

VIAGGIO

— ヴィアッジョ —

ブロードバンドルータ
MR304X / MR304DV

取扱説明書

詳細設定編

OMRON

1. はじめに

このたびは、オムロンブロードバンドルータ MR304X/MR304DV 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ブロードバンドルータです。

本取扱説明書は、『取扱説明書[簡単設定編]』より、さらに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。

■詳細設定編の内容について

本取扱説明書では、ブラウザを使った場合のブロードバンドルータ設定画面の説明を、メニュー順に説明しています。

● クイック設定

ブロードバンド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。

- 『7-1.ブロードバンドで接続』(P.20)
PPPoEおよびIPアドレスの設定方法について説明します。
- 『7-2.切断／接続状況』(P.36)
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。
- 『7-3.管理コマンド・設定』(P.40)
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。
- 『7-4.情報表示』(P.50)
設定やIP経路、ログ、WAN状況、UPnP状況、IPSec状況など本製品の情報表示の仕方について説明します。
- 『7-5.その他』(P.55)
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




ブロードバンド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。

- 『8-1.接続／相手先登録』(P.58)
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。
- 『8-2.本体設定』(P.66)
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
- 『8-3.ルータ設定』(P.68)
WAN設定や、LAN設定の設定方法について説明します。
- 『8-4.セキュリティ設定』(P.76)
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。
- 『8-5.VPN(IPSec)設定』(P.99)
VPNポリシーの設定について説明します。
- 『8-6.IPv6設定』(P.113)
IPv6の設定および表示について説明します。
- 『8-7.NAT設定』(P.114)
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。
- 『8-8.UPnP設定』(P.117)
UPnP設定について説明します。
- 『8-9.ダイナミックDNS設定』(P.118)
DDNS設定について説明します。
- 『8-10.管理コマンド・設定』(P.119)
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。

- 『8-11.切断／接続状況』(P.123)
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。
- 『8-12.情報表示』(P.124)
設定やIP経路、ログ、WAN状況、UPnP状況、IPSec状況など本製品の情報表示の仕方について説明します。
- 『8-13.その他』(P.127)
オンラインヘルプの表示方法について説明します。

2. 安全にご使用いただくために

ここに記載している事項は、安全に関わる重要な内容ですので、必ず守ってください。

 注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関わる拡大損害を示しています。
	禁止行為(してはいけないこと)を示しています。
	強制行為(必ずしなければいけないこと)を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

注意

本製品を分解したり、改造したりしないこと。

- 感電、火災、故障のおそれがあります。



雷のときは、本製品およびケーブルに触れないこと。

- 感電のおそれがあります。



本製品に水などの液体をかけたり、異物を入れないこと。

- 感電や火災のおそれがあります。万一、本製品に液体がかかったり、異物が入った場合は、ACアダプタをコンセントから抜き、周辺機器修理センタ(TEL:055-977-9048)にご連絡ください。



本製品から煙、異臭、異常音が発生した場合は、ACアダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外すこと。

また、修理、点検のため、周辺機器修理センタ(TEL:055-977-9048)にご連絡ください。

- 火災のおそれがあります。



この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないこと。

本製品の故障や破損などによって、発煙、発火、感電のおそれがあります。下記の環境には、特にご注意ください。

- 室内または製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所



同梱のACアダプタ以外のACアダプタを使用しないこと。

- 他のACアダプタを使用すると、故障、火災のおそれがあります。



電源ケーブルを傷つけないこと。

- 感電、火災のおそれがあります。



ACアダプタは、AC100Vコンセントに接続すること。また、本製品を設置、移動するときは、電源プラグを抜くこと。

- 火災や感電のおそれがあります。



梱包のポリ袋などは、小さいお子様の手の届くところに置かないこと。

- 小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げるおそれがあります。



60cm以上の高さから落とした場合は、使用を中止し、販売店または周辺機器修理センター(TEL:055-977-9048)に点検、修理を依頼すること。

- そのまま使用すると、重大な事故につながるおそれがあります。



電源プラグは確実に根元まで差し込むこと。また、電源プラグとコンセントの間のほこりは、定期的(半年に1回程度)に取り除くこと。

- 電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災のおそれがあります。



本製品を積み重ねたり、密着させて使用しないこと。

- やけどや火災のおそれがあります。



本製品は日本国以外で使用しないこと

- 本製品の仕様は国内向けです。海外ではご利用になれません。



These products are designed for use in Japan only and cannot be used in any other countries.

ご使用にあたってのお願い

本製品周辺で静電氣的障害を発生させないでください。

- 本製品は、静電氣に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。

本製品はていねいに取り扱ってください。

- 本製品に強いショックを与えると破損するおそれがあります。

本製品のお手入れをする場合は、ACアダプタをコンセントから抜いてください。

- 誤動作のおそれがあります。

本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。汚れがひどい場合は、柔らかい布に台所用中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布でからぶきしてください。

- 揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては、破損するおそれがあります。

地球環境保全のため、次のことにご協力ください。

- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご留意

この製品について

本製品を海外に持ち出される(輸出)場合は、当社カスタマサポートセンタ(TEL:0120-77-4717)にお問い合わせください。また、該非判定資料の発行をご希望の際は、当社ホームページまでお申し込みください。(URL <http://www.omron.co.jp/ped-j/gaihi/index.htm>)
お問い合わせの際、本製品の製造番号が必要です。製造番号は、本製品底面に貼付のシールに記載しております。

本製品は、パソコンなどのOA 機器に使用することを目的に設計、製造されています。医療機器や幹線通信機器、電算機システムなどの、極めて高い安全性や信頼性が要求される用途には使用しないでください。

本製品は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こすことがあります。この場合には、使用者が適切な対策で講ずるよう要求されることがあります。

本製品の故障・誤動作・停電あるいは天災等によって本製品が使用できなくなった場合、それによって生じる損害(機会損失等を含む一切の損害)に対しては、当社は一切責任を負いかねます。あらかじめご了承ください。

CD-ROM は下記を守って使用してください。

- CD-ROM の表面に傷をつけないでください。
- CD-ROM の読み取り面を触らないでください。
- CD-ROM を折り曲げないでください。
- 高湿高温、直射日光のあたる場所、ほこりの中で保管しないでください。

快適にご利用いただくために

(1)インターネット常時接続となるため、インターネットからパソコンへの不正侵入の危険性が高くなります。本製品のファイアウォール機能により、外部環境からの悪質な攻撃を防ぐことができますが(*)、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。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。

* 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。

(2)一部のCATV事業者では、ブロードバンドルータを使用して、複数のパソコンから同時にインターネットへ接続することを認めていません。CATV事業者が想定しているデータ量を超えたデータが発生することにより、全会員に十分なサービスを提供できなくなるおそれがあるためです。このような場合、CATV事業者に無断でブロードバンドルータを接続すると、規約違反になりますので、設置前にご契約のCATV事業者へご確認ください。

- (3)USBタイプのADSLモデムにはご利用できません。LANタイプのADSLモデムをご利用ください。
- (4)ご利用のFTTHサービスによっては、接続できる端末(パソコン)数が決まっています。上限を超えないようにご注意ください。

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。万が一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。

©OMRON Corporation 2004 All Rights Reserved.

3. 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。



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。

①→②→③とお進みください。

②

⋮



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** … 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。
- チェックしない**
 - 、 … 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 version 4.0 および Microsoft® Windows NT® Server operating system version 4.0 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。

4. 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.20	P.58

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.58
LAN側IPアドレスの設定	-	P.71
パソコンのIPアドレス設定	P.133	

ネットワークゲームを利用したい

ネットワークゲームを利用する場合、アプリケーション設定が必要です。

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.88

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.66

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アドレスマッピングの登録	-	P.114

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.80

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.76

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.85

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.113

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.100

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.58

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.117
パソコンの設定	P.147	

5. 目次

1.はじめに.....	1
2.安全にご使用いただくために.....	3
ご使用にあたってのお願い.....	5
ご留意.....	6
この製品について.....	6
快適にご利用いただくために.....	6
取扱説明書について.....	7
3.この取扱説明書について.....	8
表記について.....	8
画面表示について.....	9
商標について.....	9
4.利用目的別早見表.....	10
5.目次.....	13
6.ブロードバンド画面の表示.....	16
7.クイック設定.....	18
7-1.ブロードバンドで接続.....	20
7-1-1. PPPoE.....	20
7-1-2. IPアドレス自動取得(DHCP).....	31
7-1-3. 固定IPアドレス.....	33
7-2.切断／接続状況.....	36
7-2-1. PPTP.....	36
7-2-2. PPPoE.....	38
7-3.管理コマンド・設定.....	40
7-3-1. 再起動.....	40
7-3-2. 設定の消去.....	41
7-3-3. ユーザ・パスワード変更.....	42
7-3-4. アクセス権限.....	44
7-3-5. ファームウェア更新.....	47
7-3-6. 設定メンテナンス.....	48
7-4.情報表示.....	50
7-4-1. 設定.....	50
7-4-2. IP経路.....	50
7-4-3. ログ.....	51
7-4-4. WAN状況.....	52
7-4-5. UPnP状況.....	53
7-4-6. IPSec状況.....	54
7-5.その他.....	55
7-5-1. オンラインヘルプ.....	55

8.詳細設定	56
8-1.接続／相手先登録	58
8-1-1. 相手先登録.....	59
8-2.本体設定	66
8-3.ルータ設定	68
8-3-1. WAN	68
8-3-2. LAN.....	71
8-3-3. DMZ.....	75
8-4.セキュリティ設定	76
8-4-1. ファイアウォール設定.....	76
8-4-2. ログ通知設定	80
8-4-3. セキュリティオプション	82
8-4-4. インターネットアクセス制御	85
8-4-5. アプリケーション設定.....	88
8-4-6. スケジュール設定	90
8-4-7. MACアドレスフィルタ設定.....	92
8-4-8. URLフィルタリング設定.....	94
8-4-9. 証明書(https)	96
8-5.VPN(IPSec)設定	99
8-5-1. VPNポリシー	100
8-5-2. 証明書(IPSec).....	110
8-6.IPv6設定	113
8-6-1. 共通設定	113
8-7.NAT設定	114
8-8.UPnP設定	117
8-9.ダイナミックDNS設定	118
8-10.管理コマンド・設定	119
8-10-1. 再起動.....	119
8-10-2. 設定の消去.....	119
8-10-3. ユーザ・パスワード変更.....	120
8-10-4. アクセス権限	120
8-10-5. ファームウェア更新	121
8-10-6. 設定メンテナンス	121
8-11.切断／接続状況	123
8-11-1. PPTP	123
8-11-2. PPPoE	123
8-12.情報表示	124
8-12-1. 設定	124
8-12-2. IP経路.....	124
8-12-3. ログ	125
8-12-4. WAN状況.....	125
8-12-5. UPnP状況.....	126
8-12-6. IPSec状況	126
8-13.その他	127
8-13-1. オンラインヘルプ	127

9.コマンドを使った設定方法.....	128
9-1.ハイパーターミナルを使った設定方法.....	128
9-2.コマンドプロンプトを使った設定方法.....	131

10.付録(パソコンの設定).....	133
10-1.IPアドレスを手動で割り当てる.....	133
10-1-1. Windows XP/Server 2003の場合.....	133
10-1-2. Windows Me/98/95の場合.....	136
10-1-3. Windows 2000の場合.....	139
10-1-4. Windows NT 4.0の場合.....	141
10-1-5. Mac OS 8.x/9.xの場合.....	144
10-1-6. Mac OS X 10.0.x~10.2.8の場合.....	145
10-1-7. Mac OS X 10.3.x(Panther)の場合.....	146
10-2.UPnP機能の設定.....	147
10-2-1. パソコンの設定.....	147
10-2-2. UPnP機能の動作確認.....	151

11.修理・問い合わせ.....	152
修理のご案内.....	152
修理依頼票 MR304X/MR304DV.....	153
各種問い合わせのご案内.....	155

6. ブロードバンド画面の表示

* 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。

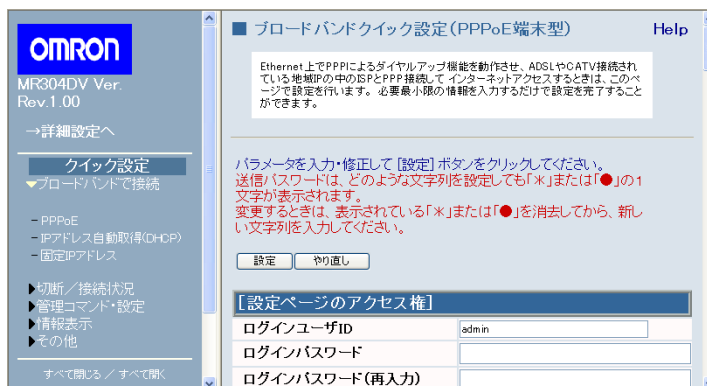


2. アドレス欄に、本製品のIPアドレス「192.168.2.1」を入力し<Enter>キーを押します。

- * 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、『取扱説明書 [簡単設定編] 12. 困ったときには』を参照してください。



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『7-1-1.PPPoE』(P.20) または 『7-3-3. ユーザ・パスワード変更』(P.42) を参照してください。

7. 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。

ブラウザでブロードバンド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.20
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.31
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.33
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.36
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.38
管理コマンド・設定		
再起動	ルータを再起動します。	P.40
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.41
ユーザ・パスワード変更	ブロードバンド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.42
アクセス権限	ブロードバンドルータ設定画面のアクセス権限を設定します。	P.44
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.47
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.48
情報表示		
設定	設定情報を表示します。	P.50
IP経路	IP経路情報を表示します。	P.50
ログ	ログを表示または消去します。	P.51
WAN状況	WANの設定状況を表示します。	P.52
UPnP状況	UPnPの設定状況を表示します。	P.53
IPSec状況	IPSecの設定状況を表示します。	P.54

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.55

7-1. ブロードバンドで接続

補足

- 設定手順については、『取扱説明書[簡単設定編] 10-3. ブロードバンドルータの設定』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。

7-1-1. 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、『8-1.接続／相手先登録』(P.58)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、『8-1. 接続／相手先登録』(P.58)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

■ ブロードバンドクイック設定 (PPPoE端末型)
Help

Ethernet上でPPPoE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。

パラメータを入力・修正して [設定] ボタンをクリックしてください。
 送信パスワードは、どのような文字列を設定しても「*」または「●」の1文字が表示されます。
 変更するときは、表示されている「*」または「●」を消去してから、新しい文字列を入力してください。

設定
やり直し

[管理者のアクセス情報]

ログインユーザID	<input type="text" value="admin"/>
ログインパスワード	<input type="password"/>
ログインパスワード(再入力)	<input type="password"/>

[LAN側設定]

本体のIPアドレス/サブネットマスク長	<input type="text" value="192.168.2.1/24"/>
DHCPサーバ機能	<input type="radio"/> OFF <input checked="" type="radio"/> ON
LANポートの開始IPアドレス/個数	<input type="text" value="192.168.2.2/99"/>
ドメイン名	<input type="text"/>

[PPPoE設定:メイン]

以下の内容で設定を行う	<input type="checkbox"/> (設定済み:接続相手先登録#0)
相手先名称	<input type="text" value="プロバイダ(メイン)"/>
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	<input type="text"/>
送信ユーザID	<input type="text"/>
送信パスワード	<input type="password"/>
DNSサーバアドレス	<input type="text"/>

[PPPoE設定:メイン(予備)]

以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#1)
相手先名称	<input type="text" value="プロバイダ(予備)"/>
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	<input type="text"/>
送信ユーザID	<input type="text"/>
送信パスワード	<input type="password"/>
DNSサーバアドレス	<input type="text"/>

[PPPoE設定:サブ#1]

以下の内容で設定を行う	<input type="checkbox"/> (設定済み:接続相手先登録#2)
相手先名称	<input type="text" value="フレッツ・スクウェア(NTT東日本)"/>
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	<input type="text"/>
送信ユーザID	<input type="text" value="guest@fleets"/>
送信パスワード	<input type="password" value="●"/>
DNSサーバアドレス	<input type="text"/>
宛先ドメイン名/宛先アドレス	<input type="text" value=".fleets"/>
プロトコル	<input type="text"/>
宛先ポート番号	<input type="text"/>
送信元アドレス	<input type="text"/>

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.23)
2. 管理者のアクセス情報：ブロードバンド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.23)
3. LAN側設定：LANポートの情報を設定します。(P.24)
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.24)
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.25)
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.25)

21

[PPPoE設定:サブ#2]	
以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#3)
相手先名称	フレッツ・スクウェア(NTT西日本)
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	
送信ユーザID	flets@flets
送信パスワード	●●●●
DNSサーバアドレス	
宛先ドメイン名/宛先アドレス	.flets
プロトコル	
宛先ポート番号	
送信元アドレス	
[PPPoE設定:サブ#3]	
以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#4)
相手先名称	BROBA
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	
送信ユーザID	
送信パスワード	
DNSサーバアドレス	
宛先ドメイン名/宛先アドレス	.broba.cc
プロトコル	
宛先ポート番号	
送信元アドレス	
[PPPoE設定:サブ#4]	
以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#5)
相手先名称	速度確認
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	
送信ユーザID	speed@speed.flets
送信パスワード	●●●●
DNSサーバアドレス	
宛先ドメイン名/宛先アドレス	.speed
プロトコル	
宛先ポート番号	
送信元アドレス	
[PPPoE設定:サブ#5]	
以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#6)
相手先名称	
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	
送信ユーザID	
送信パスワード	
DNSサーバアドレス	
宛先ドメイン名/宛先アドレス	
プロトコル	
宛先ポート番号	
送信元アドレス	
[PPPoE設定:サブ#6]	
以下の内容で設定を行う	<input type="checkbox"/> (未設定:接続相手先登録#7)
相手先名称	
サービス名 <small>(プロバイダから指定された時のみ入力)</small>	

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.25)

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.23)

2. 管理者のアクセス情報：ブロードバンド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. ログインユーザ名 (初期値:admin)

4. ログインパスワード (初期値:なし)

5. ログインパスワード(再入力)

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.25)

7. クイック接続：PPPoE接続を操作します。(P.30)

8. クイック切断：PPPoE接続の切断を操作します。(P.30)

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.30)

チャンネル	状況
PPPoE1	空き
PPPoE2	空き
PPPoE3	空き
PPPoE4	空き

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 : ブロードバンド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)	ブロードバンド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)	ブロードバンド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、ブロードバンド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、『7-3-3. ユーザ・パスワード変更』(P.42)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:DdcilHbkk 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。

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『8-1.接続／相手先登録』(P.58)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「*」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。

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。
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。

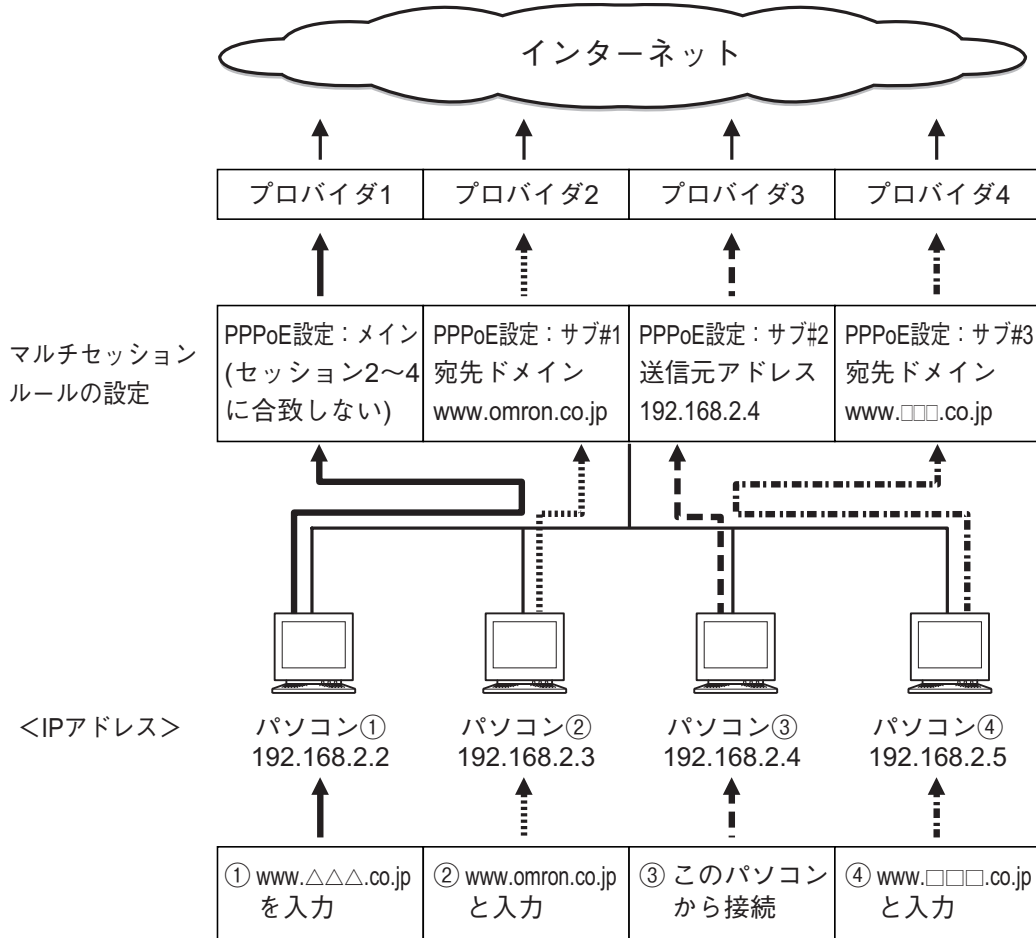
項目	説明
送信パスワード	<p>プロバイダから指定されたパスワード(ログインパスワード/認証パスワードともいう)を入力してください。</p> <p>例:DdciHbkk</p> <p>大文字・小文字を間違えないように入力してください。</p> <p>入力時「●」または「*」の1文字で表示されます。</p>
DNSサーバアドレス	<p>プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。</p>
宛先ドメイン名/宛先アドレス	<p>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。</p> <p>→『8-1-1.相手先登録』(P.59)</p> <p>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。</p>
プロトコル	<p>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使用する相手先に設定する場合は、「tcp」と入力します。</p> <p>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。</p>
宛先ポート番号	<p>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。</p>
送信元アドレス	<p>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。</p>

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@fleets」 NTT西日本の場合…「fleets@fleets」
送信パスワード	:	NTT東日本の場合…「guest」 ^(*1) NTT西日本の場合…「fleets」 ^(*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…「.fleets」 NTT西日本の場合…「fleets」
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.fleets/」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、2004年8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。

7-1-2. 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、『8-10-2. 設定の消去』(P.119)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

■ ブロードバンドで接続(IPアドレス自動取得(DHCP)) Help

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の設定を行います。

パラメータを入力・修正して [設定] ボタンをクリックしてください。

[設定] [やり直し]

[管理者のアクセス情報]

ログインユーザID	admin
ログインパスワード	
ログインパスワード(再入力)	

[基本設定] プロバイダから指定がある時に入力

ゲートウェイアドレス	
DNSサーバアドレス(プライマリ)	
DNSサーバアドレス(セカンダリ)	
DNSサーバアドレス(サード)	
DNSサーバアドレス(フォース)	

DNSサーバアドレスには、プロバイダから指定されたDNSサーバアドレスを入力してください。
DNSサーバが不明な場合は、契約したプロバイダにお問い合わせください。

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：ブロードバンド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。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 : ブロードバンド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)	ブロードバンド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)	ブロードバンド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、ブロードバンド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、『7-3-3. ユーザ・パスワード変更』(P.42)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。

7-1-3. 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、『8-10-2. 設定の消去』(P.119)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]－[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、『8-1. 接続／相手先登録』(P.58)および『8-3-2.LAN』(P.71)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、『8-1. 接続／相手先登録』(P.58)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

■ ブロードバンドで接続(固定IPアドレス) Help

Static 接続(プロバイダから固定のIPアドレスを指定)利用するインターネット接続サービスをご利用の場合の設定を行います。

パラメータを入力・修正して **[設定]** ボタンをクリックしてください。

[管理者のアクセス情報]

ログインユーザID	admin
ログインパスワード	
ログインパスワード(再入力)	

[基本設定]

IPアドレス/サブネットマスク長	
ゲートウェイアドレス	
DNSサーバアドレス(プライマリ)	
DNSサーバアドレス(セカンダリ)	
DNSサーバアドレス(サード)	
DNSサーバアドレス(フォース)	

DNSサーバアドレスには、プロバイダから指定されたDNSサーバアドレスを入力してください。
DNSサーバが不明な場合は、契約したプロバイダにお問い合わせください。

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：ブロードバンド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 : ブロードバンド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)	ブロードバンド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)	ブロードバンド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、ブロードバンド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、『7-3-3. ユーザ・パスワード変更』(P.42)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。

7-2. 切断／接続状況

7-2-1. 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

The screenshot shows a web-based settings interface for PPTP. It is divided into two main sections: '切断(PPTP)' (Disconnect PPTP) and '接続状況(PPTP)' (PPTP Connection Status). The '切断(PPTP)' section includes a description, instructions, a dropdown menu for '切断するチャンネル' (Channel to disconnect) set to 'PPTP1', and a '切断' (Disconnect) button. The '接続状況(PPTP)' section contains two tables, one for 'PPTP1' and one for 'PPTP2'. Each table lists various connection parameters such as status, time, mode, link protocol, and IP address. Two callouts are present: one pointing to the '切断するチャンネル' dropdown and another pointing to the '接続状況(PPTP)' tables.

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。

チャンネル	PPTP1
接続状況	空き
接続時刻	
接続モード	
リンクプロトコル	
相手先ルータアドレス	
相手先DNSサーバアドレス	
無通信時間/自動切断時間(秒)	
経過時間/最大接続時間(分)	
割り当てIPアドレス	

チャンネル	PPTP2
接続状況	空き
接続時刻	
接続モード	
リンクプロトコル	
相手先ルータアドレス	
相手先DNSサーバアドレス	
無通信時間/自動切断時間(秒)	
経過時間/最大接続時間(分)	
割り当てIPアドレス	

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。

7-2-2. 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。

チャンネル	PPPoE1
接続状況	空
接続時刻	
接続モード	
リンクプロトコル	
相手先ルータアドレス	
相手先DNSサーバアドレス	
経過時間/最大接続時間(分)	
割り当てIPアドレス	
チャンネル	PPPoE2
接続状況	空
接続時刻	
接続モード	
リンクプロトコル	
相手先ルータアドレス	
相手先DNSサーバアドレス	
経過時間/最大接続時間(分)	
割り当てIPアドレス	
チャンネル	PPPoE3
接続状況	空
接続時刻	
接続モード	
リンクプロトコル	
相手先ルータアドレス	
相手先DNSサーバアドレス	
経過時間/最大接続時間(分)	

The screenshot shows a network configuration window. At the top, there is a table with two columns: '割り当てIPアドレス' (Assigned IP Address) and 'チャンネル' (Channel). The 'チャンネル' column contains 'PPPoE4'. Below this, a list of connection details is shown, including '接続状況' (Connection Status) which is '空き' (Available), '接続時刻' (Connection Time), '接続モード' (Connection Mode), 'リンクプロトコル' (Link Protocol), '相手先ルータアドレス' (Peer Router Address), '相手先DNSサーバアドレス' (Peer DNS Server Address), '経過時間/最大接続時間(分)' (Elapsed Time/Maximum Connection Time (min)), and '割り当てIPアドレス' (Assigned IP Address). Below the table, there is a control panel with a dropdown menu labeled '切断するチャンネル' (Disconnect Channel) set to 'PPPoE1' and a button labeled '切断' (Disconnect).

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。

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。

7-3. 管理コマンド・設定

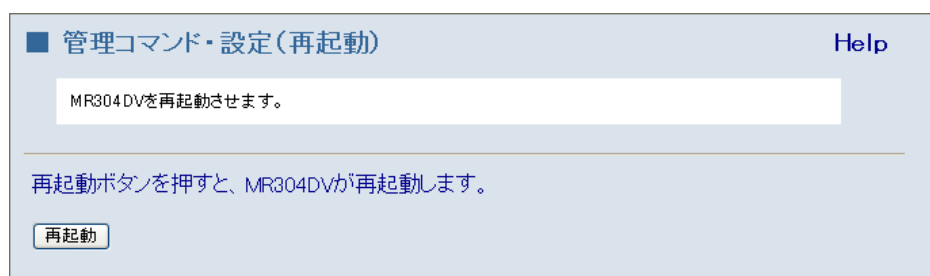
7-3-1. 再起動

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[閉じる]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。

7-3-2. 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。

7-3-3. ユーザ・パスワード変更

ブロードバンド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

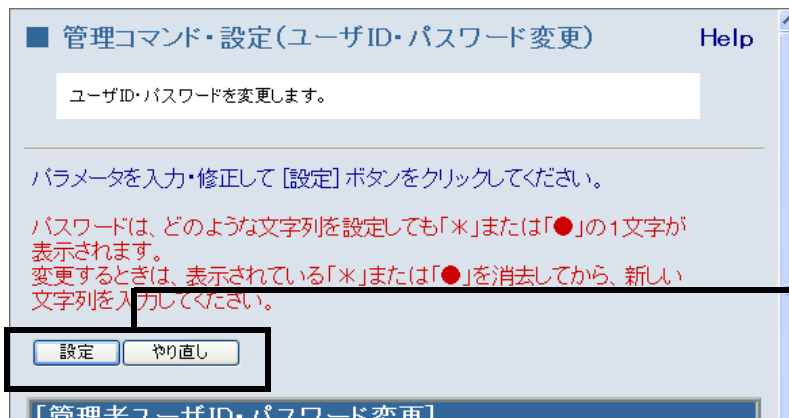
1. [管理コマンド・設定]→[ユーザ・パスワード変更]の順にクリックします。
 - ・ 詳細設定画面を表示している場合は、[→クイック設定へ]をクリックしてから、上記メニューをクリックします。
 - ・ 詳細設定画面の[管理コマンド・設定]→[ユーザ・パスワード変更]をクリックしても同様の画面が表示されます。

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、『7-3-4. アクセス権限』(P.44)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ブロードバンド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。

[管理者ユーザID・パスワード変更]	
ユーザID	admin
パスワード	●
パスワード(再入力)	●
[ユーザ1 ユーザID・パスワード変更]	
ユーザID	user01
パスワード	●
パスワード(再入力)	●
[ユーザ2 ユーザID・パスワード変更]	
ユーザID	
パスワード	
パスワード(再入力)	
[ユーザ3 ユーザID・パスワード変更]	
ユーザID	
パスワード	
パスワード(再入力)	

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。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、ブロードバンド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	ブロードバン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。

7-3-4. アクセス権限

ブロードバンド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

管理コマンド・設定(アクセス権限) Help

ユーザごとに、設定ページの参照/変更を設定します。

パラメータを入力・修正し [実行] ボタンをクリックしてください。

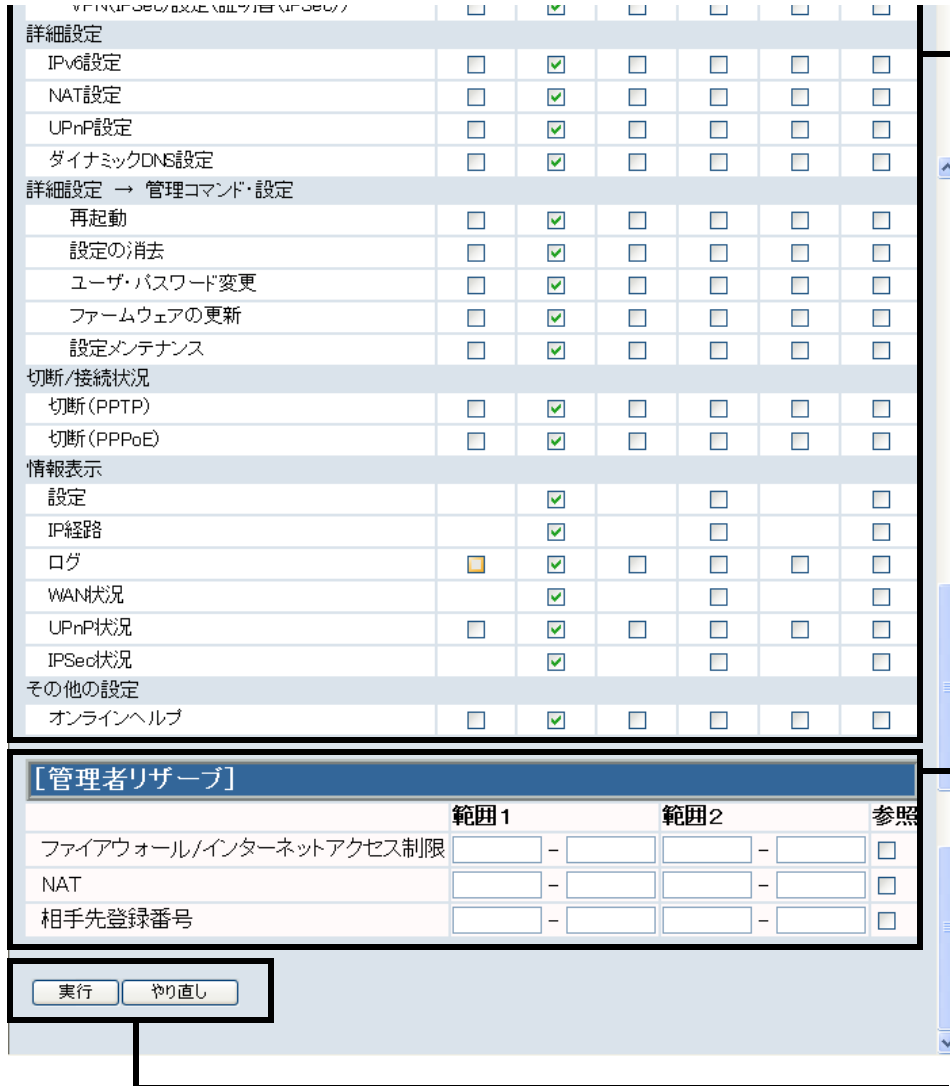
実行 やり直し

[設定ページ・ユーザー一覧]

アクセス許可	user01		user2		user3	
	変更	参照	変更	参照	変更	参照
ページ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
全ページ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
クイック設定						
ブロードバンドクイック設定 (PPPoE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ブロードバンドクイック設定 (DHCP)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ブロードバンドクイック設定 (固定IPアドレス)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
詳細設定						
接続/相手先登録	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
本体設定	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
詳細設定 → ルータ設定						
ルータ設定 (WAN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ルータ設定 (LAN)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ルータ設定 (DMZ)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ルータ設定 (シリアルポート)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
詳細設定 → セキュリティ設定						
セキュリティ設定 (ファイアウォール)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (ログ)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (セキュリティオプション)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (インターネットアクセス制限)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (アプリケーション)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (スケジュール)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (MACアドレスフィルタ)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (URLフィルタ)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
セキュリティ設定 (証明書 (https))	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
詳細設定 → VPN(IPSec)設定						
VPN(IPSec)設定 (VPNポリシー)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN(IPSec)設定 (証明書 (IPSec))	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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。



2. 設定ページ・ユーザー一覧：変更または参照を許可する設定画面を各ユーザーごとに設定します。

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・ユーザー一覧 : 変更または参照を許可する設定画面を各ユーザーごとに設定します。

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。
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。

7-3-5. 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。

7-3-6. 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。

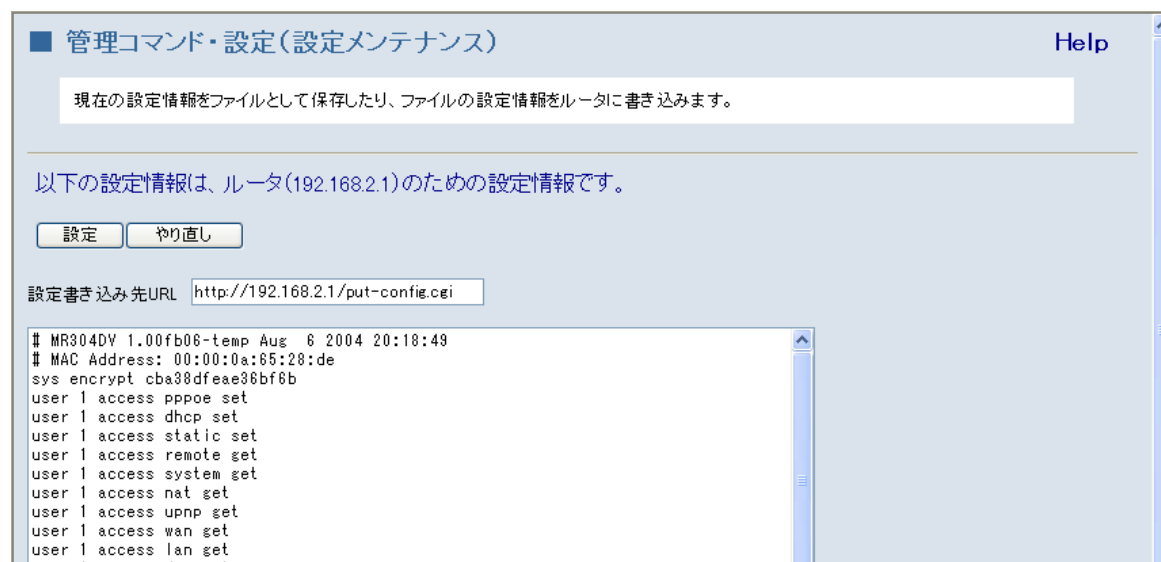
保存したテキストファイルから設定を復元したい場合は、設定メンテナンス画面を表示し、保存したテキストファイルから設定情報をコピーして、設定メンテナンス画面にペーストし、[設定]をクリックします。

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。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。
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。

7-4. 情報表示

7-4-1. 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。

```
# MR304DV 1.00fb06-temp Aug 6 2004 20:18:49
# MAC Address: 00:00:0a:65:28:de
sys encrypt a8c13ce5ccce93c6
user 1 access pppoe set
user 1 access dhcp set
user 1 access static set
user 1 access remote set
user 1 access system get
user 1 access nat get
user 1 access upnp get
user 1 access wan get
user 1 access lan get
user 1 access dmz get
user 1 access serial get
user 1 access firewall get
user 1 access log get
user 1 access securityoption get
```

7-4-2. 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

# Destination Route	destination	gateway	mode	if	metric	tll	remote
192.168.0.0/24	192.168.2.1	DRCT	0	0	-		
192.168.0.1/32	192.168.2.1	DRCT	0	0	-		

7-4-3. ログ

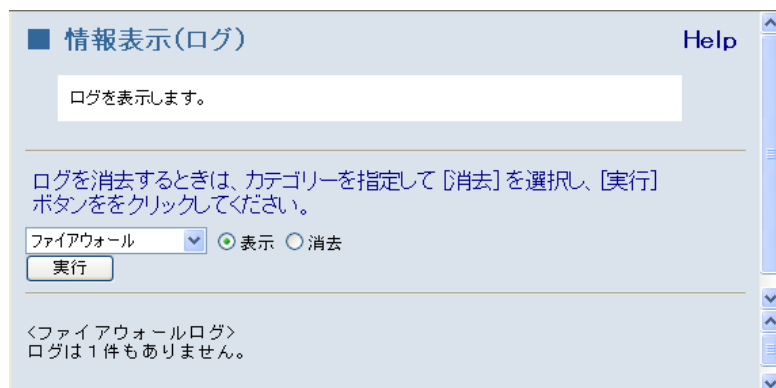
ログの表示および消去を操作します。以下のログを表示または消去することができます。

- 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。

7-4-4. 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

■ 情報表示(WAN状況)
Help

WANに関する情報の一覧です。

最新のWAN状況を表示するにはブラウザでこのページを更新してください。

WAN側Ethernet状況	
MACアドレス	00:00:0a:65:2a:87
IPアドレス	0.0.0
サブネットマスク	0.0.0
デフォルトゲート	0.0.0
DNSサーバアドレス	0.0.0
ドメイン名	

PPPoEの接続状況は[こちら](#)で見ることができます。

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。
デフォルトゲートウェイ	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。

7-4-5. 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

■ 情報表示(UPnP状況)
Help

UPnPに関する情報の一覧です。

ポートマッピングテーブルを消去するときは [消去] ボタンをクリックしてください。

消去

UPnP状況	
UPnP機能	自動削除設定
ON	自動削除しない

ポートマッピングテーブル						
番号	WAN側IP	WAN側ポート	LAN側IP	LAN側ポート	プロトコル	残り時間(秒)

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 Mode	UPnP機能がON/OFFを表示します。
Timer	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。→『8-8.UPnP設定』(P.117)
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。

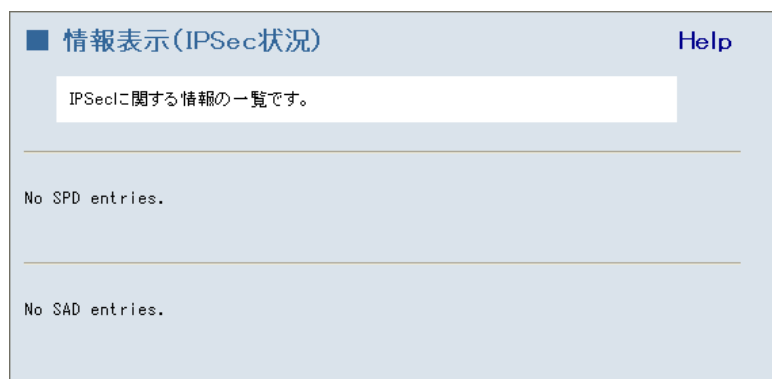
7-4-6. IPSec状況

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。

7-5. その他

7-5-1. 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せん。

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。

8. 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.58
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.66
ルータ設定		
WAN	WANポート情報を設定を行います。	P.68
LAN	LANポートの設定を行います。	P.71
DMZ	DMZポートの設定を行います。	P.75
セキュリティ設定		
ファイアウォール設定	ファイアウォールを設定します。	P.76
ログ通知設定	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.80
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.82
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.85
アプリケーション設定	アプリケーションの登録・編集・消去を操作します。	P.88
スケジュール設定	スケジュールの登録を行います。	P.90
MACアドレスフィルタ設定	MACアドレスフィルタを設定します。	P.92
証明書(https)	HTTPS用の証明書をインストールします。	P.96
VPN(IPSec)設定		
VPNポリシー	VPNポリシーを設定します。	P.100
証明書(IPSec)	IPSec用の証明書をインストールします。	P.110
IPv6設定／表示		
共通設定	IPv6を設定します。	P.113
NAT設定	NATアドレスマッピングを設定します。	P.114
UPnP設定	UPnPを設定します。	P.117
ダイナミックDNS設定	DDNSを設定します。	P.118

メニュー	説明	参照ページ
管理コマンド・設定		
再起動	ルータを再起動します。	P.119
設定の消去	ルータの設定を各項目別によりセットすることができます。	P.119
ユーザ・パスワード変更	ブロードバンド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.120
アクセス制御	ブロードバンドルータ設定画面のアクセス権限を設定します。	P.120
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.121
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.121
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.123
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.123
情報表示		
設定	設定情報を表示します。	P.124
IP経路	IP経路情報を表示します。	P.124
ログ	ログを表示または消去します。	P.125
WAN状況	WANの設定状況を表示します。	P.125
UPnP状況	UPnPの設定状況を表示します。	P.126
IPSec状況	IPSecの設定状況を表示します。	P.126
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.127

8-1. 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 [ブロードバンドルータで接続] → [PPPoE] の設定で相手先の登録を行ってください。→ 『7-1-1.PPPoE』 (P.20)

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

■ 接続／相手先登録
Help

相手先の情報を登録したり、相手先に回線を手動で接続します。

入力・修正、接続したい登録番号を選んで [実行] ボタンをクリックしてください。

登録番号 接続 登録 消去

■ 相手先登録一覧

登録番号	相手先名称	接続形式	送信ユーザID	接続モード	PPTPサーバ機能	受信ユーザID
------	-------	------	---------	-------	-----------	---------

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	<ul style="list-style-type: none"> ● [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、『8-1-1. 相手先登録』(P.59)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。

8-1-1. 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

■ 相手先登録
Help

相手先の情報を登録します。

パラメータを入力・修正し [実行] ボタンをクリックしてください。

送信パスワード/受信パスワードは、どのような文字列を設定しても「*」または「●」の1文字が表示されます。
変更するときは、表示されている「*」または「●」を消去してから、新しい文字列を入力してください。

【相手先情報】

登録番号	<input type="text" value="0"/>
相手先名称	<input type="text"/>

【接続機能】

接続方式	<input type="text" value="PPTP"/>
PPTPアドレス	<input type="text"/>
送信ユーザID	<input type="text"/>
送信パスワード	<input type="password"/>
DNSサーバアドレス	<input type="text"/>
接続形態	<input type="text" value="端末型接続"/>

【マルチセッション選択ルール】

宛先ドメイン名/宛先アドレス	<input type="text"/>
プロトコル	<input type="text"/>
宛先ポート番号	<input type="text"/>
送信元アドレス	<input type="text"/>

【接続切断モード設定】

接続モード	<input type="text" value="手動接続"/>
最大接続時間	<input type="text" value="0"/> 分
自動切断タイマ	<input type="text" value="900"/> 秒

【PPTPサーバ機能】

PPTPサーバ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
受信ユーザID	<input type="text"/>
受信パスワード	<input type="password"/>

【暗号化設定】

暗号化	<input type="text" value="しない"/>
-----	----------------------------------

【MTU設定】

MTUサイズ	<input type="text" value="1454"/>
--------	-----------------------------------

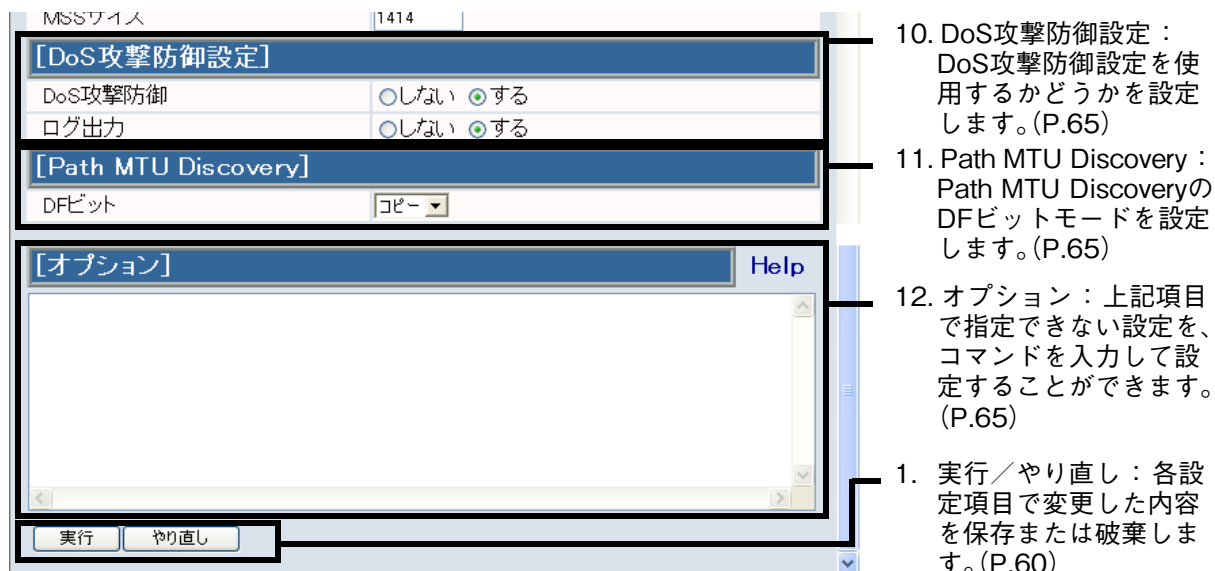
【MSS設定】

MSS変換機能	<input type="radio"/> OFF <input checked="" type="radio"/> ON
MSSサイズ	<input type="text" value="1414"/>

【DoS攻撃防御設定】

DoS攻撃防御	<input type="radio"/> しない <input checked="" type="radio"/> する
---------	---

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.60)
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.60)
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.60)
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.62)
5. 接続切断モード設定：接続切断モードを設定します。(P.63)
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.64)
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.64)
8. MTU設定：送信可能なデータの最大値を設定します。(P.64)
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.64)



- 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.65)
- 11. Path MTU Discovery：Path MTU DiscoveryのDFビットモードを設定します。(P.65)
- 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.65)
- 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.60)

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。

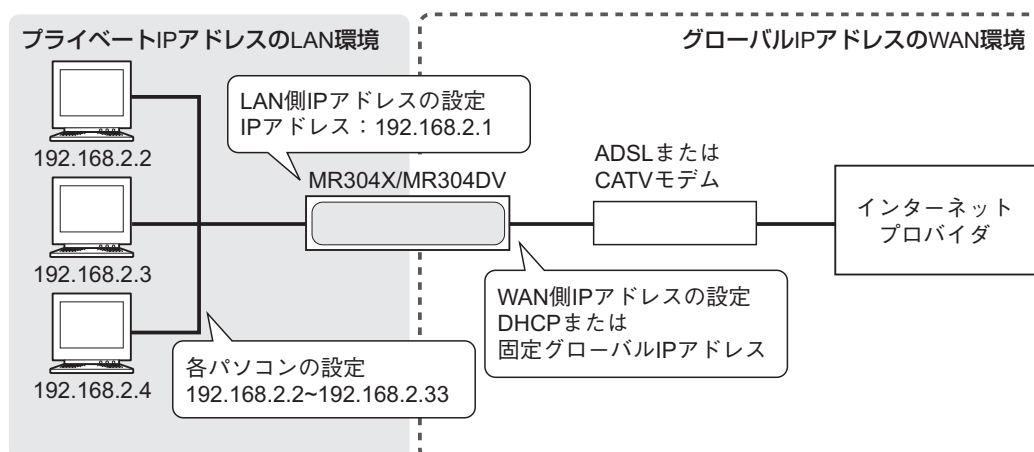
項目	説明
送信パスワード	プロバイダから指定されたパスワード(ログインパスワード／認証パスワードともいう)を入力してください。 例:DdciHbkk 大文字・小文字を間違えないように入力してください。 入力時「●」または「*」の1文字で表示されます。
DNSサーバアドレス	プロバイダから指定されたDNSサーバアドレス(ドメインネームサーバアドレス)がある場合に、指定されたDNSサーバアドレスを入力します。複数指定がある場合は、いずれか1つを入力してください。指定がない場合は、入力しないでください。
接続形態	LAN側に接続されたパソコンではプライベートIPアドレスを使用しWAN側のIPアドレ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

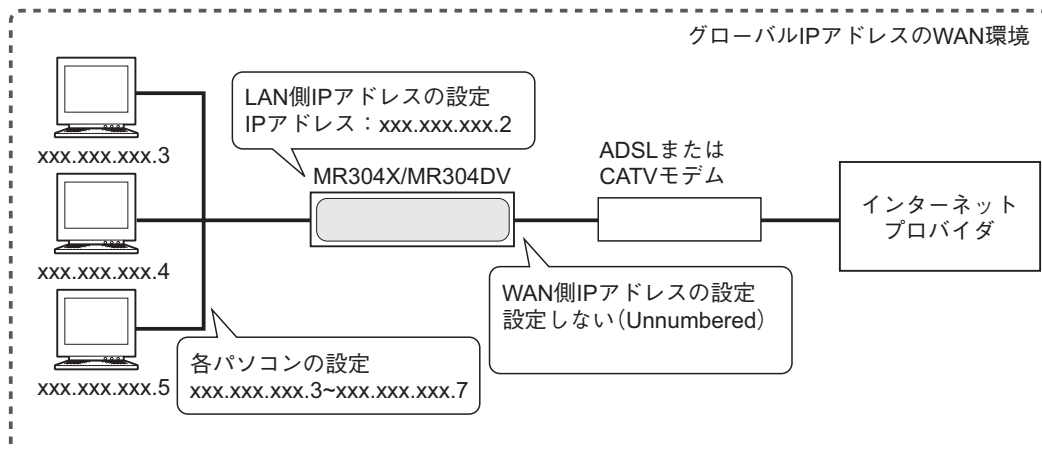
端末型接続を利用するか、LAN型接続を利用するかは、プロバイダから複数のグローバルIPアドレスを割り当てられているかいないかによって決まります。

端末型接続の例



プロバイダから指示されたIPアドレスの設定がDHCPである場合、または指示されたグローバル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、『8-3-2.LAN』(P.71)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.yyy
- 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、『8-3-2.LAN』(P.71)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.28)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.29)および『BROBAを設定する場合』(P.29)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	<ul style="list-style-type: none"> ● 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の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場合は「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。 <ul style="list-style-type: none"> ● 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。 <ul style="list-style-type: none"> ● [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。 <ul style="list-style-type: none"> ● 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 ● セッションキーアライブ機能 ● セッションキーアライブ拡張機能 [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。

8-2. 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。

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。

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、ブロードバンド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の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。

8-3. ルータ設定

8-3-1. 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

■ ルータ設定 (WAN) Help

WANを設定します。

パラメータを入力・修正して [設定] ボタンをクリックしてください。
以下の項目を入力・修正して、[設定] ボタンをクリックしてください。
設定を変更した場合は、再起動ボタンを押しが、または本装置を再起動してください。

[基本]

IPアドレス	<input type="radio"/> DHCPサーバから取得 <input checked="" type="radio"/> 手入力 (DHCPをOFF)
DHCPクライアントID	<input type="text"/>
MTUサイズ	<input type="text"/>

[手入力の時]

IPアドレス/サブネットマスク長	<input type="text" value="172.16.15.154/24"/>
ゲートウェイアドレス	<input type="text" value="172.16.15.2"/>
DNSサーバアドレス(プライマリ)	<input type="text" value="172.16.15.3"/>
DNSサーバアドレス(セカンダリ)	<input type="text" value="172.16.15.4"/>
DNSサーバアドレス(サード)	<input type="text"/>
DNSサーバアドレス(フォース)	<input type="text"/>

[MACアドレス]

MACモード	<input checked="" type="radio"/> 工場出荷値 <input type="radio"/> 手入力 <input type="radio"/> PCのアドレス
MACアドレス	<input type="text" value="00:00:0a:65:2a:87"/>

[オプション] Help

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。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. 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	<p>本製品のMACアドレスの設定方法を選択します。</p> <ul style="list-style-type: none"> ● 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	<p>[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。</p>

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	<p>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。</p> <ul style="list-style-type: none"> ● LAN型接続モード設定 <p>[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。</p>

8-3-2. 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

The screenshot shows the 'ルータ設定 (LAN)' configuration page. It includes a 'Help' button, a 'LANを設定します。' message, and a 'パラメータを入力・修正して [設定] ボタンをクリックしてください。' instruction. Below are several sections: [基本], [DHCPサーバ], [AutoDNS], [リモートアクセスサーバ], [Path MTU Discovery], and [オプション].

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.72)
2. 基本：LAN側の基本設定を行います。(P.72)
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.72)
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.73)
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.73)
6. Path MTU Discovery：Path MTU Discovery機能を設定します。(P.74)
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.74)

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. 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	MR304X/MR304DV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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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)	<ul style="list-style-type: none"> ● 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)	<ul style="list-style-type: none"> ● 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	<p>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。</p> <ul style="list-style-type: none"> ● 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 <p>[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。</p>

*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。

8-3-3. 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。 ^(*)
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、[オプション]欄に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)

8-4. セキュリティ設定

8-4-1. ファイアウォール設定

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]→[ファイアウォール設定]の順にクリックします。

設定画面の説明

■ ファイアウォール設定
Help

ファイアウォールを設定します。

パラメータを入力・修正し、操作を選んで [実行] ボタンをクリックしてください。

登録番号(優先順位) 登録 消去 検索 新規

[ファイアウォール登録]

動作	条件が一致すれば通す
送信元IPアドレス	全て
	開始IPアドレス <input type="text"/>
	終了IPアドレス <input type="text"/>
発信先IPアドレス	全て
	開始IPアドレス <input type="text"/>
	終了IPアドレス <input type="text"/>
ポート番号 プロトコル	<input checked="" type="radio"/> リストから選択 ALL(TCP_UDP:1-65534)
	<input type="radio"/> 手動で設定
	プロトコル <input type="text" value="TCP"/>
	発信元ポート 全て から <input type="text"/>
	送信先ポート 全て から <input type="text"/>
	ICMPタイプ <input type="text" value="値を入力"/>
ログ表示	表示する
スケジュール	<input type="radio"/> 常に有効 <input type="radio"/> 時間内無効 <input type="radio"/> 時間内有効

■ ファイアウォール一覧
Help

登録番号	タイプ	動作	送信元IPアドレス	接続先IPアドレス	発信元ポート	送信先ポート	プロトコル	ログ表示	スケジュール
59	アクセス制限	通さない	全て	169.254.0.0/255.255.0.0		全て		表示する	
60	DNS		QUERY Type: 6						
61	その他	回線が接続されていなければ通す	全て	全て	全て	全て	TCPFIN	表示する	

62	その他	回線が接続されている場合に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。	全て	全て	NETBIOS		表示する
63	その他	回線が接続されている場合に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。	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る場合に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。	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	<p>実行する操作を選択します。</p> <ul style="list-style-type: none"> ● [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	<p>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。</p> <ul style="list-style-type: none"> ● 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に許可する場合は[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	<p>送信元IPアドレスの条件を設定します。</p> <ul style="list-style-type: none"> ● 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	<p>発信先IPアドレスの条件を設定します。</p> <ul style="list-style-type: none"> ● 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。

項目	説明										
ポート番号 プロトコル	<p>ポート番号／プロトコルの条件を設定します。</p> <ul style="list-style-type: none"> ● 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。 										
	<table border="1"> <thead> <tr> <th>項目</th> <th>説明</th> </tr> </thead> <tbody> <tr> <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>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>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>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> </tbody> </table>	項目	説明	プロトコル	条件に指定するプロトコルの種類を選択します。	発信元ポート	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。	送信先ポート	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。	ICMPタイプ	[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。
項目	説明										
プロトコル	条件に指定するプロトコルの種類を選択します。										
発信元ポート	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。										
送信先ポート	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。										
ICMPタイプ	[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。										
ログ表示	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。										
スケジュール	<p>ファイアウォールのスケジュールを設定します。</p> <ul style="list-style-type: none"> ● 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.90) ● 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.90) 										
ファイアウォール一覧	登録されているファイアウォール一覧を表示します。										

8-4-2. ログ通知設定

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]→[ログ通知設定]の順にクリックします。

設定画面の説明

■ ログ設定 Help

ログの出力レベル、ログ取得オプション、SYSLOGサーバ転送オプションの設定をします。

パラメータを入力・修正して [設定] ボタンをクリックしてください。

[設定] [やり直し]

[基本]

ログ出力レベル DEBUG INFO NOTICE

[ログ取得オプション]

DoS攻撃防御	<input checked="" type="radio"/> 出力しない <input type="radio"/> 出力する
インターネット接続	<input checked="" type="radio"/> 出力しない <input type="radio"/> 出力する
アクセス制限	<input checked="" type="radio"/> 出力しない <input type="radio"/> 出力する
ファイアウォール	<input checked="" type="radio"/> 出力しない <input type="radio"/> 出力する
VPN	<input checked="" type="radio"/> 出力しない <input type="radio"/> 出力する

[SYSLOGサーバ転送オプション]

SYSLOGホストアドレス

SYSLOGファシリティ

DoS攻撃防御	<input checked="" type="radio"/> 転送しない <input type="radio"/> 転送する
インターネット接続	<input checked="" type="radio"/> 転送しない <input type="radio"/> 転送する
アクセス制限	<input checked="" type="radio"/> 転送しない <input type="radio"/> 転送する
ファイアウォール	<input checked="" type="radio"/> 転送しない <input type="radio"/> 転送する
VPN	<input checked="" type="radio"/> 転送しない <input type="radio"/> 転送する

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。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. 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。

8-4-3. 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

セキュリティ設定(セキュリティオプション) Help

ルータへのアクセス制限および、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。

パラメータを入力・修正して [設定] ボタンをクリックしてください。

[設定] [やり直し]

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。

[VPNパススルー設定]	
IPsecパススルー	<input checked="" type="radio"/> 透過しない <input type="radio"/> 透過する
LAN側IPsecホストアドレス	<input type="text"/>
PPTPパススルー	<input checked="" type="radio"/> 透過しない <input type="radio"/> 透過する
LAN側PPTPホストアドレス	<input type="text"/>
L2TPパススルー	<input checked="" type="radio"/> 透過しない <input type="radio"/> 透過する
LAN側L2TPホストアドレス	<input type="text"/>
3. ステルスモード：ステルスモードを設定します。

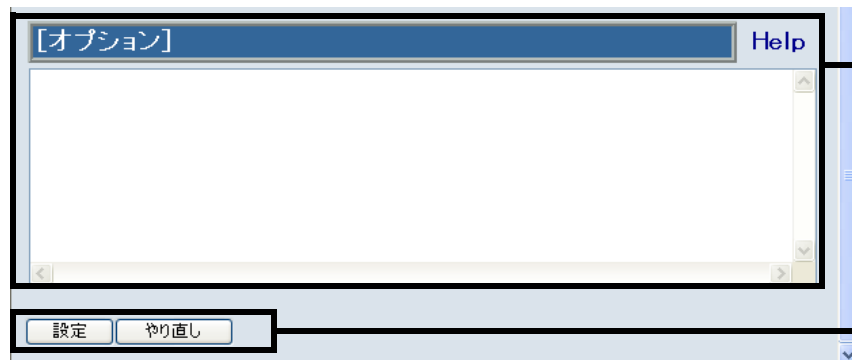
[ステルスモード設定]	
ステルスモード	<input checked="" type="radio"/> ON <input type="radio"/> OFF
ログ出力	<input checked="" type="radio"/> する <input type="radio"/> しない
4. SPI設定：SPIを使用して受信パケットを監視するかどうかを設定します。

[SPI設定]	
SPI	<input checked="" type="radio"/> ON <input type="radio"/> OFF
ログ出力	<input checked="" type="radio"/> する <input type="radio"/> しない
5. DMZホスト設定：DMZホストを設定します。

[DMZホスト設定]	
DMZホストアドレス	<input type="text"/>
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。

[DoS攻撃防御設定] 全ての接続／相手先に適用されます	
DoS攻撃防御	<input checked="" type="radio"/> ON <input type="radio"/> OFF
メール通知機能	<input type="radio"/> ON <input checked="" type="radio"/> OFF
送信先メールアドレス	<input type="text"/>
送信元メールアドレス	<input type="text"/>
SMTPサーバアドレス	<input type="text"/>
POP Before SMTP機能	<input type="radio"/> ON <input checked="" type="radio"/> OFF
POP3サーバアドレス	<input type="text"/>
ユーザ名	<input type="text"/>
パスワード	<input type="text"/>

[オプション] Help



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。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. 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 : 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コマンドに回答しなくなります。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し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。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。 [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。

8-4-4. 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

■ インターネットアクセス制限
Help

インターネットアクセス制限の設定をします。

パラメータを入力・修正し、操作を選んで [実行] ボタンをクリックしてください。

登録番号(優先順位) 登録 消去 検索 新規

[インターネットアクセス制限 登録]

送信元IPアドレス	全て	開始IPアドレス	終了IPアドレス		
発信先IPアドレス	全て	開始IPアドレス	終了IPアドレス		
ポート番号 プロトコル	<input checked="" type="radio"/> リストから選択	ALL(TCP_UDP:1-65534)		<input type="radio"/> 手動で設定	
	プロトコル	TCP		発信元ポート	全て から
				送信先ポート	全て から
				ICMPタイプ	値を入力
ログ表示	表示する				
スケジュール	<input type="radio"/> 常に有効 <input type="radio"/> 時間内無効 <input type="radio"/> 時間内有効				

■ インターネットアクセス制限一覧
Help

登録番号	タイプ	動作	送信元IPアドレス	接続先IPアドレス	発信元ポート	送
1	ファイアウォール	通さない	全て	192.168.0.1	全て	
2	ファイアウォール	通す	全て	全て		
3	ファイアウォール	通す	全て	全て		
45	その他	通さない	10.0.0.0/255.0.0.0	全て		
46	ファイアウォール	通す	全て	全て		

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	<p>実行する操作を選択します。</p> <ul style="list-style-type: none"> ● [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。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。
送信元IPアドレス	<p>送信元IPアドレスの条件を設定します。</p> <ul style="list-style-type: none"> ● 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	<p>発信先IPアドレスの条件を設定します。</p> <ul style="list-style-type: none"> ● 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。

項目	説明										
ポート番号 プロトコル	<p>ポート番号／プロトコルの条件を設定します。</p> <ul style="list-style-type: none"> ● 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。 										
	<table border="1"> <thead> <tr> <th>項目</th> <th>説明</th> </tr> </thead> <tbody> <tr> <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>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>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>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> </tbody> </table>	項目	説明	プロトコル	条件に指定するプロトコルの種類を選択します。	発信元ポート	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。	送信先ポート	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。	ICMPタイプ	[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。
	項目	説明									
	プロトコル	条件に指定するプロトコルの種類を選択します。									
	発信元ポート	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。									
送信先ポート	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。										
ICMPタイプ	[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。										
ログ表示	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。										
スケジュール	<p>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。</p> <ul style="list-style-type: none"> ● 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.90) ● 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.90) 										
インターネットアクセス制御一覧	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。										

8-4-5. アプリケーション設定

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]→[アプリケーション設定]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	<p>実行する操作を選択します。</p> <ul style="list-style-type: none"> ● [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。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。
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。

8-4-6. スケジュール設定

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。
 - 『8-4-1. ファイアウォール設定』 (P.76)
 - 『8-4-4. インターネットアクセス制御』 (P.85)
 - 『8-4-7.MAC アドレスフィルタ設定』 (P.92)
 - 『8-4-8.URL フィルタリング設定』 (P.94)

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]→[スケジュール設定]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。

曜日	開始時刻1	終了時刻1	開始時刻2	終了時刻2
日曜日	00:00	00:00	00:00	00:00
月曜日	00:00	00:00	00:00	00:00
火曜日	00:00	00:00	00:00	00:00
水曜日	00:00	00:00	00:00	00:00
木曜日	00:00	00:00	00:00	00:00
金曜日	00:00	00:00	00:00	00:00
土曜日	00:00	00:00	00:00	00:00

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。

■ セキュリティ設定(スケジュール時刻設定)
Help

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

パラメータを入力・修正して [設定] ボタンをクリックしてください。
 曜日毎にアクセス制限を行う「開始/終了」時刻を入力します。
 1日の中で2回のスケジュール設定が可能です。
 0:00をまたいだ設定(23:45~4:30など)はできません。
 終了時刻は設定した時刻の「直前まで」となります(1日の終わりまでとしたい場合には、24:00と入力します)。

[スケジュールの登録/削除]

機能	<input checked="" type="radio"/> 登録 <input type="radio"/> 削除			
曜日	日曜日 ▼			
番号	1 ▼			
開始時刻	00	:	00	
終了時刻	00	:	00	

曜日	開始時刻1	終了時刻1	開始時刻2	終了時刻2
日曜日	00:00	00:00	00:00	00:00
月曜日	00:00	00:00	00:00	00:00
火曜日	00:00	00:00	00:00	00:00
水曜日	00:00	00:00	00:00	00:00
木曜日	00:00	00:00	00:00	00:00
金曜日	00:00	00:00	00:00	00:00
土曜日	00:00	00:00	00:00	00:00

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	週力時刻を入力します。

8-4-7. MACアドレスフィルタ設定

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。

登録番号	MACアドレス	登録番号	MACアドレス
0		16	
1		17	
2		18	
3		19	
4		20	
5		21	
6		22	
7		23	
8		24	
9		25	
10		26	
11		27	

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、ブロードバンド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。

■ セキュリティ設定 (MACアドレス登録/削除) Help

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。

Message
パラメータを入力・修正して [設定] ボタンをクリックしてください。

[設定] [やり直し]

[MACアドレスの登録/削除]

機能 登録 削除

登録番号 0

MACアドレス

スケジュール 常に有効

登録番号	MACアドレス	スケジュール	登録番号	MACアドレス	スケジュール
0			16		
1			17		
2			18		
3			19		
4			20		
5			21		
6			22		

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。 <ul style="list-style-type: none"> ● 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.90) ● 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.90)

8-4-8. URLフィルタリング設定

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フィルタリング]の順にクリックします。

設定画面の説明

■ セキュリティ設定 (URLフィルタ)
Help

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。

Message

パラメータを入力・修正して [設定] ボタンをクリックしてください。

[URLフィルタリング]

有効	文字列	比較方法	処理	ログ	スケジュール
✓ 1	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 2	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 3	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 4	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 5	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 6	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 7	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 8	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 9	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 10	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 11	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 12	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 13	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 14	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 15	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 16	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 17	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 18	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 19	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 20	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 21	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 22	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 23	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 24	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 25	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 26	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 27	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 28	<input type="text"/>	を含む	拒否	ログ表示	常に有効
✓ 29	<input type="text"/>	を含む	拒否	ログ表示	常に有効

<input checked="" type="checkbox"/> 30	<input type="text"/>	を含む	拒否	ログ表示	常に有効
<input checked="" type="checkbox"/> 31	<input type="text"/>	を含む	拒否	ログ表示	常に有効
上記の条件に一致しなかったもの		通過	ログ非表示		

設定 やり直し

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。
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。 <ul style="list-style-type: none"> ● 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.90) ● 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.90)
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。

8-4-9. 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。

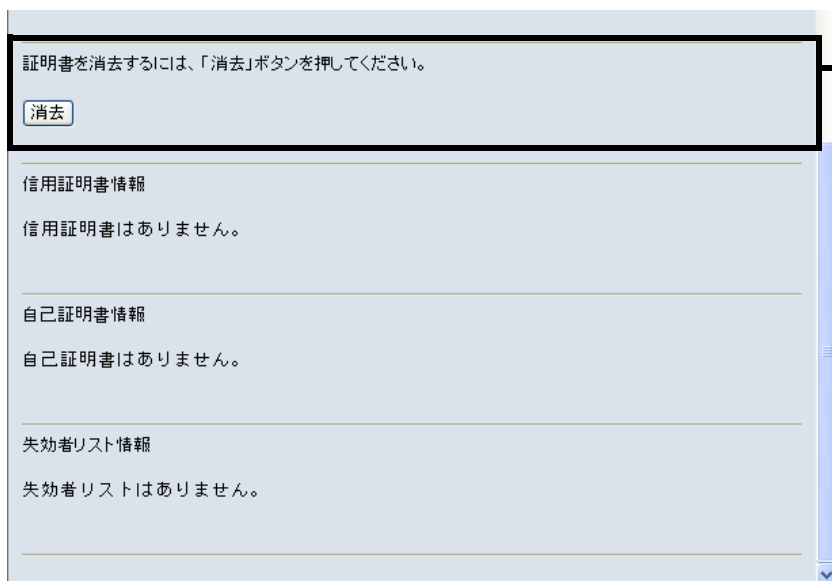
表示方法

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。

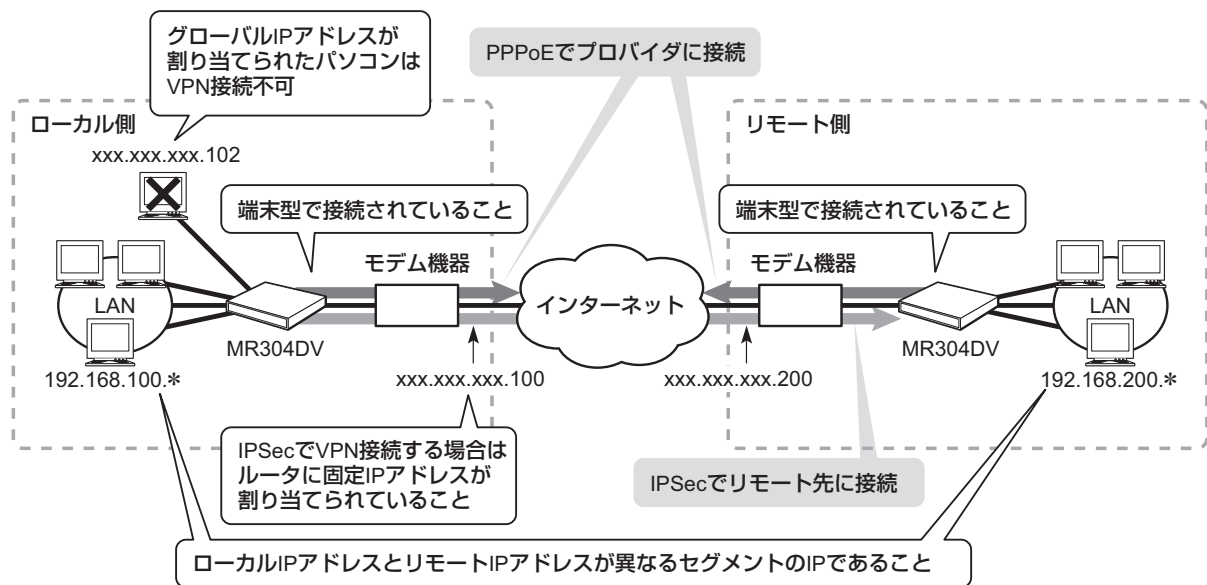
3. 証明書の消去 : 証明書を消去します。

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。

8-5. 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『8-4-3.セキュリティオプション』(P.82)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。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。
- スター型(センター拠点)のトンネル接続を行った場合、拠点同士の接続は拠点同士でトンネル接続するメッシュ型の接続方式を行う必要があります。
- 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。

8-5-1. 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

The screenshot shows the 'VPN Policy Settings' page. At the top, there is a 'Help' link and a description: 'VPN Policy Settings'. Below this is a section for 'Basic Settings' with a radio button for 'Do not use' selected for the IPsec function. A second section is for 'Registration', with a text box containing '1', a radio button for 'Register' selected, and an 'Execute' button. A third section at the bottom is for 'VPN Policy Settings Overview' with a table of columns: 'Registration Number', 'Use', 'Gateway Address', 'Local IP Address', 'Remote IP Address', and 'Key Exchange'.

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	<ul style="list-style-type: none"> ● [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]	<ul style="list-style-type: none"> ● [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.101)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

VPN(IPSec) 設定 (VPNポリシー) Help

VPNポリシーを設定します。

以下の項目を入力・修正して、[設定] ボタンをクリックしてください。

[設定] やり直し

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.102)
2. 基本：VPNポリシーの基本情報を設定します。(P.102)
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.103)
4. 認証：認証方式を設定します。(P.104)
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.104)

[基本]

登録番号 1

ポリシー 使用しない 使用する

[IPアドレス]

リモートゲートウェイアドレス 動的 固定

IPアドレス 0.0.0.0

ローカルIPアドレス 単一アドレス

開始IPアドレス 0.0.0.0

終了IPアドレス 0.0.0.0

サブネットマスク 0.0.0.0

リモートIPアドレス 単一アドレス

開始IPアドレス 0.0.0.0

終了IPアドレス 0.0.0.0

サブネットマスク 0.0.0.0

[認証]

認証プロトコル ESP

アルゴリズム(AH) MD5

アルゴリズム(ESP) MD5

暗号化プロトコル ESP

アルゴリズム 3DES

[キー交換]

キー管理方式 手動キー交換 IKE (Internet Key Exchange)

方向 両方向

ローカルIDタイプ IPアドレス

ID

リモートIDタイプ IPアドレス

ID

相手認証方式 事前共有鍵を使用する 証明書を使用する

事前共有鍵

ハッシュアルゴリズム	MD5
暗号化アルゴリズム	3DES
交換モード	メインモード
IKE Keep Alive	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
IPアドレス	0.0.0.0
pingトライ間隔	6 (秒)
pingトライ回数	10 (回)
IKE自動接続	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ISAKMPトライ間隔	5 (秒)
ISAKMPトライ回数	10 (回)
ISAKMP SA 有効期間	28800 (秒)
IPSec SA 有効期間	28800 (秒)
DH グループ	Group 2 (1024 Bit)
IKE PFS	無効
[Path MTU Discovery]	
DFビット	コピー
[NAT-Traversal]	
NAT-Traversal機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
IKEネゴシエーション機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
<input type="button" value="設定"/> <input type="button" value="やり直し"/>	

- 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.104)
- 6. Path MTU Discovery：Path MTU DiscoveryのDFビットモードを設定します。(P.109)
- 7. NAT-Traversal：NAT-Traversal機能を設定します。(P.109)
- 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.102)

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]の状態を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どうかを選択します。[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	<ul style="list-style-type: none"> ● 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	<p>VPN接続を許可するローカルIPアドレスを設定します。</p> <ul style="list-style-type: none"> ● 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。 ● 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。
リモートIPアドレス	<p>[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。</p> <ul style="list-style-type: none"> ● 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。



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せんが、同時に2つ以上接続することはできません。

4. 認証 : 認証方式を設定します。

項目	説明
認証プロトコル	<p>認証に使用するプロトコルを選択します。</p> <ul style="list-style-type: none"> ● 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	<p>[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。</p> <p>[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。</p>

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	<p>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。</p> <ul style="list-style-type: none"> ● 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.105) ● 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.107)

手動キー交換を選択した場合

[キー交換]	
キー管理方式	<input checked="" type="radio"/> 手動キー交換 <input type="radio"/> IKE (Internet Key Exchange)
AH キー イン	<input type="text"/>
AH キー アウト	<input type="text"/>
AH SPI イン	<input type="text" value="256"/>
AH SPI アウト	<input type="text" value="256"/>
ESP 暗号 キー イン	<input type="text"/>
ESP 暗号 キー アウト	<input type="text"/>
ESP ハッシュ キー イン	<input type="text"/>
ESP ハッシュ キー アウト	<input type="text"/>
ESP SPI イン	<input type="text" value="256"/>
ESP SPI アウト	<input type="text" value="256"/>

項目	説明
AHキーイン	<p>[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 Inbound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。</p> <ul style="list-style-type: none"> ● [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	<p>[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 Outbound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。</p> <ul style="list-style-type: none"> ● [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	<p>[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。</p> <p>[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。</p>
AH SPIアウト	<p>[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。</p> <p>[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。</p>
ESP暗号化キーイン	<p>[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 Inbound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。</p> <ul style="list-style-type: none"> ● [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	<p>[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Outbound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。</p> <ul style="list-style-type: none"> ● [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	<p>[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Inbound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。</p> <ul style="list-style-type: none"> ● [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	<p>[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Outbound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。</p> <ul style="list-style-type: none"> ● [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 SPIイン	<p>[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。</p> <p>[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。</p>
ESP SPIアウト	<p>[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。</p> <p>[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。</p>



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

[キー交換]	
キー管理方式	<input type="radio"/> 手動キー交換 <input checked="" type="radio"/> IKE (Internet Key Exchange)
方向	両方向
ローカルIDタイプ	IPアドレス
ID	
リモートIDタイプ	IPアドレス
ID	
相手認証方式	<input checked="" type="radio"/> 事前共有鍵を使用する <input type="radio"/> 証明書を使用する
事前共有鍵	
ハッシュアルゴリズム	MD5
暗号化アルゴリズム	3DES
交換モード	メインモード
IKE Keep Alive	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
IPアドレス	0.0.0.0
ping/トライ間隔	6 (秒)
ping/トライ回数	10 (回)
IKE自動接続	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ISAKMP/トライ間隔	5 (秒)
ISAKMP/トライ回数	10 (回)
ISAKMP SA 有効期間	28800 (秒)
IPSec SA 有効期間	28800 (秒)
DH グループ	Group 2 (1024 Bit)
IKE PFS	無効

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。 →『8-5-2.証明書(IPSec)』(P.110)

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。 <ul style="list-style-type: none"> ● 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. 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。 <ul style="list-style-type: none"> ● [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。

7. 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。

8-5-2. 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。

8-6. IPv6設定

8-6-1. 共通設定

本製品はIPv6のブリッジ機能に対応しています。
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。

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]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。
動作モード	IPv6の動作方法を選択します。 <ul style="list-style-type: none"> ● 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。
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。 [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。

8-7. 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 64 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

NAT 設定
Help

プライベートアドレスをグローバルアドレスに変換するためのルールを設定します。

パラメータを入力・修正し、操作を選んで [実行] ボタンをクリックしてください。

登録番号(優先順位) 登録 消去 検索 新規

[アドレスマッピング登録]

プライベートIPアドレス	全て <input type="button" value="▼"/> 開始IPアドレス <input type="text"/> 終了IPアドレス <input type="text"/>
グローバルIPアドレス	<input checked="" type="radio"/> 動的に取得 <input type="button" value="dynamic"/> <input type="button" value="▼"/> <input type="radio"/> 手動で設定 <input type="text"/>
ポート番号 プロトコル	<input checked="" type="radio"/> リストから選択 <input type="button" value="ALL(TCP_UDP:1-65534)"/> <input type="button" value="▼"/> <input type="radio"/> 手動で設定 プロトコル <input type="button" value="TCP"/> <input type="button" value="▼"/> ポート番号 <input type="button" value="全て"/> <input type="button" value="▼"/> から <input type="text"/> ICMPタイプ <input type="button" value="値を入力"/> <input type="text"/>
インタフェース	全て <input type="button" value="▼"/>
latestオプション	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

アドレスマッピング一覧
Help

登録番号	プライベートアドレス	プロトコル	ポート番号	グローバルアドレス	インタフェース	オプション
------	------------	-------	-------	-----------	---------	-------

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。1～32まで登録できます。
登録／消去／検索／新規	<p>実行する操作を選択します。</p> <ul style="list-style-type: none"> ● [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	<p>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。</p> <ul style="list-style-type: none"> ● 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	<p>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。</p> <ul style="list-style-type: none"> ● 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。

項目	説明								
ポート番号 プロトコル	<p>通信を許可するポート番号／プロトコルを設定します。</p> <ul style="list-style-type: none"> ● 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 border="1"> <thead> <tr> <th>項目</th> <th>説明</th> </tr> </thead> <tbody> <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> </tbody> </table>	項目	説明	プロトコル	通信を許可するプロトコルの種類を選択します。	ポート番号	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。	ICMPタイプ	[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。
	項目	説明							
	プロトコル	通信を許可するプロトコルの種類を選択します。							
ポート番号	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。								
ICMPタイプ	[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。								
インターフェース	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。								
latestオプション	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。								



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。

8-8. 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。パソコンのUPnP設定については、『10-2.UPnP機能の設定』(P.147)を参照してください。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。

8-9. 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

■ ダイナミックDNS設定
Help

ダイナミックDNSを設定します

パラメータを入力・修正して [設定] ボタンをクリックしてください。
 送信パスワードは、どのような文字列を設定しても「*」または「●」の1文字が表示されます。
 変更するときは、表示されている「*」または「●」を消去してから、新しい文字列を入力してください。

設定
やり直し

[ダイナミックDNS設定]

ダイナミックDNS登録	<input checked="" type="radio"/> しない <input type="radio"/> する
登録経路	#0
ドメイン名	<input type="text"/>
DDNSサーバアドレス	<input type="text"/>
ログイン名(サブドメイン名)	<input type="text"/>
パスワード	<input type="password"/>
パスワード(再入力)	<input type="password"/>

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。

8-10. 管理コマンド・設定

8-10-1. 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[閉じる]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、『7-3-1.再起動』(P.40)を参照してください。

8-10-2. 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、『7-3-2.設定の消去』(P.41)を参照してください。

8-10-3. ユーザ・パスワード変更

ブロードバンド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、『7-3-3. ユーザ・パスワード変更』(P.42)を参照してください。

8-10-4. アクセス権限

ブロードバンド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

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、『7-3-4. アクセス権限』(P.44)を参照してください。

8-10-5. 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、『7-3-5. ファームウェア更新』(P.47)を参照してください。

8-10-6. 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、『7-3-6. 設定メンテナンス』(P.48)を参照してください。

8-11. 切断／接続状況

8-11-1. 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、『7-2-1.PPTP』(P.36)を参照してください。

8-11-2. 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、『7-2-2.PPPoE』(P.38)を参照してください。

8-12. 情報表示

8-12-1. 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せん。

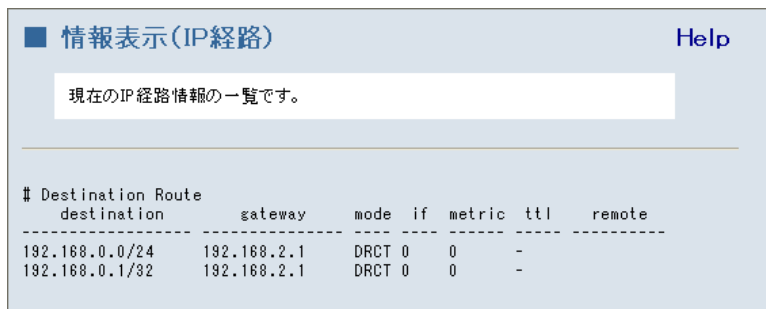


8-12-2. IP経路

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せん。



8-12-3. 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せん。

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、『7-4-3.ログ』(P.51) を参照してください。

8-12-4. 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、『7-4-4.WAN状況』(P.52) を参照してください。

8-12-5. 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、『7-4-5.UPnP状況』(P.53)を参照してください。

8-12-6. 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、『7-4-6.IPSec状況』(P.54)を参照してください。

8-13. その他

8-13-1. 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せん。

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。

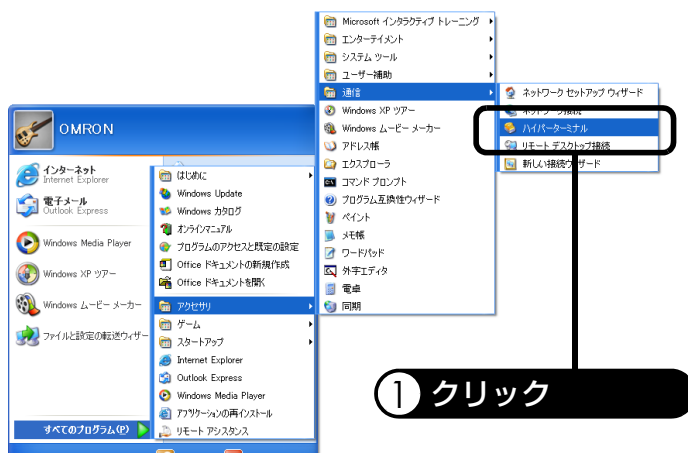
9. コマンドを使った設定方法

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。

9-1. 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。

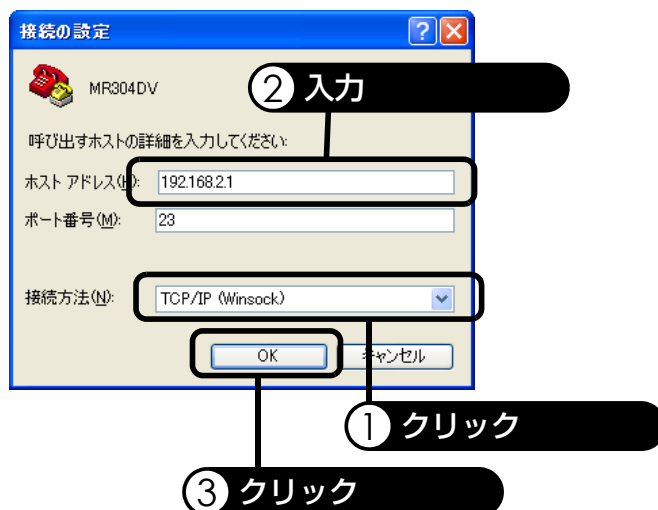


2. 接続の設定画面が表示されるので、[名前]欄に任意の接続名を入力し、[OK]をクリックします。



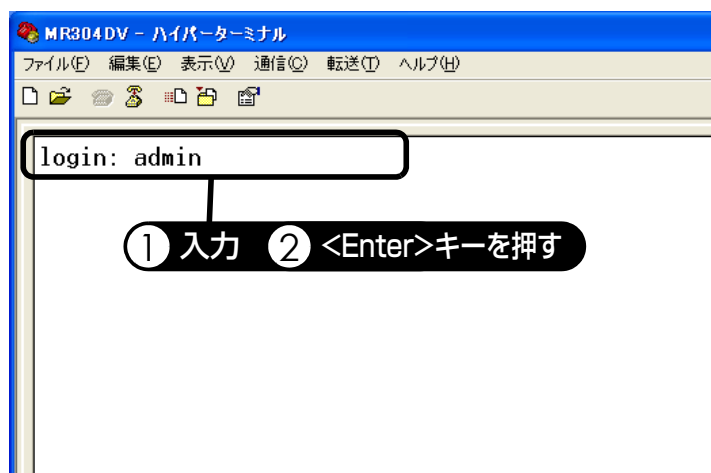
3. [接続方法]欄で[TCP/IP (Winsock)]を選択し、[ホストアドレス]欄に「192.168.2.1」を入力して、[OK]をクリックします。

- ・ 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。



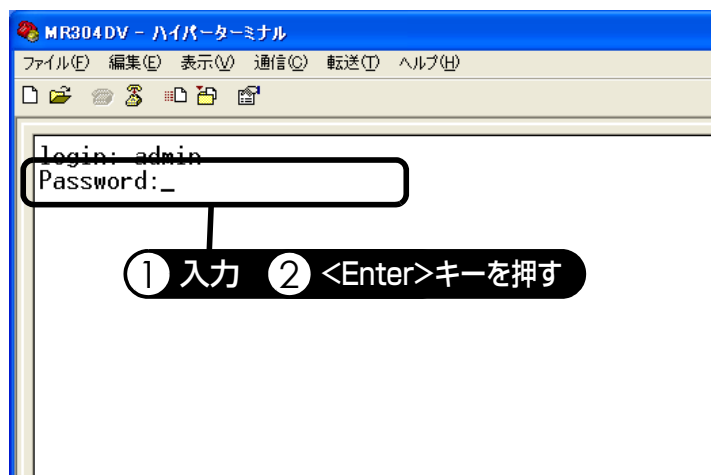
4. ハイパーターミナル画面が表示され、「login:」が画面に表示されます。

- 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。



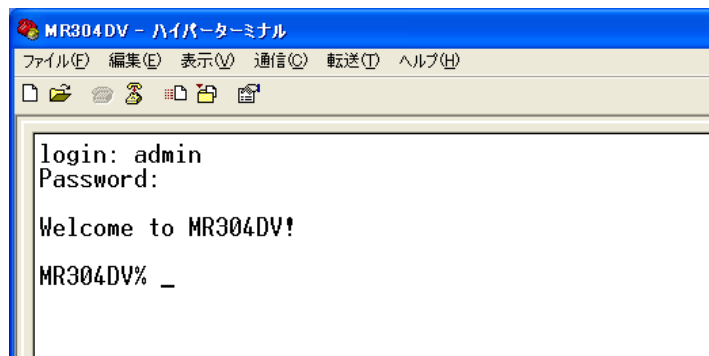
補足

- ・ 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 MR304DV!」が表示されます。

- ・ 本機の名称を変更している場合には、「MR304DV」の代わりに設定した名称が表示されます。
- ・ MR304Xの場合は、「MR304DV」の代わりに「MR304X」が表示されます。

以上でログインは完了です。



9-2. 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。

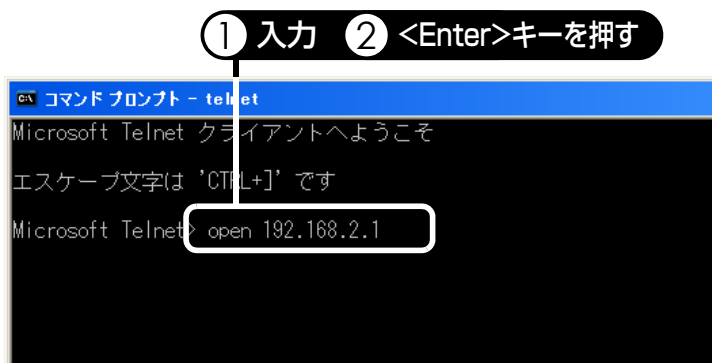
1. [スタート]－[すべてのプログラム]－[アクセサリ]－[コマンドプロンプト]の順にクリックします。



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。

① 入力 ② <Enter>キーを押す

```

c# Telnet 192.168.2.1
login: admin_
    
```

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。

① 入力 ② <Enter>キーを押す

```

c# Telnet 192.168.2.1
login: admin
Password: _
    
```

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 MR304DV!」
が表示されます。
・本機の名称を変更している
場合には、「MR304DV」の
代わりに設定した名称が表
示されます。
・MR304Xの場合は、
「MR304DV」の代わりに
「MR304X」が表示されま
す。

```

c# Telnet 192.168.2.1
login: admin
Password:
Welcome to MR304DV!
MR304DV% _
    
```

以上でログインは完了です。

10. 付録(パソコンの設定)

10-1. IPアドレスを手動で割り当てる

個々のパソコンに手動でIPアドレスを割り当てる場合、このパソコンの設定を行います。
ネットワークの設定は各OSによって手順が異なります。

- 『10-1-1.Windows XP/Server 2003の場合』(P.133)
- 『10-1-2.Windows Me/98/95の場合』(P.136)
- 『10-1-3.Windows 2000の場合』(P.139)
- 『10-1-4.Windows NT 4.0の場合』(P.141)
- 『10-1-5.Mac OS 8.x/9.xの場合』(P.144)
- 『10-1-6.Mac OS X 10.0.x~10.2.8の場合』(P.145)
- 『10-1-7.Mac OS X 10.3.x(Panther)の場合』(P.146)

10-1-1. Windows XP/Server 2003の場合

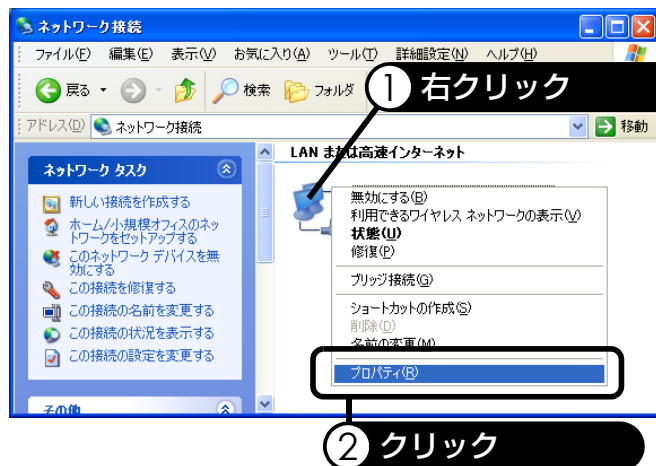
1. [スタート]—[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[ネットワーク接続]をダブルクリックします。



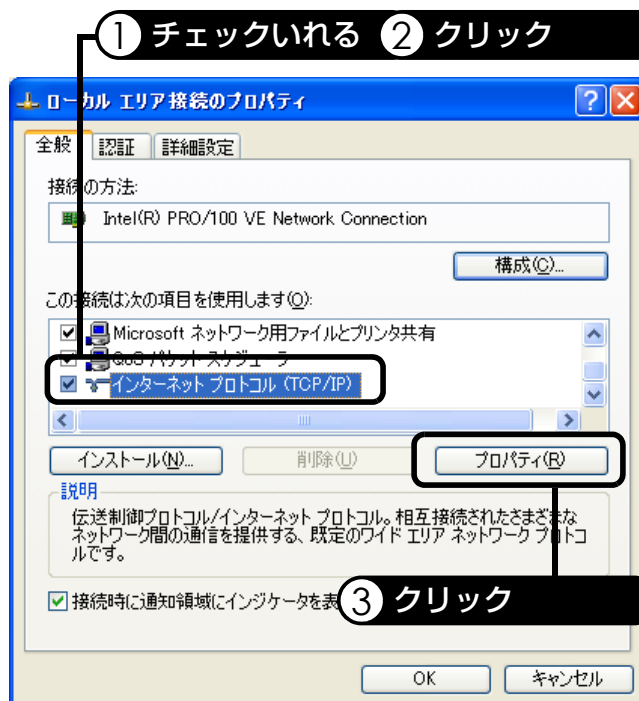
補足

- [ネットワーク接続]が表示されない場合は、画面左上の [クラシック表示に切り替える] をクリックしてください。

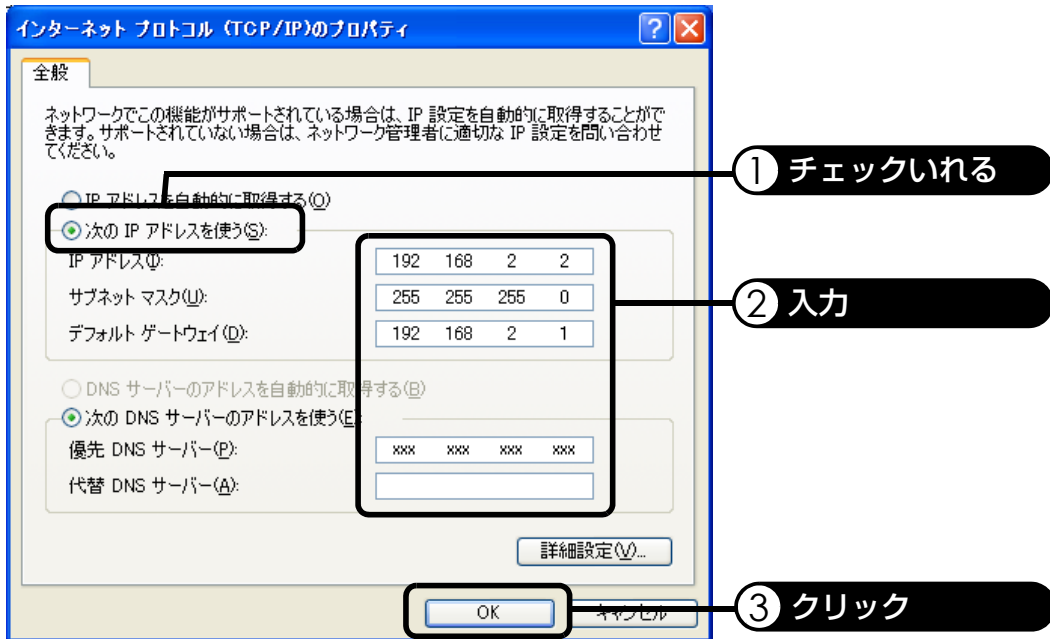
2. [ローカルエリア接続]を右クリックし、[プロパティ]をクリックします。



3. [インターネットプロトコル (TCP/IP)]のチェックが入っていることを確認し、選択してから、[プロパティ]をクリックします。



4. [次のIPアドレスを使う]を選択し、各項目に以下の説明にしたがい設定を入力します。入力を完了したら、[OK]をクリックします。



- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入ります)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ デフォルトゲートウェイ
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。
- ・ 優先DNSサーバ／代替DNSサーバ
プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力します。

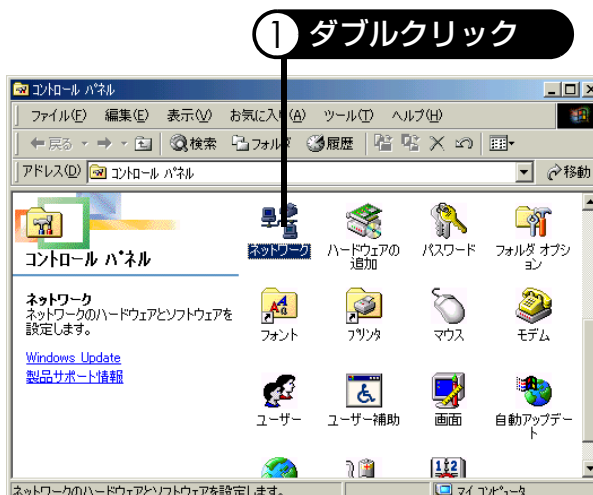
5. [OK]をクリックして[ローカルエリア接続のプロパティ]画面を閉じます。

6. 「再起動しますか」と表示されたら、指示に従ってパソコンを再起動してください。

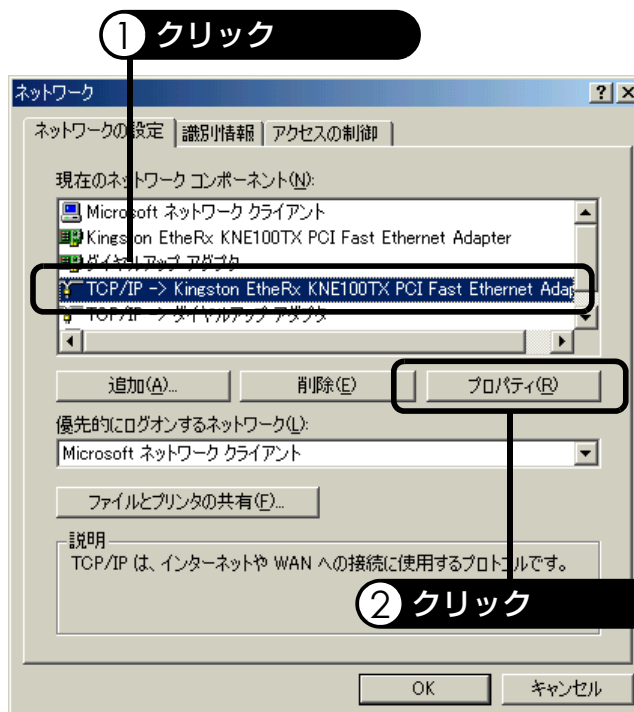
TCP/IPの設定は以上です。

10-1-2. Windows Me/98/95の場合

1. [スタート]－[設定]－[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[ネットワーク]をダブルクリックします。

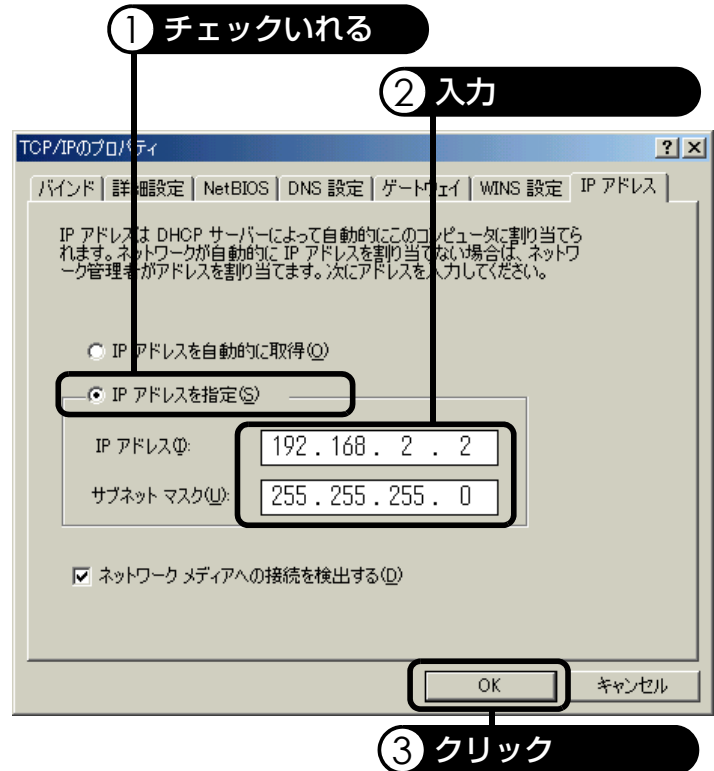


2. [TCP/IP]をクリックし、[プロパティ]をクリックします。



3. [IPアドレスを指定]を選択し、各項目に以下の説明にしたがい設定を入力します。

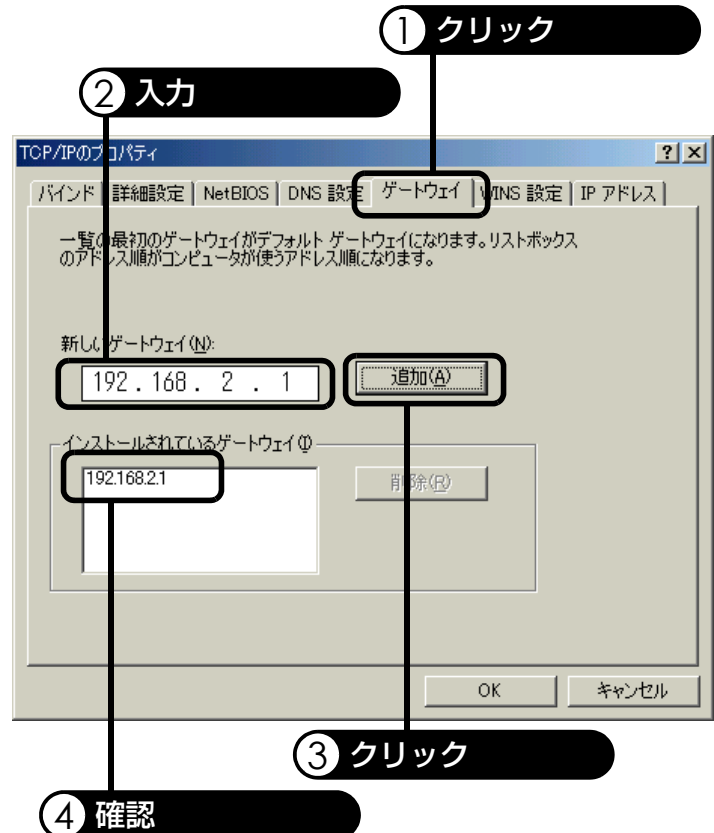
- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入ります)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。



4. [ゲートウェイ]タブをクリックします。

5. [新しいゲートウェイ]欄にゲートウェイアドレスを入力し、[追加]をクリックします。[追加]をクリックしたら、入力したゲートウェイアドレスが[インストールされているゲートウェイ]欄に追加されたことを確認してください。

- ・ [新しいゲートウェイ]欄には、本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。



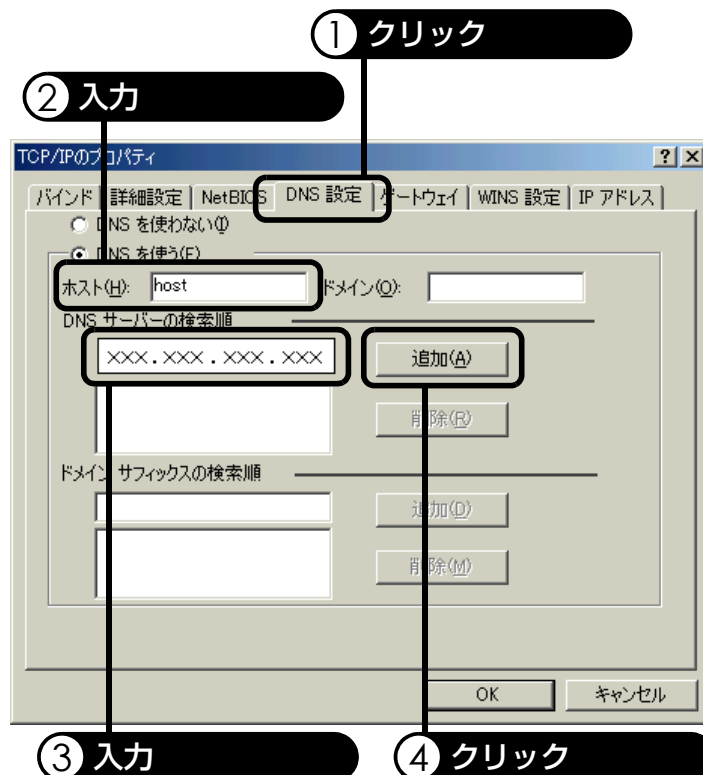
6. [DNS設定]タブをクリックします。

7. [ホスト]欄にパソコンの名称を入力します。

- ・ ホスト名は、プロバイダから指定がない限り適当な名前を入力して構いません。

8. [DNSサーバの検索順]下の欄に、プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力し、[追加]をクリックします。

[追加]をクリックしたら、入力したグローバルIPアドレスが入力欄下の一覧に追加されたことを確認してください。



9. [OK]をクリックして、[TCP/IPのプロパティ]画面と[ネットワーク]画面を閉じます。

10. 「再起動しますか」と表示されたら、指示に従ってパソコンを再起動してください。

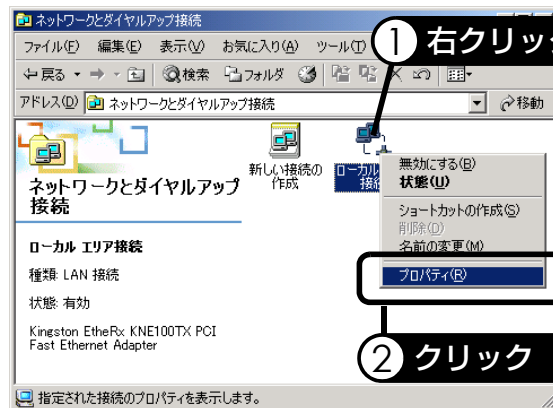
TCP/IPの設定は以上です。

10-1-3. Windows 2000の場合

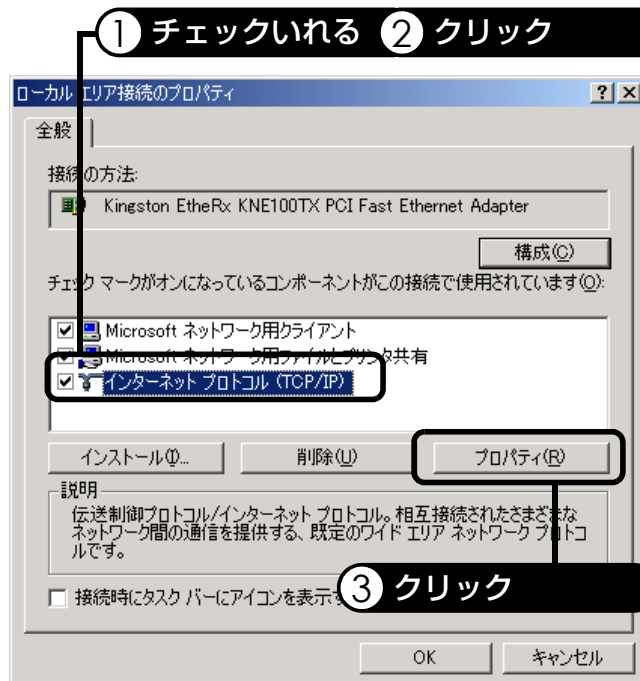
1. [スタート]－[設定]－[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[ネットワークとダイヤルアップ接続]をダブルクリックします。



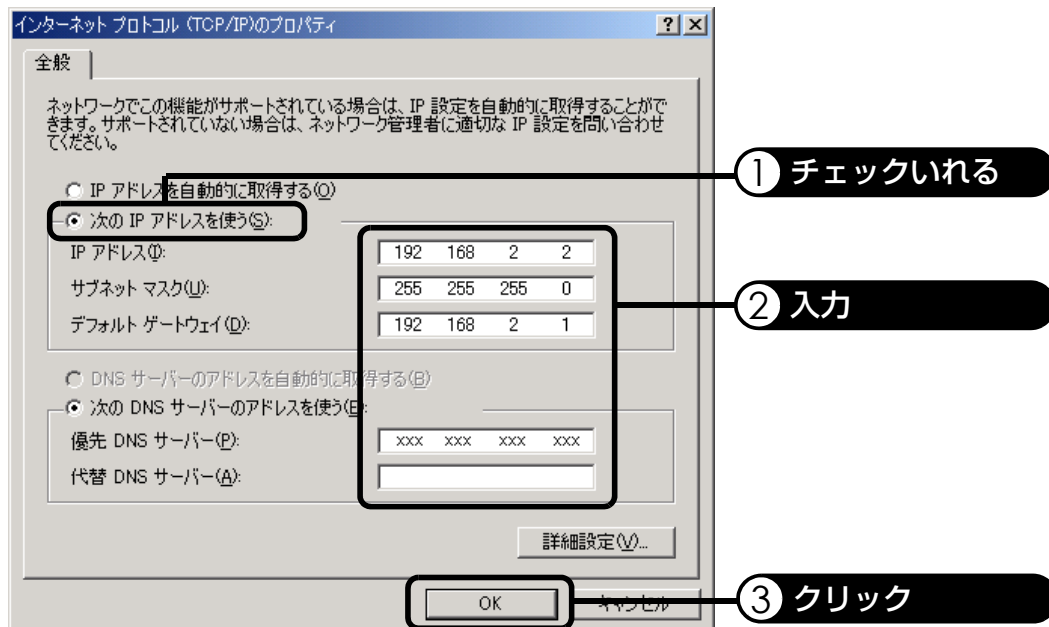
2. [ローカルエリア接続]を右クリックし、[プロパティ]をクリックします。



3. [インターネットプロトコル (TCP/IP)]のチェックが入っていることを確認し、選択してから、[プロパティ]をクリックします。



4. [次のIPアドレスを使う]を選択し、各項目に以下の説明にしたがい設定を入力します。入力を完了したら、[OK]をクリックします。



- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入ります)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ デフォルトゲートウェイ
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。
- ・ 優先DNSサーバ／代替DNSサーバ
プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力します。

5. [OK]をクリックして[ローカルエリア接続のプロパティ]画面を閉じます。

6. 「再起動しますか」と表示されたら、指示に従ってパソコンを再起動してください。

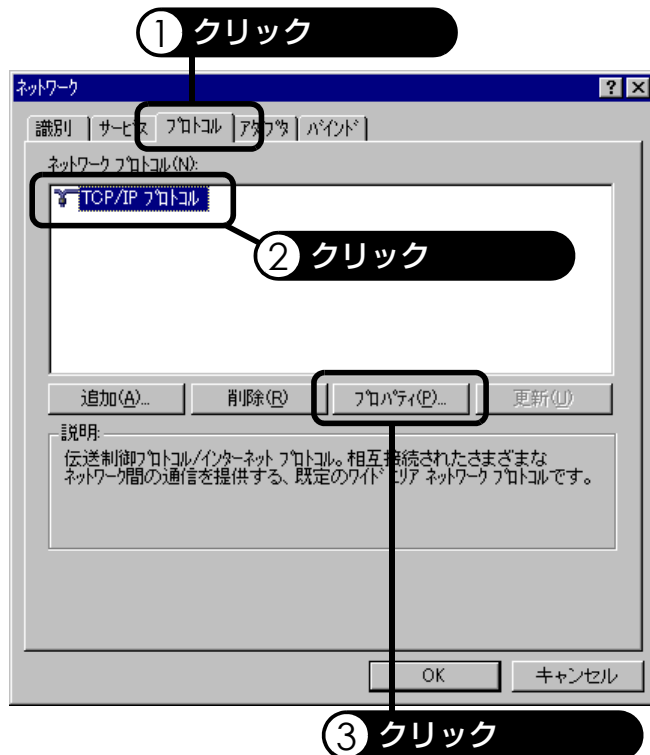
TCP/IPの設定は以上です。

10-1-4. Windows NT 4.0の場合

1. [スタート]－[設定]－[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[ネットワーク]をダブルクリックします。

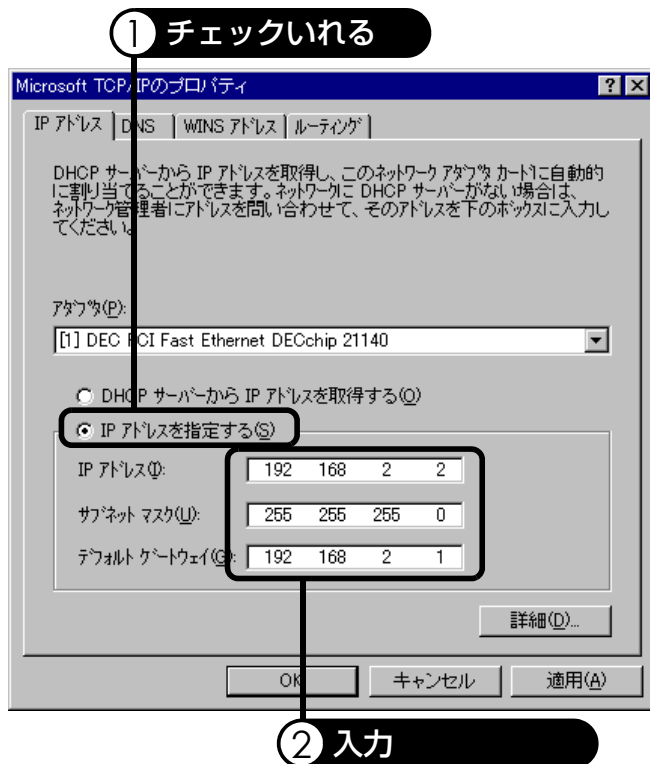


2. [プロトコル]タブをクリックし、[TCP/IPプロトコル]をクリックしてから[プロパティ]をクリックします。



3. [IPアドレスを指定する]を選択し、各項目に以下の説明にしたがい設定を入力します。

- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入りません)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ デフォルトゲートウェイ
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。

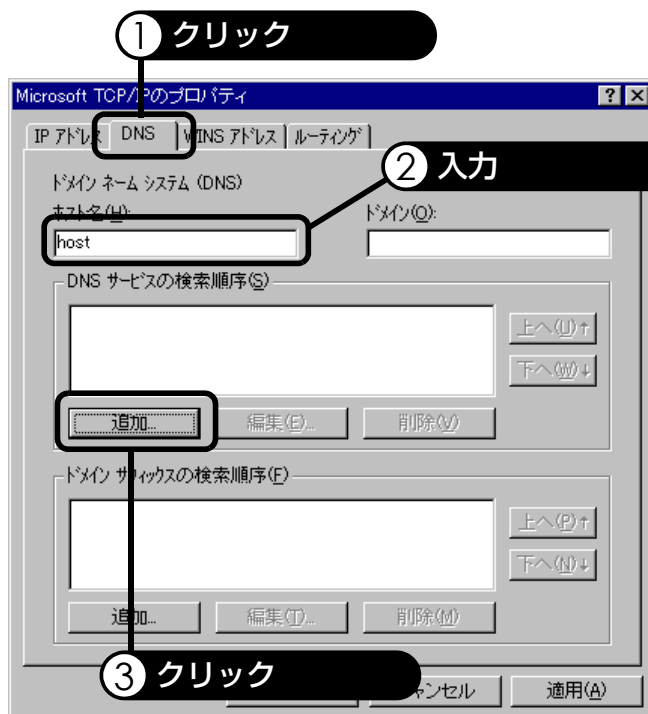


4. [DNS設定]タブをクリックします。

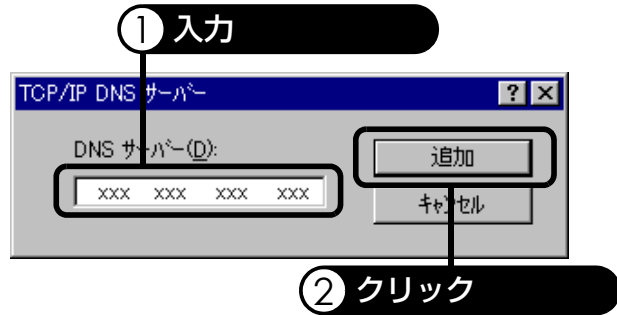
5. [ホスト名]欄にパソコンの名称を入力します。

- ・ ホスト名は、プロバイダから指定がない限り適当な名前を入力して構いません。

6. ホスト名を入力したら、[DNSサービス検索順序]欄にある[追加]をクリックします。



7. [DNSサーバ]欄に、プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力し、[追加]をクリックします。



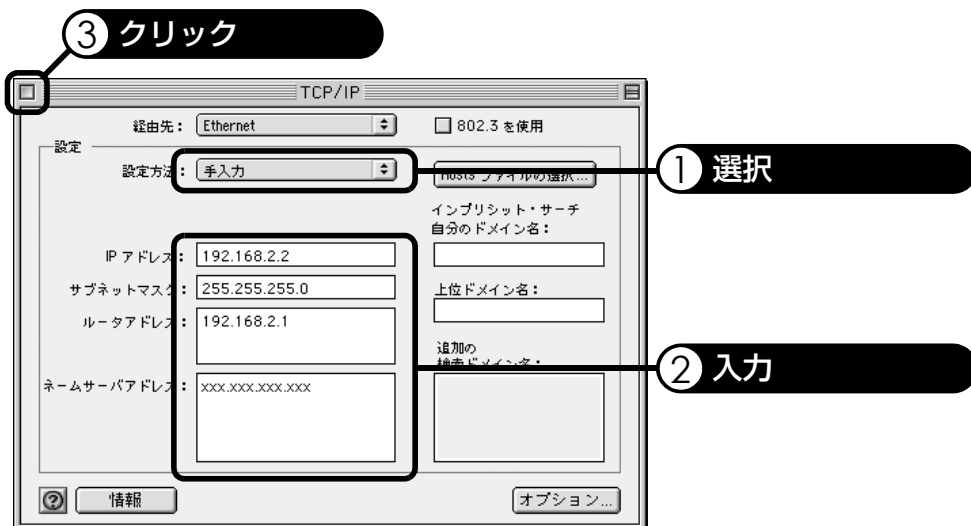
8. 入力したグローバルIPアドレスが入力欄下の一覧に追加されたことを確認し、[OK]をクリックします。



9. [OK]をクリックして[ネットワーク]画面を閉じます。
10. 「再起動しますか」と表示されたら、指示に従ってパソコンを再起動してください。
TCP/IPの設定は以上です。

10-1-5. Mac OS 8.x/9.xの場合

1. アップルメニューから[コントロールパネル]—[TCP/IP]の順にクリックします。
2. [設定方法]欄で[手入力]を選択し、以下の説明にしたがい各項目に設定を入力します。入力を完了したら、左上のクローズボックスをクリックし、画面を閉じます。保存画面が表示された場合は[保存]をクリックします。



- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入ります)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ ルーターアドレス
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。
- ・ ネームサーバアドレス
プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力します。

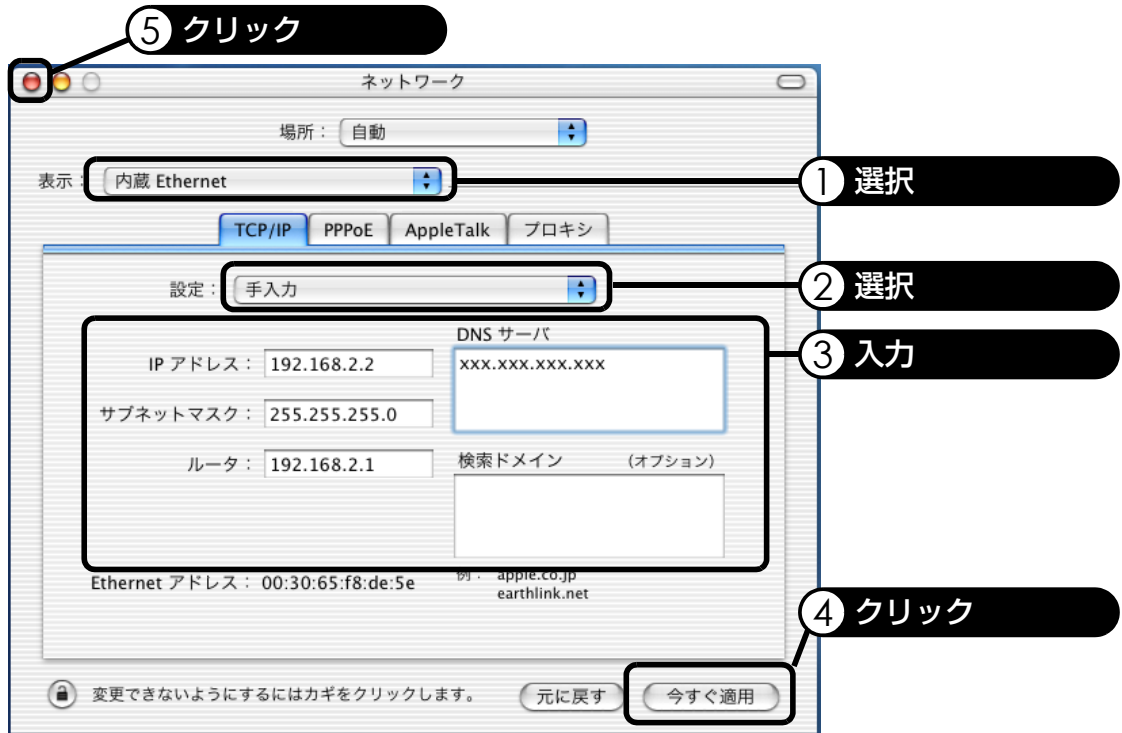
補足

- 上記画面と異なる場合は、TCP/IP の [編集] — [利用者モード] を選択し、[詳しい情報も指定] を選択し、[OK] をクリックしてください。

TCP/IPの設定は以上です。

10-1-6. Mac OS X 10.0.x~10.2.8の場合

1. アップルメニューから[場所] - [ネットワーク環境設定]の順にクリックします。
2. [表示]^(*1)欄で[内蔵Ethernet]を選択し、[設定]欄で[手入力]を選択します。以下の説明にしたがい各項目に設定を入力します。入力を完了したら、[今すぐ適用]^(*2)をクリックし、左上のクローズボックスをクリックして画面を閉じます。



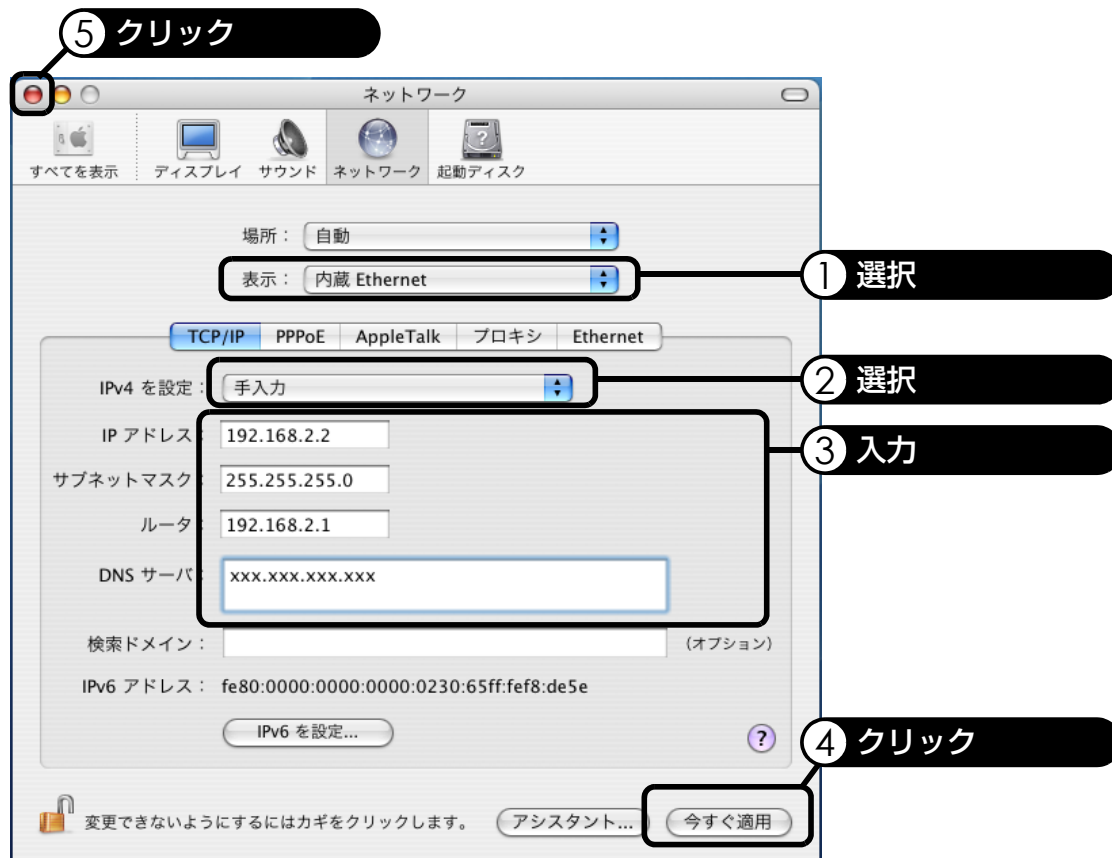
- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2~254までの数値が入ります)を入力します。
- ・ サブネットマスク^(*3)
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ ルータ^(*3)
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。
- ・ DNSサーバ^(*4)
プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力します。

*1 [表示]は、お使いのMac OS Xのバージョンによっては、[設定]で表示されます。
 *2 [今すぐ適用]は、お使いのMac OS Xのバージョンによっては、[保存]で表示されます。
 *3 [サブネットマスク]および[ルータ]はお使いのMac OS Xのバージョンによっては表示されません。
 *4 [DNSサーバ]は、お使いのMac OS Xのバージョンによっては、[ドメインネームサーバ]で表示されます。

TCP/IPの設定は以上です。

10-1-7. Mac OS X 10.3.x(Panther)の場合

1. アップルメニューから[場所] - [ネットワーク環境設定]の順にクリックします。
2. [表示]欄で[内蔵Ethernet]を選択し、[設定]欄で[手入力]選択します。各項目に以下の説明にしたがい設定を入力します。
入力を完了したら、[今すぐ適用]をクリックし、左上のクローズボックスをクリックして画面を閉じます。



- ・ IPアドレス
パソコンに割り当てるIPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.*」(*は2～254までの数値が入ります)を入力します。
- ・ サブネットマスク
サブネットマスクを入力します。本製品のLAN側IPアドレスを変更していない場合は、「255.255.255.0」を入力します。
- ・ ルーター
本製品のLAN側IPアドレスを入力します。本製品のLAN側IPアドレスを変更していない場合は、「192.168.2.1」を入力します。
- ・ DNSサーバ
プロバイダから提供されたDNSサーバのグローバルIPアドレスを入力します。

TCP/IPの設定は以上です。

10-2. UPnP機能の設定

10-2-1. パソコンの設定

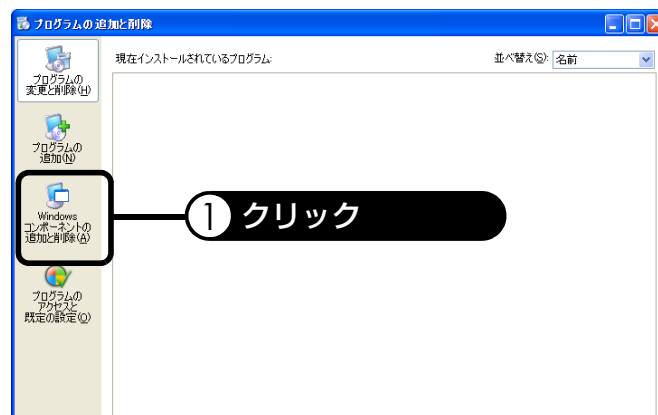
UPnP機能はWindows XPまたはWindows Me/98でのみ設定できます。

Windows XPの場合

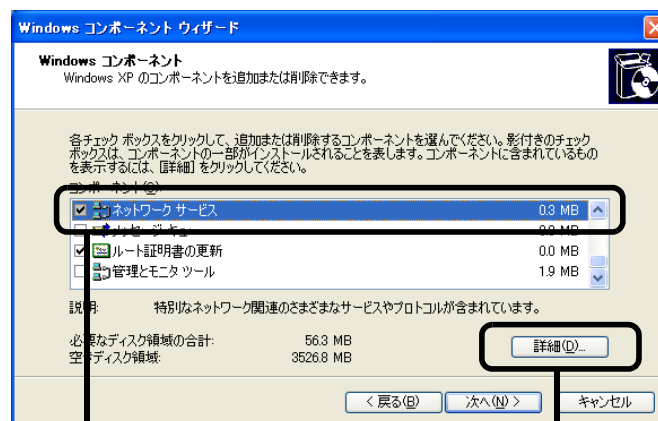
1. [スタート]－[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[プログラムの追加と削除]をダブルクリックします。



2. [Windowsコンポーネントの追加と削除]をクリックします。



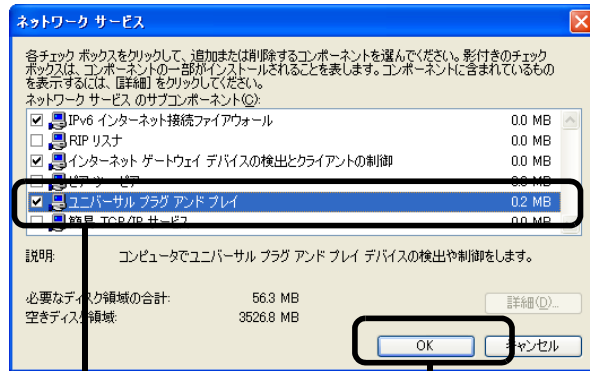
3. [ネットワークサービス]を選択し、[詳細]をクリックします。



① 選択

② クリック

4. [ユニバーサルプラグアンドプレイ]をチェックし、[OK]をクリックします。



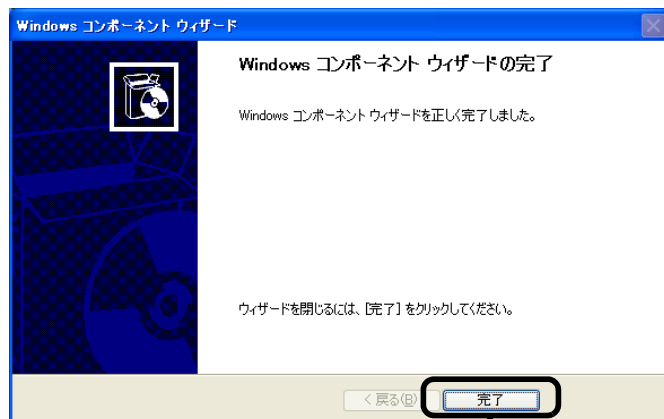
① チェックいれる

② クリック

5. [次へ]をクリックします。

・ [次へ]をクリックすると、インストールを開始します。途中で「"Windows XP CD-ROM"ラベルの付いたCDをCD-ROMドライブに挿入して[OK]をクリックしてください。」と表示された場合は、画面の指示に従ってください。

6. インストールの完了画面が表示されたら、[完了]をクリックします。



① クリック

7. 開いている画面をすべて閉じて、パソコンを再起動します。

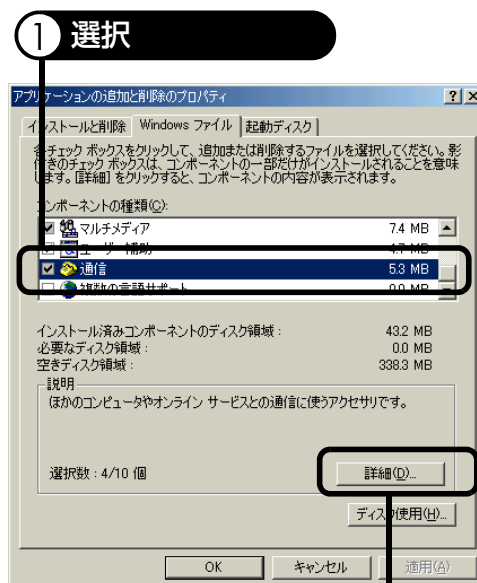
UPnP機能の設定は以上です。
引き続き、『10-2-2.UPnP機能の動作確認』(P.151)へお進みください。

Windows Me/98の場合

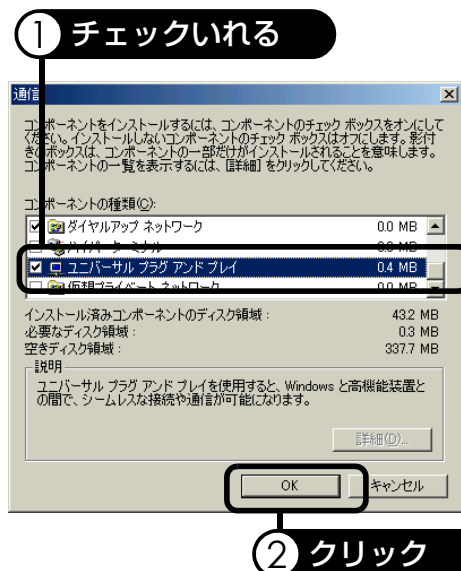
1. [スタート]－[設定]－[コントロールパネル]の順にクリックします。
[コントロールパネル]画面が表示されるので[アプリケーションの追加と削除]をダブルクリックします。



2. [Windowsファイル]タブをクリックし、[コンポーネントの種類] (または [ファイル種類]) で [通信] を選択し、[詳細] をクリックします。



3. [ユニバーサルプラグアンドプレイ]をチェックし、[OK]をクリックします。



4. [OK]をクリックします。
- ・ [次へ] をクリックすると、インストールを開始します。途中で「ファイルSSd papi.dllが見つかりません。続けるには"Windows Millennium Edition"のラベルが付いたディスクが必要です。」と表示された場合は、画面の指示に従ってください。
5. 開いている画面をすべて閉じて、パソコンを再起動します。

UPnP機能の設定は以上です。
引き続き、『10-2-2.UPnP機能の動作確認』(P.151)へお進みください。

10-2-2. UPnP機能の動作確認

* Windows XPの画面を参照してご説明しております。

1. [スタート]－[マイネットワーク]の順にクリックします。
 - ・ Windows 98/Meの場合は、デスクトップの[マイネットワーク] (Windows Meの場合)または[ネットワークコンピュータ] (Windows 98の場合)をダブルクリックしてください。
2. [MR304DV]が追加されていることを確認してください。
 - ・ 表示される名称は、詳細設定画面の[本体設定]→[本体の名称]で設定された名称になります。本体の名称を変更している場合は、[MR304DV]の代わりに設定した名称が表示されます。



3. [MR304DV]をダブルクリックして、ブロードバンドルータ設定画面が表示されたら、本製品およびパソコンのUPnP機能は正常に動作しています。

* MR304Xの場合、[MR304DV]が[MR304X]と表示されます。

11. 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丁目13番地11号
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:055-977-9048

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 MR304X/MR304DV

● 修理依頼時、この依頼票に必要な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	<input type="checkbox"/> 有り…保証書を同梱ください。 <input type="checkbox"/> 無し…保証期間内でも有償となります。		
故障状況	発生頻度	<input type="checkbox"/> 常時発生 <input type="checkbox"/> 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)	<input type="checkbox"/> 代金引換 <input type="checkbox"/> 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ー行

TEL: ☎ 0120-77-4717 FAX番号:055-977-0575

- お客様が当社カスタマサポートセンター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『取扱説明書[簡単設定編]12.困ったときには』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

(MR304X/MR304DV)

※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): _____		
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 <input type="checkbox"/> 未加入 <input type="checkbox"/> 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: _____ <input type="checkbox"/> 未加入/加入予定 <input type="checkbox"/> 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 からのご利用いただけます)


FAX : 055 - 977 - 0575

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 : 〒411-8511 静岡県三島市松本 66

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 : 055 - 977 - 9048

FAX : 055 - 977 - 9092

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 : 055 - 977 - 9068

FAX : 055 - 977 - 9092

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 : 〒411-8511 静岡県三島市松本 66

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/>

* 無断複写・転載を禁止します。 * 乱丁本・落丁本はお取り替えいたします。

VIAGGIO

ヴィアジジョ

ブロードバンドルータ
MR304X/MR304DV
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

