超高速ブロードバンドルータ（VPN 機能付）
BSR14

ユーザーズマニュアル

パーソル株式会社

はじめに

このマニュアルは「クイック接続マニュアル」に掲載されていない本製品(BSR14)**の機能について説明したマニュアルです。ご注意、接続方法、かんたん設定ウィザード、サポートなどの説明については製品に添付されている「クイック接続マニュアル」および「サポートシート」をお読みください。**

ご注意　重要

- 高度な機能をご使用になる場合にご注意
  ここで説明している「バーチャルサーバー」「特殊 AP**」「**VPN**」などは、コンピュータおよびインターネットに関するセキュリティの知識が十分にないと、外部から不正アクセスなどの攻撃を受ける恐れがある機能です。セキュリティに関する知識がない方は、これらの設定を変更しないでください。また、セキュリティに関する知識がある場合でも設定については十分にご注意願います。**

目　次

1. 設定ユーティリティを表示する

WEB **ブラウザを使って本製品の設定ユーティリティに接続する方法を説明します。**

1 本製品と **LAN** で接続されたパソコンを起動します。

2 通常ご使用になっている **WEB** ブラウザを開きます。

3 WEB ブラウザの「アドレス」に「http://192.168.123.254」と入力し、キーボードの[**Enter** キー]を押します。

●「192.168.123.254」**はデフォルト(初期値)でのアドレスです。アドレスを変更した場合は、そのアドレスを入力します。**

4 [システムパスワード]に「admin」と入力し、[ログイン]ボタンをクリックします。

●「admin」**はデフォルト(初期値)でのパスワードです。パスワードを変更した場合は、そのアドレスを入力します。**

MEMO **安全のためにパスワードは定期的に変更することをお勧めします。変更したパスワードは忘れないように注意してください。**

2．システム状態

[システム状態]では、本製品の状態を確認できます。

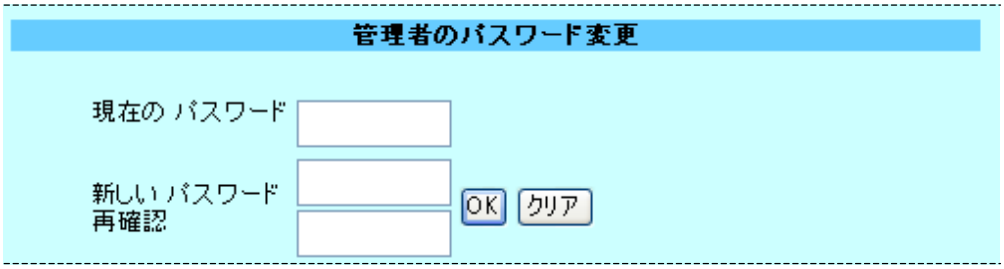
残りのリース時間※	動的 IP アドレスの場合に表示されます。残りのリース時間を表示します。 書換･･･手動で IP アドレスとリース時間を更新します。 開放･･･手動で IP アドレスを開放します。
IP アドレス サブネットマスク ゲートウェイ ドメインネームサーバ	WAN 側の IP アドレスをはじめとする各アドレスを表示します。
接続時間※	PPPoE 接続と Unnumbered PPPoE 接続の場合に表示されます。インターネットにどのくらいの時間接続しているかを示します。 接続･･･手動でインターネット接続を実行します。 切断･･･インターネット接続を手動で切断します。
[更新]ボタン	表示されているシステム状態を最新の状態に更新します。

※の項目は接続方法の種類によって表示されます。

3．管理者設定

3-1 管理者設定の項目

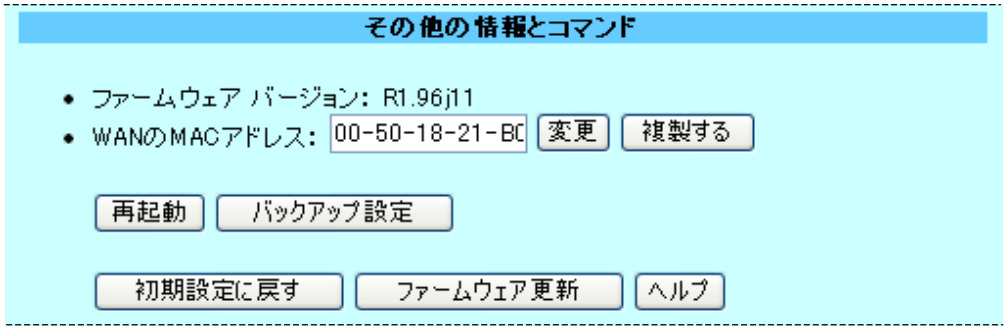
3- 1- 1　管理者のパスワード



本製品の設定を変更するには、パスワードが必要です。パスワードの初期設定は[admin]ですが、第三者に設定を変更されないよう必ずパスワードを変更しておいてください。変更は次の操作で行います。

① [現在のパスワード]に現在のパスワードを入れます(初期設定：admin)。
② [新しいパスワード]に新しいパスワードを入力します。
③ [再確認]に、②で入力したパスワードをもう一度入力します。
④ [OK]ボタンをクリックします。

3- 1- 2　その他の情報とコマンド



ファームウェアバージョン	現在のファームウェアのバージョンが表示されます。
WAN の MAC アドレス	WAN 側の MAC アドレスを表示します。 変更･･･････WAN 側の MAC アドレスを変更します。表示中の MAC アドレスを上書きした後、このボタンをクリックします。 複製する･･･パソコン側の MAC アドレスを WAN 側の MAC アドレスとしてコピーすることができます。

■ボタンの機能

再起動	設定ユーティリティの内容を変更した場合に、このボタンをクリックします。本製品が再起動して新しい設定が有効になります。
バックアップ設定	本製品の設定状態をファイルに保存します。次の「設定をバックアップする」を参照してください。
初期設定に戻す	本製品の設定状態を工場出荷時の設定(デフォルト値)に戻します。
ファームウェア更新	本製品のファームウェアを更新します。次の「ファームウェアを更新する」を参照してください。

3-2 設定をバックアップする

① [バックアップ設定]ボタンをクリックします。
② (ファイルのダウンロード)画面が表示されます。[保存]ボタンをクリックします。
③ (名前を付けて保存)画面が表示されます。保存する場所とファイル名を指定し、[保存]をクリックします。このとき拡張子は[bin]にしてください。
④ (ダウンロードの完了)画面が表示されます。[閉じる]ボタンをクリックします。
⑤ これで設定した内容がファイルに保存されました。

MEMO 保存したファイルは、ファームウェアの更新と同じ方法で読み込むことができます。次のファームウェアを更新する」を参照してください。

3-3 ファームウェアを更新する

ファームウェアを更新するには、当社のホームページ「http://www.persol-jp.com」からファームウェア用のファイルをダウンロードしてください。ファームウェアを更新すると最新の機能で本製品をお使いただけます。

注意
- ファームウェアの更新中は、他の操作をしないでください。また、完全に作業を終わるまで本製品の電源を切らないでください。更新中に他の動作が割り込んだりするとファームウェアの更新に失敗する恐れがあります。また、完全に作業が終わる前に電源を切ると、故障の原因になりますのでご注意ください。
- ファームウェアの更新には多少時間がかかる場合があります。

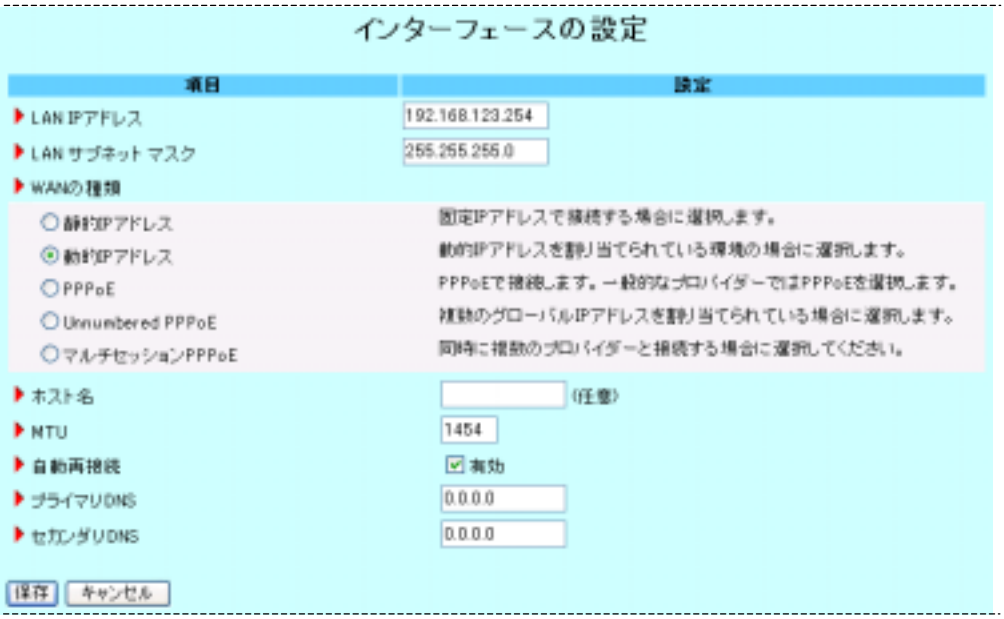
① (管理者設定)画面にある[ファームウェア更新]ボタンをクリックします。
② (ファームウェア更新)画面が表示されます。[参照]ボタンをクリックします。
[参照]ボタンを使わずにファイルのある場所を入力することもできます。
③ [参照]ボタンをクリックした場合は、(ファイルの選択)画面が表示されます。更新ファイルのある場所とファイル名を選び、[開く]ボタンをクリックします。
④ (ファームウェア更新)画面の[更新]ボタンをクリックします。
⑤ 更新が終わると「正常に更新されました」と表示されます。しばらくすると(システム状態)画面が表示されます。
⑥ これでファームウェアが更新されました。

MEMO ファームウェアのアップグレードを終了した後、まれに数分経過しても(システム状態)画面が表示されないことがあります。この場合、次の操作をしてください。
1. 本製品の前面にある M1 ランプが速く点滅していないか確認します。
2. 本製品の電源を切ります。
3. 1 分後、もう一度電源を入れます。
4. ブラウザから本製品に接続します。

4．基本設定

インターネットに接続するための基本的な事項を設定します。画面は接続方法(WAN の種類)によって異なります。「簡単設定ウィザード」でも同じ設定ができますが、基本設定では接続方法ごとにひとつの画面ですべてを設定できるようになっています。

4-1 基本設定



■ 接続方法(**WAN** の種類)を変更するには

[基本設定]の[インターフェースの設定]からご利用になる接続方法ボタンをクリックします。

■ **本製品では** LAN **サブネットマスクの変更ができます。変更可能な範囲は** 255.255.255.0 **から** 255.255.255.248 **です。またサブネットマスクを変更する場合は** LANIP **アドレスの有効な範囲は** 192.168.×.×**となります。これらの変更をする場合は** DHCP **も設定に合わせて変更してください。通常はトラブルを避けるために変更しないでください。**

■ **[静的** IP **アドレス]を選択した場合は[**NAT **を無効にする]機能を利用できます。通常はトラブルを避けるために使用しないでください。**

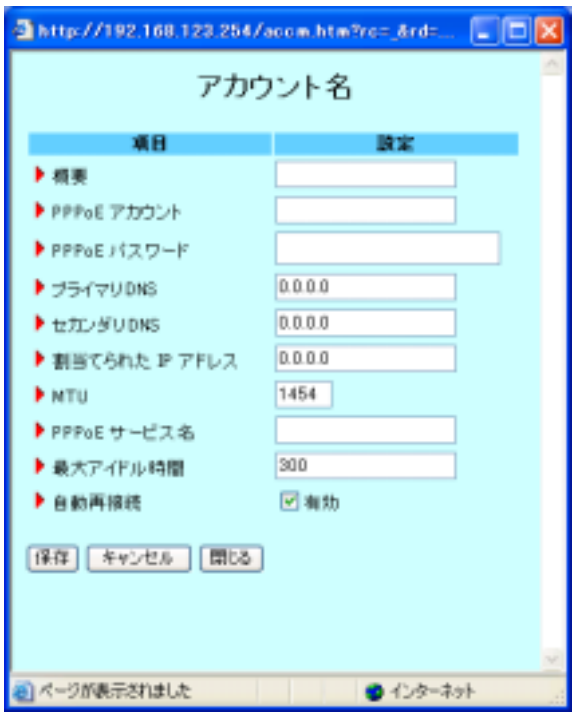
■ 各設定項目の内容については・・・
本製品に添付された「クイック接続マニュアル」の簡単設定ウィザードの各項目の説明をお読みください。

4-2 マルチセッション PPPoE で複数の接続先に同時に接続する

「マルチセッション PPPoE 接続」の場合は同時に 5 か所まで接続することができます。複数の接続事業者と契約している場合やフレッツスクエアなどに同時に接続する場合に便利です。

①本製品の設定ユーティリティの[基本設定]の[インターフェースの設定]からマルチセッション PPPoE を選択します。

②登録したいセッション番号のエディットをクリックし接続先のアカウント、パスワード、DNS などの情報をそれぞれ登録します。



③通常使用するセッションをマスターに設定しルーティングにより振り分けるセッションをスレーブに設定します。

MEMO

●マルチセッション PPPoE **を利用して複数の接続先と通信するには必ずのルーティングを登録する必要があります。ルーティングの設定はマルチセッション** PPPoE IP **もしくはマルチセッション** PPPoE **ドメインにて行ってください。**

●各セッションを確立するのに時間がかかる場合があります。

●マルチセッション PPPoE **と** VPN **を同時に使用することはできません。**

4-3 マルチセッション PPPoE のルーティング設定をする

マルチセッションを正常に使用するためには必ずルーティングの設定をする必要があります。ここでは例として NTT 東日本のフレッツスクエアを設定します。

5-3-1　IP アドレスによるルーティング

①[基本設定]のマルチセッション PPPoE IP **を選択します。ここでは宛先のネットワークを** IP **アドレスで指定することができます。**IP **アドレスを登録しルーティングするセッション番指定してください。**

②設定を有効にする場合は[有効]にチェックを入れ[保存]ボタンをクリックしてください。

5-3-2　ドメインによるルーティング

①[基本設定]のマルチセッション PPPoE **ドメインを選択します。ここでは宛先のネットワークをドメインで指定することができます。ドメインを登録しルーティングするセッション番号を指定してください。**

②設定を有効にする場合は[有効]にチェックを入れ[保存]ボタンをクリックしてください。

5. DHCP サーバー設定

本製品の DHCP サーバーを使うと、ネットワークに接続されているパソコンなどに IP アドレスを自動的に割り当てることができます。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。また、項目の先頭にある▸マークが青色の項目を変更した場合は、保存後に[再起動]ボタンをクリックして再起動してください。

※ [その他の設定>>]はボタンをクリックしたときに表示される項目です。

DHCP サーバー	DHCP サーバー機能を有効または無効にします。IP アドレスを手動で割り当てる場合など、別の方法で IP アドレスを指定しない限り、[有効]に設定します。 [有効]にした場合は、[IP プール開始アドレス][IP プール終了アドレス]を設定します。
リリース タイム	DHCP 配信による IP アドレスの貸し出し時間を設定します。
IP プール開始アドレス/ IP プール終了アドレス	[DHCP サーバー]を有効にした場合に、各パソコンやネットワーク周辺機器に割り付ける IP アドレスの範囲を指定します。
ドメイン名	特に設定は不要です。プロバイダからの情報で[ドメイン名]を入力する必要がある場合だけ設定します。
プライマリ DNS サーバー※ セカンダリ DNS サーバー※	これらの項目に入力する必要がある場合だけ設定します。
プライマリ WINS サーバー※ セカンダリ WINS サーバー※	これらの項目に入力する必要がある場合だけ設定します。
ゲートウェイ※	[ゲートウェイ]を入力する必要がある場合だけ設定します。

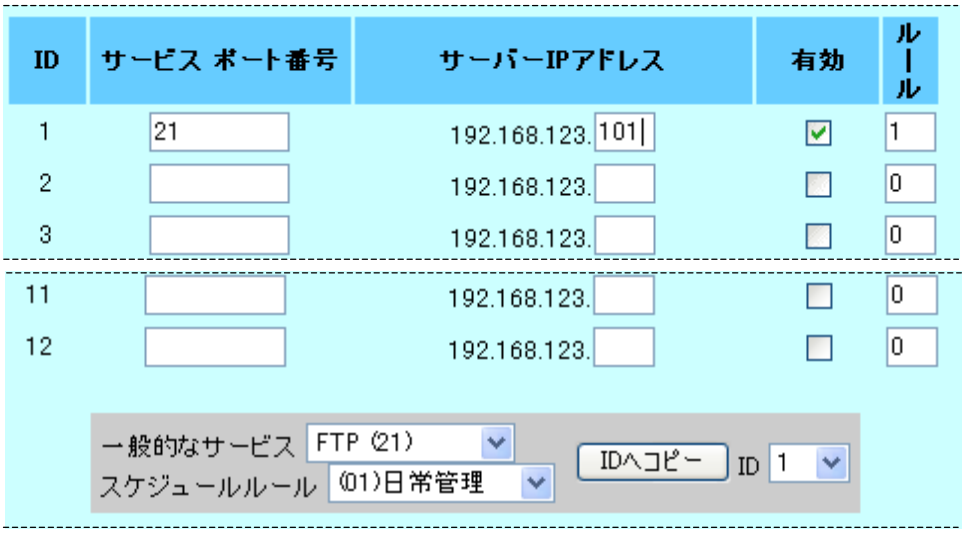
■ボタンの機能

その他の設定	オプション項目を表示します。
クライアントリスト	[DHCP クライアントリスト]画面が表示されます。この画面には DHCP サーバー機能で管理している各パソコンやネットワーク周辺機器の IP アドレス、ホスト名、MAC アドレスが表示されます。
MAC アドレス制御	ネットワーク上で IP アドレスを固定したいパソコンがある場合に使います。このボタンをクリックすると[MAC アドレス制御]画面が表示されます。 P24「13. MAC アドレス制御」を参照してください。

6．仮想サーバー

本製品は NAT/IP マスカレード機能を装備しています。そのため、インターネット側から本製品に接続された LAN 側のパソコンには接続できません。これに対して、仮想サーバー機能はあらかじめ設定された条件で LAN 側のパソコンをインターネットに開放する機能です。
この機能を使うと、LAN 側の特定のパソコンを FTP サーバーとして開放した場合、FTP サーバーとして開放されたパソコンの 21 番ポートだけにインターネット側から接続することができます。他のパソコンにはインターネット側からの接続は一切許可されません。また、FTP サーバーとして使用しているパソコンも 21 番ポート以外には、インターネット側から接続することはできません。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。再起動するように表示されますので、[再起動]ボタンをクリックして再起動してください。



サービスポート番号	インターネットサービスのポート番号を入力します。テンプレートの一覧から選んでコピーすることもできます。
サーバーIP アドレス	仮想サーバーとして使うパソコンの IP アドレスを入力します。
有効	設定したサービスを有効または無効にします。
ルール	スケジュール設定で設定したルールを指定すると、そのルールに従って運用することができます。

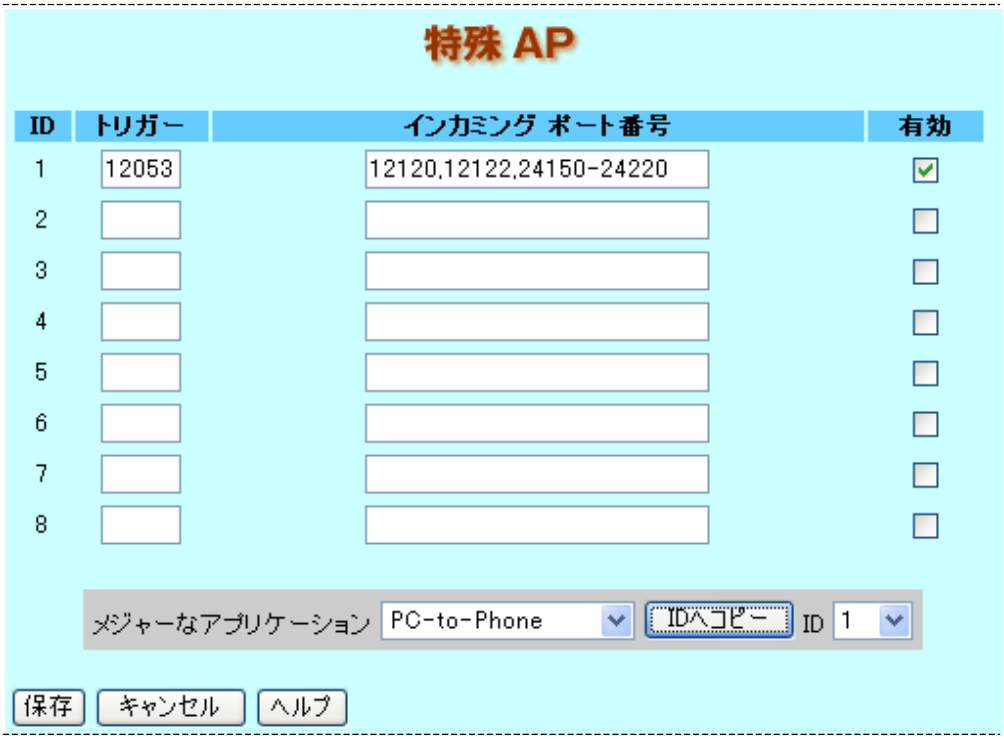
■テンプレートの使い方
テンプレートに登録されたサービスを利用する場合は簡単にサービスを登録できます。同じようにあらかじめ設定したスケジュールルールを登録できます。
テンプレートのサービスを登録するとデフォルトで[有効]がオンになります。

① [一般的なサービス]でサービスの種類を選びます。
② [ID]で、サービスを割り当てるクライアントの ID を選びます。
③ [ID へコピー]ボタンをクリックします。
④ 指定した ID にサービスポート番号がコピーされます。
※[スケジュールルール]の場合は登録したスケジュールルール名を選び、②以降の操作をします。

7．特殊 AP

インターネットゲーム、ビデオ会議などのインターネット対応のプリケーションを利用するには、指定されたポートをインターネット側に開放する必要があります。特殊 AP(アプリケーション)機能を利用すると、あらかじめ設定されたアプリケーションにだけ指定されたポートを開放します。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。再起動するように表示されますので、[再起動]ボタンをクリックして再起動してください。



トリガー	使用するアプリケーションが発行するアウトバウンドポート番号を入力します。テンプレートの一覧から選んでコピーすることもできます。
インカミングポート番号	トリガーパケットが検出されたときに開放するポート番号を入力します。ハイフン「-」を使うと連続したポート番号を範囲指定できます。 例：2000-2038
有効	サービスを有効または無効にします。

■テンプレートの使い方

テンプレートに登録されたメジャーなアプリケーションを利用する場合は簡単にサービスを登録できます。テンプレートではデフォルトで[有効]になります。

① [メジャーなアプリケーション]からでアプリケーションの種類を選びます。
② [ID]でリストのどの ID に登録したいかを選びます。
③ [ID へコピー]ボタンをクリックします。
④ 指定した ID にインカミングポート番号がコピーされます。

8．その他の項目

[その他の項目]では、DMZ ホスト、リモート管理、タイムアウトなどの設定ができます。

設定を変更した場合は[保存]ボタンをクリックします。また、項目の先頭にある ▶ マークが青色の項目を変更した場合は、保存後に[再起動]ボタンをクリックして再起動してください。

UPnP 設定	UPnP 機能を使用する場合は[有効]を選びます。デフォルト値は UPnP 機能を使用するように設定されています。
DMZ ホスト IP アドレス	インターネットゲーム、ビデオ会議、インターネット電話など双方向通信を利用するパソコンを DMZ ホストに設定します。DMZ ホストにするパソコンの IP アドレスを入力し、[有効]を選びます。
リモート管理者ホスト	遠隔地からインターネットを介して設定ユーティリティを使う場合に設定します。遠隔地(リモート側)のパソコンの IP アドレスを入力し、[有効]を選びます。この項目を[有効]にした場合、設定ユーティリティにアクセスするポート番号は 88 になります。通常のポート番号とは異なりますのでご注意ください。
管理者タイムアウト	設定ユーティリティの使用中に、設定時間を過ぎると自動的にログアウトする時間を設定します。「0」を入力するとタイムアウトしません。
WAN 側から PING を受け付けない	[有効]を選ぶと、WAN 側からの PING を受け付けなくなります。

注意

DMZ ホストは指定したパソコンを全面的にインターネットに開放するため、不正なアタックを受けやすくなりますので、必要な場合だけ設定してください。

MEMO

●リモート管理者ホストについて

[リモート管理者ホスト]を有効にすると、WEB サーバーポート番号は 88 になります。通常のポート番号と異なりますのでご注意ください。

9．フィルタリング

左フレームの「セキュリティ設定」にある「フィルタリング」をクリックすると、インターネット側から LAN 側のパソコンへのアクセスの制限(IN 制御)および LAN 側のパソコンからインターネット側へのアクセスの制限(OUT 制御)の設定ができます。設定は IN 制御、OUT 制御それぞれ 8 通りまでです。

9-1 パケットフィルタリング OUT 制御

LAN 側のパソコンからインターネット側へのアクセスを制限することができます。設定できる数は 8 個までです。

MEMO
- ●設定を変更した場合は[保存]ボタンをクリックします。
- ●[パケットフィルタリング IN 制御]ボタンをクリックすると、(パケットフィルタリング IN 制御)画面に切り替わります。

注意
[パケットフィルタリング OUT 制御]の[有効]をオンにしただけではフィルタリングは実行されません。必ず、各 ID についてフィルタリングの内容を設定してください。

パケットフィルタリング OUT 制御	「有効」をチェックするとパケットフィルタリング OUT 制御の機能全体が有効になります。ただし、各 ID の「有効」をチェックしていない場合は、その ID の設定内容は反映されません。
全てのパケットを通過させます。・・・	この項目を選ぶと、LAN 側からのすべてのパケットがルータを通過してインターネット側へ出ることができます。この設定だけであれば、フィルタリング機能を設定していないのと同じです。ただし、一覧に登録されたパケットだけは通過することができません。 ※各 ID の「有効」をチェックしておく必要があります。

(続きは次ページへ)

全てのパケットを拒否します。‥‥	この項目を選ぶと、LAN 側からのすべてのパケットがルータを通過してインターネット側へ出ることができなくなります。ただし、一覧に登録されたパケットだけは通過することができます。 ※各 ID の「有効」をチェックしておく必要があります。
ID	登録番号です。
送信元 IP:ポート番号	LAN 側のプライベート IP アドレスと、「：」のあとにポート番号を入力します。
受信先 IP:ポート番号	インターネット側のグローバル IP アドレスと、「：」のあとにポート番号を入力します。
有効	登録した内容は ID ごとに有効/無効を設定できます。チェックしている場合に、その ID の登録内容は有効になります。
ルール	スケジュール設定で設定したルールを指定すると、そのルールに従って運用することができます。

■ボタンの機能

保存	設定した内容を保存します。
パケットフィルタリング IN 制御	OUT 制御の画面表示時は IN 制御の画面を表示するボタンが表示されます。
MAC レベル	MAC アドレス制御画面(→P24)が表示されます。

9- 1- 1　IP アドレス/ポート番号の入力ルール

IP アドレスとポート番号では範囲指定などができます。

■IP アドレスの設定

ひとつの IP アドレスを入力する以外に、範囲を指定することで連続した IP アドレスを指定することができます。また、IP アドレスの入力欄を空白にし、ポート番号だけを入力すると、すべての IP アドレスに対してそのポート番号を指定したことになります。

例：ひとつだけ指定→192.168.123.100
　　連続した範囲の指定→192.168.123.105-192.168.123.110
　　※カンマ区切りによる複数の入力には対応していません。

■ポート番号の設定

ひとつのポート番号を入力する以外に、範囲を指定することで連続したポート番号を指定することができます。また、ポート番号の前に「T」と入力することで TCP だけを、「U」と入力することで UDP だけが指定されます。ポート番号だけを入力した場合は、TCP と UDP の両方が指定されます。

例：80→TCP と UDP のポート番号 80 が有効
　　T20-23→TCP のポート番号 20～23 が有効
　　U100→UDP のポート番号 100 が有効
　　※カンマ区切りによる複数の入力には対応していません。

9-2 パケットフィルタリング IN 制御

インターネット側から LAN 側のパソコンへのアクセスを制限することができます。設定できる数は 8 個までです。

MEMO
●設定を変更した場合は[保存]ボタンをクリックします。
●[パケットフィルタリング OUT 制御]ボタンをクリックすると、(パケットフィルタリング OUT 制御)画面に切り替わります。

注意
[パケットフィルタリング IN 制御]の[有効]をオンにしただけではフィルタリングは実行されません。必ず各 ID についてフィルタリングの内容を設定してください。

パケットフィルタリング IN 制御	「有効」をチェックするとパケットフィルタリング IN 制御の機能全体が有効になります。ただし、各 ID の「有効」をチェックしていない場合は、その ID の設定内容は反映されません。
全てのパケットを通過させます。・・・	この項目を選ぶと、インターネット側からのすべてのパケットがルータを通過して LAN 側に入ることができます。この設定だけであれば、フィルタリング機能を設定していないのと同じです。ただし、一覧に登録されたパケットだけは通過することができません。 ※各 ID の「有効」をチェックしておく必要があります。
全てのパケットを拒否します。・・・	この項目を選ぶと、インターネット側からのすべてのパケットがルータを通過して LAN 側を入ることができなくなります。ただし、一覧に登録されたパケットだけは通過することができます。 ※各 ID の「有効」をチェックしておく必要があります。
ID	ID 登録番号です。

(続きは次ページへ)

送信先 IP:**ポート番号**	**インターネット側のグローバル** IP **アドレスと、「：」のあとにポート番号を入力します。**
受信先 IP:**ポート番号**	LAN **側のプライベート** IP **アドレスと、「：」のあとにポート番号を入力します。**
有効	**登録した内容は** ID **ごとに有効/無効を設定できます。チェックしている場合に、その** ID **の登録内容は有効になります。**
ルール	**スケジュール設定で設定したルールを指定すると、そのルールに従って運用することができます。**

■ボタンの機能

保存	**設定した内容を保存します。**
パケットフィルタリング OUT **制御**	IN **制御の画面表示時は** OUT **制御の画面を表示するボタンが表示されます。**
MAC **レベル**	MAC **アドレス制御画面**(→P24)**が表示されます。**

IP **アドレスとポート番号の指定方法については範囲指定などができます。**P19「10-1-1 IP **アドレス/ポート番号の入力ルール」を参考にしてください。**

10. ドメインフィルター

左フレームの「セキュリティ設定」にある「ドメインフィルター」をクリックすると、登録したドメインへのアクセスを禁止したり、登録したドメインにアクセスした場合にそのログを残すことができます。最大 9 個のドメイン名とその他のドメインについて設定できます。

MEMO

設定を変更した場合は[保存]ボタンをクリックします。
ドメインフィルターが動作しない場合はコマンドプロンプトから"ipconfig /flushdns"を行ってください。

ドメインフィルター	「有効」をチェックするとドメインフィルター機能が有効になります。※
DNS ログ要求	「有効」をチェックするとログを保存する機能が有効になります。※
ドメインフィルター除外ホスト	ここに指定した範囲にある IP アドレスを持つクライアントについては、この機能が有効の場合でもここでの制限から除外されます。クライアントのローカル IP アドレスの最下位ブロックの数値を入力します。
ID	ID 登録番号です。
ドメイン名	アクセスを制限したドメイン名を入力します。 (例)「.com(com ドメインすべてが対象)」「xxx.com(指定したドメイン名が対象)」
動作	フィルターの内容を指定します。「Drop」を有効にするとアクセスを禁止します。「log」を有効にするとアクセスログを保存します。
有効	登録した内容は ID ごとに有効/無効を設定できます。チェックしている場合に、その ID の登録内容は有効になります。

※各 ID にある「有効」をチェックしていない場合は、その ID の設定内容は反映されません。

11. URL ブロック

左フレームの「セキュリティ設定」にある「URL ブロック」をクリックすると、登録した URL へのアクセスを禁止することができます。最大 5 個の URL を設定できます。特定の URL を登録できるほかキーワードを入力することで、そのキーワードを含む URL へのアクセスを禁止することができます。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。再起動するように表示されますので、[再起動]ボタンをクリックして再起動してください。

URL ブロック	「有効」をチェックすると URL フィルター機能が有効になります。ただし、各 ID にある「有効」をチェックしていない場合は、その ID の設定内容は反映されません。
ID	ID 登録番号です。
URL	特定の URL またはキーワードを指定します。キーワードを指定した場合、そのキーワードが含まれる URL へのアクセスが制限されます。 (例)「chat」とキーワードを指定すると、「chat」という文字が入ったすべての URL へのアクセスが制限されます。
有効	登録した内容は ID ごとに有効/無効を設定できます。チェックしている場合に、その ID の登録内容は有効になります。

12. MAC アドレス制御

左フレームの「セキュリティ設定」にある「MAC アドレス制御」をクリックすると、各パソコンが持つ MAC アドレスと IP アドレスが固定されるように設定できます。さらに、その設定により登録されたパソコンから本製品へ接続を許可するのか拒否するのかを選ぶことができます。また、登録していないすべてのパソコンから本製品へ接続を許可するか、拒否するのかを選ぶことができます。

MEMO

- (MAC アドレス制御)画面を表示するには、左フレームから[DHCP サーバー]を選び、[MAC アドレス制御]ボタンをクリックした場合も同様です。
- 設定を変更した場合は[保存]ボタンをクリックします。また、項目の先頭にある ▶ マークが青色の項目を変更した場合は、保存後に[再起動]ボタンをクリックして再起動してください。
- VPN を使用する場合ルータが PC の MAC アドレスを認識（クライアントリストに表示されます。）している必要があります。DHCP を無効にしている場合は手動で MAC アドレスを入力してください。

MAC アドレス制御	MAC アドレス制御の有効/無効を設定します。この機能を有効にするには、さらに[接続制御]を有効にする必要があります。
接続制御	コントロールテーブルで設定した内容に従って本製品への接続を制御する場合に有効にます。実際にこの機能を有効にするには、[MAC アドレス制御]も有効にする必要があります。 また、一覧に登録しなかったパソコンについて、本製品への接続の許可/拒否を設定します。
MAC アドレス	各パソコンの MAC アドレスを入力します。2 桁ずつ「-」で区切って入力します。 例：00-XX-03-CX-00-E3
IP アドレス	[MAC アドレス]で MAC アドレスを登録したパソコンの IP アドレスを入力します。
有効	登録したパソコンから本製品への接続を許可する場合はチェックします。許可しない場合はチェックしません。

■ボタンの機能

前のページに戻る	前ページの設定画面に移動します。
次のページに進む	次ページの設定画面に移動します。

■テンプレートの使い方

テンプレートには本製品に接続されているパソコンの MAC **アドレスがリストで表示され、指定の** ID **に登録することができます。**

① [**クライアント**]**で登録したいパソコンの** MAC **アドレスを選びます。**

② [ID]**でリストのどの** ID **に登録したいかを選びます。**

③ [ID **へコピー**]**ボタンをクリックします。**

④ 指定した ID **に** MAC **アドレスが登録されます。**

パソコンの IP アドレスがわからない場合

別紙「インターネットに接続できなかったとき」の「確認 5 **ローカル** IP **アドレスが正常に取得できているかを確認します。」をお読みください。**

13. 時刻設定

左フレームの「高度な設定」にある「時刻設定」をクリックすると、NTP(Network Time Protocol)を使って時刻を合わせます。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。

NTP サーバーに接続	NTP を使って時刻を設定する場合はこちらを選択します。
タイムサーバー	NTP を使う場合、どのタイプサーバーを利用するかを一覧の中か選択します。
タイムゾーン	使用する時刻の標準時となる地域を選択します。日本の場合は「Seoul, Tokyo, Yakutsk」を選択します。
クライアント PC の時刻を使用する	クライアントのパソコンの時計を使って時刻を設定する場合はこちらを選択します。パソコンの時計自体は OS のコントロールパネルで設定します。
マニュアル設定	手動で時刻を設定します。[日時]で年月日を[時間]で時刻を設定します。

■ボタンの機能

今すぐ NTP 接続する	設定したタイプサーバーに接続し、時刻を設定します。
保存	設定した内容を保存します。

14. システムログ

左フレームの「高度な設定」にある「システムログ」をクリックすると、本製品のシステムログを参照することができます。またログは指定したシスログサーバーに保存することができます。また、E-mail で送ることもできます。

MEMO
設定を変更した場合は[保存]ボタンをクリックします。
[システムログの IP アドレス]を使用する場合はシスログサーバーを構築する必要があります。

システムログの IP アドレス	システムログを保存するサーバーのプライベート IP アドレスを設定します。さらに[有効]をクリックすることで、この機能が有効になります。
SMTP IP/ポート番号	SMTP サーバーの IP アドレスとポート番号を設定します。ポート番号は IP アドレスの後ろに「:」で区切って入力します。デフォルトは 25 番です。 (例) 192.168.123.100:25
E-mail に警告を送る	システムログを送信する E-mail アドレスを入力します。
E-mail の件名	送信する時の E-mail の件名を入力します。

■ボタンの機能

ログを見る	保存されたシステムログを見る場合にクリックします。
保存	設定した内容を保存します。

15. ダイナミック DNS

左フレームの「高度な設定」にある「ダイナミック DNS」をクリックすると、固定のグローバル IP アドレスがなくてもホスト名を使ってサーバーを公開できるダイナミック DNS 機能を利用できます。ただし、この機能を利用するには、リストに表示されるプロバイダに登録する必要があります。この機能を利用すると LAN 上のパソコンがサーバーとしてインターネットに公開されますのでセキュリティにはご注意ください。

MEMO

●設定を変更した場合は[保存]ボタンをクリックします。再起動するように表示されますので、[再起動]ボタンをクリックして再起動してください。
●VPN-DDNS を使用する場合も同様にダイナミック DNS の設定を行ってください。

ダイナミック DNS	ダイナミック DNS を使用する場合は[有効]を選びます。
プロバイダ	リストの中からダイナミック DNS に対応したプロバイダを選択します。本製品で利用できるプロバイダはリストにあるプロバイダだけです。
ホストネーム名	プロバイダから指定されたホスト名を入力します。プロバイダによっては E-mail を入力する場合があります。 (例)persol.dynadns.org
ユーザネーム名	プロバイダにログインするためのユーザ名またはキーを入力します。
パスワード	プロバイダの認証に使用するパスワードを入力します。

16. SNMP

左フレームの「高度な設定」にある「SNMP」をクリックすると、ネットワークを集中管理するためのプロトコル「SNMP(Simple Network Management Protocol)」を設定できます。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。

SNMP	「ローカル」をチェックすると LAN 側からの要求に対応します。[リモート]をチェックすると WAN 側からの要求に対応します。
コミュニティ名 (読み込みのみ)	読み込みだけに使用するコミュニティ名を入力します。本製品からの SMMP の値を引き出すために必要です。
コミュニティ名 (書き込み)	書き込みおよび読み込みに使用するコミュニティ名を入力します。本製品への SNMP の値をセットするために必要です。
IP	IP アドレスを指定します。
SNMP バージョン	本製品では V1 と V2c をサポートしています。どちらかを選択してください。

17. ルーティング

左フレームの「高度な設定」にある「ルーティング」をクリックすると、ルーティング機能を設定することができます。ルーティングは RIPv1/v2 またはスタティックルーティングを使うことができます。スタティックルーティングでは 8 個まで登録できます。

RIP	本製品は RIPv1/v2 に対応しています。
スタティック ルーティング	ルーティングテーブルに手動で入力します。LAN 側から WAN 側へのルーティングのみをサポートしています。ルーティングテーブルに WAN 側から LAN 側へのルーティングを入力しても動作しません。スタティックルーティングを設定するときは、「RIP」を無効にしてください。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。保存後に[再起動]ボタンをクリックして再起動してください。

RIP	[有効]をチェックすると RIP 機能が有効になります。本製品は RIPv1/v2 をサポートしています。使用方法に合わせて選択してください。スタティックルーティングを使う場合は必ず無効にしてください。
宛先 IP※	パケットの宛先となるサブネットアドレスを入力します。
サブネットマスク※	[宛先 IP]で入力したサブネットアドレスのサブネットマスクを入力します。
ゲートウェイ※	サブネットワークを入力した次のゲートウェイアドレスを入力します。
Hop※	Hop 数を入力します。
項目※	設定したルーティングを有効にする場合にチェックします。

※スタティックルーティングの場合に手動で入力します。

18. スケジュール設定

左フレームの「高度な設定」にある「スケジュール」をクリックすると、仮想サーバー、パケットフィルタリング OUT 制御、パケットフィルタリング IN 制御について、設定した内容が有効になる曜日と時間をスケジュールとして設定し、ルールとして保存することができます。１週間の有効になる曜日と時間を設定することで一定時間の間だけ､仮想サーバーなどの機能を有効にすることができます。複数のルールを登録できますので年間の運用に合わせた管理も可能です。

MEMO 設定を変更した場合は[保存]ボタンをクリックします。

スケジュール	登録したルールを有効にしたい場合はここをチェックします。
ルール	登録したルールの ID が表示されます。
ルール名	スケジュールを作成したときに入力した名称が表示されます。
動作	すでに登録済みのルールを編集または削除します。

■ボタンの機能

編集	登録済みのルールのスケジュールを変更します。
削除	登録済みのルールを削除します。
保存	設定した内容を保存します。
新規登録	新しいルールのスケジュールを登録します。

18-1 新しいルールを登録する

新しいルールを登録するために、そのルールのスケジュールを作成します。[スケジュール x]の設定欄にルールの名称を入力し、各曜日の開始時間と終了時間を 00:00～24:00 の間で設定します。開始時間より終了時間が早くなるような設定をするとエラーになります。

スケジュール	設定したスケジュールのルール名を入力します。
日曜日～土曜日	各曜日ことの開始時間と終了時間を設定することになります。開始時間と終了時間を 00:00～24:00 の間で設定します。終了時間が開始時間より早くならないように設定します。
毎日	日曜日～月曜日まで同じ時間に開始、終了を設定する場合はこちらに設定すると便利です。
動作	すでに登録済みのルールを編集または削除します。

19.VPN

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プライベートネットワーク同士を通信させるものです。

BSR14 では、VPN 接続として IPSec サーバ･クライアント機能（メインモード･アグレッシブモード）、VPN-DDNS(*1)を搭載し、最大 40 トンネルの同時アクセスが可能です。また、BSR14 では IPSec パススルーモードをサポートしています。

VPN クライアント･サーバー設定を行う場合は必ず[VPN-IPsec]を[有効-組み込み]にチェックを入れトンネル数を定義してください。メインモードを使用する場合基本的にイニシエータ、レスポンダーの両方で固定グローバル IP アドレスが必要になります。アグレッシブモードは固定グローバル IP アドレス×動的グローバル IP アドレスでの接続を可能にするモードです。固定グローバル IP アドレスは、レスポンダーモードを選択し、動的グローバル IP アドレスにはイニシエータモードを選択してください。VPN-DDNS は動的グローバル IP 同士をサポートします。

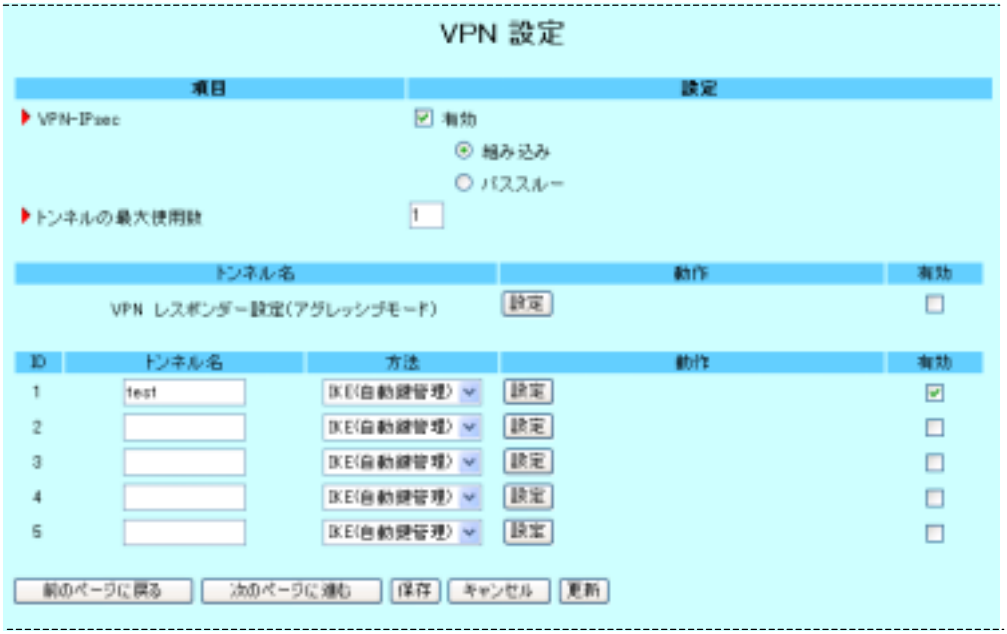
また本製品では、IKE メインモード･アグレッシブモードにてハブ&スポーク VPN（スター型）を構築することが可能です。この場合のルーティングの設定は全て VPN 設定にて行います。

*1：VPN-DDNS は 1 対 1 のみに対応します。

19-1 VPN の設定

19-1-1 IKE モードの設定

① VPN-IPsec 有効にチェックを入れ組み込みを選択しトンネル数を定義してください。
② 鍵交換方法を IKE を選択し設定をクリックしてください。



③ トンネル名を入力してください。トンネル名には自由な名前をつけることが出来ます。
④ ローカルサブネット、ローカルネットマスクを入力してください。（LAN ネットワーク）
⑤ リモートサブネット、リモートネットマスクを入力してください。（リモート LAN ネットワーク）
⑥ リモートゲートウェイを入力してください。VPN 接続する機器のリモート側のグローバル IP アドレスを入力してください。
⑦ 接続時間を入力してください。接続時間は 3600～28800 秒で設定してください。
⑧ カプセル化プロトコルを選択してください。カプセル化プロトコルには ESP、AH、ESP＋AH があります。EPS は AH に比べてセキュリティが高い設定です。
⑨ PFS を使用する場合は有効にチェックを入れてください。PFS を有効にするとよりセキュリティが高

い設定になります。

⑩ アグレッシブモード（イニシエータ）を使用する場合は有効にチェックを入れてください。（*1）

⑪ プレシェアードキーを入力してください。プレシェアードキー（事前共有鍵）はリモート、ローカル共に同じ必要があります。

⑫ アグレッシブモードを使用する場合は使用方法に合わせてリモート ID、ローカル ID を入力してください。

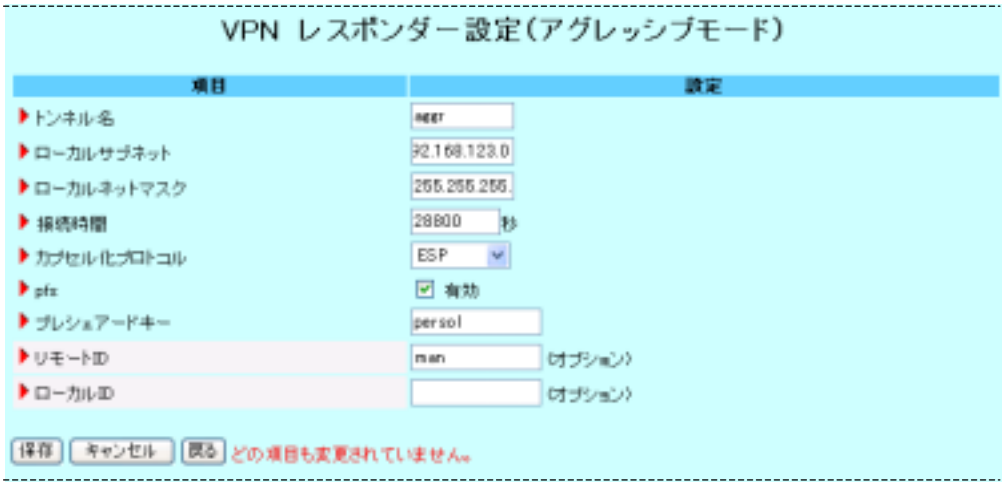
⑬ 設定を完了したら[保存]をクリックしてください。設定したトンネルが有効にチェックが入っていることを確認し設定は完了です。

MEMO

アグレッシブモード（イニシエータ）は動的グローバル IP アドレス環境などに使用します。使用するにはリモート側がアグレッシブモードレスポンダーの設定をする必要があります。
本製品のではハブ&スポーク（スター型 VPN）に対応しております。構築するには TCP/IP や VPN、セキュリティの知識が必要になります。これらの知識がない場合は思わぬトラブルが発生する可能性がありますので十分注意してください。またこれらの知識についてはサポートいたしませんのでご了承ください。

19-1-2　VPN レスポンダー設定（アグレッシブモード）

① VPN-IPsec 有効にチェックを入れ組み込みを選択しトンネル数を定義してください。
② VPN レスポンダー設定（アグレッシブモード）の設定をクリックしてください。
③ トンネル名を入力してください。トンネル名には自由な名前をつけることが出来ます。
④ ローカルサブネット,ローカルネットマスクを入力してください。（LAN ネットワーク）
⑤ 接続時間を入力してください。最大接続時間は 28800 秒です。
⑥ カプセル化プロトコルを選択してください。カプセル化プロトコルには ESP、AH、ESP＋AH があります。EPS は AH に比べてセキュリティが高い設定です。
⑦ PFS を使用する場合は有効にチェックを入れてください。PFS を有効にするとよりセキュリティが高い設定になります。
⑧ プレシェアードキーを入力してください。プレシェアードキーはリモート、ローカル共に同じ必要があります。
⑨ リモート ID、ローカル ID を入力してください。アグレッシブモードでは IP ではなく ID で認証するためレスポンダーの場合リモート ID が必ず必要になります。リモート ID とは接続相手側で指定したローカル ID になります。



⑩ 設定を完了したら[保存]をクリックしてください。設定したトンネルが有効にチェックが入っていることを確認して設定は完了です。

注意

レスポンダー設定は固定グローバル IP アドレスを使用してください。メインモードとアグレッシブモード同士の設定では接続できません。

19-1-3 手動鍵管理の設定

① VPN-IPsec 有効にチェックを入れ、組み込みを選択しトンネル数を定義してください。
② 鍵交換方法から手動鍵管理を選択し設定をクリックしてください。

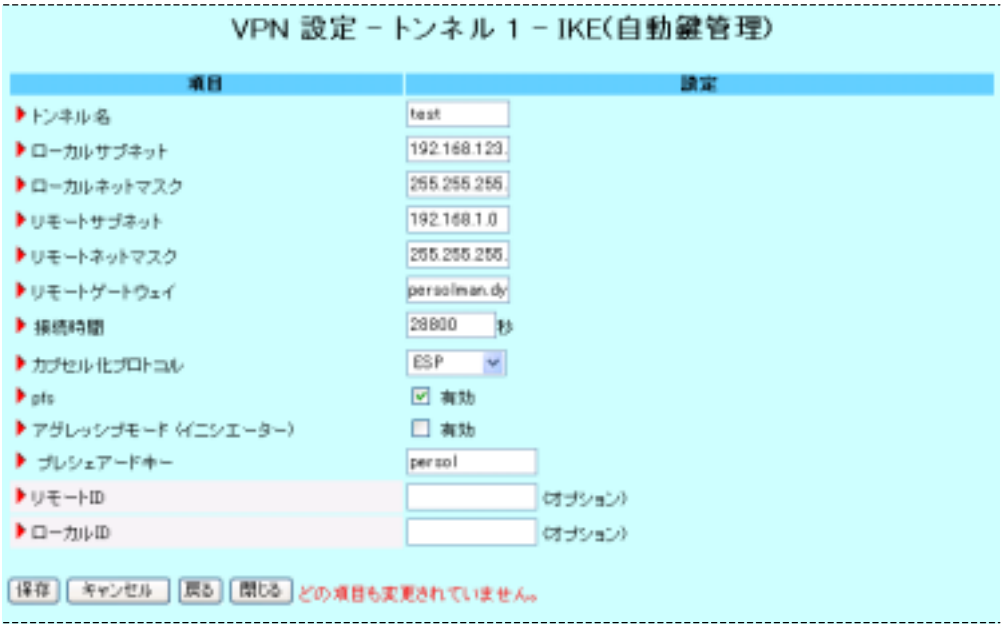
③ トンネル名を入力してください。トンネル名には自由な名前をつけることが出来ます。
④ ローカルサブネット、ローカルネットマスクを入力してください。(LAN ネットワーク)
⑤ リモートサブネット、リモートネットマスクを入力してください。(リモートネットワーク)
⑥ リモートゲートウェイを入力してください。VPN 接続する機器のグローバル IP アドレスを入力してください。
⑦ 接続時間を入力してください。最大接続時間は 28800 秒です。
⑧ カプセル化プロトコルを選択してください。カプセル化プロトコルには ESP、AH があります。EPS は AH に比べてセキュリティが高い設定です。
⑨ ローカル SPI、リモート SPI を入力してください。SPI は SA を認識するために必要になります。
⑩ 暗号化アルゴリズムを 3DES もしくは DES のどちらかを選択してください。3DES は DES よりもセキュリティは上がりますがスループットは下がります。また暗号化アルゴリズムはカプセル化プロトコル ESP を選択したときのみ選択できます。
⑪ 暗号鍵を 16 進数で入力してください。
⑫ 認証アルゴリズムを NONE、SHA1、MD5 から選択してください。
⑬ 認証鍵を入力してください。
⑭ 設定を完了したら[保存]をクリックしてください。設定したトンネルが有効にチェックが入っていることを確認して設定は完了です。

19-2 VPN-DDNS

本製品ではＤＤＮＳを利用した動的IP同士のＶＰＮ構築をすることができます。これにより固定IPアドレスをプロバイダーからレンタルなしで非常に安価にＶＰＮ構築することができます。ただし VPN-DDNS は1対1の VPN 接続のみサポートします。

① まず始めに DDNS サービスからドメイン名を取得してください。
② DDNS 設定を選択し取得したホスト名（ドメイン名）を入力し、DDNS サービスに登録したユーザー名とパスワードを入力してください。

③ 19-1-1 と同様に VPN の設定 IKE モードを選択しリモートゲートウェイにリモートのホスト名（ドメイン名）を入力してください。



※ 画面はリモートホスト名が persolman.dyndns.org の場合です。

注意

- ●VPN-DDNS を使用する場合は基本設定から“ 最大アイドル時間 ”を“ 0 ”にし“ 自動再接続 ”にチェックを入れてください。
- ●DDNS のドメイン取得については各サービス業者にお尋ねください。
- ●VPN-DDNS では必ず IKE メインモードをご使用ください。
- ●DDNS の特性上 VPN 接続に時間がかかる場合があります。この場合は“ コマンドプロンプト ”より“ ipconfig /flushdns ”を行いその後、使用しているドメイン名に“ ping ”を行い 5 分ほど待ってから VPN 接続してください。

19-3 IPsec パススルー

LAN 内でプライベート IP アドレスを持つ VPN クライアントを、WAN へ通過させる機能です。通常では、プライベート IP アドレスを持つクライアントが外部と通信を行う場合、IP マスカレードによりアドレス変換を行います。しかし、通常の IP マスカレードでは、VPN のパケットは通過できません。IPsec パススルーでは Ipsec のパケットを通過させることができるようにする機能です。BSR14 では Ipsec のパススルーのみ対応しています。

設定を行う場合は VPN 設定メニューから VPN-IPsec を有効にしパススルーを選択してください。

20. VPN 用語解説

■ AH

AH (認証ヘッダー)プロトコルは、パケットと発信元の信頼性、安全性を提供するプロトコルです。プレシェアードキーと MD5 あるいは SHA-1 ハッシュ関数を使用して HMAC を算出しチェックサムによってそのパケットを認証します。

■ MD5

任意に指定した長さのキーワードと 16 バイト鍵から 128 ビットハッシュを生産するアルゴリズム。

■ SHA-1

任意に指定した長さのキーワードと 20 バイト鍵から 160 ビットハッシュを生産するアルゴリズム。SHA-1 は 160 ビットハッシュを生成し MD5 より大きなハッシュのため、一般的に MD5 より安全とされています。

■ ESP

ESP プロトコルは暗号化、認証、安全性を提供するプロトコルです。ESP は IP パケット全体をカプセル化し、新たに IP ヘッダーを現在の暗号化済みパケットに追加します。この新たに追加された IP ヘッダーはネットワークを通じてデータを送信するために必要な宛先アドレスを追加しています。
また ESP では暗号化に以下の暗号化アルゴリズムを選択します。

■ DES

56 ビット鍵での暗号化アルゴリズム

■ 3DES

168 ビット鍵を使用、3 回の DES アルゴリズムを使用し暗号化するため強力なセキュリティを提供します。より強力なセキュリティを求める場合は3DEC を使用することをおすすめします。

■ 鍵管理

鍵の管理は、VPN を使用するために非常に重要です。IPSec では、手動鍵交換および自動鍵交換の IKE を使用することができます。

■ 手動鍵交換

手動の鍵を使用する場合には管理者はパラメータを設定します。しかし遠距離にわたる手動鍵管理は直接鍵を渡すのは別としてネットワークを利用しての交換の場合常に盗聴の危険にあるといえます。

■ IKE

多くのトンネルを作成し管理する必要がある場合、各設定を手動で行わなくてもよい方法が IKE です。IPSec では IKE プロトコルを使用して鍵の自動生成を行います。

■ 事前共有鍵 (プレシェアードキー) IKE

認証を行うために事前共有鍵を使用する IKE で、お互いが前もって事前共有鍵を交換しう必要があります。IKE プロトコルを使用して定期的にその鍵を自動的に変更します。自動的に鍵を交換することによりセキュリティにも優れ、管理者の手間も軽減できます。

■ PFS

PFS (Perfect Forward Secrecy) を使用すると、セキュリティ・パラメータをトンネルに追加することができます。PFS を有効にすると暗号化鍵と認証鍵が生成されるたびに新しい DH 鍵交換が行われます。トンネル伝送に PFS を追加すると VPN の暗号化に使用される鍵の検出が大幅に難しくなります。セキュリティをより強化したい場合におすすめします。

■ Main Mode とAggressive Mode

フェーズ 1 は、 Main Mode か Aggressive Mode のいずれかで行われます。
Main Mode :イニシエータとレスポンダーは、IPsec SA を作成するために 6 つのメッセージを送信します。
Aggressive Mode (アグレッシブモード):イニシエータおよびレスポンダーは Main Mode と同じ目的を達成しますが、3 つのメッセージを送信するだけです。

動的 IP の VPN クライアントが VPN を使用する場合には Aggressive Mode が使用されなければなりません。 動的 IP を使用する場合は ID を使用し VPN を構築してください。IP アドレスを使用することもできますが動的に変更されてしまうため実際の管理には不向きだと考えられています。

■ SPI

SPI はある IPSec のパケットがどの SA に対応しているかを区別するために、IPSec のヘッダー中に Security Parameters Index(SPI)というポインタによって指定しています。

超高速ブロードバンドルータ（VPN 機能付） BSR14
ユーザーズマニュアル 2003 年 12 月 25 日 第 1 版 発行
パーソル株式会社