PLANEX COMM.

VPN-41FE

User's Manual

User's Manual Version : VPN-41FE_Manual_V1

目次

I. ハードウェアのインストール

本章では、ハードウェアインターフェースと物理的インストールを説明します。

1.1 LED ランプ

LED ランプの説明

LED	色	説明
Power ランプ	緑点灯	電源 ON 時
	消灯	電源 OFF 時
DIAG ランプ	緑点滅	起動時、自己判断時、リセット動作時
	緑点灯	故障時
	消灯	正常動作時
LAN ランプ	緑点灯	リンク確立時
	緑点滅	データ送受信時
	消灯	リンク未確立時
WAN ランプ	緑点灯	リンク確立時
	緑点滅	データ送受信時
	消灯	リンク未確立時
USB ランプ	緑点灯	USB デバイス利用可能時
	消灯	USB デバイス利用不可時

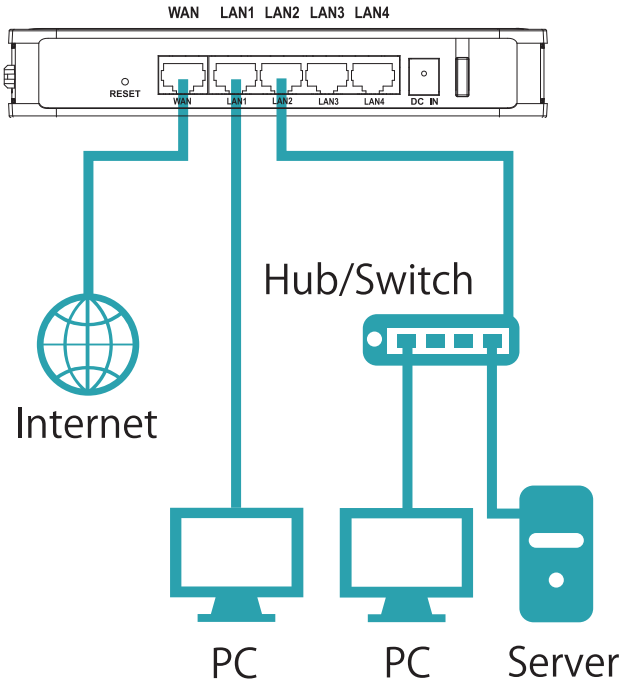
リセット

動作	説明
リセットボタンを 5 秒間押します	ウォームスタート DIAG インジケーター : DIAG LED がゆっくり点滅している状態です。
リセットボタンを 10 秒以上押します	工場出荷時の設定 DIAG インジケーター : DIAG LED が早く点滅している状態です。

1.2 ネットワーク接続

WAN 接続 : WAN ポートを、xDSL モデム、ファイバーモデム、スイッチングハブ、または外部ルータ経由でインターネットに接続します。

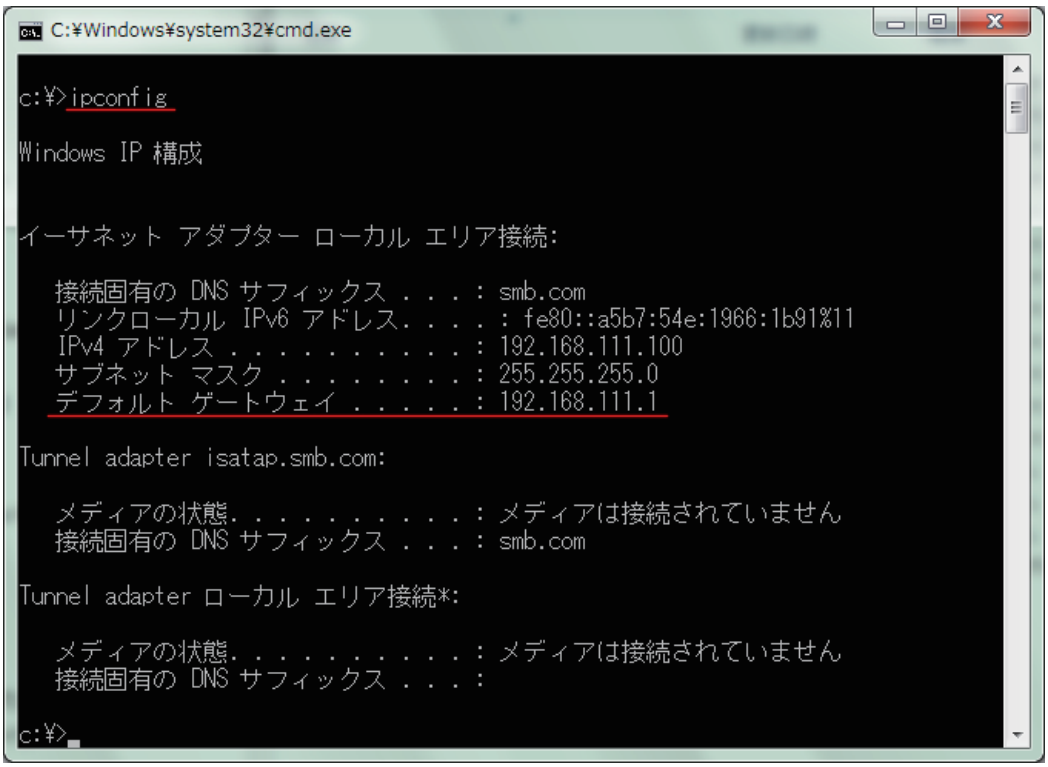
LAN 接続 :LAN ポートを、スイッチングハブまたは PC に直接接続できます。「物理ポート管理」を設定後、サーバーを用いてポートをモニタリングまたはポート経由でフィルタリングできます。



II. ルータのログイン

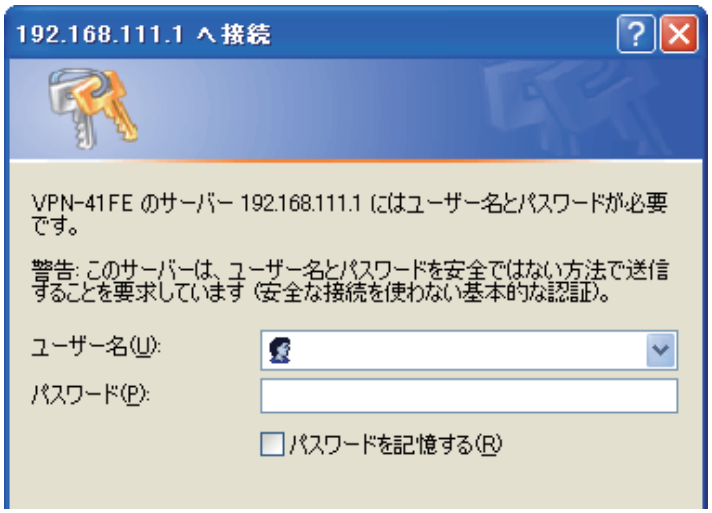
本章では、ルータ接続後に表示される Web ベースの UI を中心に説明します。

最初に、ルータに接続された LAN 内の PC 経由でコマンドプロンプトに接続して、ルータの IP アドレスを確認します。[スタート] → [ファイル名を指定して実行] をクリックし、「cmd」と入力してコマンドプロンプトを起動します。「ipconfig」と入力し、デフォルト ゲートウェイ アドレスが、以下の画面に表示される「192.168.111.1」であることを確認します。デフォルトゲートウェイがルータのデフォルト IP アドレスでもあることを確認します。



※「ipconfig」と入力して、IP アドレスとデフォルト ゲートウェイが表示されない場合、ないし取得されている IP アドレスが「0.0.0.0」および「169.X.X.X」になっている場合、回線に問題がないか、コンピュータ ネットワーク カードが適切に接続されているか確認することをお勧めいたします。

次に、IE などの Web ブラウザーを起動し、アドレス欄に「192.168.111.1」を入力します。ログイン画面が以下のとおり表示されます :



ルータのユーザー名とパスワードの初期設定は、それぞれ「admin」と「password」です。ログイン パスワードはこの後の設定で変更できます。

※セキュリティ上、ログイン後にパスワードを変更することをお勧めいたします。パスワードを安全なものにしてください。そうでない場合、ルータにログインできません。リセットボタンを 10 秒以上押すと、すべての設定が初期値に戻ります。

ログイン後、Web ベースの UI が表示されます。Web ページの右上端で言語を選択します。選択された言語は青で表示されます。以下のとおり、「日本語」を選択します。

III. ホーム

ホームページでは、本製品のすべてのパラメーターとステータスが参照として表示されます。

3.1 WAN ステータス

WAN IP 側アドレス :	WAN ポートの現在の IP 構成です。
デフォルトゲートウェイ :	プロバイダー (ISP) から取得した、現在の WAN ゲートウェイの IP アドレスです。
DNS:	DNS の現在の IP 構成です。
使用中の下りバンド幅 (%):	各 WAN の現在の使用中の下りバンド幅 (%) です。
使用中の上りバンド幅 (%):	各 WAN の現在の使用中の上りバンド幅 (%) です。
DDNS 設定 :	ダイナミック ドメイン ネームが有効になっているか示す。 初期設定は「オフ」です。
手動接続 :	「自動的に IP を取得する」が選択されている場合、2 つのボタン (「リリース」と「更新」) が表示されます。PPPoE ないし PPTP などの WAN 接続が選択されている場合、「切断」と「接続」が表示されます。

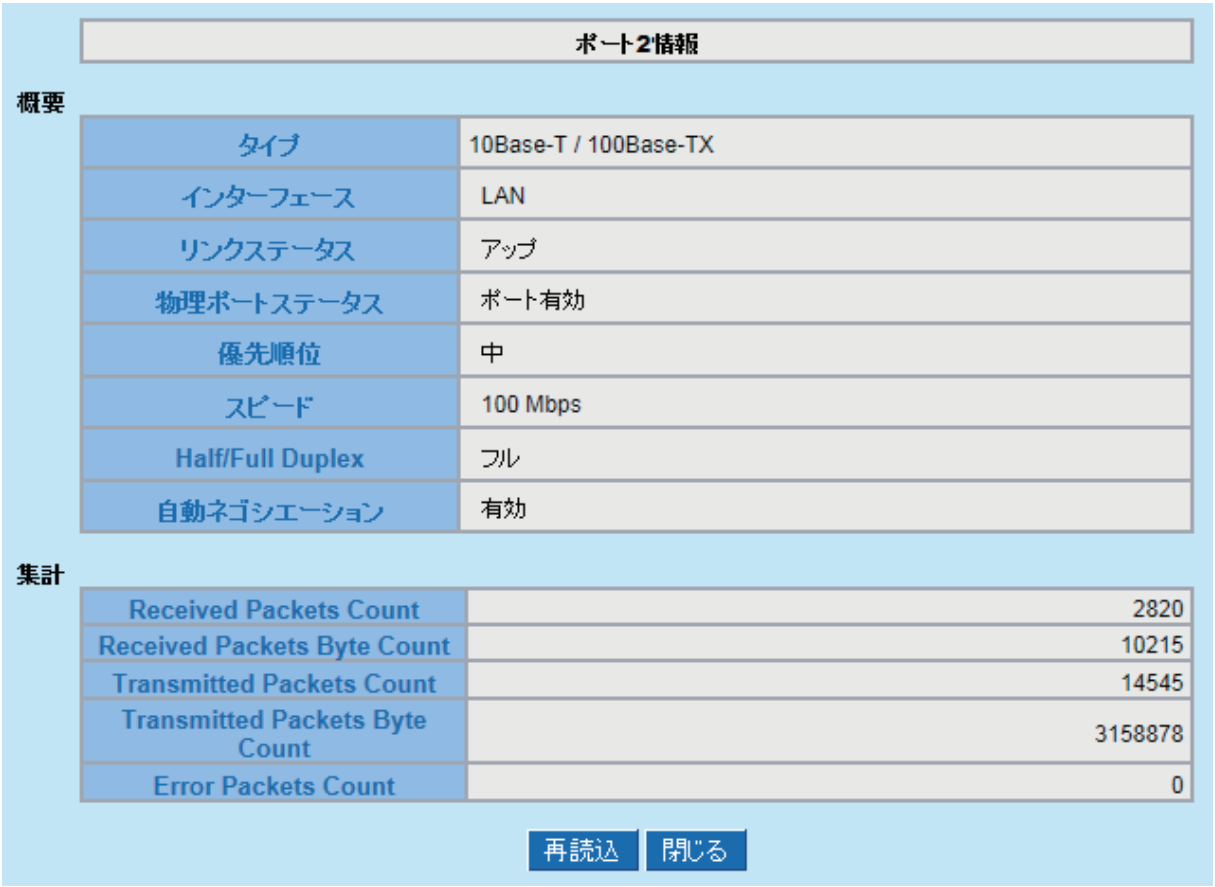
3.2 物理ポートステータス

物理ポートステータス

ポートID	1	2	3	4
インターフェース	LAN			
ステータス	有効	接続	有効	有効

ポートID	Internet
インターフェース	WAN1
ステータス	接続

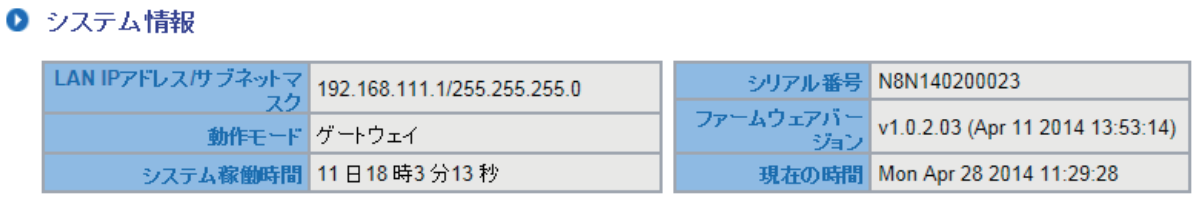
接続されたポートや有効なポートをそれぞれふくむ、すべてのシステムポートのステータスが、このホームページに表示されます (上記の表を参照)。各ステータスボタンをクリックすると、別のウィンドウが表示され、選択されたポートの詳細データ (設定ステータスの概要や統計をふくむ) が表示されます。



現在のポート設定ステータス情報が、ポート情報画面に表示されます。

例 : タイプ (10Base-T ／ 100Base-TX)、インターフェース (WAN ／ LAN)、リンクステータス (アップ／ダウン)、物理ポートステータス (ポート有効／ポート無効)、優先順位 (高または中)、スピード (10Mbps または 100Mbps)、Half/Full Duplex (ハーフ／ フル)、自動ネゴシエーション (有効／無効)。表には、送受信パケットの統計、送受信パケットバイト数、エラーパケット数も表示されます。

3.3 システム情報



● LAN IP アドレス／サブネットマスク : デバイスの現在の IP アドレスとサブネットマスクです。初期値はそれぞれ「192.168.111.1」と「255.255.255.0」です。

●動作モード : 現在の動作モードを示します。「ゲートウェイ」または「ルータ」のいずれかのモードになります。初期設定は「ゲートウェイ」モードです。

●システム稼働時間 : これまでのデバイス稼働時間です。

●シリアル番号 : この番号は、デバイスのシリアル番号です。

●ファームウェアバージョン : デバイスの現在のソフトウェア バージョン情報です。

●現在の時刻 : デバイスの現在の時刻です。

注意 : 正確な時刻に合わせるには、デバイスとリモート NTP サーバーを最初に同期してください。

3.4 セキュリティ ステータス

セキュリティステータス

ファイアウォール	ステータス
SPI (Stateful Packet Inspection)	オン
DoS (Denial of Service)	オン
WAN側のリクエストをブロック	オン
ARPウィルス攻撃の防御	オン
リモート管理	オフ
アクセスルール	0ルール設定済

● SPI (Stateful Packet Inspection):SPI (ステートフル パケット インスペクション) がオンまたはオフかどうか表示します。初期設定は「オン」です。

● DoS (Denial of Service):DoS 攻撃防御が有効かどうか表示します。初期設定は「オン」です。

● WAN 側のリクエストをブロック : インターネット接続拒否が有効かどうか表示します。初期設定は「オン」です。

● ARP ウイルス攻撃の防御 :ARP ウイルス攻撃の防御が有効かどうか表示します。初期設定は「オフ」です。

●リモート管理 : リモート管理が有効 (「オン」または「オフ」) かどうか表示します。ハイパーリンクをクリックして、設定画面に入り管理します。初期設定は「オフ」です。

●アクセスルール : 本製品に適用されているアクセスルール数です。

3.5 VPN および GRE ステータス

VPN ステータス

IPSec VPN設定	ステータス
使用中のトンネル	0
利用可能なトンネル	10

● IPSec VPN 設定 :VPN ルータの VPN 設定情報です。

●使用中のトンネル :VPN (仮想プライベートネットワーク) に設定されているトンネル数です。

●利用可能なトンネル :VPN (仮想プライベートネットワーク) に利用可能なトンネル数です。

GREステータス

GRE	ステータス
GREトンネル接続	0
使用中のトンネル	0

● GRE トンネル接続 :GRE に設定されているトンネル数です。

●使用中のトンネル :GRE に使用されているトンネル数です。

3.6 ログ

ログ

ログの送信先	無効

●ログの送信先 :Syslog サーバが有効か無効かを表示します。

IV. ネットワーク

4.1 ネットワーク接続

4.1.1 ホスト名とドメイン名

ホスト名：	SMB	(ISPによっては設定が必要です)
ドメイン名：	smb.com	(ISPによっては設定が必要です)

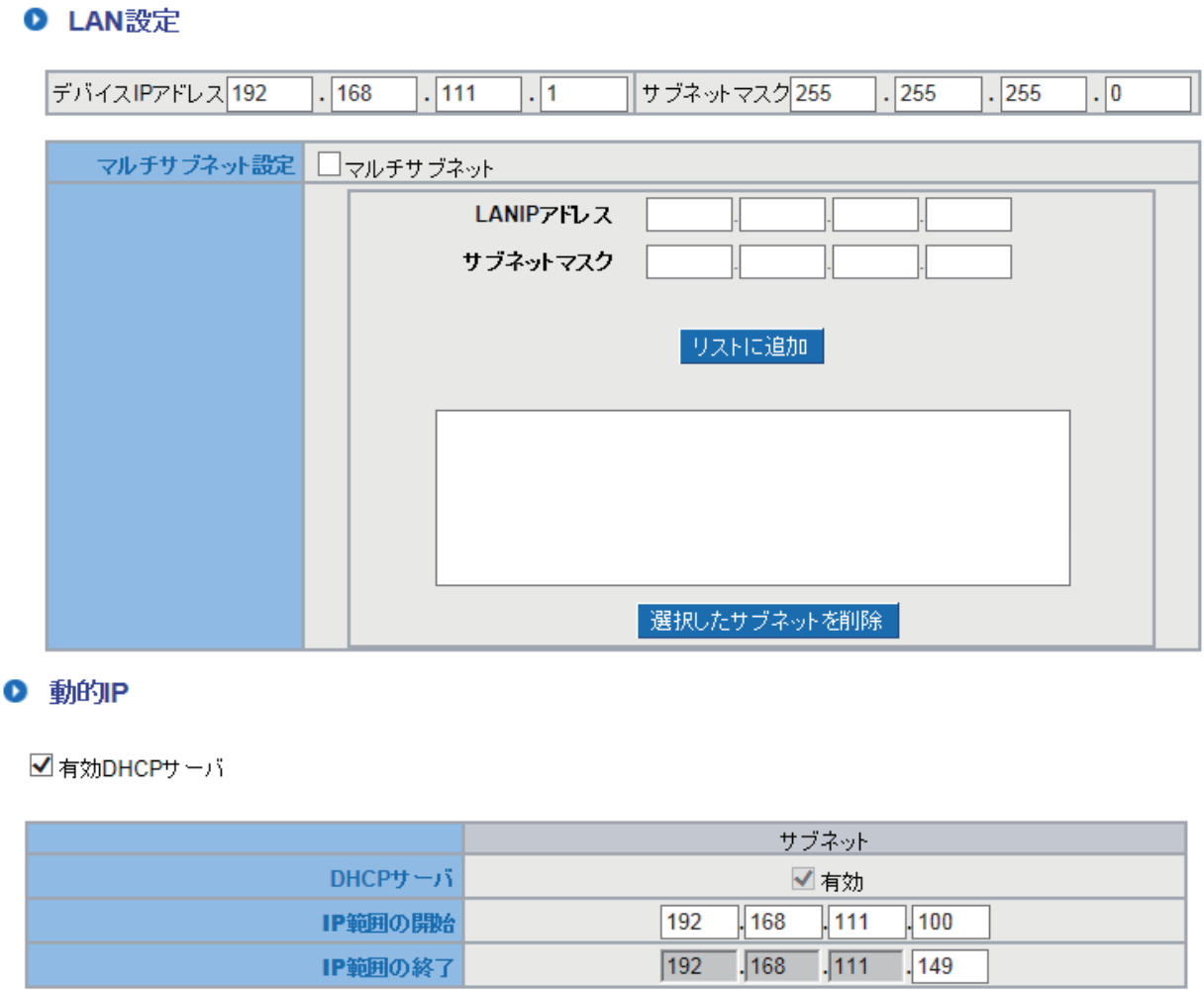
ホスト名とドメイン名は 2 つのテキストボックスにそれぞれ入力できます。この設定はほとんどの環境で必要ありませんが、いくつかの国のいくつかの ISP (インターネットサービスプロバイダ) によっては設定が必要となることがあります。

4.1.2 LAN 設定

デバイスの現在の LAN の IP アドレスの設定情報です。初期設定は、「192.168.111.1」です。サブネットマスクの初期設定は「255.255.255.0」です。設定は、実際のネットワーク構造に準じて変更できます。

マルチサブネット設定：

「ユニファイド IP 管理」をクリックし、次ページの図に示す設定ページを開きます。それぞれの IP アドレスとサブネットマスクを入力します。



ルータネットワークセグメントやマルチネットセグメント構成と異なる IP セグメントを入力できます。この機能を設定することで、インターネットに直接アクセスできます。

4.1.3 WAN 設定

WAN設定

インターフェース	接続タイプ	設定.
WAN1	自動的にIPを取得する	編集

インターフェース	現在のポートの接続状況を表示します。
接続タイプ	「自動的に IP を取得する」、「固定 IP 接続」、「PPPoE (Point-to-Point Protocol over Ethernet：イーサネット上のポイント・ツー・ポイント・プロトコル)」、「L2TP」、「透過ブリッジ」、「Router Plus NAT モード」または「PPPoE Unnumbered」から選択します。
設定	詳細設定での変更です。「編集」をクリックし、高度な設定ページを開きます。

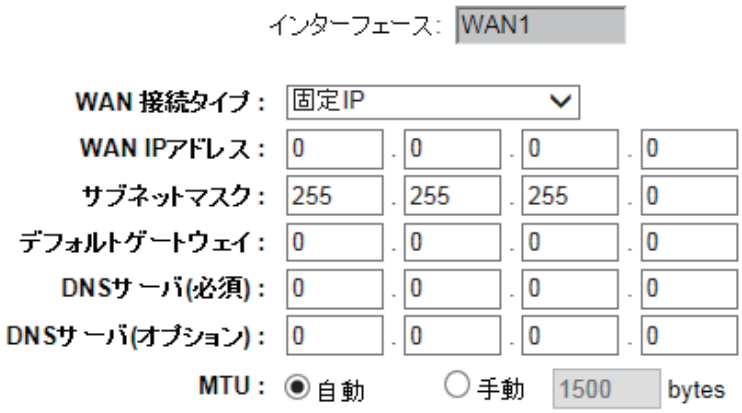
自動的に IP を取得する：

このモードは、DHCP を使用して IP アドレスを自動的に取得する接続モードで広く使われています。デバイスの初期設定の接続モードです。この接続モードを使用すると、DHCP クライアントが IP アドレスを自動的に取得します。異なる接続モードを使用している場合は、以下の説明を参照して、適切な設定を選んでください。DNS アドレスを設定することもできます。目的のオプションをチェックし、ユーザー定義の DNS アドレスを入力します。

以下の DNS サーバアドレスを使用する	ユーザー定義の DNS アドレスを選択します。
DNS サーバ	ISP (インターネットサービスプロバイダ) が指定した DNS サーバ IP アドレスを入力します。少なくとも 1 つの IP グループを入力してください。IP グループを最大 2 つまで入力できます。
MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、「1492」)。初期設定は「自動」です。

固定 IP：

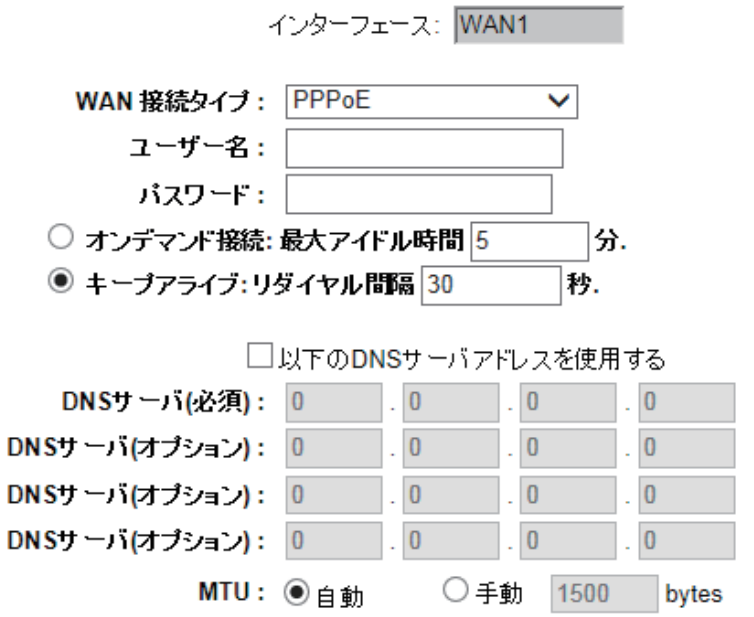
ISP (インターネットサービスプロバイダ) が固定 IP (1 つの IP または 8 つの IP アドレスなど) を発行する場合は、この接続モードを選びます。以下の手順に従い、ISP (インターネットサービスプロバイダ) が発行した IP アドレスを、該当するテキストボックスに入力します。



WAN IP アドレス：	ISP (インターネットサービスプロバイダ) が発行した利用可能な固定 IP アドレスを入力します。
サブネットマスク：	ISP (インターネットサービスプロバイダ) が発行した固定 IP アドレスのサブネットマスクを入力します。 例：発行された 8 つの IP アドレス：255.255.255.248 発行された 16 つの固定 IP アドレス：255.255.255.240
デフォルトゲートウェイ：	ISP (インターネットサービスプロバイダ) が発行したデフォルトゲートウェイを入力します。ADSL をお使いの場合は、ATU-R 対応 IP アドレスになります。光ファイバーをお使いの場合は、光ファイバー対応スイッチ IP アドレスを入力します
DNS サーバ :	ISP (インターネットサービスプロバイダ) が発行した DNS サーバ IP アドレスを入力します。少なくとも 1 つの IP グループを入力してください。 IP グループを最大 2 つまで入力できます。
MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、1492)。 初期設定は「自動」です。

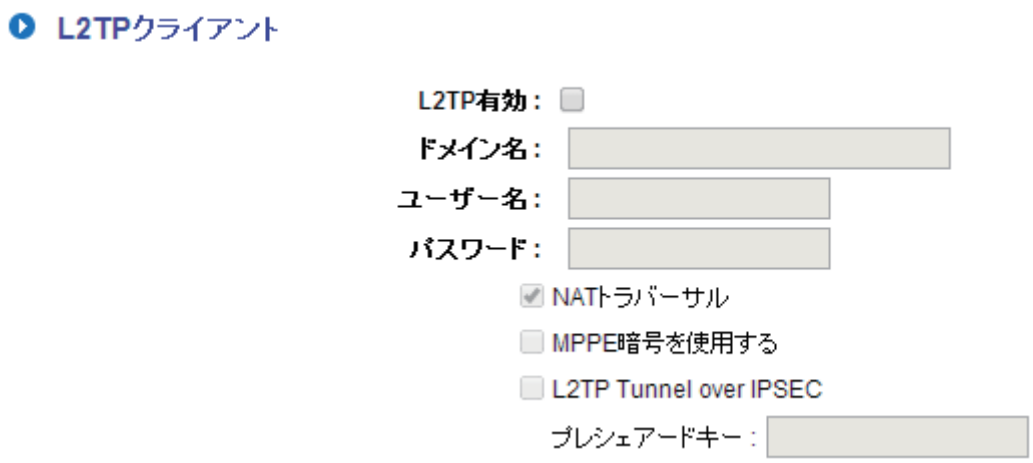
PPPoE：

ADSL の仮想ダイアルアップ接続 (ADSL の PPPoE に適している) のためのオプションです。



ユーザー名	ISP (インターネットサービスプロバイダ) が発行したユーザー名を入力します。
パスワード	ISP (インターネットサービスプロバイダ) が発行したパスワードを入力します。
オンデマンド接続	PPPoE ダイヤル接続に対して自動ダイヤル機能を利用できます。クライアントポートがインターネットへの接続を試みる際に、デバイスが自動的にダイヤルアップ接続を行います。一定時間回線を使用していない場合は、システムが自動的に接続を切断します (パケット送受信がない場合の自動切断時間の初期設定は 5 分です)。
キープアライブ	PPPoE ダイヤル接続の状態を継続し、回線が切断された場合は自動的にリダイヤルできます。また、リダイヤルの開始までの待ち時間を設定できます。初期設定は 30 秒です。
以下の DNS サーバアドレスを使用する	ユーザー定義の DNS アドレスを選択します。
DNS サーバ	ISP (インターネットサービスプロバイダ) が指定した DNS サーバ IP アドレスを入力します。少なくとも 1 つの IP グループを入力してください。 IP グループを最大 4 つまで入力できます。
MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、1492)。 初期設定は「自動」です。

L2TP：



L2TP 有効 :	L2TP を有効の状態にします。初期設定は、無効の状態になっています。
ドメイン名 :	接続先の PC の IP アドレスを 1 つ (IPv4 または IPv6) か、あるいはドメイン名を入力します。
ユーザー名 :	リモートユーザー名を入力します。
パスワード :	リモートユーザー名に対応するパスワードを入力します。

● NAT トラバーサル：NAT デバイスが L2TP パケットに対応していないことがあるため、NAT を使用しているデバイスを通過するときに、L2TP が機能しない場合があります。NAT トラバーサルを有効にすると、この問題を回避できます。この項目を有効にすると、L2TP トラフィックが NAT デバイスを通過できるようになります。

● MPPE 暗号を使用する：経路上のパケットを Microsoft Point to Point Encryption によって暗号化します。L2TP による VPN 接続の場合、通信経路上のパケットは暗号化されないため、本機能ないしは後述する L2TP Tunnnel over IPSEC の利用をおすすめします。

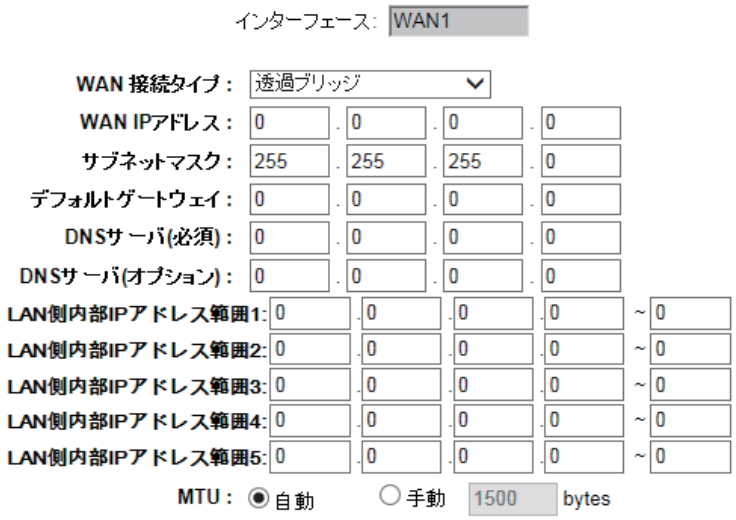
● L2TP Tunnnel over IPSEC：IPSEC によるコネクション上に L2TP トンネリングを行います。通信の機密性や完全性を IPSEC にて実現する為、セキュアな通信を可能にします。IKEv1 による Pre Shared Key にのみ対応しております。

透過ブリッジ：

すべてのイントラネットの IP アドレスをインターネットの IP アドレスとして適用している場合や、プライベートネットワーク IP アドレスをすべてのイントラネット IP アドレス (例：192.168.111.X) として代用したくない場合は、この機能を使用して、オリジナルの構造の変更なしに既存のネットワークを統合できます。「WAN 接続タイプ」で「透過ブリッジ」

モードを選びます。こうすれば、オリジナルのインターネットの IP アドレスをイントラネットの IP 構成で保持した状態で、インターネットに正常に接続できます。

2 つの WAN が構成されている場合でも、「WAN 接続タイプ」で「透過ブリッジ」モードを選んで、通常とおりにロードバランシングできます。

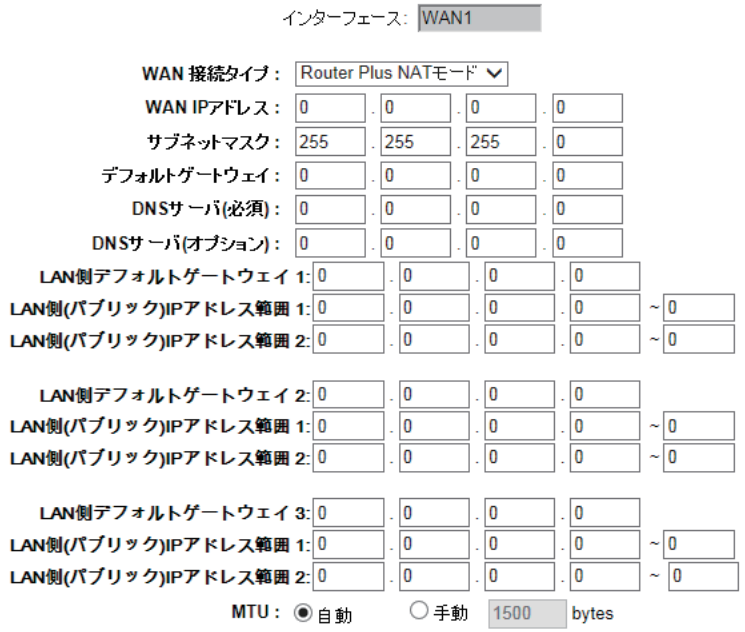


WAN IP アドレス	ISP (インターネットサービスプロバイダ) が発行した固定 IP アドレスのうち、1 つを入力します。
サブネットマスク	ISP (インターネットサービスプロバイダ) が発行した固定 IP アドレスのサブネットマスクを入力します。 例 : 発行された 8 つの IP アドレス：255.255.255.248. 発行された 16 つの固定 IP アドレス：255.255.255.240.
デフォルトゲートウェイ	ISP (インターネットサービスプロバイダ) が発行した固定 IP アドレスのデフォルトゲートウェイを入力します。ADSL をお使いの場合は、ATU-R 対応 IP アドレスになります。
DNS サーバ	ISP (インターネットサービスプロバイダ) が指定した DNS サーバ IP アドレスを入力します。少なくとも 1 つの IP グループを入力してください。IP グループを最大 2 つまで入力できます。
LAN 側内部 IP アドレス範囲	ISP (インターネットサービスプロバイダ) が発行した利用可能な IP アドレス範囲を入力します。ISP (インターネットサービスプロバイダ) が 2 つの連続していない範囲を発行した場合、「LAN 側内部 IP アドレス範囲 1」と「LAN 側内部 IP アドレス範囲 2」にそれぞれ入力できます。
MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、1492)。 初期設定は「自動」です。

Router Plus NAT モード：

パブリック IP アドレスをデフォルトデートウェイとして適用するときに、LAN 接続した PC にこのパブリック IP アドレスを 設定すると、その PC はパブリック IP アドレスを使用してインターネットに接続できます。他の PC は「NAT」モードを使用してインターネットに接続できます。

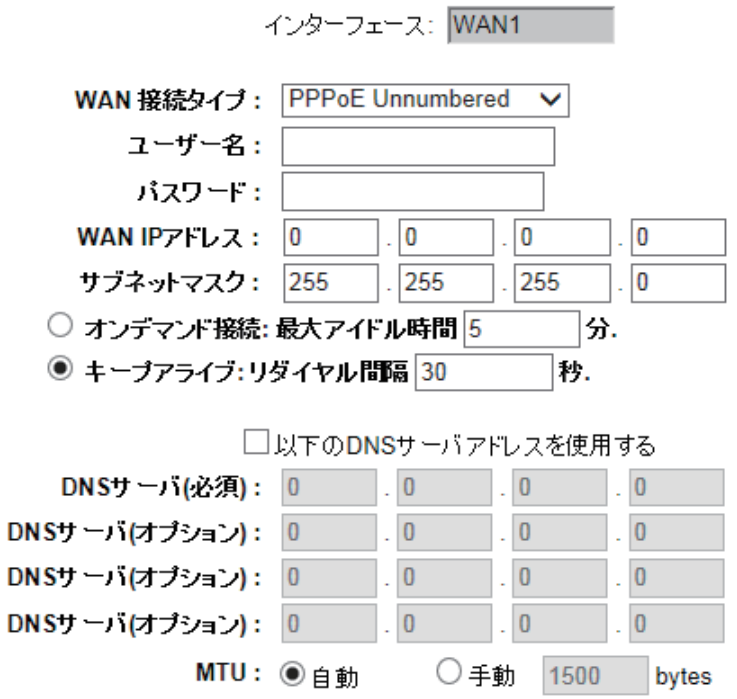
この WAN ネットワークで「Router Plus NAT」モードが有効の場合でも、負荷分散機能をこの WAN ネットワークで使用できます。



WAN IP アドレス	パブリック IP アドレスを入力します。
サブネットマスク	パブリック IP アドレスのサブネットマスクを入力します。
デフォルトゲートウェイ	お使いの ISP (インターネットサービスプロバイダ) が提供する WAN のデフォルトゲートウェイを入力します。
DNS サーバ	DNS サーバ IP アドレスを入力します。この項目は入力が必須です。DNS サーバ IP アドレスは最大 2 つまで利用可能です。
LAN 側デフォルトゲートウェイ	ISP (インターネットサービスプロバイダ) が提供する IP アドレスのうち、1 つをデフォルトゲートウェイとして入力します。
LAN 側 (パブリック)IP アドレス範囲	ISP (インターネットサービスプロバイダ) が提供する IP アドレス範囲を入力します。複数の IP アドレス範囲がある場合は、グループ 1 とグループ 2 を設定してください。 また、グループ 2 に対して、デフォルトゲートウェイと IP アドレス範囲を設定できます。
MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例:ADSL の PPPoE MTU の場合、1492)。初期設定は「自動」です。

[OK] をクリックして設定を保存するか、[キャンセル] をクリックして変更を保存せずに設定を終了します。

PPPoE アンナンバードモード：



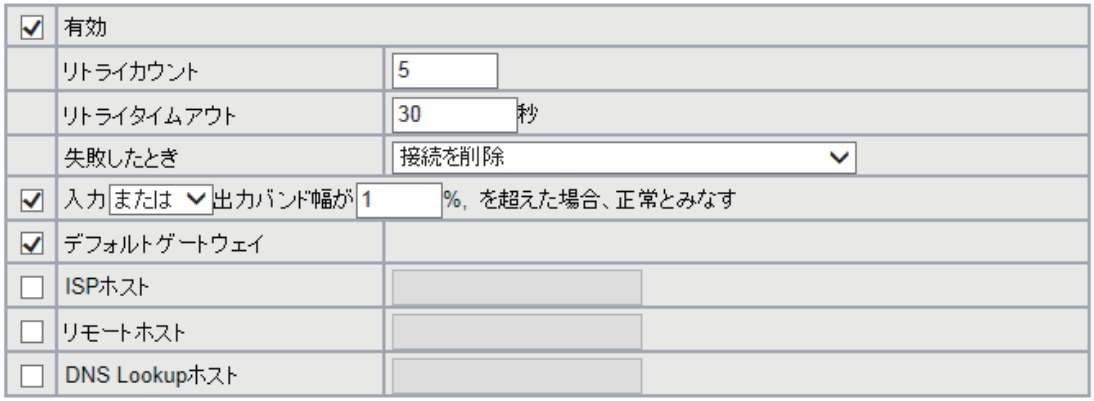
ユーザー名前	ISP (インターネットサービスプロバイダ) が発行したユーザー名を入力します。
パスワード	ISP (インターネットサービスプロバイダ) が発行したパスワードを入力します。
WAN IP アドレス	パブリック IP アドレスを入力します。
サブネットマスク	パブリック IP アドレスのサブネットマスクを入力します。
オンデマンド接続	PPPoE ダイヤル接続に対して自動ダイヤル機能を利用できます。クライアントポートがインターネットへの接続を試みる際に、デバイスが自動的にダイヤルアップ接続を行います。一定時間回線を使用していない場合は、システムが自動的に接続を切断します (パケット送受信がない場合の自動切断時間の初期設定は 5 分です)。
キープアライブ	PPPoE ダイヤル接続の状態を継続し、回線が切断された場合は自動的にリダイヤルできます。また、リダイヤルの開始までの待ち時間を設定できます。初期設定は 30 秒です。
以下の DNS サーバアドレスを使用する	ユーザー定義の DNS アドレスを選択します。
DNS サーバ	ISP (インターネットサービスプロバイダ) が指定した DNS サーバ IP アドレスを入力します。少なくとも 1 つの IP グループを入力してください。 IP グループを最大 2 つまで入力できます。

MTU	MTU は、Maximum Transmission Unit (最大伝送ユニット) の略です。「自動」または「手動」のいずれかを選びます。初期設定は「1500」です。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、1492)。 初期設定は「自動」です。

4.1.4 ネットワーク検出サービス

●外部のネットワークサービスを検出するシステムです。このオプションが選択されている場合、「リトライ」または「リトライタイムアウト」などの情報が表示されます。2 つの WAN が外部接続に使用されている場合は、必ず ネットワーク検出サービスを有効にして、WAN がトラフィック過負荷状態にあるとデバイスが誤って判断したことによる不要な切断を回避します。

ネットワークサービス検出



有効	クリックすると、ネットワーク検出サービスが有効になります。
リトライカウント：	ネットワーク検出サービスのリトライ回数を選びます。初期設定は 5 回です。設定した「リトライタイム」の間にインターネットから応答がない場合は、「外部接続が切断された」と判断されます。
リトライタイムアウト：	外部接続検出待ち時間の遅延時間です。初期設定は「30 秒」です。リトライタイムアウト後に、外部接続検出が再起動します。

失敗したとき	(1) システムログにエラーコンディションを出力する：ISP (インターネットサービスプロバイダ) で接続障害が検出された場合は、エラーメッセージがシステムログに記録されます。この回線は削除できないため、この回線を利用するユーザーが正常に接続できないことがあります。 このオプションは、WAN 接続のうち 1 つに障害が発生した状況や、この WAN を経由して宛先 IP アドレスへ向うトラフィックが、別の WAN に移動して宛先に到達できない状況に適しています。例えば、WAN2 が対応していない「10.0.0.1」から「10.254.254.254」までのトラフィックが WAN1 を経由するようにしたい場合は、このオプションを選択します。WAN1 接続が切断されると、「10.0.0.1」から「10.254.254.254 」までのパケットが WAN2 を経由して伝送できないため、WAN1 接続が切断されたときに接続を削除する必要はありません。 (2) 接続を削除する：ISP (インターネットサービスプロバイダ) で接続障害が検出された場合は、エラーメッセージはシステムログに記録されません。この WAN を経由して伝送されるパケットがもう一方の WAN に自動的に移され、元々の WAN が修復され再接続されたときにこの WAN に戻されます。 このオプションは、WAN 接続のうち 1 つに障害が発生したときや、この WAN を経由して宛先 IP アドレスへ向うトラフィックが、もう一方の WAN を経由して宛先に到達しなければならないときに適しています。こうすれば、WAN 接続のうちどれが切断しても、他の WAN がバックアップの役割を担うことができ、接続状態を保っている WAN にトラフィックを移動させることができます。
フィードバックサーバの検出：	
デフォルトゲートウェイ：	ADSL ルータの IP アドレスなど、ローカルデフォルト通信ゲートウェイの場所が、デバイスによって自動的に入力されます。そのため、この機能が必要な場合は、このオプションにチェックを入れるだけで設定できます。 注意！ ADSL ネットワークのゲートウェイによっては、パケット検出に影響を及ぼしません。光ファイバーボックスをお使いの場合、または ISP (インターネットサービスプロバイダ) が発行した IP アドレスがパブリック IP アドレスで、ISP (インターネットサービスプロバイダ) のポートではなく、ネットカフェのポートにゲートウェイが位置する場合は、このオプションを有効にしないでください。
ISP ホスト：	ISP (インターネットサービスプロバイダ) の DNS アドレスなど、ISP (インターネットサービスプロバイダ) のポートが検出された場所です。この機能に IP アドレスを設定するときに、この IP アドレスが確実かつ迅速に応答することができるか確認してください (ISP (インターネットサービスプロバイダ) の DNS アドレスを入力してください)。
リモートホスト：	リモートネットワークセグメントとして検出される場所です。このリモートホストの IP アドレスが、より確実かつ迅速に応答するかを、確認してください。(ISP (インターネットサービスプロバイダ) の DNS アドレスを入力してください)。
DNS Lookup ホスト：	DNS サーバが検出された場所です。また、2 つの異なる WAN に対して同じ Web アドレスをこのテキストボックスに入力しないでください。

V. イントラネット構成

本章では、ポートの構成方法と、イントラネットの IP アドレスの設定方法について説明します。

5.1 ポートステータス

●ポート管理を確認することによって、WAN ポートと LAN ポートのステータスを簡単に確認できます。

概要：

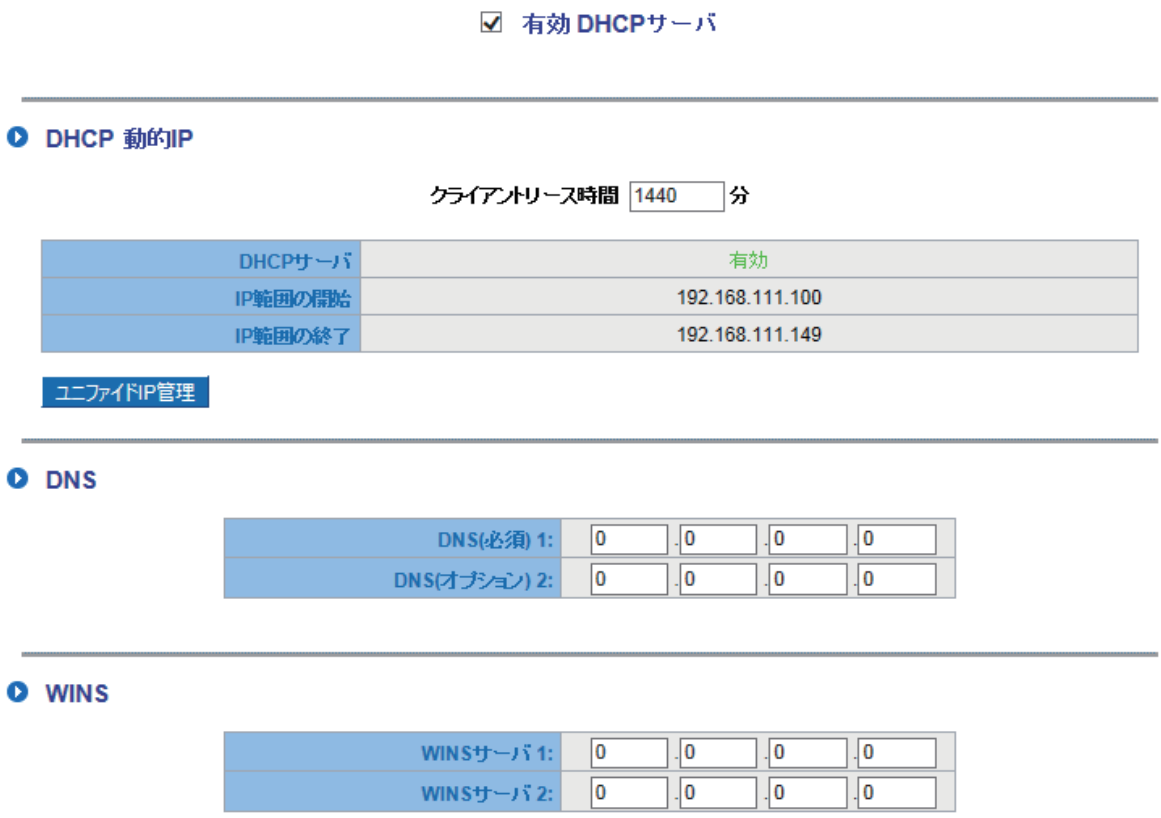
「タイプ」、「インターフェース」、「リンクステータス (アップ / ダウン)」、「物理ポートステータス (ポート有効)、「優先順位 (高または中)」、「スピード (10Mbps または 100Mbps)」、「Half/Full Duplex(ハーフ / フル)」、「自動ネゴシエーション (有効 / 無効)」 のメニューがあり、それぞれ設定できます。

集計：

この特定のポートのパケットデータを表示します。データには、送受信パケット数、送受信パケットバイト数、エラーパケット数が含まれています。[再読込] ボタンをクリックして、すべてのリアルタイムメッセージを更新します。

5.2 IP ／ DHCP

組み込み DHCP サーバでは、LAN に接続された PC に IP アドレスが自動的に割り当てられます (この機能は、NT サーバの DHCP サービスに似ています)。各 PC それぞれの IP アドレスを覚えて設定する手間がなくなります。PC をオンにすると、デバイスから IP アドレスを自動取得します。この機能を使用すると、管理が楽になります。



動的 IP：

有効 DHCP サーバ	このオプションをチェックすると、DHCP サーバによる IP アドレスの自動取得が有効になります。この機能が有効のとき、すべての PC が IP アドレスを自動取得します。このオプションを有効にしないときは、各 PC それぞれの仮想固定 IP アドレスを個別に設定してください。
クライアントリース時間：	PC が取得する IP アドレスのリース時間を設定します。初期設定は「1440 分」です（1 日）。環境に応じて、時間を変更できます。時間は分単位です。
IP 範囲の開始：	DHCP サーバが自動的にリースする始点 IP アドレスです。DHCP サーバが、この IP アドレスを起点としてリースを開始します。初期設定の始点 IP アドレスは、「192.168.111.100」です。
IP 範囲の終了：	DHCP サーバが自動的にリースする終点 IP アドレスです。初期設定の終点 IP アドレスは、「192.168.111.149」です。

DNS (ドメイン名サービス)

PC のポートにリースされている IP アドレスの DNS を確認します。このサーバの IP アドレスを直接入力します。

DNS(必須) 1：	DNS アドレスを入力します。
DNS(オプション) 2：	DNS アドレスを入力します。

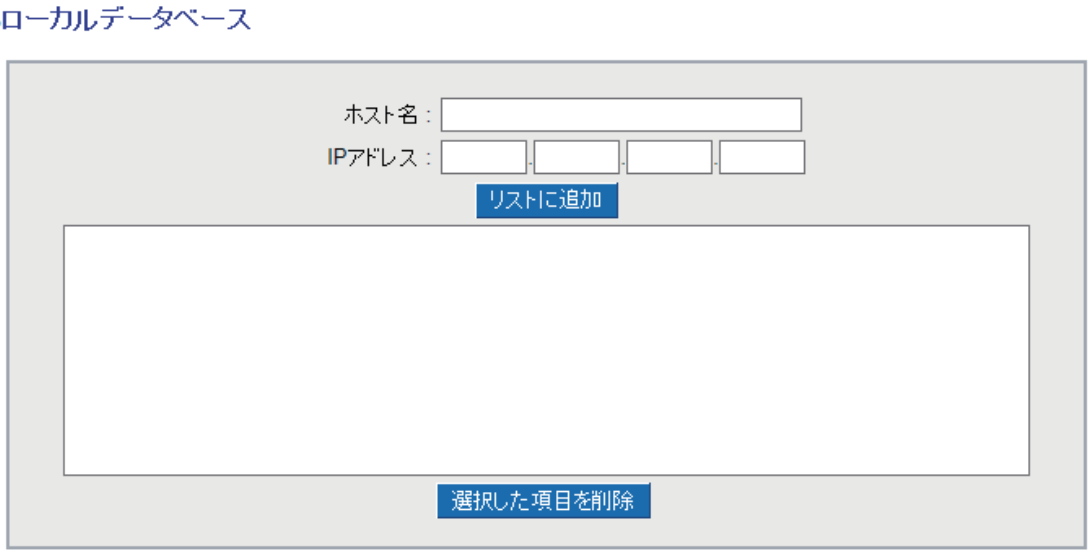
WINS

ネットワークに WINS サーバが存在する場合は、そのサーバの IP アドレスを直接入力できます。

WINS サーバ：	WINS サーバの IP アドレスを入力します。
OK：	[OK] をクリックして、ネットワーク構成の変更を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

DNS ローカルデータベース

通常は、DNS サーバが ISP (インターネットサービスプロバイダ) の DNS サーバまたは内部の自己定義の DNS サーバに向けられます。また、デバイスは、「DNS ローカルデータベース」と呼ばれる「かんたんな」自己定義の DNS サービスを提供します。このサービスを使うと、ホストドメイン名に対応する IP アドレスがマッピングされます。



ホスト名	Web サイトのホストドメイン名を入力します。 例：www.google.com
IP アドレス	上の欄に入力したホストドメイン名に対応する IP アドレスを入力します。
リストに追加：	以下のリスト欄に、項目を追加します。

注意！

(1) 必ず DCHP サーバのサービスを有効にして、DNS ローカルデータベースを有効にしてください。

(2) DCHP サーバの DNS アドレスを、ルータの LAN 側 IP アドレスとして設定してください。

5.3 DHCP ステータス

DCHP サーバの 現在のステータスと設定レコードの情報を表示します。情報は、ネットワークの変更が必要なときに、管理者の参照になります。

DHCP サーバ：	現在の DCHP サーバの IP アドレスです。
使用中の動的 IP：	DCHP サーバがリースする動的 IP アドレス数です。
使用中の静的 IP：	DCHP サーバがリースする固定 IP アドレス数です。
利用可能な DHCP：	DCHP サーバでまだ利用可能な IP アドレス数です。
合計：	DCHP サーバでリース設定されている IP アドレス総数です。
ホスト名：	現在の PC の名前です。
IP アドレス：	現在の PC が取得している IP アドレスです。
MAC アドレス：	現在の PC の実際の MAC アドレスです。
クライアントリース時間：	DCHP サーバがリリースしている IP アドレスのリース時間です。
削除：	IP アドレスのリースのレコードを削除します。

5.4 IP および MAC のバインド

管理者が「IP & MAC バインディング」機能を適用して、ユーザーがインターネットアクセス用に PC を追加したり、プライベート IP アドレスを変更できないようにします。

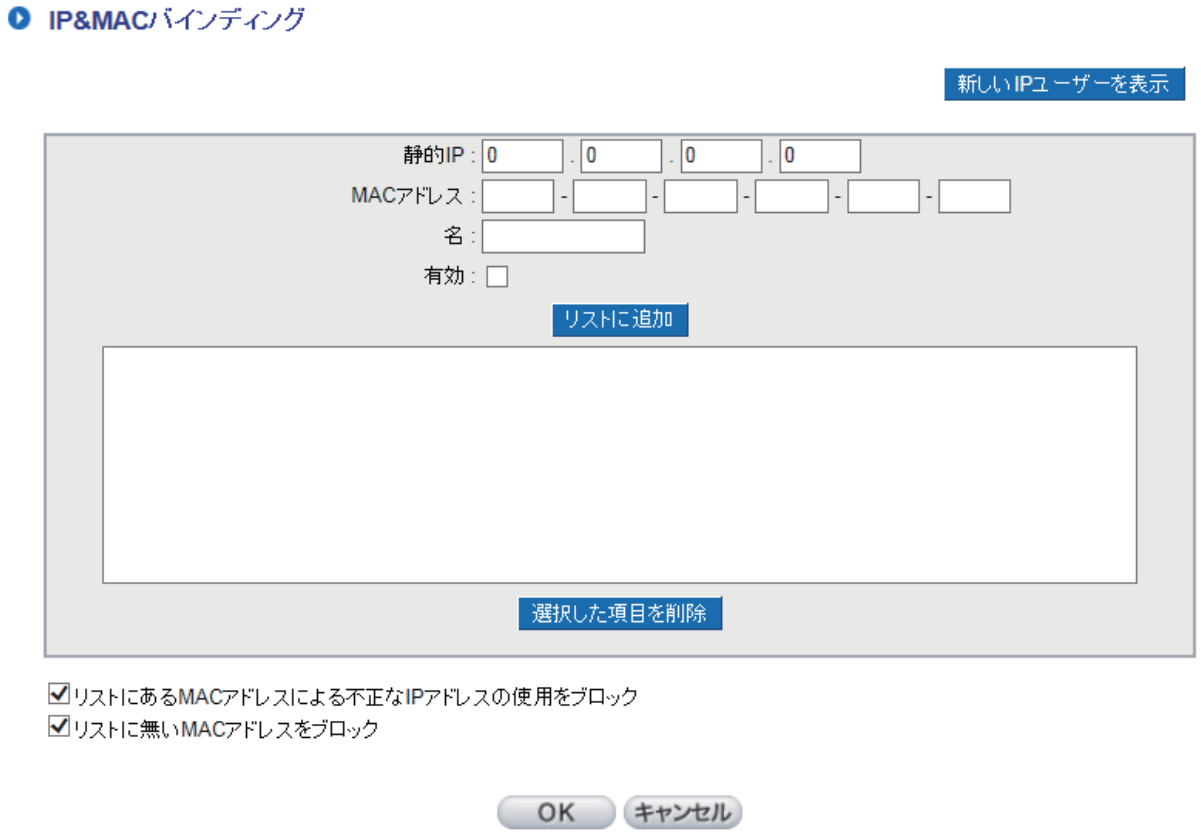
この機能を設定するには、2 つの方法があります

リストに無い MAC アドレスをブロック

この方法を使用して、リストにある MAC アドレスのみが、DHCP サーバから IP アドレスを取得し、インターネットにアクセスできるようにします。この方法を適用するときは、以下の図のとおり、固定 IP アドレスを「0.0.0.0」と入力します。

IP&MACバインディング

IP&MAC バインディング



静的 IP：	固定 IP アドレスを入力するには 2 つの方法があります： 1.MAC アドレスを設定して、DHCP サーバから IP アドレスを取得する場合に、特定の IP アドレスを割り当てる必要がなければ、テキストボックスに「0.0.0.0」と入力します。テキストボックスは空白のままにできません。 2.DHCP サーバから 固定 IP アドレスを PC に都度割り当てる場合、対象の PC に割り当てる IP アドレスをテキストボックスに入力します。これにより、バインドするサーバまたは PC が、再起動するたびに仮想固定 IP アドレスを取得します。
MAC アドレス：	バインドするサーバまたは PC 用の実固定 MAC アドレス (ネットワークカードに記載されているアドレス) を入力します。
名：	クライアントを識別するために、バインドするユーザー名またはユーザーのアドレスを入力します。最大文字数は 12 です。
有効：	この設定を有効の状態にします。
リストに追加：	設定や変更をリストに追加します。
選択した項目を削除：	選択したバインディングをリストから削除します。
追加：	新しいバインディングを追加します。

リストにある MAC アドレスによる不正な IP アドレスの使用をブロック：リストに追加した機器は、リストで設定した IP アドレス以外を使用するとインターネットに接続できなくなります。

新しい IP ユーザーを表示：

●バインディングのために管理者が MAC アドレスを 1 つずつ確認する手間が軽減されます。また、MAC アドレスを手動で入力すると、手作業のためミスが起こりがちです。このリストを確認することによって、トラフィックが発生しているものの、まだバインドされていないすべての MAC アドレスを管理者が確認できます。また、バインドされた特定の MAC アドレスがリストに表示されているのを管理者が知った場合は、ユーザーがプライベート IP アドレスを変更しているということになります。

名：	バインドするユーザー名またはユーザーのアドレスを入力します。最大文字数は 12 です。
有効：	バインドする項目を選択します。
送信：	設定を有効の状態にします。
全てを選択：	リストのすべての項目をバンディングに選択します。
再読込：	リストを更新します。
閉じる：	リストを閉じます。

VI.QoS（サービス品質）

QoS は、Quality of Service (サービス品質) の略です。主な機能として、いくつかのサービスと IP アドレスによるバンド幅の使用を制限してバンド幅を残す、ないし特定のアプリケーションまたはサービスを優先させることと、その他のユーザーがバンド幅を共有することを許可する、ないし安定性と信頼性に優れたネットワーク通信に万全を期すこと、この 2 つがあります。

6.1 バンド幅管理

6.1.1 ISP より提供された最大バンド幅

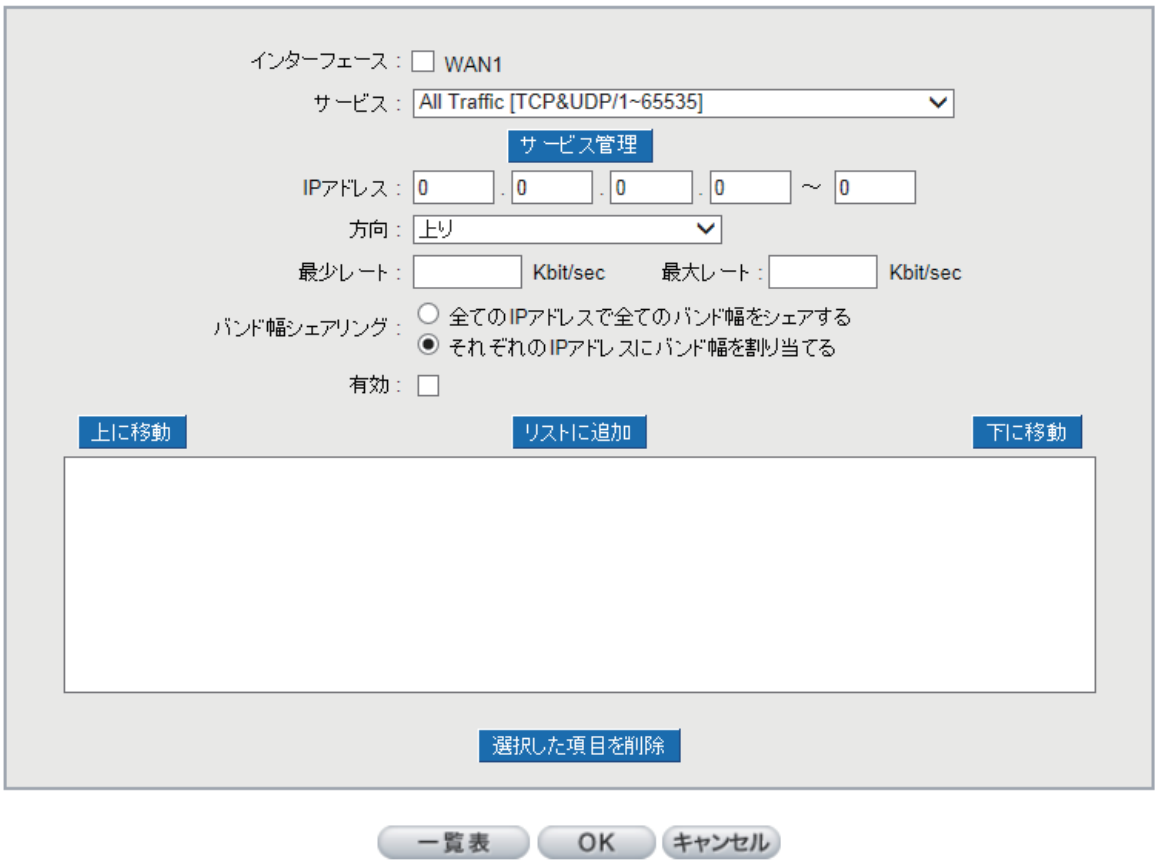
「WAN1」の WAN のバンド幅を入力するテキストボックスに、バンド幅の供給元に対してユーザーが申請した、上りと下りのバンド幅を入力します。バンド幅 QoS が、ユーザーが入力したデータに応じて計算を行います。言い換えると、WAN の実際の総バンド幅に応じて、各 IP アドレスとサービスポートの上りと下りの最小レートが保証されます。

注意！
この例での計算に使われる単位は Kbit です。ソフトウェアによっては、下り / 上りの速度の単位を KB で表示します。 1 KB は 8 Kbit になります。

6.1.2 QoS

レート制御：
ネットワーク管理者は、実際のバンド幅に応じて、各 IP アドレスまたは IP 範囲に対して、ハンド幅または使用率の制限を設定できます。ネットワーク管理者は、特定のサービスポートに対して、バンド幅制御を設定することもできます。また、内部サーバが存在する場合は、外部接続の保証バンド幅制御を設定できます。

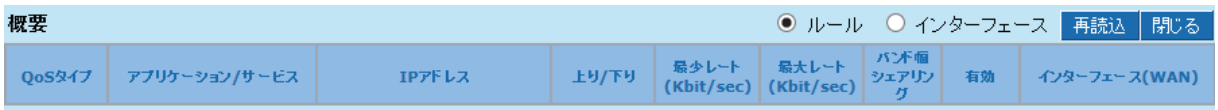
サービス品質



インターフェース :	どの WAN に対して QoS ルールを実行すべきか選択します。1 つのルールまたは複数のルールを選択できます。
サービス：	QoS ルールでどのバンド幅制御を設定するか選択します。各 IP アドレスのすべてのサービスのバンド幅を制御する場合は、「全て(TCP&UDP)1 ～ 65535」を選択します。FTP でアップロードやダウンロードを行うときのみ制御する必要がある場合は、「FTP Port 21 ～ 21」を選択します。サービスポート番号の初期設定リストを参照してください。
IP アドレス：	どのユーザーを制御するか選択します。1 つの IP アドレスのみを制限する場合は、「192.168.111.100 ～ 100」などの IP アドレスを入力します。ルールは、IP アドレス「192.168.111.100」のみを制御します。 IP 範囲を制御する場合は、「192.168.111.100 ～ 150」などの IP 範囲を入力します。ルールは、「192.168.111.100」から「192.168.111.150」までの IP アドレスを制御します。デバイスに接続している、すべてのイントラネットユーザーを制御する場合は、IP アドレスのテキストボックスに「0」を入力します。こうすると、すべてのイントラネットの IP アドレスが制限されます。QoS は、クラス B の範囲も制御できます。

方向：	上り：イントラネットの IP アドレスのアップロードバンド幅です。 下り：イントラネットの IP アドレスのダウンロードバンド幅です。 LAN 側のサービス (上り) : 外部接続用サーバがデバイス内に構築されている場合は、このオプションを使用して、外部からこのサーバに入ってくるトラフィックのバンド幅を制御します。 LAN 側のサービス (下り) : イントラネット内に Web サイトが存在する場合は、このオプションを使用して、外部からこのサーバに入ってくるアップロードバンド幅を制御します。
最小＆最大レート： Kbit/ 秒	最小バンド幅：このルールによって、利用可能な最小のバンド幅が保証されます。 最大バンド幅：このルールによって、利用可能な最大のバンド幅が制限されます。最大のバンド幅は、このルールの下で設定された上限値を超えることはありません。 注意！このルールでの計算に使われる単位は Kbit です。ソフトウェアによっては、ダウンロード / アップロードの速度の単位を KB で表示します。1 KB は 8 Kbit になります。
バンド幅シェアリング	全ての IP アドレスで全てのバンド幅をシェアする：このオプションを選択している場合は、すべての IP アドレスまたはサービスポートが、バンド幅の範囲 (最小から最大までのバンド幅) を共有します。 それぞれの IP アドレスにバンド幅を割り当てる：このオプションを選択している場合は、各 IP アドレスまたはサービスポートが、このバンド幅 (最小から最大) を持ちます。例えば、各 PC の IP アドレスに対してルールが設定されている場合は、各 PC の IP アドレスが同じバンド幅を持ちます。 注意：「バンド幅をシェアする」を選択している場合は、実際の使用条件に配慮し、バンド幅が小さ過ぎると、ネットワーク障害を引き起こす可能性のある不適切な設定を回避してください。例えば、FTP があまりにも多くのバンド幅を占有しないようにする場合には、「バンド幅をシェアする」を選択すると、FTP で如何に大量にダウンロードしても、占有バンド幅の総数は固定されています。
有効：	ルールを有効の状態にします。
リストに追加：	このルールをリストに追加します。
上に移動＆下に移動：	リストの一番下から一番上に向かって、QoS ルールが実行されます。言い換えると、リストの下に行くほど、実行優先順位が高くなります。優先順位に応じて、順番を入れ替えることができます。通常は、BT や eMule などの、制限する必要のあるサービスポートをリストの一番下に移動します。そして、特定の IP アドレスのルールをリストの上位に移動します。
選択した項目を削除：	サービスリストで選択したルールを削除します。
一覧表：	バンド幅に対して設定されたすべてのレート制御ルールを表示します。[編集] をクリックして変更します。
OK：	[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

一覧表：

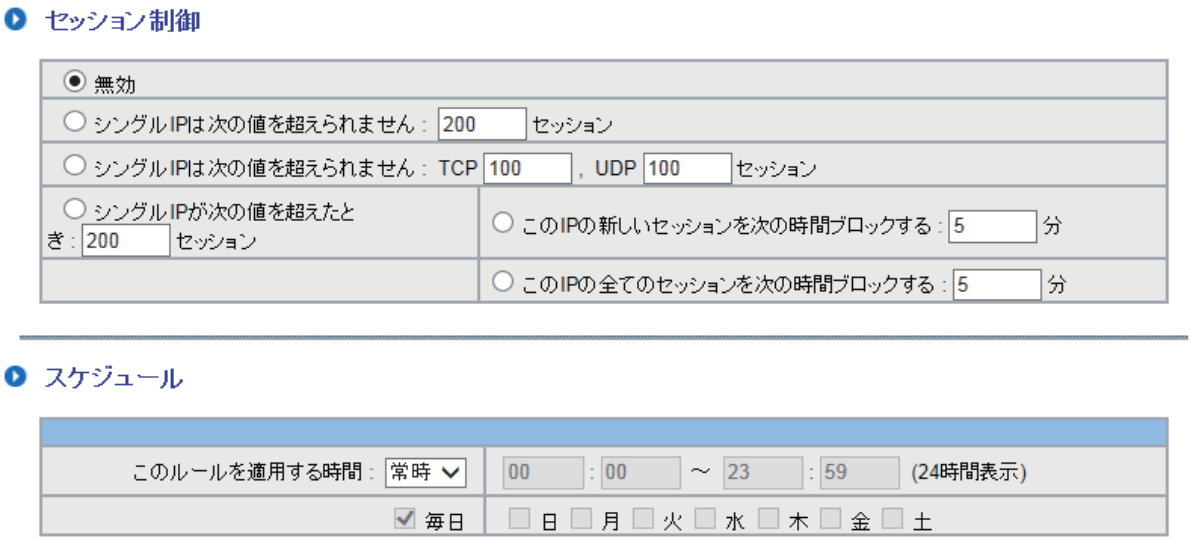


6.2 セッション制御

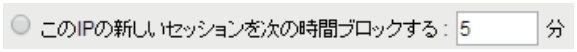
セッション管理は、イントラネット上の PC の最大許容同時セッション数を制御します。この機能は、BT、Thunder、eMule などの P2P ソフトウェアがイントラネット内で使用されていて、膨大な数のセッションを引き起こしているときに、接続数を管理するのにとても便利です。適切なセッション数制限を設定することで、P2P ソフトウェアが作成するセッション数を効果的に制御します。バンド幅使用を制限するのにも効果があります。

また、イントラネット上の PC が Worm.Blaster のようなウイルスに攻撃されて、膨大な数のセッションリクエストを送信する場合に、セッション制御によってそれも制限されます。

セッション制限とスケジュール：



無効：	ルールを無効の状態にします。
シングル IP は 次の値を超えられません：	外部からのイントラネット上の各 PC への最大セッション数を制限できます。外部からのセッション数が上限値に達すると、新しいセッションを作成するために、既存のセッションのいくつかを閉じます。例えば、BT や P2P をダウンロードに使用中にセッションが上限値を超えたときは、BT や P2P を閉じるまで、その他のサービスに接続できません。

シングル IP が次の値を超えたとき：	 この機能を選択している場合は、ユーザーのポートセッションが上限値に達すると、5 分間新しいセッションを開始できません。前回のセッションを閉じたとしても、設定時刻が終わるまで、新しいセッションを開始できません。  この機能を選択している場合は、ユーザーのポート接続が上限値に達すると、このユーザーが接続しているすべての回線が切断され、5 分間インターネットに接続できません。遅延時間が終わるまで、新しい接続を開始できません。
スケジュール：	「常時」を選択している場合は、ルールが 24 時間実行されます。「From…」を選択している場合は、設定した時刻範囲に応じてルールが実行されます。例えば、時刻制御が、月曜日から金曜日の午前 8:00 から午後 6:00 までの場合は、以下の図を参照して、ルールを設定できます。
OK：	[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

免除されたサービスポートまたは IP アドレス

サービス：	サービスポートを選択します。
送信元 IP：	IP 範囲または IP グループを入力します。
有効：	ルールを有効の状態にします。

リストに追加：	このルールをリストに追加します。
選択した項目を削除：	サービスリストで選択したルールを削除します。
OK：	[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

VII. ファイアウォール

本章では、ネットワークセキュリティに万全を期すためのファイアウォールの全体ポリシー、アクセスルール、コンテンツフィルタ設定について説明します。

7.1 全体ポリシー

初期設定では、ファイアウォールは有効の状態になっています。ファイアウォールが無効に設定されている場合は、SPI や DoS などの機能や、アウトバウンドパケットの応答が自動的に無効になります。その間は、リモート管理機能が有効になります。ネットワークアクセスルールとコンテンツフィルタは無効になります。

ファイアウォール：	ファイアウォールを有効 / 無効の状態にします。
SPI (Statefle Packet Inspection)：	パケット自動認証検出技術を有効の状態にします。ファイアウォールは、主にネットワーク層で動作します。各接続の動的認証を実行して、アプリケーション手順に対してアラーム機能も実行します。その間に、パケット認証ファイアウォールが、非標準の通信プロトコルを使用している接続を拒否します。
DoS (Denial of Service)：	SYN フラッド攻撃、Smurf 攻撃や、DoS 攻撃、Ping of Death 攻撃、IP スプーフィング攻撃などの Dos 攻撃を防ぎます。
WAN 側のリクエストをブロック：	有効に設定された場合は、接続中のアウトバウンド ICMP と異常パケット応答をシャットダウンします。WAN 側の IP アドレスに対して外部から ping を実行しようとした場合は、初期設定値を有効にして、アウトバウンド応答を拒否するよう設定されているため、実行できません。
リモート管理：	インターネットにリモート接続して、デバイスの Web ベースの UI を表示するには、この機能を有効の状態にします。リモートブラウザ IP のフィールドに、デバイスの有効な外部 IP アドレスを (WAN 側の IP アドレス) を入力して、可変ポート制御の初期設定を変更します (初期設定は「80」で、変更可能です)。

マルチキャストパススルー：	たくさんの音声 / 画像ストリーミングメディアがネットワークに存在しています。ブロードキャスティングによって、クライアントがこのタイプのパケットメッセージフォーマットを受け取ることができます。初期設定は、無効の状態になっています。
ARP ウイルス攻撃の防御：	この機能は、PC の通信障害を引き起こす APR スプーフィングの攻撃からイントラネットを守るためのものです。この APR ウイルス攻撃は、インターネットカフェで発生することが多いです。攻撃を受けると、すべてのオンライン上の PC がすぐさま切断されるか、オンライン接続に失敗します。この機能を有効にすると、このタイプのウイルスの攻撃を防ぎます。

7.2 アクセスルール

設定のオン / オフを切り替えて、パケットがインターネットにアクセスするのを許可したり禁止したりできます。社内から社外、社外から社内など、異なるネットワークアクセスルールの設定を選択できます。IP アドレスと通信ポート番号に対して、異なるパケットを設定して、インターネットアクセスルールをフィルタできます。

ネットワークアクセスルールは、IP アドレス、送信先 IP アドレスと、IP 通信プロトコルのステータスを追うことで、ネットワークパケットトラフィックを管理して、ファイアウォールによってアクセスが許可されているか確認します。

7.2.1 デフォルトルール

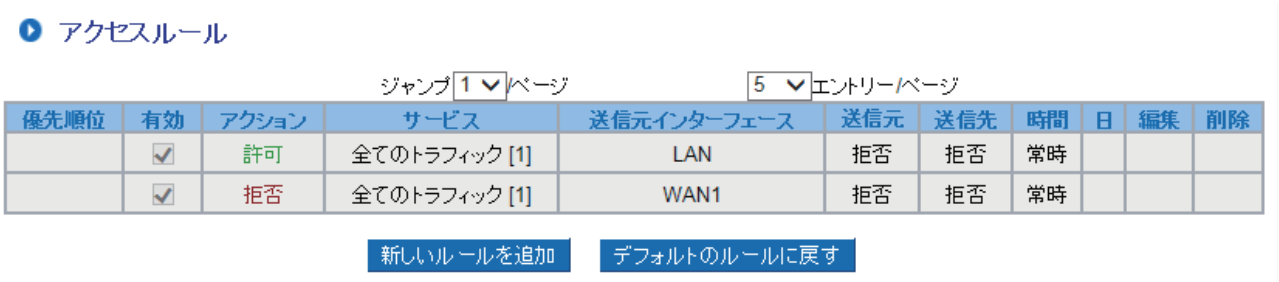
デバイスは、ユーザーとの親和性に優れたネットワークアクセス制限ツールを備えています。ユーザーがネットワークアクセスルールを定義できます。ネットワークを有効 / 無効の状態にするかを選択して、すべてのインターネットアクセスを保護できます。以下に、インターネットアクセスルールを説明します：

* 初期設定では、LAN からのすべてのトラフィックが許可されています。
* 初期設定では、LAN からのすべてのトラフィックが禁止されています。

アクセスルールを定義して、デフォルトルールの規定値以上の設定を行うことができます。ただし、以下の 4 つの追加サービス項目は常にオンになっていて、ユーザーが定義のするその他の設定の影響を受けません。

* 初期設定では、HTTP サービス (LAN からデバイス) は、オンになっています (管理のため)。
* 初期設定では、DHCP サービス (LAN からデバイス) は、オンになっています (自動 IP アドレス取得のため)

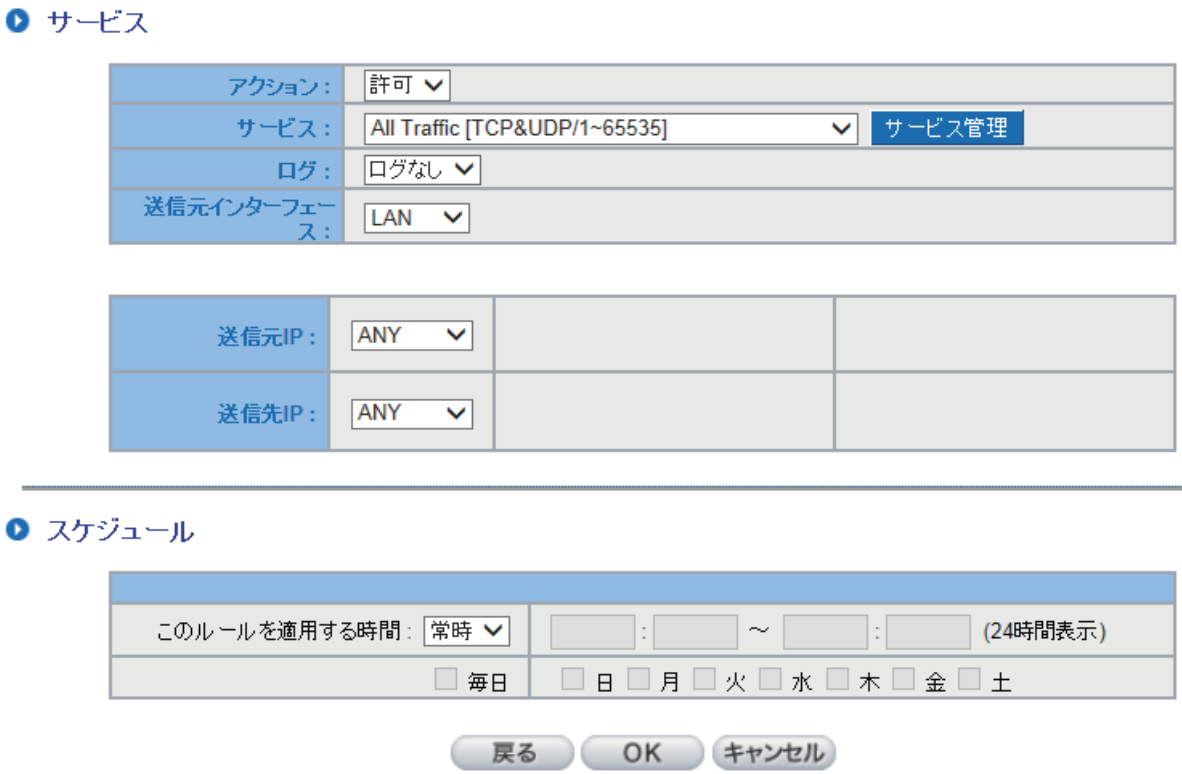
* 初期設定では、DNS サービス (LAN からデバイス) は、オンになっています (DNS サービス分析のため)。
* 初期設定では、Ping サービス (LAN からデバイス) は、オンになっています (接続とテストのため)。



デフォルトルールに加えて、すべてのネットワークアクセスルールが、上記のとおり表示されます。ユーザーは、各ネットワークアクセスルールの優先順位に従うか、自分で優先順位を定義することができます。デバイスは、ルールの優先順位に 1 つずつ従いますので、すべてのルールの優先順位が設定ルールに則するようにします。

編集：	ネットワークアクセスルールの項目を定義します。
削除：	項目を削除します。
新しいルールを追加：	新しいネットワークアクセスルールを作成します。
デフォルトのルールに戻す：	すべての設定を初期設定に戻し、ユーザー定義設定をすべて削除します。

7.2.2 新しいルールを追加する

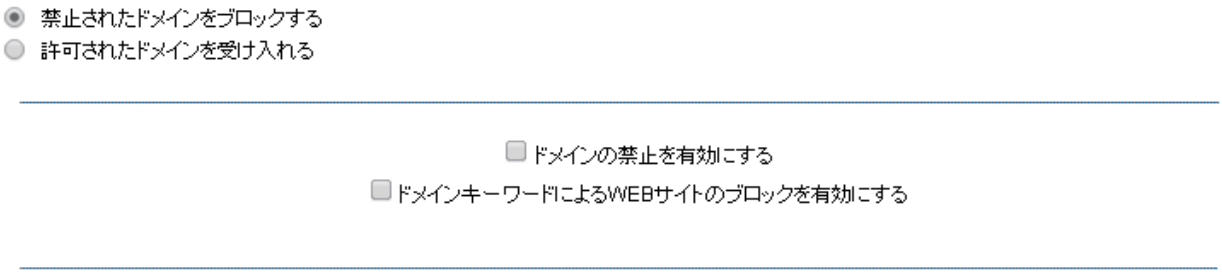


アクション：	許可：この制御ルールを順守するパケットの通過を許可します。 拒否：この制御ルールを順守しないパケットの通過を拒否します。
サービス：	ドロップダウンメニューから、許可するサービスや、許可しないサービスを選択します。
サービス管理：	管理対象サービスがドロップダウンメニューにない場合は、[サービス管理] をクリックして、新しいサービスを追加します。 ポップアップウィンドウで、サービス名、通信プロトコル、ポートを入力して、[リストに追加] ボタンをクリックして新しいサービスを追加します。
ログ：	ログなし：ログが記録されていません。 Create Log when matched: イベントがログに記録されます。
送信元インターフェース：	ユーザーに許可されているいないにかかわらず、送信元ポートを選択します (例：LAN、WAN、任意)。ドロップダウンメニューから選択します。
送信元 IP：	送信元 IP 範囲を選択します (例：任意、単一、範囲、プリセット IP グループ名)。「単一」または「範囲」を選択している場合、単一 IP アドレスまたはセッション内の IP アドレスを入力します。
送信先 IP：	送信先 IP 範囲 (任意、単一、範囲、プリセット IP グループ名など) を選択します。「単一」または「範囲」を選択している場合、単一 IP アドレスまたはセッション内の IP アドレスを入力します。
スケジュール：	「常時」を選択して、24 時間体制でルールを適用します。「From」を選択すると、設定された時刻に応じて、操作を実行します。
このルールを適用する時間：	「常時」を選択して、24 時間体制でルールを適用します。「From」を選択している場合、実行開始時刻が以下のとおり表示されます。

… ～ … :	この制御ルールには時間制限があります。設定方法は、08:00 から 18:00 (午前 8 時から午後 6 時) など、24 時間表示になっています。
Day Control:	「毎日」を選択すると、毎日この時間帯が制御されます。週の特定曜日のみを制御する場合は、制御対象曜日を直接選択します。
OK :	[OK] をクリックして、設定を保存します。
キャンセル :	変更せずに終了するには、[キャンセル] をクリックします。

7.3 URL フィルタ

デバイスは、特定の禁止されたドメインをブロックするモードと、特定の Web ページにアクセスを許可するモードの、2 つの Web ページ制限モードに対応しています。2 つのうち、選択できるのは 1 つだけです。

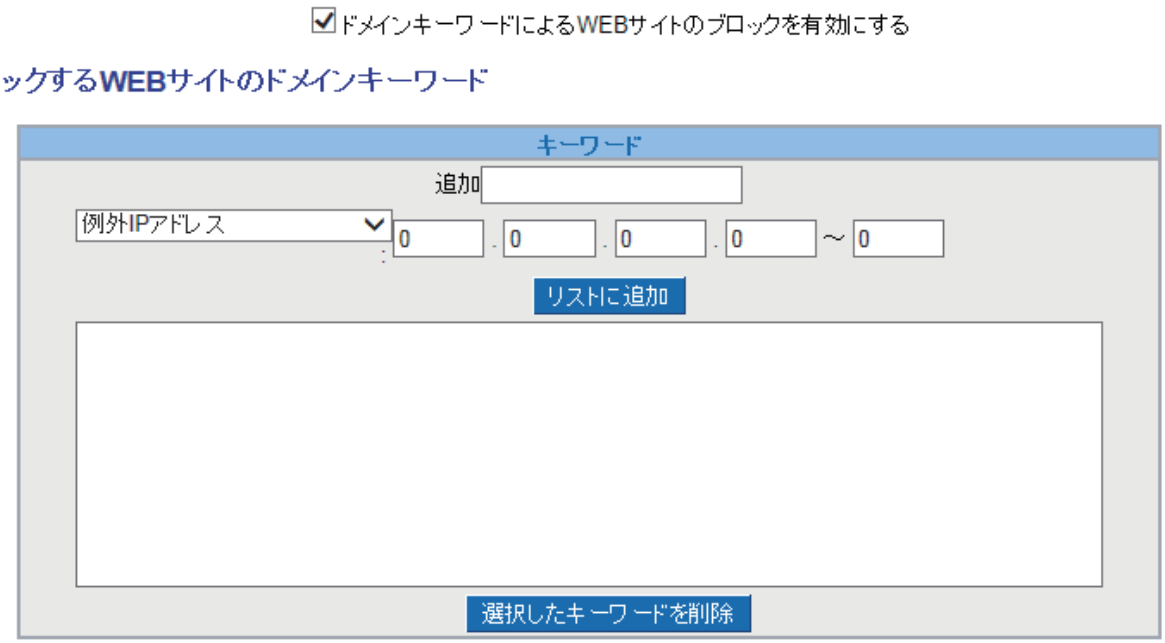


禁止されたドメインをブロックする

www.sex.com など、Web サイトを完全な形で入力します。

追加：	www.playboy.com など、制御する Web サイトを入力します。
リストに追加：	[リストに追加] をクリックして、制御する新しい Web サイトを作成します。
選択したドメインを削除：	複数の制御された Web サイトをクリックして選択してから、このオプションをクリックして削除します。

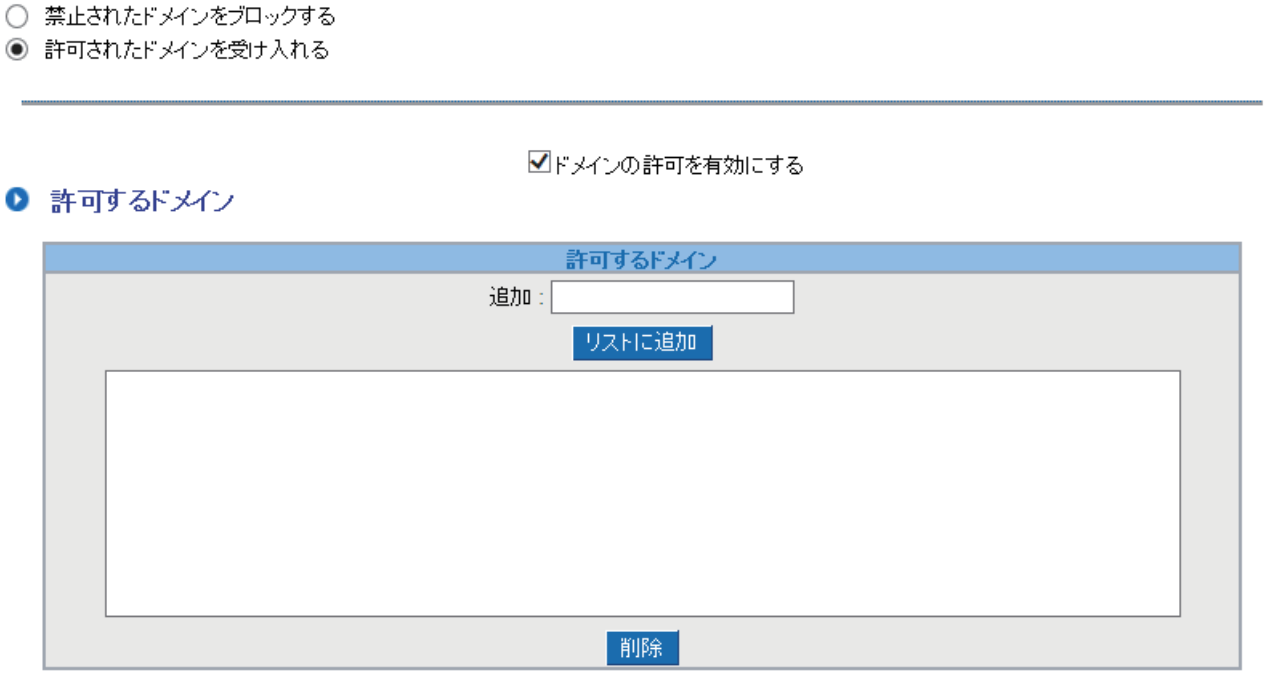
キーワードでブロックされた WEB サイト：



ドメインキーワードによる WEB サイトのブロックを有効にする：	クリックして、この機能を有効の状態にします。初期設定は、無効の状態になっています。例えば：「sex」というストリングを入力した場合は、「sex」が含まれている Web サイトがブロックされます。
Keywords（Only for Englishkeyword）：	キーワードを入力します。
リストに追加：	この新しいサービス項目コンテンツをリストに追加します。
選択した項目を削除：	サービス項目コンテンツをリストから削除します。
OK：	[OK] をクリックして、変更したパラメーターを保存します。
キャンセル：	[キャンセル] をクリックして、パラメーターに行ったすべての変更をキャンセルします。

許可されたドメインを受け入れる

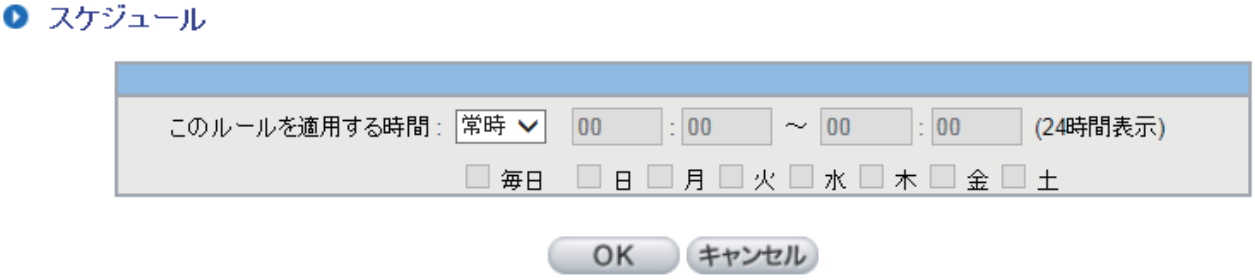
企業や学校によっては、社員や学生が、特定の Web サイトへのアクセスのみを許可されます。これがこの機能の目的です。



ドメインの許可を有効にする：	機能を有効の状態にします。初期設定は、「無効」の状態になっています。
追加：	www.google.com などの許可されたドメイン名を入力します。
リストに追加：	ルールをリストに追加します。
削除：	一つあるいは複数のルールを選択してから、クリックして削除します。

URL フィルタスケジュール

「常時」を選択して、24 時間体制でルールを適用します。「From」を選択すると、設定された時刻に応じて、操作を実行します。例えば、時刻制御が、月曜日から金曜日の午前 8:00 から午後 6:00 までの場合は、以下の図の例に従って、操作を制御します。



常時：	「常時」を選択して、24 時間体制でルールを適用します。「From」を選択すると、設定された時刻に応じて、操作を実行します。
…to…：	「常時」を選択して、24 時間体制でルールを適用します。 「From」を選択している場合、実行開始時刻が以下のとおり表示されます。
Day Control:	この制御ルールには時間制限があります。設定方法は、08:00 から 18:00 (午前 8 時から午後 6 時) など、24 時間表示になっています。

VIII. 拡張機能

8.1 DMZ ホスト／ポート範囲転送

8.1.1 DMZ ホスト

NAT モードが有効なときは、ネットワークゲームなど、仮想 IP アドレスに対応していないアプリケーションの使用が必要となることがあります。 デバイスの WAN 側の実 IP アドレスを、以下のとおり、イントラネットの仮想 IP アドレスに直接マッピングしてください：

「DMZ ホスト」機能を選択している場合は、この機能をキャンセルするには、「DMZ プライベート IP アドレス」で「0」を入力します。これで、この機能を閉じます。

変更が完了したら、[OK] をクリックして、ネットワーク構成への変更を保存するか、[キャンセル] をクリックして、変更せずに終了します。

8.1.2 ポート範囲フォワーディング

ポートフォワーディング仮想ホストを設定する：サーバの機能 (WWW、FTP、メールなどの外部サービス用サーバ) がネットワークに含まれている場合、ファイアウォール機能を使用して、ホストを仮想ホストとして設定し、実 IP アドレス (インターネットの IP アドレス) をポート 80 (WWW のサービスポートはポート 80 です) に変換して、内部サーバに直接アクセスしてください。設定ページで、「192.168.111.50」や、ポート 80 などの Web サーバのアドレスを設定している場合は、「http://211.243.220.43.」などのデバイスの実 IP アドレスを入力して、インターネットからこの Web ページにアクセスします。

この時点で、デバイスの実 IP アドレスが、ポート 80 によって「192.168.111.50」に変換され、Web ページにアクセスします。

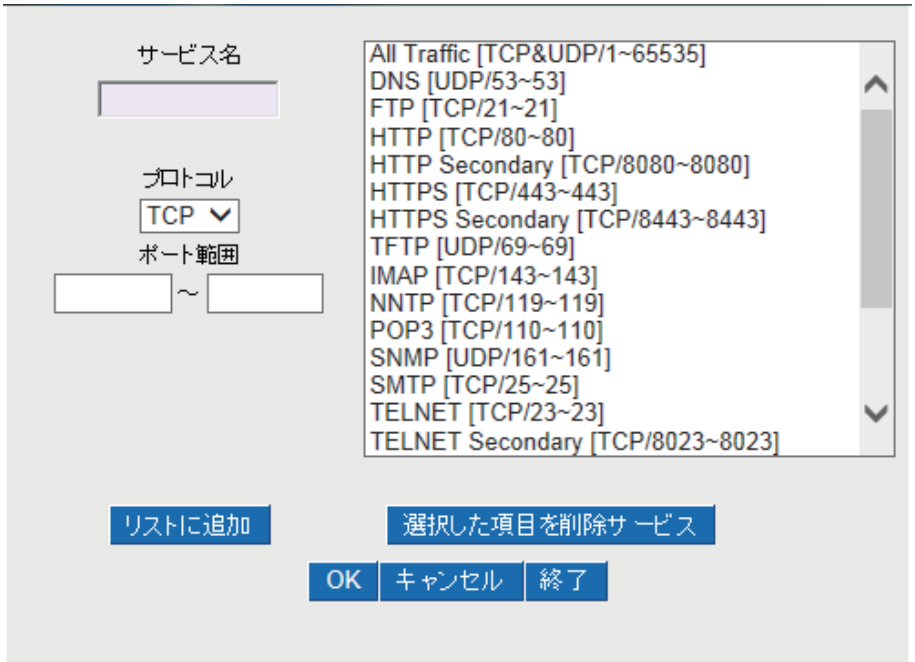
同様に、その他のサービスを設定するには、サーバの TCP または UDP ポート番号と仮想ホストの IP アドレスを入力します。

サービス：	このオプションで、有効にする対象となる仮想ホストのサービスポートのデフォルトリストを選択します。 例：「All (TCP&UDP) 0 ～ 65535, 80 (80~80) for WWW」や「21 ～ 21 for FTP」。サービスポートの初期設定リストを参照してください。

IP アドレス：	仮想ホストの IP アドレスを入力します。
インターフェース :	WAN ポートを選択します。
有効：	この機能を有効の状態にします。
サービス管理：	サービスポートのリストから、サービスポートを追加 / 削除します。
リストに追加：	アクティブなサービスコンテンツを追加します。

サービス管理

上記で説明したリストにあるサービスは使用頻度の高いサービスですが、有効にする対象となるサービスがリストにない場合は、「サービス管理」を使用して、以下のとおり、ポートを追加 / 削除してください：

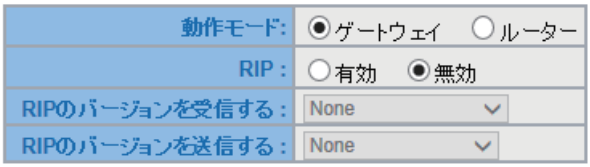


サービス名：	E-donkey など、リストにある、有効にする対象となるサービスポート名を入力します。
プロトコル：	サービスポートに TCP または UDP のどちらかを選択します。
ポート範囲：	この機能を有効にするには、有効にする対象となるサービスポートの場所の範囲を入力します。
リストに追加：	サービスをサービスリストに追加します。
選択した項目を削除：	選択したサービスを削除します。
OK：	[OK] ボタンをクリックして変更を保存します。
キャンセル：	[キャンセル] ボタンをクリックして変更をキャンセルします。[OK] ボタンをクリックする前であれば、有効となります。
終了：	この設定ウィンドウを閉じます。

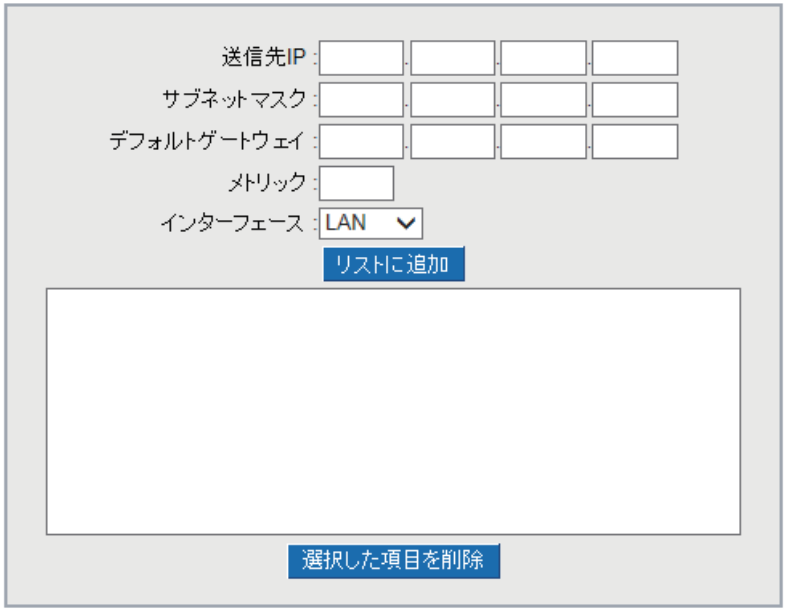
8.2 ルーティング

本章では、動的ルーティング情報プロトコルと静的ルーティング情報プロトコルについて説明します。

動的ルーティング



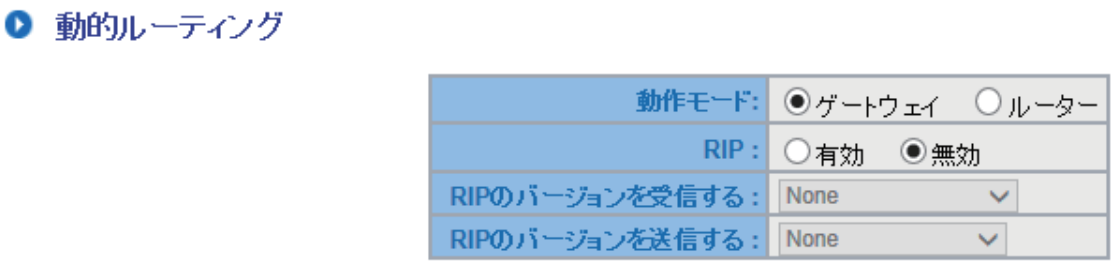
静的ルーティング



8.2.1 動的ルーティング

ルーティング情報プロトコル (Routing Information Protocol) の略は「RIP」です。IP 環境には、RIP I と RIP II の 2 つのタイプの RIP があります。通常は、1 つのルータのみがネットワークに存在するため、普段は静的ルーティングのみを使用します。複数のルータがネットワークに存在するときに RIP を使用します。管理者がパスリストを 1 つずつすべてのルータに割り当てたくない場合に、RIP がパスを更新します。

RIP はとても単純なルーティングプロトコルです。ディスタンスベクタ方式を使用しています。ディスタンスベクタ方式によって、実際のセッション速度ではなく、ルータ数に応じて通信距離が決定されます。従って、最速のルータを通過するパスではなく、最小数のルータを通過するパスが選択されることがあります。

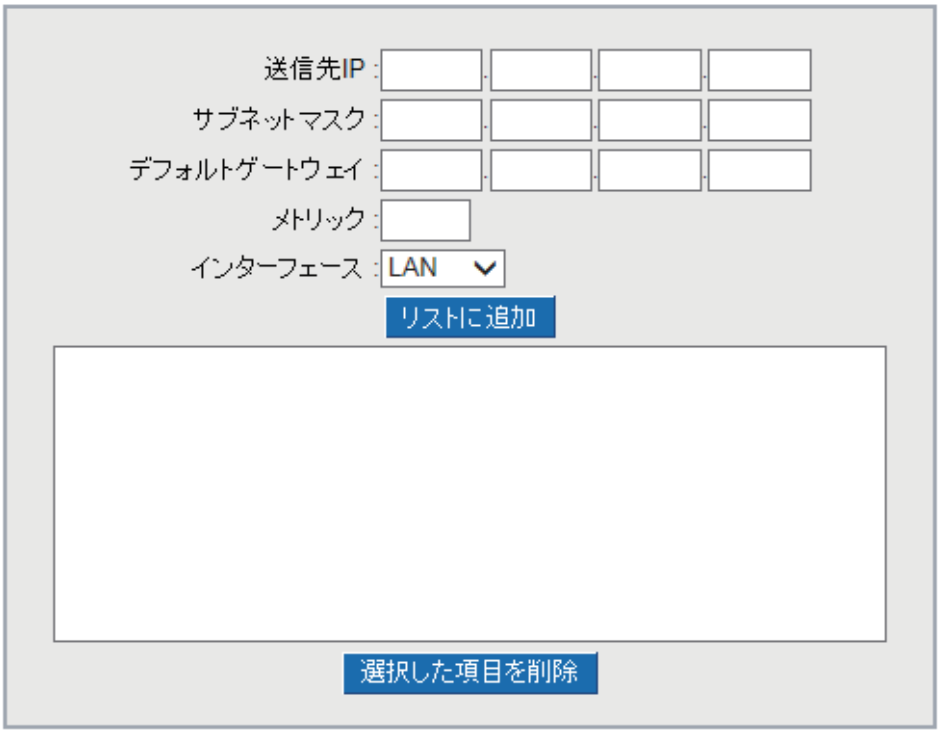


動作モード：	デバイスのワーキングモードを選択します：「ゲートウェイ」モードまたは「ルータ」モード
RIP:	[有効] をクリックして、RIP 機能を有効の状態にします。
RIP のバージョンを受信する：	アップ / ダウンボタンを使用して、「None」、「RIPv1」、「RIPv2」、「Both RIPv1 and v2」のうち、1 つを動的 RIP を送信するための「TX」機能として選択します。
RIP のバージョンを送信する：	アップ / ダウンボタンを使用して、「None」、「RIPv1」、「RIPv2-Broadcast」、「RIPv2-Multicast」のうち、1 つを動的 RIP を受信するための「RX」機能として選択します。

8.2.2 静的ルーティング

●複数のルータと IP サブネットが存在するときは、デバイスのルーティングモードを静的ルーティングとして設定します。静的ルーティングによって、異なるネットワークノードが必要なパスを自動的に検索することができます。異なるネットワークノードが互いにアクセスできるようにもなります。(図中の) [一覧表] ボタンをクリックして、現在のルーティング一覧を表示します。

静的ルーティング



送信先 IP： サブネットマスク：	リモートネットワーク IP の場所と、ルーティングするサブネットを入力します。例えば、IP として「192.168.2.0」を、サブネットとして「255.255.255.0」を入力します。
デフォルトゲートウェイ：	ルーティングするネットワークノードのデフォルトゲートウェイの場所です。
メトリック：	IP ルータレイヤ数です。デバイスに 2 つのルータが存在する場合は、ルートレイヤに「2」を入力します。初期設定は「1」です (最大は 15 です)。
インターフェース :	ネットワークを接続する場所として、「WAN」ポートまたは「LAN」ポートを選択します。
リストに追加：	ルーティングルールをリストに追加します。
選択した項目を削除：	選択したルーティングルールをリストから削除します。
一覧表：	現在のルーティングテーブルを表示します。
OK：	[OK] をクリックして、ネットワーク設定の変更を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

8.3 One-to-One NAT

デバイスと ATU-R の両方に、実 IP アドレス 1 つのみが必要なため、ISP (インターネットサービスプロバイダ) が複数の実 IP アドレス (8 つ以上の ADSL の固定 IP アドレスなど) を発行した場合は、1 つを除く残りの実 IP アドレスをイントラネット上の PC の仮想 IP アドレスにマッピングできます。これらの PC は、イントラネットのプライベート IP アドレスを使

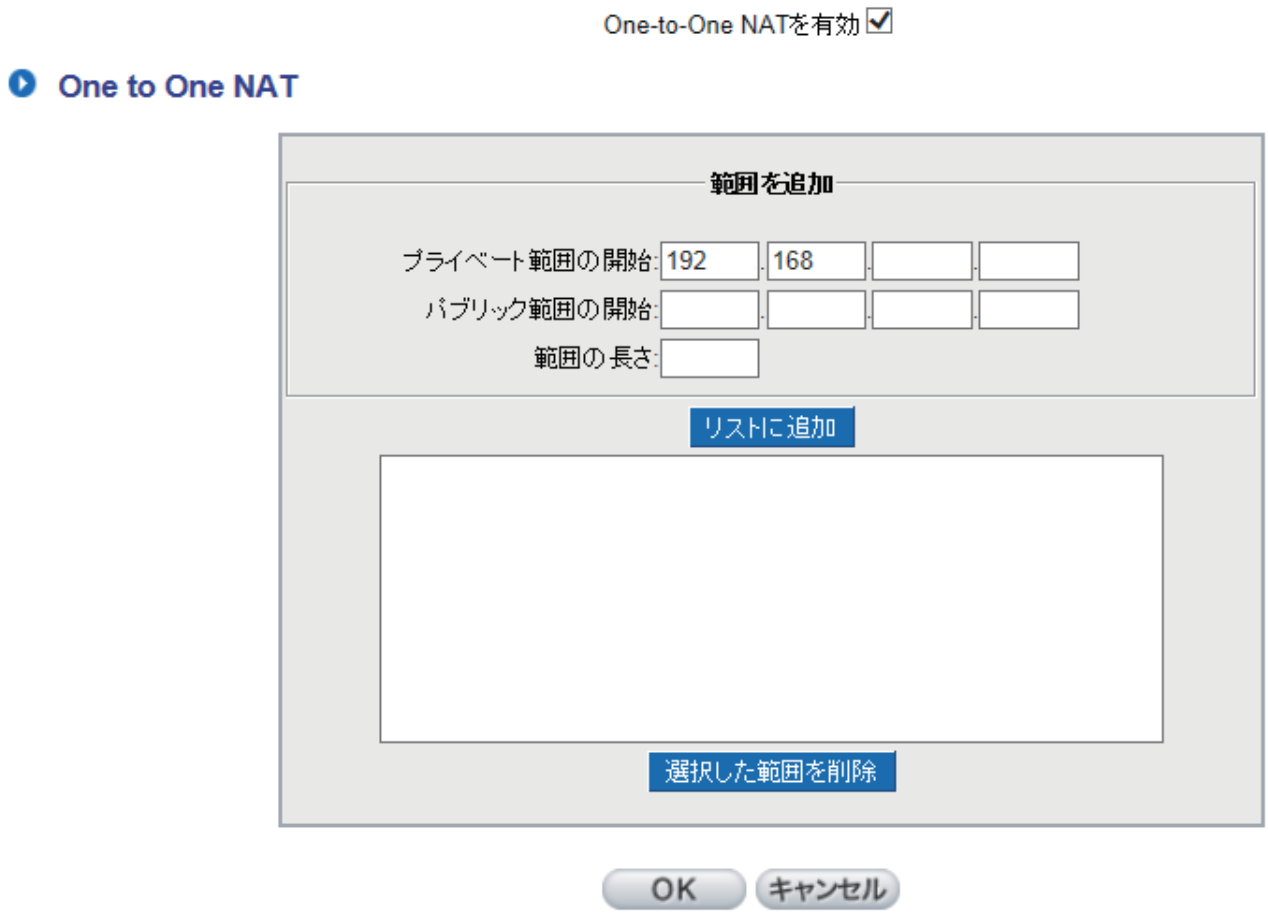
用していますが、One-to-One NAT マッピングを実行すると、各自にそれぞれパブリック IP アドレスが割り当てられます。

●例えば、パブリック IP アドレスを必要とする Web サーバが 2 つある場合は、管理者がいくつかのパブリック IP アドレスを、社内のプライベート IP アドレスに直接マッピングすることができます。

例：ユーザーは「210.11.1.1」から「210.11.1.5」までの 5 つの IP アドレスを使用できます。そのうちの 1 つ、「210.11.1.1」を、WAN 側の実 IP アドレスとして設定し、NAT で使用しています。その他 4 つの実 IP アドレスを、以下のとおり、マルチ DMZ の 実 IP アドレスとしてそれぞれ設定できます：

210.11.1.2 → 192.168.111.3
210.11.1.3 → 192.168.111.4
210.11.1.4 → 192.168.111.5
210.11.1.5 → 192.168.111.6

注意！
デバイスの WAN 側の IP アドレスを、One-to-One NAT の IP 構成に含めることはできません。



One-to-One NAT を　有効：	One-to-One NAT 機能を有効 / 無効の状態にします (このオプションをチェックして、機能を有効の状態にします)。
プライベート範囲の開始：	イントラネットの One-to-One NAT 機能のプライベート IP アドレスを入力します。
パブリック範囲の開始：	インターネットの One-to-One NAT 機能のパブリック IP アドレスを入力します。
範囲の長さ：	インターネットにおける実際の IP アドレスの最終的な IP アドレス数です (WAN 側の IP アドレスは含めません)。
リストに追加：	この設定を、One-to-One NAT リストに追加します。
選択した項目を削除：	選択した One-to-One NAT リストを削除します。
OK：	[OK] をクリックして、ネットワーク構成の変更を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

注意！
One-to-One NAT モードは、ファイアウォールのワーキングモードを変更します。この機能が設定された場合は、LAN ポートにマッピングされているインターネットの IP サーバないし PC が インターネットに公開されます。インターネットユーザーが One-to-One NAT サーバないし PC に頻繁に接続するのを回避するには、ファイアウォールに説明するとおり、適切なアクセス拒否ルールを設定してください。

8.4 DDNS：ダイナミックドメインネームサービス

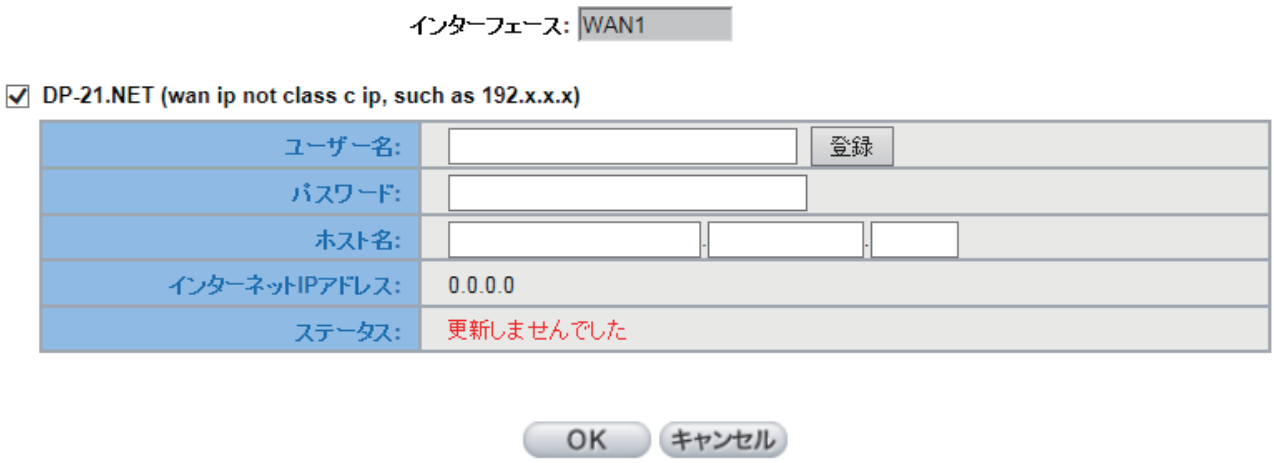
DDNS は、「DP-21」の動的 Web アドレス転送に対応しています。動的 IP アドレスで作成された Web サイトへの VPN 接続と、動的 IP リモートコントロールに使用します。例えば、ADSL の PPPoE タイムベースシステムの実 IP アドレス、ないしケーブルモデムの実 IP アドレスが、ときどき変更されます。Web サイトなどのサービスを作成したいユーザーのために、この問題を解決する目的で、動的 Web アドレス転送の機能を提供しています。www.dp-21.net からこのサービスを適用できます。

また、DDNS サーバが安定していないという問題を解決するために、デバイスが、異なるサービスの動的 IP アドレスを同時に更新することができます。

DDNS設定

インターフェース	ステータス	ホスト名	設定.
WAN1	DP_21 無効	DP_21:---	編集

設定を編集する「WAN」ポートを選択します。ハイパーリンクをクリックして、設定画面に入り、設定を編集します。



インターフェース	ユーザーが選択した WAN ポートです。
DDNS	「DP-21.NET」の左にあるチェックボックスをクリックします。
ユーザー名	DDNS に設定された名前です。 「abc.dp-21.net」など、Web サイトのアドレスを、DP-21. ユーザー名として完全な形で入力します。
パスワード	DDNS に設定されたパスワードです。
ホスト名	DDNS から適用した Web サイトのアドレスを入力します。 例えば、「abc.dp-21.net」と入力します。
インターネット IP アドレス	ISP (インターネットサービスプロバイダ) が発行した実動的 IP アドレスを入力します。
ステータス	DDNS によって更新された、現在の IP 機能のステータスです。
OK	変更が完了したら、[OK] をクリックして、ネットワーク設定への変更を保存します。
キャンセル	変更せずに終了するには、[キャンセル] をクリックします。

8.5 MAC クローン

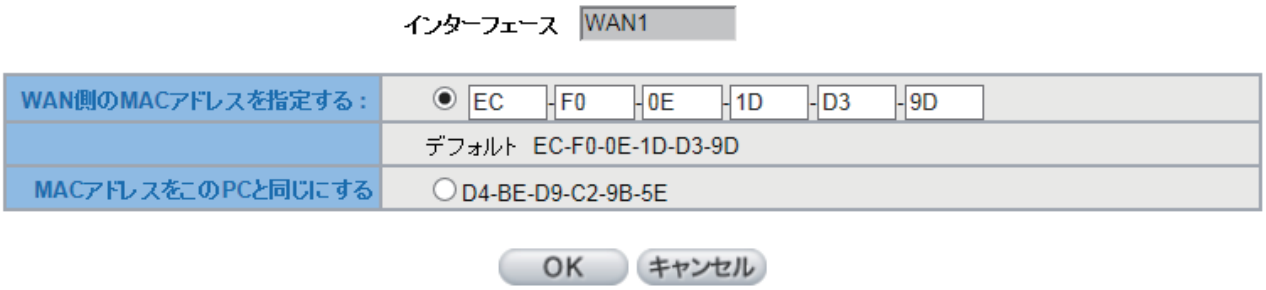
ISP (インターネットサービスプロバイダ) が、おもにケーブルモードのユーザーに適している、IP アドレス配信用の固定 MAC アドレス (ネットワークカードの物理アドレス) を要求することがあります。ネットワークカードの物理アドレス (MAC アドレス：00-xx-xx-xx-xx-xx) をこの画面で入力します。デバイスが、ISP (インターネットサービスプロバイダ) から IP アドレスを要求するときに、この MAC アドレスを適用します。

MACクローン

インターフェース	MACアドレス	設定.
WAN1	EC-F0-0E-1D-D3-9D	編集

設定を編集する WAN ポートを選択します。ハイパーリンクをクリックして、設定画面に入り、設定を編集します。MAC アドレスを手動で入力します。[OK] をクリックして、設定を保存します。設定を削除するには、[キャンセル] をクリックします。

MAC アドレスの初期設定は WAN 側の MAC アドレスです。

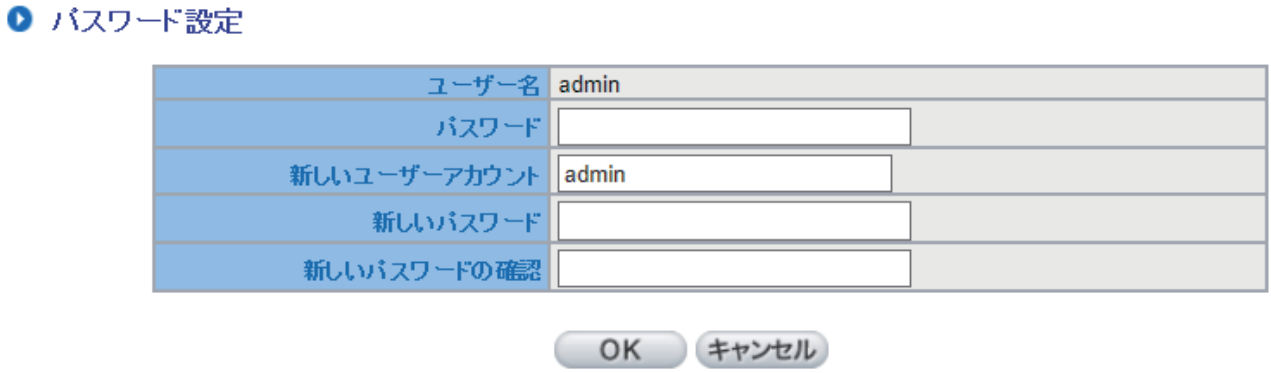


IX. システムツール

本章では、デバイスを制御するための管理ツールと、ネットワーク接続をテストするための管理ツールについて説明します。

9.1 パスワード設定

ルータ設定ウィンドウにログインするたびに、パスワードを入力する必要があります。ルータのユーザー名とパスワードの初期設定は、それぞれ「admin」と「password」です。セキュリティ上、最初のログイン後にパスワードを変更してください。パスワードを安全なものにしてください。そうでない場合は、ルータにログインできません。リセットボタンを 10 秒以上押すと、ルータを初期設定に戻せます。

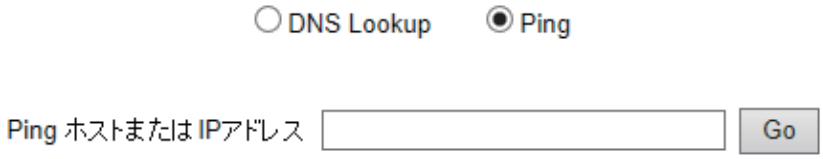


ユーザー名：	初期設定は「admin」です。
パスワード：	オリジナルパスワードを入力します (初期設定は「password」です)。
新しいユーザーアカウント：	新しいユーザー名を入力します (例：「planex」)。
新しいパスワード：	新しいパスワードを入力します。
新しいパスワードの確認：	確認のため、新しいパスワードをもう一度入力します。
OK：	[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。[OK] をクリックして、設定を保存する前であれば、有効となります。

ユーザー名とパスワードをすでに変更している場合は、現在のユーザー名とパスワードでログインし、ユーザー名とパスワードを初期設定に戻す必要がある場合は、「admin」を新しいユーザー名として、「password」を新しいパスワードとして入力します。

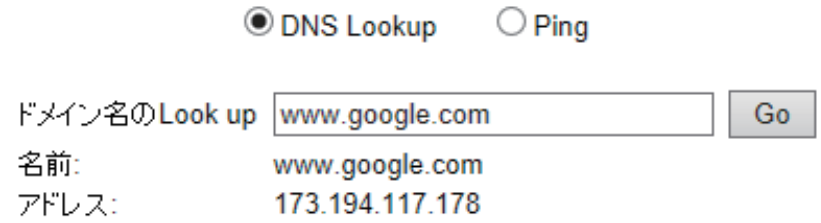
9.2 診断

デバイスは、ユーザーがネットワーク関連の問題を解決するのに役に立つ、かんたんなオンラインネットワーク診断ツールを提供しています。このツールには、DNS Lookup (ドメイン名照会テスト) と Ping (パケット送受信テスト) が含まれています。

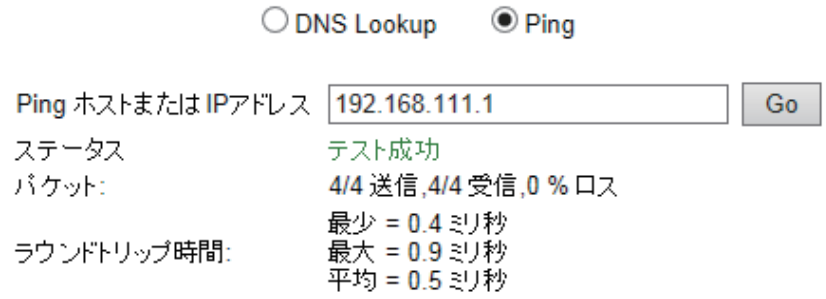


DNS Lookup

このテスト画面で、テスト実施対象のネットワークのホスト名を入入力します。例えば、www.google.com と入力して、[Ｇｏ] をクリックして、テストを開始します。結果はこのページに表示されます。



Ping



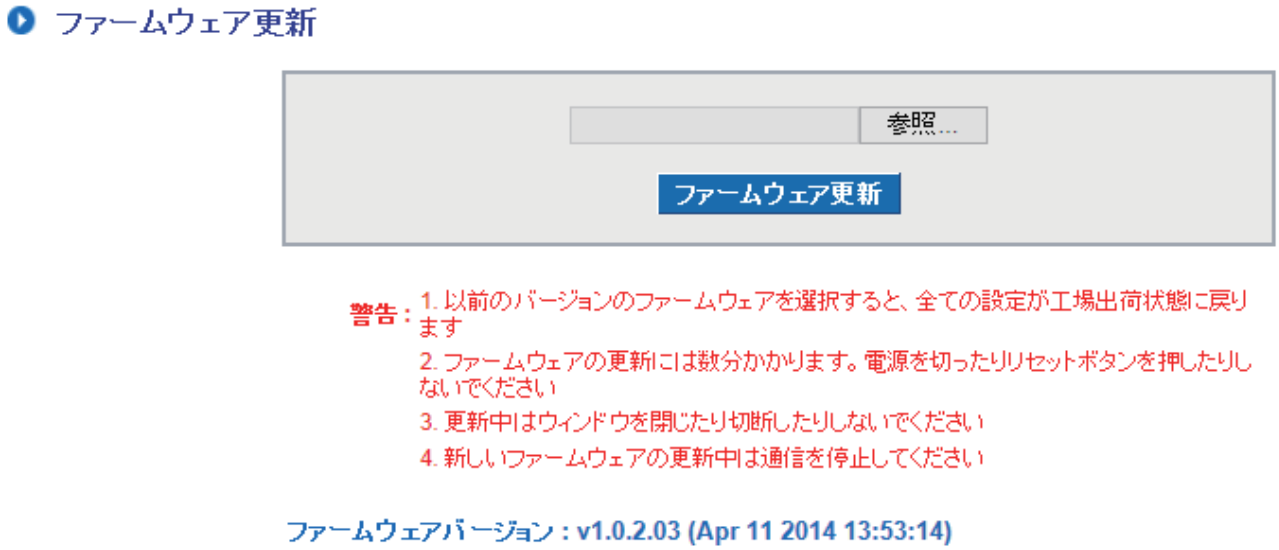
この項目で、アウトバウンドセッションの現在の状況がわかり、オンライン上に PC が存在するか確認できます。

このテスト画面で、「192.168.5.20」など、テスト実施対象のホストの IP アドレスを入力します。[Go] をクリックして、テストを開始します。結果はこのページに表示されます。

9.3 ファームウェアの更新

●「ファームウェア更新」ページで、デバイスのファームウェアを直接アップグレードできます。すべてのソフトウェアバージョン情報をあらかじめ確認してください。ソフトウェアのファイルを検索し、「今すぐファームウェア更新」をクリックして、指定したファイルのアップグレードを完了します。

注意！
ファームウェアをアップグレードする前に、警告をお読みください。
アップグレード中は、このページを閉じないでください。ページを閉じた場合、アップグレードに失敗します。



警告：1. 以前のバージョンのファームウェアを選択すると、すべての設定が工場出荷状態に戻ります。
2. ファームウェアの更新には数分かかります。電源を切ったりリセットボタンを押したりしないでください。
3. 更新中はウィンドウを閉じたり切断したりしないでください。
4. 新しいファームウェアの更新中は通信を停止してください。

9.4 設定のバックアップ

設定ファイルをインポート：

パラメーター設定のすべてのバックアップ内容をデバイスに統合します。アップグレードする前に、すべてのソフトウェアバージョン情報を確認してください。バックアップのパラメーターファイル「config.exp」を検索します。ファイルを選択し、「インポート」をクリックして、ファイルをインポートします。

設定ファイルをエクスポート：

すべてのパラメーター設定をバックアップします。「エクスポート」をクリックして、保存場所を選び、「config.exp」ファイルを保存します。

9.5 SNMP

Simple Network Management Protocol (SNMP) は、ネットワークに接続されている通信機器をネットワーク経由で監視し管理するためのプロトコルで、重要なネットワーク管理項目でもあります。この SNMP 通信プロトコルを介して、ネットワーク管理機能を備えたプログラム (例：SNMP Tools-HP Open View) が、リアルタイムでの管理による通信をサポートします。デバイスは、標準 SNMP v1/v2c に対応し、SNMP ネットワーク管理ソフトウェアと一貫性があり、オンラインデバイスの稼働状況とネットワークのリアルタイム情報を掌握します。

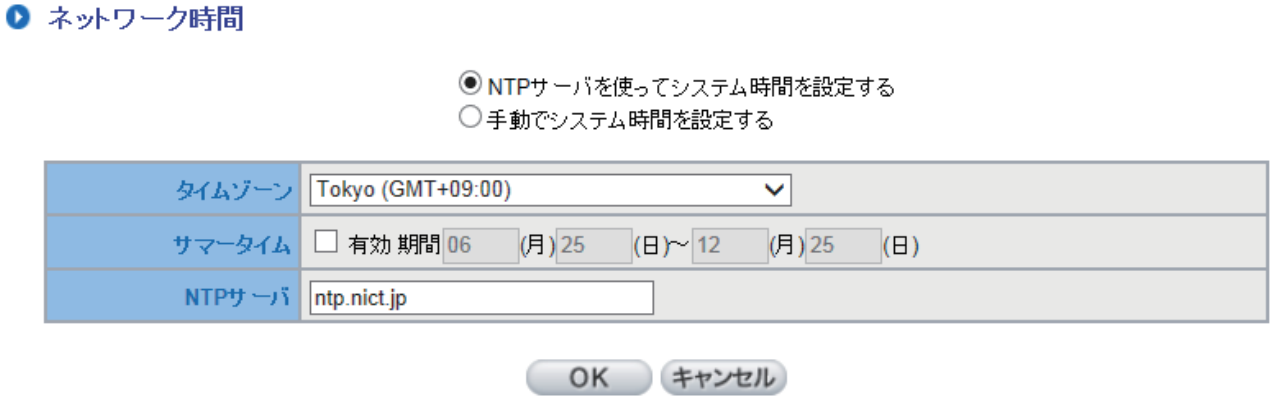
SNMP設定

有効 SNMP：	SNMP 機能を有効の状態にします。初期設定は、有効の状態になっています。
システム名：	「planex」などのデバイス名を設定します。
システムコンタクト：	デバイス管理者名を設定します (例：「Yamada」)。
システムロケーション：	デバイスの場所を指定します (例：「Tokyo」)。
GET コミュニティ名：	デバイスの SNMP データを確認するグループ名またはコミュニティ名を設定します。初期設定は「public」です。
SET コミュニティ名：	デバイスの SNMP データを受信するグループ名またはコミュニティ名を設定します。初期設定は「private」です。
TRAP コミュニティ名：	ユーザーパラメーター (トラップを受信するホスト PC に必要なパスワード) を設定して、トラップメッセージを受信します。
SNMP Trap の送信先：	トラップを受信するホスト PC の IP アドレスを 1 つ (IPv4 または IPv6) かあるいはドメイン名を設定します。
OK：	[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。

9.6 時間

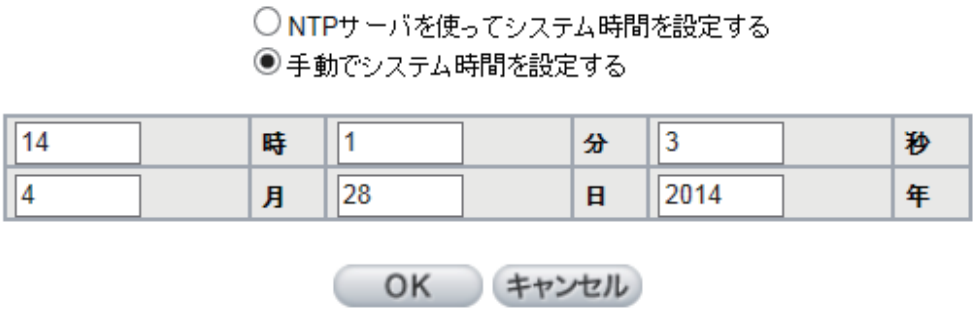
ルータで、時間設定を調整します。システムログに記録されているイベント発生の正確な時刻、インターネットリソースへのアクセス終了 / 開始時間を把握することができます。搭載された NTP サーバ同期機能を選択するか、時間基準を設定します。

NTP サーバを使ってシステム時間を設定する：
ルータは、時間を自発的に更新する NTP サーバを搭載しています。



タイムゾーン：	プルダウンのタイムゾーンリストから、現在の場所を選択して、正確な現地時間を表示します。
サマータイム：	「サマータイム制度」を採用している地域の場合は、日付範囲を入力します。デバイスがサマータイムの期間に合わせて時刻を自動的に調整します。
NTP サーバ：	使いたい時刻サーバがある場合には、サーバの IP アドレスを入力します。
OK：	変更が完了したら、[OK] をクリックして、設定を保存します。
キャンセル：	変更せずに終了するには、[キャンセル] をクリックします。[OK] をクリックして、設定を保存する前であれば、有効となります。

手動でシステム時間を設定する：
時間、日付、西暦年を正確に入力します。



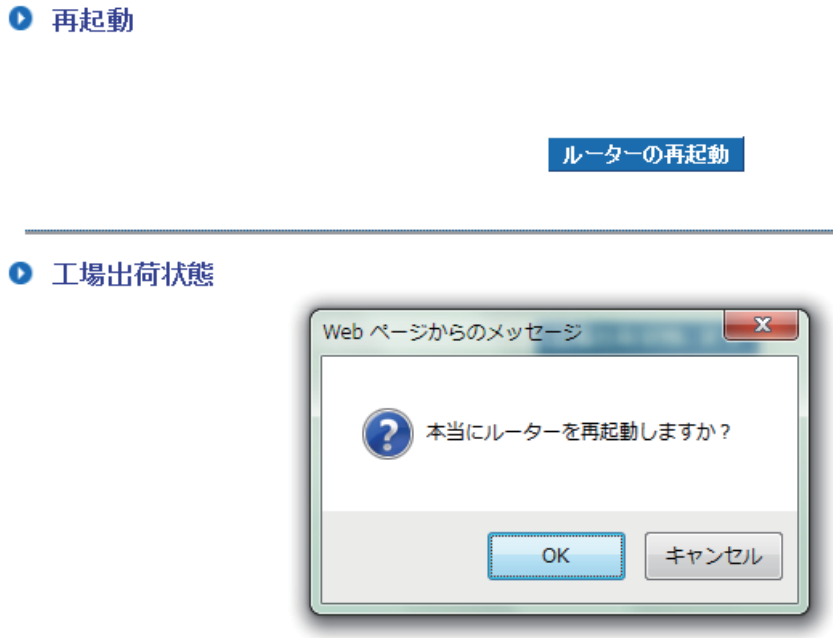
変更が完了したら、[OK] をクリックして、設定を保存します。変更せずに終了するには、[キャンセル] をクリックします。[OK] をクリックして、設定を保存する前であれば、有効となります。

9.7 再起動

「システムリカバリー」ボタンでデバイスを再起動します。

再起動

以下の図に示す「ルーターの再起動」ボタンをクリックすると、ダイヤログボックスがポップアップとして表示され、デバイスを再起動するかどうか確認します。

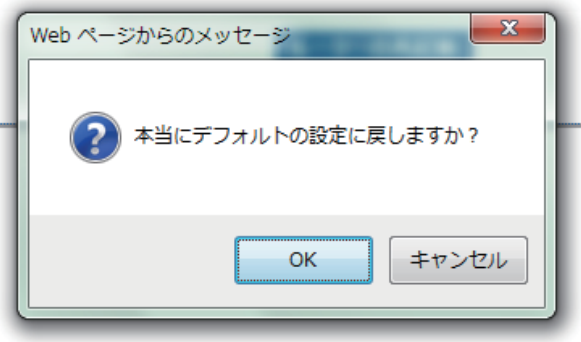


工場出荷状態に戻す

「工場出荷状態に戻す」をクリックすると、ダイヤログボックスがポップアップとして表示され、デバイスを工場出荷状態に戻すかどうか確認します。

再起動

工場出荷状態



ファームウェアをアップグレードする前に、現在の設定を保存してください。システムの安定に万全を期すため、ファームウェアをアップグレードした後に、システムを工場出荷状態に戻して、設定ファイルをインポートしてください。

X. ポート管理

本章では、ポートの構成方法と、イントラネットの IP アドレスの設定方法について説明します。

10.1 設定

ポートの番号、優先順位、スピード、Half/Full Duplex を選択し、各ポートの接続を設定するために自動ネゴシエーション機能を有効 / 無効にすることで、デバイスを介して、WAN ポート、LAN ポート、DMZ ポートの設定をかんたんに管理できます。

ポート設定

ポートID	インターフェース	無効	優先順位	スピード	Half/Full Duplex	自動ネゴシエーション	ポートVLAN
1	LAN	☐	中	10M 100M	Half Full	☑ 有効	VLAN1
2	LAN	☐	中	10M 100M	Half Full	☑ 有効	VLAN1
3	LAN	☐	中	10M 100M	Half Full	☑ 有効	VLAN1
4	LAN	☐	中	10M 100M	Half Full	☑ 有効	VLAN1
5	WAN1	☐	中	10M 100M	Half Full	☑ 有効	

OK キャンセル

ミラーポート:「Port 1 をミラーポートとして有効にする」を選択すると、「LAN 1 」がミラーポートとして設定されます。LAN から WAN へのすべてのトラフィックがミラーポートにコピーされます。管理者はミラーポートを介してトラフィックを制御またはフィルタできます。この機能が有効になると、「LAN 1」が「物理ポートステータスのミラーポート」としてホームページに表示されます。

●無効
イーサネットポートを無効の状態にします。設定を選択すると、イーサネットポートがただちにシャットダウンし、接続できなくなります。初期設定は「オン」です。

●優先順位：
イーサネットポートのパケット配信の高 / 中の優先順位を設定します。「高」に設定した場合は、パケット配信するにあたり、ポートが最優先されます。初期設定は「中」です。

●スピード：

イーサネットポートのネットワークハードウェア接続速度を選択します。選択肢は、「10Mbps」と「100Mbps」です。

● Half/Full Duplex：
イーサネットのネットワークハードウェア接続速度のワーキングモードを選択します。選択肢は、「フル」と「ハーフ」です。

●自動ネゴシエーション：
「自動ネゴシエーション」モードを使用すると、各ポートが自動的にスピードと Half/Full Duplex を調整かつ収集します。従って、「自動ネゴシエーションを有効にする」を選択した場合は、管理者が手動による設定を行わずに、ポートの設定が行われます。

● VLAN：
管理者が LAN ポートを複数の切断されたネットワークセッションとして設定します。すべてのセッションがデバイスを介してインターネットに接続できます。
(同じ VLAN 内の) 同じネットワークセッションのメンバーがお互いを確認して、通信できます。異なる VLAN のメンバーはその他のメンバーの存在を知ることはありません。

● VLAN 全部：
「VLAN 全部」ポートを VLAN のパブリック領域に設定して、その他の VLAN ネットワークに接続できるようにします。サーバをイントラネット用に構築して、すべての VLAN グループがこのサーバにアクセスできるようにします。ネットワークポートの 1 つを「VLAN 全部」として設定します。「VLAN 全部」にサーバを接続して、異なる VLAN グループの PC がこのサーバに接続できるようにします。また、管理者がいる場所にあるポートを「VLAN 全部」に設定して、そこからネットワーク全体に接続して、ネットワーク管理が容易にできるようにします。

10.2 ポートステータス

概要：
「タイプ」、「インターフェース」、「リンクステータス (アップ / ダウン)」、「物理ポートステータス (ポート有効)、「優先順位 (高または中)」、「スピードステータス (10Mbps または 100Mbps)」、「Half/Full Duplex (ハーフ / フル)」、「自動ネゴシエーション (有効 / 無効)」、のメニューがあり、それぞれ設定できます。

集計：
この特定のポートのパケットデータを表示します。データには、送受信パケット数、送受信パケットバイト数、エラーパケット数が含まれています。[再読込] ボタンをクリックして、すべてのリアルタイムメッセージを更新します。

XI.GRE

11.1 GRE の概要

GRE概要

GREトンネル番号：	0 使用中のトンネル	10 利用可能なトンネル

GREトンネルステータス

No.	名	ステータス	インターフェース	ローカルグループ	リモートグループ	リモートゲートウェイ	設定.

追加トンネル

11.1.1 GRE 概要

使用中の GRE トンネル数と利用可能なトンネル数です。

GRE概要

GREトンネル番号：	0 使用中のトンネル	10 利用可能なトンネル

11.1.2 GRE トンネルステータス

GRE トンネルの設定とステータスを表示します。

GREトンネルステータス

No.	名	ステータス	インターフェース	ローカルグループ	リモートグループ	リモートゲートウェイ	設定.

追加トンネル

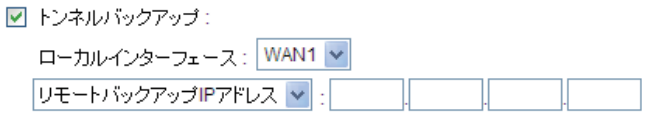
●ステータス

1. 接続待機中です
トンネルが接続されるのを待っています。

2. 切断
接続プロセスが終了しましたが、接続できません。

3. 接続
トンネルが接続されました。

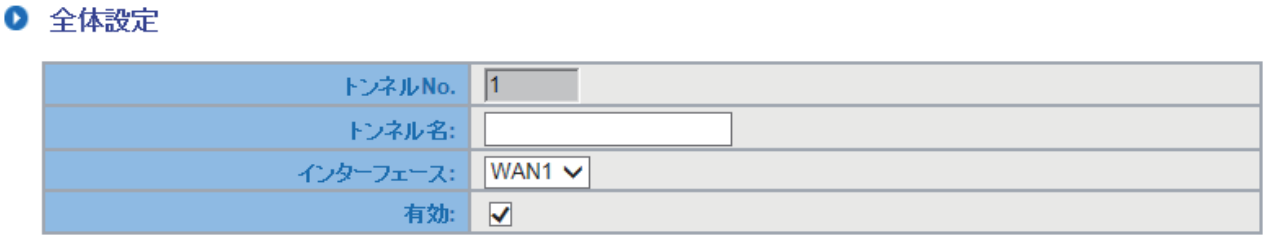
4. トンネルバックアップ：セカンダリ
メイントンネルが機能していない間は、セカンダリトンネルが有効の状態です。トンネルバックアップが表示されます。



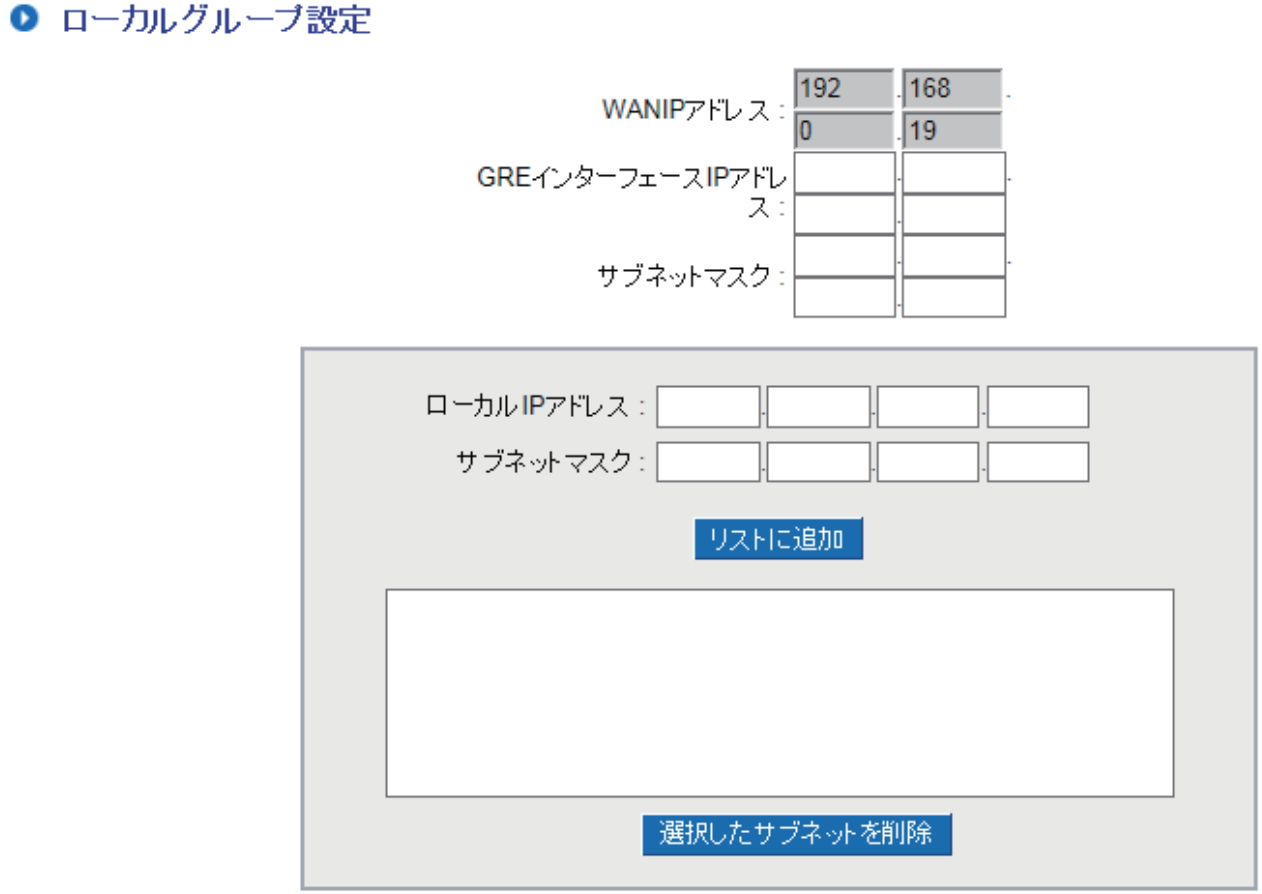
11.2 GRE 設定

11.2.1 全体設定

初期設定は「有効」です。設定されると、ルールが自動的に有効の状態になります。



11.2.2 ローカルグループ設定



WAN IP アドレス：システムによって WAN 側の IP アドレスが空欄に入力されます。

GRE インターフェース IP アドレス：システムが両サイド (ローカル / リモートサイト) を自動的に検出します。 ここに入力されたホストの IP アドレスが利用可能です。

ローカル IP アドレス／サブネットマスク：ローカルホストの IP アドレスを入力します。

11.2.3 リモートグループ設定

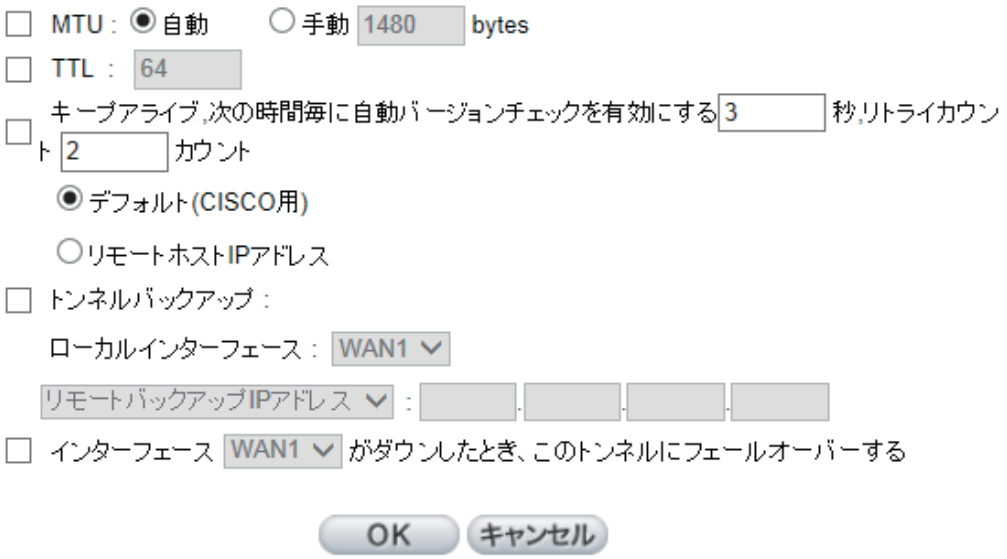
WAN 側 IP アドレス：リモートホストの IP アドレスを入力します。IP アドレスがない場合は、ドメイン名を入力します。

GRE インターフェース IP アドレス / サブネットマスク：システムが接続を自動的に検出します。IP アドレスで接続してください。IP アドレスで接続できない場合は、システムが再接続します。

送信先 IP アドレス / サブネットマスク：接続できる IP アドレスとサブネットマスクを入力します。

11.2.4 詳細設定

詳細 + ボタンをクリックして、詳細設定を設定します。



*MTU：「自動」または「手動」のいずれかを選びます。異なるネットワーク環境に対して異なる値を設定できます (例：ADSL の PPPoE MTU の場合、「1492」)。初期設定は「自動」です。

*TTL: パケットの寿命。ルーティングが正しくないため、パケットが送信できない場合に、TTL が減少し「0」になっていると、ルータがこのパケットを廃棄し、パケット発行元にそれを通達します。

* キープアライブ：この項目をチェックしている場合は、システムが GRE トンネルのリモートホストに特定のパケットを送信して、接続ステータスを確認します。 リトライ回数が設定値を超えて、リモートサイトからの応答を受信しない場合、システムはトンネルがダウンしていると認識します。アクティブサイトの場合は、システムがトンネルを自動的に構築します。
(1) デフォルト (CISCO 対応)：リモートサイトが Cisco のキープアライブプロトコルに対応している場合は、「デフォルト」を選択します。
(2) リモートホスト IP アドレス：リモートサーバが Cisco GRE キープアライブプロトコルに対応していない場合は、この項目をチェックします。

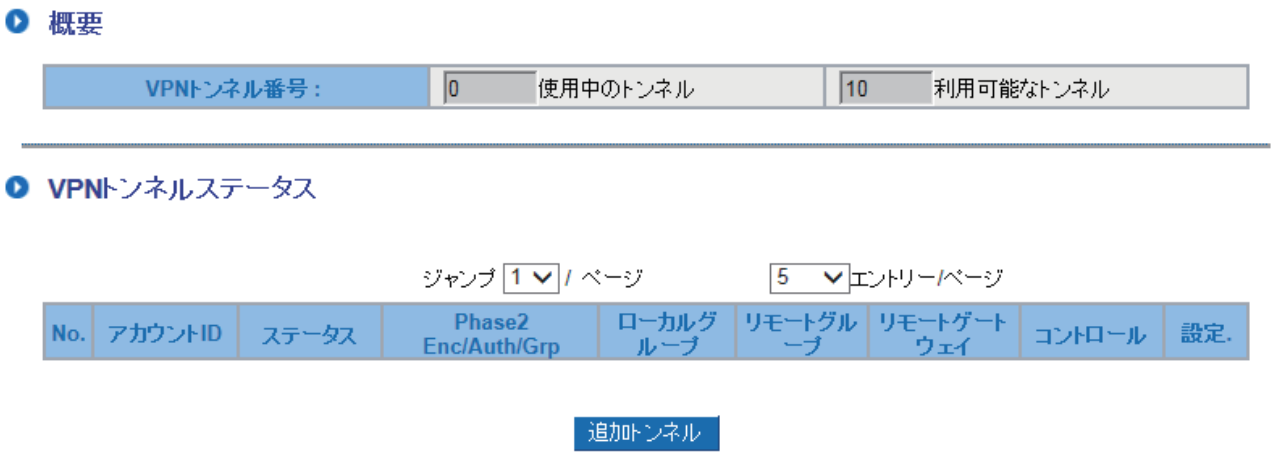
* トンネルバックアップ：メインとバックアップのトラフィックの両方が GRE トンネル経由で送信されます。

*WAN1 がダウンしたときこのトンネルにフェールオーバーする
メイントラフィックがその他のタイプのトンネル (例：MPLS) 経由で送信され、GRE トンネルがバックアップトンネルとして構成されます。GRE トンネルは、メイントンネルが切断されたときにのみ、有効の状態になります。

XII.VPN（仮想プライベートネットワーク）

12.1.IPSec VPN

12.1.1 概要



「VPN トンネルステータス」、VPN トンネルの現在のステータスを、下記に詳しく説明します。

ジャンプ__/ページ、__エントリー/ページ	「前」または「次」ページをクリックして、見たい VPN トンネルページを閲覧します。または、ページ番号を直接選択して、「3」、「5」、または「全て」など、すべての VPM トンネルステータスを閲覧します。
アカウント ID：	「XXX オフィス」など、VPN トンネルの現在の接続名を表示します。トンネル設定が複数ある場合は、それぞれに別の名前をつけて混同を避けてください。 注意：このトンネルをこのデバイス以外のその他の VPN デバイスに接続する場合は、トンネル名をホスト側の名前と同じにして、検証を容易にする必要があることがあります。そうすることで、このトンネルを確実に有効の状態にすることができます。
No.	搭載された VPN 機能を設定するには、トンネル番号を選択します。
ステータス：	接続に成功した場合は、「(接続)」と表示されます。 ホスト名解決に失敗した場合は、(「ホスト名解決に失敗」) と表示されます。 ホスト名を解決中の場合は、(「ホスト名解決中」)、接続待機中の場合は、(「接続待機中」) とそれぞれ表示されます。 「IPSec」設定で「手動」の設定を選択した場合は、ステータスメッセージに「手動」と表示されます。なお、「トンネル」のテスト機能は、この手動設定には利用できません。

Phase2 Encrypt/Auth/Group	暗号化方式 (DES/3DES)、認証 (MD5/SHA1)、グループ (1/2/5) などの設定値を表示します。 「IPSec」設定で「手動」の設定を選択した場合は、フェーズ 2 DH グループは表示されません。
ローカルグループ：	VPN 接続のローカル側のセキュアグループの設定を表示します。
リモートグループ：	リモート VPN 接続のセキュアグループの設定を表示します。
リモートゲートウェイ：	IP アドレスを設定して、リモート VPN デバイスに接続します。VPN デバイスに有効な IP アドレスまたはドメイン名を設定してください。
コントロール：	[接続] をクリックして、トンネルステータスを検証します。テスト結果が更新されます。切断するには、 [切断] をクリックして、VPN 接続を切断します。
設定 . :	[編集] と [削除] の 2 つのアイコンを使用して、項目を設定します。 [編集] をクリックして、項目を表示し、設定を変更します。ごみ箱のアイコン をクリックすると、すべてのトンネル設定が削除されます。

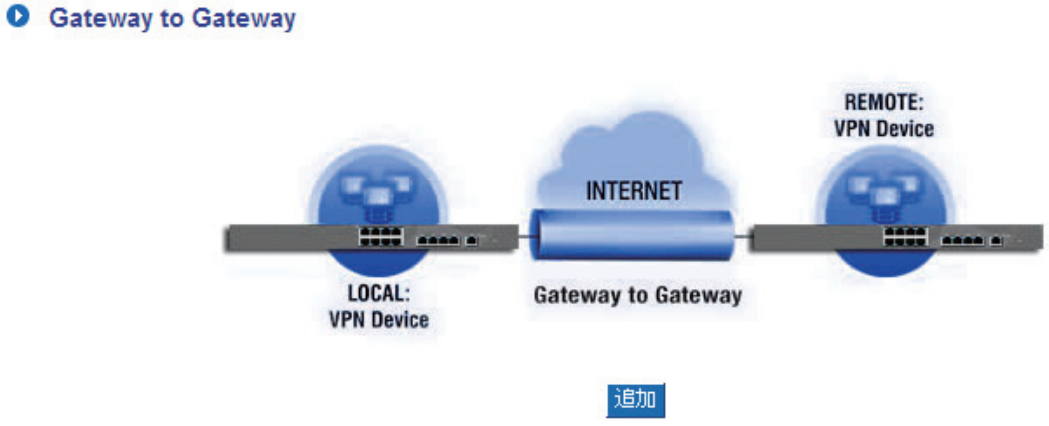
12.1.2. 新しい VPN トンネルを追加する

デバイスは、「Gateway to Gateway」トンネルまたは「Client to Gateway」トンネルに対応しています。

2 つの VPN デバイスによって、インターネット経由で VPN トンネルを接続します。新しい VPN トンネルが追加されると、「Gateway to Gateway」または「Client to Gateway」の設定ページが表示されます。

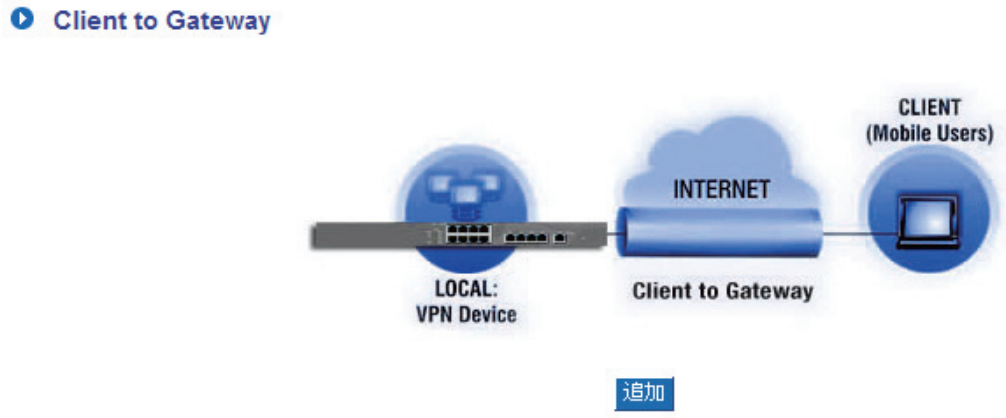
Gateway to Gateway：

[追加] をクリックして、「Gateway to Gateway」の設定ページを表示します。

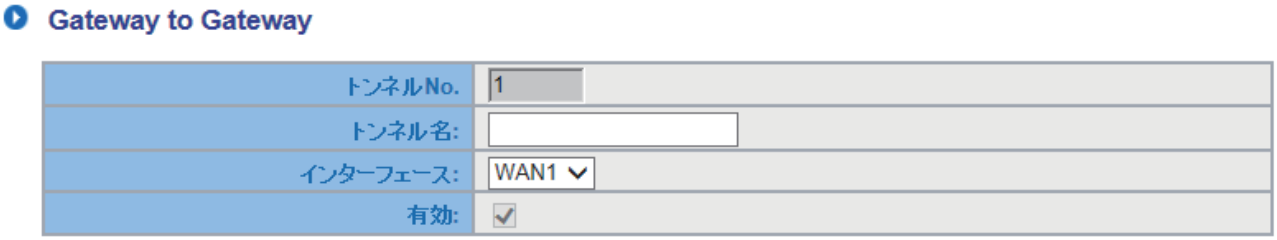


Client to Gateway：

[追加] をクリックして、「Client to Gateway」の設定ページを表示します。



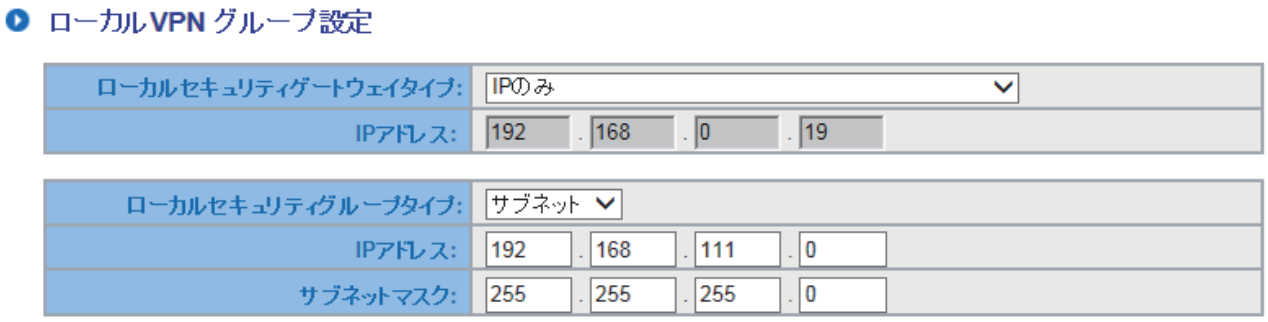
12.1.2.1.「Gateway to Gateway」設定



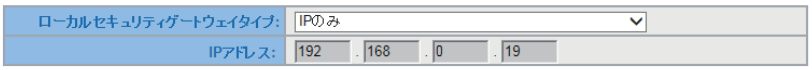
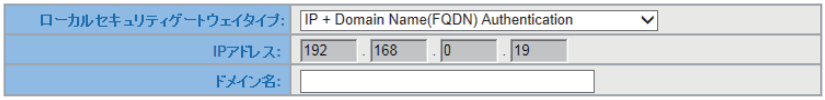
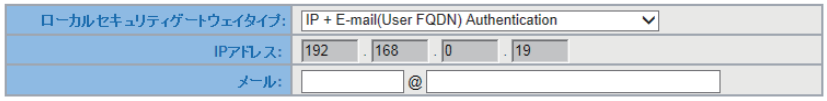
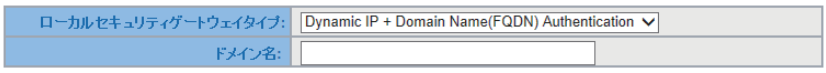
以下の項目を入力して、2 つのデバイス間に VPN トンネルを設定します。

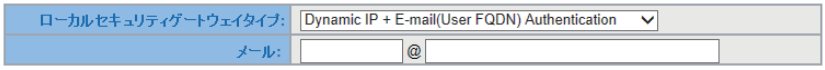
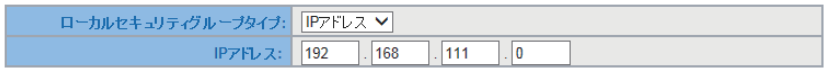
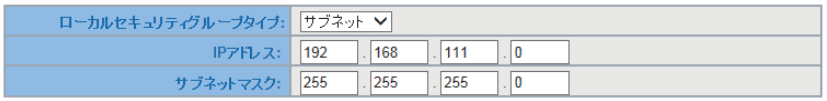
トンネル No.：	搭載された VPN 機能を設定するには、トンネル番号を選択します。
トンネル名：	「XXX オフィス」など、VPN トンネルの現在の接続名を表示します。それぞれに別の名前をつけて混同を避けてください。 注意：このトンネルをその他の VPN デバイスに接続する場合は、トンネル名をホスト側の名前と同じにして、検証を容易にする必要があることがあります。そうすることで、このトンネルを確実に有効の状態にすることができま
インターフェース :	プルダウンメニューから、この VPN トンネルに使用するインターフェースを選択します。
有効：	クリックすると、VPN トンネルが有効の状態になります。初期設定は「オン」です。後から、このトンネル機能を有効にすることもできます。

ローカルグループ設定：



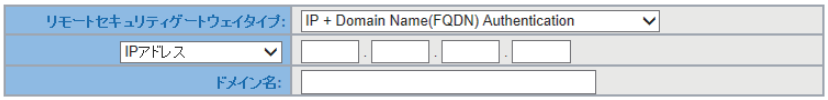
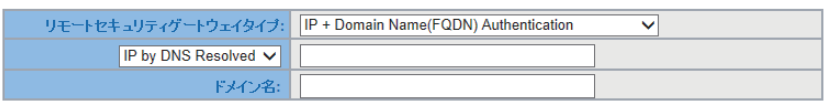
「ローカルセキュリティゲートウェイタイプ」の設定は、リモートタイプ (リモートセキュリティゲートウェイタイプ) の設定と同じにします。

ローカルセキュリティゲートウェイタイプ：	ローカルゲートウェイの認証タイプは、以下の 5 つ動作モードに対応しています： **IP のみ** **IP + ドメイン名 (FQDN) 認証** **IP + メールアドレス (ユーザー FQDN) 認証** **動的 IP + ドメイン名 (FQDN) 認証** **動的 IP + メールアドレス (ユーザー FQDN) 認証** **(1) IP のみ：** IP アドレスのみを使用する場合は、IP アドレスを入力して、このトンネルにアクセスする方法に限定されます。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。  **(2) IP + ドメイン名 (FQDN) 認証：** IP アドレスとドメイン名を使用する場合は、ドメイン名と IP アドレスを入力します。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。FQDN は、ホスト名とドメイン名を組み合わせたもので、例えば、「vpn.server.com」などのインターネットから取得します。 この IP アドレスとドメイン名を、VPN のセキュリティゲートウェイタイプで設定したものと同じにして、接続を確立できるようにします。  **(3) IP + メールアドレス (ユーザー FQDN) 認証：** IP アドレスとメールアドレスを使用する場合は、IP アドレスとメールアドレスを入力して、このトンネルにアクセスします。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。  **(4) 動的 IP + ドメイン名 (FQDN) 認証：** 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。VPN 接続するために、リモート VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、ドメイン名を入力します。 

	(5) 動的 IP + メールアドレス (ユーザー FQDN) 認証： 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。IP アドレスは入力しません。VPN 接続するために、VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、メール認証用にメールアドレスを入力します。 
ローカルセキュリティグループタイプ：	ローカル VPN 接続のアクセスタイプを設定します。複数の項目がありますので、それぞれのパラメーターを適宜設定してください。 **1.IP アドレス** VPN トンネルを構築するために入力する 唯一の IP アドレスを設定します。  参考：この VPN トンネル接続では、IP アドレス「192.168.111.0」を持つ PC 群 が接続を確立できます。 **2. サブネット**  このサブネットのローカル PC が VPN トンネルに接続できます。 参照：VPN トンネル接続する際に、IP アドレス「192.168.111.0」とサブネットマスク「255.255.255.0」を持つ PC のみがリモート VPN に接続できます。

リモートグループ設定：

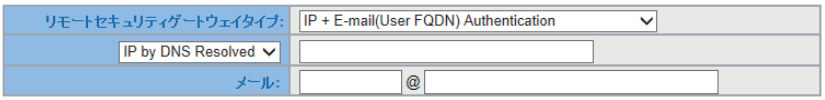
●リモートゲートウェイの認証タイプ (「リモートセキュリティゲートウェイタイプ」) の設定は、リモート接続されたローカルセキュリティゲートウェイの認証タイプ (ローカルセキュリティゲートウェイタイプ) の設定と同じにします。

リモートセキュリティゲートウェイタイプ：	リモートゲートウェイの認証タイプは、以下の 5 つの動作モードに対応しています： **IP のみ** - IP アドレスのみを使用した認証 **IP + ドメイン名 (FQDN) 認証** - IP アドレス + ドメイン名を使用した認証 **IP + メールアドレス (ユーザー FQDN) 認証** - IP アドレス + メールアドレスを使用した認証 **動的 IP + ドメイン名 (FQDN) 認証** - 動的 IP アドレス + ドメイン名を使用した認証 **動的 IP + メールアドレス (ユーザー FQDN) 認証** - 動的 IP アドレス + メールアドレスを使用した認証 **(1) IP のみ：** IP アドレスのみを使用する場合は、IP アドレスを入力して、このトンネルにアクセスする方法に限定されます。  リモートクライアントの IP アドレスがわからない場合は、「DNS による IP 解決」を選択して、DNS で IP アドレスに変換します。設定が完了したら、「概要」のリモートゲートウェイに該当する IP アドレスが表示されます。  **(2) IP + ドメイン名 (FQDN) 認証：** IP アドレスとドメイン名を使用する場合は、認証用の IP アドレスとドメイン名を入力します。FQDN は、ホスト名とドメイン名を組み合わせたものです。 FQDN のドメイン名に対応する任意の名前を入力します。この IP アドレスとドメイン名を、リモート VPN のセキュリティゲートウェイタイプで設定したものと同じにして、接続を確立できるようにします。  リモート IP アドレスがわからない場合は、「DNS による IP 解決」を選択して、DNS で IP アドレスに変換します。ドメイン名はインターネット上で公開されなければなりません。設定が完了したら、「概要」のリモートゲートウェイに該当する IP アドレスが表示されます。 

(3) IP + メールアドレス (ユーザー FQDN) 認証：

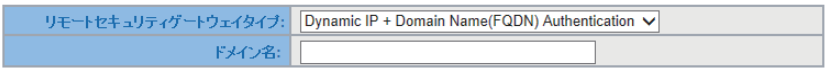
IP アドレスとメールアドレスを使用する場合は、IP アドレスとメールアドレスを入力して、このトンネルにアクセスします。

リモート IP アドレスがわからない場合は、「DNS による IP 解決」を選択して、DNS で IP アドレスに変換します。ドメイン名はインターネット上で公開されなければなりません。設定が完了したら、「概要」のリモートゲートウェイに該当する IP アドレスが表示されます。



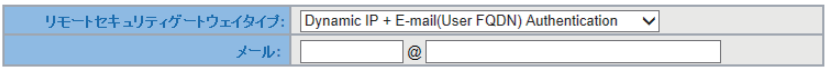
(4) 動的 IP + ドメイン名 (FQDN) 認証：

動的 IP アドレスを使用してデバイスに接続する場合は、動的 IP アドレス、ホスト名、ドメイン名を組み合わせます。



(5) 動的 IP + メール (アドレスユーザー FQDN) 認証：

動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。VPN 接続するために、リモート VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、メール認証用にメールアドレスを入力します。



IPSec 設定：

ルータは、事前鍵共有方式 (自動) を用いた IKE の自動暗号化に対応しています。

IPSec VPN設定設定

キーイングモード:	IKE with Preshared Key
フェーズ1 DHグループ:	グループ1
フェーズ1 暗号化:	DES
フェーズ1 認証:	MD5
フェーズ1 SAライフタイム:	0 秒
Perfect Forward Secrecy	☑
フェーズ2 DHグループ:	グループ1
フェーズ2 暗号化:	DES
フェーズ2 認証:	MD5
フェーズ2 SAライフタイム:	0 秒
プレシェアードキー:	

IKE プロトコル：

「PFS (Perfect Forward Secrecy)」が有効の場合は、IKE との連携時に成立したフェーズ 2 共有キーを使用して、暗号化と認証を行います。PFS が有効のときは、ブルートフォース攻撃をしかけてキーを奪おうとするハッカーが、この短い間にフェーズ 2 キーを取得することができません。

• **Perfect Forward Secrecy：**PFS オプションをチェックしているときは、VPN デバイスと VPN クライアントの PFS 機能を必ず有効にします。

• **フェーズ 1/ フェーズ 2 DH** グループ：Diffie-Hellman グループのグループ 1、グループ 2、グループ 5 を選択できます。

• **フェーズ 1/ フェーズ 2 暗号化：**VPN トンネルに暗号化方式を使用できるよう設定します。このパラメーターの設定を、DES (64 ビット暗号化方式)、3DES (128 ビット暗号化方)、AES (セキュリティコードを使用して情報を暗号化する標準の暗号化方式) に設定したリモート暗号化のパラメーターと同じにします。128 ビット、192 ビット、256 ビット暗号化キーに対応しています。

• **フェーズ 1/ フェーズ 2 認証：**VPN トンネルに認証方式を使用できるよう設定します。このパラメーターの設定を、リモート認証方式「MD5」または「SHA1」に設定したパラメーターと同じにします。

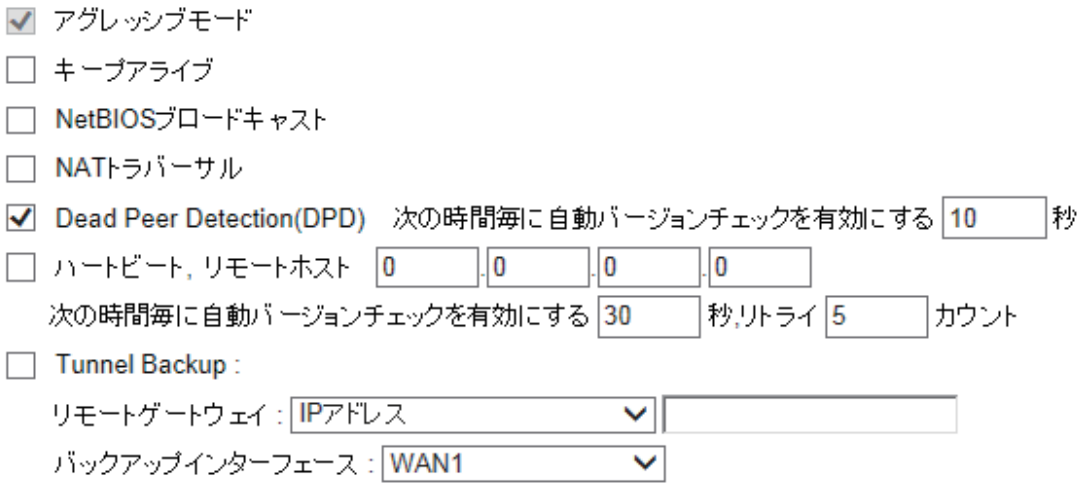
・フェーズ 1 SA ライフタイム：初期設定では、この交換コードのライフタイムは「28800 秒 (または 8 時間)」です。VPN 接続の有効時間内にその他の交換用パスワードを自動生成して、セキュリティを保証します。

・フェーズ 2 SA ライフタイム：初期設定では、この交換コードのライフタイムは「3600 秒 (または 1 時間)」です。VPN 接続の有効時間内にその他の交換用パスワードを自動生成して、セキュリティを保証します。

・プレシェアードキー：自動 (IKE) オプションの場合、「プレシェアードキー」のテキストボックスに任意の数字や文字を入力すると 、VPN トンネル接続時に、ユーザーが入力した内容を、システムが交換用パスワードと認証メカニズムに自動的に変換します。この交換用パスワードは、最大 30 文字までです。

詳細設定

詳細



詳細設定には、「メイン」モードと「アグレッシブ」モードの 2 つがあります。「メイン」モードの初期設定は、VPN 動作モードに設定されています。ほとんどの VPN デバイスと同じ方法で接続します。

●アグレッシブモード：おもに、リモートデバイスで適用されています。IP 接続は、動的 IP アドレスを接続に使用する場合に、セキュリティ制御を強化するよう設計されています。

●キープアライブ：このオプションを選択している場合は、VPN トンネルによって VPN 接続が維持されます。おもに、支社や本社のリモートノードの接続や、リモート動的 IP アドレスに使用されています。

● NetBIOS ブロードキャスト：このオプションを選択している場合は、接続中の VPN トンネルを NetBIOS ブロードキャストパケットが通過します。その他のマイクロソフトネットワークとの接続が容易になりますが、この VPN トンネルを使用しているトラフィックが増加します。

● NAT トラバーサル：NAT デバイスが IPSec パケットに対応していないことがあるため、NAT を使用しているデバイスを通過するときに、IPSec が機能しない場合があります。NAT トラバーサルを有効にすると、この問題を回避できます。この項目を有効にすると、IPSec トラフィックが NAT デバイスを通過できるようになります。

● Dead Peer Detection (DPD)：このオプションを選択している場合は、接続中の VPN トンネルが定期的に HELLO/ACK メッセージパケットを送信して、VPN トンネルの両端が接続されている状態か検出します。一方の端が切断されている場合は、デバイスがトンネルを

自動的に切断して、新しい接続を作成します。各 DPD メッセージパケットの送信時間を設定することができます。初期設定は「10 秒」です。

●ハートビート：VPN トンネルの「ハートビート検出」機能です。このオプションを選択している場合は、システムが定期的に ICMP ACK パケットを、VPN トンネルのあるリモートホストに送信します。また、リモートホストが ICMP ACK 応答パケットを送信元に送ります。リトライ設定回数を超えた後も、ICMP ACK 応答パケットをまだ受信していない場合は、ハートビートの送信元が、この VPN トンネルを切断します。この状況で、VPN トンネルイニシエータである場合は、システムがトンネルを再接続しようと試みます。
パッシブパーティの場合は、システムが、イニシエータがトンネルを再構築するまで待機します。

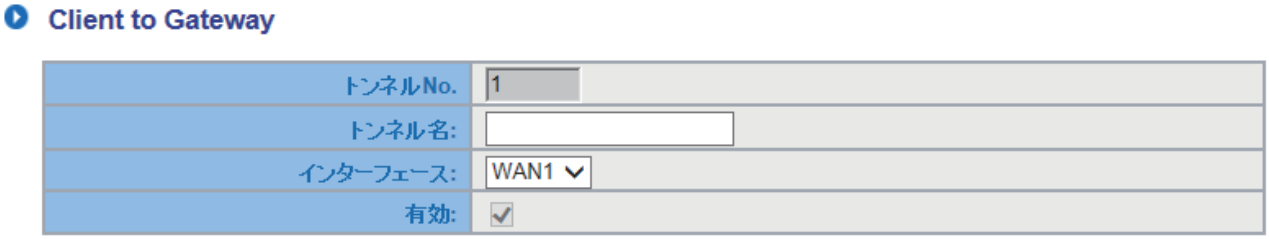
リモートホスト	「ハートビート検出」のリモート終点です。「ハートビート検出」の終点を常に設定します。応答を迅速に送ることのできる、堅牢性と安定性に優れたサーバを選択してください。VAN のリモート終点にあるデバイスの LAN 側の IP アドレスを、「ハートビート検出」のターゲットとして使用してください。
間隔	初期設定では、「ハートビート」の間隔は「30 秒」です。VPN トンネルを構築した後、システムが ICMP エコーリクエストを 30 秒ごとに送り返します。
リトライ	初期設定では、リトライ回数は「5」です。初期設定のリトライ回数を超えた後も「ハートビート」が機能しない場合は、システムが VPN トンネルを切断します。

「VPN ハートビート検出」機能と「DPD」機能は、安定性に優れた VPN ソリューションを提供するために使用されています。 この 2 つの機能の相違点は、「ハートビート検出」を非 IPSec プロトコルに使用できることです。「ハートビート検出」を使用して、VPN トンネルを監視し、トンネルが存在して円滑に動作しているか確認できます。一方、「DPD」機能は、IPSec プロトコルにのみ利用可能です。

● Tunnel Backup：バックアップの VPN トンネルを構成します。

12.1.2.2.「Client to Gateway」設定

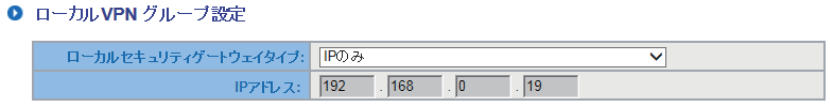
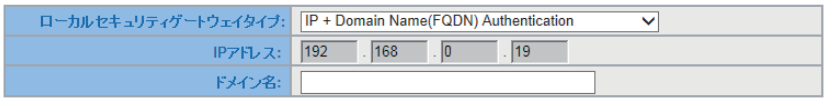
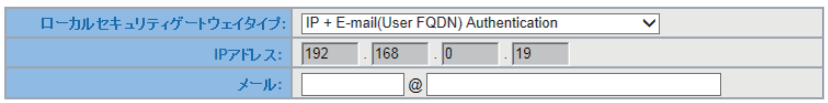
管理者が デバイス間に VPN トンネルを構築する方法を以下に説明します。
(1) トンネルでの状況：

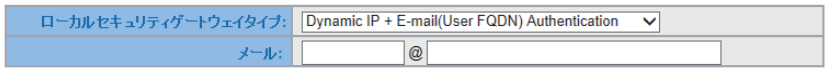
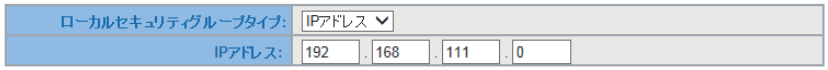
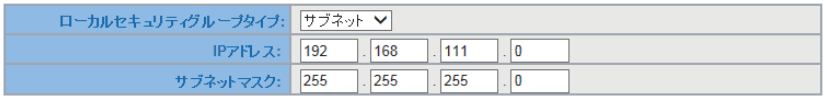


トンネル No.：	搭載された VPN 機能を設定するには、トンネル番号を選択します。
トンネル名：	「XXX オフィス」など、VPN トンネルの現在の接続名を表示します。それぞれに別の名前をつけて混同を避けてください。 注意：このトンネルをその他の VPN デバイスに接続する場合は、トンネル名をホスト側の名前と同じにして、検証を容易にする必要があることがあります。そうすることで、このトンネルを確実に有効の状態にすることができます。
インターフェース：	VPN チャンネルのノードとなるポートを選択します。VPN 接続に適用されます。
有効：	[有効] をクリックすると、VPN トンネルが有効の状態になります。初期設定は「オン」です。設定後に、このトンネル機能を有効にすることもできます。

ローカルグループ設定

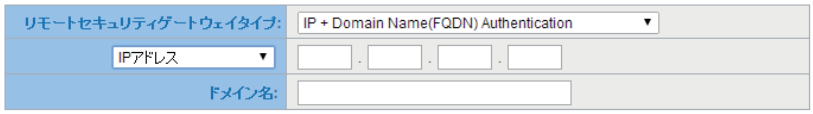
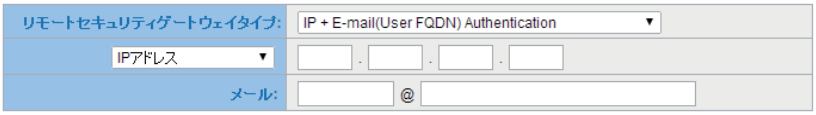
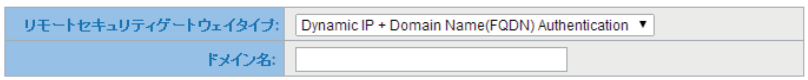
ローカルゲートウェイ認証タイプ (「ローカルセキュリティゲートウェイタイプ」) の設定は、リモートタイプ (リモートセキュリティゲートウェイタイプ) の設定と同じにします。

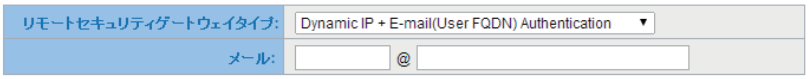
ローカルセキュリティゲートウェイタイプ：	ローカルゲートウェイの認証タイプは、以下の 5 つ動作モードに対応しています： **IP のみ** - IP アドレスのみを使用した認証 **IP + ドメイン名 (FQDN) 認証** - IP アドレス + ドメイン名を使用した認証 **IP + メールアドレス (ユーザー FQDN) 認証** - IP アドレス + メールアドレスを使用した認証 **動的 IP + ドメイン名 (FQDN) 認証 -** IP アドレス + ドメイン名を使用した認証 **動的 IP + メールアドレス (ユーザー FQDN) 認証 -** 動的 IP アドレス + メールアドレスを使用した認証 **(1) IP のみ：** IP アドレスのみを使用する場合は、IP アドレスを入力して、このトンネルにアクセスする方法に限定されます。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。  **(2) IP + ドメイン名 (FQDN) 認証：** IP アドレスとドメイン名を使用する場合は、ドメイン名と IP アドレスを入力します。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。FQDN は、ホスト名とドメイン名を組み合わせたもので、例えば、「vpn.server.com」などのインターネットから取得します。この IP アドレスとドメイン名を、VPN のセキュリティゲートウェイタイプで設定したものと同じにして、接続を確立できるようにします。  **(3) IP + メールアドレス (ユーザー FQDN) 認証：** IP アドレスとメールアドレスを使用する場合は、IP アドレスとメールアドレスを入力して、このトンネルにアクセスします。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。 

	(4) 動的 IP + ドメイン名 (FQDN) 認証： 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。VPN 接続するために、リモート VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、ドメイン名を入力します。  **(5) 動的 IP + メールアドレス (ユーザー FQDN) 認証：** 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。IP アドレスは入力しません。VPN 接続するために、VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、メール認証用にメールアドレスを入力します。 
ローカルセキュリティグループタイプ：	ローカル VPN 接続のアクセスタイプを設定します。複数の項目がありますので、それぞれのパラメーターを適宜設定してください。 **4.IP アドレス** VPN トンネルを構築するために入力する 唯一の IP アドレスを設定します。  参照：VPN トンネル接続する際に、IP アドレス「192.168.111.0」を持つ PC が接続を確立できます。  参照：VPN トンネル接続する際に、IP アドレス「192.168.111.0」とサブネットマスク 「255.255.255.0」を持つ PC のみがリモート VPN に接続できます。

リモートグループ設定：

リモートゲートウェイ認証タイプ (「リモートセキュリティゲートウェイタイプ」) の設定は、リモート接続されたローカルセキュリティゲートウェイ認証タイプ (ローカルセキュリティゲートウェイタイプ) の設定と同じにします。

トンネル名：	ローカルゲートウェイの認証タイプは、以下の 5 つ動作モードに対応しています： **IP のみ** **IP + ドメイン名 (FQDN) 認証** **IP + メールアドレス (ユーザー FQDN) 認証** **動的 IP + ドメイン名 (FQDN) 認証** **動的 IP + メールアドレス (ユーザー FQDN) 認証** **(1) IP のみ：** IP アドレスのみを使用する場合は、IP アドレスを入力して、このトンネルにアクセスする方法に限定されます。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。  **(2) IP + ドメイン名 (FQDN) 認証：** IP アドレスとドメイン名を使用する場合は、ドメイン名と IP アドレスを入力します。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。FQDN は、ホスト名とドメイン名を組み合わせたもので、 例えば、「vpn.server.com」などのインターネットから取得します。この IP アドレスとドメイン名を、VPN のセキュリティゲートウェイタイプで設定したものと同じにして、接続を確立できるようにします。  **(3) IP + メールアドレス (ユーザー FQDN) 認証：** IP アドレスとメールアドレスを使用する場合は、IP アドレスとメールアドレスを入力して、このトンネルにアクセスします。WAN 側の IP アドレスは自動的にこの空欄に入力されます。これ以上の設定は必要ありません。  **(4) 動的 IP + ドメイン名 (FQDN) 認証：** 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。VPN 接続するために、リモート VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、ドメイン名を入力します。 

	(5) 動的 IP + メールアドレス (ユーザー FQDN) 認証： 動的 IP アドレスを使用してデバイスに接続する場合は、このオプションを選択して、VPN 接続します。IP アドレスは入力しません。VPN 接続するために、VPN ゲートウェイがデバイスに接続する必要がある場合は、デバイスが認証を開始して、VPN トンネル接続に応答します。このオプションを選択して、VPN 接続する場合は、メール認証用にメールアドレスを入力します。 

IPSec 設定

暗号管理プロトコル：

VPN トンネルに暗号化と認証方式を使用できるよう設定するときに、交換用パスワードのパラメーターの設定を、リモートで設定したものと同じにします。設定方法は、「自動 (IKE)」と「手動」の 2 つです。設定するときに、2 つのうちいずれかを選択します。

IKE プロトコル：

「PFS (Perfect Forward Secrecy)」が有効の場合は、IKE との連携時に成立したフェーズ 2 共有キーを使用して、暗号化と認証を行います。PFS が有効のときは、ブルートフォース攻撃をしかけてキーを奪おうとするハッカーが、この短い間にフェーズ 2 キーを取得することができません。

● **Perfect Forward Secrecy：**PFS オプションをチェックしているときは、VPN デバイスと VPN クライアントの PFS 機能を必ず有効にします。

●**フェーズ 1/ フェーズ 2 DH グループ：**Diffie-Hellman グループのグループ 1、グループ 2、グループ 5 を選択できます。

●**フェーズ 1/ フェーズ 2 暗号化：**VPN トンネルに暗号化方式を使用できるよう設定します。このパラメーターの設定を、DES (64 ビット暗号化方式)、3DES (128 ビット暗号化方)、AES (セキュリティコードを使用して情報を暗号化する標準の暗号化方式) に設定したリ

モート暗号化のパラメーターと同じにします。128 ビット、192 ビット、256 ビット暗号化キーに対応しています。

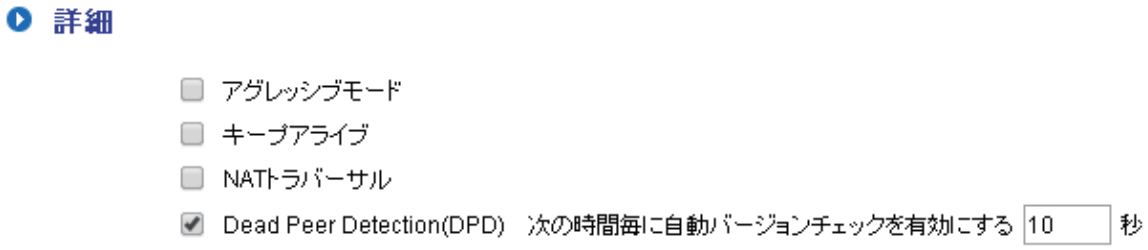
●フェーズ 1/ フェーズ 2 認証：VPN トンネルに認証方式を使用できるよう設定します。このパラメーターの設定を、リモート認証方式「MD5」または「SHA1」に設定したパラメーターと同じにします。

●フェーズ 1 SA ライフタイム：初期設定では、この交換コードのライフタイムは「28800 秒 (または 8 時間)」です。VPN 接続の有効時間内にその他の交換用パスワードを自動生成して、セキュリティを保証します。

●フェーズ 2 SA ライフタイム：初期設定では、この交換コードのライフタイムは「3600 秒 (または 1 時間)」です。VPN 接続の有効時間内にその他の交換用パスワードを自動生成して、セキュリティを保証します。

●プレシェアードキー：自動 (IKE) オプションの場合、「プレシェアードキー」のテキストボックスに任意の数字や文字を入力すると、VPN トンネル接続時に、ユーザーが入力した内容を、システムが交換用パスワードと認証メカニズムに自動的に変換します。この交換用パスワードは、最大 30 文字までです。

詳細設定



詳細設定には、「メイン」モードと「アグレッシブ」モードの 2 つがあります。「メイン」モードの初期設定は、VPN 動作モードに設定されています。ほとんどの VPN デバイスと同じ方法で接続します。

●**アグレッシブモード：**おもに、リモートデバイスで適用されています。IP 接続は、動的 IP アドレスを接続に使用する場合に、セキュリティ制御を強化するよう設計されています。

●**キープアライブ：**このオプションを選択している場合は、VPN トンネルによって VPN 接続が維持されます。おもに、支社や本社のリモートノードの接続や、リモート動的 IP アドレスに使用されています。

● **NAT トラバーサル：**NAT デバイスが IPSec パケットに対応していないことがあるため、NAT を使用しているデバイスを通過するときに、IPSec が機能しない場合があります。NAT トラバーサルを有効にすると、この問題を回避できます。この項目を有効にすると、IPSec トラフィックが NAT デバイスを通過できるようになります。

● **Dead Peer Detection (DPD)：**このオプションを選択している場合は、接続中の VPN トンネルが定期的に HELLO/ACK メッセージパケットを送信して、VPN トンネルの両端が接続されている状態か検出します。一方の端が切断されている場合は、デバイスがトンネルを自動的に切断して、新しい接続を作成します。各 DPD メッセージパケットの送信時間を設定することができます。初期設定は「10 秒」です。

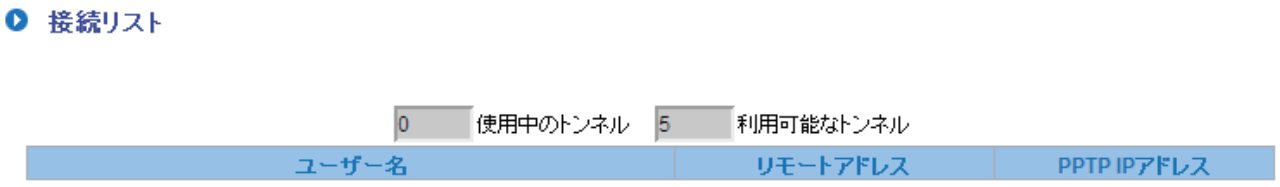
12.2 PPTP

VPN 接続を行うための単一のデバイスを使用しているユーザーに対して、ポイント・トゥ・ポイント・トンネルプロトコルを作成する Window XP/ 2000 の PPTP に対応しています。

PPTP サーバ有効：	このオプションを選択すると、ポイント・トゥ・ポイント・トンネルプロトコルを使用する PPTP サーバが有効の状態になります。
PPTP IP アドレス範囲：	[ユニファイド IP 管理] をクリックして、設定画面を表示し、リモートユーザーにローカルネットワークに入るときの IP アドレスを提供します。IP 範囲開始：始点 IP アドレスを入力します。IP 範囲終了：終点 IP アドレスを入力します。 
ユーザー名：	リモートユーザー名を入力します。
新しいパスワード： パスワードの確認：	パスワードを入力し、確認のためもう一度新しいパスワードを入力します。

リストに追加：	新しいアカウントとパスワードを追加します。
選択したユーザーを削除：	選択したユーザーを削除します。

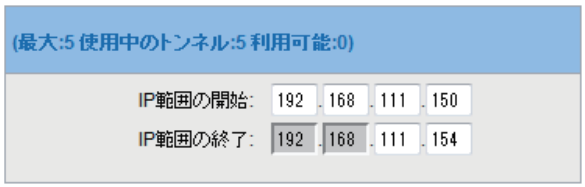
全ての PPTP ステータス：ユーザー名、リモートアドレス、PPTP IP アドレスを含む、すべての接続中のユーザーを表示します。



12.3 L2TP

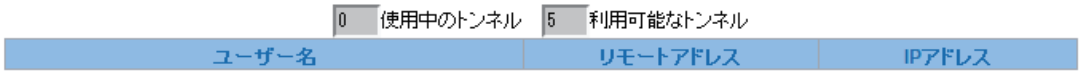
VPN 接続を行うための単一のデバイスを使用しているユーザーに対して、レイヤ 2 トンネルプロトコルを作成するデバイスの L2TP に対応しています。

有効 L2TP サーバ：	このオプションを選択すると、レイヤ 2 トンネルプロトコルを使用する L2TP サーバが有効の状態になります。
MPPE 暗号を使用する:	このオプションを選択すると、MPPE(Microsoft Point to Point Encryption) が有効の状態になります。
L2TP IP アドレス範囲：	［ユニファイド IP 管理］をクリックして、設定画面を表示し、リモートユーザーにローカルネットワークに入るときの IP アドレスを提供します。 IP 範囲の開始：始点 IP アドレスを入力します。 IP 範囲の終了：終点 IP アドレスを入力します。

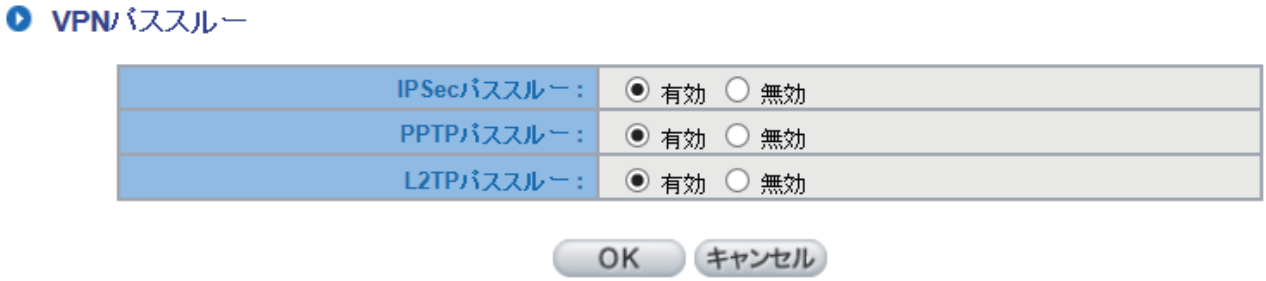
	PPTP/L2TP IPアドレス範囲 
プレシェアードキー：	接続にプレシェアードキーを使用する場合は、テキストボックスに任意の数字や文字を最大 30 文字で入力し、「有効」をチェックします。
ユーザー名：	リモートユーザー名を入力します。
新しいパスワード： パスワードの確認：	パスワードを入力し、確認のためもう一度新しいパスワードを入力します。
リストに追加：	新しいアカウントとパスワードを追加します。
選択したユーザーを削除：	選択したユーザーを削除します。

L2TP トンネルステータス：ユーザー名、リモートアドレス、IP アドレスを含む、すべての接続中のユーザーを表示します。

L2TPトンネルステータス



12.4 VPN パススルー



● **IPSec パススルー：**このオプションを「有効」にした場合は、VPN-IPSec パケットを通過させて外部の VPN デバイスに PC を接続します。

● **PPTP パススルー：**このオプションを「有効」にした場合は、VPN- PPTP パケットを通過させて外部の VPN デバイスに PC を接続します。

● **L2TP パススルー：**このオプションを「有効」にした場合は、VPN-L2TP パケットを通過させて外部の VPN デバイスに PC を接続します。

変更した後に、[OK] ボタンをクリックして、ネットワーク設定を保存します。[キャンセル] ボタンをクリックすると、元の設定が維持されます。

XIII. ログ

ログ管理とルックアップから、関係する動作ステータスを確認します。設定と操作が容易になります。

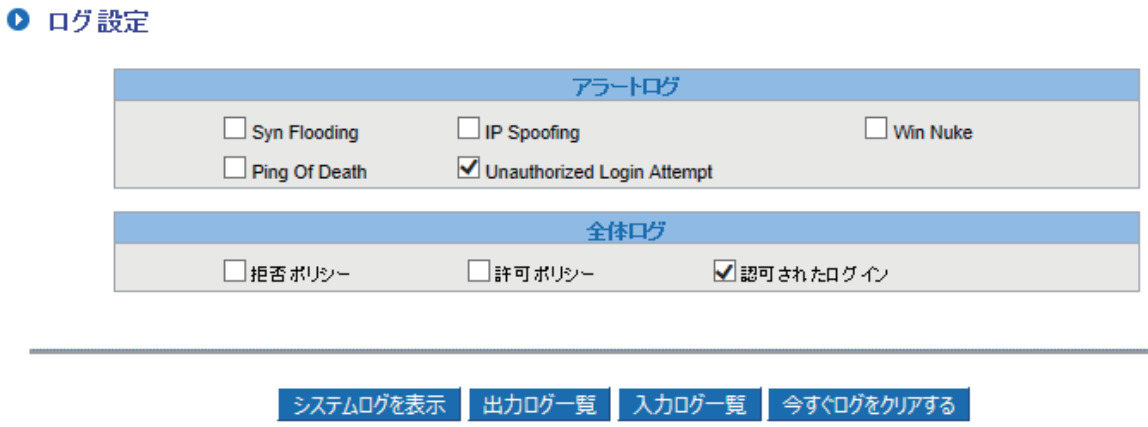
13.1 システムログ

システムログには、システムログ、メールアラート、ログ設定の 3 つのオプションがあります。

Syslog 設定

Syslog を有効にする：	このオプションを選択した場合は、「システムログ」機能が有効の状態になります。
Syslog サーバ：	デバイスによって、外部システムのログサーバに、ログ収集機能が付与されます。システムログは、業界標準の通信プロトコルです。関係するシステムメッセージをネットワークから動的に取得するよう設計されています。システムログは、接続時に使用されている送信元 IP アドレスと送信先 IP アドレス、サービス番号、タイプの情報を提供します。この機能を適用するには、システムログサーバ名または IP アドレスをテキストボックスに入力します。
メールアラート：	このオプションを選択した場合は、「メールアラート」機能が有効の状態になります。
メールサーバ：	すべてのログを送信する場合は、メールサーバ名、または IP アドレスを入力します。例：mail.abc.com
メールの送信先：	システムログの受信側のメールアドレスです。例：abc@mail.abc.com
ログキューの長さ：	ログのエントリ数を設定します。初期設定は「50」です。ここで設定したエントリ数に達したときに、ログメールが自動的に送信されます。
ログ時間の閾値：	ログの送信間隔を設定します。初期設定は「10 分」です。ここで設定した送信間隔に達したときに、ログメールが自動的に送信されます。デバイスが、どのパラメータが最初に閾値に達するか検出し、そのパラメータのログメッセージをユーザーに送信します。
E- mail Log Now：	このボタンをクリックすると、ログがただちに送信されます。

ログ設定



アラートログ

デバイスは、以下のアラートメッセージを提供します。クリックして、各機能を有効の状態にします：「Syn Flooding」、「IP Spoofing」、「Win Nuke」、「Ping of Death」、「Unauthorized Login Attempt」

Syn Flooding：	syn パケットを短期間に大量に送り付けて、接続情報を記録するシステムのストレージ領域をオーバーロードさせます。
IP Spoofing：	パケットを盗聴して、ハッカーがネットワーク上で送信されたデータを妨害します。ハッカーが情報にアクセスした後に、送信者の IP アドレスを変更して、送信元システムのリソースにアクセスします。
Win Nuke：	サーバがトロイの木馬による攻撃を受ける、ないしトロイの木馬を仕掛けられます。
Ping Of Death：	送信データが、IP プロトコルが処理できる最大パケット数を超えることによって、システムが使用不能になります。
Unauthorized Login Attempt：	デバイスへの侵入者を特定した場合に、メッセージがシステムログに送信されます。

全体ログ

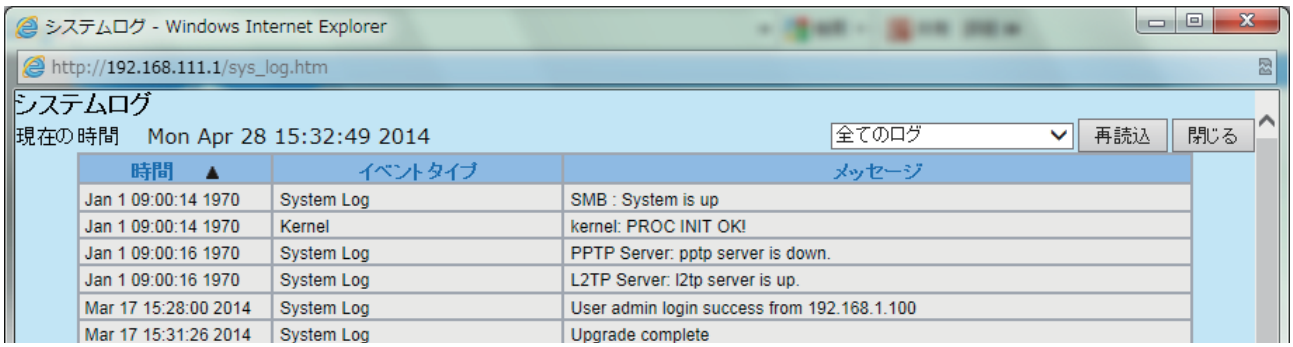
デバイスは、以下のアラートメッセージを提供します。クリックして、各機能を有効の状態にします：「拒否ポリシー」、「許可ポリシー」、「許可されたログイン」

拒否ポリシー：	例えば、アクセスルールにより、リモートユーザーがシステムに入れない場合は、システムログにメッセージが記録されます。
許可ポリシー：	例えば、アクセスルールを順守していることにより、リモートユーザーがシステムに入る場合は、システムログにメッセージが記録されます。
認可されたログイン：	リモート側または LAN 側からデバイスにログインすることも、システムに無事に入れるということになります。システムログにメッセージが記録されます。

ログのオンライン照会を許可する 4 つのボタンについて以下に説明します。

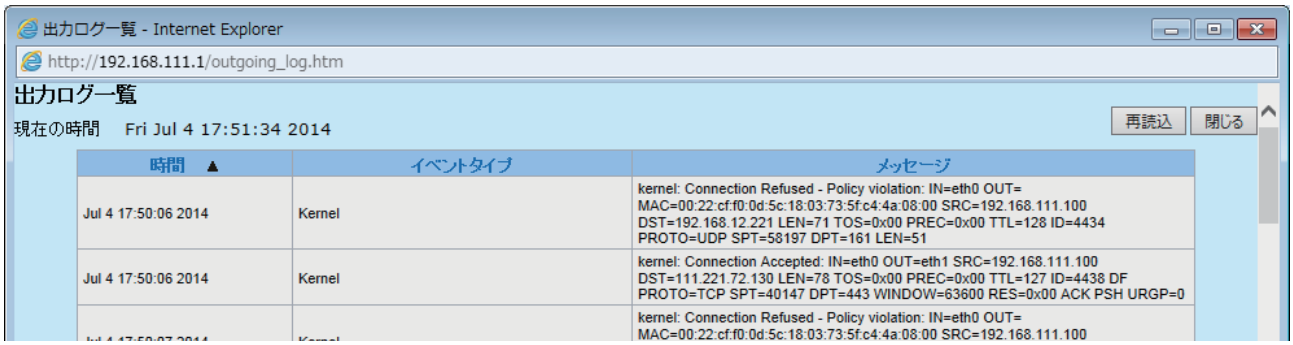
システムログを表示：

システムログを閲覧します。デバイス経由でメッセージの内容をオンラインで読むことができます。以下の図に示すとおり、「全てのログ」、「システムログ」、「アクセスログ」、「ファイアウォールログ」、「VPN ログ」が含まれています。



出力ログ一覧：

内部 PC からインターネットに送信されるシステムパケットログを表示します。適用されている LAN 側 IP アドレス、送信先 IP アドレス、サービスポートが含まれています。以下の図を参照してください。



入力ログ一覧：

ファイアウォールに入ってくるシステムパケットログを表示します。外部送信元 IP アドレス、送信先 IP アドレス、サービスポートが含まれています。以下の図を参照してください。

今すぐログをクリアする：

ログにある現在の情報をすべて消去します。

13.2 システム情報

デバイスには、リアルタイム監視機能が装備されています。ポートの場所、デバイス名、WAN の現在の接続ステータス、IP アドレス、MAC アドレス、サブネットマスク、デフォルトゲートウェイ、DNS、送受信パケット総数、送受信バイト総数、送受信バイト / 秒、受信したエラーパケット総数、廃棄パケット総数、セッション数、新規セッション数 / 秒、上り下りブロードバンド使用率など、システムの現在の稼働情報を提示します。

システム情報

インターフェース	WAN1	LAN		
デバイス名	eth1	eth0		
ステータス	接続	---		
デバイスIPアドレス	192.168.0.19	192.168.111.1		
MACアドレス	EC-F0-0E-1D-D3-9D	EC-F0-0E-1D-D3-9C		
サブネットマスク	255.255.255.0	255.255.255.0		
デフォルトゲートウェイ	192.168.0.99	---		
DNS	192.168.0.99	---		
ネットワークサービス検出	テスト成功	---		
Received Packets	待機中	待機中	待機中	待機中
Transmitted Packets	待機中	待機中	待機中	待機中
Total Packets	待機中	待機中		
Received Packets Byte	待機中	待機中	待機中	待機中
Transmitted Packets Byte	待機中	待機中	待機中	待機中
Total Packets Byte	待機中	待機中		
Received Byte/Sec	待機中	待機中	待機中	待機中
Transmitted Byte/Sec	待機中	待機中	待機中	待機中
Error Packets	待機中	待機中	待機中	待機中
Dropped Packets	待機中	待機中	待機中	待機中
セッション	0	---		
New セッション/秒	0	---		
使用中の上りバンド幅	待機中	待機中	待機中	待機中
使用中の下りバンド幅	待機中	待機中	待機中	待機中

13.3 トラフィック情報

「システム情報」ページに 6 つのメッセージが表示され、トラフィックをより良く管理・制御できるようにします。

入力 IP アドレス：

送信元 IP アドレス、バイト / 秒、パーセンテージが表示されます。

出力 IP アドレス：

送信元 IP アドレス、バイト / 秒、パーセンテージが表示されます。

出力ポート：

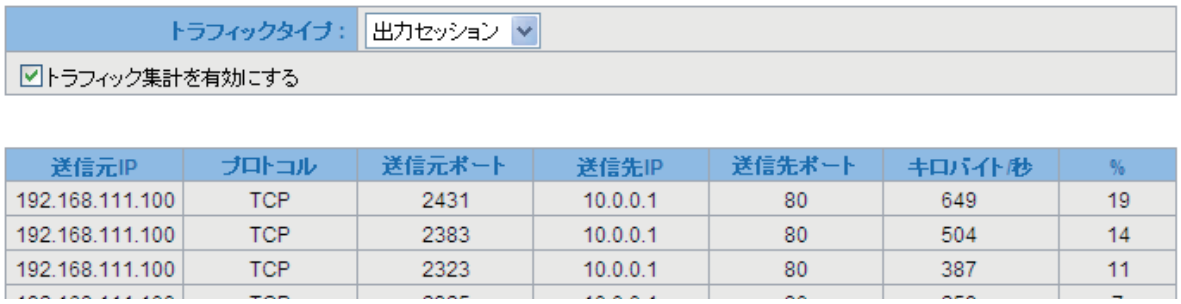
ネットワークプロトコルタイプ、送信先ポート、バイト / 秒、パーセンテージが表示されます。

トラフィック情報

入力ポート：

ネットワークプロトコルタイプ、送信先ポート、バイト / 秒、パーセンテージが表示されます。

トラフィック情報



出力セッション：

送信元 IP アドレス、ネットワークプロトコルタイプ、送信元ポート、送信先 IP アドレス、送信先ポート、バイト / 秒、パーセンテージが表示されます。

トラフィック情報

入力セッション：

送信元 IP アドレス、ネットワークプロトコルタイプ、送信元ポート、送信先 IP アドレス、送信先ポート、バイト / 秒、パーセンテージが表示されます。

13.4 IP/ ポート情報

管理者が特定の IP アドレスに (または特定のポートから)、この IP アドレスがアクセスしたアドレスについて、ないしこのサービスポートを使用したユーザー (送信元 IP アドレス) について、照会できます。 これにより、認証が必要であるものの、複数の WAN ではなく単一の WAN ポートを許可する Web サイトの特定が容易になります。管理者は、プロトコルバインディングのための送信先 IP アドレスを検索して、このログイン問題を解決できます。例えば、特定のポートのソフトウェアが拒否されたときは、この特定のソフトウェアのサーバポートの IP アドレスにこの機能を適用します。また、BT ないし P2P ソフトウェアを検索するには、この機能を選択して、ポートからユーザーを照会します。

特定の IP ステータス：

照会対象の IP アドレスを入力すると、リモートデバイスに接続されているすべての送信先 IP アドレスと、ポート数が表示されます。

特定のポートステータス：

サービスポート番号を入力すると、このポートが現在使用している IP アドレスが表示されます。

IP/ポート情報

有効 IP/ポート情報 ポート ▼ ポート : 80 検索

送信元IP	プロトコル	送信元ポート	インターフェース (WAN)	送信先IP	送信先ポート	下り バイト/秒	上り バイト/秒
192.168.111.107	TCP	50403	WAN1	192.168.111.113	80	339	342
192.168.111.107	TCP	50404	WAN1	192.168.111.113	80	26	26
192.168.111.107	TCP	50401	WAN1	192.168.111.113	80	0	0
192.168.22.150	TCP	50368	WAN1	192.168.22.100	80	0	0
192.168.22.150	TCP	50369	WAN1	192.168.22.100	80	0	0
192.168.111.107	TCP	50400	WAN1	192.168.111.113	80	0	0

再読込

XIV. ログアウト

Web ベースの UI の右上端に、ログアウトボタンがあります。このボタンをクリックすると、ポップアップウィンドウが表示されます。[OK] をクリックして、Web ベースの UI をログアウトします。[キャンセル] をクリックすると、UI に戻ります。次回ログインするには、Web ブラウザーを起動して、ログイン用の IP アドレス、ユーザー名とパスワードを入力します。