコンと正しく接続されている場合には、LANケーブルを接続した[LAN]ポートの[Link/Act]ランプが、緑色に点灯します。

対策3 ブラウザの設定に間違いがないことを確認してください。
ブラウザの設定がLAN経由になっていることを確認してください。
Macintoshをお使いの場合は、次の設定を確認してください。

● Macintosh の場合
ブラウザの[編集]－[初期設定]－[ネットワーク]を選択して表示される[プロキシ]画面で、「Webプロキシ」にチェックマークが付いている場合は、外してください。

対策4 ルータのIPアドレスを変更していないことを確認してください。
IPアドレスを変更している場合は、アドレスの入力欄に変更したIPアドレスを入力してください。変更したIPアドレスがわからない場合は、ルータをリセットするとIPアドレスが「192.168.2.1」になります。リセット方法は背面パネルにある[リセット]ボタンを10秒以上押します。ルータの全ての設定を、工場出荷状態に戻すことができます。

対策5
ルータの設定に使用するパソコンは、直接接続されているか、同一LAN上で接続されていることを確認してください。
異なるLANセグメントからでは、ルータの設定画面を開くことができません。

対策6
すでに構成されているLAN環境にルータを導入する場合は、ルータのIPアドレス「192.168.2.1」を他の機器で使用していないことを確認してください。
他の機器で使用している場合は、ルータに別のIPアドレスを割り当てるまで、その機器の電源を切ってください。

対策7
お使いのパソコンの設定を確認してください。

対策8
パソコンのローカルIPアドレスを取得し直してください。
方法は、『9.困ったときには』の『7.IPアドレスが競合してしまう(複数台のパソコンを接続した場合にメッセージが表示される)』(P.158)のパソコンの設定を行ってください。

DMZポートに接続している場合

対策1
前面パネルのDMZポートの[Link/Act]ランプが点灯または点滅している場合は正しくクロスケーブルで接続できています。DMZポートの[Link/Act]ランプが消灯している場合は、接続しているケーブルが正しくないか、接続した機器の電源が入っていません。DMZポートはクロスケーブルを使用します。クロスケーブルを別途お買い求め頂き、接続してください。

対策2
DMZポートには複数台の機器を接続できません。1台のみ直接クロスケーブルで接続してください。ハブを接続することもできません。

対策3
『LANポートに接続している場合』の対策1、3、4、6～8(P.154～P.155)を参照してください。

3. インターネットに接続できない

対策1
[WAN]ランプが点灯していることを確認してください。
[WAN]ランプが点灯していない場合は、以下の対策を参照して、設定を確認してください。
(1) パソコンやルータ、モデム機器がそれぞれ正しく接続されていることを確認してください。
モデム機器が、ADSLやFTTH、CATV回線と接続(リンク)した状態になってから設定を開始してください。(お使いのモデム機器によっては、ランプの点灯などで確認できます。)
接続(リンク)できない場合は、モデム機器の電源を入れ直し、接続(リンク)されたことを確認してください。
(2) ルータの設定が正しい手順で行われていることを確認してください。
設定方法については、『5-2.ルータの設定』(P.15)を参照してください。また、すでに構成されているLAN環境にルータを導入する場合は、『7-3-2.LAN』(P.79)を参照してください。

対策2 Bフレッツやフレッツ・ADSLなどPPPoEに対応した事業者に接続する場合、ユーザ名、パスワードが間違って入力していないことを確認してください。ユーザ名は@を含むフルドメインで入力してください。

対策3 ADSLをご利用の場合は、ADSL接続ソフトが起動していないことを確認してください。起動していなくても接続できない場合は、アンインストール(削除)してください。

対策4 Bフレッツやフレッツ ADSLなどPPPoEに対応した事業者をご利用で、モデムに「PPPoEブリッジ機能」を設定している場合は、解除して「ブリッジモード」に設定を変更してください。

対策5 本製品とモデムの電源を10分間程度切り、モデム→ルータの順に電源を入れてみてください。

4. ホームページが表示されない

対策1 『9.困ったときには』の『3.インターネットに接続できない』(P.155)を確認してください。

対策2 アドレス欄に表示させたいURLアドレスが、正しく入力されていることを確認してください。他のホームページアドレスでも同様に表示できないか確認してください。

対策3 プロバイダからDNS情報を送信していない場合があります。
その場合はプロバイダから提供されているDNSサーバIPアドレスをパソコンに設定してください。設定方法は、次の対策4を参照してください。

対策4 パソコンのIPアドレスを固定で設定している場合は、プロバイダから提供されているDNSサーバIPアドレスをパソコンに設定してください。

● WindowsXP/Server 2003/2000 の場合
[次のDNSサーバのアドレスを使う]にチェックマークをつけ、DNSサーバIPアドレスを入力し、[OK]をクリックしてください。

● WindowsMe/98/95 の場合
[DNS設定]タブをクリックし、[DNSを使う]にチェックマークをつけ、[ホスト]に任意の名前を入力します。[DNSの検索順]にDNSサーバIPアドレスを入力し、[追加]－[OK]の順にクリックしてください。その後、パソコンを再起動してください。

● Windows NT 4.0 の場合
[DNS]タブをクリックし、[ホスト名]に任意の名前を入力します。[DNSの検索順]にDNSサーバIPアドレスを入力し、[追加]－[OK]の順にをクリックしてください。その後、パソコンを再起動してください。

● Mac OS 8.x/9.x/Mac OS X の場合
[ネームサーバアドレス]または[ドメインネームサーバ(オプション)]にDNSサーバIPアドレスを入力、左上のクローズボックスをクリックしてください。

＊ [ネームサーバアドレス]欄に入力できないときには、TCP/IPの[編集]－[利用者モード]を選択し、[詳しい情報も指定]をクリックし、[OK]をクリックしてください。[ネームサーバアドレス]欄が入力できるようになります。

5. ルータに設定したIPアドレスやパスワードを忘れてしまった

対策1

工場出荷状態に戻します。背面パネルにある[リセット]ボタンを10秒以上押します。ルータのすべての設定を、初期状態に戻すことができます。初期状態のIPアドレスは「192.168.2.1」です。
その後、設定しなおしてご利用ください。

6. Windows Me/98/95で[ネットワーク]画面に「TCP/IP→xxxxx(お使いのLANアダプタ名)」が表示されない

対策1

以下の設定内容を確認してください。

(1) [スタート]－[設定]－[コントロールパネル]－[ネットワーク]の順にダブルクリックし、[ネットワーク]画面を表示して、「xxxxx(お使いのLANアダプタ名)」が表示されていることを確認してください。表示されている場合は、(2)以降へ進んでください。表示されていない場合は、お使いのLANアダプタが正しく認識されていない可能性があります。LANアダプタの再インストールをお試しください。

(2) [追加]をクリックしてください。

(3) [プロトコル]を選択し、[追加]をクリックしてください。

(4) [製造元]は[Microsoft]を選択し、[ネットワークプロトコル]は[TCP/IP]を選択し、[OK]をクリックしてください。

(5) [ネットワーク]画面に「TCP/IP－＞xxxxx(お使いのLANアダプタ名)」が表示されます。

(6) [ネットワーク]画面を閉じるときに、パソコンの再起動を求める確認メッセージが表示される場合は、[はい]をクリックして、パソコンを再起動してください。

＊ ネットワークの設定を変更する場合、WindowsのCD-ROMを要求される場合があります。その場合は、画面の指示に従って操作してください。

7. IPアドレスが競合してしまう(複数台のパソコンを接続した場合にメッセージが表示される)

対策1

IPアドレスを固定(DHCP使わない)されている場合は、IPアドレスが他のパソコンと同じ値になっていないかご確認ください。
IPアドレスを自動的に取得(DHCP使う)されている場合は、各OS別に対策方法が異なります。
以下の手順にしたがって設定をおこなってください。

● Windows XP の場合
(1) [ローカルエリア接続の状態]－[サポート]タブを開いてください。
(2) [修復(P)]ボタンをクリックしてください。

● Windows Me/98/95 の場合
(1) [IP設定]の画面を表示してください。
(2) [すべて解放]－[すべて更新(またはすべて書き換え)]の順にクリックしてください。

● Windows 2000/NT 4.0 の場合
(1) [コマンドプロンプト]画面を表示してください。
(2) 「ipconfig /release」(ipconfigと/releaseの間は半角スペース)と入力し、<Enter>キーを押してください。
(3) 「ipconfig /renew」(ipconfigと/renewの間は半角スペース)と入力し、<Enter>キーを押してください。

● Mac OS 8.x/9.x の場合
(1) [TCP/IP]画面を表示し、設定を確認してください。
(2) [設定方法]が[手入力]になっている場合は IP アドレスが他のパソコンと同じ値になっていないかを確認してください。
[設定方法]が[DHCPサーバを参照]になっている場合は、パソコンを再起動してください。

● Mac OS X の場合
(1) [TCP/IP]画面を表示し、設定を確認してください。
(2) [TCP/IP]タブの[設定]が[手入力]になっている場合は IP アドレスが他のパソコンと同じ値になっていないかを確認してください。
[TCP/IP]タブの[設定]が[DHCPサーバを参照]になっている場合は、パソコンを再起動してください。

8. Netscape Navigatorにてルータの設定画面を開くと、「Java Script error」が表示される。または表示色が変化する。

対策1

お使いのNetscape Navigatorを最新バージョンにアップグレードした後、ルータの設定画面を開いてください。

9.　ファームウェアアップグレード後に、ルータの設定画面が表示されない。

対策1

パソコンのIPアドレスの解放／書き換え（更新）を行ってください。方法は『9.困ったときには』の『7.IPアドレスが競合してしまう（複数台のパソコンを接続した場合にメッセージが表示される）』（P.158）の対策1を参照してください。

10. ファイアウォール設定したが、設定が有効になっていない。

対策1

ルータの設定画面の［管理コマンド・設定］にて［再起動］をクリックしてください。

10. 用語集

インターネット関連

ブラウザ

インターネットでホームページを見るときに使用するソフトウェアです。
Internet Explorer や Netscape Navigator が代表的です。

プロバイダ

パソコンをインターネットに接続するサービスを提供する会社です。ADSL によるインターネット接続を行う場合には、プロバイダとの契約が必要です。ISP と表現することもあります。

ネットワーク関連

10BASE-T

伝送速度が 10Mbps で、ツイストペアケーブルを使用するイーサネットの規格です。接続する機器間は、最長 100m まで延長できます。

100BASE-TX

伝送速度が 100Mbps で、カテゴリー5 以上の UTP ケーブルを使用するイーサネットの規格です。接続する機器間は、最長 100m まで延長できます。

ADSL回線(非対称デジタル加入回線)

すでに一般家庭に広く普及している電話回線で、音声伝送では使わない高い周波数域を使って、インターネットへの高速接続を実現する通信手段です。異なる周波数域を利用するため、電話とインターネットを同時に使用できます。

ADSLモデム

ADSL 回線に接続するためのデータ変調／復調装置です。通常のアナログモデムと同様に、デジタルデータを変調してアナログ信号に変換したり、その逆を行います。

CATV(ケーブルテレビ)

CATV は、家庭に直接専用ケーブルを引き込みます。このテレビ配信用ケーブルを利用してインターネットに接続するのが CATV 接続です。

DHCPサーバ機能

ネットワークにアクセスしてきた相手に、自動で IP アドレスを割り当てる機能です。ネットワークに接続するときは、接続する機器に IP アドレスを設定しなければなりませんが、DHCP サーバ機能を使用すれば、IP アドレスを自動で設定してくれるため、設定する必要がなくなります。

DNS

インターネット上の IP アドレスとドメイン名を対応させるシステムのことです。IP アドレスとドメイン名の対応に関する情報をサーバが保有しているため、ユーザは数字の羅列である IP アドレスではなく、ドメイン名を指定してインターネットにアクセスできます。

Ethernet

LAN を構築するときの通信方式の規格（プロトコル）です。接続方法と通信速度を決めています。

FTTH

各家庭に光ファイバーケーブルを引き込み、高速にインターネットに接続できるサービスです。

IPSec

VPN を利用する際に通信を暗号化するための規格です。

IPアドレス

インターネットやLAN上で各パソコンを識別するための番号で、「192.168.2.1」のような 4 組の数字で表現します。インターネットに接続するときは、それぞれのパソコンが個別のIPアドレスを持つ必要がありますが、プロバイダを通じて接続するときは、通常は自動で割り当てられるため、特に設定する必要はありません。

LAN(ローカルエリアネットワーク)

家庭やオフィスなど、限られた範囲で構築するコンピュータネットワークのことです。ローカルエリアネットワーク（LAN）の略でランと読みます。LAN を構築することにより、LAN 内にある周辺機器を共有したり、同じ LAN 内のパソコン同士でデータのやり取りを行うことが可能です。

MACアドレス

Ethernet 機器が持つ 6 バイトのアドレスです（例：00 00 F4 30 00 01）。MAC アドレスは、機器固有のもので、同じアドレスは存在しません。

NAPT

NAPT とは、1 つのグローバル IP アドレスを、複数のプライベート IP アドレスで共有する機能です。この機能を持つことにより、1 つのグローバル IP アドレスを LAN 上で共有することができるため、複数台のパソコンから同時にインターネット接続することができます。

PPP

パソコン同士が 1 対 1 で通信を行うときに使われるプロトコルです。電話回線を使ったダイヤルアップ接続などで使われます。

PPPoA

PPPoA（PPP over ATM）は、ATM ネットワーク上で PPP でプロバイダに接続を実現する機能です。

PPPoE

PPPoE（PPP over Ethernet）は、LAN の通信方式であるイーサネットを介して、PPP でのプロバイダ接続を実現する機能です。

PPTP

暗号通信のためのプロトコルです。2 台のコンピュータで行う通信を暗号化します。インターネットを介した LAN 間接続をしたり、リモートアクセスしたりするときに使います。

TCP/IP

インターネットでのデータ通信に使用されている通信方法（プロトコル）です。異なるプラットフォーム間でデータ転送するための通信基準になっています。

VPN

公衆回線やインターネット経由で事業所間などを接続する技術です。通信相手を認証したり通信を暗号化して、セキュリティで保護することで、あたかも専用線を引いているように通信できます。バーチャル・プライベート・ネットワークと言います。

WAN(ワイドエリアネットワーク)

電話回線などを使って、別の建物にあるコンピュータ同士でデータのやり取りを行えるように設定されている場合は、LAN ではなく WAN といいます。LAN よりも広範囲にわたるネットワーク環境です。インターネットは WAN になります。

クライアント

インターネットや LAN 上で、サーバが持っている機能やデータを利用するコンピュータです。

ケーブルモデム

CATV を使用したインターネット接続には、一般の電話線からインターネット接続する際の「モデム」の役割を果たす「ケーブルモデム」が必要です。CATV 接続用のケーブルモデムは、原則的に市販されていません。
CATV 事業者がケーブルモデム自体でユーザの個別認識を行っているため、また、CATV 回線の品質保持の問題から、CATV 事業者で把握していないケーブルモデムが回線上に接続されるのを防ぐためです。CATV 事業者からレンタルしたケーブルモデムをご使用ください。

サーバ

インターネットや LAN 上で、自身の持っている機能、周辺機器、データなどを、他のコンピュータ（クライアント）に提供するコンピュータです。WEB サーバやメールサーバ、プリンタサーバなどがあります。

ファイアウォール

LAN 環境などのサーバやコンピュータ、および LAN 環境内の情報などを、外部からのウィルスや不正侵入者から守る装置や機能の総称です。

プロトコル

コンピュータとコンピュータがデータ通信するときの方法のことです。PPP や TCP/IP などが代表的なプロトコルです。

ルータ

ネットワーク間（LAN と LAN、LAN と WAN）の接続を行うネットワーク機器の 1 つで、ネットワークアドレスの情報を元にネットワーク間のパケットの送信を行います。

その他

ファームウェア

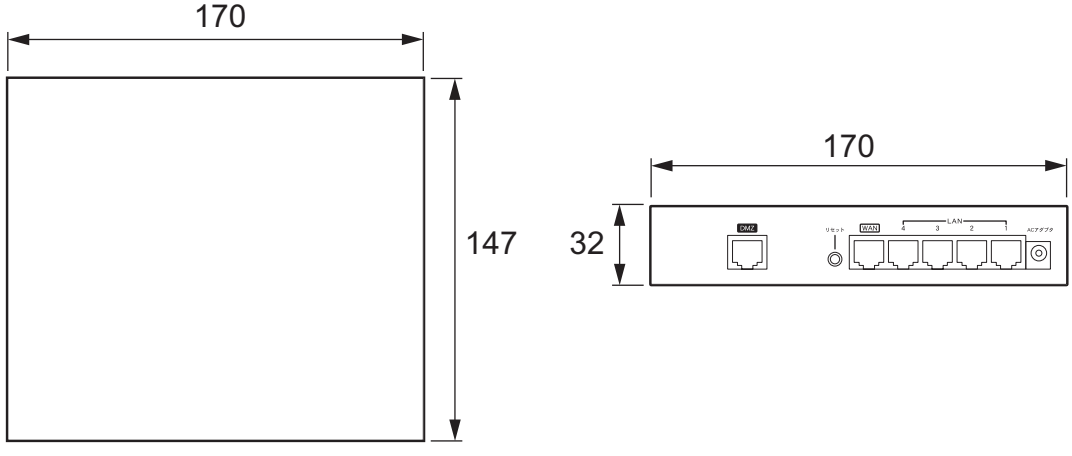
ハードウェアの内部に搭載されていて、ハードウェアの機能や性能、動作の制御に関わるプログラムです。

11. 仕様

ハードウェア

CPU	Cavium CN200		
フラッシュメモリサイズ	2MB		
ネットワーク インターフェース	WANポート	ポート数	1
		規格	IEEE802.3(10BASE-T) IEEE802.3u(100BASE-TX)
		コネクタ形状	RJ-45(メス)
	LANポート	ポート数	4
		規格	IEEE802.3(10BASE-T) IEEE802.3u(100BASE-TX)
		コネクタ形状	RJ-45(メス)
		MDI/MDI-X自動認識機能(全4ポート)	
	DMZポート	ポート数	1
		規格	IEEE802.3(10BASE-T) IEEE802.3u(100BASE-TX)
		コネクタ形状	RJ-45(メス)
LED	電源×1、状態×1、LAN(Link/Act)×4、LAN(10/100)×4、WAN×1、PPPoE×1、DMZ(Link/Act)×1、DMZ(10/100)×1		
電源	入力	AC100V±5%、50/60Hz(専用ACアダプタ)	
	消費電力	最大8W	
環境条件	温度0～40℃　湿度25～85%(結露なきこと)		
本体外形寸法	170(W)×147(D)×32(H)mm		
本体質量	約700g以下(ACアダプタ除く)		
電波障害防止	VCCIクラスA		
保証	購入日より1年間保証		

外形寸法図(単位:mm)



ソフトウェア

サポートプロトコル	IP		
アドレス変換	NAT、NAPT（変換規則はNATとNAPTあわせて64件まで登録可能。）		
DHCP機能	サーバ機能		接続可能クライアント数　最大253台
	クライアント機能		
ドメイン名／ホスト名入力	対応		
仮想サーバ機能	対応（PPPoEの4セッションすべてで使用可能）		
MTU値調整機能	対応（設定可能範囲540-1500）		
MACアドレス変更	MACアドレスクローン		可能
	手動変更		可能
PPPoE	PPPoEクライアント機能 （接続数4セッション）		LAN側からのインターネット接続要求時に自動的にPPPoE接続を開始
	IPアンナンバード		対応（NATとの併用可能）
	自動接続機能		
	セッション・キープ・アライブ		
	無通信時自動切断機能		
ルーティング	IPv4	動的ルーティング（RIP1）、静的ルーティング（最大64件）	
	IPv6	静的ルーティング IPv6/IPv4 Dual Stack、IPv6 over IPv4 Tnunnel ※ FLET'S.Net動作確認済(*1)	
ファイアウォール機能	SPI（ステートフルパケットインスペクション）		
	DoS攻撃防御		
	パケットフィルタリング		WAN ↔ LAN WAN ↔ DMZ
	ステルスモード		
アクセスコントロール	MACアドレスフィルタ		
	IPアドレスフィルタ		
	URLフィルタ		
	スケジュール設定		
ログ機能	WEB		ログ対象（DoS攻撃、インターネット接続、アクセスコントロール、ファイアウォール、VPN）
	SYSLOG		

VPN(*2)	対応プロトコル		IPSec(クライアント、パススルー)
			PPTP(サーバ(ユーザ数:2)、クライアント、パススルー)
			L2TP(パススルー)
	IPSec仕様	暗号方式	DES、3DES
		ハッシュ方式	MD5、SHA-1
		トンネル数	50(*3)
		鍵交換方式	Manual、IKE(メインモード、アグレッシブモード)
		その他	IKEキープアライブ、NAT+VPN
NAT Traversal	対応		
Path MTU Discovery	対応		
DMZ	専用ポートを装備		
UPnP	対応		
DDNS	ieServer.Net		
NTP	NTPクライアント対応(NTPサーバのIPアドレス設定可能)		
設定	設定方法		ブラウザ／CLI 設定の保存および復元可能
	ユーザアカウント数		4ユーザ(管理者1＋一般3) 一般ユーザには指定した設定項目を変更させないことも可能
	パスワード設定		可能(最大40文字まで)
	リモート設定		telnetにより可能
	工場出荷値設定		本体リセットボタンの長押しにより可能。ブラウザおよびCLIにより個別の設定項目のみ初期化可能。
	ファームウェアアップグレード		ブラウザおよびCLI(tftp)によりアップグレード可能

*1　FLET'S.NetはNTT東日本が提供するサービスです。
*2　VPN接続は、両側のルータのグローバルIPアドレスが動的の場合はご利用になれません。また、VPN接続を行うネットワークは、同一セグメントのネットワーク同士ではご利用になれません。
*3　トンネル数は50個ですが、そのうち動的なIPアドレスの接続は1箇所のみとなります。

12. 修理・問い合わせ

修理のご案内

修理を希望される場合の依頼方法は2つあります。

1. お買い上げ店に持ち込んでいただく方法
2. 商品を当社周辺機器修理センタへ直送していただく方法
   （出張修理サービスは行っておりません。ご了承ください。）

＜周辺機器修理センタへ直送していただく方法＞

1. 修理依頼手順

① 「修理依頼票」をコピーしてください。

② 「修理依頼票」に必要事項をすべて記入してください。

故障内容や発生頻度などを詳しく記入してください。

③ 製造番号／発送日／発送時の送り状No.を控えとして以下に記入してください。

修理品の問い合わせ時に必要です。

製造番号	
発送日	年　　月　　日
発送業者	
送り状No.	

④ 「修理依頼票」を修理品に同梱し、下記宛先に発送してください。

（送料はお客様負担にてお願いします。）

〒491-0914
愛知県一宮花池4-13-11
株式会社 エイスタッフ内
オムロン周辺機器修理センタ宛
TEL:03−3436−7213

2. 修理期間

おおむね1～2週間

＊ 故障状況によっては、1ヶ月以上要する場合がありますのでご了承ください。

3. 修理代金お支払方法（有償修理の場合）

有償での修理代金は、代金引換または銀行振込にてお支払ください。

- 代金引換……ヤマト運輸株式会社のコレクトサービスを利用します。
- 先行銀行振込……振り込み確認後、修理品を発送させていただきます。

修理依頼票 MR504DV

- 修理依頼時、この依頼票に必要事項をすべて記入の上、製品に同梱してお送りください。

依頼日	平成　　年　　月　　日(　　)		
フリガナ			印
お名前			
ご住所	〒		
会社名 部署名			
電話番号		携帯電話番号	
FAX番号			
E-Mail			
製造番号			
保証書	□ 有り…保証書を同梱ください。 □ 無し…保証期間内でも有償となります。		
故障状況	発生頻度	□ 常時発生　□ 時々発生(具体的に…例:週１回) [　　]	
	症状とご要望 ※ 故障内容を詳しく記入してください。		
お支払い方法 (有償の場合)	□ 代金引換　□ 銀行振込 (完了品の発送はお振込み確認後となります。)		

オムロンカスタマサポートセンタ行
TEL: 0120−77−4717　FAX番号:03−3436−7059

- お客様が当社カスタマサポートセンタにお問い合わせいただくときに本票をご利用ください。
- お問い合わせの前に『9.困ったときには』(P.154)をご一読ください。

※ 本製品底面に貼ってある製造番号をご記入ください。

お問い合わせ票

(MR504DV)

※本紙をコピーしてご利用ください。

お名前			
電話番号		FAX番号	
メールアドレス			
ご住所	〒		
購入日／台数	年　月　日／　台	製造番号※	
パソコン	メーカー名:　型式名: OS名(例:Windows XP): CPU:　メモリ:		
ADSL/FTTH CATV事業者	事業者名: 固定IPアドレスサービス契約　有(　　)個　・　無 □ 未加入　□ 加入済み(工事完了日　年　月　日)		
(ADSL回線の場合) ADSLモデム	メーカー名:　型式名:		
プロバイダ <どちらかを選択>	プロバイダ名: □ 未加入／加入予定　□加入済		
具体的な内容<エラーメッセージ／詳しい症状／発生頻度／配線図をお書きください>			

各種問い合わせのご案内

技術的な お問い合わせは周辺機器カスタマサポートセンタまで。
オムロン株式会社
周辺機器カスタマサポートセンタ
TEL　：0120 − 77 − 4717(携帯電話／ PHS からもご利用いただけます)
FAX　：03 − 3436 − 7059
メールアドレス　：omron_support@omron.co.jp
受付時間　：月曜日〜土曜日　9:00 〜 17:30(12:00 〜 13:00 を除く)
＊祝祭日、当社の休日を除く
住所　：〒 105 − 0001　東京都港区虎ノ門 3-4-10

修理 のお問い合わせは周辺機器修理センタまで。
オムロン株式会社
周辺機器修理センタ
TEL　：03 − 3436 − 7213
FAX　：03 − 3436 − 7195
メールアドレス　：omron_syuri@omron.co.jp
受付時間　：月曜日〜金曜日　9:30 〜 17:00(12:00 〜 13:00 を除く)
＊祝祭日、当社の休日を除く
住所　：〒 491−0914　愛知県一宮市花池 4-13-11
株式会社　エイスタッフ内　オムロン周辺機器修理センタ

通信販売 のお問い合わせはオムロンダイレクトまで。
オムロン株式会社
周辺機器オムロンダイレクト
TEL　：03 − 3436 − 7212
FAX　：03 − 3436 − 7195
メールアドレス　：omron_direct@omron.co.jp
受付時間　：月曜日〜金曜日　9:30 〜 17:00(12:00 〜 13:00 を除く)
＊祝祭日、当社の休日を除く
住所　：〒 105 − 0001　東京都港区虎ノ門 3-4-10

オムロン周辺機器商品はインターネット でもお買い求めいただけます。
ホームページアドレス　http://www.omron.co.jp/ped-j/

高速 VPN アクセスルータ
MR504DV
取扱説明書

OMRON

周辺機器事業部
〒105−0001　東京都港区虎ノ門3-4-10
TEL:03−3436−7228

オムロン株式会社

第1版
08/05
K1N-D-05050A