613-000685 Rev.E 081128

ベーシックVPNアクセス・ルーター

CentreCOM® AR260S V2

リファレンスマニュアル

Allied Telesis

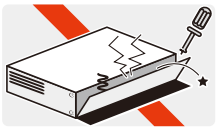
安全のために

必ずお守りください

警告 下記の注意事項を守らないと**火災・感電**により、**死亡や大けが**の原因となります。

分解や改造をしない

本製品は、取扱説明書に記載のない分解や改造はしないでください。
火災や感電、けがの原因となります。



雷のときはケーブル類・機器類にさわらない

感電の原因となります。

異物は入れない　水は禁物

火災や感電のおそれがあります。水や異物を入れないように注意してください。万一水や異物が入った場合は、電源プラグをコンセントから抜いてください。（当社のサポートセンターまたは販売店にご連絡ください。）

通風口はふさがない

内部に熱がこもり、火災の原因となります。

湿気やほこりの多いところ、油煙や湯気のあたる場所には置かない

内部回路のショートの原因になり、火災や感電のおそれがあります。

表示以外の電圧では使用しない

火災や感電の原因となります。
本製品に付属の AC アダプターは AC100-120V で動作します。

付属の電源アダプター以外使用しない

火災や感電の原因となります。
必ず、付属の AC アダプターを使用してください。

コンセントや配線器具の定格を超える使い方はしない

たこ足配線などで定格を超えると発熱による火災の原因となります。

設置・移動の時は電源プラグを抜く

感電の原因となります。

ケーブル類を傷つけない

特に電源ケーブルは火災や感電の原因となります。
電源ケーブルやプラグの取扱上の注意
・加工しない、傷つけない。
・重いものをのせない。
・熱器具に近づけない、加熱しない。
・ケーブル類をコンセントから抜くときは、必ずプラグを持って抜く。


傷つけない

正しく設置する　縦置き注意

取扱説明書に従って、正しく設置してください。
不適切な設置により、放熱が妨げられると、発熱による火災の原因となります。


正しく設置

ご使用にあたってのお願い

次のような場所での使用や保管はしないでください

・直射日光の当たる場所
・暖房器具の近くなどの高温になる場所
・急激な温度変化のある場所（結露するような場所）
・湿気の多い場所や、水などの液体がかかる場所（仕様に定められた環境条件下でご使用ください）
・振動の激しい場所
・ほこりの多い場所や、ジュータンを敷いた場所（静電気障害の原因になります）
・腐食性ガスの発生する場所

静電気注意

本製品は、静電気に敏感な部品を使用しています。部品が静電破壊されるおそれがありますので、コネクターの接点部分、ポート、部品などに素手で触れないでください。

取り扱いはていねいに

落としたり、ぶつけたり、強いショックを与えたりしないでください。

お手入れについて

清掃するときは電源を切った状態で

誤動作の原因になります。


プラグを抜く

機器は、乾いた柔らかい布で拭く

汚れがひどい場合は、柔らかい布に薄めた台所用洗剤（中性）をしみこませ、固く絞ったもので拭き、乾いた柔らかい布で仕上げてください。

ぬらさない　中性洗剤使用　固く絞る

お手入れには次のものは使わないでください

石油・シンナー・ベンジン・ワックス・熱湯・粉せっけん・みがき粉
（化学ぞうきんをご使用のときは、その注意書に従ってください。）


シンナー類不可

はじめに

このたびは、CentreCOM AR260S V2 をお買い上げいただき、誠にありがとうございます。

CentreCOM AR260S V2 は、SOHO 向けベーシック VPN アクセス・ルーターです。

本リファレンスマニュアルでは、CentreCOM AR260S V2 の GUI 設定について解説しています。本製品を活用するための参考資料としてご利用ください。

なお、設定を行う前に必要なこと、例えばルーターや LAN/WAN の配線、インターネットへの接続などについては説明しておりません。これらに関しては、製品付属の冊子「取扱説明書」をご覧ください。

本書の構成

章構成

本書は大きな機能ごとに、以下のような章構成になっています。また、各章では一部を除き、「機能の概要」、「設定手順」、「設定画面の解説」の流れになっています。

「1 運用・管理」では

本製品の運用・管理に関する以下の設定について説明します。

- ログイン
- 再起動
- ログアウト
- 機能の有効化 / 無効化の設定
- 設定管理クライアント / ログインパスワードの設定
- システム情報の設定
- システム時刻の設定
- SNMP エージェントの設定
- ログの記録
- 設定の初期化
- 設定内容のバックアップ
- バックアップファイルの復元
- ファームウェアの更新
- テクニカルサポート情報の取得
- Ping の送信

「2 LAN 側インターフェースの設定」では

LAN 側インターフェースの IP 情報や DHCP サーバー機能に関する設定について説明します。

「3 WAN 側インターフェースの設定」では

WAN 側の接続形態別（DHCP、PPPoE、固定 IP）に WAN 側インターフェースやダイナミック DNS に関する設定について説明します。

「4 ルーティングの設定」では

ルーティングに関する設定について説明します。本製品では、スタティックルーティングをサポートしています。

「5 ファイアウォール /NAT の設定」では

ファイアウォールおよび NAT 機能に関する以下の設定について説明します。

- アクセス制御の設定
- ステルスモードの設定
- セルフアクセスルールの設定
- NAT の設定
- NAT プールの設定
- タイムアウトの設定
- トラフィックの確認
- URL フィルターの設定
- DoS 検出の設定
- UPnP の設定

「6 VPN の設定」では

VPN 機能に関する設定について説明します。本製品の VPN 機能は IPsec に準拠しています。

対象ファームウェアバージョンについて

本書は、本製品のファームウェアバージョン「3.1.0」をもとに記述されています。本製品をご使用の際は、必ず弊社 Web ページに掲載のリリースノートをお読みになり、最新の情報をご確認ください。リリースノートには、バージョンごとの注意事項や最新情報が記載されています。

表記上の注意

本書で使用しているアイコンは次の意味で使用しています。

アイコン	意 味	説 明
 ヒント	ヒント	知っていると便利な情報、操作の手助けになる情報を示しています。
 注意	注意	物的損害や使用者が傷害を負うことが想定される内容を示しています。
 警告	警告	使用者が死亡または重傷を負うことが想定される内容を示しています。
	参照	関連する情報が書かれているところを示しています。

例について

本書では、設定画面に数多くの入力例を使用しています。電話番号、IP アドレス、ドメイン名、ログイン名、パスワードなどに具体的な文字列や値を使用していますが、これらは例として挙げただけの架空のものです。実際に運用を行う場合は、お客様の環境におけるものをご使用ください。

最新情報

製品の出荷後は、弊社 Web サイトでマニュアル等の正誤情報や改版されたマニュアル、アップデートされたファームウェアなどの最新の情報を公開しています。

http://www.allied-telesis.co.jp/

目次

1　運用・管理

本章では、本製品の運用・管理に関する以下の設定について説明します。

- ログイン
- 再起動
- ログアウト
- 機能の有効化 / 無効化の設定
- 設定管理クライアント / ログインパスワードの設定
- システム情報の設定
- システム時刻の設定
- SNMP エージェントの設定
- ログの記録
- 設定の初期化
- 設定内容のバックアップ
- バックアップファイルの復元
- ファームウェアの更新
- テクニカルサポート情報の取得
- Ping の送信

1.1　ログイン

本製品にログインするには以下の手順を実行します。

ヒント　**ここでは、本製品の LAN 側インターフェースの IP アドレスがデフォルト設定 (192.168.1.1) であるものとします。**

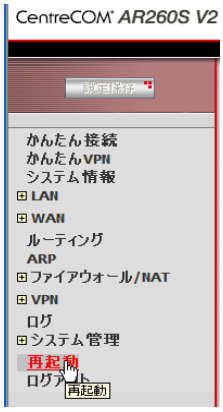
1. Web ブラウザーを起動後、アドレス欄に「192.168.1.1」を指定してアクセスします。
2. ダイアログで「ユーザー名」と「パスワード」を入力し「OK」ボタンをクリックします。本製品のデフォルトではユーザー名「manager」、パスワード「friend」です。

3. 本製品の設定画面が表示されたらログインは完了です。

1.2 再起動

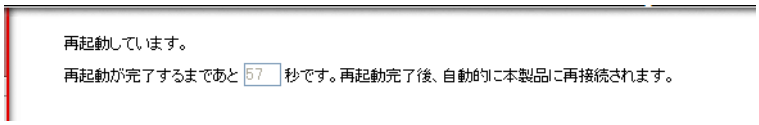
本製品を再起動するには以下の手順を実行します。

1. メニューから「再起動」をクリックします。

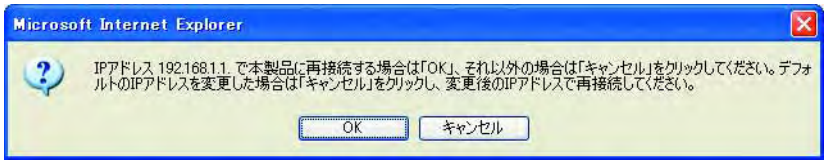


2.「適用」ボタンをクリックします。

3. 以下の画面が表示され、再起動に必要な時間がカウントダウンされます。カウントダウン終了までしばらくお待ちください。



4. カウントダウンが終了すると、以下のダイアログが表示されます。



本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

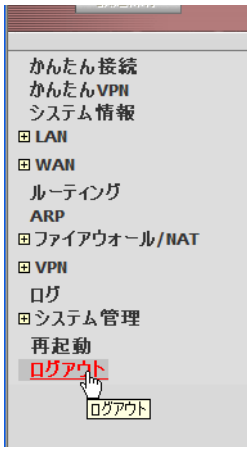
ヒント **変更後の本製品の IP アドレスが、接続するコンピューターと異なるサブネットになる場合、本製品に接続できなくなります。必要に応じてコンピューターの TCP/IP 設定も変更してください。**

5. 以上で再起動は完了です。

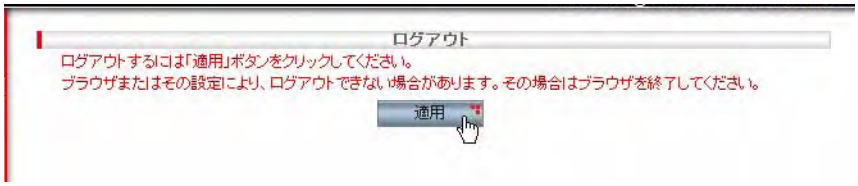
1.3 ログアウト

本製品からログアウトするには以下の手順を実行します。

1. メニューから「ログアウト」をクリックします。



2.「適用」ボタンをクリックします。



3. 以下のダイアログが表示されたら「はい」ボタンをクリックします。

4. 以上でログアウトは完了です。

1.4 機能の有効化 / 無効化の設定

1.4.1 概要

本製品では、以下の各種機能を「サービスの有効 / 無効」ページで有効化 / 無効化することができます。

- ファイアウォール機能
- ブリッジ機能
- VPN 機能 /SA の強制確立
- DNS リレー機能
- DHCP サーバー機能
- SNTP 機能
- SNMP 機能
- ダイナミック DNS 機能
- リセットスイッチによる初期化機能

1.4.2 機能の有効化 / 無効化

各機能を有効化 / 無効化するには以下の手順を実行します。

1. メニューから「システム管理」->「サービスの有効 / 無効」の順にクリックします。

2. 機能の有効 / 無効を選択し、「適用」ボタンをクリックします。ここでは、以下の機能を無効にしています。

- VPN
- リセットスイッチによる初期化

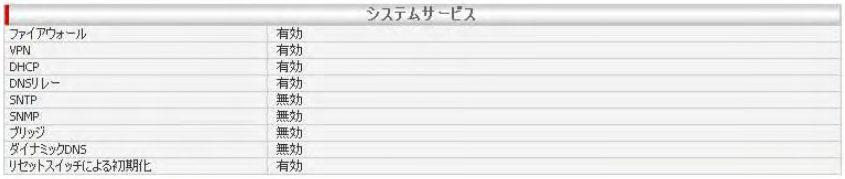
3. 以上で設定は完了です。

1.4.3 機能の有効 / 無効の確認

機能の有効 / 無効を確認するには以下の手順を実行します。

1. メニューから「システム情報」をクリックします。

2.「システムサービス」に機能の有効 / 無効が一覧表示されます。



1.4.4 「サービスの有効 / 無効」ページの解説

サービスの有効 / 無効ページについて解説します。「サービスの有効 / 無効」ページでは、サービスを有効 / 無効にすることができます。

メニューから「システム管理」->「サービスの有効 / 無効」の順にクリックすると設定画面が表示されます。

パラメーター	オプション	説明
ファイアウォール	有効 / 無効	ファイアウォール機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。ファイアウォールを無効にした場合、外部からのアクセスが容易になりますのでご注意ください。ファイアウォールの設定については「P.101 ファイアウォール /NAT の設定」を参照してください。デフォルトは「有効」です。
	セルフアクセス	有効の場合、設定されているルールに従って、本製品宛のパケットをチェックします。通過ルールにマッチした場合のみ許可し、それ以外の場合には破棄されます。 無効の場合、設定されているルールに関係なく、本製品宛のパケットをすべて許可します。 デフォルトは「有効」です。
	アクセス制御	有効の場合、設定されているルールに従って、本製品を経由するパケットをチェックします。通過ルールにマッチした場合のみ許可し、それ以外の場合には破棄されます。 無効の場合、設定されているルールに関係なく、本製品を経由するパケットをすべて許可します。 デフォルトは「有効」です。
	NAT	有効の場合、設定されているルールに従って、本製品宛、または本製品を経由するパケットが NAT ルールにマッチするかチェックします。NAT ルールにマッチしたパケットはルールに従ってアドレス等の変換が行われます。 無効の場合、設定されているルールに関係なく、アドレス等の変換を行いません。 デフォルトは「有効」です。
	URL フィルター	有効の場合、LAN 側からアクセスされる HTTP パケットに対し、URL フィルターに登録されているルールに従って、URL の合否を判定（通過または破棄）しま

			す。 無効の場合、URL フィルターに登録されているルールに関係なく、HTTP パケットの解析を行いません。 デフォルトは「無効」です。
		DoS	有効の場合、設定されている DoS（Denial of Service）アタック種別に従って、WAN 側からアクセスされるパケットに対し、アタック検知処理が実行されます。アタックを検知した場合は、該当パケットに対して「通過」または「破棄」を選択することができます。 無効の場合、アタック検知処理は実行されません。 デフォルトは「有効」です。
		UPnP	有効の場合、UPnP クライアントからの要求に応答し、その要求に応じたポートマッピングルールを作成します。 無効の場合、UPnP クライアントの要求に応答しません。 デフォルトは「無効」です。
ブリッジ		有効 / 無効	ブリッジ機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。ブリッジを有効にした場合、設定しているプロトコルのパケットを LAN、WAN 間で中継します。デフォルトは「無効」です。
		IPv6 ブリッジ	有効の場合、IPv6 のパケットを中継します。無効の場合は中継されません。 デフォルトは「有効」です。
		PPPoE ブリッジ	有効の場合、PPPoE パケットを中継します。無効の場合は中継されません。 デフォルトは「無効」です。
VPN		有効 / 無効	VPN サービスを有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。「P.151 VPN の設定」の設定を行う場合は、あらかじめ VPN サービスを有効にしてください。 デフォルトは「有効」です。
SA の強制確立		有効 / 無効	SA の強制確立を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。VPN サービスに「有効」を選択している場合のみ表示されます。 SA の強制確立とは、本製品と対向機器が保持する ISAKMP SA あるいは、IPsec SA に矛盾が発生した場合、本製品から新たに SA を再確立させる機能です。SA の矛盾とは、対向機器が使用している SA を本製品が保持していない状態を示します。 デフォルトは「無効」です。
DHCP		有効 / 無効	DHCP サーバー機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。無効にした場合は、LAN 内のコンピューターの IP 設定を正確に行ってください。DHCP サーバー機能の詳細については「P.62 DHCP サーバーの設定」を参照してください。デフォルトは「有効」です。

SNTP	有効 / 無効	外部 SNTP サーバーから時刻情報を取得する場合は「有効」、取得しない場合は「無効」ラジオボタンをクリックします。SNTP サーバーの詳細については「P.33 システム時刻の設定」を参照してください。デフォルトは「無効」です。
DNS リレー	有効 / 無効	DNS リレー機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。デフォルトは「有効」です。
SNMP	有効 / 無効	SNMP 機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。SNMP 機能の詳細については「P.38 SNMP エージェントの設定」を参照してください。デフォルトは「無効」です。
ダイナミック DNS	有効 / 無効	ダイナミック DNS 機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。デフォルトは「無効」です。
リセットスイッチによる初期化	有効 / 無効	リセットスイッチを押した場合に、本製品の設定をデフォルト値に戻す機能を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンを選択します。デフォルトは「有効」です。この設定は「設定保存」では保存されません。「リセットスイッチによる初期化」を無効にした状態で、管理者パスワードを忘れた場合、本製品の設定を初期化することができなくなりますのでご注意ください。
「適用」ボタン		設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

1.5 設定管理クライアント / ログインパスワードの設定

1.5.1 概要

本製品では、「設定管理 / パスワード」ページで、クライアントに対して本製品の設定権限を付与し、設定管理クライアントとして登録することができます。また、ログインパスワードは管理者レベルのユーザーとユーザーレベルのユーザーに対してそれぞれパスワードが設定されています。ここでは、設定管理クライアントとパスワードに関して説明します。

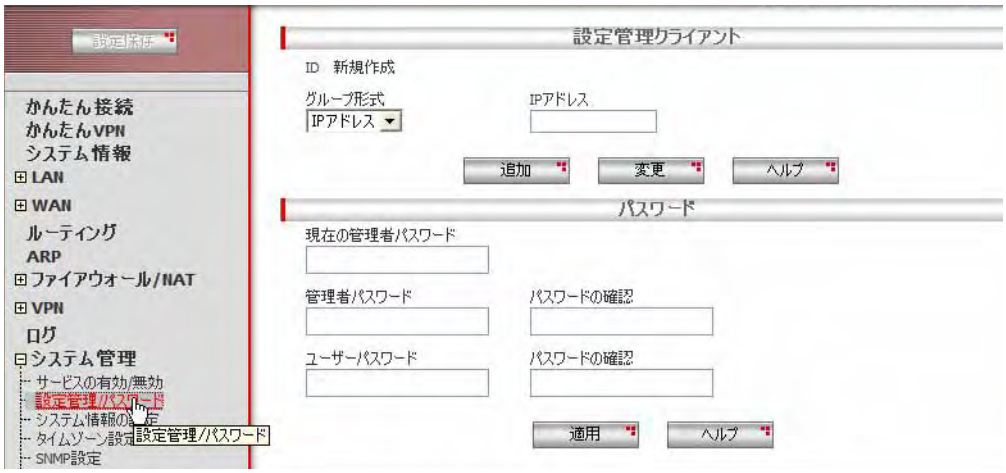
1.5.2 設定管理クライアントの設定

ここでは、設定管理クライアントの設定方法について説明します。

1.5.2.1 設定管理クライアントの作成

設定管理クライアントを作成するには以下の手順を実行します。

1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。



2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のように設定するものとします。

グループ形式	IP アドレス
IP アドレス	192.168.1.10

注意 設定管理クライアントには、現在本製品を操作している端末が含まれる IP アドレスまたはネットワークアドレスを最初に設定してください。最初に登録していない場合、その後の操作ができなくなります。

ヒント

WAN 側のクライアントを設定管理クライアントとして追加した場合、セルフアクセスルールで WAN 側からのアクセスについて HTTP の 80 番ポートをオープンする必要があります。セルフアクセスルールについては「P.112 セルフアクセスルールの設定」を参照してください。

3. 以上で設定は完了です。

1.5.2.2 設定管理クライアントの変更

設定管理クライアントを変更するには以下の手順を実行します。

1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
2. 「設定管理クライアントリスト」テーブルの該当クライアント左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

1.5.2.3 設定管理クライアントの削除

1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
2. 「設定管理クライアントリスト」テーブルの該当クライアント左部にあるラジオボタンをクリックして選択します。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

1.5.2.4 設定管理クライアントの確認

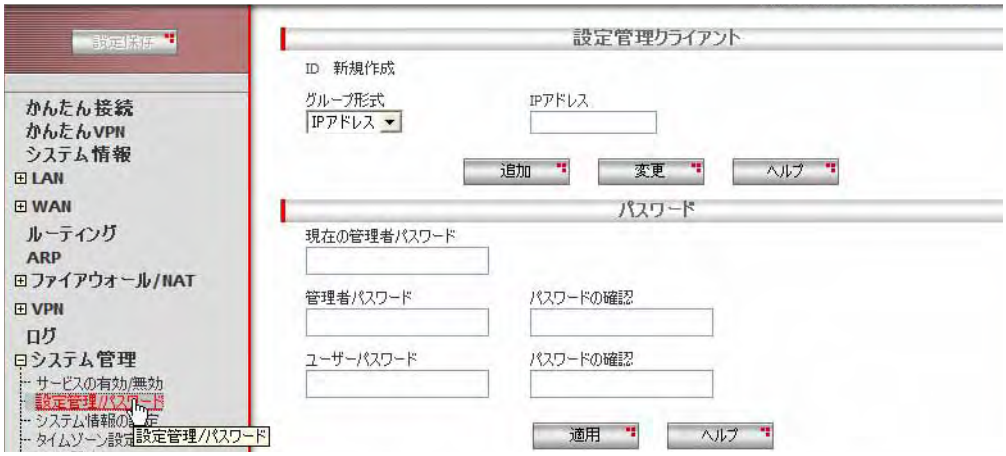
1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
2. 「設定管理クライアントリスト」テーブルにクライアントが一覧表示されます

1.5.3 パスワードの設定

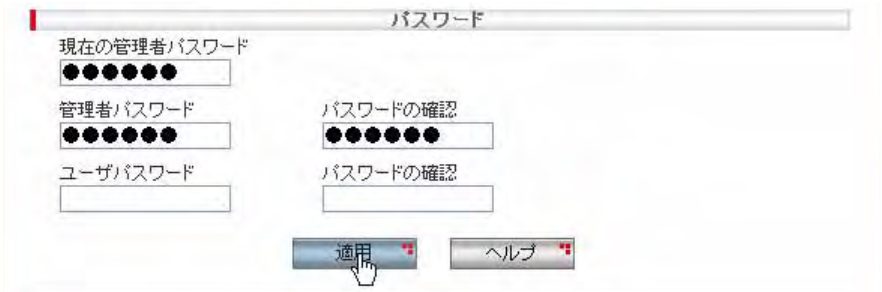
本製品に設定されている管理者レベル / ユーザーレベルのパスワードは以下のとおりです。ここでは、パスワードの設定について説明します。

ユーザー名	レベル	パスワード
manager	管理者	friend
guest	ユーザー	guest

1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。



2.「パスワード」テーブルで各パラメーターを入力し、「適用」ボタンをクリックします。ここでは、現在の管理者レベルのログインパスワード「friend」を「AR260S」に変更するものとします。



ヒント **「現在の管理者パスワード」には、現在設定されている管理者レベルのパスワードを入力してください。**

3. ログイン画面が表示されますので、「パスワード」に新しく設定したパスワードを入力して「OK」ボタンをクリックします。

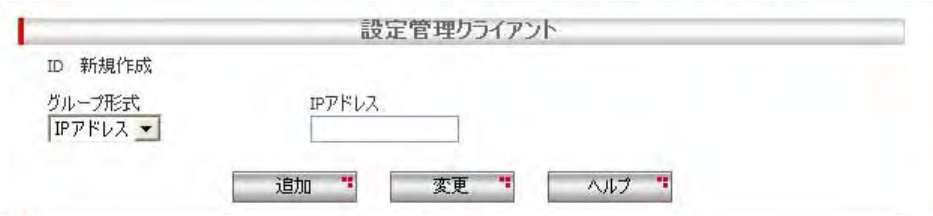
4. 以上で設定は完了です。

1.5.4 「設定管理クライアント / パスワード」ページの解説

「設定管理クライアント / パスワード」ページについて解説します。

1.5.4.1 設定管理クライアント

設定管理クライアントとは、本製品の設定権限をもつクライアントです。「設定管理クライアント」テーブルでは、クライアントを IP アドレスで指定して、本製品の設定権限を付与することができます。



注意 設定管理クライアントを設定した場合、設定されたクライアント以外のクライアントからは本製品の設定が不可能になりますのでご注意ください。

パラメーター	オプション	説明
ID		設定管理クライアントを新規に追加する場合は「新規追加」、既存のクライアントの設定を変更 / 削除する場合は該当の ID 番号が表示されます。
グループ形式		クライアントの指定方法を選択します。
	IP アドレス	クライアントを IP アドレスで指定する場合に選択します。
	サブネット	クライアントをサブネットで指定する場合に選択します。

IP アドレス	グループ形式に「IP アドレス」を選択した場合にのみ表示されます。クライアントの IP アドレスを入力します。
ネットワークアドレス	グループ形式に「サブネット」を選択した場合にのみ表示されます。指定するクライアントのネットワークアドレスを入力します。
サブネットマスク	グループ形式に「サブネット」を選択した場合にのみ表示されます。指定するクライアントのサブネットマスクを入力します。
「追加」ボタン	クライアントを追加登録します。30 件までのエントリーを追加することができます。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン	設定内容の変更を保存します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

1.5.4.2 パスワード

本製品には以下の 2 種類のユーザー名 / パスワードがあります。

ユーザー名	パスワード	説明
manager	friend	管理者レベルのユーザー名とパスワードです。管理者には設定変更の権限があります。パスワードは変更することができますが、ユーザー名を変更することはできません。
guest	guest	ユーザーレベルのユーザー名とパスワードです。設定を参照することはできますが、変更する権限はありません。パスワードは変更することができますが、ユーザー名を変更することはできません。

「パスワード」テーブルでは、本製品のユーザー（manager/guest）に対してパスワードを設定します。

パラメーター	オプション	説明
現在の管理者パスワード		「管理者パスワード」、「ユーザーパスワード」を設定する前に現在の管理者パスワードを入力します。ここに誤ったパ

		スワードを入力した場合、以下のパスワードの設定ができません。
管理者パスワード		「manager」に対するパスワードを設定変更します。新しく設定するパスワードを入力します。半角英数字（または一部の記号）で 32 文字以内で入力してください。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + − . （ピリオド） = @ [ ] ^ _（下線） { } ~ , （カンマ）
	パスワードの確認	確認のために、再度同じパスワードを入力します。
ユーザーパスワード		「guest」に対するパスワードを設定変更します。新しく設定するパスワードを入力します。半角英数字（または一部の記号）で 32 文字以内で入力してください。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + − . （ピリオド） = @ [ ] ^ _（下線） { } ~ , （カンマ）
	パスワードの確認	確認のために、再度同じパスワードを入力します。
「適用」ボタン		設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映され、再び本製品へのログインを求めるダイアログが表示されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

1.5.4.3 設定管理クライアントリスト

「設定管理クライアントリスト」テーブルには、「設定管理クライアント」で設定したクライアントが一覧表示されます。

パラメーター	説明
ID	クライアントの ID が表示されます。各クライアントの設定内容を変更または削除するには、対象 ID のラジオボタンを選択します。
グループ形式	クライアントの指定形式が表示されます。

グループアドレス	クライアントの IP 情報が表示されます。
「削除」ボタン	クリックすると「設定管理クライアントリスト」から選択したクライアントを削除します。


注意

設定管理クライアントリストに表示されたクライアント以外からは本製品にアクセスできませんのでご注意ください。

1.6 システム情報の設定

1.6.1 概要

本製品では「システム情報」ページで「システム名」、「システムロケーション」、「連絡先」を設定することができます。ここで設定された項目は、SNMP でそれぞれ sysName、sysLocation、sysContact として扱われます。

ここでは、これらの情報の設定方法について説明します。

1.6.2 システム情報の設定

システム情報を設定するには以下の手順を実行します。

1. メニューから「システム管理」->「システム情報」の順にクリックします。

2. 各パラメーターを入力し「適用」ボタンをクリックします。ここでは、以下のように設定するものとします。

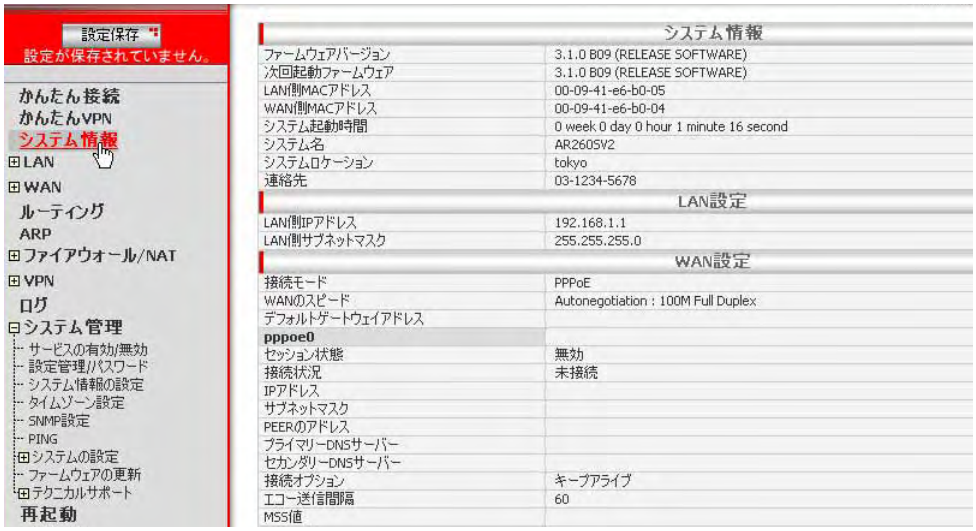
システム名	AR260SV2
システムロケーション	tokyo
連絡先	03-1234-5678

3. 以上で設定は完了です。

1.6.3 システム情報の確認

システム情報を確認するには以下の手順を実行します。

1. メニューから「システム情報」をクリックします。



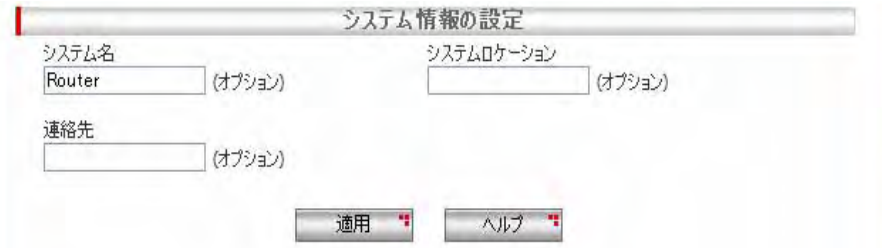
2.「システム情報」に設定したシステム情報が表示されます。

パラメーター	説明
ファームウェアバージョン	現在起動しているファームウェアのバージョンが表示されます。
次回起動ファームウェア	再起動後に起動するファームウェアのバージョンが表示されます。ファームウェア更新を行ったとき、次に起動するファームウェアのバージョンを確認できます。
LAN 側 MAC アドレス	本製品の LAN 側の MAC アドレスが表示されます。
WAN 側 MAC アドレス	本製品の WAN 側の MAC アドレスが表示されます。プロバイダーに本製品の MAC アドレスを通知する場合は、この MAC アドレスを通知してください。
システム起動時間	本製品が起動してから経過した時間が表示されます。
システム名	「システム管理」の「システム情報」ページで設定した「システム名」(sysName) が表示されます。

システムロケーション	「システム管理」の「システム情報」ページで設定した「システムロケーション」(sysLocation) が表示されます。
連絡先	「システム管理」の「システム情報」ページで設定した「連絡先」(sysContact) が表示されます。

1.6.4 「システム情報」ページの解説

「システム情報」ページについて解説します。



パラメーター	説明
システム名	本製品のシステム名を入力します。入力は任意です。デフォルトは「Router」です。半角英数字（または一部の記号）で 128 文字以内で入力してください。また、システム名の先頭文字は、アルファベット文字でなければなりません。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + - . (ピリオド) = @ [ ] ^ _ (下線) { } ~ , (カンマ)
システムロケーション	本製品の設置場所を入力します。半角英数字（または一部の記号と、先頭以外の空白文字）で 63 文字以内で入力してください。入力は任意です。
連絡先	連絡先を入力します。半角英数字（または一部の記号と、先頭以外の空白文字）で 63 文字以内で入力してください。入力は任意です。
「適用」ボタン	設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

1.7 システム時刻の設定

1.7.1 概要

本製品ではシステム時刻を「タイムゾーン設定」ページで設定します。本製品は SNTP クライアント機能を持つため、外部 SNTP サーバーを利用した時刻同期が可能です。

ここでは手動で時刻を設定する方法と、外部 SNTP サーバーを利用するための設定方法を説明します。

1.7.2 システム時刻の設定

システム時刻を設定するには以下の手順を実行します。

1. メニューから「システム管理」->「タイムゾーン設定」の順にクリックします。

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは、「2007 年 1 月 23 日 12 時 34 分 00 秒」に設定し、タイムゾーンは「GMT+9:00」を選択するものとします。

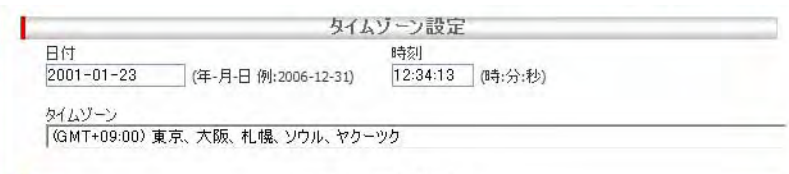
3. 以上で設定は完了です。SNTP サービスを動作させるには、SNTP 機能を有効にする必要があります。設定方法は「P. 18 機能の有効化 / 無効化の設定」を参照してください。

1.7.3 システム時刻の確認

システム時刻を確認するには以下の手順を実行します。

1. メニューから「システム管理」->「タイムゾーン設定」をクリックします。

2.「タイムゾーン設定」テーブルに現在の時刻が表示されます。



1.7.4 SNTP サーバーの設定

SNTP サーバーとは、時刻情報サーバーを階層的に構成し、時刻を同期するサーバーです。本製品は SNTP クライアント機能をもつため、外部 SNTP サーバーの IP アドレスを指定し、時刻を同期することができます。SNTP サーバーの IP アドレスを指定するには以下の手順を実行します。

1. メニューから「システム管理」->「タイムゾーン設定」をクリックします。

2.「SNTP サービスの設定」テーブルの各パラメーターを設定し「適用」ボタンをクリックします。ここでは、SNTP サーバー 1 ～ 4 をそれぞれ「192.168.1.5」、「133.243.238.243」、「133.243.238.244」、「210.173.160.27」、更新間隔を「120 分」に設定するものとします。

3. 以上で設定は完了です。

1.7.5 「タイムゾーン設定」ページの解説

「タイムゾーン設定」ページについて解説します。「タイムゾーン設定」ページでは、本製品のシステム時刻や外部 SNTP サーバーを設定します。

1.7.5.1 タイムゾーン設定

「タイムゾーン設定」テーブルでは、システム時刻とタイムゾーンを設定します。

パラメーター	説明
日付	日付を入力します。入力形式は「西暦年－月－日」です。
時刻	時刻を入力します。入力形式は「時：分：秒」です。
タイムゾーン	タイムゾーンを選択します。

ヒント

本製品はリアルタイムクロック機能を持たないため、電源をオフにするとシステム時刻は「2001 年 1 月 1 日 9 時 0 分 0 秒」に戻ります。

1.7.5.2 SNTP サービスの設定

「SNTP サービスの設定」テーブルでは、時刻の同期を行う外部の SNTP サーバーを設定します。

パラメーター		説明
SNTP サーバー 1 ～ 4		外部の SNTP サーバーの IP アドレスを入力します。SNTP サーバー 1 ～ 4 はすべて異なる IP アドレスを入力する必要があります。
更新間隔		SNTP サーバーと同期を行う間隔を分単位で入力します。1 分～ 525600 分の範囲で入力してください。
送信元 IP アドレス		SNTP パケットの送信元 IP アドレスを入力します。
	自動選択	SNTP パケットが送信されるインターフェースの IP アドレスを本製品が自動的に選択します。VPN 経由で送信する場合は、「自動選択」を選択せず、「LAN」を選択してください。
	LAN	送信元 IP アドレスとして、本製品の LAN 側 IP アドレスを使用します。VPN 経由で送信する場合は、こちらを選択します。
	WAN	送信元 IP アドレスとして、本製品の WAN 側 IP アドレスを使用します。「eth0」（固定 IP/DHCP 使用時）、「pppoe0」または「pppoe1」（PPPoE 使用

	時）のいずれかを選択します。なお、PPPoE が、アンナンバード設定の場合は、LAN 側 IP アドレスが使用されます。
「適用」ボタン	設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

SNTP サービスを動作させるには、SNTP 機能を有効にする必要があります。設定方法は「P.18 機能の有効化 / 無効化の設定」を参照してください。

1.8 SNMP エージェントの設定

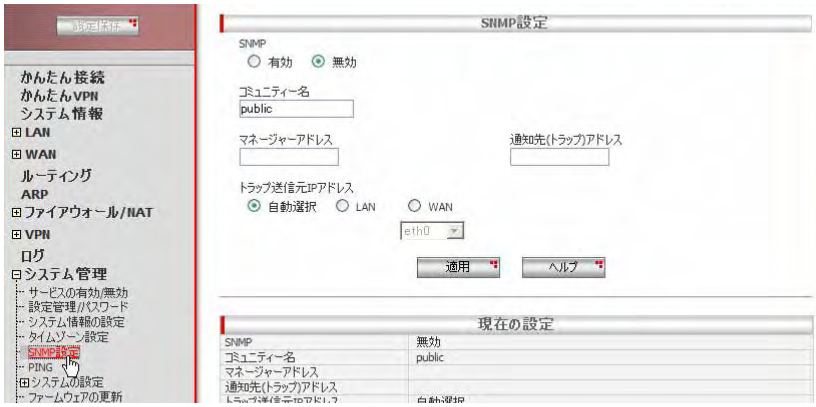
1.8.1 概要

本製品では SNMP エージェント機能をサポートしています。「SNMP」ページで SNMP エージェントを設定し、有効にすると SNMP マネージャーから本製品の設定を参照したり、変更することができます。ここでは、SNMP エージェントの設定について説明します。

1.8.2 SNMP エージェントの設定

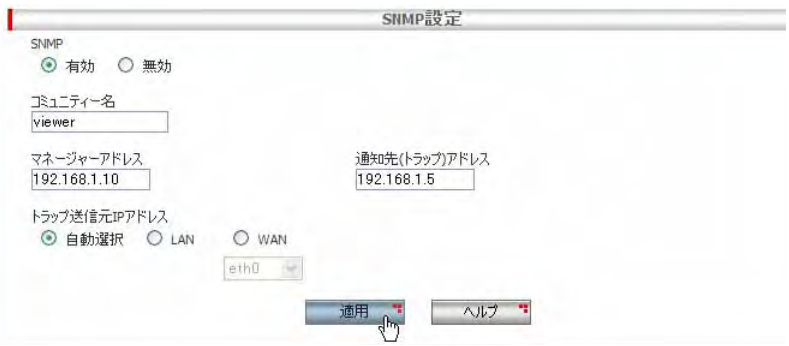
SNMP エージェントの設定を行うには以下の手順を実行します。

1. メニューから「システム管理」->「SNMP 設定」の順にクリックします。



2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

SNMP	有効
コミュニティー名	viewer
マネージャーアドレス	192.168.1.10
通知先（トラップ）アドレス	192.168.1.5
トラップ送信元 IP アドレス	自動選択



3. 以上で設定は完了です。

1.8.3 SNMP 設定情報の確認

設定した SNMP 情報を確認するには以下の手順を実行します。

1. メニューから「システム管理」->「SNMP 設定」の順にクリックします。

2.「現在の設定」テーブルに設定された情報が表示されます。

1.8.4 「SNMP 設定」ページの解説

「SNMP 設定」ページについて解説します。「SNMP 設定」ページでは、本製品が SNMP エージェントとして動作する場合の設定を行います。

1.8.4.1 SNMP 設定

SNMP 設定テーブルでは、SNMP エージェントの設定を行います。

パラメーター	オプション	説明
SNMP	有効 / 無効	SNMP を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンをクリックします。(「P.18 機能の有効化 / 無効化の設定」での設定と同じです。)
コミュニティー名		SNMP 管理ホストが本製品の情報を読み出す場合に使用する平文テキストのパスワードを入力します。半角英数字（または一部の記号）で 63 文字以内で入力してください。デフォルトは「public」です。 一部の記号として入力可能な文字は以下のとおりです。 ! # % & ( ) + - . (ピリオド) = @ [ ] ^ _ (下線) { } ~ , (カンマ)
マネージャーアドレス		本製品へのアクセスを許可する SNMP マネージャーの IP アドレスを入力します。何も入力されていない場合、すべての SNMP マネージャーからのアクセスを許可します。

通知先（トラップ）アドレス		トラップ通知先の IP アドレスを入力します。
トラップ送信元 IP アドレス		SNMP トラップパケットの送信元 IP アドレスの設定を選択します。
	自動選択	SNMP トラップパケットが送信されるインターフェースの IP アドレスを本製品が自動的に選択します。VPN 経由で送信する場合は、「自動選択」を選択せず、「LAN」を選択してください。
	LAN	SNMP トラップパケットの送信元 IP アドレスとして、本製品の LAN 側 IP アドレスを使用します。VPN 経由で送信する場合は、こちらを選択します。
	WAN	SNMP トラップパケットの送信元 IP アドレスとして、本製品の WAN 側 IP アドレスを使用します。「eth0」（固定 IP/DHCP 使用時）、「pppoe0」または「pppoe1」（PPPoE 使用時）のいずれかを選択します。なお、PPPoE が、アンナンバード設定の場合は、LAN 側 IP アドレスが使用されます。
「適用」ボタン		設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

1.8.4.2 SNMP 設定情報

「SNMP 設定情報」テーブルでは、「SNMP 設定」テーブルで設定した内容が一覧表示されます。

現在の設定

SNMP	無効
コミュニティー名	public
マネージャーアドレス	
通知先(トラップ)アドレス	
トラップ送信元IPアドレス	自動選択

パラメーター	説明
SNMP	SNMP の有効 / 無効が表示されます。
コミュニティー名	本製品の情報を読み出す場合のパスワードが表示されます。
マネージャーアドレス	本製品へのアクセスを許可する SNMP マネージャーの IP アドレスが表示されます。
通知先（トラップ）アドレス	トラップ通知先の IP アドレスが表示されます。
トラップ送信元 IP アドレス	SNMP トラップパケットの送信元 IP アドレスの設定が表示されます。

1.9 ログの記録

1.9.1 概要

本製品では機能ごとの各ログを「ログ」ページで選択して記録することができます。また、記録したログはログリストに表示したり、syslog サーバーに送信することもできます。ここでは、ログ機能の設定について説明します。

ヒント

ログメッセージ内容の詳細は、「P.182 ログメッセージ一覧」を参照してください。

1.9.2 ログの設定

ログ機能を設定するには以下の手順を実行します。

1. メニューから「ログ」をクリックします。

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

ログ種類：IP、DHCP、PPP、VPN、ETH、ブリッジ、システム、アプリケーション	警告
ログ種類：NAT、ファイアウォール	情報
ログサーバー IP アドレス	192.168.1.126
送信元 IP アドレス	自動選択

3. 以上で設定は完了です。

1.9.3 ログの確認

ログをファイルで確認するには以下の手順を実行します。

1. メニューから「ログ」をクリックします。

2.「ログリスト」にログが表示されます。
「更新」ボタンをクリックすると表示内容が更新されます。
「クリア」ボタンをクリックするとログをクリアすることができます。
「ログ保存」ボタンをクリックすると表示されているすべてのログをファイルに一括保存することができます。

1.9.4 「ログ」ページの解説

「ログ」ページについて解説します。「ログ」ページでは、ログの設定を行います。

1.9.4.1 システムログ設定

メニューから「ログ」をクリックすると設定画面が表示されます。

パラメーター	オプション	説明
ログ種類		各種ログメッセージの種類ごとに出力レベルを設定することができます。 以下の 9 種類のログを記録することができます。
	IP	IP、ICMP、ARP、TCP、UDP、IP ルーティングに関連するログが記録されます。

	DHCP	DHCP サーバー、DHCP クライアントに関連するログが記録されます。
	PPP	PPPoE に関連するログが記録されます。
	VPN	IPsec、ISAKMP に関連するログが記録されます。
	ETH	Ethernet に関連するログが記録されます。
	NAT	NAT に関連するログが記録されます。
	ファイアウォール	ファイアウォールに関連するログが記録されます。
	ブリッジ	ブリッジに関連するログが記録されます。
	システム	フラッシュファイルシステム、ログ、ユーザー等に関連するログが記録されます。
	アプリケーション	DNS リレー、SNTP、SNMP、HTTP サーバー、ダイナミック DNS に関連するログが記録されます。
ログ種類（選択項目）		ドロップダウンリストから出力レベルを選択します。初期値では、「通知」レベルのログが出力されます。出力レベルは、6 段階で定義されています。
	なし	指定の機能に関するログは出力しません。
	エラー	エラーレベルのログを出力します。
	警告	警告（エラーを含む）のログを出力します。
	通知	通知（警告・エラーを含む）のログを出力します。
	情報	情報（通知・警告・エラーを含む）のログを出力します。
	デバッグ	すべてのログレベルのログを出力します。 このレベルは、問題が発生した際に使用する場合のみ選択してください。
ログサーバー IP アドレス		ログメッセージを syslog サーバーに送信する場合、syslog サーバーの IP アドレスを入力します。

送信元 IP アドレス		Syslog サーバーに送信するパケットの送信元 IP アドレスの設定を選択します。
	自動選択	Syslog サーバーへのパケットが送信されるインターフェースの IP アドレスを本製品が自動的に選択します。VPN 経由で送信する場合は、「自動選択」を選択せず、「LAN」を選択してください。
	LAN	送信元 IP アドレスとして、本製品の LAN 側 IP アドレスを使用します。VPN 経由で送信する場合は、こちらを選択します。
	WAN	送信元 IP アドレスとして、本製品の WAN 側 IP アドレスを使用します。「eth0」（固定 IP/DHCP 使用時）、「pppoe0」または「pppoe1」（PPPoE 使用時）のいずれかを選択します。なお、PPPoE が、アンナンバード設定の場合は、LAN 側 IP アドレスが使用されます。
「適用」ボタン		設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

1.9.4.2 ログリスト

ログリストには、「システムログ設定」の設定に従って、ログが記録されます。

パラメーター		説明
ログリスト		ログの内容が表示されます。ログに表示されるインターフェース名は、以下のように読み替えてください。
	［ログに記録される名称］	［AR260S V2 のインターフェース名］
	fastEthernet 0	eth0
	vlan 1	eth1（LAN）
	fastEthernet 0.1	pppoe0
	fastEthernet 0.2	pppoe1
	fastEthernet 0.3	pppoe2
	fastEthernet 0.4	pppoe3

「更新」ボタン	クリックすると、ログの表示が更新されます。
「クリア」ボタン	クリックすると、確認のダイアログが表示され、「OK」ボタンをクリックすると、ログがクリアされます。
「ログ保存」ボタン	クリックすると、「ファイルのダウンロード」ダイアログが表示されるので、「保存」をクリックして、ログ情報をファイルに保存します。

1.10　設定の初期化

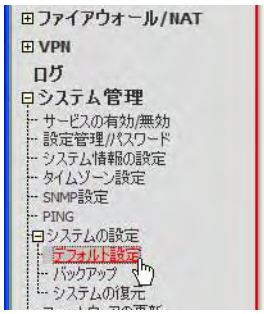
本製品に設定した内容を初期化（デフォルト設定に戻す）する手順を説明します。

ヒント

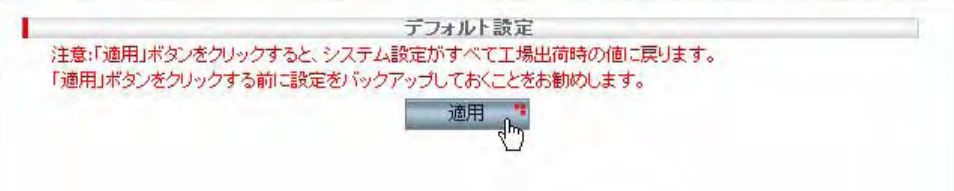
本製品をデフォルト設定に戻す前に、現在の設定をバックアップしておくことをお勧めします。バックアップについては「P.48 設定内容のバックアップ」を参照してください。

1.10.1　GUI 設定画面からの初期化

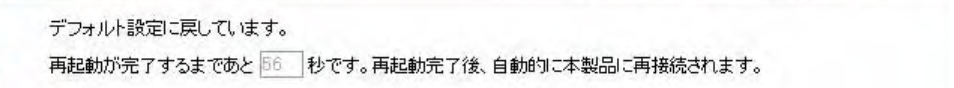
1. メニューから「システム管理」->「システムの設定」->「デフォルト設定」の順にクリックします。



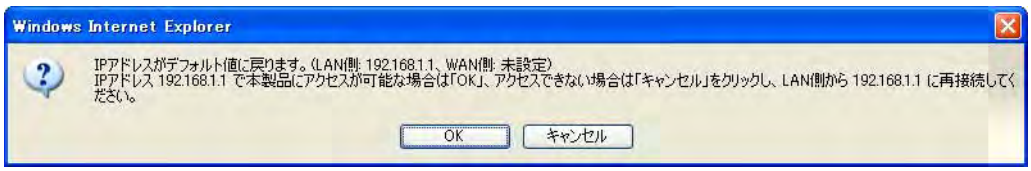
2.「適用」ボタンをクリックします。



3. 以下の画面が表示され、必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。



4. カウントダウンが終了すると、以下のダイアログが表示されます。



初期化後は、「キャンセル」ボタンをクリックして、工場出荷時のアドレス 192.168.1.1 に接続してください。（初期化前から 192.168.1.1 にアクセスしていた場合は、「OK」ボタンをクリックすると自動的に再接続できます。）

5. 以上で完了です。

1.10.2　リセットスイッチによる初期化

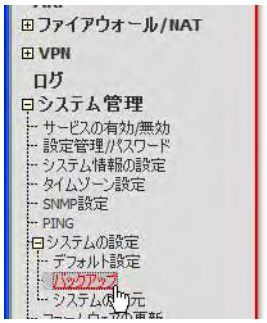
「リセットスイッチによる初期化」は「リセットスイッチによる初期化」サービスを有効にしないと実行できません。サービスを有効にする手順については「P.18 機能の有効化 / 無効化の設定」を参照してください。

1. 本製品の電源をオフにして、しばらく待ちます。
2. リセットスイッチを押しながら、本製品の電源スイッチをオンにし、SYSTEM LED が短く 3 回点滅するまで、リセットスイッチを押し続けます。
3. 以上で完了です。

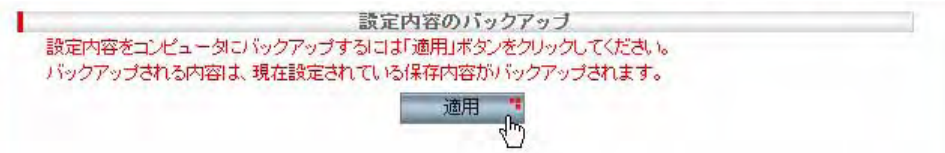
1.11 設定内容のバックアップ

本製品で設定した内容をコンピューターにバックアップする手順を説明します。

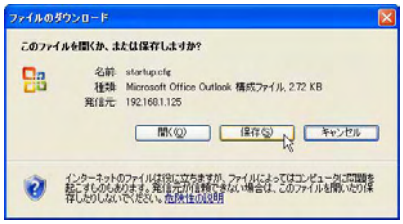
1. メニューから「システム管理」->「システムの設定」->「バックアップ」の順にクリックします。



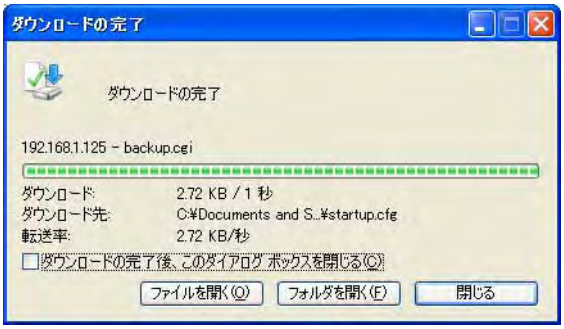
2.「適用」ボタンをクリックします。



3. 以下の画面が表示されたら「保存」ボタンをクリックして、バックアップファイルの保存場所を指定し、ダイアログの「保存」ボタンをクリックします。



4.「ダウンロードの完了」ダイアログが表示されたら「閉じる」をクリックします。



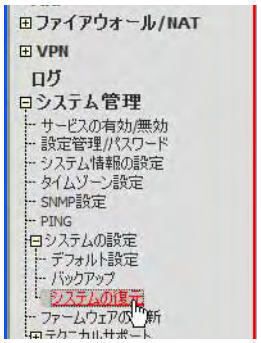
5. 以上で完了です。

ヒント **設定内容のバックアップ中は本製品の通信は停止しません。**

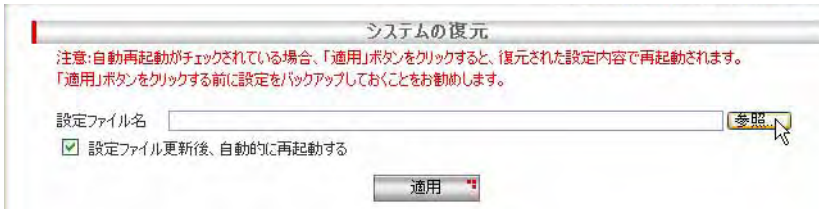
1.12　バックアップファイルの復元

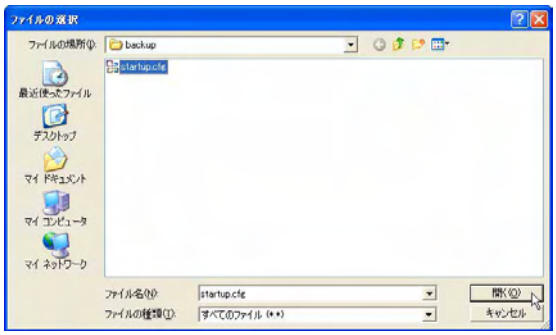
バックアップした本製品の設定ファイルを復元する手順を説明します。

1. メニューから「システム管理」->「システムの設定」->「システムの復元」の順にクリックします。

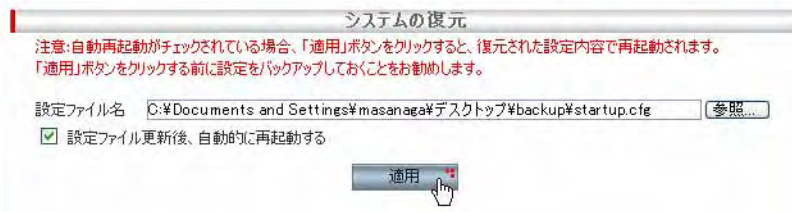


2.「参照」ボタンをクリックして、バックアップファイルを指定し「開く」ボタンをクリックします。





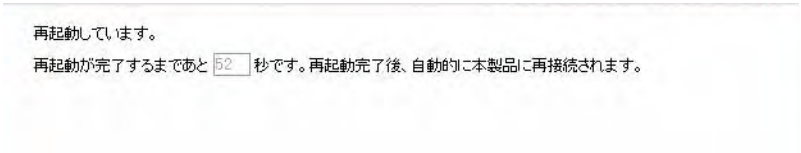
3.「適用」ボタンをクリックします。



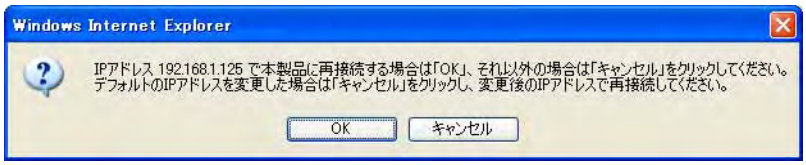
ヒント

現在の設定内容が上書きされるので、「適用」ボタンをクリックする前に設定をバックアップしておくことをおすすめします。
「設定ファイル更新後、自動的に再起動する」がチェックされている場合、「適用」ボタンをクリックすると、復元された設定内容で再起動されます。（チェックされていない場合は再起動は行われません。）

4. 以下の画面が表示され、必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。



5. カウントダウンが終了すると、以下のダイアログが表示されます。



復元後も本製品に接続するための IP アドレスが変わらない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

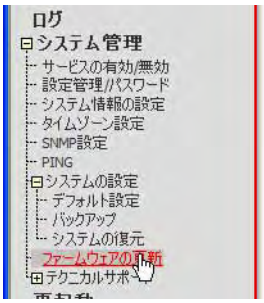
復元により IP アドレスが変更される場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、復元後の IP アドレスを指定して手動で本製品に再接続する必要があります。

6. 以上で完了です。

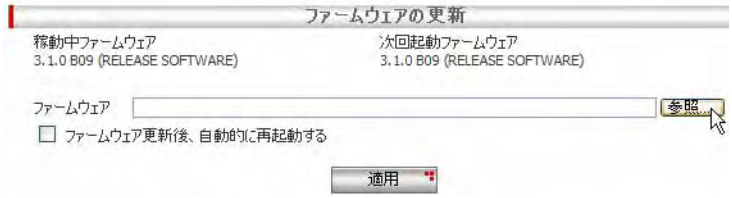
1.13　ファームウェアの更新

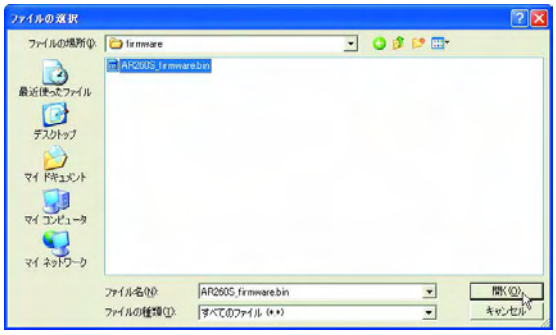
「ファームウェアの更新」ページでは、本製品のファームウェアを新しいバージョンのファームウェアに更新することができます。

1. メニューから「システム管理」->「ファームウェアの更新」の順にクリックします。



2.「参照」ボタンをクリックして、ファームウェアファイルを指定し「開く」ボタンをクリックします。



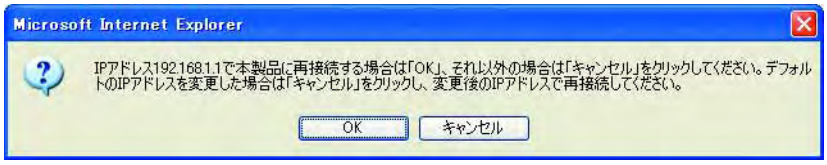


3.「適用」ボタンをクリックします。（ファームウェア更新後自動で再起動する場合は「ファームウェア更新後、自動的に再起動する」にチェックを入れます。）

4. ファームウェアインストール中であることを示す画面が表示され、インストール完了と再起動までに必要な時間がカウントダウンされます。カウントダウンが終了するまでしばらくお待ちください。

ヒント　**ファームウェア更新中に電源をオフにすることやケーブルの抜き差しはしないでください。**

5. カウントダウンが終了すると、以下のダイアログが表示されます。



本製品に接続するための IP アドレスを変更していない場合は「OK」ボタンをクリックします。「OK」ボタンをクリックした場合は、自動的に本製品に再接続されます。

IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

ヒント

変更後の本製品の IP アドレスが、接続するコンピューターと異なるサブネットになる場合、本製品に接続できなくなります。必要に応じてコンピューターの TCP/IP 設定も変更してください。

6. 以上で完了です。

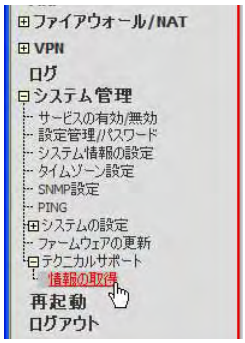
ヒント

本製品に設定した情報は、ファームウェア更新後も引き継がれます。

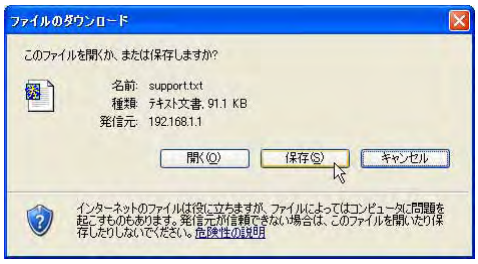
1.14　テクニカルサポート情報の取得

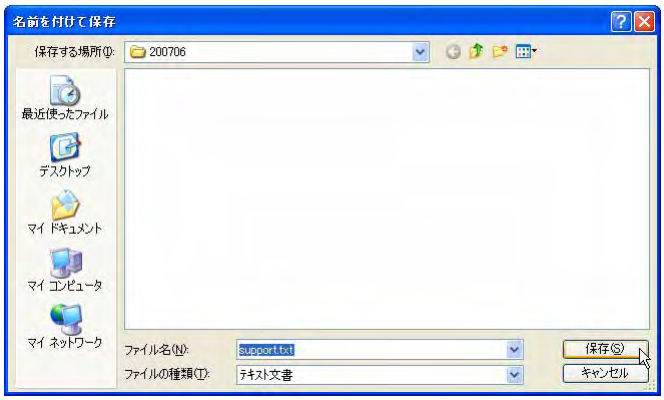
「情報の取得」ページでは、本製品で発生した問題を解決するために必要な情報を取得します。（通常使用することはありません。）テクニカルサポート情報を保存するには、以下の手順を実行します。

1. メニューから「システム管理」->「テクニカルサポート」->「情報の取得」の順にクリックします。



2.「適用」ボタンをクリックします。「ファイルのダウンロード」ダイアログが表示されるので、「保存」をクリックして、情報ファイルの保存を行います。





1.15 Ping の送信

1.15.1 概要

本製品から Ping を送信することで、指定の IP アドレスに対する接続状況を確認できます。

ここでは、Ping 送信の実行方法について説明します。

1.15.2 Ping の送信

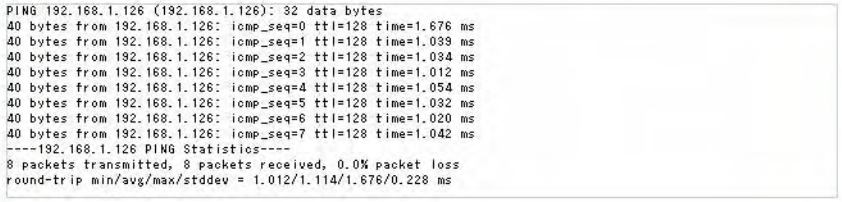
Ping の送信は、以下の手順で行います。

1. メニューから「システム管理」->「PING」の順にクリックします。

2. 各パラメーターを入力し「実行」ボタンをクリックします。ここでは、以下のように設定するものとします。

宛先 IP アドレス	192.168.1.126
送信元 IP アドレス	自動選択
パケット長	32
送信回数	8

3. 画面下のフィールドに実行結果が表示されます。



ヒント

Ping 実行時のエラー（Host unreachable や Net unreachable）が発生したとき、発生数が少ない場合、エラーメッセージが表示されないことがあります。

1.15.3 「PING」ページの解説

「PING」ページについて解説します。

パラメーター		説明
宛先 IP アドレス		Ping の宛先 IP アドレスを入力します。
送信元 IP アドレス		Ping の送信元 IP アドレスを入力します。
	自動選択	Ping パケットが送信されるインターフェースの IP アドレスを本製品が自動的に選択します。VPN 経由の Ping を実行する場合は、「自動選択」を選択せず、「LAN」を選択してください。
	LAN	送信元 IP アドレスとして、本製品の LAN 側 IP アドレスを使用します。VPN 経由の Ping を実行する場合は、こちらを選択します。
	WAN	送信元 IP アドレスとして、本製品の WAN 側 IP アドレスを使用します。「eth0」（固定 IP/DHCP 使用時）、「pppoe0」または「pppoe1」（PPPoE 使用時）のいずれかを選択します。なお、PPPoE が、アンナンバード設定の場合は、LAN 側 IP アドレスが使用されます。
パケット長		送信する Ping パケットのデータ部分の長さを入力します。設定可能な範囲は、32 ～ 1024 です。（単位：バイト）
送信回数		Ping パケットの送信回数を入力します。設定可能な範囲は、1 ～ 100 回です。
「実行」ボタン		設定した内容で Ping を送信します。

「ヘルプ」ボタン	操作のヒントを参照することができます。

2 LAN 側インターフェースの設定

2.1 概要

本章では、本製品の LAN 側インターフェースに関する設定の手順について説明します。本製品の LAN 側インターフェースに関する設定は以下のとおりです。

- IP アドレスの設定
- DHCP サーバーの設定
- IP アドレスの静的割り当ての設定
- LAN 側インターフェースのトラフィック確認

2.2 IP アドレスの設定

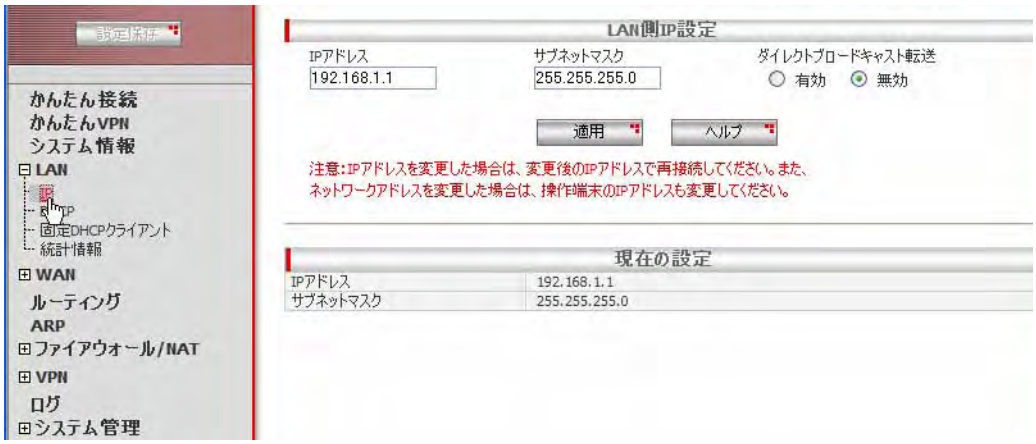
LAN 側インターフェースの IP アドレスの設定は「IP」ページで行います。ログイン時には、ここで設定した IP アドレスを使用します。

2.2.1 設定

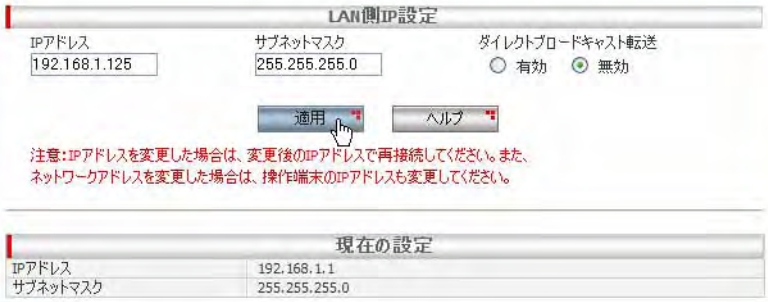
LAN 側インターフェースに IP アドレスを割り当てるには以下の手順を実行します。

ヒント 本製品の LAN 側インターフェースの IP アドレスは、デフォルトで「192.168.1.1」に設定されています。この手順では LAN 側の IP アドレスを「192.168.1.125/24」、ダイレクトブロードキャスト転送を無効に設定します。

1. メニューから「LAN」->「IP」の順にクリックします。



2. IP アドレスに「192.168.1.125」、サブネットマスクに「255.255.255.0」を入力し「適用」ボタンをクリックします。



3. IP アドレスが変更されるので、変更後の IP アドレス（192.168.1.125）を Web ブラウザーのアドレス欄に指定して、再び管理ページにアクセスします。

4. これで設定は完了です。

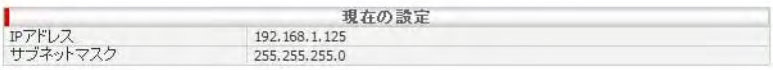
ヒント　**次回再起動時に IP アドレスの変更を有効にするには、画面左上の「設定保存」で設定を保存してください。**

2.2.2　確認

LAN 側インターフェースに割り当てた IP アドレスは以下の手順で確認します。

1. 変更後の IP アドレスを Web ブラウザーのアドレス欄に指定して設定画面にアクセスし、メニューから「LAN」->「IP」の順にクリックします。

2.「現在の設定」テーブルに、現在の IP アドレスとサブネットマスクが表示されます。

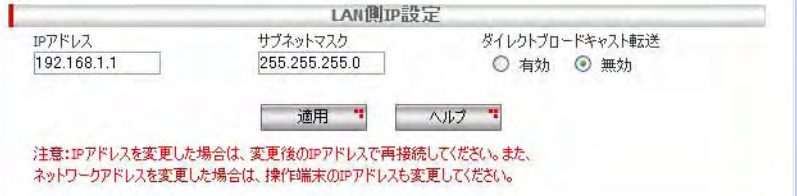


2.2.3　「IP」ページの解説

「IP」ページについて解説します。「IP」ページでは本製品の LAN 側に関する設定を行います。

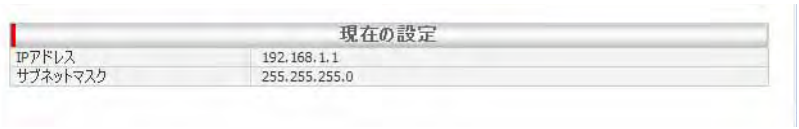
2.2.3.1　LAN 側 IP 設定

メニューから「LAN」->「IP」の順にクリックすると以下の画面が表示されます。



パラメーター	説明
IP アドレス	本製品の LAN 側 IP アドレスを入力します。デフォルトでは「192.168.1.1」です。ここで設定した IP アドレスを使用して本製品の設定画面にアクセスします。
サブネットマスク	LAN 側サブネットマスクを入力します。
ダイレクトブロードキャスト転送	WAN 側インターフェースに到着したパケットの宛先が、LAN 側インターフェースに割り当てられたサブネットに対応するブロードキャストパケットであったとき、LAN 側インターフェースにブロードキャストパケットを転送するかどうかを設定します。有効に設定すると、ブロードキャストパケットを LAN 側インターフェースに転送します。デフォルトでは「無効」です。
「適用」ボタン	入力した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

2.2.3.2 現在の設定



パラメーター	説明
IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。

2.3 DHCP サーバーの設定

DHCP（Dynamic Host Configuration Protocol）は、クライアントに対して動的に IP アドレスを提供する機能です。DHCP サーバーは、クライアントの要求に対して、あらかじめプールされた IP アドレスの中から使用されていないアドレスを選び、一定期間クライアントに割り当てます。本製品の DHCP サーバーの設定は「DHCP」ページで行います。

2.3.1 デフォルト設定

DHCP サーバーに関するデフォルト設定は以下のとおりです。

パラメーター		デフォルト値
DHCP サーバー		有効
IP アドレスプール		
	始点 IP アドレス	192.168.1.223
	終点 IP アドレス	192.168.1.254
サブネットマスク		255.255.255.0
リース期限		12 時間
デフォルトゲートウェイ		192.168.1.1
プライマリー DNS サーバー		192.168.1.1

2.3.2 設定

DHCP サーバーの設定を行うには以下の手順を実行します。

1. メニューから「LAN」->「DHCP」の順にクリックします。

2. 各パラメーターの値を入力し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

IP アドレスプール		
	始点 IP アドレス	192.168.1.200
	終点 IP アドレス	192.168.1.240
リース期限		14 日
プライマリー DNS サーバー		192.168.1.10
セカンダリー DNS サーバー		192.168.1.12

3. 以上で設定は完了です。

ヒント **DHCP サーバーの起動と停止については「P.18 機能の有効化 / 無効化の設定」を参照してください。**

2.3.3 確認

DHCP サーバーの設定は以下の手順で確認します。

1. メニューから「LAN」->「DHCP」の順にクリックします。

2.「現在の設定」テーブルに、DHCP サーバーの設定が表示されます。その下の「クライアント一覧」テーブルには本製品が IP アドレスを割り当てた DHCP クライアントの一覧が表示されます。「更新」ボタンをクリックすると表示内容が更新されます。

2.3.4 「DHCP」ページの解説

「DHCP」ページについて解説します。「DHCP」ページでは、本製品の DHCP サーバー機能についての設定を行います。

2.3.4.1 DHCP サーバー設定

メニューから「LAN」->「DHCP」の順にクリックすると以下の画面が表示されます。

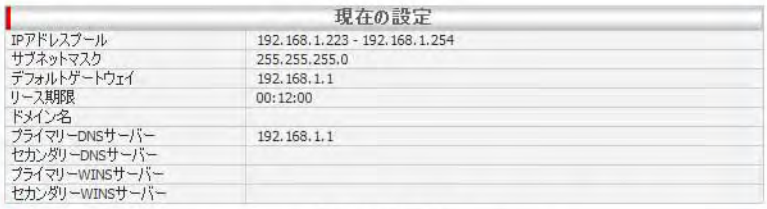
パラメーター	オプション	説明
IP アドレスプール		
	始点 IP アドレス	DHCP サーバー機能によって割り当てる IP アドレスの始点 IP アドレスを入力します。初期状態は、192.168.1.223 が設定されています。
	終点 IP アドレス	DHCP サーバー機能によって割り当てる IP アドレスの終点 IP アドレスを入力します。初期状態は、192.168.1.254 が設定されています。

サブネットマスク	IP アドレスプールに使用するサブネットマスクが表示されます。サブネットマスクは、「LAN 側 IP 設定」で、設定されているサブネットマスクの値が使用されます。
リース期限	IP アドレスをクライアントにリースする期限を入力します。初期状態は、12 時間が設定されています。設定可能な範囲は、1 分～ 365 日 23 時間 59 分です。
ドメイン名	DHCP クライアントに配布するドメイン名を入力します。入力可能文字数は、1 ～ 128 文字です。入力は任意です。
デフォルトゲートウェイ	デフォルトゲートウェイの IP アドレスが表示されます。通常は、本製品の LAN 側の IP アドレスです。
プライマリー DNS サーバー	プライマリー DNS サーバーの IP アドレスを入力します。通常は、本製品の LAN 側の IP アドレスです。入力は任意です。
セカンダリー DNS サーバー	セカンダリー DNS サーバーの IP アドレスを入力します。入力は任意です。
プライマリー WINS サーバー	プライマリー WINS サーバーの IP アドレスを入力します。入力は任意です。
セカンダリー WINS サーバー	セカンダリー WINS サーバーの IP アドレスを入力します。入力は任意です。
「適用」ボタン	入力した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

ヒント

本製品の DHCP サーバー機能は、原則として終点 IP アドレスから割り当てを行います。

2.3.4.2 現在の設定

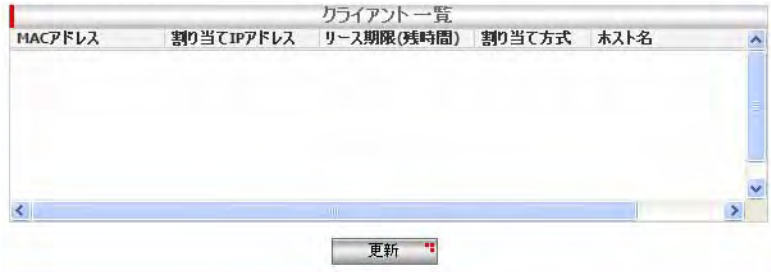


現在の設定	
IPアドレスプール	192.168.1.223 - 192.168.1.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.1.1
リース期限	00:12:00
ドメイン名	
プライマリーDNSサーバー	192.168.1.1
セカンダリーDNSサーバー	
プライマリーWINSサーバー	
セカンダリーWINSサーバー	

パラメーター	**説明**
IP アドレスプール	本製品に設定された IP アドレスプールが表示されます。
サブネットマスク	IP アドレスプールのサブネットマスクが表示されます。
リース期限	クライアントに割り当てた IP アドレスのリース期限が表示されます。

ドメイン名	DHCP クライアントに配布するドメイン名が表示されます。
デフォルトゲートウェイ	デフォルトゲートウェイのアドレスが表示されます。
プライマリー DNS サーバー	プライマリー DNS サーバーの IP アドレスが表示されます。
セカンダリー DNS サーバー	セカンダリー DNS サーバーの IP アドレスが表示されます。
プライマリー WINS サーバー	プライマリー WINS サーバーの IP アドレスが表示されます。
セカンダリー WINS サーバー	セカンダリー WINS サーバーの IP アドレスが表示されます。

2.3.4.3 クライアント一覧



パラメーター	説明
MAC アドレス	IP アドレスを割り当てたクライアントの MAC アドレスが表示されます。
割り当て IP アドレス	クライアントに割り当てた IP アドレスが表示されます。
リース期限（残時間）	クライアントに割り当てられた残り時間が表示されます。
割り当て方式	IP アドレスの割り当て方式が表示されます。
ホスト名	クライアントのホスト名（DHCP プロトコルにより通知されてきた場合に限り）が表示されます。
「更新」ボタン	クリックすると「クライアント一覧」の表示内容を更新することができます。

2.4 IP アドレスの静的割り当ての設定

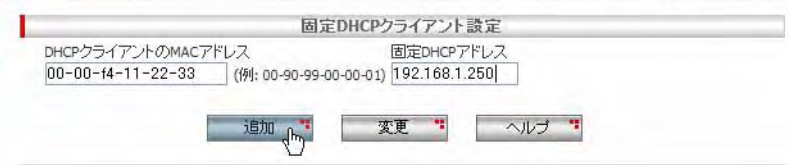
本製品では、DHCP サーバー機能の一部として、IP アドレスをクライアントに固定的に割り当てる機能（固定 DHCP クライアント機能）があります。固定 DHCP クライアント機能の設定は「固定 DHCP クライアント」ページで行います。

2.4.1 設定

固定 DHCP クライアントを追加するには以下の手順を実行します。

1. メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

2. 各パラメーターに値を入力し「追加」ボタンをクリックします。ここでは、MAC アドレス「00-00-f4-11-22-33」のクライアントに固定 DHCP アドレスとして「192.168.1.250」を割り当てるものとします。



3. 以上で設定は完了です。

2.4.2 固定 DHCP クライアントの削除

追加した固定 DHCP クライアントを削除するには以下の手順を実行します。

1. メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

2.「固定 DHCP クライアント一覧」で、削除するクライアント左部のラジオボタンをクリックします。

3.「削除」ボタンをクリックします。

4. 以上で設定は完了です。

2.4.3 確認

追加された固定 DHCP クライアントを確認するには以下の手順を実行します。

1. メニューから「LAN」->「固定 DHCP クライアント」の順にクリックします。

2.「固定 DHCP クライアント一覧」テーブルに固定 DHCP クライアントの一覧が表示されます。

2.4.4 「固定 DHCP クライアント」ページの解説

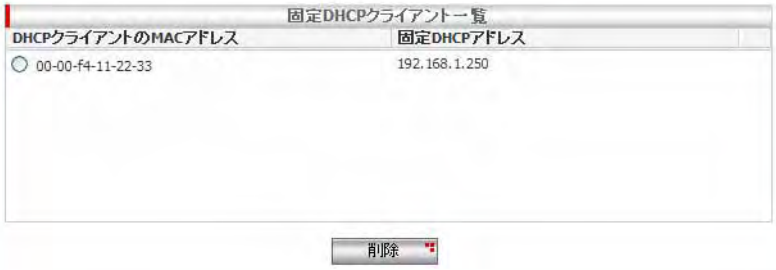
「固定 DHCP クライアント」ページについて解説します。「固定 DHCP クライアント」ページでは、本製品の DHCP サーバー機能で固定的に IP アドレスを割り当てるクライアントを登録します。

2.4.4.1 固定 DHCP クライアント設定

メニューから「LAN」->「固定 DHCP クライアント」の順にクリックすると以下の画面が表示されます。

パラメーター	説明
DHCP クライアントの MAC アドレス	IP アドレスを固定的に割り当てるクライアントの MAC アドレスを入力します。
固定 DHCP アドレス	クライアントに固定的に割り当てる IP アドレスを入力します。
「追加」ボタン	クライアントを追加登録します。追加できるクライアントは 8 台までです。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン	登録されている設定情報を変更します。はじめに「固定 DHCP クライアント一覧」から変更したい項目のラジオボタンを選択してから、内容を編集します。「変更」ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

2.4.4.2 固定 DHCP クライアント一覧



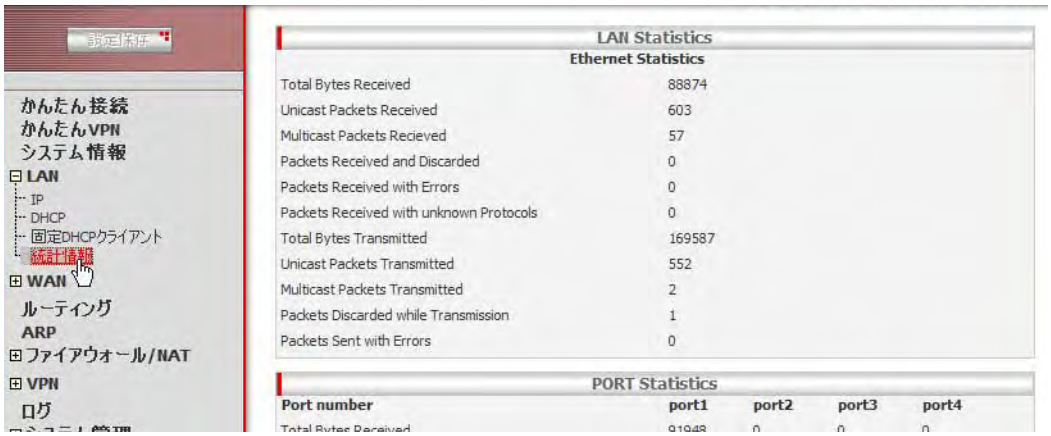
パラメーター	説明
DHCP クライアントの MAC アドレス	IP アドレスが固定的に割り当てられているクライアントの MAC アドレスが表示されます。
固定 DHCP アドレス	クライアントに固定的に割り当てられている IP アドレスが表示されます。
「削除」ボタン	ラジオボタンで選択した登録項目を一覧から削除します。

2.5 トラフィックの確認

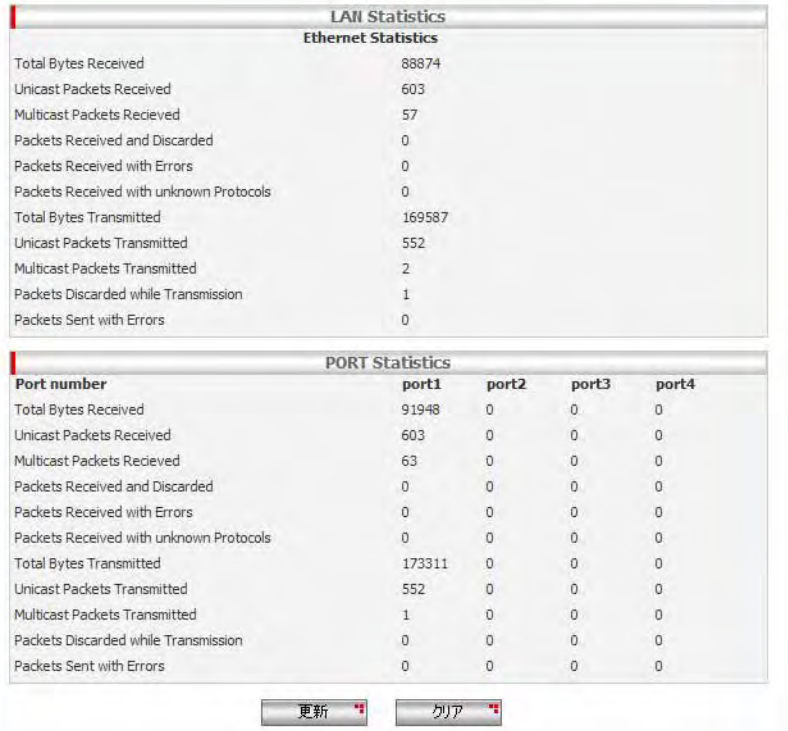
本製品では、LAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。LAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

2.5.1 確認

1. メニューから「LAN」->「統計情報」をクリックします。



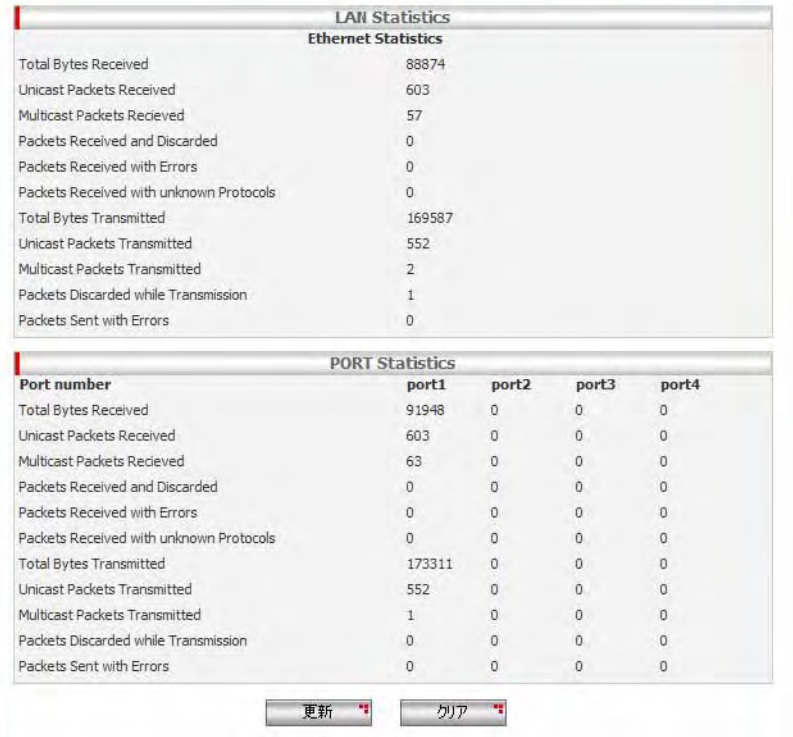
2.「LAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。



2.5.2 「統計情報」ページの解説

「統計情報」ページでは、本製品の LAN 側インターフェースのパケット転送に関する統計を参照することができます。

メニューから「LAN」->「統計情報」の順にクリックすると以下の画面が表示されます。



「LAN Statistics」には LAN 側インターフェース全体の統計情報が表示され、「PORT Statistics」にはポートごと（port1 ～ port4）の統計情報が表示されます。

パラメーター	説明
Total Bytes Received	受信パケットの総バイト数がカウントされます。
Unicast Packets Received	受信ユニキャストパケットの総数がカウントされます。
Multicast Packets Received	受信マルチキャストパケットの総数がカウントされます。
Packets Received and Discarded	破棄されたパケット数がカウントされます。
Packet Received with Errors	エラーパケット数がカウントされます。
Packets Received with unknown Protocols	未サポートプロトコルのパケット数がカウントされます。
Total Bytes Transmitted	転送パケットの総バイト数がカウントされます。
Unicast Packets Transmitted	転送ユニキャストパケット数がカウントされます。
Multicast Packets Transmitted	転送マルチキャストパケット数がカウントされます。

Packets Discarded while Transmission	転送中に破棄されたパケット数がカウントされます。
Packets Sent with Errors	転送されたエラーパケット数がカウントされます。
「更新」ボタン	統計情報の表示内容を更新します。
「クリア」ボタン	統計情報のカウンターをクリアします。

3 WAN 側インターフェースの設定

3.1 概要

本章では、本製品の WAN 側インターフェースに関する設定を「WAN」ページで行う手順について説明します。本製品の WAN 側インターフェースに関する設定は以下のとおりです。

- DHCP を使用した WAN 側ネットワークへの接続設定
- PPPoE を使用した WAN 側ネットワークへの接続設定
- 固定 IP を使用した WAN 側ネットワークへの接続設定
- ダイナミック DNS の設定
- WAN 側インターフェースのトラフィック確認

WAN 側インターフェースの通信速度はデフォルトでは自動（オートネゴシエーション）に設定されていますが、メニューの「WAN」->「インターフェース設定」から自動 / 固定（10BASE-T/100BASE-TX、Full Duplex/Half Duplex）を切り替えることができます。

3.2 DHCP を使用した WAN 側ネットワークへの接続

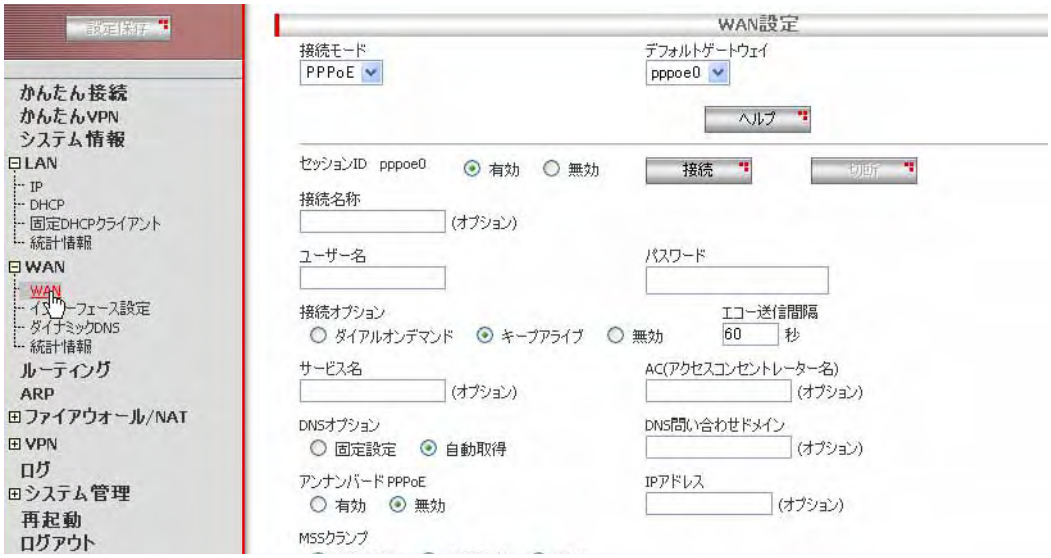
WAN 側インターフェースを DHCP で接続する場合の手順について説明します。おもに CATV のインターネット接続サービスなどで多く使用される接続形態です。

3.2.1 設定

WAN 側インターフェースを DHCP で接続するには以下の手順を実行します。

インターネット接続サービスを提供するサービスプロバイダーから、設定に必要な情報を提供されている場合は事前にご用意ください。詳細についてはプロバイダーにお問い合わせください。

1. メニューから「WAN」->「WAN」の順にクリックします。



2. 接続モードに「DHCP」を選択します。

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは以下のように設定するものとします。

ダイレクトブロードキャスト転送	無効
デフォルトゲートウェイ	使用する
DNS オプション	自動取得

4. 以上で設定は完了です。

3.2.2 設定の確認

WAN 側の設定は以下の手順で確認します。

1. メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。

現在の設定	
基本設定が完了しました。現在の設定は以下のとおりです。	
LAN設定	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
DHCP	有効
WAN設定	
WANのスピード	
接続モード	DHCP
デフォルトゲートウェイアドレス	
プライマリーDNSサーバー	
セカンダリーDNSサーバー	
接続状況	未接続
IPアドレス	
サブネットマスク	

3.3 PPPoE を使用した WAN 側ネットワークへの接続

WAN 側インターフェースを PPPoE で接続する場合の手順について説明します。おもに ADSL などのインターネット接続サービスなどで多く使用される接続形態です。

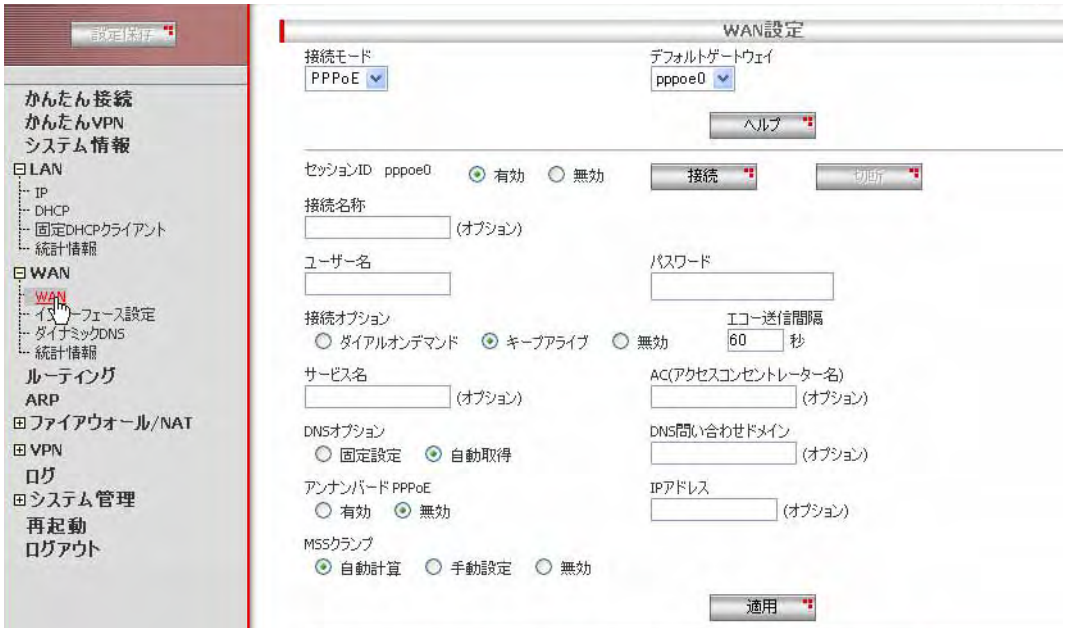
3.3.1 設定

WAN 側インターフェースを PPPoE で接続するには以下の手順を実行します。

ヒント

インターネット接続サービスを提供するサービスプロバイダーから、設定に必要な情報を提供されている場合は事前にご用意ください。詳細についてはプロバイダーにお問い合わせください。

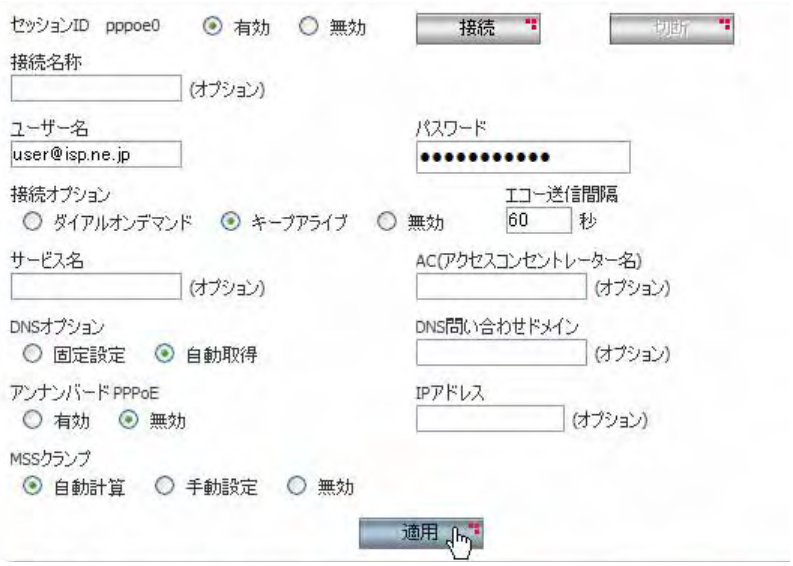
1. メニューから「WAN」->「WAN」の順にクリックします。



2. 接続モードに「PPPoE」を選択します。

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは、デフォルトゲートウェイ「pppoe0」に以下のように設定するものとします。

アンナンバード PPPoE	無効（デフォルト）
ユーザー名	user@isp.ne.jp（プロバイダーから提供されたと仮定します）
パスワード	isppassword（プロバイダーから提供されたと仮定します）
接続オプション	キープアライブ、エコー送信間隔 60 秒（デフォルト）
DNS オプション	自動取得（デフォルト）
MSS クランプ	自動計算（デフォルト）



4. 以上で設定は完了です。

3.3.2 設定の確認

WAN 側の設定は以下の手順で確認します。

1. メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。マルチセッションで接続している場合は、セッションごとに設定の詳細が表示されます。

現在の設定

基本設定が完了しました。現在の設定は以下のとおりです。

LAN設定	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
DHCP	有効
WAN設定	
WANのスピード	
接続モード	PPPoE
デフォルトゲートウェイアドレス	pppoe0
pppoe0	
セッション状態	有効
接続状況	未接続
IPアドレス	
PEERのアドレス	
プライマリーDNSサーバー	
セカンダリーDNSサーバー	
サブネットマスク	
接続オプション	キープアライブ
エコー送信間隔	60
MSS値	
pppoe1	
セッション状態	無効
接続状況	未接続
IPアドレス	
PEERのアドレス	
プライマリーDNSサーバー	
セカンダリーDNSサーバー	
サブネットマスク	
接続オプション	キープアライブ
エコー送信間隔	60
MSS値	

3.3.3 PPPoE セッションの切断 / 接続

PPPoE セッションを手動で切断 / 接続するには以下の手順を実行します。

1. メニューから「WAN」->「WAN」の順にクリックします。

2. 画面の「セッション ID」の表示を確認し、「切断 / 接続」ボタンをクリックします。ここでは切断されたセッション（pppoe0）を「接続」するものとします。

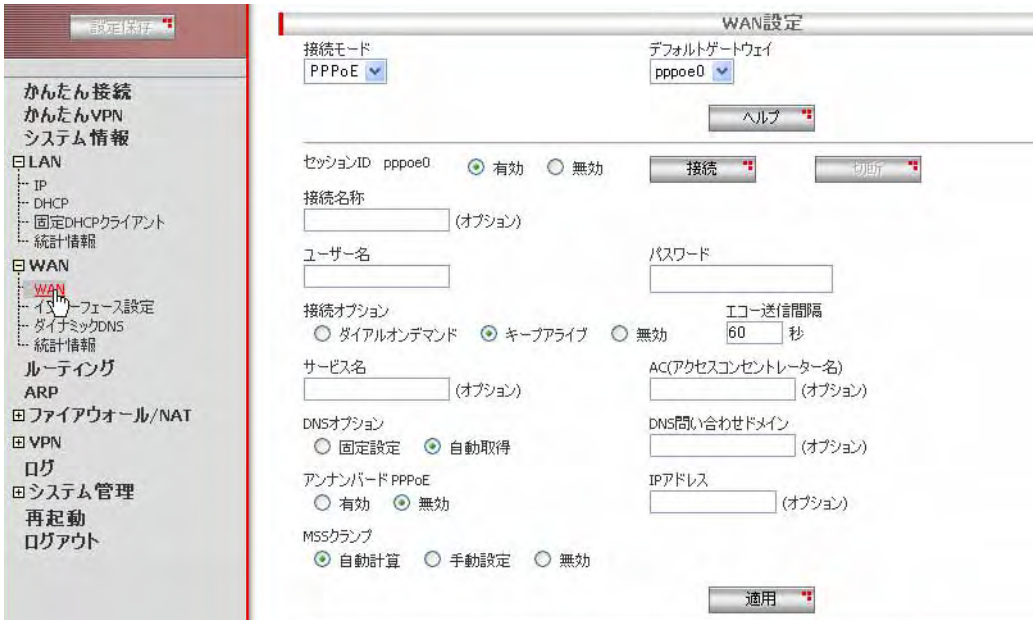
3.4 固定 IP アドレスを使用した WAN 側ネットワークへの接続

WAN 側インターフェースを固定 IP アドレスで接続する場合の手順について説明します。おもに PPPoE 接続サービス以外で固定 IP アドレスを割り当てられているサービスで使用します。

3.4.1 設定

WAN 側インターフェースを固定 IP アドレスで接続するには以下の手順を実行します。

1. メニューから「WAN」->「WAN」の順にクリックします。



2. 接続モードに「固定 IP」を選択します。

3. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは、以下のように設定するものとします。

IP アドレス	200.100.10.54
サブネットマスク	255.255.255.0
ゲートウェイアドレス	200.100.10.1
プライマリー DNS サーバー	200.100.10.32

4. 以上で設定は完了です。

3.4.2 設定の確認

WAN 側の設定は以下の手順で確認します。

1. メニューから「WAN」->「WAN」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。

3.5 ダイナミック DNS の設定

ダイナミック DNS を利用する場合の手順について説明します。
ダイナミック DNS の設定を行う場合には、事前に DynDNS（http://www.dyndns.com/）からアカウントを取得し、Dynamic DNS サービスに FQDN を登録しておいてください。

3.5.1 設定

ダイナミック DNS を利用するには以下の手順を実行します。

1. メニューから「WAN」->「ダイナミック DNS」の順にクリックします。

2. 各パラメーターに値を入力し「適用」ボタンをクリックします。ここでは、以下のように設定するものとします。

登録するインターフェース	pppoe0
登録する FQDN	test.dyndns.org
DynDNS のアカウント名	dnsuser
DynDNS のパスワード	dnspassword

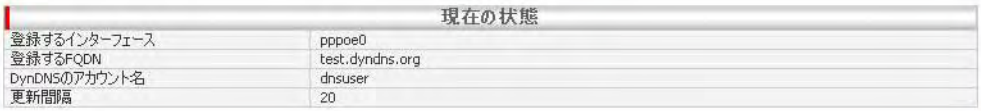
3. 以上で設定は完了です。

3.5.2 設定の確認

WAN 側の設定は以下の手順で確認します。

1. メニューから「WAN」->「ダイナミック DNS」の順にクリックします。

2.「現在の設定」テーブルに、現在の設定が表示されます。



現在の状態	
登録するインターフェース	pppoe0
登録するFQDN	test.dyndns.org
DynDNSのアカウント名	dnsuser
更新間隔	20

3.6 「WAN」ページの解説

「WAN」ページについて解説します。「WAN」ページでは本製品の WAN 側に関する設定を行います。

3.6.1 WAN 設定

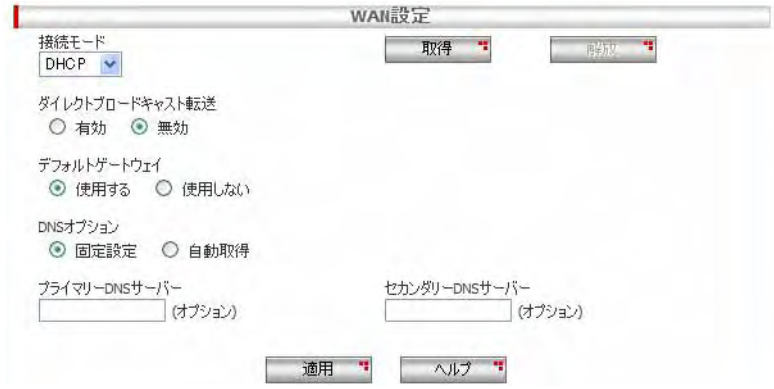
メニューから「WAN」->「WAN」の順にクリックすると以下の画面が表示されます。

パラメーター	説明
接続モード	WAN ポートの接続モードを「DHCP」、「PPPoE」、「固定 IP」の 3 つのオプションから選択します。選択するオプションによって、設定画面に表示されるパラメーターが異なります。

ヒント 以降の説明は、各オプション別に記載します。

3.6.1.1 接続モードに「DHCP」を選択した場合

接続モードに「DHCP」を選択すると、以下の画面が表示されます。



ヒント ご契約の ISP が DHCP をサポートしている場合に選択します。CATV のインターネット接続サービスなどは通常 DHCP 接続になります。

パラメーター	オプション	説明
ダイレクトブロードキャスト転送	有効 / 無効	LAN 側インターフェースに到着したパケットの宛先が、WAN 側インターフェースに割り当てられたサブネットに対応するブロードキャストパケットであったとき、WAN 側インターフェースにブロードキャストパケットを転送するかどうかを設定します。有効に設定すると、ブロードキャストパケットを WAN

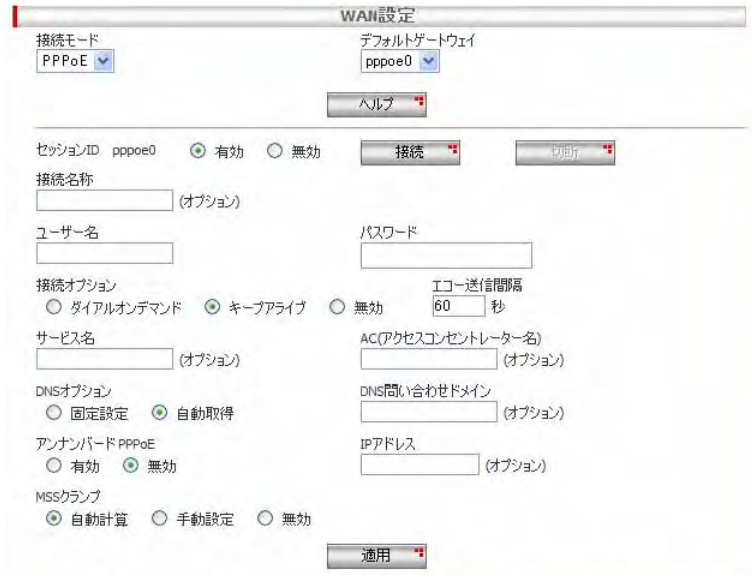
		側インターフェースに転送します。デフォルトでは「無効」です。
デフォルトゲートウェイ	使用する / 使用しない	DHCP サーバーから通知されるデフォルトルートを使用するかどうかを設定します。「使用しない」を選択した場合、動作としては、DHCP クライアントのパラメーター要求リストからルーターオプションをはずします。もし、DHCP サーバーがこれを無視してルーターオプションを応答した場合には、デフォルトゲートウェイアドレスとしてそのまま登録します。デフォルトでは「使用する」です。
DNS オプション	固定設定 / 自動取得	プライマリー DNS サーバー、セカンダリー DNS サーバーを手動で入力する場合は「固定設定」、自動で取得する場合は「自動取得」ラジオボタンを選択します。
プライマリー DNS サーバー		ISP から DNS の情報が提供されている場合に入力します。指定されていない場合は入力しないでください。
セカンダリー DNS サーバー		ISP から DNS の情報が提供されている場合に入力します。指定されていない場合は入力しないでください。
「適用」ボタン		入力した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

パラメーター	**オプション**	**説明**
LAN 設定		本製品の LAN 側インターフェースに関する情報が表示されます。
	IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示されます。
WAN 設定		本製品の WAN 側インターフェースに関する情報が表示されます。

	接続モード	現在の接続モードが表示されます。
	デフォルトゲートウェイアドレス	デフォルトゲートウェイのアドレスが表示されます。
	プライマリー DNS サーバー	プライマリー DNS サーバーのアドレスが表示されます。
	セカンダリー DNS サーバー	セカンダリー DNS サーバーのアドレスが表示されます。
	接続状況	接続状況が表示されます。
	IP アドレス	WAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	WAN 側インターフェースに設定されているサブネットマスクが表示されます。

3.6.1.2 接続モードに「PPPoE」を選択した場合

接続モードに「PPPoE」を選択すると、以下の画面が表示されます。



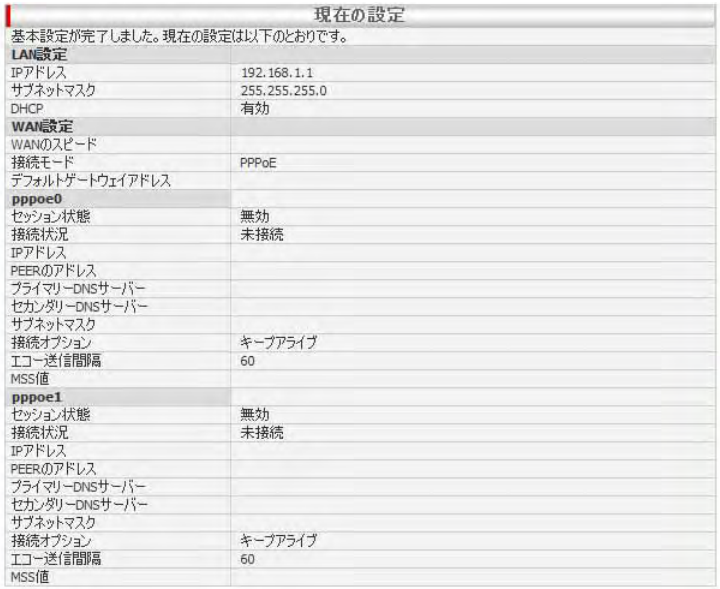
ヒント

ご契約の ISP が PPPoE をサポートしている場合に選択します。ADSL 回線を利用する ISP では通常 PPPoE 接続になります。

パラメーター	オプション	説明
「ヘルプ」ボタン		操作のヒントを参照することができます。
デフォルトゲートウェイ		デフォルトゲートウェイとして設定する PPPoE セッションをリストから選択します。

		デフォルトゲートウェイを別途設定したい場合は、「なし」を選択します。
セッション ID		本製品では、PPPoE を最大 4 セッション登録することができます。pppoe0 ～ pppoe3 のセッション名で区別されます。 pppoe2 および pppoe3 は、画面下の「セッションの新規作成」-「追加」ボタンで追加できます。 セッション ID の右の「有効」「無効」のボタンは、接続動作を行うか行わないかを設定します。設定内容を削除せず、一時的に接続しない場合には、「無効」を選択した後、「適用」ボタンをクリックしてください。 セッション ID の右の「接続」または「切断」ボタンをクリックして、指定した PPPoE セッションを接続 / 切断することができます。「接続」は、保存されている設定内容で接続します。
接続名称		PPPoE セッションに個別の名称をつける場合に設定します。半角英数字（または一部の記号）で 1 ～ 15 文字で入力してください。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + - .（ピリオド）= @ [ ] ^ _（下線）{ } ~，（カンマ）
ユーザー名		ISP から提供された PPPoE 接続に使用するユーザー名を入力します。半角英数字（または一部の記号）で 1 ～ 64 文字で入力してください。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + - .（ピリオド）= @ [ ] ^ _（下線）{ } ~，（カンマ）
パスワード		ISP から提供された PPPoE 接続に使用するパスワードを入力します。半角英数字（または一部の記号）で 1 ～ 32 文字で入力してください。 入力可能な一部の記号は以下のとおりです。 ! # % & ( ) + - .（ピリオド）= @ [ ] ^ _（下線）{ } ~，（カンマ）
接続オプション		接続する際のオプションを選択します。
	ダイアルオンデマンド	ダイアルオンデマンドを有効にする場合に選択します。 ダイアルオンデマンド機能を有効にした場合、PPPoE インターフェースが接続状態になるまでに到着したフォワーディングパケットは、PPP インターフェースにて破棄されます。
	タイムアウトまでの時間	「ダイアルオンデマンド」を有効にした場合にのみ表示されます。無通信時にインターネット接続を切断するまでの時間を入力します。1 ～ 65535 秒の範囲で入力してください。（デフォルトは 60 秒です。）
	キープアライブ	キープアライブを有効にする場合に選択します。
	エコー送信間隔	「キープアライブ」を有効にした場合にのみ表示されます。無通信時でもインターネット接続を切断しないために送るエコーの送信間隔を入力します。1 ～ 43200 秒の範囲で入力してください。（デフォルトは 60 秒です。）
	無効	接続オプションを使用しない場合に選択します。

サービス名		ISP から提供された PPPoE サービス名を入力します。半角英数字（または一部の記号）で 1 ～ 64 文字で入力してください。指定されていない場合は入力しないでください。
AC（アクセスコンセントレーター）名		ISP から提供された PPPoE AC（アクセスコンセントレーター）名を入力します。半角英数字（または一部の記号）で 1 ～ 64 文字で入力してください。指定されていない場合は入力しないでください。
DNS オプション	固定設定 / 自動取得	プライマリー DNS サーバー、セカンダリー DNS サーバーを手動で入力する場合は「固定設定」、自動で取得する場合は「自動取得」ラジオボタンを選択します。
DNS 問い合わせドメイン		この PPPoE セッション ID の DNS 自動取得により取得した DNS サーバーに、特定のドメイン名を持ったドメインネームを問い合わせる場合、そのドメイン名を入力します。入力可能文字数は、1 ～ 128 文字です。設定できるドメイン名は 1 つです。例えば、example.com、example.net や example.org 等のドメイン名をそのまま入力してください。
プライマリー DNS サーバー		ISP から DNS の情報が提供されている場合に入力します。指定されていない場合は入力しないでください。
セカンダリー DNS サーバー		ISP から DNS の情報が提供されている場合に入力します。指定されていない場合は入力しないでください。
アンナンバード PPPoE	有効 / 無効	アンナンバード PPPoE を有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンを選択します。
IP アドレス		IPCP で固定アドレスを使用する場合、ここに ISP から割り当てられた IP アドレスを入力します。固定 IP アドレス契約をしていない場合は、入力しないでください。
MSS クランプ	自動計算 / 手動設定 / 無効	MSS クランプに最適な値を自動設定する場合は「自動計算」、値を手動設定する場合は「手動設定」、値を設定しない場合は「無効」ラジオボタンを選択します。
	クランプ値	MSS クランプを「手動設定」に設定した場合、クランプ値を設定します。初期状態は、40 バイトです。設定可能な範囲は、0 ～ 942 です。（単位：バイト）
「適用」ボタン		入力した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。
セッションの新規作成	「追加」ボタン	PPPoE セッションを 4 個まで追加することができます。（pppoe2、pppoe3） 一度追加したセッションは、設定画面から直接削除することはできません。削除するには、リセットスイッチの操作、または「システム管理」->「システムの設定」->「デフォルト設定」により本製品を工場出荷時の状態に戻す必要があります。



現在の設定

基本設定が完了しました。現在の設定は以下のとおりです。

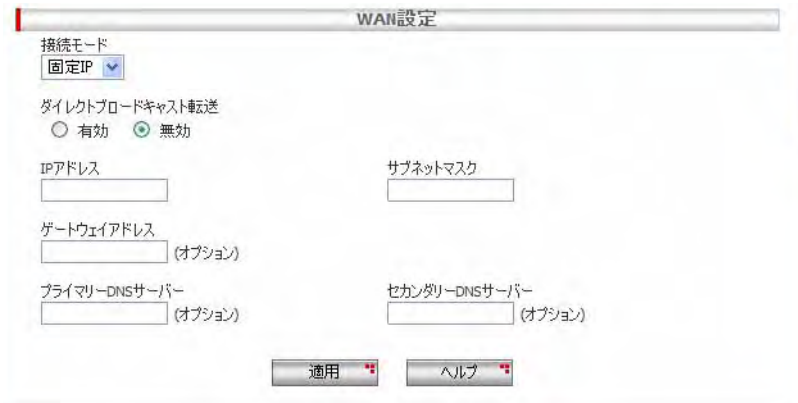
LAN設定	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
DHCP	有効
WAN設定	
WANのスピード	
接続モード	PPPoE
デフォルトゲートウェイアドレス	
pppoe0	
セッション状態	無効
接続状況	未接続
IPアドレス	
PEERのアドレス	
プライマリーDNSサーバー	
セカンダリーDNSサーバー	
サブネットマスク	
接続オプション	キープアライブ
エコー送信間隔	60
MSS値	
pppoe1	
セッション状態	無効
接続状況	未接続
IPアドレス	
PEERのアドレス	
プライマリーDNSサーバー	
セカンダリーDNSサーバー	
サブネットマスク	
接続オプション	キープアライブ
エコー送信間隔	60
MSS値	

パラメーター	オプション	説明
LAN 設定		本製品の LAN 側インターフェースに関する情報が表示されます。
	IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示されます。
WAN 設定		本製品の WAN 側インターフェースに関する情報が表示されます。
	接続モード	現在の接続モードが表示されます。
	デフォルトゲートウェイアドレス	デフォルトゲートウェイアドレスが表示されます。
	セッション ID	情報が表示されているセッション ID が表示されます。
	セッション状態	セッションの有効 / 無効が表示されます。
	接続状況	セッションの接続状況が表示されます。
	IP アドレス	セッションで割り当てられた WAN 側の IP アドレスが表示されます。

PEER のアドレス	接続された PPPoE サーバーのアドレスが表示されます。
プライマリー DNS サーバー	プライマリー DNS サーバーのアドレスが表示されます。
セカンダリー DNS サーバー	セカンダリー DNS サーバーのアドレスが表示されます。
サブネットマスク	セッションで割り当てられた WAN 側のサブネットマスクが表示されます。
接続オプション	セッションに設定された接続オプションが表示されます。
エコー送信間隔	「キープアライブ」を有効にした場合、エコー送信間隔の値が表示されます。
MSS 値	MSS クランプの値が表示されます。「自動計算」を指定している場合、実際に設定された値が表示されます。

3.6.1.3 接続モードに「固定 IP」を選択した場合

接続モードに「固定 IP」を選択すると、以下の画面が表示されます。



ヒント

固定 IP アドレスを使用して接続する場合に選択します。

パラメーター		説明
ダイレクトブロードキャスト転送	有効 / 無効	LAN 側インターフェースに到着したパケットの宛先が、WAN 側インターフェースに割り当てられたサブネットに対応するブロードキャストパケットであったとき、WAN 側インターフェースにブロードキャストパケットを転送するかどうかを設定します。有効に設定すると、ブロードキャストパケットを WAN 側インターフェースに転送します。デフォルトでは「無効」です。

IP アドレス	ISP から提供された IP アドレスを入力します。インターネット側から本製品へのアクセスにはこの IP アドレスが使用されます。
サブネットマスク	ISP から提供されたサブネットマスクを入力します。
ゲートウェイアドレス	ISP から提供されたゲートウェイの IP アドレスを入力します。
プライマリー / セカンダリー DNS サーバー	ISP から提供されたプライマリー / セカンダリー DNS サーバーの IP アドレスを入力します。指定されていない場合は入力しないでください。

パラメーター	オプション	説明
LAN 設定		本製品の LAN 側インターフェースに関する情報が表示されます。
	IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示されます。
WAN 設定		本製品の WAN 側インターフェースに関する情報が表示されます。
	接続モード	現在の接続モードが表示されます。
	デフォルトゲートウェイアドレス	デフォルトゲートウェイアドレスが表示されます。
	プライマリー DNS サーバー	プライマリー DNS サーバーのアドレスが表示されます。
	セカンダリー DNS サーバー	セカンダリー DNS サーバーのアドレスが表示されます。
	接続状況	接続状況が表示されます。PPPoE とは異なり、実際にリンクが確立していなくて

	も、IP アドレスが設定されると「接続」と表示されます。
IP アドレス	WAN 側の IP アドレスが表示されます。
サブネットマスク	WAN 側のサブネットマスクが表示されます。

3.6.2 ダイナミック DNS 設定

メニューから「WAN」->「ダイナミック DNS」の順にクリックすると以下の画面が表示されます。

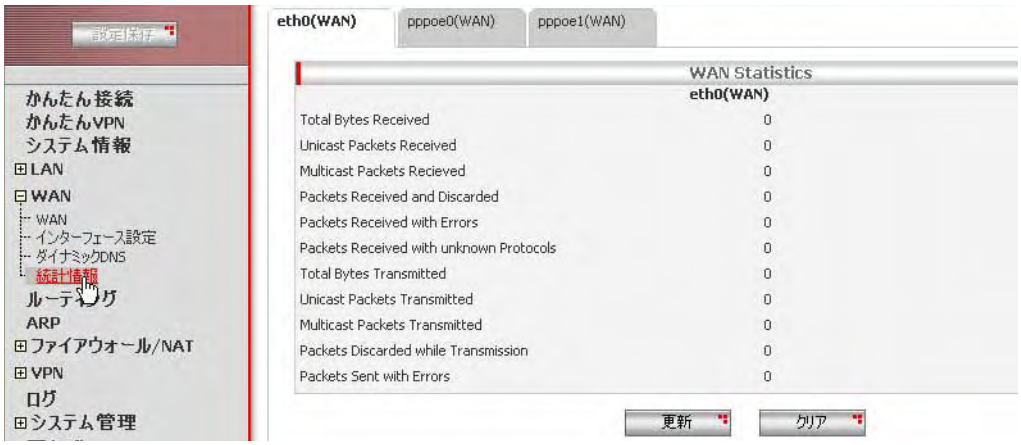
パラメーター	説明
登録するインターフェース	ここで設定したインターフェースに割り振られた IP アドレスがダイナミック DNS の IP アドレスとして使用されます。
登録する FQDN	DynDNS に登録している FQDN を設定します。入力可能文字数は、1 ～ 128 文字です。
DynDNS のアカウント名	DynDNS に登録しているアカウント名を設定します。入力可能文字は、1 ～ 64 文字の半角英数字（または一部の記号）です。(DynDNS による制限とは異なります。) 一部の記号として入力可能な文字は以下のとおりです。 ! # % & ( ) + – . (ピリオド) = @ [ ] ^ _ (下線) { } ~ , (カンマ)
DynDNS のパスワード	DynDNS に登録しているパスワードを設定します。入力可能文字数は、1 ～ 32 文字の半角英数字（または一部の記号）です。(DynDNS による制限とは異なります。) 一部の記号として入力可能な文字は以下のとおりです。 ! # % & ( ) + – . (ピリオド) = @ [ ] ^ _ (下線) { } ~ , (カンマ)
更新間隔	IP アドレスの再登録を行うまでの更新間隔を設定します。(単位：日) 初期状態は 20 です。設定可能な範囲は、0 ～ 255 です。 IP アドレスに変更があった場合には、ここで設定された間隔とは関係なく再登録を行います。

3.7 トラフィックの確認

本製品では、WAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。WAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

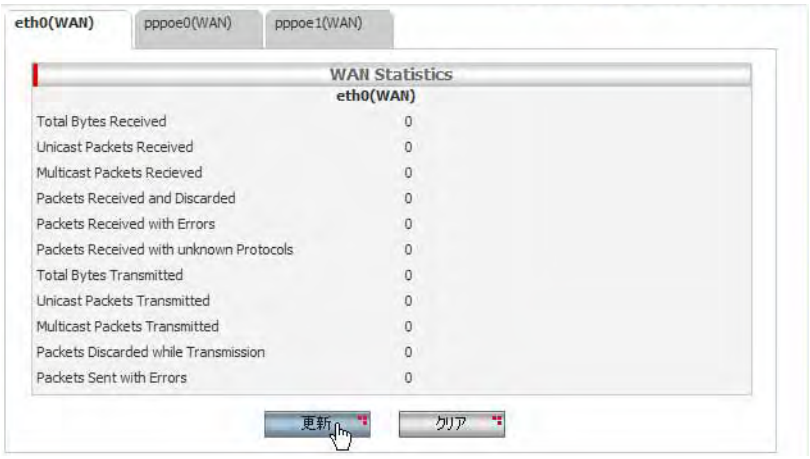
3.7.1 確認

1. メニューから「WAN」->「統計情報」をクリックします。



2. 統計情報を参照したいインターフェースを選択します。初期状態では、「eth0(WAN)」が選択されます。

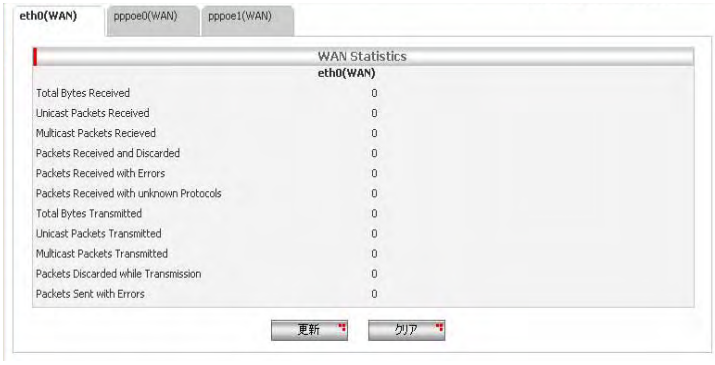
3.「WAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。カウンターを初期化するには「クリア」をクリックします。



3.7.2 「統計情報」ページの解説

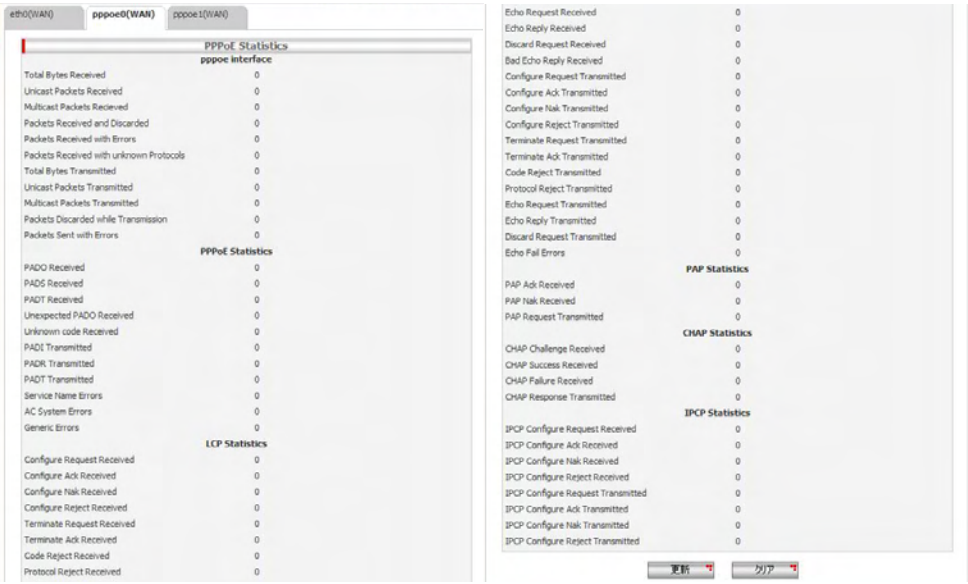
「統計情報」ページについて解説します。「統計情報」ページでは、本製品の WAN 側インターフェースのパケット転送に関する統計を参照することができます。

「eth0(WAN)」を選択すると以下の画面が表示されます。



パラメーター	説明
Total Bytes Received	受信パケットの総バイト数
Unicast Packets Received	受信ユニキャストパケットの総数
Multicast Packets Received	受信マルチキャストパケットの総数
Packets Received and Discarded	破棄されたパケット数
Packet Received with Errors	エラーパケット数
Packets Received with unknown Protocols	未サポートプロトコルのパケット数
Total Bytes Transmitted	転送パケットの総バイト数
Unicast Packets Transmitted	転送ユニキャストパケット数
Multicast Packets Transmitted	転送マルチキャストパケット数
Packets Discarded while Transmission	転送中に破棄されたパケット数
Packets Sent with Errors	転送されたエラーパケット数
「更新」ボタン	統計情報の表示内容を更新します。
「クリア」ボタン	統計情報のカウンター値を初期化します。

PPPoE インターフェースを選択すると以下の画面（PPPoE Statistics）が表示されます。



パラメーター		説明
pppoe interface		PPPoE インターフェースの情報を表示します。（各パラメーターの意味は、「eth0(WAN)」の場合と同様です。）
PPPoE Statistics		PPPoE 統計情報を表示します。
	PADO Received	PADO パケットを受信した回数
	PADS Received	PADS パケットを受信した回数
	PADT Received	PADT パケットを受信した回数
	Unexpected PADO Received	PADO 受信状態でない状態で PADO を受信した回数
	Unknown code Received	未定義のディスカバリパケットを受信した回数
	PADI Transmitted	PADI パケットを送信した回数
	PADR Transmitted	PADR パケットを送信した回数
	PADT Transmitted	PADT パケットを送信した回数（＊）
	Service Name Errors	Service-Name-Error Tag を受信した回数（＊）
	AC System Errors	AC-System-Error Tag を受信した回数（＊）
	Generic Errors	Generic-Error Tag を受信した回数（＊）
	（＊）PPPoE インターフェース単位ではなく、装置単位の値を表示します。	

LCP Statistics　　LCP 統計情報を表示します。

Configure Request Received	受信した ConfigureRequest パケットの数
Configure Ack Received	受信した ConfigureACK パケットの数
Configure Nak Received	受信した ConfigureNAK パケットの数
Configure Reject Received	受信した ConfigureReject パケットの数
Terminate Request Received	受信した Terminate パケットの数
Terminate Ack Received	受信した TerminateACK パケットの数
Code Reject Received	受信した CodeReject パケットの数
Protocol Reject Received	受信した ProtocolReject パケットの数
Echo Request Received	受信した EchoRequest パケットの数
Echo Reply Received	受信した EchoReply パケットの数
Discard Request Received	受信した DiscardRequest パケットの数
Bad Echo Reply Received	意図しない EchoReply パケットの受信数
Configure Request Transmitted	送信した ConfigureRequest パケットの数
Configure Ack Transmitted	送信した ConfigureACK パケットの数
Configure Nak Transmitted	送信した ConfigureNAK パケットの数
Configure Reject Transmitted	送信した ConfigureReject パケットの数
Terminate Request Transmitted	送信した Terminate パケットの数
Terminate Ack Transmitted	送信した TerminateACK パケットの数
Code Reject Transmitted	送信した CodeReject パケットの数
Protocol Reject Transmitted	送信した ProtocolReject パケットの数
Echo Request Transmitted	送信した EchoRequest パケットの数
Echo Reply Transmitted	送信した EchoReply パケットの数
Discard Request Transmitted	送信した DiscardRequest パケットの数（＊）

	Echo Fail Errors	LCP Echo タイムアウトの回数
	（＊）現在の仕様ではカウントされません。	
PAP Statistics		PAP 統計情報を表示します。
	PAP Ack Received	受信した PAP AuthenticateAck パケットの数
	PAP Nak Received	受信した PAP AuthenticateNak パケットの数
	PAP Request Transmitted	送信した PAP AuthenticateRequest パケットの数
CHAP Statistics		CHAP 統計情報を表示します。
	CHAP Challenge Received	受信した CHAP Challenge パケットの数
	CHAP Success Received	受信した CHAP Success パケットの数
	CHAP Failure Received	受信した CHAP Failure パケットの数
	CHAP Response Transmitted	送信した CHAP Response パケットの数
IPCP Statistics		IPCP 統計情報を表示します。
	IPCP Configure Request Received	受信した ConfigureRequest パケットの数
	IPCP Configure Ack Received	受信した ConfigureACK パケットの数
	IPCP Configure Nak Received	受信した ConfigureNAK パケットの数
	IPCP Configure Reject Received	受信した ConfigureReject パケットの数
	IPCP Configure Request Transmitted	送信した ConfigureRequest パケットの数
	IPCP Configure Ack Transmitted	送信した ConfigureACK パケットの数
	IPCP Configure Nak Transmitted	送信した ConfigureNAK パケットの数
	IPCP Configure Reject Transmitted	送信した ConfigureReject パケットの数
「更新」ボタン		統計情報の表示内容を更新します。
「クリア」ボタン		統計情報のカウンター値を初期化します。

4　ルーティングの設定

4.1　概要

ルーティングには、RIP(Routing Information Protocol) などのプロトコルを使用して行うダイナミックルーティングと、スタティックルートを手動で設定してルーティングを行うスタティックルーティングがありますが、本製品では、スタティックルーティングのみサポートしています。本章では、本製品のルーティング機能を「ルーティング」ページで設定する手順を説明します。

4.2　スタティックルーティング

スタティックルーティングを設定する手順について説明します。

4.2.1　設定

スタティックルーティングを設定するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

2. 各パラメーターに値を入力し「追加」ボタンをクリックします。ここでは、以下のように設定するものとします。

宛先ネットワークアドレス		192.168.2.0
宛先サブネットマスク		255.255.255.0
ゲートウェイ	アドレス	192.168.3.1
優先度		1（高、通常設定）

3. 以上で設定は完了です。

4.2.2 設定の確認

スタティックルーティングの設定は以下の手順で確認します。

1. メニューから「ルーティング」をクリックします。

2.「ルーティングテーブル」に、現在のルーティング設定が表示されます。

4.2.3 スタティックルーティングの変更

スタティックルーティングを変更するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

2.「ルーティングテーブル」の該当ルート左部にあるラジオボタンをクリックします。

3.「スタティックルーティング設定」で各パラメーターの値を変更し「変更」ボタンをクリックします。

4. 以上で設定は完了です。

4.2.4 スタティックルーティングの削除

スタティックルーティングを削除するには以下の手順を実行します。

1. メニューから「ルーティング」をクリックします。

2.「ルーティングテーブル」の該当ルート左部にあるラジオボタンをクリックして選択します。

3.「削除」ボタンをクリックします。

4. 以上で設定は完了です。

4.3 「ルーティング」ページの解説

「ルーティング」ページについて解説します。「ルーティング」ページでは本製品のルーティングに関する設定を行います。

4.3.1 スタティックルーティング設定

パラメーター	オプション	説明
宛先ネットワークアドレス		ルーティングの宛先ホスト、またはネットワークアドレスを入力します。
宛先サブネットマスク		宛先ホスト、またはネットワークのサブネットマスクを入力します。
ゲートウェイ		スタティックルーティングでパケットを転送するためのゲートウェイアドレス、またはインターフェースを選択し、以下のいずれかの項目を入力します。
	アドレス	ゲートウェイの IP アドレスを入力します。
	インターフェース	転送先のインターフェースを選択します。 「null（破棄）」を選択すると、そのルーティングにマッチするパケットは破棄されます。
優先度		ルーティング情報に優先度を設定します。1（通常設定）が最も高く、10 が最も低い優先度になります。同じルート情報が存在した場合に、優先度の高い方が選択されます。
「追加」ボタン		ルーティングを追加登録します。30 件までのルーティングを追加することができます。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン		ドロップダウンリストで既存のルートを選択した場合にアクティブになります。設定内容の変更を保存します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン		操作のヒントを参照することができます。

4.3.2 ルーティングテーブル

パラメーター	オプション	説明
宛先ネットワークアドレス		ルーティングの宛先ホスト、またはネットワークアドレスが表示されます。
宛先ネットマスク		宛先ホスト、またはネットワークのサブネットマスクが表示されます。
ゲートウェイアドレス		WAN 側のネットワークへパケットを転送するためのゲートウェイアドレスが表示されます。
Active		有効なルート情報には、＊印が表示されます。
インターフェース		転送先のインターフェースが表示されます。
優先度		ルーティング情報の優先度が表示されます。
「削除」ボタン		ルーティング情報を削除します。（削除を行うには、あらかじめ削除するルーティング情報の左のラジオボタンを選択します。）

ヒント

DHCP サーバーから取得したデフォルトゲートウェイは、優先度 254 として登録されます。このルート情報を修正・削除することはできません。

ヒント

バージョン 3.0.0 以前に登録されたデフォルトゲートウェイは、優先度 254 で登録されています。このルート情報を選択した場合、表示される優先度は、254 ではなく 10 として表示されますので、適切な優先度を選択してください。なお、バージョン 3.0.0 から、デフォルトゲートウェイ（DHCP サーバーから取得されたもの以外）の優先度は、1 として登録されます。

5　ファイアウォール /NAT の設定

5.1　概要

ファイアウォールは、ルールを作成し、そのルールにマッチするパケットの通過を許可 / 拒否する機能です。本製品はステートフルインスペクション型ファイアウォール機能を搭載しており、WAN 側からのパケットはデフォルトですべて破棄します（ファイアウォールを無効に設定した場合は無効になります）。また、NAT は WAN 側へ向けたパケットに対してインターフェース ENAT が有効に設定されています（Outbound アクセスルール）。本章では、以下の機能について説明します。

- アクセス制御
- ステルスモード
- セルフアクセス
- NAT
- NAT プール
- タイムアウト
- URL フィルター
- DoS
- UPnP

5.2　アクセス制御の設定

アクセス制御で、本製品を経由する WAN 側から LAN 側（Inbound）、LAN 側から WAN 側（Outbound）へのトラフィックを制御します。アクセス制御は「ファイアウォール /NAT」->「アクセス制御」ページで設定します。

5.2.1　デフォルトのルール

アクセスリストを設定するインターフェースには eth0（WAN）、pppoe0（WAN）、pppoe1（WAN）があり、それぞれのアクセスリストにはデフォルトのルールが設定されています。デフォルトの設定内容は下記のとおりです。このルールが設定されていることで、LAN 側から WAN 側へ向けた通信が可能になります。

方向	Inbound
動作	設定なし（すべて破棄）

方向	Outbound
動作	通過
優先度	1
送信元	すべて
宛先	すべて
送信元ポート	すべて
宛先ポート	すべて
プロトコル	すべて

ログ	無効

ヒント

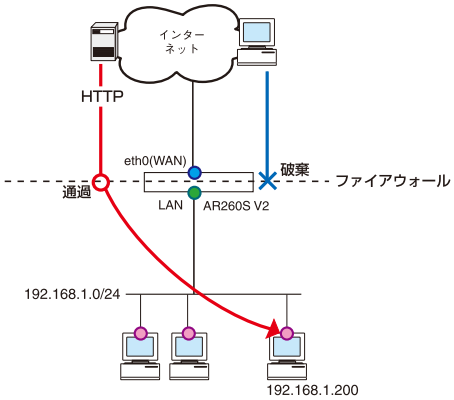
デフォルトのルールの優先度を変更したり、他に Outbound アクセスルールを追加した場合、インターネットへの通信ができなくなることもありますので、ルールを追加する場合は正確に設定してください。

5.2.2 ルールの作成

ルールを作成するには以下の手順を実行します。

ヒント

ここでは eth0(WAN) に対して下図のようなルールで設定を行うものとします。



1. メニューから「ファイアウォール /NAT」->「アクセス制御」の順にクリックします。

2. ここでは、設定するインターフェースとして、「eth0（WAN)」が選択されていることを確認します。また、「アクセス制御」に「有効」が選択されていることを確認します。

3.「アクセスリスト設定」の各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のルールを設定するものとします。

方向		Inbound
動作		通過
優先度		1
送信元		すべて
宛先		すべて
送信元ポート		すべて
宛先ポート		ポート指定
	ポート番号	80
プロトコル		TCP
ログ		無効

4. WAN 側から LAN 側のホストへのアクセスを可能にするために、NAT の設定を行います。NAT の設定方法については、「P. 118 NAT の設定」を参照してください。

5. 画面左上の「設定保存」ボタンをクリックして、設定を保存します。

6. 本製品を再起動します。再起動の方法については「P. 16 再起動」を参照してください。

7. 以上で設定は完了です。

5.2.3 ルールの変更

ルールを変更するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アクセス制御」の順にクリックします。

2.「Inbound アクセス制御リスト」または「Outbound アクセス制御リスト」テーブルから、変更するルールのラジオボタンをクリックして選択します。

3. 各パラメーターを変更します。

4.「変更」ボタンをクリックします。

5. 必要に応じて他の設定を行ったあと、画面左上の「設定保存」ボタンをクリックして設定を保存します。

6. 本製品を再起動します。再起動の方法については「P. 16 再起動」を参照してください。

7. 以上で設定は完了です。

5.2.4 ルールの削除

ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アクセス制御」の順にクリックします。
2. 「Inbound アクセス制御リスト」または「Outbound アクセス制御リスト」テーブルから、削除するルールのラジオボタンをクリックして選択します。
3. 「削除」ボタンをクリックします。
4. 必要に応じて他の設定を行ったあと、画面左上の「設定保存」ボタンをクリックして設定を保存します。
5. 本製品を再起動します。再起動の方法については「P.16 再起動」を参照してください。
6. 以上で設定は完了です。

5.2.5 ルールの確認

ルールを確認するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アクセス制御」の順にクリックします。
2. ルールを確認するインターフェースを eth0(WAN)、pppoe0(WAN)、pppoe1(WAN) から選択します。
3. 画面下部の「Inbound アクセス制御リスト」、「Outbound アクセス制御リスト」テーブルに現在のルールが一覧表示されます。

4. 「設定一覧」タブをクリックすることで、現在設定されているすべてのルールを一覧で表示することもできます。また、「絞り込み」-「インターフェース」／「方向」を選択して「適用」ボタンをクリックすると、一覧表示内容を絞り込むこともできます。

5.2.6 「アクセス制御」ページの解説

「アクセス制御」ページについて解説します。「アクセス制御」ページでは本製品の送受信トラフィックに関するアクセス制御の設定を行い、ファイアウォールのルールを設定します。

5.2.6.1 アクセス制御設定

メニューから「ファイアウォール /NAT」->「アクセス制御」の順にクリックすると以下の画面が表示されます。

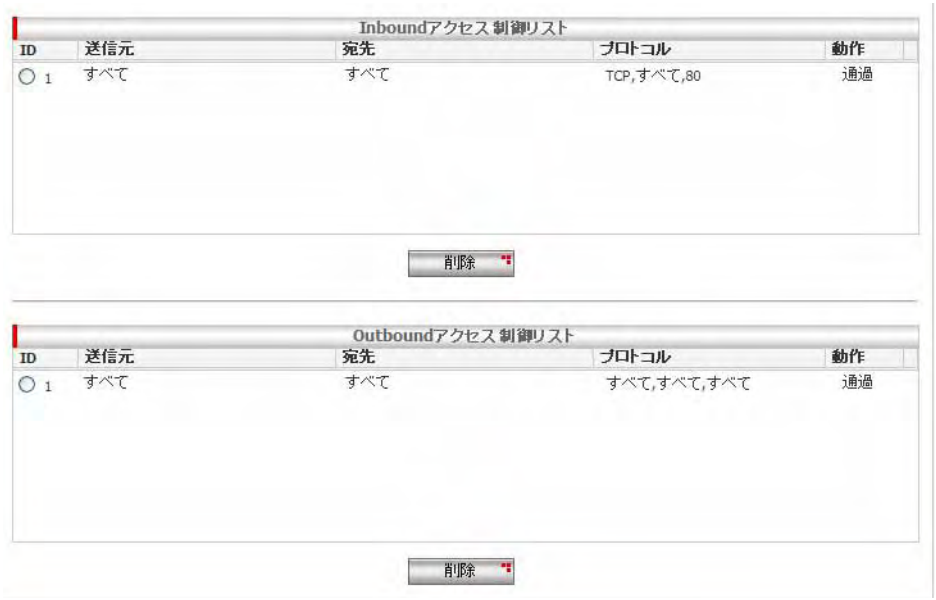
パラメーター	オプション	説明
アクセス制御		該当インターフェース上でアクセス制御を行うかどうかを設定します。デフォルトでは「有効」です。
ID		ルールの ID です。ルールを選択している場合には、選択しているルールの ID

			が表示されます。未選択時には ID は表示されません。
方向			ルールを適用する方向を決定します。「Inbound」の場合、受信したパケットに対して評価が行われ、「Outbound」の場合、送信するパケットに対して評価が行われます。
動作	通過 / 破棄		ルールにマッチしたパケットに対するアクションを選択します。マッチしたパケットを転送する場合は「通過」、破棄する場合は「破棄」を選択します。
優先度			ルールの優先度を選択します。数字が小さくなると優先度が高くなります。ルールが複数存在する場合、優先度が高い順にパケットにマッチングされます。
送信元			ルールを適用する送信元ネットワークの指定方法を選択します。
	すべて		送信元のすべてのコンピューターにルールを適用する場合に選択します。
	IP アドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
		IP アドレス	タイプに「IP アドレス」を選択した場合にのみ表示されます。ルールを適用するコンピューターの IP アドレスを入力します。
	サブネット		ルールを適用するコンピューターをサブネット単位で指定する場合に選択します。
		ネットワークアドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターのネットワークアドレスを入力します。
		サブネットマスク	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターのサブネットマスクを入力します。
宛先			ルールを適用する宛先ネットワークの指定方法を選択します。
	すべて		宛先のすべてのコンピューターにルールを適用する場合に選択します。
	IP アドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
		IP アドレス	タイプに「IP アドレス」を選択した場合にのみ表示されます。ルールを適用するコンピューターの IP アドレスを入力します。

	サブネット		ルールを適用するコンピューターをサブネット単位で指定する場合に選択します。
		ネットワークアドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターのネットワークアドレスを入力します。
		サブネットマスク	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターのサブネットマスクを入力します。
送信元ポート			ルールを適用する送信元ポートの指定方法を選択します。
	すべて		すべてのアプリケーションにルールを適用する場合に選択します。
	ポート指定		特定のポートを使用するアプリケーションにルールを適用する場合に選択します。
		ポート番号	タイプに「ポート指定」を選択した場合にのみ表示されます。ルールを適用するアプリケーションで使用するポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
	範囲指定		特定の範囲のポートを使用するアプリケーションにルールを適用する場合に選択します。
		始点ポート	タイプに「範囲指定」を選択した場合にのみ表示されます。ポートを指定する範囲の始点ポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
		終点ポート	タイプに「範囲指定」を選択した場合にのみ表示されます。ポートを指定する範囲の終点ポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
宛先ポート			ルールを適用する宛先ポートの指定方法を選択します。
	すべて		すべてのアプリケーションにルールを適用する場合に選択します。
	ポート指定		特定のポートを使用するアプリケーションにルールを適用する場合に選択します。
		ポート番号	種類に「ポート指定」を選択した場合にのみ表示されます。ルールを適用するアプリケーションで使用するポート番号を

			入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
	範囲指定		特定の範囲のポートを使用するアプリケーションにルールを適用する場合に選択します。
		始点ポート	種類に「範囲指定」を選択した場合にのみ表示されます。ポートを指定する範囲の始点ポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
		終点ポート	種類に「範囲指定」を選択した場合にのみ表示されます。ポートを指定する範囲の終点ポート番号を入力します。ポート番号は 1 ～ 65535 の範囲で入力してください。
プロトコル			ルールを適用するプロトコルをドロップダウンリストから選択します。
ログ	有効 / 無効		ルールにマッチした際にそのことをログに記録するかどうかを選択します。「有効」の場合はログに記録し、「無効」の場合はログに記録しません。
「追加」ボタン			ルールを追加登録します。ボタンをクリックしても、本製品を再起動するまで設定内容は反映されません。
「変更」ボタン			設定内容の変更を保存します。ボタンをクリックすると設定内容は即座に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができます。

5.2.6.2 Inbound アクセス制御リスト /Outbound アクセス制御リスト



パラメーター	説明
ID	ルールの ID 番号が表示されます。ルールの追加または削除を行うには、該当する ID のラジオボタンを選択します。
送信元	ルールが適用される送信元コンピューターの IP アドレスが表示されます。
宛先	ルールが適用される宛先コンピューターの IP アドレスが表示されます。
プロトコル	ルールが適用されるプロトコル、送信元ポート番号、宛先ポート番号が表示されます。
動作	ルールに設定された動作です。通過 / 破棄のいずれかが表示されます。
「削除」ボタン	選択したルールを削除します。ボタンをクリックしても、本製品を再起動するまで設定内容は反映されません。

5.3 ステルスモードの設定

ステルスモードは、本製品に対する外部からのポートスキャンなどに対して本製品からの応答を返さないようにする機能です。ステルスモードを有効にすると、該当インターフェース上でルーター宛のパケットがルールにより破棄された場合に、ICMP Unreachable または TCP Reset を返さないようにします。ただし、セルフアクセスルールで特定のポートをオープンしている場合は、そのポートに対しての応答を返します。セルフアクセスルールについては「P. 112 セルフアクセスルールの設定」を参照してください。

5.3.1 ステルスモード

ステルスモードの設定について説明します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

2. 設定を行うインターフェースのタブをクリックして選択したあと、ステルスモードの設定を行います。

パラメーター	オプション	説明
ステルスモード	有効 / 無効	ステルスモードを有効にする場合は「有効」、無効にする場合は「無効」ラジオボタンを選択します。デフォルト設定は「無効」です。
「適用」ボタン		設定した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。

5.4 セルフアクセスルールの設定

セルフアクセスルールは、本製品本体へ向けたアクセスを制御するルールです。

セルフアクセスの設定を有効にするには、「サービスの有効 / 無効」ページでファイアウォールを有効にし、「セルフアクセス」をチェックする必要があります。

セルフアクセスを行う場合、優先度の高い（小さい値ほど高優先度）セルフアクセス制御ルールから順に評価され、マッチするものがあった場合、その時点で評価が終了します。マッチしたルールの動作が「破棄」であった場合、送信元に対して ICMP Unreachable(Communication administratively prohibited by filtering)、または TCP Reset を返信します。

セルフアクセスルールは「セルフアクセス」ページで設定します。

5.4.1 デフォルト設定

本製品では、デフォルトで以下のセルフアクセスルールが設定されています。

インターフェース	送信元	サービス	動作
eth0, pppoe0, pppoe1	すべて	UDP, 500	通過

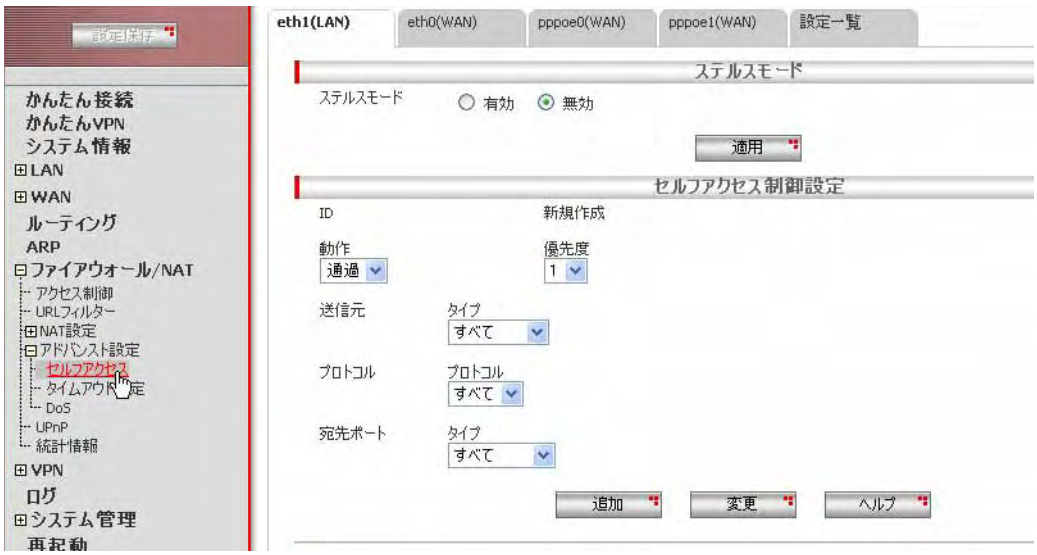
ヒント デフォルトのルールを削除、変更しないでください。削除や変更を行った場合、正常な通信ができなくなる場合があります。

ヒント TCP の 80 番ポートは本製品を設定する際に使用します。

5.4.2 ルールの作成

ルールを作成するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。



2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のルールでルールを設定するものとします。

インターフェース		eth1（LAN）
動作		通過
優先度		1
送信元		すべて
プロトコル		TCP
宛先ポート	ポート指定	80

3. 以上で設定は完了です。

5.4.3 ルールの変更

ルールを変更するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。
2. 「セルフアクセスルール」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

5.4.4 ルールの削除

ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。
2. 「セルフアクセスルール」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

5.4.5 ルールの確認

ルールを確認するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「セルフアクセス」の順にクリックします。

2. 確認するインターフェースのタブを選択します。

3.「セルフアクセス制御リスト」テーブルにルールが一覧表示されます。

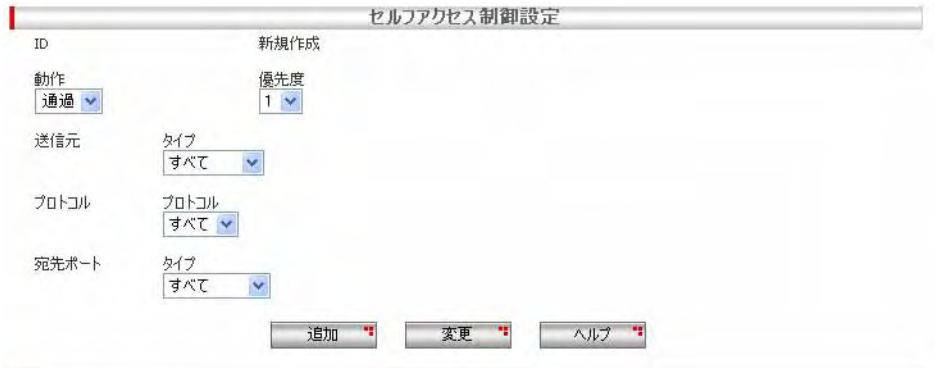
4.「設定一覧」タブをクリックすることで、現在設定されているすべてのルールを一覧で表示することもできます。また、「絞り込み」-「インターフェース」を選択して「適用」ボタンをクリックすると、一覧表示内容を絞り込むこともできます。

5.4.6 「セルフアクセス」ページの解説

「セルフアクセス」ページについて解説します。「セルフアクセス」ページでは、本製品本体に着信したパケットの処理ルールについて設定します。

5.4.6.1 セルフアクセス設定

メニューから「ファイアウォール」->「アドバンスト設定」->「セルフアクセス」の順にクリックすると以下の画面が表示されます。



パラメーター		オプション	説明
ID			ルールの ID です。ルールを選択している場合には、選択しているルールの ID が表示されます。未選択時には ID は表示されません。
動作			ルールにマッチした際にそのパケットをどう取り扱うかを決定します。「通過」の場合、パケットは転送され、「破棄」の場合、パケットは破棄されます。
優先度			ルールの優先度です。数字が小さいほど優先度が高くなります。
送信元			ルールを適用する送信元ネットワークの指定方法をリストから選択します。
	すべて		送信元ネットワークのすべてのコンピューターを適用する場合に選択します。
	IP アドレス		ルールを適用するコンピューターの IP アドレスを指定する場合に選択します。
		IP アドレス	コンピューターの IP アドレスを入力します。
	サブネット		ルールを適用するコンピューターをサブネット単位で指定する場合に選択します。
		ネットワークアドレス	ネットワークアドレスを入力します。
		サブネットマスク	サブネットマスクを入力します。
	範囲指定		ルールを適用するコンピューターのアドレスを範囲指定で指定する場合に選択します。
		始点 IP アドレス	指定する範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	指定する範囲の終点 IP アドレスを入力します。

プロトコル			ルールを適用するプロトコルをリストから選択します。
宛先ポート			ルールを適用する宛先ポート番号の指定方法をリストから選択します。
		すべて	すべてのポート番号にルールを適用する場合に選択します。
	ポート指定		特定のポート番号を指定する場合に選択します。
		ポート番号	ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
	範囲指定		特定範囲のポート番号を指定する場合に選択します
		始点ポート番号	指定する範囲の始点ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
		終点ポート番号	指定する範囲の終点ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
「追加」ボタン			ルールを追加登録します。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン			設定内容の変更を保存します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができます。

5.4.6.2 セルフアクセスルール

現在設定されているセルフアクセスルールが一覧表示されます。

パラメーター	説明
ID	ルールの ID です。
送信元	送信元の IP アドレスまたはサブネットが表示されます。

サービス	ルールが適用されるプロトコルとポートの番号が表示されます。ポート番号が指定されないプロトコルについては、「0」と表示されます。
動作	有効なアクセスの動作として通過 / 破棄のいずれかが表示されます。
「削除」ボタン	選択したルールを削除します。ボタンをクリックすると設定内容が即時に反映されます。

5.5 NAT の設定

このオプションを使用して、NAT ルールを設定し、該当インターフェースにおける NAT の設定を行います。

NAT の設定を有効にするには、「サービスの有効 / 無効」ページでファイアウォールを有効にし、「NAT」をチェックする必要があります。

NAT 設定はインターフェースごとに設定することができ、画面上部のタブを選択することで、どのインターフェースに対して設定を行うかを決定します。(NAT の種類についての詳細は、「P. 176 NAT について」を参照してください。)

5.5.1 新規にルールを追加

新規にルールを追加する場合は、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT」の順にクリックします。

2. 必要な情報を入力します。ここでは以下のパラメーターを入力するものとします。

インターフェース		eth0 (WAN)
NAT タイプ		ポートフォワーディング
対象プロトコル		TCP
対象ポート番号	タイプ	ポート指定
	ポート番号	80
フォワード先 IP アドレス		192.168.1.200
フォワード先ポート番号		無変換

3.「追加」ボタンをクリックしてルールを追加します。

4. 以上で設定は完了です。

5.5.2 既存のルールを変更

既存のルールを変更するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT」の順にクリックします。画面上部のタブから、ルールを変更するインターフェースを選択します。

2.「NAT 設定リスト」から変更を行う項目のラジオボタンを選択します。

3.「NAT 設定」で各項目を修正後、「変更」ボタンをクリックします。

4. 以上で設定は完了です。

5.5.3 既存のルールを削除

既存のルールを削除するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT」の順にクリックします。画面上部のタブから、ルールを削除するインターフェースを選択します。
2. 「NAT 設定リスト」から、削除を行う項目のラジオボタンを選択します。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

5.5.4 「NAT」ページの解説

「NAT」ページについて解説します。「NAT」ページでは、NAT ルールを設定し、該当インターフェースにおける NAT の設定を行います。(NAT の種類についての詳細は、「P.176 NAT について」を参照してください。)

5.5.4.1 NAT 設定テーブル

NAT に関する設定を行うテーブルです。メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
NAT タイプ		適用する NAT の種類をリストから選択します。
NAT タイプ	スタティック NAT	1:1 の IP アドレスの変換を行います。該当インターフェース上で送信する場合には送信元 IP アドレスを変換し、受信した場合には宛先 IP アドレスを変換します。この時、ポート番号は変換されません。この設定を行う場合、変換前の IP アドレスと NAT IP アドレスは同じ数にする必要があります。
	変換前の IP アドレス	変換前のネットワークとして、IP アドレスとサブネットマスクを入力します。
	NAT IP アドレス	変換後のネットワークとして、IP アドレスとサブネットマスクを入力します。
	宛先 IP アドレス（オプション）	宛先 IP アドレスと宛先サブネットマスクを指定します。宛先を限定する必要がない場合は、入力する必要はありません。

NAT タイプ	ダイナミック NAT		n:1 の IP アドレスの変換を行います。該当インターフェース上で送信する場合のみ NAT 変換を行い、送信元 IP アドレスを変換します。このとき、変換後 IP アドレスとしてインターフェースの IP アドレスが使用され、ポート番号は変換されません。使用可能な変換後 IP アドレスがない場合、パケットは破棄されます。
	変換前の IP アドレス		変換前のネットワークとして、IP アドレスとサブネットマスクを入力します。
NAT タイプ	ENAT		n:m の IP アドレスとポート番号の変換を行います。該当インターフェース上で送信する場合のみ NAT 変換を行い、送信元 IP アドレスと送信元ポート番号を変換します。使用可能な変換後ポート番号がない場合、パケットは破棄されます。
	変換前の IP アドレス		変換前の IP アドレスの指定方法をリストから選択します。
		すべて	すべての送信元 IP アドレスを適用する場合に選択します。
		IP アドレス	特定の送信元 IP アドレスを指定する場合に選択します。 IP アドレス : 送信元 IP アドレスを入力します。
		サブネット	送信元 IP アドレスをサブネット単位で指定する場合に選択します。 IP アドレス : 送信元 IP アドレスを入力します。 サブネットマスク : 送信元サブネットマスクを入力します。
	宛先 IP アドレス		宛先 IP アドレスの指定方法をリストから選択します。
		すべて	すべての宛先 IP アドレスを適用する場合に選択します。
		IP アドレス	特定の宛先 IP アドレスを指定する場合に選択します。 IP アドレス : 宛先 IP アドレスを入力します。
		サブネット	宛先 IP アドレスをサブネット単位で指定する場合に選択します。 IP アドレス : 宛先 IP アドレスを入力します。 サブネットマスク : 宛先サブネットマスクを入力します。
	NAT IP アドレス		変換後の IP アドレスとして使用するプールを選択します。プールに関しては「P.125 NAT プールの設定」を参照してください。
NAT タイプ	インターフェース ENAT		n:1 の IP アドレスとポート番号の変換を行います。該当インターフェース上で送信する場合のみ NAT 変換を行い、送信元 IP アドレスと送信元ポート番号を変換します。このとき変換後 IP アドレス

			としてインターフェースの IP アドレスが使用されます。使用可能な変換後ポート番号がない場合、パケットは破棄されます。
	変換前の IP アドレス		変換前の IP アドレスの指定方法をリストから選択します。
		すべて	すべての送信元 IP アドレスを適用する場合に選択します。
		IP アドレス	特定の送信元 IP アドレスを指定する場合に選択します。
			IP アドレス : 送信元 IP アドレスを入力します。
		サブネット	送信元 IP アドレスをサブネット単位で指定する場合に選択します。
			IP アドレス : 送信元 IP アドレスを入力します。
			サブネットマスク : 送信元サブネットマスクを入力します。
	宛先 IP アドレス		宛先 IP アドレスの指定方法をリストから選択します。
		すべて	すべての宛先 IP アドレスを適用する場合に選択します。
		IP アドレス	特定の宛先 IP アドレスを指定する場合に選択します。
			IP アドレス : 宛先 IP アドレスを入力します。
		サブネット	宛先 IP アドレスをサブネット単位で指定する場合に選択します。
			IP アドレス : 宛先 IP アドレスを入力します。
			サブネットマスク : 宛先サブネットマスクを入力します。
NAT タイプ	ポートフォワーディング		n:1 の IP アドレスとポート番号の変換を行い、「バーチャルサーバー」とも呼ばれます。該当インターフェース上で受信する場合のみ NAT 変換を行い、宛先 IP アドレスと宛先ポート番号を変換します。ポート番号に関しては明示的に指定されている場合のみ変換します。使用可能な変換後ポート番号がない場合、パケットは破棄されます。
	対象プロトコル		プロトコルをリストから選択します。
		プロトコル番号	対象プロトコルで「指定」を選択した場合のみ入力します。ルールを適用するプロトコル番号を入力します。設定可能な範囲は、1 ～ 255 です。
	対象ポート番号		対象プロトコルで「TCP」、「UDP」を選択した場合のみ入力します。ポート番号の指定方法をリストから選択します。
		ポート指定	特定のポート番号を指定する場合に選択します。
			ポート番号 : 宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。

		範囲指定	特定範囲のポート番号を指定する場合に選択します。 開始ポート番号 : 指定する範囲の開始宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。 終了ポート番号 : 指定する範囲の終了宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
	フォワード先 IP アドレス		変換後の IP アドレスを入力します。
	フォワード先ポート番号		対象プロトコルで「TCP」、「UDP」を選択した場合のみ入力します。ポート番号の指定方法をリストから選択しま。
		無変換	宛先ポート番号の変換を行わない場合に選択します。
		ポート指定	特定のポート番号を指定する場合に選択します。 ポート番号 : 宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
		範囲指定	特定範囲のポート番号を指定する場合に選択します。 開始ポート番号 : 指定する範囲の開始宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。 終了ポート番号 : 指定する範囲の終了宛先ポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
NAT タイプ	パススルー		1:1 の IP アドレスの変換を行います。該当インターフェース上で送信する場合のみ NAT 変換を行い、送信元 IP アドレスを変換します。このとき変換後 IP アドレスとしてインターフェースの IP アドレスが使用されます。指定した IP アドレス以外のパケットを送信しようとした場合、そのパケットは破棄されます。
	対象トラフィック		変換前の IP アドレスとプロトコルを指定します。
		IP アドレス	送信元 IP アドレスを入力します。
		本装置	本製品が送信するパケットが対象となります。
		プロトコル	ルールを適用するプロトコルをリストから選択します。
「追加」ボタン			ルールを追加登録します。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン			設定内容の変更を保存します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン			操作のヒントを参照することができます。

注意 **本製品配下の端末に対して IKE と ESP のパススルーを設定する場合は、本製品の VPN 機能を無効にしてください。**

5.5.4.2 NAT 設定リスト

現在設定されている NAT 設定リストが一覧表示されます。

パラメーター	説明
送信元	送信元が表示されます。
変換	変換の内容が表示されます。
宛先	対象となる宛先が表示されます。
プロトコル	変換対象のプロトコル、およびポート番号が表示されます。
タイプ	NAT タイプが表示されます。
「削除」ボタン	選択したルールを削除します。ボタンをクリックすると設定内容が即時に反映されます。

5.6 NAT プールの設定

NAT プールは、NAT 設定を行うときに利用する IP アドレスのグループです。「NAT 設定」で設定を行う場合に、プール名を指定することで設定内容を呼び出すことができます。

5.6.1 NAT プールの作成

新規に NAT プールを追加する場合は、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT プール」の順にクリックします。

2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下の内容を設定するものとします。

プール名	p1
始点 IP アドレス	192.168.1.100
終点 IP アドレス	192.168.1.150

3. 以上で設定は完了です。登録されている NAT プールは、「NAT プールリスト」で確認できます。

5.6.2 NAT プールの変更

既存の NAT プールを変更するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT プール」の順にクリックします。
2. 「NAT プールリスト」テーブルの該当 NAT プール左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

5.6.3 NAT プールの削除

既存の NAT プールを削除するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「NAT 設定」->「NAT プール」の順にクリックします。
2. 「NAT プールリスト」テーブルの該当 NAT プール左部にあるラジオボタンをクリックします。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

5.6.4 「NAT プール」ページの解説

「NAT プール」ページについて解説します。「NAT プール」ページでの設定は、NAT の「ダイナミック NAT」に関連づけることができます。

5.6.4.1 NAT プール設定

メニューから「ファイアウォール」->「NAT 設定」->「NAT プール」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
プール名		NAT プールのプール名を入力します。入力可能文字数は、1 ～ 15 文字です。英数字文字と一部の記号が入力可能です。
始点 IP アドレス		指定する範囲の始点 IP アドレスを入力します。
終点 IP アドレス		指定する範囲の終点 IP アドレスを入力します。
「追加」ボタン		NAT プールを追加登録します。
「変更」ボタン		設定内容の変更を保存します。

「ヘルプ」ボタン	操作のヒントを参照することができます。

5.6.4.2 NAT プールリスト設定

「NAT プールリスト設定」テーブルには以下の内容が表示されます。

パラメーター	オプション	説明
プール名		NAT プールのプール名が表示されます。
始点 IP アドレス		NAT プールの始点 IP アドレスが表示されます。
終点 IP アドレス		NAT プールの終点 IP アドレスが表示されます。
「削除」ボタン		選択した NAT プールを削除します。

5.7 タイムアウトの設定

タイムアウトの設定を行うことで、ファイアウォール、NAT のセッション保持時間の設定を行うことができます。

5.7.1 タイムアウト設定の追加

新規にタイムアウト設定を追加する場合は、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「タイムアウト」の順にクリックします。

2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下の内容を設定するものとします。

設定名	Tcp80
プロトコル	TCP
宛先ポート	80
保持時間	300

3. 以上で設定は完了です。登録されているタイムアウト値は、「タイムアウト設定リスト」で確認できます。

5.7.2 タイムアウトの変更

既存のタイムアウトを変更するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「タイムアウト」の順にクリックします。
2. 「タイムアウト設定リスト」テーブルの該当タイムアウト左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

5.7.3 タイムアウト設定の削除

既存のタイムアウト設定を削除するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「タイムアウト」の順にクリックします。
2. 「タイムアウト設定リスト」テーブルの該当タイムアウト左部にあるラジオボタンをクリックします。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

ヒント

「DefaultTcp」、「DefaultUdp」、「DefaultIcmp」、「TcpReset」、「DefaultDNS」は、特別な設定として扱われ、削除することはできません。(変更は可能です。)

5.7.4 「タイムアウト設定」ページの解説

「タイムアウト設定」ページについて解説します。このページでは、ファイアウォール、NAT のセッション保持時間の設定を行うことができます。

5.7.4.1 タイムアウト設定

メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「タイムアウト」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
設定名		追加するタイムアウト時間の設定名を入力します。入力可能な文字数は、1 ～ 15 文字です。
プロトコル		タイムアウト時間を適用するプロトコルをリストから選択します。
宛先ポート		タイムアウト時間を適用するポート番号を入力します。設定可能な範囲は、1 ～ 65535 です。
保持時間		タイムアウト時間を入力します。設定可能な範囲は、1 ～ 604800 です。（単位：秒）一部の項目は設定可能な範囲が異なります。詳しくは次項「タイムアウト設定リスト」のヒントを参照してください。
デフォルト		各プロトコルに応じた標準の保持時間を「保持時間」に設定します。
「追加」ボタン		タイムアウト設定を追加登録します。
「変更」ボタン		設定内容の変更を保存します。
「ヘルプ」ボタン		操作のヒントを参照することができます。

5.7.4.2 タイムアウト設定リスト

「タイムアウト設定リスト」テーブルには以下の内容が表示されます。

パラメーター	オプション	説明
設定名		タイムアウト時間の設定名が表示されます。
プロトコル		タイムアウト時間を適用するプロトコルが表示されます。
宛先ポート		タイムアウト時間を適用するポート番号が表示されます。

保持時間	タイムアウトまでの保持時間が表示されます。
「削除」ボタン	選択したタイムアウト設定を削除します。

「DefaultTcp」、「DefaultUdp」、「DefaultIcmp」、「TcpReset」、「DefaultDNS」は、特別な設定として扱われ、削除することはできません。（変更は可能です。）入力可能な保持時間は 0 ～ 604800（秒）となり、0 を入力した場合、タイムアウトしない設定になります。
これらのデフォルトのタイムアウト設定は、他にマッチするタイムアウト設定がない場合に適用されます。（デフォルト以外のタイムアウト設定にマッチする場合は、マッチする設定が優先されます。）

5.8 トラフィックの確認

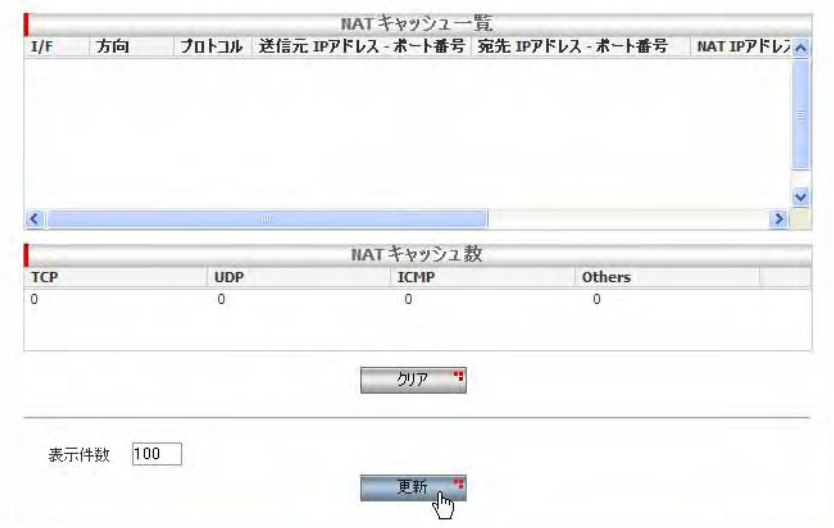
本製品では、ファイアウォールの統計を「統計情報」ページで一覧表示できます。

5.8.1 確認

統計情報を確認するには以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「統計情報」の順にクリックします。

2. ファイアウォールおよび NAT の統計情報が一覧表示されます。「アクセスリストキャッシュ数」および「NAT キャッシュ数」の下にある「クリア」ボタンをクリックすると、各キャッシュリストをクリアすることができます。「更新」ボタンをクリックすると、表示内容を更新することができます。

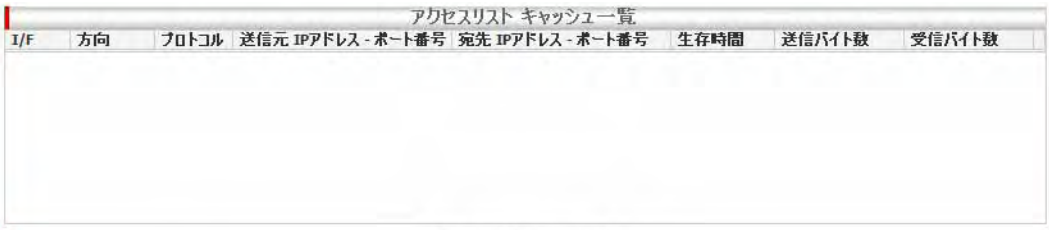


5.8.2 「統計情報」ページの解説

「統計情報」ページについて解説します。「統計情報」ページでは、ファイアウォールおよび NAT に関する統計情報を参照できます。

5.8.2.1 アクセスリスト キャッシュ一覧

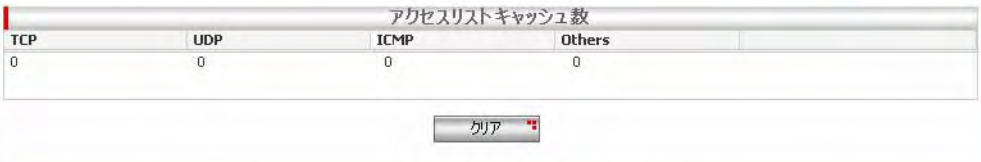
アクセスリストのキャッシュに関する情報が一覧表示されます。



パラメーター	説明
I/F	キャッシュを保持しているインターフェースが表示されます。
方向	通信の方向が表示されます。
プロトコル	通信プロトコルが表示されます。
送信元 IP アドレス－ポート番号	送信元の IP アドレスとポート番号が表示されます。
宛先 IP アドレス－ポート番号	宛先の IP アドレスとポート番号が表示されます。
生存時間	セッションが切れるまでの時間が秒単位で表示されます。
送信バイト数	送信元から宛先へ転送されたパケットのバイト数が表示されます。
受信バイト数	宛先から送信元へ転送されたパケットのバイト数が表示されます。

5.8.2.2 アクセスリストキャッシュ数

アクセスリストのキャッシュ数が一覧表示されます。



パラメーター	説明
TCP	TCP を使用したセッション数が表示されます。

UDP	UDP を使用したセッション数が表示されます。
ICMP	ICMP を使用したセッション数が表示されます。
Others	TCP/UDP/ICMP 以外のプロトコルを使用したセッション数が表示されます。
「クリア」ボタン	クリックすると、アクセスリストキャッシュ一覧、およびアクセスリストキャッシュ数をクリアします。

5.8.2.3 NAT キャッシュ一覧

NAT キャッシュに関する情報が一覧表示されます。

パラメーター	説明
I/F	送信元インターフェースが表示されます。
方向	通信の方向が表示されます。
プロトコル	通信プロトコルが表示されます。
送信元 IP アドレス－ポート番号	送信元の IP アドレスとポート番号が表示されます。
宛先 IP アドレス－ポート番号	宛先の IP アドレスとポート番号が表示されます。
NAT IP アドレス－ポート番号	NAT が使用された場合、変換後の NAT IP アドレスとポート番号が表示されます。
生存時間	セッションが切れるまでの時間が秒単位で表示されます。
送信バイト数	送信元から宛先へ転送されたパケットのバイト数が表示されます。
受信バイト数	宛先から送信元へ転送されたパケットのバイト数が表示されます。

5.8.2.4 NAT キャッシュ数

NAT キャッシュ数が一覧表示されます。

パラメーター	説明
TCP	TCP を使用したセッション数が表示されます。
UDP	UDP を使用したセッション数が表示されます。
ICMP	ICMP を使用したセッション数が表示されます。
Others	TCP/UDP/ICMP 以外のプロトコルを使用したセッション数が表示されます。
「クリア」ボタン	クリックすると、NAT キャッシュ一覧、および NAT キャッシュ数をクリアします。

5.8.2.5 表示件数指定 / 表示内容更新

表示件数の指定と、表示内容の更新を行えます。

パラメーター	説明
表示件数	一覧に表示する件数を設定します。
「更新」ボタン	クリックすると、指定された表示件数で表示内容を更新します。

5.9 URL フィルターの設定

URL フィルターを使用すると、HTTP 経由でアクセスする URL の合否を判定し、アクセス可能な URL かどうかを制御することができます。

URL フィルターの設定を有効にするには、「サービスの有効 / 無効」ページでファイアウォールを有効にし、「URL フィルター」をチェックする必要があります。

5.9.1 URL フィルタールールの追加

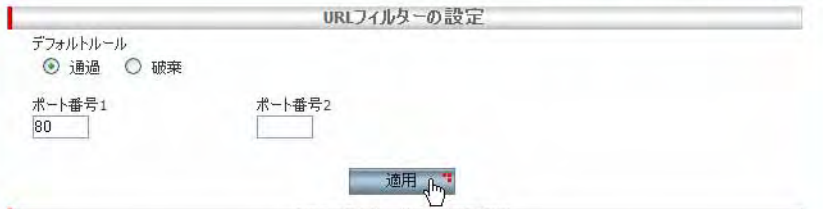
新規に URL フィルタールールを追加する場合は、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「URL フィルター」の順にクリックします。

2.「URL フィルタールールの設定」の各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下の内容を設定するものとします。

キーワード	example.net
比較条件	含む
動作	破棄
ログ	有効

3.「URL フィルターの設定」でデフォルトルールを確認します。ここでは、「デフォルトルール」を「通過」に、「ポート番号 1」を「80」に設定し、「適用」ボタンをクリックします。



4. 以上で設定は完了です。URL フィルターを有効にする方法については「P. 18 機能の有効化 / 無効化の設定」を参照してください。
   登録されている URL フィルターは、「URL フィルターリスト」で確認できます。

5.9.2 URL フィルタールールの変更

既存の URL フィルタールールを変更するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「URL フィルター」の順にクリックします。
2. 「URL フィルターリスト」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

5.9.3 URL フィルタールールの削除

既存の URL フィルタールールをリストから削除するには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「URL フィルター」の順にクリックします。
2. 「URL フィルターリスト」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

5.9.4 「URL フィルター」ページの解説

「URL フィルター」ページについて解説します。このページでは、URL フィルターのデフォルトルールの設定、および URL フィルターリストの編集を行うことができます。

5.9.4.1 URL フィルターの設定

メニューから「ファイアウォール /NAT」->「URL フィルター」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
デフォルトルール		登録されているルールにマッチしなかった場合の動作を選択します。初期状態は、「破棄」です。
	通過	登録されているルールにマッチしなかった場合、該当の HTTP パケットを転送します。
	破棄	登録されているルールにマッチしなかった場合、該当の HTTP パケットを破棄します。この場合、送信元 IP アドレス宛に TCP RESET を送信します。
ポート番号 1/ ポート番号 2		URL フィルター機能が監視する TCP ポート番号を指定します。監視できるポート番号数は、最大 2 つです。80 番以外のポート番号を監視する場合や、複数のポート番号を監視する場合には、それぞれ監視するポート番号を入力します。何も入力されていない場合は、初期状態と同じく 80 番が監視ポートになります。
「適用」ボタン		設定内容の変更を保存します。

5.9.4.2 URL フィルタールールの設定

「URL フィルタールールの設定」には以下の内容が表示されます。

パラメーター	オプション	説明
ID		ルールの ID です。ルールを選択している場合には、選択しているルールの ID（1 ～ 31）が表示されます。未選択時には ID は表示されません。
キーワード		HTTP パケット内に存在する URL 文字列で検索するキーワードを入力します。入力可能な文字数は、1 ～ 64 文字です。大文字・小文字は区別しません。 URL フィルターの評価は、LAN 側から受信された HTTP「GET」「CONNECT」パケットの「Request URI」と「Host」部に示されている文字列中に「キーワード」が存在するかどうかを評価します。
比較条件		検索するキーワードの比較条件を選択します。
	含む	URL 文字列にキーワード文字列が含まれるかどうかを検索します。含まれた場合、ルールにマッチしたと判定します。
	含まない	URL 文字列にキーワード文字列が含まれないかどうかを検索します。含まれていなかった場合、ルールにマッチしたと判定します。
	すべて対象	この比較条件が選択された場合、すべての HTTP パケットに対して、ルールにマッチしたと判定します。（キーワードの指定はできません。）
動作		ルールにマッチした際の動作を選択します。 URL フィルターは、HTTP パケットに対して、最初に登録されたルールから順に評価し、ルールにマッチするものがあった場合、ここで指定された動作を実行します。（マッチしたルールより後のルールは評価されません。）マッチしたルールの動作が「通過」であった場合、該当の HTTP パケットはそのまま転送され、「破棄」であった場合、該当する HTTP パケットの送信元に TCP RESET を送信します。
	通過	該当の HTTP パケットを転送します。
	破棄	該当の HTTP パケットを破棄します。この場合、送信元 IP アドレス宛に TCP RESET を送信します。
ログ		ルールにマッチした際にそのことをログに記録するかどうかを選択します。「有効」の場合はログに記録し、「無効」の場合はログに記録しません。

5.9.4.3 URL フィルターリスト

「URL フィルターリスト」テーブルには、現在設定されている URL フィルタールールのリストが表示されます。以下の内容が表示されます。

パラメーター	オプション	説明
ID		ルールの ID を表示します。
比較条件		HTTP パケット内に存在する URL 文字列で検索するキーワードの比較条件（含む / 含まない / すべて対象）を表示します。
動作		ルールにマッチした際の動作（通過 / 破棄）を表示します。
ログ		ルールにマッチした際にそのことをログに記録するかどうか（有効 / 無効）を表示します。
キーワード		HTTP パケット内に存在する URL 文字列で検索するキーワードを表示します。

5.10 DoS 検出の設定

DoS 検出 / 防御の設定を使用すると、WAN 側から入ってくるパケットに対して、DoS（Denial of Service）アタックや不正アクセス等の検知を制御することができます。検知したアタックや不正アクセスのパケットについて、破棄することもできます。

DoS アタックの検知を有効にするには、「サービスの有効 / 無効」ページでファイアウォールを有効にし、「DoS」をチェックする必要があります。検知するすべてのアタック種別の初期状態は、有効です。

DoS アタックや不正アクセス等を検知したことをログに記録することができます。また、DoS アタックの検知タイミングを変更することができます。

Flood 系アタックや Scan 系アタックの種別については、アタック検知後は、独自のアルゴリズムを使用し、ある一定時間をアタック継続中とみなし、「アタック検知後の動作」の振る舞いに従い、その期間は該当するパケットを「通過」または「破棄」します。アタックの継続を終了とみなした場合は、アタック継続中を解除します。

5.10.1 DoS 検出 / 防御の設定

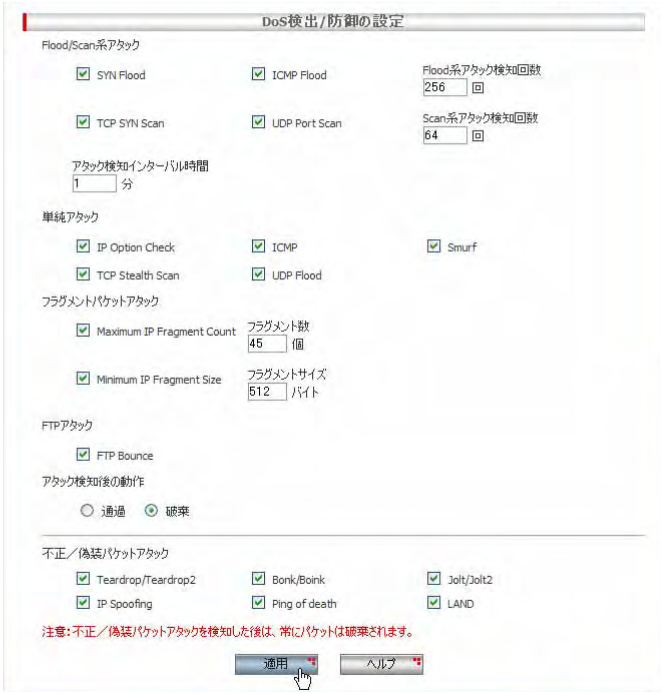
DoS 検出 / 防御の設定を行うには、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「DoS」の順にクリックします。

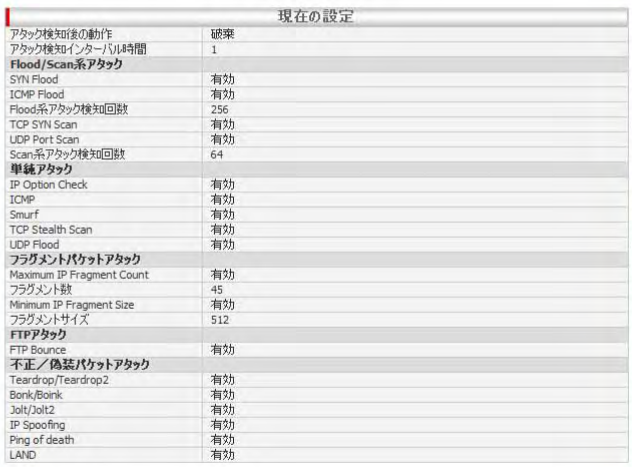
2.「DoS 検出 / 防御の設定」の各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下の内容を設定するものとします。

Flood/Scan 系アタック		（すべて有効）
	Flood/Scan 系アタック検知回数	256 回
	Scan 系アタック検知回数	64 回
	アタック検知インターバル時間	1 分
単純アタック		（すべて有効）
フラグメントパケットアタック		（すべて有効）
	フラグメント数	45 個

	フラグメントサイズ	512 バイト
FTP アタック	FTP Bounce	有効
アタック検知後の動作		破棄
不正／偽装パケットアタック		（すべて有効）



3. 以上で設定は完了です。登録されている設定内容は、画面下の「現在の設定」で確認できます。

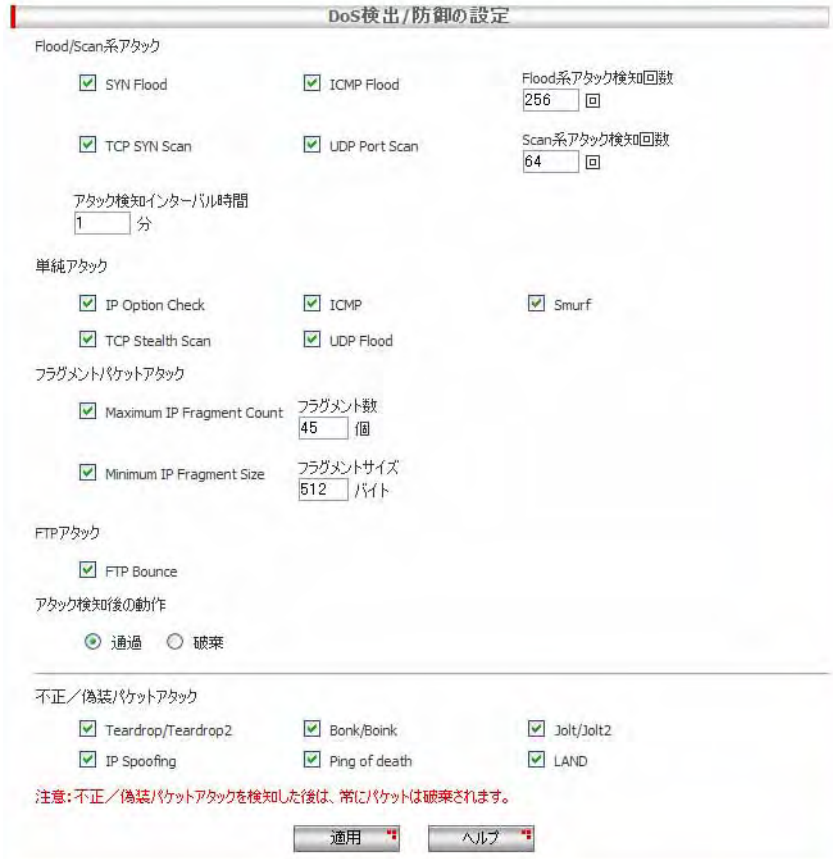


5.10.2 「DoS」ページの解説

「DoS」ページについて解説します。このページでは、DoS 検出 / 防御の設定、および現在の設定の表示を行うことができます。

5.10.2.1 DoS 検出 / 防御の設定

メニューから「ファイアウォール /NAT」->「アドバンスト設定」->「DoS」の順にクリックすると以下の画面が表示されます。



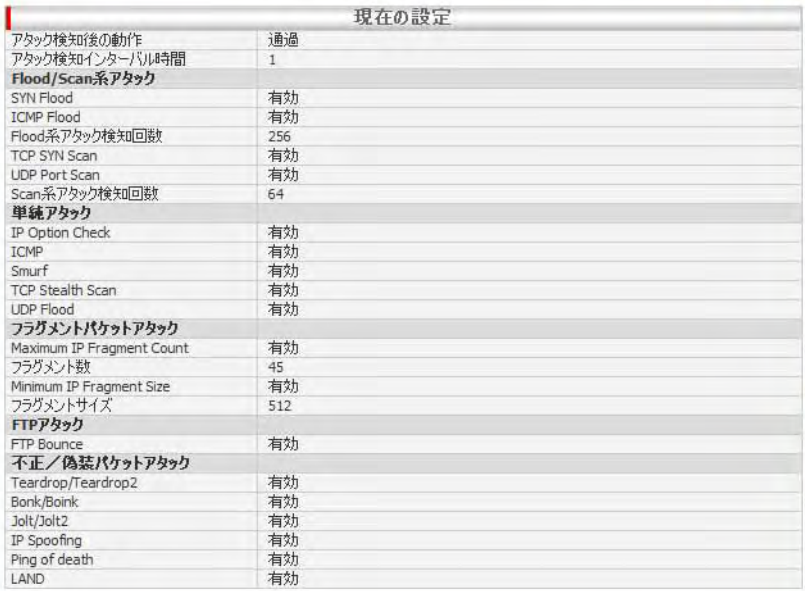
パラメーター	オプション	説明
Flood/Scan 系アタック		ネットワークサービスの提供を停止させるアタックおよびサービスの状態を検査する不正アクセスの種別です。これらのアタック検知条件は、「アタック検知インターバル時間」で指定された時間内に「Flood 系アタック検知回数」または「Scan 系アタック検知回数」で指定された回数を超えた場合です。
	SYN Flood	ある TCP/SYN パケットが、アタック検知条件を超えた場合に検知します。
	ICMP Flood	ある ICMP パケットが、アタック検知条件を超えた場合に検知します。
	Flood 系アタック検知回数	Flood 系アタックで検知する閾値を設定します。初期状態は、256 回です。設定可能な範囲は、1 ～ 10000 回です。
	TCP SYN Scan	TCP/SYN パケットにおいて、過去の送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号リストと比較一致し、ある時間内に規定回数に達した場合に、検知します。

	UDP Port Scan	UDP パケットにおいて、過去の送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号リストと比較し、送信元 IP アドレス、宛先 IP アドレスが一致し、宛先ポート番号が一致しない場合で、ある時間内に規定回数に達した場合に、検知します。
	Scan 系アタック検知回数	Scan 系アタックで検知する閾値を設定します。初期状態は、64 回です。設定可能な範囲は、1 ～ 10000 回です。
	アタック検知インターバル時間	「Flood 系アタック検知回数」および「Scan 系アタック検知回数」にてアタック検出を行う基準時間の閾値を設定します。初期状態は、1 分間です。設定可能な範囲は、1 ～ 1440 分です。例えば、アタック検知インターバル時間が 5 分、Flood 系アタック検知回数が 100 回と設定されていたとします。この場合は、5 分以内で 100 回目のアタックパケットを検知した際、アタック検知を開始し、継続中状態となります。
単純アタック		パケットの状態により検知するアタック種別です。
	IP Option Check	Security、Timestamp、Loose Source Routing、Strict Source Routing、Record Route、Stream ID、これらのオプション付き IP パケットを受信した場合に検知します。
	ICMP	Source quench、Timestamp request、Timestamp reply、Information request、Information reply、Mask request、Mask reply、これらの TYPE 種別の ICMP パケットを受信した場合に検知します。
	Smurf	ICMP エコーリクエストの宛先アドレスがブロードキャストアドレスの場合に検知します。
	TCP Stealth Scan	以下、いずれかの TCP パケットの場合に検知します。 ・TCP 制御フラグに何もセットされていない ・TCP 制御フラグに FIN/URG/PUSH のみがセットされている ・TCP 制御フラグに FIN のみがセットされている ・TCP 制御フラグに SYN/FIN のみがセットされている ・TCP 制御フラグに SYN/RST のみがセットされている
	UDP Flood	宛先ポートが chargen(19) ポートでかつ、送信元ポート番号が echo(7) の UDP パケットの場合に検知します。
フラグメントパケットアタック		フラグメントパケットに関するアタック種別です。
	Maximum IP Fragment Count	フラグメント数で指定されている数を超える IP フラグメントパケットの場合に検知します。
	フラグメント数	Maximum IP Fragment Count アタックで検知する最大フラグメント数の閾値を設定します。初期状態は、45 個です。設定可能な範囲は、1 ～ 512 個です。

	Minimum IP Fragment Size	フラグメントサイズで指定されているフラグメントサイズ数より小さい IP フラグメントパケットの場合に検知します。
	フラグメントサイズ	Minimum IP Fragment Size アタックで検知する最小フラグメントサイズの閾値を設定します。初期状態は、512 バイトです。設定可能な範囲は、64 ～ 1024 バイトです。
FTP アタック		FTP コマンドを改ざんするアタック種別です。
	FTP Bounce	以下、いずれかの FTP パケットの場合に検知します。 ・本来の受信先とは異なる IP アドレスを PORT コマンドで指定した ・PORT コマンドで、1024 番以下のポート番号を通知した
アタック検知後の動作		Flood/Scan 系アタック、単純アタック、FTP アタック、フラグメントパケットを検知した際、該当のパケットを通過させるか破棄するかを選択します。初期状態は、「通過」です。
不正／偽装パケットアタック		パケットの改ざんやなりすましなどによるアタック種別です。 「不正／偽装パケットアタック」に分類されるアタック種別は、「アタック検知後の動作」の状態に関係なく、該当パケットは破棄されます。
	Teardrop/Teardrop2	すでに処理したフラグメントオフセット値に重複するようなオフセット値が設定されている ICMP、UDP パケットの場合に検知します。
	Bonk/Boink	UDP ジィダーに重複するようなフラグメントオフセット値が設定されている UDP パケットの場合に検知します。
	Jolt/Jolt2	65536 バイト以上に設定された ICMP エコーリプライあるいは、UDP パケットの場合に検知します。
	IP Spoofing	以下、いずれかの IP パケットの場合に検知します。 ・AR260S V2 のインターフェースに設定されているいずれかの IP アドレスが送信元アドレスになっている IP パケットを受信した ・NAT 変換後として予約している IP アドレスが送信元アドレスになっている IP パケットを受信した ・受信したインターフェース以外のインターフェースのネットワークに属する IP アドレスが送信元になっているパケットを受信した場合
	Ping of death	65536 バイト以上に設定された ICMP パケットの場合に検知します。
	LAND	宛先 IP アドレス／ポート番号と送信元 IP アドレス／ポート番号が同一の TCP/SYN パケットの場合に検知します。
「適用」ボタン		設定内容の変更を保存します。

5.10.2.2 現在の設定

「現在の設定」には、現在設定されている DoS 検出 / 防御の設定内容が表示されます。



現在の設定	
アタック検知後の動作	通過
アタック検知インターバル時間	1
Flood/Scan系アタック	
SYN Flood	有効
ICMP Flood	有効
Flood系アタック検知回数	256
TCP SYN Scan	有効
UDP Port Scan	有効
Scan系アタック検知回数	64
単純アタック	
IP Option Check	有効
ICMP	有効
Smurf	有効
TCP Stealth Scan	有効
UDP Flood	有効
フラグメントパケットアタック	
Maximum IP Fragment Count	有効
フラグメント数	45
Minimum IP Fragment Size	有効
フラグメントサイズ	512
FTPアタック	
FTP Bounce	有効
不正／偽装パケットアタック	
Teardrop/Teardrop2	有効
Bonk/Boink	有効
Jolt/Jolt2	有効
IP Spoofing	有効
Ping of death	有効
LAND	有効

パラメーター	オプション	説明
アタック検知後の動作		Flood/Scan 系アタック、単純アタック、FTP アタック、フラグメントパケットを検知した際、該当のパケットの通過 / 破棄の設定を表示します。
アタック検知インターバル時間		「Flood 系アタック検知回数」および「Scan 系アタック検知回数」にてアタック検出を行う基準時間の閾値（分）を表示します。
Flood/Scan 系アタック		現在設定されている「Flood/Scan 系アタック」の各項目を表示します。（SYN Flood、ICMP Flood、Flood 系アタック検知回数、TCP SYN Scan、UDP Port Scan、Scan 系アタック検知回数）
単純アタック		現在設定されている「単純アタック」の各項目を表示します。（IP Option Check、ICMP、Smurf、TCP Stealth Scan、UDP Flood）
フラグメントパケットアタック		現在設定されている「フラグメントパケットアタック」の各項目を表示します。（Maximum IP Fragment Count、フラグメント数、Minimum IP Fragment Size、フラグメントサイズ）
FTP アタック		現在設定されている「FTP アタック」の項目（FTP Bounce）を表示します。
不正／偽装パケットアタック		現在設定されている「不正／偽装パケットアタック」の各項目を表示します。（Teardrop/Teardrop2、Bonk/Boink、Jolt/Jolt2、IP Spoofing、Ping of death、LAND）

5.11 UPnP の設定

UPnP（ユニバーサル プラグ アンド プレイ）の設定を行うと、UPnP クライアントから自由にポートマッピングルールの追加 / 削除が行えるようになります。そのため、VoIP などのポートマッピングルールの設定が必要なサービスでも、事前に設定することなく通信が行えるようになります。

UPnP を有効にするには、「サービスの有効 / 無効」ページでファイアウォールを有効にし、「UPnP」をチェックする必要があります。

注意 接続可能な VoIP アダプタは 1 台のみです。

5.11.1 UPnP の設定

UPnP の設定を行う場合は、以下の手順を実行します。

1. メニューから「ファイアウォール /NAT」->「UPnP」の順にクリックします。

2. 各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下の内容を設定するものとします。

外部インターフェース	pppoe0
タイムアウト設定	無効

3. 以上で設定は完了です。登録されているポートマッピングルールは、「ポートマッピングルールリスト」で確認できます。

5.11.2 「UPnP」ページの解説

「UPnP」ページについて解説します。このページでは、UPnP の外部インターフェース、ポートマッピングルールのタイムアウトの設定を行うことができます。

5.11.2.1 ユニバーサル プラグ アンド プレイ設定

メニューから「ファイアウォール /NAT」->「UPnP」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
外部インターフェース		外部インターフェースを設定します。ここで設定したインターフェースで受信したパケットが UPnP によって作成されたポートマッピングルールの対象となります。
タイムアウト設定		ポートマッピングルールにタイムアウト時間を設定するかどうかを選択します。
	有効 / 無効	有効にした場合、指定したタイムアウト時間がルールに設定されるようになります。無効にした場合には、タイムアウトしないルールとなります。UPnP クライアントが明示的にタイムアウト時間を指定した場合、有効 / 無効に関係なくそのタイムアウト時間が優先して設定されます。
	タイムアウト	タイムアウト設定を有効にした場合、タイムアウト時間を設定します。設定可能な範囲は 1 ～ 86400 です。(単位 : 秒)
「適用」ボタン		設定内容の変更を保存します。

5.11.2.2 ポートマッピングルールリスト

「ポートマッピングルールリスト」テーブルには以下の内容が表示されます。

パラメーター	オプション	説明
プロトコル		ルールが適用されるプロトコルが表示されます。
外部 IP アドレス － ポート番号		ルールが適用される宛先 IP アドレスとポート番号が表示されます。
内部 IP アドレス－ポート番号		転送先の IP アドレスとポート番号が表示されます。
生存時間		タイムアウトまでの生存時間が表示されます。タイムアウト時間がない場合、「---」と表示されます。
補足説明		UPnP クライアントが補足説明を付けていた場合、その説明が表示されます。（最大 63 文字まで表示されます。）

6 VPN の設定

6.1 概要

VPN（Virtual Private Network）は、ネットワーク間に VPN（Virtual Private Network）を構築し、パケットを暗号化して通信を行い、ネットワーク間の通信のセキュリティーを低コストで実現する機能です。本製品の VPN は IPsec（IP Security）に準拠しています。IPsec とは、IP に暗号化や認証などのセキュリティー機能を付加する一連のプロトコル群です。本製品では「VPN 接続」ページで VPN を構築することができます。

6.2 VPN の設定

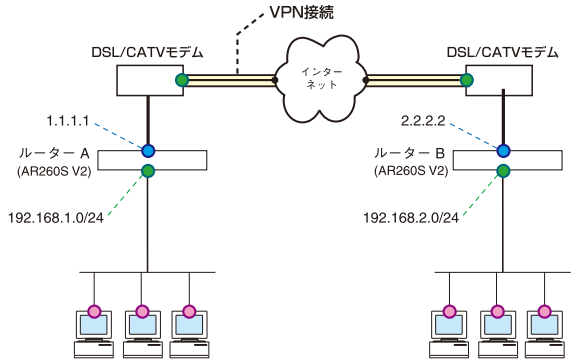
VPN でネットワーク間を接続するなど、VPN ゲートウェイ間で接続する場合に使用します。

6.2.1 ポリシーの作成

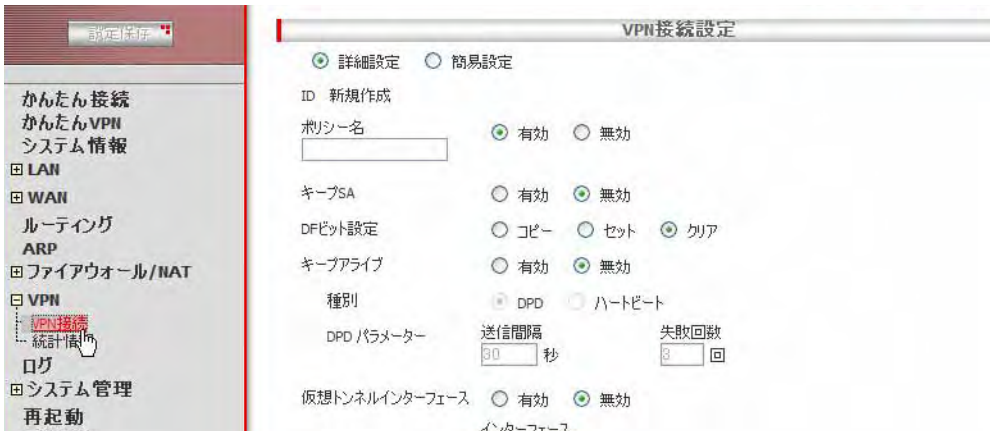
ポリシーを作成するには以下の手順を実行します。

ヒント

ここでは、下図のようなネットワーク構成でルーター A のポリシーを作成するものとします。



1. メニューから「VPN」->「VPN 接続」の順にクリックします。



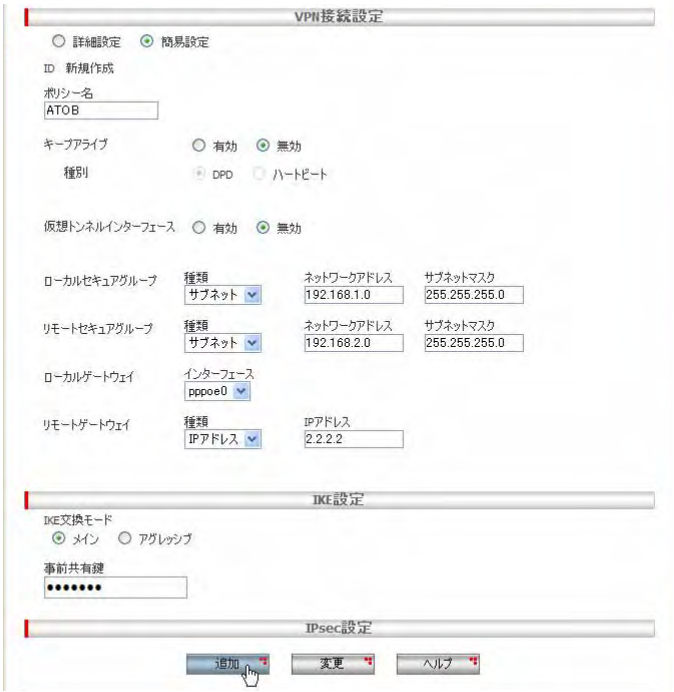
2. 各パラメーターを設定し「追加」ボタンをクリックします。ここでは以下のようにポリシーを設定するものとします。

VPN 接続設定テーブル

簡易設定 / 詳細設定		簡易設定
ポリシー名		ATOB
キープアライブ		無効
仮想トンネルインターフェース		無効
ローカルセキュアグループ	種類	サブネット
	ネットワークアドレス	192.168.1.0
	サブネットマスク	255.255.255.0
リモートセキュアグループ	種類	サブネット
	ネットワークアドレス	192.168.2.0
	サブネットマスク	255.255.255.0
ローカルゲートウェイ	インターフェース	pppoe0
リモートゲートウェイ	種類	IP アドレス
	IP アドレス	2.2.2.2

IKE 設定

IKE 交換モード	メイン
事前共有鍵	atobkey



3. ファイアウォールを有効にしている場合は以下の設定が必要です。

・ISAKMP のパケットが遮断されないようにセルフアクセスのルールを追加します。（初期状態で、UDP=500 は許可されています。）

・リモートセキュアグループからローカルセキュアグループ宛の通信が遮断されないように Inbound アクセスのルールを追加します。

・ローカルセキュアグループからリモートセキュアグループ宛の通信が遮断されないように Outbound アクセスのルールを追加します。（初期状態で、Outbound アクセスはすべて許可されています。）

・Inbound/Outbound には、以下のような設定を行います。（Inbound/Outbound アクセスのルールの作成について詳細は「P.101 ファイアウォール /NAT の設定」を参照してください。）

Outbound アクセスのルール

動作			通過
送信元		タイプ	サブネット
		ネットワークアドレス	192.168.1.0
		サブネットマスク	255.255.255.0
宛先		タイプ	サブネット
		ネットワークアドレス	192.168.2.0
		サブネットマスク	255.255.255.0

Inbound アクセスのルール

動作			通過
送信元		タイプ	サブネット

		ネットワークアドレス	192.168.2.0
		サブネットマスク	255.255.255.0
宛先		タイプ	サブネット
		ネットワークアドレス	192.168.1.0
		サブネットマスク	255.255.255.0

4. 以上で設定は完了です。VPN サービスを有効にする方法については「P. 18 機能の有効化 / 無効化の設定」を参照してください。

6.2.2 ポリシーの変更

ポリシーを変更するには以下の手順を実行します。

1. メニューから「VPN」->「VPN 接続」の順にクリックします。
2. 「サイト間アクセスルール」テーブルの該当ポリシー左部にあるラジオボタンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

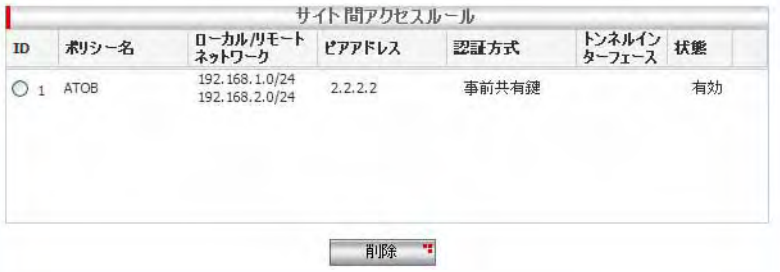
6.2.3 ポリシーの削除

ポリシーを削除するには以下の手順を実行します。

1. メニューから「VPN」->「VPN 接続」の順にクリックします。
2. 「サイト間アクセスルール」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 以上で設定は完了です。

6.2.4 ポリシーの確認

1. メニューから「VPN」->「VPN 接続」の順にクリックします。
2. 「サイト間アクセスルール」テーブルにポリシーが一覧表示されます。



6.2.5 「VPN 接続」ページの解説

「VPN 接続」ページについて解説します。

6.2.5.1 VPN 接続設定

メニューから「VPN」->「VPN 接続」の順にクリックすると以下の画面が表示されます。

パラメーター	オプション	説明
詳細設定 / 簡易設定		初期状態では、「詳細設定」が選択されており、すべての設定項目が表示されます。「簡易設定」を選択すると、VPN 設定に必要な最低限の設定項目だけが表示されます。初めての方には、「簡易設定」を選択してから設定を行うことをおすすめします。
ID		VPN 接続ポリシーを変更 / 削除する場合、対象 ID が表示されます。新規追加の場合は「新規作成」と表示されます。
ポリシー名		IPsec 設定を区別する名称を入力します。入力可能な文字数は、1 ～ 15 文字です。一度設定したポリシー名は変更できません。もし、変更が必要な場合は、一度、削除してから再度設定してください。

有効 / 無効			設定した IPsec ポリシーを有効にするか、無効にするかを選択します。初期状態は、「有効」です。ポリシーを無効にした場合、セキュアグループに該当する Outbound パケットは、IPsec 処理を行わず、そのままのパケットでネットワークに送出されます。
キープ SA			IPsec パケットを送受信するインターフェースが使用不能な状態（例：PPPoE 接続が切断した場合／ Ethernet ケーブルが切断された場合）になったとき、本製品が保持する ISAKMP SA/IPsec SA を消去するかどうかを設定します。有効に設定すると、ISAKMP SA/IPsec SA を保持し続けます。初期状態は、「無効」です。本製品に付与される WAN 側 IP アドレスが不定の場合は無効にする必要があります。
DF ビット設定			IPsec プロトコルによってカプセルしたパケットの外側 IP ヘッダーに付随する DF bit 値を設定します。初期状態は、「クリア」です。通信不能状態を作り出す可能性があるため、特別な場合以外は「クリア」を選択することを推奨します。
		コピー	IPsec 処理を行う内側パケットの DF bit 値をコピーします。
		セット	無条件に DF bit をセットします。
		クリア	無条件に DF bit をクリアします。
キープアライブ			対向装置への送達確認を行うかどうかを設定します。初期状態は、「無効」です。キープアライブを有効にした場合、プロトコルの選択が可能です。
	種別		キープアライブで使用するプロトコルを、「DPD」と「ハートビート」から選択します。 DPD を動作させるためには、プロトコル仕様上、対向機器でも DPD を有効にする必要があります。 ハートビートは、ハートビートキープアライブ機能を持っている AR ルーターのみと送達確認を行うことができます。 ハートビートのパラメーターは、送信間隔：20 秒、失敗回数：3 回が固定設定されています。
	DPD パラメーター		「種別」に「DPD」を指定した場合、以下のパラメーターを設定します。
		送信間隔	対向機器からの IPsec 通信がなく、かつ対向機器から DPD パケットが到達しない状態がこの時間だけ続くと DPD による送達確認を 4 います。初期状態は、30 秒です。設定可能な値範囲は 5 秒～ 3600 秒（1 時間）です。
		失敗回数	送達確認を行い、対向機器から応答が得られない状態がこの回数だけ続くと、この設定に関連した SA を削除します。初

	期状態は、3 回です。設定可能な値範囲は 1 ～ 64 回です。
仮想トンネルインターフェース	「無効」にした場合、ローカルセキュアグループ、リモートセキュアグループが一致するパケットが IPsec 処理の対象となります。「有効」にした場合、仮想トンネルインターフェース宛にルーティングされたパケットが IPsec 処理の対象となります。初期状態は「無効」です。 仮想トンネルインターフェースを有効にし、ルーティング優先度を設定することで、IPsec 通信の冗長化が可能です。このとき、キープアライブとの併用が必要です。また、仮想トンネルインターフェースを使用する場合、セキュアグループには「すべて」が設定されます。
インターフェース	IPsec 処理で使用する仮想トンネルインターフェースを選択します。「新規作成」では、新たに仮想トンネルインターフェースを作成します。最大 10 個まで作成することが可能です。仮想トンネルインターフェースを有効にした場合、「ルーティング」設定で IPsec を使用する通信に対して仮想トンネルインターフェースを宛先とするルートを設定する必要があります。さらに、IPsec SA が確立していないと、仮想トンネルインターフェース向けのルートが有効にならないため、デフォルトルートに従って、平文のままインターネットに送出される可能性があります。これを回避するため、仮想トンネルインターフェース向けのルートの設定に加え、null（破棄）ルートを低優先で設定しておくことをお勧めします。 例えば、フェーズ 2 ID のリモートが、192.168.10.0/24 の場合には、「宛先ネットワークアドレスに 192.168.10.0、宛先サブネットマスクに 255.255.255.0、インターフェースに tunnel0、優先度に 1」を設定します。そして、「宛先ネットワークアドレスに 192.168.10.0、宛先サブネットマスクに 255.255.255.0、インターフェースに null、優先度に 10」を続いて設定します。
ローカルセキュアグループ	IPsec 対象となるローカルネットワークを設定します。 Outbound（本製品から送信される）パケットは、送信元 IP アドレスがローカルセキュアグループに一致し、宛先 IP アドレスがリモートセキュアグループに一致する場合、暗号化されます。 Inbound （本製品で受信された）パケットは、送信元 IP アドレスがリモートセキュアグループに一致し、宛先 IP アドレスがローカルセキュアグループに一致する、暗号化されたパケットの場合に復号化されます。 通常、本製品の LAN 側ネットワークを入力します。設定方法には、以下の選択肢があり、それぞれパラメーターを必要とします。 内部 NAT を使用する場合は、NAT 処理を行う前のアドレスを入力します。
すべて	ローカルネットワークのアドレスをフィルター条件に含めません。リモートセキュアグループが一致すれば、すべてのパケットを IPsec 処理します。

IP アドレス		ローカルネットワークに存在するホスト 1 台が送受信するパケットに対してのみ IPsec を適用する場合に選択します。これに該当しないホストから送出されるパケットは、本製品の LAN 側ネットワークに接続されていても、IPsec 処理を受けません。
	IP アドレス	IPsec 処理対象とするホストの IP アドレスを記述します。
サブネット		ローカルネットワーク上に存在する複数のホストを IPsec 対象とする場合に指定します。ネットワークアドレスとサブネットマスクにより設定します。
	ネットワークアドレス	ローカルネットワークのネットワークアドレスを入力します。ホストアドレス部は 0 でなければなりません。
	サブネットマスク	上記ネットワークアドレスに対応するサブネットマスクを入力します。マスク値は、マスク長に変換できる値でなければなりません。
リモートセキュアグループ		IPsec 対象となるリモートネットワークを設定します。
すべて		リモートのすべてのコンピューターにポリシーを適用する場合に選択します。
IP アドレス		ポリシーを適用するコンピューターを IP アドレスで 1 台指定する場合に選択します。
	IP アドレス	リモートセキュアグループの種類に IP アドレスを選択した場合にのみ表示されます。ポリシーを適用するコンピューターの IP アドレスを入力します。
サブネット		ポリシーを適用するコンピューターをサブネットで指定する場合に選択します。
	ネットワークアドレス	リモートセキュアグループの種類に「サブネット」を選択した場合にのみ表示されます。ポリシーを適用するグループのネットワークアドレスを入力します。
	サブネットマスク	リモートセキュアグループの種類に「サブネット」を選択した場合にのみ表示されます。ポリシーを適用するグループのサブネットマスクを入力します。
ローカルゲートウェイ		IPsec パケットの送受信を行うインターフェースを選択します。パケットルーティングの結果、セキュアグループに該当するパケットが、選択されたインターフェースを通過する場合に IPsec 処理が行われます。ルーティングによってパケットが異なるインターフェースから出

			力される場合は、IPsec 処理が行われません。
リモートゲートウェイ			IPsec 通信を行う対向機器を設定します。
	任意		任意の IP アドレスを持つ機器から接続を受け付け、ISAKMP ネゴシエーションを開始します。この場合、本製品が、イニシエーターとなって ISAKMP ネゴシエーションを開始することはありません。
	IP アドレス		リモートゲートウェイで IP アドレスを選択した場合に対向機器の IP アドレスを設定します。一般的に対向機器の WAN 側 IP アドレスとなります。
		IP アドレス	リモートゲートウェイの種類に「IP アドレス」を選択した場合にのみ表示されます。リモートゲートウェイの IP アドレスを入力します。
内部 NAT			RFC2709 で定義された NAT を使用可能にするかどうかを設定します。初期状態は、「無効」です。この設定を有効にすることで、IPsec 対象となるパケットを NAT 処理後に IPsec 処理することを可能にします。 この設定を無効にした場合、インターフェースに NAT が設定されていたとしても、IPsec 対象となるパケットは NAT 処理を受けません。 内部 NAT を実現するためには、本設定に加えて、ファイアウォール設定で対応する NAT 設定を行う必要があります。 また、一般的に内部 NAT を行う場合、IPsec フェーズ 2 ID を、ローカルセキュアグループとは異なる値にする必要があるため、下記のフェーズ 2 ローカル ID を設定する必要があります。
フェーズ 2 ID			内部 NAT を適用する場合、セキュアグループの設定値と実際に対向機器に対して送信されるパケットの内容にて矛盾が発生します。また、仮想トンネルインターフェースを使用した場合、対向機器に対し送信する自装置のネットワーク情報と対向装置のネットワーク情報を設定しなければなりません。これらの場合に必要な、フェーズ 2 ISAKMP ネゴシエーションに設定する ID を指定します。 フェーズ 2 ID には IP アドレス型、またはサブネット型のみが使用可能であり、マスク長を伴った IP アドレスを設定する必要があります。
	ローカル		フェーズ 2 ローカル ID を設定します。
	リモート		フェーズ 2 リモート ID を設定します。
NAT トラバーサル			NAT トラバーサルを使用するかどうかを選択します。初期状態は「無効」です。この設定を有効にすることで、NAT 装置を経由する IPsec 通信が可能になります。また、有効にした場合でも NAT 装置を検出しなかった場合、NAT トラバーサルを用いた通信は行いません。 この設定を無効にした場合、NAT 装置を

	経由する IPsec 通信が行えなくなります。

ヒント

IPsec の 1 フレームが取り扱うことのできる最大フレームサイズは、以下のいずれかの条件の場合、32 キロバイトとなります。
・自身宛・自身発のパケット送受信（例：ping -s 64000 192.168.1.1）
・ファイアウォールルール設定インターフェースのパケットフォワーディング
・NAT 設定インターフェースのパケットフォワーディング

ヒント

仮想トンネルインターフェースを有効にし、リモートゲートウェイに「任意」以外を設定した場合、設定が完了すると同時に ISAKMP ネゴシエーションを開始します。また、VPN 接続設定が変更された場合など、IPsec SA が削除された場合も ISAKMP ネゴシエーションを開始します。

ヒント

一度作成した仮想トンネルインターフェース（tunnel0 など）を直接削除することはできません。
削除を行うには、リセットスイッチの操作、または「システム管理」->「システムの設定」->「デフォルト設定」により本製品を工場出荷時の状態に戻す必要があります。

6.2.5.2 IKE 設定

パラメーター		説明
IKE 交換モード		ISAKMP 交換をメインモードで行うか、アグレッシブモードで行うかを選択します。初期状態は、「メインモード」です。対向機器と一致している必要があり、リモートゲートウェイで「任意」を選択した場合は、アグレッシブモードを使用するのが一般的です。
	メイン	メインモードを使用する場合に選択します。メインモードではネゴシエーション中の ID 情報を保護します。
	アグレッシブ	アグレッシブモードを使用する場合に選択します。アグレッシブモードではネゴシエーション中に ID 情報を保護しません。メインモードに比べて IKE トンネルの交換プロセスが少ないので処理が高速です。
ローカル ID		フェーズ 1 ネゴシエーション時に対向機器に対して送信する、本製品のフェーズ 1 ID を設定します。対向機器のリモート ID 設定と一致している必要があります。

	未定義		フェーズ 1 ID を指定しない場合に選択します。「未定義」を選択した場合、「リモートゲートウェイ」で指定した IP アドレスがフェーズ 1 ID に使用されます。
	FQDN		フェーズ 1 ID を FQDN(Fully Qualified Domain Name) で指定する場合に選択します。
		FQDN	FQDN 型フェーズ 1 ID を設定します。文字列中に '@' を含むことはできません。入力可能な文字数は、1 ～ 32 文字です。
	E-mail		フェーズ 1 ID を E-mail アドレスで指定する場合に選択します。
		E-mail	E-mail Address 型フェーズ 1 ID を設定します。文字列中に '@' を含まなければなりません。入力可能な文字数は、1 ～ 32 文字です。
リモート ID			フェーズ 1 ネゴシエーション時に対向機器から受信するフェーズ 1 ID として受け入れ可能なものを設定します。IKE 設定の「IKE 交換モード」で「アグレッシブ」を選択した場合にのみ表示されます。対向機器のローカル ID の設定と一致している必要があります。
		未定義	フェーズ 1 ID を指定しない場合に選択します。「未定義」を選択した場合、「リモートゲートウェイ」で指定した IP アドレスがフェーズ 1 ID に使用されます。
	FQDN		フェーズ 1 ID を FQDN(Fully Qualified Domain Name) で指定する場合に選択します。
		FQDN	FQDN 型フェーズ 1 ID を設定します。文字列中に '@' を含むことはできません。入力可能な文字数は、1 ～ 32 文字です。
	E-mail		フェーズ 1 ID を E-mail アドレスで指定する場合に選択します。
		E-mail	E-mail Address 型フェーズ 1 ID を設定します。文字列中に '@' を含まなければなりません。入力可能な文字数は、1 ～ 32 文字です。
事前共有鍵			ISAKMP ネゴシエーションの認証に用いる事前共有鍵の文字列を設定します。入力可能な文字数は、1 ～ 32 文字です。対向機器との間で、完全に一致していなければなりません。
IKE 暗号化 / 認証アルゴリズム			ISAKMP SA を形成するために用いる暗号・認証アルゴリズム、および Diffie-Hellman グループを選択します。初期状態では、「3DES & SHA1-DH2」です。こ

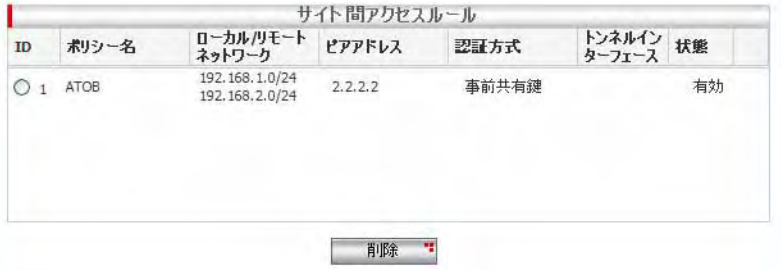
	の設定値は、対向機器との間で、完全に一致していなければなりません。
有効期限	ISAKMP SA の寿命を設定します。初期状態は、3600 秒です。設定可能な値範囲は 600 秒（10 分）～ 259200 秒（3 日）です。秒、分、および時間の単位を用いて設定が可能です。表示には、これらのうち最適な単位で表示されます。

6.2.5.3 IPsec 設定

パラメーター	説明
IPsec 暗号化 / 認証アルゴリズム	IPsec SA を形成する際に使用するプロトコル、および暗号・認証アルゴリズムを選択します。初期状態は、「ESP 3DES HMAC SHA1」です。この設定値は、対向機器と一致する必要があります。
PFS グループ	「DH-1」、「DH-2」、「DH-5」から選択します。PFS グループを指定しない場合は「なし」を選択します。
有効期限	IPsec SA の寿命を設定します。初期状態は、3600 秒です。設定可能な値範囲は 300 秒（5 分）～ 259200 秒（3 日）です。秒、分、および時間の単位を用いて設定が可能です。表示には、これらのうち最適な単位で表示されます。下記のファイルサイズによる寿命を設定した場合でも、上記範囲内での有効期限を設定する必要があります。
ファイルサイズ	通信量に従った IPsec SA の寿命を設定します。（単位：キロバイト）値の範囲は 1 キロバイト ～ 4 ギガバイトです。0 を設定すると、通信量に従った寿命を設定しません。
「追加」ボタン	VPN ポリシーを追加登録します。ボタンをクリックすると設定内容が即時に反映されます。
「変更」ボタン	「サイト間アクセスルール」で選択した項目の編集を行った場合、内容の変更を保存します。ボタンをクリックすると設定内容が即時に反映されます。
「ヘルプ」ボタン	操作のヒントを参照することができます。

6.2.6 サイト間アクセスルール

VPN ポリシーが一覧表示されます。



パラメーター	説明
ID	ポリシーの ID 番号が表示されます。
ポリシー名	ポリシー名が表示されます。
ローカル / リモートネットワーク	ローカル / リモートセキュアグループに関する情報が表示されます。
ピアアドレス	リモートゲートウェイの IP アドレスが表示されます。
認証方式	鍵管理方式が表示されます。
トンネルインターフェース	設定されているトンネルインターフェースが表示されます。
状態	VPN の有効 / 無効が表示されます。
「削除」ボタン	ラジオボタンで選択した既存のルールを削除します。ボタンをクリックすると設定内容が即時に反映されます。

6.3 VPN トラフィックの確認

「統計情報」ページでは、本製品の VPN に関するパケット転送の統計を参照することができます。

6.3.1 確認

VPN トラフィックの状況を確認するには以下の手順を実行します。

1. メニューから「VPN」->「統計情報」をクリックします。

2. 参照するタブを「SA」、「基本統計情報」、「詳細統計情報」から選択すると、各情報を表示できます。表示を更新するには各画面の「更新」ボタンをクリックします。

6.3.2 「統計情報」ページの解説

「統計情報」ページでは、VPN 接続に関する統計情報を参照できます。

6.3.2.1 SA - IKE SA

「SA」タブの「IKE SA」テーブルには、以下の情報が表示されます。

パラメーター	説明
ポリシー名	IKE SA のポリシー名が表示されます。
ローカル ID	IKE SA 確立時のローカル ID が表示されます。
リモート ID	IKE SA 確立時のリモート ID が表示されます。
ローカルポート	IKE SA 確立時に使用するローカルポートの番号が表示されます。
リモートポート	IKE SA 確立時に使用するリモートポートの番号が表示されます。
SA 状態	フェーズ 1 のステータスが表示されます。
鍵交換タイプ	IKE 交換モードが表示されます。
イニシエータ	本製品がイニシエーターとして動作している場合に「Yes」、レスポンダーとして動作している場合に「No」が表示されます。
「削除」ボタン	リストから選択された項目を削除します。

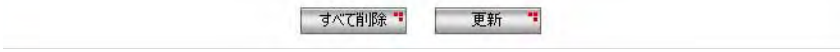
6.3.2.2 SA - IPsec SA

「SA」タブの「IPsec SA」テーブルには、以下の情報が表示されます。

パラメーター	説明
ポリシー名	IPsec SA のポリシー名が表示されます。
SPI	SPI（Security Parameter Index）が表示されます。
プロトコル	VPN トンネルで使用されているプロトコルが表示されます。
送信元アドレス	VPN トンネルのローカルゲートウェイの IP アドレスが表示されます。
送信先アドレス	VPN トンネルのリモートゲートウェイの IP アドレスが表示されます。
トンネル MSS	使用する仮想トンネルインターフェースの MSS 値が表示されます。
イニシエータ	本製品がイニシエーターとして動作している場合に「Yes」、レスポンダーとして動作している場合に「No」が表示されます。

6.3.2.3 SA （共通）

「SA」タブの画面下部には、以下のボタンが表示されます。



パラメーター	説明
「すべて削除」ボタン	一覧に含まれる IKE SA および IPsec SA の内容がすべて削除されます。
「更新」ボタン	「SA」タブの表示内容を、最新の情報に更新します。

6.3.2.4 基本統計情報

メニューから「VPN」->「統計情報」の順にクリックして、「基本統計情報」タブをクリックすると、以下の画面が表示されます。

パラメーター	オプション	説明
IPsec 統計情報		IPsec SA のパケットの統計情報が一覧表示されます。
	AH Packets Done	転送された AH パケット数がカウントされます。
	AH Packets Failed	破棄された AH パケット数がカウントされます。
	ESP Packets Done	転送された ESP パケット数がカウントされます。
	ESP Packets Failed	破棄された ESP パケット数がカウントされます。
	Acquires	IPsec モジュールから ISAKMP モジュールへ SA の確立が要求された回数がカウントされます。
IKE 統計情報		IKE のネゴシエーションの情報が一覧表示されます。
	IKE Phase1 Negotiations Done	完了した IKE フェーズ 1 のネゴシエーション数がカウントされます。
	IKE Phase1 Negotiations Failed	失敗した IKE フェーズ 1 のネゴシエーション数がカウントされます。
	IKE Phase2 Negotiations Done	完了した IKE フェーズ 2 のネゴシエーション数がカウントされます。
	IKE Phase2 Negotiations Failed	失敗した IKE フェーズ 2 のネゴシエーション数がカウントされます。

「更新」ボタン	表示されている内容を、最新の情報に更新します。

6.3.2.5 詳細統計情報

メニューから「VPN」->「統計情報」の順にクリックして、「詳細統計情報」タブをクリックすると、以下の画面が表示されます。

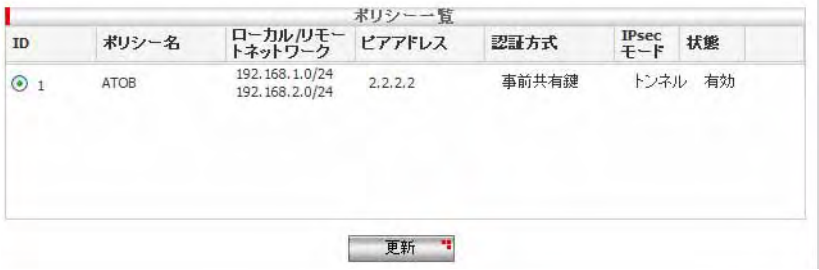
詳細統計情報

ISAKMP 装置全体 統計情報	
Unknown Cookie Quick	0
Unknown Cookie Info	0
Length Error	0
Invalid Version	0
Borken Packet	0
No Policy	0
IPsec 装置全体 統計情報	
Length Error	0
In Unknown SPI	0
In Policy Drop	0

ISAKMP ポリシー別 統計情報	
Out Packet	0
In Packet	0
Resend Packet	0
Rerecv Packet	0
Out Info Packet	0
In Info Packet	0
Recv Acquire	0
Main Mode Start	0
Main Mode Success	0
Agg Mode Start	0
Agg Mode Success	0
Quick Mode Start	0
Quick Mode Success	0
Force ISAKMP	0
Force IPsec	0
No Memory	0
Prop Mismatch	0
ID Mismatch	0
Quick Hash Fail	0
Info Hash Fail	0
Auth Fail	0
Timeout	0
Canceled	0
Send Fail	0
Invalid Exchange Type	0
Invalid Flags	0
Invalid Payload Type	0
Not Enough Payload	0
DH Process Fail	0
Random Process Fail	0
Hash Process Fail	0
Encrypt Fail	0
Decrypt Fail	0
Securit yError	0
IPsec Config Fail	0
Parse Fail	0
Padding Error	0

IPsecポリシー別 統計情報

Out Start	0
In Start	0
Out ESP Start	0
Out FF ESP Start	0
Out AH Start	0
In ESP Start	0
In AH Start	0
Out ESP Success	0
Out AH Success	0
In ESP Success	0
In AH Success	0
Out Success	0
In Success	0
SA Search	0
SA Acquire	0
Out Pendded	0
In Pendded	0
No Memory	0
No Encrypt Memory	0
No Decrypt Memory	0
Encrypt Fail	0
Decrypt Fail	0
IPsec Send Fail	0
Plain Send Fail	0
Tunnel Fail	0
In Auth Fail	0
In Replay	0
Invalid Padding	0
Out No SA	0
In No SA	0
Canot SA Use	0
Crypto Busy	0
SA Install Fail	0



ポリシー一覧

ID	ポリシー名	ローカル/リモートネットワーク	ピアアドレス	認証方式	IPsecモード	状態
1	ATOB	192.168.1.0/24 192.168.2.0/24	2.2.2.2	事前共有鍵	トンネル	有効

更新

パラメーター	オプション	説明
ISAKMP 装置全体 統計情報		ISAKMP 装置全体 統計情報が一覧表示されます。
IPsec 装置全体 統計情報		IPsec 装置全体 統計情報が一覧表示されます。
ISAKMP ポリシー別 統計情報		ISAKMP ポリシー別 統計情報が一覧表示されます。
IPsec ポリシー別 統計情報		IPsec ポリシー別 統計情報が一覧表示されます。
ポリシー一覧		ポリシー一覧が表示されます。
ポリシー一覧	「更新」ボタン	表示されているポリシー一覧を最新の情報に更新します。

7　付録

7.1　デフォルト設定

本製品のデフォルト設定は以下のとおりです。

7.1.1　ユーザー名 / パスワードのデフォルト設定

ユーザー名	レベル	パスワード
manager	管理者	friend
guest	ユーザー	guest

本製品ではユーザー名を変更することはできません。

7.1.2　設定ページ別のデフォルト設定

「LAN」/「IP」		
	IP アドレス	192.168.1.1
	サブネットマスク	255.255.255.0
	ダイレクトブロードキャスト転送	無効
「LAN」/「DHCP」		
	IP アドレスプール	192.168.1.223 ～ 192.168.1.254
	サブネットマスク	255.255.255.0
	デフォルトゲートウェイ	192.168.1.1
	リース期限	00:12:00
	ドメイン名	空白（未設定）
	プライマリー DNS サーバー	192.168.1.1
	セカンダリー DNS サーバー	空白（未設定）
	プライマリー WINS サーバー	空白（未設定）
	セカンダリー WINS サーバー	空白（未設定）
「LAN」/「固定 DHCP クライアント」		
		設定なし
「WAN」/「WAN」/PPPoE（pppoe1、pppoe2）（デフォルト）		
	アンナンバード PPPoE	無効
	DNS オプション	自動取得

	MSS クランプ	自動計算
	クランプ値	40 バイト
	接続オプション	キープアライブ
	エコー送信間隔	60 秒
「WAN」/「WAN」/DHCP		
	ダイレクトブロードキャスト転送	無効
	DNS オプション	自動取得
「WAN」/「WAN」/固定 IP		
	ダイレクトブロードキャスト転送	無効
「WAN」/「インターフェース設定」		
	リンク設定	自動
「WAN」/「ダイナミック DNS 設定」		
	登録するインターフェース	未設定
	更新間隔	20 日
「ルーティング」		
	宛先ネットワークアドレス	192.168.1.0
	宛先サブネットマスク	255.255.255.0
	ゲートウェイ	インターフェース /eth1
「ARP」		
		設定なし
「ファイアウォール /NAT」/「アクセス制御」		
	Inbound アクセス	設定なし（遮断）
	Outbound アクセス	すべて透過
「ファイアウォール /NAT」/「URL フィルター」		
	デフォルトルール	破棄
	ポート番号 1	80
	ポート番号 2	設定なし
	URL フィルタールールの設定	設定なし
「ファイアウォール /NAT」/「NAT 設定」/「NAT」		
	pppoe1、pppoe2	インターフェース ENAT （送信元：すべて、宛先：すべて、プロトコル：すべて）
	NAT プール	設定なし
「ファイアウォール /NAT」/「アドバンスト設定」/「セルフアクセス」		

	ステルスモード	無効	
	セルフアクセス制御設定	LAN（eth1）	設定無し
		WAN（eth0、pppoe0、pppoe1）	UDP500 通過
「ファイアウォール /NAT」/「アドバンスト設定」/「タイムアウト設定」			
		DefaultTcp 300 秒、DefaultUdp 60 秒、 DefaultIcmp 60 秒、TcpRest 5 秒、DefaultDNS 20 秒	
「ファイアウォール /NAT」/「アドバンスト設定」/「DoS」			
Flood/Scan 系アタック			SYN Flood, ICMP Flood, TCP SYN Scan, UDP Port Scan（すべて有効）
	Flood/Scan 系アタック検知回数		256 回
	Scan 系アタック検知回数		64 回
	アタック検知インターバル時間		1 分
単純アタック			IP Option Check, ICMP, Smurf, TCP Stealth Scan, UDP Flood（すべて有効）
フラグメントパケットアタック			Maximum IP Fragment Count, Minimum IP Fragment Size（すべて有効）
		フラグメント数	45 個
		フラグメントサイズ	512 バイト
FTP アタック		FTP Bounce	有効
アタック検知後の動作			通過
不正／偽装パケットアタック			Teardrop/Teardrop2, Bonk/Boink, Jolt/ Jolt2, IP Spoofing, Ping of death, LAND（すべて有効）
「ファイアウォール /NAT」/「UPnP」			
	外部インターフェース	未設定	
	タイムアウト設定	無効	
「VPN」/「VPN 接続」			
		設定なし	
「ログ」/「システムログ設定」			
	ログ種類	IP：通知、DHCP：通知、PPP：通知、VPN：通知、 ETH：通知、NAT：通知、ファイアウォール：通知、 ブリッジ：通知、システム：通知、アプリケーション：通知	
	ログサーバー IP アドレス	空白（未設定）	
	送信元 IP アドレス	自動選択	
「システム管理」/「サービスの有効 / 無効」			
	ファイアウォール	有効 セルフアクセス、アクセス制御、NAT 、DoS：有効	

		URL フィルター：無効
	ブリッジ	無効 IPv6 ブリッジ：有効 PPPoE ブリッジ：無効
	VPN	有効 SA の強制確立：無効
	DNS リレー	有効
	DHCP	有効
	SNTP	無効
	SNMP	無効
	ダイナミック DNS	無効
	リセットスイッチによる初期化	有効
「システム管理」/「設定管理 / パスワード」		
	設定管理クライアント	空白（未設定）
	管理者パスワード	friend（ユーザー名 :manager）
	ユーザーパスワード	guest（ユーザー名 :guest）
「システム管理」/「システム情報」		
	システム名（sysName）	Router
	システムロケーション	空白（未設定）
	連絡先	空白（未設定）
「システム管理」/「タイムゾーン設定」		
	日付	2001 年 1 月 1 日
	時刻	0 時 0 分 0 秒
	タイムゾーン	GMT+9:00
	SNTP サーバー 1	133.243.238.243
	SNTP サーバー 2	133.243.238.244
	SNTP サーバー 3	210.173.160.27
	SNTP サーバー 4	210.173.160.57
	更新間隔	60 分
	送信元 IP アドレス	自動選択
「システム管理」/「SNMP」		
	SNMP	無効
	コミュニティー名	public

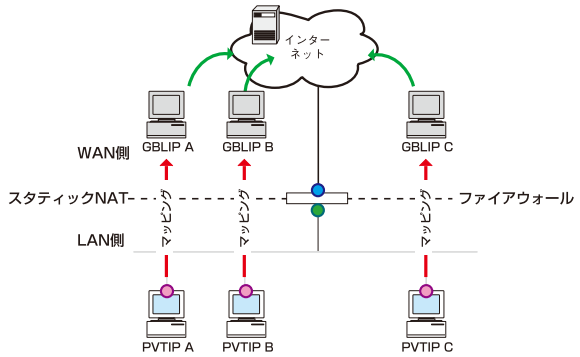
通知先アドレス（トラップホスト）	空白（未設定）
トラップ送信元 IP アドレス	自動選択

7.2 NAT について

NAT(Network Address Translation) とは、ローカルネットワーク内のみで使用するプライベート IP アドレスとグローバル IP アドレスを相互に変換し、プライベート IP アドレスを使用するローカルネットワーク内のクライアントからインターネットにアクセスできるようにする仕組みです。本製品ではスタティック NAT、ダイナミック NAT、ENAT、インターフェース ENAT を使用できます。

7.2.1 スタティック NAT

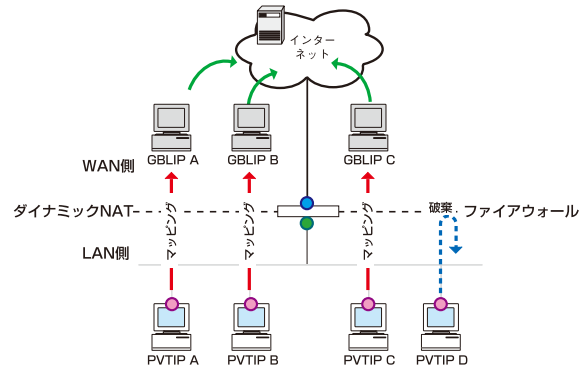
スタティック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で固定的にマッピングします。管理者が意図的に変更しない限りマッピングは固定的に行われます。つまり、1 台のクライアントのプライベート IP アドレスに対して、常に同じグローバル IP アドレスがマッピングされます。グローバル IP アドレスはプライベート IP アドレスと同じ数必要です。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

7.2.2 ダイナミック NAT

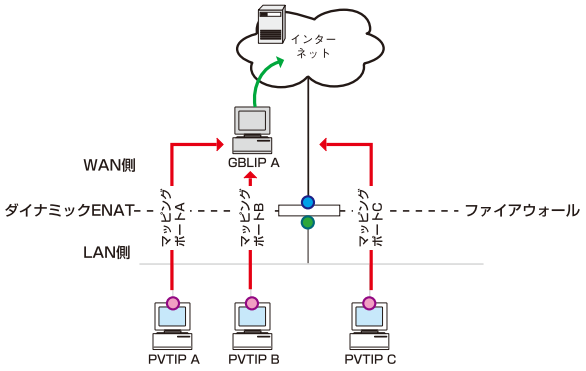
ダイナミック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で動的にマッピングします。動的にマッピングするため、グローバル IP アドレスとプライベート IP アドレスの数は同じである必要はありませんが、使用できるグローバル IP アドレスがない場合、クライアントの送出したパケットは破棄されます。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

7.2.3 ENAT

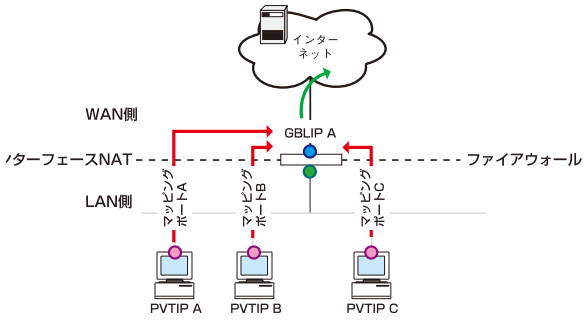
NAPT(Network Address and Port Translation)、または IP マスカレードとも呼ばれます。ENAT では、複数のプライベート IP アドレスに 1 つのグローバル IP アドレスと複数のポートをマッピングします。グローバル IP アドレスが 1 つのみの場合でも、異なるポートを使用して複数のクライアントからインターネットに接続できます。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

7.2.4 インターフェース ENAT

インターフェース ENAT は ENAT と同じ仕組みです。ただし、使用するグローバル IP アドレスは、本製品の WAN 側インターフェースに割り当てられたグローバル IP アドレスです。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

7.3 トラブルシューティング

ここでは、本製品使用中のトラブルの代表的な例と、その対応方法について説明します。

7.3.1 LED に関するトラブル

LED に関するトラブルについて説明します。

7.3.1.1 電源をオンにしても POWER LED が点灯しない

以下の事項を確認してください。

1. 本製品付属の AC アダプターを使用していますか？電源アダプターは付属のものをご使用ください。
2. AC アダプターの出力プラグは本製品にきちんと接続されていますか？接続されていないと電源が供給されません。
3. AC アダプターの AC プラグは電源コンセントにきちんと差し込まれていますか？接続されていないと電源が供給されません。

7.3.1.2 UTP ケーブルを接続しても WAN LED が点灯しない

以下の事項を確認してください。

1. UTP ケーブルはそれぞれ本製品の WAN ポート、モデムのポートにきちんと接続されていますか？接続されていないとリンクが確立しないため WAN LED が点灯しません。
2. モデムの電源はオンになっていますか？モデムの電源がオンになっていないとリンクが確立しないため WAN LED が点灯しません。
3. 本製品の電源をオンにしてモデムに接続してから 80 秒以上経過していますか？本製品の起動には 80 秒ほどかかります。
4. 本製品とモデムの接続にはストレートケーブルを使用していますか？モデムとの接続にはストレートケーブルを使用してください。

7.3.1.3 UTP ケーブルを接続しても LAN LED が点灯しない

以下の事項を確認してください。

1. UTP ケーブルはそれぞれ本製品の LAN ポート、対向のハブ、コンピューターにきちんと接続されていますか？接続されていないとリンクが確立しないため、LAN LED が点灯しません。
2. ハブやコンピューターの電源はオンになっていますか？電源がオンになっていないとリンクが確立しないため、LAN LED が点灯しません。
3. 適切な UTP ケーブルを使用していますか？ 100BASE-TX で通信する場合はカテゴリー 5 以上、10BASE-T で通信する場合はカテゴリー 3 以上のケーブルを使用してください。

7.3.2 インターネットへのアクセスに関するトラブル

インターネットへのアクセスに関するトラブルについて説明します。

7.3.2.1 インターネットにアクセスできない

以下の事項を確認してください。

1. 本製品に対して Ping コマンドを実行した場合に、正しく応答がありますか？応答がない場合、本製品との通信ができていません。

2. コンピューターに IP アドレスを手動で割り当てている場合、デフォルトゲートウェイの IP アドレスは正しく設定されていますか？設定されていない場合は、再度正しく設定を行ってください。

3. コンピューターに IP アドレスを手動で割り当てている場合、DNS サーバーの IP アドレスは正しく設定されていますか？ DNS サーバーの IP アドレスはご契約のプロバイダーから指定されている場合があります。詳細については、ご契約のプロバイダーにお問い合わせください。

4. NAT は正しく設定されていますか？プライベートネットワークからインターネットにアクセスするには、プライベート IP アドレスをグローバル IP アドレスに NAT 変換する設定が必要です。デフォルト設定では、インターフェース ENAT が設定されています。

7.3.2.2 Web ページを表示できない

以下の事項を確認してください。

1. コンピューターに IP アドレスを手動で割り当てている場合、DNS サーバーの IP アドレスは正しく設定されていますか？ DNS サーバーの IP アドレスはご契約のプロバイダーから指定されている場合があります。詳細については、ご契約のプロバイダーにお問い合わせください。

2. DNS サーバーに対して Ping コマンドを実行した場合に、正しく応答がありますか？応答がない場合、DNS サーバーとの通信ができていません。

7.3.3 GUI 設定に関するトラブル

GUI 設定に関するトラブルについて説明します。

7.3.3.1 ログインパスワードを忘れた

以下の事項を確認してください。

1. デフォルトのパスワードを変更していますか？変更していない場合はユーザー名「manager」、パスワード「friend」でログインできます。デフォルトのユーザー名とパスワードでログインできない場合は「P.47 リセットスイッチによる初期化」を実行してください。初期化が完了したら再度デフォルトのユーザー名とパスワードでログインします。


ヒント

「リセットスイッチによる初期化」機能を無効にしている場合、リセットスイッチを使用した初期化は行えません。


注意

初期化の手順を実行すると、現在の設定内容はすべて消去されますのであらかじめご注意ください。

7.3.3.2 設定画面が表示されない

以下の事項を確認してください。

1. ご使用の Web ブラウザーは Internet Explorer 6 または 7 ですか？本製品でサポートする Web ブラウザーは Internet Explorer 6 または 7 です。

2. Web ブラウザーのプロキシー設定がオンになっていませんか？本製品の設定画面にアクセスする場合は、プロキシー設定をオフにしてください。

3. Web ブラウザーの JavaScript が無効になっていませんか？本製品の設定画面を表示するには JavaScript を有効にしてください。

4. 本製品とコンピューターのサブネットマスクが異なっていませんか？本製品の設定画面にアクセスする場合は、本製品とコンピューターは同じネットワークに属する必要があります。

7.4 ログメッセージ一覧

本製品が出力するログメッセージの一覧です。表示メッセージ（エラーレベル、MSGNO、MESSAGE）と意味を、モジュール（MOD）別に示します。

- 以下の一覧には、未サポートの内容も含まれています。
- ログ出力の設定方法については「P.41 ログの記録」を参照してください。

7.4.1 プロセスモニター（PMON）

MOD：PMON

ログの種類：システム

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	701	System ready	プロセス モニターの初期化動作が完了しました。
DEBUG	702	Module found : [%s]	モジュール名をプロセス モニターに登録しました。
DEBUG	703	Undefined module : [%s]	発見されたモジュールは未定義です。
DEBUG	704	Module enabled : [%s]	モジュールが有効化されたため、監視対象に加えました。
DEBUG	705	Module disabled : [%s]	モジュールが無効化されたため、監視対象から除外しました。
DEBUG	706	Unknown Module : [%s]	未定義のモジュールに対する設定が見つかりました。
DEBUG	707	Module ID fixed [%s] with %d	モジュール ID が決定しました。
DEBUG	708	Checking restart module [%s] : Inital restart %s	モジュールの異常頻度を調べています。
DEBUG	709	Checking module status : [%s]	モジュールの状態を調べています。
DEBUG	710	Module ID not found for [%s]	モジュール ID を決定できません。
DEBUG	711	Module monitor failed for [%s]	モジュールの監視設定に失敗しました。
INFO	009	Start monitoring [%s]	モジュールの始動成功を確認しました。
WARNING	007	[%s] terminated unexpectedly. Restarting	モジュールが異常停止しました。再始動します。
WARNING	008	[%s] restarted	モジュールの再始動を行いました。
ERROR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERROR	002	Initialization failed : %s	起動できませんでした。
ERROR	003	Abandoned [%s]	モジュールを再始動できなかったため切り離します。
ERROR	004	Restart failed [%s] for %s	モジュールの再始動に失敗しました。
ERROR	005	Config DIR not found at %s	設定ディレクトリーが見つかりません。
ERROR	006	Config file not found at %s	設定ファイルが見つかりません。
ERROR	010	No config file at %s	更新しようとした設定ファイルが見つかりません。

7.4.2 フラッシュファイルシステム（FFS）

MOD：FFS

ログの種類：システム

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	701	[%s] read of %d bytes	ファイルから読み込みが行われました。
DEBUG	702	[%s] wrote of %d bytes	ファイルに対して書き込みが行われました。
DEBUG	703	[%s] looked up	ファイル属性が参照されました。
DEBUG	704	Device looked up	デバイス属性が参照されました。
DEBUG	705	Control interface ready : %d	ファイル システムを操作するインターフェースの準備が整いました。
DEBUG	706	File system ready	ファイル システムの動作準備が整いました。
DEBUG	707	Operation requested : %2d	ファイル システムへの操作要求を受け付けました。
DEBUG	708	Operation failed : %2d	ファイル操作要求が失敗しました。
DEBUG	709	Operation completed : %d	ファイル操作が完了しました。
DEBUG	710	File Operation started : %d	ファイル操作が開始されました。
DEBUG	711	Sending Progress : %s	進捗情報を送信しています。
DEBUG	712	Progress information failed with %s	進捗情報の送信に失敗しました。
DEBUG	713	File list open requested	ファイル一覧が要求されました。
DEBUG	714	File [%s] open requested in read mode	読み出しモードでファイル オープンが要求されました。
DEBUG	715	File [%s] open requested in write mode	書き込みモードでファイル オープンが要求されました。
DEBUG	716	Read requested	ファイルの読み出しが要求されました。
DEBUG	717	Write requested	ファイルの書き込みが要求されました。
DEBUG	718	Close requested	ファイル クローズが要求されました。
DEBUG	719	File [%s] delete requested	ファイル削除が要求されました。
DEBUG	720	File attributes look up requested	ファイル属性の参照が要求されました。
DEBUG	721	Device attributes look up requested	デバイスの状態参照が要求されました。
DEBUG	722	File system check requested mode : %d	ファイル システムのチェックが要求されました。
DEBUG	723	Raw copy requested : %s / %s	RAW コピーが要求されました。
DEBUG	724	File system check phase-%d	ファイル システムのチェックを段階ごとに行っています。
DEBUG	725	File write completed	ファイルへの書き込みが完了しました。
DEBUG	726	Incomplete file closed with error	破損したファイルが閉じられました。
DEBUG	727	Block %d marked as garbage	ガーベージ ブロックを生成しました。後に回収されます。
DEBUG	728	Compare file checksum 0x%X with 0x%X	ファイルのチェックサムを比較します。
DEBUG	729	Wrote : Block %d / Size %d / Offset %Ld	ファイルへの書き込みを行いました。
DEBUG	730	Read : Block %d / Size %d / Offset %Ld	ファイルからの読み出しを行いました。
DEBUG	731	EOF reached	ファイルを最後まで読み込みました。

DEBUG	732	Block %d erase	ガーベージ ブロックを消去し、回収します。
DEBUG	733	Operating %d block	データを読み書きするブロックを決定しました。
DEBUG	734	File found : [%s]	ファイル システム上にファイルを発見しました。
DEBUG	735	File system busy	ファイル システムに対して同時に複数の要求が行われました。
DEBUG	736	Garbage block #%d	未消去のガーベージ ブロックが見つかりました。
DEBUG	737	Raw erase requested : %s	RAW デバイス消去が要求されました。
INFO	011	[%s] opened in %s mode	ファイルがオープンされました。
INFO	012	[%s] closed	ファイルがクローズされました。
INFO	013	[%s] deleted	ファイルが削除されました。
INFO	014	File system check started	ファイル システムのチェックが開始されました。
INFO	015	File system check completed	ファイル システムのチェックが完了しました。
NOTICE	010	Error corrected in phase-%d on block #%d	ファイル システムのエラーを修復しました。
WARNING	006	File system full (Device full)	ファイル システムの空き容量が足りません。
WARNING	007	File system full (Entry full)	作成できるファイル数の上限を超えました。
WARNING	008	Inconsistency found in phase-%d on block #%d	ファイル システムに修復可能なエラーを発見しました。
WARNING	009	Corrupt file : [%s]	破損したファイルがあります。
ERROR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERROR	002	Initialization failed : %s	起動できませんでした。
ERROR	003	Read failed : [%s]	ファイルが破損しているため、読み込みできませんでした。
ERROR	004	Write failed : [%s]	ファイルの書き込みに失敗しました。
ERROR	005	Block erase failed : %d	ブロック消去に失敗しました。

7.4.3 ログ (LOG)

MOD : LOG

ログの種類 : システム

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	001	Logging started	ログ機能が起動しました。
DEBUG	002	Logging reconfigured	ログ機能の再設定が行われました。
INFO	003	Logging buffer cleared	ログバッファーをクリアしました。
ERROR	004	Failed to open old log device	保存用ログデバイスのオープンに失敗しました。
ERROR	005	Kernel logging buffer is full	カーネルログバッファー容量がいっぱいになりました。すべてのカーネルログが処理されるまで、カーネルログへの記録を中断します。

7.4.4 ARP (ARP)

MOD : ARP

ログの種類 : IP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	%s: ARP request for %r transmitted	ARP request パケットを送信しました。
DEBUG	701	%s: Start to retransmit ARP request for %r	ARP request パケットを再送します。
DEBUG	702	%s: Send ARP reply (IP: %r MAC: %s) to %r	ARP reply パケットを送信しました。
DEBUG	703	%s: Queued packet transmitted	キューイングされていたパケットが送信されました。
DEBUG	704	%s: ARP %s received (send IP: %r MAC: %s target IP: %r MAC: %s)	ARP パケットを受信しました。
DEBUG	705	%s: Start making ARP entry for %r	ARP エントリーの作成を開始しました。
DEBUG	706	%s: ARP %s ignored (send IP: %r MAC: %s target IP: %r MAC: %s)	ARP パケットを無視しました。
DEBUG	707	%s: 0.0.0.0 included in %s of received ARP packet	不正な IP アドレス (0.0.0.0) が受信 ARP ヘッダーに含まれていました。
INFO	015	%s: Transmit packet dropped (%s)	送信パケットが破棄されました。
INFO	018	%s: ARP entry completed (IP: %r MAC: %s)	ARP エントリーの登録が完了しました。
INFO	019	%s: ARP entry aged out (IP: %r MAC: %s)	ARP エントリーが寿命の満了により削除されました。
INFO	020	%s: Static ARP entry registered (IP: %s MAC: %s)	スタティック ARP エントリーが登録されました。
INFO	021	ARP entry %s deleted	ARP エントリーがユーザーの操作によって削除されました。
INFO	022	%s: ARP entry (IP: %r MAC: %s) updated from %s	ARP エントリーが更新されました。
INFO	023	%s: Expiry time reached but remained (IP: %r) (referred from other module)	ARP エントリーの期限が満了しましたが、他のモジュールから参照されているため削除しません。
NOTICE	016	%s: ARP request retry for %r exceeds limit	ARP request パケット再送回数が制限超過しました。
NOTICE	017	Queued Transmit packet purged (%s)	送信パケットがすべて破棄されました。
WARNING	011	%s: Failed overwrite static ARP (IP: %r MAC: %s)	スタティック ARP エントリーの上書きに失敗しました。
WARNING	012	%s: Failed overwrite ARP entry (wrong I/F) (IP: %r MAC: %s I/F: %s)	受信したインターフェースが適切ではなかったため ARP エントリーを上書きしませんでした。
WARNING	013	%s: %r Hardware address length changed to %d from %d	ハードウェアアドレスの長さが変更されました。
WARNING	014	%s: Hardware address of %r length mismatch %d I/F: %d	ハードウェアアドレスの長さがインターフェースのものと一致しません。
WARNING	004	%s: Failed to create ARP entry (%s) (IP: %r)	ARP エントリーの作成に失敗しました。
ERR	001	Memory allocation failed	メモリーの確保に失敗しました。
ERR	002	%s: Buffer length %s	パケットバッファーの長さが不正です。
ERR	003	Incorrect protocol address type %04x received	受信パケットのプロトコルアドレスタイプが不正です。
ERR	005	%s: Internal error: ARP %s corruption	ARP パケットが不正です。

ERR	007	%s: Bad sender address (broadcast) received from %r	受信 ARP パケットの送信元ハードウェアアドレスに誤ったアドレス（ブロードキャスト）が使用されています。
ERR	008	%s: Duplicated IP %r from %s	重複した IP アドレスが検出されました。
ERR	009	Delete ARP failed (data corruption)	データが壊れているため ARP エントリーの削除に失敗しました。
ERR	010	%s: Failed to create ARP entry (%s) (IP: %r MAC: %s)	ARP エントリーの作成に失敗しました。

7.4.5 Ethernet (ETH)

MOD：ETH

ログの種類：ETH

エラーレベル	MSGNO	MESSAGE	意味
INFO	005	%s: Statistics counter initialized	インターフェースの統計情報カウンターが初期化されました。
NOTICE	001	%s: Link UP	インターフェースのリンクがアップしました。
NOTICE	002	%s: Link DOWN	インターフェースのリンクがダウンしました。

7.4.6 PPPoE (PPPOE)

MOD：PPPOE

ログの種類：PPP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	002	pppoe_ioctl: %s in %s	pppoe_ioctl コマンドが発生しました。
DEBUG	003	Conflicting PPPoE state: %s in %s	PADI を送信する際、PPPoE 状態矛盾が発生しました。
DEBUG	005	Restart PPPoE interface. I/F is %s	PPPoE インターフェースの再起動が発生しました。
DEBUG	006	%s: PPPoE start is stopped because interface status is DOWN	インターフェースがダウン状態のため、PPPoE の起動を停止します。
DEBUG	007	%s: PPPoE enable commad is not executed	PPPoE enable コマンドが実行されていません。
DEBUG	008	%s: PPP bind profile command is not executed	PPP bind profile コマンドが実行されていません。
DEBUG	009	%s: Specified PPP profile %s is not found	指定された PPP profile が見つかりません。
DEBUG	010	%s: %s address is not assigned	IPv4 アドレスまたは IPv6 アドレスが割り当てられていません。
DEBUG	011	%s: Failed to set %s	PPPoE 情報の設定に失敗しました。
DEBUG	012	Configured mru (%d) is larger than PPPoE interface mtu (%d)	PPPoE インターフェース MTU を超えた MRU 値が設定されています。MRU をインターフェース MTU に変更します。
DEBUG	411	%s: Failed to access PPPoE interface	PPPoE インターフェースをオープンできませんでした。
DEBUG	413	%s: Failed to send packet. Interface is DOWN	インターフェースが DOWN 状態のため、送信できません。

DEBUG	414	%s: Failed to send packet. Error (=%d) occurred	送信エラーが発生したため、送信できません。
DEBUG	415	Failed to send PADT (session-id: %d)	PADT の送信に失敗しました。
INFO	001	Received %s: oldState: %s newState: %s in %s	受信した PPPoE パケットの種別と状態変化を表示します。
INFO	004	%s: oldState: %s newState: %s	変化した PPPoE の状態を表示します。
INFO	100	%s: Retransmission %s: retry count is %d	PPPoE 制御パケットの再送信が発生しました。
INFO	407	Received PADO, but could not find request for it	PADO パケットを受け取りましたが、該当する PPPoE インスタンスを見つけることができませんでした。パケットを破棄します。
NOTICE	200	%s: PPPoE interface is UP	PPPoE インターフェースが UP になりました。
NOTICE	201	%s: PPPoE interface is DOWN	PPPoE インターフェースが DOWN になりました。
NOTICE	202	%s: PPPoE interface is DOWN immediately	PPPoE インターフェースを強制的にダウンさせました。
WARNING	300	%s: Go back to PADI. Retry %d of PADR was exceeded	PADR の MAX 再送回数を超えたため、PPPoE セッションは、PADI 送信から開始されます。
WARNING	301	%s: PPPoE reconnection and PPP idle-timer are enabled. Reconnecting PPPoE	PPPoE 自動再接続と PPP アイドルタイマーの両方が有効ですが、PPPoE は再接続されます。
WARNING	302	%s: IPV6 interface mtu (%d) is smaller than IPV6 minimum mtu %d	IPv6 インターフェース MTU が最小 MTU サイズよりも小さい値です。
WARNING	409	Received unknown session 0x%x PPPoE, sending PADT	受信した PPPoE データパケットに該当する PPPoE セッションがありませんでした。受信した PPPoE パケットを破棄し、PADT を送信します。
ERR	400	%s: Received unknown host unique tag	一致する Host unique が存在しません。
ERR	401	PPPoE packet too short: %d	受信した PPPoE パケットの長さが短すぎます。パケットを破棄します。
ERR	402	Failed to get PPPoE header	PPPoE ヘッダーを取り出すことができませんでした。パケットを破棄します。
ERR	403	Unknown version/type packet: 0x%x	不明なバージョン／タイプの PPPoE パケットです。パケットを破棄します。
ERR	404	Invalid packet length (data available = %d, packet size = %d)	実パケット長以上の値が PPPoE パケットに設定されています。パケットを破棄します。
ERR	405	%s: PPPoE tag parse error	TAG フィールドが存在しない PPPoE パケットです。パケットを破棄します。
ERR	406	%s: Tag 0x%x length 0x%x is too long	TAG タイプに対する TAG フィールド長が一致しません。パケットを破棄します。
ERR	408	PPPoE data packet is dropped because it is too short packet: %d bytes	PPPoE データパケットが短すぎます。パケットを破棄します。
ERR	410	%s: PPPoE Session terminated. %s max retransmission exceeded	PPPoE パケットの再送回数が満了したため、PPPoE セッションの接続を中止します。
ERR	412	%s: Failed to send packet. No lower-layer interface is bound	PPPoE インターフェースが、下位層インターフェースにくくり付けられていないため、パケットを送信できません。

7.4.7 PPP (PPP)

MOD : PPP

ログの種類：PPP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	001	Create PPP interface %s	PPP インターフェースを作成します。
DEBUG	002	Destroy PPP interface %s	PPP インターフェースを削除します。
DEBUG	003	Output %s: prot=%s type=%s id=0x%x len=%d	アウトプット PPP パケット情報を表示します。
DEBUG	004	Input %s: prot=%s state=%s type=%s id=0x%x len=%d	受信した PPP パケット情報を表示します。
DEBUG	005	Event: prot=%s %s (state=%s) in %s	PPP イベント状態を表示します。
DEBUG	006	Event: prot=%s %s (state=%s) rst_counter=%d in %s	PPP イベント状態を表示します。
DEBUG	007	State: prot=%s oldState=%s newState=%s in %s	変化した PPP の状態を表示します。
DEBUG	008	%s	受信した PPP 管理パケットの内容を表示します。
DEBUG	009	%s: Send Conf-ACK for received %s Conf-REQ	受信した Conf-REQ に対して、Conf-ACK を送信します。
DEBUG	010	%s: Send IPV6CP %s (suggest IF ID: %s)	受信した Conf-REQ に対して、示唆するインターフェース識別子を含む IPV6CP が送信されます。
DEBUG	011	Input %s: prot=%s type=%s id=0x%x len=%d	受信した PPP 認証パケットの内容を表示します。
DEBUG	012	%s: %s authentication success	認証が成功しました。
DEBUG	013	%s: At least one NCP is not opened	1 つ以上の NCP が OPEN 状態となっていないため、LCP を閉じます。
DEBUG	014	%s: Changed interface mtu %lu to %lu	インターフェース mtu が変更されました。
INFO	100	%s: Loopback mode detected. Magic number (0x%lx) is the same	LCP magic number が同じであったため、ループバックモードを検出しました。LCP を閉じます。
NOTICE	200	%s: Send Conf-NAK for received %s Conf-REQ	受信した Conf-REQ に対して、Conf-NAK を送信します。
NOTICE	201	%s: Received %s, unknown 0x%x packet type	不明な認証オプションタイプを受信しました。
NOTICE	202	%s: PAP request is sent. Remaining retry counter is %d	PAP レスポンスを受信しなかったため、PAP Request を再送信します。
NOTICE	203	%s: Idle timeout (%d seconds) expired	PPP idle timeout 時間が満了しました。LCP を閉じます。
NOTICE	204	%s: Max_failure (%d) of %s Conf-REQ exceeded. Send Conf-REJ	受信した Conf-REQ の最大失敗回数を超えたため、Conf-REJ を送信します。
NOTICE	205	%s: %s is UP	LCP または、IPCP または、IPV6CP のいずれかが UP になりました。
NOTICE	206	%s: %s is DOWN	LCP または、IPCP または、IPV6CP のいずれかが DOWN になりました。
NOTICE	207	%s: CHAP Response is sent. Remaining retry counter is %d	CHAP Success または Failure を受信しなかったため、CHAP Response を再送信します。
WARNING	300	%s: Received %s, but either username or password was not set	認証パケットを受信しましたが、ユーザーまたはパスワードが設定されていません。
WARNING	301	%s: Failed to send PAP request because either user or password was not set	ユーザー名またはパスワードが設定されていないため、PAP リクエストを送信できません。
WARNING	302	%s: Failed to send CHAP CHALLENGE because username was not set	ユーザー名が設定されていないため、CHAP チャレンジを送信できません。

WARNING	303	%s: Failed to send chap response because password was not set	パスワードが設定されていないため、CHAP レスポンスを送信できません。
ERR	400	%s: PPP packet too small (%d bytes)	受信した PPP パケット長が短すぎます。パケットを破棄します。
ERR	401	%s: Upper-layer input queue exceeded (%d)	PPP 上位レイヤーの最大受信キューレングスを超えたため、パケットを破棄します。
ERR	402	%s: Failed to send data with unknown address family %d	送信データの PPP プロトコル種別が不明です。パケットを破棄します。
ERR	403	%s: Failed to create PPP output data buffer	送信データバッファーを確保できません。
ERR	404	%s: PPP %s output queue exceeded (%d)	PPP 送信キューレングスを超えたため、パケットを破棄します。
ERR	405	%s: Received %s, invalid %s length %d	受信した PPP 管理パケットのレングス長が不正です。解析を終了します。
ERR	406	%s: Received %s, illegal %s in state %s	受信した PPP 管理パケットは、PPP 状態に矛盾しています。解析を終了します。
ERR	407	%s: Received %s, received id=0x%x and id=0x%x mismatches	受信した PPP 管理パケットは、Identifier 部が一致しません。解析を終了します。
ERR	408	%s: Received LCP Echo Request in closed state	LCP Echo-Request パケットを受信しましたが、LCP は closed 状態です。解析を終了します。
ERR	409	%s: Received LCP Echo Request with invalid length (%d bytes)	LCP Echo-Request パケットを受信しましたが、パケットレングス長が不正です。解析を終了します。
ERR	410	%s: Received LCP Echo Reply with mismatched id	LCP Echo-Reply パケットを受信しましたが、Identifier 部がミスマッチです。解析を終了します。
ERR	411	%s: Received LCP Echo Reply with invalid (%d bytes)	LCP Echo-Reply パケットを受信しましたが、パケットレングス長が不正です。解析を終了します。
ERR	412	%s: Received %s with unknown code type. Send Code-REJ for 0x%x	Unknown PPP code タイプを受信したため、Code-REJECT を返信します。
ERR	413	%s: Failed to create PPP control packet data buffer for %s	PPP 管理パケットのデータバッファーを確保できません。
ERR	414	%s: Authentication failed %d times. Stop retrying	認証に失敗したため、リンク接続交渉を終了します。
ERR	415	%s: %s authentication failed. %s	認証が失敗しました。認証側からのアクション待ちとなります。
ERR	416	%s: %s authentication failed (%s, %s), send %s	認証が失敗したため、failure message を返信します。
ERR	417	%s: PAP Request failed. Retry exceeded its limit	PAP Request の再送回数が満了したため、PAP 認証を終了します。
ERR	418	%s: LCP keepalive timeout	LCP keepalive タイムアウトが発生しました。LCP を閉じます。
ERR	419	%s: prot=%s, illegal %s event in state %s	現在の状態では発生しない矛盾した PPP イベントが発生しました。
ERR	420	%s: %s closed. Max_failure (%d) of Conf-REQ exceeded	受信した Conf-REQ の最大失敗回数を超えたため、IPCP or IPV6CP を終了します。
ERR	421	%s: IPCP closed because candidate IP address for unnumbered I/F was not found	PCP を閉じます。unnumbered I/F に適切な IP アドレスを取得できませんでした。
ERR	422	%s: %s closed.Max_failure (%d) of received Conf-NAK exceeded	受信した Conf-NAK の最大失敗回数を超えたため、IPCP or IPV6CP を終了します。
ERR	423	%s: IPV6CP closed. IPV6-IFIDs (local and peer) were zero	IPV6CP を閉じます。お互いの IPV6-IFID の値が 0 です。

ERR	424	%s: IPV6CP closed. Received Conf-REJ with IPV6-IFID	IPV6CP を閉じます。受信した Conf-REJ に IPV6-IFID が存在します。
ERR	425	%s: CHAP Response failed. Retry exceeded its limit	CHAP Response の再送回数が満了したため、CHAP 認証を終了します。

7.4.8 IP (IP)

MOD : IP

ログの種類 : IP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
DEBUG	701	%s: IP packet discarded (%s) (%r -> %r)	受信したパケットの IP アドレスに問題が見つかりました。
DEBUG	702	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
DEBUG	703	%s: IP packet discarded (%s) (%s: %d/OPT: %02X) (%r -> %r)	IP ヘッダーオプション処理中にパケットが破棄されました。
DEBUG	704	%s: IP packet discarded (%s) (OPT: %02X) (%r -> %r)	ソースルーティング指定されたパケットが破棄されました。
DEBUG	705	%s: IP packet discarded (%s) (OPT: %02X) (%r -> %r)	レコードルートオプション付きのパケットが破棄されました。
DEBUG	706	%s: IP packet with timestamp option discarded (%s) (%s: %d) (%r -> %r)	タイムスタンプオプション付きのパケットが破棄されました。
DEBUG	707	%s: IP packet with timestamp option discarded (%s) (%r -> %r)	タイムスタンプオプション付きのパケットが破棄されました。
DEBUG	708	%s: IP packet with timestamp option discarded (lack of space) (FLAG: %d/PTR: %d/LEN: %d) (%r -> %r)	記録エリアが不足したため、タイムスタンプオプション付きのパケットが破棄されました。
DEBUG	709	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
DEBUG	710	IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
INFO	003	%s: Received IP header error (%s)	受信したパケットの IP ヘッダーに問題が見つかりました。
INFO	004	%s: Received IP header error (%s: %d)	受信したパケットの IP ヘッダーに問題が見つかりました。
INFO	006	%s: Bad IP checksum packet found by %s (%r -> %r)	受信したパケットの IP checksum の値が不正です。
INFO	007	%s: Received IP header error (%s HDR: %d TOTAL: %d)	受信したパケットの IP ヘッダーに問題が見つかりました。
INFO	022	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
NOTICE	001	%s: IP address not found at received I/F	受信したインターフェースで IP アドレスが見つかりませんでした。
NOTICE	009	%s: Payload length mismatch (PKT: %d BUF: %d)	パケット長とヘッダーの Payload 長が不一致です。
NOTICE	010	%s: Fragment packet size wrong (LEN: %d)	フラグメントパケットのサイズが不正です。
NOTICE	018	%s: Fragment packet discarded (%s) (%r -> %r)	フラグメント化されたパケットが破棄されました。
NOTICE	019	%s: Fragment packet discarded (%s: %d) (%r -> %r)	フラグメント化されたパケットが破棄されました。
NOTICE	021	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。

NOTICE	023	IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
NOTICE	025	%s: Fragment packet discarded (%s) (%r -> %r)	フラグメント化されたパケットが破棄されました。
NOTICE	026	%s: Packet in fragment queue discarded (%s) (%r -> %r)	フラグメントキュー中のパケットが破棄されました。
NOTICE	030	IP option header insert failed (%s: %d) (%r -> %r)	IP オプションヘッダーの挿入に失敗しました。
ERR	002	%s: Memory allocation failed for IP header (%s)	IP ヘッダーへのメモリ割り当てに失敗しました。
ERR	008	%s: Memory allocation failed for multicast IP dest (%r -> %r)	IP ヘッダーのメモリ割り当てに失敗しました。
ERR	011	%s: IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
ERR	024	%s: Packet discarded (%s: %u) (%r -> %r)	パケットは破棄されました。
ERR	027	IP packet discarded (%s) (%r -> %r)	パケットは破棄されました。
ERR	031	IP option header insert failed (%s) (%r -> %r)	IP オプションヘッダーの挿入に失敗しました。

7.4.9 ルーティング (NETM)

MOD : NETM

ログの種類 : IP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	900	Resolve error occurred (id:%u code:%d)	名前の解決においてエラーが発生しました。
DEBUG	901	Resolve result (id:%u) is (%r)	名前が解決されました。
DEBUG	902	Resolve result (id:%u) is (%s)	名前が解決されました。
DEBUG	903	Query insterted into pending queue (%s)	Query が Pending Queue に入りました。
DEBUG	904	Failed to get buffer size of tapping interface	Tapping インターフェースのバッファーサイズの取得に失敗しました。
DEBUG	905	Failed to create tapping read buffer (size:%d)	Tapping 受信バッファーを確保できません。
DEBUG	906	Failed to read tapping buffer (return code:%d errno:%d)	Tapping 受信バッファーからの読み出しに失敗しました。
DEBUG	907	Failed to send %s packet	PPPoE PADI あるいは、DHCP Discover パケットの送信に失敗しました。
DEBUG	908	Failed to open tapping socket (return code:%d)	Tapping ソケットの生成に失敗しました。
DEBUG	909	Send network information (client: %s / type: %s)	ネットワーク情報を各モジュールに配送しました。
DEBUG	910	Receive network information (client: %s / type: %s)	ネットワーク情報をモジュールから受信しました。
DEBUG	911	Failed to coonect SNMP-agent: %d	SNMP エージェントに接続できませんでした。
DEBUG	912	Coonect SNMP-agent	SNMP エージェントへ接続を開始します。
INFO	001	%s: Administrative status UP	インターフェースが使用可能に設定されました。
INFO	002	%s: Administrative status DOWN	インターフェースが使用不可能に設定されました。
INFO	003	%s: Re-initialized	ユーザーによってインターフェースがリセットされました。

INFO	005	%s: Administrative status DOWN	DHCP クライアントが設定されたインターフェースが使用不可能に設定されました。
INFO	007	Resolve reply received(id:%u)	DNS リゾルバーでリプライを受信しました。
INFO	008	Qyery transmit(id:%u Name server: %r)	DNS リゾルバーで Query を送信しました。
INFO	011	No answer replay: %s	ネームサーバーから回答が得られませんでした。
NOTICE	010	Unsupported response received (id:%u type:%d class:%d)	DNS リゾルバーでサポートしていない応答を受信しました。
WARNING	004	%s: Interface name information setup failed	インターフェース名の情報設定に失敗しました。
WARNING	006	Name server error(id:%u err:%s)	DNS リゾルバーでエラーが発生しました。
WARNING	009	Qyery transmit error(id:%u err:%d)	Query 送信時に DNS リゾルバーでエラーが発生しました。

7.4.10 ファイアウォール (FLT)

MOD : FLT

ログの種類 : ファイアウォール

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	008	BLOCKED: %s %s %r:%u -> %r:%u on %s	不許可フィルタールールと一致したため、パケットを破棄しました。
DEBUG	009	BLOCKED: %s %s %R[%u] -> %R[%u] on %s	不許可フィルタールールと一致したため、パケットを破棄しました。
DEBUG	010	BLOCKED: %s %s %r:%u -> %r:%u on %s (no match rule)	一致するフィルタールールが存在しないため、パケットを破棄しました。
DEBUG	011	BLOCKED: %s %s %R[%u] -> %R[%u] on %s (no match rule)	一致するフィルタールールが存在しないため、パケットを破棄しました。
DEBUG	701	Found FTP command: %s	FTP ALG の対象コマンドを発見しました。
DEBUG	702	Found TFTP opcode: %d	TFTP ALG の対象オペレーションコードを発見しました。
DEBUG	703	Created cache: proto=%s in=%r:%u %s out=%r:%u on %s	キャッシュが作成されました。
DEBUG	704	Created cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	キャッシュが作成されました。
DEBUG	705	Deleted cache: proto=%s in=%r:%u %s out=%r:%u on %s	キャッシュが削除されました。
DEBUG	706	Deleted cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	キャッシュが削除されました。
DEBUG	707	Created pending cache: proto=%s in=%r:%u %s out=%r:%u on %s	保留キャッシュが作成されました。
DEBUG	708	Created pending cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	保留キャッシュが作成されました。
DEBUG	709	Deleted pending cache: proto=%s in=%r:%u %s out=%r:%u on %s	保留キャッシュが削除されました。
DEBUG	710	Deleted pending cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	保留キャッシュが削除されました。
DEBUG	711	Changed to normal cache: proto=%s in=%r:%u %s out=%r:%u on %s	保留キャッシュが正式なキャッシュに変更されました。
DEBUG	712	Changed to normal cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	保留キャッシュが正式なキャッシュに変更されました。
DEBUG	713	Failed to insert in dynamic cache list (in): %s %s %r:%u -> %r:%u on %s	ダイナミックキャッシュをインサイドリストに追加できませんでした。
DEBUG	714	Failed to insert in dynamic cache list (in): %s %s %R[%u] -> %R[%u] on %s	ダイナミックキャッシュをインサイドリストに追加できませんでした。

DEBUG	715	Failed to insert in dynamic cache list (out): %s %s %r:%u -> %r:%u on %s	ダイナミックキャッシュをアウトサイドリストに追加できませんでした。
DEBUG	716	Failed to insert in dynamic cache list (out): %s %s %R[%u] -> %R[%u] on %s	ダイナミックキャッシュをアウトサイドリストに追加できませんでした。
DEBUG	717	Failed to insert in dynamic cache list: %s %s %r:%u -> %r:%u on %s	ダイナミックキャッシュをリストに追加できませんでした。
DEBUG	718	Failed to insert in dynamic cache list: %s %s %R[%u] -> %R[%u] on %s	ダイナミックキャッシュをリストに追加できませんでした。
DEBUG	719	Failed to insert in static cache list (in): %s %s %r:%u -> %r:%u on %s	スタティックキャッシュをインサイドリストに追加できませんでした。
DEBUG	720	Failed to insert in static cache list (in): %s %s %R[%u] -> %R[%u] on %s	スタティックキャッシュをインサイドリストに追加できませんでした。
DEBUG	721	Failed to insert in static cache list (out): %s %s %r:%u -> %r:%u on %s	スタティックキャッシュをアウトサイドリストに追加できませんでした。
DEBUG	722	Failed to insert in static cache list (out): %s %s %R[%u] -> %R[%u] on %s	スタティックキャッシュをアウトサイドリストに追加できませんでした。
DEBUG	723	Failed to insert in static cache list: %s %s %r:%u -> %r:%u on %s	スタティックキャッシュをリストに追加できませんでした。
DEBUG	724	Failed to insert in static cache list: %s %s %R[%u] -> %R[%u] on %s	スタティックキャッシュをリストに追加できませんでした。
DEBUG	725	Loosened connection: proto=%s in=%r:%u %s out=%r:%u (flag=%#x seq=%u ack=%u len=%u ackskew=%d) on %s	終了したキャッシュと一致しました。
DEBUG	726	Loosened connection: proto=%s in=%R[%u] %s out=%R[%u] (flag=%#x seq=%u ack=%u len=%u ackskew=%d) on %s	終了したキャッシュと一致しました。
DEBUG	727	Source idled out of PAWS: proto=%s in=%r:%u %s out=%r:%u on %s	送信元の PAWS がタイムアウトしました。
DEBUG	728	Source idled out of PAWS: proto=%s in=%R[%u] %s out=%R[%u] on %s	送信元の PAWS がタイムアウトしました。
DEBUG	729	Destination idled out of PAWS: proto=%s in=%r:%u %s out=%r:%u on %s	宛先の PAWS がタイムアウトしました。
DEBUG	730	Destination idled out of PAWS: proto=%s in=%R[%u] %s out=%R[%u] on %s	宛先の PAWS がタイムアウトしました。
DEBUG	731	Failed to normalize on first packet (%u)	最初のパケットで正常化に失敗しました。
DEBUG	732	PASSED: Failed to create static cache: proto=%s in=%r:%u %s out=%r:%u on %s	スタティックキャッシュの登録に失敗しましたが、パケットは転送しました。
DEBUG	733	PASSED: Failed to create static cache: proto=%s in=%R[%u] %s out=%R[%u] on %s	スタティックキャッシュの登録に失敗しましたが、パケットは転送しました。
DEBUG	734	Filter module was enabled	フィルターモジュールが有効になりました。
DEBUG	735	Filter module was disabled	フィルターモジュールが無効になりました。
DEBUG	736	Failed to insert in pending cache list: %s %s %r:%u -> %r:%u on %s	保留キャッシュをリストに追加できませんでした。
DEBUG	737	Failed to insert in pending cache list: %s %s %R[%u] -> %R[%u] on %s	保留キャッシュをリストに追加できませんでした。
INFO	046	PASSED: %s %s %r:%u -> %r:%u on %s	許可フィルタールールと一致しました。
INFO	047	PASSED: %s %s %R[%u] -> %R[%u] on %s	許可フィルタールールと一致しました。
NOTICE	007	Failed to add tag	タグの追加に失敗しました。
NOTICE	012	BLOCKED: Invalid interface: %s	受信したインターフェースがフィルター対象のインターフェースではないため、パケットを破棄しました。
NOTICE	013	BLOCKED: Checksum error: %s %s %r:%u -> %r:%u on %s	チェックサムが正しくないため、パケットを破棄しました。

NOTICE	014	BLOCKED: UDP destination port was zero: %s %s %r:%u -> %r:%u on %s	受信した UDP パケットの宛先ポート番号が 0 であるため、パケットを破棄しました。
NOTICE	015	BLOCKED: UDP packet length too big: %s %s %r:%u -> %r:%u on %s	UDP ヘッダーのパケット長が実際のパケット長を超えていたため、パケットを破棄しました。
NOTICE	016	BLOCKED: UDP packet length too small: %s %s %r:%u -> %r:%u on %s	UDP パケット長が 8 バイト未満であるため、パケットを破棄しました。
NOTICE	017	BLOCKED: Found IP option	IP option を持っているパケットであるため、パケットを破棄しました。
NOTICE	018	BLOCKED: Header length too small	ヘッダー長が必要最低限に達していないため、パケットを破棄しました。
NOTICE	019	BLOCKED: Header length information too small	ヘッダー長情報が必要最低限に達していないため、パケットを破棄しました。
NOTICE	020	BLOCKED: IP header length information was bigger than IP packet length: %s %s %r -> %r on %s	IP ヘッダーのヘッダー長情報が、IP ヘッダーのパケット長を超えているため、パケットを破棄しました。
NOTICE	021	BLOCKED: Illegal fragment packet with DF-bit set: %s %s %r -> %r on %s	フラグメント禁止ビットが設定されているフラグメントパケットを検出したため、パケットを破棄しました。
NOTICE	022	BLOCKED: Fragment packet was not multiple of 8 bytes: %s %s %r -> %r on %s	8 バイト単位で構成されていないフラグメントパケットを検出したため、パケットを破棄しました。
NOTICE	023	BLOCKED: Total of the fragment packet length was too big: %s %s %r -> %r on %s	フラグメントオフセットとパケット長の合計が 65535 バイトを超えたため、パケットを破棄しました。
NOTICE	024	BLOCKED: Fragment packet was already completed: %s %s %r -> %r on %s	すでに完了したフラグメントパケットを受信したため、パケットを破棄しました。
NOTICE	025	BLOCKED: Failed to reassemble fragment packet: %s %s %r -> %r on %s	フラグメントパケットの再構成に失敗したため、パケットを破棄しました。
NOTICE	026	BLOCKED: Fragment deny rule: %s %s %r -> %r on %s	フラグメントパケット不許可ルールに一致したため、パケットを破棄しました。
NOTICE	027	BLOCKED: Failed to get header of %s: %s %r -> %r on %s	パケットのヘッダーを取得できなかったため、パケットを破棄しました。
NOTICE	028	BLOCKED: IPv6 header length too big: %s %R -> %R on %s	IPv6 パケット長が 65535 バイトを超えたため、パケットを破棄しました。
NOTICE	029	BLOCKED: IPv6 payload length was not zero: %s %R -> %R on %s	ジャンボペイロードオプションが有効であるにも関わらず、IPv6 ヘッダーのペイロード長が 0 ではないため、パケットを破棄しました。
NOTICE	030	BLOCKED: Jumbo payload length too small: %s %R -> %R on %s	ジャンボペイロード長が 65535 バイト以下であるため、パケットを破棄しました。
NOTICE	031	BLOCKED: IPv6 packet length was incorrect: %s %R -> %R on %s	パケット長が実際のパケット長と異なっているため、パケットを破棄しました。
NOTICE	032	BLOCKED: IPv6 fragment packet length was zero: %s %R -> %R on %s	フラグメントパケットでありながら、パケット長もジャンボペイロード長も 0 であるため、パケットを破棄しました。
NOTICE	033	BLOCKED: SYN and RST flag were set: %s %s %r:%u -> %r:%u on %s	SYN フラグと RST フラグが共に有効な TCP パケットであるため、パケットを破棄しました。
NOTICE	034	BLOCKED: SYN and ACK and RST flag was not set: %s %s %r:%u -> %r:%u on %s	SYN、ACK、RST フラグが共に無効なパケットであるため、パケットを破棄しました。

NOTICE	035	BLOCKED: ACK flag was not set, and FIN, PUSH or URG flag was set: %s %s %r:%u -> %r:%u on %s	ACK フラグが無効であるにもかかわらず、FIN、PUSH、URG のいずれかのフラグが有効なパケットであるため、パケットを破棄しました。
NOTICE	036	BLOCKED: Data offset value was less than 20 bytes: %s %s %r:%u -> %r:%u on %s	データオフセットの値が 20 バイト未満であるため、パケットを破棄しました。
NOTICE	037	BLOCKED: TCP TIMESTAMP option was overlapping: %s %s %r:%u -> %r:%u on %s	TIMESTAMP オプションが重複して設定されているため、パケットを破棄しました。
NOTICE	038	BLOCKED: Illegal TCP TIMESTAMP option: %s %s %r:%u -> %r:%u on %s	不正な TIMESTAMP オプションを検出したため、パケットを破棄しました。
NOTICE	039	BLOCKED: Illegal TCP TIMESTAMP option (no RFC 1323): %s %s %r:%u -> %r:%u on %s	RFC 1323 に準拠しない TIMESTAMP オプションを検出したため、パケットを破棄しました。
NOTICE	040	BLOCKED: Sequence number error: proto=%s in=%r:%u %s out=%r:%u (flag=%#x seq=%u ack=%u len=%u ackskew=%d reason=%#x) on %s	不正なシーケンス番号を検出したため、パケットを破棄しました。
NOTICE	041	BLOCKED: Sequence number error: proto=%s in=%R[%u] %s out=%R[%u] (flag=%#x seq=%u ack=%u len=%u ackskew=%d reason=%#x) on %s	不正なシーケンス番号を検出したため、パケットを破棄しました。
NOTICE	042	BLOCKED: Received invalid ICMP: %r -> %r type=%d code=%d (proto=%s in=%r:%u %s dst=%r:%u seq=%u)	受信した ICMP のデータが正しくないため、パケットを破棄しました。
NOTICE	043	BLOCKED: Received invalid ICMPv6: %R -> %R type=%d code=%d (proto=%s in=%R[%u] %s out=%R[%u] seq=%u)	受信した ICMPv6 のデータが正しくないため、パケットを破棄しました。
NOTICE	044	BLOCKED: ICMP error message was too short (%s): %s %s %r:%u -> %r:%u on %s	ICMP エラーメッセージが短すぎるため、パケットを破棄しました。
NOTICE	045	BLOCKED: IPv6 option was too short in ICMPv6 packet: %s %s %R[%u] -> %R[%u] on %s	ICMPv6 パケットにおいて、IPv6 のオプション長が短すぎるため、パケットを破棄しました。
NOTICE	048	BLOCKED: IPv6 header length information was bigger than IP packet length: %s %R -> %R on %s	IPv6 ヘッダーのヘッダー長情報が、IPv6 ヘッダーのパケット長を超えているため、パケットを破棄しました。
NOTICE	049	BLOCKED: Fragment bit of ICMP error message packet was set: %s %s %r:%u -> %r:%u on %s	ICMP エラーメッセージであるにもかかわらず、フラグメントビットが有効だったため、パケットを破棄しました。
NOTICE	050	BLOCKED: Fragment bit of ICMPv6 error message packet was set: %s %s %R[%u] -> %R[%u] on %s	ICMPv6 エラーメッセージであるにもかかわらず、フラグメントビットが有効だったため、パケットを破棄しました。
NOTICE	051	BLOCKED: Fragment offset length was less than IP packet length: %s %s %r -> %r	フラグメントオフセットの値が IP パケット長よりも小さいため、パケットを破棄しました。
NOTICE	052	Matched logging rule: %s: %s %s %r:%u -> %r:%u on %s	ログ出力ルールと一致しました。
NOTICE	053	Matched logging rule: %s: %s %s %R[%u] -> %R[%u] on %s	ログ出力ルールと一致しました。
NOTICE	054	Failed to parse FTP command: %s: %s %s %r:%u -> %r:%u	FTP コマンドの解析に失敗したため、パケットを破棄しました。

NOTICE	055	BLOCKED: Failed to create dynamic cache: %s %s %r:%u -> %r:%u on %s	ダイナミックキャッシュの登録に失敗したため、パケットを破棄しました。
NOTICE	056	BLOCKED: Failed to create dynamic cache: %s %s %R[%u] -> %R[%u] on %s	ダイナミックキャッシュの登録に失敗したため、パケットを破棄しました。
NOTICE	057	BLOCKED: IPv6 fragment packet jumbo payload length was not zero: %s %R -> %R on %s	フラグメントパケットでありながら、ジャンボペイロード長が設定されているため、パケットを破棄しました。
NOTICE	058	BLOCKED: ICMPv6 error message was too short (%s): %s %s %R[%u] -> %R[%u] on %s	ICMP エラーメッセージが短すぎるため、パケットを破棄しました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERR	002	Failed to attach interface %s	インターフェースの設定に失敗しました。
ERR	003	Failed to detach interface %s	インターフェースの開放に失敗しました。
ERR	004	Failed to create cache (reached limit)	最大キャッシュ数に達しているため、キャッシュを作成できませんでした。
ERR	005	Failed to cache fragment packet	フラグメントパケットのキャッシュに失敗しました。
ERR	006	Failed to get tag	タグの取得に失敗しました。

7.4.11 NAT (NAT)

MOD : NAT

ログの種類 : NAT

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	701	Found FTP command: %s	FTP ALG の対象コマンドを発見しました。
DEBUG	702	Found TFTP opcode: %d	TFTP ALG の対象オペレーションコードを発見しました。
DEBUG	703	Created cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	キャッシュが作成されました。
DEBUG	704	Deleted cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	キャッシュが削除されました。
DEBUG	705	Created pending cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	保留キャッシュが作成されました。
DEBUG	706	Deleted pending cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	保留キャッシュが削除されました。
DEBUG	707	Changed to normal cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	保留キャッシュが正式なキャッシュに変更されました。
DEBUG	708	Failed to insert in dynamic cache list (in): proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	ダイナミックキャッシュをインサイドリストに追加できませんでした。
DEBUG	709	Failed to insert in dynamic cache list (out): proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	ダイナミックキャッシュをアウトサイドリストに追加できませんでした。
DEBUG	710	Failed to insert in dynamic cache list: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	ダイナミックキャッシュをリストに追加できませんでした。
DEBUG	711	Loosened connection: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u (flag=%u seq=%u ack=%u len=%u ackskew=%d) on %s	終了したキャッシュと一致しました。
DEBUG	712	Source idled out of PAWS: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	送信元の PAWS がタイムアウトしました。

DEBUG	713	Destination idled out of PAWS: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	宛先の PAWS がタイムアウトしました。
DEBUG	714	Failed to normalize on first packet (%u)	最初のパケットで正常化に失敗しました。
DEBUG	715	Matched NAT rule: %s %s %r:%u -> %r:%u on %s	NAT ルールと一致しました。
DEBUG	716	NAT module was enabled	NAT モジュールが有効になりました。
DEBUG	717	NAT module was disabled	NAT モジュールが無効になりました。
DEBUG	718	Failed to insert in pending cache: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u on %s	保留キャッシュをリストに追加できませんでした。
NOTICE	005	Failed to add tag	タグの追加に失敗しました。
NOTICE	007	Checksum error: %s %s %r:%u -> %r:%u on %s	チェックサムが正しくないため、パケットを破棄しました。
NOTICE	008	UDP destination port was zero: %s %s %r:%u -> %r:%u on %s	受信した UDP パケットの宛先ポート番号が 0 であるため、パケットを破棄しました。
NOTICE	009	Incorrect UDP packet length: %s %s %r:%u -> %r:%u on %s	UDP ヘッダーのパケット長が実際のパケット長を超えていたため、パケットを破棄しました。
NOTICE	010	UDP packet length was too small: %s %s %r:%u -> %r:%u on %s	UDP パケット長が 8 バイト未満であるため、パケットを破棄しました。
NOTICE	011	Found IP option	IP option を持っているパケットであるため、パケットを破棄しました。
NOTICE	012	Header length was too small	ヘッダー長が必要最低限に達していないため、パケットを破棄しました。
NOTICE	013	Header length information was too small	ヘッダー長情報が必要最低限に達していないため、パケットを破棄しました。
NOTICE	014	IP header length information was bigger than IP packet length: %s %s %r -> %r on %s	IP ヘッダーのヘッダー長情報が、IP ヘッダーのパケット長を超えているため、パケットを破棄しました。
NOTICE	015	Illegal fragment packet with DF-bit set: %s %s %r -> %r on %s	フラグメント禁止ビットが設定されているフラグメントパケットを検出したため、パケットを破棄しました。
NOTICE	016	Fragment packet was not multiple of 8 bytes: %s %s %r -> %r on %s	8 バイト単位で構成されていないフラグメントパケットを検出したため、パケットを破棄しました。
NOTICE	017	Total of the fragment packet length was too big: %s %s %r -> %r on %s	フラグメントオフセットとパケット長の合計が 65535 バイトを超えたため、パケットを破棄しました。
NOTICE	018	Fragment packet was already completed: %s %s %r -> %r on %s	すでに完了したフラグメントパケットを受信したため、パケットを破棄しました。
NOTICE	019	Failed to reassemble fragment packet: %s %s %r -> %r on %s	フラグメントパケットの再構成に失敗したため、パケットを破棄しました。
NOTICE	020	Failed to get header of %s: %s %r -> %r on %s	パケットのヘッダーを取得できなかったため、パケットを破棄しました。
NOTICE	021	SYN and RST flag were set: %s %s %r:%u -> %r:%u on %s	SYN フラグと RST フラグが共に有効な TCP パケットであるため、パケットを破棄しました。
NOTICE	022	ACK or RST flag was not set: %s %s %r:%u -> %r:%u on %s	ACK フラグと RST フラグが共に無効なパケットであるため、パケットを破棄しました。
NOTICE	023	ACK flag was not set, and FIN, PUSH or URG flag was set: %s %s %r:%u -> %r:%u on %s	ACK フラグが無効であるにもかかわらず、FIN、PUSH、URG のいずれかのフラグが有効なパケットであるため、パケットを破棄しました。

NOTICE	024	Data offset value was less than 20 bytes: %s %s %r:%u -> %r:%u on %s	データオフセットの値が 20 バイト未満であるため、パケットを破棄しました。
NOTICE	025	TCP TIMESTAMP option was overlapping: %s %s %r:%u -> %r:%u on %s	TIMESTAMP オプションが重複して設定されているため、パケットを破棄しました。
NOTICE	026	Illegal TCP TIMESTAMP option: %s %s %r:%u -> %r:%u on %s	不正な TIMESTAMP オプションを検出したため、パケットを破棄しました。
NOTICE	027	Illegal TCP TIMESTAMP option (no RFC 1323): %s %s %r:%u -> %r:%u on %s	RFC 1323 に準拠しない TIMESTAMP オプションを検出したため、パケットを破棄しました。
NOTICE	028	Sequence number error: proto=%s in=%r:%u %s map=%r:%u %s out=%r:%u (flag=%u seq=%u ack=%u len=%u ackskew=%d reason=%u) on %s	不正なシーケンス番号を検出したため、パケットを破棄しました。
NOTICE	029	Received invalid ICMP: %r -> %r type=%d code=%d (proto=%s in=%r:%u %s map=%r:%u %s dst=%r:%u seq=%u)	受信した ICMP のデータが正しくないため、パケットを破棄しました。
NOTICE	030	ICMP error message was too short (%s): %s %s %r:%u -> %r:%u on %s	ICMP エラーメッセージが短すぎるため、パケットを破棄しました。
NOTICE	031	ICMP error message packet with fragment bit set: %s %s %r:%u -> %r:%u on %s	ICMP エラーメッセージであるにもかかわらず、フラグメントビットが有効であったため、パケットを破棄しました。
NOTICE	032	Fragment offset length was less than IP packet length: %s %s %r -> %r	フラグメントオフセットの値が IP パケット長よりも小さいため、パケットを破棄しました。
NOTICE	033	Failed to parse FTP command: %s: %s %s %r:%u -> %r:%u	FTP コマンドの解析に失敗したため、パケットを破棄しました。
NOTICE	034	Failed to create dynamic cache: %s %s %r:%u -> %r:%u on %s	ダイナミックキャッシュの登録に失敗したため、パケットを破棄しました。
NOTICE	035	Failed to create path-through cache: %s %s %r -> %r on %s	すでにパススルーキャッシュが存在しているため、パケットを破棄しました。
NOTICE	036	Failed to allocate mapping port: %s %s %r:%u -> %r:%u on %s	マッピングポートの割り当てに失敗しました。
NOTICE	037	Packet length exceeded 65535 bytes by the ALG process	ALG 処理によりパケット長が 65535 バイトを超えたため、パケットを破棄しました。
NOTICE	038	Failed to allocate mapping IP address: %s %s %r:%u -> %r:%u on %s	マッピング IP アドレスの割り当てに失敗しました。
NOTICE	039	Matched logging rule: %s: %s %r:%u -> %r:%u on %s	ログ出力ルールと一致しました。
NOTICE	040	BLOCKED (match NAT address): %s %s %r:%u -> %r:%u on %s	送信元 IP アドレスか宛先 IP アドレスが NAT 変換後のアドレスと一致するため、パケットを破棄しました。
NOTICE	041	BLOCKED (no match pass-through address): %s %s %r:%u -> %r:%u on %s	許可されているパススルーアドレスではないため、パケットを破棄しました。
WARNING	042	Failed to set NAT because static ARP already exists: %r	スタティック ARP の設定がすでに存在しているため、NAT の設定に失敗しました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERR	002	Failed to create cache (reached limit)	最大キャッシュ数に達しているため、キャッシュを作成できませんでした。
ERR	003	Failed to cache fragment packet	フラグメントパケットのキャッシュに失敗しました。
ERR	004	Failed to get tag	タグの取得に失敗しました。
ERR	006	Internal Error: Invalid interface %s	内部エラーです。受信したインターフェースがフィルター対象のインターフェースではないため、パケットを破棄しました。

7.4.12 ISAKMP (ISKMP)

MOD : ISKMP

ログの種類 : VPN

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	Access-list modified	アクセスリストが変更されたため IPsec フィルターへの影響を調査します。
DEBUG	701	Updating SPD (type %d, %s)	IPsec フィルターパラメーターを更新します。
DEBUG	702	SP parameters missing	IPsec フィルターを構築するのに必要なパラメーターが不足しています。
DEBUG	703	Processing ISAKMP message: %d	ISAKMP メッセージパケットの処理を開始します。
DEBUG	704	Received network layer information	ネットワークレイヤーのモジュールからイベントが通知されたため、処理を実行します。
DEBUG	705	IPsec module event: %d	IPsec モジュールからイベントが通知されたため、処理を実行します。
DEBUG	706	%s SA installed: SPI %08x	IPsec モジュールに SA を設定します。
DEBUG	707	Allocate inbound SPI	IPsec モジュールに対して SPI の割り当てを要求します。
DEBUG	708	Ignore acquire: %s	IPsec モジュールからの SA 要求を無視しました。
DEBUG	709	State machine %d / %d / %d	内部情報（状態遷移）を表示します。
DEBUG	710	%s mode, id info %s	ISAKMP パケットのモードと識別情報を表示します。
DEBUG	711	SA lifetime modified %ld %s	RESPONDER LIFETIME 通知を受けて SA の寿命を変更しました。
DEBUG	712	IPsec SA already deleted	ISAKMP モジュールより IPsec SA の消去を試みましたが、SA はすでに削除されていました。
DEBUG	200	Send ISAKMP packet: %d bytes	ISAKMP パケットを送信します。
DEBUG	201	Received ISAKMP packet: %d bytes	ISAKMP パケットを受信したため、解析を行います。
DEBUG	210	Setting ISAKMP payload %s	ISAKMP パケットに Payload をセットしました。
DEBUG	211	Found ISAKMP payload %s	ISAKMP パケット内に Payload を発見しました。
DEBUG	216	ID value Type: %s / Value: %s	ID の値を表示します。
DEBUG	217	Proposal attribute %s: %s	SA ペイロードに含まれるプロポーサルの値を表示します。
DEBUG	218	Sent NOTIFY payload: %s	送信した NOTIFY ペイロードのタイプ名を表示します。
DEBUG	219	Received NOTIFY payload: %s	受信した NOTIFY ペイロードのタイプ名を表示します。
DEBUG	225	Propose SPI: %08x	ISAKMP ネゴシエーション中に本装置が提案した SPI を表示します。
DEBUG	229	Searching %s policy for %s(%s)	Responder 動作時に、対向機器から受信したパケットに対応する設定ポリシーを検索します。
DEBUG	231	Received Vendor ID payload: %s	Vendor ID ペイロードを受信しました。
DEBUG	232	Sent Vendor ID payload: %s	Vendor ID ペイロードを送信しました。

DEBUG	714	Reset DPD timeout counter %s/%d	DPD タイムアウトカウンターがリセットされました。
DEBUG	715	Received DPD %s sequence number %d from %s. Expected %d	DPD パケットに記述されているシーケンス番号を表示します。
DEBUG	716	Last IPsec traffic from %s %d sec	DPD 対向機器より IPsec パケットが到達した後の経過時間を表示します。
DEBUG	717	Received heartbeat sequence number %d from %s. Expected %d	Heartbeat パケットに記述されているシーケンス番号を表示します。
DEBUG	718	Resolve cancel for %s(%s)	名前解決を中止しました。
DEBUG	719	DNS response received (id: %u)	ホスト名の問い合わせに対する応答を受信しました。
DEBUG	720	NAT-T established: %s	NAT-Traversal の使用が合意されました。
DEBUG	721	%s NAT was detected	NAT の存在が検出されました。
DEBUG	722	Negotiation request by always-up-sa ignored (%s)	always-up-sa によるネゴシエーション要求を無視しました。
DEBUG	723	Received UDP keepalive from %s	UDP キープアライブパケットを受信しました。
DEBUG	724	Sent UDP keepalive to %s	UDP キープアライブパケットを送信しました。
DEBUG	725	Tunnel update %s: %s	トンネルインターフェースに関する情報を更新します。
DEBUG	726	Remove SA %s/%s	SA 情報がリストから削除されました。
DEBUG	727	Packet discard in IPsec %s	IPsec モジュールでパケットの破棄が発生しました。
DEBUG	728	List length %s: %d	内部情報として保持しているデータリストの要素数を表示します。
INFO	220	IPsec SA for policy %s acquired	IPsec モジュールより IPsec SA のネゴシエーションが要求されました。
INFO	221	IPsec Re-KEY for policy %s for %s	IPsec SA が寿命に達したため、Re-KEY 動作を行います。
INFO	223	%s mode negotiation packet %s	ネゴシエーションパケットを正常に処理しました。
INFO	214	Received DELETE payload DOI %s / SPI %s	DELETE ペイロードを受信しました。
INFO	015	Invalid access-list: %s	IPsec に使用できる Access-list の条件を満たしていません。
INFO	036	Unexpected DPD packet received from %s	対向機器より使用が合意されていない DPD パケットが到達しました。
INFO	212	Sent ISAKMP information to %s	ISAKMP Information パケットを送信しました。
INFO	213	Received ISAKMP information from %s	ISAKMP Information パケットを受信しました。
INFO	713	IPsec SA expired in ISAKMP module: %08x	ISAKMP モジュールで管理している IPsec SA が寿命に達しました。
INFO	235	Received ISAKMP heartbeat from %s	ISAKMP heartbeat パケットを受信しました。
INFO	236	Sent ISAKMP heartbeat to %s	ISAKMP heartbeat パケットを送信しました。
INFO	243	IPsec SA for policy %s acquired (always-up-sa)	always-up-sa option が有効であるため IPsec SA のネゴシエーションが要求されました。
INFO	244	Unknown Cookie for %s mode from %s	未知の Cookie を持ったパケットを受信したため破棄しました。
INFO	246	FQDN peer %s policy %s address updated to %r (FQDN: %s)	IPv4 FQDN 設定されているピアのアドレスを解決し、設定しました。
INFO	247	FQDN peer %s policy %s address updated to %R(FQDN: %s)	IPv6 FQDN 設定されているピアのアドレスを解決し、設定しました。

INFO	248	FQDN address expire on %s policy %s	FQDN 設定されたポリシーの解決済みアドレスが無効化されました。
NOTICE	226	Delete IPsec SA %08x by DELETE information	DELETE インフォーメーションを受けたため、IPsec SA を削除します。
INFO	202	Received re-transmission ISAKMP packet from %s	対向機から再送パケットを受信しました。
INFO	203	Re-transmission ISAKMP packet to %s	対向機からの応答がないため再送を行いました。
NOTICE	204	Start Phase-I (%s) negotiation as %s with %s	Phase-I ネゴシエーションを開始します。
NOTICE	205	Start Phase-II negotiation as %s with %s	Phase-II ネゴシエーションを開始します。
NOTICE	206	Phase-I negotiation succeeded with %s	Phase-I ネゴシエーションが完了しました。
NOTICE	207	Phase-II negotiation succeeded with %s	Phase-II ネゴシエーションが完了しました。
NOTICE	208	ISAKMP SA created: %s	ISAKMP SA が生成されました。
NOTICE	209	ISAKMP SA expired: %s	ISAKMP SA が寿命により削除されました。
NOTICE	215	Received INITIAL CONTACT from %s	INITIAL CONTACT を受信しました。
NOTICE	224	ISAKMP SA delete: %s	ISAKMP SA を削除しました。
NOTICE	227	Delete %s SA for %s	設定変更もしくはインターフェース状態の変化に伴い 、SA の削除を実行しました。
NOTICE	228	Negotiation canceled for never initiate policy	イニシエーターとして動作できない設定であるため、ネゴシエーションを中止しました。
NOTICE	230	Received RESPONDER LIFETIME from %s	RESPONDER LIFETIME を受信しました。
NOTICE	233	DPD keepalive timed out with %s	DPD によるキープアライブでタイムアウトが発生しました。
NOTICE	234	Delete ISAKMP SA %s by DELETE information	DELETE インフォーメーションを受けたため、ISAKMP SA を削除します。
NOTICE	035	Received malformed DPD packet from %s: %s	DPD プロトコルとして異常なパケットを受信したため破棄しました。
NOTICE	038	Received malformed heartbeat packet from %s: %s	Heartbeat プロトコルとして異常なパケットを受信したため破棄しました。
NOTICE	237	Keepalive sequence number mismatch %d from %s. Expected %d	Keepalive シーケンス番号が予期した値と異なるため、パケットを破棄しました。
NOTICE	238	Negotiation canceled (Peer hostname is not resolved)	対向機のホスト名が解決されていないため、ネゴシエーションを中止しました。
INFO	239	Start to resolve peer host for %s (ID:%u)	対向機のホスト名問い合わせを開始しました。
NOTICE	245	%s interface status change: %s	トンネルインターフェースの状態が変化しました。
WARNING	222	Negotiation started since %s force SA enabled for %s	Force SA が設定されているため、ネゴシエーションを開始しました。
WARNING	039	Unexpected heartbeat packet received from %s	受信設定がされていないにもかかわらず heartbeat パケットが到達しました。
ERR	240	Failed to resolve for %s (Code: %s ID: %d)	対向機のホスト名問い合わせ中にエラーが発生しました。
ERR	241	Unknown resolving request(ID: %d)	DNS の応答に対応する問い合わせが見つかりませんでした。
WARNING	242	Resolve timeout for FQDN: %s (ID: %d)	名前解決がタイムアウトしました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERR	002	No ISAKMP proposal: %s	設定された ISAKMP プロポーザルが見つかりません。
ERR	003	No IPsec proposal: %s	設定された IPsec プロポーザルが見つかりません。

ERR	004	No consistent DH group in aggressive mode	Aggressive モードで使用するプロポーザルの DH group はすべて同じでなければいけません。
ERR	005	Parameter missing in ISAKMP policy %s (%s)	ISAKMP ポリシーに必要なパラメーターが設定されていません。
ERR	006	Parameter missing in ISAKMP proposal %s (%s)	ISAKMP プロポーザルに必要なパラメーターが設定されていません。
ERR	007	Parameter missing in IPsec policy %s (%s)	IPsec ポリシーに必要なパラメーターが設定されていません。
ERR	008	Parameter missing in IPsec proposal %s (%s)	IPsec プロポーザルに必要なパラメーターが設定されていません。
ERR	009	Internal data error: %s	ソフトウェア内部のデータに矛盾が発生しました。
ERR	011	Failed to start up: %s	起動に失敗しました。
ERR	012	Negotiation abandoned: %s	ISAKMP ネゴシエーションを継続できない状態にあるため、中止します。
ERR	013	Unknown Cookie for quick mode from %s	未知の Cookie を持った Quick モードパケットを受信したため破棄しました。
ERR	014	Invalid ISAKMP packet: %s	不正なパラメーターを持った ISAKMP パケットを受信したため破棄しました。
ERR	016	Negotiation timeout: %s	再送限界を超えたためネゴシエーションを中止します。
ERR	017	Packet security error: %s	暗号化されているべきパケットが暗号化されていません。または、暗号化されるべきではないパケットが暗号化されています。
ERR	018	Padding length error %d / %d	受信したパケットのパディング長が誤っています。
ERR	019	Decrypt failed: %s	暗号化された ISAKMP パケットの復号に失敗しました。
ERR	020	No ISAKMP policy for %s as %s	PEER アドレスに対応する ISAKMP ポリシーが見つかりません。
ERR	021	Not enough payload: %s	対向機から受信したパケットに必須ペイロードが含まれていません。
ERR	022	ID mismatched	ID が一致しないためネゴシエーションを継続できません。
ERR	023	Authentication fail	対向機を認証できないためネゴシエーションを継続できません。
ERR	024	Proposal mismatched	プロポーザルが一致しないためネゴシエーションを継続できません。
ERR	025	Failed to send packet	パケット送信に失敗したため、ネゴシエーションを中断しました。
ERR	026	Re-KEY failed: %s	Re-KEY の開始に失敗しました。
ERR	027	Failed to parse payload at %s	ISAKMP パケット中に含まれるペイロードの解析に失敗したためネゴシエーションを中断します。
ERR	028	Invalid UDP packet: %s	受信した UDP パケットが不正であったため、無視しました。
ERR	029	Hash failed: %s	パケットのハッシュ値が一致しなかったため破棄しました。
ERR	030	Received unexpected packet: %s	予期しないパケットを受信したため破棄しました。
ERR	031	Internal error: IPsec module error %d	IPsec モジュールより内部エラーが通知されました。

ERR	032	Internal error: Phase1 state mismatch %s/%d	ISAKMP Phase-1 ネゴシエーション中に状態遷移の矛盾が発生しました。
ERR	033	Internal error: Phase2 state mismatch %s/%d	ISAKMP Phase-2 ネゴシエーション中に状態遷移の矛盾が発生しました。
ERR	034	DPD keepalive failed with %s	DPD による Keepalive に失敗しました。SA を消去します。
ERR	037	Heartbeat keepalive failed with %s	Heartbeat による Keepalive に失敗しました。SA を消去します。
ERR	040	Keepalive sequence No overflowed for %s	許容範囲外の Keepalive シーケンス番号を受信しました。

7.4.13 IPsec (IPSEC)

MOD : IPSEC

ログの種類 : VPN

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	Processing for IPsec outbound packet	IPsec 対象パケットとして送出処理を行います。
DEBUG	701	Packet queued: %s	パケットがキューに格納されました。
DEBUG	702	Packet dequeued	パケットがキューから取り出されました。
DEBUG	703	Filter check %s/%s: %d/%r[%d]	IPv4 パケットが IPsec フィルター条件に一致するか調べています。
DEBUG	704	Filter check %s/%s: %d/%R[%d]	IPv6 パケットが IPsec フィルター条件に一致するか調べています。
DEBUG	705	SA search	パケットに適用する Outbound SA を探します。
DEBUG	706	Using soft expired SA: %08x	Soft expire を迎えた SA が使用されました。
DEBUG	707	SA deletion suspended: %08x	Expire となった IPsec SA が使用中であるため削除が保留されました。
INFO	202	Inbound SPI value allocated: %08x	ISAKMP ネゴシエーションのための Inbound SPI 値が決定されました。
INFO	205	SA delete requested %s/%08x	ISAKMP モジュールより IPsec SA の削除を要求されました。
INFO	208	Found Non-EPS marker from %s	パケット内に Non-ESP マーカーが検出されました。ISAKMP パケットとして処理します。
NOTICE	200	Create IPsec SA %s/%08x	IPsec SA が生成しました。
NOTICE	201	IPsec SA expired %s/%08x	IPsec SA が寿命により削除されます。
NOTICE	203	IPsec SA deleted %s/%08x	IPsec SA が削除されます。
NOTICE	204	SA deleted prior to soft expiration SPI: %08x / %d sec	Soft expire に達する前の SA が削除されました。
NOTICE	206	Cannot be fragmented	パケットに DF ビットが設定されていたため、フラグメント化できませんでした。
NOTICE	207	SA MTU updated SPI: %8x/MTU: %ld	IPsec SA に対する MTU が更新されました。
WARNING	008	Packet queue for SA negotiation is full: %s	SA 確立待ちのパケットキューがあふれたためパケットを破棄しました。
WARNING	009	SA timeout: %d packet (s)	ISAKMP ネゴシエーションに失敗したため、送信待ちになっていたパケットを破棄しました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。

ERR	002	Unknown SPI from %s / %08x	受信した IPsec パケットの SPI 値が未知のものであったため、破棄しました。
ERR	003	Replay attack detected	Replay 攻撃と判断したため、パケットを破棄しました。
ERR	004	ICV invalid	パケットの完全性チェックに失敗しました。パケットを破棄しました。
ERR	005	Padding invalid: Field value %d / Real length %d	付加されていたパディングが異常だったため、パケットを破棄しました。
ERR	006	Failed in tunneling process	トンネルパケット生成に失敗しました。
ERR	007	Failed to allocate encryption memory: %s	暗号処理のためのメモリーが確保できませんでした。
ERR	010	Internal error: Synchronization failed %s	ISAKMP – IPsec モジュール間でデータの同期に異常が発生しました。
ERR	011	Unusable SA: %s/%08x	IPsec 処理の途中で SA が使用できなくなったため、パケットを破棄しました。
ERR	012	Failed to acquire SA	IPsec モジュールから ISAKMP モジュールへの SA 要求に失敗しました。
ERR	013	Failed to install SA %s/%s	IPsec SA の構築に失敗しました。
ERR	014	Crypto failed for hardware limitation	ハードウェアの制限により暗号化もしくは復号化が失敗しました。
ERR	015	Internal error: PF_socket overflow	ISAKMP – IPsec モジュール間通信のバッファーがあふれました。
ERR	016	Invalid MTU value from %r: %s / %d	不正な MTU 値が通知されたため、無視しました。

7.4.14 DHCP クライアント (DHCPC)

MOD : DHCPC

ログの種類 : DHCP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	400	%s: State transition to %s	新しい状態に移行しました。
DEBUG	401	%s: IP address was deleted with no lease info	リース情報はありませんでしたが、IP アドレスは削除されました。
DEBUG	402	DHCP client process started	DHCP クライアントプロセスを起動しました。
DEBUG	403	DHCP client process stopped	DHCP クライアントプロセスを停止しました。
DEBUG	404	Read the conf file again	定義ファイルを再読み込みします。
DEBUG	405	%s: Received DHCP client startup request from NETM	DHCP クライアント開始要求を NETM から受け取りました。
DEBUG	406	%s: Received DHCP client release request from NETM	DHCP クライアント解放要求を NETM から受け取りました。
DEBUG	407	%s: State updated in NETM (NEW: %s/Prev: %s)	NETM 内部の DHCP クライアントステートが更新されました。
DEBUG	408	%s: Event %s invoked in NETM (State: %s)	DHCP クライアントでイベントが発生しました。
DEBUG	409	%s: Retry for %s request occurred in NETM (State: %s)	DHCP クライアントのリクエストに対する再試行が発生しました。
DEBUG	410	%s: Send DHCP client startup request from NETM	DHCP クライアント開始要求を NETM から送信しました。

DEBUG	411	%s: Send DHCP client release request from NETM	DHCP クライアント解放要求を NETM から送信しました。
DEBUG	412	%s: Received address (%s) delete event from NETM	アドレス削除イベントを NETM から受け取りました。
DEBUG	413	%s: Received address (%s) add event from NETM	アドレス追加イベントを NETM から受け取りました。
INFO	109	%s: required option '%s (%d)' was not found in DHCPOFFER from %s	DHCPOFFER パケット内に要求したオプションが含まれていませんでした。DHCPOFFER パケットは破棄されました。
INFO	118	%s: Received BOOTREPLY from %s	BOOTREPLY パケットを受信しました。 BOOTREPLY パケットは破棄されました。
INFO	300	%s: Received DHCPACK from %s	DHCPACK パケットを受け取りました。
INFO	301	%s: Received DHCPOFFER from %s	DHCPOFFER パケットを受け取りました。
INFO	302	%s: Received DHCPNAK from %s	DHCPNAK パケットを受け取りました。
INFO	303	%s: Sent DHCPDISCOVER to %s	DHCPDISCOVER パケットを送信しました。
INFO	304	%s: Sent DHCPREQUEST to %s	DHCPREQUEST パケットを送信しました。
INFO	305	%s: Sent DHCPDECLINE to %s	DHCPDECLINE パケットを送信しました。
INFO	306	%s: Sent DHCPRELEASE to %s	DHCPRELEASE パケットを送信しました。
INFO	307	%s: Received DHCPOFFER from %s with unknown id (%d)	不明な ID のパケットを受け取りました。 DHCPOFFER パケットは破棄されました。
INFO	308	%s: Received DHCPNAK from %s with unknown id (%d)	不明な ID のパケットを受け取りました。 DHCPNAK パケットは破棄されました。
INFO	309	%s: Received DHCPACK from %s with unknown id (%d)	不明な ID のパケットを受け取りました。 DHCPACK パケットは破棄されました。
INFO	310	%s: Bound to %s	新しい IP アドレスを割り当てました。
INFO	311	%s: T1 timer expired	T1 タイマーが期限切れになりました。
INFO	312	%s: T2 timer expired	T2 タイマーが期限切れになりました。
INFO	313	%s: Assigned IP address (%s) is already in use	割り振られた IP アドレスはすでに使用されています。
INFO	314	%s: IP address (%s) deleted due to releasing lease info	リース情報を削除したため、IP アドレスは削除されました。
INFO	315	%s: IP address (%s) deleted	IP アドレスは削除されました。
NOTICE	001	DHCP client started	DHCP クライアントを起動しました。
NOTICE	002	DHCP client stopped	DHCP クライアントを停止しました。
WARNING	101	%s: Received DHCPACK with uncertain address (%s) from %s	宛先不明なパケットを受け取りました。 DHCPACK パケットは破棄されました。
WARNING	103	%s: Received DHCPOFFER with uncertain address (%s) from %s	宛先不明なパケットを受け取りました。 DHCPOFFER パケットは破棄されました。
WARNING	105	%s: Received DHCPNAK with uncertain address (%s) from %s	宛先不明なパケットを受け取りました。 DHCPACK パケットは破棄されました。
WARNING	106	%s: Received DHCPACK in wrong state (%s) from %s	DHCP クライアントは DHCPACK を受け取る状態ではありません。DHCPACK パケットは破棄されました。
WARNING	107	%s: No expiry time on offered lease from %s	リース情報中に正しい期限がありません。この DHCPACK パケットは破棄され、ホスト情報を再要求します。
WARNING	108	%s: Received DHCPNAK in wrong state (%s) from %s	DHCP クライアントは DHCPNAK を受け取る状態ではありません。DHCPNAK パケットは破棄されました。

WARNING	111	%s: Received DHCPOFFER of the same client IP address from %s	サーバーから同じクライアント IP アドレスを持つ DHCPOFFER を受け取りました。DHCPOFFER パケットは破棄されました。
WARNING	113	%s: Received DHCPNAK from %s with no lease info	リース情報がないため、この DHCPNAK パケットは破棄されました。
WARNING	316	%s: Invalid IP address %r via DHCP protocol received (%s)	不適切な IP アドレスを DHCP プロトコルで受信しました。
WARNING	317	%s: Invalid IP address %r via DHCP protocol received (other error: %d)	内部的な要因により不適切と思われる IP アドレスを DHCP プロトコルで受信しました。
ERR	003	Failed to start DHCP client	DHCP クライアントを開始できませんでした。
ERR	200	Memory allocation failure (%s, %d)	メモリ確保に失敗しました。

7.4.15 SNMP (SNMP)

MOD : SNMP

ログの種類 : アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	002	Agent is being reconfigured	SNMP エージェントが設定の再読み込みを行います。
DEBUG	003	Agent restarted	SNMP エージェントが再起動しました。
DEBUG	011	Received SNMPv%d packet from %s (type: %s, %d bytes, transid: %d)	SNMP パケットを受信しました。
DEBUG	013	Sent SNMPv%d packet to %s (type: %s, %d bytes, transid: %d)	SNMP パケットを送信しました。
DEBUG	015	Ready to receive SNMP packets (local port: %s, sd: %d)	SNMP エージェントが SNMP パケット受信可能状態になりました。
DEBUG	046	Community ¥"%s¥" - traptype %d: %s (%s)	SNMP エージェント送信の有効／無効を設定しました。
DEBUG	048	Trapdelay timer %d secs: traptype %d (%s)	SNMP トラップ送信の待ち時間を設定しました。
DEBUG	204	MIB registration succeeded: ¥"%s¥"	MIB が登録されました。
DEBUG	051	Registered alarm (id: %d, interval: %d.%03d, flag: %d)	アラームを登録しました。
DEBUG	052	Unregistered alarm (id: %d)	アラームを削除しました。
DEBUG	053	No alarm (id: %d) to unregister	削除するアラームが見つかりませんでした。
DEBUG	054	Running alarm (id: %d)	アラームを実行します。
DEBUG	055	Alarm (id: %d) completed	アラームが実行されました。
DEBUG	056	Scheduled alarm (id: %d) in %d.%03d	アラームをスケジュールしました。
DEBUG	057	No alarm to schedule	スケジュールするアラームが見つかりませんでした。
DEBUG	058	Updated alarm (id: %d, interval: %d.%03d, flag: %d)	アラームを更新しました。
DEBUG	059	No alarm (id: %d) to update	更新するアラームが見つかりませんでした。
DEBUG	060	Illegal interval (%d.%03d) specified for a repeated alarm (id: %d, flag: %d)	繰り返し実行するアラームに対して、不正なインターバルが指定されました。
DEBUG	212	Registered view ¥"%s¥" (OID: %s, type: %s)	view が登録されました。
DEBUG	213	Set view access for community ¥"%s¥" (Read: ¥"%s¥", Write ¥"%s¥")	アクセス可能な view がコミュニティーへ設定されました。
DEBUG	301	Ready to receive smux connection; [%r]:%d (sd: %d)	SNMP エージェントが、smux 接続要求を受信可能な状態になりました。

DEBUG	302	Received a trap (type: %d, spec: %d) from peer	SNMP エージェントが smux peer から Trap メッセージを受信しました。
DEBUG	303	Accepted a smux peer [%r]:%d (fd %d)	SNMP エージェントが smux peer との接続を受け入れました。
DEBUG	304	Denied a smux peer %r:%d (fd %d), max number (%d) of peers already connected	smux peer の最大接続数を超えたため、smux 接続要求を拒否しました。
DEBUG	305	Refused a smux peer: auth failure (oid: %s, password: ¥"%s¥", descr: ¥"%s¥")	認証に失敗したため、smux 接続要求を拒否しました。
DEBUG	306	Failed to build smux message	smux メッセージを構築できませんでした。
DEBUG	307	Sent smux msg (type: %s, fd: %d, reqOID: %s)	smux メッセージを peer に送信しました。
DEBUG	308	Failed to parse variable bindings in smux	smux メッセージ内の variable bindings の読み取りに失敗しました。
DEBUG	309	Bad variable type (%d) in variable bindings in smux	smux メッセージの variable bindings の中に、不適切な型の値が含まれています。
DEBUG	310	Disconnected a smux peer (fd: %d)	SNMP エージェントが、smux peer との接続を切断しました。
DEBUG	311	Starting smux authentication process (oid: %s)	smux 接続の認証を開始します。
DEBUG	312	Smux authentication succeeded	smux 接続の認証が成功しました。
DEBUG	313	Smux connection request receive error (fd: %d)	smux 接続要求メッセージを正常に受信できませんでした。
DEBUG	314	Smux OpenPDU parse error (fd: %d)	smux OpenPDU の読み取りに失敗しました。
DEBUG	315	Not received smux OpenPDU (fd: %d)	SNMP エージェントは、OpenPDU ではない smux メッセージを受信しました。
DEBUG	316	Received smux OpenPDU from peer (fd: %d)	smux OpenPDU を受信しました。
DEBUG	317	Received smux RReqPDU on fd %d (oid: %s, prio: %d, ope: %d)	smux RReqPDU を受信しました。
DEBUG	318	Sent smux ClosePDU on fd %d (reason: %d)	smux Close PDU を送信しました。
DEBUG	319	Sent smux RRspPDU on fd %d (prio: %d)	smux Register Response PDU を送信しました。
DEBUG	320	Received smux msg (type: %s, fd: %d)	smux メッセージを受信しました。
DEBUG	321	Smux receive error on fd %d: error %d (%s)	smux メッセージを正常に受信できませんでした。
DEBUG	432	Ready to get SNMP statistics information	SNMP メッセージの統計情報が取得可能になりました。
DEBUG	901	ASN1 parse error (%s)	ASN1 メッセージの読み取りに失敗しました。
INFO	042	Will not send the trap (type %d: %s) to %s for community ¥"%s¥"	ユーザー設定により、当該トラップは送信されません。
INFO	047	Established Trap-v%d session to [%s], community ¥"%s¥"	SNMP トラップ送信先ホストが登録されました。
NOTICE	001	Agent started	SNMP エージェントが起動しました。
NOTICE	005	Agent stopped	SNMP エージェントが終了しました。
NOTICE	041	Detected a trap event: type %d (%s)	SNMP トラップの対象イベントが発生しました。
NOTICE	043	Sent v%d trap (type: %d, spec: %d) to %s for community ¥"%s¥"	SNMP トラップが送信されました。
WARNING	014	Received unknown type of message: %02X (transid: %d)	未知のタイプの SNMP パケットを受信しました。
WARNING	031	Failed to build SNMPv%d PDU	SNMP PDU を構築できませんでした。
WARNING	032	Cannot find element %s to build SNMPv%d PDU	SNMP PDU を構築するためのデータが不足しています。

WARNING	033	Failed to add element %s on building SNMP PDU	SNMP PDU を構築する際に、データを追加できませんでした。
WARNING	035	Failed to build SNMP Trap PDU	SNMP Trap PDU を構築できませんでした。
WARNING	036	Cannot find variable bindings to build SNMPv2 Trap PDU	SNMPv2 Trap PDU を構築するための variable bindings が見つかりません。
WARNING	050	Improper data was retrieved from the system	システムから取得したデータは適切ではありません。
WARNING	201	Received unsupported request mode (%d) from %d	サポートされていないモードの SNMP 要求を受信しました。
WARNING	202	Received unrecognized request mode (%d) from %d	未知のモードの SNMP 要求を受信しました。
WARNING	203	Received invalid PDU msg type (%d)	不正なメッセージタイプの SNMP パケットを受信しました。
WARNING	205	MIB registration failed: ¥"%s¥"	MIB の登録に失敗しました。
WARNING	211	Cannot find access control information	アクセス制限に関する設定がありません。
WARNING	414	UDP/IPv4 packet receive error on fd %d: error %d (%s)	UDP/IPv4 パケットが正常に受信できませんでした。
WARNING	424	UDP/IPv6 packet receive error on fd %d: error %d (%s)	UDP/IPv6 パケットが正常に受信できませんでした。
WARNING	433	SNMP packet parse error (%d) from %s	SNMP パケットの読み取りに失敗しました。
ERR	004	Detected invalid number of messages: %d	検知したメッセージ数が不正です。
ERR	016	Failed to start agent: Improper protocol/port (%s) specified	指定された受信プロトコル・ポートが不正であるため、SNMP Agent が起動できませんでした。
ERR	017	Failed to start agent: Not supported protocol/port (%s) specified	指定された受信プロトコル・ポートが未サポートであるため、SNMP エージェントが起動できませんでした。
ERR	018	Failed to start agent: Failed to register the specified protocol/port (%s)	指定された受信プロトコル・ポートが、SNMP パケット受信用に登録できなかったため、SNMP エージェントが起動できませんでした。
ERR	049	Failed to access the system resource	システム資源にアクセスできません。
ERR	101	Agent is exiting...	SNMP エージェントが異常終了します。

7.4.16 DNS リレー (PDNS)

MOD : PDNS

ログの種類 : アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	007	Sent query to %s, Query (%d), Answer (%d), Authority (%d), Additional (%d), Queries (%s, type %s, class %s)	Proxy DNS が問い合わせメッセージを送信しました。
DEBUG	008	Sent response to %s, Query (%d), Answer (%d), Authority (%d), Additional (%d), Queries (%s, type %s, class %s)	Proxy DNS が応答メッセージを送信しました。
DEBUG	009	Received query from %s, Query (%d), Answer (%d), Authority (%d), Additional (%d), Queries (%s, type %s, class %s)	Proxy DNS が問い合わせメッセージを受信しました。
DEBUG	010	Received response from %s, Query (%d), Answer (%d), Authority (%d), Additional (%d), Queries (%s, type %s, class %s)	Proxy DNS が応答メッセージを受信しました。

DEBUG	027	Received response error message from %s (reply code=%d, opcode=%d)	エラー応答メッセージを受け取りました。別のネームサーバーに再度問い合わせます。
DEBUG	023	Duplicate id (%d) packet from %s	このパケットと問い合わせ中のパケットの ID が重複しています。このパケットは破棄しました。
INFO	004	Cache cleared	キャッシュデータをクリアしました。
INFO	005	Static DNS server (%s) added	静的 DNS サーバーを追加しました。
INFO	006	Dynamic DNS server (%s) added	動的 DNS サーバーを追加しました。
INFO	030	No authority record found in response from %s	この応答メッセージの権威レコードを発見できませんでした。サーバーエラーを送信します。
INFO	036	Invalid operation while processing response	応答メッセージ処理中に不正な操作が発生しました。サーバーエラーを送信します。
INFO	025	Received response from %s with unknown id (%d)	不明な ID のパケットを受け取りました。応答パケットは破棄されました。
NOTICE	001	Proxy DNS started	Proxy DNS が起動しました。
NOTICE	002	Proxy DNS stopped	Proxy DNS が終了しました。
WARNING	012	Dad TSIG (%s, %d)	TSIG が正しくありません。このパケットは破棄されました。
WARNING	013	Bad operation code (%d) from %s	オペレーションコードが正しくありません。エラーを示すパケットを送信しました。
WARNING	014	Wrong query header counts (%s)	クエリーヘッダー内の要素数が正しくありません。エラーを示すパケットを送信しました。
WARNING	015	Failed to extract domain name from query (%s)	問い合わせメッセージからドメイン名の取得に失敗しました。エラーを示すパケットを送信しました。
WARNING	016	Query message length was short (%s)	クエリーメッセージ長が短すぎます。エラーを示すパケットを送信しました。
WARNING	017	Name server count was wrong (%s)	ヘッダーのネームサーバー数が正しくありません。エラーを示すパケットを送信しました。
WARNING	018	Bad query name (%s) from %s	問い合わせされた名前が正しくありません。エラーを示すパケットを送信しました。
WARNING	019	Query denied (%s)	問い合わせは拒否されました。エラーを示すパケット送信しました。
WARNING	020	Max cname number exceeded while processing request from %s	この問い合わせは CNAME 最大数を超えました。サーバーエラーを送信します。
WARNING	021	Failed to make query message while processing query from %s	問い合わせ処理中にクエリーの作成に失敗しました。サーバーエラーを送信します。
WARNING	022	No address for root server while processing request packet from %s	ルートサーバーのアドレスがありませんでした。サーバーエラーを送信します。
WARNING	026	Message format error in received response from %s (%s)	応答メッセージの形式が誤っています。別のネームサーバーに再度問い合わせします。
WARNING	028	Received response from unexpected server (%s)	問い合わせを送ったサーバーでないサーバーから応答パケットを受け取りました。この応答パケットは破棄しました。
WARNING	029	Received from lame server (%s)	不十分なサーバーから応答を受け取りました。別なネームサーバーに再度問い合わせします。
INFO	031	Maximum referrals exceeded in resolving %s(%s) (DNS client %s)	名前解決中に再帰参照の上限回数を超えました。クライアントに対してサーバーエラーメッセージを送信しました。

WARNING	032	Authority name server's address not found (%s)	権威ネームサーバーのアドレスが見つかりませんでした。このパケットは破棄しました。
WARNING	033	Message length was too short (%s)	メッセージ長が短すぎます。このパケットは破棄しました。
WARNING	034	Message from unaccepted server (%s)	受信を許可されていないサーバーからメッセージを受け取りました。このパケットは破棄しました。
WARNING	035	Packet with zero source port received from %s	ソースポートが 0 のパケットです。このパケットは破棄しました。
WARNING	037	Recursive queries for CNAME %s exceeded (DNS client %s)	CNAME の再帰参照が上限回数を超えました。クライアントに対してサーバーエラーメッセージを送信しました。
WARNING	038	Failed to make query message while processing response from %s	応答処理中にクエリーの作成に失敗しました。サーバーエラーを送信しました。
ERR	011	Memory allocation failure (%s, %d)	メモリ確保に失敗しました。

7.4.17 DHCP サーバー (DHCPS)

MOD : DHCPS

ログの種類 : DHCP

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	401	Started DHCP Server Process	DHCP サーバープロセスを起動しました。
DEBUG	402	Stopped DHCP Server Process	DHCP サーバープロセスを停止しました。
DEBUG	403	Restarted DHCP Server Process	DHCP サーバープロセスを再起動しました。
INFO	101	Received %s message from %s (pool %s)	メッセージを受信しました。
INFO	102	Sent %s message to %s (pool %s)	メッセージを送信しました。
INFO	316	Abandoned lease %s was marked as usable	破棄されたリースが再度、利用可能になりました。
INFO	104	Received message from invalid network client %s (pool %s)	無効なネットワークからメッセージを受信しました。
INFO	301	Lease %s expired	リース期限が終了しました。
INFO	305	Requested lease %s was unavailable	リクエストされたリースは使用可能ではありませんでした。
INFO	306	Requested lease %s was unknown	リクエストされたリースは未知のものでした。
INFO	307	Lease time for %s was updated	IP アドレスリースタイムが更新されました。
INFO	308	Renewal time for %s was updated	リース延長要求タイムアウト時間が更新されました。
INFO	309	Rebinding time for %s was updated	リース更新要求タイムアウト時間が更新されました。
INFO	310	Requested lease %s was fixed for other (pool %s)	リクエストされたリースは固定的に他のクライアントに割り当てられています。
INFO	311	Requested lease %s was unavailable (pool %s)	リクエストされたリースは使用可能ではありませんでした。
INFO	312	Requested lease %s was out of range (pool %s)	リクエストされたリースは割り当て範囲外でした。
INFO	315	Static lease assgined for clinet %s	クライアントに静的リースが設定されました。
INFO	317	Lease %s was out of range	リースは割り当て範囲外でした。

INFO	313	Leases %s was abandoned	リースを破棄しました。
INFO	203	Reclaiming abandoned lease %s	割り当てを中断しているアドレスを割り当て可能なアドレスとして再生します。
NOTICE	001	DHCP Server started	DHCP サーバーを起動しました。
NOTICE	002	DHCP Server stopped	DHCP サーバーを停止しました。
NOTICE	107	Ignored received %s message from %s (pool %s)	受信メッセージを無視しました。
WARNING	103	Received DHCP message with unknown type from %s (pool %s)	メッセージタイプが不明な DHCP パケットを受信しました。
WARNING	105	Received message from disallowed client %s (pool %s)	許可されていないクライアントからメッセージを受信しました。
WARNING	106	Received invalid message from %s (pool %s)	無効なメッセージを受信しました。
WARNING	108	Received message with different Server ID from %s (pool %s)	サーバー ID が異なるメッセージを受信しました。
WARNING	109	Received unknown Server ID from %s (pool %s)	未知のサーバー ID のメッセージを受信しました。
WARNING	110	Declined lease %s was abandoned (pool %s)	割り当てを拒否されたリースを破棄しました。
WARNING	111	Declined lease %s was not found (pool %s)	割り当てを拒否されたリースは存在しませんでした。
WARNING	202	Used all free leases in pool %s	割り当て可能なリースをすべて使用しました。
ERR	201	No free lease in pool %s	割り当て可能なリースが存在しませんでした。
ERR	302	Client %s had duplicated leases	クライアントに対して複数のリースが存在しました。
ERR	303	Client %s had dynamic and static leases	クライアントに対し動的リースと静的リースが存在しました。
ERR	304	Leases %s conflicted	リースが競合しました。
ERR	314	Detected duplicate address %s assigned %s	重複アドレスを発見しました。
ERR	404	DHCP Server Process running already	DHCP サーバープロセスがすでに起動中です。
ERR	901	Encountered Fatal Internal Error (%s:%4d)	致命的な内部エラーが発生しました。
ERR	902	Encountered Internal Error (%s:%4d)	内部エラーが発生しました。

7.4.18 HTTP サーバー (HTTPS)

MOD：HTTPS

ログの種類：アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	003	Access permitted by acl %s	アクセスリストにより、リモートホストのアクセスを許可しました。
INFO	004	Access denied by acl %s	アクセスリストにより、リモートホストのアクセスを拒否しました。
NOTICE	001	HTTP server started	HTTP サーバーが起動しました。
NOTICE	002	HTTP server stopped	HTTP サーバーが終了しました。
ERR	005	Failed to read acl	アクセスリストの読み込みに失敗しました。

7.4.19 SNTP (NTP)

MOD : NTP

ログの種類 : アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	001	Faild to open file (%s)	NTP クライアントファイルのオープンに失敗しました。または内容が不正です。
DEBUG	002	Failed to start ntp client	NTP クライアントの起動に失敗しました。
DEBUG	003	Failed to fork ntp client	NTP クライアントのデーモン処理に失敗しました。
DEBUG	004	Failed to create pid file	NTP クライアントのプロセス ID ファイルの生成に失敗しました。
DEBUG	005	No server can be used, exiting	指定された NTP サーバーを使用できませんでした。
DEBUG	006	No valid response from servers	指定された NTP サーバーから適切な応答がありませんでした。
DEBUG	007	Failed to resolve host %s	ホスト名の名前解決に失敗しました。
DEBUG	008	getaddrinfo() failed	getaddrinfo が失敗しました。
DEBUG	009	socket() failed	socket が失敗しました。
DEBUG	010	setsockopt() SO_REUSEADDR failed	setsockopt が失敗しました。
DEBUG	011	bind() failed	bind が失敗しました、あるいは、NTP ポートがすでに使用中です。
DEBUG	012	Can't find family compatible socket to send ntp packet	NTP パケットを送るための互換性のあるアドレスファミリーを見つけることができません。
DEBUG	013	Failed to send a packet to server (%s)	NTP パケットの送信に失敗しました。
DEBUG	014	Failed to adjust the time of day	時刻の設定に失敗しました。
NOTICE	100	NTP client started	NTP クライアントが起動しました。
NOTICE	101	NTP client stopped	NTP クライアントが終了しました。
INFO	102	Time acquired from NTP server (%s)	NTP サーバーから取得した時間を設定しました。

7.4.20 ユーザー (LOGIN)

MOD : LOGIN

ログの種類 : アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
NOTICE	001	Login succeeded (%s from %s)	ユーザーのログインに成功しました。
NOTICE	002	Login failed (%s from %s)	ユーザーがログインに失敗しました。
NOTICE	003	Login failed (Unknown user: %s from %s)	登録されていないユーザーがログインに失敗しました。
NOTICE	004	Logout (%s)	ユーザーがログアウトしました。

7.4.21 システム (SYSTM)

MOD : SYSTM

ログの種類 : システム

エラーレベル	MSGNO	MESSAGE	意味
NOTICE	001	System started	システムが起動しました。
NOTICE	002	Clock was set manually	装置の時計が手動で設定されました。
NOTICE	003	Timezone was set	装置のタイムゾーンが変更されました。
NOTICE	004	Timezone was set back to default	装置のタイムゾーンがデフォルトに戻されました。

7.4.22 URL フィルター (UFLT)

MOD : UFLT

ログの種類 : ファイアウォール

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	020	BLOCKED: matched with %s %s %r -> %r on %s	不許可 URL フィルタールールと一致したため、パケットを破棄しました。
DEBUG	021	PASSED: matched with %s %s %r -> %r on %s	許可 URL フィルタールールと一致したため、パケットを通過させました。
DEBUG	022	BLOCKED: %r -> %r on %s (implicit deny rule)	一致する URL フィルタールールが存在しないため、パケットを破棄しました。
NOTICE	001	URL Filter enabled	URL フィルターが有効にされました。
NOTICE	002	URL Filter disabled	URL フィルターが無効にされました。
NOTICE	010	BLOCKED: matched with %s %s %r -> %r on %s	不許可 URL フィルタールールと一致したため、パケットを破棄しました。
NOTICE	011	PASSED: matched with %s %s %r -> %r on %s	許可 URL フィルタールールと一致したため、パケットを通過させました。

7.4.23 DoS 検出 (IDS)

MOD : IDS

ログの種類 : ファイアウォール

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	Clear attack event: %s	アタック情報が消去されました。
DEBUG	701	Failed to add event tree (%s) : %s %r -> %r (%s, %s)	アタックイベントの追加に失敗しました。
DEBUG	702	Add event entry (%s) : %s %r -> %r (%s, %s, count=%u)	アタックイベントを追加しました。
DEBUG	703	Remove event entry (%s) : %s %r -> %r (%s, %s, count=%u)	アタックイベントを削除しました。
DEBUG	704	Add timeout entry (%s): %s %r -> %r (%s, %s, count=%u)	タイムアウトイベントを追加しました。
DEBUG	705	Remove timeout entry (%s): %s %r -> %r (%s, %s, count=%u)	タイムアウトイベントを削除しました。
DEBUG	706	Exceed threshold (%s): %s %r -> %r (%s, %s, count=%u, interval=%u)	アタックイベント発生回数がしきい値を超えました。

DEBUG	707	Exceed max event counter (%s): %s %r -> %r (%s, %s, count=%u)	アタックイベント数が最大イベント数を超えました。
NOTICE	010	IDS enabled	IDS が有効になりました。
NOTICE	011	IDS disabled	IDS が無効になりました。
NOTICE	012	IDS type enabled: %s	アタック別 IDS が有効になりました。
NOTICE	013	IDS type disabled: %s	アタック別 IDS が無効になりました。
NOTICE	014	Attack start: %s %r -> %r (%s, %s)	アタックが開始しました。
NOTICE	015	Attack finish: %s %r -> %r (%s, %s)	アタックが終了しました。
NOTICE	016	Detect attack: %s %r -> %r (%s, %s)	アタックを検出しました。
NOTICE	017	BLOCKED: Detect attack: %s %r -> %r (%s, %s)	アタックを検出したためパケットを破棄しました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERR	002	Removed unknown type timeout	未知のタイムアウトイベントが削除されました。

7.4.24 仮想トンネルインターフェース（TUN）

MOD：TUN

ログの種類：VPN

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	701	%s : Tunneling address information erased	トンネルの情報が消去されました。
DEBUG	704	%s : Tunneling address information setup finished	トンネル情報の設定に成功しました。
DEBUG	705	%s : Start setup tunnel information (%s)	トンネル情報の作成を開始しました。
INFO	001	%s : Tunnel interface created	トンネルインターフェースが作成されました。
INFO	002	%s : Tunnel interface deleted	トンネルインターフェースが削除されました。
INFO	003	%s : Configured for %s tunnel	トンネルインターフェースのモードが設定されました。
INFO	004	%s : Tunneling %s %s address configured %s	トンネリングに用いるアドレスが設定されました。
INFO	005	%s : Tunneling %s %s address cleared	トンネリングに用いるアドレスの設定が消去されます。
INFO	006	%s : Operational status up	トンネルインターフェースが有効になりました。
INFO	007	%s : Operational status down	トンネルインターフェースが無効になりました。
INFO	010	%s : Tunneling %s hostname configured %s	トンネリングに用いるホスト名が設定されました。
INFO	011	%s : Tunneling %s hostname cleared	トンネリングに用いるホスト名が消去されます。
INFO	023	%s : Packet discarded (%s)	IPsec ポリシーが見つからなかったためパケットが破棄されました。
INFO	030	%s : DFbit configured for %s	トンネルインターフェースの DFbit に関する動作が設定されました。
INFO	031	%s : DFbit configuration cleared for %s	トンネルインターフェースの DFbit に関する動作がクリアされました。

INFO	032	%s : Tunnel mode configuration cleard	トンネルインターフェースのモードがクリアされました。
INFO	033	%s : Interface MTU updated %d	トンネルインターフェースの MTU が更新されました。
INFO	034	%s : Interface MSS updated %d	トンネルインターフェースの MSS が更新されました。
NOTICE	013	%s : Packet discarded (%s)	Interface が送信可能な状態ではないためにパケットが破棄されました。
WARNING	016	%s : Receive queue overflowed	受信キューがオーバーフローしました。
WARNING	017	%s : Tunneling source %s address was not found on own interfaces	トンネルインターフェースに設定されている始点アドレスを持つインターフェースが見つかりませんでした。
WARNING	019	%s : Tunnel packet discarded (address missmatch) src:%s dst:%s	受信トンネリングパケットのアドレスがトンネルと一致しないために破棄しました。
WARNING	020	%s : Tunnel packet from %s wrong (%s)	受信トンネリングパケットに問題があります。
WARNING	028	%s : Tunnel packet discarded (%s address missmatch) %s	受信トンネリングパケットのアドレスがトンネルと一致しないために破棄しました。
WARNING	029	%s : DFbit configuration of the interface strange (%s)	DFbit に関する設定に異常が見つかりました。
ERR	008	%s : Installing %s address failed (%s)	トンネルアドレス情報の設定に失敗しました。
ERR	009	%s : Uninstalling %s %s address failed (%s)	トンネルアドレス情報の消去に失敗しました。
ERR	012	%s : Tunnel packet nested %d times exceeding nest limit	トンネルパケットのカプセル化が制限値を超えました。
ERR	014	%s : Packet discarded (%s)	ドライバーにエラーが発生したためパケットが破棄されました。
ERR	015	%s : Setting tunnel address failed (%s)	トンネリングアドレスの設定に失敗しました。
ERR	018	%s : %s %s	トンネルインターフェースのアドレスが不正です。
ERR	021	%s : Memory allocation failed (%s)	メモリの取得に失敗しました。
ERR	022	%s : Attach to %s protocol stack failed (%s)	プロトコルスタックへのアタッチに失敗しました。
ERR	025	%s : Tunnel interface creation failed (%s)	トンネルインターフェースの作成に失敗しました。
ERR	026	%s : Tunnel interface delete failed (%s)	トンネルインターフェースの削除に失敗しました。
ERR	027	%s : Tunnel information update failed (%s)	トンネルインターフェースの更新に失敗しました。

7.4.25 ブリッジ (IRB)

MOD : IRB

ログの種類 : ブリッジ

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	104	bridge-group %d : dynamic FDB entry learned(%s w/ %s)	Dynamic FDB エントリーを生成しました。
DEBUG	105	bridge-group %d : dynamic FDB entry deleted(%s w/ %s)	自動的に学習した FDB エントリーを削除しました。

DEBUG	109	bridge-group %d : %d of dynamic FDB entries ageout	Dynamic FDB エントリーがタイムアウトしました。
DEBUG	201	MAC filter rule hits : %s	Frame と MAC filter rule が一致しました。
DEBUG	302	bridge-group %d : %d of bridge cache(s) ageout	ブリッジキャッシュがタイムアウトしました。
INFO	003	%s : BVI interface created	BVI インターフェースを作成しました。
INFO	004	%s : BVI interface deleted	BVI インターフェースを削除しました。
INFO	005	bridge-group %d created	ブリッジグループを作成しました。
INFO	006	bridge-group %d deleted	ブリッジグループを削除しました。
INFO	007	%s : join in bridge-group %d	ブリッジグループへインターフェースを追加しました。
INFO	008	%s : break away from bridge-group %d	ブリッジグループからインターフェースを削除しました。
INFO	101	%s on bridge-group %d static FDB entry added	Static FDB エントリーを設定しました。
INFO	102	%s on bridge-group %d, static FDB entry deleted	Static FDB エントリーを削除しました。
INFO	301	bridge-group %d : filter cache entries cleared(%s)	ブリッジキャッシュをクリアしました。
NOTICE	001	Integrated Routing Bridge was enabled	IRB モジュールが有効になりました。
NOTICE	002	Integrated Routing Bridge was disabled	IRB モジュールが無効になりました。
NOTICE	107	bridge-group %d : all FDB entries cleard	すべての FDB エントリーを削除しました。
NOTICE	108	bridge-group %d : all dynamic FDB entries flushed	自動的に学習した FDB エントリーをすべて削除しました。
WARNING	106	bridge-group %d : FDB entries size limited	FDB エントリー数が上限に達しました。
ERR	103	Internal error : FDB entry add failed(%s on bridge-group %d)	Static FDB エントリーを追加できませんでした。

7.4.26 UPnP (UPNPD)

MOD : UPNPD

ログの種類 : ファイアウォール

エラーレベル	MSGNO	MESSAGE	意味
DEBUG	700	%d active incoming HTTP connections	アクティブな HTTP コネクションが存在しています。
DEBUG	702	UPnP permission rule %d matched : port mapping %s	許可されたポートマッピングルールです。
DEBUG	703	No permission rule matched : accept by default (n_perms=%d)	許可されていないポートマッピングルールです。
DEBUG	705	Set nextnatpmptoclean_timestamp to %u	次回のタイムアウト時間を設定しました。
DEBUG	706	Failed to send packet (%s)	パケットの送信に失敗しました。
DEBUG	707	HTTP listening on port %d	HTTP の待ち受けを開始しました。
DEBUG	708	Received signal %d, good-bye	シグナルを受信したため、終了します。
DEBUG	709	Failed to broadcast good-bye notifications	SSDP good-bye の送信に失敗しました。
DEBUG	710	Listening for NAT-PMP traffic on port %u	NAT-PMP の待ち受けを開始しました。
DEBUG	711	HTTP connection from %r:%d	HTTP に接続されました。
DEBUG	712	HTTP REQUEST : %s %s (%s)	HTTP Request を受信しました。
DEBUG	713	SOAPAction: %s	SOAP アクションを受信しました。

DEBUG	714	System uptime is %d seconds	System uptime を取得しました。
INFO	100	SSDP M-SEARCH from %r:%d	SSDP M-SEARCH を受信しました。
INFO	101	Invalid SSDP M-SEARCH from %r:%d	不正な SSDP M-SEARCH を受信しました。
INFO	104	AddPortMapping: external port %hu to %s:%hu protocol %s for: %s	ポートマッピングルールの追加要求を受信しました。
INFO	105	GetSpecificPortMappingEntry: rhost='%s' %s %s found => %s:%u (%lu) desc='%s'	ポートマッピングルールの取得要求を受信しました。
INFO	106	DeletePortMapping: external port: %hu, protocol: %s	ポートマッピングルールの削除要求を受信しました。
INFO	107	GetGenericPortMappingEntry: index=%d	ポートマッピングルールの取得要求を受信しました。
INFO	110	Send UPnPError %d: %s	UPnP エラーを送信しました。
INFO	117	No SOAPAction in HTTP headers	SOAP アクションが含まれていませんでした。
INFO	122	Redirection permission check failed for %hu->%s:%hu %s	許可されていないポートマッピングルールを設定しようとしました。
INFO	123	Ignoring redirect request as it matches existing redirect	すでに存在するポートマッピングルールと同じ内容を追加しようとしました。
INFO	124	Port %hu protocol %s already redirected to %s:%hu	すでに存在するポートマッピングルールと同じポート番号を追加しようとしました。
INFO	125	Redirecting port %hu to %s:%hu protocol %s (%lu) for: %s	ポートマッピングルールを追加します。
INFO	127	Removing redirect rule port %hu %s	ポートマッピングルールを削除します。
INFO	129	NAT-PMP request received from %r:%hu %dbytes	NAT-PMP リクエストを受信しました。
INFO	130	NAT-PMP public address request	パブリックアドレス要求を受信しました。
INFO	131	NAT-PMP port mapping request : %hu->%s:%hu %s lifetime=%us	ポートマッピングルールの追加要求を受信しました。
INFO	132	NAT-PMP %s port %hu mapping removed	ポートマッピングルールを削除しました。
INFO	133	Port %hu %s already redirected to %s:%hu, replacing	すでに存在するポートマッピングルールと同じ内容を追加しようとしました。
INFO	134	Expired NAT-PMP mapping port %hu %s removed	タイムアウトしたポートマッピングルールを削除しました。
INFO	136	Failed to send SSDP announce	SSDP アナウンスを送信できませんでした。
NOTICE	102	Unknown udp packet received from %r:%d	不正な UDP パケットを受信しました。
NOTICE	103	Client %r tried to redirect port to %s	送信元 IP アドレスとは異なる IP アドレスのポートマッピングルールが要求されました。
NOTICE	108	QueryStateVariable: Unknown: %s	不正な QueryStateVariable パラメーターを受信しました。
NOTICE	109	SoapMethod: Unknown: %s	不正な SOAP アクションを受信しました。
NOTICE	111	Failed to remove port mapping	ポートマッピングルールの削除に失敗しました。
NOTICE	119	%s not found, responding ERROR 404	存在しない URL を要求されました。
NOTICE	120	SUBSCRIBE was not supported yet.	まだ SUBSCRIBE 要求はサポートしていません。
NOTICE	121	Unsupported HTTP Command %s	未対応の HTTP コマンドを受信しました。
NOTICE	128	Removed %d unused rules	使用していないポートマッピングルールを削除しました。
NOTICE	135	No address associated with rule	指定された IP アドレスに関連したルールは存在しません。

WARNING	050	Failed to add multicast membership for address %r	マルチキャストグループに追加できませんでした。
WARNING	051	Truncated output	サイズオーバーにより、データが欠けた状態で送信しました。
WARNING	052	Unexpected HTTP state: %d	HTTP が予期しない状態になりました。
WARNING	053	Discarding NAT-PMP request (too short) %dBytes	サイズが小さすぎたため、パケットを破棄しました。
WARNING	054	Unsupported NAT-PMP version : %u	サポートしていないバージョンの NAT-PMP パケットを受信しました。
WARNING	055	Failed to remove NAT-PMP mapping eport %hu, protocol %s	ポートマッピングルールの削除に失敗しました。
WARNING	056	Failed to add NAT-PMP %hu %s->%s:%hu '%s'	ポートマッピングルールの追加に失敗しました。
WARNING	057	Failed to send NAT-PMP packet: sent only %d bytes out of %d	一部のデータしか送信できませんでした。
WARNING	058	Failed to cleaning expired NAT-PMP mappings	ポートマッピングルールのクリーニングに失敗しました。
WARNING	059	Failed to receive %s	パケットの受信に失敗しました。
WARNING	060	Failed to send %s	パケットの送信に失敗しました。
ERR	001	Memory allocation failed for %s	メモリーの確保に失敗しました。
ERR	002	Internal error: %s	内部的エラーが発生しました。
ERR	003	Failed to open pidfile for writing %s	PID ファイルを開くことができませんでした。
ERR	004	Failed to write to pidfile %s	PID ファイルに情報を書き込むことができませんでした。
ERR	005	Failed to get IP address for interface %s	インターフェースから IP アドレスを取得できませんでした。
ERR	006	Failed to convert hostname '%s' to IP address	ホスト名を IP アドレスに変換できませんでした。
ERR	007	Failed to get data for interface %s	インターフェースの情報を取得できませんでした。
ERR	008	Failed to update UPnP configuration	コンフィグレーションファイルの更新に失敗しました。

7.4.27 ダイナミック DNS (DDNS)

MOD : DDNS

ログの種類 : アプリケーション

エラーレベル	MSGNO	MESSAGE	意味
NOTICE	001	Updating IP address of %s	ダイナミック DNS サーバーに IP アドレスの更新を行います。
NOTICE	002	Status: %s	更新に対するダイナミック DNS サーバーからの返答を表示します。
NOTICE	003	Failed to communicate with server	ダイナミック DNS サーバーとの通信に失敗しました。

ご注意

- 本書に関する著作権などの知的財産権は、アライドテレシス株式会社（弊社）の親会社であるアライドテレシスホールディングス株式会社が所有しています。アライドテレシスホールディングス株式会社の同意を得ることなく本書の全体または一部をコピーまたは転載しないでください。
- 弊社は、予告なく本書の一部または全体を修正、変更することがあります。
- 弊社は、改良のため製品の仕様を予告なく変更することがあります。

商標について

- CentreCOM は、アライドテレシスホールディングス株式会社の登録商標です。
- Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- 初期に参照している NTP サーバーは、インターネットマルチフィード株式会社のものです。http://www.jst.mfeed.ad.jp/
- その他、この文書に記載されているソフトウェアおよび周辺機器の名称は各メーカーの商標または登録商標です。

マニュアルバージョン

2006 年 12 月 13 日	Rev. A	初版
2007 年 6 月 22 日	Rev. B	第 2 版
2008 年 1 月 25 日	Rev. C	第 3 版
2008 年 10 月 24 日	Rev. D	第 4 版
2008 年 11 月 28 日	Rev. E	第 5 版