GIDEON

ユーザーズ
ガイド

for Linux

ギデオン
ゲートウェイセキュリティ

はじめに

この度は、『ギデオン ゲートウェイセキュリティ』をお買い上げいただきまして誠にありがとうございます。本ユーザーズガイドは、製品概要、インストール方法、各種設定方法、導入後の運用上の注意事項などを説明しています。

対象読者は、システムのインストールを行う方、システム管理者、ネットワーク管理者です。本製品の運用・管理を行うには、Linuxの基礎知識およびシステム管理の経験が必要になります。ご使用前に必ずご一読いただきますようお願いいたします。

■　テスト用ウイルスファイルについて

本製品には、ウイルス検出機能のテスト用に、無害なウイルスファイルsample/eicar.comが収録されています。
このファイルをメールに添付して送信することで、実際にウイルス検出が行われていることを検証できます。
テスト用ウイルスファイルは、ウイルス検出機能の動作検証にのみご利用ください。その他の目的でご利用になられた場合、お客様の責任になりますので、ご注意ください。

目次

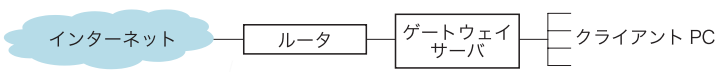
第1章 製品の使用に関して

1.1 製品の概要

近年、スパムメールの増加に伴う業務効率の低下や、メールに添付されるコンピュータウイルス、スパイウェアによる情報漏洩など、社内データの電子化が進む反面、セキュリティを脅かす危険度は年々上がっています。

『ギデオン ゲートウェイセキュリティ』(以下、ゲートウェイセキュリティと省略)は、企業のLinuxゲートウェイサーバにアンチスパム機能、アンチウイルス機能を追加するソフトウェアです。SMTP、POP3、HTTP、FTPの各プロトコルを監視し、スパム判定・転送のほか、ネットワーク経由のウイルス、スパイウェアの侵入・流出を検知し、駆除します。
スパムメール低減とネットワーク経由のウイルス感染を防止し、安心できるネットワーク環境を提供します。

設置・構成例



1.2 導入からライセンス更新の流れ

本製品の導入から運用・保守、ライセンス更新までの流れは以下のとおりです。

● 導入

① ユーザ登録およびパスワード発行
製品CDに収録されたREADMEファイルに従って、ユーザ登録を行ってください。ユーザ登録が完了すると、「お客様登録No」「パスワード」が発行されます。

② インストール
マシン環境を整え、製品をサーバにインストールします。

③ 管理画面から各種設定
「3.6.1 基本設定」の記載に従い、発行された「お客様登録No」および「パスワード」を設定してください。その後「3.6 共通設定」の記載に従い、その他の設定を行ってください。

④ 動作確認
「第4章 動作確認」の記載に従い、製品CDに収録されたサンプルウイルスを用いて動作確認を行ってください。

● 運用・保守

① 定義ファイルの自動更新
「3.4 更新状況」の記載に従い、更新が正常におこなわれていることを随時確認してください。

② ウイルス検出・処理
「3.5 検出状況」の記載に従い、日常の運用・管理を行ってください。

● ライセンス更新

本製品は1年ごとのライセンス更新が必要です。更新期間が近くなりましたら、ご案内を差し上げます。

1.3 本製品の特長･機能

■ 本製品の特長

- スパムメール対策、ウイルス対策の統合ソフトウェア
- GUI管理画面から設定可能
- クライアントPCの設定変更が不要
- 定義ファイル、モジュールの自動更新でメンテナンスフリーの運用

■ アンチスパム機能

- スパムメールの検知率95%
- メールヘッダ解析、メッセージの本文解析、メールシグネチャデータベース、DNSルックアップ、URLデータベース解析、ユーザ定義（ホワイトリスト、ブラックリスト）などによる複合解析
- スパムメール転送機能
- スパム判定スコアのカスタマイズ
- スパム検出ログ、各種サービスログのダウンロード

■ アンチウイルス機能

- あらゆる圧縮形式（約900種類以上）／255階層の多段圧縮に対応
- メールでの通知機能
- ユーザ、またはドメイン名毎にウイルスチェックのOn/Offが可能
- Kaspersky社製のコアエンジンを組込み、ウイルスを完全に検出、駆除（約25万種のウイルスパターン(2006年11月現在)、新種ウイルスに数分間隔で対応）

1.4 推奨動作環境（2010年4月現在）

注意

ご購入いただいたソフトをインストールする前に、ご利用環境を確認してください。以下の使用条件を満たさない場合は、インストールしたソフトが正しく動作しない可能性がありますのでご注意ください。使用条件などの最新情報は、下記のURLを参照してください。

URL: http://www.gideon.co.jp/products/

- 対応Linuxディストリビューション

  RedHat Enterprise Linux AS/ES/WS（Version 3/4/5）
  CentOS 4/5
  Turbolinux 10/11 Server
  TurboLinux Appliance Server 2.0/3.0
  など、主要なRedHat互換OS（インテルアーキテクチャ）。

  上記に含まれていないディストリビューションでも動作実績がある場合があります。ギデオン インフォメーションセンターにお問い合わせください（連絡先は巻末に記載）。

- Linux のコマンドiptables が動作すること

- 推奨メモリサイズ 約512MB以上

- ハードディスク空領域512MB程度（インストール直後は必要ありませんが、定義ファイルやログなど、運用上将来の使用率増加を見積もった空き領域を確保してください）

後述のGUI管理画面を使用するにはクライアントPCのブラウザにFlash Playerバージョン7以降がプラグインでインストールされている必要があります。Flashのバージョンが古い場合、GUI管理画面の表示が文字化けしたり、ボタンが正しく動作しません。

1.5 インストール対象サーバ環境

本製品をインストールするサーバでは以下の要件を備えている必要があります。

● Linuxで構築されたゲートウェイサーバが正常に稼動していること
本製品を導入するゲートウェイサーバが正しく稼動していることを確認してください。

● iptables が動作する環境
インストール時にiptablesが動作しない場合、インストールに失敗します。

● サーバとして正常に動作する容量、処理能力を備えていること

ウイルス検出のため一時的にメール文書の容量が必要になります。ディスクまたはメモリに、プロセス同時起動分の容量を確保してください。また、ウイルス検出のための処理負荷が増えます。
推奨メモリサイズは、約512MB以上です。

1.6 インストール後のシステム環境

インストールが完了すると、iptables起動スクリプトを変更します。
アンインストール時には、元のiptables起動スクリプトに戻します。

1.7 システムバージョンアップによる更新の注意

本製品を導入したサーバに対して、前記ソフトのバージョンアップやパッチ更新を行う場合、以下の点にご注意ください。

前記ソフトをアップデートすると、設定ファイルなどが置き換えられ、本製品のインストール時に設定した項目が消去され、ウイルス検出機能が無効になる可能性があります。
前記ソフトのアップデートは、本製品を一旦アンインストール（後述）してから行ってください。その後、サーバが正常に動作していることを確認してから、本製品を再インストールし、再度、動作確認をしてください。

注意

サーバのプログラムだけでなく、サーバの設定ファイルだけ変更する場合も同様の手順になります。

1.8 インターネット接続による更新の注意

定義ファイルおよびモジュールは、インターネット上のサイトから更新しますが、ネットワーク上のフィルタリングやファイヤーウォールの設定（または設定変更）により、更新ができなくなることがあります。導入後およびネットワークの設定を変更した場合には、更新が正常に行われることを確認してください。

1.9 ご利用上の注意

本製品をご利用いただく上で、以下の点にご注意ください。

● 定義ファイルの更新
定義ファイルは自動更新されますが、逐次バージョンが最新になっていることを確認してください。定義ファイルのバージョンが古い場合、最近発生したウイルスやスパムが検知されない恐れがあります。バージョンの確認方法については後述します。

● 容量管理
ディスク容量やメモリ容量不足など、システムの資源がなくなった場合は、正しく動作しない可能性があります。必要な容量を確保してください。

以下のような場合には、ご使用の規模により、「アンチスパム・アンチウイルス」の機能が正常に動作しないことがあります。問題が発生した場合、すぐにギデオン サポートセンターにお問い合わせください。

● スペックが低いマシンでは、サーバ負荷が異常に上がったとき、正しく動作しない場合があります。CPUのスペックアップとディスクI/Oの転送速度を向上させることをお勧めします。

● ご使用のOSが古い場合、処理するプログラムが多いとシステム上の制限によりウイルススキャンのプロセスが最後まで正常に完結しない場合があります。その場合OSのアップデートまたはシステム設定の制限値の調整など、チューニングが必要になります。システム管理者にご相談ください。

● 本製品はスパムメール、ウイルス感染の危険を最小限にとどめるために有効なソフトです。しかし、これまでに述べたような理由や予期できない原因により、スパムメール、ウイルス感染を100%排除するものではない点にご留意ください。

第2章 インストール・アンインストール

各製品のインストール ・アンインストールの方法について説明します。

Linux ディストリビューションにより、インストールパッケージが異なりますのでご注意ください。

RPM パッケージ　：RedHat、SuSE、Turbolinux など
DEB パッケージ　：Debian など
TGZ パッケージ　：Slackware など

注意

インストール前の確認：
Linux サーバが正しく稼動していることを確認した後、以下の手順で本製品をインストールします。

また、CD-ROM ドライブの有無、ファイル転送方法の違いにより、インストールの手順が異なります。以下のいずれかの手順でインストールの準備をしてください。

CD-ROMドライブ付きマシンへインストールする

《手順1》製品CD をドライブに入れる

《手順2》ログイン名およびパスワードを入力する

(1) root ユーザでログインしてください。
(2) 一般ユーザでログインしている場合は、スーパーユーザで操作してください。

以下のようにイタリックの部分を入力して、Enter キーを押しパスワードを入力することで、ルート権限でログインできます。

```
server~>su -
```

《手順3》製品CD をマウント（読込み可能に）する

CD のマウントについては、システムのコマンドを参照してください。
例えば、以下のようにイタリックの部分を入力して、Enter キーを押します。

```
server:~#mount /mnt/cdrom
```

CDをマウントした後、お使いのディストリビューションに合ったパッケージをインストールします。各製品のインストール方法をご覧ください。

インストール終了後、CD をアンマウントしてください。アンマウントについては、システムのコマンドを参照してください。
例えば、以下のようにイタリックの部分を入力して、Enter キーを押します。

```
server:~#umount /mnt/cdrom
```

Windowsクライアントからサーバにインストールする

以下に例説します。インストール先のサーバ名は「av」とします。
まず、LAN 上（またはクロスケーブルで直接接続）で、クライアントマシンとavサーバが通信できるようにします。クライアント（Windows）マシンに製品CDを入れ、以下の手順でインストールします。

《手順1》DOS プロンプトを表示する

Windows のスタートメニューをクリックして、[ファイル名を指定して実行] を選択します。「ファイル名を指定して実行」画面の「名前」に「command」と入力して、[OK] ボタンをクリックします。
または「アクセサリ」から「コマンドプロンプト」を開いてください。
表示された画面に、CD が入っている「ドライブ名:」（例えば、E:）を入力します。

《手順2》製品CD のインストール用ファイルを確認

CD の内容を参照し、以下のファイル名および0 バイトでないことを確認し、システムに応じたインストール用ファイルを転送します。

・RPM パッケージ　：RPM-gav-gproxy-antispamplus.tgz
・DEB パッケージ　：DEB-gav-gproxy-antispamplus.tgz
・TGZ パッケージ　：SH-gav-gproxy-antispamplus.tgz

《手順3》ファイルをav に転送

以下のようにイタリックの部分を入力して、《手順2》で確認したファイルをftpでav に転送します。

```
E:\>ftp av
```

次に、「ユーザアカウント」および「パスワード」を入力した後、以下を行います。
以下のようにイタリックの部分を入力し、ファイルを転送します。


```
ftp>binary
200 Type set to I.
ftp>cd /tmp
ftp>put パッケージ名
ftp>ls
ftp>quit
```

《手順4》telnet でログインする

以下のようにイタリックの部分を入力します。

```
E:\>telnet av
```

av にtelnet でログインします。
続いて、「ユーザアカウント」および「パスワード」を入力後、以下のようにイタリックの部分を入力します。

```
$su
Password:********
#cd /tmp
```

インストールするパッケージをサーバに転送しログインした後、インストールを行います。各製品のインストール方法をご覧ください。

インターネットからファイルを取得しインストールする

《手順1》サーバにログインする

サーバにルート権限でログインし、/tmp ディレクトリに移動します。

《手順2》インストールするパッケージをダウンロードする

以下のコマンドで、インストールするパッケージをダウンロードします。

```
# wget http://download.gideon.co.jp/ファイル名
```

注意

ダウンロードするパッケージは、「Windows クライアントからサーバにインストールする」の《手順2》に記載のファイルを参照してください。

2.1 ギデオン ゲートウェイセキュリティ のインストール

● CD-ROMからインストールする場合、以下のコマンドを入力します。

RPM パッケージ

```
# /mnt/cdrom/RPM-gav-gproxy-antispamplus install
```

DEB パッケージ

```
# /mnt/cdrom/DEB-gav-gproxy-antispamplus install
```

TGZ パッケージ

```
# /mnt/cdrom/SH-gav-gproxy-antispamplus install
```

● 「Windowsクライアントからサーバにインストールする」、「インターネットからファイルを取得しインストールする」の場合は、/tmp ディレクトリに移動した後、以下のコマンドを入力します。

RPM パッケージ

```
# tar zxvf RPM-gav-gproxy-antispamplus.tgz
# ./RPM-gav-gproxy-antispamplus install
```

コンソールに画面2.1のように、メッセージが表示されます。これでインストールは完了です。

```
# ./RPM-gav-gproxy-antispamplus install
======== RPM-gav-gproxy-antispamplus
---- Executing 'rpm -ihv /home/admin/./packages/gav-common.i386.rpm' command.
Preparing...                ########################################### [100%]
   1:gav-common             ########################################### [100%]
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
                        :
                     (中略)
                        :
Starting kas-license ... done
Starting ap-process-server ... done
Stopping gproxy-smtp: [  OK  ]
Starting gproxy-smtp: [  OK  ]
Stopping gproxy-pop: [  OK  ]
Starting gproxy-pop: [  OK  ]
----------------------
Installation SUCCEEDED.
----------------------
```

画面2.1

DEB パッケージ

```
# tar zxvf DEB-gav-gproxy-antispamplus.tgz
# ./DEB-gav-gproxy-antispamplus install
```

[注意] インストール途中でソフトウェアを最新の状態に更新するために、コンソールに

Now, update? [Y/n]

と表示されますので、必ず “y” を入力してください。上記表示に “y” を入力しますとソフトウェアを最新版に更新する処理が実行されますので、終了までに10 分程度の時間がかかります。コンソール画面に上記メッセージが表示されずにインストール動作が終了してしまった場合は、弊社までお問合せ下さい。

TGZ パッケージ

```
# tar zxvf SH-gav-gproxy-antispamplus.tgz
# ./SH-gav-gproxy-antispamplus install
```

● パッケージファイルの削除

以下のようにイタリックの部分を入力して、パッケージファイルを削除します。

```
# cd /tmp
# rm -f packages/gav*
```

「お客様登録No」「パスワード」の設定

「3.6.1 基本設定」を参照して「お客様登録No」「パスワード」を設定してください。

※上記設定後、モジュール更新を押すことによりアンチスパム広告画面から設定画面に切り替わります。
※「パスワード」等が設定されていない場合、定義ファイルの更新が行われません。必ずこの手順を実行してください。

注意

CD-ROMドライブが無く、インターネットに接続していない場合は、前述の「CD-ROMドライブがないマシンの場合の手順」で、CD-ROMからファイルを転送後、インストールを行ってください。

2.2 インストール時のシステム変更

ゲートウェイセキュリティをインストールする際に、次の項目が実行されます。それによりシステムの変更などが生じます。

1. iptables の起動スクリプト /etc/init.d/iptables の書き換え
2. /etc/GwAV のディレクトリ下に設定ファイルを追加
3. /usr/local/gwav のディレクトリ下に主要なモジュール、定義ファイルを追加
4. /var/log/gwav のディレクトリ下にログ関連ファイルを追加
5. /usr/local/ap-mailfilter のディレクトリ下にスパム構文解析モジュール、スパムデータベースを追加

2.3 アンインストール

本製品のアンインストールは次の手順で行います。まず、root 権限でログインし、それぞれのパッケージに合わせたコマンドを入力し、Enter キーを押します。

RPM パッケージのアンインストール

```
# /etc/GwAV/uninst/RPM-gav-gproxy-antispamplus uninstall
```

DEB パッケージのアンインストール

```
# /etc/GwAV/uninst/DEB-gav-gproxy-antispamplus uninstall
```

TGZ パッケージのアンインストール

```
# /etc/GwAV/uninst/SH-gav-gproxy-antispamplus uninstall
```

注意

アンインストールする際は、あらかじめゲートウェイセキュリティを停止し、処理が完了していることを確認してから実行してください。

第3章 アンチウイルス設定

管理GUI用サービス起動と停止

管理画面を利用するためのサービスを起動するには、インストール後、root権限でログインし、以下のイタリック部分のコマンドを実行します。

```
# /usr/local/gwav/gwav-gui-control
==== GUI setting ====
  Use web-interface for anti-virus □Yes/No□ [No]: y
Starting mini_httpd:                                       [  OK  ]
Starting mini_httpsd:                                      [  OK  ]
------------------------------------------------------------------
```

このサービスを停止するには、上記「y」に替わり「n」を入力します。

管理・設定画面のアクセス方法

クライアントPCから本製品がインストールされたシステムのGUI管理画面にアクセスします。WEBブラウザのアドレスバーで、以下のようにシステムのホスト名またはIPアドレスとポート番号（777）を指定します。

http://antivirus.gideon.co.jp:777/

セキュリティが気になる場合は、HTTPSでポート番号（999）を指定します。

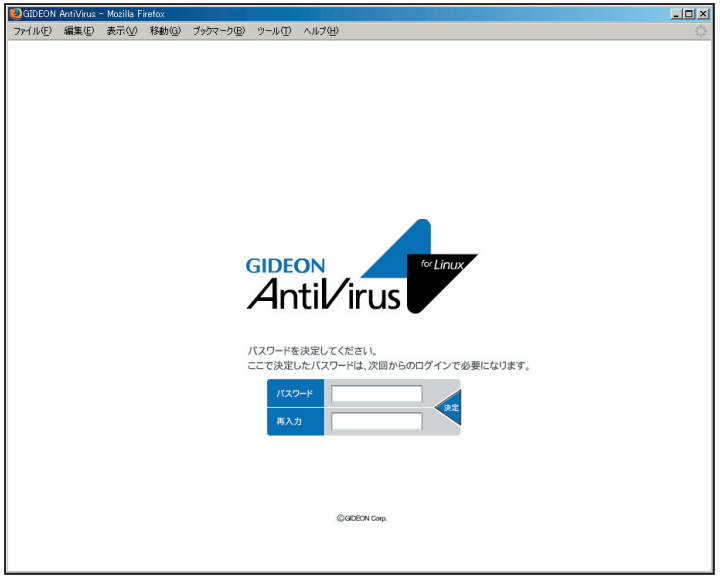
https://antivirus.gideon.co.jp:999/

※ お使いのWEBブラウザおよびファイヤーウォールで、上記のポート番号を許可するように設定してください。また上記ポートにアクセスするには、本製品インストール後に、システム上で必要スクリプトを実行し、ウェブサーバサービスを起動させておく必要があります。

3.1 初回のログイン

ゲートウェイセキュリティを導入後、はじめて管理・設定画面にアクセスすると、画面3.1パスワード設定画面が表示されます。

次回からログインするときには、ここで設定されたパスワードを入力する必要があります。



画面3.1

3.2 ログイン

管理･設定画面にアクセスすると、画面3.2 ログイン画面が表示されます。
初回のログインで設定したパスワードを入力します。パスワード入力後［ログイン］ボタンをクリックします。

パスワードの変更

既存のパスワードを入力して［変更］ボタンをクリックします。
画面3.1が表示されます。初回のログインと同様にパスワードを再設定します。
(半角英数20文字以内)

画面3.2

3.3 概説

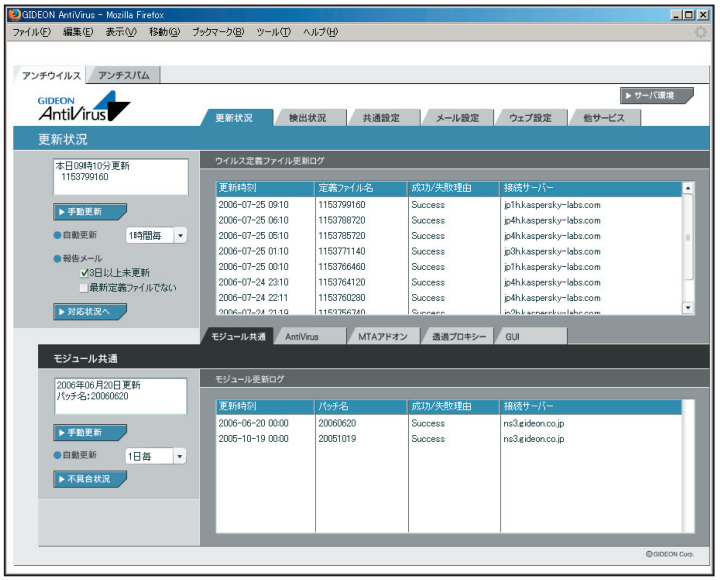
ログインすると、画面3.3 管理･設定画面が表示されます。
ここでは管理･設定画面の各メニューについて説明します。

■主に日常の管理で必要なメニュー

タブ名	説　明
更新状況	ウイルス定義ファイルや更新モジュールが自動更新され、その更新状況を一覧表示します
検出状況	検出ウイルスの履歴情報を一覧表示します
サーバ環境	負荷やエラーメッセージなどの状況を表示します

■初期に設定及び確認するメニュー

タブ名	説　明
共通設定	ライセンス(お客様登録No, パスワード)の設定を確認します HTTPプロキシ経由で更新する場合の設定を行います 警告メールの送信先メールアドレスの設定を行います
メール設定	警告メールなどのメッセージのカスタマイズを行います
ウェブ設定	ウイルスをチェックしないファイルを確認します



画面3.3

3.4 更新状況

●ウイルス定義ファイル更新ログ（画面3.3 上段部分）

最新のウイルスに対応する、定義ファイルの更新状況を表示します。

［手動更新］ボタンをクリックすると、その時点で最新の定義ファイルの取得を行います。既に更新済みの場合は、新たに更新されません。

自動更新の頻度は、初期設定では1時間毎に設定されています。緊急対策が必要な場合は手動更新を行ってください。

［対応状況へ］ボタンをクリックすると、最新のウイルス情報に関する情報サイトを表示します。

●モジュール更新ログ(画面3.3 下段部分)

［手動更新］ボタンをクリックすると、その時点で最新のモジュール（修正パッチモジュール、アップデートモジュールなど）の取得を行います。既に更新済みの場合は新たに更新されません。

自動更新の頻度は、初期設定では1日1回の更新に設定されています。緊急対策が必要な場合は手動更新を行ってください。

［不具合状況］ボタンをクリックすると、モジュールの不具合などに関する情報サイトを表示します。

個別のモジュール群（AntiVirus MTAアドオン 透過プロキシー GUI）の更新状況は、各タブをクリックすると表示されます。

3.5 検出状況

管理･設定画面の「検出状況」タブをクリックすると、画面3.5が表示されます。

「検出統計情報」では、「本日」「昨日」「今月」「先月」「総合計(検出開始時からの合計)」に分類して、各期間のウイルス検出件数を表示します。
また検出頻度の高いウイルス名を、各期間ごとに表示します。
[月次詳細]ボタンをクリックすると、当月を含め、過去の月のウイルス検出サマリレポートを閲覧できます。また管理者宛にそのレポートを送信することができます。

「検出ログ」では最新の1000件までの検出ウイルスを表示します。

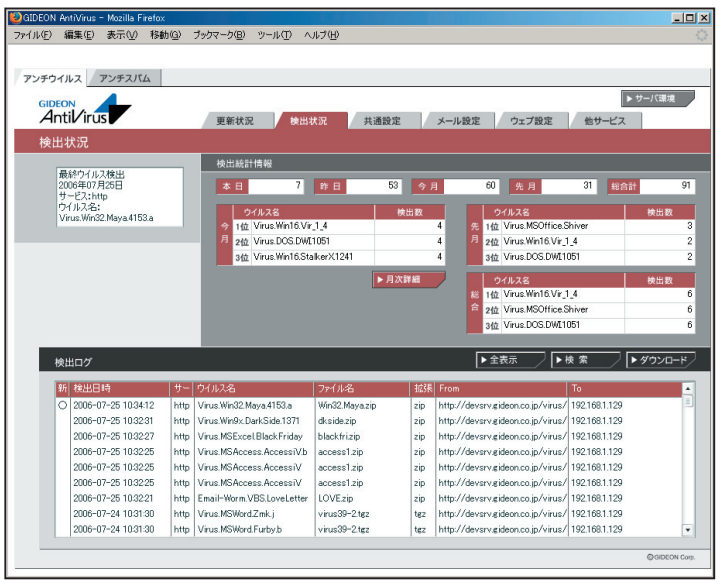
● ダウンロード

検出ログを CSV ファイルとしてダウンロードできます。
検出ログは http/ftp/smtp/pop3 ごとにファイルが別れています。
ダウンロードする際は、『検出ログのダウンロード』 ダイアログ中のリストより選択してからダウンロードボタンをクリックしてください。
ダウンロードした CSV ファイルには各ウイルスが検出された際の詳細な情報が含まれています。

● 詳細情報

検出ログのリストをクリックすることで、 検出された際の詳細な情報が閲覧できます。

[検索]ボタンをクリックすると、表示項目の内容で検索することができます。
[全表示]ボタンをクリックすると、検索表示から元の一覧表示に戻ります。



画面3.5

3.6 共通設定

管理･設定画面の「共通設定」タブをクリックすると、画面3.6.1が表示されます。
各種設定を行った後に[このページを以前の設定に戻す]ボタンをクリックすると、設定の変更をおこなった状態の一つ前の状態に戻します。
[このページを初期設定に戻す]ボタンをクリックすると、このページで設定可能な項目を、初期設定（工場出荷時）に戻します。

3.6.1 基本設定

●ライセンス

「（お客様）登録No」「パスワード」が設定されていることを確認してください。

製品ご購入時に設定されていない場合、またはライセンスを変更された場合には入力が必要となります。
「（お客様）登録No」および「パスワード」を入力後、[更新]ボタンをクリックしてください。

[検証]ボタンをクリックすると、入力された「（お客様）登録No」「パスワード」が正しいかどうか確認できます。誤って入力した場合は再入力してください。

※契約期間が終了している場合には認証できないことがあります。

●管理者のメールアドレス

「報告メール」には、保守運用のための報告メールや管理画面の情報を送信するメールアドレスを記述します。
「警告メール」には、ウイルス検出時の警告メールを送信するメールアドレスを記述します。
複数アドレスを指定する場合、下記のように半角スペースで区切ります。

```
aaa@domain.jp bbb@domain.jp
```

メールアドレスを入力後、[更新]ボタンをクリックしてください。
初期設定値:なし

※ネームサーバーで解決できない内部メールサーバーなどへは送信できない場合があります。

●警告メールに記入するFROMフィールド

警告メールに受信時のメール「From:」に記載される名前とそのメールアドレスを指定します。
「名前部」は、このシステムから送信されたことが判る名前を指定します。
「アドレス部」は、実際にアカウントが存在するアドレスを指定します。
「名前部」および「アドレス部」を入力後、[更新]ボタンをクリックしてください。
初期設定値：
「名前部」なし
「アドレス部」導入システム毎に異なるため、メール返信可能なメールアドレスを設定してください。

画面3.6.1

3.6.2 詳細設定

共通設定画面の「詳細設定」タブをクリックすると、画面3.6.2が表示されます。

●メール送信で使用するSMTPサーバー

警告メールなどを送信するために使うメール（SMTP）サーバーを指定します。
例えば、自社の正式なメールサーバー名（FQDN）が、mail.domain.jpであれば、そのメールサーバー名を指定します。
入力後、［更新］ボタンをクリックしてください。
初期設定値:なし

●テンポラリディレクトリ

ゲートウェイセキュリティが一時的に使用するディスク領域です。絶対パスで指定します。
容量は100MB以上必要とします。
初期設定値:/var/tmp（通常は変更不要）
変更する場合は入力後、［更新］ボタンをクリックしてください。

●エラーとして扱わないAntiVirusエンジンの戻り値

ある特定のエラーで警告メールを抑制する数値を指定します。
入力後、［更新］ボタンをクリックしてください。
初期設定値:なし

●感染メール保存ディレクトリ設定

ゲートウェイセキュリティでは使用しません。

画面3.6.2

3.6.3 更新環境設定

共通設定画面の「更新環境設定」タブをクリックすると、画面3.6.3が表示されます。

ゲートウェイセキュリティはHTTPサイトにアクセスすることで、モジュールおよび定義ファイルを更新します。ゲートウェイセキュリティから特定のHTTPプロキシサーバーを経由しないと外部のURLにアクセスできない場合には、「更新のためにHTTPプロキシーを使用する」を選択してください。

「プロキシーのIPアドレス」「ポート番号」は必須項目です。

「ID」「パスワード」が設定されている場合には、それぞれ入力が必要です。

入力後、[更新]ボタンをクリックしてください。

初期設定値:更新のためにHTTPプロキシーを使用しない

画面3.6.3

3.7 メール設定

管理・設定画面の「メール設定」タブをクリックすると表示されます。SMTPおよびPOP3でのウイルスチェックをする場合の管理・設定をおこないます。

各種設定をおこなった後に[このページを以前の設定に戻す]ボタンをクリックすると、設定の変更をおこなった状態の一つ前の状態に戻します。

[このページを初期設定に戻す]ボタンをクリックすると、このページで設定可能な項目を、初期設定(工場出荷時)に戻します。

「SMTP」は、インターネットやイントラネットで電子メールを送信するためのプロトコルで、ここではそのサービスを意味します。サーバー間でメールのやり取りをしたり、クライアントがサーバーにメールを送信する際に用いられるサービスです。

「POP3」は、インターネットやイントラネット上で、電子メールを保存しているサーバーからメールを受信するためのプロトコルで、ここではそのサービスを意味します。

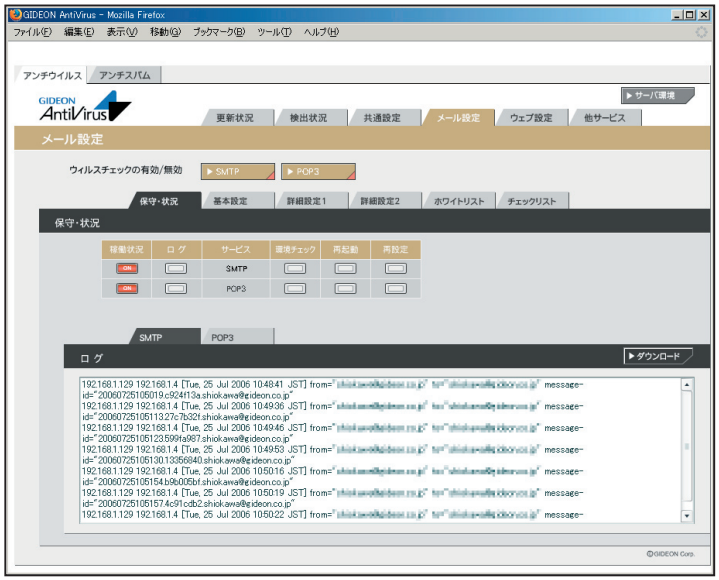
「ウイルスチェックの有効/無効」の[SMTP]または[POP3]ボタンをクリックして次画面で有効または無効を設定します。

[SMTP]ボタン、[POP3]ボタンのそれぞれ右下三角がオレンジ色になっている場合は有効になっている状態です。

3.7.1 保守･状況

メール設定画面の「保守･状況」タブをクリックすると、画面3.7.1が表示されます。

稼働状況　：ONはプロトコルの監視システムが動作しています。
　　OFFは動作していません。
ログ　：最新のログを取得し、下のログ一覧に表示します。
サービス　：SMTPまたは POP3 のサービス。
環境チェック　：該当ボタンをクリックすると、システムの詳細情報を表示します。[管理者に結果を送信する]ボタンをクリックすると、表示されている内容を管理者宛に送信します。
再起動　：サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力されている)の場合にクリックします。
再設定　：サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生している場合にクリックします。
SMTP - ログ - ダウンロード
　：ダウンロードボタンをクリックすることで、SMTPのアクセスログがダウンロードできます。ダウンロードする際は、『SMTPログのダウンロード』ダイアログ中のリストより選択してからダウンロードボタンをクリックしてください。
POP3 - ログ - ダウンロード
　：ダウンロードボタンをクリックすることで、POP3のアクセスログがダウンロードできます。
　ダウンロードする際は、『POP3ログのダウンロード』ダイアログ中のリストより選択してからダウンロードボタンをクリックしてください。



画面3.7.1

3.7.2 基本設定

メール設定画面の「基本設定」タブをクリックすると、画面3.7.2が表示されます。

●受信者への警告メール設定

メールがウイルスに感染していた場合、メールの受信者に送信する警告メールについての設定です。

挙動　：警告メール送信する場合、「警告メールに感染メールのヘッダーを添付する」または「警告メールのみを送信する」の選択ができます。
メールヘッダーには送信経路などの情報が含まれています。

Subject　：警告メールのサブジェクト名と感染メールSubject(元メールのサブジェクト)を連結することができます。

本文　：置換文字列を使用して、警告メール本文に感染メールの情報を表示することができます。

(置換文字列)	(表示内容)
__SUBJECT__	：感染メールSubjectを表示します。
__VIRUS_SENDER__	：送信者のメールアドレスを表示します。ただし、詐称されている場合もあります。
__MESSAGE_ID__	：感染メールMessage-Idを表示します。
__MESSAGE_HEADER__	：感染メールのヘッダー全てを表示します。

入力後、[更新]ボタンをクリックしてください。
初期設定値：感染メールの場合、警告を付けてメールを送信する

●送信者への警告メール設定

メールがウイルスに感染していた場合に、メールの送信者に送る警告メールについての設定です。
ウイルス感染メールは、送信者のメールアドレスを詐称している可能性が高い

ため、警告メールを送信した場合スパムのように扱われることがあります。
したがって「送信者に警告メールを送信しない」設定を推奨します。

Subject　：警告メールのサブジェクト名と感染メールSubject(元メールのサブジェクト)を連結することができます。

本文　：置換文字列を使用して、警告メール本文に感染メールの情報を表示することができます。

(置換文字列)	(表示内容)
__SUBJECT__	：感染メールSubjectを表示します。
__VIRUS_SENDER__	：送信者のメールアドレスを表示します。

入力後、[更新]ボタンをクリックしてください。
初期設定値：送信者に警告メールを送信しない

画面3.7.2

3.7.3 詳細設定1

メール設定画面の「詳細設定1」タブをクリックすると、画面3.7.3が表示されます。

●チェックに使用するポート

ゲートウェイセキュリティではウイルスチェックのために、別ポートにパケットを転送します。
他のサービスなどで既に利用している場合は、未使用ポート番号に変更してください。
入力後、[更新]ボタンをクリックしてください。
初期設定値:SMTP 9025　POP3 9110

●監視する接続先のポート

SMTPまたはPOP3のサービスが使っているポート番号を指定します。
通常、SMTPのポート番号は25、POP3のポート番号は110を指定します。
入力後、[更新]ボタンをクリックしてください。
初期設定値:SMTP 25　POP3 110

●送信元IPアドレスの復元

ゲートウェイセキュリティでは使用しません。

●管理者への警告メール設定

メールがウイルスに感染していた場合、警告メールを管理者に送信することができます。「3.6.1 基本設定」で設定した、警告メールの送信先へ送信します。

Subject ：警告メールのサブジェクト名と感染メール Subject(元メールのサブジェクト)を連結することができます。
本文　　：置換文字列を使用して、警告メール本文に感染メールの情報を表示することができます。

(置換文字列)	(表示内容)
__SUBJECT__	：感染メールSubjectを表示します。
__VIRUS_SENDER__	：送信者のメールアドレスを表示します。ただし、詐称されている場合があります。
__MESSAGE_ID__	：感染メールMessage-Idを表示します。
__MESSAGE_HEADER__	：感染メールのヘッダー全てを表示します。

入力後、[更新]ボタンをクリックしてください。
初期設定値：管理者に警告メールを送る

画面3.7.3

3.7.4 詳細設定2

メール設定画面の「詳細設定2」をクリックすると画面3.7.4 が表示されます。

●初期の接続待機数

サービスを効率良く処理するため、同時並行処理を行う初期のプロセス待機数を指定します。この初期接続待機の数を多く設定すると同時接続数が多い場合処理効率は上がりますが、システムのメモリなどを消費します。SMTPもしくはPOP3のサービスで、初期で接続待機する数を設定します。

初期設定値:SMTP 50 POP3 10

●最大同時接続数

同時接続可能な接続(セッション)数です。この接続数以上はビジーとなり、接続待ち状態になります。SMTPもしくはPOP3の場合は、同時利用者の最大数にほぼ同数です。

初期設定値:SMTP 250 POP3 250

●待機数を超えた場合の接続増加数

現在の接続待機数より多くの接続要求がきた場合、待機数を増やす単位。

初期設定値:SMTP 10 POP3 10

●最大ファイルサイズ

チェックするメールの最大サイズを指定します。最大サイズを超えるメールは、次の「最大ファイルサイズを超えた場合の処理」に従います。

初期設定値:SMTP 100(MB)　POP3 100(MB)

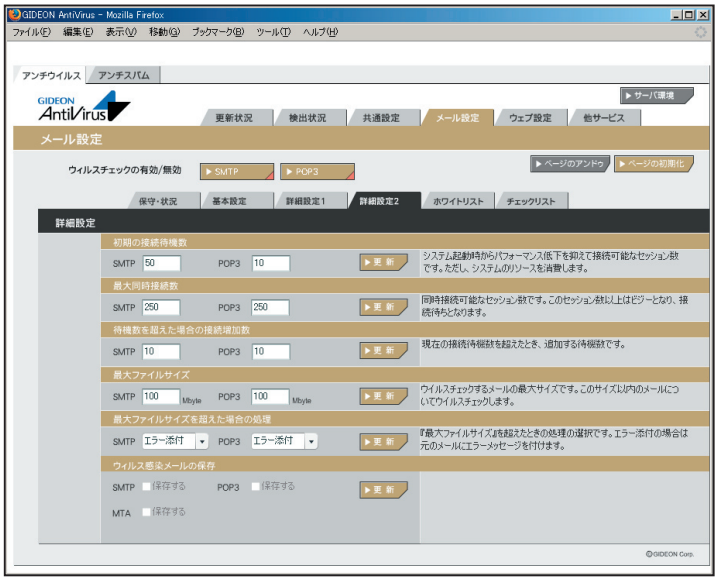
●最大ファイルサイズを超えた場合の処理

『最大ファイルサイズ』を超えた時の処理で『エラー添付』もしくは『通過』が選択できます。『エラー添付』は、元のメールにエラーメッセージを付けます。『通過』は、元メールをそのまま送受信します。

初期設定値:SMTP『エラー添付』POP3『エラー添付』

●ウイルス感染メールの保存

ゲートウェイセキュリティでは使用しません。



画面3.7.4

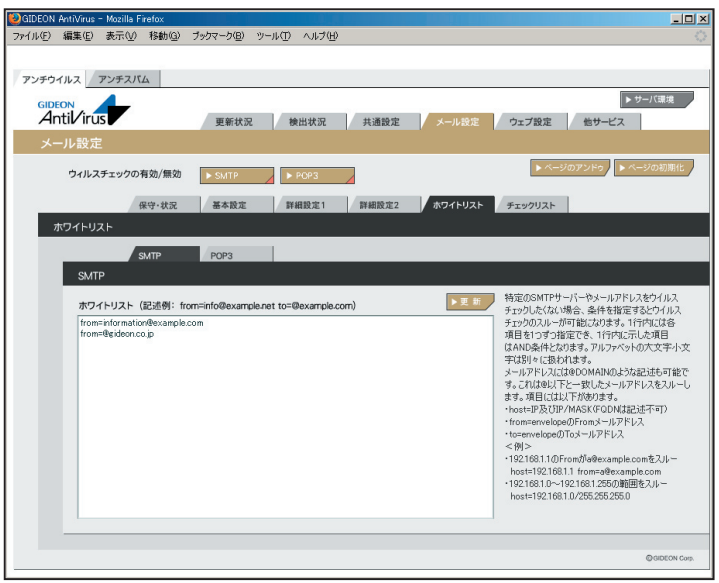
3.7.5 ホワイトリスト

メール設定画面の「ホワイトリスト」タブをクリックすると、画面3.7.5が表示されます。

特定のSMTPサーバやメールアドレスをウイルスチェックの対象外にする場合、ホワイトリストにその条件を記述します。from=information@example.com、to=@example.com、またはIPアドレスの記述で範囲指定も可能です。

送受信のいずれか一方だけ、またはいずれにもマッチといった指定ができます。1行に書かれた項目は "AND" として処理されます。

入力後[更新]ボタンをクリックしてください。
初期設定値:なし



画面3.7.5

3.7.6 チェックリスト

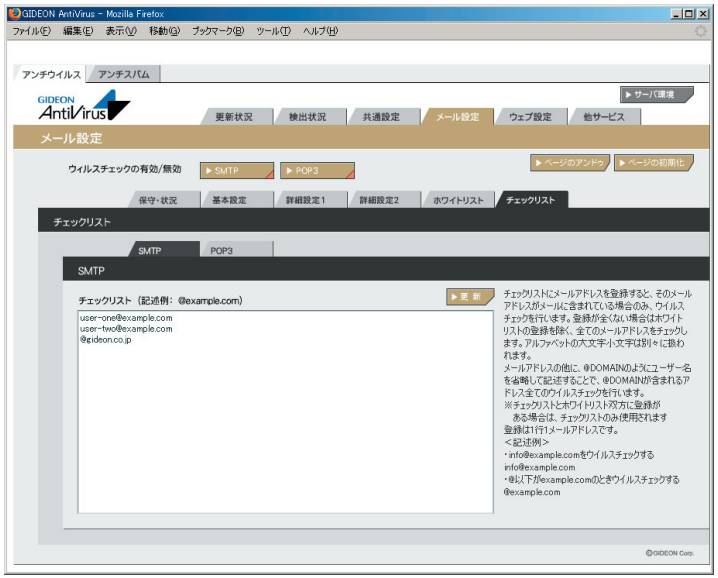
メール設定画面の「チェックリスト」タブをクリックすると、画面3.7.6が表示されます。チェックリストに何も記載しない場合には、サーバで処理するすべてのメールアドレスがウイルス検出対象となります。チェックリストに登録すると、登録されたメールアドレスのみが検出対象となります。

チェックリストの欄に、検出対象とするメールアドレス（例:eee@fff.co.jp）またはドメイン名（例:@fff.co.jp）を入力します。「@fff.co.jp」を登録すると、@fff.co.jpが含まれるメールアドレスすべてがメール送受信時に検出対象となります。

チェックリストに登録がある場合、ホワイトリストをチェックした後にチェックリストをチェックします。

入力後［更新］ボタンをクリックしてください」。

初期設定値 :なし



画面3.7.6

3.8 ウェブ設定

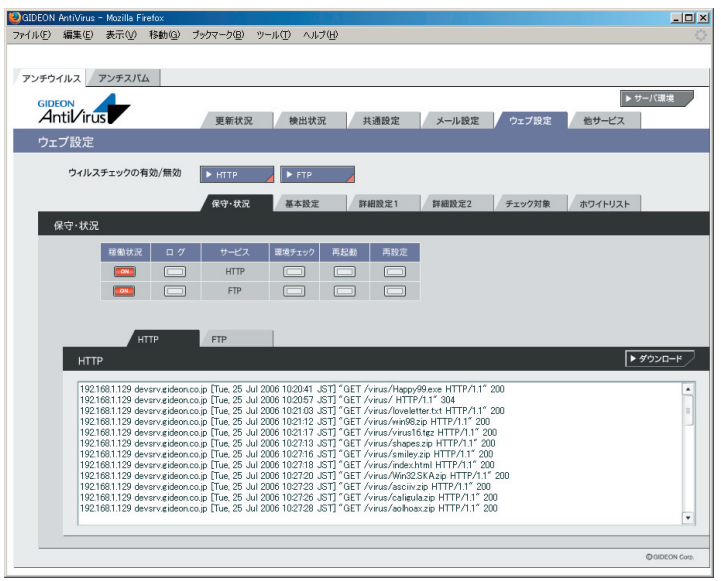
管理･設定画面の「ウェブ設定」タブをクリックすると、画面3.8が表示されます。HTTPおよびFTPでのウイルスチェックをする場合の管理･設定をおこないます。

HTTPは、Webサーバーとクライアント（Webブラウザなど）がデータを送受信するのに使われるプロトコルで、ここではそのサービスを意味します。

FTPは、インターネットやイントラネットなどのTCP/IPネットワークにおけるファイル転送に使用されるプロトコルで、ここではそのサービスを意味します。

「ウイルスチェックの有効/無効」の［HTTP］または［FTP］ボタンをクリックして、次画面で有効または無効を設定します。

［HTTP］ボタン、［FTP］ボタンのそれぞれ右下三角がオレンジ色になっている場合は有効になっている状態です。



画面3.8

3.8.1 保守･状況

ウェブ設定画面の「保守･状況」タブをクリックすると、画面3.8が表示されます。

稼働状況　：ON はプロトコルの監視プロセスが動作しています。
OFFは動作していません。

ログ　：最新のログを取得し、下のログ一覧に表示します。

サービス　：HTTPまたはFTPのサービス。

環境チェック　：ボタンをクリックすると、システムの詳細情報を表示します。
［管理者に結果を送信する］ボタンをクリックすると、表示されている内容を管理者宛に送信します。

再起動　：サービス（プロセス）を再起動させます。サービスが異常な状況（動作エラーが出力されている）の場合にクリックします。

再設定　：サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生している場合にクリックします。

HTTP - ログ - ダウンロード
：ダウンロードボタンをクリックすることで、HTTPのアクセスログがダウンロードできます。
ダウンロードする際は、『HTTPログのダウンロード』ダイアログ中のリストより選択してからダウンロードボタンをクリックしてください。

FTP - ログ - ダウンロード
：ダウンロードボタンをクリックすることで、FTPのアクセスログがダウンロードできます。
ダウンロードする際は、『FTPログのダウンロード』ダイアログ中のリストより選択してからダウンロードボタンをクリックしてください。

3.8.2 基本設定

ウェブ設定画面の「基本設定」タブをクリックすると、画面3.8.2が表示されます。

●ファイル種別、ウイルスチェックの有効/無効

アクセス効率化のために、ウイルスチェックをするファイルの種類を選択をします。
［画像］［動画］［サウンド］［ウェブ文書］ボタンは、それぞれ有効/無効のトグルになっています。
有効化した場合、右下三角がオレンジ色になります。
初期設定値:「画像」「動画」「サウンド」「ウェブ文書」 が無効

●感染時にファイルに埋め込む、もしくは置き換えるメッセージ

ファイルが感染していることを知らせる場合のメッセージを設定します。HTMLの場合、ウイルスが検出された時にこのメッセージを表示します。
メッセージは日本語の表示はできません。半角英数文字で記述します。
入力後、［更新］ボタンをクリックしてください。
初期設定値:画面3.8.2表示文字列

●最大受信サイズを超えた際に置き換えるメッセージ

最大受信サイズを超えたことを知らせる場合のメッセージを設定します。
日本語のメッセージ表示が可能です。
入力後、［更新］ボタンをクリックしてください。
初期設定値:画面3.8.2表示文字列

●すでに感染していたページにアクセスした際に置き換えるメッセージ

すでに感染しているページにアクセスした際に表示するメッセージを設定します。
ウイルスを検出したURLのサイトに、60分以内に再度アクセスした場合、ウイルスチェックをすること無しにウイルスと判断します。ウイルスサイトに同時に多くのユーザーがアクセスすることを回避するためです。

日本語でのメッセージ表示が可能です。
入力語、[更新]ボタンをクリックしてください。
初期設定値:画面3.8.2表示文字列

画面3.8.2

3.8.3 詳細設定1

ウェブ設定画面の「詳細設定1」タブをクリックすると、画面3.8.3が表示されます。

●チェックに使用するポート

ゲートウェイセキュリティではウイルスチェックのために別ポートにパケットを転送します。他のサービスなどですでに利用している場合は、未使用ポート番号に変更してください。
入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 9080　FTP 9021

●監視する接続先のポート

HTTPまたはFTPサービスが使用しているポート番号を指定します。
通常、HTTPのポート番号は80、FTPのポート番号は21を指定します。
プロキシサーバー経由でインターネットに接続している場合、HTTPポートにプロキシサーバーが受け付けるポート番号を指定してください。
例: HTTP 8080

プロキシサーバーを使用するネットワーク環境の多くは、ブラウザでプロキシサーバーの設定がされています。ブラウザからその設定を参照してポート番号を指定することもできます。ほとんどの場合、「3.6.3 更新環境設定」で設定するプロキシサーバーのIPアドレス・ポートと同じ設定になります。

入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 80, 3128, 8080　FTP 21

●送信元IPアドレスの復元

ゲートウェイセキュリティでは使用しません

●ウイルス感染メールの保存

ゲートウェイセキュリティでは使用しません。

●管理者への警告メール

HTTPもしくはFTPサービスでウイルスに感染していた場合、警告メールを管理者に送信することができます。「3.6.1 基本設定」で設定した、警告メールの送信先へ送信します。

Subject　：警告メールのサブジェクト名 を設定します。

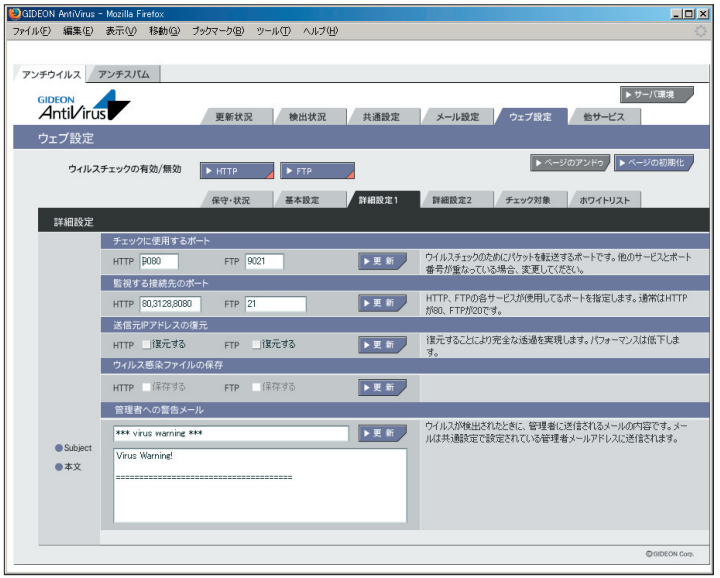
本文　　：警告メールに固有のメッセージを記載します。

入力後、[更新]ボタンをクリックしてください。

初期設定値:画面3.8.3表示文字列

●ウイルス感染メールの保存

ゲートウェイセキュリティでは使用しません。



画面3.8.3

3.8.4 詳細設定2

ウェブ設定画面の「詳細設定2」タブをクリックすると、画面3.8.4が表示されます。

●初期の接続待機数

サービスを効率良く処理するため、同時並行処理を行う初期のプロセス待機数を指定します。この初期接続待機の数を多く設定すると同時接続数が多い場合処理効率は上がりますが、システムのメモリなどを消費します。

HTTP もしくはFTP のサービスで、初期で接続待機する数を設定します。
クライアントからWEB サーバには一回のサイトアクセスで複数セッションを同時に使用するためデフォルト値を大きく設定しています。
入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 500 FTP 5

●最大同時接続数

同時接続可能な接続(セッション) 数です。この接続数以上はビジーとなり、接続待ち状態になります。HTTP もしくはFTP の場合は、同時利用者の最大数にほぼ同数です。

入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 1000 FTP 50

●待機数を超えた場合の接続増加数

設定した接続待機数を超えた接続要求がきた場合に、待機数を増加させる処理を実行します。以下の初期設定値では、1 回の処理で50 待機プロセスを増分します。

入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 50 FTP 1

●ダウンロードの最大ファイルサイズ

ウイルス検出するダウロードファイルの最大ファイルサイズです。

この最大ファイルサイズ未満のファイルはウイルスを検出する対象になります。

入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 10[MB]FTP 10[MB]

●ダウンロードの最大ファイルサイズを超えた場合の処理

『ダウンロードの最大ファイルサイズ』を超えた時の処理で『通過』もしくは『エラー停止』が選択できます。
『通過』は、ウイルスチェックせずそのまま通信をおこないます。『エラー停止』の場合は、ダウンロードを停止します。
入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP『通過』FTP『通過』

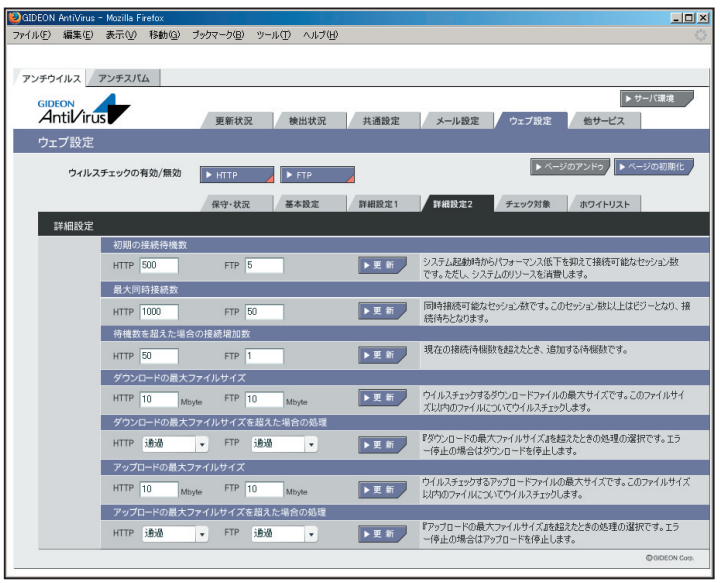
●アップロードの最大ファイルサイズ

ウイルス検出するアップロードファイルの最大ファイルサイズです。
この最大ファイルサイズ未満のファイルはウイルスを検出する対象になります。
入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP 10[MB]FTP 10[MB]

●アップロードの最大ファイルサイズを超えた場合の処理

『アップロードの最大ファイルサイズ』を超えた時の処理で『通過』もしくは『エラー停止』が選択できます。『通過』は、ウイルスチェックせずそのまま通信をおこないます。『エラー停止』の場合は、アップロードを停止します。

入力後、[更新]ボタンをクリックしてください。
初期設定値:HTTP『通過』FTP『通過』



画面3.8.4

3.8.5 チェック対象

ウェブ設定画面の「チェック対象」タブをクリックすると、画面3.8.5が表示されます。

●ウイルスチェックしないファイル

ウイルスチェックをしないファイルを個別に指定できます。HTTPではContent-Typeと拡張子が一致したファイルはチェックしません。
入力後、[更新]ボタンをクリックしてください。

HTTP初期設定値
Content-Type ：画面3.8.5表示文字列
拡張子 ：画面3.8.5表示文字列
スクリプト ：ウェブ文書中のスクリプトのウイルスチェックを行わない
FTP初期設定値
拡張子 ：画面3.8.5表示文字列

画面3.8.5

3.8.6 ホワイトリスト

ウェブ設定画面の「ホワイトリスト」タブをクリックすると、画面3.8.6 が表示されます。ホワイトリストは、特定の接続先サイトなどをウイルスチェック対象外とするリストです。

HTTP

ホストリストの書式は以下の通りです。一行内に項目のどちらか一項目、もしくはAND 条件の場合は両項目が記述できます。

項目は以下の2個の指定が可能です。
host=FQDN または IP または IP/MASK
path=『/』文字から始まるファイル名を含むパス

-----例-----

http://www.example.com/file.zip をスルーする場合、以下のように記載します。
　host=www.mple.com path=/file.zip

全ての/cgi-bin/bbs.cgi?s=1&e=100 をスルーする場合、以下のように記載します。
　path=/cgi-bin/bbs.cgi?s=1&e=100

192.168.1.0 ～ 192.168.1.255 をスルーする場合、以下のように記載します。
　host=192.168.1.0/255.255.255.0

入力後、[更新]ボタンをクリックしてください。
初期設定値 :設定なし

FTP

ホストリストの書式は以下の通りです。

一行内に項目のどちらか一項目もしくはAND 条件の場合は両項目が記述できます。

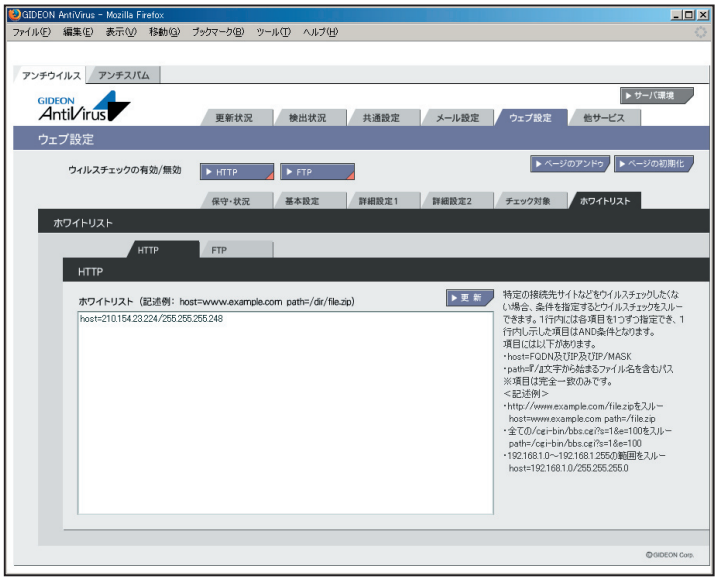
項目は以下の2個の指定が可能です。
　host=IP または　IP/MASK
　path=『/』文字から始まるファイル名を含むパス

-----例-----

ftp://192.168.1.100/pub/file.exe をスルーする場合、
以下のように記載します。
　host=192.168.1.100 path=/pub/file.zip

192.168.1.0 ～ 192.168.1.255 をスルーする場合、
以下のように記載します。
　host=192.168.1.0/255.255.255.0

入力後、[更新]ボタンをクリックしてください。
初期設定値 :設定なし



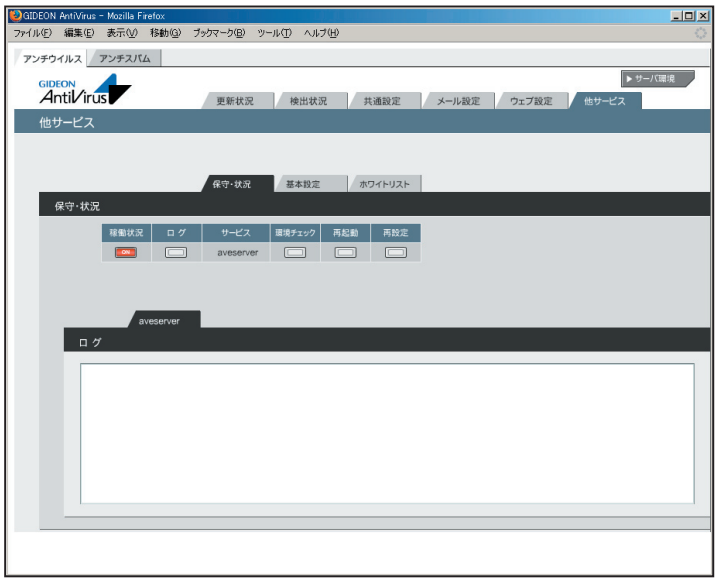
画面3.8.6

3.9 他サービス

管理・設定画面の「他サービス」タブをクリックすると、画面3.9.1 が表示されます。

3.9.1 保守・状況

稼働状況　：ON の場合、サービスが動作しています。
　　OFF の場合、動作していません。
ログ　：最新のログを取得し、下のログ一覧に表示します。
サービス　：aveserverのサービス。
環境チェック　：ボタンをクリックすると、システムの詳細情報を表示します。
　　［管理者に結果を送信する］ボタンをクリックすると、表示されている内容を管理者宛に送信します。
再起動　：サービス(プロセス)を再起動させます。サービスが異常な状況(動作エラーが出力されている)の場合にクリックします。
再設定　：サービスを初期の設定に戻します。システムの異常で、設定のエラーが発生している場合にクリックします。



画面3.9.1

3.9.2 基本設定

他サービス画面の「基本設定」タブをクリックすると、画面3.9.2が表示されます。

●ウイルスチェックするネットワークの範囲

ウイルスチェックをする、接続元のネットワークの範囲を設定する場合に入力します。例えばローカルネットワークが、 192.168.1.1 から 192.168.1.255 の範囲でのアクセスに制約する場合、192.168.1.0/255.255.255.0 と設定します。
設定しない場合は、全てのネットワーク範囲についてウイルスチェックを行います。
入力後、[更新]ボタンをクリックしてください。
初期設定値:設定なし

画面3.9.2

3.9.3 ホワイトリスト(サーバホワイトリスト)

他サービス画面の「ホワイトリスト」タブをクリックします。
サーバのIPアドレスもしくはサーバのIPアドレスとポート番号を指定することで、指定に一致したサーバをウイルスチェックから完全に除外することができます。メール設定やウェブ設定のホワイトリストはHTTP/SMTP などのプロトコルを監視しながらチェックのみ行わないという方法ですが、本項目のホワイトリストの場合は監視そのものも行いません。

よって本項目を指定することにより、プロトコルを監視によって発生していたパフォーマンスの低下や、プロトコル解析に失敗していたために発生していたトラブル(ネットワーク経由の業務ソフトなどでの不具合)を回避することができます。

設定項目は以下となります。

・host=接続先のIPアドレス
・port=ポート番号

-----例-----
サーバ192.168.1.1 のポート80番をスルーする場合、以下のように1行に記載します。

host=192.168.1.1 port=80

入力後、[更新]ボタンをクリックしてください。
初期設定値:設定なし

3.10 サーバー環境

画面右肩の[サーバー環境]ボタンをクリックすると画面3.10.1が表示されます。

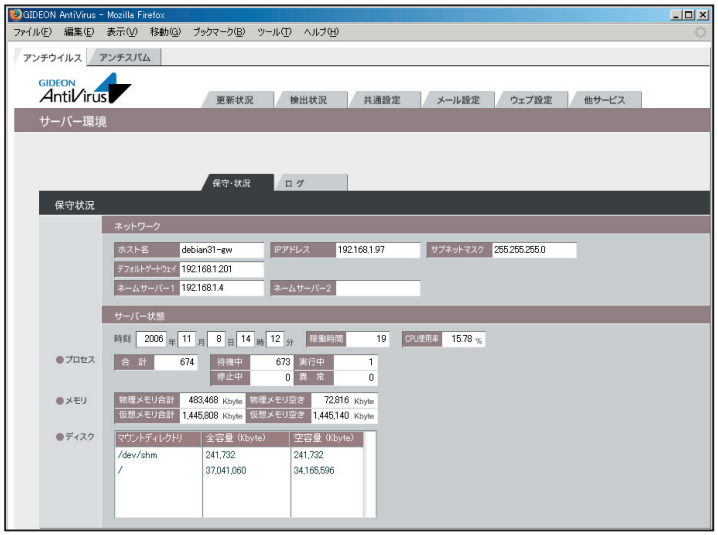
3.10.1 保守・状況

●ネットワーク

ゲートウェイセキュリティ導入サーバがネットワークに接続されており、正常に動作している場合、ネットワークに関連する情報を表示します。初期の設置時からの変更や、ネットワークの設定を変更した場合、このネットワーク情報を確認してください。

●サーバー状態

時刻	:内部時計の時刻
稼働時間	:連続稼働時間
CPU使用率	:表示した時点でのCPUの利用度を%で表示します。システム稼働状態を表示します。
プロセス	:稼働中のプロセス数などを表示します。ウイルス検出プロセスなどが増えると、プロセス数も増大します。
メモリ	:メモリ(実メモリ、仮想メモリ)の使用容量(KB)を表示します。特に仮想メモリを多く使っている場合、パフォーマンスが極端に低下することがあります。このような場合、再起動することで解消します。
ディスク	:ディスクの使用容量(KB)を表示します。通常は十分な空き容量が残っています。空き容量が極端に少ない場合、再起動することを推奨します。



画面3.10.1

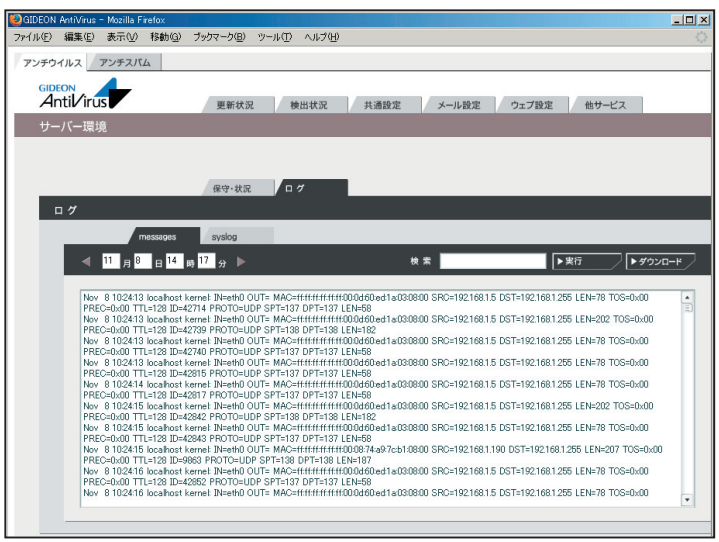
3.10.2 ログ

サーバー環境画面の「ログ」タブをクリックすると、画面3.10.2 が表示されます。

システムエラーログとして、「messages」または「syslog」の一覧が表示され、エラーや異常を発見するために利用します。

また、ログの一覧で検索したい文字列で特定のエラーを絞ることができます。

また、 ダウンロードボタンをクリックすると、 ログをファイルとしてダウンロードできます。



画面3.10.2

3.11 リスクウェア(Winnyプログラム)の検出設定

本製品は、ウイルス送受信の危険性を伴うWinnyプログラムをリスクウェアとして検知する機能があります。この機能を有効化することで、Winny本体やその亜種のWEBやFTPでのダウンロード・アップロード、またメール添付での送受信を防ぐことができます

この機能はデフォルト設定では有効となっておりません。
ウイルス検出エンジンに使われる設定ファイルを編集し「拡張定義ファイル」を読み込ませることによって、「リスクウェア」というカテゴリーで検出するようになります。

まず、root権限でシステムにログインして、/usr/local/gwav/ave/kav/5.x/etc/kav4unix.confファイルをviエディタなどで編集します。ファイル内の記述で［aveserver.options］の項目があるかご確認ください。

```
----------
［aveserver.options］
...
UseAVbasesSet = extended ←この行を追加
----------
```

もし、［aveserver.options］がなければ、［ ］行とともに、ファイルの最下部に2行追加してください。
その後

```
# /etc/rc.d/init.d/aved restart
```

を実行してaveserverエンジンを再起動します。

以上で、Winny実行プログラムを検出・削除するようになります。メール添付

の送受信、ウェブ/FTPサイトからのダウンロード・アップロード時に検出します。

拡張定義ファイルが有効になったかどうかの確認

以下を実行して対応ウイルス数が更新されたか、ご確認ください。

```
# cd /usr/local/gwav/ave/kav/5.x/bin
# ./avbasestest ../db/bases
Standard AV bases are OK, latest update: 13-04-2006, total records:
176536.
Extended AV bases are OK, latest update: 13-04-2006, total records:
187908.
Redundant AV bases are OK, latest update: 13-04-2006, total records:
187908.

# ./aveclient -c -p /var/run/aveserver
RECORDS 187908 ← 上記 "Extended AV bases..." 行のウイルス対応数にマッチします
UPDATED 13-04-2006
....
```

重要

リスクウェアの検出を有効にすると、ご利用のサーバスペックによってはスループットが低下する場合があります。その場合は本機能を無効にしてお使いください。

第4章 アンチスパム設定

4.1 アンチスパム機能動作までの手順

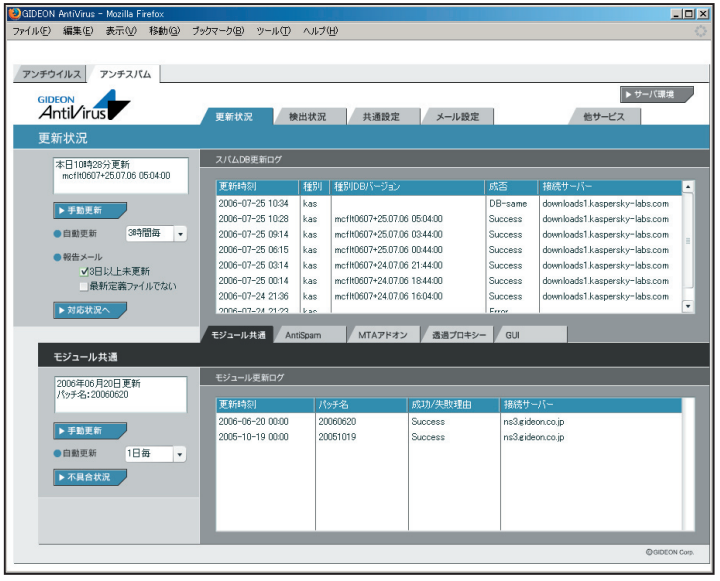
アンチスパム機能を正しく動作させるために、以下の手順に従い設定してください。

《手順1》 GUI画面の起動

GUI画面を起動し、管理・設定画面にアクセスします。起動方法は、本ユーザーズガイド「第3章 アンチウイルスの使い方」の管理・設定画面の項を参照してください。

《手順2》 アンチスパム設定画面

管理・設定画面の左上「アンチスパム」タブをクリックすると(画面 4.1-1)、アンチスパム設定画面が表示されます。この画面からアンチスパムの各種設定を行います。



画面 4.1-1

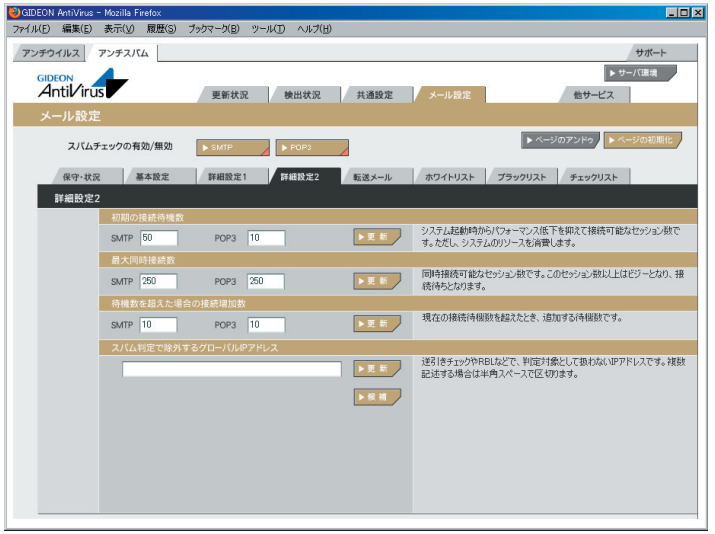
《手順3》 データベースの手動更新

アンチスパム設定画面上部「更新状況」タブをクリックするとスパムDBが表示されます。[手動更新]ボタンをクリックして、その時点で最新のデータベースの取得を行います。通信回線速度にもよりますが、初期の更新には約10分程度時間がかかります。

《手順4》 スパム判定で除外するグローバルIPアドレスの設定

アンチスパム設定画面の「メール設定」タブをクリックします。続いて「詳細設定2」タブをクリックすると画面4.1-2が表示されます。

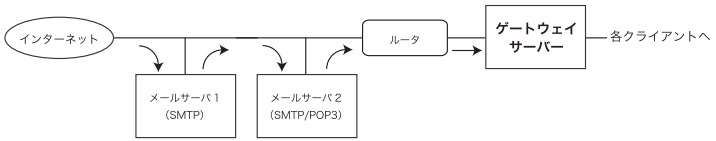
ゲートウェイセキュリティでは、受信したメールの直前のグローバルIPアドレスをチェックしてスパム判定を行います。したがってゲートウェイセキュリティの上位に位置するメールサーバのグローバルIPアドレスをスパム判定対象から除外する指定が必要です。



画面 4.1-2

「スパム判定で除外するグローバルIPアドレス」欄に、ゲートウェイセキュリティの上位に位置するメールサーバのグローバルIPを指定します。

-----例-----



上記の経路で外部からのメールを受信し、自社内部リレーメールサーバの後ろにゲートウェイセキュリティを導入した場合を例にとります。

- ゲートウェイセキュリティの直前におかれたすべての受信メールサーバIPアドレスを、スパム判定対象外に指定します。上記例の場合、「メールサーバ1」「メールサーバ2」のIPを「スパム判定で除外するグローバルIPアドレス」に入力して下さい。その後［更新］ボタンをクリックします。
- 外部MTAが転送目的のサーバであれば、該当するグローバルIPも入力してください。
- プライベートIPはスパム判定には使わないため、グローバルIPのみを指定します。

（注）グローバルIPが不明な場合は、受信しているメールソフトのヘッダを参照してください。

重要

受信経路の連続したスパム判定対象外メールサーバのグローバルIPを漏れなく記載する必要があります。

《手順5》 ユーザにスパムを配信しないようにする設定

アンチスパム設定画面上部「メール設定」タブをクリックします。続いて「転送メール」タブをクリックします。

画面下部「転送メール設定」の欄に以下の設定をすることで、ユーザにスパムメールが配信されないように指定できます。

- 「転送下限スコアに達していたら転送」を選択
- 「受信先への配信を停止する」にチェックマークをつける
- テキストボックスに転送対象アドレスと転送先アドレスを記述

-----例-----

@example.comが付くメールアドレスへのスパムメールを配信停止させたい場合は以下のように記述します。

@example.com spam@example.co.jp

上記設定を行うことにより、@example.com宛のスパムはspam@example.co.jpに転送され、実際のユーザへの配信は停止します。

（注）事前にexample.co.jpのメールサーバ上にspamというメールボックスが作成されている必要があります。

画面 4.1-3

4.2 アンチウイルスとの共通機能について

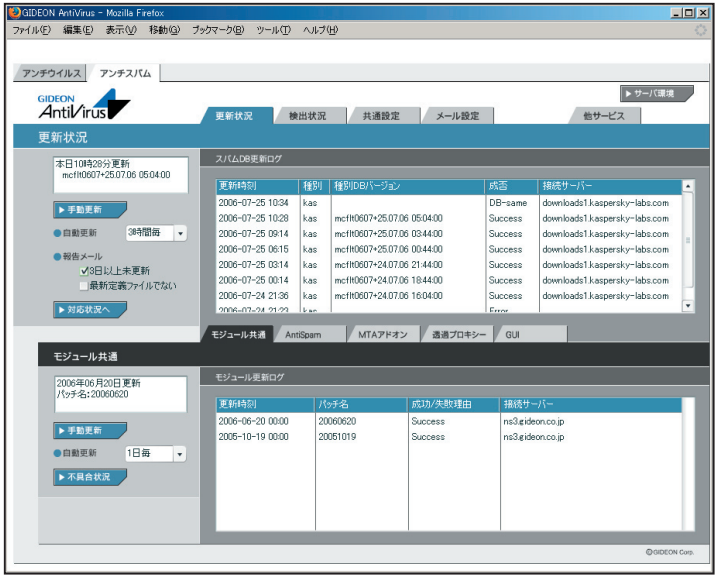
本編では、アンチウイルスと共通の機能については説明を割愛しています。以下の項目については、本ユーザーズガイド「第3章 アンチウイルス設定」を参照してください。

- 「共通設定」
- 「メール設定」の「保守・状況」および「sendmail」
- 「他サービス」
- 「サーバ環境」

4.3 更新状況

●スパムDB更新

アンチスパム設定画面の上部「更新状況」タブをクリックします。ここではスパムデータベース（スパムDB）の更新状況を閲覧できます。
スパムDB は、スパムメールを特定するための情報を格納したデータベースです。カスペルスキーのアンチスパムエンジンが利用するスパムDB を更新します。



画面 4.3

このスパムDB は、初期設定では3 時間毎に自動更新します。自動更新の間隔を変更することも可能です。推奨は3 時間毎です。

[手動更新]ボタンをクリックすると、現時点での最新のスパムDB への更新を試みます。
通常は自動更新によりスパムDB の更新が行われるため、手動更新を実行する必要はありません。

「報告メール」は、スパムDB の更新状況をメールでお知らせするものです。
「3 日以上未更新」は、3 日以上スパムDB の更新がない場合に管理者宛にメール送信します。
「最新定義ファイルでない」は、システム上のスパムDB が最新でない場合に管理者宛にメール送信します。

[対応状況]ボタンをクリックすると、スパムDB に関する情報サイトを表示します。

●モジュール

モジュールとは、アンチスパムが動作するために必要な実行ファイルやスクリプト、またはそれらが参照するファイルを指します。
「モジュール共通」では、モジュール全ての更新状況を示します。
その他の各タブ（「AntiSpam」、「MTA アドオン」、「透過プロキシー」、「GUI」）は、モジュールを機能別に分けた状態での更新状況を示します。

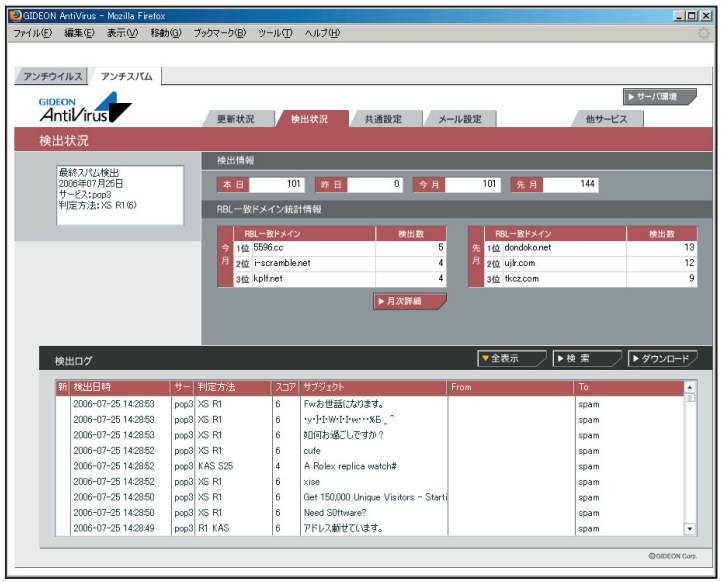
「モジュール共通」では、モジュール更新ログを閲覧できます。これは自動更新・手動更新された更新パッチの履歴です。手動更新は［手動更新］ボタンにより行うことができます。
その他のタブでは、更新の詳細が「更新履歴」で閲覧できます。
［強制更新］ボタンは通常はクリックしないでください。
［不具合状況］ボタンをクリックすると、パッチに関する情報サイトを表示します。

4.4 検出状況

アンチスパム設定画面の上部 「検出状況」タブをクリックします。ここではスパムメールと判定したメール情報の履歴や統計情報などを閲覧できます。

●検出情報

検出状況画面の上部「検出情報」欄では、スパムメールと判定したメールの検出数が表示されます。
「本日」、「昨日」、「今月」、「先月」のスパムメール検出数を表示します。



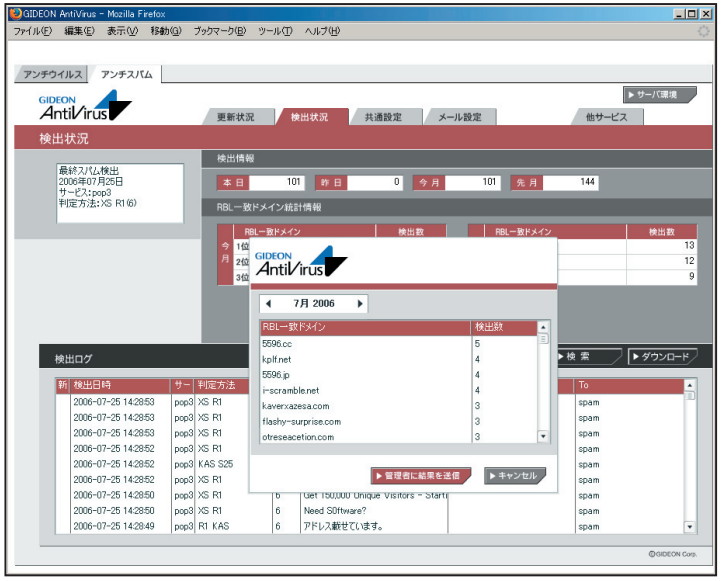
画面 4.4-1

●RBL一致ドメイン統計情報

検出状況画面の「RBL 一致統計情報」欄では、スパムメール判定方法の1つであるxSPAM 方式の統計情報が表示されます。

xSPAM 方式はメール本文中に含まれるURL が、ブラックリストにのっていないかどうかをチェックします。実際にはRBL (Realtime Black List) と言われるDNS サービスを検索します。
表示された検出数は、スパムと判定されたドメインが何通のメールに含まれていたかを表します。

[月次詳細]ボタンをクリックすると、月内にスパムと判定した全てのRBL 一致ドメインとその検出数を閲覧できます。
[管理者に結果を送信]ボタンをクリックすると、その内容を管理者へメールで送信します。



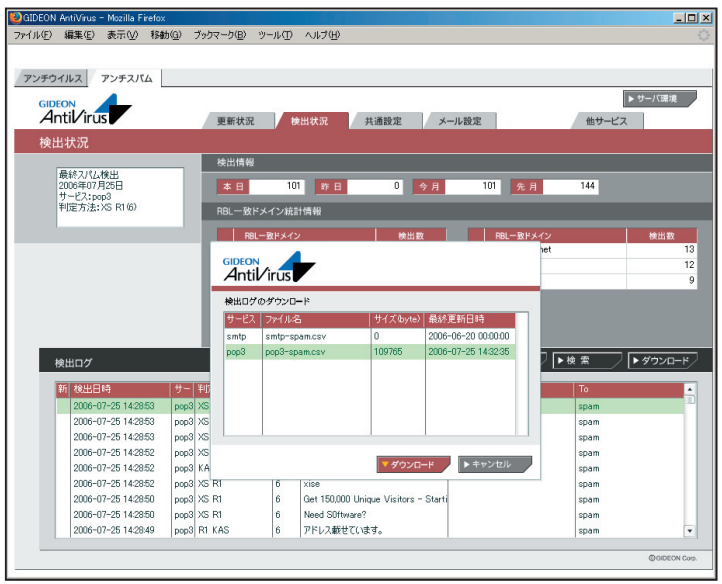
画面 4.4-2

●検出ログ

検出状況画面の下部「検出ログ」欄では、検出したスパムメールの情報リストを閲覧できます。

選択行をクリックすると詳細情報を表示します。各タイトル項目をクリックするとソートします。

[全表示]ボタンをクリックすると、検出ログの最新リストを再表示します。[検索]ボタンをクリックすると、項目での絞り込み検索ができます。また、検出ログは［ダウンロード]ボタンをクリックすることで、CSV ファイルとしてクライアントPC に保存することができます。



画面 4.4-3

4.5 メール設定

4.5.1 保守･状況

本項は、アンチウイルスでの設定と共通です。詳細は、本ユーザーズガイドの「第3章 アンチウイルス設定」を参照してください。

4.5.2 基本設定

アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「基本設定」タブをクリックします。ここではスパム判定の基本的な設定を行います。本製品はスパム判定基準に、検知率を高め誤検知を防ぐスコアリングロジックを用いています。複数の判定方法ごとにスコア（点数）を設定し、該当した場合にスコアが加算されます。高スコアほどスパムである可能性が高く、合計が一定の値を超えた場合にスパムと判定します。

画面 4.5.2

●スパムと判定した場合のSubject

受信したメールがスパム判定で一定のスコアを超えた場合、ユーザにはSubject にコメントを付したメールが送信されます。

メール設定 基本設定画面の「スパムと判定した場合のSubject」欄に、画面の表示例のように指定した場合、ユーザは以下のSubjectを受信します。

[SPAM 3: RES KAS] 元Subject

これはスパム判定名RES および KAS の合計スコアが 3 であり、スパムの疑いがあることを表します。

変更する場合は、入力後に［更新］ボタンをクリックしてください。

●スパム判定基準

アンチスパムPlusでは以下の 6 通りの判定方法を基にスパム判定を行っています。

BL：ユーザ定義ブラックスリスト

・ユーザが設定したブラックリストに基ずく判定
・推奨スコア4（検知度上位）

XS：URLフィルタリング

・ メール本文中のURL がRBL に登録されているか否かをチェック
・推奨スコア3（検知度中位）
・稀にスパムではないドメインがRBL に登録されることがある。

R1：RBL(リアルタイムブラックリスト)

・接続元のIP アドレスがRBL に登録されているか否かをチェック
・推奨スコア3（検知度中位）
・稀にスパム送信の踏み台にされている企業などのサーバからのメールがスパムと判定されることがある。

S25：発信元チェック

・メールヘッダのReceivedに記述された命名規則がスパムでよく用いられる形式か否かをチェック
・推奨スコア1（検知度低位）
・形式的なチェックのため検知率は高くない。

RES：逆引きチェック

・送信元のIP アドレスなどが逆引き可能か否かで信頼性をチェック
・推奨スコア1（検知度低位）
・検知率は一般に高いが誤検知もある。

KAS：本文解析

・カスペルスキーアンチスパムDB を検索してメール本文をチェック
・推奨スコア3（検知度中位）
・英語、ロシア語などのメール解析に優れている。

「カスタマイズを利用する」を選択すると判定基準スコアを変更できます。

（注）判定方法のスコアは推奨値を使用することをお勧めします。また「アクション」の「SMTP のみ受信拒否」のスコア変更は慎重に行ってください。

●アクション

スコアの合計が、設定した総合スコア以上になったときに該当するアクションが実行されます。

Subject：

変更設定したスコアに達したとき、メールの Subject が「スパムと判定した場合の Subject」で設定したものに変更されます。
スコアの値を高く設定すると、スパムの可能性がより高いメールのみ Subject が変更されます。

POP3のみ本文変更：
詳細設定1の「POP3 のみ本文変更のとき置き換える本文」で設定したメール本文に置き換ります。

SMTP/MTA受信拒否：
この総合スコアに達したとき、メールを受信しません。従って、このメールは保存されません。スコアをカスタマイズする際は、特に慎重に行ってください。

●追加ヘッダ
スパム判定の総合スコアが設定した値になると、自動的にメールヘッダに以下の情報を付加します。メールクライアントのメールヘッダによるメールの振り分けの判断に利用できます。

（ヘッダ表示）	（内容）
X-Spam-Status: NONE	スパムに該当せず
X-Spam-Status: SUSPICION	スパムと疑わしい
X-Spam-Status: SPAM	スパムに該当

また、ヘッダには以下に類する行も付加されます。

（ヘッダ表示例）	（内容）
X-Spam-Level: 3	スパム判定スコア3
X-Spam-Method: R1	判定方法R1でチェック

重要

送られてきたメールをスパムと判定する総合スコアは、「追加ヘッダ行」のX-Spam-Status: SPAMで指定した値を用います。この値を高く設定するとスパムの可能性がより高いメールに限定してスパムと判定します。値はお客様のポリシーに応じてカスタマイズを行って下さい。

4.5.3 詳細設定1

アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「詳細設定1」タブをクリックします。

●キャッシュ制御
逆引きチェック（RES）で得た結果、もしくはRBLへの登録問い合わせをキャッシュとして保存しておきます。

［クリア］ボタンをクリックすると、保存したキャッシュを消去します。逆引きキャッシュとRBL キャッシュの双方のキャッシュを消去します。
「保存期間」は、逆引きの結果やRBL の登録問い合わせを行って追加されたキャッシュ項目の有効日数を決定します。

●POP3のみ本文変更のとき置き換える本文
基本設定のアクションの「POP3 のみ本文変更」で設定した総合スコアを超えたときに置き換わる本文です。
本文の中には、以下のタグ文字列を含むことで、スパムメールの特定の情報に置き換わります。

（ヘッダ表示）	（内容）
__SPAM_STATUS__	: NONE/SUSPISION/SPAM のいずれか。基本設定の追加ヘッダと同等
__SPAM_TOTAL_SCORE__	: このメールのスパム判定方法による総合スコア
__SPAM_JUDGE_NAME__	: このメールの判定方法（複数ある場合空白区切り）
__SUBJECT__	: このメールのSubject（MIME デコードあり）
__ORIGINAL_SUBJECT__	: このメールのSubject（MIME デコードなし。メールヘッダに書かれている形式）

画面 4.5.3

4.5.4 詳細設定2

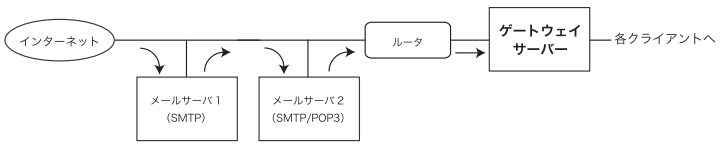
アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「詳細設定2」タブをクリックします。

●スパム判定で除外するグローバルIPアドレス

本製品では、受信したメールの直前のグローバルIPアドレスをチェックしてスパム判定を行います。したがってゲートウェイセキュリティ導入サーバと外部との間に転送用その他のサーバが接続されている場合には、それらのグローバルIPアドレスをスパム判定対象から除外する指定が必要です。

「スパム判定で除外するグローバルIPアドレス」の欄に、メールを受信する経路上の、スパム判定しないグローバルなIPを指定します。

-----例-----



上記の経路で外部からのメールを受信し、自社内部リレーメールサーバの後ろにゲートウェイセキュリティを導入した場合を例にとります。

- ゲートウェイセキュリティ導入サーバの直前におかれたすべての受信メールサーバIPアドレスを、スパム判定対象外に指定します。上記例の場合、「メールサーバ1」「メールサーバ2」のIPを「スパム判定で除外するグローバルIPアドレス」に入力して下さい。その後[更新]ボタンをクリックします。
- 外部MTAが転送目的のサーバであれば、該当するグローバルIPも入力してください。
- プライベートIPはスパム判定には使わないため、グローバルIPのみを指定します。

(注)グローバルIPが不明な場合は、受信しているメールソフトからヘッダを参照してください。

重要

受信経路の連続したスパム判定対象外メールサーバのグローバルIPを漏れなく記載する必要があります。

画面 4.5.4

4.5.5 転送メール

4.5.5.1 基本

スパム判定で総合スコアが「転送下限スコア」で指定した値を超えた場合に、そのメールを転送する設定をします。
初期設定値：転送しない

転送する場合は「転送下限スコアに達していたら転送」ラジオボタンにチェックを入れます。
チェックを入れると以下の項目が入力可能になります。

● 転送下限スコア

転送する下限のスコアを入力します。入力したスコア以上のメールはすべて転送されます。

● 受信先への配信を停止する

チェックを入れることにより、smtp の場合、受信先へメールを送信しません。POP3 では適用されません。

● POP3サーバのメール削除

チェックを入れることによりPOP3 サーバ上にあるスパムメールを削除します。
チェックを入れると「POP 認証」「APOP 認証」のタブが有効になります。

● 転送の指定方法

smtp の場合、転送下限スコアに達した場合にそのメールを転送することができます。
POP3 の場合、上記「POP3 サーバのメール削除」が有効な場合、転送の指示によりPOP3 サーバのメールを削除します。ただし、「4.4.6 チェックリスト」の「POP3 削除」による削除リストが指定された場合は、そのリストが優先されます。

転送の対象となるメールアドレス（例：user-one@example.com）を行頭から指定し、半角スペースに続いて転送先メールアドレス（例：spam-admin@example.com）を指定します。
転送先メールアドレスは半角スペースで区切ることで複数指定可能です。
また、転送対象のメールアドレスは、@ から始めることで、ドメインが一致するメールアドレスをすべて転送対象にすることができます。

-----例1-----

user-one@example.com 宛のメールを、spam-admin@example.com と mail-admin@example.com に転送する場合は、以下のように入力します。

user-one@example.com spam-admin@example.com mail-admin@example.com

-----例2-----

@example.com に後方一致するメールアドレス宛のメールをspam-admin@example.com に転送する場合は、以下のように入力します。

@example.com spam-admin@example.com

4.5.5.2 POP認証

「自動的にユーザリストを追加する」にチェックを入れると、クライアントPC からPOP3 で接続したユーザ情報を自動的に取得します。

4.5.5.3 APOP認証

メールの取得にAPOP（パスワードの暗号化）を利用している場合、利用ユーザすべての登録が必要になります。

記載例：
POP3 のユーザID が「user-one」、パスワードが「1234」、POP3 サーバIP アドレスが「192.168.0.1」の場合、以下のように記載します。

user=user-one password=1234 host=192.168.0.1

画面 4.5.5

4.5.6 ホワイトリスト

アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「ホワイトリスト」タブをクリックします。
ホワイトリストに登録することで、スパムチェックを行わない条件を指定できます。
1 行内に指定した条件は、複数のAND 条件となります。
指定できる条件は以下のものがあります。

host:　有効送信元IPアドレス。　IPアドレス/マスクと指定することで範囲も設定可能。ホスト名は不可
from:　エンベロープFrom
to:　エンベロープTo

有効送信元IP アドレスとは、前項の「4.5.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

-----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2

-----例2-----

送信元IP アドレス192.168.1.2 から送信され、from がsender@example.net の場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.2 from=sender@example.net

-----例3-----

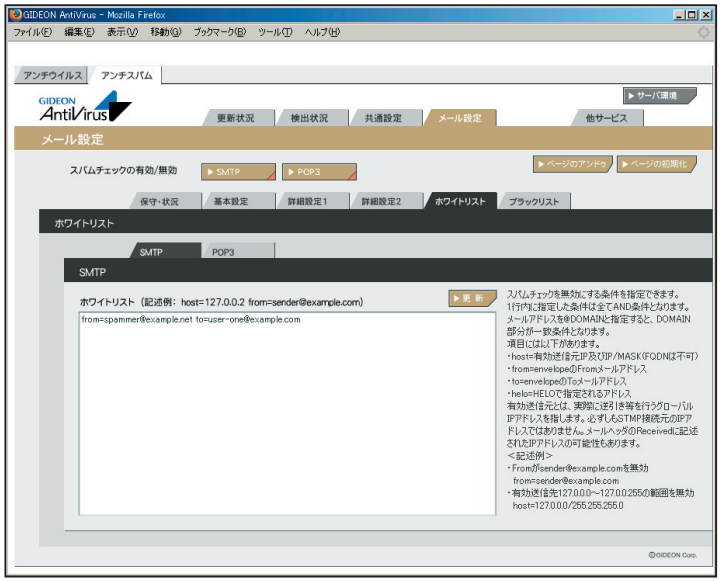
送信元IP アドレス192.168.1.0 ～192.168.1.255 から送信されてきた場合、スパムチェックしない指定は、以下のように入力します。

host=192.168.1.0/255.255.255.0

-----例4-----

送信元IP アドレス192.168.1.2 から送信され、from が@example.net の場合、スパムチェックしない指定は、以下のように入力します。。
この指定の場合、example.net の該当メールアドレスは全てスパムチェックしない指定になります。

host=192.168.1.2 from=@example.net



画面 4.5.6

4.5.7 ブラックリスト

アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「ブラックリスト」タブをクリックします。ブラックリストはスパム判定方法のひとつとして適用します。判定スコアは、「4.5.2 基本設定」の「BL ユーザ定義ブラックリスト」で指定します。指定できる条件には以下のものがあります。

host：　有効送信元IP アドレス。IP アドレス/ マスクと指定することで範囲も設定可能。ホスト名は不可
from：　エンベロープFrom
to：　エンベロープTo

有効送信元とは、前項の「4.5.4 詳細設定2」で設定された「スパム判定で除外するグローバルIP アドレス」以外の送信元IP アドレスを指定します。

-----例1-----

送信元IP アドレス192.168.1.2 から送信されてきた場合、ブラックリストを適用するには、以下のように入力します。

host=192.168.1.2

-----例2-----

送信元IP アドレス192.168.1.2 から送信され、from がsender@example.net の場合、ブラックリストを適用するには、以下のように入力します。

host=192.168.1.2 from=sender@example.net

-----例3-----

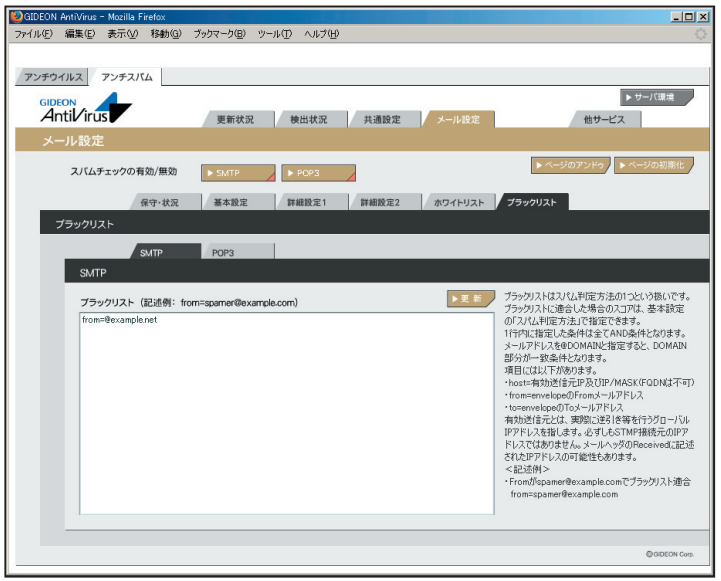
送信元IP アドレス192.168.1.0 ～192.168.1.255 から送信されてきた場合、ブラックリストを適用するには、以下のように入力します。

host=192.168.1.0/255.255.255.0

-----例4-----

送信元IP アドレス192.168.1.2 から送信され、from が@example.net の場合、ブラックリストを適用するには、以下のように入力します。

host=192.168.1.2 from=@example.net



画面 4.5.7

4.5.8 チェックリスト

個別のメールアドレスの入力や、@DOMEIN のようにドメインごとに設定をすることができます。

● SMTP

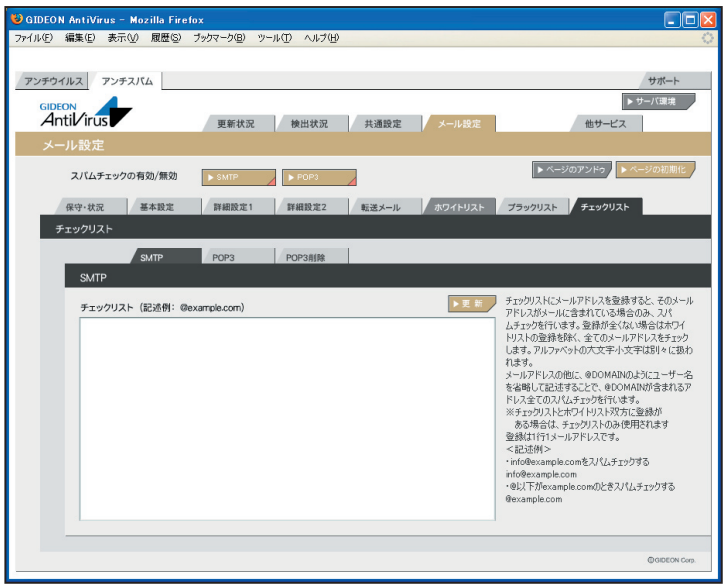
特定のアドレスのみスパム判定をする場合に、そのメールアドレスを登録します。登録が全くない場合にはホワイトリストの登録を除き、すべてのメールアドレスをチェックします。
個別のメールアドレスの入力や、@DOMEIN のようにドメインごとに設定をすることができます。

● POP3

登録された項目が一致した場合のみ「POP3 でスパムチェック」を行います。チェックリストに登録が全くない場合は、ホワイトリストに登録されている以外のすべてのメールをチェックします。
記述方法は、ユーザID@IP アドレスとなります。「@IP アドレス」と記述すると、POP3 サーバすべてのメールをスパムチェックします。

● POP3削除

登録された項目が一致した場合のみ「POP3 サーバのメール削除」を行います。
※POP3 サーバのメール削除は、【メール設定】－【転送メール】－【基本】で設定可能です。
チェックリストに登録がなく、「POP3 サーバのメール削除」が有効になっている場合は、転送メール指定を行ったPOP3 アカウントすべてにメール削除が実行されます。
記述方法は、ユーザID@IP アドレスとなります。「@IP アドレス」と記述すると、POP3 サーバすべてのメールをスパムチェックします。
※チェックリスト、ホワイトリスト双方に同じ登録がある場合、チェックリストのみ有効となります。



画面 4.5.8

第5章 動作確認

5.1 ウイルス検出機能の動作確認テスト

以下に2通りのテスト方法を示します。

※テストを行う前に、本製品に収録されている無害なウイルスファイル「eicar.com」を添付したメール（ウイルス検出用メール）を準備してください。

●テスト方法　メールクライアントからメールを添付する

(1) 本製品を導入したサーバを経由する経路のクライアントのメーラからウイルス検出用メールを送信します。ウイルス検出用メールは、存在するユーザアカウントに送信してください。

(2) クライアントのメーラから送信したメールアカウントで、サーバからメールを受信します。

(1) で送信したメールに、ウイルス検出の警告メッセージが含まれていれば、ウイルス検出機能が正常に動作していることになります。

5.2 メールログでの確認

前述の方法でメールを受信すると、管理画面のウイルス検出状況でウイルスを検出したログで確認することができます。

「3.5 検出状況」でログ一覧が表示されます。

5.3 トラブルシューティング

本製品が正常に動作していない場合、サポートに必要な詳細情報をギデオンサイトにアップロードできます。

(1) root権限でログインして、以下のコマンドを実行します。

```
#/usr/local/gwav/checker  -w -log
```

サポート窓口へお問い合わせの際、必要に応じてこのメールに記載されている

内容を送付してください。

お問い合わせについては、「付録 サポートサービス」を参照してください。さらなるデバッグ情報が必要な場合など、サポートセンターから指示させていただきます。

5.4 動作しない場合

ウイルス検出機能が正常に動作しない場合、以下のURLで当該バージョンのバグ情報や最新の更新情報などを確認してください。

・アップデート情報については、以下のURLを参照してください。

http://www.gideon.co.jp/updates/

・よくあるご質問（FAQ）については、以下のURLを参照してください。

http://www.gideon.co.jp/support/

第6章 よくある質問と回答

Windowsファイル共有、P2Pファイル共有には対応していますか?

現在のところWindowsファイル共有には対応しておりません。P2Pファイル共有については、HTTP経由で行うものについてはウイルスチェックしますが、それ以外のプロトコルを使用するものについては現在のところ対応していません。また、HTTP経由でもプロトコルが暗号化されている場合はパケットの中身を検査できませんので、ウイルスチェック対象外となります。

ファイアウォールやVPN機能はありますか?

一般的に「オールインワン」ですべてのセキュリティ対策をする製品のようなファイアウォール機能は有していません。
ゲートウェイセキュリティは、スパムメール判定、ウイルス、スパイウェア、マルウェアなどの検出に特化した位置づけの製品です。ファイアウォールやVPN機能につきましては、すでにお持ちの機器で対応していただくことになります。

アドウェア、スパイウェアには対応していますか?

はい、対応しています。

ゲートウェイセキュリティを導入することで、クライアントPCのアンチウイルスソフトは必要なくなるのでしょうか?

本製品はネットワークでのウイルス検知には対応しますが、ローカルPCのフロッピーやCD-ROMなどのメディアから直接感染するウイルスには対応していません。このような場合、個別にクライアントソフトをお使いいただき、本製品と併用することでより強固なセキュリティ対策となります。

ユーザ数とは何を意味しているのでしょうか?

本製品を通過するクライアントPCの台数です。メールサーバ同士のSMTP通信をウイルスチェックする場合は、クライアントPCの台数が存在しません。詳しくは、お問い合わせください。

機器の設定等行ってもらえるのでしょうか?

基本的にお客様ご自身で設置・設定をお願いいたします。ユーザマニュアルをご覧いただくか、購入後の技術サポート窓口にご連絡いただきますと、メールまたはお電話にて迅速な対応が可能です。
また、弊社で提携しているパートナー様により、別途(別料金にて)設置サービスをとりおこなうことも可能です。設置サービスについて詳しくはお問い合わせください。

株式会社ギデオンインフォーメーションセンター
(こちらは技術サポート窓口ではありませんのでご注意ください)
E-Mail info@gideon.co.jp
TEL 045-590-1216

ウイルス定義ファイル更新の仕組みはどうなっていますか?

本製品からHTTPポートを使い、インターネット上の定義ファイルアップデートに接続して定義ファイルをダウンロードします。したがって、本製品からインターネット上の任意のウェブサイトに対してアクセスできなければなりません。

HTTPプロキシがゲートウェイセキュリティの上位に位置する場合、ソフトウェア上でそのプロキシを指定することにより、プロキシ経由で定義ファイルダウンロードが可能です。設定方法について詳しくはユーザーズマニュアルをご覧ください。

GUI管理画面にログインするパスワードを忘れてしまいました。

GUI管理画面を開いたときに、パスワード入力フィールドでパスワードを入力しても「パスワードが違う」と言われる、もしくはログインパスワードを忘れてしまった場合、以下の方法でパスワードをリセットできます。

ゲートウェイセキュリティ導入サーバにrootユーザでローカルログインします。初期パスワードは製品に同梱された「ソフトウェアライセンス及びサポートサービス証書」に記載されていますので参照してください。rootアカウントにてログイン後、直接"/etc/GwAV/cgi.password"ファイルを消してください。
("rm /etc/GwAV/cgi.password"を実行。)次回GUI管理画面にアクセスして、新しいパスワードを入力してください。

アンチウイルス検出エンジンは、スキャンするファイルの形式により様々な「リターンコード」という番号を返します。"8"は「破損したファイル」を意味します。実際に「破損したファイル」が存在する場合もありますが、ログに多発している場合、WindowsUpdateなどが原因となっていることが考えられます。WindowsUpdateでは、ファイルが破損しているというよりも、スキャンエンジンが「破損している」と解釈してこのような出力をするだけなので、実際に問題はありません。WindowsUpdateをはじめとして、HTTPプロトコルを使って様々な種類のやりとりをするクライアントエージェントがあります。このメッセージが出ないようにするには"/usr/local/gwav/ave/gwav.conf"ファイルの中に"VIRUS_SCAN_FAILED_NOWARNING_CODE=8"行を追加して、HTTPのウイルスチェックサービスを再起動してください。

定義ファイルはどの程度の頻度で更新されるのでしょうか?

新種のウイルスの対応は、開発センターで数分おきに行われています。
24時間、365日体制で新種・亜種のウイルスに対応しております。

製品に関するお問合わせは、弊社ホームページからご依頼下さい。また良くある質問(FAQ)等の最新情報も併せて掲載していますので、下記のURLをご参照願います。

http://www.gideon.co.jp/

第7章 運用･管理

7.1 メールによる各種情報の通知

管理レポートには月次レポートだけでなく、日ごろの重要なアナウンス（アップデートのご案内や新たに見つかった不具合のレポートなど）が含まれることがあります。インストール後、必ず実在の管理者宛にメールが届くように設定してください。設定は、「3.6.1 基本設定」の「管理者のメールアドレス」から行ってください。

7.2 更新の確認

定期的に、更新の確認を行ってください。特に、新種のウイルスが出現した場合、正常に更新されていないと対応が遅れることになり、被害を受ける可能性があります。

更新の確認については、「3.4 更新状況」の「ウイルス定義ファイル更新ログ」および「モジュール更新ログ」を参照してください。

7.3 システム運用上の確認

ゲートウェイセキュリティが何らかの理由で停止した場合、サーバのシステムログでその内容を確認してください。スパムメールなどの攻撃で、サーバの負荷が過大になり停止する場合があります。また、定期的に/var/tmp領域に不要なファイルが残っていないかを確認してください。

本製品に関するシステム運用でご不明な場合やトラブル発生などの際は、ギデオン サポートセンター（本書巻末に連絡先が記載されています）にお問い合わせください。システム運用に詳しいスタッフが適切なアドバイスをご提供いたします。

本製品とは直接関係ないシステム設定･運用についてはご担当のシステム管理者にご相談ください。

サポートサービス（アップデートを含む）は、1年ごとの契約となっております。
サービス内容は以下のとおりです。

■ サービス内容

1. HTTPからのダウンロードによる最新バージョンの提供
2. E-Mailによるお問い合わせの受付および回答(*) (**)
3. E-Mailによる情報提供（不定期）
4. ウイルス感染の疑いがあるファイルの検証
   （ウイルス誤認識の場合のファイル検査）
5. 導入･運用に関わるコンサルティング(*) (**) (***)

*サポートセンターで無償で受け付けるインシデント数は3インシデントとなっています。製品が本来提供すべき機能･条件を満たさない製品不具合の問い合わせは含まれません。お客様固有の使用環境に由来する質問、トラブルなどが該当します。範囲:「アンチウイルス」のインストールと設定画面から行える設定に関するお問い合わせ

**出張によるサポートは別料金となります。ご利用をご希望のお客様はギデオン インフォメーションセンターにお問い合わせください。

***導入･運用の請負は別契約となります。弊社パートナー企業のご紹介が可能です。コンタクト希望のお客様はギデオン インフォメーションセンターにお問い合わせください。

注意事項

a. サポートを受ける窓口は、1契約あたり1ヶ所のみに限定させていただきます。
b. 本製品では、定義ファイルおよび各種モジュールは、インターネット経由で最新のものに自動更新されます。場合によっては手動にて操作いただく場合があります。ご不明な点はサポートセンターまでお問い合わせください。
c. 更新は、1年ごとのライセンス継続更新が原則となります。
　継続更新がなされなかった場合は、再契約の際に、正規更新料の120%の費用がかかります。

■ 製品のサポート情報

以下のウェブサイトで、製品のサポート情報を入手できます。

http://www.gideon.co.jp/support/

■ サポート依頼フォーム

状況を正確に把握するため、メールで以下の項目を記載してお問い合わせください。

1. お客様登録No.　または製品シリアルNo.
（お客様登録No. 例:AVM12345）
（製品シリアルNo. 例:GS-12345）
2. お客様名
3. ご質問内容、発生現象
できるだけ具体的に記述してください。
- 発生頻度
- ログの記録などの具体的な情報
- 再現テスト手順（特に再現性がある場合）

問題解決のため、おわかりになる範囲で以下の項目等をお知らせください。

4. サーバ機種名
5. サーバ設定の変更等

お客様がサーバの初期設定を変更された場合、「変更事項」と「変更を行った理由」

6. ソフトの利用環境

例えば、以下のような情報が判断材料になります。

・インストールしたサーバOSとそのバージョン
・ネットワーク構成・経路
・上記ネットワーク構成中、どのサーバに製品を導入したか
・クライアントのメーラ・ブラウザなどの情報
・メール送受信の経路上でウイルス対策ソフトが動作しているかどうか
・設定ファイル（/etc/GwAV/GWAV.conf, /etc/GwAV/gwav-mta.conf）

上記以外にも必要な情報のご提供を依頼する場合があります。

■ お問合わせ

株式会社 ギデオン
〒223-0056横浜市港北区新吉田町3382-7
http://www.gideon.co.jp/

●サポートセンター（技術的お問合せ）
E-mail: sp@gideon.co.jp　TEL 045-590-3655

●インフォメーションセンター（その他のお問合せ）
E-mail: info@gideon.co.jp　TEL 045-590-1216

受付時間/9:00～17:00（祝祭日を除く、月～金）

ギデオン ゲートウェイセキュリティ
ユーザーズガイド

2011年3月3日　　第2版発行

発行所　株式会社ギデオン
〒223-0056
神奈川県横浜市港北区新吉田町3382-7
http://www.gideon.co.jp/