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

第１章　はじめにお読みください 3

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 4

１－２.【アクセス制限実施・解除申請書】ご返送のお願い 5

第２章　FortiGate WEB CONFIG の機能 6

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. [ファイアーウォール] の詳細機能説明 17

２－２－３. [アンチウィルス] 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＆リポート] 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、ファイアー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.【ファイアー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.【ファイアーウォール　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

【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

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。

■アカウント設定情報

ファイアーウォールアドレス	
ユーザー名	
パスワード	

■ご注意
・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;:/.,@!"#$%&()

■お問い合わせ先
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
〒710-0845 岡山県倉敷市西富井636-30
URL: http://www.chiroro.co.jp/

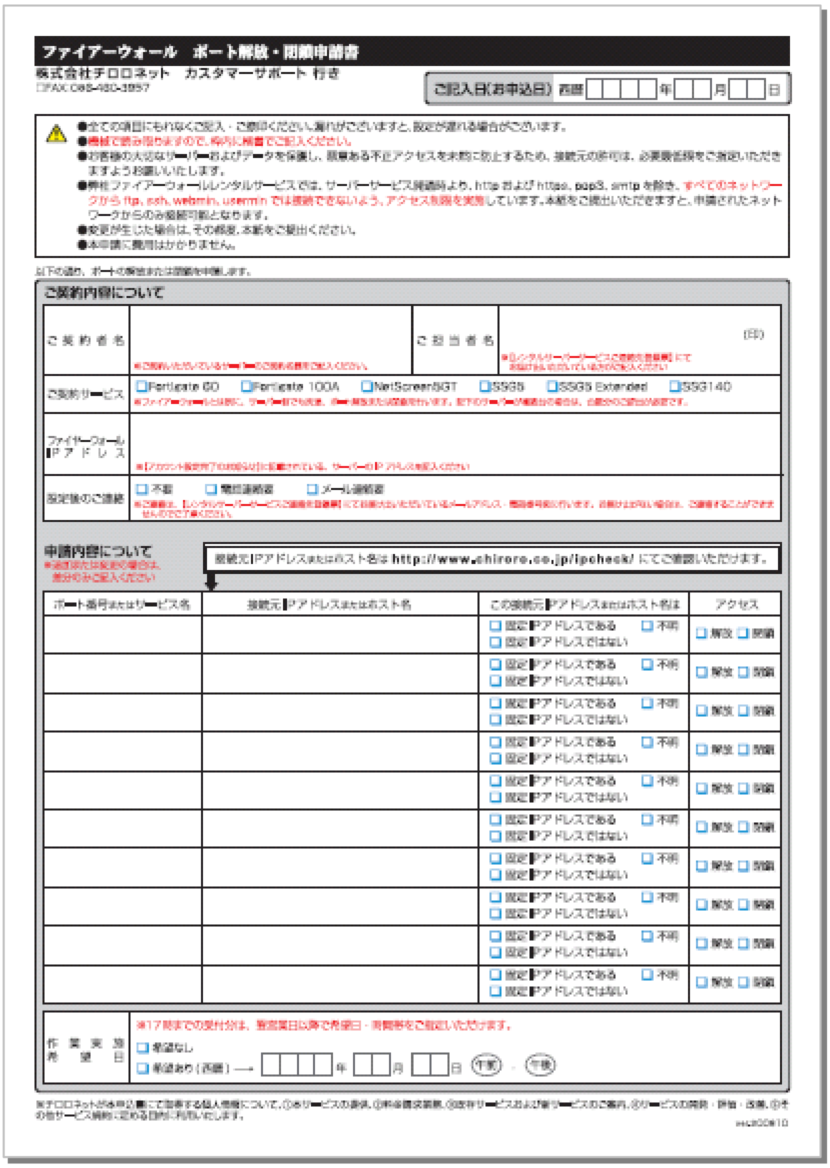
ISO 27001:2005準拠フォーマット(FWコンソール設定完了0902版)

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。

1－2.【ファイアーウォール　ポート解放・閉鎖申請書】ご返送のお願い

ファイアーウォールオプションサービスでは、悪意ある不正アクセスを未然に防止するため、サービス開通時は、**すべてのネットワークから WEB CONFIG による接続ができないよう、アクセス制限を実施**しております。そのため、お客様のご利用環境にあわせ、必要最低限の範囲から接続できるよう、接続元の許可申請をお願いいたします。ファイアーウォールのアクセス許可は最大 3 件までとさせていただいております。（1 件でネットワークアドレス＋マスクで、複数の範囲は 1 件とさせていただきます。）

また、接続元が不要になった場合・追加になった場合は、都度、本紙をご提出ください。本紙をご提出いただかず、お客様にて接続制限等の設定ファイルを書き換えられた場合は、弊社からも接続できなくなり、サポートをご提供できなくなる恐れがありますのでご注意ください。



本紙は、弊社ホームページ（http://www.chiroro.co.jp/）よりダウンロードいただけます。

第2章　FortiGate WEB CONFIG の機能

この章では、FotiGate 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. [ファイアーウォール] の詳細機能説明
２－２－３. [アンチウィルス] 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＆リポート] 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

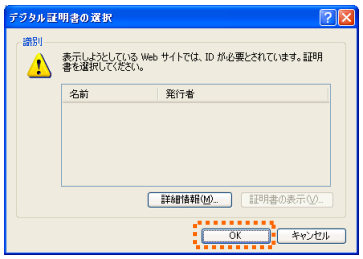
お手元に、【ファイアーウォール用アカウント設定完了のお知らせ】をご用意ください。

① ブラウザ（Internet Explorer、Safari、FireFox 等）を起動します。

② アドレス欄に、【ファイアー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、『ファイアーウォールアドレス』を入力し、Enter キーを押します。

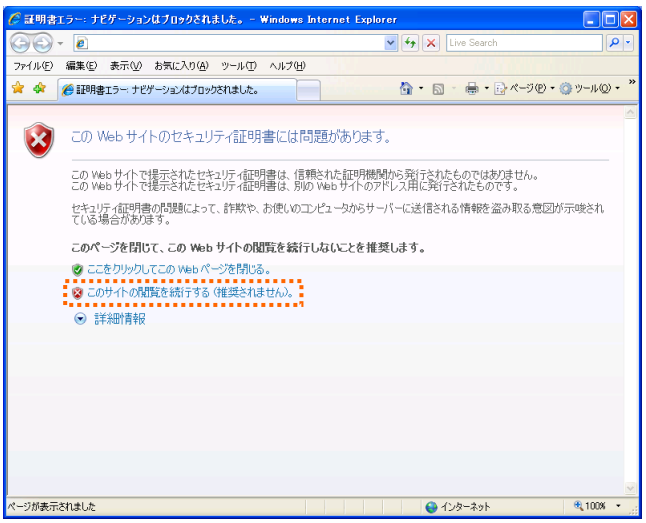
ファイアーウォールアドレス	例）https:// 211.125.117.250/

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。

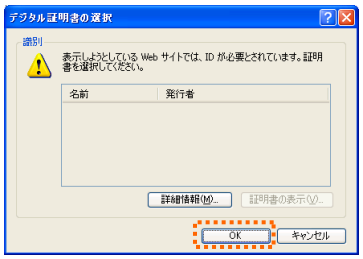


④ 次に、［このサイトの閲覧を続行する（推奨されません。）］をクリックします。

※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。



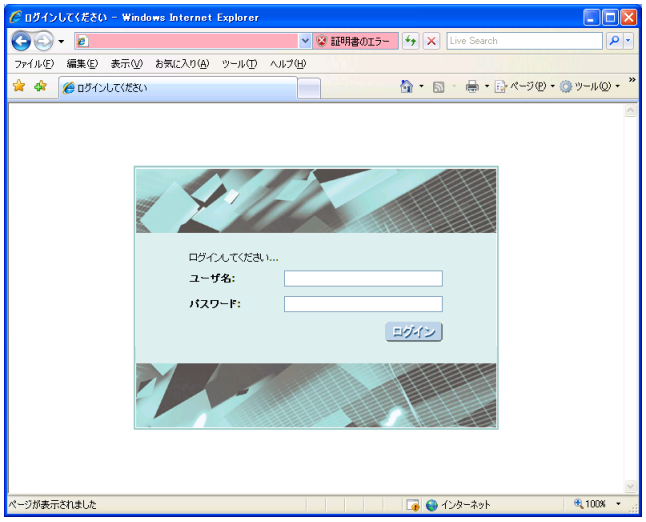
⑤ 再び、右のような画面が表示されますので、［OK］ボタンをクリックします。



⑥ 右のような画面が表示されますので、【ファイアー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。

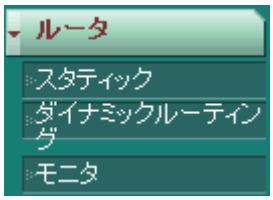
⚠ ✓ 30分間何も操作しないと、自動的にログアウトされます。

■ 各メニュー説明

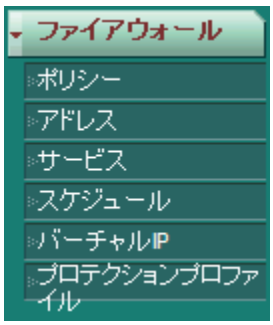
各機能の設定の権限を以下の 3 種類とさせていただいております。

×	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

	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。

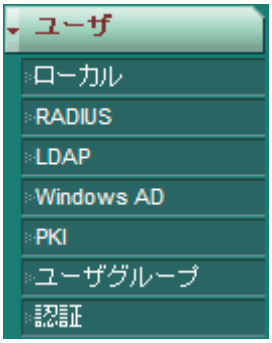


スタティック	×	パケットの宛先IP アドレスとネットマスクを定義し設定します。
ダイナミックルーティング	×	ネットワーク設定として、FortiGate インタフェースと DNS の設定を行います。
モニタ	×	DHCP を用いてクライアントのネットワーク構成を自動で行います。

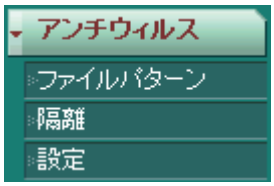


ポリシー	△	FortiGate を通過するすべてのトラフィックを制御します。
アドレス	△	ファイアーウォール アドレスを追加、編集、および削除します。
サービス	△	ファイアーウォールで許可または拒否する通信の種類を決定します。
スケジュール	△	ポリシーがアクティブまたは非アクティブになる時期を制御できます。
バーチャルIP	△	FortiGat を介した接続が可能になります。
プロテクションプロファイル	○	特定の目的に合わせて調整可能な設定のグループです。

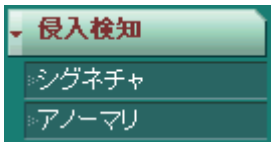
IPSEC	×	IPSEC暗号化通信によるVPNの設定を行います。
PPTP	×	PPTP 暗号化通信による VPN の設定を行います。
SSL	×	SSL 暗号化通信による VPN の設定を行います。
証明書	×	CAルート証明書、証明書失効リストのインポート、バックアップと復元。



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。

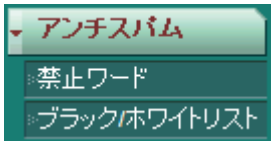


	権限	内容
ファイルパターン	○	ウイルスのファイルパターンを設定します。
隔離	○	ブロックされたファイルや感染したファイルの隔離設定を行います。
設定	○	ウイルス定義の一覧リストとグレーウェアリストが確認できます。

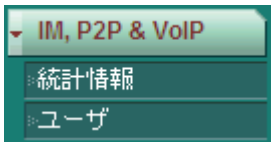


シグネチャ	○	シグネチャ型の不正侵入設定を行います。
アノーマリ	○	アノーマリ型の不正侵入設定を行います。

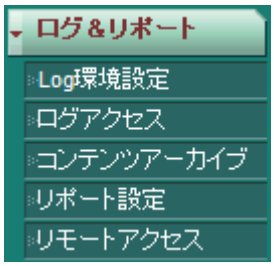
コンテンツブロック	○	特定の単語やパターンをブロックすることによりWebコンテンツを制御します。
URLフィルタ	○	特定 URL へのアクセスの許可やブロックを制御します。
FortiGuard - ウェブフィルタ	○	FortiGuard-Webにより、Webサイトの許可、ブロック、監視を行います。



禁止ワード	○	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。
ブラック/ホワイトリスト	○	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。



統計情報	△	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。
ユーザ	△	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。

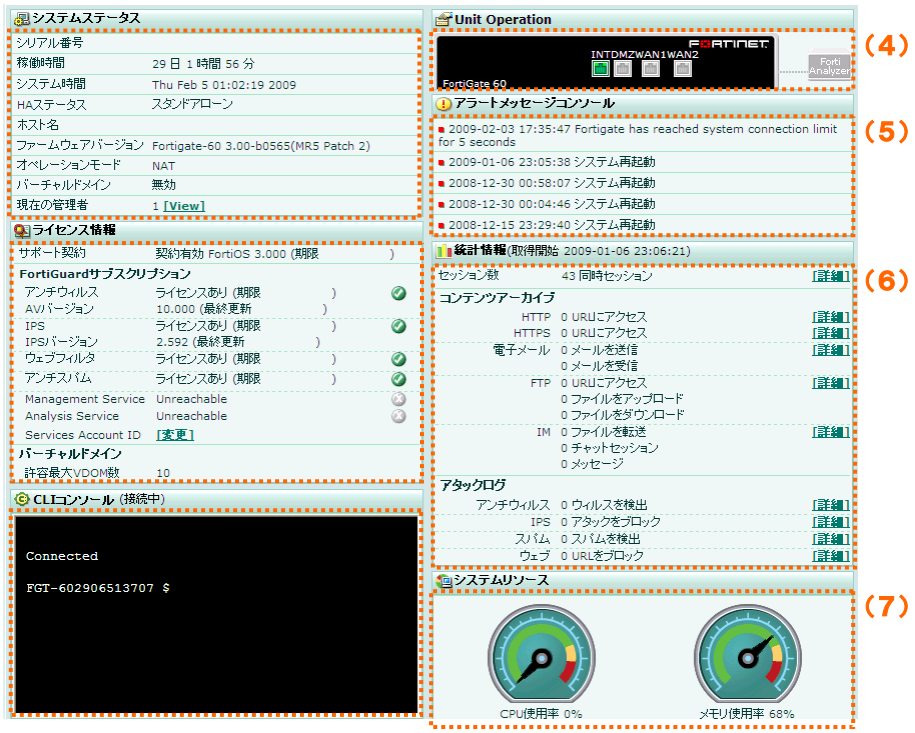


Log環境設定	△	ネットワーク活動やトラフィックの記録環境を設定できます。
ログアクセス	△	各ログ情報の表示や保存、分析が行えます。
コンテンツアーカイブ	△	アーカイブされたログを表示することができます。
リポート設定	△	FortiAnalyzer レポートの設定、表示、印刷を行うことができます。
リモートアクセス	△	帯域と流量がグラフで確認できます。

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 [閲覧のみ可] の権限となっております。



（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　：　アンチウィルス、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、アンチウィ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。

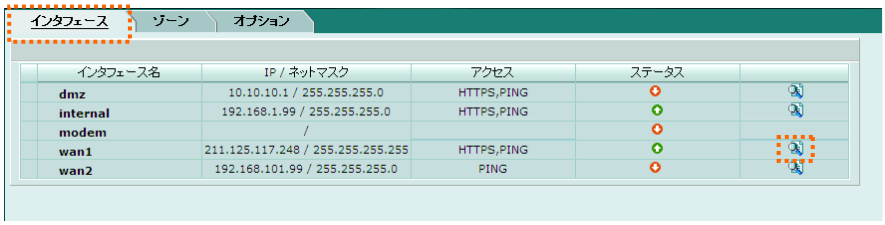
（６）統計情報　：　ネットワークトラフィックや保護に関して、FortiGate での状況の確認ができます。

（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

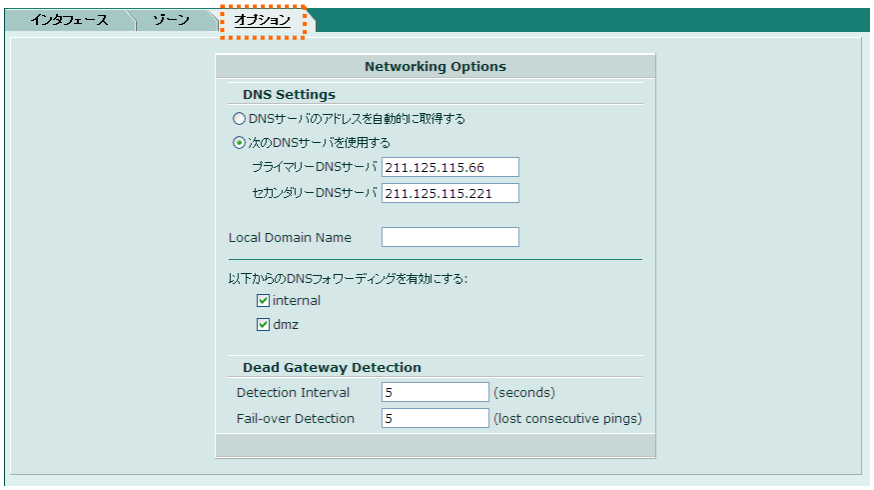
［ネットワーク］は［閲覧のみ可］の権限となっております。

（１）インタフェース ： ［インタフェース］タブから［ ］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。



（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。

（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。

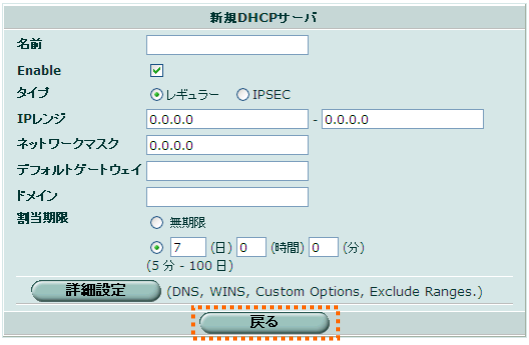


■ [DHCP] 画面

[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。



（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。

■ [設定] 画面

[設定] は [閲覧のみ可] の権限となっております。

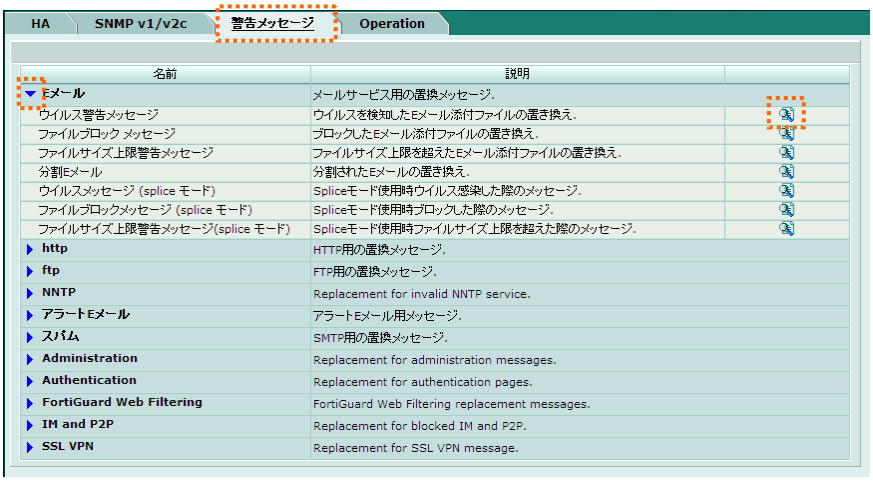
（1） HA ： [HA] タブをクリックすると以下の [HA] 設定画面が表示されます。

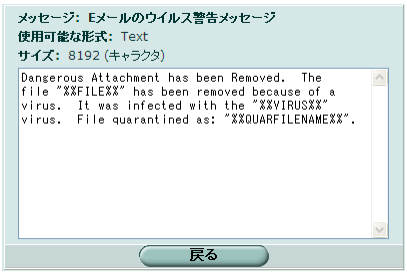
[HA] とは、高い可用性を持つコンピュータシステムのことで、稼働率が高いほど高可用性であると言えます。一般的に稼働率を高めるためには、クラスタリングや多重化、自動バックアップ、ホットスワップなどの技術を用います。

ここでは、この機能はご利用いただけません。

（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。

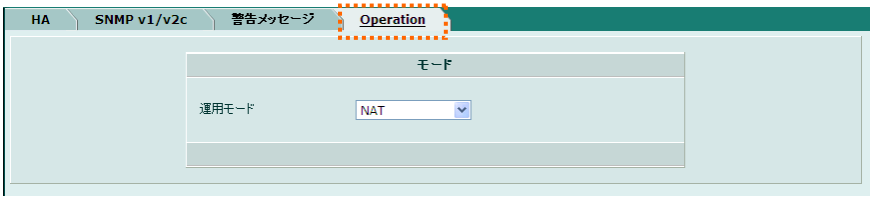
（3）警告メッセージ ： ［警告メッセージ］タブをクリックすると以下の［警告メッセージ］確認画面が表示されます。［▼］ボタンをクリックすると、項目の内容が展開でき、さらに、［ ］ボタンをクリックすると、［警告の際のメッセージ］が表示されます。





例えば、電子メールにウィ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。

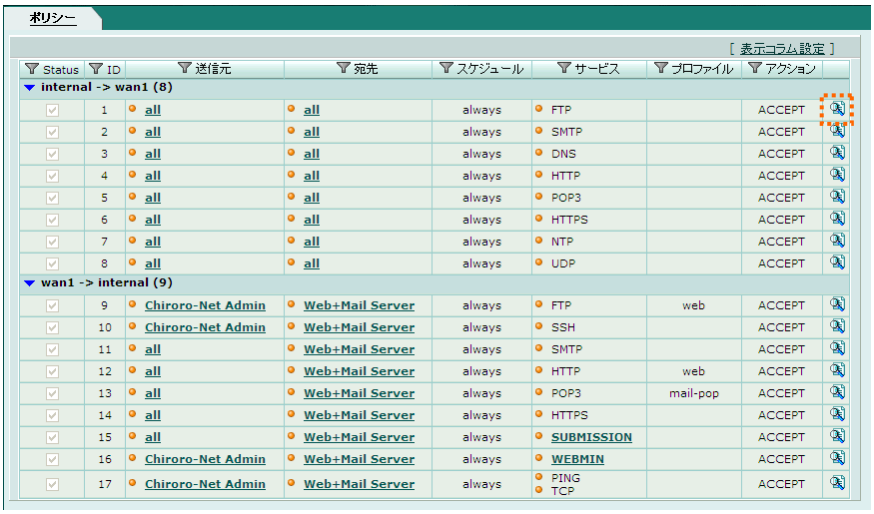


2－2－2. [ファイアーウォール] の詳細機能説明

■ [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。

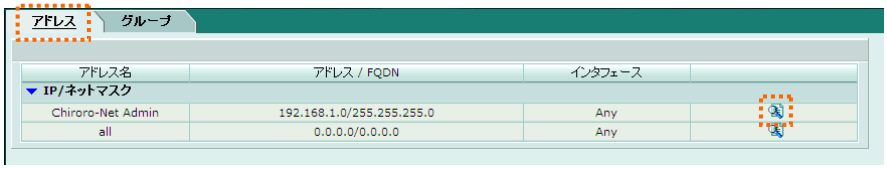


■ [アドレス] 画面

[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。



（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。

■ [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。

（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。

（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。

■ [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。

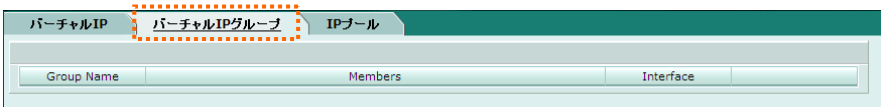
（2）繰返し ： [繰返し] タブをクリックすると以下の [繰返し（反復）スケジュール] 確認画面が表示されます。[ ] ボタンをクリックすると、[スケジュールを編集] 画面が表示されます。

■ [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。[ ] 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。

（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、ファイアーウォール 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。

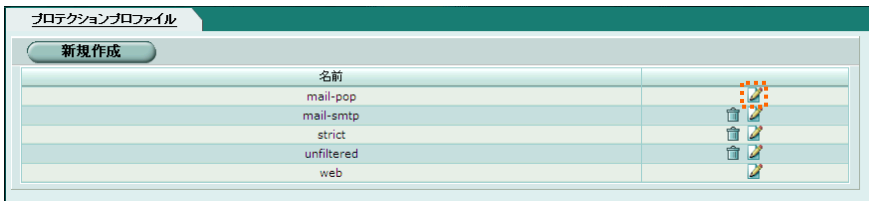


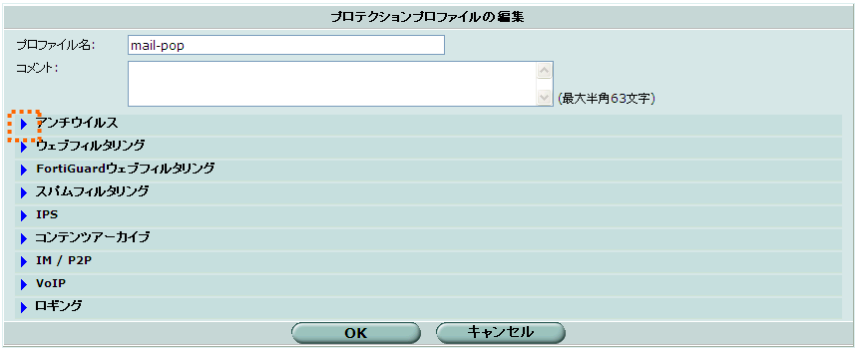
（3）IP プール ： [IP プール] タブをクリックすると以下の [IP プール] 確認画面が表示されます。

■ ［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ー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。

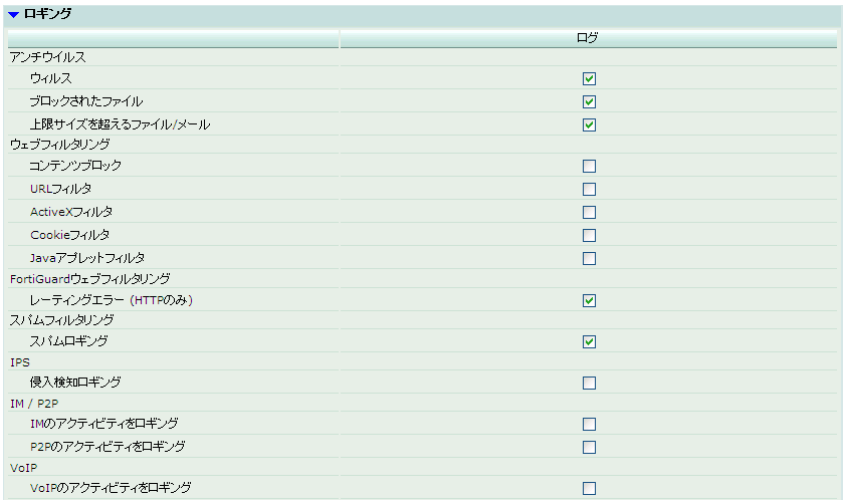




さらに、［ ］ボタンをクリックすると、項目の内容が展開でき、プロファイルの設定が行えます。以下は［mail-pop］のプロファイル設定例です。

・ **アンチウィルス** ：POP3 の必要な箇所にチェックを入れます。

- スパムフィルタリング ：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。



- ロギング ： ここでは、POP のログを設定したいので、[ウィルス] [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。

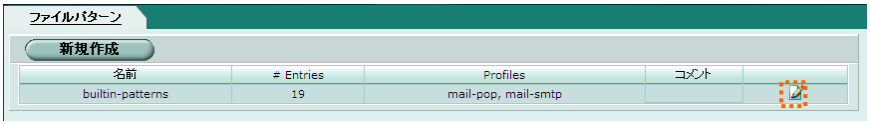
2－2－3. [アンチウィルス] の詳細機能説明

■ [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。

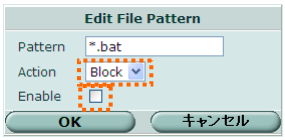
脅威である可能性のあるすべてのファイルをブロックし、アクティブなコンピュータ ウィルス攻撃を阻止するためのファイルパターンを設定できます。



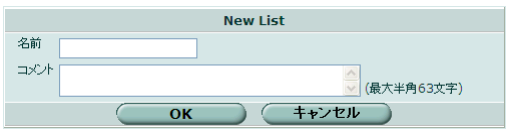
さらに、[ ] ボタンをクリックすると、[ファイルパターン編集] 確認画面が表示されます。

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。



[新規作成] 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?] と入力

※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"
a|b	"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。

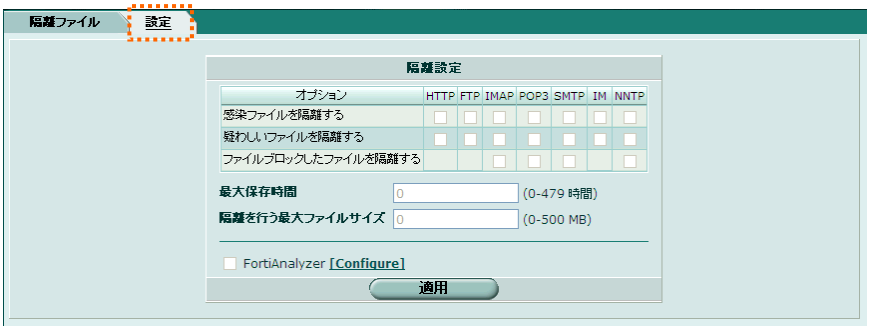
■ [隔離] 画面

[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。

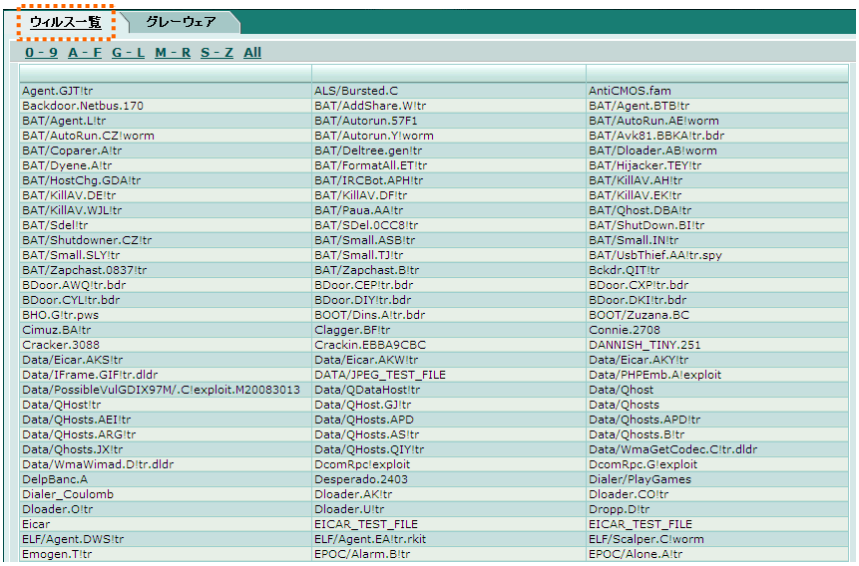
（2）設定 ： [設定] タブをクリックすると以下の [隔離設定] 確認画面が表示されます。



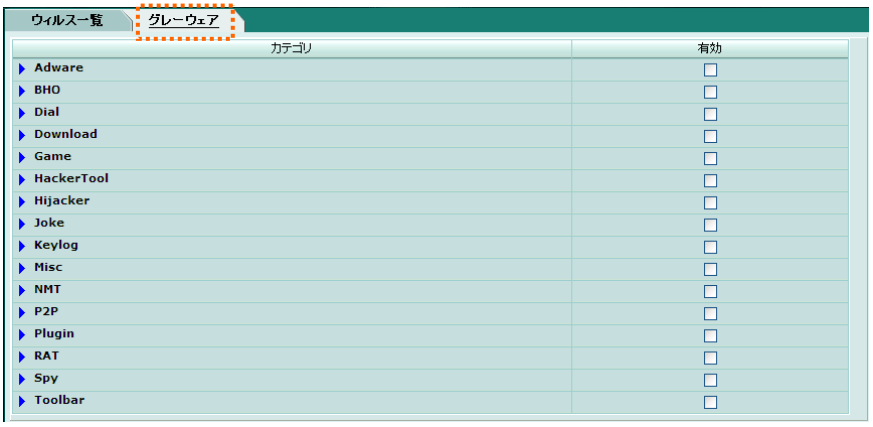
■ [アンチウィルス設定] 画面

[アンチウィルス設定] 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。



（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。



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。

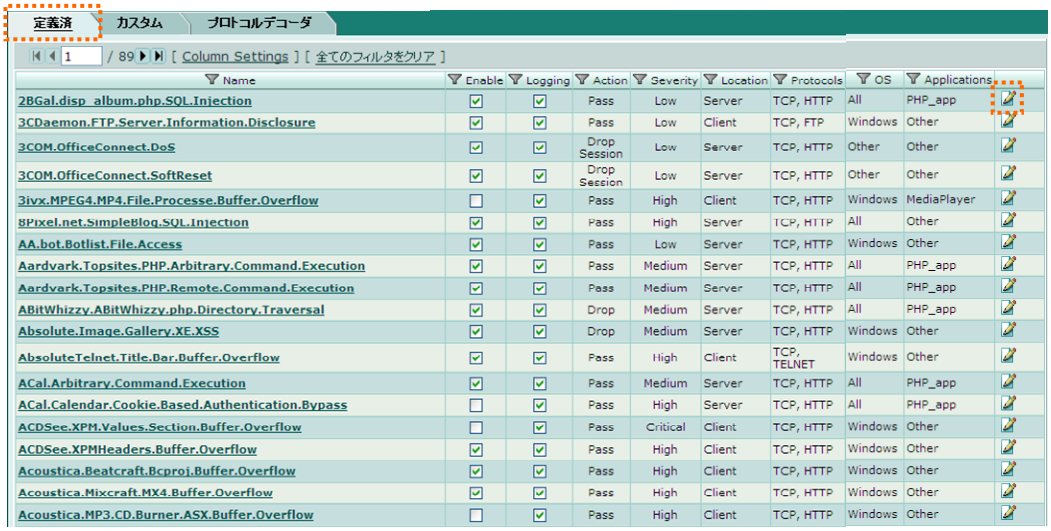
2－2－4. [侵入検知] の詳細機能説明

■ [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。

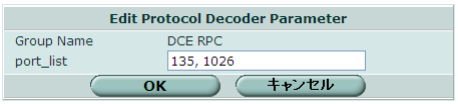


[事前定義 IPS シグネチャの設定] 画面では、各シグネチャに対して、FortiGate IPS が攻撃を検出したときに実行するアクションを設定できます。

（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。

（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。

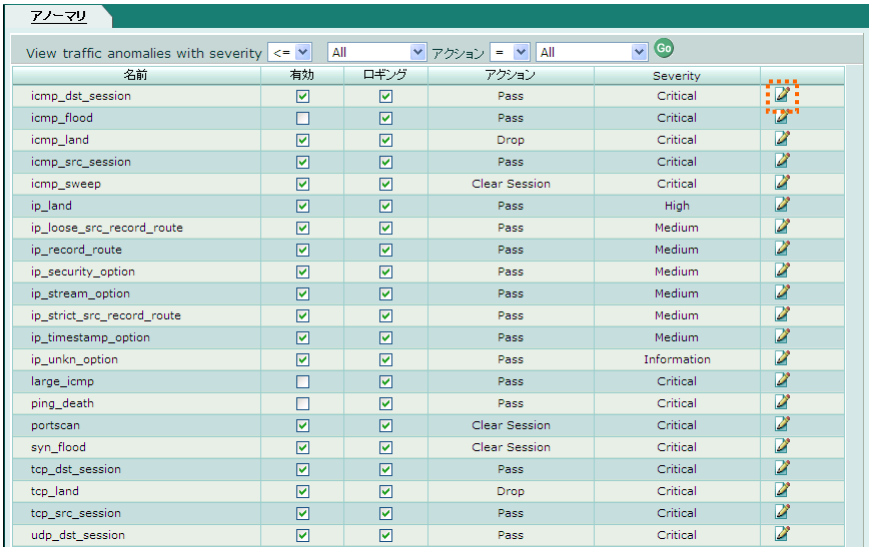
[ ] ボタンをクリックすると、[プロトコルデコーダ] 編集画面が表示されます。

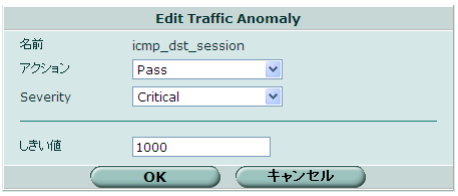


■ [アノーマリ] 画面

[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。





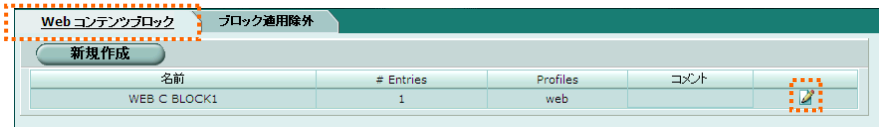
２－２－５．[Web フィルタ] の詳細機能説明

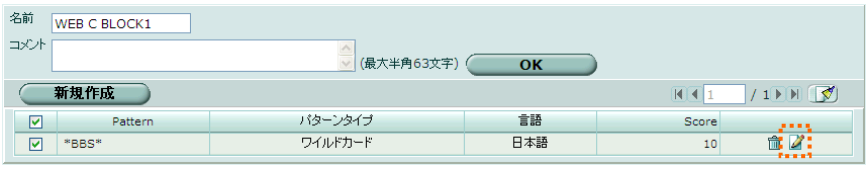
■ [コンテンツブロック] 画面

[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ー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。

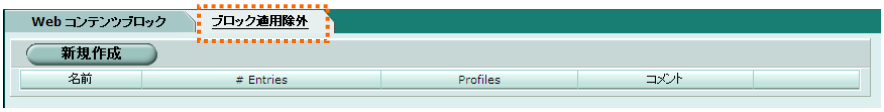
（１）Web コンテンツブロック ： [Web コンテンツブロック] タブをクリックすると以下の [Web コンテンツブロック] のリスト確認画面が表示されます。
[ ] ボタンをクリックすると、[Web コンテンツブロック] 画面が表示されます。





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。

（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。



■ [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。

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。

■ [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になることがあります。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）ローカルカテゴリー ： [ローカルカテゴリー] タブをクリックすると以下の [ローカルカテゴリー] 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

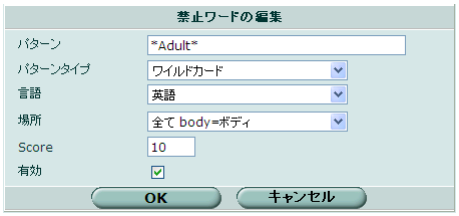
■ [禁止ワード] 画面

[禁止ワード] は [閲覧・変更可] の権限となっております。

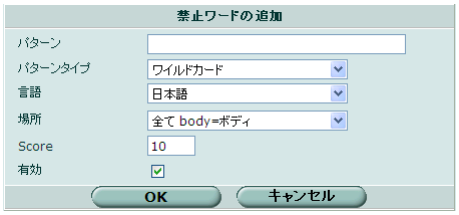
特定の単語またはパターンを含む電子メール メッセージをブロックすることによって、スパムを制御します。プロテクション プロファイルで有効になっている場合、FortiGate は、電子メール メッセージ内の単語またはパターンを検索します。一致が見つかると、その単語に割り当てられた値が合計されていきます。ユーザ定義のしきい値を超えると、そのメッセージはスパムとしてマークされます。一致が見つからない場合、その電子メール メッセージは次のフィルタに渡されます。

[ ] 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。

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。



[新規作成] 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。

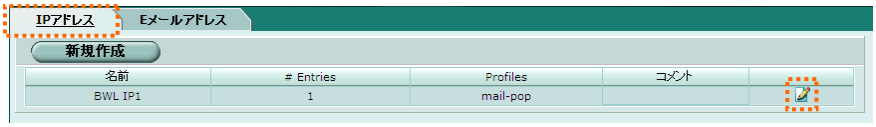
■ [ブラック/ホワイトリスト] 画面

[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。

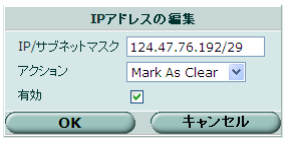
プロテクション プロファイルで有効になっている場合、FortiGate は、受信電子メールのフィルタ処理に IP アドレス リストと電子メール アドレス リストの両方を使用します。

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。



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。

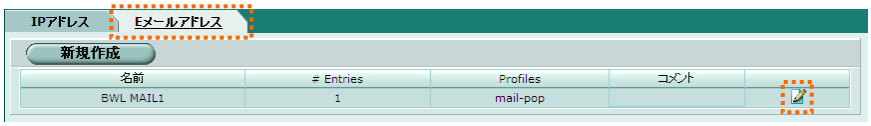


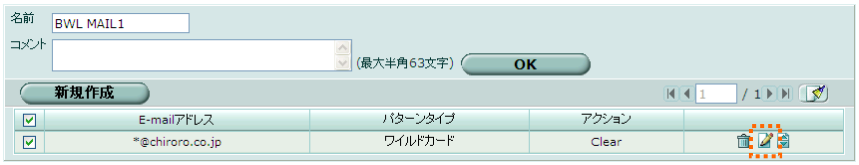
[新規作成] をクリックすると、IP アドレスを追加することもできます。

[IP/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] か [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

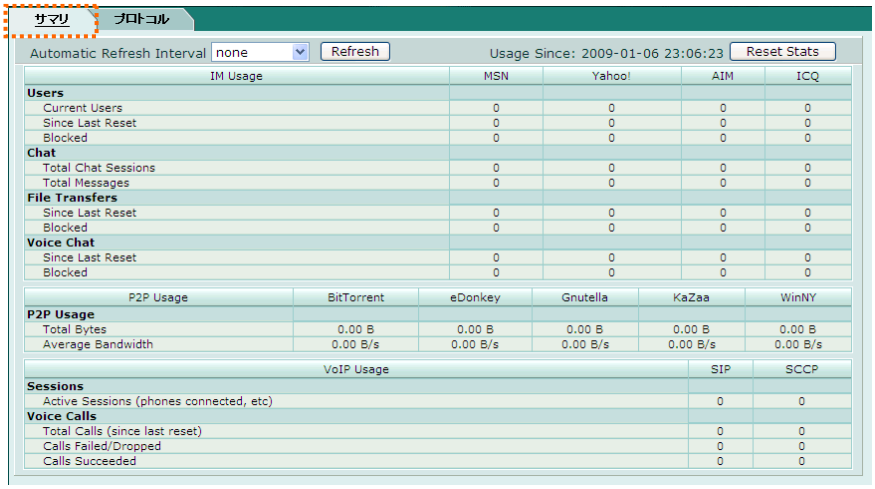
[アクション] では、スパムと判定するには [Mark as Spam] を、許可するには [Mark as Clear] を選択します。

2－2－7. [IM,P2P & VoIP] の詳細機能説明

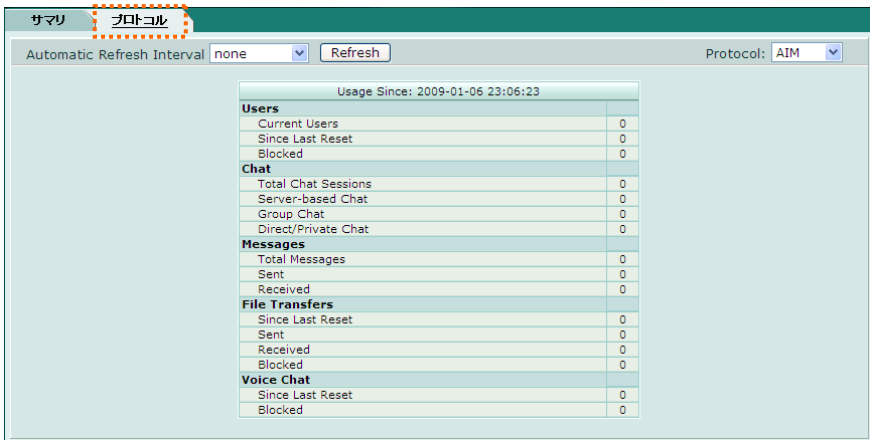
■ [統計情報] 画面

[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。



（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。

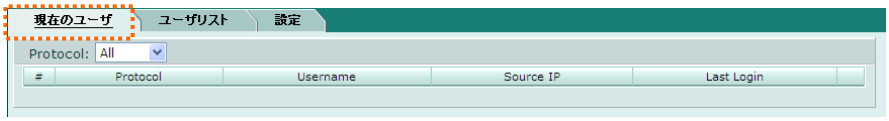


■ ［ユーザ］画面

［ユーザ］は［閲覧のみ可］の権限となっております。

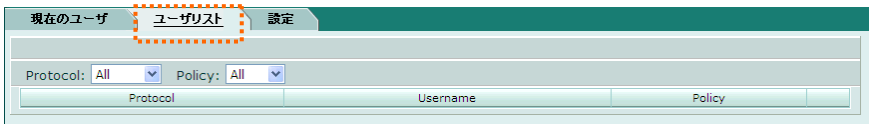
（１）ユーザ　：　［ユーザ］タブをクリックすると以下の［ユーザ］画面が表示されます。

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。



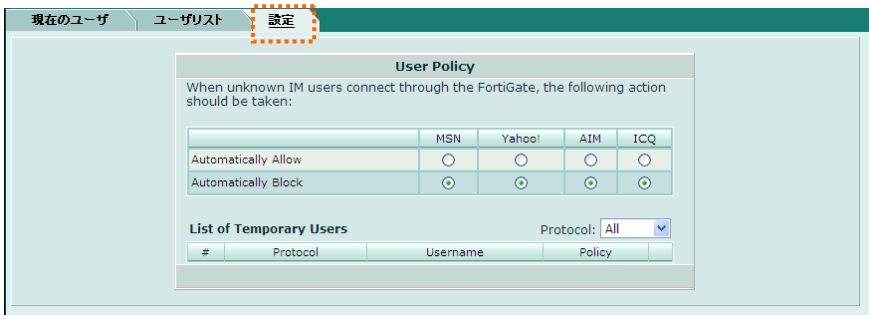
（２）ユーザリスト　：　［ユーザリスト］タブをクリックすると以下の［ユーザリスト］画面が表示されます。

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

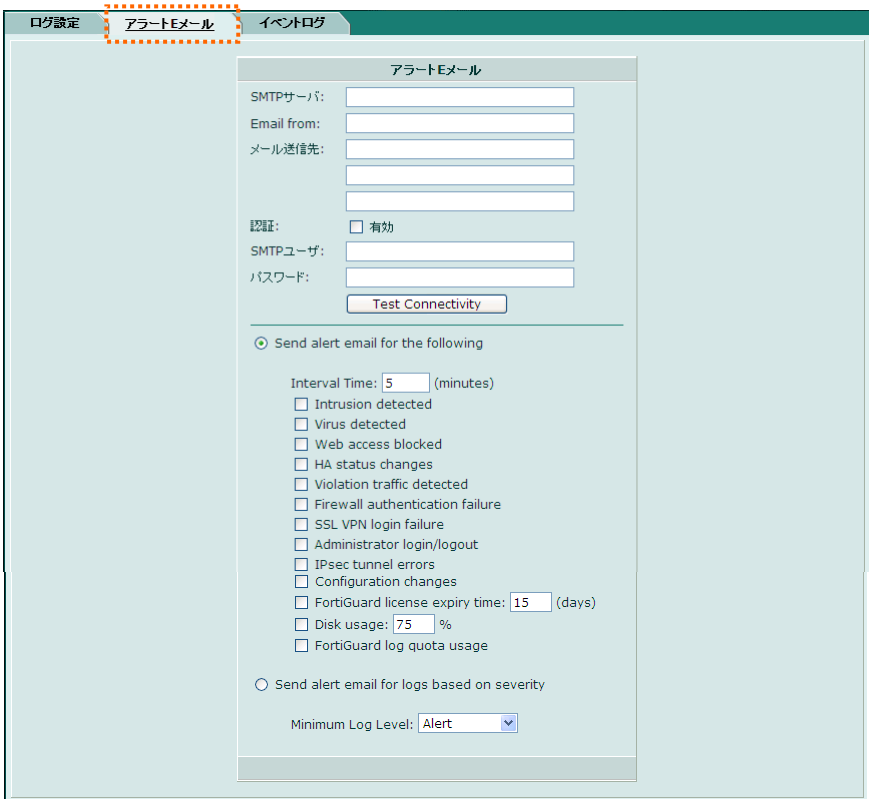
■ [Log 環境設定] 画面

[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。

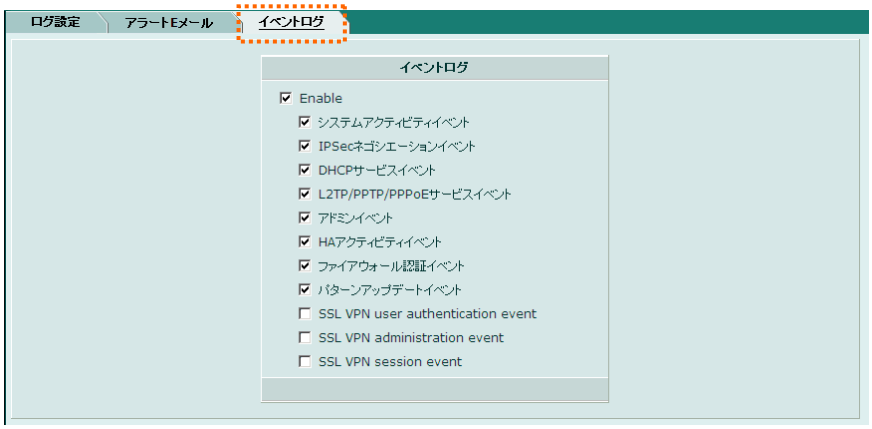
（1）ログ設定 ： [ログ設定] タブをクリックすると以下の [ログ設定] 画面が表示されます。

（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。

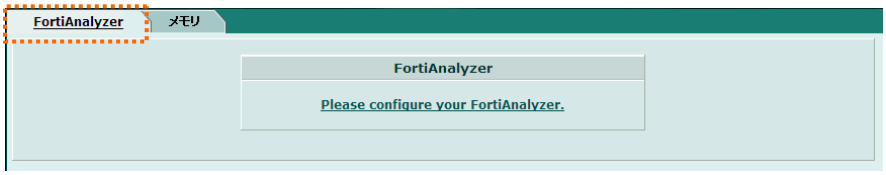


■ [ログアクセス] 画面

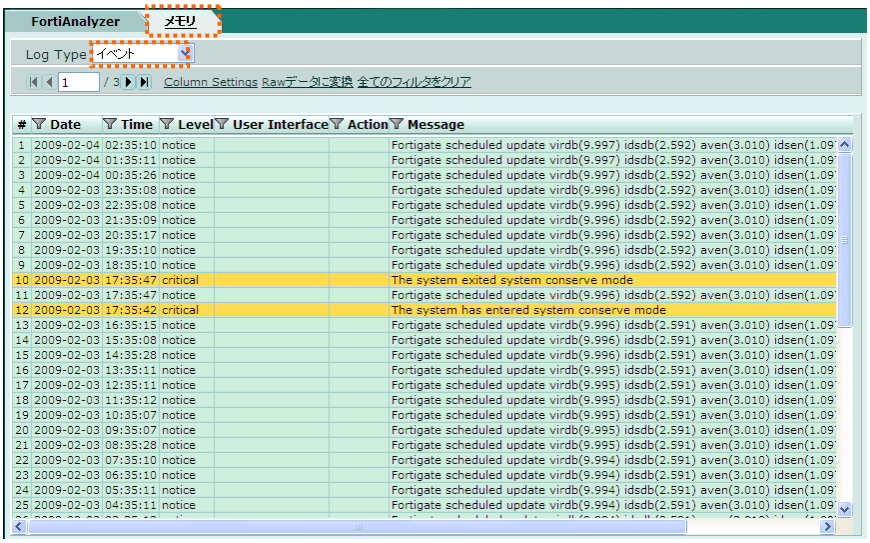
[ログアクセス] は [閲覧のみ可] の権限となっております。

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。



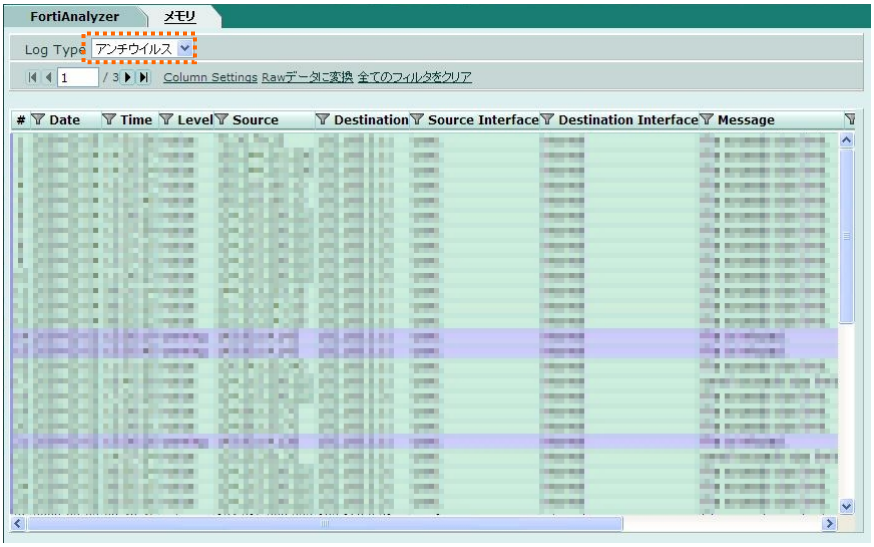
（2）メモリ ： [メモリ] タブをクリックすると以下の [メモリ] の [イベント] リスト画面が表示されます。
FortiGate のメモリバッファ内のログメッセージが表示されます。



さらに、[Log Type]リストからログの種類を選択できます。

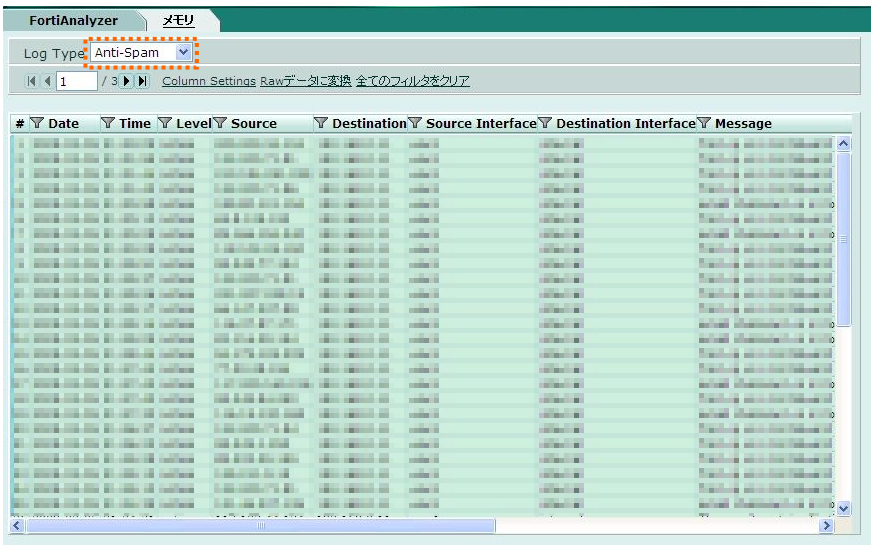
以下の画面は[アタック]リストです。

以下の画面は[アンチウィルス]リストです。

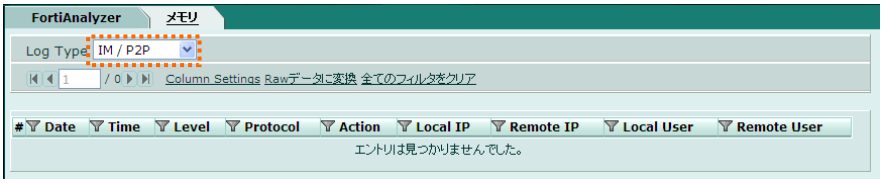


以下の画面は[ウェブフィルタ]リストです。

以下の画面は[Anti-Spam]リストです。



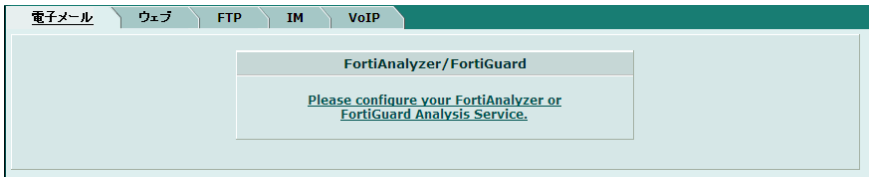
以下の画面は [IM/P2P] リストです。



以下の画面は [VoIP] リストです。

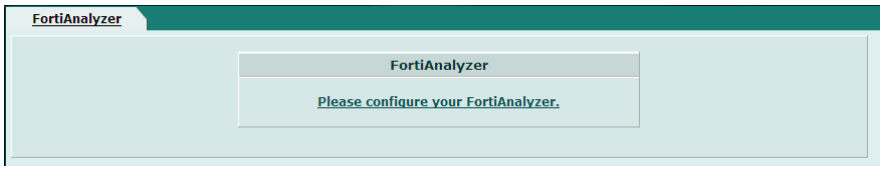
■ ［コンテンツアーカイブ］画面

［コンテンツアーカイブ］はすべてご利用いただけません。



■ ［リポート設定］画面

［リポート設定］はご利用いただけません。

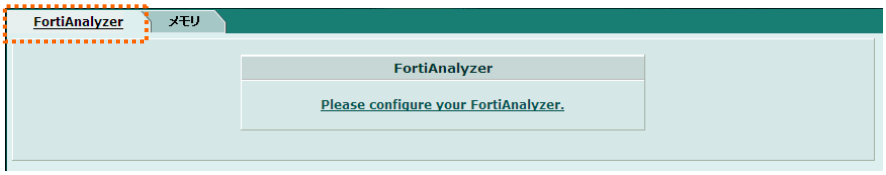


■ [リモートアクセス] 画面

[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。