OnePointWall

取扱説明書

Version 1.0

はじめに

このたびは、OnePointWall をご購入いただき、ありがとうございます。
本製品は、通信のパケットを解析し、外部からの攻撃等を自在に防ぎ、また組織内部の好ましくない通信を止めるといった通常のファイヤーウォールでは行えない機能を提供いたします。
操作は単純、且つ機能は強力です。十分、ご活用していただけましたら幸いです。
なお、このソフトウェアに記載されている事柄は、将来予告なしに変更されることがありますので、ご了承ください。

同梱品をご確認ください

梱包箱の中に、次の品物がそろっているかご確認ください。
万一欠品、または破損が生じているとき等は、お手数ですが購入先までお問い合わせください。

・インストール用 CD-ROM　　（1枚）
・取扱説明書[本書]　　（1冊）
・OnePointWall ご使用案内　　（1枚）
・ユーザー登録カード　　（1枚）

ご使用になる前の注意事項

＊ 本製品を権限のないネットワーク上で使用する場合は、あらかじめ権利者の承諾、同意が必要となります。
＊ 本製品をプライバシーの侵害目的で使用すると訴えられることがあります。
＊ 通信事業者が本製品によって知りえた顧客の通信内容を利用することは、法律で禁じられています。
＊ 大規模ネットワークでは、別途ネットワーク設計が必要になることもあります。

取扱説明書のご注意

・本書の内容の一部又は全部を無断転記することは禁止されています。
・このソフトウェア及びハードウェアに記載されている事柄は、将来予告なしに変更されることがあります。ご了承ください。

使用上の注意

本製品をご使用いただくにあたり、下記注意事項をよくお読みになり必ず守ってお使いください。

ルール上の注意

OnePointWall の設置場所と使用目的によっては、規則違反のルールがあります。安易に全てにチェックをつけてしまうとトラブル発生の原因となります。必ずその経路でその通信が必要とされているかを確認してから使用してください。どうしても使用する場合は、マルチユーザーモードで上手く除外ルールを作ってください。

□ Web アップロード系

- Web ベースのグループウェアでアップロードができなくなる。
- Web メールで添付ができなくなる。
- 使用する場合は外部との接点に必要な場合がある。
- 外部の ASP を使っている場合。

□ファイヤーウォール系

- 部署間においてファイルサーバーが見えなくなる。
- 部署間においてドメインログオンが見えなくなる。
- 他社内の通信ができなくなる。

□ SMTP 系

- 普段使用する To: Cc:の上限を把握してから運用する。

□ VPN 系

- IPsec を使用しているところで VPN 全てを使用する。

目　次

概要

OnePointWall は、ブリッジ型のファイヤーウォールです。P2P ソフトウェアである Winny や WinMX、またファイヤーウォールで止めることのできない VPN ソフトウェアの SoftEther、SSH 等の通信のみをブロックする点では、特化したファイヤーウォールとも考えられます。

通常のファイヤーウォールのとの違い

・特徴のあるパケットのみをブロックする
・ブリッジタイプであるので、IP アドレスの変更等、ネットワークの再設定が不要
・L2 のスイッチグハブと同様に存在が見えにくく、アタックの対象にならない
・中から外への通信のブロックに注力している
・SoftEther、Winny といったファイヤーウォールでは止まらない通信が止まる
・IM でのアップロードやメッセージの送信といったアクションごとにブロックができる

これら機能により、全てとはいかないまでも、多様な情報漏洩手段を回避できます。

旧バージョンとの大きな違い

・1 つの OnePointWall で様々な通信をブロック可能
・完全独自エンジンによる、小型化と高速化
・Web インターフェイスの高機能化
・Windows インターフェイスの付与
・インストール可能
・USB メモリもしくは HDD インストールが必要
・IDS モードとファイヤーウォールモードの２種類が選択可能
・独立していた Winny のブロックが統合
・マルチユーザーモードによるネットワーク・サーバ単位での権限委譲が可能に
・ユーザールールが作成可能

1　使用方法

止めたい通信の流れるネットワークの間に、OnePointWall 用のマシンをはさみます。
OnePointWall は、透過的に動作するため、その他の設定は特に必要ありません。
ログを USB ストレージに保存する場合は、あらかじめ OnePointWall 用のマシンに設置して起動してください。
具体的な取扱方法として、OnePointWall をファイヤーウォールと LAN 用スイッチの間に設置することで、透過の的を限定してフィルタリングします。(図1参照)
注.　管理ポートご使用の場合は、USB ストレージ等で設定を記述する必要があります。

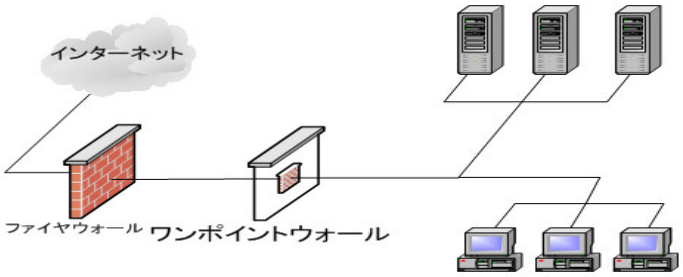

図1　OnePointWall の設置例

2　仕様

■　提供媒体

CD-ROM

■　必要ハードウェア

- CD-ROM ブート可
- ネットワークインターフェイスX2
- PentiumIII(coppermine)　800MHz 以上の CPU
- 64MB 以上のメモリ

■　推奨ハードウェア

- Pentium4 2.0GHz 以上
- 512MB 以上のメモリ
- ネットワークインターフェイスX3　(1 つは管理用)
- USB2.0
- 128MB 以上の USB メモリもしくは USB ハードディスク

遅延　　0.09ms
スループット低下率　　1%以下
※数値は全て実際の機器での測定値であり、保証する値ではありません。

3　ログイン

コンソールもしくはシリアルコンソールよりログインできます。

シリアル設定は、115200bps　8bit　パリティーなしにして下さい。

但し、シリアルコンソールログインする場合は、別途シリアルクロスケーブルが必要となります。

一般アカウント	block
管理権限アカウント	root

パスワードは OnePointWall ご使用案内をご覧下さい。

3．1　インストール方法

OnePointWall は CD 起動のほかにハードディスクにインストールすることができます。
インストールする場合は、OnePointWall 起動後にインストールするデバイスを指定してコマンドを実行してください。

書式：opw_install.pl　インストールデバイス
［例］# opw_install.pl hda
インストールデバイスは OnePointWall をインストールするディスクを指定します。IDE ハードディスクのプライマリマスタの場合は hda 、プライマリスレイブの場合は hdb となります。
同じように、SCSI ディスクの 1 番目の場合は sda と指定してください。
＊USB メモリは sd*と認識されてしまいますので、あらかじめ USB メモリを抜いてインストールしてください。
インストール後のサイズは 60MB、インストール時間は 1 分ほどです。

```
Enabling DMA acceleration for: hda.
 Network device eth0 detected, DHCP broadcasting for IP. (Backgrounding)
no autofs mounts configured!
 Automounter started for: floppy cdrom hda.
Loading /etc/console/boottime.kmap.gz
INIT: Entering runlevel: 5
Starting OPW: one point wall test
opw[202]: CheckLicense: License Error
.


One Point Wall 1.0 block tty1

block login: root
Password:
NetAgent Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@tty1[root]# opw_install.pl hda
OnePointWall Install (1/5) Fdisk /dev/hda
OnePointWall Install (2/5) format disk /dev/hda
OnePointWall Install (3/5) copy system.
OnePointWall Install (4/5) write boot loader.
Warning: Unable to determine video adapter in use in the present system.
OnePointWall Install (5/5) finished.
root@tty1[root]# _
```

３．２　エンジン起動・停止方法

■　エンジンの場所

/usr/local/bin/opw

標準で入っているエンジンです。アップデートが無い場合はこちらを使用して起動しています。

/log/opw

エンジンのアップデートがあると/log ディレクトリに新しいバージョンが保存されるため、こちらから起動します。

■　起動オプション

USAGE: /usr/local/bin/opw [-options]

OPTIONS:

-V	opw のバージョン表示
-h	ヘルプを表示
-Q	ブリッジモードで起動
-D　　I	DS モードで起動
-d	デバッグモード
-i <iface>	IDS モードでキャプチャ NIC を指定
-r <rules>	コンパイル済みパターンファイルを指定
-s <hostIP>	alert を指定 IP に syslog で送信
-c <confs>	設定ファイルを指定
-f <pktfile>	offline モードで pcap 形式ファイルから検知

■　標準的な起動・停止方法

以下のコマンドを実行すると、-c /log/onepoint.conf オプションで起動します。

なお、keep_opw も起動や停止が同時に行われます。

起動	/usr/local/bin/opw_exec start
停止	/usr/local/bin/opw_exec stop
再起動	/usr/local/bin/opw_exec restart

pcap 形式ファイルから検知を行いコンソールに表示させる場合は以下のようにします。

/log/opw -c /log/onepoint.conf -f /log/test.pkt -D -d

＊　注意　＊

2 重起動を行わないようになっているため別プロセスで opw 起動時は opw の起動は行われません。起動が行えない場合は/var/run/opw/opw.pid、keep_opw.pid を確認してください。

opw の起動・停止時には/log/messages に以下のログが出力されます。
なおその他の opw に関するエラーログなども/log/messages に出力されます。
ファシリティ、プライオリティ：user,info

Dec　4 23:00:44 block opw [1119]: OnePointWall　starting: bridge mode
Dec　5 00:36:56 block opw [1119]: OnePointWall　exiting

4 OnePointWall 設定

4．1 ディレクトリ構造

OnePointWall を使用する際のディレクトリ構造は、次のようになっています。

/usr/local/bin/

opw	ブロック・検知用エンジン
opwc.pl	ルールコンパイラ
keep_opw	opw を継続起動させるプログラム
opw_exec	opw 起動プログラム
opwc_exec	opwc.pl 実行プログラム

/usr/bin/

start	サーバ等起動プログラム
show	ステイタス、ログ表示プログラム

/etc/

passwd	ユーザー名およびユーザー管理ネットワーク
shadow	パスワードファイル
sys_name	OnePointWall バージョン(インストール時) CD 起動時は/cdrom/ sys_name

/var/www/

.htpasswd	Web アクセス用パスワードファイル
*.cgi	Web ユーザインターフェース用 CGI
*.html	Web ユーザインターフェース用 HTML

/log/

onepoint.conf	設定ファイル
opw.rules	標準ルールファイル
user.rules	ユーザ定義ルールファイル
opw.pat	コンパイル済みパターンファイル
alert.log	ブロック・検知ログ
messages	syslog ログファイル その他 syslog ログファイルも/log ディレクトリに保存されます。

以下は更新時に/log に保存されるファイルです。

opw

opwc.pl

keep_opw

passwd

shadow

.htpasswd

/log/user/ユーザー名

onepoint.conf	ユーザー用設定ファイル

/var/run/

opw.pid	opw のプロセス ID が格納されたファイル
keep_opw.pid	keep_opw のプロセス ID が格納されたファイル

CD 起動の時、USB ストレージに保存されるのは/log ディレクトリのみです。

4.2 初期設定

OnePointWall の初期設定は次の通りです。

NIC が 2 枚以上の時

IP アドレス	192.168.1.241
ネットマスク	255.255.255.0
ユーザー	root
パスワード	OnePointWall ご使用案内をご覧下さい。
モード	ブリッジモード(ファイヤーウォール)
ユーザーモード	シングルモード
管理用 NIC	eth2
ブリッジ NIC	eth0,eth1

NIC が 1 枚の時（NIC が 2 枚以上の場合と異なる項目のみ）

モード	IDS モード
管理用 NIC	eth0
IDS 用 NIC	eth0

4．3　Web ユーザインターフェース画面

OnePointWall は管理ホストのブラウザより設定、管理を行うことができます。

画面は下図の赤線枠で囲ったように、3 つのブロックに分けられます。

図 2　インターフェース

ヘッダー部

常に画面上に表示されている部分です。

図 3　ヘッダー

ユーザー	現在ログインしているユーザー名です。
メッセージ	現在ログインしているユーザーあてに残されたメッセージです。
エンジンバージョン	OnePointWall のエンジンバージョンです。
パターンファイル	標準ルールファイルのバージョンです。

メニュー部

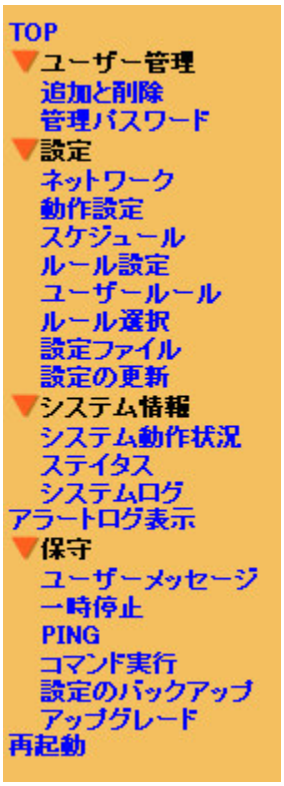

図 4　メニュー

［ 各項目の説明 ］

・ **TOP**

Web ブラウザからログイン直後の画面です。ライセンス情報の確認が行えます。

・ **ユーザー管理**

ユーザーの追加･削除やパスワード変更を行います。

・ **設定**

OnePointWall の設定や適用ルールの変更などを行います。

・ **システム情報**

OnePointWall のシステムの動作状況やログの確認が行えます。

・ **アラートログ表示**

OnePointWall がブロックや検知を行った時間やアドレスの確認をすることができます。

・ **保守**

設定のバックアップやアップグレードなど保守に関する項目です。

・ **再起動**

システムの停止･再起動を行います。

表示部

メニューで選択された項目を表示して各種情報の表示や入力を行います。

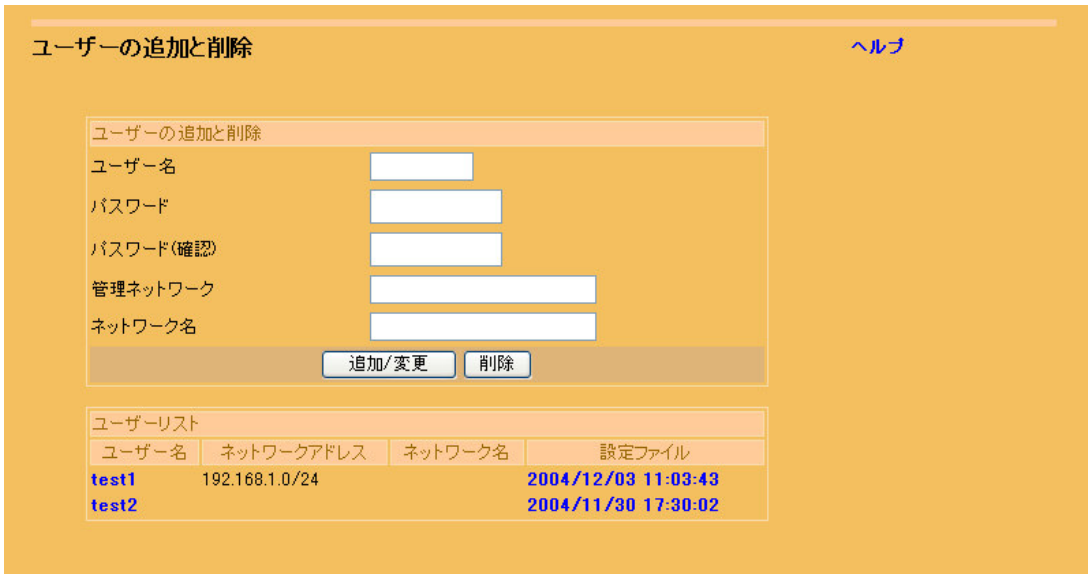

図 5　表示部分

5　各画面の説明

5．1　TOP

ライセンス情報の入力、確認を行います。

図 6　ライセンス情報

・ライセンス情報　　登録されているライセンス情報
・ライセンスの更新　　ライセンスキーを入力してライセンスの登録・更新

5．2　ユーザー管理

OnePointWall はネットワーク毎の異なったルール設定、及び管理用にユーザーを作成することができます。但し、ユーザーを作成できるのは管理者権限(root)のみです。

A　追加と削除

ユーザーの追加、変更、及び削除を行い、登録ユーザー情報を確認できます。

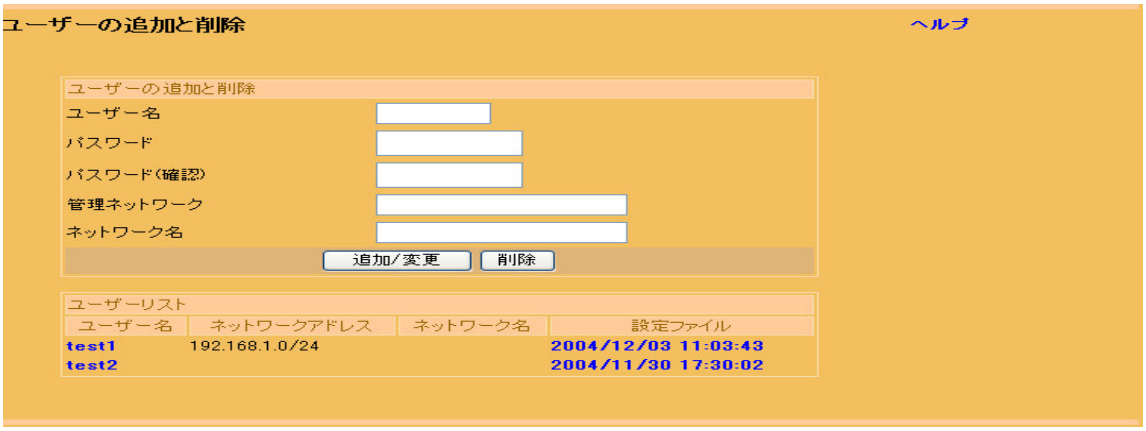

図 7　ユーザーの追加と削除

ユーザーを追加する場合

ユーザー名	追加するユーザー名
パスワード	追加するユーザーのパスワード
パスワード確認	確認用のパスワード入力欄。
管理ネットワーク	ユーザーが管理するネットワーク、MAC アドレスの指定を行います。ルールのホームネットワークに反映されます。
ネットワーク名	管理ネットワークを識別するための名前

入力が終わったら、追加／変更ボタンをクリックして下さい。

ユーザーを変更する場合

ユーザーリストのユーザー名をクリックすると、入力用のテキストボックスにユーザー情報が入りますので、変更して追加／変更ボタンを押下します。
パスワードが空欄の場合、パスワードは変更されません。

ユーザーを削除する場合

ユーザーリストのユーザー名をクリックすると、入力用のテキストボックスにユーザー情報が入りますので、削除ボタンをクリックして下さい。

■ ユーザーリスト

登録したユーザー情報のリストです。

＊設定ファイル欄はそのユーザーの設定ファイルが更新された時間が表示されます。

B 管理パスワード

ログインしているユーザーのパスワードの変更が行えます。

図 8 パスワードの変更

パスワード	変更するパスワード
パスワード(確認)	チェック用のパスワード入力欄

5. 3　設定

A　ネットワーク設定

OnePointWall 自身のネットワーク設定を行います。

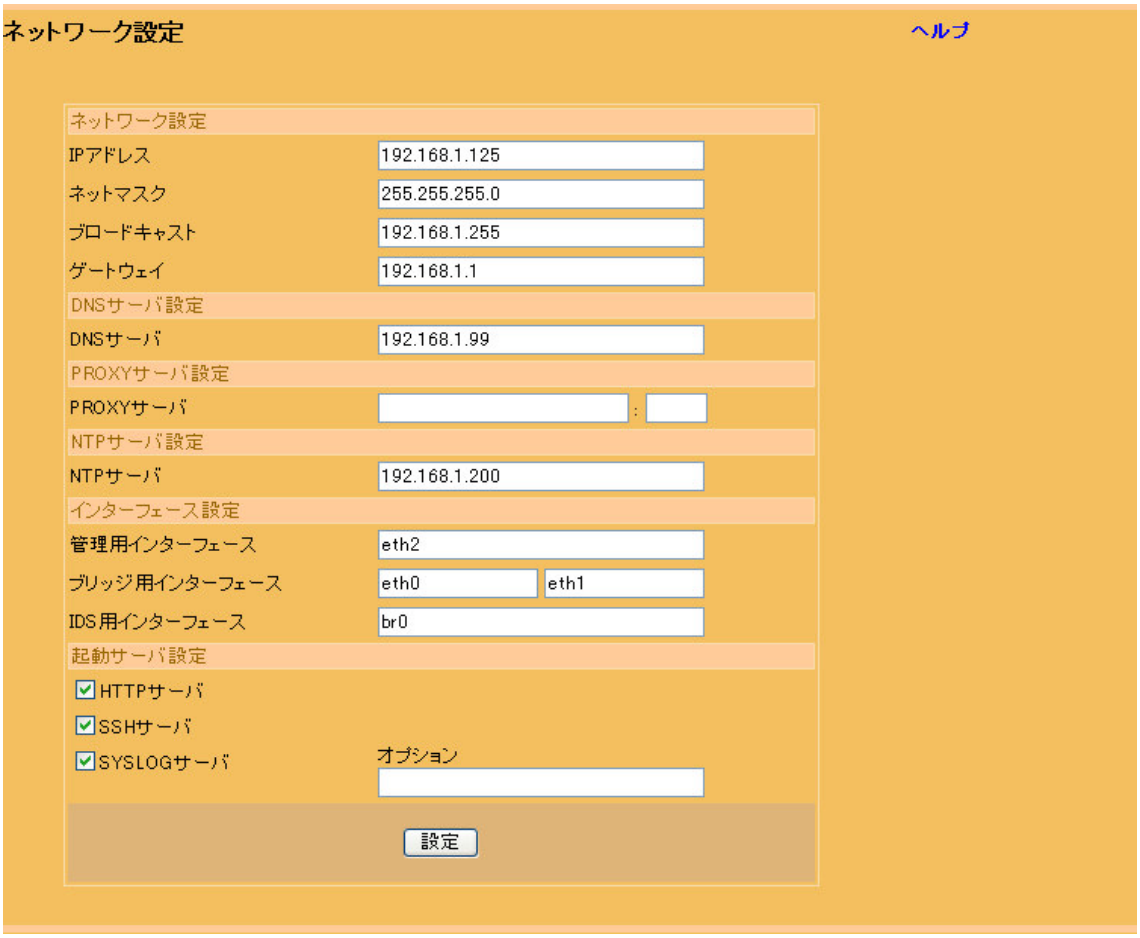

図 9　ネットワーク設定

■　ネットワーク設定

IP アドレス	OnePointWall に割り当てる IP アドレス(管理用ポート)
ネットマスク	ネットワークを識別するためのネットマスク
ゲートウェイ	ネットワーク外の PC へアクセスするための出入り口となるルータ等の IP アドレス

■　DNS サーバ

DNS サーバ	OnePointWall がドメイン名を IP アドレスに名前解決するためのサーバ

■ PROXY サーバ

PROXY サーバ	OnePointWall が外部 Web サーバに接続するための代理サーバ PROXY 経由でパターンファイルのアップデートを行うとき等に使用します。

■ NTP サーバ

NTP サーバ	OnePointWall のシステム時間を合わせるための NTP サーバ

■ インターフェース設定

管理用インターフェース	管理用の IP アドレスを割り当てる NIC
ブリッジ用インターフェース	ブリッジ用に割り当てる NIC （2 枚指定）
IDS 用インターフェース	IDS の検知用にパケットを取得する NIC

■ 起動サーバ設定

HTTP サーバ	管理用 HTTP サーバの起動有無
SSH サーバ	リモート管理用 SSH サーバの起動有無
SYSLOG サーバ	システムログ出力用 SYSLOG サーバの起動有無
オプション	SYSLOG サーバのオプションを指定

B 動作設定

OnePointWall の基本動作を設定します。

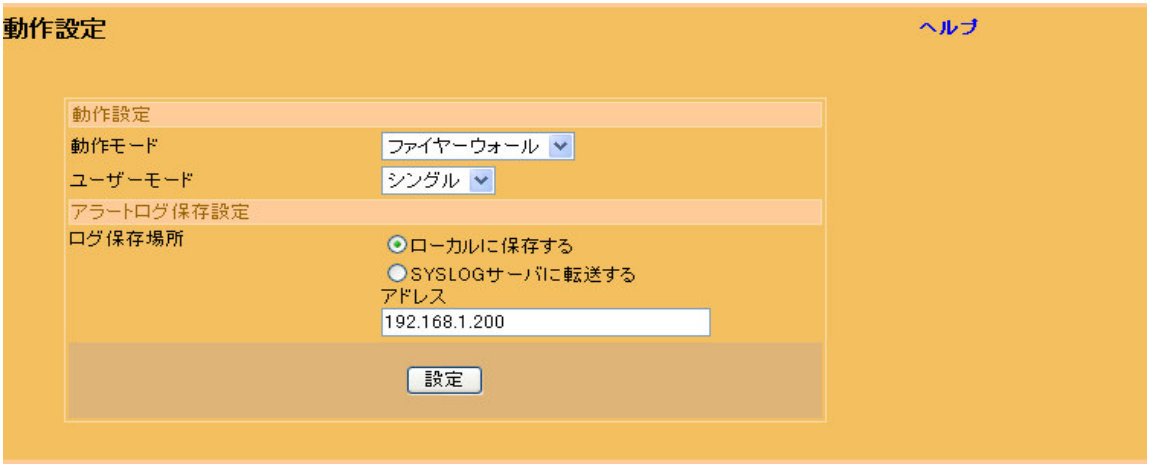

図 10 動作設定

■ 動作設定

動作モード	OnePointWall の基本動作である、ファイヤーウォールモードと IDS モードの選択
ユーザーモード	シングルユーザー、又はマルチユーザーかを指定

＊　シングルユーザーは、一人の管理者がネットワークを管理し、ネットワーク毎のルール適用状況を変更する必要が無い場合に使用します。
＊　マルチユーザーは管理者がネットワークを分割して、それぞれ分割されたネットワークを複数の管理者で管理する場合、またはネットワーク毎にルールを変更する際に使用します。

■　アラートログ保存設定

ログ保存場所　　ローカルに保存するか他のマシンの SYSLOG サーバを指定できます。SYSLOG サーバを指定するときは、SYSLOG サーバの IP アドレスを入力してください。

＊　syslog に出力する際のファシリティ、プライオリティは以下の通りです。
　local3,info

C スケジュール

自動アップデート関連のタイミング等の設定を行います。

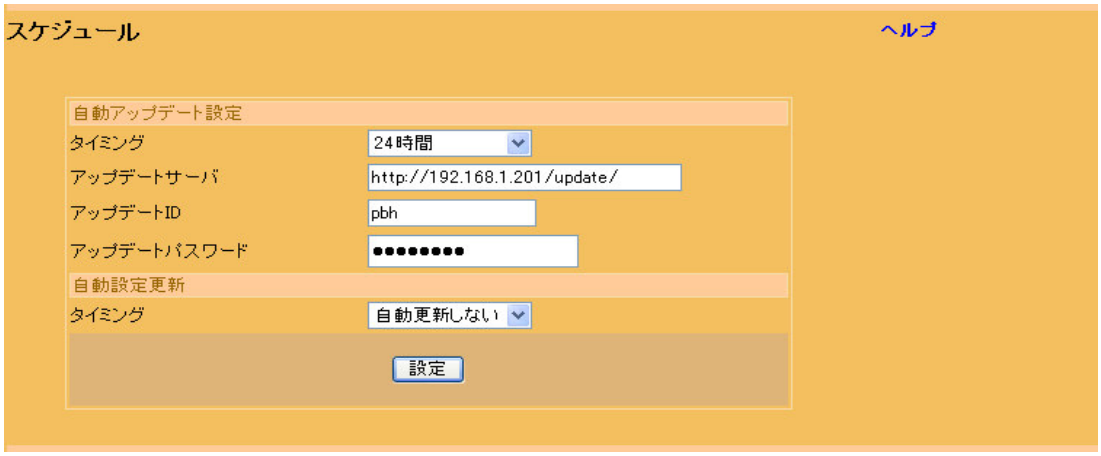

図 11　スケジュール

■　自動アップデート設定

タイミング　　パターンファイル等の自動アップデートを行うタイミングを指定します。自動アップデートを行わない場合は、自動更新しないを選択してください。

アップデートサーバ　　アップデートサイトを指定してください。通常は弊社公式アップデートサイト http://www.onepointwall.jp/update を指定してください。
なお複数台の OnePointWall を導入している場合は、ネットワーク内部にアップデートサーバを構築してそのサーバからアップデートすることも可能です。

アップデート ID　　アップデートサーバにアクセスするための ID

アップデートパスワード　　アップデートサーバにアクセスするためのパスワード

■ 自動設定更新

タイミング　　設定変更などがあった場合、反映されていない設定があれば、設定ファイル、パターンファイルの再読込みを行います。

D ルール設定

ルールファイルには変数が埋め込まれていることがあります。コンパイル時にパターンファイルに反映させるためのアドレスを定義します。

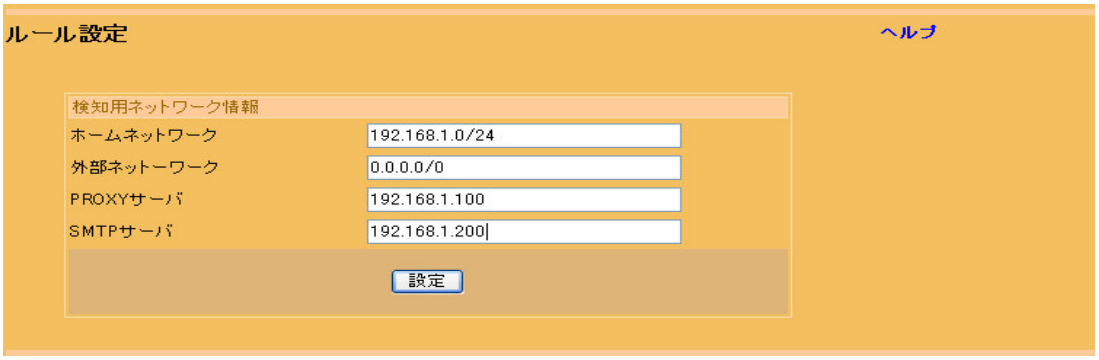

図 12　ルール設定

■ 検知用ネットワーク情報

ホームネットワーク　　パターンファイルに反映させるための内部ネットワークを定義します。

外部ネットワーク　　外部ネットワークを定義します。

PROXY サーバ　　PROXY サーバの IP アドレスを定義します。

SMTP サーバ　　SMTP サーバの IP アドレスを定義します。

E ユーザールール

ユーザールールのアップロード、ダウンロードを行います。

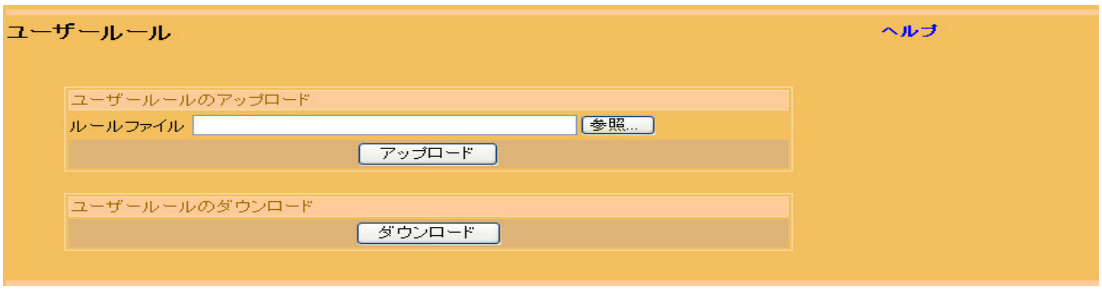

図 13　ユーザールール

アップロード	ユーザールールを作成した場合はここからアップロードして下さい。
ダウンロード	ユーザールールを編集、またはバックアップするため現在 OnePointWall に保存されているユーザールールをダウンロードできます。

F ルール選択

適用するルールの選択を行います。チェックを付けた項目が適用されます。

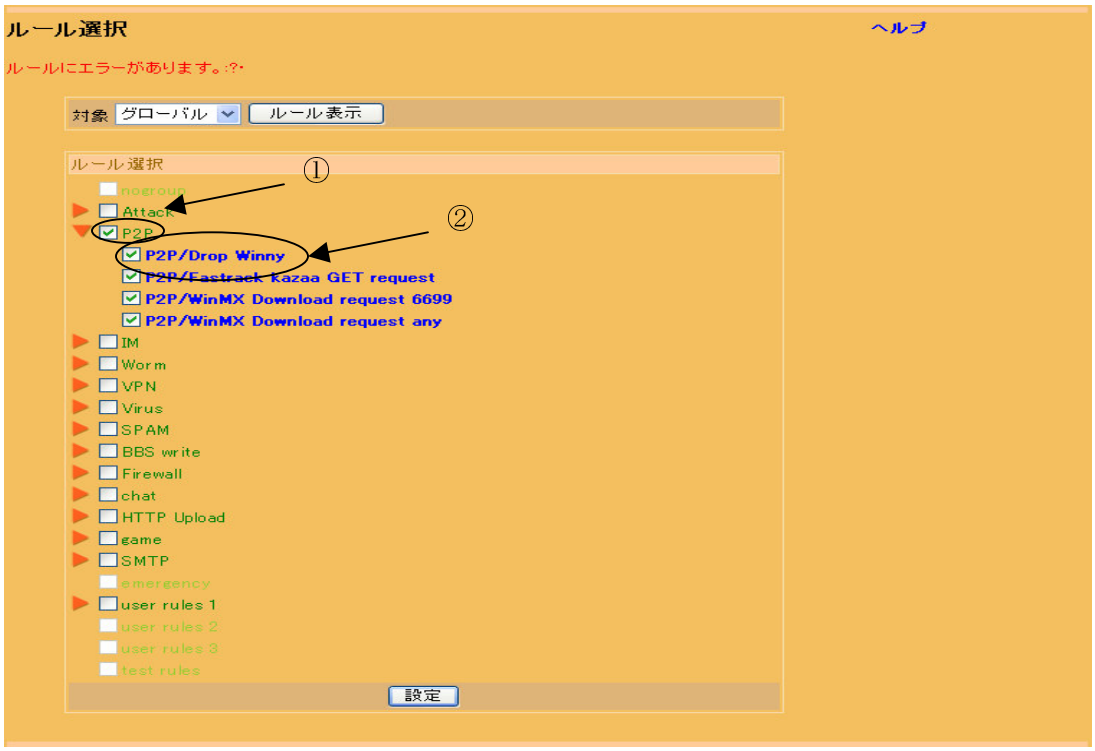

図 14 ルール選択

図１４の①はそのグループを検査するかどうかのチェックボックスです。チェックされたグループのルールはすべて適用されます。

②はそのルールを適用するかどうかのチェックボックスです。グループのチェックが無いとき、このチェックを個別に選択します。

管理ユーザー(root)は、他のユーザーの設定を変更できます。root 以外のユーザーは、自分のネットワークに関する変更のみ可能です。

設定ボタンを押下して、設定を保存してください。

詳しいルールの説明は、を参照ください

。

G 設定ファイル

OnePointWall 用設定ファイル(onepoint.conf)のアップロード、ダウンロードが行えます。また更新履歴からの変更も可能です。

図 15 設定ファイルの変更

アップロード	管理用ホストに保存してある設定ファイルをアップロードすることができます。
更新履歴	設定ファイルの更新履歴を行うことができます。世代管理を行っているため、戻すボタンで以前の設定ファイルに戻すことが可能です。ファイル名をクリックするとファイルをダウンロードします。

H 設定の更新

各設定を反映させます。

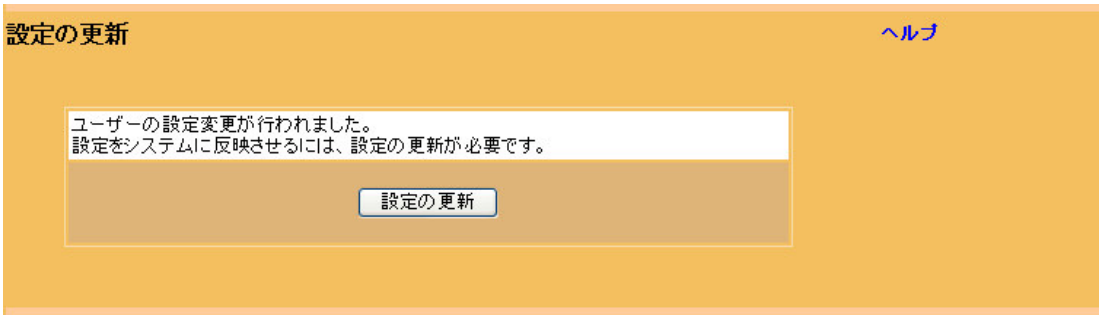

図 16 設定の更新

上記で行ってきた設定を反映させます。管理者権限(root)のみ可能です。ユーザー更新の反映は、自動更新設定もしくは管理者に更新を依頼することになります。

５．４　システム情報

OnePointWall のシステム動作状況を確認できます。

正常動作しているかどうかシステムの動作を見るときは、この項目で行って下さい。

A　システム動作状況

OnePointWall の動作状況の確認を行います。

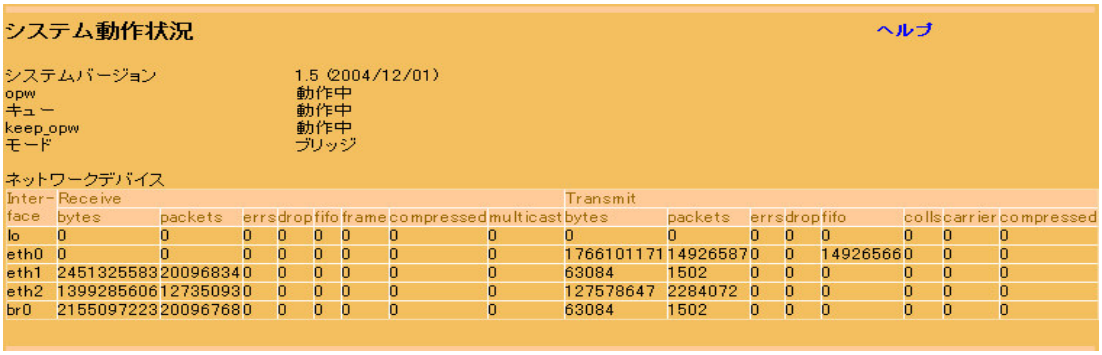

図 17　システム動作状況

システムバージョン	OnePointWall のバージョンです。
opw	検知用のエンジンが動作中かどうかを表示します。
キュー	パケットを検知用エンジンに引き渡す設定になっているかを表示します。
keep_opw	検知用のエンジンが何らかの理由で動作していない場合、自動的に起動しなおすプログラムです。このプロセスが動作中かどうかを表示します。
モード	ファイヤーウォールモードか IDS モードでの動作かを表示します。
ネットワークデバイス	システムが認識しているネットワークデバイスについての情報を表示します。

B　ステイタス

システムリソースの利用状況等を表示します。

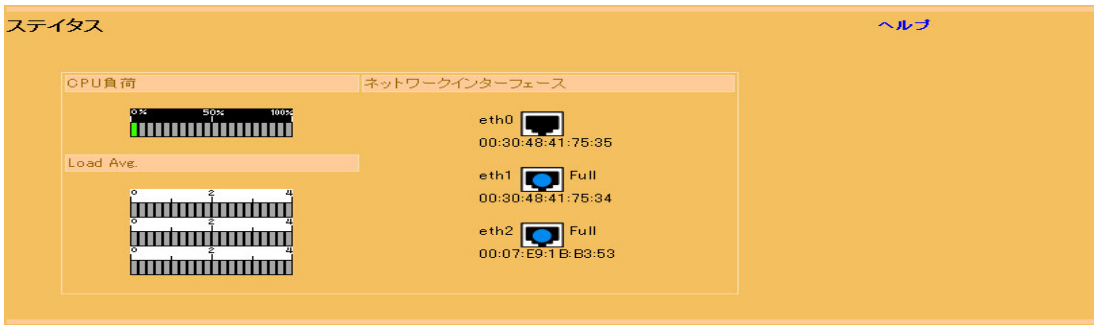

図 18　ステイタス

CPU 負荷	CPU の負荷をグラフで表示します。
Load Avg.	ロードアベレージを表示します。
ネットワークインターフェース	ネットワークインターフェースの接続状況を表示します。 なお表示されている数字は MAC アドレスです。

C システムログ

syslog で出力されたログ(/log/messages)を表示します。

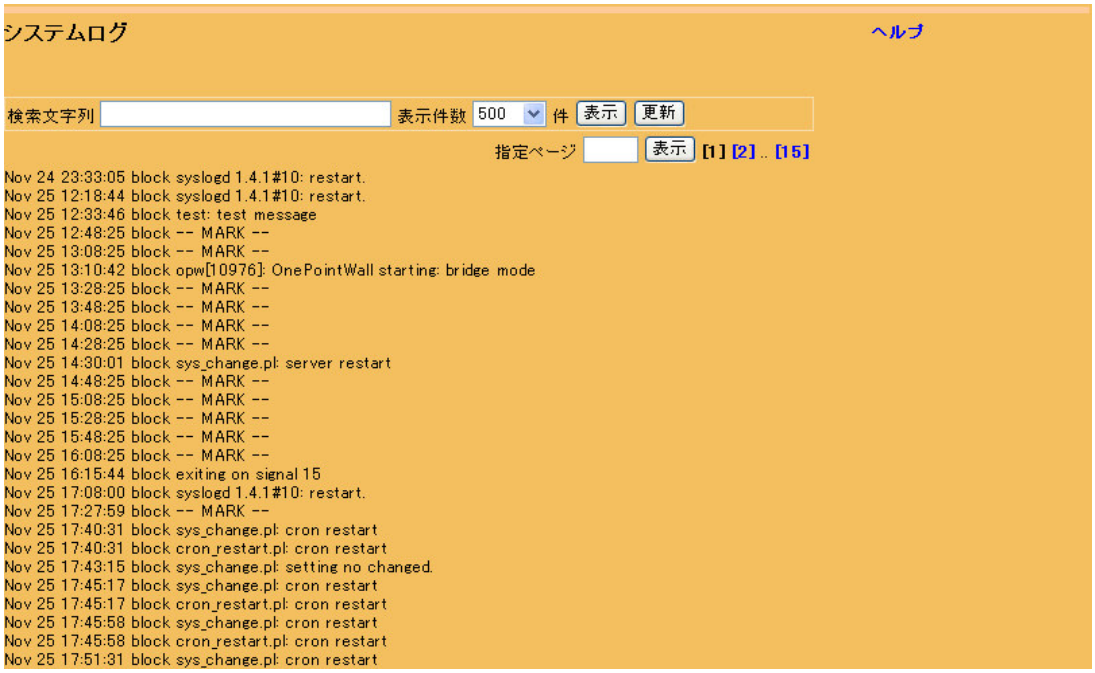

図 19 システムログ

システムログ	システムログを表示します。検索文字列、表示件数を指定した表示が可能です。検索文字列を入力して表示した場合は、その検索文字列の入った行だけを表示します。

5．5　アラートログ表示

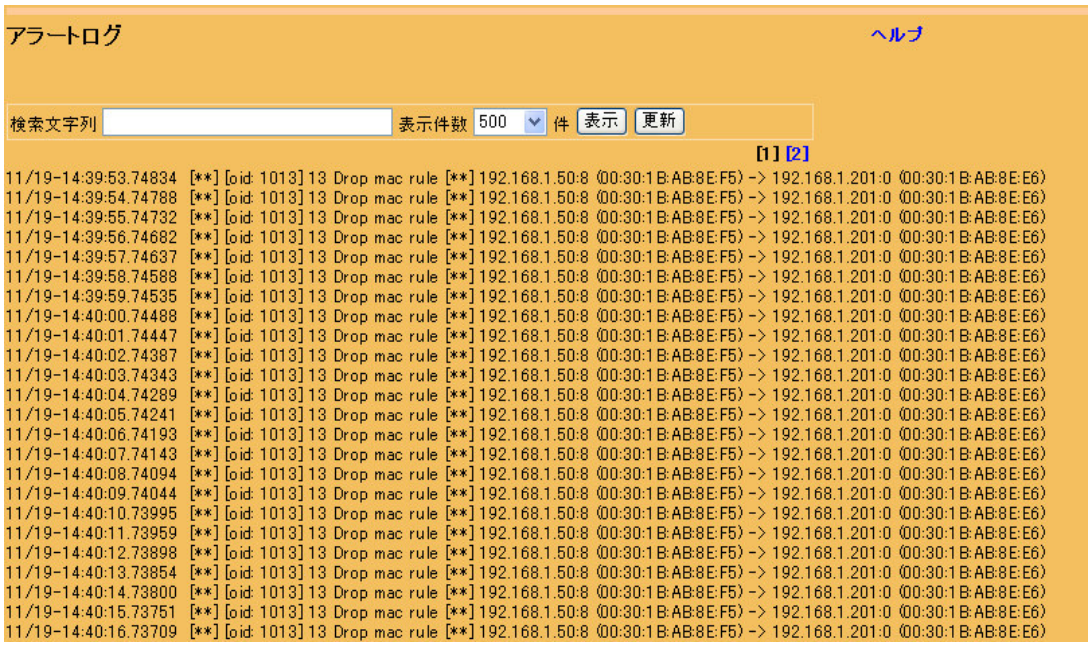

図 20　アラートログ

アラートログ　　OnePointWall がブロック、及び検知したログの閲覧ができます。SYSLOG 経由で他のサーバに転送している場合は、ログは表示されません。

＊ログの形式

検知日時 [**] メッセージ [**] Source IP:Port(MAC) -> Destination IP:Port(MAC)

10/19-15:23:25.520513 [**] [oid: 1] Drop testrule [**] 192.168.1.50:32815 (11:22:33:44:55:66) -> 192.168.1.201:80 (44:55:66:77:88:99)

5．6　保守

OnePointWall の運用、保守に関する項目です。

A　ユーザーメッセージ

他のユーザーにメッセージを残す場合に使用します。管理画面上部のメッセージ欄に表示されます。

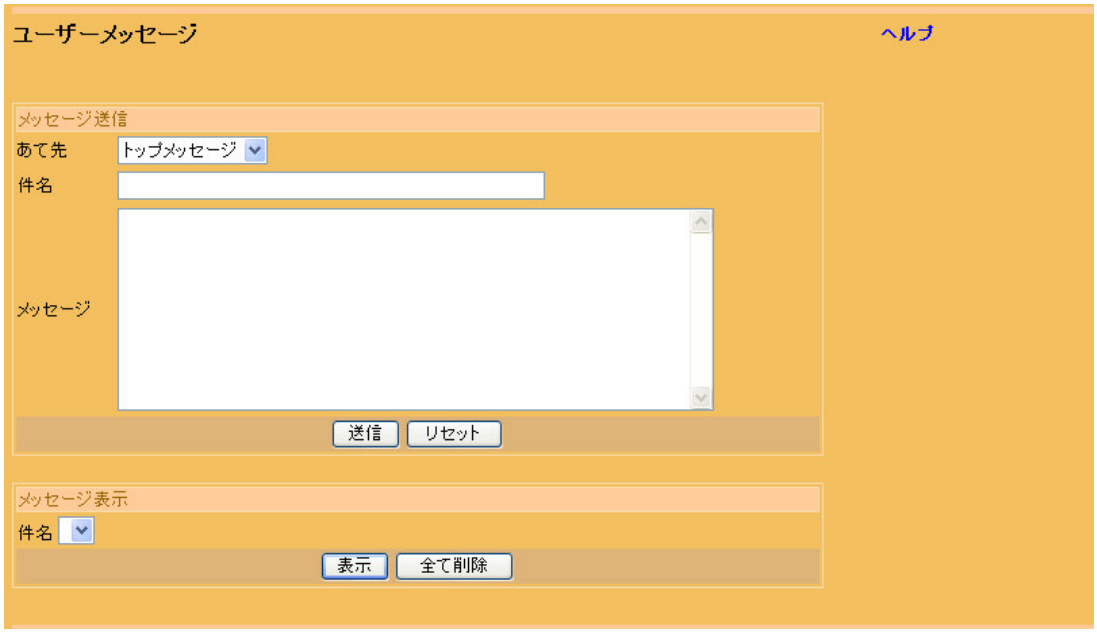

図 21　ユーザーメッセージ

■　メッセージ送信

あて先	管理者(root)は他のユーザーへ、ユーザーは管理者にそれぞれメッセージを送信することができます。管理者はトップメッセージを選択するとユーザー全員にメッセージが送られます。
件名	メッセージの件名です。
メッセージ	メッセージの本文です。

■　メッセージ表示

以前ログインユーザー宛てに送信されたメッセージの表示、及び削除を行います。

B　ping

OnePointWall がネットワークに正しく接続されたか確認するために OnePointWall から、ping を出します。

図 22　PING

アドレス　　IP アドレスか DNS サーバを設定しているときはホスト名を入力することができます。

C　コマンド実行

保守を行うために必要なコマンドが実行できます。

図 23　コマンド実行

コマンド　　コマンドを入力します。

D　設定のバックアップ

現在のシステム情報(設定ファイル等)をバックアップ、リストアします。

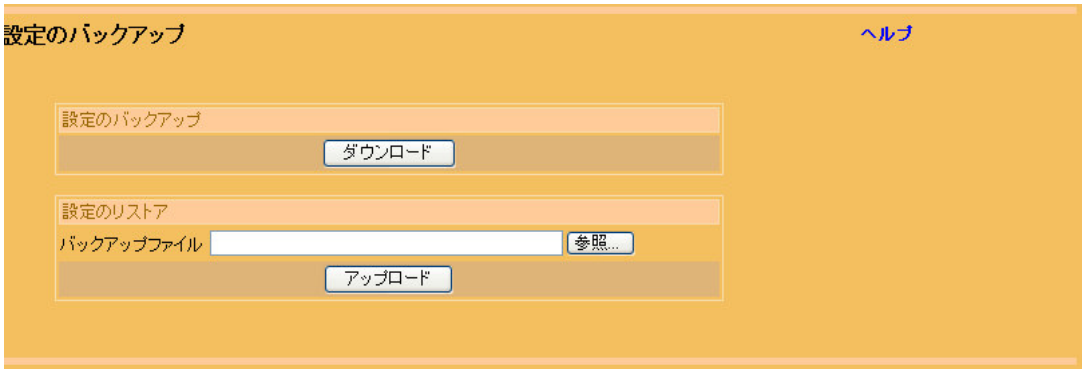

図 24　設定のバックアップ

設定のバックアップ	すべての設定ファイル、ルールファイル等、管理用ホストに設定を保存します。
設定のリストア	設定をバックアップ時のものに戻します。バックアップファイルを選択してアップロードボタンを押下してください。

E アップグレード

OnePointWall のシステムのバージョンアップを行います。

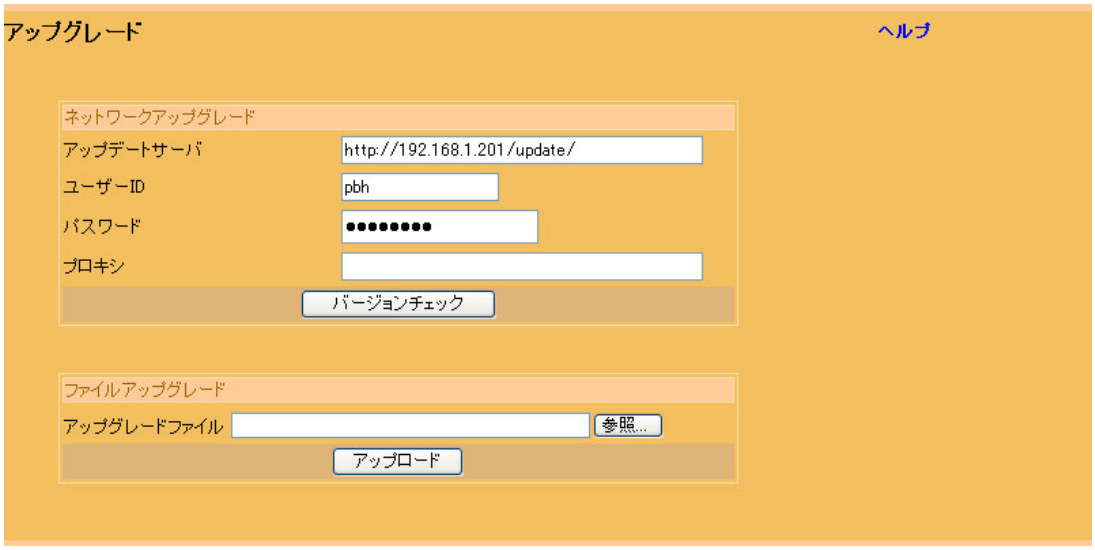

図 25 アップグレード

■ ネットワークアップグレード

スケジュール自動アップデートを管理しないような場合、アップデートサーバに新しいルール等があるかチェックし、手動でアップデートできます。但し、入力した項目はスケジュール項目の自動アップデート設定には反映されません。

アップデートサーバ	アップデートサイトを指定して下さい。 公式サーバの URL は http://www.onepointwall.jp/update となります。
ユーザーID	アップデートサーバにアクセスするための ID を入力して下さい。
パスワード	アップデートサーバにアクセスするためのパスワードを入力して下さい。
プロキシ	一時的にプロキシサーバを変更したいときに使用して下さい。

■ ファイルアップグレード

ハードディスクにインストールして運用しているユーザーは OnePointWall のアップグレードパッチが提供された場合、パッチを適用することができます。

アップグレードファイル　　OnePointWall のアップグレードサイトからダウンロードしたパッチを指定して下さい。アップロードボタンを押下するとアップロードが始まります。

5. 7　再起動

システムの再起動、停止を行います。

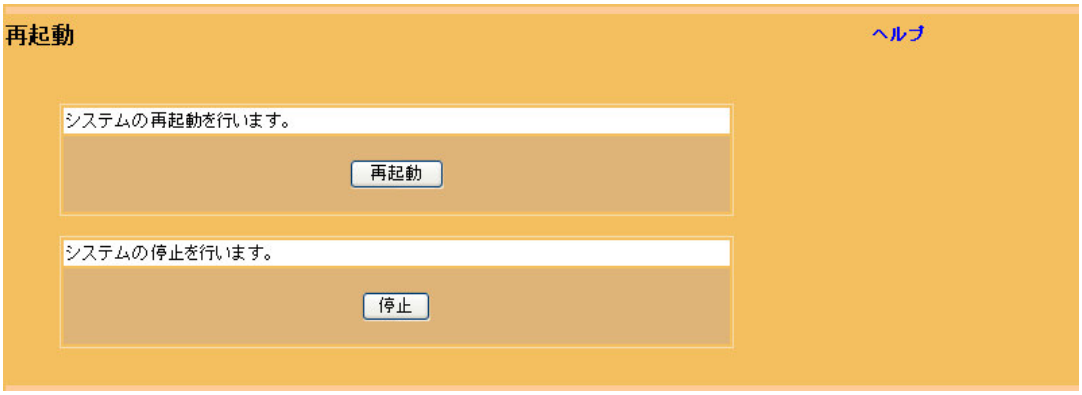

図 26　再起動

システムの再起動　　OnePointWall のシステムを再起動します。
システムの停止　　OnePointWall のシステムをシャットダウンします。

6　ユーザー(root 以外)でのログインについて

一般ユーザーで扱うことのできる項目は限定されます。

基本的に行えることは、自分のパスワード変更、管理ネットワークに適用するルール変更、管理者へのメッセージ送信になります。

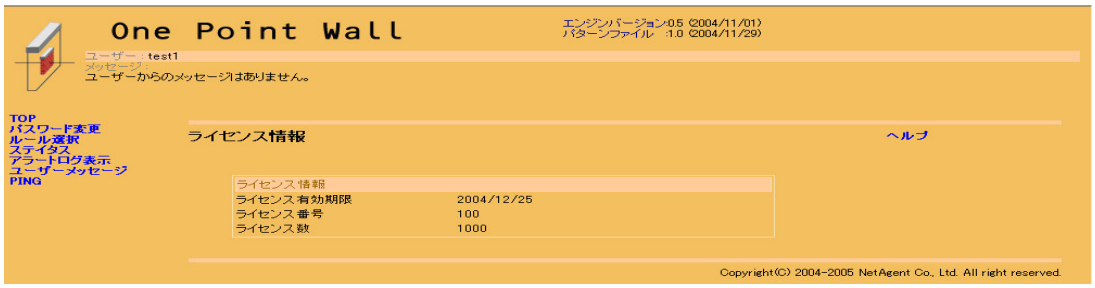

図 27　一般ユーザー画面

6．1　設定手順

■　初回起動時

初めて OnePointWall を使用するときは、次の手順で設定を行ってください。

①　ログイン

ブラウザのアドレス欄に初期アドレスを入力します。

基本認証のダイアログボックスが表示されますので、ユーザー名:root と初期パスワードを入力します。

②　ライセンスキーの入力

TOP 画面よりライセンスキーを入力して下さい。正しいライセンスキーが入力されるまで、OnePointWall はブロックを行いません。

③　パスワードの変更

ユーザー管理の管理パスワード画面を開いて、管理者のパスワードを変更して下さい。

④　設定

OnePointWall の設定を行います。画面左側のメニューより設定を開きます。

上の項目から順次設定して下さい。

⑤　設定の更新

設定を更新します。動作モード等システムの動作変更を行った場合、再起動が必要になります。画面の指示に従って下さい。

■　初回起動以降

初回起動以降は、設定したアドレスやパスワードを使用して OnePointWall の管理や、ログの閲覧を行います。

7 ルールについて

7．1 使用可能なルール

ルールグループ	ルール内容
Attack	XSS や SQL injection に対応した Attack に関するルール
P2P	Winny、WinMX、Kazza 等の P2P ソフトウェアに関するルール
IM	MSN messager、AOL、等の messager に関するルール
Worm	Sasser、NIMDA、MS Blaster 等の Worm に関するルール
VPN	SoftEther、OpenVPN 等の VPM に関するルール
Virus	Virus に関するルール
BBS write	2ちゃんねるや slashdot jp に対する書き込みに関するルール
Firewall	Firewall 的な使い方が可能なルール（内部への telnet、FTP 等）
chat	IRC、ICQ 等のチャットに関するルール
HTTP Upload	画像掲示板や yahoo breafcase 等の HttpUpload に関するルール
game	FF11 や Lineage などのオンラインゲームに関するルール
emergency	危険度高レベルのワームが発生した場合など、緊急時に提供するルール（正式版が出るまでのパッチ的な使用となる）
user rules	User が作成して利用することの出来るルール
Test	Test 用のルール（user rules 等の仮運用時に用いる）

７．２　ルールの記述

A　ルールヘッダ

OnePointWall ルールの構成上、最も基本的な形は以下になります。

```
drop tcp $EXTERNAL_NET any -> $HOME_NET 23
```

これは外部ネットワークから内部ネットワークに対して、telnet 接続のパケットが流れた場合に、該当パケットをドロップするというルールです。これだけでは OnePointWall の管理者にとって、どのような内容の警告であるか判断がつきません。また、シグニチャが判別できないため、上記のままでは OnePointWall で動作させることができません。
このように、OnePointWall がとるべきアクションと、どのようなパケットに対してアクションを適用するかといった情報のみをルールヘッダと呼びます。細かい内容を次で確認してみましょう。

B　ルールオプション

drop tcp $EXTERNAL_NET any -> $HOME_NET 23 (msg: “TEST/telnet-daemon-active”; flag: A+; length: 1;　content: “|ff|”; rev:1; oid:63; gid:99;)

これも外部ネットワークから内部ネットワークに対して、telnet 接続のパケットが流れた場合にパケットをドロップするというルールです。ただし、ルールヘッダ以下の”()”の中にいくつかのパラメータが記述されています。これはルールオプションといい、ルールヘッダの内容をより詳細に記述したものです。
このルールオプションの意味は、TCP フラグビットに Ack とそれ以外が立っており、TCP のペイロードの１バイト目までにバイナリの|ff|がセットされている場合に「telnet-daemon-active」というメッセージを出す、という意味です。
しかし、今の段階では内容を理解する必要はありません。次に詳細な記述を行います。

C　ルールヘッダ構成

ここではルールヘッダを構成する各パラメータについて説明していきます。

■　第１パラメータ(必須)

OnePointWall ルールに記述されている内容に一致したパケットが流れた場合に、OnePointWall がどのようなアクションを取るかを記述します。

drop	ルールにマッチするパケットを遮断します。
pass	ルールにマッチするパケットを通過します。

replace	ルールにマッチするパケットを置き換えます。
log	ルールにマッチするパケットを記録します。
qos [n] (予約)	帯域制御を行います。<帯域制御 [n]制御番号>

■ 第2パラメータ(必須)

OnePointWall ルールで評価するプロトコル(protocol)を記述します。

tcp	ルールを TCP で評価します。
udp	ルールを UDP で評価します。
icmp	ルールを ICMP で評価します。
mac	ルールを MAC で評価します。
ip	ルールを IP で評価します。

■ 第3パラメータ(必須)

OnePointWall ルールで評価する対象、通常はパケットの送信元アドレス(mac or ip)を記述します。

第 2 パラメータが mac の場合は MAC アドレス指定します。

IP アドレスは単一のホストもしくはネットワークでの記述が可能です。

192.168.1.100	送信元が 192.168.1.100 のパケットを評価します。
192.168.1.100/32	上記と同じです。
192.168.1.0/24	192.168.1.1～192.168.1.254 までの IP アドレスを対象とします。

IP アドレス及びネットワークは not を指定することが可能です。

not 192.168.1.100	送信元が 192.168.1.100 以外のパケットを評価します
not 192.168.1.0/24	192.168.1.0～192.168.1.255 までの IP アドレス以外を対象とします

any と記述すると、任意の MAC アドレスまたは IP アドレスが対象となります。

■ 第4パラメータ(TCP,UDP,ICMP は必須)

OnePointWall ルールで評価する対象、通常はパケットの送信元ポート番号(sport)を記述します。

ICMP の場合は type を指定できます。

itype

タイプ	意味
0	エコー応答(echo reply)
3	あて先不達(destination unreachable)
4	送信元抑制(source quench)
5	経路変更要求(redirect)
8	エコー要求(echo request)
11	時間超過(time exceeded)
12	パラメータ異常(parameter problem)

13　　タイムスタンプ要求(timestamp request)
14　　タイムスタンプ応答(timestamp reply)
15　　情報要求(information request)
16　　情報応答(information reply)
17　　アドレス・マスク要求(address mask request)
18　　アドレス・マスク応答(address mask reply)

TCP/UDP ポートは"-"を用いることによって範囲指定することができます。
また、","で区切ることにより、最大 5 件（4 回までの区切りが可能）指定することができます。
80-100　　TCP/UDP ポート 80～100 までを指定
1012,2000　　TCP/UDP ポート 1012 と 2000 を指定
80-100,101-1000,1012,2000,2005-3000　　TCP/UDP ポート 80～100、101～1000、1012、2000、2005～3000 を指定
any と記述すると任意の TCP/UDP ポートが対象となります。

■ 第5パラメータ(必須)
OnePointWall ルールで評価する対象、通常はパケットの宛先アドレス(mac or ip)を記述します。
IP アドレスは単一のホストもしくはネットワークでの記述が可能です。
192.168.1.100　　宛先が 192.168.1.100 のパケットを評価します。
192.168.1.100/32　　上記と同じです。
192.168.1.0/24　　192.168.1.1～192.168.1.254 までの IP アドレスを対象とします。
any と記述すると、任意の MAC アドレスまたは IP アドレスが対象となります。
IP アドレス及びネットワークは not を指定することが可能です。
not 192.168.1.100　　宛先が 192.168.1.100 以外のパケットを評価します
not 192.168.1.0/24　　192.168.1.1～192.168.1.254 までの IP アドレス以外を対象とします
any と記述すると、任意の MAC アドレスまたは IP アドレスが対象となります。

■ 第6パラメータ(TCP,UDP,ICMP は必須)
OnePointWall ルールで評価する対象、通常はパケットの宛先ポート番号(dport)を記述します。
ICMP の場合は code を指定できます。
＊コードはここでは省略します。TCP/IP のプロトコル解析書等を参照して下さい。

TCP/UDP ポートは"-"を用いることによって範囲指定することができます。
また、","で区切ることにより、最大 5 件（4 回までの区切りが可能）指定することができます。
80-100　　TCP/UDP ポート 80～100 までを指定
1012,2000　　TCP/UDP ポート 1012 と 2000 を指定

80-100,101-1000,1012,2000,2005-3000	TCP/UDP ポート 80～100、101～1000、1012、2000、2005～3000 を指定

any と記述すると任意の TCP/UDP ポートが対象となります。

D　ルールオプション構成

■ msg オプション

Alert ログに表示するメッセージを記述します。後からログを見て理解できるような記述にするように心がけてください。

書式：　msg:"メッセージ";

[例]

msg:"FW/TCP Connection to HOME NET";

ログに FW/TCP Connection to HOME NET と表示する

■ dsize オプション

パケットのペイロード部分のサイズを指定することができます。

書式：　dsize:データサイズ;

[例]

- dsize:1<;　　ペイロード長 1 バイト以下
- dsize:100>;　ペイロード長 100 バイト以上
- dsize:146;　　ペイロード長 146 バイト

■ window オプション

TCP の window サイズを指定することができます。

書式：window:window サイズ;

[例]

window:16765;　　window サイズが 16765 バイト

■ flag オプション

TCP ヘッダーのシーケンスフラグを記述することができます。

書式：　flag: TCP フラグ;

TCP フラグ	記述方法	名称	意味
URG	U	緊急データフラグ	他のデータよりも先に(緊急に)処理すべきデータ
ACK	A	確認応答フラグ	確認応答フラグが”有効”に設定されている
PSH	P	プッシュ要求フラグ	受信したデータをすぐアプリケーション層に渡す
RST	R	リセット・セッションフラグ	セッションを強制終了する
SYN	S	同期シーケンス番号フラグ	セッションを開始する
FIN	F	最終データ送信フラグ	通信の完了を示す

flag オプションは以下の修飾子を記述可能です。

+ AND 条件を表します。

[例]

- flag:PA;　　プッシュ要求フラグと確認応答フラグ
- flag:U+;　　緊急データフラグとそれ以外のいずれか

●ルールオプション（マッチング）

以下のオプションは content や regexp と併用して使用します。対象の content、regexp より前に記述するようにしてください。

■ length オプション

length で指定した文字列の範囲内でマッチングします。regexp の場合は length で対象とした長さの文字列範囲内でマッチングを行います。この項目を指定すると処理が早いので、出来る限り設定するようにしてください。

書式 :　length:検索開始位置からの検索する長さ;

[例]

length:10;　　ペイロードの 10 バイトの範囲内でマッチングを行う（10 バイト目でマッチ終了）

■ nocase オプション

マッチングする際に大小文字の区別をしない。

書式 :　nocase;

[例]

nocase; content:"NETAGENT";

NETAGENT でも netagent でもマッチする

■ distance オプション

前回一致した場所からの検索開始位置指定を示します。2 回目以降のマッチングは、前回マッチ対象とした部分を切り出して行います。

書式:　distance:前回検索位置から次回検索位置までの長さ;

[例]

content:"netaegnt"; distance:1; content:"co"; distance:1; content:"jp";

「netagent」を検索後 1 バイトスキップして「co」を検索する。更にその後 1 バイトスキップしてから「jp」の検索を行う。

■ offset オプション

主に 1 回目のマッチで使用します。マッチ開始場所がペイロードの始めからの場合は省略できます。この項目を指定した方が処理が早いので、出来る限り設定してください。

書式:　offset:検索開始位置;

[例]

offset:4; content:"|00 01 86 A0|";

ペイロードの先頭から4バイトまでを無視し、5バイト目から検索を行い、|00 01 86 A0|のコンテントがある場合にマッチします。

■ content オプション

マッチングさせる文字列を指定します。バイナリで指定する場合は、マッチング対象文字列を「|」で囲って使用します。

書式 :　content:"マッチング文字列";

[例]

- content:"POST";　POST のコンテントがある場合にマッチ
- content:"|50 4F 53 54|";

|50 4F 53 54|のコンテント（POST）がある場合にマッチ

■ regexp オプション

正規表現を利用してマッチングさせる対象を指定します。

書式 :　regexp:"マッチング正規表現";

[例]

regexp:"/pm_path=(http|https|ftp)/";

pm_path=http、pm_path=https、pm_path=ftp のいずれかにマッチさせる。

content 及び regexp の前に offset,length,nocase,distance を記述します。

2つめ以降のマッチは前の content 及び regexp の後に、offset,length,nocase,distance を記述して content 及び regexp を記述します。

[例]

length:4; content:"GET"; distance:5; nocase; content:"search";

ペイロード4バイトまでに"GET"があり、そこから5バイトスキップして"search"もしくは"SEARCH"があるパケットにマッチさせる。

■ rev オプション

シグネチャのリビジョンを記述します。基本的に oid オプションと併用され、特定のシグネチャの修正状況を表す際に利用されます。

書式 :　rev: シグネチャバージョン;

[例]

rev:2;

■ oid オプション

OnePointWall のシグネチャの ID を記述します。oid はシグネチャを特定するために利用するため、必ずユニークな番号を割り振ります。

1～10000 番までは予約されていますので、**ユーザールールを作成する場合は 10001 番以降を割り振るようにしてください。**

書式 :　oid: シグネチャ ID;

[例]

oid:500;

■ gid オプション

シグネチャのグループを記述します。

書式 :　gid: シグネチャグループ ID;

[例]

gid:3;

OnePointWall で用意されているグループは以下の通りです。

;group:0,"nogroup";

;group:1,"Attack";

;group:2,"P2P";

;group:3,"IM";

;group:4,"Worm";

;group:5,"VPN";

;group:6,"Virus";

;group:7,"SPAM";

;group:8,"BBS write";

;group:9,"Firewall";

;group:10,"chat";

;group:12,"HTTP Upload";

;group:13,"game";

;group:14,"SMTP";

;group:96,"user rules 1";

;group:97,"user rules 2";

;group:98,"user rules 3";

;group:99,"test rules";

E ip 専用のオプション

■ ip_proto オプション

IP ヘッダのプロトコル・フィールドに設定されている値をチェックできます。使用可能なプロトコル番号、プロトコル名は通常/etc/protocols に一覧として用意されています。

書式: ip_proto:プロトコル番号;

[参照]

```
ip          0          IP                  # internet protocol, pseudo protocol number
icmp        1          ICMP                 # internet control message protocol
igmp        2          IGMP                 # Internet Group Management
ggp         3          GGP                  # gateway-gateway protocol
ipencap 4              IP-ENCAP             # IP encapsulated in IP (officially ``IP'')
st          5          ST                   # ST datagram mode
tcp         6          TCP                  # transmission control protocol
egp         8          EGP                  # exterior gateway protocol
pup         12         PUP                  # PARC universal packet protocol
udp         17         UDP                  # user datagram protocol
hmp         20         HMP                   # host monitoring protocol
xns-idp 22             XNS-IDP              # Xerox NS IDP
rdp         27         RDP                  # "reliable datagram" protocol
iso-tp4 29             ISO-TP4              # ISO Transport Protocol class 4
xtp         36         XTP                  # Xpress Tranfer Protocol
ddp         37         DDP                  # Datagram Delivery Protocol
idpr-cmtp 38           IDPR-CMTP            # IDPR Control Message Transport
ipv6        41         IPv6                 # IPv6
ipv6-route 43          IPv6-Route           # Routing Header for IPv6
ipv6-frag 44           IPv6-Frag            # Fragment Header for IPv6
idrp        45         IDRP                 # Inter-Domain Routing Protocol
rsvp        46         RSVP                 # Reservation Protocol
gre         47         GRE                  # General Routing Encapsulation
esp         50         ESP                  # Encap Security Payload for IPv6
ah          51         AH                   # Authentication Header for IPv6
skip        57         SKIP                 # SKIP
ipv6-icmp 58           IPv6-ICMP            # ICMP for IPv6
ipv6-nonxt 59          IPv6-NoNxt           # No Next Header for IPv6
ipv6-opts 60           IPv6-Opts            # Destination Options for IPv6
```

```
rspf        73   RSPF            # Radio Shortest Path First.
vmtp        81   VMTP            # Versatile Message Transport
ospf        89   OSPFIGP         # Open Shortest Path First IGP
ipip        94   IPIP            # IP-within-IP Encapsulation Protocol
encap       98   ENCAP           # Yet Another IP encapsulation
pim         103  PIM             # Protocol Independent Multicast
```

F replace 専用オプション

検索文字を置換文字に置き換える場合に利用します。replace 専用のオプションです。TCP セッションをとめずに特定のパケットのペイロードのみを置換することができます。
before と after のバイト数は必ず同じにする必要があります。足りない場合は空白で埋めてください。
書式:　　before:検索文字;　after:置換文字;
[例]

replace tcp 192.168.1.80 any $EXTERNAL_NET 80 (msg:"TEST/replace dummy.html"; before:" | 47 45 54 20 2F 73 75 70 70 6F 72 74 2E 68 74 6D 6C 20 48 54 54 50 2F 31 2E 31|"; after:" |47 45 54 2F 64 75 6D 6D 79 2E 68 74 6D 6C 20 48 54 54 50 2F 31 2E 31 20 20 |" ; rev:1; oid:1000; gid:99; ";)
「GET/support.html HTTP/1.1」のリクエストがあった場合に「GET/dummy.html HTTP/1.1」に置き換える。

●サンプルルール

drop tcp 192.168.1.0/24 any -> 192.168.1.0/24 80 (msg:"1 Drop 192/24 to 192/24 redbar"; offset:4; length:11; content:"/redbar.png"; distance:1; length:8; content:"HTTP/1.1"; rev:1; oid:1;gid:99;)
drop udp any any -> 0.0.0.0/0 665 (msg:"11 Drop udp any to any";content:"test"; rev:1; oid:11;gid:99;)
drop mac 00:30:1B:AB:09:01 -> any (msg:"MAC/ 00:30:1B:AB:09:01 stop"; gid:99;)

G ルール作成の手引き

不適切なルールは、OnePointWall のパフォーマンスを低下させ、止めるべきではない正規のパケットを止めてしまうことにつながります。
OnePointWall ルールを作成するにあたって、以下の点を注意して下さい。

● プロトコル仕様書を信用し(すぎ)ない

仕様書はあくまで仕様書です。プロトコルのバージョンや実装によってかなり違いがありますので、実際に流れているパケットを自分の目で確かめてルールを書きましょう。

● マッチング対象範囲を絞れるものは絞る

dsize、offset、length などを使える場合は積極的に使いましょう。パフォーマンスが向上します。

● 常時チューニングを行う

一度作ったルールは、テスト運用しながらチューニングをかけパフォーマンスや誤検知率の改善を図ってください。また、ソフトウェアのバージョンアップには注意してください。

● マッチングさせる内容を適切に選択する

マッチングさせる内容が間違っていると当然のことながら誤検知が発生します。Content 文字列の場合、短すぎると誤検知を発生する可能性が高くなります。複数の条件を指定して適切に止めてください。

8 ルールファイルコンパイル方法

■ コンパイラの場所

/usr/local/bin/opwc.pl

標準で入っているコンパイラです。アップデートが無い場合はこちらを使用します。

/log/opwc.pl

コンパイラのアップデートがあると/log ディレクトリに新しいバージョンが保存されますので、こちらを使用します。

■ コンパイラオプション

USAGE: /usr/local/bin/opwc.pl [-options]

OPTIONS:

-v	バージョンを表示
-h	ヘルプを表示
-c	ルールのエラーチェックを行う
-o <outfile>	出力ファイルを指定
-d <opw.rules>	標準ルールファイルを指定
-u <user.rules>	ユーザー定義ルールファイルを指定

■ 標準的なコンパイル方法

オプションを指定しないとデフォルト設定でコンパイルを行います。

/log/opwc.pl

/log/opw.rules と/log/user.rules をコンパイルして/log/opw.pat に出力。

但し、/log/onepoint.conf で選択されているものに限ります。

ユーザールールのチェックのみを行うときは以下のようにします。(コンパイルは実行しない)

/log/opwc.pl -c -u /log/user.rules

＊ 注意

コンパイルしたが検知に反映されていない場合は、以下のことに注意してください。

・/log/onepoint.conf の USE_RULES、USE_GROUP に該当ルールの oid,gid が記述されているか。

・文法エラーのため、コンパイルがされていない。

９ トラブルシューティング

●ネットワークカードがどれに割り当てられているのかわからない

Web インターフェースのステイタス画面に、各割り当てネットワークカードの MAC アドレスが表示されています。メーカーで提供するネットワークカードには、大抵 MAC アドレスが記載されていますので、カードに記載の MAC アドレスと比較してどこに割り当てられているのかを判別して下さい。また、コンソール画面で cat /proc/pci とコマンド打つと、PCI デバイスの一覧が表示されます。表示された情報にはネットワークカードのメーカー名や割り当てられている IRQ が表示されますので、コマンド /sbin/ifconfig の値と比べて、どこに割り当てられているのかを調べる方法もあります。

●ネットワークカードの割り当てが毎回変わる

ネットワークカードの種別が全て同じで PCI スロットを使用している場合、このような現象が発生します。これは、IRQ を共有しているためです。PCI スロットの５番目は使用しないようにすると、解決する場合が多いです。ネットワークカードを挿す位置を変更してみて下さい。

●ネットワークの負荷が異常に高くなった

ファイヤーウォールモード（ブリッジモード）で、同じハブもしくは同じネットワークのハブにブリッジになっているネットワークカードを挿していませんか。
ブリッジからの出入りのパケットを同じネットワークに流すと、ブロードキャストストームと呼ばれるパケットがループした状態になります。

●ライセンスエラーが発生する

ライセンスキーを入れていない場合、**ライセンスの有効期限が切れた場合は、検知やブロック機能が働かなくなります**。有効期限が切れる前に新しいライセンスを購入して下さい。USB メモリやハードディスクにインストールしないで、CD-ROM 機能のみの場合は、addlin コマンドでライセンスキーをコンソールから入れてください。

●通信がとまらない

ルール設定でとめる通信のチェックがされているかどうか確認してください。ホームネットや外部ネットワークが指定されている場合があります。
ライセンス有効期限が切れている場合も考えられます。Web 画面よりライセンスの有効期限を確認してください。

ＴＯ：ＮｅｔＡｇｅｎｔサポートセンター

ＴＥＬ：０３－５６１９－１３３３　ＦＡＸ：０３-５６１９-１２４４

ｅ－ｍａｉｌ：opw-support@netagent.co.jp

以下のフォームは、サポートを受ける場合に必要な情報になります。確認できる範囲内でご記入の上、ご連絡ください。
また、サポートはメールでもお受けします。以下のフォームにある情報をご記入のうえ、上記のメールアドレスまでご連絡ください。

お名前		TEL		FAX	
ご住所					
E-Mail					
商品名 型番		バージョン		購入日	
ライセンス番号					
エラー状況について	（発生したエラーや、エラーの発生したネットワーク構成をお書きください）				