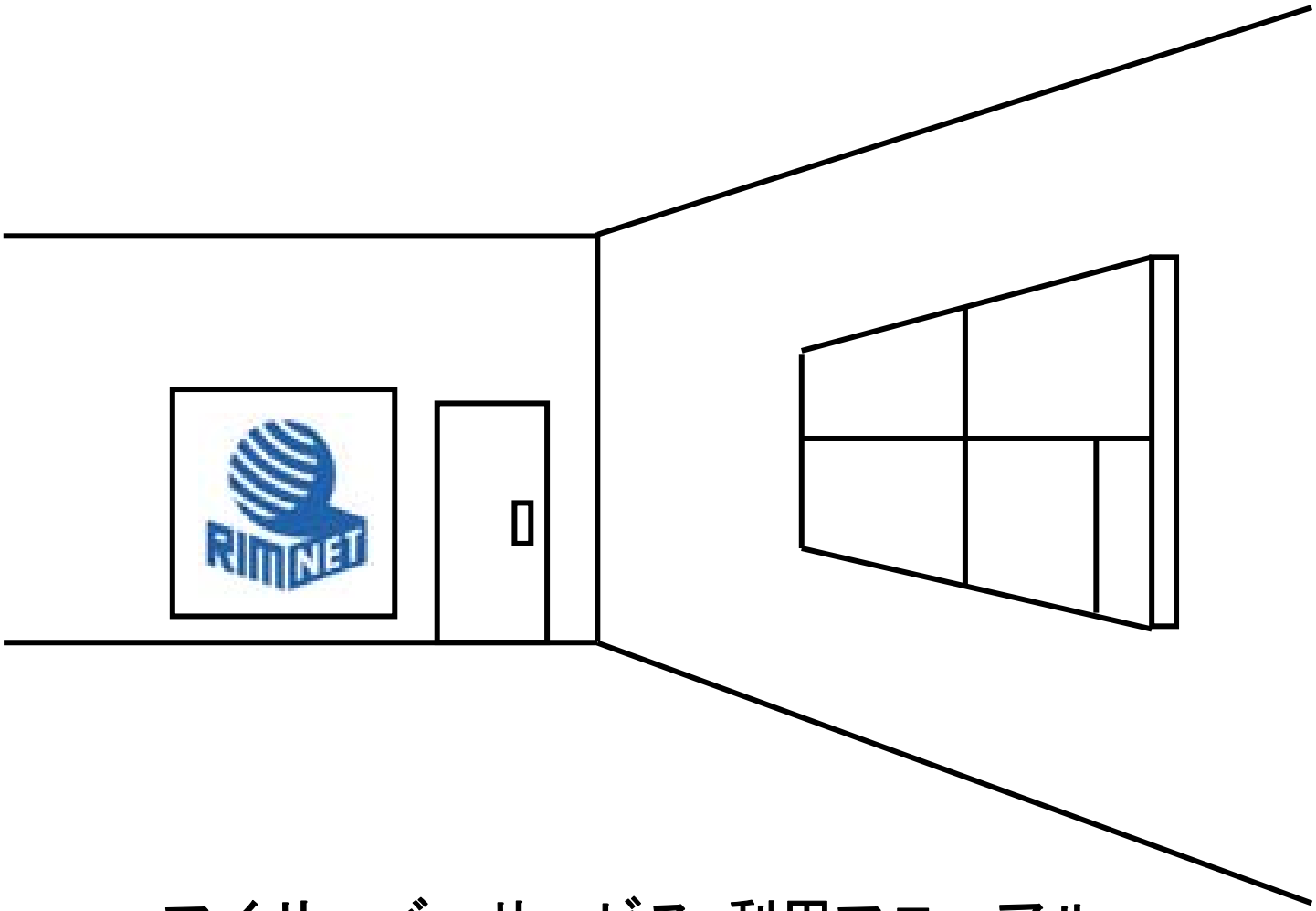


マイサーバーサービス 利用マニュアル
（セキュリティ / ファイアウォール）
マイサーバーVPS compact

RIMNET http://www.rim.or.jp/support/

Members Guide Book **2010/07**

はじめに

本利用マニュアルでは、マイサーバーVPS compact の「セキュリティ」及び「ファイアウォール」の設定を解説します。

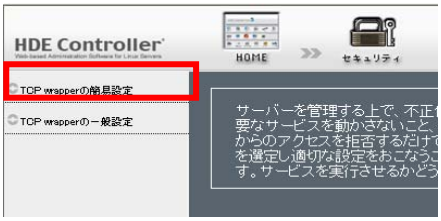
目次

１．セキュリティ

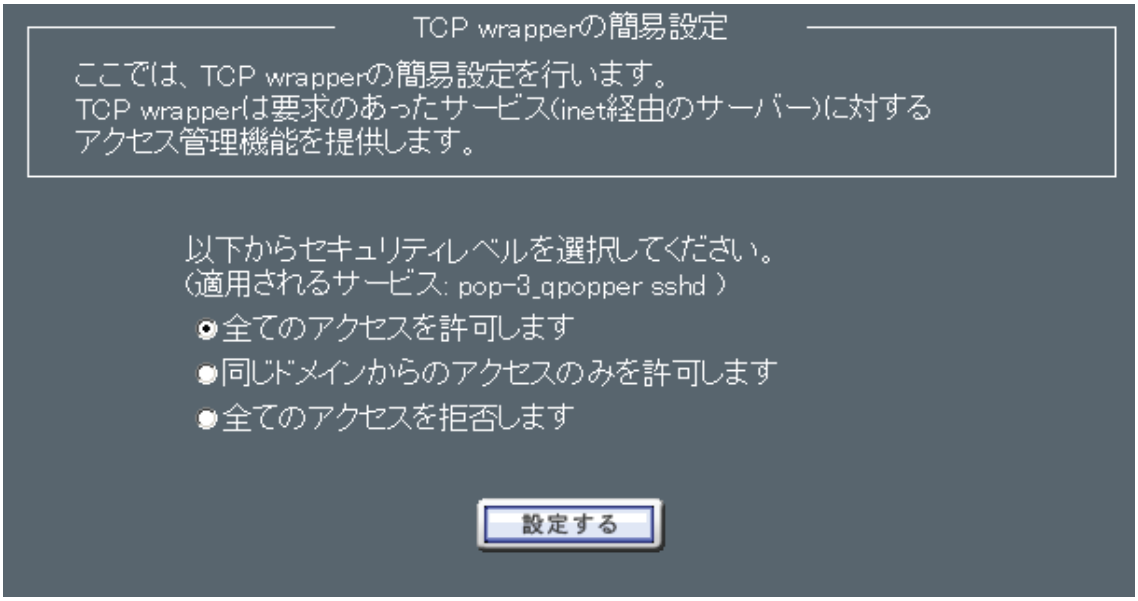
１－１．概要

本利用マニュアルでは、マイサーバーVPS compact の「セキュリティ」の設定を解説します。

１－２．TCP wrapper の簡易設定



外部からのアクセスに対する、セキュリティレベルを設定します。



●TCP wrapper の簡易設定

セキュリティレベルを、以下から選択します。

・全てのアクセスを許可します。

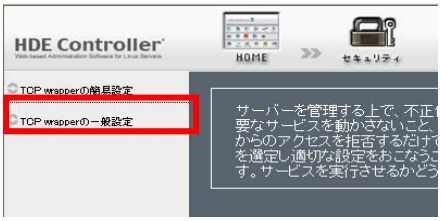
・同じドメインからのアクセスのみを許可します。

・全てのアクセスを拒否します。

「設定する」をクリックして設定を終了します。

TCP wrapper の一般設定でアクセスポリシーを設定されていた場合、この設定を行うことにより
上書きされますので、ご注意ください。

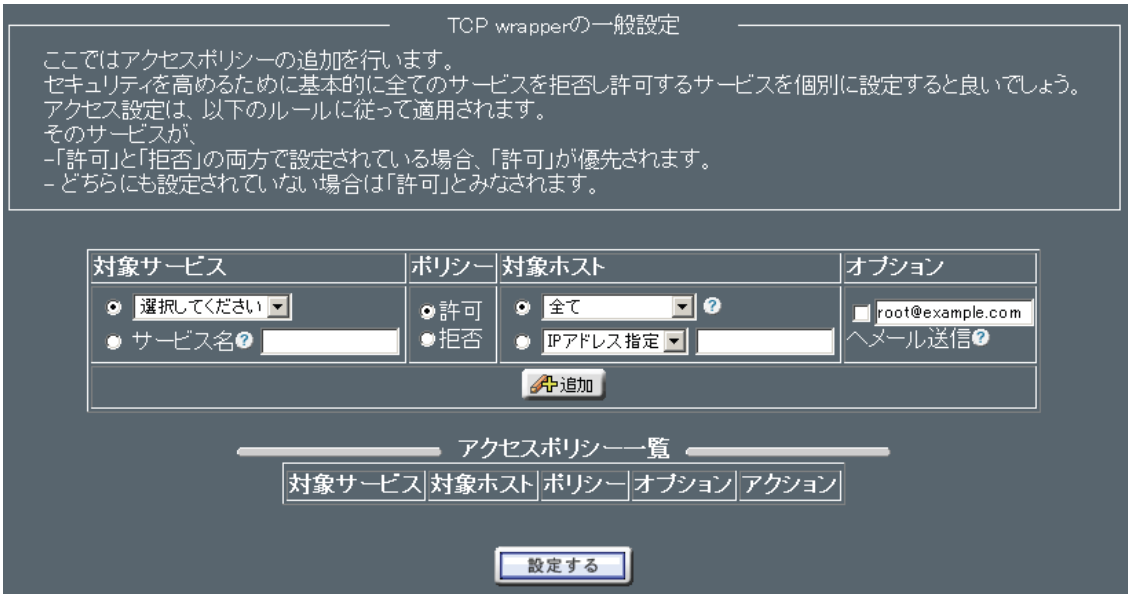
●TCP wrapper の一般設定



サービス毎にアクセスポリシーを決定し、セキュリティレベルを設定します。

●アクセスポリシーの追加

「対象サービス」のメニューからアクセスの規制の対象となるサービスを選択します。



アクセスのポリシーを「許可」、「拒否」のいずれか選択します。

対象ホストを、ネットワークの範囲を指定するか、IP アドレスを指定するか、選択します。

ネットワークの範囲は、
・全て(ALL)
・同じネットワーク
・同じドメイン、
いずれかを選択します。

「IP アドレス指定」を選択した場合は、対象となる IP アドレスを入力します。

規制の対象となるアクセスがあった際、管理者にメールで通知する場合は、「オプション」のチェックボックスにチェックを入れ、通知先となるメールアドレスを入力します。
次に、「追加」をクリックしてアクセスポリシーを追加します。

●既存のポリシーを削除する場合
アクセスポリシー一覧から「削除」をクリックします。

最後に、「設定する」をクリックして設定を終了します。

２．ファィアウォール

２－１．概要

本利用マニュアルでは、マイサーバーVPS compact の「ファイアウォール」の設定を解説します

２－２．ファイアウォールについて

●概要

ファイアウォールでは外部からのアクセスや攻撃を防御することをパケットフィルターで設定・管理することができます。

パケットフィルター系のメニューでの設定内容は、パケットフィルターの再起動、または Linux の再起動を行うことで反映されます。

●パケットフィルター

パケットフィルターは IP 層でのフィルタリングを行います。
アプリケーション層でのフィルタリングと違い、より高速にフィルタリング処理を行うことができます。
単純なパケットフィルタリングでは ftp のような複数ポートが関連付けられて処理をする場合などに完全対応することはできません。
HDE Controller では iptables のステートフル・インスペクションに対応していますので、このような場合も正確なフィルタリングを行うことができます。

パケットフィルターは下記の 3 種類を独立してフィルタリングすることができます。

●入力パケットフィルタリング

他のホストから送信されたパケットを受信するときのフィルタリングです。
ホスト=入力=>Linux

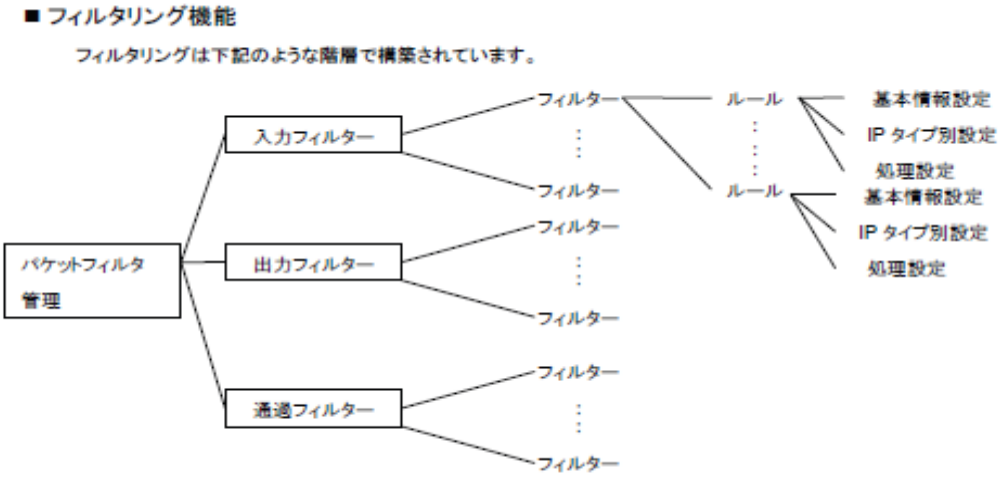
●出力パケットフィルタリング

他のホストへ送信するパケットのフィルタリングです。
ホスト<=出力=Linux

●通過パケットフィルタリング

他のホストから他のホストへ送信するパケットで、このサーバーを通過して送信されるようなパケットのフィルタリングです。

ホスト=入力=>Linux(転送)=出力=>ホスト



パケットフィルター管理は、入力フィルター、出力フィルター、通過フィルターの 3 つからなっています。

各 3 つのフィルターは、それぞれの複数のフィルターとして定義されています。
フィルターは、複数のルールを束ねた情報になります。

フィルターには個別に名称・コメント・有効化・簡易パケットフィルターへの表示(可視化)設定・ルールが設定できます。

●フィルター名

全てのフィルターには名前が必要です。
名前は英数字とアンダーラインでのみ構成でき(1 文字目は英字のみ)20 文字まで使用することができます。
フィルター名は受信・送信・通過別であれば同名を使用することができますが、その中では同名は使用できません。

●コメント

フィルターのコメントです。
使用目的などを記述するといいでしょう。
このコメントは「簡易パケットフィルター管理」の項目名を兼ねます。

●有効化

フィルターの有効化の設定です。
ここをチェックすると該当フィルターは有効になります。
一時的にフィルターをはずしたりするときに利用できます。

●可視化
「簡易パケットフィルター管理」で該当フィルターを表示するかどうかを指定します。
ここをチェックすると「簡易パケットフィルター管理」で表示されますが、チェックをはずすと表示されません。
日常の管理者には「簡易パケットフィルター管理」を渡す場合に、変更されたくないフィルターはチェックを外し、表示させないようにするといいでしょう。

●ルール
実際のフィルタリングルールの設定です。
フィルタリングルールはひとつのフィルターで複数個使用することができます。

●パケットフィルター画面構成
パケットフィルターの画面構成は下記のようになっています。

●パケットフィルター設定
パケットフィルターの全体的な設定を行います。
また、iptables としての設定もここで行います。

●パケットフィルター管理
フィルタリングルールの管理を行います。
HDE Controller で実現可能な設定項目はすべてここで設定を行うことが可能です。

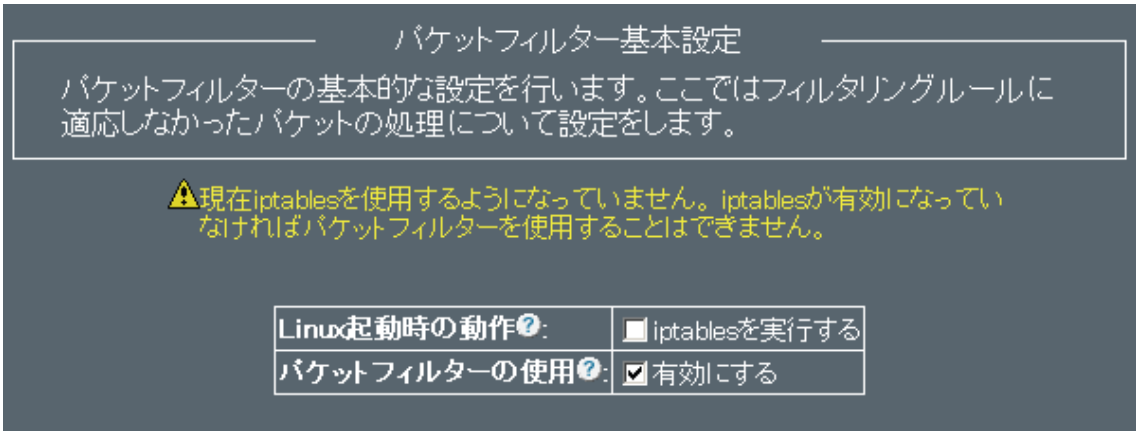
●簡易パケットフィルター管理
フィルタリングルールを簡易的に表示した管理画面です。
表示する項目は「パケットフィルター管理」メニューで修正することができます。

●パケットフィルター状態
フィルタリング状態を閲覧することができます。
この画面で iptables の起動・停止を行うこともできます。

２－２．パケットフィルター設定

パケットフィルター全体の設定を行います。
ここでの設定のほとんどはパケットのフィルタリング処理全体に影響します。

●基本設定



●Linux 起動時の動作

Linux を起動したときに同時にパケットフィルターを起動するかどうか指定をします。

チェックを付けると Linux を起動したときに同時に起動します。

iptables はパケットフィルターだけではなく、マスカレードやポートフォワード(NAPT)も構築します。

iptables を起動しなければマスカレードおよびポートフォワードを使用することはできません。

●パケットフィルターの使用

iptables を起動したときに、パケットフィルターを設定するかどうかを指定します。

チェックを付けると iptables の起動時にパケットフィルターを設定します。

●フィルター毎のデフォルトルール

各フィルター毎のデフォルト処理を設定します。

この設定は、各フィルターのフィルタリングルール全てに適応しなかった場合に適応されます。

パケット受信

受信するパケットのデフォルトルールを指定します。

「許可」を選ぶとパケットを受信し、「破棄」を選ぶとパケットを破棄します。

パケット送信

送信するパケットのデフォルトルールを指定します。

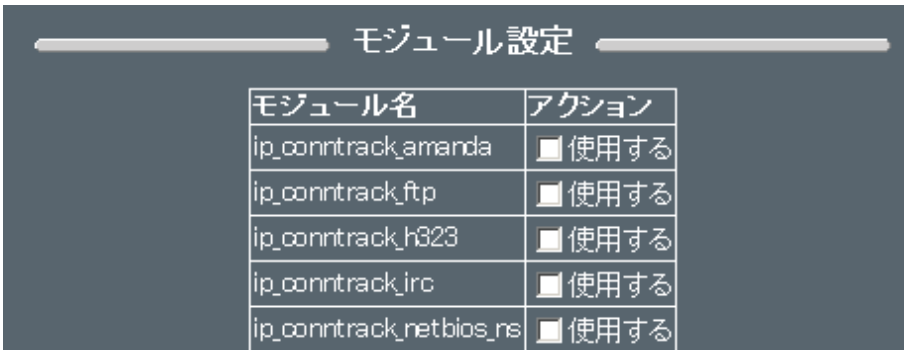
「許可」を選ぶとパケットを送信し、「破棄」を選ぶとパケットを破棄します。

パケット通過

通過するパケットのデフォルトルールを指定します。

「許可」を選ぶとパケットを通過転送し、「破棄」を選ぶとパケットを破棄します。

●高度な設定



●モジュール設定

iptables で使用するモジュールを設定します。

モジュールは主にステートフル系と NAT 系があります。

ステートフル系

このモジュールは主に複数ポートを用いるアプリケーションに対して制御を行う場合に使用します。

例えば ftp のアクティブ接続や IRC の DCC 機能などが該当します。

ステートフル系のモジュールは ip_conntrack で始まるモジュール名が該当します。

NAT 系

インターネットとのルーター・ゲートウェイを設置し、プライベートネットワークを構築した環境では

通常 NAT や NAPT を使用しますが、そのような環境で Linux を使用する場合、アプリケーション層のアドレス変換も行わなければなりません。

NAT 系のモジュールはそういった場合に使用します。

NAT 系のモジュールは ip_nat で始まるモジュール名が該当します。

iptables で使用するモジュールの詳細はインターネット上に公開される情報等をご確認下さい。

●その他の設定

TCP/IP の MSS の自動調整

ADSL 回線などでルーター・ゲートウェイにする場合にチェックします。

ここをチェックすることで、分断されたパケットを正確に送受信することができるようになります。

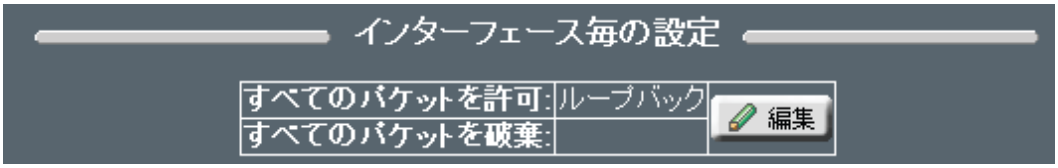
Web ブラウザなどで「一部のサイトが見られない」といった場合にチェックをいれると改善される場合があります。

２－３．パケットフィルター管理

フィルタリングルールの構築を行います。

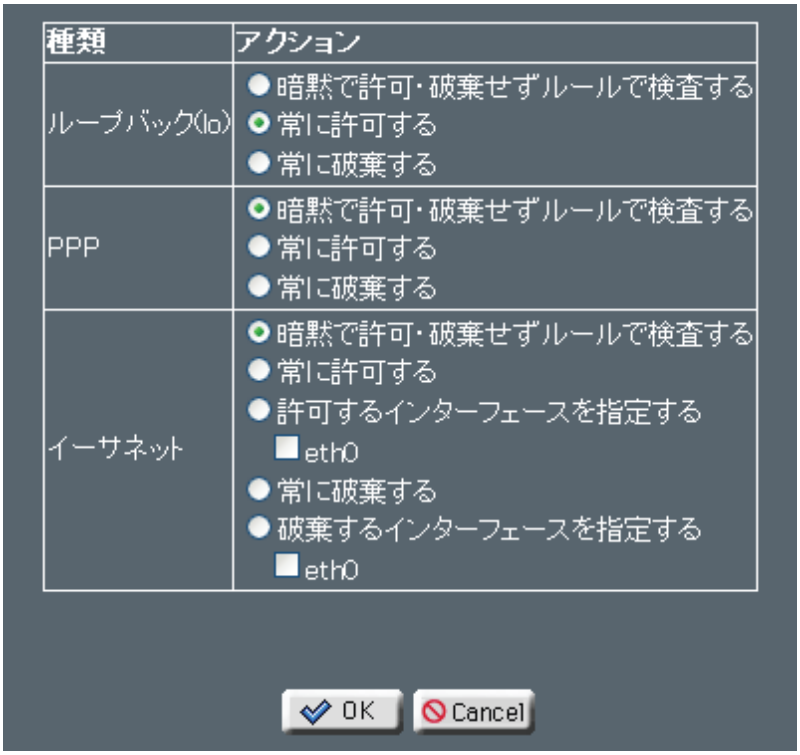
●インターフェース毎の設定

この画面ではネットワークインターフェース毎のパケットの処理を設定します。



ネットワークインターフェース毎にフィルタリングを行うときに使用します。

使用する場合は「編集」をクリックします。



ここの設定対象になったインターフェースを対象としたパケットはフィルタリングルールで検査されませんので注意してください。

●ループバック(lo)

ループバックインターフェース(lo)に対してのパケットの処理を設定します。

・ 暗黙で許可・破棄せずにルールで検査する

ループバックインターフェースに対するパケットをフィルタリングルールで検査します。

・ 常に許可する

ループバックインターフェースに対するパケットをすべて許可します。

・ 常に破棄する

ループバックインターフェースに対するパケットをすべて破棄します。

※ループバックインターフェースはほとんどの場合において常に破棄する必要はありません。

常に破棄すると多くのアプリケーションが処理を行えなくなる可能性があります

●PPP

・ 暗黙で許可・破棄せずにルールで検査する

PPP インターフェースに対するパケットをフィルタリングルールで検査します。

・ 常に許可する

PPP インターフェースに対してのパケットをすべて許可します。

・ 常に破棄する

PPP インターフェースに対してのパケットをすべて破棄します。

●イーサネット

・ 暗黙で許可・破棄せずにルールで検査する

インターフェース単位での許可・破棄はせずにすべての処理をフィルタリングルールの検査によって行います。

・ 常に許可する

イーサネットインターフェースに対してのパケットをすべて許可します。

・ 常に許可するインターフェースを指定する

指定されたイーサネットインターフェースに対してのパケットをすべて許可します。

・ 常に破棄する

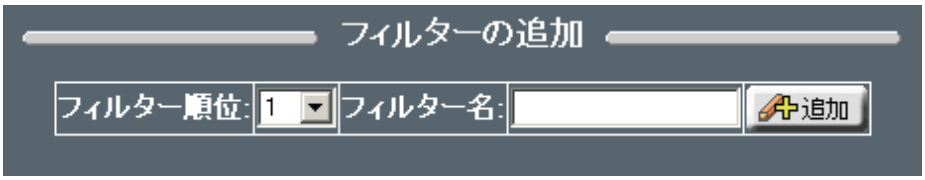
イーサネットインターフェースに対してのパケットをすべて許可します。

・ 常に破棄するインターフェースを指定する

指定されたイーサネットインターフェースに対してのパケットをすべて破棄します。

●フィルター追加

フィルター(フィルタリングルール群)を追加するときに使用します。



●フィルター順位

新規に追加する順位を指定します。

既にその番号の順位がある場合は下にずれることになります。

●フィルター名

フィルタリンググループ名を指定します。

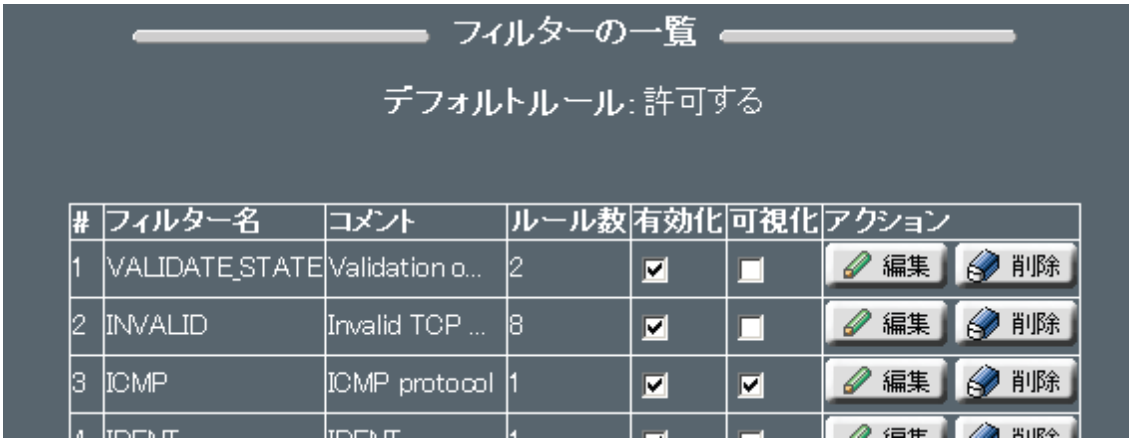
名前は半角英数字とアンダーラインの組み合わせで 20 文字まで指定できます。

●フィルター一覧

登録されているフィルターグループの一覧です。

各項目は「フィルタリング機能」を参照ください。

各項目を記入し、「追加」をクリックするとフィルターが追加されます。



フィルタリングルールを設定するため追加されたフィルター名の「編集」をクリックします。

●ルール管理

ルール管理ではフィルター内に定義するフィルタリングルールの管理を行います。

また、フィルターの名称・コメントなどの設定をすることもできます。

●フィルター設定

フィルタリングルールを管理するフィルターの設定を行います。

●フィルター名

フィルター名を設定します。有効文字数などはフィルター管理の画面に準じます。

●コメント

フィルターにコメントを設定します。

ここで設定したコメントが「簡易パケットフィルター管理」メニューの一覧表示に使用されます。

●有効化

フィルタリンググループをパケットフィルタリングの設定に使用するかどうかを指定します。

●可視化

「簡易パケットフィルター管理」メニューで該当フィルタリングルールを表示するかどうかを指定します。

※可視化を有効に使うことで、サーバー設置者が「パケットフィルター管理」メニューでフィルタリングルールを構築し、操作されたくないフィルタリングルールの可視化のチェックボックスをはずす、サーバー運用者が「簡易パケットフィルター管理」メニューを用いて 設定の調整を行うといったことができます。

●ルール追加

フィルタリングルールを追加します。フィルタリングルールの追加はルール順位で追加する順位を指定します。

追加したルールは「すべてのパケットを許可」として追加されるので、該当番号の「編集」をクリックし、

フィルタリングルールの編集作業に入ります。

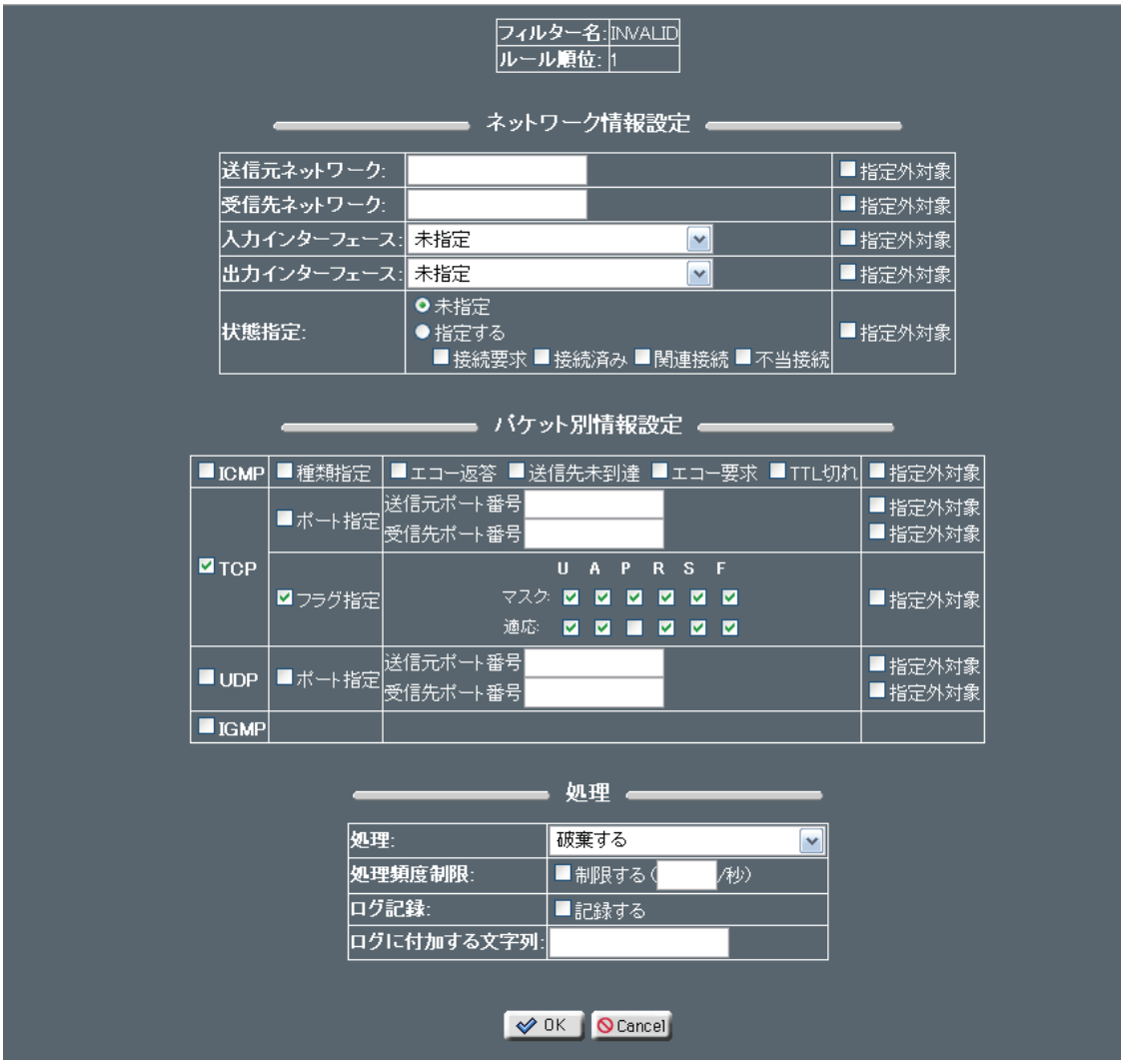
●ルール一覧

フィルターに含まれるルールの一覧です。「編集」をクリックすることで各ルールを編集することができます。

※指定外対象をチェックすることで入力値以外を対象とする設定が可能です。

●ルール設定

この画面ではフィルタリングルールの設定を行います。



●基本情報

基本情報はフィルタリングルールの順位とルールが含まれるフィルター名が表示されます。

ネットワーク情報設定

ネットワーク設定はパケット検査の基本的な設定を行います。

●送信元ネットワーク

パケットの送信元ネットワークの情報を設定します。

パケットを受信・通過転送をする場合はこの項目はパケットの送信元を指定します。

パケットを送信する場合はこの項目は自分自身のネットワークのいずれかを指定します。

未指定の場合はすべてのネットワークからのパケットが対象になります。

●受信先ネットワーク

パケットの送信先ネットワークの情報を設定します。

パケットを受信する場合はこの項目は自分自身のネットワークのいずれかを指定します。

パケットを送信・通過転送をする場合はこの項目はパケットの送信先を指定します。

未指定の場合はすべてのネットワークからのパケットが対象になります。

●入力インターフェース

パケットを受信・通過転送するときのインターフェースを指定します。

インターフェースは固有の名称(eth0 など)でも指定できますし、インターフェースの

カテゴリー(すべてのイーサネットインターフェースなど)という指定もできます。

入力インターフェースの設定は送信フィルターでは使用しません。

未指定の場合はすべてのインターフェースからのパケットが対象になります。

●出力インターフェース

パケットを送信・通過転送するときのインターフェースを指定します。

インターフェースは固有の名称(eth0 など)でも指定できますし、インターフェースの

カテゴリー(すべてのイーサネットインターフェースなど)という指定もできます。

出力インターフェースの設定は受信フィルターでは使用しません。

未指定の場合はすべてのインターフェースからのパケットが対象になります。

●状態指定

パケットに関連するネットワークのセッション接続状態による検査を行います。

未指定

パケットのセッション接続の検査は行いません。

指定する

パケットのセッション接続の検査を行います。

状態検査は下記種類のいずれかを組合わせて指定できます。

接続要求	新規にセッション確立を要求するパケット(ACK)を対象とします
接続済み	既に接続されているセッションのパケットを対象とします
関連接続	複数ポートでセッションが確立しているパケットを対象とします
不当接続	TCPフラグが不正な場合など不当なパケットを対象とします

指定外対象をチェックすることで入力値以外を対象とする設定が可能です。

●パケット別情報

対象になるパケットのプロトコルの設定をします。

ICMP・TCP/IP・UDP・IGMP の指定ができ、指定する場合はプロトコルのチェックボックスをチェックします。

いずれのプロトコルのチェックをしなかった場合はすべてのプロトコルが対象になります。

エコー返答	エコー要求(ping)への返答(pong)パケットです。主にpingコマンドで使用されます。
送信先未到達	送信先機器が無かった場合のルーターなどからの返答です
エコー要求	エコー要求(ping)パケットです。主にpingコマンドで使用されます。
TTL切れ	パケットの生存期間(TTL)が切れた時の応答パケットです。 主にtracerouteなどで利用されます。

●TCP

TCP/IP のチェックボックスにチェックを入れると、

TCP/IP パケットを対象とした検査を行います。TCP/IP パケットは下記の条件を追加指定することができます。

※入力値としてカンマを使用する場合は、同時にコロンを使用することができません。

●ポート指定

パケットの送信元ポートと送信先ポートをそれぞれ指定します。

ポートは「カンマ(,)」区切りで複数指定することができます。

また「コロン(:)」を使用してポートを範囲指定することができます。

※入力値としてカンマを使用する場合は、同時にコロンを使用することができません。

●フラグ指定

検査対象になる TCP フラグを指定します。

フラグはマスクと値を別々に指定します。

マスクは対象のパケットからビット演算でマスクします(チェックがついているビットのみ残す)。

次にマスク後の値と指定の値を比較して同じ値になった場合は、そのパケットが処理対象になります。

●UDP

UDP のチェックボックスにチェックを入れると、UDP パケットを対象とした検査を行います。

UDP パケットは下記の条件を追加指定することができます。

※入力値としてカンマを使用する場合は、同時にコロンを使用することができません。

●IGMP

IGMP のチェックボックスにチェックを入れると、IGMP パケットを対象とした検査を行います。

IGMP は追加で指定できる条件はありません。

●処理

ルールに適応したパケットの処理を設定します。

●処理

適応したパケットの処理方法を指定します。

許可する	対象のパケットを正常処理します。
破棄する	対象のパケットを単に破棄します。
拒否する	対象のパケットを拒否します。この場合パケットの拒否をしたことを、送信元に通知します。
**** を実行する（他のフィルタリングルールに推移する）	別のフィルタリングルールに検査を推移します。

●処理頻度制限

適応するパケットの制限をします。これは DoS 的なパケットを防御するような場合に使用します。

設定例(2 つのルールで指定します)

ICMP を「10 パケット/秒」まで受ける

●ICMP を拒否する

この例では 1 秒以内に 10 個までのパケットは許可しますが、それ以上に送られたパケットは拒否することになります。

●ログ記録

対象のパケットを処理するときにログにパケットの情報を記録します。

「ログ管理」の「ログ閲覧」から確認できます。

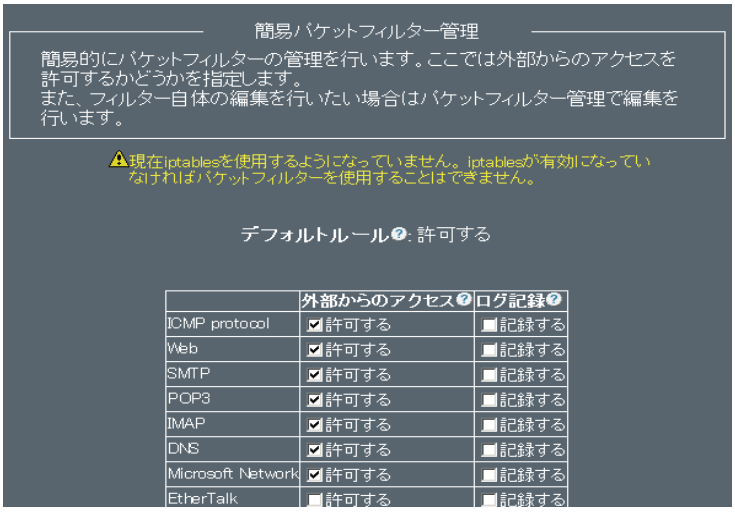
●ログに追加する文字列

ログに記録するメッセージの行頭に指定の文字列を付加します。

ログ監視などと併用することで不正なパケットを検知することができます。

２－４．簡易パケットフィルタ管理

「パケットフィルター管理」メニューをより簡易的なインターフェースにしたメニューです。



項目は「パケットフィルター管理」メニューで「可視化」がチェックされたフィルタリンググループです。

外部からのアクセスの「許可する」をチェックすることで該当フィルタリンググループ内のルールを全て「許可する」にします。

チェックを外すと全て「破棄する」にします。

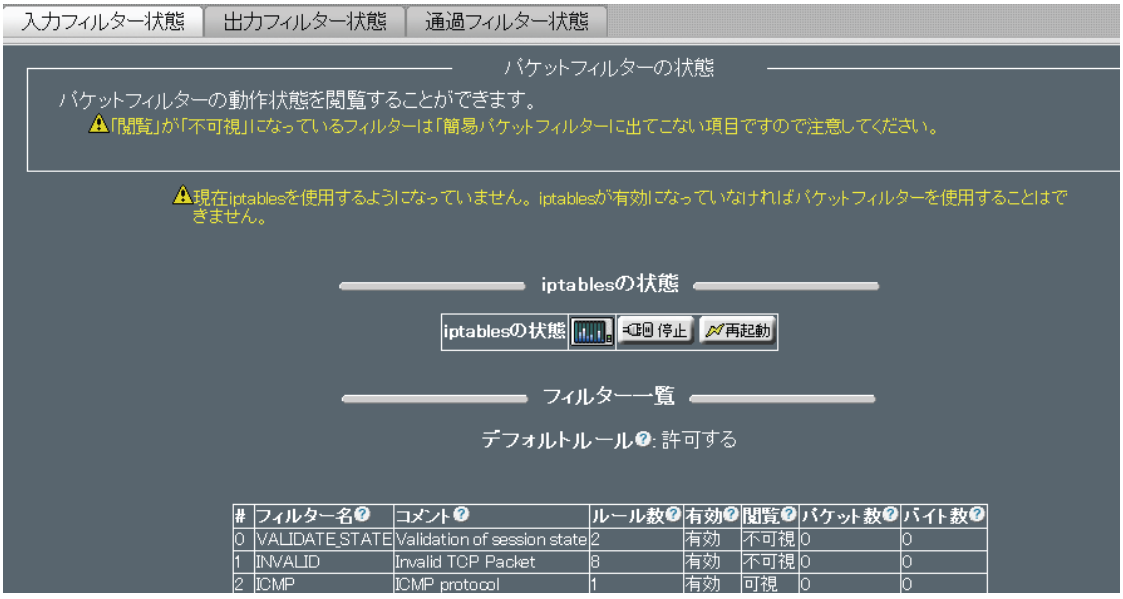
「ログ記録する」をチェックすると全てのフィルタリングルールに適応したときにログ記録をします。
チェックを外すとログ記録をしません。

※このメニューで出てくる項目は全て「パケットフィルター管理」メニューにてフィルタリンググループに「可視化」をチェックしたメニューのみです。
「簡易パケットフィルター管理」メニューで表示したい場合は該当フィルタリンググループの可視化をチェックしてください。

２－５．パケットフィルタ状態

●パケットフィルター状態

「パケットフィルター管理」および「簡易パケットフィルター管理」メニューで設定したフィルターの状態を表示することができます。



状態は入力・出力・通過の個別に表示することができます。

フィルタリングルール毎に適応パケットのパケット数・バイト数を表示します。

フィルターの状態はフィルター内のルール別に表示することはできず、全ルールで適応した総パケット数と総バイト数になります。

また、iptables の起動状態の確認が可能です。

必要に応じて起動、再起動、停止を行うことができます。

●パケットフィルターの構築
簡単な構築
あまりネットワークやパケットフィルターに詳しくない方にお勧めの方法です。

まず、「パケットフィルター設定」で「基本設定」を行い、その後「簡易パケットフィルター管理」で設定を行います。

●少し複雑な構築
積極的なフィルタリングを行いたい方にお勧めの方法です。
まず、簡単な構築の手順に従って設定します。
その後、「パケットフィルター管理」で既存のフィルタのルールの変更や新規にフィルターを作成し、
フィルタリングルールを設定します。

「パケットフィルター管理」のフィルターには、異常なパケットの破棄ルールが標準で用意されているのでそれを使用します。
独自でルールを作成する場合は下記のことに注意して構築します。

●状態指定で「不当接続」を破棄する
●TCP/IP は異常な TCP フラグの定義をして、すべて破棄する

マイサーバーサービス 利用マニュアル
(セキュリティ / ファイアウォール)
マイサーバーVPS compact

発行元：株式会社イージェーワークス
発効日：2010 年 7 月 9 日　rev1

リムネット カスタマーサポートセンターの連絡先
電 話 窓 口：0120-678-309
ファックス：045-472-2777
メ　ー　ル：support@rim.or.jp
受 付 時 間：24 時間 365 日