VPNルーター

CentreCOM® AR260S

リファレンスマニュアル

Allied Telesis

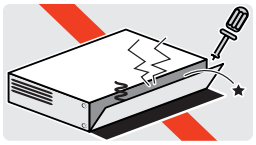
安全のために

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。

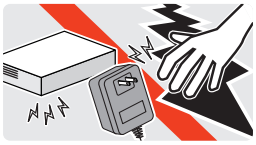
分解や改造をしない

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。

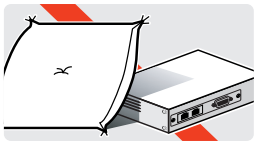


異物は入れない　水は禁物

火災や感電の恐れがあります。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。

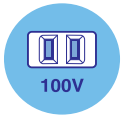


湿気やほこりの多いところ、油煙や湯気のあたる場所には置かない

内部回路のショートの原因になり、火災や感電の恐れがあります。

表示以外の電圧では使用しない

本製品に付属の AC アダプターは 100V で動作します。



付属の AC アダプター以外で使用しない

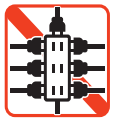
火災や感電の原因となります。
必ず、付属の AC アダプターを使用してください。

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。

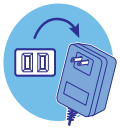
コンセントや配線器具の定格を超える使い方はしない

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・移動のときは電源プラグを抜く

感電の原因となります。



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（湿度80%以下の環境でご使用ください）
- 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。
部品が静電破壊する恐れがありますので、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下さい。

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、堅く絞ったものでふき、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・みがき粉・シンナー・ベンジン・ワックス・熱湯・粉せっけん
（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 をお買い上げいただき、誠にありがとうございます。

CentreCOM AR260S 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 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 / ログオフ
- 再起動
- 設定内容の初期化 / バックアップ / 復元
- ファームウェアの更新
- 設定管理クライアント / パスワードの設定
- SNMP エージェントの設定
- システム情報の設定
- システム情報の確認
- システム時刻 /SNTP サーバーの設定
- ファイアウォール、VPN など各機能の有効化 / 無効化
- ログの記録

「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 ファイアウォールの設定」では

ファイアウォール機能に関する設定について説明します。本製品のファイアウォール機能は大きくわけて以下の 6 つになります。

- Inbound アクセス
- Outbound アクセス
- ステルスモード
- セルフアクセス
- URL フィルター
- DoS アタックプロテクト

「6 各種ポリシーとサービスの設定」では

「5 ファイアウォールの設定」で使用する各種ポリシー（IP プール、NAT プール）とサービスに関する設定について説明します。

「7 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。

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。

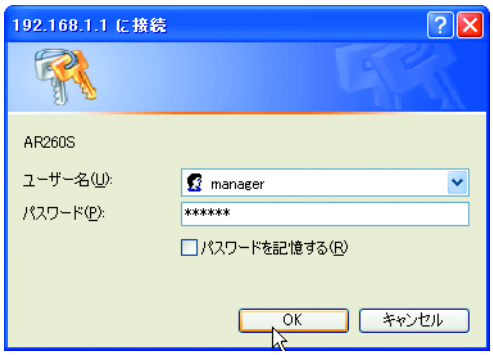
- ログイン
- 再起動
- ログアウト
- 機能の有効化 / 無効化
- 設定管理クライアント / パスワードの設定
- システム情報の設定
- システム時刻の設定
- SNMP エージェントの設定
- 設定の初期化
- 設定内容のバックアップ
- 設定内容の復元
- ファームウェアの更新
- ログの記録
- システム情報の確認

1.1　ログイン

本製品にログインするには以下の手順を実行します。

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

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



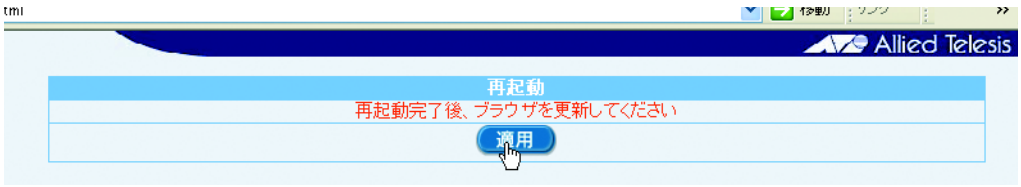
3. 本製品の設定画面が表示されたらログインは完了です。

1.2 再起動

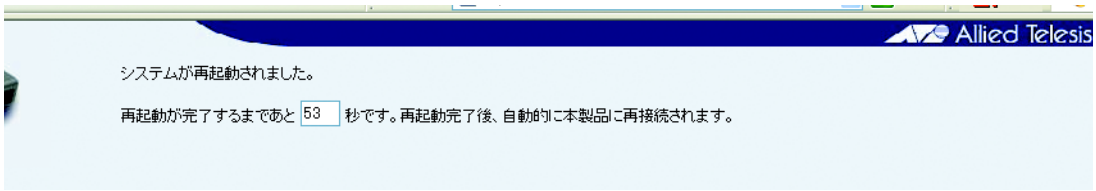
本製品を再起動するには以下の手順を実行します。

1. メニューから「再起動」をクリックします。

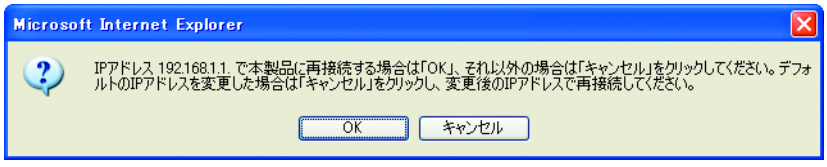
2.「適用」ボタンをクリックします。



3. 以下の画面が表示され、再起動に必要な時間がカウントダウンされます。カウントダウン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。



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。

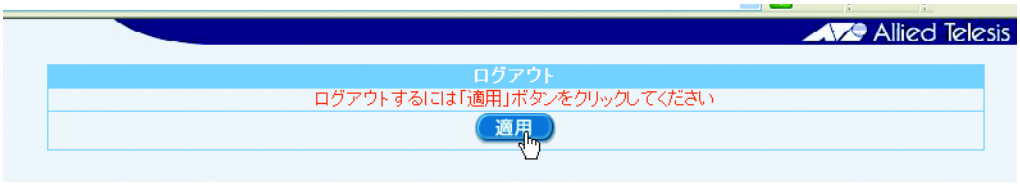
5. 以上で再起動は完了です。

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
- 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

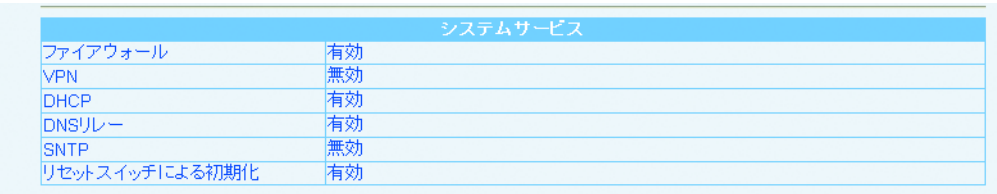
3. 以上で設定は完了です。

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。

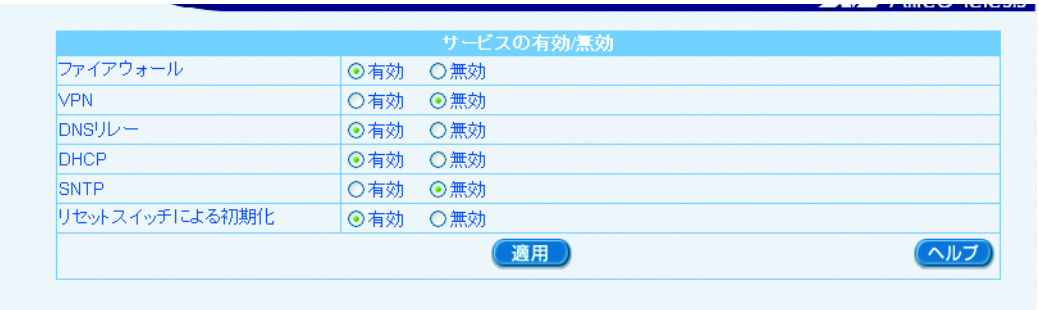


システムサービス	
ファイアウォール	有効
VPN	無効
DHCP	有効
DNSリレー	有効
SNTP	無効
リセットスイッチによる初期化	有効

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。



サービスの有効/無効		
ファイアウォール	◉有効	○無効
VPN	○有効	◉無効
DNSリレー	◉有効	○無効
DHCP	◉有効	○無効
SNTP	○有効	◉無効
リセットスイッチによる初期化	◉有効	○無効
	適用	ヘルプ

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.93 ファイアウォールの設定」を参照してください。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.145 VPN の設定」の設定を行う場合は、あらかじめ VPN サービスを有効にしてください。デフォルトは「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.56

		DHCP サーバーの設定」を参照してください。デフォルトは「有効」です。
SNTP	有効 / 無効	外部 SNTP サーバーから時刻情報を取得する場合は「有効」、取得しない場合は「無効」ラジオボタンをクリックします。SNTP サーバーの詳細については「P.33 システム時刻の設定」を参照してください。デフォルトは「無効」です。
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」、リブートのみ行う場合は「無効」ラジオボタンを選択します。デフォルトは「有効」です。「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。

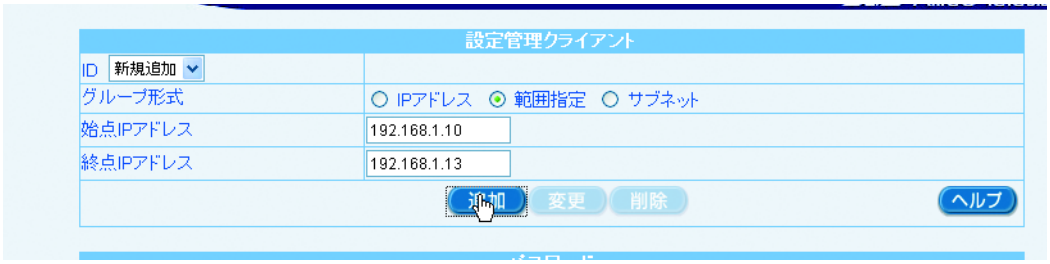
ヒント 設定管理クライアントを設定した場合、設定されたクライアント以外からは本製品の設定ができませんのでご注意ください。

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」テーブルの ID ドロップダウンリストから「新規追加」を選択します。

3. 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	範囲指定
始点 IP アドレス	192.168.1.10
終点 IP アドレス	192.168.1.13



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

4. 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。

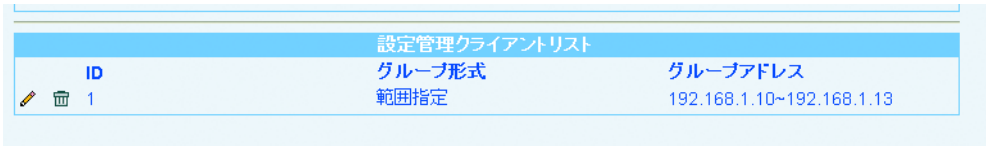
1. メニューから「システム管理」->「設定管理 / パスワード」の順にクリックします。
2. ID ドロップダウンリストから変更するクライアントの ID を選択します。または、「設定管理クライアントリスト」テーブルの該当クライアント左部にある「えんぴつ」アイコンをクリックします。
3. 各パラメーターを変更します。
4. 「変更」ボタンをクリックします。
5. 以上で設定は完了です。

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. ID ドロップダウンリストから削除するクライアントの ID を選択し「削除」ボタンをクリックします。または、「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「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

1.5.2.4　設定管理クライアントの確認

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



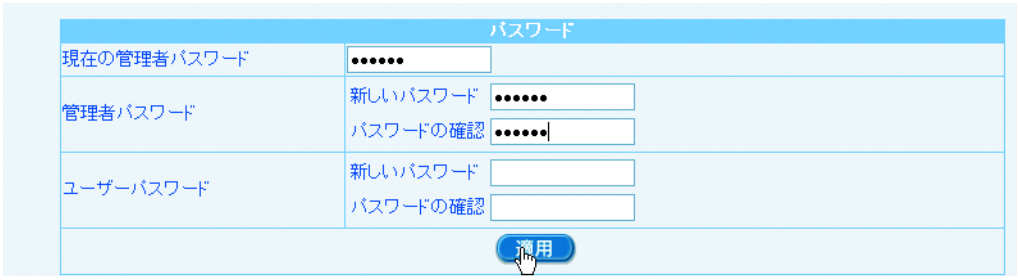
1.5.3 パスワードの設定

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

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

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

2.「パスワード」テーブルで各パラメーターを入力し、「適用」ボタンをクリックします。ここでは、現在の管理者レベルのログインパスワード「friend」を「ar260s」に変更するものとします。



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

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

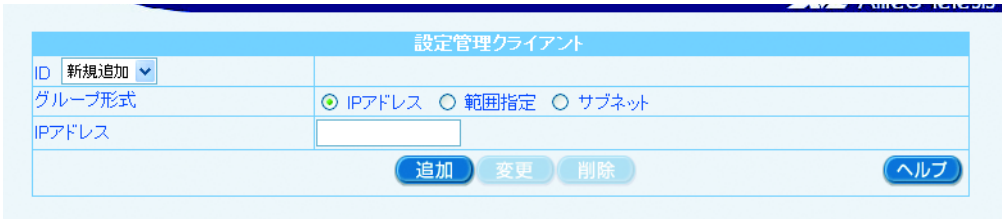
4. 以上で設定は完了です。

1.5.4 「設定管理クライアント / パスワード」ページの解説

「設定管理クライアント / パスワード」ページについて解説します。

1.5.4.1 設定管理クライアント

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



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

パラメーター	オプション	説明
IDドロップダウンリスト		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 番号を選択します。
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。
	範囲指定	クライアントを IP アドレスの範囲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。
始点 IP アドレス / 終点 IP アドレス	グループ形式に「範囲指定」を選択した場合にのみ表示されます。指定する IP アドレスの範囲の始点 / 終点 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	ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。クライアントを追加登録します。8 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	ドロップダウンリストで既存のクライアントの ID 番号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。
「削除」ボタン	ドロップダウンリストで既存のクライアントの ID 番号を選択した場合にアクティブになります。選択したクライアントを削除します。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。
「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。

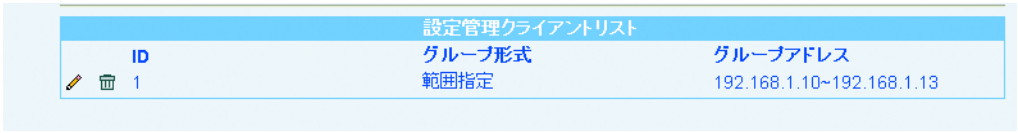
「パスワード」テーブルでは、本製品のユーザー（manager/guest）に対してパスワードを設定します。

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。
	新しいパスワード	新しく設定するパスワードを入力します。半角英数字で 16 文字以内で入力してください。
	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。
	新しいパスワード	新しく設定するパスワードを入力します。半角英数字で 16 文字以内で入力してください。
	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。
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。
「えんぴつ」アイコン	クリックすると「設定管理クライアントリスト」の該当クライアントの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「設定管理クライアントリスト」から該当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 (SysName)」、「システムロケーション (SysLocation)」、「連絡先 (SysContact)」を設定することができます。ここでは、システム情報の設定について説明します。

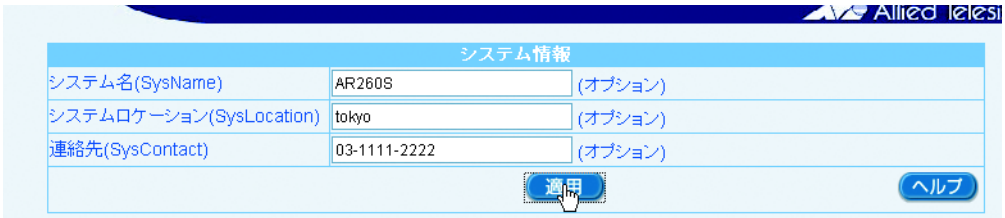
1.6.2 設定

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(SysName)	AR260S
システムロケーション (SysLocation)	tokyo
連絡先(SysContact)	03-1111-2222



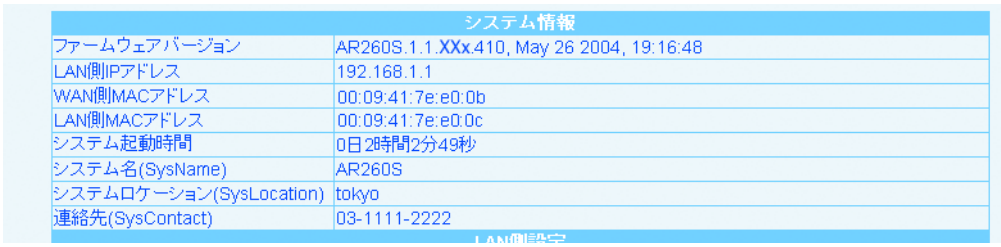
3. 以上で設定は完了です。

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。

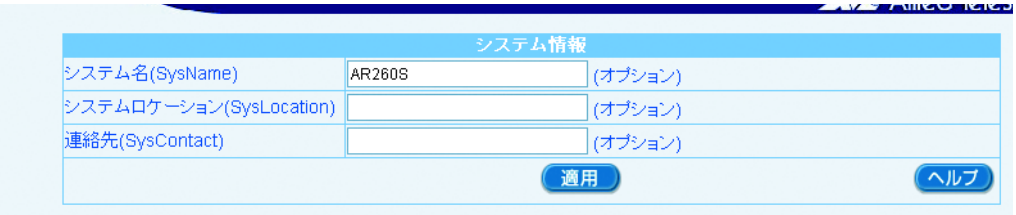


パラメーター	説明
ファームウェアバージョン	本製品のファームウェアのバージョンが「1.1.XXx.410」のように表示されます。「XX」の部分には数字、「x」には小文字の英字が表示されます。
LAN 側 IP アドレス	本製品の LAN 側インターフェースの IP アドレスが表示されます。
WAN 側 MAC アドレス	本製品の WAN 側の MAC アドレスが表示されます。プロバイダーに本製品の MAC アドレスを通知する場合は、この MAC アドレスを通知してください。
LAN 側 MAC アドレス	本製品の LAN 側の MAC アドレスが表示されます。
システム起動時間	本製品が起動してから経過した時間が表示されます。
システム名 (SysName)	「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 (SysLocation)	「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 (SysContact)	「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 (SysName)	本製品のシステム名を入力します。デフォルトは「AR260S」です。半角英数字で 63 文字以内で入力してください。入力は任意です。
システムロケーション (SysLocation)	本製品の設置場所を入力します。半角英数字で 31 文字以内で入力してください。入力は任意です。
連絡先 (SysContact)	連絡先を入力します。半角英数字で 31 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もつため、時刻を一度設定すると、その後は外部の SNTP サーバーとの通信により、時刻を同期します。ここでは、時刻を同期するための外部 SNTP サーバーを本製品に設定する方法についても説明します。

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、「2004 年 4 月 22 日 19 時 30 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。

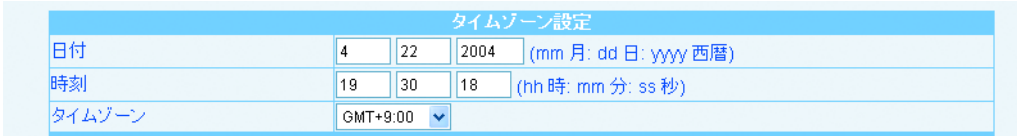
3. 以上で設定は完了です。

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 ～ 5 をそれぞれ「192.168.10.5」、「133.100.11.8」、「133.40.41.175」、「130.69.251.23」、「128.105.39.11」、更新間隔を「1 分」に設定するものとします。

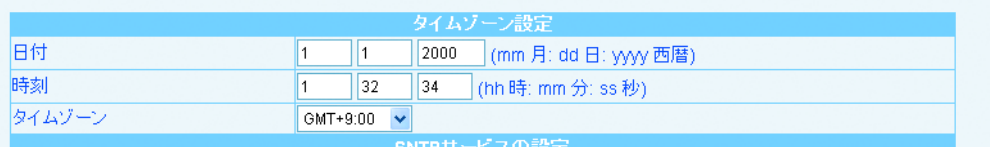
3. 以上で設定は完了です。

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。

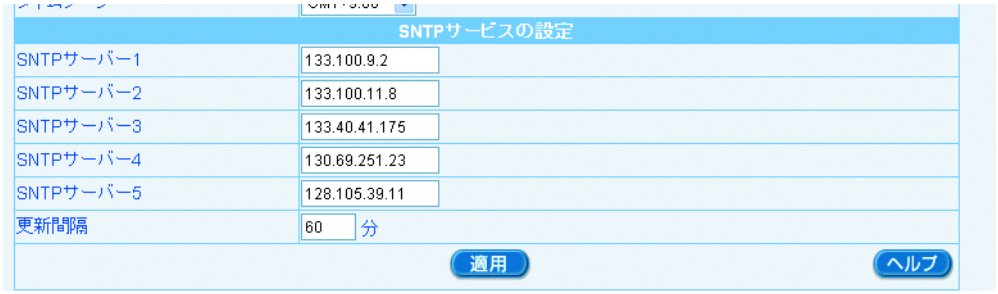


パラメーター	説明
日付	日付を入力します。入力形式は「月 : 日 : 西暦年」です。
時刻	時刻を入力します。入力形式は「時 : 分 : 秒」です。
タイムゾーン	タイムゾーンを選択します。

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「2000 年 1 月 1 日 0 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 ～ 5	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 ～ 5 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～ 99 分の範囲で入力してください。
「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。

1.8 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」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
RO コミュニティー名	viewer
RW コミュニティー名	secret
通知先アドレス	192.168.10.5

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」の順にクリックします。

2.「SNMP 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」ページの解説

「SNMP ページ」について解説します。「SNMP」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。
RO コミュニティー名		SNMP 管理ホストが本製品の情報を読み出す場合に使用する平文テキストのパスワードを入力します。半角英数字で 15 文字以内で入力してください。デフォルトは「public」です。
RW コミュニティー名		SNMP 管理ホストが本製品の情報を読み出す場合、および設定を書き込む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。半角英数字で 15 文字以内で入力してください。デフォルトは「private」です。
通知先アドレス		SNMP 管理ホストの IP アドレスを入力します。
「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。

SNMP設定	
SNMP	無効
ROコミュニティー名	public
RWコミュニティー名	private
通知先アドレス	

パラメーター	説明
SNMP	SNMP の有効 / 無効が表示されます。
RO コミュニティー名	本製品の情報を読み出す場合のパスワードが表示されます。
RW コミュニティー名	本製品の情報を読み出す場合、および設定を書き込む場合のパスワードが表示されます。
通知先アドレス	SNMP 管理ホストの IP アドレスが表示されます。

1.9 ログの記録

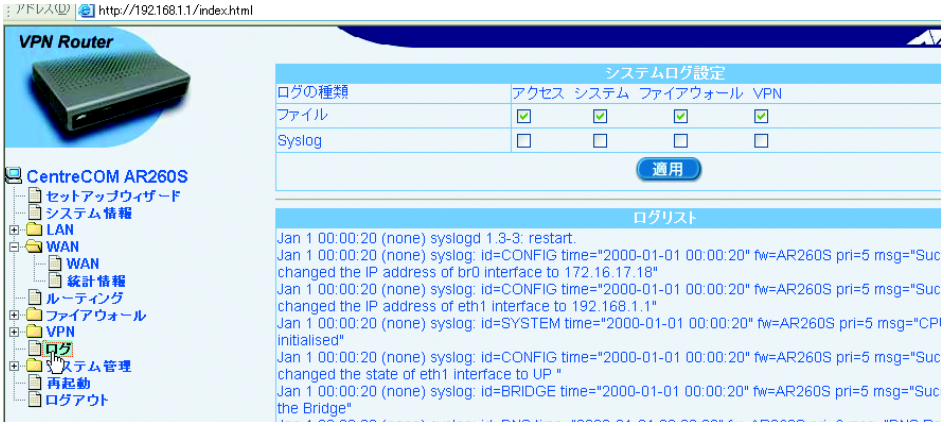
1.9.1 概要

本製品では「アクセス」、「システム」、「ファイアウォール」、「VPN」の 4 種類の各ログを「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

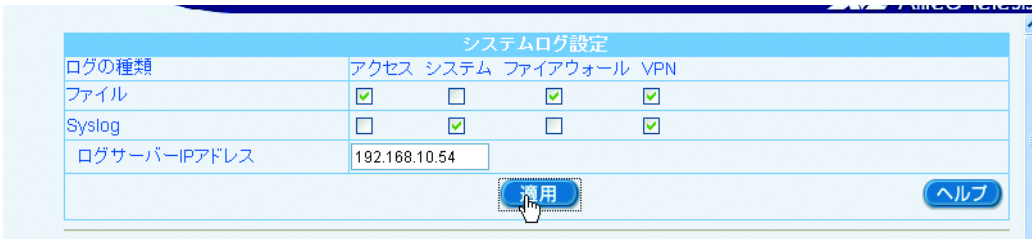
ログ機能を設定するには以下の手順を実行します。

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。

アクセス	ファイル
システム	Syslog
ファイアウォール	ファイル
VPN	Syslog、ファイル
ログサーバー IP アドレス	192.168.10.54



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。

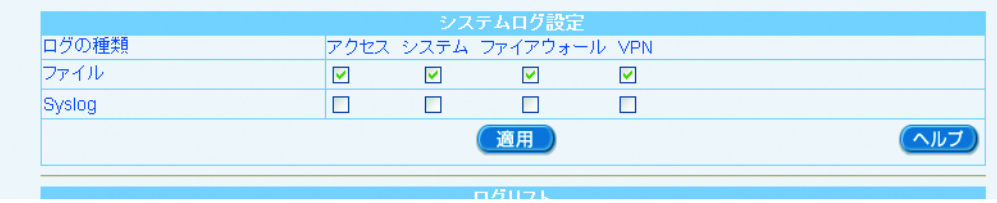
2.「ログリスト」にログが表示されます。また「更新」ボタンをクリックすると表示内容が更新されます。

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。

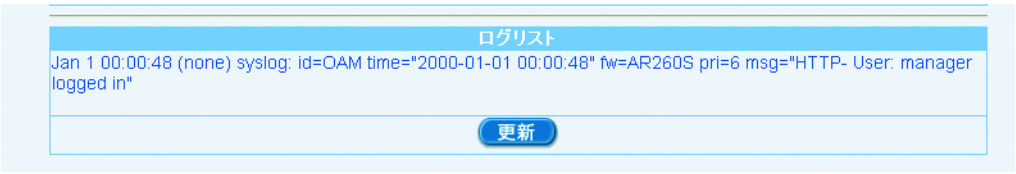


パラメーター	オプション	説明
ログの種類		アクセス、システム、ファイアウォール、VPN の 4 種類のログを記録することができます。
	アクセス	本製品へのアクセスに関するログです。
	システム	本製品のシステムに関するログです。
	ファイアウォール	ファイアウォールを経由した通信のログです。
	VPN	VPN 通信に関するログです。
ファイル		ログを「ログリスト」テーブルに表示する場合にチェックを入れます。チェックは、ログの種類ごとに入れます。ログのサイズは 64Kbyte を超えると（およそ 450 件分）古い順から上書きされます。
Syslog		ログをリモート syslog サーバーに送信する場合にチェックを入れます。ログのサイズが 64Kbyte を超えると自動的にサーバーに送信されます。チェックは、ログの種類ごとに入れます。Syslog のログ送出の出力監視レベルは PRI に対応しています。

ログサーバー IP アドレス	「Syslog」にチェックを入れた場合にのみ表示されます。ログを送信する syslog サーバーの IP アドレスを入力します。
「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」でファイルにチェックを入れた場合に、ログが記録されます。



パラメーター	説明
「更新」ボタン	クリックすると、ログの表示が更新されます。

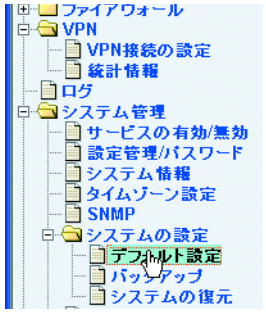
1.10 設定の初期化

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。

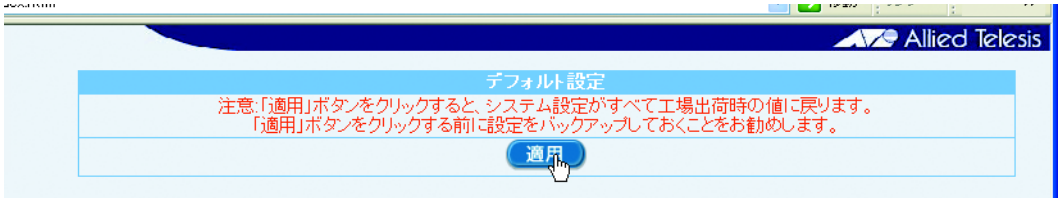
ヒント　本製品をデフォルト設定に戻す前に、現在の設定をバックアップしておくことをお勧めします。バックアップについては「P.46 設定内容のバックアップ」を参照してください。

1.10.1 GUI 設定画面からの初期化

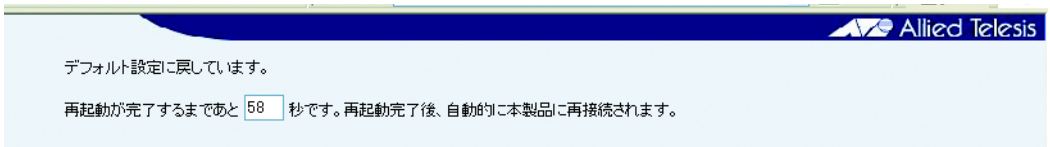
1. メニューから「システム管理」->「システムの設定」->「デフォルト設定」の順にクリックします。



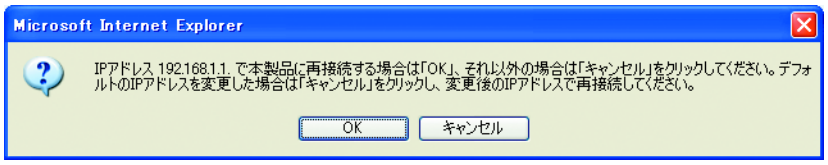
2.「適用」ボタンをクリックします。



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。



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。

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、5 秒以上待ちます。

2. 本製品の電源をオンにして 5 秒以上経過したらリセットスイッチを短く押します。

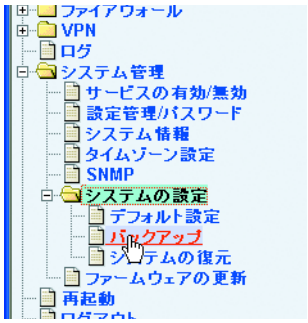
3. しばらくすると ALARM LED が一瞬消灯しますので、消灯している間にリセットスイッチをもう一度短く押します。

4. 以上で完了です。

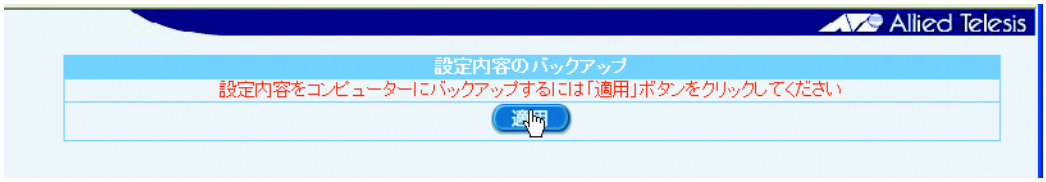
1.11 設定内容のバックアップ

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。

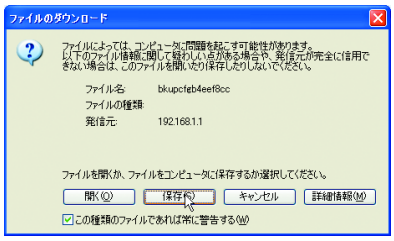
1. メニューから「システム管理」->「システムの設定」->「バックアップ」の順にクリックします。

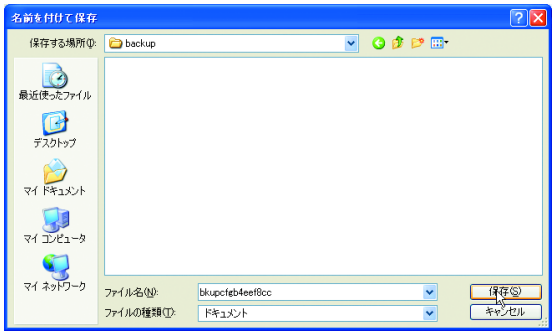


2.「適用」ボタンをクリックします。

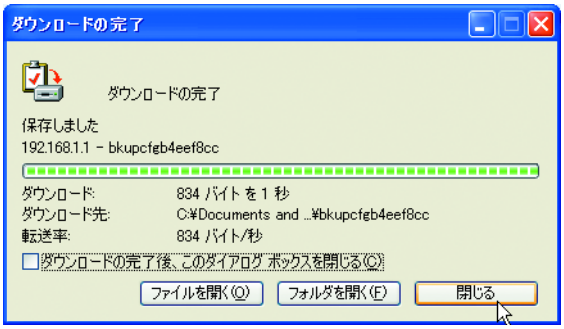


3. 以下の画面が表示されたら「保存」ボタンをクリックして、バックアップファイルの保存場所を指定し、ダイアログの「保存」ボタンをクリックします。





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。

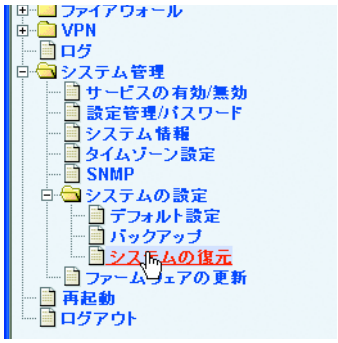
ヒント **設定内容のバックアップ中は本製品の通信は停止しません。**

ヒント **保存したバックアップファイルはバイナリファイルです。テキストエディタで編集することはできません。**

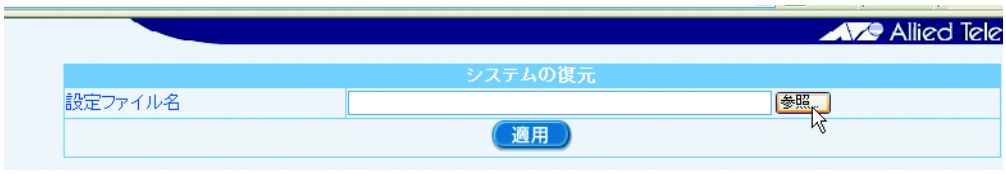
1.12　バックアップファイルの復元

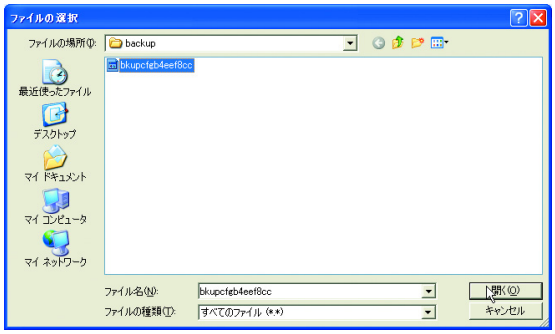
バックアップした本製品の設定ファイルを復元する手順を説明します。

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。



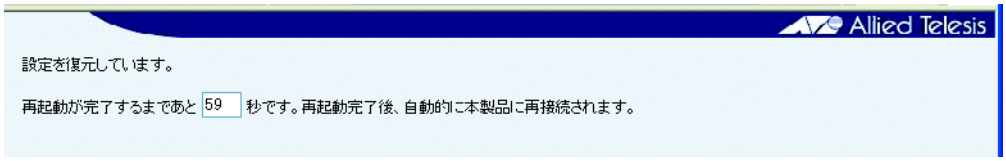
2.「参照」ボタンをクリックして、バックアップファイルを指定し「開く」ボタンをクリックします。



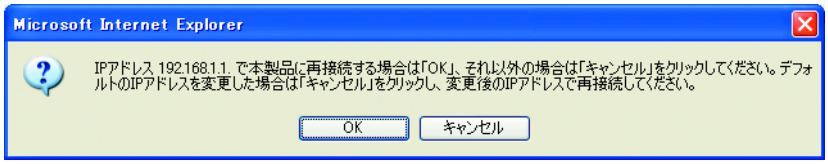


3.「適用」ボタンをクリックします。

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。



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。

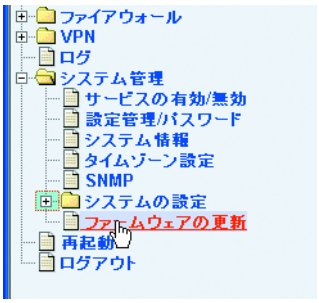
IP アドレスを変更した場合は「キャンセル」ボタンをクリックします。「キャンセル」ボタンをクリックした場合は、変更後の IP アドレスを指定して手動で本製品に再接続する必要があります。

6. 以上で完了です。

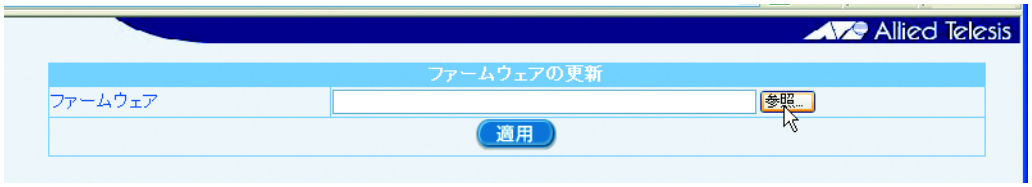
1.13　ファームウェアの更新

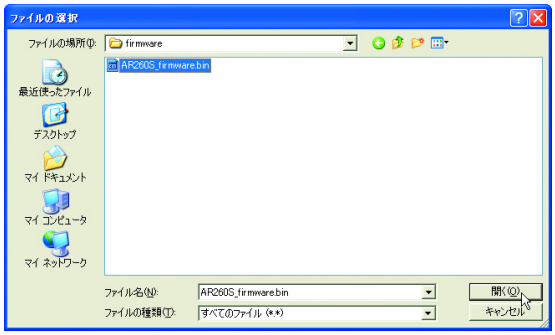
「ファームウェアの更新」ページでは、本製品のファームウェアを新しいバージョンのファームウェアに更新することができます。

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。



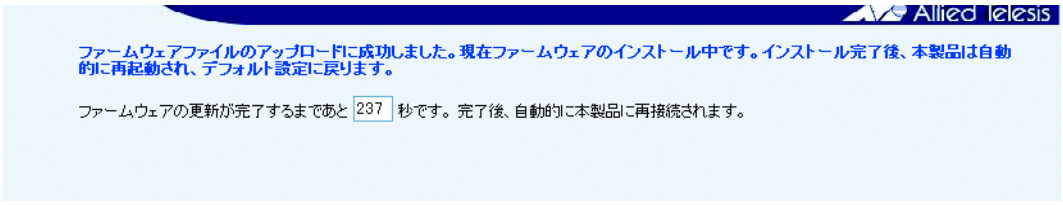
2.「参照」ボタンをクリックして、ファームウェアファイルを指定し「開く」ボタンをクリックします。





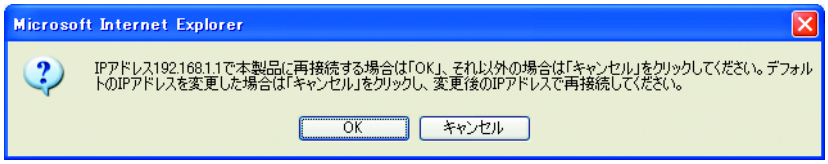
3.「適用」ボタンをクリックします。

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。



ヒント **ファームウェア更新中にリセットボタンを押さないでください。また、電源をオフにすることやケーブルの抜き差しもしないでください。**

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。

6. 以上で完了です。

ヒント **ファームウェアの更新中、本製品の通信は停止しますので、運用中にファームウェアの更新を実行しないようご注意ください。**

ヒント **ファームウェア更新後でも、更新前の設定は引き継がれます。**

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

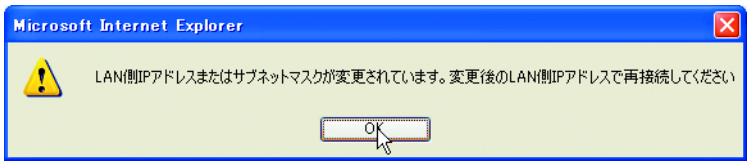
LAN 側インターフェースに IP アドレスを割り当てるには以下の手順を実行します。

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「192.168.10.1/24」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「192.168.10.1」、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. 以下のメッセージが表示されますので「OK」ボタンをクリックします。



4. これで設定は完了です。

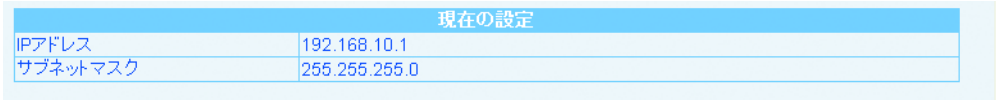
ヒント　**次回、本製品の設定を行う場合は変更後の IP アドレスでアクセスしてください。**

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. 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

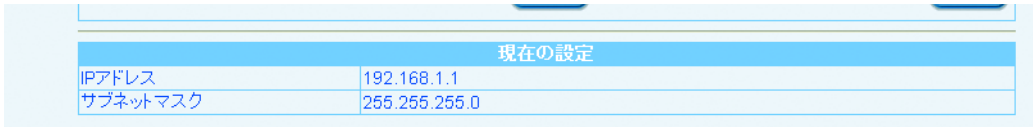
「IP」ページについて解説します。「IP」ページでは本製品の LAN 側に関する設定を行います。

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。
「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	192.168.1.10
	終点 IP アドレス	192.168.1.200
サブネットマスク		255.255.255.0
リース期限		14 日
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

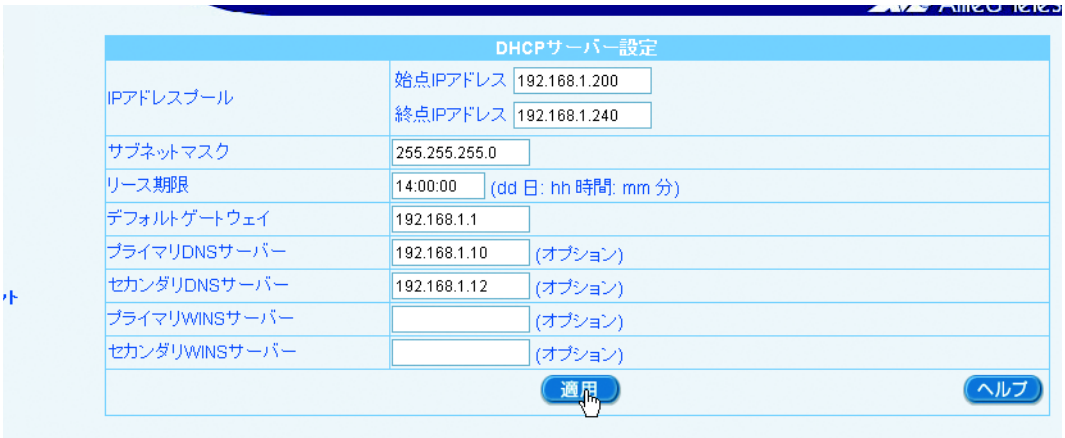
2.3.2 設定

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
サブネットマスク		255.255.255.0
リース期限		14 日
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		192.168.1.10
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。

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。
	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。
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を入力します。
リース期限		クライアントに割り当てる IP アドレスのリース期限を入力します。1 分～ 99 日 23 時間 59 分の範囲で入力してください。
デフォルトゲートウェイ		デフォルトゲートウェイの IP アドレスを入力します。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	192.168.1.10 ~ 192.168.1.200
サブネットマスク	255.255.255.0
リース期限	14:00:00 (dd 日: hh 時間: mm 分)
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
セカンダリDNSサーバー	
プライマリWINSサーバー	
セカンダリWINSサーバー	

パラメーター	**説明**
IP アドレスプール	本製品に設定された IP アドレスプールが表示されます。
サブネットマスク	IP アドレスプールのサブネットマスクが表示されます。
リース期限	クライアントに割り当てた IP アドレスのリース期限が表示されます。
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	IP アドレスを割り当ててから経過した時間が表示されます。
「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「ごみ箱」アイコンをクリックします。

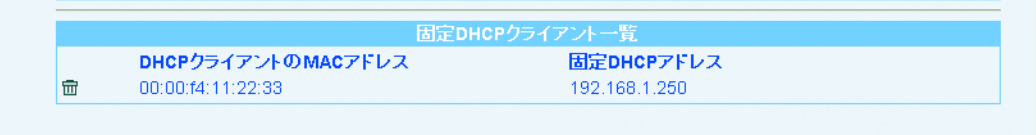
3. 以上で設定は完了です。

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

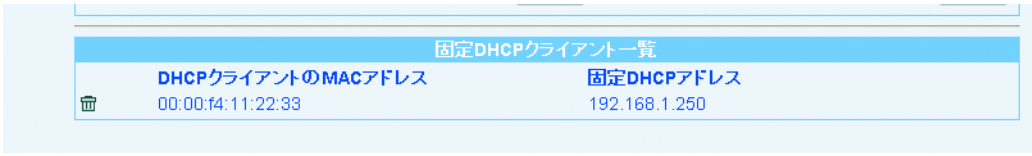
「固定 DHCP クライアント」ページについて解説します。「固定 DHCP クライアント」ページでは、本製品の DHCP サーバー機能で固定的に IP アドレスを割り当てるクライアントを登録します。

2.4.5 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 10 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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

2.4.6 固定 DHCP クライアント一覧



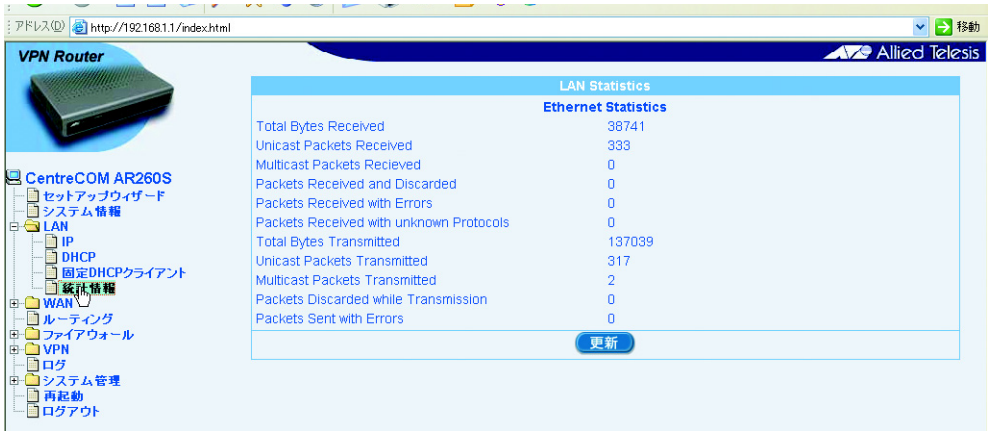
パラメーター	説明
DHCP クライアントの MAC アドレス	IP アドレスが固定的に割り当てられているクライアントの MAC アドレスが表示されます。
固定 DHCP アドレス	クライアントに固定的に割り当てられている IP アドレスが表示されます。
「ごみ箱」アイコン	クリックすると「固定 DHCP クライアント一覧」から該当クライアントを削除します。

2.5 トラフィックの確認

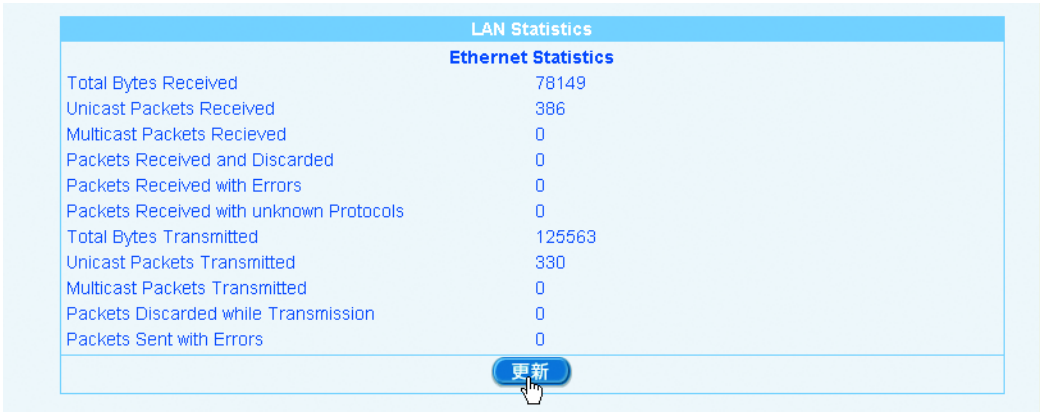
本製品では、LAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。LAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

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。



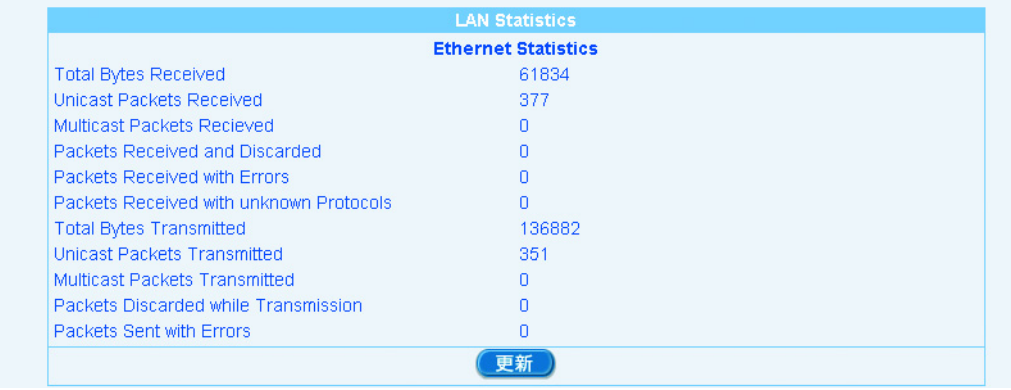
2.「LAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。



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。

ホスト名	mycomputer（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
MAC クローニング	有効、「00:00:f4:11:22:33」に設定する

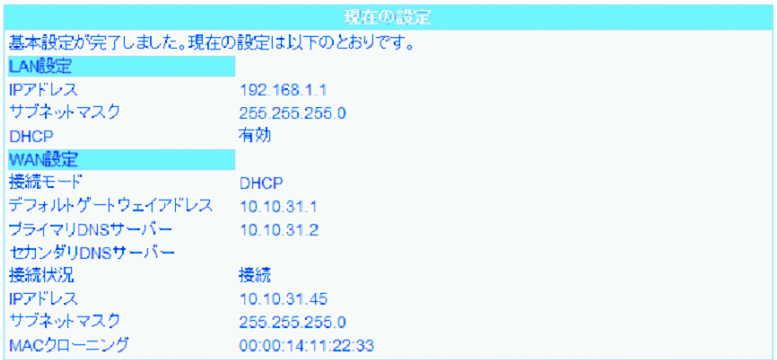
4. 以上で設定は完了です。

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。



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、セッション ID「PPPoE:0」に以下のように設定するものとします。

Unnumbered PPPoE	無効
ホスト名	mycomputer（プロバイダーから提供されたと仮定します）
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	ダイアルオンデマンド、タイムアウトまでの時間 60 秒

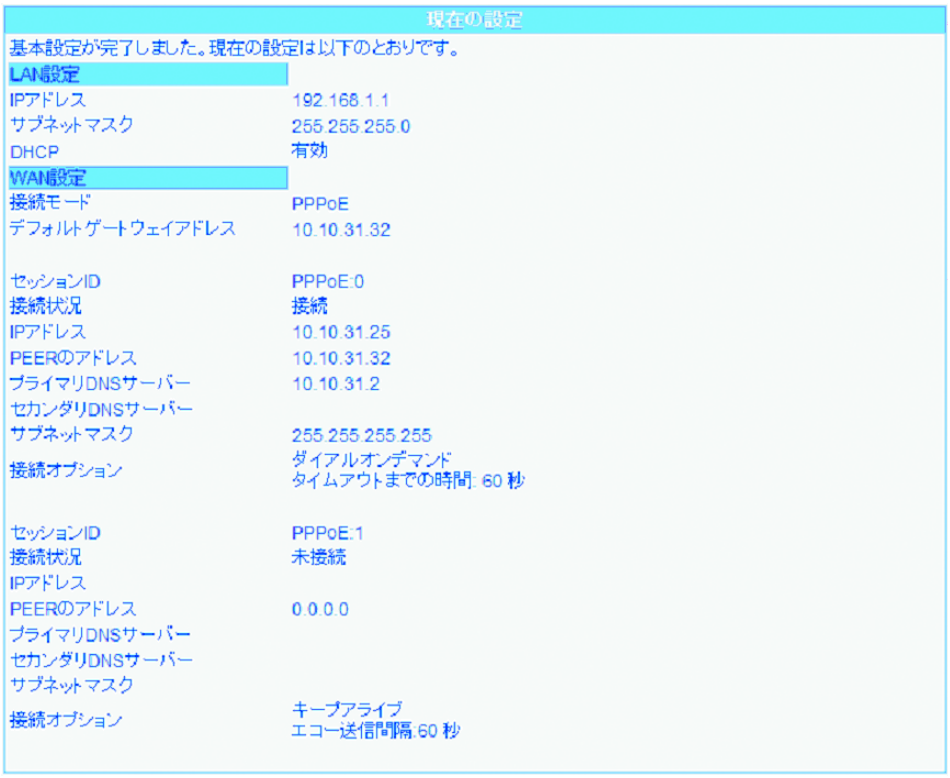
4. 以上で設定は完了です。

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。



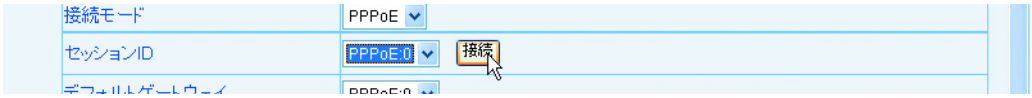
3.3.3 PPPoE セッションの切断 / 接続

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. 切断 / 接続するセッションを選択します。ここでは「PPPoE:0」を選択するものとします。

3.「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を「接続」するものとします。



4. 以上で設定は完了です。

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

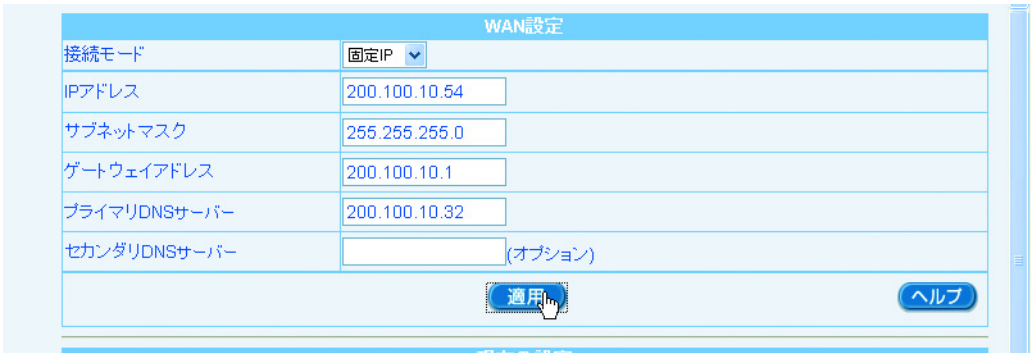
WAN 側インターフェースを固定 IP アドレスで接続するには以下の手順を実行します。

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。

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

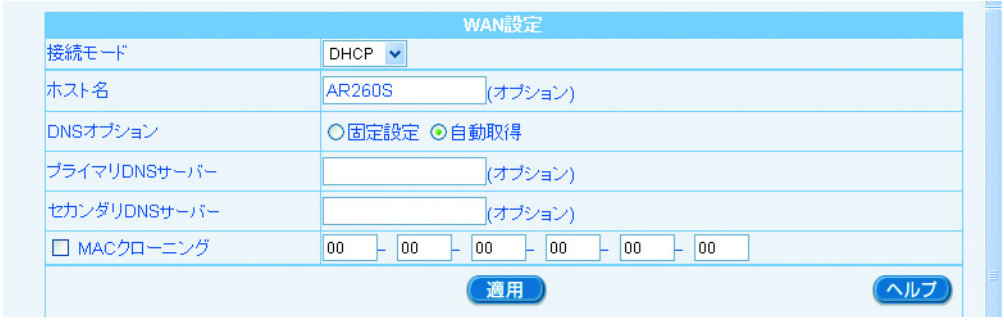
メニューから「WAN」->「WAN」の順にクリックすると以下の画面が表示されます。

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
ホスト名		本製品のホスト名を入力します。半角英数字で 63 文字以内で入力してください。プロバイダーに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。
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。
MAC クローニング		本製品の WAN 側の MAC アドレスを、ここで指定した MAC アドレスに見せかける機能です。チェックボックスにチェックを入れると MAC クローニング機能が有効になります。また、有効にした場合は本製品に擬似的に割り当てる MAC アドレスを入力します。
「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。

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。
	MAC クローニング	MAC クローニングの有効 / 無効が表示されます。

3.5.1.2　接続モードに「PPPoE」を選択した場合

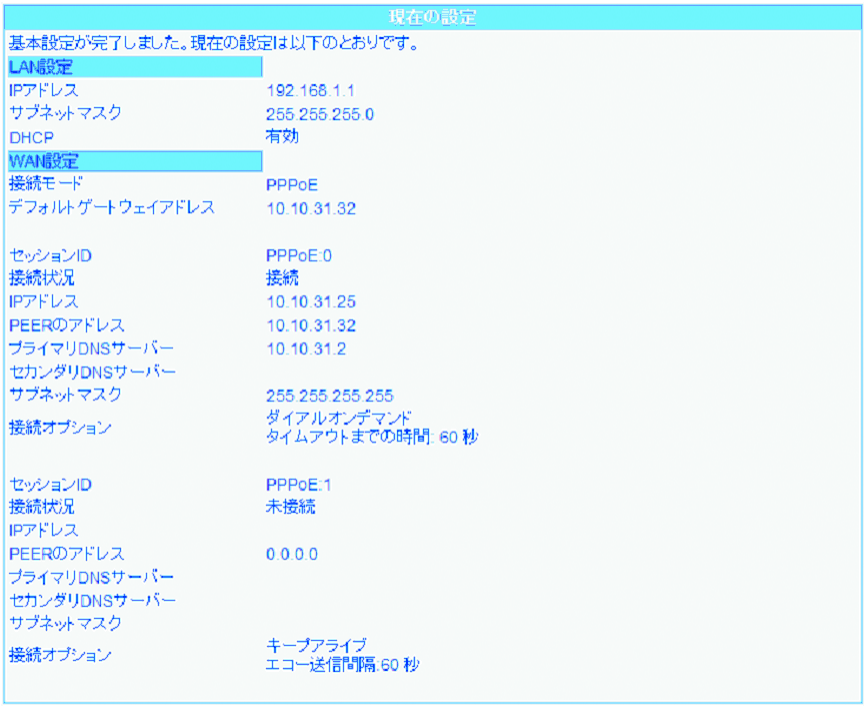
接続モードに「PPPoE」を選択すると、以下の画面が表示されます。

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
セッション ID		確立するセッションの ID を選択します。
	PPPoE:0	1 つ目のセッションを設定、表示する場合に選択します。
	PPPoE:1	2 つ目のセッションを設定、表示する場合に選択します。
	「接続 / 切断」ボタン	選択したセッションを接続、切断する場合にクリックします。
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。
	PPPoE:0	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。
	PPPoE:1	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。

Unnumbered PPPoE	有効 / 無効		Unnumbered 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。
ホスト名			本製品のホスト名を入力します。半角英数字で 63 文字以内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。
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 63 文字以内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 63 文字以内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 80 文字以内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 15 文字以内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。
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。
		MSS の値	MSS クランプを有効にした場合に、MSS（Maximum Segment Size）の値を入力します。40 ～ 120bytes の範囲で入力してください。
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。
	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。60 秒～ 600 秒の範囲で入力してください。
	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。60 秒 ～ 600 秒の範囲で入力してください。
	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。

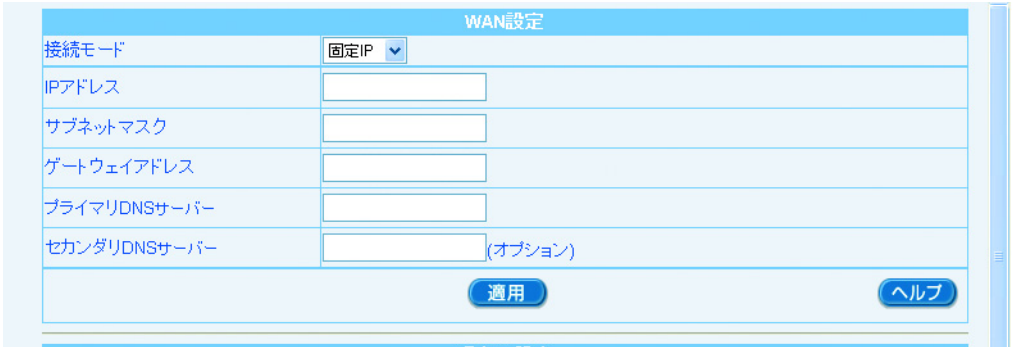


パラメーター	オプション	説明
LAN 設定		本製品の LAN 側インターフェースに関する情報が表示されます。
	IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示されます。
WAN 設定		本製品の WAN 側インターフェースに関する情報が表示されます。
	接続モード	現在の接続モードが表示されます。

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
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。

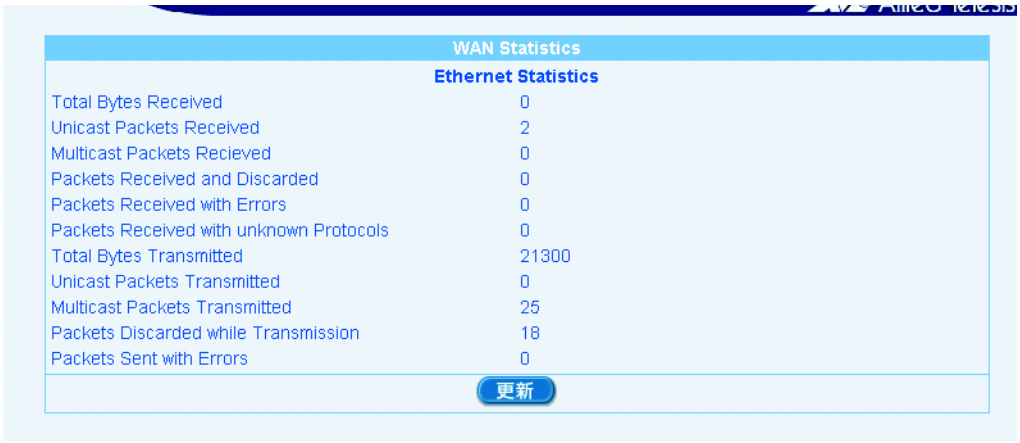
パラメーター	オプション	説明
LAN 設定		本製品の LAN 側インターフェースに関する情報が表示されます。
	IP アドレス	現在本製品の LAN 側インターフェースに設定されている IP アドレスが表示されます。
	サブネットマスク	現在本製品の LAN 側インターフェースに設定されているサブネットマスクが表示されます。
	DHCP	DHCP サーバー機能の有効 / 無効が表示されます。
WAN 設定		本製品の WAN 側インターフェースに関する情報が表示されます。
	接続モード	現在の接続モードが表示されます。
	デフォルトゲートウェイアドレス	デフォルトゲートウェイアドレスが表示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

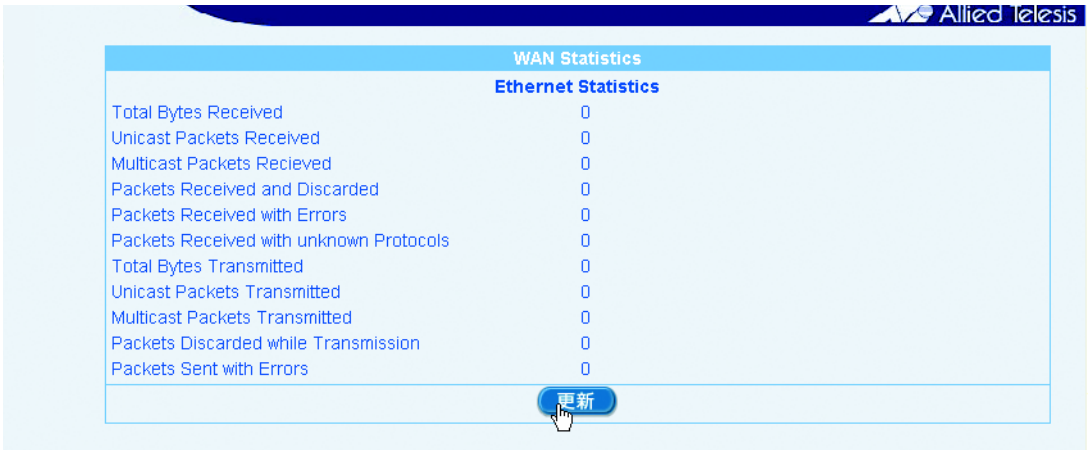
本製品では、WAN 側インターフェースで送受信するパケットのトラフィックを統計情報として一覧表示できます。WAN 側インターフェースの送受信トラフィックは「統計情報」ページで確認します。

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。



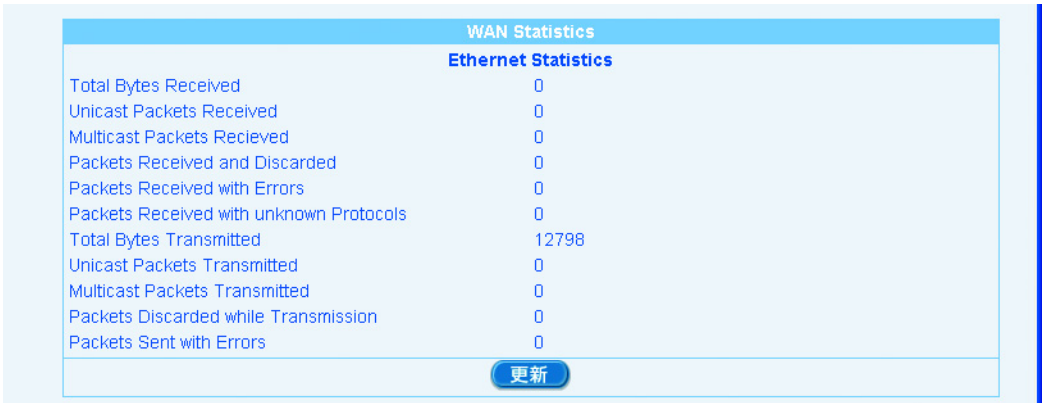
2.「WAN Statistics」が表示されます。表示を更新するには「更新」ボタンをクリックします。



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。

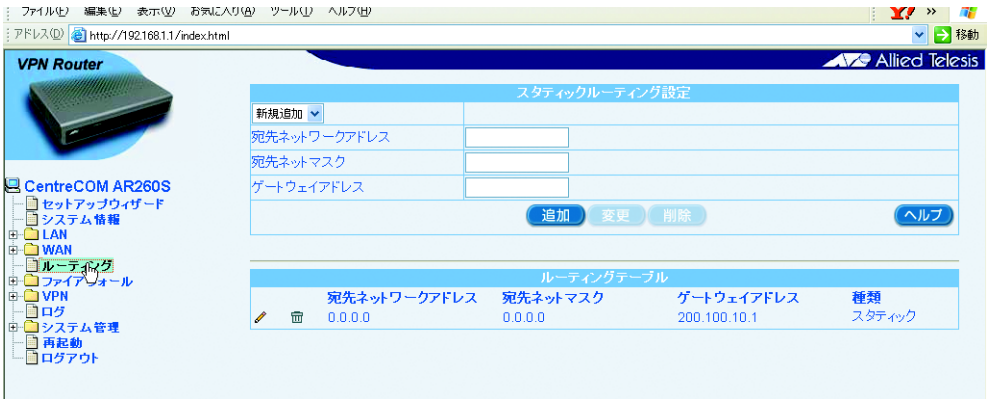
4.2　スタティックルーティング

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. ドロップダウンリストから「新規追加」を選択します。

3. 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	192.168.1.1

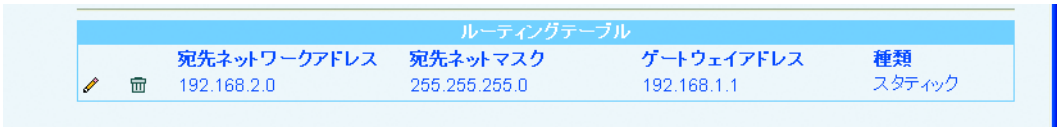
4. 以上で設定は完了です。

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.「スタティックルーティング設定」テーブルのドロップダウンリストから変更するルートを選択します。または、「ルーティングテーブル」の該当ルート左部にある「えんぴつ」アイコンをクリックします。

3. 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.「スタティックルーティング設定」テーブルのドロップダウンリストから削除するルートを選択し「削除」ボタンをクリックします。または、「ルーティングテーブル」の該当ルート左部にある「ごみ箱」アイコンをクリックします。

3. 以上で設定は完了です。

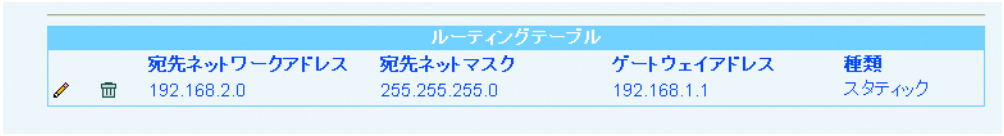
4.3 「ルーティング」ページの解説

「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	説明
ドロップダウンリスト	ルートを新規追加する場合は「新規追加」、既存のルートを変更 / 削除する場合は、該当のルートの宛先ネットワークアドレスを選択します。
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。
ゲートウェイアドレス	宛先ホスト、またはネットワークへパケットを転送するゲートウェイの IP アドレスを入力します。
「追加」ボタン	ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。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。
「削除」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。選択したルートを削除します。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

4.3.2 ルーティングテーブル



パラメーター	説明
宛先ネットワークアドレス	登録されたルートの宛先ネットワークアドレスが表示されます。
宛先ネットマスク	登録されたルートの宛先ネットマスクが表示されます。
ゲートウェイアドレス	登録されたルートのゲートウェイアドレスが表示されます。
種類	ルーティングの種類が表示されます。
「えんぴつ」アイコン	クリックすると「ルーティングテーブル」の該当ルートの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「ルーティングテーブル」から該当ルートを削除します。

5　ファイアウォールの設定

5.1　概要

ファイアウォールは、ポリシーを作成し、そのポリシー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 NAT が有効に設定されています（Outbound アクセスルール）。本章では、本製品の以下の 6 つのファイアウォール機能について説明します。

- Inbound アクセスルール
- Outbound アクセスルール
- ステルスモード
- セルフアクセス
- URL フィルター
- DoS アタックプロテクト

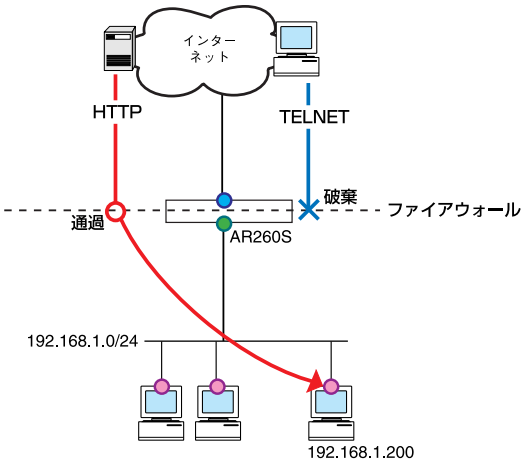
5.2　Inbound アクセスルールの設定

Inbound ルールは、本製品を経由する WAN 側から LAN 側へ向けたトラフィックを制御するルールです。Inbound アクセスルールは「Inbound アクセス」ページで作成します。

5.2.1　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ポリシー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」->「Inbound アクセス」の順にクリックします。

2. ID ドロップダウンリストから「新規追加」を選択します。

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

アクション			通過
優先度			1
送信元			全て
宛先			全て
送信元ポート			全て
宛先ポート			サービス
		サービス	HTTP
NAT			IP アドレス
		IP アドレス	192.168.1.200
ログ			無効
VPN			無効

ヒント

「送信元」、「宛先」で「IP プール」を選択する場合、「宛先ポート」で定義されていない「サービス」を選択する場合、「NAT」で「NAT プール」を選択する場合は、各設定をあらかじめ行っておく必要があります。「IP プール」、「NAT プール」、「サービス」の設定方法の詳細については「P.129 各種ポリシーとサービスの設定」を参照してください。

4. 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。

5. 以上で設定は完了です。

5.2.2 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」->「Inbound アクセス」の順にクリックします。

2. ID ドロップダウンリストから変更するルールの ID を選択します。または、「Inbound アクセス制御リスト」テーブルの該当ルール左部にある「えんぴつ」アイコ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. 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。

5.2.3 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」->「Inbound アクセス」の順にクリックします。

2. ID ドロップダウンリストから削除するルールの ID を選択し「削除」ボタンをクリックします。または、「Inbound アクセス制御リスト」テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。

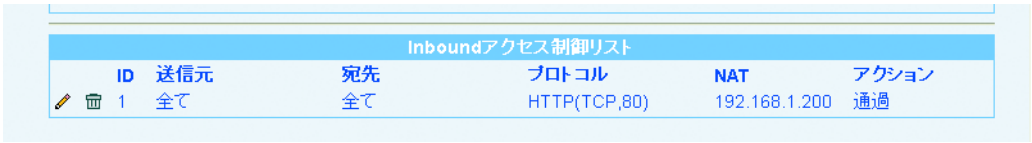
3. 本製品を再起動します。再起動の方法については「P. 16 再起動」を参照してください。

4. 以上で設定は完了です。

5.2.4 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」->「Inbound アクセス」の順にクリックします。
2. 「Inbound 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。

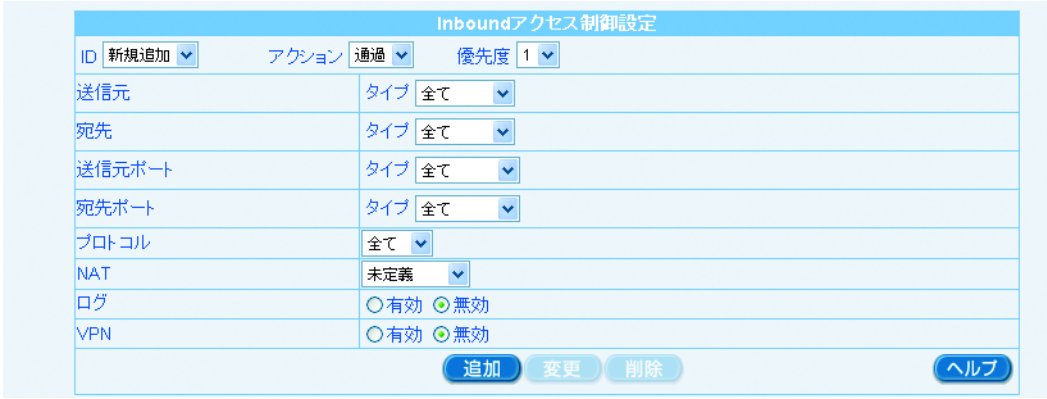


5.2.5 「Inbound アクセス」ページの解説

「Inbound アクセス」ページについて解説します。「Inbound アクセス」ページでは本製品の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。

5.2.5.1 Inbound アクセス制御設定テーブル

メニューから「ファイアウォール」->「Inbound 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 ドロップダウンリスト		ファイアウォールのルールを新規追加する場合は「新規追加」、既存のルールを変更 / 削除する場合は該当の ID 番号を選択します。
アクション	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。
	全て	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。
		アドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターの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。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合にのみ表示されます。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	タイプに「範囲指定」を選択した場合にのみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあらかじめ設定した IP プールで指定する場合に選択します。IP プールの設定方法については「P.129 IP プールの設定」を参照してください。
		IP プール	タイプに「IP プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の IP プール名をドロップダウンリストから選択します。
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。
	全て		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。
		アドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターの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。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合にのみ表示されます。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	タイプに「範囲指定」を選択した場合にのみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあらかじめ設定した IP プールで指定する場合に選択します。IP プールの設定方法については「P.129 IP プールの設定」を参照してください。
		IP プール	タイプに「IP プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の IP プール名をドロップダウンリストから選択します。
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。
	全て		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。
	全て		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。
	サービス		ポートを指定せずに、あらかじめ定義されたサービスにルールを適用する場合に選択します。
		サービス	タイプに「サービス」を選択した場合にのみ表示されます。ドロップダウンリストからルールを適用するサービスを選択します。リストにないサービスを指定する場合は、あらかじめ定義しておいてください。サービスの設定方法については「P.139 サービスの設定」を参照してください。
プロトコル			宛先ポートパラメーターに「全て」、「ポート指定」、「範囲指定」を選択した場合に表示されます。サービスを選択した場合には表示されません。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。
NAT			ルールに設定する NAT の種類を選択します。

	未定義		ルールに NAT を設定しない場合に選択します。
	IP アドレス		IP アドレスを指定してルールに NAT を設定する場合に選択します。
		IP アドレス	NAT に「IP アドレス」を選択した場合にのみ表示されます。本製品で受信したパケットの転送先コンピューターの IP アドレスを指定します。この機能は DMZ、またはバーチャルサーバー機能と呼ばれます。
	NAT プール		ルールに設定する NAT をあらかじめ作成した NAT プールで指定する場合に選択します。DMZ、またはバーチャルサーバー機能の動作をするプールのみ選択可能です。NAT プールの作成方法については「P.134 NAT プールの設定」を参照してください。
		プール	NAT に「NAT プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の NAT プールから選択します。
ログ	有効 / 無効		ルールのログを記録する場合は「有効」、記録しない場合は「無効」ラジオボタンを選択します。
VPN	有効 / 無効		VPN 通信を使用する場合は「有効」、使用しない場合は「無効」を選択します。
「追加」ボタン			ID ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。ルールを追加登録します。Inbound/Outbound アクセスを合わせて 150 件までのルールを追加することができます。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			ID ドロップダウンリストで既存のルールの ID 番号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。
「削除」ボタン			ID ドロップダウンリストで既存のルールの ID 番号を選択した場合にアクティブになります。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。
「ヘルプ」ボタン			操作のヒントを参照することができます。

5.2.5.2 Inbound 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。
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、サービス名、ポート番号が表示されます。
NAT	ルールに設定された NAT の内容が表示されます。
アクション	ルールに設定されたアクションです。通過 / 破棄のいずれかが表示されます。
「えんぴつ」アイコン	クリックすると「Inbound アクセス制御リスト」の該当ルールの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「Inbound アクセス制御リスト」から該当ルールを削除します。

5.3 Outbound アクセスルールの設定

Outbound アクセスルールは、本製品を経由する LAN 側から WAN 側へ向けたトラフィックを制御するルールです。
Outbound アクセスルールは「Outbound アクセス」ページで作成します。

5.3.1 デフォルトポリシー

Outbound アクセスルールにはデフォルトでポリシーが設定されています。ポリシーの内容は下記のとおりです。このポリシーが設定されていることで、LAN 側からインターネットへ向けたパケットの IP アドレスは全て pppoe0 インターフェースの IP アドレスに変換され、インターネット通信が可能になります。

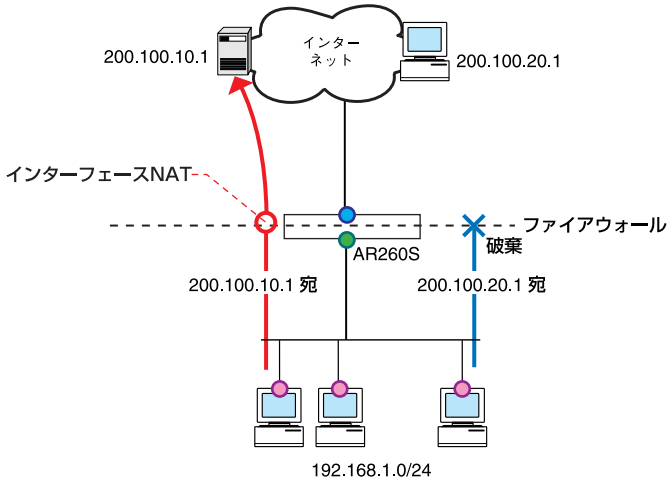
アクション	通過
優先度	1
送信元	全て
宛先	全て
送信元ポート	全て
宛先ポート	全て
プロトコル	全て
NAT	インターフェース NAT（pppoe0）
ログ	無効
VPN	無効

デフォルトのポリシー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。

5.3.2 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ポリシーで設定を行うものとします。



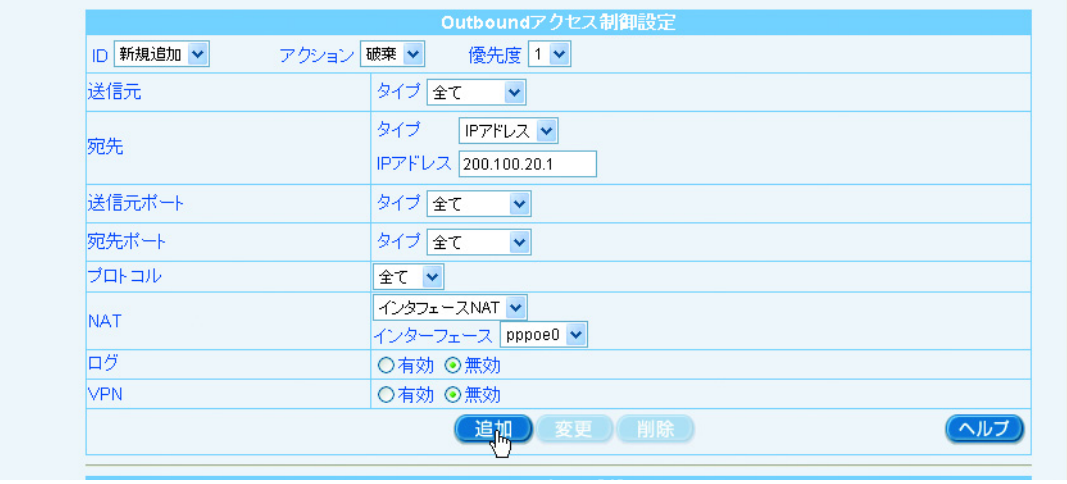
1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。

2. ID ドロップダウンリストから「新規追加」を選択します。

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

アクション	破棄
優先度	1
送信元	全て
宛先	IP アドレス

	IP アドレス	200.100.20.1
送信元ポート		全て
宛先ポート		全て
プロトコル		全て
NAT		インターフェース NAT
	インターフェース	pppoe0
ログ		無効
VPN		無効



ヒント **「送信元」、「宛先」で「IP プール」を選択する場合、「宛先ポート」で定義されていない「サービス」を選択する場合、「NAT」で「NAT プール」を選択する場合は、各設定をあらかじめ行っておく必要があります。「IP プール」、「NAT プール」、「サービス」の設定方法の詳細については「P.129 各種ポリシーとサービスの設定」を参照してください。**

4. 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。

5. 以上で設定は完了です。

5.3.3 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」->「Outbound アクセス」の順にクリックします。

2. ID ドロップダウンリストから変更するルールの ID を選択します。または、「Outbound アクセス制御リスト」テーブルの該当ルール左部にある「えんぴつ」アイコ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. 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。

5.3.4 ルールの削除

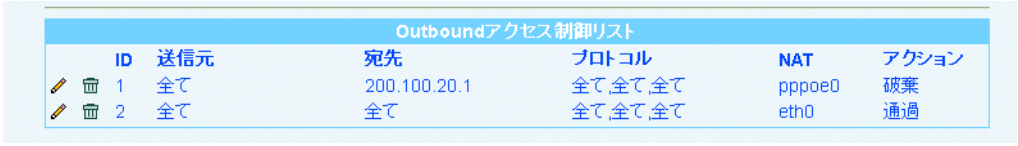
ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「Outbound アクセス」の順にクリックします。
2. ID ドロップダウンリストから削除するルールの ID を選択し「削除」ボタンをクリックします。または、「Outbound アクセス制御リスト」テーブルの該当ルール左部にある「ごみ箱」アイコンをクリックします。
3. 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。
4. 以上で設定は完了です。

5.3.5 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」->「Outbound アクセス」の順にクリックします。
2. 「Outbound 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。



5.3.6 「Outbound アクセス」ページの解説

「Outbound アクセス」ページについて解説します。「Outbound アクセス」ページでは本製品の送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。

5.3.6.1 Outbound アクセス制御設定

メニューから「ファイアウォール」->「Outbound 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 ドロップダウンリスト			ファイアウォールのルールを新規追加する場合は「新規追加」、既存のルールを変更 / 削除する場合は該当の ID 番号を選択します。
アクション	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。
	全て		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。
		アドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターの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。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合にのみ表示されます。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	タイプに「範囲指定」を選択した場合にのみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあらかじめ設定した IP プールで指定する場合に選択します。IP プールの設定方法については「P.129 IP プールの設定」を参照してください。

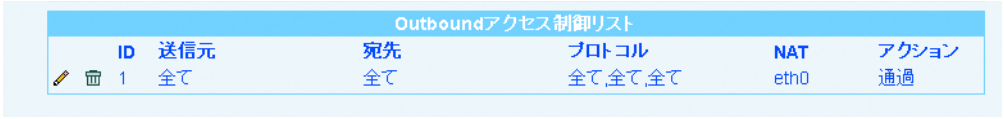
		IP プール	タイプに「IP プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の IP プール名をドロップダウンリストから選択します。
宛先			ルールを適用する宛先ネットワークの指定方法を選択します。
	全て		宛先のすべてのコンピューターにルールを適用する場合に選択します。
	IP アドレス		ルールを適用するコンピューターを IP アドレスで指定する場合に選択します。
		IP アドレス	タイプに「IP アドレス」を選択した場合にのみ表示されます。ルールを適用するコンピューターの IP アドレスを入力します。
	サブネット		ルールを適用するコンピューターをサブネット単位で指定する場合に選択します。
		アドレス	タイプに「サブネット」を選択した場合にのみ表示されます。ルールを適用するコンピューターの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。
	範囲指定		ルールを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
		始点 IP アドレス	タイプに「範囲指定」を選択した場合にのみ表示されます。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	タイプに「範囲指定」を選択した場合にのみ表示されます。指定する範囲の終点 IP アドレスを入力します。
	IP プール		ルールを適用するコンピューターをあらかじめ設定した IP プールで指定する場合に選択します。IP プールの設定方法については「P.129 IP プールの設定」を参照してください。
		IP プール	タイプに「IP プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の IP プール名をドロップダウンリストから選択します。
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。

	全て		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。
	全て		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。

	サービス		ポートを指定せずに、あらかじめ定義されたサービスにルールを適用する場合に選択します。
		サービス	タイプに「サービス」を選択した場合にのみ表示されます。ドロップダウンリストからルールを適用するサービスを選択します。サービスの設定方法については「P.139 サービスの設定」を参照してください。
プロトコル			宛先ポートパラメーターに「全て」、「ポート指定」、「範囲指定」を選択した場合に表示されます。「サービス」を選択した場合には表示されません。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。
NAT			ルールに設定する NAT の種類を選択します。
	未定義		ルールに NAT を設定しない場合に選択します。
	IP アドレス		IP アドレスを指定してルールに NAT を設定する場合に選択します。
		IP アドレス	NAT に「IP アドレス」を選択した場合にのみ表示されます。本製品で受信したパケットの転送先コンピューターの IP アドレスを指定します。
	NAT プール		ルールに設定する NAT をあらかじめ作成した NAT プールで指定する場合に選択します。NAT プールの作成方法については「P.134 NAT プールの設定」を参照してください。
		プール	NAT に「NAT プール」を選択した場合にのみ表示されます。あらかじめ設定されている既存の NAT プールから選択します。
ログ	有効 / 無効		ルールのログを記録する場合は「有効」、記録しない場合は「無効」ラジオボタンを選択します。
VPN	有効 / 無効		VPN 通信を使用する場合は「有効」、使用しない場合は「無効」を選択します。
「追加」ボタン			ID ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。ルールを追加登録します。Inbound/Outbound アクセスを合わせて 150 件までのルールを追加することができます。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			ID ドロップダウンリストで既存のルールの ID 番号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。

「削除」ボタン	ID ドロップダウンリストで既存のルールの ID 番号を選択した場合にアクティブになります。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

5.3.6.2 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。
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、サービス名、ポート番号が表示されます。
NAT	ルールに設定された NAT の内容が表示されます。
アクション	ルールに設定されたアクションです。通過 / 破棄のいずれかが表示されます。
「えんぴつ」アイコン	クリックすると「Outbound アクセス制御リスト」の該当ルールの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「Outbound アクセス制御リスト」から該当ルールを削除します。

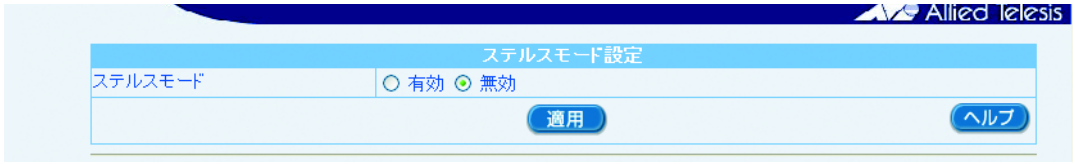
5.4 ステルスモードの設定

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。ただし、セルフアクセスルールで特定のポートをオープンしている場合は、そのポートに対しての応答を返します。セルフアクセスルールについては「P. 112 セルフアクセスルールの設定」を参照してください。

5.4.1 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」->「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。



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。
「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 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。セルフアクセスルールは「セルフアクセス」ページで設定します。

5.5.1 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。

プロトコル	ポート	方向
ICMP	0	LAN からのアクセス
TCP	80	LAN からのアクセス
UDP	161	LAN からのアクセス
UDP	162	LAN からのアクセス
UDP	53	LAN からのアクセス
TCP	10081	LAN からのアクセス
UDP	500	WAN からのアクセス

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 LAN 側コンピューターから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。

5.5.2 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」->「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. ドロップダウンリストから「新規追加」を選択します。

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

プロトコル	TCP
ポート	21
LAN 側からのアクセス	有効
WAN 側からのアクセス	無効

ヒント **セルフアクセスルールを設定する場合は「LAN 側からのアクセス」と「WAN 側からのアクセス」のうち、必ずどちらか一方を「有効」にする必要がありますのでご注意ください。**

4. 以上で設定は完了です。

5.5.3 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」->「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. ドロップダウンリストから変更するルールを選択します。または、「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「えんぴつ」アイコンをクリックします。
3. 各パラメーターを変更します。

アクセスの方向（「LAN 側からのアクセス」、「WAN 側からのアクセス」）のみ変更可能です。

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。

5.5.4 ルールの削除

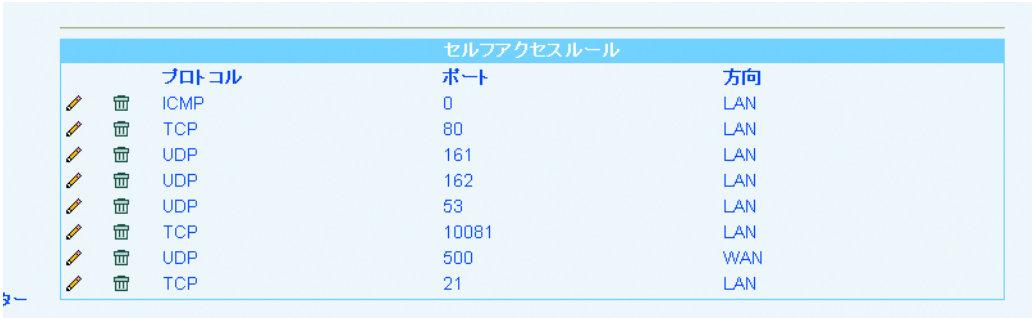
ルールを削除するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「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. ドロップダウンリストから削除するルールを選択し「削除」ボタンをクリックします。または、「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「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

5.5.5 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」->「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」テーブルにルールが一覧表示されます。



セルフアクセスルール

		プロトコル	ポート	方向
		ICMP	0	LAN
		TCP	80	LAN
		UDP	161	LAN
		UDP	162	LAN
		UDP	53	LAN
		TCP	10081	LAN
		UDP	500	WAN
		TCP	21	LAN

5.5.6 「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。

5.5.6.1 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
ドロップダウンリスト		セルフアクセスルールを新規に追加する場合は「新規追加」、既存のルールを変更 / 削除する場合は該当のルールを選択します。
プロトコル		ルールを適用するプロトコルを選択します。
ポート		プロトコルに「TCP」、「UDP」を選択した場合にのみ表示されます。ルールを適用するプロトコルで使用するポート番号を入力します。
LAN 側からのアクセス	有効 / 無効	LAN 側からの本製品へのアクセスを有効にするルールを作成する場合は「有効」、無効にするルールを作成する場合は「無効」ラジオボタンを選択します。本パラメーターを無効にした場合は、「WAN 側からのアクセス」を有効にする必要があります。
WAN 側からのアクセス	有効 / 無効	WAN 側からの本製品へのアクセスを有効にするルールを作成する場合は「有効」、無効にするルールを作成する場合は「無効」ラジオボタンを選択します。本パラメーターを無効にした場合は、「LAN 側からのアクセス」を有効にする必要があります。
「追加」ボタン		ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。ルールを追加登録します。50 件までのルール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ル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。
「削除」ボタン		ドロップダウンリストで既存ルールを選択した場合にアクティブになります。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

5.5.6.2 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
プロトコル	ルールが適用されるプロトコルが表示されます。
ポート	ルールが適用される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。
方向	有効なアクセスの方向が LAN/WAN のいずれかで表示されます。

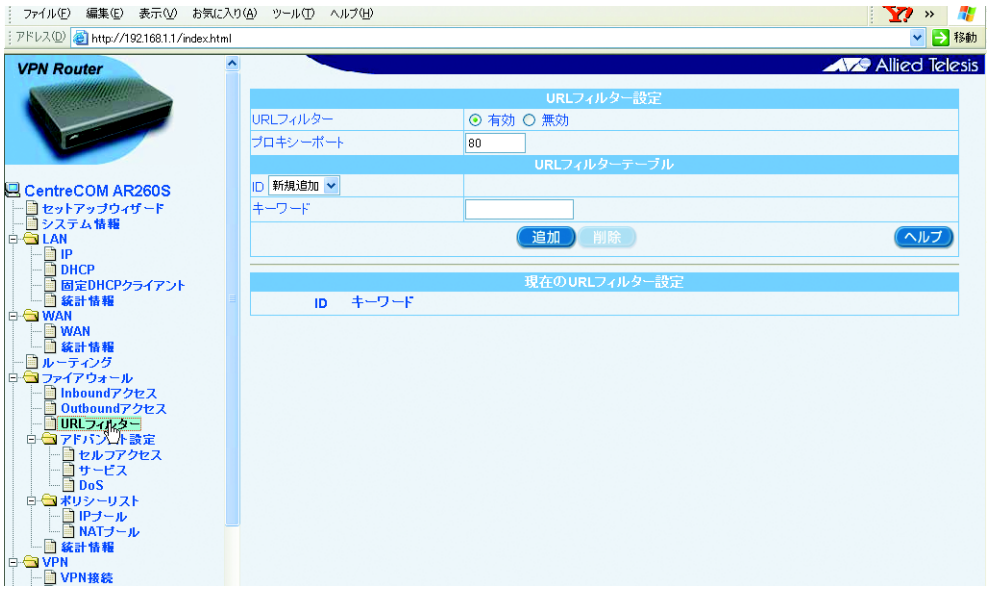
5.6 URL フィルターの設定

URL フィルターは、指定したキーワードを URL に含む Web サイトへのアクセスを制限する機能です。ここでは、URL フィルターの有効 / 無効、キーワードの追加方法、フィルターの確認を「URL フィルター」ページで行う手順について説明します。

5.6.1 URL フィルターの有効 / 無効

URL フィルターを有効 / 無効にするには以下の手順を実行します。また、コンピューターで使用しているプロキシーポートも指定します。

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



2.「URL フィルター設定」テーブルで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 URL フィルターを「有効」、プロキシーポートを「1080」に設定するものとします。

3. 以上で設定は完了です。

5.6.2 キーワードの追加

URL フィルターを有効にしたら、キーワードを追加します。キーワードを追加すると、そのキーワードを URL に含む Web サイトへのアクセスが制限されます。

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

2.「URL フィルターテーブル」の ID ドロップダウンリストから「新規追加」を選択します。

3. キーワードを入力し「追加」ボタンをクリックします。ここでは、キーワードに「abcnews」を指定するものとします。

4. 以上で設定は完了です。

5.6.3 プロキシーポートの変更

プロキシーポー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」->「URL フィルター」の順にクリックします。
2. 「現在の URL フィルター設定」テーブルの該当キーワード左部にある「えんぴつ」アイコンをクリックします。
3. プロキシーポートの値を変更します。
4. 「追加」ボタンをクリックします。
5. 以上で設定は完了です。

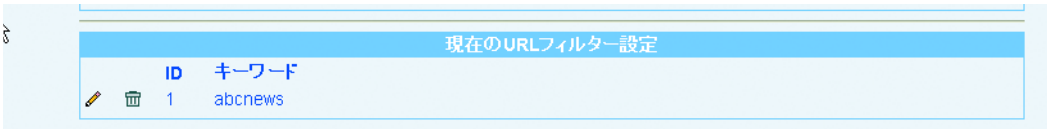
5.6.4 キーワードの削除

キーワード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」->「URL フィルター」の順にクリックします。
2. 「現在の URL フィルター設定」テーブルの該当キーワード左部にある「ごみ箱」アイコンをクリックします。または、「URL フィルターテーブル」の ID ドロップダウンリストから該当のキーワードを選択し「削除」ボタンをクリックします。
3. 以上で設定は完了です。

5.6.5 キーワードの確認

1. メニューから「ファイアウォール」->「URL フィルター」の順にクリックします。
2. 「現在のフィルター設定」テーブルにキーワードが一覧表示されます。



5.6.6 「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。「URL フィルター」ページでは、キーワードを指定して特定の Web サイトへのアクセスを制限できる URL フィルター機能に関する設定をします。

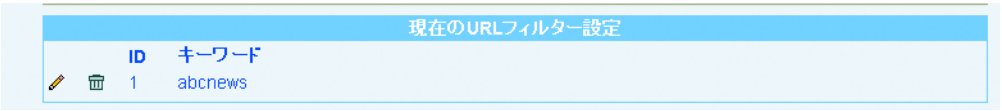
5.6.6.1 URL フィルター設定 /URL フィルターテーブル

URL フィルターの有効 / 無効を設定するテーブルです。メニューから「ファイアウォール」->「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
URL フィルター	有効 / 無効	URL フィルター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。
プロキシーポート		コンピューターの Web ブラウザーに設定したプロキシーポートの番号を入力します。ここでプロキシーポートを設定した場合でも、コンピューター側のブラウザーにもプロキシー設定をおこなってください。
ID		キーワードを新規に追加する場合は「新規追加」、既存のキーワードを削除する場合は該当のキーワードを選択します。
キーワード		URL フィルターに指定するキーワードを入力します。半角英数字で 15 文字以内で入力してください。
「追加」ボタン		ID ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。キーワードを追加登録します。10 件までのキーワード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。
「削除」ボタン		ID ドロップダウンリストで既存のキーワードを選択した場合にアクティブになります。選択したキーワードを削除します。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。
「ヘルプ」ボタン		操作のヒントを参照することができます。

5.6.6.2 現在のフィルター設定

現在設定されている URL フィルターが一覧表示されます。



パラメーター	説明
ID	キーワードの ID 番号が表示されます。
キーワード	指定されているキーワードが表示されます。
「えんぴつ」アイコン	クリックすると「現在の URL フィルター設定」の該当キーワードの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「現在の URL フィルター設定」から該当キーワードを削除します。

5.7 DoS アタックプロテクトの設定

DoS アタックとは、ネットワークのルーターなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃です。本製品には、有効 / 無効を設定できる DoS アタックプロテクトと、無条件に有効に設定されたプロテクトがあります。DoS アタックプロテクトの設定は「DoS」ページで行います。

無条件に設定されたプロテクトについては、プロテクトを無効にすることはできません。

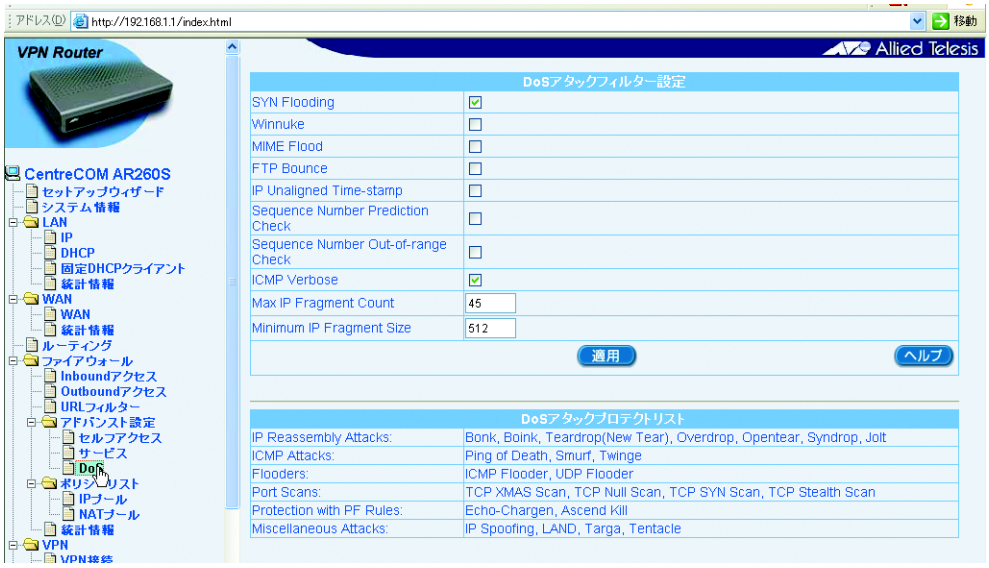
5.7.1 デフォルト設定

本製品では、「SYN Flooding」、「ICMP Verbose」に対してプロテクトが有効に設定されています。

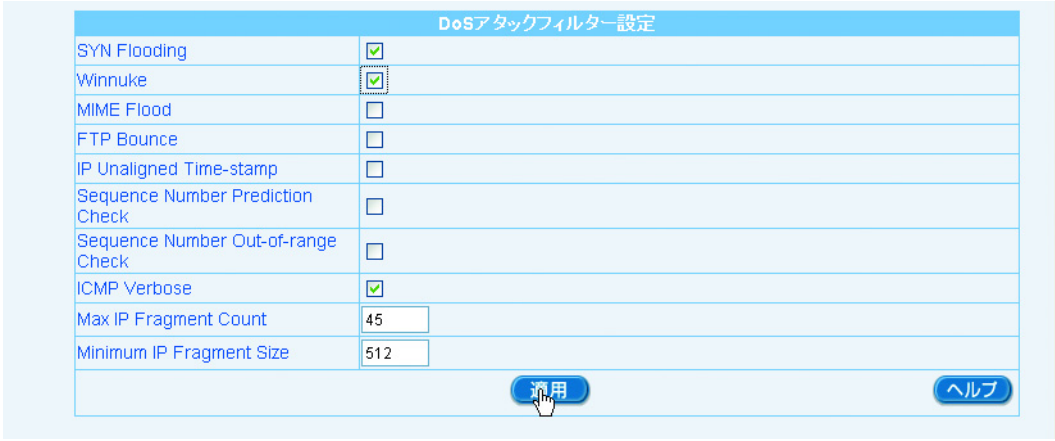
5.7.2 DoS アタックプロテクトの有効 / 無効

DoS アタックプロテクトを有効 / 無効に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」->「アドバンスト設定」->「DoS」の順にクリックします。



2. プロテクトを有効にする DoS アタックにチェックを入れ「適用」ボタンをクリックします。ここでは、「SYN Flooding」、「Winnuke」、「ICMP Verbose」に対するプロテクトを有効にするものとします。



3. 以上で設定は完了です。

5.7.3 DoS アタックプロテクトリストの確認

無条件にプロテクトを有効に設定されたアタックのリス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「ファイアウォール」->「アドバンスト設定」->「DoS」の順にクリックします。

2.「DoS アタックプロテクトリスト」に無条件に有効な DoS アタックプロテクトの一覧が表示されます。

5.7.4 「DoS」ページの解説

「DoS」ページについて解説します。「DoS」ページでは、DoS アタックに対するプロテクトの有効 / 無効を設定します。

5.7.4.1 DoS アタックフィルター設定

メニューから「ファイアウォール」->「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	説明
SYN Flooding	SYN Flooding に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは有効です。
Winnuke	Winnuke に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
MIME Flood	MIME Flood に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
FTP Bounce	FTP Bounce に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
IP Unaligned Time-stamp	IP Unaligned Time-stamp に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
Sequence Number Prediction Check	Sequence Number Prediction Check に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
Sequence Number Out of Range Check	Sequence Number Out of Range Check に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは無効です。
ICMP Verbose	ICMP Verbose に対するプロテクトを有効にする場合はチェックを入れます。デフォルトは有効です。
MAX IP Fragment Count	ファイアウォールを通過させるパケットのフラグメントサイズの最大しきい値を入力します。PPPoE で接続している場合には必ず入力してください。0 ～ 90 の

	範囲で入力してください。デフォルトは 45 です。
Minimum IP Fragment Size	ファイアウォールを通過させるパケットのフラグメントサイズの最小しきい値を入力します。1 ～ 65534 の範囲で入力してください。デフォルトは 512 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。

5.7.4.2 DoS アタックプロテクトリスト

本製品でプロテクトが有効になっているアタックが一覧表示されます。DoS アタックフィルター設定テーブルで設定した内容は反映されません。

DoSアタックプロテクトリスト	
IP Reassembly Attacks:	Bonk, Boink, Teardrop(New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP Attacks:	Ping of Death, Smurf, Twinge
Flooders:	ICMP Flooder, UDP Flooder
Port Scans:	TCP XMAS Scan, TCP Null Scan, TCP SYN Scan, TCP Stealth Scan
Protection with PF Rules:	Echo-Chargen, Ascend Kill
Miscellaneous Attacks:	IP Spoofing, LAND, Targa, Tentacle

パラメーター	**説明**
IP Reassembly Attacks	本製品でプロテクトが有効になっている IP Reassembly Attack の一覧が表示されます。
ICMP Attacks	本製品でプロテクトが有効になっている ICMP Attack の一覧が表示されます。
Flooders	本製品でプロテクトが有効になっている Flooder の一覧が表示されます。
Port Scans	本製品でプロテクトが有効になっている Port Scan の一覧が表示されます。
Protection with PF Rules	本製品でプロテクトが有効になっている Protection with PF Rule の一覧が表示されます。
Miscellaneous Attacks	本製品でプロテクトが有効になっている Miscellaneous Attack の一覧が表示されます。

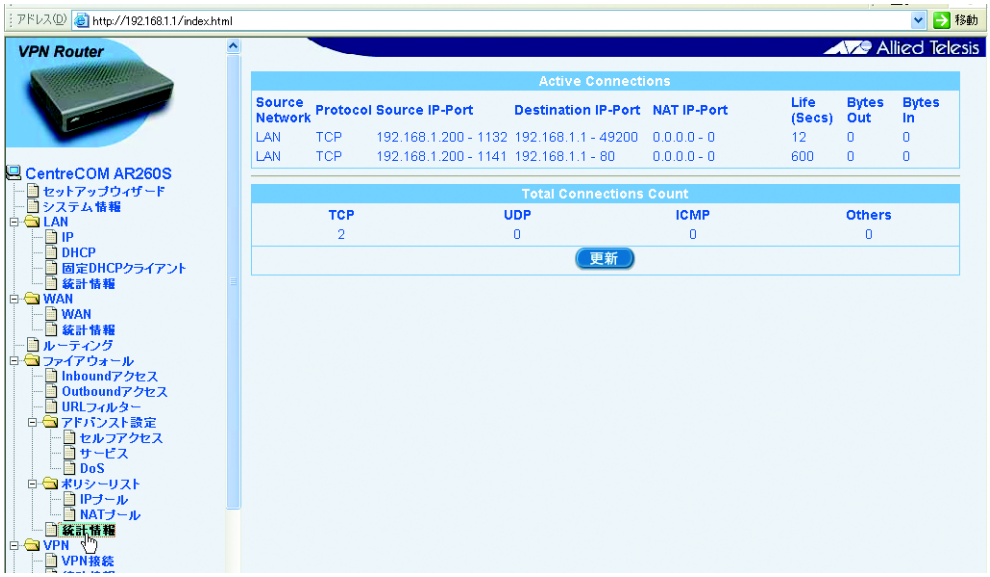
5.8 トラフィックの確認

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。

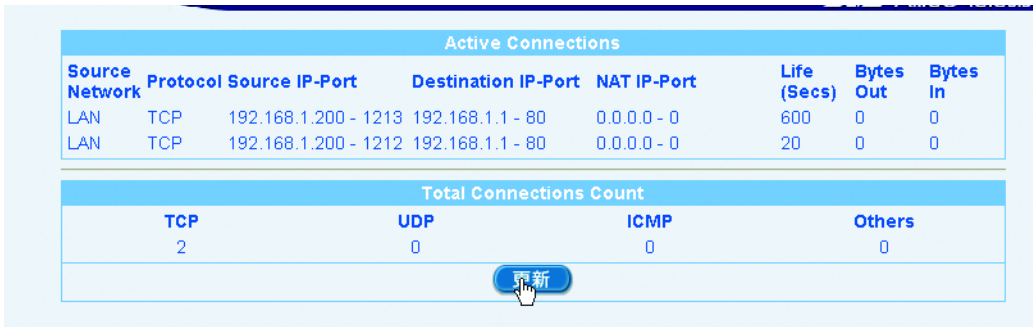
5.8.1 確認

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」->「統計情報」の順にクリックします。



2. ファイアウォール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。

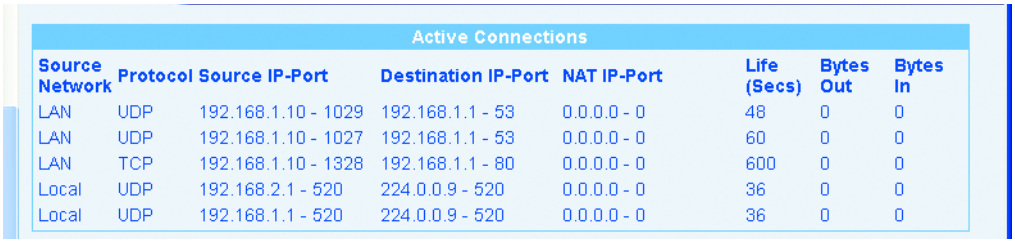


5.8.2 「統計情報」ページの解説

「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、ファイアウォールに関する統計情報を参照できます。

5.8.2.1 Active Connections

ファイアウォールを経由したセッションに関する情報が一覧表示されます。



Active Connections

Source Network	Protocol	Source IP-Port	Destination IP-Port	NAT IP-Port	Life (Secs)	Bytes Out	Bytes In
LAN	UDP	192.168.1.10 - 1029	192.168.1.1 - 53	0.0.0.0 - 0	48	0	0
LAN	UDP	192.168.1.10 - 1027	192.168.1.1 - 53	0.0.0.0 - 0	60	0	0
LAN	TCP	192.168.1.10 - 1328	192.168.1.1 - 80	0.0.0.0 - 0	600	0	0
Local	UDP	192.168.2.1 - 520	224.0.0.9 - 520	0.0.0.0 - 0	36	0	0
Local	UDP	192.168.1.1 - 520	224.0.0.9 - 520	0.0.0.0 - 0	36	0	0

パラメーター	説明
Souce Network	送信元のネットワークが表示されます。
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。

5.8.2.2 Total Connections Count

現在通信中のセッション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。
「更新」ボタン	クリックすると表示内容を更新します。

6　各種ポリシーとサービスの設定

6.1　概要

本製品では、ファイアウォールの Inbound/Outbound アクセスルールを作成する際の送信元、宛先、宛先ポート、NAT パラメーターに、あらかじめ作成したポリシー（IP プール、NAT プール）やサービスを指定することができます。ファイアウォールの設定内容によっては、パラメーターに指定するポリシーやサービスをあらかじめ作成しておくことで設定を容易にすることができます。本章では、以下のポリシーとサービスの設定について説明します。

- IP プール
- NAT プール
- サービス

6.2　IP プールの設定

IP プールは、複数の IP アドレスをプール（グループ）として命名し、ファイアウォール設定時のパラメーター指定を容易にするものです。ファイアウォール（Inbound/Outbound アクセス）の設定で、送信元または宛先パラメーターに使用します。IP プールの設定は「IP プール」ページで行います。

6.2.1　IP プールの追加

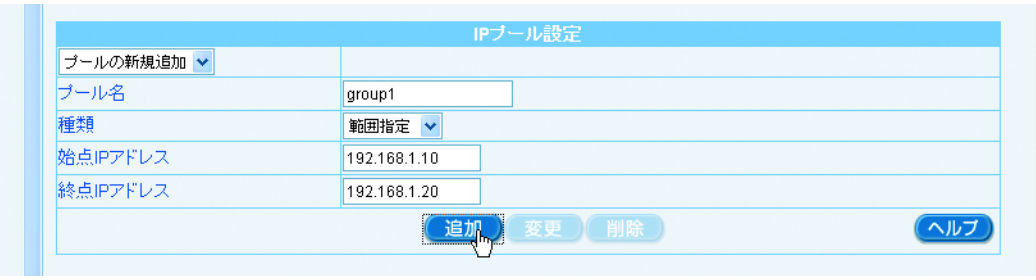
IP プールを追加するには以下の手順を実行します。

1. メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。

2. ドロップダウンリストから「プールの新規追加」を選択します。

3. 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 IP プールを設定するものとします。

プール名	group1
種類	範囲指定
始点 IP アドレス	192.168.1.10
終点 IP アドレス	192.168.1.20



4. 以上で設定は完了です。

6.2.2 IP プールの変更

IP 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」->「ポリシーリスト」->「IP プール」の順にクリックします。
2. ドロップダウンリストから変更する IP プールを選択します。または、「IP プールリスト」テーブルの該当プール左部にある「えんぴつ」アイコ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 IP プールの削除

IP プールを削除するには以下の手順を実行します。

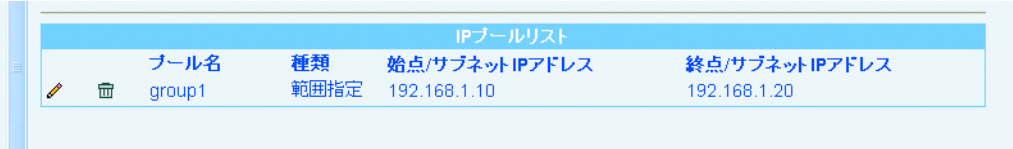
1. メニューから「ファイアウォール」->「ポリシーリスト」->「IP プール」の順にクリックします。
2. ドロップダウンリストから削除する IP プールを選択し、「削除」ボタンをクリックします。または、「IP プールリスト」テーブルの該当プール左部にある「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

6.2.4 IP プールの確認

IP プ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」->「ポリシーリスト」->「IP プール」の順にクリックします。

2.「IP プールリスト」テーブルに IP プールが一覧表示されます。



6.2.5 「IP プール」ページの解説

「IP プール」ページについて解説します。「IP プール」ページでは、IP プールを定義します。定義した IP プールは、Inbound/Outbound アクセスルールを設定する場合に使用します。

6.2.5.1 IP プール設定

IP プールを定義するテーブルです。メニューから「ファイアウォール」->「ポリシーリスト」->「IP 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
ドロップダウンリスト			IP プールを新規に追加する場合は「プールの新規追加」、既存の IP プールを変更 / 削除する場合は該当プールを選択します。
プール名			プール名を入力します。半角英数字で 15 文字以内で入力してください。
種類			プールの種類を選択します。
	範囲指定		IP アドレスの範囲を指定して IP プールを定義する場合に選択します。
		始点 IP アドレス	種類パラメーターに「範囲指定」を選択した場合にのみ表示されます。範囲を指定する IP アドレスの始点 IP アドレスを入力します。
		終点 IP アドレス	種類パラメーターに「範囲指定」を選択した場合にのみ表示されます。範囲を指定する IP アドレスの終点 IP アドレスを入力します。
	サブネット		サブネットを指定して IP プールを定義する場合に選択します。
		サブネットアドレス	種類パラメーターに「サブネット」を選択した場合にのみ表示されます。IP プールに指定するサブネットのサブネットアドレスを入力します。
		サブネットマスク	種類パラメーターに「サブネット」を選択した場合にのみ表示されます。IP プールに指定するサブネットのサブネットマスクを入力します。
	IP アドレス		IP アドレスを指定して IP プールを定義する場合に選択します。

	IP アドレス	種類パラメーターに「IP アドレス」を選択した場合にのみ表示されます。IP プールに指定する IP アドレスを入力します。
「追加」ボタン		ドロップダウンリストで「プールの新規追加」を選択した場合にアクティブになります。IP プールを追加登録します。50 件までのプール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 IP プール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。
「削除」ボタン		ドロップダウンリストで既存の IP プールを選択した場合にアクティブになります。選択した IP プールを削除します。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。
「ヘルプ」ボタン		操作のヒントを参照することができます。

6.2.5.2 IP プールリスト

設定された IP プールが一覧表示されます。

パラメーター	説明
プール名	IP プール名が表示されます。
種類	IP プールの種類（IP アドレス / 範囲指定 / サブネット）が表示されます。
始点 / サブネット IP アドレス	IP プールの種類が範囲指定の場合は始点 IP アドレス、サブネットの場合はサブネットアドレス、IP アドレスの場合は IP アドレスが表示されます。
終点 / サブネット IP アドレス	IP プールの種類が範囲指定の場合は終点 IP アドレス、サブネットの場合はサブネットアドレスが表示されます。種類が IP アドレスの場合は何も表示されません。
「えんぴつ」アイコン	クリックすると「IP プールリスト」の該当プールの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「IP プールリスト」から該当プールを削除します。

6.3 NAT プールの設定

NAT プールは、NAT タイプを指定して NAT を定義し、ファイアウォールポリシー（Inbound/Outbound アクセス）作成時に使用するための NAT のグループです。Inbound アクセスでは、スタティック / ダイナミック NAT、ENAT, インターフェース NAT、Outbound アクセスではスタティック / ダイナミック NAT、ENAT をポリシーに設定する場合は、あらかじめ NAT プールを作成する必要があります。NAT プールの設定は「NAT プール」ページで行います。本製品で設定できる NAT プールは以下のとおりです。

- スタティック NAT プール
- ダイナミック NAT プール
- ENAT プール
- インターフェース NAT プール

6.3.1 NAT プールの追加

NAT プール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「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。

2. ドロップダウンリストから「プールの新規追加」を選択します。

3. 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 NAT プールを設定するものとします。

プール名	enat1
プールタイプ	ENAT
NAT IP アドレス	1.1.1.1

4. 以上で設定は完了です。

6.3.2 NAT プールの変更

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」->「ポリシーリスト」->「NAT プール」の順にクリックします。
2. ドロップダウンリストから変更する NAT プールを選択します。または、「NAT プールリスト」テーブルの該当プール左部にある「えんぴつ」アイコ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。

6.3.3 NAT プールの削除

NAT プールを削除するには以下の手順を実行します。

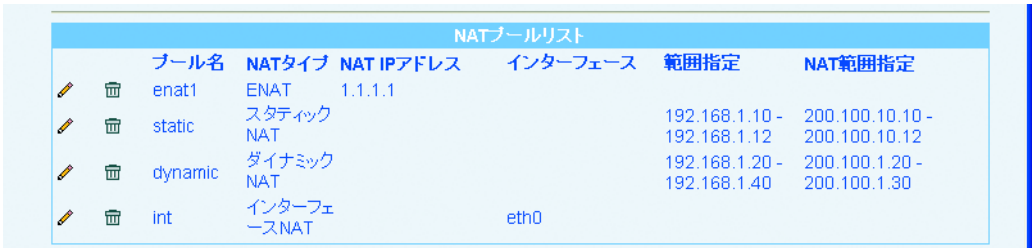
1. メニューから「ファイアウォール」->「ポリシーリスト」->「NAT プール」の順にクリックします。
2. ドロップダウンリストから削除する NAT プールを選択し、「削除」ボタンをクリックします。または、「NAT プールリスト」テーブルの該当プール左部にある「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

6.3.4 NAT プールの確認

NAT プ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」->「ポリシーリスト」->「NAT プール」の順にクリックします。

2.「NAT プールリスト」テーブルに NAT プールが一覧表示されます。



6.3.5 「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」ページでは、NAT プールを定義します。定義した NAT プールは、Inbound/Outbound アクセスルールを設定する場合に使用します。

6.3.5.1 NAT プール設定

NAT プールを設定するテーブルです。メニューから「ファイアウォール」->「ポリシーリスト」->「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。

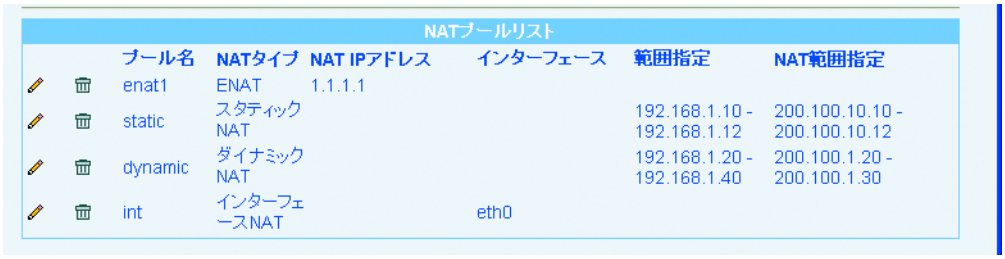
パラメーター	オプション	説明
ドロップダウンリスト		NAT プールを新規に追加する場合は「プールの新規追加」、既存のプールを変更 / 削除する場合は該当プールを選択します。
プール名		プール名を入力します。半角英数字で 15 文字以内で入力してください。
プールタイプ		NAT プールの指定方法を選択します。
	スタティック NAT	プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で変換する場合に選択します。ポート変換は行いません。1 対 1 で変換するため、グローバル IP アドレスはプライベート IP アドレスと同じ数にしてください。

	ダイナミック NAT	複数のプライベート IP アドレスを、複数のグローバル IP アドレスに変換する場合に選択します。ポート変換は行いません。動的に変換するため、グローバル IP アドレスはプライベート IP アドレスの数と同じである必要はありませんが、変換時に使用可能なグローバル IP アドレスがない場合にはパケットは破棄されます。
	ENAT	NAPT とも呼ばれます。複数のプライベート IP アドレスを、ポートを変換して 1 つのグローバル IP アドレスに変換する場合に選択します。
	インターフェース NAT	複数のプライベート IP アドレスを、ポートを変換して、WAN 側インターフェースのグローバル IP アドレスに変換する場合に選択します。
変換前の IP アドレス		プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。プライベート IP アドレスを指定します。
	始点 IP アドレス	プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。スタティック NAT/ダイナミック NAT に指定する始点 IP アドレスを入力します。
	終点 IP アドレス	プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。スタティック NAT/ダイナミック NAT に指定する終点 IP アドレスを入力します。
NAT IP アドレス		プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。グローバル IP アドレスを指定します。
	始点 NAT IP アドレス	プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。スタティック NAT/ダイナミック NAT に指定する始点 NAT IP アドレスを入力します。
	終点 NAT IP アドレス	プールタイプに「スタティック NAT」、「ダイナミック NAT」を選択した場合にのみ表示されます。スタティック NAT/ダイナミック NAT に指定する終点 NAT IP アドレスを入力します。
NAT IP アドレス		プールタイプに「ENAT」を選択した場合にのみ表示されます。ENAT で指定するグローバル IP アドレスを入力します。
NAT インターフェース		プールタイプに「インターフェース NAT」を選択した場合にのみ表示されます。インターフェース NAT に指定するインターフェースを eth0/pppoe0/pppoe1 から選択します。

「追加」ボタン	ドロップダウンリストで「プールの新規追加」を選択した場合にアクティブになります。IP プールを追加登録します。31 件までのプール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 NAT プール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。
「削除」ボタン	ドロップダウンリストで既存の NAT プールを選択した場合にアクティブになります。選択した NAT プールを削除します。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

6.3.5.2 NAT プールリスト

設定した NAT プールが一覧表示されます。



パラメーター	説明
プール名	プール名が表示されます。
NAT タイプ	NAT プールの種類が表示されます。
NAT IP アドレス	NAT タイプが ENAT の場合に NAT IP アドレスが表示されます。
インターフェース	インターフェース NAT の場合に、指定されたインターフェースが表示されます。
範囲指定	スタティック / ダイナミック NAT の場合に、指定したプライベート IP アドレスの範囲が表示されます。
NAT 範囲指定	スタティック / ダイナミック NAT の場合に、指定したグローバル IP アドレスの範囲が表示されます。

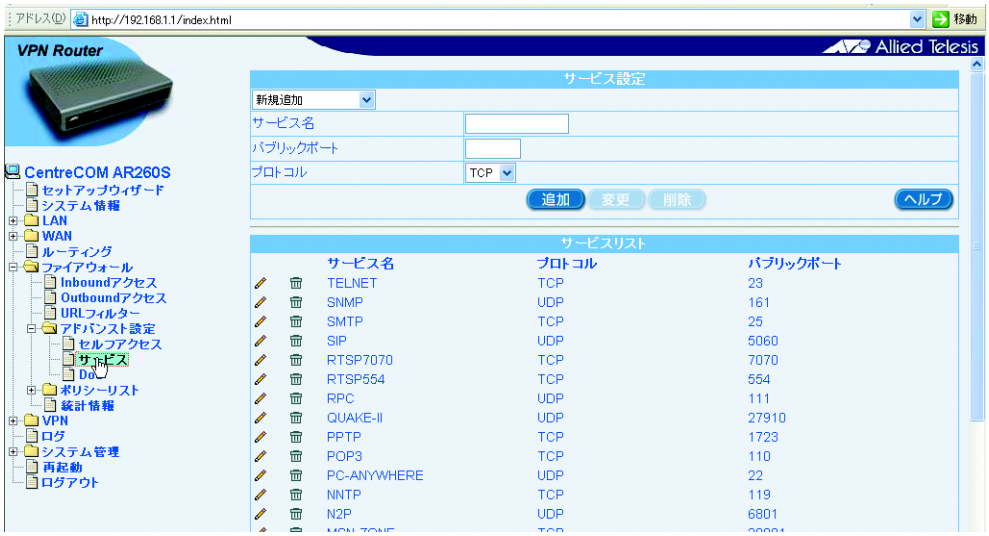
6.4 サービスの設定

サービスは、特定ポートを使用するアプリケーションです。ファイアウォールを設定する場合に宛先ポートパラメーターでサービスを選択する場合に使用します。本製品に既に登録されているサービス以外のサービスを指定する場合に、「サービス」ページで新たにサービスを定義して追加することができます。

6.4.1 サービスの作成

サービス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」->「アドバンスト設定」->「サービス」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。ここでは以下のように設定するものとします。

サービス名	service1
パブリックポート	1080
プロトコル	TCP

3. 以上で設定は完了です。

6.4.2 サービスの変更

サービス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」->「アドバンスト設定」->「サービス」の順にクリックします。
2. ドロップダウンリストから変更するサービスを選択します。または、「サービスリスト」テーブルの該当サービス左部にある「えんぴつ」アイコ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。

6.4.3 サービスの削除

サービス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」->「アドバンスト設定」->「サービス」の順にクリックします。
2. ドロップダウンリストから削除するサービスを選択し、「削除」ボタンをクリックします。または、「サービスリスト」テーブルの該当サービス左部にある「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

6.4.4 サービスの確認

サービス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」->「アドバンスト設定」->「サービス」の順にクリックします。

2.「サービスリスト」テーブルにサービスが一覧表示されます。

サービスリスト

		サービス名	プロトコル	パブリックポート
		TELNET	TCP	23
		SNMP	UDP	161
		SMTP	TCP	25
		SIP	UDP	5060
		RTSP7070	TCP	7070
		RTSP554	TCP	554
		RPC	UDP	111
		QUAKE-II	UDP	27910
		PPTP	TCP	1723
		POP3	TCP	110
		PC-ANYWHERE	UDP	22
		NNTP	TCP	119
		N2P	UDP	6801
		MSN-ZONE	TCP	28801
		MSN	TCP	1863
		MSG2	UDP	47624
		MSG1	TCP	47624
		L2TP	UDP	1701
		IRC	TCP	6667
		IMAP4	TCP	143
		ILS	TCP	389
		IKE	UDP	500
		ICQ-2002	TCP	5190
		ICQ-2000	TCP	5191
		HTTPS	TCP	443
		HTTP	TCP	80
		H323GK	UDP	1719
		H323	TCP	1720
		FTP	TCP	21
		FINGER	TCP	79
		DNS	UDP	53
		DIABLO-II	TCP	4000
		CUSEEME	TCP	7648
		BATTLE-NET-UDP	UDP	6112
		BATTLE-NET-TCP	TCP	6112
		AOL	TCP	5190

6.4.5 「サービス」ページの解説

「サービス」ページについて解説します。「サービス」ページでは、既存のサービスの変更 / 削除、サービスの新規登録を行います。

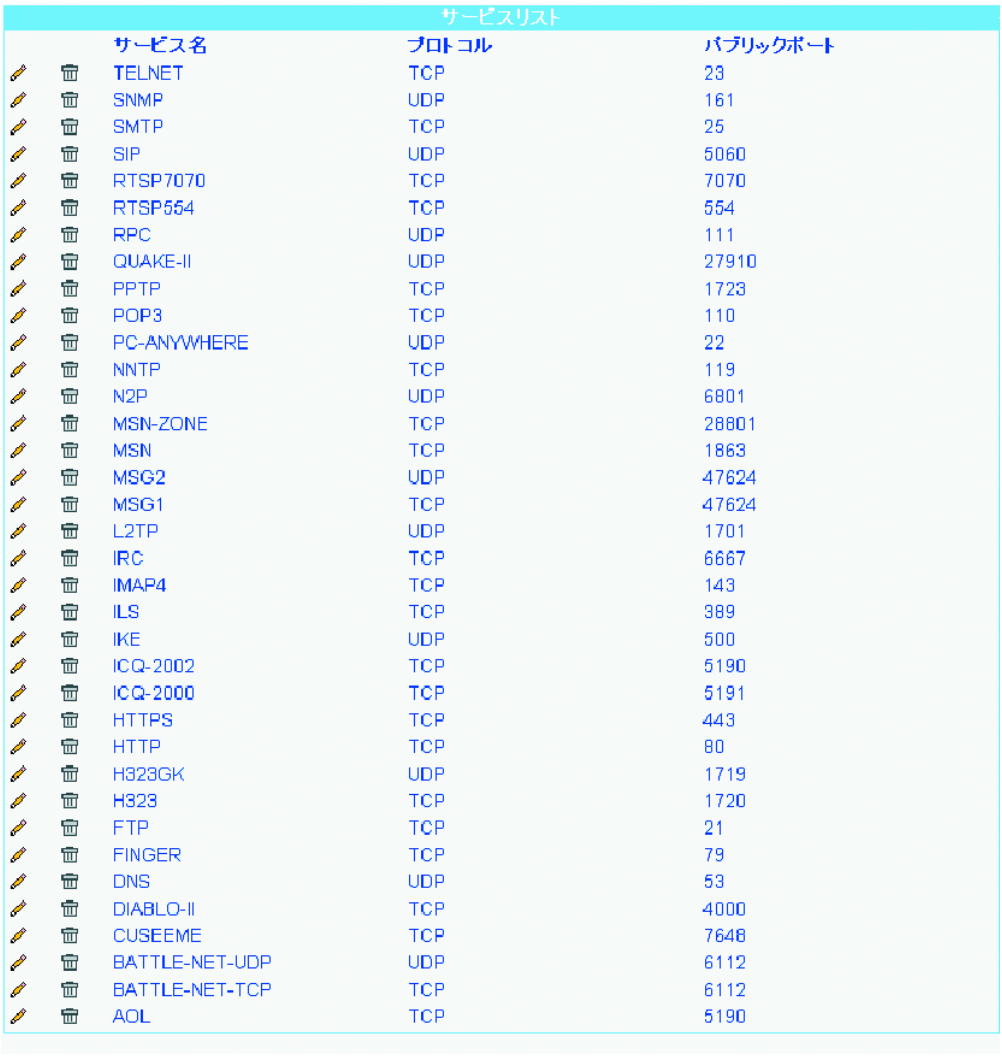
6.4.5.1 サービス設定

メニューから「ファイアウォール」->「アドバンスト設定」->「サービス」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	説明
ドロップダウンリスト	サービスを新規に追加する場合は「新規追加」、既存のサービスを変更 / 削除する場合は、該当サービスを選択します。
サービス名	サービス名を入力します。半角英数字で 15 文字以内で入力します。
パブリックポート	サービスで使用するポートの番号を入力します。
プロトコル	サービスで使用するプロトコルを選択します。
「追加」ボタン	ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。サービスを追加登録します。50 件までのサービス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サービス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。
「削除」ボタン	ドロップダウンリストで既存のサービスを選択した場合にアクティブになります。選択したサービスを削除します。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

6.4.5.2 サービスリスト

現在設定されているサービスが一覧表示されます。



サービスリスト

		サービス名	プロトコル	パブリックポート
		TELNET	TCP	23
		SNMP	UDP	161
		SMTP	TCP	25
		SIP	UDP	5060
		RTSP7070	TCP	7070
		RTSP554	TCP	554
		RPC	UDP	111
		QUAKE-II	UDP	27910
		PPTP	TCP	1723
		POP3	TCP	110
		PC-ANYWHERE	UDP	22
		NNTP	TCP	119
		N2P	UDP	6801
		MSN-ZONE	TCP	28801
		MSN	TCP	1863
		MSG2	UDP	47624
		MSG1	TCP	47624
		L2TP	UDP	1701
		IRC	TCP	6667
		IMAP4	TCP	143
		ILS	TCP	389
		IKE	UDP	500
		ICQ-2002	TCP	5190
		ICQ-2000	TCP	5191
		HTTPS	TCP	443
		HTTP	TCP	80
		H323GK	UDP	1719
		H323	TCP	1720
		FTP	TCP	21
		FINGER	TCP	79
		DNS	UDP	53
		DIABLO-II	TCP	4000
		CUSEEME	TCP	7648
		BATTLE-NET-UDP	UDP	6112
		BATTLE-NET-TCP	TCP	6112
		AOL	TCP	5190

パラメーター	説明
サービス名	サービス名が表示されます。
プロトコル	サービスで使用されるプロトコルが表示されます。
パブリックポート	サービスで使用されるポートの番号が表示されます。
「えんぴつ」アイコン	クリックすると「サービスリスト」の該当サービスの設定内容を変更することができます。
「ごみ箱」アイコン	クリックすると「サービスリスト」から該当サービスを削除します。

7 VPN の設定

7.1 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。

7.2 VPN の設定

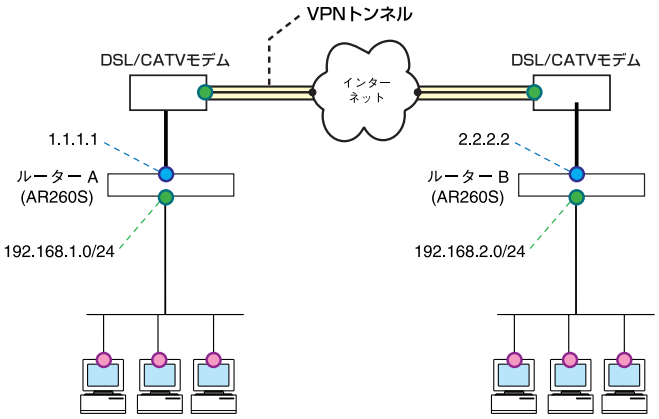
VPN トンネルでネットワーク間を接続するなど、VPN ゲートウェイ間で接続する場合に使用します。

7.2.1 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。

ヒント ポリシーを作成する前に、あらかじめ VPN サービスを有効にしておいてください。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。



1. メニューから「VPN」->「VPN 接続」の順にクリックします。

2. ID ドロップダウンリストから「新規追加」を選択します。

3. 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
VPN		有効
優先度		1
VPN 無通信監視		有効
無通信時間		60 秒
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

IKE 設定

IKE 交換モード	Main
事前共有鍵	atobkey
IKE 暗号化 / 認証アルゴリズム	全て

IPSec 設定

IPSec 暗号化 / 認証アルゴリズム	全て
PFS グループ	DH-2
有効期限	3600 秒 /75000KByte

4. ファイアウォールを有効にしている場合は、ファイアウォールで ISAKMP/IPSec のパケットが遮断されないように、以下の設定を含めた Outbound/Inbound アクセスのルールを追加します。Outbound/Inbound アクセスのルールの作成については「P. 93 ファイアウォールの設定」を参照してください。

Outbound アクセスのルール

アクション		通過
送信元	タイプ	サブネット
	アドレス	192168.1.0
	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
NAT			未定義
VPN			有効

Inbound アクセスのルール

アクション			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
NAT			未定義
VPN			有効

5. 以上で設定は完了です。

7.2.2 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. ID ドロップダウンリストから変更するポリシーを選択します。または、「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「えんぴつ」アイコ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。

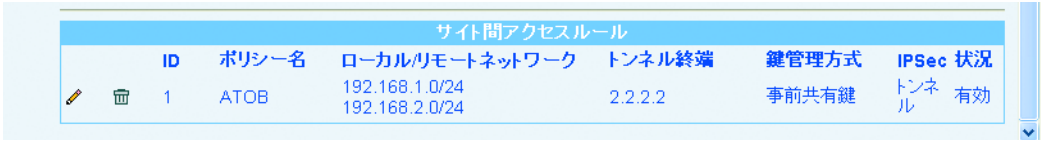
7.2.3 ポリシーの削除

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. ID ドロップダウンリストから削除するポリシーの ID を選択し「削除」ボタンをクリックします。または、「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「ごみ箱」アイコンをクリックします。
3. 以上で設定は完了です。

7.2.4 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。



7.2.5 「VPN 接続」ページの解説

「VPN 接続」ページについて解説します。

7.2.5.1 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 接続ポリシーを新規に追加する場合は「新規追加」、既存のポリシーを変更 / 削除する場合は該当ポリシーの ID 番号を選択します。
ポリシー名		ポリシー名を入力します。半角英数字で 31 文字以内で入力してください。
有効 / 無効		作成したポリシー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。
優先度		ポリシー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。ポ

			リシー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。
VPN 無通信監視	有効 / 無効		VPN の通信が「無通信時間」で指定した時間発生しなかった場合に、IPSec SA を削除する機能です。VPN 無通信監視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。
		無通信時間	VPN 無通信監視で「有効」を選択した場合にのみ表示されます。無通信時に IPSec SA を消去するまでの時間を 60 秒 ～ 600 秒の範囲で指定します。
ローカルセキュアグループ			VPN ポリシーを適用するローカルセキュアグループの指定方法を選択します。
	全て		LAN 側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	ローカル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	ローカル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	ローカル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。
	範囲指定		ポリシーを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
		始点 IP アドレス	ローカルセキュアグループの種類に「範囲指定」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 IP アドレスの範囲の始点 IP アドレスを入力します。
		終点 IP アドレス	ローカルセキュアグループの種類に「範囲指定」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 IP アドレスの範囲の終点 IP アドレスを入力します。
リモートセキュアグループ			VPN ポリシーを適用するリモートセキュアグループの指定方法を選択します。

全て		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。
範囲指定		ポリシーを適用するコンピューターを IP アドレスの範囲で指定する場合に選択します。
	始点 IP アドレス	リモートセキュアグループの種類に「範囲指定」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 IP アドレスの範囲の始点 IP アドレスを入力します。
	終点 IP アドレス	リモートセキュアグループの種類に「範囲指定」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 IP アドレスの範囲の終点 IP アドレスを入力します。

ローカルゲートウェイ		VPN 通信パケットを送受信するローカルのインターフェース（eth0/pppoe0/pppoe1）をドロップダウンリストから選択します。
リモートゲートウェイ		VPN ポリシーを適用するリモートゲートウェイの指定方法を選択します。
全て		VPN 接続のピアが AR260S の場合で、IP アドレスが固定されていない場合に選択します。「全て」を選択した場合「ローカル ID」と「リモート ID」を指定してください。
IP アドレス		リモートゲートウェイを IP アドレスで指定する場合に選択します。
	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。

ローカル ID			ISAKMP フェーズ 1 でリモートゲートウェイに送信する ID ペイロードの内容を指定します。IKE 設定の「IKE 交換モード」で「Aggressive」を選択した場合にのみ表示されます。おもに、本製品の IP アドレスが不定の場合に設定します。
	未定義		ID ペイロードの内容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 ID ペイロードに使用されます。
	IP アドレス		ID ペイロードの内容を IP アドレスで指定する場合に選択します。
		IP アドレス	「ローカル ID」で「IP アドレス」を選択した場合にのみ表示されます。ID ペイロードに指定する IP アドレスを入力します。
	FQDN		ID ペイロードの内容を FQDN(Fully Qualified Domain Name) で指定する場合に選択します。
		FQDN	「ローカル ID」で「FQDN」を選択した場合にのみ表示されます。ID ペイロードに指定する FQDN を入力します。
	E-mail		ID ペイロードの内容を E-mail アドレスで指定する場合に選択します。
		E-mail	「ローカル ID」で「E-mail」を選択した場合にのみ表示されます。ID ペイロードに指定する E-mail アドレスを入力します。
リモート ID			ISAKMP フェーズ 1 でリモートゲートウェイから受信する ID ペイロードの内容を指定します。IKE 設定の「IKE 交換モード」で「Aggressive」を選択した場合にのみ表示されます。おもに、リモートゲートウェイの IP アドレスが不定の場合に設定します。
	未定義		ID ペイロードの内容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 ID ペイロードに使用されます。
	IP アドレス		ID ペイロードの内容を IP アドレスで指定する場合に選択します。
		IP アドレス	「ローカル ID」で「IP アドレス」を選択した場合にのみ表示されます。ID ペイロードに指定する IP アドレスを入力します。
	FQDN		ID ペイロードの内容を FQDN(Fully Qualified Domain Name) で指定する場合に選択します。

	FQDN	「ローカル ID」で「FQDN」を選択した場合にのみ表示されます。ID ペイロードに指定する FQDN を入力します。
E-mail		ID ペイロードの内容を E-mail アドレスで指定する場合に選択します。
	E-mail	「ローカル ID」で「E-mail」を選択した場合にのみ表示されます。ID ペイロードに指定する E-mail アドレスを入力します。

7.2.5.2 IKE 設定

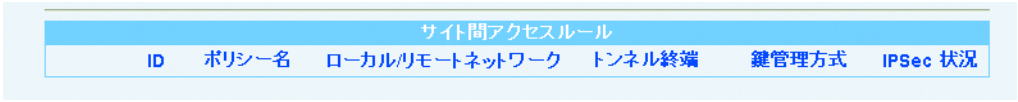
パラメーター		説明
IKE 交換モード		IKE 交換フェーズのモードを選択します。
	Main	Main モードを使用する場合に選択します。Main モードではネゴシエーション中の ID 情報を保護します。
	Aggressive	Aggressive モードを使用する場合に選択します。Aggressive モードではネゴシエーション中に ID 情報を保護しません。Main モードに比べて IKE トンネルの交換プロセスが少ないので処理が高速です。
事前共有鍵		事前共有鍵を入力します。半角英数字で 50 文字以内で入力してください。
IKE 暗号化 / 認証アルゴリズム		ドロップダウンリストから使用する暗号化 / 認証アルゴリズムの組み合わせを選択します。VPN 機器間の通信で双方がサポートするアルゴリズムの組み合わせを適用する場合は「全て」を選択してください。
有効期限		鍵の有効期限を設定します。単位は「秒」、「分」、「時間」、「日」から選択できます。IKE 暗号化 / 認証アルゴリズムに「全て」を選択した場合は設定できません。600 秒～ 30 日の範囲で設定してください。

7.2.5.3 IPSec 設定

パラメーター	説明
IPSec 暗号化 / 認証アルゴリズム	ドロップダウンリストから使用する暗号化 / 認証アルゴリズムの組み合わせを選択します。VPN 機器間の通信で双方がサポートするアルゴリズムの組み合わせを適用する場合は「全て」を選択してください。
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「未定義」を選択します。
有効期限	IPSec 暗号化 / 認証アルゴリズムにすべてを選択した場合は設定できません。単位を「秒」、「分」、「時間」、「日」または「Kbyte」から選択できます。300 秒～ 30 日、または 1000KBytes ～ 1000000KBytes の範囲で設定してください。
「追加」ボタン	ID ドロップダウンリストで「新規追加」を選択した場合にアクティブになります。VPN ポリシーを追加登録します。10 件までのポリシ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	ID ドロップダウンリストで既存のルールの ID 番号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。
「削除」ボタン	ID ドロップダウンリストで既存のルールの ID 番号を選択した場合にアクティブになります。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。
「ヘルプ」ボタン	操作のヒントを参照することができます。

7.2.6 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。
トンネル終端	リモートゲートウェイの IP アドレスが表示されます。
鍵管理方式	鍵管理方式が表示されます。
IPSec	IPSec の動作モードが表示されます。
状況	VPN の有効 / 無効が表示されます。

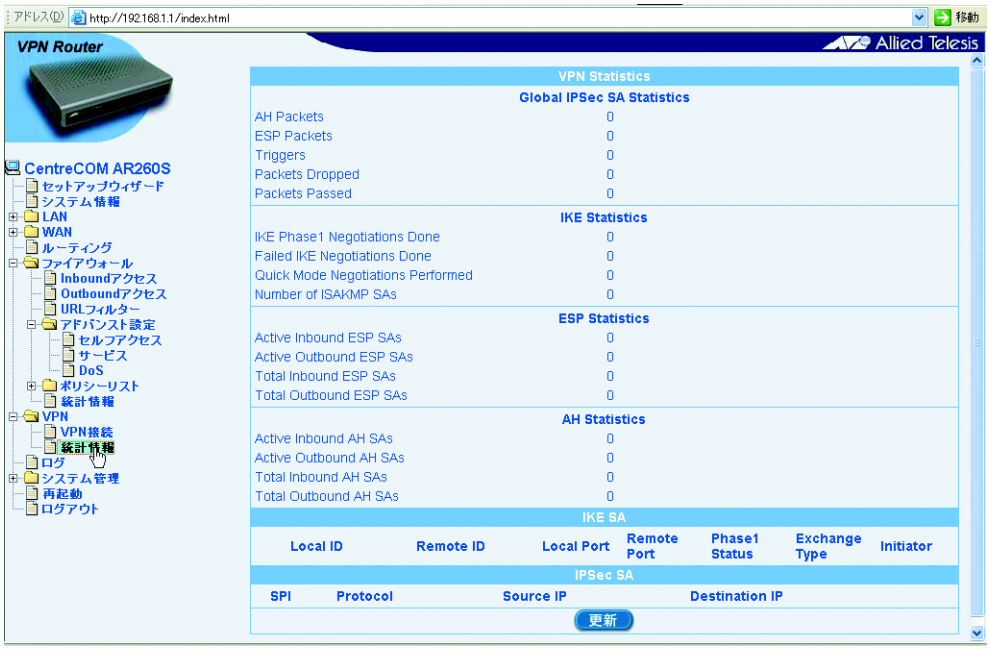
7.3 VPN トラフィックの確認

「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。

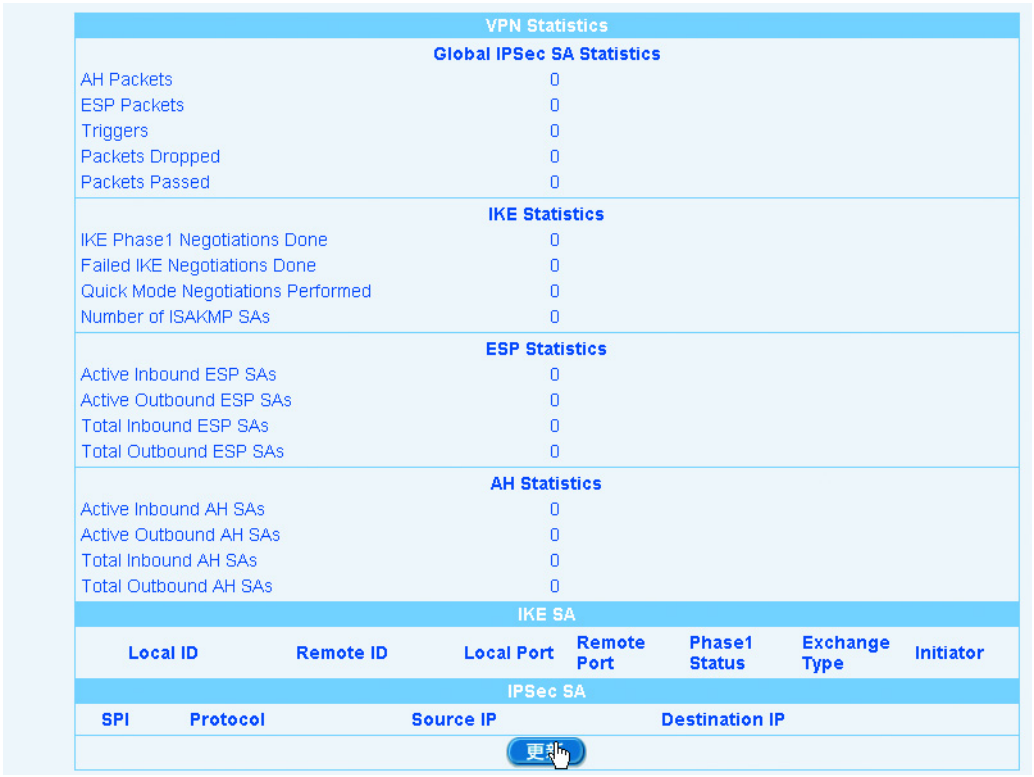
7.3.1 確認

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.「VPN Statistics」、「IKE SA」、「IPSec SA」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。

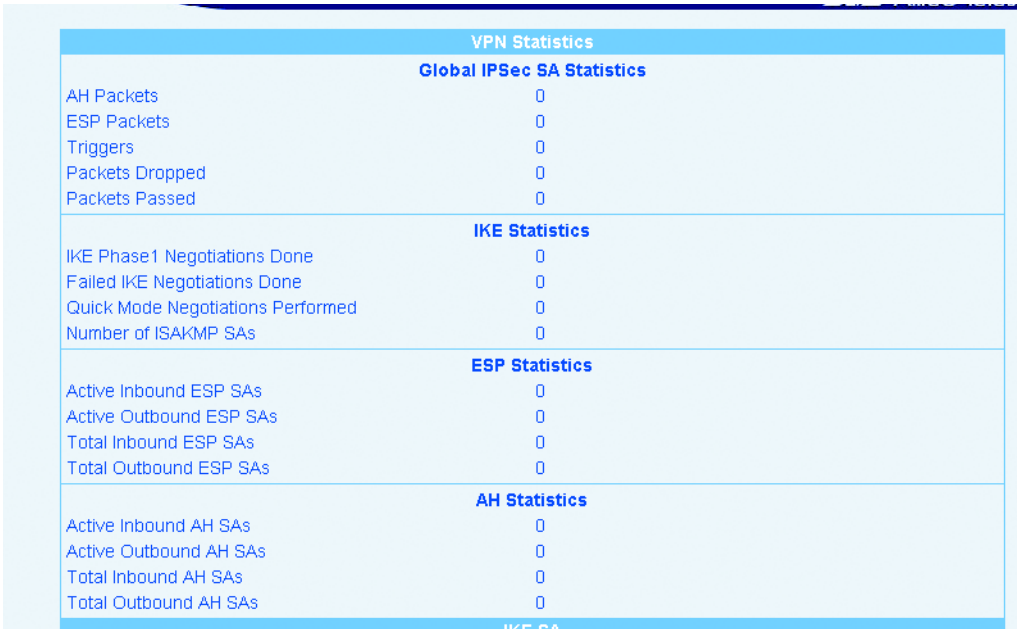


7.3.2 「統計情報」ページの解説

「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。

7.3.2.1 VPN Statistics

メニューから「VPN」->「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。



VPN Statistics	
Global IPSec SA Statistics	
AH Packets	0
ESP Packets	0
Triggers	0
Packets Dropped	0
Packets Passed	0
IKE Statistics	
IKE Phase1 Negotiations Done	0
Failed IKE Negotiations Done	0
Quick Mode Negotiations Performed	0
Number of ISAKMP SAs	0
ESP Statistics	
Active Inbound ESP SAs	0
Active Outbound ESP SAs	0
Total Inbound ESP SAs	0
Total Outbound ESP SAs	0
AH Statistics	
Active Inbound AH SAs	0
Active Outbound AH SAs	0
Total Inbound AH SAs	0
Total Outbound AH SAs	0

パラメーター	オプション	説明
Global IPSec SA Statistics		IPSec SA のパケットの統計情報が一覧表示されます。
	AH Packets	AH パケット数がカウントされます。
	ESP Packets	ESP パケット数がカウントされます。
	Triggers	LAN 側から IPSec パケット送信時、VPN トンネルを新規に作成する場合にカウントされます。
	Packets Dropped	破棄されたパケット数がカウントされます。
	Packets Passed	転送されたパケット数がカウントされます。
IKE Statistics		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。

	Failed IKE Negotiations Done	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。
	Quick Mode Negotiations Performed	完了したクイックモードでのネゴシエーション数がカウントされます。
	Number of ISAKMP SAs	フェーズ 1 の SA の数がカウントされます。
ESP Statistics		ESP に関する情報が一覧表示されます。
	Active Inbound ESP SAs	有効な Inbound ESP SA の数がカウントされます。
	Active Outbound ESP SAs	有効な Outbound ESP SA の数がカウントされます。
	Total Inbound ESP SAs	IKE SA が確立してからの Inbound ESP SA の総数がカウントされます。
	Total Outbound ESP SAs	IKE SA が確立してからの Outbound ESP SA の総数がカウントされます。
AH Statistics		AH に関する情報が一覧表示されます。
	Active Inbound AH SAs	有効な Inbound AH SA の数がカウントされます。
	Active Outbound AH SAs	有効な Outbound AH SA の数がカウントされます。
	Total Inbound AH SAs	IKE SA が確立してからの Inbound AH SA の総数がカウントされます。
	Total Outbound AH SAs	IKE SA が確立してからの Outbound AH SA の総数がカウントされます。

7.3.2.2 IKE SA

パラメーター	説明
Local ID	IKE SA 確立時のローカル ID が表示されます。
Remote ID	IKE SA 確立時のリモート ID が表示されます。
Local Port	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。
Remote Port	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。
Phase1 Status	フェーズ 1 のステータスが表示されます。
Exchange Type	IKE 交換モードが表示されます。
Initiator	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。

7.3.2.3 IPSec SA

パラメーター	説明
SPI	SPI（Security Parameter Index）が表示されます。
Protocol	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。
Source IP	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。
Destination IP	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。
「更新」ボタン	クリックすると表示内容を更新します。

8 付録

8.1 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。

8.1.1 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。

8.1.2 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
「LAN」/「DHCP」		
	IP アドレスプール	192.168.1.10 ～ 192.168.1.200
	サブネットマスク	255.255.255.0
	リース期限	14 日
	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
「WAN」/「WAN」		
	接続モード	PPPoE
	Unnumbered PPPoE	無効
	ホスト名	AR260S
	DNS オプション	自動取得
	MSS クランプ	有効
	MSS の値	40Bytes
	接続オプション	キープアライブ
	エコー送信間隔	60 秒

「ファイアウォール」/「アドバンスト設定」/「セルフアクセス」

	ステルスモード	無効
	セルフアクセスルール	ICMP（LAN 側）、TCP（80 番、LAN 側）、UDP（161 番、LAN 側）、UDP（162 番、LAN 側）、UDP（53 番、LAN 側）、TCP（10081 番、LAN 側）、UDP（500 番、WAN 側）

「ファイアウォール」/「アドバンスト設定」/「DoS」

	DoS アタックフィルター設定	SYN Flooding（有効）、Winnuke（無効）、MIME Flood（無効）、FTP Bounce（無効）、IP Unaligned Time-stamp（無効）、Sequence Number Prediction Check（無効）、Sequence Number Out-of-range Check（無効）、ICMP Verbose（有効）
		MAX IP Fragment Count: 45
		Minimum IP Fragment Size: 512

「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
	VPN	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」

	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）	AR260S

「システム管理」/「タイムゾーン設定」

	日付	2000 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	133.100.9.2
	SNTP サーバー 2	133.100.11.8
	SNTP サーバー 3	133.40.41.175
	SNTP サーバー 4	130.69.251.23
	SNTP サーバー 5	128.105.39.11
	更新間隔	60 分

「システム管理」/「SNMP」

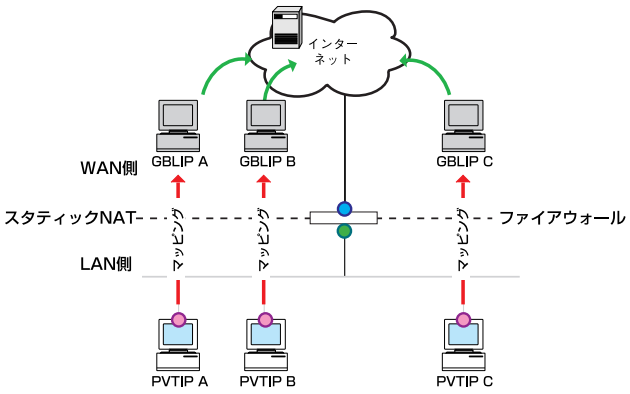
	SNMP	無効
	RO コミュニティー名	public
	RW コミュニティー名	private

8.2 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 NAT を使用することができます。

8.2.1 スタティック NAT

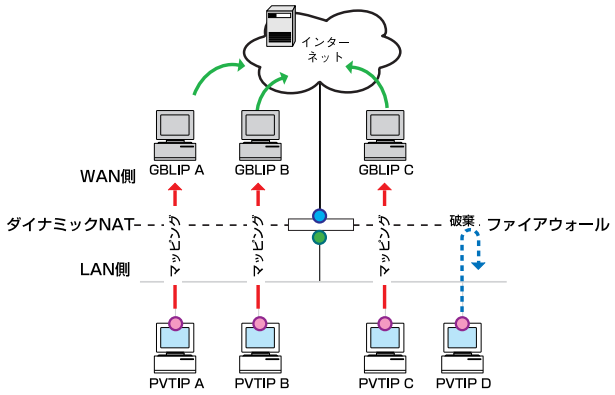
スタティック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で固定的にマッピングします。管理者が意図的に変更しない限りマッピングは固定的に行われます。つまり、1 台のクライアントのプライベート IP アドレスに対して、常に同じグローバル IP アドレスがマッピングされます。グローバル IP アドレスはプライベート IP アドレスと同じ数必要です。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

8.2.2 ダイナミック NAT

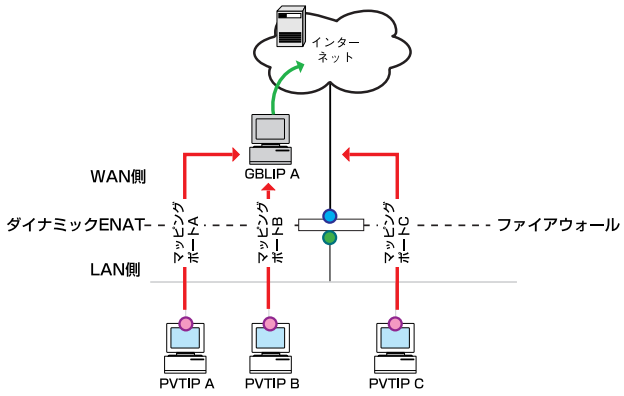
ダイナミック NAT では、プライベート IP アドレスをグローバル IP アドレスに 1 対 1 で動的にマッピングします。動的にマッピングするため、グローバル IP アドレスとプライベート IP アドレスの数は同じである必要はありませんが、使用できるグローバル IP アドレスがない場合、クライアントの送出したパケットは破棄されます。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

8.2.3 ENAT

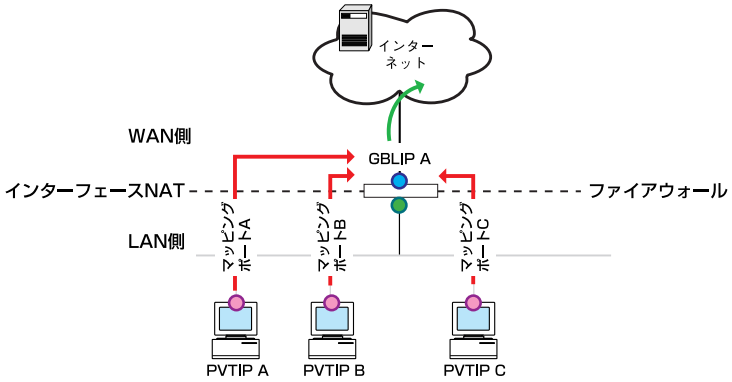
NAPT(Network Address and Port Translation)、または IP マスカレードとも呼ばれます。ENAT では、複数のプライベート IP アドレスに 1 つのグローバル IP アドレスと複数のポートをマッピングします。グローバル IP アドレスが 1 つのみの場合でも、異なるポートを使用して複数のクライアントからインターネットに接続することができます。



GBLIP=グローバルIPアドレス
PVTIP=プライベートIPアドレス

8.2.4 インターフェース NAT

インターフェース NAT 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

8.3 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。

8.3.1 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。

8.3.1.1 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。

8.3.1.2 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 30 秒以上経過していますか？本製品の起動には 30 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。

8.3.1.3 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、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。

8.3.2 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。

8.3.2.1 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 NAT が設定されています。

8.3.2.2 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。

8.3.3 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。

8.3.3.1 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.45 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。

8.3.3.2 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 ブラウザーのバージョンは Internet Explorer6 以降ですか？本製品でサポートするバージョンは Internet Explorer6 以上です。

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

- 本マニュアルは、アライドテレシス株式会社が作成したもので、すべての権利をアライドテレシス株式会社が保有しています。本書の全部または一部を弊社の同意なしにコピーまたは転載することを固くお断りいたします。
- アライドテレシス株式会社は、予告なく本マニュアルの一部または全体を修正、変更することがありますのでご了承ください。
- アライドテレシス株式会社は、改良のため予告なく製品の仕様を変更することがありますのでご了承ください。
- 本マニュアルについて、万一記載漏れ、誤りや不審な点等がございましたらご連絡ください。
- 本製品を運用して発生した結果については、上記の各項にかかわらず責任を負いかねますのでご了承ください。

商標について

- CentreCOM はアライドテレシス株式会社の登録商標です。
- Windows、MS-DOS、Windows NT 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。
- 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

2004 年 7 月 5 日　　Rev.A　　初校

アライドテレシス株式会社
PN J613-M0099-11 Rev.A 040705