

【STIL 製品評価レポート】

FortiMail

**FORTINET**

**SOURCE  
POD**

2011年8月1日

株式会社ソースポッド

SourcePod Technical Intelligence Lab.

－ 目次 －

|                                |           |
|--------------------------------|-----------|
| <b>1. 概略</b>                   | <b>3</b>  |
| <b>2. 初期設定</b>                 | <b>5</b>  |
| 2.1 ファームウェアアップデート              | 5         |
| 2.2 サーバーモードへの切り替え              | 7         |
| 2.3 Quick Start Wizard による初期設定 | 7         |
| <b>3. ユーザー機能</b>               | <b>12</b> |
| 3.1 Web メール                    | 12        |
| 3.2 アドレス帳                      | 18        |
| 3.3 カレンダー                      | 18        |
| 3.4 環境設定                       | 19        |
| <b>4. 管理者機能</b>                | <b>22</b> |
| 4.1 モニタリング機能                   | 22        |
| 4.2 メンテナンス機能                   | 23        |
| 4.3 システム機能                     | 25        |
| 4.4 メール設定機能                    | 26        |
| 4.5 ユーザー機能                     | 28        |
| 4.6 ポリシー機能                     | 29        |
| 4.7 プロファイル機能                   | 35        |
| 4.8 アンチスパム機能                   | 37        |
| 4.9 メールアーカイブ機能                 | 37        |
| 4.10 ログとレポート機能                 | 39        |
| <b>5. 総評</b>                   | <b>43</b> |

## 1. 概略

### ■ UTM 市場のリーディングベンダー フォーティネット



フォーティネットは、ネットワークセキュリティアプライアンスの世界的なリーディングカンパニーで、UTM（統合脅威管理）市場をリードするパイオニアでもあります。主力製品である UTM「FortiGate」は、インターネットの複合的な脅威から企業ネットワークを保護する多層セキュリティ機能を提供し、世界中で 10 万社以上、75 万台以上のアプライアンスを出荷しています。また、フォーティネットでは、UTM の技術やノウハウを活かし、オールインワンのメールシステムアプライアンス「FortiMail」も提供しており、2011 年 5 月の管理画面の日本語化に合わせて、日本国内でも本格展開しています。

### ■ 製品評価の背景

アンチスパム・アンチウイルス製品は、アプライアンスでの提供が全体の約 86%（ソースポッド発行「国内メール市場分析レポート 2011」より）を占めていると言われています。しかしながら、それ以外での市場では、アプライアンスでの提供形態はまだ少ないのが現状です。

フォーティネットでは、世界中で 10 万社以上、75 万台以上のアプライアンスを提供しており、その技術力とノウハウ、すべて自社開発というポリシーも併せ持って、アンチスパム・アンチウイルスだけでなく、メールサーバーや Web メール、送信フィルタリング、暗号化、アーカイブなどをオールインワンで提供するアプライアンス製品「FortiMail」をリリースしています。

全て自社開発で提供することによる低コストの実現、クラウドサービスベンダーでの運用管理にも適したマルチテナント・仮想ホスティングに対応しており、昨今のクラウドによる運用・管理環境の変化、コスト削減への強い要望などに対しても、非常に優れたコスト・導入・運用メリットを提供しています。

2011 年 5 月の管理画面の日本語化により、日本国内でも「FortiMail」を本格展開されるということで、株式会社ソースポッドでは、注目の製品として評価させていただくこととなりました。

今回、パフォーマンスやアンチスパム・アンチウイルスの検知率のテストなどは実施せ

ず、導入時の「インストール・設定」、Web メールなどのアプリケーションが提供する「ユーザー機能」、そして設定・運用・管理に関わる「管理者機能」を中心に製品評価を実施します。

## ■ 「ForTiMail」とは？

「ForTiMail」は、「FortiGate」のメールセキュリティ機能をさらに拡張し、高機能化したオールインワン・セキュアメールアプライアンスです。独自 OS をベースにした高速 MTA に、高機能なアンチスパム・ウィルス、コンテンツフィルタ、暗号化、アーカイブ、Web メール、カレンダー機能の他、高可用性、外部ストレージ、LDAP などの外部連携を含む高い拡張性を標準搭載しています。

また、トランスペアレント、ゲートウェイ、サーバー (MTA) の 3 種類の導入形態をサポートし、メールサーバーを含む各メールセキュリティインフラを統合することで、TCO および管理工数を大幅に削減。また、スパム検知率の向上と誤検知率の低下が評価され、Virus Bulletin 誌のアンチスパムアワードを 13 期連続で受賞。なお、機器ライセンスのため、利用ユーザー数に制限はありません。

## ■ SourcePod Technical Intelligence lab とは？



株式会社ソースポッドでは、メールシステムに特化したコンサルティング事業、メディア事業、教育事業、マーケティング事業、製品・サービス検証事業を展開しています。その中で、第三者の立場で客観的に製品・サービス検証事業を行う機関が「SourcePod Technical Intelligence Lab (以下、STIL)」です。今まで評価・検証を行ったメール関連製品は、100 点以上になります。

## 2. 初期設定

---

今回の「FortiMail」評価は、エントリーモデルである「FortiMail 100C」で実施した。また、「FortiMail」には、以下の3つの動作モードが用意されているが、今回の評価ではアンチスパム・アンチウイルスにおける検知率のテストを実施しないため、メールサーバーとして利用できるサーバーモードにて初期設定を行った。

- **サーバーモード**

メールセキュリティとメールサーバー機能を1台で実装。

- **ゲートウェイモード**

SMTP リレーの経路を変更して設置。

- **トランスペアレントモード**

既存のメールサーバーやネットワーク環境へシームレスに統合。DNS レコードの変更も不要。

### 2.1 ファームウェアアップデート

PC から「FortiMail 100C」シリアルポートに接続する。その後、「FortiMail 100C」の Port1 (デフォルト IP : 192.168.1.99) と PC を LAN で接続し、PC のブラウザから管理者画面 <https://192.168.1.99/admin/> にアクセスし、admin でログインする。



図 1 : 管理者画面 - ログイン

ログイン後は、モニタリングメニューのシステムステータスが表示される。  
※表示言語は日本語を含め 8 言語から選択可能。

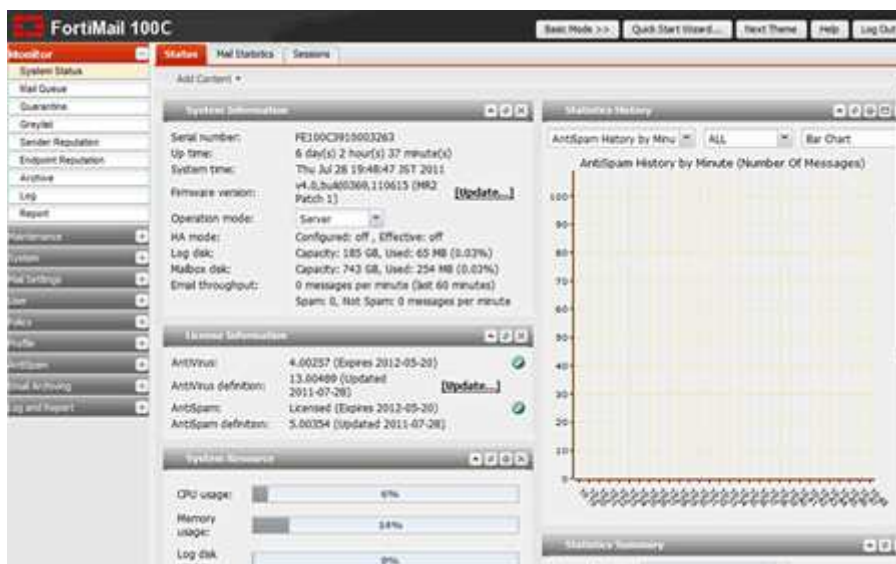


図 2 : 管理者画面 - System Status

System > Administrator > Administrator から言語を日本語に変更する。

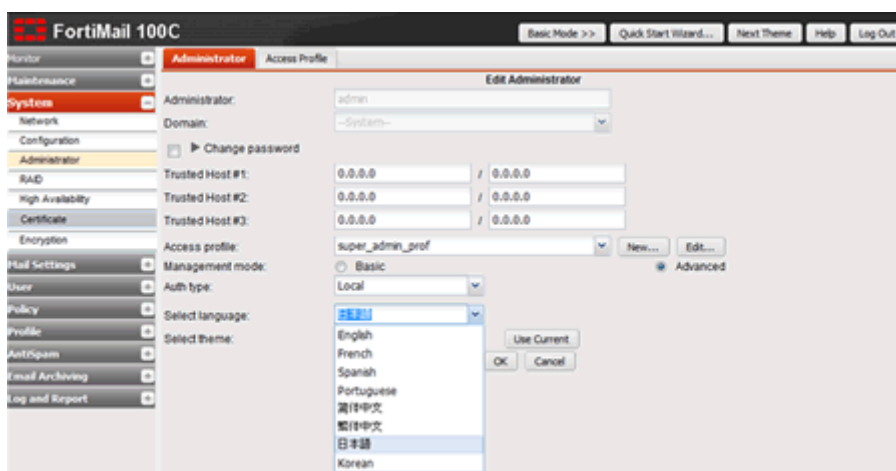


図 3：管理者画面 - 言語選択

その後、「FortiMail」を最新の状態にするために、ファームウェアのバージョンアップを行う。最新のファームウェアは、製品に同梱された CD より実施する。[Update...]から該当ファイルを指定して、ファームウェアをアップロードする。



図 4：管理者画面 - ファームウェアアップデート

## 2.2 サーバーモードへの切り替え

次に動作モードの切り替えを行う。「FortiMail」ではサーバーモード、ゲートウェイモード、トランスパレントモードが用意されているが、今回の評価ではサーバーモードを利用する。動作モードは、デフォルトでゲートウェイモードになっているため、サーバーモードに変更する。



図 5：管理者画面 - 動作モード

## 2.3 クイックスタートウィザードによる初期設定

続いて、初期設定を行う。「FortiMail」には各種設定画面が用意されているが、今回は7ステップで容易に初期設定を行うことのできる「クイックスタートウィザード」を利用する。



図 6：管理者画面 - クイックスタートウィザード

### 1) Quick Start Wizard 1/7：システム管理者のパスワード設定

まずは、システム管理者のパスワードを設定する。

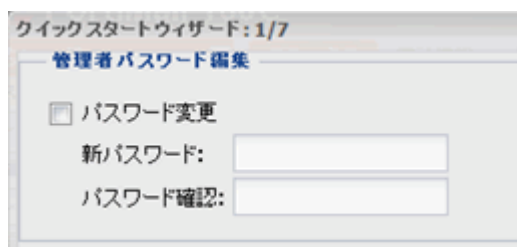


図 7：管理者画面 - クイックスタートウィザード 1/7

## 2) Quick Start Wizard 2/7 : ネットワーク&タイムゾーン設定

次にネットワークとタイムゾーンの設定を行う。ここではPort1のIPアドレスを192.168.1.99に、サブネットマスクを255.255.255.0に設定。タイムゾーンをGMT+9:00に設定し、それ以外の設定はデフォルトのままとする。



| ネットワーク設定     |                              |
|--------------|------------------------------|
| ポート1のIP:     | 192.168.1.99 / 255.255.255.0 |
| プライマリDNS:    | 208.91.112.53                |
| セカンダリDNS:    | 208.91.112.52                |
| デフォルトゲートウェイ: | 0.0.0.0                      |

| タイムセッティング   |                               |
|---|-------------------------------|
| タイムゾーン:   | (GMT+9:00)大阪、札幌、東京、ソウル        |
| <input type="radio"/> 時間設定                            | 日: 08/12/11 時: 14 分: 36 秒: 12 |
| <input checked="" type="radio"/> NTPサーバーによる自動システム時間同期 |                               |
| NTPサーバー名/IP:  | pool.ntp.org                  |

図8 : 管理者画面 - クイックスタートウィザード 2/7

## 3) Quick Start Wizard 3/7 : ローカルホストの設定

ローカルホストの設定を行う。ここでは全てデフォルト値を用いた。



| ローカルホスト設定                                  |             |
|--|-------------|
| ホスト名:                                      | FortMail    |
| ローカルドメイン名:                                 | example.com |
| POP3サーバー・ポート番号:                            | 110         |
| SMTPサーバー・ポート番号:                            | 25          |
| <input type="checkbox"/> SMTP over SSL/TLS |             |
| SMTPサーバー・ポート番号:                            | 465         |

図9 : 管理者画面 - クイックスタートウィザード 3/7

## 4) Quick Start Wizard 4/7 : ドメイン設定

次にドメインの追加を行う。sp01.example.comとsp02.example.comを作成した。



図 10：管理者画面 - クイックスタートウィザード 4/7

### 5) Quick Start Wizard 5/7：インバウンド向けアンチスパム・アンチウイルスの設定

アンチスパムとアンチウイルスの設定を行う。まずはインバウンド向けの設定を行う。ここでは全てデフォルト値を用いた。

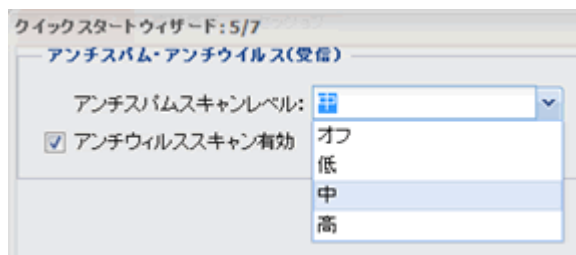


図 11：管理者画面 - クイックスタートウィザード 5/7

### 6) Quick Start Wizard 6/7：アウトバウンド向けアンチスパム・アンチウイルスの設定

続いて、アウトバウンド向けの設定を行う。ここでも全てデフォルト値を用いた。尚、アンチスパム・アンチウイルスだけではなく、フィルタリングの設定を行うこともできる。



図 12：管理者画面 - クイックスタートウィザード 6/7①



図 13：管理者画面 - クイックスタートウィザード 6/7②

## 7) Quick Start Wizard 7/7：設定確認画面

最後に、設定内容の確認画面が表示され、問題なければ登録を行う。



図 14：管理者画面 - クイックスタートウィザード 7/7

設定が完了すると、管理者ログイン画面に遷移する。ログイン後ユーザーを追加すれば、最小限の設定で「FortiMail」を利用することができる。

### 【検証者のコメント】

「FortiMail」は機能が豊富で、管理者機能が充実しているため、設定箇所は自ずと多くなる。ただし、「Quick Start Wizard」が用意されているので、主にインバウンドセキュリティ

フィ対策を目的として「FortiMail」を利用する場合は、「Quick Start Wizard」で必要最低限の項目を設定することで、すぐにでも利用を開始できる。

また、管理者画面が英語表示されているが、管理者画面の表示言語は変更できるため、日本語で「Quick Start Wizard」を利用することもできる。

アプライアンス製品であるため、インストールは必要なく、設定も容易に実施できるため、比較的容易に稼働させることのできる製品であるように感じた。

### 3. ユーザー機能

---

今回の「FortiMail」の評価では、ユーザー機能は主に Web メール上で提供しているサービスにフォーカスして実施した。以下の Web メールログイン画面より、ログインを行う。

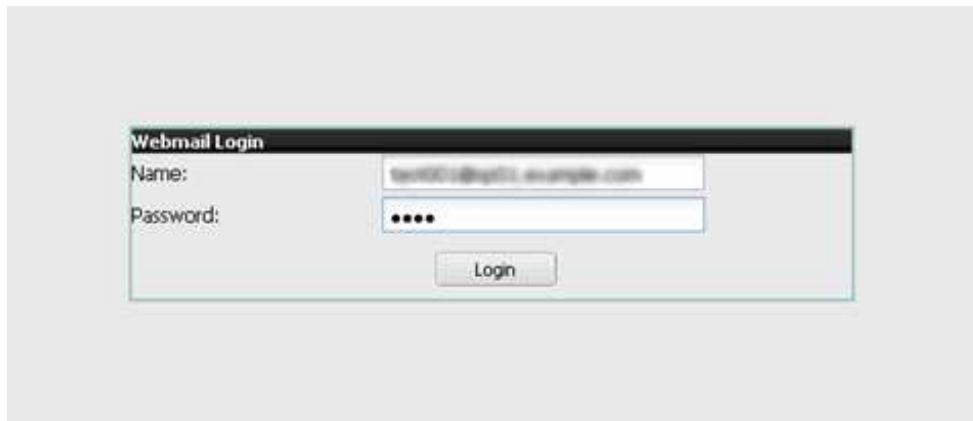


図 15 : Web メール画面 - ログイン

#### 3.1 Web メール

##### 3.1.1 メール受信画面

Web メールにログインすると、デフォルトで受信トレイが表示される。3 ペイン構造になっており、左ペインがメールボックスや各種メニュー、右ペイン上段がメール一覧、右ペイン下段がメール内容の表示と、一般的な画面構成をとっている。中央縦フレーム枠をクリックすることで、左ペインを画面左端に収納することもできる。

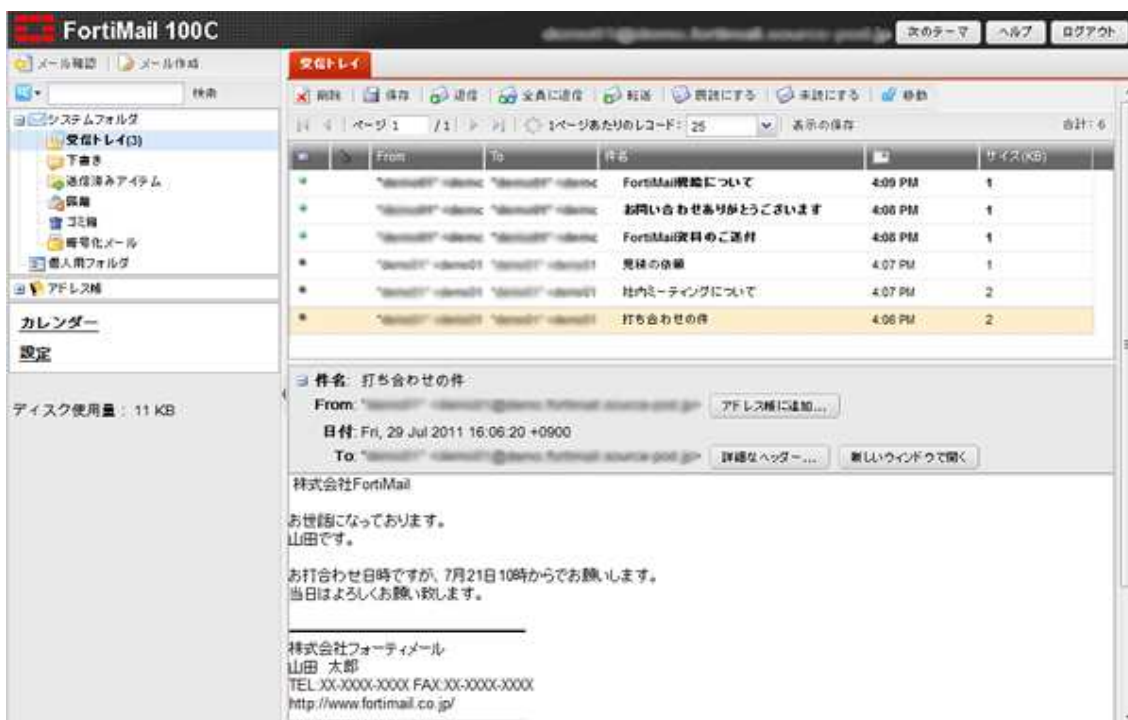


図 16 : Web メール - 受信トレイ

また、3種類の画面テーマが用意されており、右上の「次のテーマ」ボタンをクリックすると、簡単にテーマを切り替えることができる。



図 17 : Web メール - 3種類の画面テーマ

「FortiMail」の Web メールは、Ajax に対応しているため、ドラッグ&ドロップによるメールの移動や Ctrl キーを利用した複数メール選択、右クリックメニューなどを利用でき、また動作が非常に軽いため、クライアントメーラーのように利用できる。



図 18 : Web メール - ドラッグ&ドロップによるメールの移動



図 19 : Web メール -メール一覧右クリックメニュー

### 3.1.2 メール作成・送信

左ペインの「メール作成」ボタンをクリックすると、右ペインにメール作成フォーマットとして「新しいメッセージ」タブが表示される。上段に「送信」「下書き保存」「ファイ

ル添付」「アドレス帳」のメニューを表示し、その下に送信先欄、件名、本文と一般的な並びになっている。

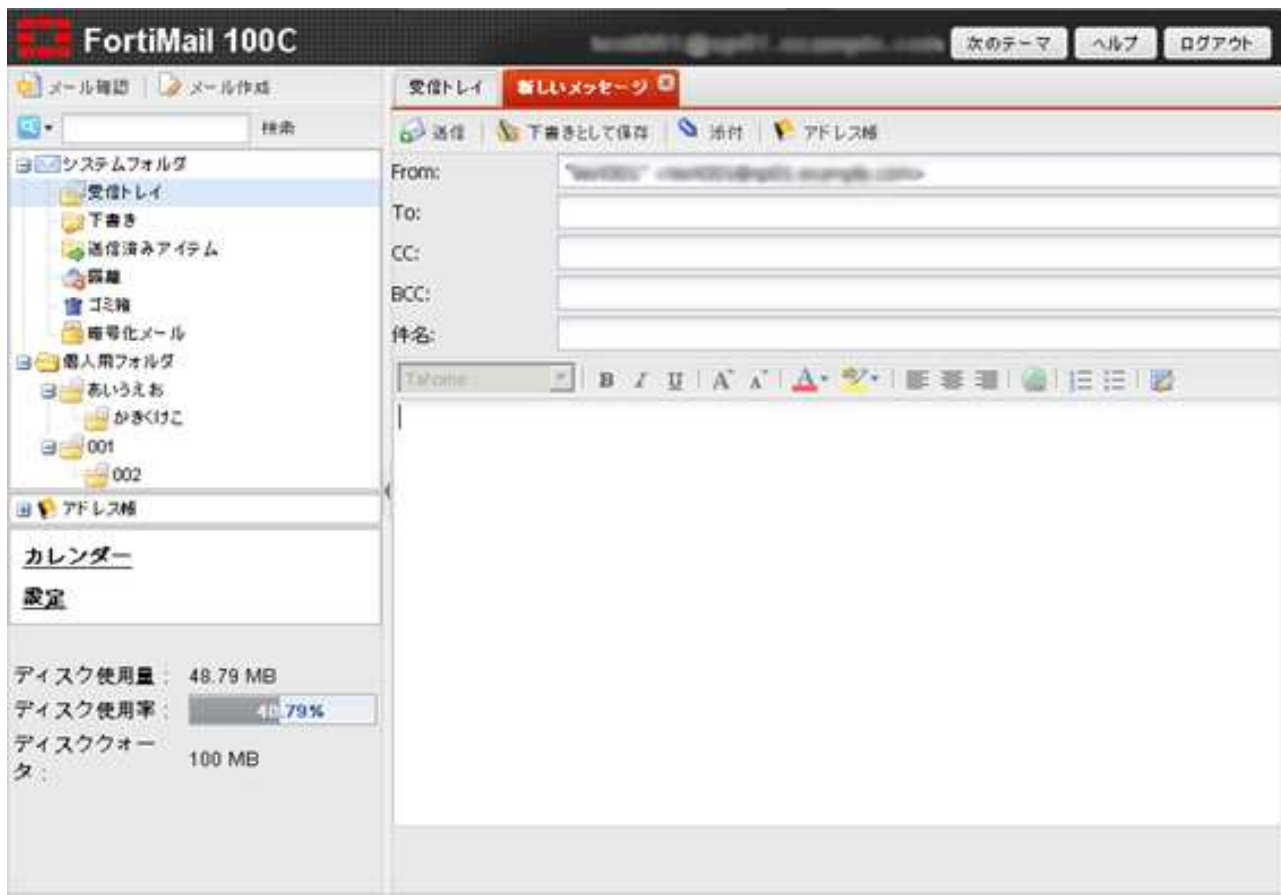


図 20 : Web メール画面 -メール作成画面

### 3.1.3 暗号化メール

「FortiMail」では、S/MIME と IBE の 2 つのメール暗号化方式に対応している。ここでは、Web メールインターフェースと連携する IBE を利用してみる。

IBE (Identity Based Encryption) では、公開鍵暗号方式の仕組みを使う。メールアドレスから暗号鍵を生成するため、内部や外部のメール送受信者や管理者は、煩雑な鍵の管理等を意識することなく、暗号化されたメールをやり取りすることができる。暗号化されたメールは、「FortiMail」内部に保存され、宛先に対しては「FortiMail」の Web メール画面へのリンクが送られる。外部アカウントのメール受信者がリンクをクリックすると、初回は IBE ユーザー登録画面で氏名やパスワードや秘密の質問などを登録する。登録後は、Web メールから暗号化メールを見ることができるようになる。

尚、IBE 暗号化メールには、メールに「securemsg.html」という添付ファイルを付与し、ローカルの「securemsg.html」がブラウザで開かれ、ログイン画面（ローカルファイル）が表示され、Web メール「暗号化メール」フォルダに保存されない「プッシュモード」と、メールにログイン画面のリンクが張られている。クリックすると、ブラウザが立ち上がり、ログイン画面（リモート）が表示され、「暗号化メール」フォルダに保存される「プルモード」が用意されており、今回はプッシュモードで実施した。

IBE で外部にメールを送ると、次のようなメールが送られる。

補足：メールはカスタマイズ（日本語化）可能です。

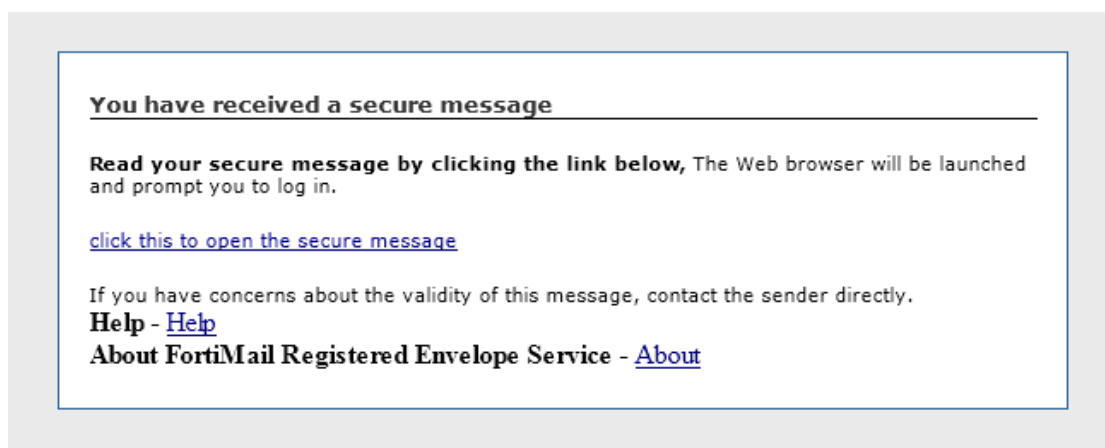


図 21：IBE 暗号メール - 通知メール

「click this to open the secure message」をクリックすると、ブラウザが起動して IBE ユーザーの登録画面が表示される。



図 22：IBE 暗号メール - 未登録ユーザーログイン画面

「Register」を押下すると、新規ユーザー登録画面が表示され、外部のメール受信者は、自分の IBE ユーザーアカウントを登録する。

新規ユーザー登録

メールアドレス: test@example.com

言語: 日本語

タイムゾーン: (GMT+9:00)大阪, 札幌, 東京, ソウル

名:

姓:

パスワード:

パスワード確認:

秘密の質問: あなたの好きな食べ物は何ですか?

答え:

図 23 : IBE 暗号メール - ユーザー登録画面②

登録が完了すると、ブラウザに次の画面が表示されるとともに、外部のメール受信者に対して、登録完了メールが送信される。登録完了後、再度最初のメールの「Click this to open the secure message」をクリックすると、今度は次の画面が表示される。

IBE 001

From: test@example.com

To: test@example.com

件名: 暗号化メール 001

パスワード:

[パスワードを忘れた場合](#)

Copyright ©2010 Fortinet, Inc. All Rights Reserved.

図 24 : IBE 暗号メール - 登録ユーザーログイン画面

ログインすると、IBE ユーザー用の Web メールから暗号化メールを見ることができる。  
※社内ユーザーは、フォルダの 1 つとして暗号化メールフォルダが表示されている。

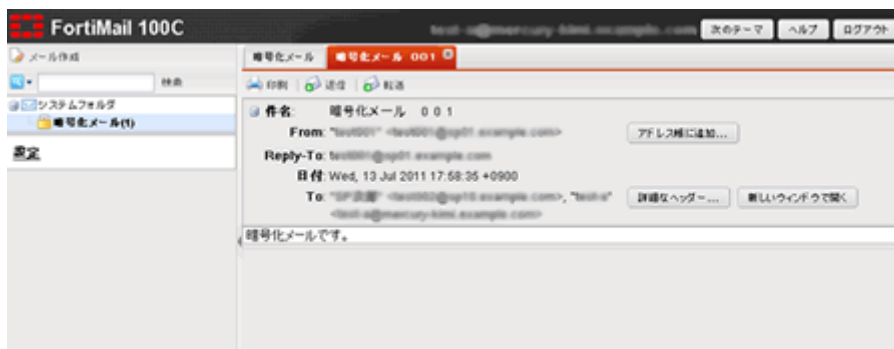


図 25 : IBE 暗号メール - Web メールによる暗号化メール表示 (プルモード)

### 3.2 アドレス帳

ユーザーが登録したアドレスと連絡先グループが「個人」フォルダに、管理者が設定したドメインのアドレス帳と連絡先グループが「ドメイン」フォルダに、システムグローバルなアドレス帳と連絡先グループが「共通」フォルダに表示される。「個人」フォルダ内のアドレス帳データは、CSV 形式か vCard 形式でインポートとエクスポートが行える。また、アドレス帳を選択して右クリックで表示されるメニューから、メールを作成することができる。



図 26 : Web メール画面 - アドレス帳

### 3.3 カレンダー

登録したスケジュール内容を、日別、週別、月別に表示することができる。また、カレンダーは、「FortiMail」アカウントの参加者と共有でき、イベント作成時に参加者を登録

すると、カレンダーに登録されると同時に、参加者全員に参加可否を確認するメールが送信される。

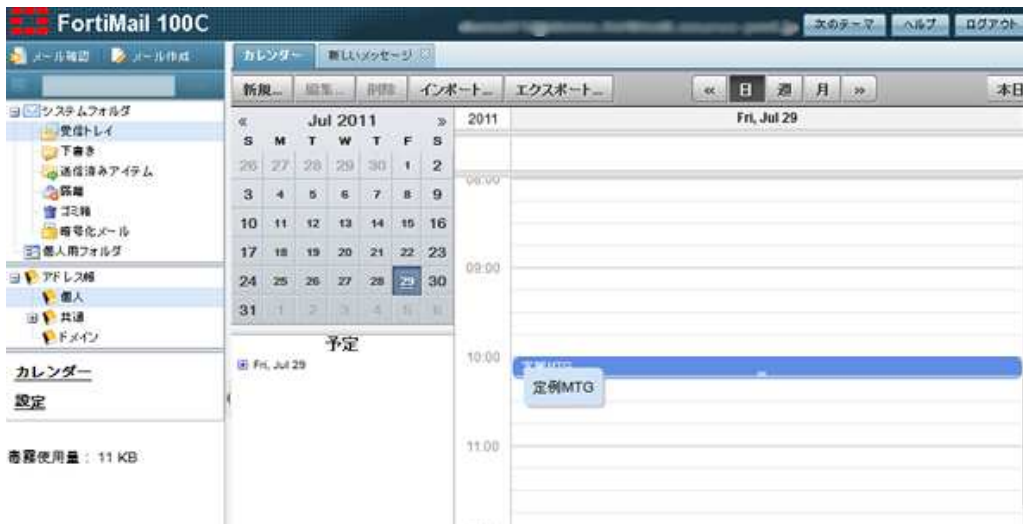


図 27 : Web メール画面 - カレンダー表示画面

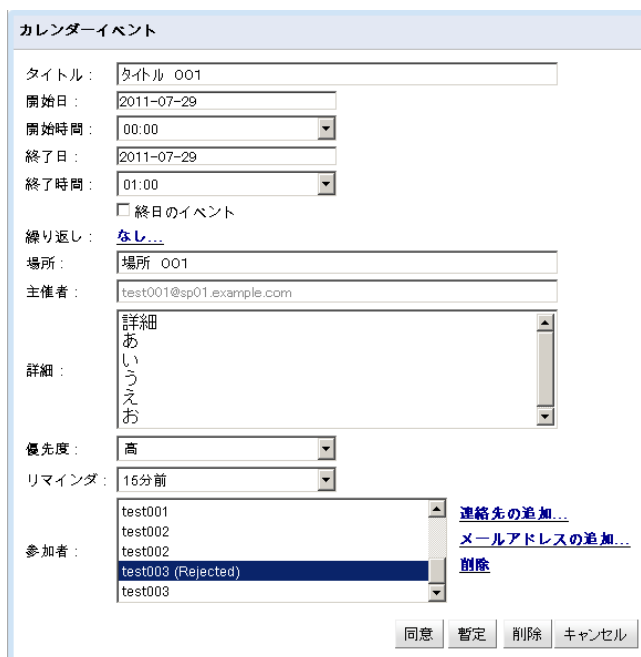


図 28 : Web メール画面 - カレンダーイベント登録画面

### 3.4 環境設定

「FortiMail」では、各ユーザー向けに、言語設定や署名、パスワード変更、転送、不在通知などの設定メニューを提供している。表示言語は 15 か国語用意されており、マルチアカ

アカウント機能でプライマリとセカンダリのアドレスを設定し、メール受信画面で切り替えて利用することができる。

図 29 : Web メール画面 - 環境設定

### 【検証者のコメント】

Web メールは、シンプルな構成だが、クライアントメーラーと変わらないくらい動作が軽いため、外出先などのオプションメーラーとしては十分に利用できる。ただし、メインメーラーとなるには機能が少ない点が否めず、今後の機能強化に期待したい。

ただし、IBE 暗号化メールの機能はよくできており、こちらは用途に応じて是非活用したい。特に強度の高い暗号化メールを、Web メール上で連携して利用できる製品が少ないため、

ユーザービリティや一元管理できる点、標準で搭載されていることによるコストという点においても優れている。

また、カレンダーは個人向けだけでなく、共有スケジューラーとして活用でき、参加者の出欠有無と連動することもできるため、社内スケジュール管理には十分活用できると言えるだろう。

## 4. 管理者機能

---

「FortiMail」の管理者機能は、シリアルコンソールや SSH 接続による管理コマンド、Web 管理者画面による操作が行える。今回は、Web 管理者画面を利用する。

「FortiMail」は、システム管理者とドメイン管理者の 2 種類の管理者によって運用・管理を行う。

- **システム管理者**

全管理者機能を利用可能な管理者。システム管理者は、初期登録された admin 以外にも複数追加できる。

- **ドメイン管理者**

ドメイン管理に必要な管理者機能のみ利用可能な管理者。1 ドメインに対し、複数のドメイン管理者を追加できる。

### 4.1 モニタリング機能

「モニタリング」機能には、「システム」「メールキュー」「隔離」「グレーリスト」「送信者評価」「エンドポイント評価」「アーカイブ」「ログ」「レポート」メニューが用意されており、各種項目をモニタリングできる。

前述した通り、管理者画面ログイン後には、「システム」のステータス一覧画面が表示される。この画面では、基本的なシステム情報やアンチウイルスやアンチスパムの更新状況、アンチスパムとアンチウイルスの統計情報の簡易ヒストリ情報や統計サマリーなどをモニタリングでき、自由に位置や表示有無を変更できる。ファームウェアなどのアップデートやシステムシャットダウンや再起動もこの画面で行う。また、Fortinet RSS Feed で、最新の脅威情報やアドバイザリレポートやニュースを閲覧することもできる。



図 30 : 管理者画面 - システムモニタリング画面 (デフォルト画面)

## 4.2 メンテナンス機能

日々の運用で必要となるメンテナンスを行う「メンテナンス」機能には、「システム」「FortiGuard」「アンチスパム」メニューが用意されている。

「システム」のメールデータバックアップオプションには、自動バックアップ設定やリストア、バックアップ先の設定などの設定が可能。メールデータのバックアップ先として、NFS、Windows サーバー、SSH ファイルシステム、USB デバイス、iSCSI を指定できる。

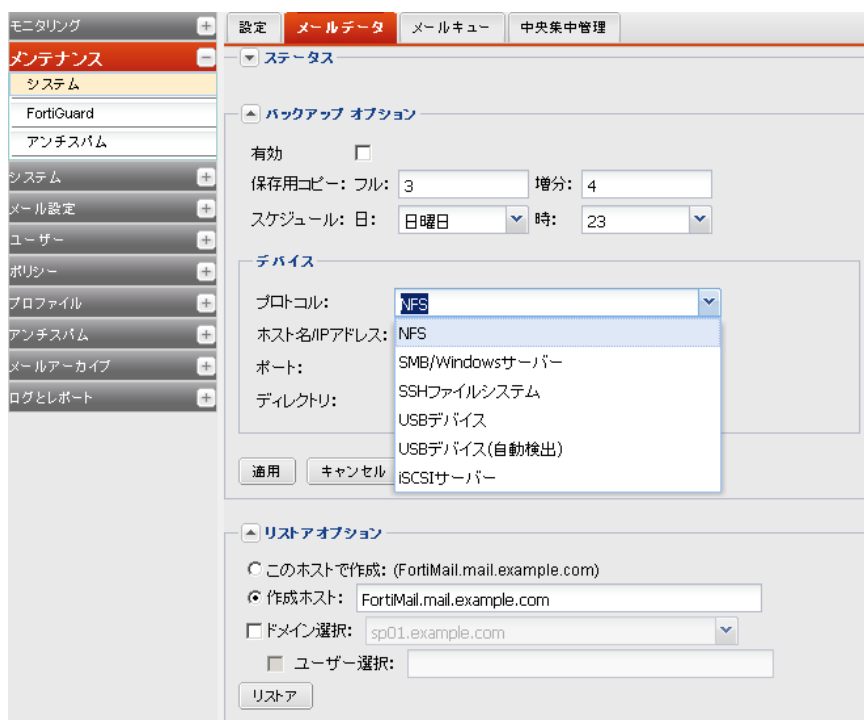


図 31 : 管理者画面 - システムメンテナンス画面

また、「FortiGuard」の「更新」では、各定義ファイルおよび AV エンジンのアップデート方法の設定が可能だが、通常はデフォルト設定で問題なく運用できる。なお、アップデート状況や FortiGuard ディストリビューションネットワークへの接続状況などもリアルタイムで確認できる。

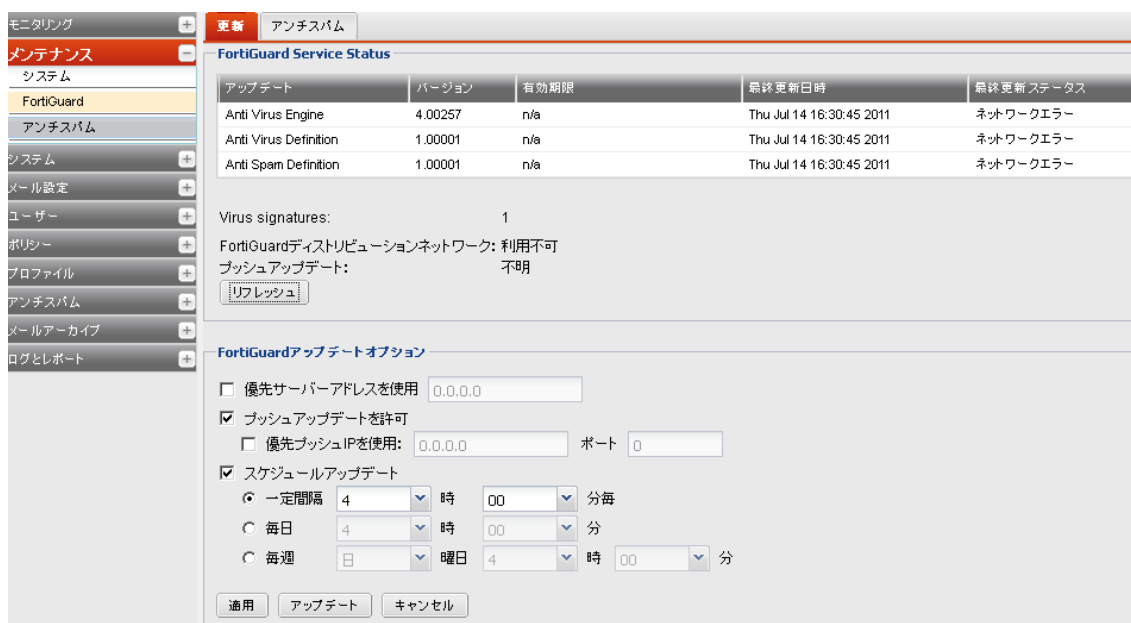


図 32 : 管理者画面 - FortiGuard 更新画面

### 4.3 システム機能

「FortiMail」の稼働に関わる主にネットワークや構成に関わる設定を行う「システム」機能には、「ネットワーク」「設定」「管理者」「RAID」「HA」「証明書」「暗号化」メニューを用意している。

「設定」では、NTP や SNMP などのインフラ管理における設定と、Web のタイムアウトやパスワードポリシー、サービスポート番号などの設定、管理者とユーザーの Web 画面のタイトルやロゴ、デフォルト言語などの各種 Web インターフェースの設定が行える。

「管理者」では、管理者アカウントの設定を行える。言語変更もこの画面から実施でき、日本語を含める 8 言語より選択できる。また、管理者ごとにアクセスプロファイルを設定できるため、システム管理者、ドメイン管理者の中でも細かく権限設定した運用もできる。

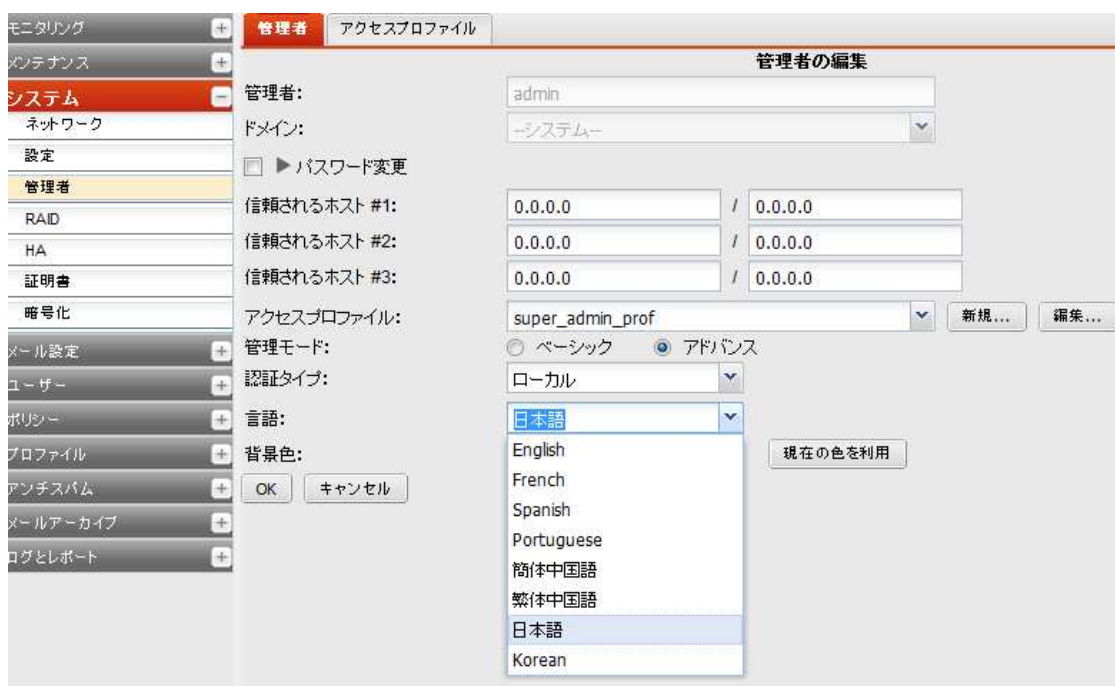


図 33 : 管理者画面 - 管理者設定画面



図 34 : 管理者画面 - 管理者アクセス権限設定画面

#### 4.4 メール設定機能

メール設定機能では、メールシステムの基本設定及び運用に関わる「設定」「ドメイン」「アドレス帳」メニューを用意している。

「設定」では、メールサーバーに関わるホスト名、ローカルドメイン名、ポート番号、暗号化通信、サブミッションポート、POP3 ポートといった基本的な設定、リレーサーバーやメールキュー、遅延メッセージ、配送時の ESMTP、LDAP と連携したドメイン検証の設定などが行える。また、メールデータ (MTA スプール、メールキュー、メールアーカイブ、ユーザーメールボックス、隔離メール等) を保存する NAS サーバー (NFS/iSCSI) を設定することができる。



図 35 : 管理者画面 - メールサーバー設定画面

また、「ドメイン」では、管理ドメインの設定として、メールルーティングの LDAP 参照、Received ヘッダー削除、ユーザー画面のデフォルト言語、最大メッセージサイズ、IP プール、隔離レポート、SMTP プロトコルのグリーディングなどの設定を行える。

「アドレス帳」では、システム全体やドメイン別のアドレス帳とグループを管理する。CSV や vCard でのエクスポート、CSV や vCard、そして LDAP からのインポートも行うことができる。

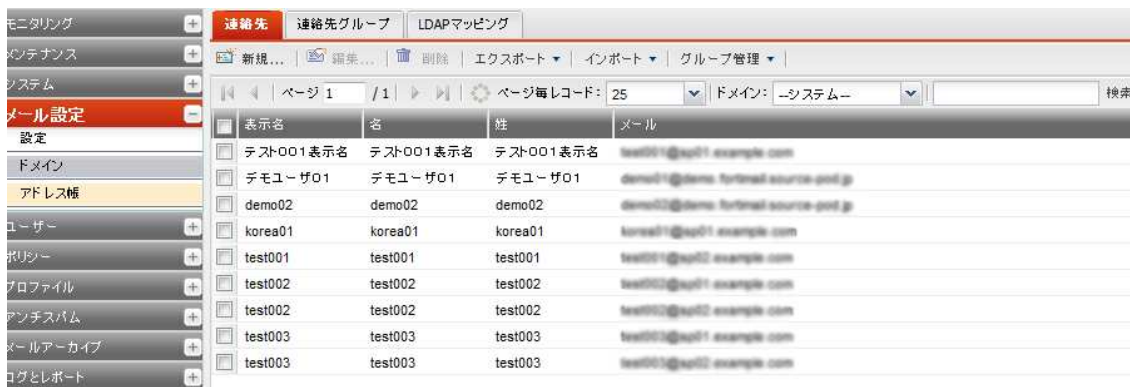


図 36 : 管理者画面 - アドレス帳設定画面

#### 4.5 ユーザー機能

「FortiMail」を利用するユーザーの管理を行う「ユーザー」機能では、「ユーザー」「ユーザーエイリアス」「アドレスマップ」「IBE ユーザー」といったメニューを用意している。

「ユーザー」登録は、手動での登録以外にも、CSV によるインポートが行える。また、パスワード参照先として、LDAP を指定することもできる。「ユーザー」設定メニューでは、ユーザー一覧からユーザーを選択し、各ユーザー表示、タイムアウト時間、バケーションや転送、アンチスパム、マルチアカウントの設定を行うことができる。ユーザーグループの管理も行える。

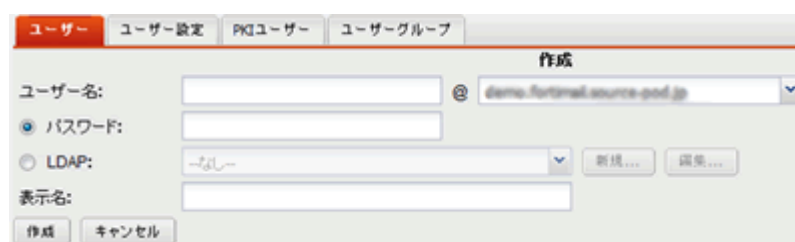


図 37 : 管理者画面 - ユーザー登録画面

「ユーザーエイリアス」では、外部/内部メールアドレスを含めたエイリアスを作成することができる。

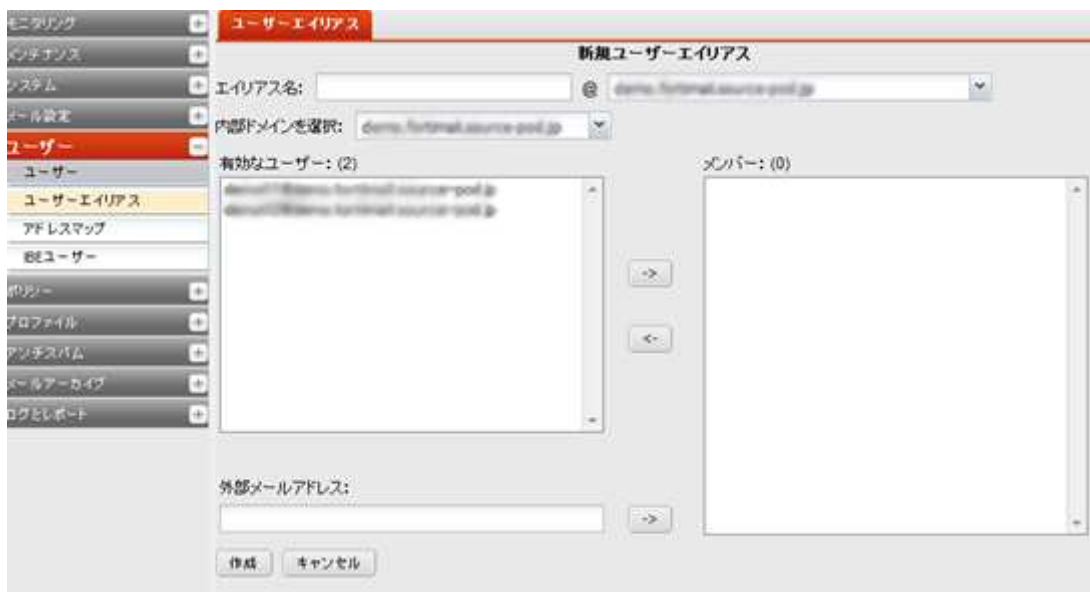


図 38 : 管理者画面 - エイリアス設定画面

## 4.6 ポリシー機能

「ポリシー」機能には、「アクセス制御」「ポリシー」メニューが用意されている。

「アクセス制御」では、送受信時のアクセス制御ルールを複数定義することができる。受信ルールでは、送信者パターン、受信者パターン、送信者 IP、リバース DNS パターン等の条件を自由に設定し、ルールに適合した際のアクションを、「バイパス」「リレー」「拒否」「破棄」の中から選択することができる。送信ルールでは、送信者パターン、受信者パターン、宛先 IP 等の条件を指定し、ルールに適合した際に適用される、TLS プロファイルや、暗号化プロファイルを設定することができる。



図 39 : 管理者画面 - 受信者アクセス制御ルール設定画面

「ポリシー」では、送信元と宛先の IP を条件にしたアクションと適用するプロファイルを設定する IP ポリシーと、メール送受信時のポリシーを設定できる受信者ポリシーを設定できる。

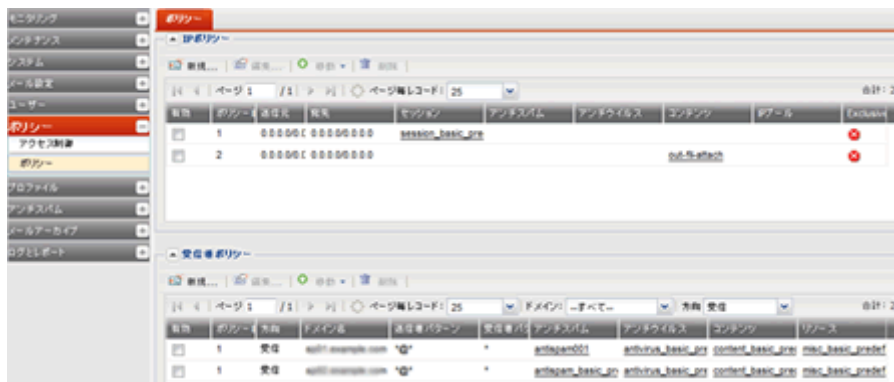


図 40 : 管理者画面 - ポリシー一覧画面

IP ポリシーでは、送信元と宛先の IP を条件にした、アクションと適用するプロファイルを設定する。

ポリシー

IPベースポリシー

有効

送信元IP/ネットマスク: 0.0.0.0 / 0

宛先: IP/ネットマスク 0.0.0.0 / 0

アクション: スキャン

プロフィール

セッション: session\_basic\_predefined [新規...] [編集...]

アンチスパム: --なし-- [新規...] [編集...]

アンチウイルス: --なし-- [新規...] [編集...]

コンテンツ: --なし-- [新規...] [編集...]

IPブール: --なし-- [新規...] [編集...]

その他

受信者ベースポリシーの一致を優先

OK キャンセル

図 41 : 管理者画面 - IP ポリシー設定画面

例えばセッションにおける設定を見ると、コネクション設定や送信者評価、エンドポイント評価、送信者検証、セッション設定、認証されないセッションの設定、SMTP リミット、エラーの処理、ヘッダー操作、リストといった設定項目があり、要望によって非常に自由度の高い、幅広い設定が行える。

尚、「FortiMail」では、各種ルールをプロフィールとして設定し、それを各ドメインやユーザーに紐付けてポリシーを作成する方法を取っているため、こちらも自由度の高いポリシーを設定できる仕組みをとっている。



図 42 : 管理者画面 - IP ポリシーにおけるセッションプロファイル設定画面

受信者ポリシーでは、メール送受信におけるポリシー設定が行える。

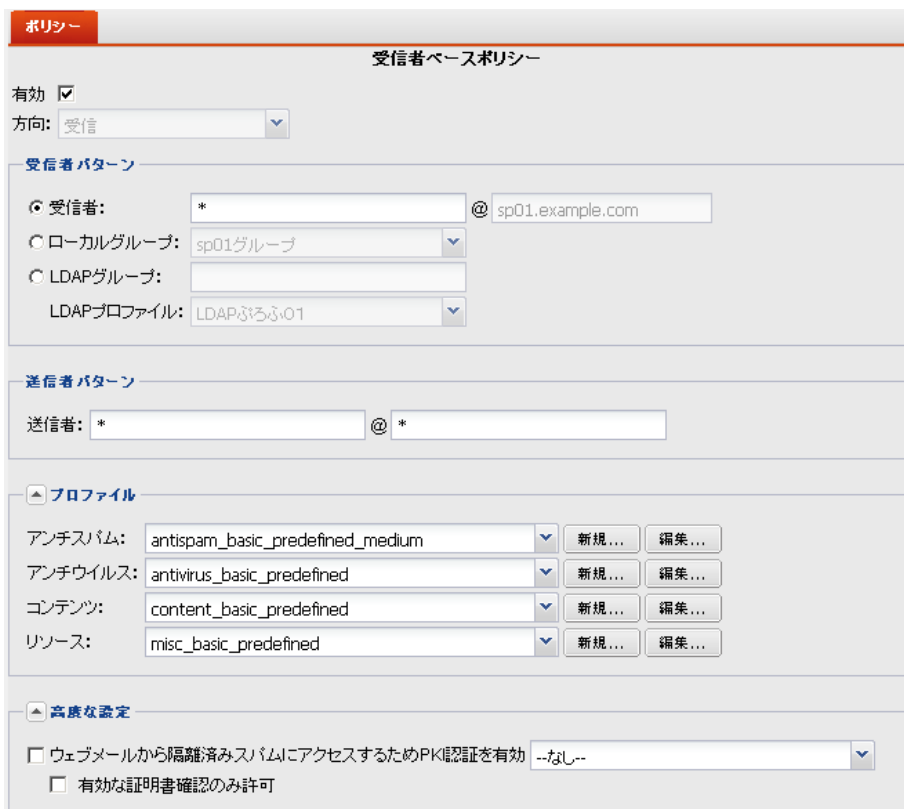


図 43 : 管理者画面 - 受信者ポリシー設定画面

アンチスパムとコンテンツのプロファイルの設定をしてみる。アンチスパムプロファイルのスキャン設定では、FortiGuard スキャン、DNSBL スキャン、ディープヘッダスキャン、SURBL スキャン、ヒューリスティックスキャンなどが設定されており、これらはデフォルト設定プロファイルをコピーして、容易に設定を変更することができる。

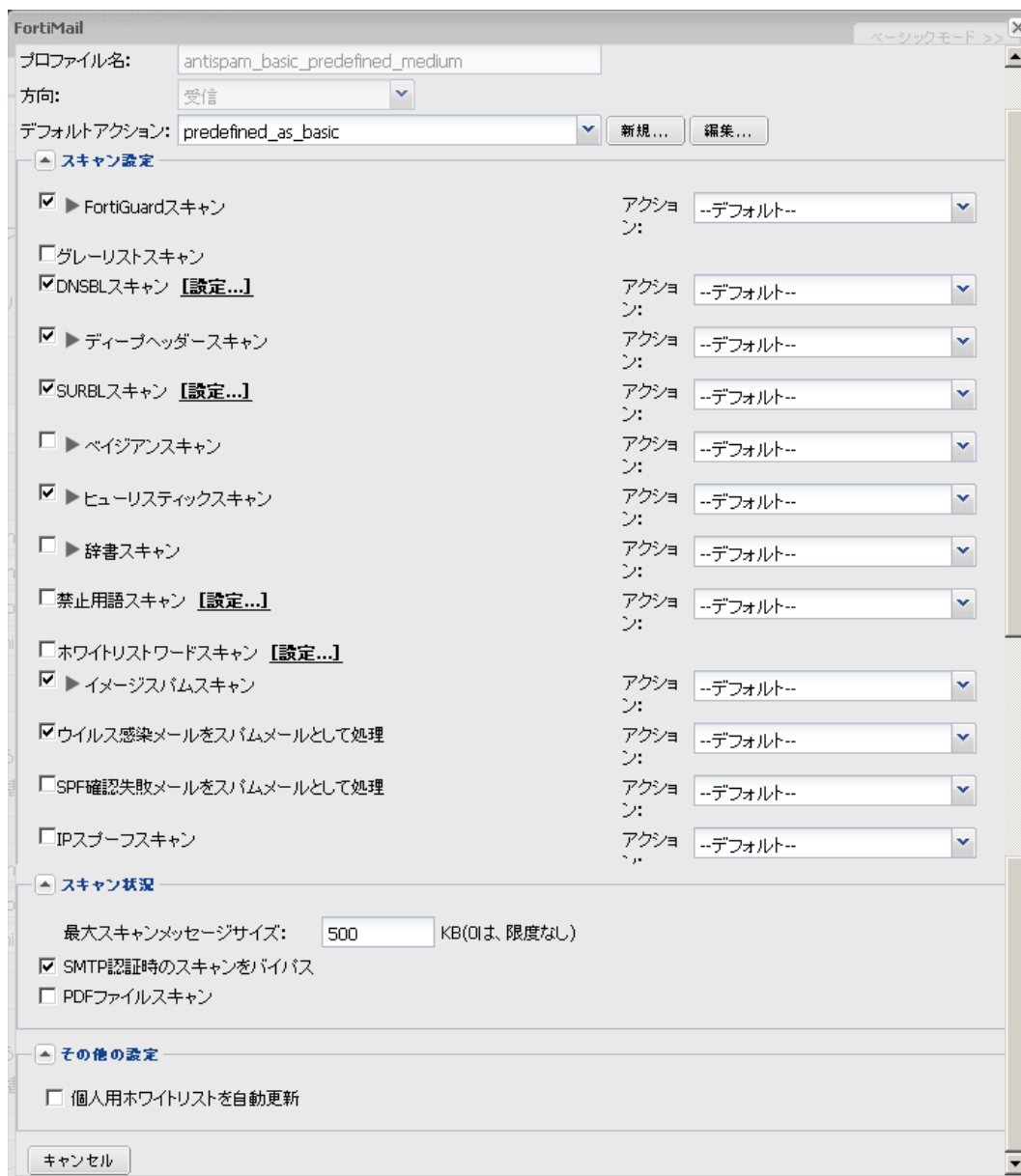


図 44：管理者画面 - 受信者ポリシーにおけるアンチスパムプロファイル設定画面

これらのスキャンの結果、スパムと判定されたメールに対するアクションは、下記より設定できる。

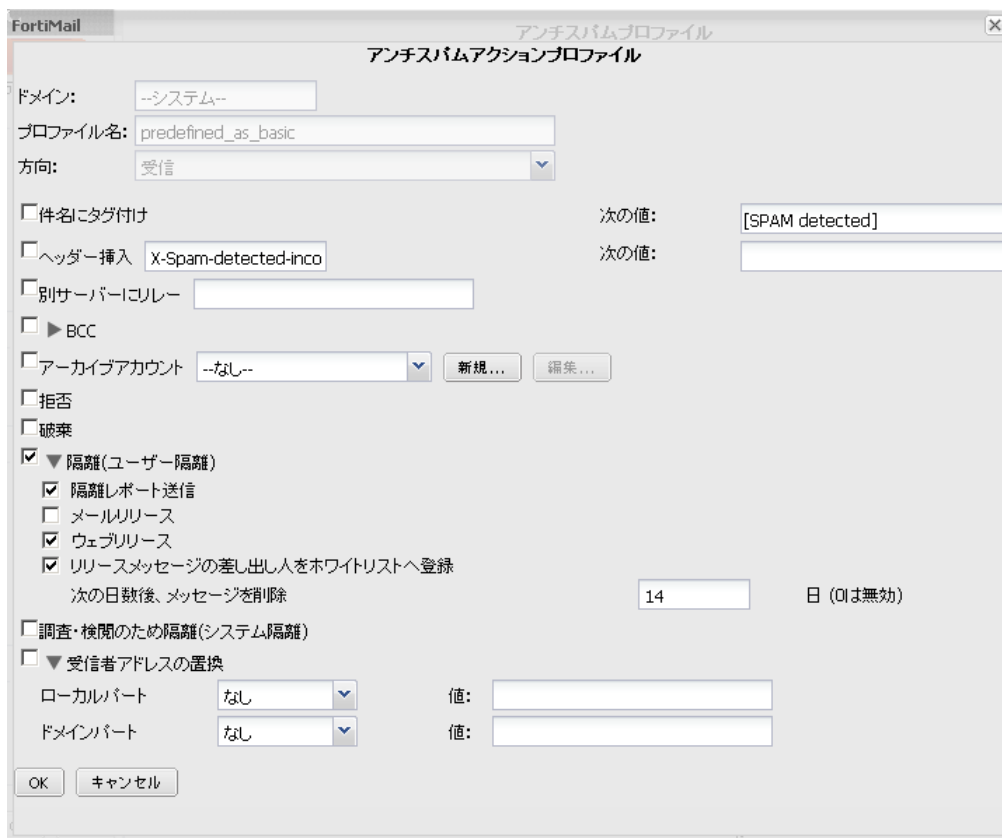


図 45 : 管理者画面 - 受信者ポリシーにおけるアンチスパムアクションプロファイル設定画面

コンテンツプロファイルでは、添付ファイルフィルタリング、ファイルタイプフィルタリング、その他の設定、スキャン条件、コンテンツモニタリングフィルタリングの設定を行える。



図 46 : 管理者画面 - 受信者ポリシーにおけるコンテンツプロファイル設定画面

また、コンテンツアクションプロファイルでは、各コンテンツフィルタに対する動作設定（アクション）をかなり詳細に設定できる。

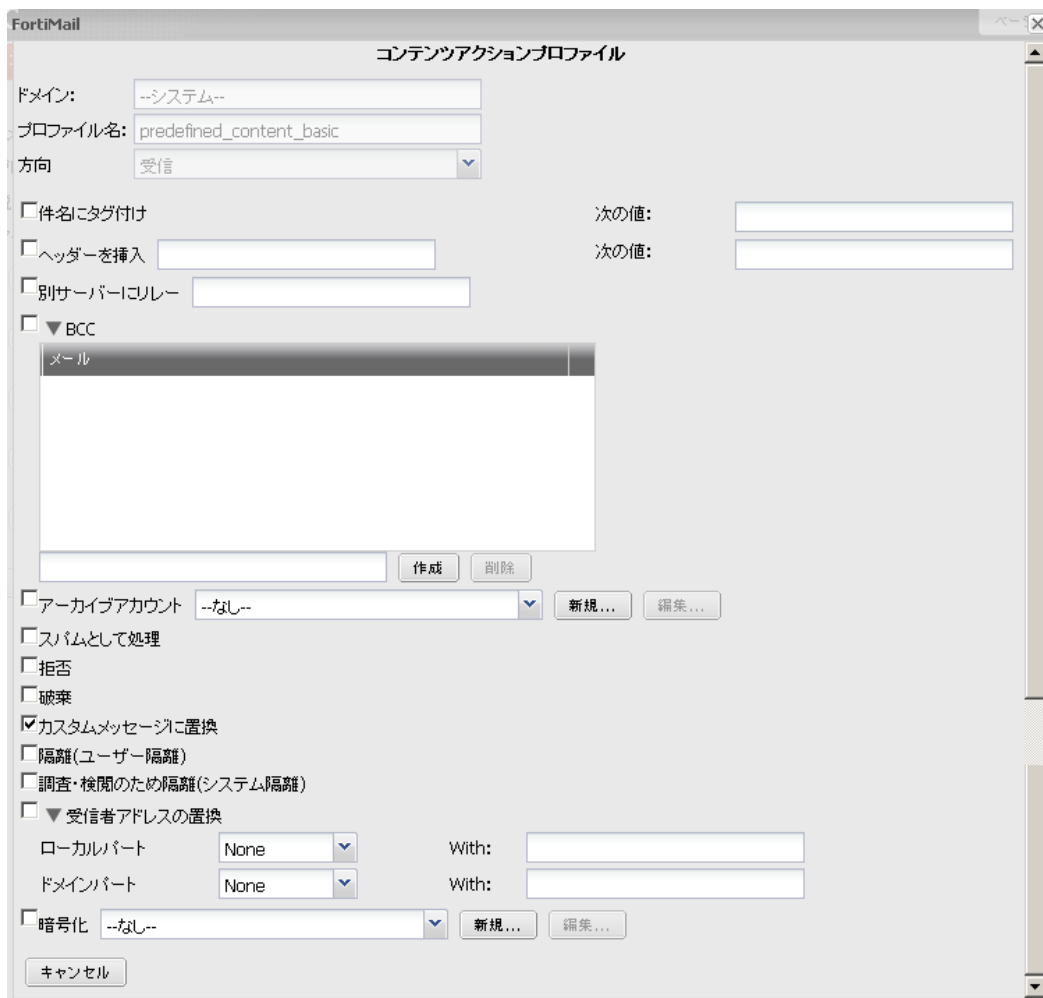


図 47 : 管理者画面 - 受信者ポリシーにおけるコンテンツアクションプロファイル設定画面

## 4.7 プロファイル機能

「FortiMail」では、各種ルールをプロファイルとして設定し、それを各ドメインやユーザーに紐付けてポリシーを作成する方法を取っている。プロファイルは前述までにも出てきたが、「セッション」「アンチスパム」「アンチウイルス」「コンテンツ」「リソース」「認証」「LDAP」「辞書」「セキュリティ」「IP プール」「グループ」といったカテゴリーを用意し、自由度の高いポリシーを設定できる仕組みをとっている。尚、「辞書」プロファイルに正規表現でパターンを登録しておくことで、様々なフィルタルールに利用できる。下記は「コンテンツ」のプロファイル設定画面だが、要件に応じてかなり柔軟に、かつ詳細な設定を行えることが分かる。

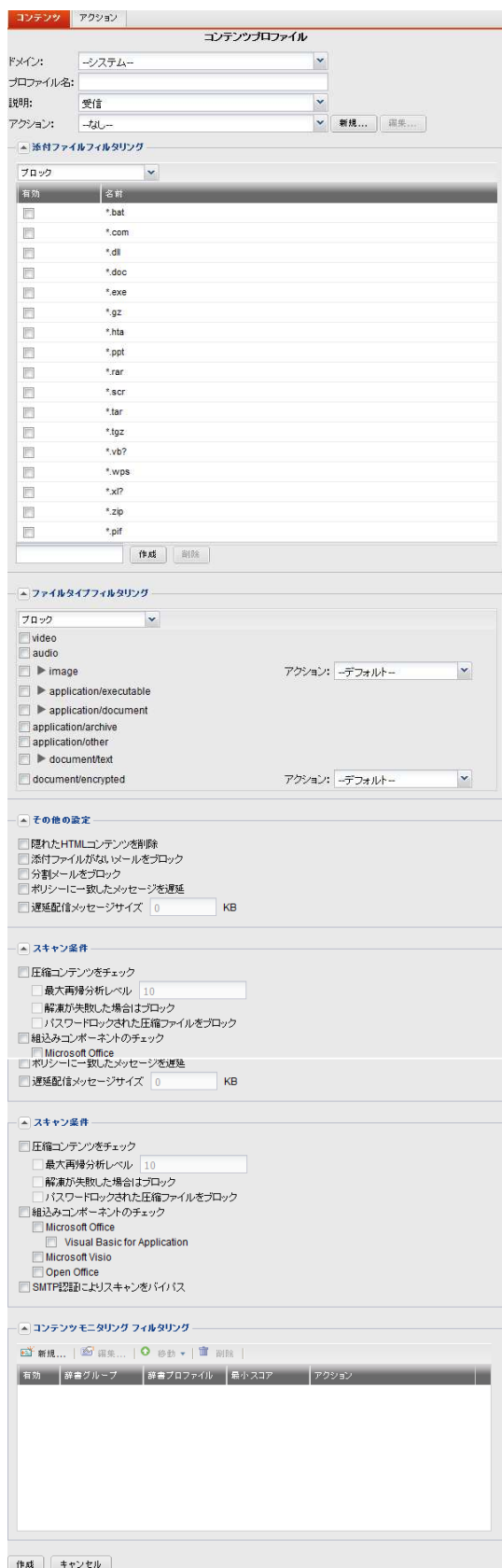


図 48 : 管理者画面 - コンテンツプロフィール設定画面

## 4.8 アンチスパム機能

「アンチスパム」機能では、ポリシー設定で行ったアンチスパムにおける隔離レポート、システム隔離、制御アカウントなどの設定を行う「隔離」、システム・ドメイン・ユーザーそれぞれのブラックリストとホワイトリストの追加・削除やバックアップ/リストアなどを設定する「ブラックリスト/ホワイトリスト」、グレーリストの TTL や期間、除外ルールなどを設定する「グレーリスト」、その他「バウンス検証」「エンドポイント評価」「ベイジアン」などのメニューが用意されている。

図 49 : 管理者画面 - アンチスパム隔離レポート設定画面

## 4.9 メールアーカイブ機能

「FortiMail」には、保存を重視したメールアーカイブを実現する「メールアーカイブ」機能が用意されている。

「メールアーカイブ」では、アーカイブアカウントを作成し、そのアカウントに対象メールを転送する方法を取っている。アーカイブをローテーションさせるサイズや期間などの指定、アーカイブ先をリモートの FTP や SFTP に指定することもできる。



図 50 : 管理者画面 - アーカイブアカウント設定画面

次にアーカイブポリシーを作成する。ここで作成したポリシーに合致したメールが、アーカイブされることになる。以上で設定は完了するため、比較的容易にアーカイブを実施できる。



図 51 : 管理者画面 - アーカイブポリシー設定画面

尚、アーカイブされたメールは、管理者画面の「モニタリング」のアーカイブから確認する。



arc02 を選択



Inbox を選択



図 52 : 管理者画面 - アーカイブ閲覧画面

アーカイブしたメールを選択し、表示ボタンをクリックすると、メールを閲覧できる。送信ボタンをクリックすると、arc02 アカウントからメールを送信することもできる。また、mbox 形式か tarball でエクスポートすることもできる。

アーカイブしたメールの検索は、メールボックスを選択し、画面上部の検索ボタンをクリックすると、検索条件を管理する画面が表示される。指定できる条件は、From、To、CC、件名、文字列、時間で、複数の条件を指定した場合は AND と OR を指定することができる。また、様々な検索条件を登録しておくことで、毎回検索条件を入力する手間が省くことができる。

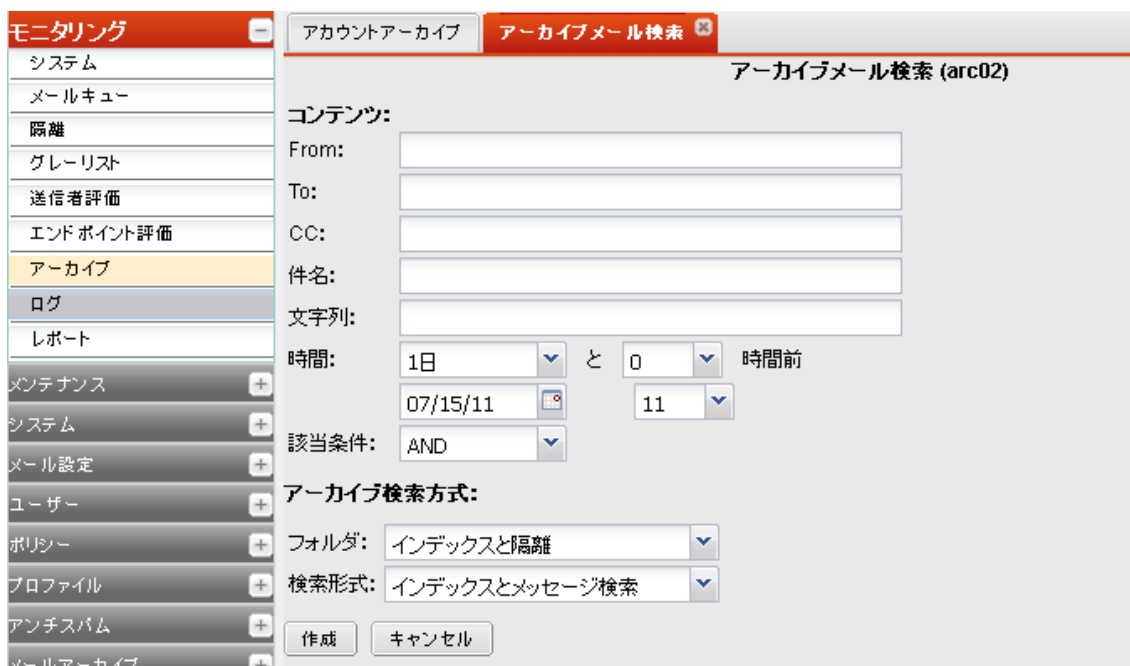


図 53 : 管理者画面 - アーカイブ検索画面

#### 4.10 ログとレポート機能

「FortiMail」の運用・管理を行う際のログ及びレポート機能を用意。ログ設定では、ローカルに保存するログ設定と、リモートにロギングする `syslog` 設定が行える。ここで設定したログは、モニタリングメニューから閲覧できる。

また、レポート設定では、膨大なクエリの中から任意のものを選んで、スケジュール設定を行い、指定したメールアドレスに対して、HTML 形式か PDF 形式のレポートを送ることができる。メールアドレスを指定しない場合は、モニタリング画面から HTML 形式のレポートを閲覧することができる。

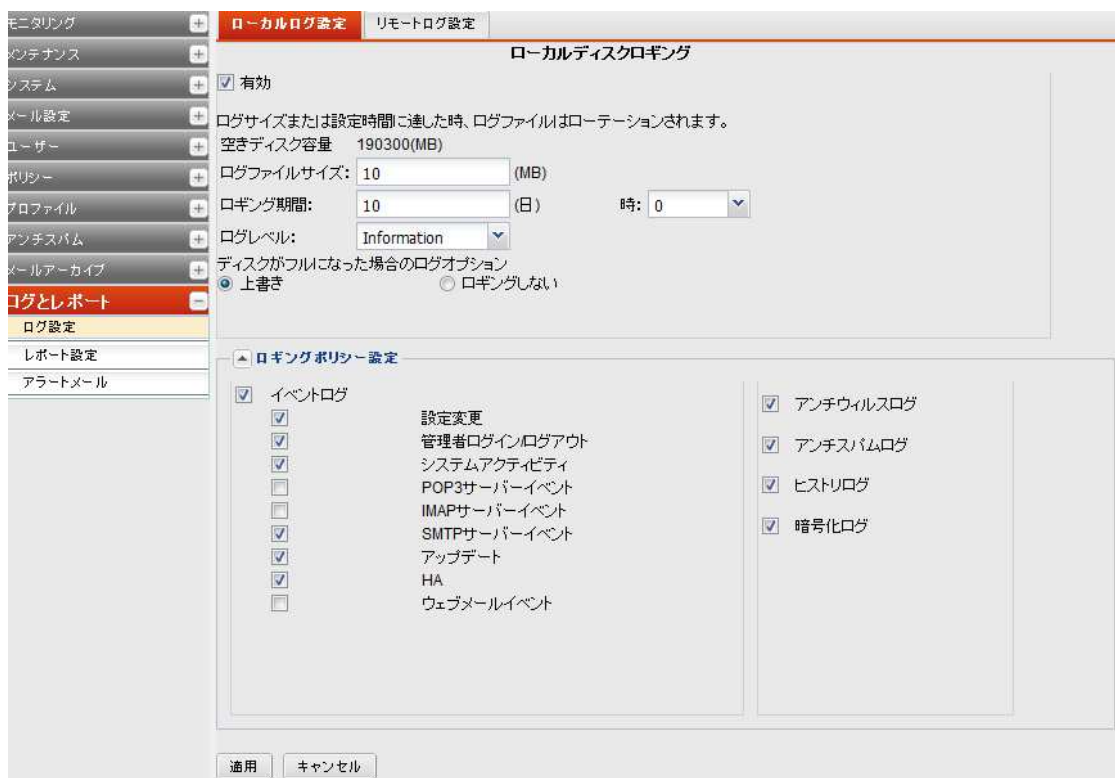


図 54 : 管理者画面 - ログ設定画面

### 【検証者のコメント】

「FortiMail」自体が、オールインワンで下記機能を全て提供するため、非常に多機能であった。一方で、多機能製品であるがために、それぞれの機能を全て本格的に利用する場合は、設定に若干時間を要するよう感じた。

- ・ アンチスパム
- ・ アンチウイルス
- ・ メールサーバー
- ・ Web メール
- ・ フィルタリング
- ・ アーカイブ
- ・ 暗号化
- ・ アプライアンス及び運用に関わる全般の設定

しかし、「FortiMail」は非常に柔軟性の高い設定ができるため、お客様側で予めメールシステムの運用ポリシーが決まっており、その内容で運用することが決まっている場合は、プロファイ

ルとアクションを定義し、それらを各設定画面で指定するという、内容を落とし込むだけの作業となる。プロファイルやアクション設定についても、デフォルト設定をコピーして簡単に作成できる。このプロファイルを利用した運用に慣れれば、様々なことに対応できるメールシステムとして利用できるようになる。

また、LDAP や RADIUS、NAS などの外部サーバーとの連携機能も豊富で、「FortiMail」1 台で既存のシステムと連携した一元管理、及びメールシステムのリプレース需要などに対応しやすい一面を持っていると言えるだろう。

## 5. 総評

---

アプライアンスと言えば、スパム対策製品というイメージが強いが、今回はアンチスパム、アンチウイルス、メールサーバー、Web メール、フィルタリング、アーカイブ、暗号化、アプライアンス及び運用に関わる全般機能を全て提供する、オールインワンのメールシステムアプライアンスの評価を行った。

日本だけでなく、ワールドワイドで多くの導入実績を持つ UTM 「FortiGate」で、アンチウイルス・アンチスパム機能、アプライアンス及び運用に関わる機能に関しては長年強化されてきている。特に、運用部分ではソフトウェアとハードウェアを個別に導入することを考えると、「FortiMail」は導入・運用・管理面で圧倒的に使いやすく、コストメリットがあることが分かった。問題は、それ以外の機能がどれほどのレベルで提供されているかであった。

初期設定の際にはウィザードが用意されているため、こちらは容易に作業が完了した。

利用者向け機能では、Web メールやカレンダー、アドレス帳を提供していたが、Web メールはシンプルで機能が少ない反面、軽快に動作し、クライアントメーラーに遜色ないほどスピーディーに利用できるのも、外出先からメールを利用する際には適しているのではないだろうか。また、カレンダーには、本格的な機能が実装されているので、社内のスケジュール管理で十分に利用できると感じた。暗号化については、最近ではパスワード付 ZIP 化が流行っているのも、強固な暗号化ニーズが少なくなっているが、本格的な暗号化を手軽に実施したいという要望に対しては、IBE 暗号で十分運用できる。

管理者向け機能では、多機能かつできることが多いため煩雑な設定が必要になりそうだが、プロファイルを上手く使い、初期設定時にある程度運用ポリシーを固めることができれば、様々なお客様の要件を満たすことのできる製品になり得る。特に、フィルタリングは詳細まで設定することができ、アーカイブは簡易コンプライアンス対策として保存と確認を目的とするものであれば、十分に運用できるものとなっていた。

今後、Web メール機能が強化されれば、文句の付けどころのない製品になる。中小・中堅企業におけるメールシステムとして、多くのお客様にとって良いソリューションとなることを期待したい。

以上