



# FORTINET 社 FortiGate WEB CONFIG ご利用の手引き

Ver. 1.00

この度は、FORTINET 社ファイアーウォール FortiGate をご利用いただき、ありがとうございます。この手引きは、FORTINET 社ファイアーウォール FortiGate の WEB CONFIG をご利用いただく上での各種機能の説明や設定方法、注意事項をまとめております。必ず、最後までご一読いただき、保存・利活用いただきますよう、お願い申し上げます。

**株式会社チロロネット カスタマーサポート**

岡山県倉敷市西富井 636-30 〒710-0845

 **0120-919-766** (24 時間 365 日受付)

FAX : **086-460-3957**

MAIL : **support@chiroro.com**

URL : **<http://www.chiroro.co.jp/>**



# もくじ

---

<b>第1章</b>	<b>はじめにお読みください</b>	<b>3</b>
	1-1. 【ファイアウォール用アカウント設定完了のお知らせ】について	4
	1-2. 【アクセス制限実施・解除申請書】ご返送のお願い	5
<b>第2章</b>	<b>FortiGate WEB CONFIG の機能</b>	<b>6</b>
	2-1. FortiGate WEB CONFIG の各機能説明	7
	2-2-1. 【システム】の詳細機能説明	11
	2-2-2. 【ファイアウォール】の詳細機能説明	17
	2-2-3. 【アンチウイルス】の詳細機能説明	23
	2-2-4. 【侵入検知】の詳細機能説明	27
	2-2-5. 【Web フィルタ】の詳細機能説明	29
	2-2-6. 【アンチスパム】の詳細機能説明	32
	2-2-7. 【IM,P2P&VoIP】の詳細機能説明	35
	2-2-8. 【ログ&レポート】の詳細機能説明	37



## 第1章 はじめにお読みください

---

この章では、ファイアウォールのコンソールをご利用いただく上での重要事項をまとめております。サービスご利用の前に、ご一読ください。

### ◇この章のもくじ

- 1-1. 【ファイアウォール用アカウント設定完了のお知らせ】について
- 1-2. 【ファイアウォール ポート解放・閉鎖申請書】ご返送のお願い



## 1-1.【ファイアーウォール用アカウント設定完了のお知らせ】について

【ファイアーウォール用アカウント設定完了のお知らせ】は、お客様がファイアーウォールのコンソールをご利用になる上で必要なファイアーウォールアドレス・ユーザー名・パスワードを記載した、重要な書面です。サーバーセキュリティ確保の観点からも、紛失や第三者への開示等を行わないよう、ご注意ください。

また、【ファイアーウォール用アカウント設定完了のお知らせ】を紛失された場合は、ご契約者様の本人確認をさせていただいた後、有償(税込 2,100 円)による再発行となります。なりすましを防止する観点から、即時発行や電話・FAX 等による通知は行わず、再発行の後、郵送させていただきますので、紛失なきよう、ご注意ください。

2009年2月5日	
<b>【重要】ファイアーウォール用アカウント設定完了のお知らせ</b>	
この度は、弊社ファイアーウォールオプションサービスにお申込みいただきまして、誠にありがとうございます。 以下の通り、ファイアーウォールのコンソール用画面を設定いたしましたのでお知らせいたします。同封のマニュアルも併せてご覧ください。 なお、本紙につきましてはサーバーのセキュリティ確保のため、他人への開示等を行わないようお願いいたします。	
<b>■アカウント設定情報</b>	
ファイアーウォールアドレス	
ユーザー名	
パスワード	
<b>■ご注意</b>	
*本書の再発行はいたしません。紛失等されました場合は、有償(2,100円:税込)にて再発行させていただきます。 *ファイアーウォールの設定方法等につきましては、別冊のマニュアルをご覧ください。 なお、設定をした結果、接続できない等の状態になりました場合は、サービス開始時の設定に戻させていただきます。 *ファイアーウォールの設定に際し、接続元のネットワーク制限をさせていただいております。 接続元を変更される場合は、都度、アクセス制限実施・解除申請書をご用意ください。作業は無償です。 *アルファベット、数字、記号の印字見本は次の通りです。 ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789;:/.!@!*"#\$%&()	
<b>■お問い合わせ先</b>	
	株式会社チロロネット カスタマーサポート ☎ 0120-919-766(24時間365日受付) 、 FAX: 086-460-3957 、 MAIL: support@chiroro.com 〒710-0846 岡山県倉敷市西番井636-30 URL: <a href="http://www.chiroro.co.jp/">http://www.chiroro.co.jp/</a>
ISO 27001:2005認証ファイアーウォールコンソール設定書(0902版)	

本ファイルと共に綴じ込んでおきますと、紛失の心配もなく安心です。





## 第2章 FortiGate WEB CONFIG の機能

---

この章では、FortiGate WEB CONFIG の設定を管理変更するための機能説明と利用方法をご案内いたします。

### ◇この章のもくじ

- 2-1. FortiGate WEB CONFIG の各機能説明
- 2-2-1. [システム]の詳細機能説明
- 2-2-2. [ファイアウォール]の詳細機能説明
- 2-2-3. [アンチウイルス]の詳細機能説明
- 2-2-4. [侵入検知]の詳細機能説明
- 2-2-5. [Web フィルタ]の詳細機能説明
- 2-2-6. [アンチスパム]の詳細機能説明
- 2-2-7. [IM,P2P&VoIP]の詳細機能説明
- 2-2-8. [ログ&レポート]の詳細機能説明



## 2-1. FortiGate WEB CONFIG の各機能説明

### ■ FortiGate WEB CONFIG 画面へのログイン方法

お手元に、【ファイアウォール用アカウント設定完了のお知らせ】をご用意ください。

- ① ブラウザ(Internet Explorer、Safari、FireFox 等)を起動します。
- ② アドレス欄に、【ファイアウォール用アカウント設定完了のお知らせ】に記載されている、『ファイアウォールアドレス』を入力し、**Enter** キーを押します。

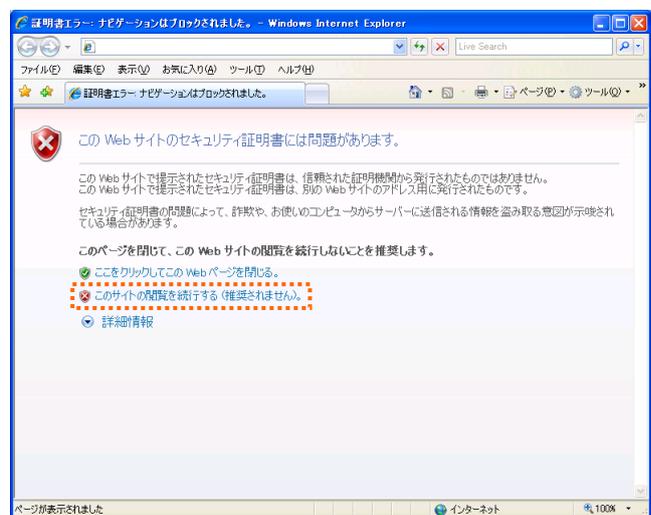
ファイアウォールアドレス	例)https:// 211.125.117.250/
--------------	-----------------------------

- ③ 右のような画面が表示されますので、**[OK]** ボタンをクリックします。



- ④ 次に、**[このサイトの閲覧を続行する (推奨されません。)]** をクリックします。

※ここでは、FORTINET 社の SSL 証明書を利用しておりますので、セキュリティ証明書のエラーが表示されます。SSL 暗号化通信は行っておりますのでご安心ください。証明書をインストールするとエラーは表示されなくなります。



- ⑤ 再び、右のような画面が表示されますので、**[OK]** ボタンをクリックします。



- ⑥ 右のような画面が表示されますので、  
【ファイアウォール用アカウント設定完了のお知らせ】に記載されている、『ユーザー名』『パスワード』を入力し、[ログイン] ボタンをクリックします。

ユーザー名	『ユーザー名』を入力します。
パスワード	『パスワード』を入力します。

※英語の大文字・小文字にご注意ください



## ■ FortiGate WEB CONFIG の基本画面

FortiGate WEB CONFIG の基本画面は以下のようになっております。



- (1)メニュー : 機能の各メニュー項目です。  
 (2)タブ : 各メニューより複数あります。  
 (3)ページ : メイン画面部分です。  
 (4)ボタンバー : ヘルプやログアウト時に使用します。

  30分間何も操作しないと、自動的にログアウトされます。

## ■ 各メニュー説明

各機能の設定の権限を以下の 3 種類とさせていただきます。

- × 権限なし : 設定や内容の閲覧も不可
- △ 閲覧のみ可 : 設定や内容の閲覧のみ可、変更は不可
- 閲覧・変更可 : 設定や内容の閲覧・変更が可能

システム	権限	内容
ステータス	△	FortiGate の現在の動作状態のスナップショットが確認できます。
ネットワーク	△	ネットワーク設定として、FortiGate インタフェースと DNS の設定を行います。
DHCP	△	DHCP を用いてクライアントのネットワーク構成を自動で行います。
設定	△	ネットワークに関係しないいくつかの機能を設定します。
管理者	×	FortiGate にアクセスしてその動作を設定します。
メンテナンス	×	システム設定のバックアップおよび復元、自動更新が設定できます。
ルータ		
スタティック	×	パケットの宛先 IP アドレスとネットマスクを定義し設定します。
ダイナミックルーティング	×	ネットワーク設定として、FortiGate インタフェースと DNS の設定を行います。
モニタ	×	DHCP を用いてクライアントのネットワーク構成を自動で行います。
ファイアウォール		
ポリシー	△	FortiGate を通過するすべてのトラフィックを制御します。
アドレス	△	ファイアウォール アドレスを追加、編集、および削除します。
サービス	△	ファイアウォールで許可または拒否する通信の種類を決定します。
スケジュール	△	ポリシーがアクティブまたは非アクティブになる時期を制御できます。
バーチャル IP	△	FortiGate を介した接続が可能になります。
プロテクションプロファイル	○	特定の目的に合わせて調整可能な設定のグループです。
VPN		
IPSEC	×	IPSEC暗号化通信によるVPNの設定を行います。
PPTP	×	PPTP 暗号化通信による VPN の設定を行います。
SSL	×	SSL 暗号化通信による VPN の設定を行います。
証明書	×	CAルート証明書、証明書失効リストのインポート、バックアップと復元。
ユーザ		
ローカル	×	ユーザアカウント、ユーザグループ、外部の認証サーバを設定します。
RADIUS	×	RADIUS サーバを使用してユーザを認証する場合に使用します。
LDAP	×	LDAP サーバを使用してユーザを認証する場合に使用します。
Windows AD	×	Windows Active Directory サーバの設定を行います。
PKI	×	PKI (Public Key Infrastructure) 認証の設定を行います。
ユーザグループ	×	ユーザ ID のリストです。
認証	×	ユーザ認証の設定を行います。

	権限	内容
<b>アンチウイルス</b> ファイルパターン 隔離 設定	..... ○ ..... ○ ..... ○	ウイルスのファイルパターンを設定します。 ブロックされたファイルや感染したファイルの隔離設定を行います。 ウイルス定義の一覧リストとグレーウェアリストが確認できます。
<b>侵入検知</b> シグネチャ アノーマリ	..... ○ ..... ○	シグネチャ型の不正侵入設定を行います。 アノーマリ型の不正侵入設定を行います。
<b>Webフィルタ</b> コンテンツブロック URLフィルタ FortiGuard - ウェブフィルタ	..... ○ ..... ○ ..... ○	特定の単語やパターンをブロックすることによりWebコンテンツを制御します。 特定 URL へのアクセスの許可やブロックを制御します。 FortiGuard-Webにより、Webサイトの許可、ブロック、監視を行います。
<b>アンチスパム</b> 禁止ワード ブラックホワイリスト	..... ○ ..... ○	特定の単語やパターンを含むメールをブロックし、スパムを制御します。 IP アドレスとメールアドレスにより、ブラックまたはホワイトリストに設定できます。
<b>IM, P2P &amp; VoIP</b> 統計情報 ユーザ	..... △ ..... △	IM、P2P、および VoIP の使用状況に関する統計を調べることができます。 IM ユーザの接続を許可またはブロックの制御ができます。
<b>ログ&amp;レポート</b> Log環境設定 ログアクセス コンテンツアーカイブ レポート設定 リモートアクセス	..... △ ..... △ ..... △ ..... △ ..... △	ネットワーク活動やトラフィックの記録環境を設定できます。 各ログ情報の表示や保存、分析が行えます。 アーカイブされたログを表示することができます。 FortiAnalyzer レポートの設定、表示、印刷を行うことができます。 帯域と流量がグラフで確認できます。



## 2-2-1. [システム]の詳細機能説明

### ■ [ステータス]画面

[ステータス]は[閲覧のみ]の権限となっております。

The screenshot shows the FortiGate system status page with the following sections highlighted by numbered callouts:

- (1) **システムステータス**: System status information including serial number, uptime, system time, HA status, host name, firmware version, operation mode, and current administrator.
- (2) **ライセンス情報**: License information for FortiGuard subscriptions, including antivirus, AV, IPS, and web filtering licenses.
- (3) **CLIコンソール**: A terminal window showing a successful connection to the FortiGate CLI.
- (4) **Unit Operation**: A status indicator for the network interface (INTDM2WAN1WAN2).
- (5) **アラートメッセージコンソール**: A log of system alerts and events, such as system reboots and connection limits.
- (6) **統計情報**: Traffic and session statistics, including session count and content filter usage.
- (7) **システムリソース**: System resource usage gauges for CPU (0%) and memory (68%).

- (1)システムステータス : シリアル番号、稼働時間、システム時間等が表示されます。
- (2)ライセンス情報 : アンチウイルス、IPS、ウェブフィルタ、アンチスパム等のライセンス期限が表示されます。
- (3)CLIコンソール : FortiOS には、CLIからしかアクセスできないコマンドがあります。画面内をクリックすると、CLI に自動的にログインされます。
- (4)Unit Operation : イーサネット インタフェースのステータスが表示されます。ネットワーク インタフェースが緑色になっている場合、そのインタフェースは接続されています。インタフェースの上にマウスポインタを置くと、IP アドレス、ネットマスク、およびインタフェースの現在のステータスが表示されます。
- (5)アラートメッセージコンソール : FortiGate に対する変更を追跡できます。再起動、ファームウェアのアップグレード、アンチウイルスエンジンの使用状況下などでのログが確認できます。
- (6)統計情報 : ネットワークトラフィックや保護に関して、FortiGate での状況の確認ができます。
- (7)システムリソース : CPU、メモリ、セッション、およびネットワークの使用率をグラフで表示します。

## ■ [ネットワーク] 画面

[ネットワーク] は [閲覧のみ可] の権限となっております。

(1) インタフェース : [インタフェース] タブから [設定] ボタンをクリックすると以下の [インタフェース] 設定画面が表示されます。なお、権限が [閲覧のみ可] の場合、入力欄に文字を入力しても、[戻る] ボタンしかございませんので、変更した設定を保存できないようになっております。

The screenshot shows the 'Interface' tab selected in the top navigation bar. Below it is a table listing network interfaces:

インタフェース名	IP / ネットマスク	アクセス	ステータス	
dmz	10.10.10.1 / 255.255.255.0	HTTPS,PING	○	[設定]
internal	192.168.1.99 / 255.255.255.0	HTTPS,PING	○	[設定]
modem	/		○	[設定]
wan1	211.125.117.248 / 255.255.255.255	HTTPS,PING	○	[設定]
wan2	192.168.101.99 / 255.255.255.0	PING	○	[設定]

Below the table is the 'Edit Interface' dialog for 'wan1'. The dialog contains the following fields and options:

- インタフェース名: wan1 (00:09:0F:13:27:22)
- Alias: [ ]
- アドレッシングモード:  マニュアル  DHCP  PPPoE
- IP/ネットマスク: 211.125.117.248/255.255.255.
- DDNS:  有効
- Pingサーバ: [ ]  有効
- 管理権限アクセス:  HTTPS  PING  HTTP  SSH  SNMP  TELNET
- MTU:  MTUよりも大きなパケットは分割する 1500 (バイト)
- Secondary IP Address: IP / ネットマスク: 0.0.0.0/24, Pingサーバ: 0.0.0.0  有効, 管理権限アクセス:  HTTPS  PING  HTTP  SSH  SNMP  TELNET
- [Add] button
- Table with columns: IP / ネットマスク, Pingサーバ, 有効, 管理権限アクセス
- Description (63 characters): [ ]
- [戻る] button

(2) ゾーン : ゾーンを使用して、関連するインタフェースと VLAN サブインタフェースをグループ化することができます。[ゾーン] タブをクリックすると以下の [ゾーン] 確認画面が表示されます。

The screenshot shows the 'Zone' tab selected in the top navigation bar. Below it is a table with the following data:

ゾーン名	所属しているインタフェース
イントラゾーンのトラフィックをブロック	

(3)オプション : ネットワーク オプションには、DNS サーバや停止ゲートウェイ検出の設定が含まれます。[オプション] タブをクリックすると以下の [オプション] 設定画面が表示されます。

The screenshot displays the 'Networking Options' configuration page. At the top, there are three tabs: 'インタフェース' (Interface), 'ゾーン' (Zone), and 'オプション' (Options), with 'オプション' being the active tab. The main content area is titled 'Networking Options' and is divided into two sections: 'DNS Settings' and 'Dead Gateway Detection'.

**DNS Settings**

- DNSサーバのアドレスを自動的に取得する
- 次のDNSサーバを使用する
- プライマリDNSサーバ:
- セカンダリDNSサーバ:
- Local Domain Name:

以下からのDNSフォワーディングを有効にする:

- internal
- dmz

**Dead Gateway Detection**

- Detection Interval:  (seconds)
- Fail-over Detection:  (lost consecutive pings)

## ■ [DHCP] 画面

[DHCP] は [閲覧のみ可] の権限となっております。

なお、DHCP の設定は利用しないため、行っておりません。

(1) サービス : [サービス] タブをクリックすると以下の [DHC サービス] 確認画面が表示されます。

[▼] ボタンをクリックすると、項目の内容が展開でき、さらに、[+] ボタンをクリックすると、[新規 DHCP サーバ] 設定画面が表示されます。

サービス	インタフェース	サーバ名/リレー IP	タイプ	有効
dmz	リレー	-	-	
	サーバ	-	-	[+]
internal	リレー	-	-	
	サーバ	-	-	[+]
wan1	リレー	-	-	
	サーバ	-	-	[+]
wan2	リレー	-	-	
	サーバ	-	-	[+]

新規DHCPサーバ

名前

Enable

タイプ  レギュラー  IPSEC

IPレンジ  -

ネットワークマスク

デフォルトゲートウェイ

ドメイン

割当期限  無期限  
 7 (日) 0 (時間) 0 (分)  
(5分 - 100日)

詳細設定 (DNS, WINS, Custom Options, Exclude Ranges.)

戻る

(2) アドレス割当 : [アドレス割当] タブをクリックすると以下のように [アドレス割り当て] 確認画面が表示されます。DHCP サーバが割り当てた IP アドレスおよび対応するクライアント MAC アドレスを確認できます。

サービス アドレス割当

インタフェース: All [▼] リフレッシュ

IP	MAC	割当期限	Status
----	-----	------	--------

## ■ [設定] 画面

[設定] は [閲覧のみ可] の権限となっております。

(1) HA : [HA] タブをクリックすると以下の [HA] 設定画面が表示されます。

[HA] とは、高い可用性を持つコンピュータシステムのことで、稼働率が高いほど高可用性であると言えます。一般的に稼働率を高めるためには、クラスタリングや多重化、自動バックアップ、ホットスワップなどの技術を用います。

ここでは、この機能はご利用いただけません。

	ポートモニタ	ハートビートインタフェース	
		Enable	プライオリティ(0-512)
dmz	<input type="checkbox"/>	<input checked="" type="checkbox"/>	50
internal	<input type="checkbox"/>	<input type="checkbox"/>	0
wan1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	50
wan2	<input type="checkbox"/>	<input type="checkbox"/>	0

(2) SNMP v1/v2c : [SNMP v1/v2c] タブをクリックすると以下の [SNMP] 設定画面が表示されます。SNMP (Simple Network Management Protocol) では、ネットワーク上のハードウェアを監視できます。ハードウェア、つまりFortiGate SNMP エージェントを設定して、SNMP マネージャにシステム情報を報告したり、トラップ (アラームやイベント メッセージ) を送信したりできます。

名前	クエリ	トラップ	有効
----	-----	------	----

- (3) 警告メッセージ : [警告メッセージ] タブをクリックすると以下の [警告メッセージ] 確認画面が表示されます。[▼] ボタンをクリックすると、項目の内容が展開でき、さらに、 ボタンをクリックすると、[警告の際のメッセージ] が表示されます。

名前	説明	
▼ <b>メール</b>	メールサービス用の置換メッセージ。	
ウイルス警告メッセージ	ウイルスを検知したメール添付ファイルの置き換え。	
ファイルブロック メッセージ	ブロックしたメール添付ファイルの置き換え。	
ファイルサイズ上限警告メッセージ	ファイルサイズ上限を超えたメール添付ファイルの置き換え。	
分割メール	分割されたメールの置き換え。	
ウイルスメッセージ (splice モード)	Spliceモード使用時ウイルス感染した際のメッセージ。	
ファイルブロックメッセージ (splice モード)	Spliceモード使用時ブロックした際のメッセージ。	
ファイルサイズ上限警告メッセージ (splice モード)	Spliceモード使用時ファイルサイズ上限を超えた際のメッセージ。	
▶ <b>http</b>	HTTP用の置換メッセージ。	
▶ <b>ftp</b>	FTP用の置換メッセージ。	
▶ <b>NNTP</b>	Replacement for invalid NNTP service.	
▶ <b>アラートEメール</b>	アラートEメール用メッセージ。	
▶ <b>スパム</b>	SMTP用の置換メッセージ。	
▶ <b>Administration</b>	Replacement for administration messages.	
▶ <b>Authentication</b>	Replacement for authentication pages.	
▶ <b>FortiGuard Web Filtering</b>	FortiGuard Web Filtering replacement messages.	
▶ <b>IM and P2P</b>	Replacement for blocked IM and P2P.	
▶ <b>SSL VPN</b>	Replacement for SSL VPN message.	

メッセージ: Eメールのウイルス警告メッセージ  
 使用可能な形式: Text  
 サイズ: 8192 (キ+ラクタ)

```
Dangerous Attachment has been Removed. The file "XXFILEXX" has been removed because of a virus. It was infected with the "XXVIRUSXX" virus. File quarantined as: "XXQUARFILENAMEXX".
```

戻る

例えば、電子メールにウイルスが含まれていた場合は、左のようなフォーマットの警告メールが届きます。

- (4) Operation : [Operation] タブをクリックすると以下の [運用モード] 設定画面が表示されます。

HA	SNMP v1/v2c	警告メッセージ	Operation
モード			
運用モード		NAT	



## 2-2-2. [ファイアウォール]の詳細機能説明

### ■ [ポリシー]画面

[ポリシー]は[閲覧のみ可]の権限となっております。

 ボタンをクリックすると、[ポリシー編集] 確認画面が表示されます。

Status	ID	送信元	宛先	スケジュール	サービス	プロファイル	アクション
▼ internal -> wan1 (8)							
<input checked="" type="checkbox"/>	1	all	all	always	FTP		ACCEPT 
<input checked="" type="checkbox"/>	2	all	all	always	SMTP		ACCEPT 
<input checked="" type="checkbox"/>	3	all	all	always	DNS		ACCEPT 
<input checked="" type="checkbox"/>	4	all	all	always	HTTP		ACCEPT 
<input checked="" type="checkbox"/>	5	all	all	always	POP3		ACCEPT 
<input checked="" type="checkbox"/>	6	all	all	always	HTTPS		ACCEPT 
<input checked="" type="checkbox"/>	7	all	all	always	NTP		ACCEPT 
<input checked="" type="checkbox"/>	8	all	all	always	UDP		ACCEPT 
▼ wan1 -> internal (9)							
<input checked="" type="checkbox"/>	9	Chiroro-Net Admin	Web+Mail Server	always	FTP	web	ACCEPT 
<input checked="" type="checkbox"/>	10	Chiroro-Net Admin	Web+Mail Server	always	SSH		ACCEPT 
<input checked="" type="checkbox"/>	11	all	Web+Mail Server	always	SMTP		ACCEPT 
<input checked="" type="checkbox"/>	12	all	Web+Mail Server	always	HTTP	web	ACCEPT 
<input checked="" type="checkbox"/>	13	all	Web+Mail Server	always	POP3	mail-pop	ACCEPT 
<input checked="" type="checkbox"/>	14	all	Web+Mail Server	always	HTTPS		ACCEPT 
<input checked="" type="checkbox"/>	15	all	Web+Mail Server	always	SUBMISSION		ACCEPT 
<input checked="" type="checkbox"/>	16	Chiroro-Net Admin	Web+Mail Server	always	WEBMIN		ACCEPT 
<input checked="" type="checkbox"/>	17	Chiroro-Net Admin	Web+Mail Server	always	PING TCP		ACCEPT 

ポリシー編集

送信元インタフェース/ゾーン: internal

送信元アドレス: all

宛先インタフェース/ゾーン: wan1

宛先アドレス: all

スケジュール: always

サービス: FTP

アクション: ACCEPT

NAT  ダイナミックIP Pool  
 固定ポート

プロテクションプロファイル: unfiltered

Log Allowed Traffic

認証: Firewall

トラフィックシェーピング

User Authentication Disclaimer

Redirect URL:

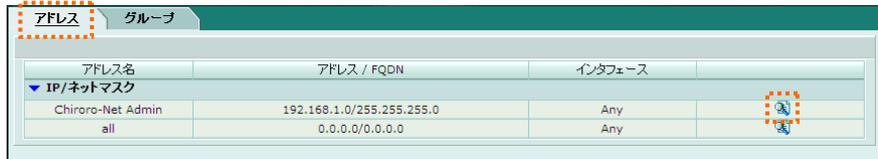
コメント (最大半角63文字):

## ■ [アドレス] 画面

[アドレス] は [閲覧のみ可] の権限となっております。

(1) アドレス : [アドレス] タブをクリックすると以下の [アドレス] 確認画面が表示されます。

[] ボタンをクリックすると、[アドレス編集] 画面が表示されます。



アドレス名	アドレス / FQDN	インタフェース
Chiroro-Net Admin	192.168.1.0/255.255.255.0	Any
all	0.0.0.0/0.0.0.0	Any



編集

アドレス名: Chiroro-Net Admin

タイプ: サブネット/IP範囲指定

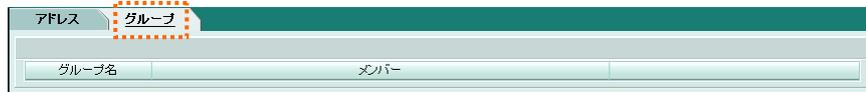
サブネット/IP範囲指定: 192.168.1.0/255.255.255.0

インタフェース: Any

戻る

(2) グループ : [グループ] タブをクリックすると以下の [グループ] 確認画面が表示されます。

アドレス グループの確認ができます。



グループ名	メンバー
-------	------

## ■ [サービス] 画面

[サービス] は [閲覧のみ可] の権限となっております。

(1) 初期設定 : [初期設定] タブをクリックすると以下の [初期設定の定義済みのサービス] 確認画面が表示されます。



サービス名	詳細
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
DCE-RPC	TCP/135 UDP/135
DHCP	UDP/67-68
DNS	TCP/53 UDP/53
ESP	IP/50
FINGER	TCP/79
FTP	TCP/21
FTP_GET	TCP/21
FTP_PUT	TCP/21
GOPHER	TCP/70
GRE	IP/47
H323	TCP/1720,1503 UDP/1719
HTTP	TCP/80
HTTPS	TCP/443
ICMP_ANY	ICMP/ANY
IKE	UDP/500,4500
IMAP	TCP/143
INFO_ADDRESS	ICMP/17
INFO_REQUEST	ICMP/15
IRC	TCP/6660-6669
Internet-Locator-Service	TCP/389
L2TP	TCP/1701 UDP/1701
LDAP	TCP/389
NFS	TCP/111,2049 UDP/111,2049
NNTP	TCP/119
NTP	TCP/123 UDP/123

(2) カスタム : [カスタム] タブをクリックすると以下の [カスタムサービス] 確認画面が表示されます。

 ボタンをクリックすると、[サービスの編集] 画面が表示されます。



サービス名	詳細
SUBMISSION	TCP/1-65535:587
WEBMIN	TCP/1-65535:10000 UDP/1-65535:10000

サービスの編集

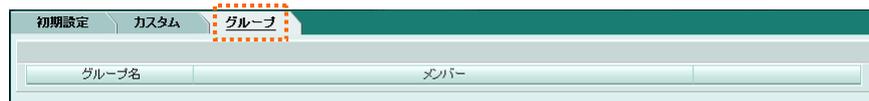
サービス名: SUBMISSION

プロトコル: TCP/UDP

プロトコル	送信元ポート		宛先ポート	
	下限値	上限値	下限値	上限値
TCP	1	65535	587	587

戻る

(3) グループ : [グループ] タブをクリックすると以下の [サービスグループ] 確認画面が表示されます。

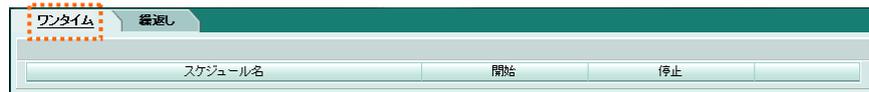


グループ名	メンバー

## ■ [スケジュール] 画面

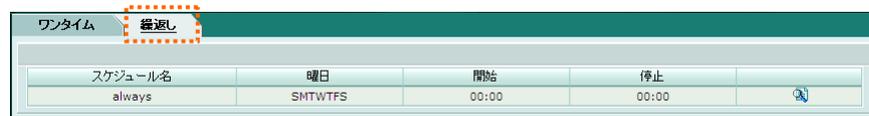
[スケジュール] は [閲覧のみ可] の権限となっております。

(1) ワンタイム : [ワンタイム] タブをクリックすると以下の [ワンタイムスケジュール] 確認画面が表示されます。指定された期間だけポリシーがアクティブまたは非アクティブになるワンタイムスケジュールを作成できます。



スケジュール名	開始	停止

(2) 繰り返し : [繰り返し] タブをクリックすると以下の [繰り返し(反復)スケジュール] 確認画面が表示されます。 ボタンをクリックすると、[スケジュールを編集] 画面が表示されます。



スケジュール名	曜日	開始	停止
always	SMTWTFS	00:00	00:00



スケジュールを編集

スケジュール名: always

曜日: 日 月 火 水 木 金 土

選択:

開始: 時 00 分 00

停止: 時 00 分 00

戻る

注1: 停止時刻を開始時刻より早い時間に設定した場合、停止時刻は翌日となります。注2: 開始時刻と停止時刻を同じ時間に設定した場合、このスケジュールは24時間動作することになります。

## ■ [バーチャル IP] 画面

[バーチャル IP] は [閲覧のみ可] の権限となっております。

(1) バーチャル IP : [バーチャル IP] タブをクリックすると以下の [バーチャル IP] 確認画面が表示されます。[編集] ボタンをクリックすると、[バーチャル IP 編集] 画面が表示されます。

バーチャルIP名	IP	サービスポート	マッピングするIP	マッピングするポート	
Web+Mail Server	wan1/211.125.117.105		192.168.1.10		

編集

バーチャルIP名

Externalインタフェース

タイプ  スタティックNAT  Server Load Balance

External IP Address/Range

Mapped IP Address/Range

ポートフォワーディング

(2) バーチャル IP グループ : [バーチャル IP グループ] タブをクリックすると以下の [バーチャル IP グループ] 確認画面が表示されます。バーチャル IP グループを作成することで、ファイアウォール ポリシー トラフィック制御を容易にすることができます。

Group Name	Members	Interface
------------	---------	-----------

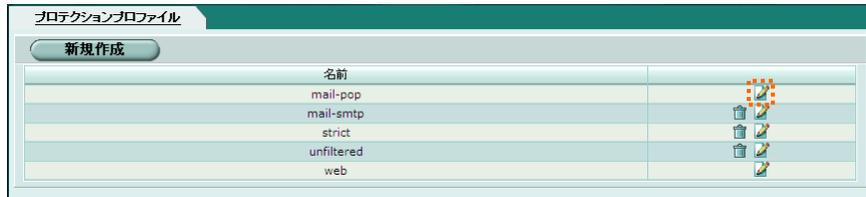
(3) IP プール : [IP プール] タブをクリックすると以下の [IP プール] 確認画面が表示されます。

Name	スタートIP	エンドIP
------	--------	-------

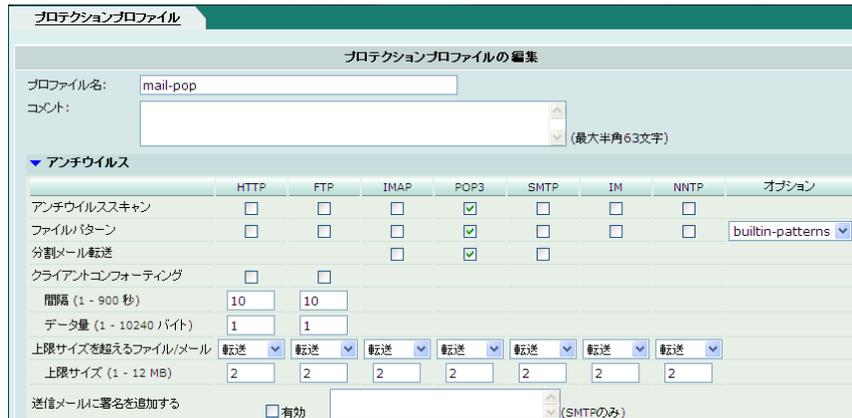
■ [プロテクションプロファイル] 画面

[プロテクションプロファイル] は [閲覧・変更可] の権限となっております。

[] ボタンをクリックすると、[プロテクションプロファイルの編集] 画面が表示されます。プロテクションプロファイルを予め設定し、さまざまなファイアウォールポリシーに登録し、保護のタイプおよびレベルをカスタマイズします。



さらに、[] ボタンをクリックすると、項目の内容が展開でき、プロファイルの設定が行えます。以下は [mail-pop] のプロファイル設定例です。



- ・ アンチウイルス : POP3 の必要な箇所にチェックを入れます。

▼ スпамフィルタリング				
	<input type="checkbox"/> IMAP	<input checked="" type="checkbox"/> POP3	<input type="checkbox"/> SMTP	オプション
<b>FortiGuardアンチスパム</b>				
IPアドレスチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
URLチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
チェックサムチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
誤検知報告リンク追加	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
IPアドレスBWLチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	BWL IP1 ▼
リバースDNSルックアップ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
メールアドレスBWLチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	BWL MAIL1 ▼
送信メールDNSチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
禁止ワードチェック	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	BLOCK WORD1 ▼ Threshold: 10
スパムアクション	タグ付加		タグ付加 ▼	
タグを付加する箇所:	<input type="radio"/> サブジェクト	<input checked="" type="radio"/> サブジェクト	<input type="radio"/> サブジェクト	
	<input type="radio"/> MIME	<input type="radio"/> MIME	<input type="radio"/> MIME	
付加するタグ:	Spam	[Spam]	Spam	

- ・ スпамフィルタリング：POP3 の必要な箇所にチェックを入れます。

サブジェクトか MIME にマークを付け、付加するタグを変更することもできます。

▼ ログ	
	ログ
<b>アンチウイルス</b>	
ウイルス	<input checked="" type="checkbox"/>
ブロックされたファイル	<input checked="" type="checkbox"/>
上限サイズを超えるファイル/メール	<input checked="" type="checkbox"/>
<b>ウェブフィルタリング</b>	
コンテンツブロック	<input type="checkbox"/>
URLフィルタ	<input type="checkbox"/>
ActiveXフィルタ	<input type="checkbox"/>
Cookieフィルタ	<input type="checkbox"/>
Javaアプレットフィルタ	<input type="checkbox"/>
<b>FortiGuardウェブフィルタリング</b>	
レーティングエラー (HTTPのみ)	<input checked="" type="checkbox"/>
<b>スパムフィルタリング</b>	
スパムロギング	<input checked="" type="checkbox"/>
<b>IPS</b>	
侵入検知ロギング	<input type="checkbox"/>
<b>IM / P2P</b>	
IMのアクティビティをロギング	<input type="checkbox"/>
P2Pのアクティビティをロギング	<input type="checkbox"/>
<b>VoIP</b>	
VoIPのアクティビティをロギング	<input type="checkbox"/>

- ・ ログ：ここでは、POP のログを設定したいので、[ウイルス] [ブロックされたファイル] [上限サイズを超えるファイル/メール] [FortiGuard ウェブフィルタリング(レーティングエラー)] [スパムフィルタリング(スパムロギング)] にそれぞれチェックを付けます。



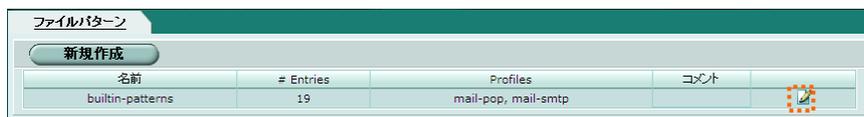
## 2-2-3. [アンチウイルス]の詳細機能説明

### ■ [ファイルパターン] 画面

[ファイルパターン] は [閲覧・変更可] の権限となっております。

ボタンをクリックすると、[ファイルパターンリスト] 確認画面が表示されます。

脅威である可能性のあるすべてのファイルをブロックし、アクティブなコンピュータ ウィルス攻撃を阻止するためのファイルパターンを設定できます。

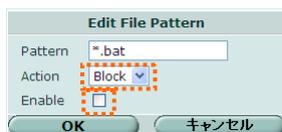


さらに、 ボタンをクリックすると、[ファイルパターン編集] 確認画面が表示されます。

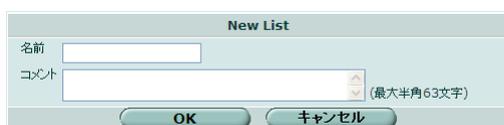


登録されている拡張子のファイルが、添付されていた場合の挙動を設定します。

[Block(通過不可)] または [Allow(通過可)] のアクションを選択したり、有効にする場合に選択します。[Enable(有効)] にチェックを入れると、[Block(通過不可)] または [Allow(通過可)] が有効になります。



をクリックすると、新しいパターンを作成することもできます。



パターンは正規表現で指示します。

例. [.lzh 形式のファイルを全て] の場合→ [\*.lzh] と入力

[.vbd, .vbe, .vbg など] の場合→ [.vb?]

※次ページに正規表現形式の詳細を記載しています。

※正規表現形式

式	一致する文字列
abc	"abc" (文字シーケンスは正確に一致するが、文字列内のどの位置にあってもよい)
^abc	文字列の先頭にある "abc"
abc\$	文字列の最後尾にある "abc"
alb	"a" または "b" のどちらか
^abc abc\$	文字列の先頭または最後尾にある文字列 "abc"
ab{2,4}c	"a" の後に 2 ~ 4 個の "b"、その後に 1 個の "c"
ab{2,}c	"a" の後に少なくとも 2 個の "b"、その後に 1 個の "c"
ab*c	"a" の後に任意個数 (0 個以上) の "b"、その後に 1 個の "c"
ab+c	"a" の後に 1 個以上の "b"、その後に 1 個の "c"
ab?c	"a" の後にオプションの "b"、その後に 1 個の "c" (つまり、"abc" または "ac" のどちらか)
a.c	"a" の後に任意の 1 文字 (改行以外)、その後に 1 個の "c"
a¥.c	正確に "a.c"
[abc]	"a"、"b"、"c" のうちの任意の 1 つ
[Aa]bc	"Abc" または "abc" のどちらか
[abc]+	複数個の "a"、複数個の "b"、複数個の "c" から成る任意の (空以外の) 文字列 ("a"、"abba"、"acbabcacaa" など)
[^abc]+	"a"、"b"、"c" をまったく含まない任意の (空以外の) 文字列 ("defg" など)
¥¥d¥d	任意の 2 桁 10 進数 (42 など)、¥d{2} と同じ
/i	パターンの大文字と小文字が区別されないようにします。たとえば、/bad language/i を指定すると、大文字/小文字には関係なく、badlanguage のすべての事例がブロックされます。
¥w+	1 つの "単語": 英数字とアンダーライン (アンダースコア) から成る空以外のシーケンス (foo、12bar8、foo_1 など)
100¥s*mk	オプションで任意数の空白 (スペース、タブ、改行) によって分けられた文字列 "100" と "mk"
abc¥b	後に単語境界が存在する場合の "abc" (たとえば、"abc!" には含まれるが、"abcd" には含まれない)
perl¥B	後に単語境界が存在しない場合の "perl" (たとえば、"perlert" には含まれるが、"perl stuff" には含まれない)
¥x	正規表現パーサーに、直前にバックスラッシュ文字がなく、かつ文字クラスにも含まれていない空白を無視するように指示します。正規表現をいくつかの部分に分割して (若干) 読みやすくするために使用します。
/x	他のテキスト内に正規表現を追加するために使用されます。パターン内の最初の文字がフォワードスラッシュ '/' である場合、その '/' は区切り記号として処理されます。このパターンには、2 つ目の '/' が含まれている必要があります。 '/' の間にあるパターンは正規表現と見なされ、2 つ目の '/' の後の任意の文字は正規表現のオプション ('i'、'x'、その他) のリストとして解析されます。2 つ目の '/' がないと、エラーが発生します。正規表現では、前や後に置かれているスペースは正規表現の一部として処理されます。

## ■ [隔離] 画面

**[隔離] は [閲覧・変更可] の権限となっております。**

ブロックされたファイルや感染したファイルを隔離できます。それらのファイル名やファイルに関する状態情報は、隔離済みファイルリストに表示され、特定のファイルを送信したり、自動送信リストに特定のファイルパターンを追加してそれらのファイルが解析のためにFortinet に自動的にアップロードできます。

(1) 隔離ファイル : [隔離ファイル] タブをクリックすると以下の [隔離ファイル] 確認画面が表示されます。



(2) 設定 : [設定] タブをクリックすると以下の [隔離設定] 確認画面が表示されます。



## ■ [アンチウイルス設定] 画面

[アンチウイルス設定] は [閲覧・変更可] の権限となっております。

(1) ウィルス一覧 : [ウィルス一覧] タブをクリックすると以下の [ウィルス一覧] 確認画面が表示されます。

ウィルス一覧		
グレーウェア		
0 - 9 A - F G - L M - R S - Z All		
Agent.GJT/tr	ALS/Bursted.C	AntiCMOS.fam
Backdoor.Netbus.170	BAT/AddShare.W/tr	BAT/Agent.BT/tr
BAT/Agent.L/tr	BAT/Autorun.57F1	BAT/Autorun.AE/worm
BAT/Autorun.CZ/worm	BAT/Autorun.Y/worm	BAT/Avk81.BBK/tr.bdr
BAT/Coparer.A/tr	BAT/Deltree.gen/tr	BAT/Dloader.AB/worm
BAT/Dyene.A/tr	BAT/FormatAll.E/tr	BAT/Hijacker.TEY/tr
BAT/HostChg.GDA/tr	BAT/IRCBot.APH/tr	BAT/KillAV.AH/tr
BAT/KillAV.DE/tr	BAT/KillAV.DF/tr	BAT/KillAV.EK/tr
BAT/KillAV.WJL/tr	BAT/Paua.AA/tr	BAT/Qhost.DBA/tr
BAT/Sdel/tr	BAT/SDel.0CC8/tr	BAT/ShutDown.BI/tr
BAT/Shutdowner.CZ/tr	BAT/Small.ASB/tr	BAT/Small.IN/tr
BAT/Small.SLY/tr	BAT/Small.TJ/tr	BAT/UsbThief.AA/tr.spy
BAT/Zapchast.0837/tr	BAT/Zapchast.B/tr	BKldr.QIT/tr
BDoor.AWQ/tr.bdr	BDoor.CEP/tr.bdr	BDoor.CX/tr.bdr
BDoor.CYL/tr.bdr	BDoor.DIV/tr.bdr	BDoor.DK/tr.bdr
BHO.G/tr.pws	BOOT/Dins.A/tr.bdr	BOOT/Zuzana.BC
Cimuz.BA/tr	Clagger.BF/tr	Connie.2708
Cracker.3088	Crackin.EBBA9CBC	DANNISH_TINY.251
Data/Eicar.AKS/tr	Data/Eicar.AKW/tr	Data/Eicar.AKY/tr
Data/Iframe.GIF/tr.ddr	DATA/JPEG_TEST_FILE	Data/PHEmb.A/exploit
Data/PossibleVulGDIX97M/.C/exploit.M20083013	Data/QDataHost/tr	Data/Qhost
Data/QHost/tr	Data/QHost.GJ/tr	Data/Qhosts
Data/QHosts.AE/tr	Data/QHosts.APD	Data/QHosts.APD/tr
Data/QHosts.ARG/tr	Data/QHosts.AS/tr	Data/QHosts.B/tr
Data/QHosts.JX/tr	Data/QHosts.QIY/tr	Data/WmaGetCodec.C/tr.ddr
Data/WmaWimad.D/tr.ddr	DcomRpc/exploit	DcomRpc.G/exploit
Delp5anc.A	Desperado.2403	Dialer/PlayGames
Dialer_Coulomb	Dloader.AK/tr	Dloader.CO/tr
Dloader.O/tr	Dloader.U/tr	Drop.D/tr
Eicar	EICAR_TEST_FILE	EICAR_TEST_FILE
ELF/Agent.DWS/tr	ELF/Agent.EA/tr.rkit	ELF/Scalper.C/worm
Emogen.T/tr	EPOC/Alarm.B/tr	EPOC/Alone.A/tr

(2) グレーウェア : [グレーウェア] タブをクリックすると以下の [グレーウェア] 確認画面が表示されます。

ウィルス一覧	
グレーウェア	
カテゴリ	有効
▶ Adware	<input type="checkbox"/>
▶ BHO	<input type="checkbox"/>
▶ Dial	<input type="checkbox"/>
▶ Download	<input type="checkbox"/>
▶ Game	<input type="checkbox"/>
▶ HackerTool	<input type="checkbox"/>
▶ Hijacker	<input type="checkbox"/>
▶ Joke	<input type="checkbox"/>
▶ Keylog	<input type="checkbox"/>
▶ Misc	<input type="checkbox"/>
▶ NMT	<input type="checkbox"/>
▶ P2P	<input type="checkbox"/>
▶ Plugin	<input type="checkbox"/>
▶ RAT	<input type="checkbox"/>
▶ Spy	<input type="checkbox"/>
▶ Toolbar	<input type="checkbox"/>

グレーウェアカテゴリを有効にすると、そのカテゴリ内にリストされているすべてのファイルがブロックされます。これらのカテゴリは、FortiGate が更新を受信したときに変更または拡張される可能性があります。



## 2-2-4. [侵入検知]の詳細機能説明

### ■ [シグネチャ]画面

[シグネチャ]は[閲覧・変更可]の権限となっております。

シグネチャ型の不正侵入設定が行えます。

(1) 定義済： [定義済]タブをクリックすると以下の[定義済]確認画面が表示されます。

 ボタンをクリックすると、[事前定義 IPS シグネチャの設定]画面が表示されます。

Name	Enable	Logging	Action	Severity	Location	Protocols	OS	Applications
2BGal.disp_album.php.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Server	TCP, HTTP	All	PHP_app
3CDaemon.FTP.Server.Information.Disclosure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Client	TCP, FTP	Windows	Other
3COM.OfficeConnect.DoS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop Session	Low	Server	TCP, HTTP	Other	Other
3COM.OfficeConnect.SoftReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop Session	Low	Server	TCP, HTTP	Other	Other
3ivx.MPEG4.MP4.File.Processor.Buffer.Overflow	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, HTTP	Windows	MediaPlayer
8Pixel.net.SimpleBlog.SQL.Injection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	TCP, HTTP	All	Other
AA.bot.Botlist.File.Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Server	TCP, HTTP	Windows	Other
Aardvark.TopSites.PHP.Arbitrary.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	TCP, HTTP	All	PHP_app
Aardvark.TopSites.PHP.Remote.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	TCP, HTTP	All	PHP_app
ABitWhizzy.ABitWhizzy.php.Directory.Traversal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Medium	Server	TCP, HTTP	All	PHP_app
Absolute.Image.Gallery.XE.XSS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Medium	Server	TCP, HTTP	Windows	Other
AbsoluteTelnet.Title.Bar.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, TELNET	Windows	Other
ACal.Arbitrary.Command.Execution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	TCP, HTTP	All	PHP_app
ACal.Calendar.Cookie.Based.Authentication.Bypass	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	TCP, HTTP	All	PHP_app
ACDSee.XPM.Values.Section.Buffer.Overflow	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	Client	TCP, HTTP	Windows	Other
ACDSee.XPMHeaders.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, HTTP	Windows	Other
Acoustica.Beatcraft.BcproJ.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, HTTP	Windows	Other
Acoustica.Mixcraft.MX4.Buffer.Overflow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, HTTP	Windows	Other
Acoustica.MP3.CD.Burner.ASX.Buffer.Overflow	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TCP, HTTP	Windows	Other

[事前定義 IPS シグネチャの設定]画面では、各シグネチャに対して、FortiGate IPS が攻撃を検出したときに実行するアクションを設定できます。

事前定義IPSシグネチャの設定

シグネチャ 2BGal.disp\_album.php.SQL.Injection

アクション

Packet Log

Severity

---

Exempt IP

Name	Source	Destination
<input type="text"/>	<input type="text"/>	<input type="text"/>

#	Name	Source	Destination

(2) カスタム： [カスタム]タブをクリックすると以下の[カスタムシグネチャリスト]確認画面が表示されます。

定義済 **カスタム** プロトコルデコーダ

View custom signatures with severity: <=

カスタムシグネチャ名	有効	ロギング	アクション	Severity

(3) プロトコルデコーダ : [プロトコルデコーダ] タブをクリックすると以下の [プロトコルデコーダ] 確認画面が表示されます。

 ボタンをクリックすると、[プロトコルデコーダ] 編集画面が表示されます。

Protocols		Ports	
Back Orifice	Auto		
DCE RPC	135, 1026		
DNS	53		
FTP	21		
H323	1720		
HTTP	Auto		
Instant Messaging	Auto		
IMAP	143		
LDAP	389		
MSSQL	1433		
NetBIOS	139, 445		
Peer-to-Peer	Auto		
POP3	110		
Protocol (L3/4) Analyser	Auto		
RADIUS	1812, 1813		
Sun RPC	111, 32771		
SIP	Auto		
SMTP	25		
SNMP	161, 162		
SSH	Auto		
SSL	Auto		
TCP Reassembler	Auto		
TFN DoS	Auto		

**Edit Protocol Decoder Parameter**

Group Name: DCE RPC  
 port\_list: 135, 1026

## ■ [アノーマリ] 画面

[アノーマリ] は [閲覧・変更可] の権限となっております。

アノーマリ型の不正侵入設定が行えます。 ボタンをクリックすると、[トラフィックアノーマリ] 編集画面が表示されます。

名前	有効	ロギング	アクション	Severity	
icmp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
icmp_flood	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
icmp_land	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Critical	
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	Critical	
ip_land	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	
ip_loose_src_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_security_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_stream_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_strict_src_record_route	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_timestamp_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	
ip_unkn_option	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Information	
large_icmp	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
ping_death	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
portscan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	Critical	
syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	Critical	
tcp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
tcp_land	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Critical	
tcp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	
udp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Critical	

**Edit Traffic Anomaly**

名前: icmp\_dst\_session  
 アクション: Pass  
 Severity: Critical

しきい値: 1000



## 2-2-5. [Web フィルタ] の詳細機能説明

### ■ [コンテンツブロック] 画面

**[コンテンツブロック] は [閲覧・変更可] の権限となっております。**

特定の単語またはパターンをブロックすることによって、Web コンテンツを制御できます。ただし、この設定をすることで、一般の方がこのファイアウォール配下のサーバーのコンテンツを、表示できなくなる場合があります。

(1) Web コンテンツブロック : [Web コンテンツブロック] タブをクリックすると以下の [Web コンテンツブロック] のリスト確認画面が表示されます。

[] ボタンをクリックすると、[Web コンテンツブロック] 画面が表示されます。

名前	# Entries	Profiles	コメント	
WEB C BLOCK1	1	web		

名前 WEB C BLOCK1  
コメント (最大半角63文字) OK

Pattern	パターンタイプ	言語	Score	
*BBS*	ワイルドカード	日本語	10	

さらに、 [] ボタンをクリックすると、[コンテンツブロックパターン] 編集画面が表示されます。

Edit Banned Pattern

Pattern \*BBS\*

パターンタイプ ワイルドカード

言語 日本語

Score 10

有効

OK キャンセル

(2) ブロック摘要除外 : [ブロック摘要除外] タブをクリックすると以下の [ブロック摘要除外] の確認画面が表示されます。

名前	# Entries	Profiles	コメント	
----	-----------	----------	------	--

## ■ [URL フィルタ] 画面

[URL フィルタ] は [閲覧・変更可] の権限となっております。

特定の URL へのアクセスを許可またはブロックするには、それらの URL を URL フィルタ リストに追加します。URL を許可またはブロックするには、テキストや正規表現（またはワイルドカード文字）を使用してパターンを追加します。FortiGate は、指定された任意の URL またはパターンに一致する Web ページを許可またはブロックし、代わりに差し替えメッセージを表示します。

 ボタンをクリックすると、[URL フィルタ] のリスト確認画面が表示されます。



名前	# Entries	Profiles	コメント
URL FILTER1	1	web	

名前: URL FILTER1  
コメント: (最大半角63文字) OK

URL	Action	Type
www.2ch.net	Block	Simple

さらに、 ボタンをクリックすると、[URL フィルタ] 編集画面が表示されます。



Edit URL Filter

URL: www.2ch.net  
Type: Simple  
Action: Block  
Enable:

OK キャンセル

## ■ [FortiGuard ウェブフィルタ] 画面

[FortiGuard ウェブフィルタ] は [閲覧・変更可] の権限となっております。

FortiGuard-Web により、Web サイトの許可、ブロック、監視を行います。

(1) 上書き設定 : [上書き設定] タブをクリックすると以下の [上書き設定] のリスト確認画面が表示されます。

あるポリシーによってブロックされている Web サイトへのアクセスがユーザに必要なことがあります。この場合、管理者はこのユーザに、ある一定の期間だけこのブロック機能を上書きさせることができます。



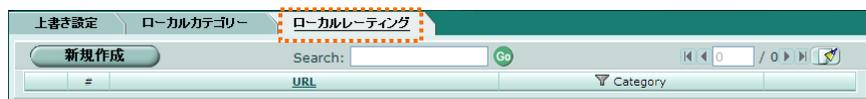
(2) ローカルカテゴリ : [ローカルカテゴリ] タブをクリックすると以下の [ローカルカテゴリ] のリスト確認画面が表示されます。

ユーザがプロファイル単位に URL のグループをブロックできるようにするために、ユーザ定義のカテゴリを作成できます。



(3) ローカルレーティング : [ローカルレーティング] タブをクリックすると以下の [ローカルレーティング] のリスト確認画面が表示されます。

ユーザは、ユーザ定義のカテゴリを作成した後、そのカテゴリに属すべき URL を指定できます。これにより、ユーザはプロファイル単位に、Web サイトのグループをまとめてブロックできるようになります。





## 2-2-6. [アンチスパム]の詳細機能説明

### ■ [禁止ワード]画面

**[禁止ワード]は[閲覧・変更可]の権限となっております。**

特定の単語またはパターンを含む電子メール メッセージをブロックすることによって、スパムを制御します。プロテクション プロファイルで有効になっている場合、FortiGate は、電子メール メッセージ内の単語またはパターンを検索します。一致が見つかったら、その単語に割り当てられた値が合計されていきます。ユーザ定義のしきい値を超えると、そのメッセージはスパムとしてマークされます。一致が見つからない場合、その電子メール メッセージは次のフィルタに渡されます。

ボタンをクリックすると、[禁止ワード]のリスト確認画面が表示されます。

名前	# Entries	Profiles	コメント
BLOCK WORD1	1	mail-pop	

さらに、 ボタンをクリックすると、[禁止ワード]編集画面が表示されます。

をクリックすると、新しい禁止ワードを追加することもできます。

[パターン]に禁止単語を入力します。

禁止単語は、1つの単語にすることも、最大 127 文字の語句にすることもできます。

[パターンタイプ]の[ワイルドカード]とは、[\*]や[?]で表現できる文字のことで、[正規表現]とは、[\*]や[?]以外に、[. ^ \$ [ ] + | ( )]の記号を使って、表現できる文字のことです。

[Score]とは、この禁止単語に適用される重み付けの数値で、登録した単語の出現回数によりカウントされます。

[Score]を超えると、スパムとしてマークされます。

## ■ [ブラック/ホワイトリスト] 画面

[ブラック/ホワイトリスト] は [閲覧・変更可] の権限となっております。

プロテクション プロファイルで有効になっている場合、FortiGate は、受信電子メールのフィルタ処理に IP アドレス リストと電子メール アドレス リストの両方を使用します。

IP アドレス リストのチェックを実行する場合、FortiGate は、メッセージの送信者の IP アドレスを IP アドレス リストに対して順番に比較します。一致が見つかった場合は、その IP アドレスに関連付けられたアクションが実行されます。一致が見つからない場合、そのメッセージは次の有効なスパム フィルタに渡されます。

- (1) IP アドレス : [IP アドレス] タブをクリックすると以下の [IP アドレス] のリスト確認画面が表示されます。[✎] ボタンをクリックすると、[IP アドレス] のリスト確認画面が表示されます。

名前	# Entries	Profiles	コメント
BWL IP1	1	mail-pop	

名前: BWL IP1  
コメント: (最大半角63文字) OK

<input checked="" type="checkbox"/>	IP/サブネットマスク	アクション	
<input checked="" type="checkbox"/>	124.47.76.192/29	Clear	✎

さらに、[✎] ボタンをクリックすると、[IP アドレスの編集] 画面が表示されます。

IPアドレスの編集

IP/サブネットマスク: 124.47.76.192/29  
アクション: Mark As Clear  
有効:

OK キャンセル

[新規作成] をクリックすると、IP アドレスを追加することもできます。

IPアドレスの追加

IP/サブネットマスク:   
アクション: Mark As Spam  
有効:

OK キャンセル

[IP/サブネットマスク] に IP アドレスまたは、IP アドレス/マスクのペアを入力します。

[アクション] では、スパムと判定するには [Mark as Spam] を、許可するには [Mark as Clear] を選択します。

[Mark as Reject] は SMTP のみの設定で、このセッションを破棄できます。

(2) E メールアドレス : [E メールアドレス] タブをクリックすると以下の [E メールアドレス] のリスト確認画面が表示されます。[✎] ボタンをクリックすると、[E メールアドレス] のリスト確認画面が表示されます。

さらに、[✎] ボタンをクリックすると、[E-mail アドレスの編集] 画面が表示されます。

[新規作成] をクリックすると、E-mail アドレスを追加することもできます。

[E-mail アドレス] に E-mail アドレスを入力します。この際、[パターンタイプ] から [ワイルドカード] が [正規表現] を設定して入力することができます。  
 例. [abcdefg.net のドメイン全て] の場合 → [\*@abcdefg.net] と入力

[アクション] では、スパムと判定するには [Mark as Spam] を、許可するには [Mark as Clear] を選択します。



## 2-2-7. [IM,P2P & VoIP] の詳細機能説明

### ■ [統計情報] 画面

[統計情報] は [閲覧のみ可] の権限となっております。

(1) サマリ : [サマリ] タブをクリックすると以下の [サマリ] 画面が表示されます。

IM、P2P、および VoIP 統計を表示すると、これらのプロトコルがネットワーク内でどのように使用されているかを調べることができます。

IM Usage		MSN	Yahoo!	AIM	ICQ	
<b>Users</b>						
Current Users		0	0	0	0	
Since Last Reset		0	0	0	0	
Blocked		0	0	0	0	
<b>Chat</b>						
Total Chat Sessions		0	0	0	0	
Total Messages		0	0	0	0	
<b>File Transfers</b>						
Since Last Reset		0	0	0	0	
Blocked		0	0	0	0	
<b>Voice Chat</b>						
Since Last Reset		0	0	0	0	
Blocked		0	0	0	0	
P2P Usage		BitTorrent	eDonkey	Gnutella	KaZaa	WinNY
<b>P2P Usage</b>						
Total Bytes		0.00 B	0.00 B	0.00 B	0.00 B	0.00 B
Average Bandwidth		0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s
VoIP Usage				SIP	SCCP	
<b>Sessions</b>						
Active Sessions (phones connected, etc)				0	0	
<b>Voice Calls</b>						
Total Calls (since last reset)				0	0	
Calls Failed/Dropped				0	0	
Calls Succeeded				0	0	

(2) プロトコル : [プロトコル] タブをクリックすると以下の [プロトコル] 画面が表示されます。

プロトコルタブでは、個別の IM プロトコルの詳細な統計が表示されます。

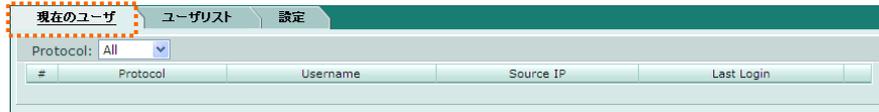
Usage Since: 2009-01-06 23:06:23	
<b>Users</b>	
Current Users	0
Since Last Reset	0
Blocked	0
<b>Chat</b>	
Total Chat Sessions	0
Server-based Chat	0
Group Chat	0
Direct/Private Chat	0
<b>Messages</b>	
Total Messages	0
Sent	0
Received	0
<b>File Transfers</b>	
Since Last Reset	0
Sent	0
Received	0
Blocked	0
<b>Voice Chat</b>	
Since Last Reset	0
Blocked	0

## ■ [ユーザ] 画面

[ユーザ] は [閲覧のみ可] の権限となっております。

(1) ユーザ : [ユーザ] タブをクリックすると以下の [ユーザ] 画面が表示されます。

FortiGate によって、現在接続されているユーザがリストに表示されます。



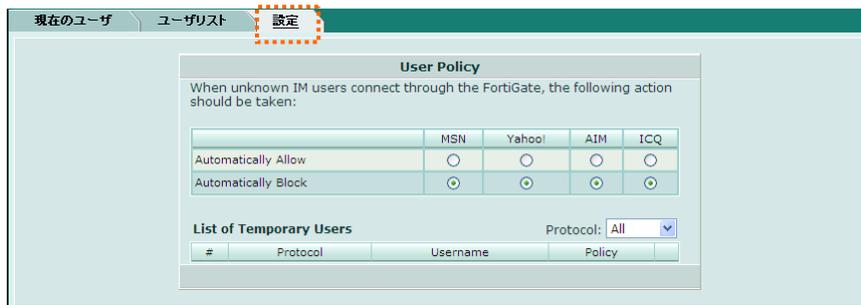
(2) ユーザリスト : [ユーザリスト] タブをクリックすると以下の [ユーザリスト] 画面が表示されます。

現在接続されているインスタント メッセージングユーザに関する情報が表示されます。



(3) 設定 : [設定] タブをクリックすると以下の [設定] 画面が表示されます。

不明なユーザに対して、IM プロトコルの一部またはすべての使用を許可してホワイト リストに追加するか、または IM プロトコルの一部またはすべての使用をブロックしてブラック リストに追加するか、のどちらかを実行できます。





## 2-2-8. [ログ & リポート]の詳細機能説明

### ■ [Log 環境設定] 画面

[Log 環境設定] は [閲覧のみ可] の権限となっております。

ネットワーク活動やトラフィックの記録環境を設定できます。

(1) ログ設定 : [ログ設定] タブをクリックすると以下の [ログ設定] 画面が表示されます。

(2) アラートEメール : [アラートEメール] タブをクリックすると以下の [アラートEメール] 画面が表示されます。

こちらの設定をご希望の場合は、カスタマーサポートまで設定内容をご指示ください。

(3) イベントログ : [イベントログ] タブをクリックすると以下の [イベントログ] 画面が表示されます。

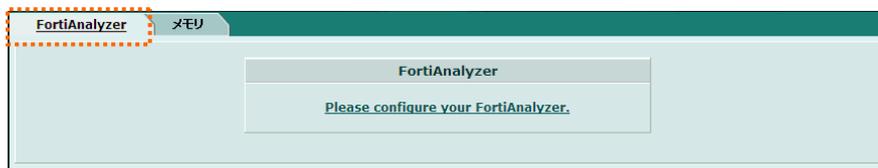


## ■ [ログアクセス] 画面

[ログアクセス] は [閲覧のみ可] の権限となっております。

各ログ情報の表示や保存、分析が行えます。

(1) FortiAnalyzer : [FortiAnalyzer] タブをクリックすると以下の [FortiAnalyzer] 画面が表示されますが、ここではご利用いただけません。



(2) メモリ : [メモリ] タブをクリックすると以下の [メモリ] の [イベント] リスト画面が表示されます。FortiGate のメモリバッファ内のログメッセージが表示されます。

#	Date	Time	Level	User Interface	Action	Message
1	2009-02-04	02:35:10	notice			Fortigate scheduled update virdb(9.997) idsdb(2.592) aven(3.010) idsen(1.09)
2	2009-02-04	01:35:11	notice			Fortigate scheduled update virdb(9.997) idsdb(2.592) aven(3.010) idsen(1.09)
3	2009-02-04	00:35:26	notice			Fortigate scheduled update virdb(9.997) idsdb(2.592) aven(3.010) idsen(1.09)
4	2009-02-03	23:35:08	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
5	2009-02-03	22:35:08	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
6	2009-02-03	21:35:09	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
7	2009-02-03	20:35:17	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
8	2009-02-03	19:35:10	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
9	2009-02-03	18:35:10	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
10	2009-02-03	17:35:47	critical			The system exited system conserve mode
11	2009-02-03	17:35:47	notice			Fortigate scheduled update virdb(9.996) idsdb(2.592) aven(3.010) idsen(1.09)
12	2009-02-03	17:35:42	critical			The system has entered system conserve mode
13	2009-02-03	16:35:15	notice			Fortigate scheduled update virdb(9.996) idsdb(2.591) aven(3.010) idsen(1.09)
14	2009-02-03	15:35:08	notice			Fortigate scheduled update virdb(9.996) idsdb(2.591) aven(3.010) idsen(1.09)
15	2009-02-03	14:35:28	notice			Fortigate scheduled update virdb(9.996) idsdb(2.591) aven(3.010) idsen(1.09)
16	2009-02-03	13:35:11	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
17	2009-02-03	12:35:11	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
18	2009-02-03	11:35:12	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
19	2009-02-03	10:35:07	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
20	2009-02-03	09:35:07	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
21	2009-02-03	08:35:28	notice			Fortigate scheduled update virdb(9.995) idsdb(2.591) aven(3.010) idsen(1.09)
22	2009-02-03	07:35:10	notice			Fortigate scheduled update virdb(9.994) idsdb(2.591) aven(3.010) idsen(1.09)
23	2009-02-03	06:35:10	notice			Fortigate scheduled update virdb(9.994) idsdb(2.591) aven(3.010) idsen(1.09)
24	2009-02-03	05:35:11	notice			Fortigate scheduled update virdb(9.994) idsdb(2.591) aven(3.010) idsen(1.09)
25	2009-02-03	04:35:11	notice			Fortigate scheduled update virdb(9.994) idsdb(2.591) aven(3.010) idsen(1.09)

さらに、[Log Type] リストからログの種類を選択できます。

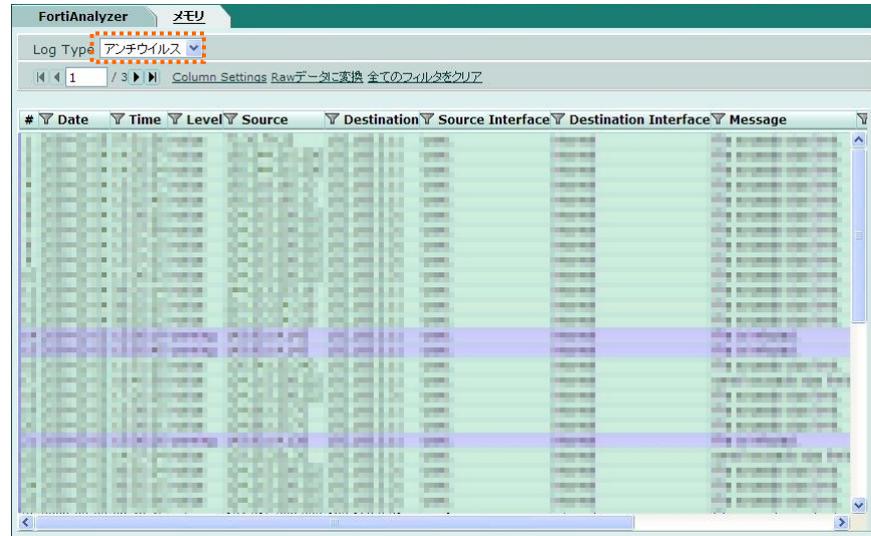
以下の画面は [アタック] リストです。



The screenshot shows the FortiAnalyzer interface with the 'Log Type' dropdown menu set to 'アタック' (Attack). The table below shows the column headers for this log type.

#	Date	Time	Level	Source	Destination	Message	Reference
エントリは見つかりませんでした。							

以下の画面は [アンチウイルス] リストです。



The screenshot shows the FortiAnalyzer interface with the 'Log Type' dropdown menu set to 'アンチウイルス' (Anti-Virus). The table below shows the column headers for this log type.

#	Date	Time	Level	Source	Destination	Source Interface	Destination Interface	Message
1	2018-08-08	10:00:00	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
2	2018-08-08	10:00:01	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
3	2018-08-08	10:00:02	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
4	2018-08-08	10:00:03	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
5	2018-08-08	10:00:04	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
6	2018-08-08	10:00:05	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
7	2018-08-08	10:00:06	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
8	2018-08-08	10:00:07	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
9	2018-08-08	10:00:08	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]
10	2018-08-08	10:00:09	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	File blocked: [redacted]

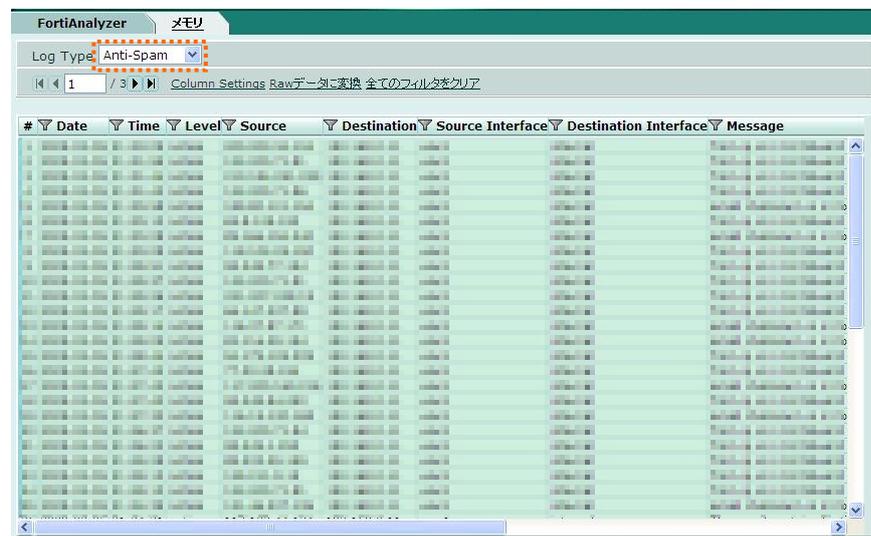
以下の画面は [ウェブフィルタ] リストです。



The screenshot shows the FortiAnalyzer interface with the 'Log Type' dropdown menu set to 'ウェブフィルタ' (Web Filter). The table below shows the column headers for this log type.

#	Date	Time	Level	Source Port	Source	Destination	Hostname	URL	Message
1	2018-08-08	10:00:00	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
2	2018-08-08	10:00:01	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
3	2018-08-08	10:00:02	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
4	2018-08-08	10:00:03	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
5	2018-08-08	10:00:04	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
6	2018-08-08	10:00:05	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
7	2018-08-08	10:00:06	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
8	2018-08-08	10:00:07	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
9	2018-08-08	10:00:08	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]
10	2018-08-08	10:00:09	Warning	80	192.168.1.100	192.168.1.1	www.example.com	http://www.example.com/	Blocked: [redacted]

以下の画面は [Anti-Spam] リストです。



The screenshot shows the FortiAnalyzer interface with the 'Log Type' dropdown menu set to 'Anti-Spam'. The table below shows the column headers for this log type.

#	Date	Time	Level	Source	Destination	Source Interface	Destination Interface	Message
1	2018-08-08	10:00:00	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
2	2018-08-08	10:00:01	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
3	2018-08-08	10:00:02	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
4	2018-08-08	10:00:03	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
5	2018-08-08	10:00:04	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
6	2018-08-08	10:00:05	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
7	2018-08-08	10:00:06	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
8	2018-08-08	10:00:07	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
9	2018-08-08	10:00:08	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]
10	2018-08-08	10:00:09	Warning	192.168.1.100	192.168.1.1	eth0/1	eth0/1	Spam detected: [redacted]

以下の画面は [IM/P2P] リストです。



以下の画面は [VoIP] リストです。



■ [コンテンツアーカイブ] 画面

[コンテンツアーカイブ] はすべてご利用いただけません。



■ [レポート設定] 画面

[レポート設定] はご利用いただけません。



## ■ [リモートアクセス] 画面

[リモートアクセス] は [閲覧のみ可] の権限となっております。

帯域と流量がグラフで確認できます。

(1) FortiAnalyzer : [FortiAnalyzer] タブをクリックすると以下の [FortiAnalyzer] 画面が表示されますが、ここではご利用いただけません。



(2) メモリ : [メモリ] タブをクリックすると以下の [メモリ] のグラフ画面が表示されます。

帯域と流量がグラフで確認できます。右の各項目のチェックを入れ替えると、グラフも変化します。

