613-000685 Rev.B 070622

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 AC100V 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。

## 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。

# 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。

## 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。

## 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。）

# 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、IPsec に準拠した高速 VPN 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、たとえばルーターや 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。

- Inbound/Outbound アクセス
- ステルスモード
- セルフアクセスルールの設定
- NAT の設定
- タイムアウトの設定
- URL フィルター
- DoS

**「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「2.0.0」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、各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 | 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 | 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 | 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。**


**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。**

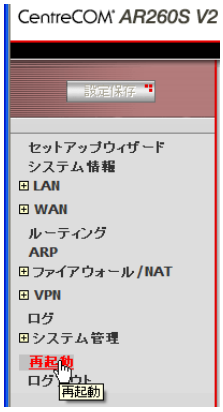
1. Web ブラウザーを起動後、アドレス欄に「192.168.1.1」を指定してアクセスします。
2. ダイアログで「ユーザー名」と「パスワード」を入力し「OK」ボタンをクリックします。本製品のデフォルトではユーザー名「manager」、パスワード「friend」です。


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。

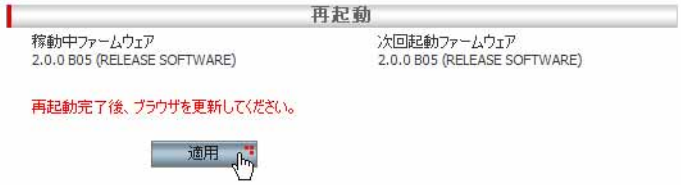
## 1.2 再起動

**本製品を再起動するには以下の手順を実行します。**

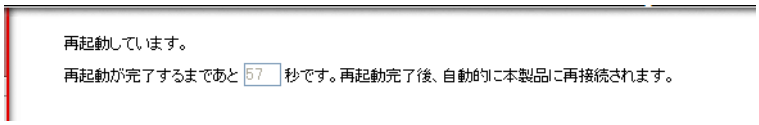
1. メニューから「再起動」をクリックします。



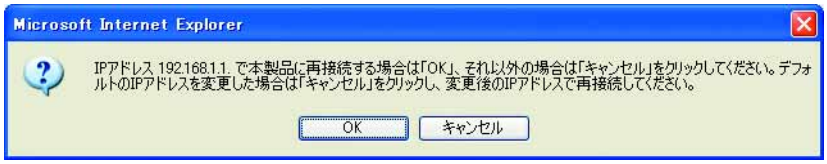

2.「適用」ボタンをクリックします。




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。

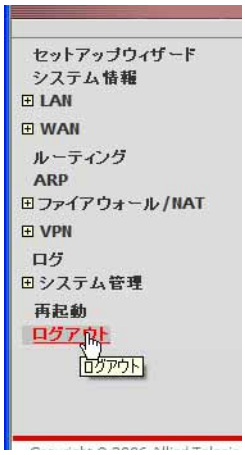
ヒント **変更後の本製品の IP アドレスが、接続するコンピューターと異なるサブネットになる場合、本製品に接続できなくなります。必要に応じてコンピュータの TCP/IP 設定も変更してください。**

5. 以上で再起動は完了です。

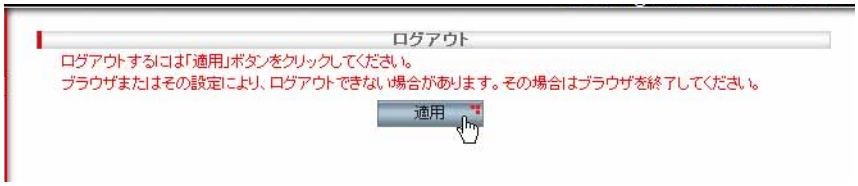
## 1.3 ログアウト

**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

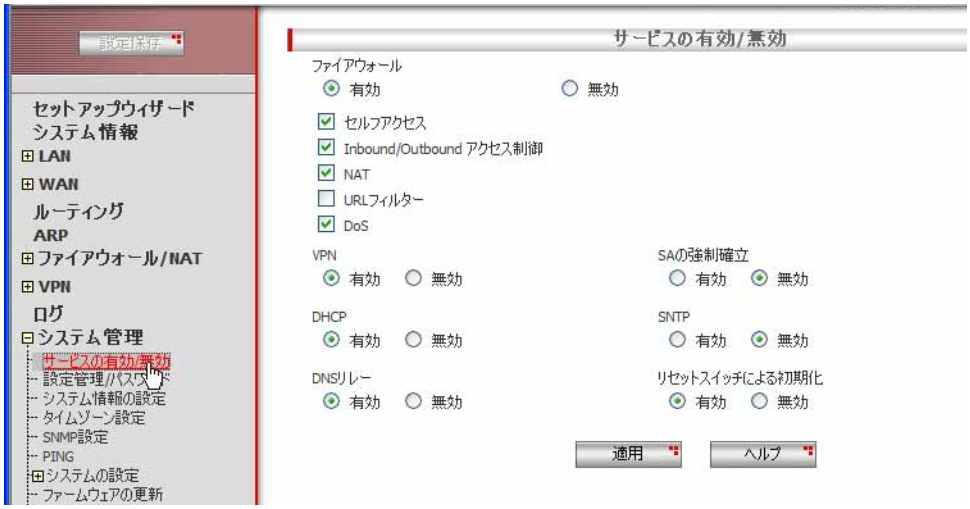
**本製品では、以下の各種機能を「サービスの有効 / 無効」ページで有効化 / 無効化することができます。**

- ファイアウォール機能
- 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
- 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

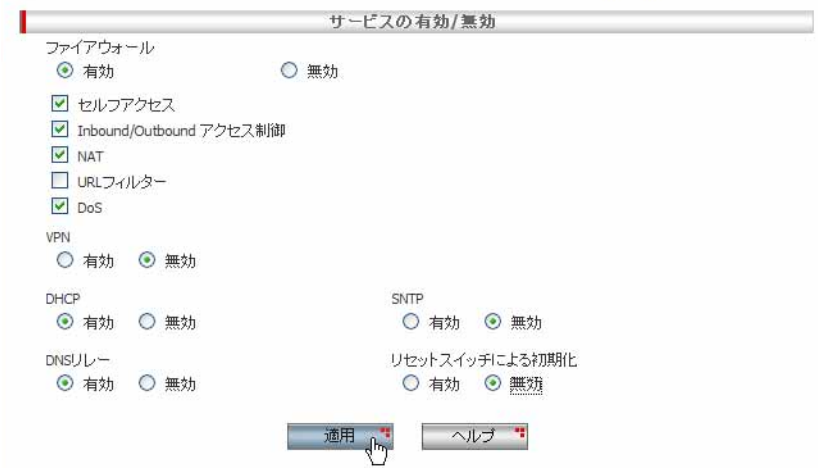
**各機能を有効化 / 無効化するには以下の手順を実行します。**

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
- SNTP
- リセットスイッチによる初期化



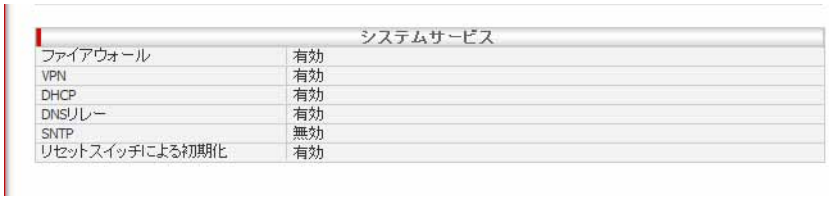

3. 以上で設定は完了です。

### 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.99 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。<br>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全て許可します。<br>デフォルトは「有効」です。 |

| | | | |
|---|---|---|---|
| | | Inbound/Outbound 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。<br>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全て許可します。<br>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。<br>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。<br>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。<br>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。<br>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。<br>無効の場合、アタック検知処理は実行されません。<br>デフォルトは「有効」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.149 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。<br>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。<br>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。<br>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。 |
| 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.34 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。 |
| 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。

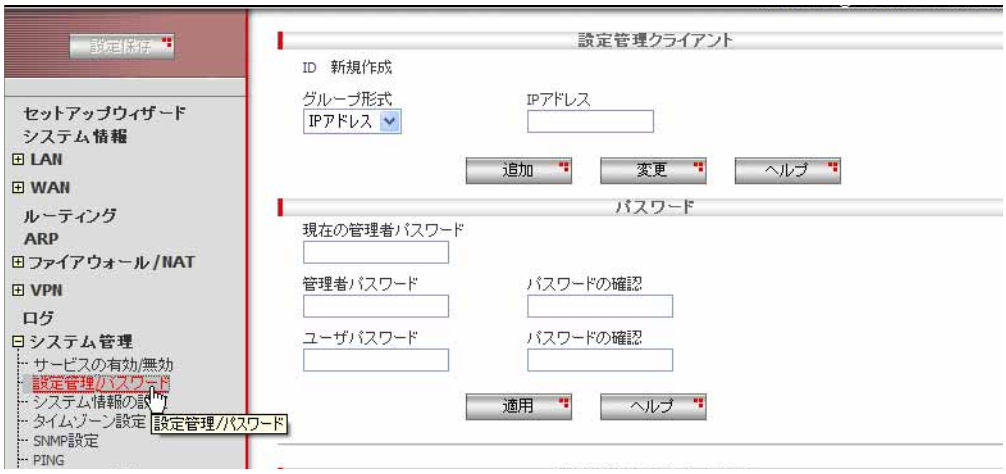
## 1.5.2 設定管理クライアントの設定

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。


**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.110 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

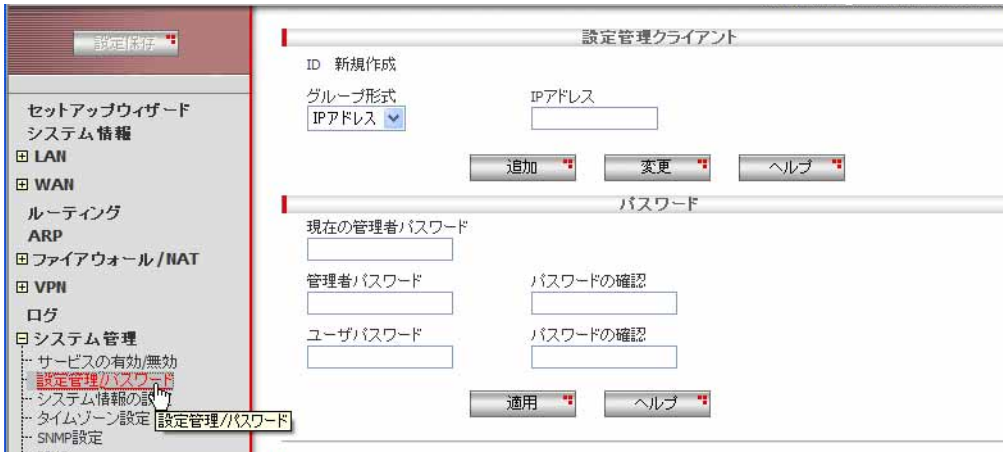
1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
2. 「設定管理クライアントリスト」テーブルにクライアントが一覧表示されます

### 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 V2」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。<br>入力可能な一部の記号は以下のとおりです。<br>! # % & ( ) + − . （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。<br>入力可能な一部の記号は以下のとおりです。<br>! # % & ( ) + − . （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 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 | 03-1111-2222 |


3. 以上で設定は完了です。

### 1.6.3 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。

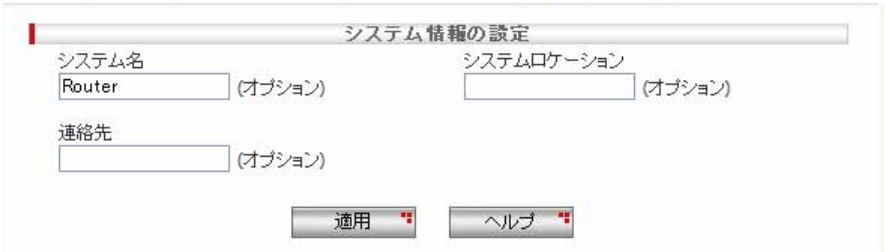

2.「システム情報」に設定したシステム情報が表示されます。


| 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 IP アドレス | 本製品の LAN 側インターフェースの IP アドレスが表示されます。 |
| 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。<br>入力可能な一部の記号は以下のとおりです。<br>! # % & ( ) + - . （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

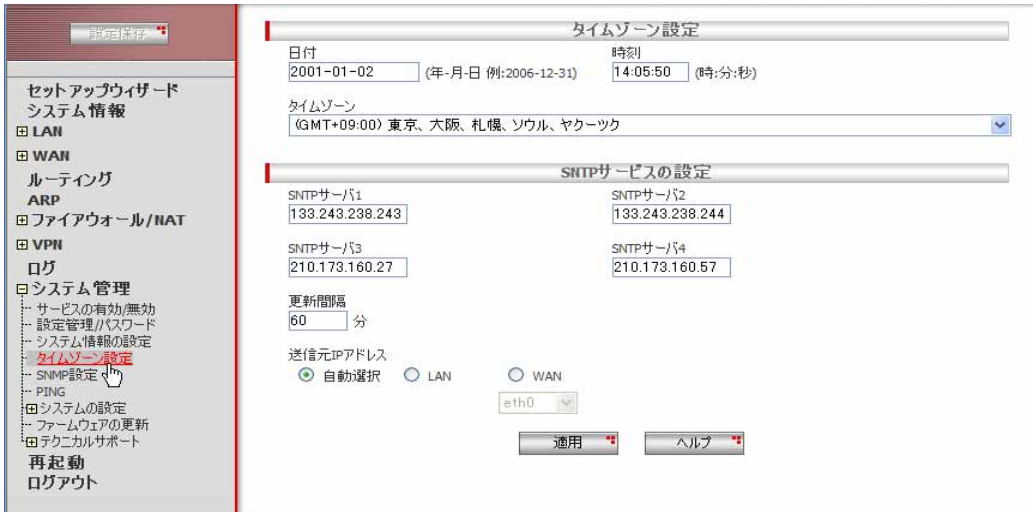
本製品ではシステム時刻を「タイムゾーン設定」ページで設定します。本製品は SNTP クライアント機能を持つため、外部 SNTP サーバーを利用した時刻同期が可能です。

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。

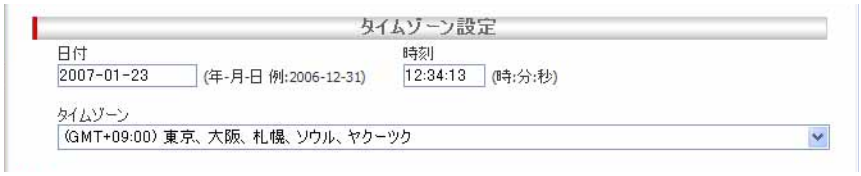

3. 以上で設定は完了です。

### 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。

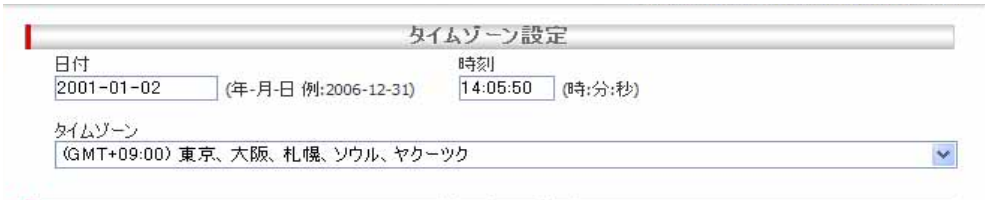

3. 以上で設定は完了です。

### 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。 |

# 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 |
| コミュニティ名 | viewer |
| マネージャアドレス | 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。 |
| コミュニティ名 | | 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。<br>一部の記号として入力可能な文字は以下のとおりです。<br>! # % & ( ) + - . （ピリオド） = @ [ ] ^ _（下線）{ } ~ , （カンマ） |
| マネージャアドレス | | 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 |
| コミュニティ名 | public |
| マネージャアドレス | |
| 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。

## 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、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。


### 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。<br>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、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。 |
| | システム | フラッシュファイルシステム、ログ、ユーザ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。 |
| | エラー | 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。<br>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 |
| 「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。 |

# 1.10　設定の初期化

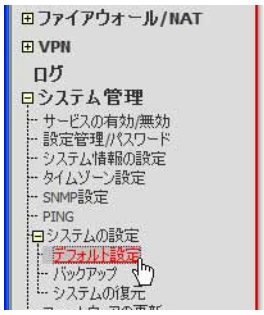
**本製品に設定した内容を初期化（デフォルト設定に戻す）する手順を説明します。**

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。**

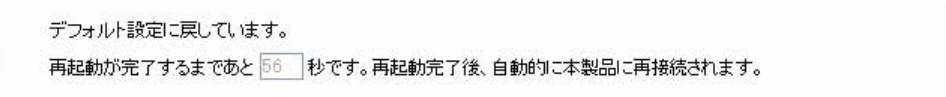
## 1.10.1　GUI 設定画面からの初期化

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。

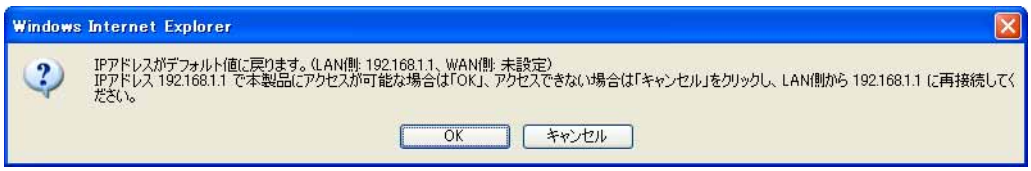



2.「適用」ボタンをクリックします。


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

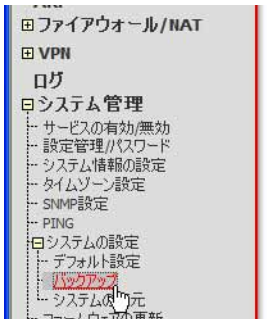

**「リセットスイッチによる初期化」は「リセットスイッチによる初期化」サービスを有効にしないと実行できません。サービスを有効にする手順については「P.18 機能の有効化 / 無効化の設定」を参照してください。**

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。

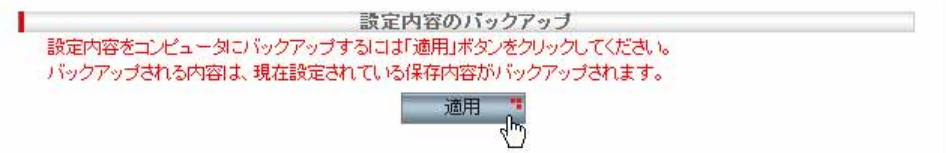
## 1.11 設定内容のバックアップ

**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。**

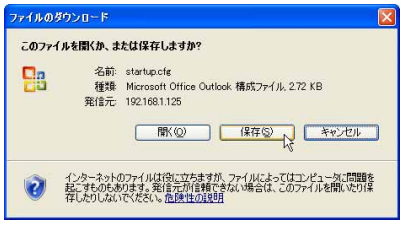
1. メニューから「システム管理」->「システムの設定」->「バックアップ」の順にクリックします。

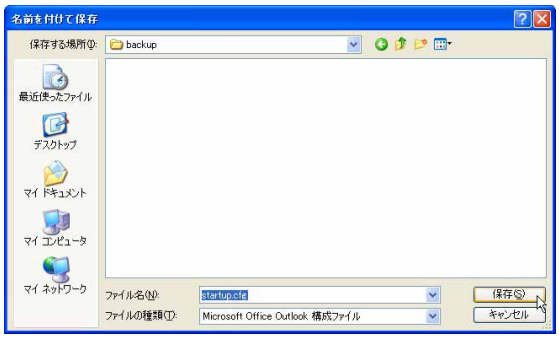



2.「適用」ボタンをクリックします。

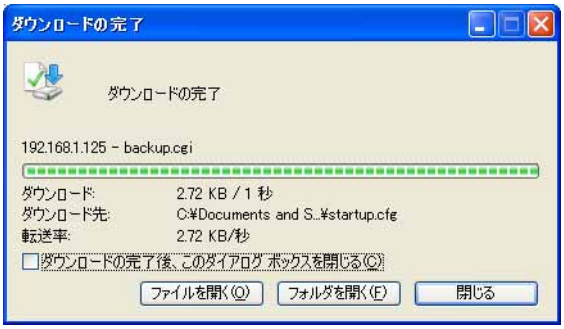



3. 以下の画面が表示されたら「保存」ボタンをクリックして、バックアップファイルの保存場所を指定し、ダイアログの「保存」ボタンをクリックします。



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。



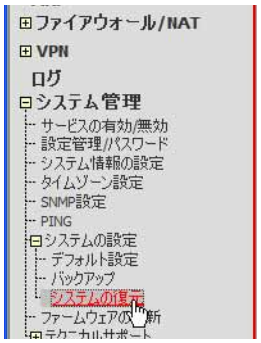

5. 以上で完了です。

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。**

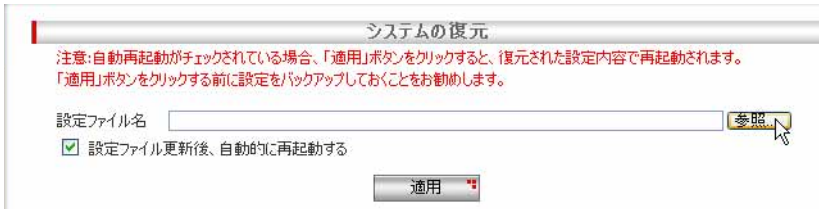
## 1.12　バックアップファイルの復元

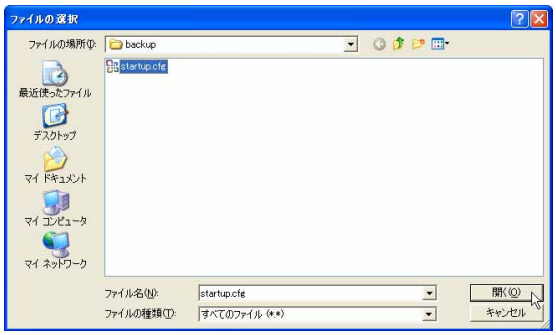
**バックアップした本製品の設定ファイルを復元する手順を説明します。**

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。

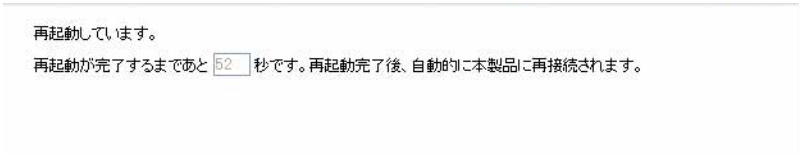


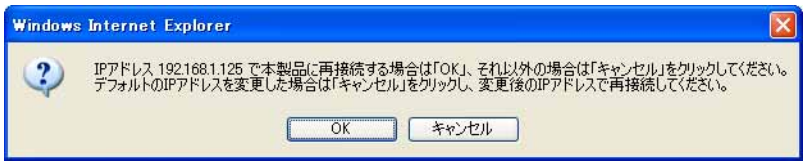

3.「適用」ボタンをクリックします。


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。

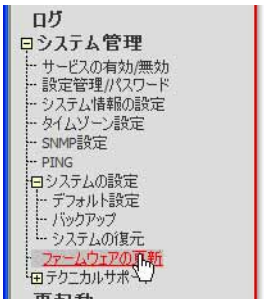
復元により IP アドレスが変更される場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、復元後の IP アドレスを指定して手動で本製品に再接続する必要があります。

6. 以上で完了です。

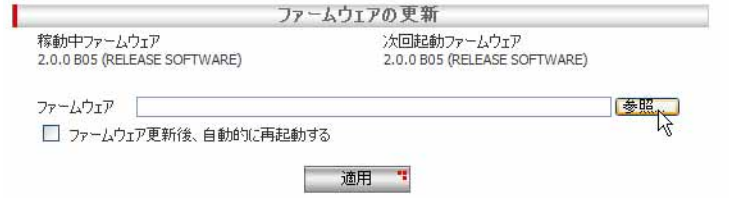
## 1.13　ファームウェアの更新

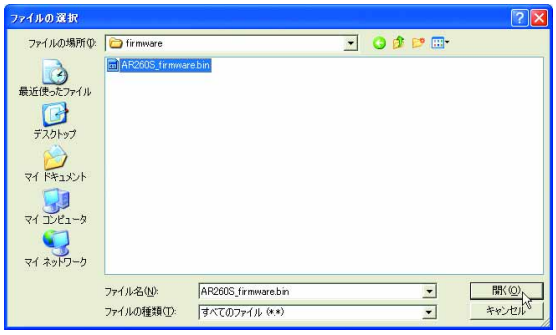
**「ファームウェアの更新」ページでは、本製品のファームウェアを新しいバージョンのファームウェアに更新することができます。**

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。



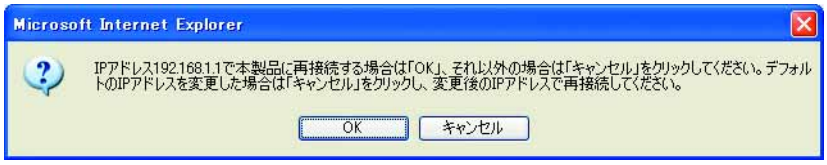




3.「適用」ボタンをクリックします。（ファームウェア更新後自動で再起動する場合は「ファームウェア更新後、自動的に再起動する」にチェックを入れます。）

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。**

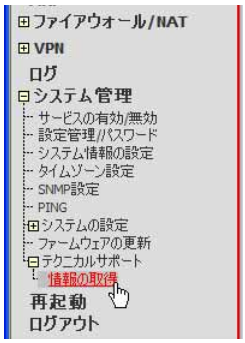
6. 以上で完了です。

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。**

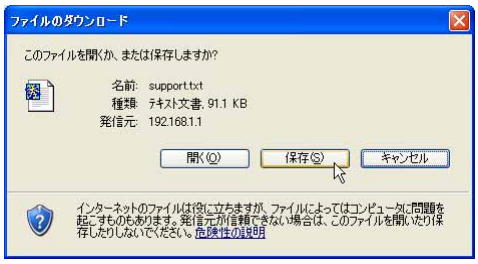
## 1.14　テクニカルサポート情報の取得

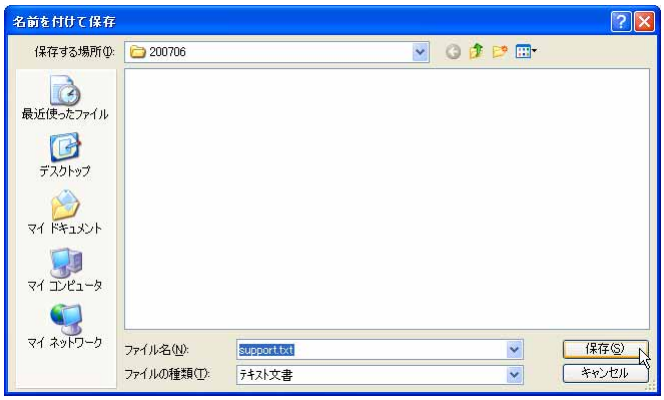
**「情報の取得」ページでは、本製品で発生した問題を解決するために必要な情報を取得します。（通常使用することはありません。）テクニカルサポート情報を保存するには、以下の手順を実行します。**

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

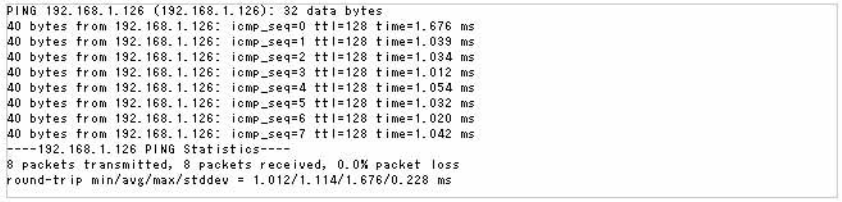
Ping の送信は、以下の手順で行います。

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 unrechable 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 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 DNS サーバー | | 192.168.1.10 |
| セカンダリ 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。 |
| 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DNS サーバー | | プライマリ 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DNS サーバー | | セカンダリ 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 WINS サーバー | | プライマリ 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WINS サーバー | | セカンダリ WINS サーバーの IP アドレスを入力します。入力は任意です。 |

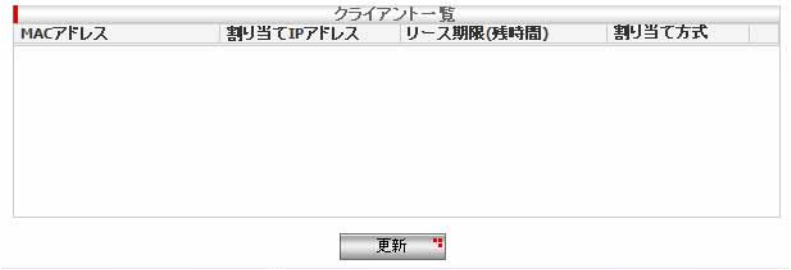
| | |
|---|---|
| 「適用」ボタン | 入力した内容を本製品の設定に適用します。ボタンをクリックすると設定内容が即時に反映されます。 |
| 「ヘルプ」ボタン | 操作のヒントを参照することができます。 |

### 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 |
| プライマリDNSサーバ | 192.168.1.1 |
| セカンダリDNSサーバ | |
| プライマリWINSサーバ | |
| セカンダリWINSサーバ | |

| **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。 |
| 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DNS サーバー | プライマリ DNS サーバーの IP アドレスが表示されます。 |
| セカンダリDNS サーバー | セカンダリ DNS サーバーの IP アドレスが表示されます。 |
| プライマリWINS サーバー | プライマリ WINS サーバーの IP アドレスが表示されます。 |
| セカンダリWINS サーバー | セカンダリ 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。 |
| 「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

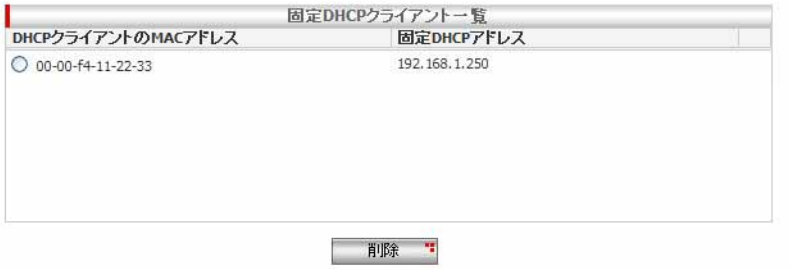
**「固定 DHCP クライアント」ページについて解説します。「固定 DHCP クライアント」ページでは、本製品の DHCP サーバー機能で固定的に IP アドレスを割り当てるクライアントを登録します。**

#### 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



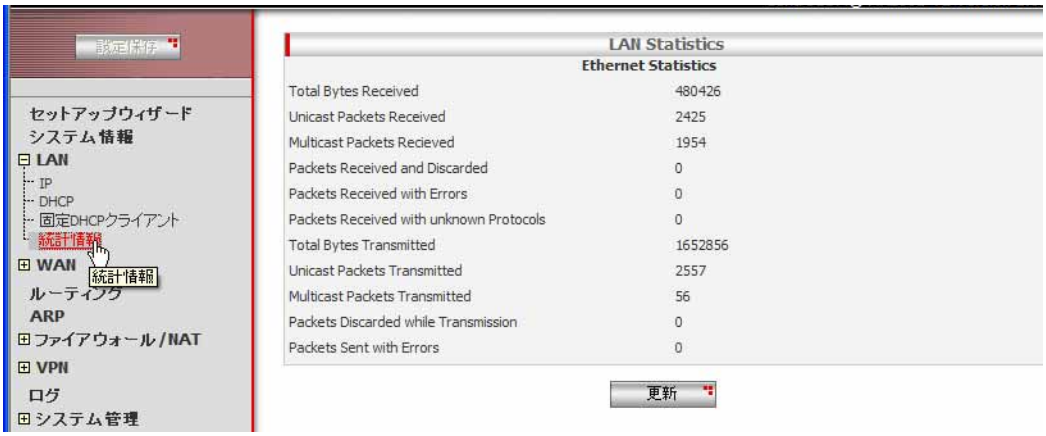

| パラメーター | 説明 |
|---|---|
| DHCP クライアントの MAC アドレス | IP アドレスが固定的に割り当てられているクライアントの MAC アドレスが表示されます。 |
| 固定 DHCP アドレス | クライアントに固定的に割り当てられている IP アドレスが表示されます。 |
| 「削除」ボタン | ラジオボタンで選択した登録項目を一覧から削除します。 |

## 2.5 トラフィックの確認

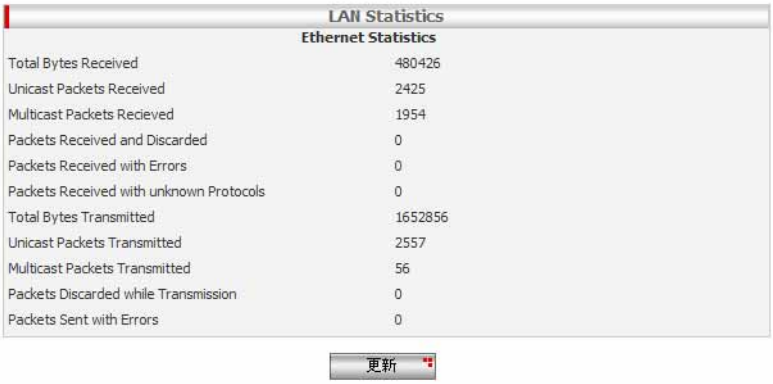
本製品では、LAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。LAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

### 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。



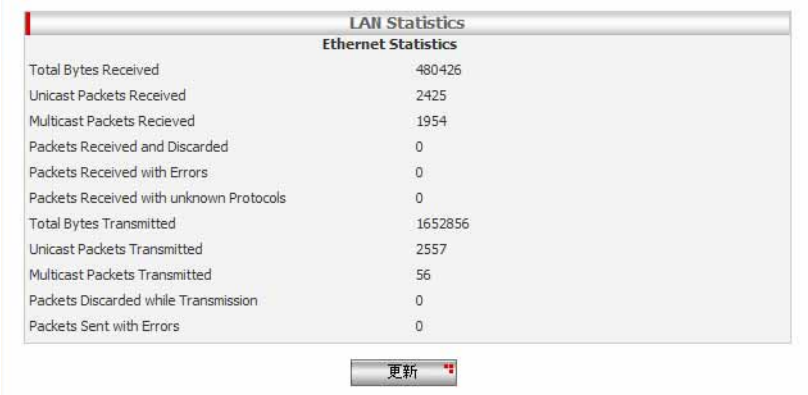

2.「LAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。



### 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。




| 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。 |

# 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
- WAN 側インターフェースのトラフィック確認

## 3.2　DHCP を使用した WAN 側ネットワークへの接続

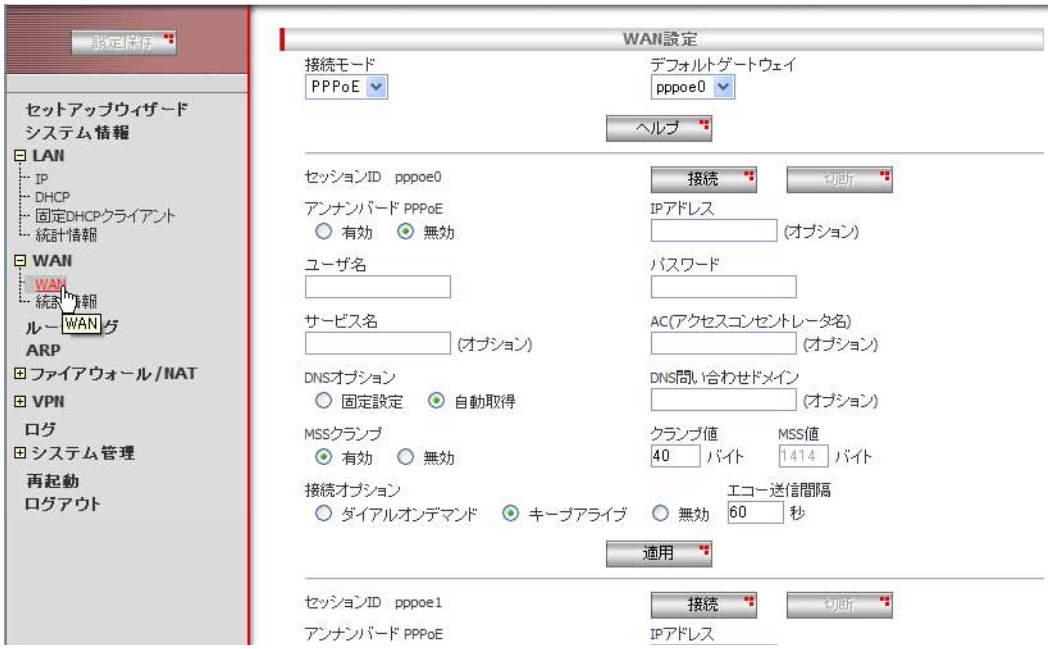
WAN 側インターフェースを DHCP で接続する場合の手順について説明します。おもに CATV のインターネット接続サービスなどで多く使用される接続形態です。

### 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。

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。

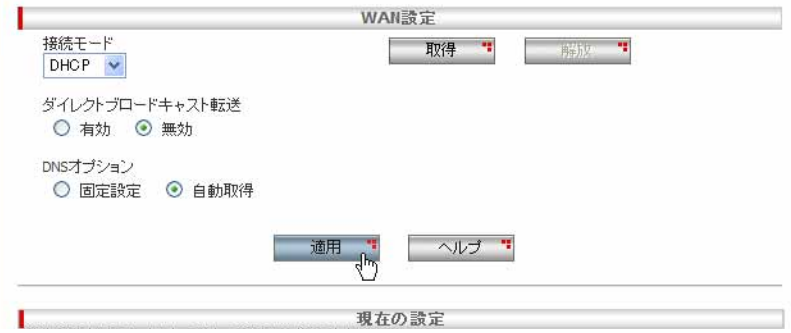
1. メニューから「WAN」->「WAN」の順にクリックします。



2. 接続モードに「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 |
| 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 | 192.168.1.125 |
| 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DNSサーバ | |
| セカンダリDNSサーバ | |
| 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 xDSL 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。

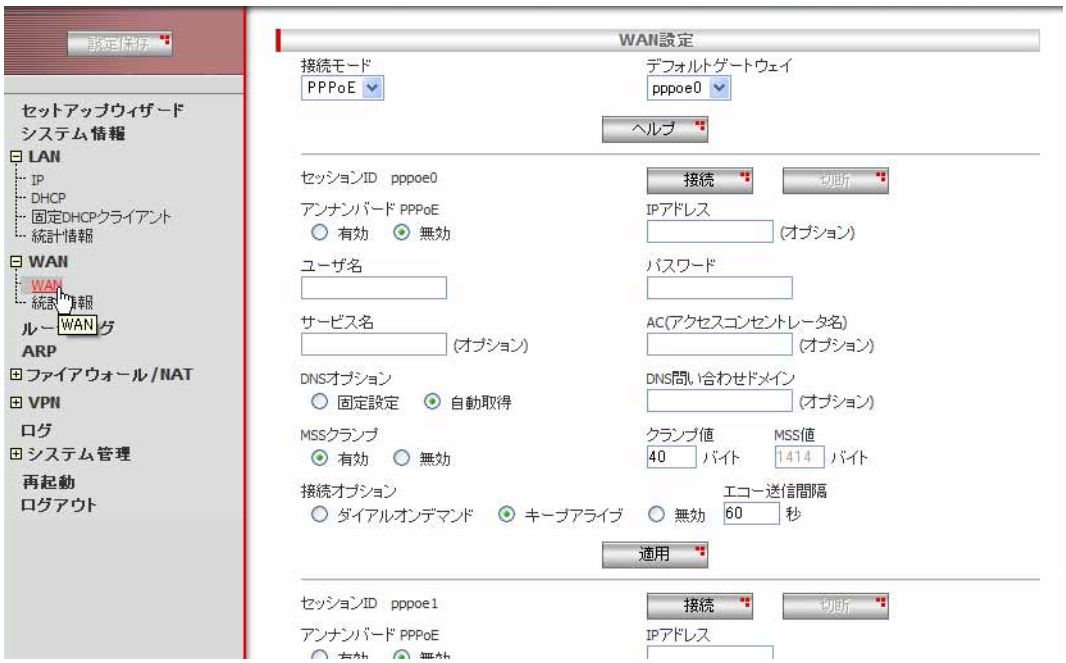
### 3.3.1 設定

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。

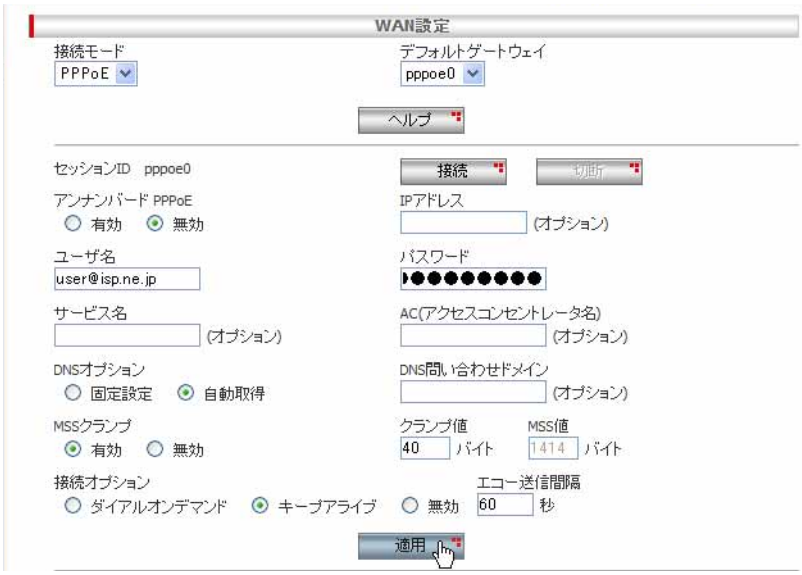
1. メニューから「WAN」->「WAN」の順にクリックします。




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。

| | |
|---|---|
| Unnumbered PPPoE | 無効 |
| 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） |
| DNS オプション | 自動取得 |
| MSS クランプ | 有効、40Bytes |
| 接続オプション | キープアライブ、エコー送信間隔 60 秒 |



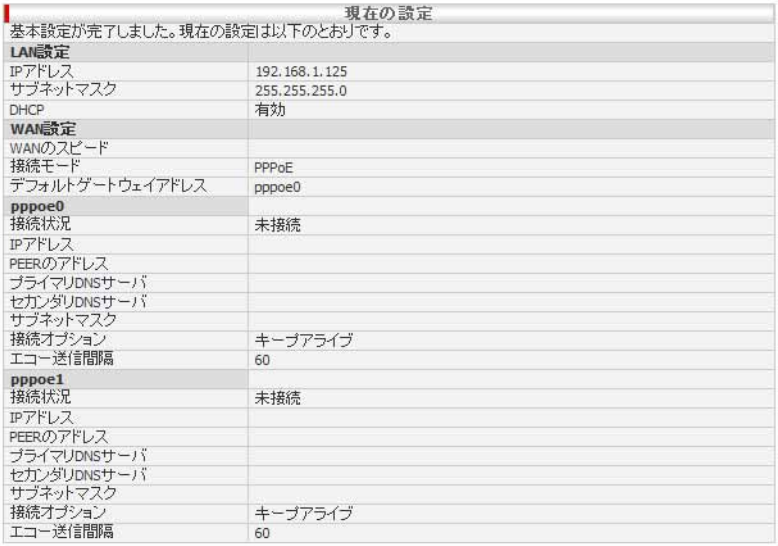

4. 以上で設定は完了です。

### 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 | 192.168.1.125 |
| 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** | |
| 接続状況 | 未接続 |
| IPアドレス | |
| PEERのアドレス | |
| プライマリDNSサーバ | |
| セカンダリDNSサーバ | |
| 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 |
| **pppoe1** | |
| 接続状況 | 未接続 |
| IPアドレス | |
| PEERのアドレス | |
| プライマリDNSサーバ | |
| セカンダリDNSサーバ | |
| 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 |

### 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。

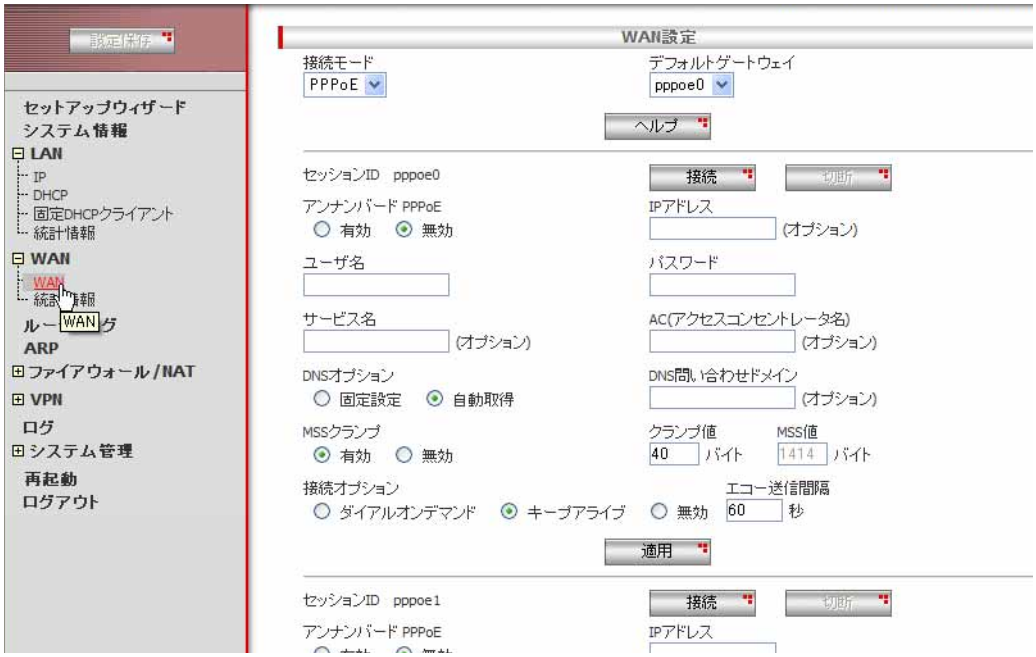
## 3.4 固定 IP アドレスを使用した WAN 側ネットワークへの接続

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 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。

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 | 固定IP |
| デフォルトゲートウェイアドレス | 200.100.10.1 |
| プライマリDNSサーバ | 200.100.10.32 |
| セカンダリDNSサーバ | |
| 接続状況 | 接続 |
| IPアドレス | 200.100.10.54 |
| サブネットマスク | 255.255.255.0 |

## 3.5 「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。

### 3.5.1 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。

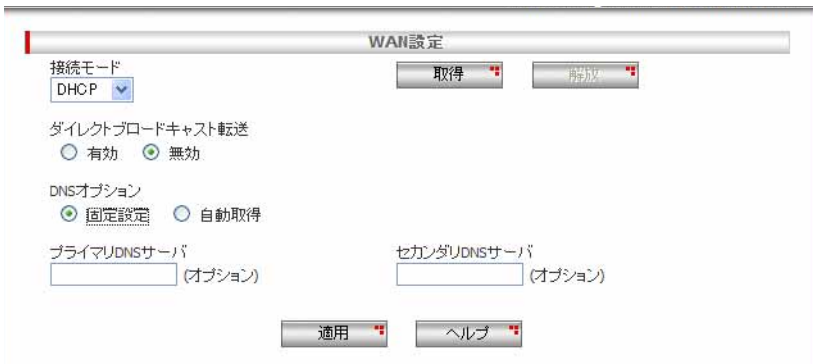

| パラメーター | 説明 |
|---|---|
| 接続モード | WAN ポートの接続モードを「DHCP」、「PPPoE」、「固定 IP」の 3 つのオプションから選択します。選択するオプションによって、設定画面に表示されるパラメーターが異なります。 |

ヒント

以降の説明は、各オプション別に記載します。

### 3.5.1.1 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。 |
| DNS オプション | 固定設定 / 自動取得 | プライマリ DNS サーバー、セカンダリ 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 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 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。 |

現在の設定

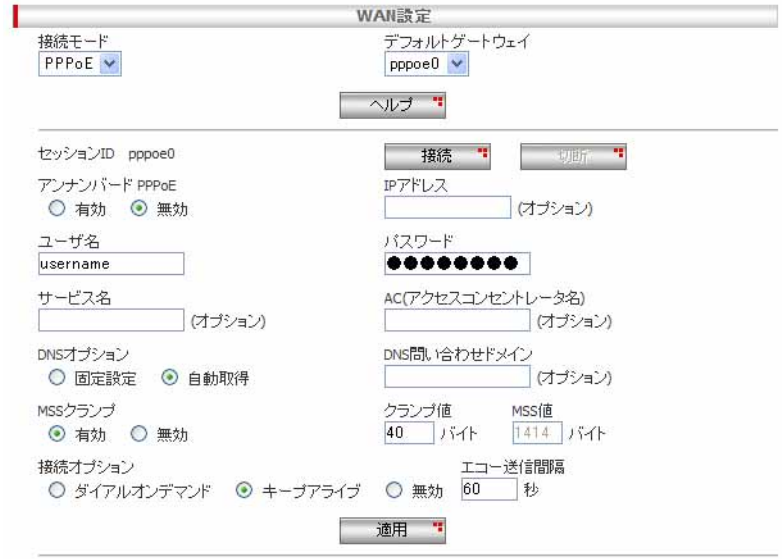
基本設定が完了しました。現在の設定は以下のとおりです。

| | |
|---|---|
| **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DNSサーバ | |
| セカンダリDNSサーバ | |
| 接続状況 | 未接続 |
| IPアドレス | |
| サブネットマスク | |

| 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 DNS サーバー | プライマリ DNS サーバーのアドレスが表示されます。 |
| | セカンダリ DNS サーバー | セカンダリ 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。 |

### 3.5.1.2 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。



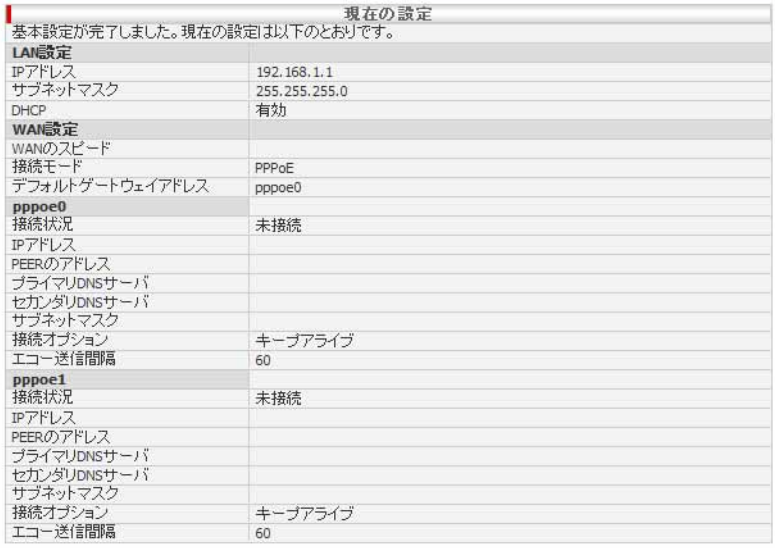

ヒント

ご契約の ISP が PPPoE をサポートしている場合に選択します。xDSL 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 |
|---|---|---|
| デフォルトゲートウェイ | | デフォルトゲートウェイを選択します。 |
| | pppoe0 | pppoe0 のゲートウェイをデフォルトゲートウェイに設定する場合に選択します。 |
| | pppoe1 | pppoe1 のゲートウェイをデフォルトゲートウェイに設定する場合に選択します。 |
| セッション ID | | 本製品では、PPPoE を最大 2 セッション登録することができます。pppoe0 と pppoe1 というセッション名で区別されます。<br>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。 |
| 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。 |

| | | | |
|---|---|---|---|
| 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。半角英数字で 1 ～ 64 文字で入力してください。 |
| 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。半角英数字で 1 ～ 32 文字で入力してください。 |
| 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 DNS サーバー、セカンダリ 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 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 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。 |
| MSS クランプ | 有効 / 無効 | | MSS の値を設定する場合は「有効」、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 クランプを有効に設定した場合、クランプ値も設定します。初期状態は、40 バイトです。設定可能な範囲は、0 ～ 942 バイトです。（単位：バイト） |
| 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。<br>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。 |
| 「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。 |



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** | |
| 接続状況 | 未接続 |
| IPアドレス | |
| PEERのアドレス | |
| プライマリDNSサーバ | |
| セカンダリDNSサーバ | |
| 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 |
| **pppoe1** | |
| 接続状況 | 未接続 |
| IPアドレス | |
| PEERのアドレス | |
| プライマリDNSサーバ | |
| セカンダリDNSサーバ | |
| 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 |

| **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。 |
| 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 DNS サーバー | プライマリ DNS サーバーのアドレスが表示されます。 |
| セカンダリ DNS サーバー | セカンダリ 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。 |

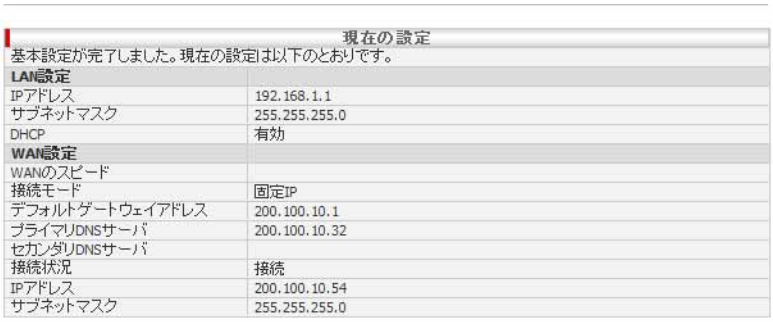
### 3.5.1.3 接続モードに「固定 IP」を選択した場合

**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 / セカンダリ DNS サーバー | | ISP から提供されたプライマリ / セカンダリ 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。 |



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 | 固定IP |
| デフォルトゲートウェイアドレス | 200.100.10.1 |
| プライマリDNSサーバ | 200.100.10.32 |
| セカンダリDNSサーバ | |
| 接続状況 | 接続 |
| IPアドレス | 200.100.10.54 |
| サブネットマスク | 255.255.255.0 |

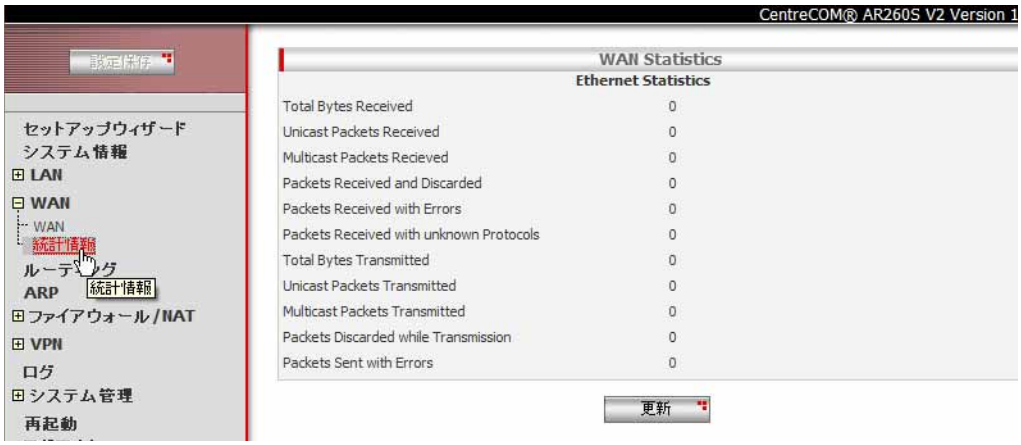
| パラメーター | オプション | 説明 |
|---|---|---|
| LAN 設定 | | 本製品の LAN 側インターフェースに関する情報が表示されます。 |
| | IP アドレス | 現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。 |
| | サブネットマスク | 現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。 |
| | DHCP | DHCP サーバー機能の有効 / 無効が表示されます。 |
| WAN 設定 | | 本製品の WAN 側インターフェースに関する情報が表示されます。 |
| | 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 DNS サーバー | プライマリ DNS サーバーのアドレスが表示されます。 |
| | セカンダリ DNS サーバー | セカンダリ 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 トラフィックの確認

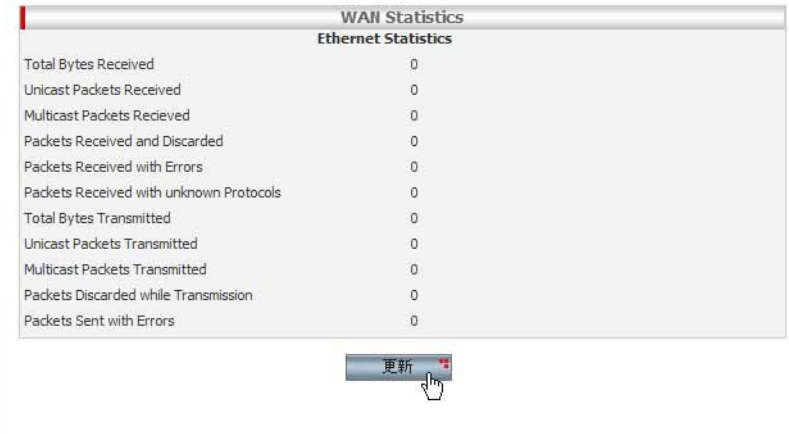
本製品では、WAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。WAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

### 3.6.1 確認

1. メニューから「WAN」->「統計情報」をクリックします。



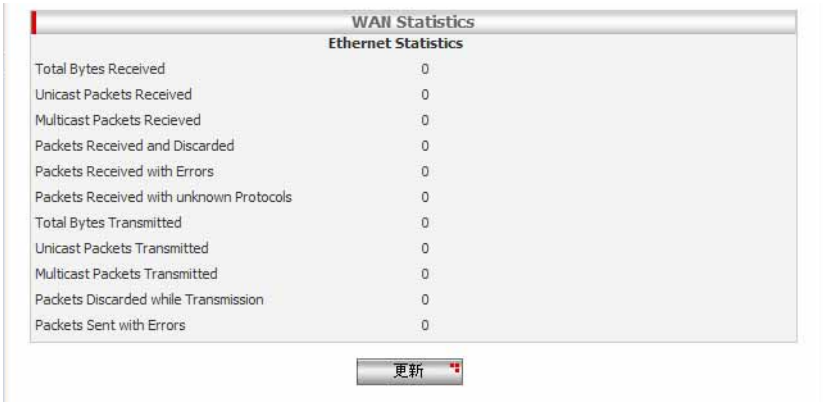

2.「WAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。



### 3.6.2 「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。**

メニューから「WAN」->「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。




| 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。 |

# 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 |
| 宛先ネットマスク | | 255.255.255.0 |
| ゲートウェイ | アドレス | 192.168.3.1 |


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。 |
| 宛先ネットマスク | | 宛先ホスト、またはネットワークのネットマスクを入力します。 |
| ゲートウェイ | | 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、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。 |
| 「追加」ボタン | | ルーティングを追加登録します。15 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。 |

# 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。

- Inbound/Outbound 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

## 5.2　Inbound/Outbound アクセス制御の設定

Inbound/Outbound 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。Inbound/Outbound アクセス制御は「ファイアウォール /NAT」->「ファイアウォール」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

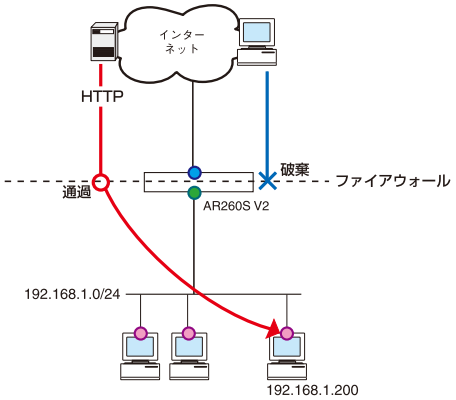
デフォルトのルールの優先度を変更したり、他に Outbound アクセスルールを追加した場合、インターネットへの通信ができなくなることもありますので、ルールを追加する場合は正確に設定してください。

### 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」->「ファイアウォール」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、「Inbound/Outbound 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. 117 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」->「ファイアウォール」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」->「ファイアウォール」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」->「ファイアウォール」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 「ファイアウォール」ページの解説

**「ファイアウォール」ページについて解説します。「ファイアウォール」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 Inbound/Outbound アクセス制御設定

メニューから「ファイアウォール /NAT」->「ファイアウォール」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 |
|---|---|---|
| Inbound/Outbound 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。 |
| | | サブネット | 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アドレスを入力します。 |
| | | 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。 |
| | | サブネット | 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アドレスを入力します。 |
| | | 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.110 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 |

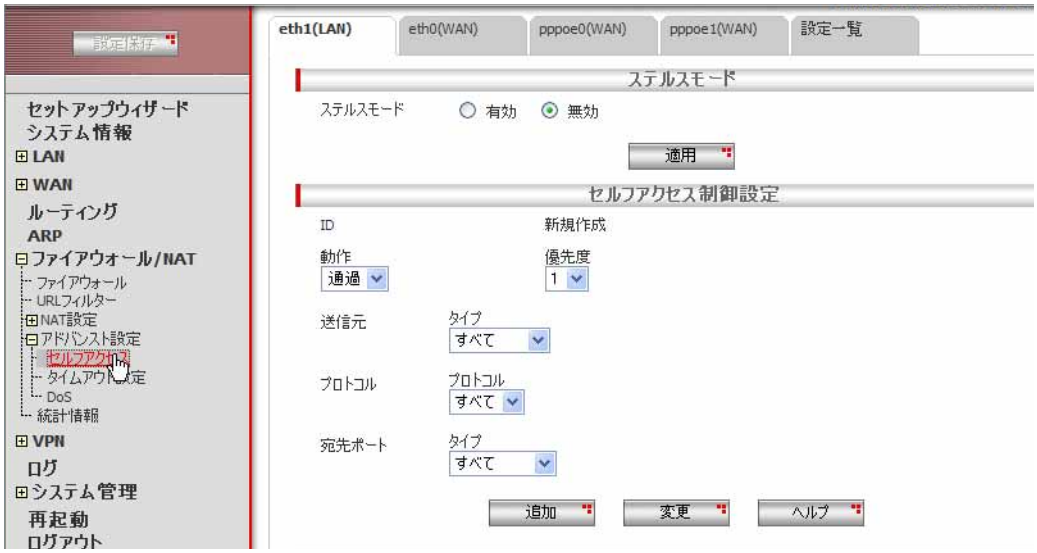

デフォルトのルールを削除、変更しないでください。削除や変更をおこなった場合、正常な通信ができなくなる場合があります。


TCP の 80 番ポートは本製品を設定する際に使用します。また、TCP の 10081 番ポートはファームウェアの更新をおこなう際に使用します。

## 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。


eth1(LAN)
eth0(WAN)
pppoe0(WAN)
pppoe1(WAN)
設定一覧
絞り込み
インターフェース
すべて
適用
ヘルプ
セルフアクセス 制御リスト
I/F
送信元
サービス
動作
eth0 すべて UDP,500 通過
pppoe0 すべて UDP,500 通過
pppoe1 すべて UDP,500 通過

### 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。 |
| | | サブネット | サブネットアドレスを入力します。 |
| | | 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毎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. 172 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.172 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、サブネット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。 |
| | | | アドレス : 送信元 IP アドレスを入力します。 |
| | | | 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。 |
| | | | アドレス : 宛先 IP アドレスを入力します。 |
| | | | 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「NAT プール」を参照して下さい。 |
| 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。<br><br>アドレス : 送信元 IP アドレスを入力します。<br><br>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。<br><br>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。<br><br>アドレス : 宛先 IP アドレスを入力します。<br><br>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」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。<br><br>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。<br><br>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。<br><br>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。 |
| | | 送信元 IP アドレス | 送信元 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。 |
| 「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。 |

### 5.5.4.2 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

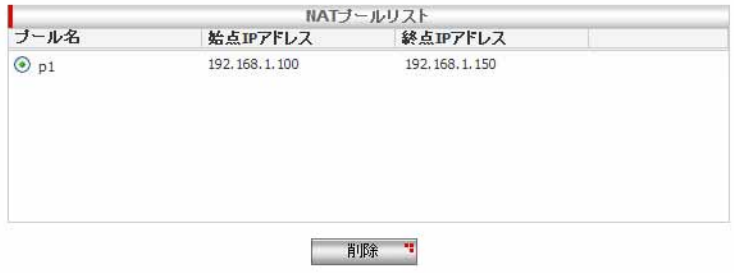
新規に NAT プールを追加する場合は、以下の手順を実行します。

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。

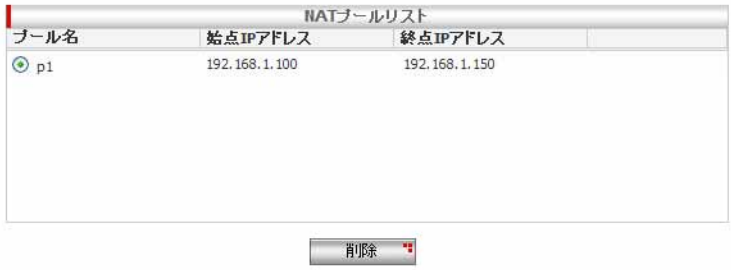
#### 5.6.4.1 NAT プール設定

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」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 秒です。（単位：秒） |
| 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」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。）**

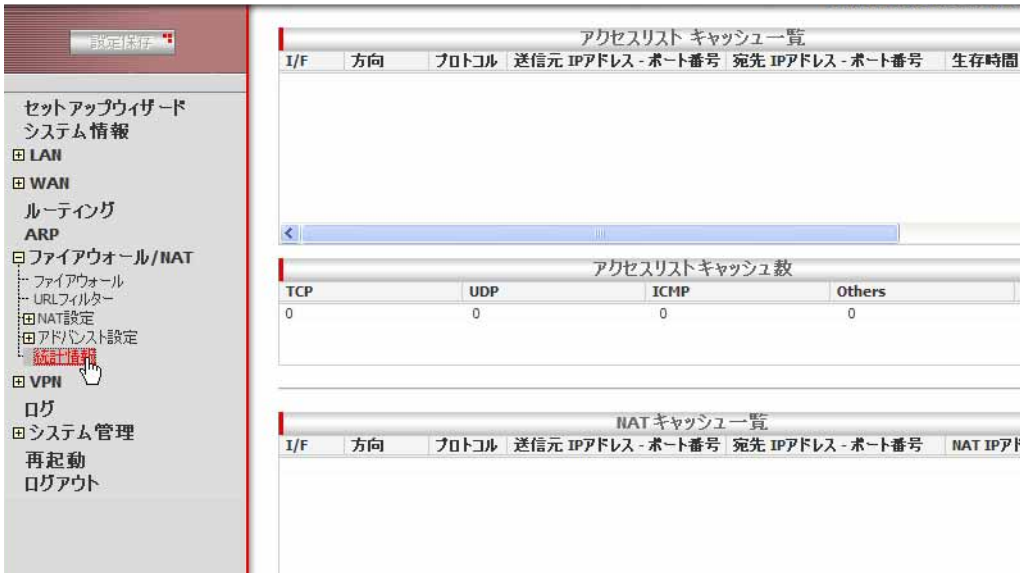
## 5.8 トラフィックの確認

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。

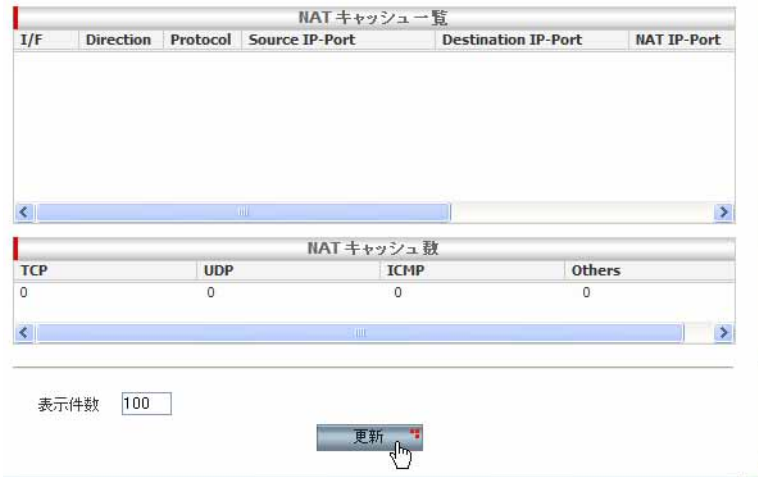
### 5.8.1 確認

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。「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。 |
| Direction | 通信の方向が表示されます。 |
| Protocol | 通信プロトコルが表示されます。 |
| Source IP-Port | 送信元の IP アドレスとポート番号が表示されます。 |
| Destination IP-Port | 宛先の IP アドレスとポート番号が表示されます。 |
| Life(Secs) | 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。 |
| Bytes Out | 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。 |
| Bytes In | 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。 |

### 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。 |
| Direction | 通信の方向が表示されます。 |
| Protocol | 通信プロトコルが表示されます。 |
| Source IP-Port | 送信元の IP アドレスとポート番号が表示されます。 |
| Destination IP-Port | 宛先の IP アドレスとポート番号が表示されます。 |
| NAT IP-Port | 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。 |
| Life(Secs) | 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。 |
| Bytes Out | 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。 |
| Bytes In | 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。 |

### 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

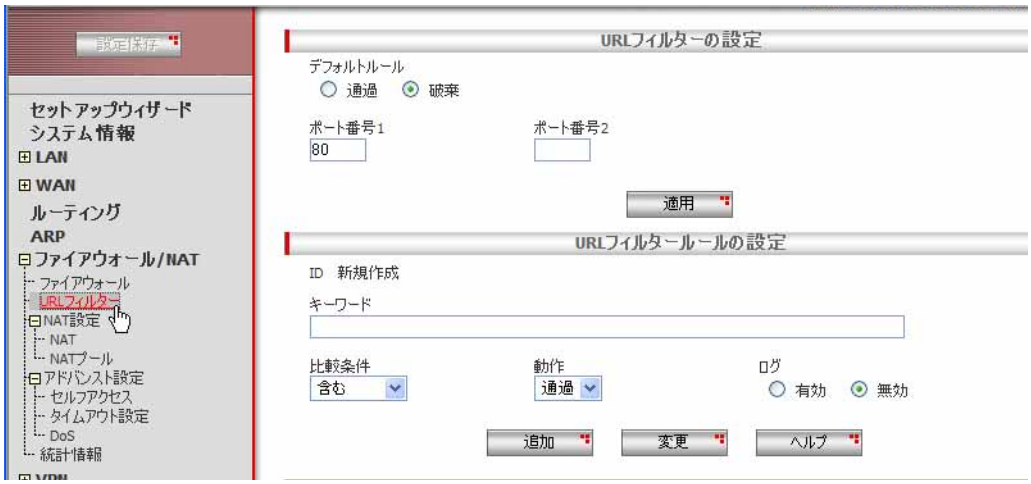
URL フィルターを使用すると、HTTP 経由でアクセスする URL の合否を判定し、アクセス可能な URL かどうかを制御することができます。

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。**

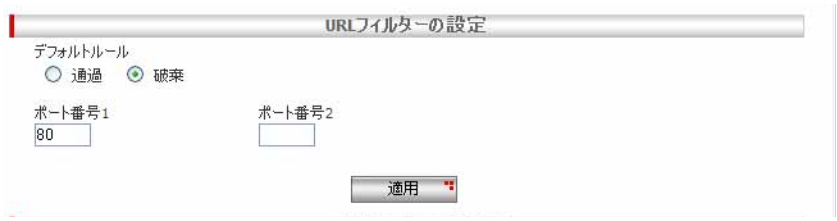
1. メニューから「ファイアウォール /NAT」->「URL フィルター」の順にクリックします。
2. 「URL フィルターリスト」テーブルの該当ルール左部にあるラジオボタンをクリックします。
3. 「削除」ボタンをクリックします。
4. 以上で設定は完了です。

### 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。<br>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。 |
| | 全て対象 | 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。<br>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 / 全て対象）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

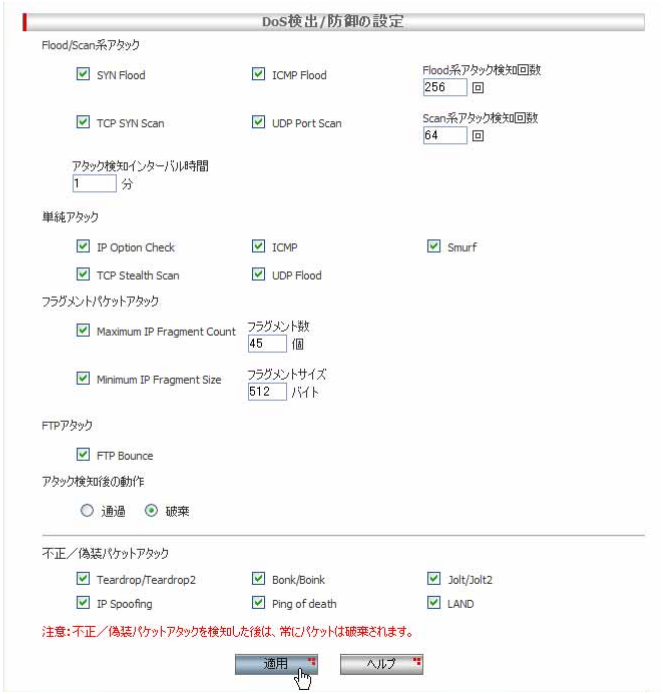
DoS 検出 / 防御の設定を行うには、以下の手順を実行します。

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。

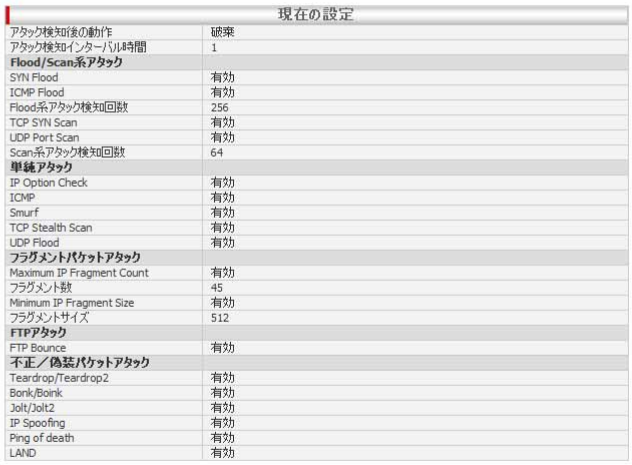

2.「DoS 検出 / 防御の設定」の各パラメーターを設定し「適用」ボタンをクリックします。ここでは以下の内容を設定するものとします。

| | | |
|---|---|---|
| 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。

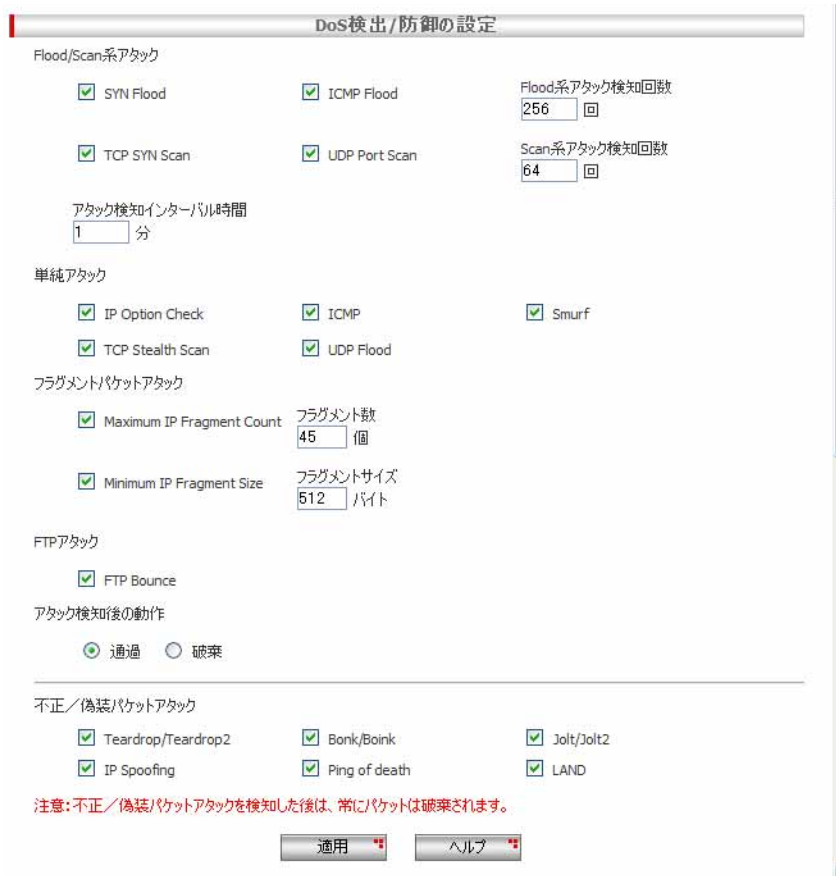


## 5.10.2 「DoS」ページの解説

「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及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。 |

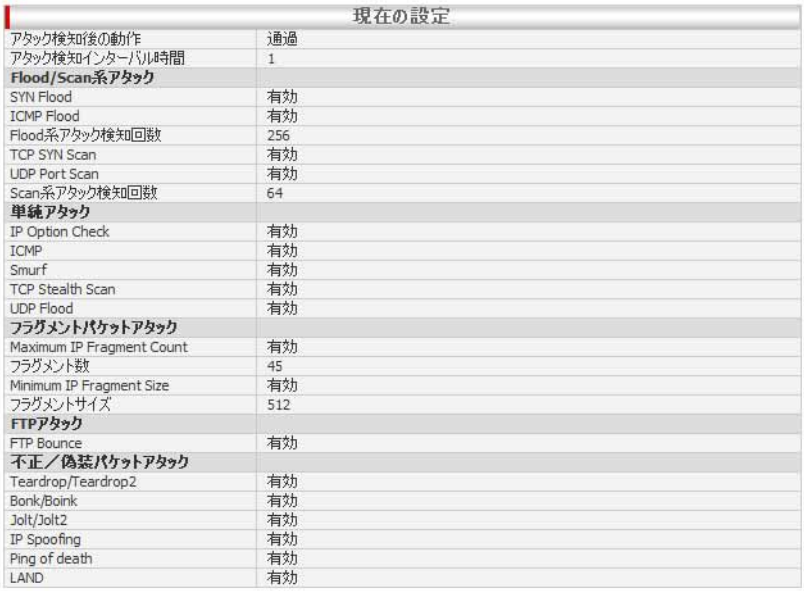
| | | |
|---|---|---|
| | TCP SYN Scan | TCP/SYN パケットにおいて、過去の送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号リストと比較一致し、ある時間内に規定回数に達した場合に、検知します。 |
| | UDP Port Scan | UDP パケットにおいて、過去の送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号リストと比較し、送信元 IP アドレス、宛先 IP アドレスが一致し、宛先ポート番号が一致しない場合で、ある時間内に規定回数に達した場合に、検知します。 |
| | Scan 系アタック検知回数 | Scan 系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」及び「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。<br>・TCP 制御フラグに何もセットされていない<br>・TCP 制御フラグに FIN/URG/PUSH のみがセットされている<br>・TCP 制御フラグに FIN のみがセットされている<br>・TCP 制御フラグに SYN/FIN のみがセットされている<br>・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。<br>・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<br>・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。<br>「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 | 既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 ヘッダ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。<br>・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<br>・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<br>・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」及び「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） |

# 6 VPN の設定

## 6.1 概要

VPN（Virtual Private Network）は、ネットワーク間に仮想的なトンネルを構築し、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

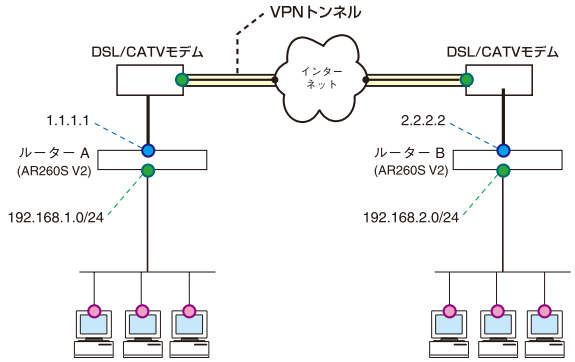
VPN トンネルでネットワーク間を接続するなど、VPN ゲートウェイ間で接続する場合に使用します。

### 6.2.1 ポリシーの作成

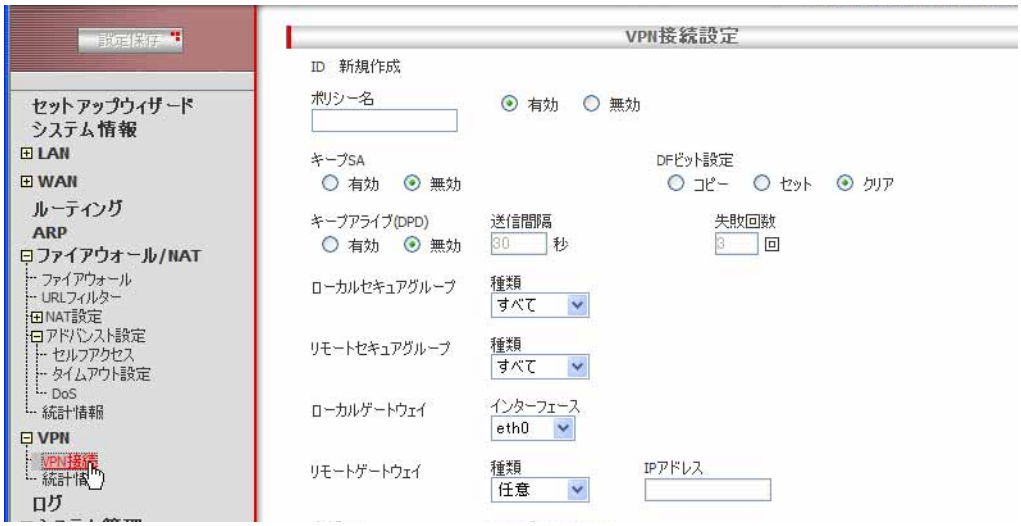
ポリシーを作成するには以下の手順を実行します。

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**

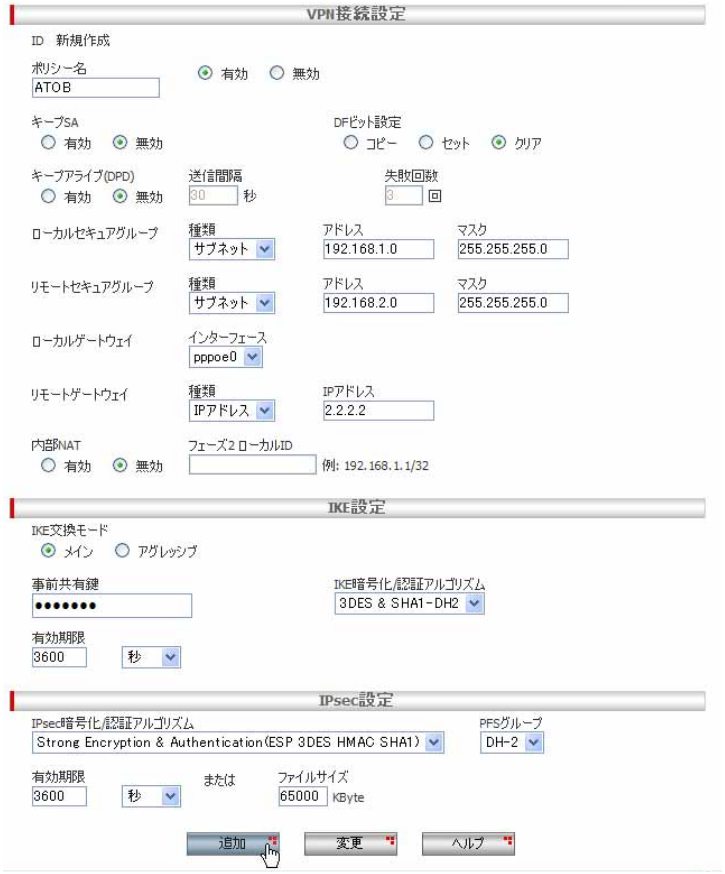
| | | |
|---|---|---|
| ポリシー名 | | ATOB |
| | 有効 / 無効 | 有効 |
| キープ SA | | 無効 |
| DF ビット設定 | | クリア |
| キープアライブ（DPD） | | 無効 |
| ローカルセキュアグループ | 種類 | サブネット |
| | アドレス | 192.168.1.0 |
| | マスク | 255.255.255.0 |
| リモートセキュアグループ | 種類 | サブネット |
| | アドレス | 192.168.2.0 |
| | マスク | 255.255.255.0 |
| ローカルゲートウェイ | 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 |
| 内部 NAT | | 無効 |

**IKE 設定**

| | |
|---|---|
| IKE 交換モード | メイン |
| 事前共有鍵 | atobkey |
| IKE 暗号化 / 認証アルゴリズム | 3DES & SHA1-DH2 |
| 有効期限 | 3600 秒 |

**IPsec 設定**

| | |
|---|---|
| IPsec 暗号化 / 認証アルゴリズム | Strong Encryption & Authentication (ESP 3DES HMAC SHA1) |
| PFS グループ | DH-2 |
| 有効期限 | 3600 秒 /65000KByte |




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.99 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 |
| | | アドレス | 192.168.1.0 |
| | | マスク | 255.255.255.0 |
| 宛先 | | タイプ | サブネット |
| | | アドレス | 192.168.2.0 |
| | | 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 |
| | | アドレス | 192.168.2.0 |
| | | マスク | 255.255.255.0 |
| 宛先 | | タイプ | サブネット |
| | | アドレス | 192.168.1.0 |
| | | 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 |
|---|---|---|---|
| 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 (DPD) | | | DPD プロトコルによる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。DPD はプロトコル仕様上、対向機器でも DPD を有効にしないと動作しません。 |
| | | 送信間隔 | 対向機器からの IPsec 通信がなく、かつ対向機器からキープアライブパケットが到達しない状態がこの時間だけ続くとキープアライブによる送達確認をおこないます。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 回～ 64 回です。 |
| 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。<br>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。<br>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。<br>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ネットマスクにより設定します。 |
| | | 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。 |
| | | マスク | 上記ネットワークアドレスに対応する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。 |
| | | 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サブネットアドレスを入力します。 |
| | | 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。<br>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。<br>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。 |
| | フェーズ 2 ローカル 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で矛盾が発生します。これを解消するための ID 設定を行います。<br>フェーズ 2 ローカル 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。 |

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

### 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 ～ 65536 キロバイトです。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。 |
| IPsecモード | IPsec の動作モードが表示されます。 |
| 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 |
|---|---|
| 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。 |

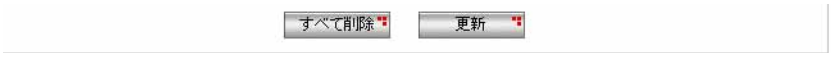
#### 6.3.2.2 SA - IPsec SA

「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。 |
| 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。 |

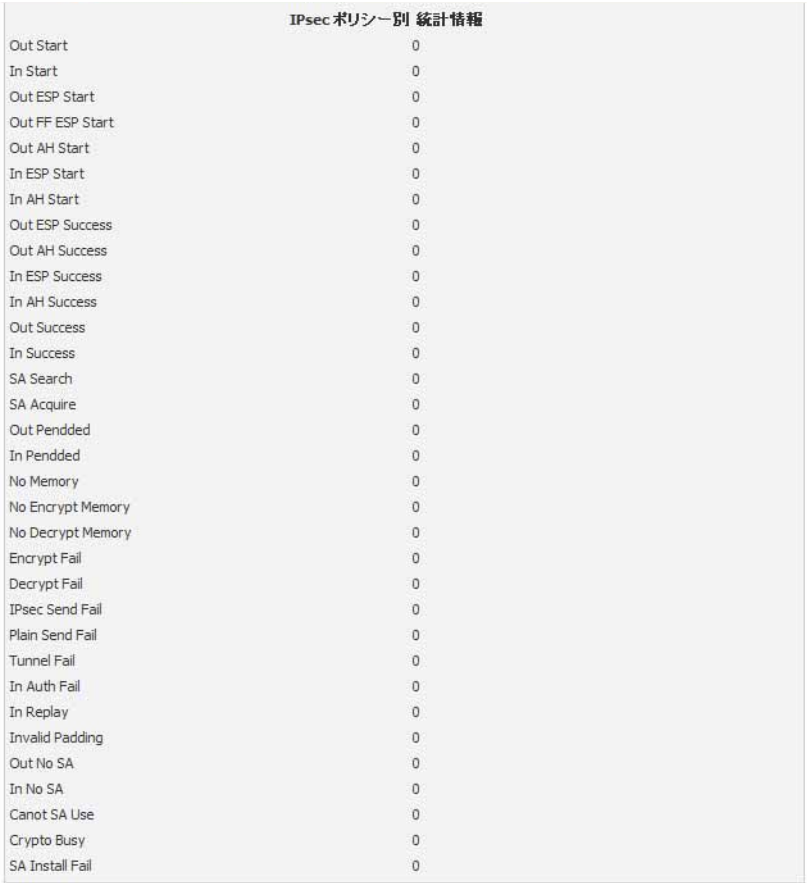
### 6.3.2.5 詳細統計情報

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<br>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 |
| | プライマリ DNS サーバー | 192.168.1.1 |
| | セカンダリ DNS サーバー | 空白（未設定） |
| | プライマリ WINS サーバー | 空白（未設定） |
| | セカンダリ 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 | 有効 |

| | | | |
|---|---|---|---|
| | 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 | |
| **「ルーティング」** | | | |
| | 宛先ネットワークアドレス | 192.168.1.1 | |
| | 宛先ネットマスク | 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」/「ファイアウォール」** | | | |
| | Inbound アクセス | 設定無し（遮断） | |
| | Outbound アクセス | すべて透過 | |
| **「ファイアウォール /NAT」/「NAT 設定」/「NAT」** | | | |
| | pppoe1、pppoe2 | インターフェース ENAT<br>（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）<br>WAN（eth0、pppoe0、pppoe1） | 設定無し<br>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 600 秒、DefaultUdp 60 秒、<br>DefaultIcmp 60 秒、TcpRest 20 秒 | |
| **「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、<br>ETH：通知、NAT：通知、ファイアウォール：通知、<br>システム：通知、アプリケーション：通知 | |

| | | |
|---|---|---|
| | ログサーバ 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<br>セルフアクセス、Inbound/Outbound アクセス制御、NAT 、DoS：有効<br>URL フィルター：無効 |
| | VPN | 有効<br>SA の強制確立：無効 |
| | DNS リレー | 有効 |
| | DHCP | 有効 |
| | SNTP | 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 |

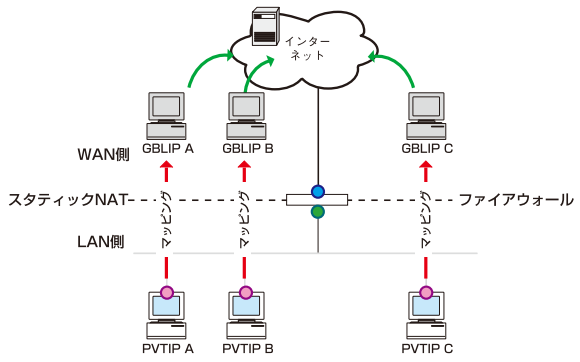
| | |
|---|---|
| 通知先アドレス（トラップホスト） | 空白（未設定） |
| トラップ送信元 IP アドレス | 自動選択 |

## 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 を使用することができます。

### 7.2.1 スタティック NAT

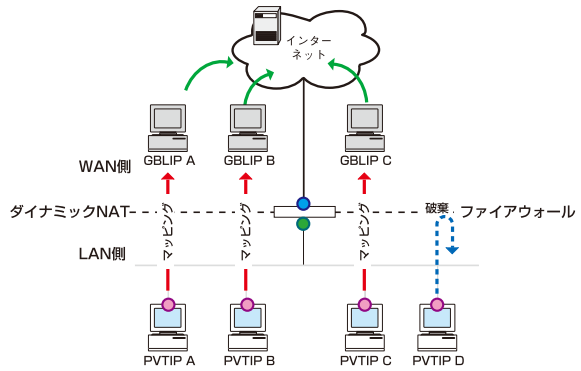
スタティック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で固定的にマッピングします。管理者が意図的に変更しない限りマッピングは固定的に行われます。つまり、1 台のクライアントのプライベート IP アドレスに対して、常に同じグローバル IP アドレスがマッピングされます。グローバル IP アドレスはプライベート IP アドレスと同じ数必要です。




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

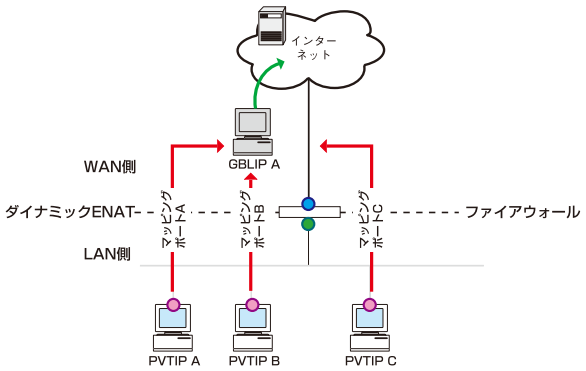
ダイナミック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で動的にマッピングします。動的にマッピングするため、グローバル IP アドレスとプライベート IP アドレスの数は同じである必要はありませんが、使用できるグローバル IP アドレスがない場合、クライアントの送出したパケットは破棄されます。




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

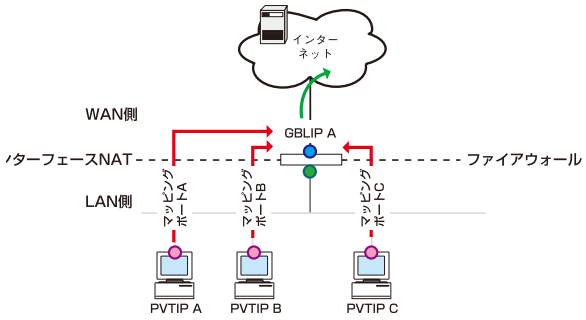
NAPT(Network Address and Port Translation)、または IP マスカレードとも呼ばれます。ENAT では、複数のプライベート IP アドレスに 1 つのグローバル IP アドレスと複数のポートをマッピングします。グローバル IP アドレスが 1 つのみの場合でも、異なるポートを使用して複数のクライアントからインターネットに接続することができます。




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 60 秒以上経過していますか？本製品の起動には 60 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」でログインすることができます。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。


「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おこなえません。


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 ですか？本製品でサポートする Web ブラウザーは Internet Explorer 6 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。

# 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