GIDEON

共通
ユーザーズ
ガイド

for Linux

ギデオン アンチウイルス
メールサーバ/アンチスパムPlus

はじめに

この度は、製品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、『ギデオン アンチウイルス メールサーバ Ver.3』および『ギデオン アンチウイルス アンチスパムPlus』共通ユーザーズガイドとなっています。本書に記載されているアンチスパム機能については『ギデオン アンチウイルス アンチスパムPlus』にのみ該当する項目です。その他は両製品共通の項目です。

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。

■著作権など

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、データのセキュリティを脅かす危険度は年々上がっています。

このようなスパムメール、ウイルス被害を防ぎ、安心した環境にするには、「メールサーバ上で対策をすること」が、最も有効な方法といえます。

『ギデオン アンチウイルス メールサーバ Ver.3』は、ウイルス、スパイウェアをメールサーバ上で検出・駆除します。感染被害の拡大を防止し、安心して利用できる環境を提供します。『ギデオン アンチウイルス アンチスパムPlus』は、『ギデオン アンチウイルス メールサーバ Ver.3』にアンチスパム機能を追加した製品です。

両製品ともに使いやすいGUI管理ツールを提供し、セキュリティを強化したシステムを提供します。

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
「3.8.1 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「3.8 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
「3.6 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
「3.7 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
- 使いやすいGUI管理画面から設定可能
- MTAのセキュリティを確保し、既存ネットワークの設定変更が不要
- 定義ファイル、モジュールの自動更新機能でメンテナンスフリー

■ 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、メールシグニチャデータベース、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、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、ウイルスを検出、駆除
  （約15万種のウイルスパターン、新種ウイルスに数分間隔で対応）

1.4 推奨動作環境

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/

■ 推奨動作環境

● 対応OS:

Linux 2.4.0 以降 (*1)

glibc バージョン 2.3 以降

● 対応CPU:

インテル社製及びインテル互換CPU

Pentium4 2GHz 以上

● 対応ディストリビューション:

Red Hat Enterprise Linux 3 ～

Turbolinux 10/11 server ～

そのほか RedHat 互換でディストリビュータがサポートを継続しているディストリビューション (*2)

● 対応MTA:

sendmail 8.8.3 以降 (*3)

qmail 1.03 以降 (*4)

postfix 0.0.20000529 以降

● メモリ:
空きメモリ容量 512MB 以上

● ハードディスク:
最低 200MB (インストールに必要な容量)
運用するにはログなどのディスク容量が別途必要になります(*5)。

● 運用端末:
管理用の GUI を利用するためには Adobe Flash Player バージョン 7.0 以上が必要になります(*6)。

注
*1) SELINUX が有効になっている環境では動作保証できません。
また、本製品は32bitで動作するソフトウエアのため、64bit版OSをご利用の場合は32bit互換ライブラリ (glibc/zlib/ncurses) を追加して頂く必要がございます。
*2) 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。
弊社インフォメーションセンターにお問い合わせ下さい。
*3) sendmail.cfには "Mlocal,M*smtp*,Mrelay" の定義が必要となります。
*4) qmailの起動スクリプトで qmail-smtpd を起動する場合、起動プロセスで使用するメモリに制約があるとき、64MBに設定します。
*5) 必要とするディスク容量は運用形態によって異なります。
*6) 運用端末の Flash Player のバージョンが古い場合、文字化けやボタンが正しく動作しない可能性があります。

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上でメールサーバが正常に稼動していること
本製品を導入するメールサーバが、内部または外部ネットを通してメールの送信、受信ができることを確認してください。
リレーホストとして本製品を利用する場合には、すでにリレーホストとして正しく動作しているネットワーク環境であることが前提になります。
本製品をインストールする前に、メールサーバの設定が正しいことを確認してください。

● メール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1GB以上 空きメモリ容量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、以下のようにシステム環境が変更されます。

● sendmailの場合

既存のsendmail.cfが、「アンチウイルス」対応用に変更されます。元のファイルは、以下の名前で保存されます。

sendmail.cf.org.gav

ローカルメール配信は、すでにシステムでインストールされている配信エージェントを用います。例えば、システムにprocmailが存在している場合、そのprocmailを使用します。
同様に、システムにmail.localが存在している場合、そのmail.localを用います。
両方とも存在している場合は、mail.localを使用します。
外部のメールサーバへのメール配信にはsmtpfeedを用います。ただし、すでにシステムがsmtpfeedを使用している場合は、システムのものを利用します。

● qmailの場合

/var/qmail/bin/qmail-queueが、以下の名前に変更され置き換えられます。

/var/qmail/bin/qmail-queue.org.gav

● postfixの場合

既存の /etc/postfix/master.cf および main.cfが、「アンチウイルス」対応用に変更されます。
元のファイルは、以下の名前で保存されます。

/etc/postfix/master.cf.org.gav
/etc/postfix/main.cf.org.gav

1.7 メールサーバの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、メールサーバ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。
メールサーバ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。
メールサーバ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、メール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

メールサーバのプログラムだけでなく、メールサーバの設定ファイル（例えば、sendmail.cf）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、ウイルススキャン後、正しくメールが配信され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。

注意

インストール前の確認
メールサーバが正しく稼動しており、メール送受信が可能であることを確認した後、本製品をサーバにインストールします。
インストールは、あらかじめメールサーバを停止して、メール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。

2.1 インストール準備

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。

2.1.1 CD-ROMドライブ付きサーバ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、インストールします。

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
```

2.1.2 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》製品インストーラをダウンロードする

以下のコマンドで､製品インストーラをダウンロードします。

```
# wget http://download.gideon.co.jp/ginstall.tgz
```

《手順3》製品インストーラを展開する

以下のコマンドで､tgz 形式の製品インストーラを展開します。

```
# tar zxf ginstall.tgz
```


2.2 インストール

2.2.1 メールサーバ Ver.3 の新規インストール

● 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。

```
# cd /mnt/cdrom
# ./ginstall -F -M [MTA名イニシャル] -P AV
```

[MTA名イニシャル]
sendmailの場合:　S
qmailの場合:　Q
postfixの場合:　P

例. MTAがpostfixのメールサーバにメールサーバ Ver.3をインストールする場合

```
# ./ginstall -F -M P -P AV
```

● 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。

```
# ./ginstall -M [MTA名イニシャル] -P AV
```

[MTA名イニシャル]
sendmailの場合:　S
qmailの場合:　Q
postfixの場合:　P

例. MTAがpostfixのメールサーバにメールサーバ Ver.3をインストールする場合

```
# ./ginstall -M P -P AV
```

なお､製品インストーラでは弊社更新サーバなどからHTTP 通信による更新モジュールのダウンロードを行いますが､もし､HTTP プロキシサーバを利用している場合は-p オプションをつけた以下のコマンドでインストールを行ってください。

```
# ./ginstall -p [http://ID:パスワード@ホスト名:ポート番号]
   -M [MTA名イニシャル] -P AV
```

[MTA名イニシャル]
sendmailの場合: S
qmailの場合: Q
postfixの場合: P

例. MTAがpostfixのメールサーバにHTTPプロキシ(ホスト名:proxy.example.com、ポート番号:8080)経由でメールサーバ Ver.3をインストールする場合

```
# ./ginstall -p http://proxy.example.jp:8080 -M P -P AV
```

「お客様登録No」「パスワード」の設定

「3.8.1 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。

※「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。

2.2.2 アンチスパムPlusの新規インストール

● 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。

```
# cd /mnt/cdrom
# ./ginstall -F -M [MTA名イニシャル] -P SP
```

[MTA名イニシャル]
sendmailの場合: S
qmailの場合: Q
postfixの場合: P

例. MTAがpostfixのメールサーバにアンチスパムPlusをインストールする場合

```
# ./ginstall -F -M P -P SP
```

● 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。


```
# ./ginstall -M [MTA名イニシャル] -P SP
```

[MTA名イニシャル]
sendmailの場合: S
qmailの場合: Q
postfixの場合: P

例. MTAがpostfixのメールサーバにアンチスパムPlusをインストールする場合

```
# ./ginstall -M P -P SP
```

なお、製品インストーラでは弊社更新サーバなどからHTTP 通信による更新モジュールのダウンロードを行いますが、もし、HTTP プロキシサーバを利用している場合は-p オプションをつけた以下のコマンドでインストールを行ってください。

```
# ./ginstall -p [http://ID:パスワード@ホスト名:ポート番号]
   -M [MTA名イニシャル] -P SP
```

[MTA名イニシャル]
sendmailの場合: S
qmailの場合: Q
postfixの場合: P

例. MTAがpostfixのメールサーバにHTTPプロキシ(ホスト名:proxy.example.com、ポート番号:8080)経由でインストールする場合

```
# ./ginstall -p http://proxy.example.jp:8080 -M P -P SP
```

「お客様登録No」「パスワード」の設定

「3.8.1 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。

※「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。

2.3 アンインストール

2.3.1 メールサーバ Ver.3 / アンチスパムPlusのアンインストール

アンインストールはroot 権限でログインした上で、以下のコマンドを入力し、Enter キーを押します。

```
# /usr/local/gwav/ginst/guninstall
```

注意

アンインストールする際は、あらかじめメールサーバを停止して、メール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

3.1 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。

3.2 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。

3.3 初回のログイン

本製品ご購入後、はじめて管理･設定画面にアクセスすると、画面3.3 パスワード設定画面が表示されます。
この画面で任意のパスワードを入力します。（半角英数20文字以内）

次回からログインするときには、このパスワードを入力する必要がありますので、忘れずにパスワードの記録を保管してください。

※下記画面を正しく表示するには、お使いの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。

画面3.3

3.4 ログイン

前項で説明した初回のログイン以後は、管理･設定画面にアクセスすると、画面3.4 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。

Qube3/Qube3Plus/MMQUBE2/MMQUBE2Plus で「アンチウイルスメールサーバ Ver.3」にアップグレードした場合

初期パスワードとして"gwantivirus" が設定されていますので、入力してログイン可能です。パスワードはすぐに変更することをお勧めします。

パスワードの変更

画面3.4 ログイン画面で既存のパスワードを入力して［変更］ボタンをクリックすると、画面3.3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3.4

3.5 概説

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

■初期に設定およ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)の設定確認、HTTPプロキシ経由で更新する場合の設定、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などが可能です
他サービス	アンチウイルスメールサーバー上で重要なサービスの状況を表示し、またウイルスチェックするネットワーク範囲の指定が可能です
サーバ環境	初期システム設定を行います

3.6 更新状況

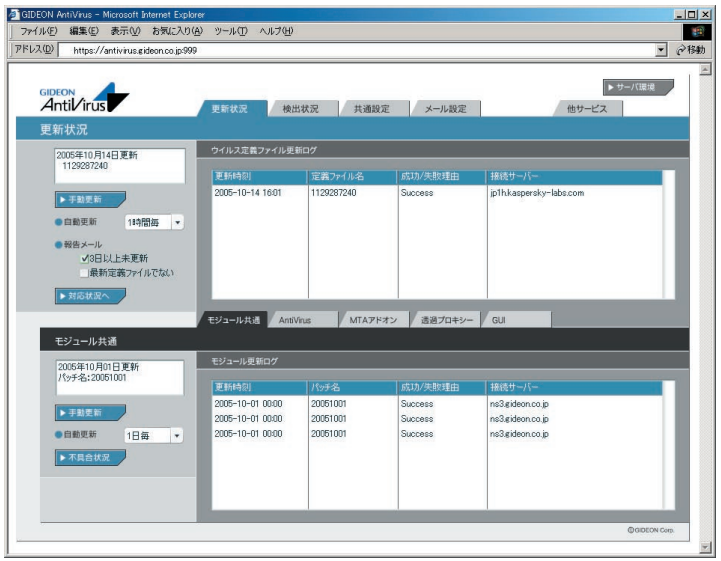
●ウイルス定義ファイル更新ログ（画面3.6 上段部分）

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。



画面3.6

●モジュール更新ログ（画面3.6 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。

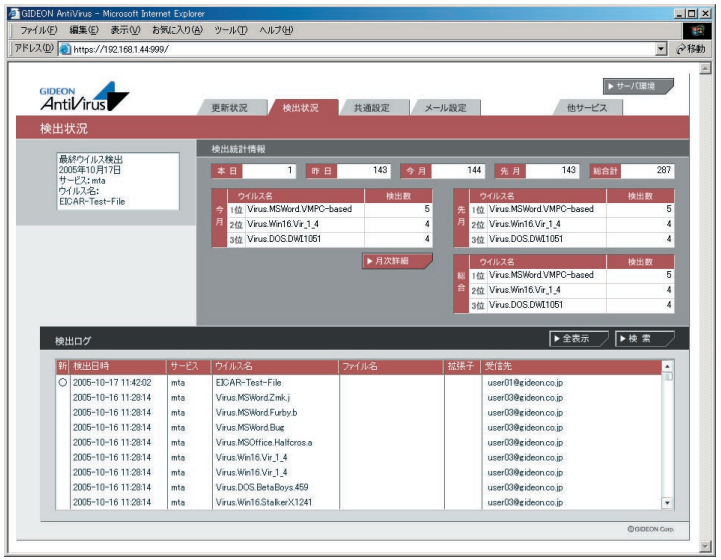
個別のモジュール群（AntiVirus MTAアドオン 透過プロキシー GUI）の更新状況は、各タブをクリックすると表示されます。

3.7 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3.7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100KBまでの検出ウイルスを表示します。
［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3.7

3.8 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3.8.1が表示されます。
各種設定を行った後に［ページのアンドゥ］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。
［ページの初期化］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。

3.8.1 基本設定

●ライセンス

ユーザ登録時に発行された「お客様登録No」「パスワード」を入力します。
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

管理者のメールアドレスを登録すると、ウイルスの検出時に管理者にも警告メールを送信します。またその他のウイルスに関するレポートなども送信します。
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。複数アドレスを指定する場合は、下記のように半角スペースで区切ります。

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

※ネームサーバで解決できない内部メールサーバ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。

画面3.8.1

3.8.2 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3.8.2が表示されます。

●メール送信で使用するSMTPサーバ

警告メールなどを送信するために使うメール（SMTP）サーバを指定します。

例えば、自社の正式なメールサーバ名（FQDN）が、mail.domain.jpであれば、そのメールサーバ名を指定します。

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

本ソフト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

ウイルス検知された感染メールを保存するためのディレクトリを指定します。

保存用ディレクトリを作成し（例 /var/tmp/virus）、ルートディレクトリから指定してください。

保存容量とは、保存する容量の上限値を入力します。この上限値を超えた場合、古いデータから消去されますのでご注意ください。

入力後、［更新］ボタンをクリックしてください。

初期設定値：なし

画面 3.8.2

3.8.3 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3.8.3が表示されます。

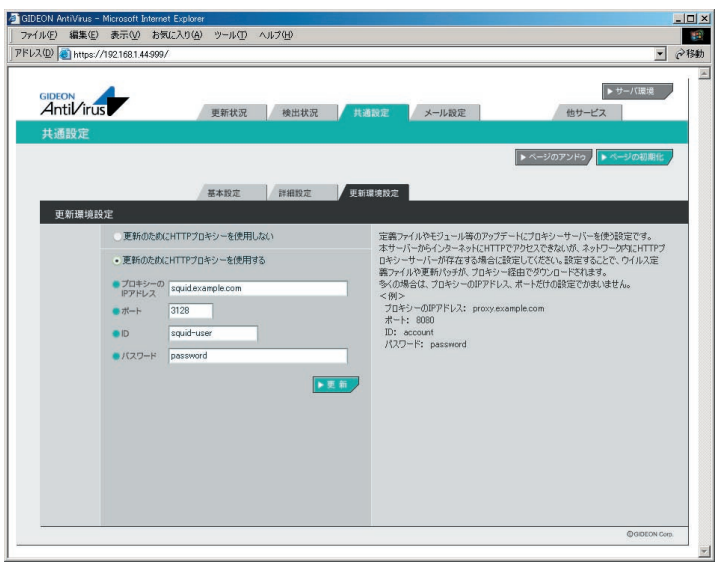
本製品は外部HTTPサイトにアクセスすることで、モジュールおよび定義ファイルを更新します。特定のHTTPプロキシサーバを経由しないと外部のURLにアクセスできない場合には、「更新のためにHTTPプロキシーを使用する」を選択してください。

「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

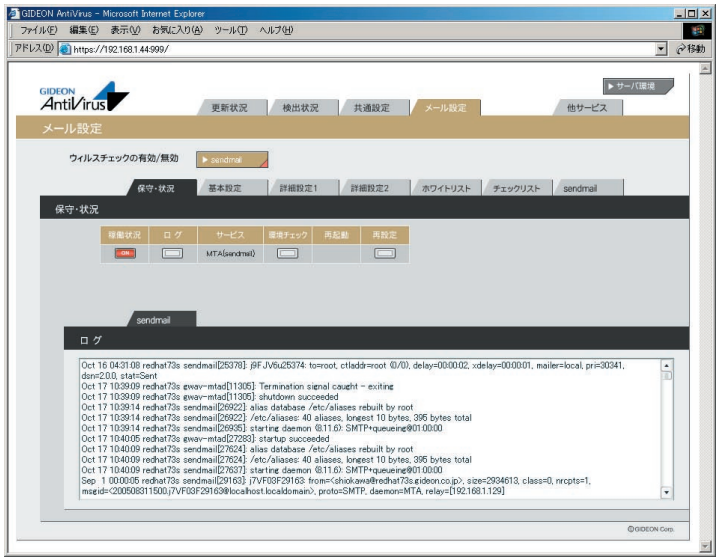


画面 3.8.3

3.9 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、画面3.9が表示されます。ここでは主にメールサーバプログラム（MTA）に関係する管理･設定をおこないます。

現在利用しているメールサーバ（sendmail、postfix）に応じて表示されます。qmailご利用の場合はsendmail、postfixに類した設定項目がないので、画面3.9のsendmailタブは表示されません。



画面3.9

3.9.1 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3.9.1が表示されます。

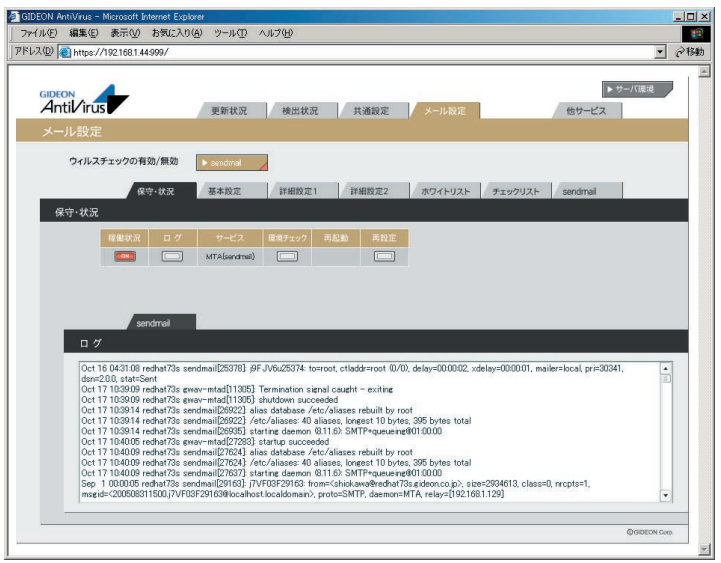
稼働状況　：ONはメールサーバデーモンが有効になっておりサービス稼動中です。OFFはメールサーバ停止中です。

ログ　：最新のログを取得し、下のログ一覧に表示します。

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。

再起動　：(本製品では使用しません。)

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再設定ボタンをクリックします。



画面3.9.1

3.9.2 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3.9.2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、受信者にメールを送信する

●送信者への警告メール設定

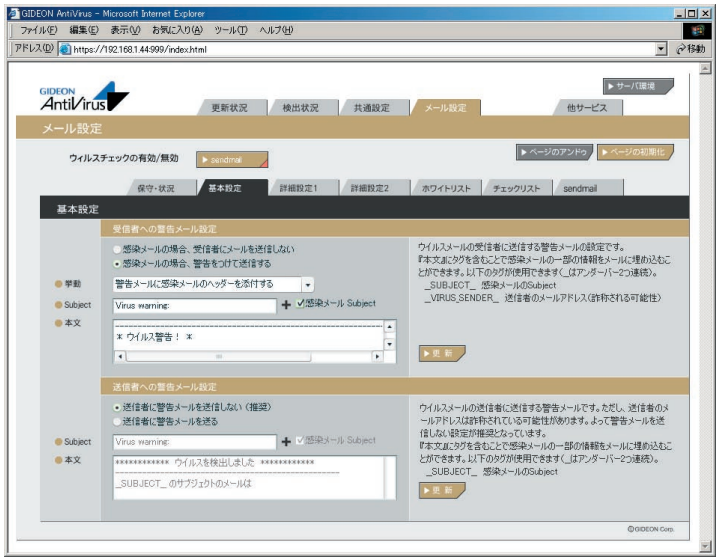
メールがウイルスに感染していた場合に、メールの送信者に送る警告メールについての設定です。

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。



画面3.9.2

3.9.3 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3.9.3が表示されます。

●チェックに使用するポート

●監視する接続先のポート

●送信元IPアドレスの復元

上記3項目は本製品では使用しません。

●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。「3.8.1 基本設定」で設定した、警告メールの送信先へ送信します。

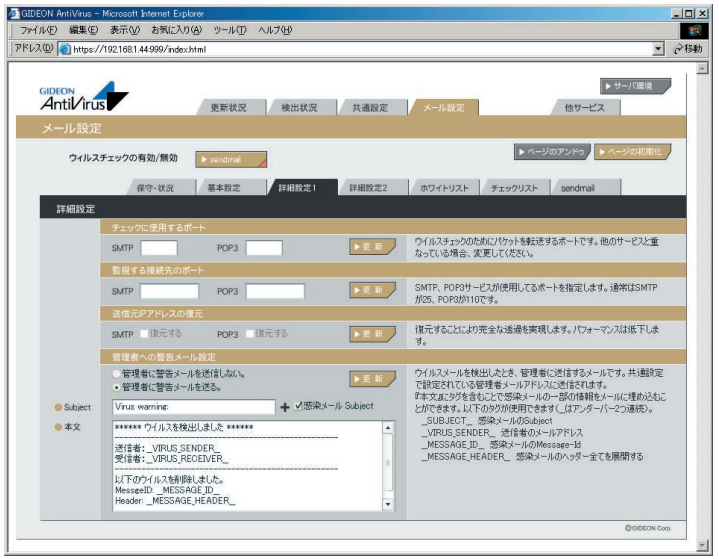
Subject ：警告メールのサブジェクト名と感染メール Subject（元メールのサブジェクト）を連結することができます。

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3.9.3

3.9.4 詳細設定 2

メール設定画面の「詳細設定2」タブをクリックすると、画面3.9.4が表示されます。

●ウイルス感染メールの保存

ウイルス感染したメールを、特定のディレクトリに保存することができます。
隔離ディレクトリの設定は、「3.8.2 詳細設定」の「感染メール保存ディレクトリ設定」で行います。

その他のメニューにつきましてはサポートしておりません。

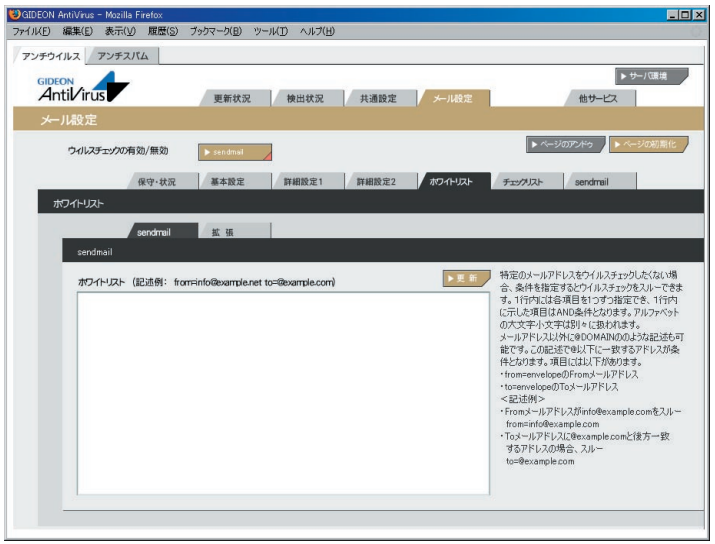
画面3.9.4

3.9.5 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3.9.5が表示されます。

ホワイトリストの欄に、ウイルスチェックの対象から除外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ウイルスチェック対象外となります。それ以外はすべてウイルスチェックされます。

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。

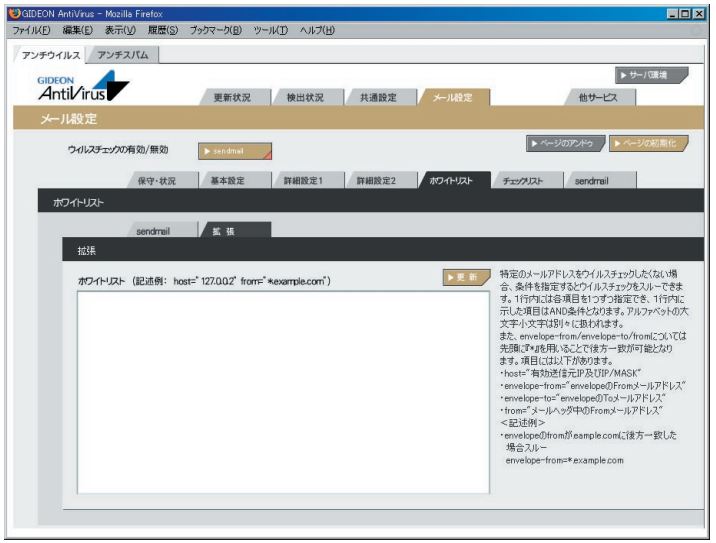


画面3.9.5

拡張ホワイトリスト設定

アンチウイルス設定画面の上部「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「拡張」タブをクリックします。拡張ホワイトリスト設定では従来の画面では設定できなかった部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

管理GUI上で新たに表示される以下のタブ画面から設定を行います。



画面 3.9.5-2

拡張ホワイトリスト記入上の注意

(1)設定の際は、従来のホワイトリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)sendmailの場合でのエンベロップToは自サーバのFQDN(ホスト名)に対応していません。
これは自サーバ上で管理しているバーチャルドメインのFQDNも含みます。
自サーバのFQDNを指定する場合は、envelope-to="*localhost"というようにFQDNをlocalhostに変更してください。

(3)拡張ホワイトリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

-----例1-----
ホストのIPアドレスが127.0.0.0～127.0.0.255の範囲にある場合:
host="127.0.0.0/255.255.255.0"

エンベロップFromのメールアドレスを記述する場合:
envelope-from="*.from_address_domain"　の後方一致のマッチング
もしくは
envelope-from="from_address"　完全一致

-----例2-----
エンベロップfromが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストにおけるアカウントを対象とする場合:
envelope-from="*.gideon.co.jp"

エンベロップToのメールアドレスを記述する場合:
envelope-to="*.to_address_domain"　の後方一致のマッチング
もしくは
envelope-to="to_address"　完全一致

-----例3-----

エンベロップToが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストに　おけるアカウントを対象とする場合:

envelope-to="*.gideon.co.jp"

From フィールドのアドレス部を記述する場合:

from="*.from_address_domain"　　の後方一致のマッチング

もしくは

from="from_address"　　完全一致

-----例4-----

Fromが@△.example.com(△はh2～h9、k2～k9、m2～m9)

のアカウントの場合:

from="*.example.com"

From フィールドのアドレス部を記述する場合:

from-name="name"

※from-name,subjectにおいて日本語を指定したい場合はRFC2047形式で記述。

-----例5-----

送信元名が「GIDEON」の場合:　from-name="GIDEON"

送信元名が「ギデオン」の場合:

from-name="=?ISO-2022-JP?B?GyRCJS4lRyUqJXMbKEIA?="

x-mailer フィールドのメーラ名を記述する場合(前方一致)

x-mailer="mailer name *"

-----例6-----

Outlook　Express5:　x-mailer =" Microsoft Outlook Express 5.* "

·Outlook　Express6:　x-mailer =" Microsoft Outlook Express 6.* "

·Outlook2000:　x-mailer =" Microsoft Outlook IMO, Build 9.*"

·Outlook2002:　x-mailer =" Microsoft Outlook, Build 10.*"

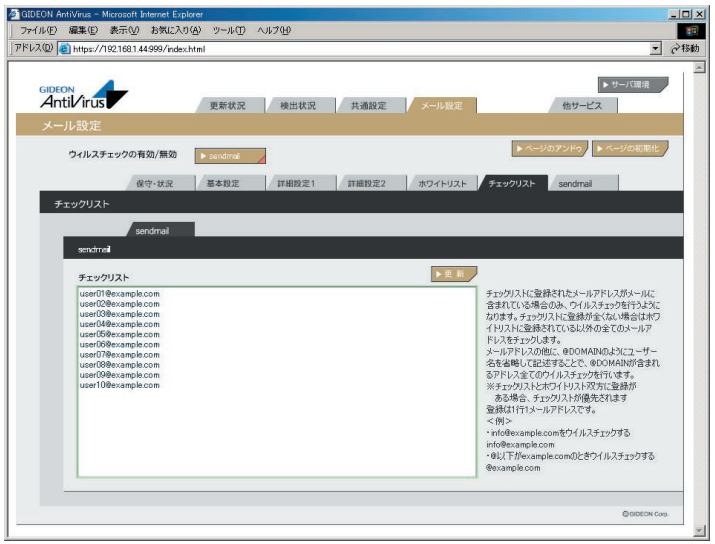
·Outlook2003:　x-mailer =" Microsoft Office Outlook, Build 11.*"

すべてAND条件の場合、以下のように半角スペースにて区切ります。

from="address" from-name="from name" x-mailer="mailer name"

3.9.6 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3.9.6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。



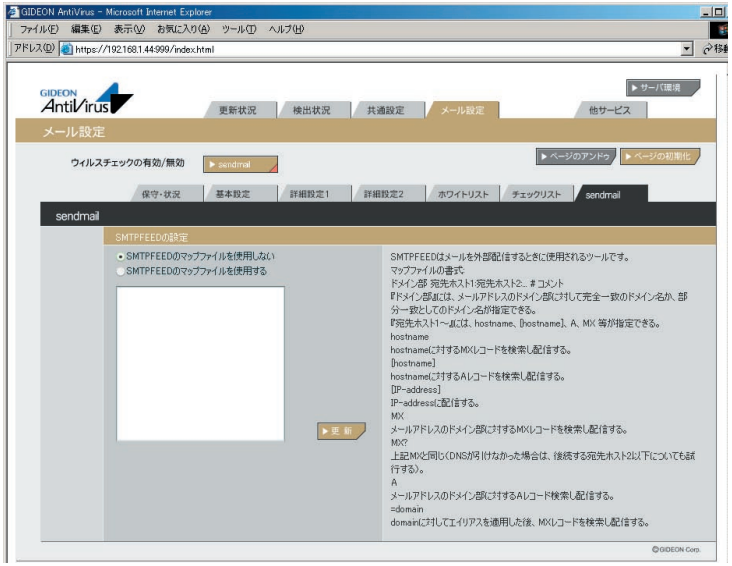
画面3.9.6

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1件でも登録がある場合、ホワイトリストの内容は無効になりますのでご注意ください。

3.9.7 sendmail

sendmailを利用している場合、メール設定画面に「sendmail」タブが表示されます。「sendmail」タブをクリックすると、画面3.9.7が表示されます。



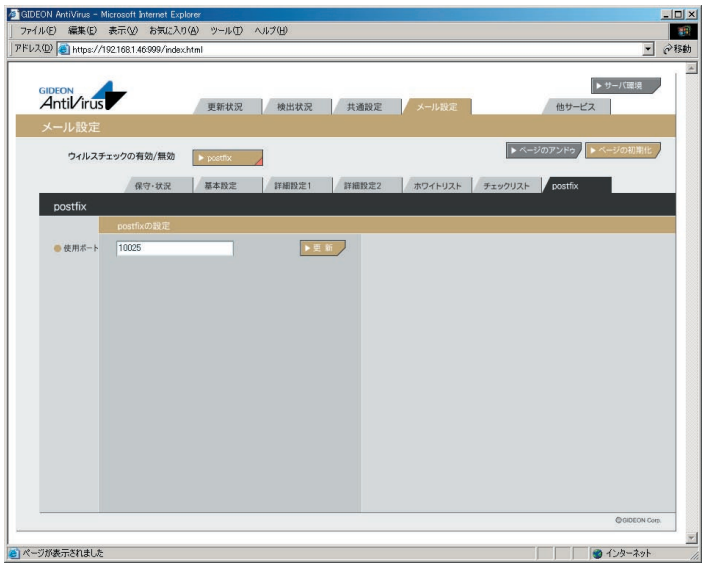
画面3.9.7

sendmailの場合は、本製品がインストールされたことにより、外部送信プログラムとしてsmtpfeedが使われるようになります。ここでは、smtpfeedの各種設定が可能です。特に、特定のドメインに対して特定のリレーサーバを指定したいときに、マップファイルの記述が必要になります。空欄に必要な行を記述します（複数行指定可能です）

3.9.8 postfix

postfixを利用している場合、メール設定画面に「postfix」タブが表示されます。「postfix」タブをクリックすると、画面3.9.8が表示されます。

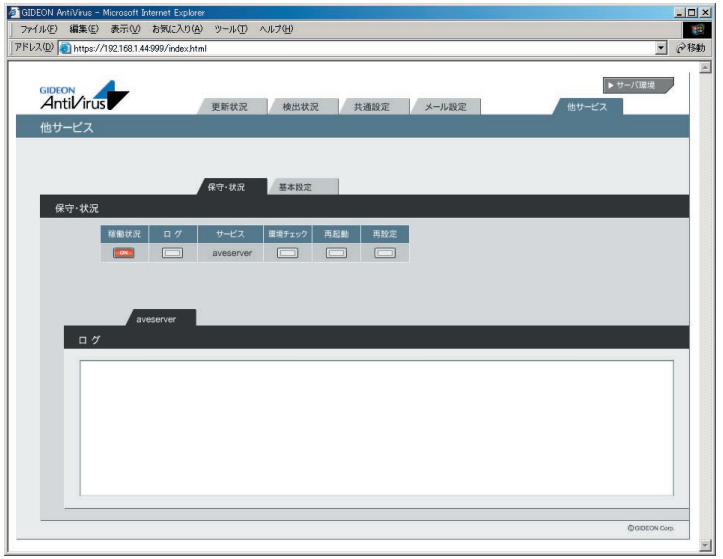
postfixの場合は、本製品がインストールされたことにより、ウイルス検出プログラムは内部のメール送信ポートを利用します。使用ポートの欄にそのポート番号を指定してください。通常は10025番ポートが使用されます。



画面3.9.8

3.10 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3.10が表示されます。「保守･状況」では本製品でウイルス検知する上で重要なサービスの状況を表示します。「基本設定」ではウイルスチェックするネットワーク範囲を指定できます。



画面3.10

3.10.1 保守･状況

「aveserver」とはアンチウイルススキャンエンジンに接続するための常駐デーモンです。

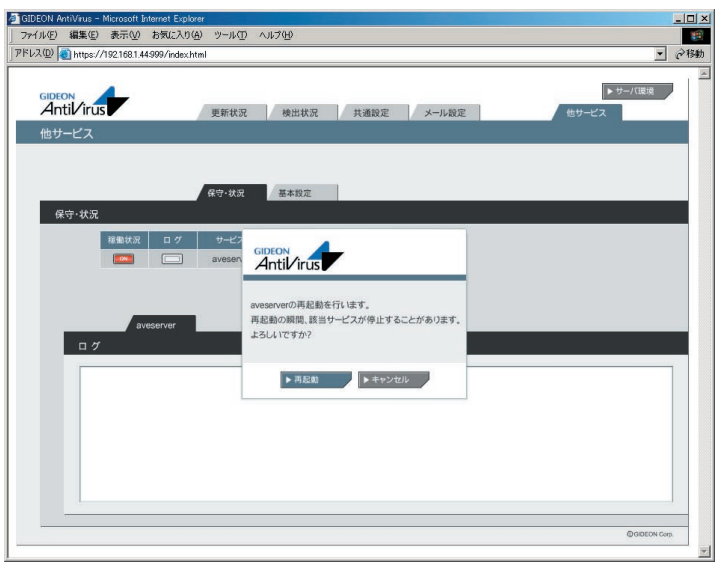
稼働状況 ：ONはサービス稼動中です。
OFFはサービス停止中です。

ログ ：最新のログを取得し、下のログ一覧に表示します。

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。

再起動 ：再起動ボタンをクリックすると、画面3.10.1が表示されます。
［再起動］ボタンをクリックするとサービスを再起動させます。

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再設定ボタンをクリックします。



画面3.10.1

3.10.2 基本設定

ウイルスチェックするネットワークの範囲を指定できます。
192.168.1.0/255.255.255.0 のような形式で記述します。
ここで指定行が存在する場合、マッチした範囲だけウイルスチェックの対象となり、その他のネットワークはウイルスチェックしません。

画面3.10.2

3.11 サーバ環境

画面右肩の［サーバ環境］ボタンをクリックすると画面3.11.1が表示されます。

3.11.1 保守･状況

●ネットワーク

本製品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、ローカルシステムで検出したネットワークに関連する情報を表示します。初期設置時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。

●サーバ状態

時刻 ：システムの内部時計の時刻

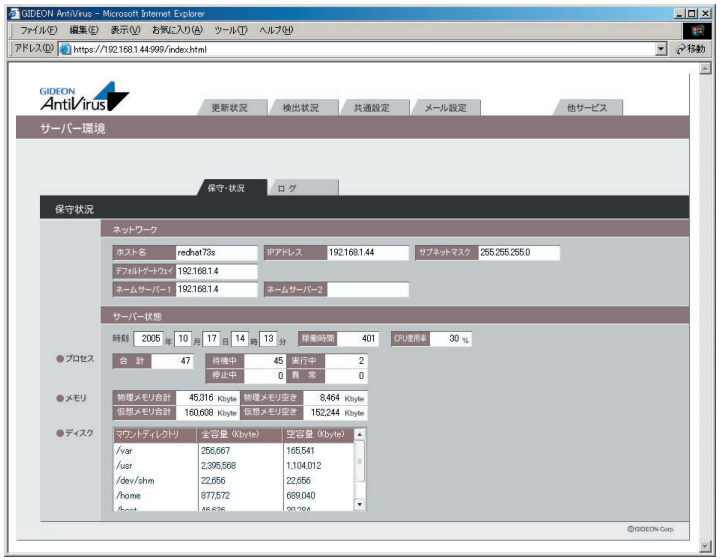
稼働時間 ：システムの連続稼働時間

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。

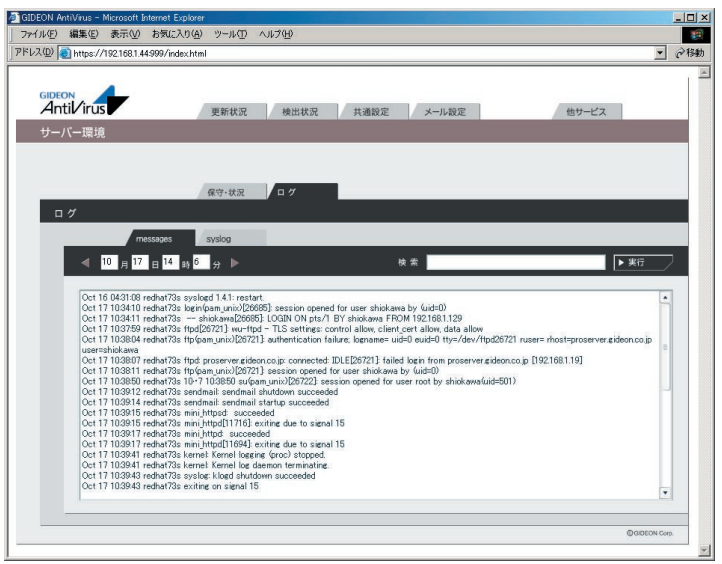
ディスク ：ディスクの使用容量（KB）を表示します。通常は十分な空き容量が残っています。空き容量が極端に少ない場合、再起動することを推奨します。



画面3.11.1

3.11.2 ログ

サーバ環境画面の「ログ」タブをクリックすると、画面3.11.2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は特定のエラーを絞ることができます。



画面3.11.2

3.11.3 スキャンコード一覧

メールログに“SCANNED:X”として表示される、Xの番号について説明します。

数値	状況
0	ウイルスに感染していない
1	aveserverに接続することができない
3	ウイルスである疑いがある
4	ウイルスに感染している
6	スキャン結果不明 （暗号化されている、パスワードが掛かっている）
7	gwavが原因のエラー （ファイルが見つからない、ファイルを読むことができない）

上記スキャンコードは、受信者宛の元メールに“Virus Check ERROR (X)”という記述が付加されます。
数値が“0”の場合は元のメールをそのまま配信します。それ以外の場合は警告を付加して配信します。

本製品を、メールサーバにインストール後、実際に動作するかどうかを検証します。
本製品には、sampleディレクトリに、テスト用ウイルスファイル「eicar.com」が収録されています。ウイルス検出機能の動作確認をする場合にご利用ください。
なお、このウイルスファイルは無害であり、ウイルスに感染することはありません。

注意

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。

第4章 動作確認

4.1 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1　サーバ上でコマンドを実行する場合

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/gwav-checker --virus-test name
```

上記のコマンドを実行すると、指定した送信者（「name」）へウイルス検出用メールを送信します。
コマンドパラメータ「name」には、本製品を導入したサーバ上に存在するローカルユーザアカウント、「postmaster」などの管理者アカウント、または受信可能な正式なメールアドレス（aaa@bbb.ccc）を指定します。

注意

qmailを利用している場合は、ドメインの最後に「.」を付けてください。
「@gideon.co.jp」ではなく「@gideon.co.jp.」と記述します。

-----例-----

(1) 本製品を導入したメールサーバに、「sato」というメールアカウントが存在する場合、以下のコマンドでウイルス検出用メールを送信します。

```
#/usr/local/gwav/gwav-checker --virus-test sato
```


(2) 正しく動作した場合、ウイルスが検出され、警告メールが受信者（「sato」）に届きます。

警告メールではなく、通常のメールとして受信した場合は、「アンチウイルス」の設定が間違っているか、またはメールサーバの設定が間違っている可能性があります。
例えば、メールサーバがsendmailの場合、sendmailパッケージに含まれるsendmail.cfを間違った記述で変更すると、本製品が正常に動作しなくなる可能性があります。

●テスト方法2　メールクライアントからメールを添付する場合

(1) 本製品を導入したサーバへ、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。

4.2 メールログでの確認

前述の方法でメールを受信すると、メールログにもウイルスを検出したログが記録されます。
メールログは、「3.9.1 保守・状況」でログ一覧が表示されます。
ログファイル内で、「SCANNED:X（Xはスキャンコード数値）」という記載があることを確認してください。

4.3 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、動作するために必要な日本語詳細情報をメールで取得できます。

(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/gwav-checker --mail
```

送信先は、ウイルス検出の場合に報告する、宛先メールアドレスになります。この送信者の初期設定は、postmasterになっています。
ウイルス検出の場合に報告する宛先メールアドレスについては、「3.7 メール」を参照してください。

(2) システムや設定ファイルの内容などの情報もメールで取得する場合、以下のコマンドを実行します。

```
#/usr/local/gwav/gwav-checker --all --mail
```

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。

4.4 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/faq/

第5章 ファイルチェック機能

本製品の主機能はメールサーバ(MTA)向けアンチウイルスソフトウェアですが、付加機能として、特定ディレクトリを指定して定期的にウイルスチェックする機能があります。またその結果をメールで報告します。

5.1 概要

/etc/GwAV/checkdirファイルに、チェックするディレクトリリストを記述します。そして、/usr/local/gwav/gwav-file-controlコマンドにより、ウイルスチェックの周期などを設定します。

-----例-----

1日に1度、/var/wwwディレクトリをチェックする場合、root権限で以下のイタリック部分のコマンドを実行します。1日に一度チェックする場合は「d」を指定します。

```
# /usr/local/gwav/gwav-file-control
==== Local file-system scanning setting ====
 Interval□None/Daily/Weekly/Monthly□ [none]: d
 Start time□hh:mm□ [01:30]: 01:30
 Checked directories□delimitation is space□ []: /var/www
----------------------------------------
Interval: daily, 01:30 - every day
Directory-list:
 /var/www
----------------------------------------
```


注意

ウイルス検出時には、処理負荷が大きくなりますので、特定のディレクトリに限って利用されることを推奨します。特に、"/(ルート)"パーティションの指定は避けてください。

ファイルチェック中にメールのウイルス検出を行うと、メール処理が遅くなったり、場合によってはメール処理ができない可能性もあります。
このようなメール処理に与える影響を考慮し、ファイルチェックの所用時間および負荷を検討した上で、日常の運用・管理を行ってください。

5.2 ディレクトリリストの記述

ディレクトリリストは、/etc/GwAV/checkdirファイルに記述します。ウイルスチェックは、ディレクトリリスト1行ごとに行われます。
ディレクトリリストに記述されていない場合、ウイルスチェックは実行されません。

●ディレクトリ名の書式について

ディレクトリ名は、/home/sambaのように「/」で始まるリスト文字列を記述します。ディレクトリの書式として、/bin/shが解釈可能なメタ文字(*,?など)が使用できます。

-----例-----

/home配下のディレクトリで、そのディレクトリがpublic_html
ディレクトリを持つ場合は、以下のように指定します。

```
/home/*/public_html
```

●文字コードの扱いについて

ファイル名に全角文字を使用している場合、ディレクトリリストの文字のエンコーディングの種類を指定することで、日本語文字（ISO-2022-JP）コードに正しく変換され、報告メールに表示されます。サポートしているエンコーディングの種類は、以下のとおりです。

［エンコーディングの種類］

シフトJISコード	: CP932
EUC コード	: EUC-JP
Samba-CAP コード	: Samba-CAP
Samba-HEX コード	: Samba-HEX
Unicode（UTF-7）	: UTF-7
Unicode（UTF-8）	: UTF-8

エンコーディングの種類は、ディレクトリリストの行の2つ目の項目に、半角スペースまたはタブで区切って記述します。
ただし、sambaで使用しているディレクトリについては、設定ファイルからエンコーディングの種類を自動判別するので、記述する必要はありません。

-----例-----

/home/shareディレクトリ内ファイル名で、シフトJISコードで記述されている場合、以下のように指定します。

```
/home/share CP932
```


5.3 実行結果の報告

指定されたディレクトリのウイルスチェックが完了すると、その実行結果がメールで報告されます。
報告先は、/etc/GwAV/GWAV.confの中のVIRUS_REPORT_TOで指定したメールアドレスになります。
メールのサブジェクトは、以下の形式で記述されます。
[AntiVirus for Linux] directory report（YYYY-MM-DD hh:mm:ss）

YYYY-MM-DD hh:mm:ssは、チェック開始日時を示します。

リスト6-3は、/etc/GwAV/checkdirに/var/spool/*　EUC-JP
が記述されている場合の、ウイルスチェック実行結果の報告メールです。

```
Subject: [AntiVirus for Linux] directory report
□2005-10-17 01:30:37□
From: アンチウイルスシステム <MAILER-DAEMON@example.com>
To: antivirus-info@example.com
START: 2005-10-17 01:30:37
  END: 2005-10-17 01:30:43
Directory list:
  /var/www
Result message:
  /var/www
  ウイルスに感染しているファイルはありません。
  --------
  [17-10-2005 01:30:38 I] Kaspersky Anti-Virus On-
Demand Scanner for Linux. Version 5.5.2/RELEASE
build #92, compiled May 23 2005, 19:19:43
  [17-10-2005 01:30:38 I] Copyright □C□ Kaspersky
Lab, 1997-2005.
..........
  [17-10-2005 01:30:41 I] There are 145215 records
loaded, the latest update 17-10-2005
  [17-10-2005 01:30:41 I] Config file: /usr/local/
gwav/ave/kav/5.5/etc/kav4unix.conf
  [17-10-2005 01:30:41 I] The scan path: /var/www
  [17-10-2005 01:30:42 I] Scan summary: Files=298
Folders=10 Archives=0 Packed=0 Infected=0
Warnings=0 Suspicios=0 Cured=0 CureFailed=0
Corrupted=0 Protected=0 Error=0 ScanTime=00:00:02
ScanSpeed=425.134 Kb/s
```

リスト5-3

5.4 ファイルチェックの設定方法

ファイルチェックの周期などの設定を行う場合、以下のイタリック部分のコマンドを実行します。

指定されたディレクトリリストを対象に、1日に一度の周期でチェックする場合、以下のように指定します。

指定する周期の最初の文字を、大文字または小文字で入力し、Enterキーを押します。例えば、Dailyを指定する場合、「*D*」または「*d*」を入力します。

```
# /usr/local/gwav/gwav-file-control
==== Local file-system scanning setting ====
  Interval□None/Daily/Weekly/Monthly□ [none]: d
  Start time□hh:mm□ [01:30]: 01:30
  Checked directories□delimitation is space□ []: /var/www
----------------------------------------
Interval: daily, 01:30 - every day
Directory-list:
  /var/www
----------------------------------------
```

周期(Interval)設定:

None	ファイルチェックを行わない
Daily	1日に一度ファイルチェックを行う
Weekly	1週間に一度ファイルチェックを行う
Monthly	1ヶ月に一度ファイルチェックを行う

ファイルチェックの設定内容を確認する場合、以下のコマンドを実行します。

```
# ./gwav-file-control --status
```

5.5 sambaによるファイル共有に関する情報

sambaによるファイル共有を行っている場合、以下のコマンドを実行して、現在の設定を確認できます。

```
# /usr/local/gwav/samba-info --all
```

リスト5-5は、このコマンド実行結果を表示した例です。

```
command: /usr/sbin/smbd
config: /etc/samba/smb.conf
directory: /home/share /var/www
client-code-page: 932
coding-system: cap
```

リスト5-5

5.6 コマンドの使い方について

/usr/local/gwavにある以下のコマンドの利用方法については、--helpオプションで表示されます。

```
/usr/local/gwav/gwav-file --help
/usr/local/gwav/gwav-file-control --help
/usr/local/gwav/samba-info --help
```

第6章 アンチスパム設定

6.1 アンチスパム機能動作までの手順

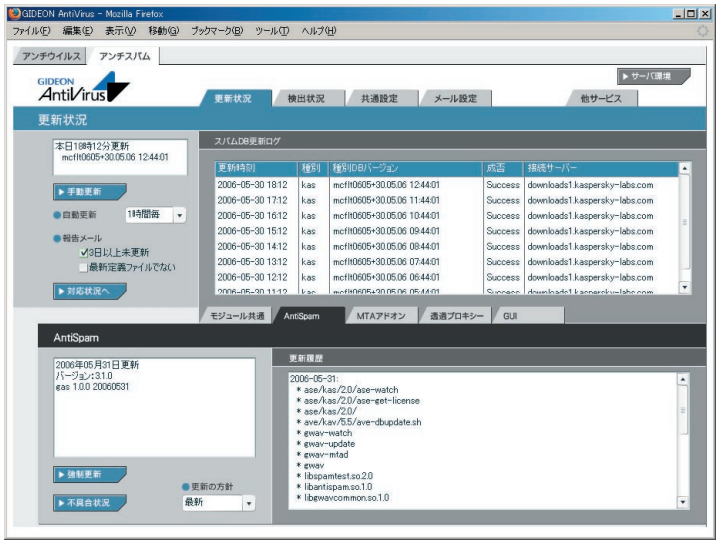
アンチスパムPlusを導入後、アンチスパム機能を正しく動作させるために、以下の手順に従い設定してください。

《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、「第3章 アンチウイルス設定」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、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6.1

《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、その時点で最新の定義ファイルの取得を行います。

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

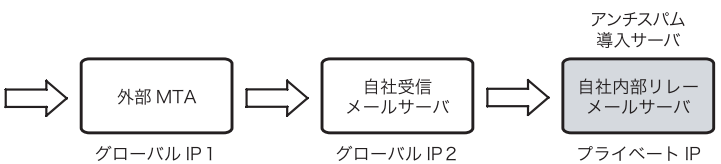
アンチスパム設定画面の「メール設定」タブをクリックします。続いて「詳細設定2」タブをクリックします。

アンチスパムPlus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。

したがって本製品を導入したサーバと、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」欄に、本製品を導入したメールサーバ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にアンチスパムを導入した場合を例にとります。

- アンチスパム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。グローバルIP2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、グローバルIP1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。

重要

メール受信の経路上にある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。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情報などを参照してください。

《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「詳細設定2」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.comに転送され、実際のユーザへの配信は停止します。本書「3.9.4 詳細設定2」の説明を参照してください。

注意

事前にメールサーバ上に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。

6.2 アンチウイルスとの共通機能について

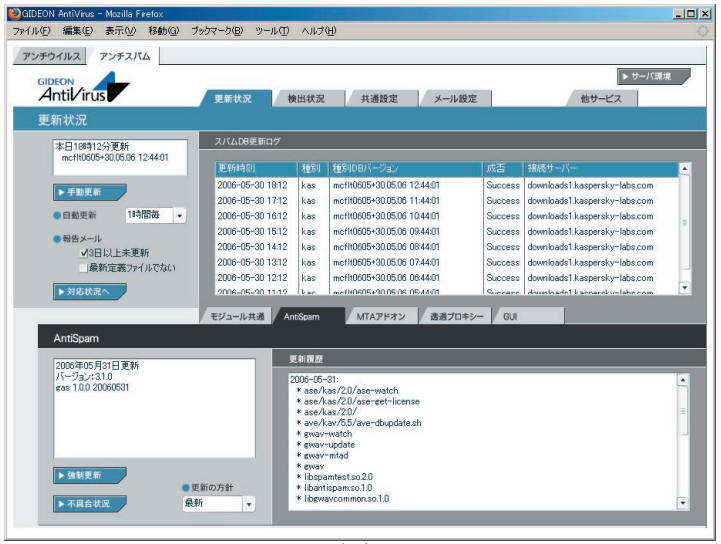
本書では、アンチウイルスと共通の機能については説明を割愛しています。以下の項目については「第3章 アンチウイルス設定」を参照してください。

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

6.3 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（種別：kas)が利用するスパムDB を更新します。



画面6.3

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。

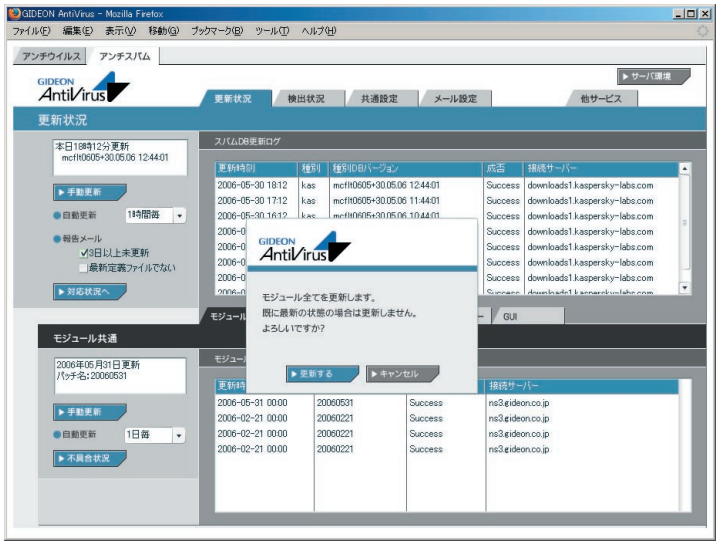
「報告メール」は、スパムDB の更新状況をメールでお知らせするものです。
「3 日以上未更新」は、3 日以上スパムDB の更新がない場合に管理者宛にメール送信します。
「最新定義ファイルでない」は、システム上のスパムDB が最新でない場合に管理者宛にメール送信します。

[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。



画面6.3-2

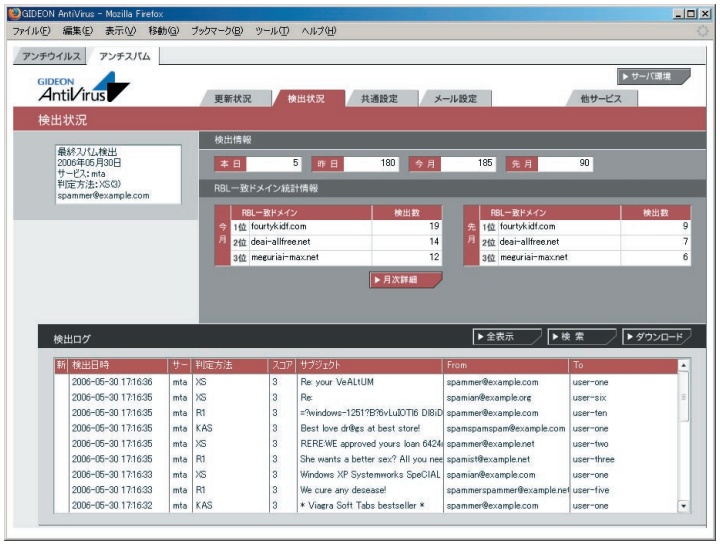
6.4 検出状況

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。



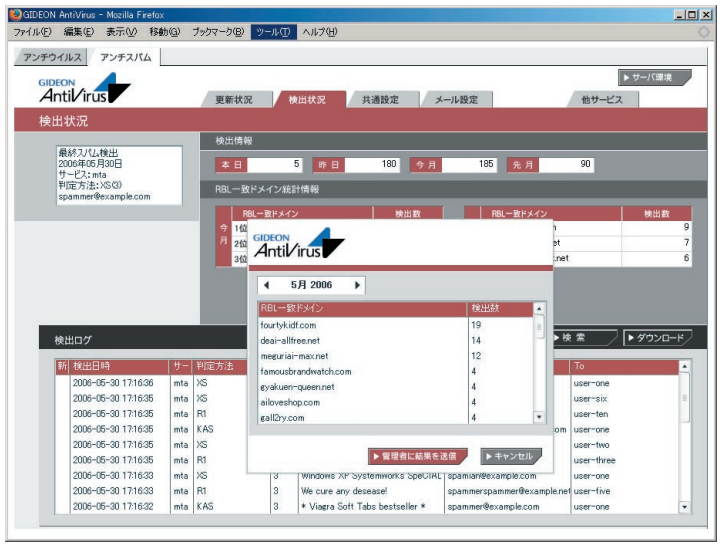
画面6.4

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ひとつである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。

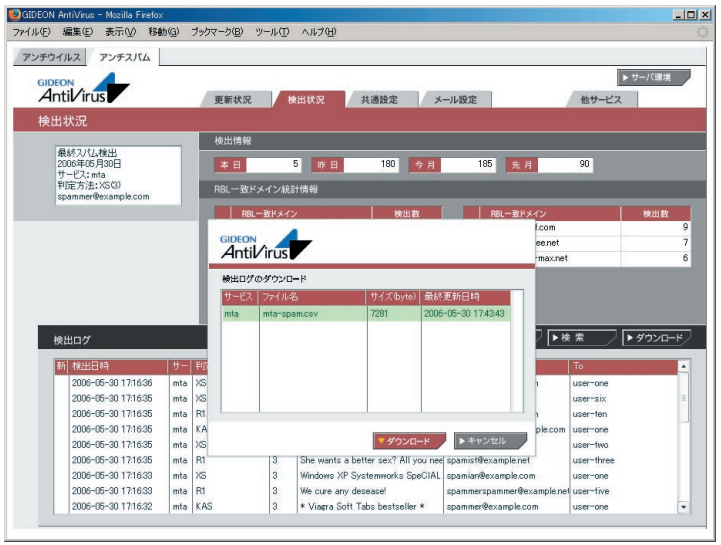


画面6.4-2

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6.4-3

6.5 メール設定

6.5.1 保守･状況

本項は、アンチウイルスでの設定と共通です。詳細は本書「3.9.1 保守 ･状況」を参照してください。

6.5.2 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。アンチスパムPlusで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6.5.2

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。
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づく判定
・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。

注意

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**: メールサーバ版では使用しないため無効化してあります。

・**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。

6.5.3 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。

（注）上記の項目以外は、メールサーバ版では無効化されています。

画面6.5.3

6.5.4 詳細設定2

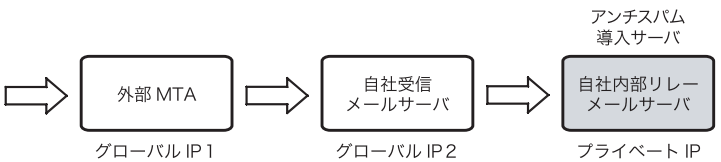
アンチスパム設定画面の上部「メール設定」タブをクリックし、続いて「詳細設定2」タブをクリックします。

スパム判定で除外するグローバルIPアドレス

アンチスパムPlus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。したがって本製品を導入したサーバと、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、本製品を導入したメールサーバで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-----



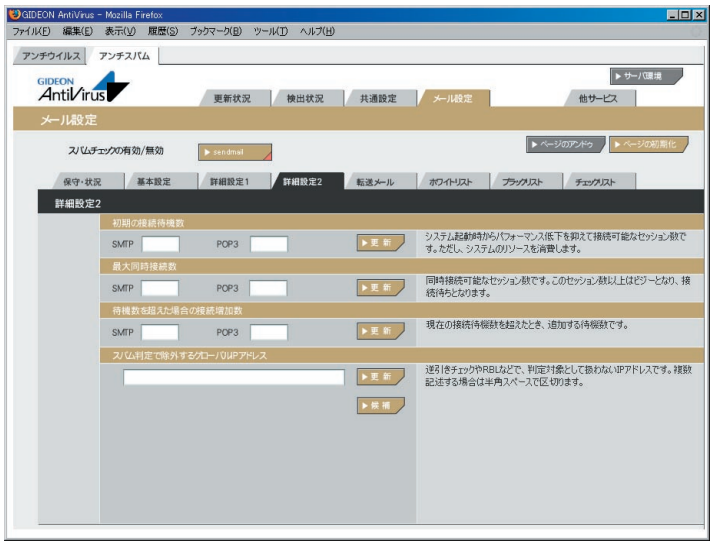
上記の経路で外部からのメールを受信し、自社内部リレーメールサーバにアンチスパムを導入した場合を例にとります。

- アンチスパム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。グローバルIP2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、グローバルIP1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。

重要

メール受信の経路上にある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。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情報などを参照してください。



画面6.5.4

6.5.5 転送メール設定

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します。

「受信先への配信を停止する」をチェックすると、ユーザにはスパムメールが配信されず、転送指定先へメールが転送されます。

画面6.5.5

転送の指定方法

転送対象のメールアドレスを行頭から指定し、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@ 以下が一致するメールアドレスをすべて転送対象にできます。

(注)大文字、小文字を区別するため、user@example.com と

USER@EXAMPLE.COM とは別個のアドレスとなります。

-----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
```

sendmail ローカル配信の場合の注意事項

sendmailがローカルのユーザへ配信する場合、 アドレスの "@domain" 部分を削除して配信するためローカルのホスト名を指定する必要があります。

sendmail.cf もしくはsendmail.cw もしくはlocal-host-names 等にローカルホストが記述されていない場合、/etc/hostsで記載されているホスト名を参照します。
もしこれらにローカルホスト名が記載されていない場合、user@localhost のようにローカルユーザ名の後に@localhost を付加してください。

6.5.6 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

有効送信元とは、前項の「2.3.4 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。

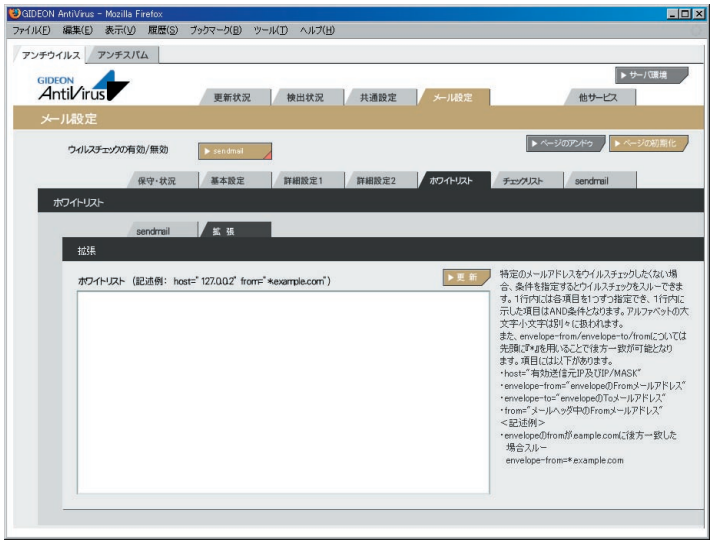
```
host=192.168.1.2 from=@example.net
```

画面 6.5.5

拡張ホワイトリスト設定

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「ホワイトリスト」タブ「拡張」タブをクリックします。拡張ホワイトリスト設定では従来の画面では設定できなかった部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

管理GUI上で新たに表示される以下のタブ画面から設定を行います。



画面 6.5.5-2

拡張ホワイトリスト記入上の注意

(1)設定の際は、従来のホワイトリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)sendmailの場合でのエンベロップToは自サーバのFQDN(ホスト名)に対応していません。
これは自サーバ上で管理しているバーチャルドメインのFQDNも含みます。
自サーバのFQDNを指定する場合は、envelope-to="*localhost"というようにFQDNをlocalhostに変更してください

(3)拡張ホワイトリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

-----例1-----
ホストのIPアドレスが127.0.0.0～127.0.0.255の範囲にある場合:
host="127.0.0.0/255.255.255.0"

エンベロップFromのメールアドレスを記述する場合:
envelope-from="*.from_address_domain"　の後方一致のマッチング
もしくは
envelope-from="from_address"　完全一致

-----例2-----
エンベロップfromが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストにおけるアカウントを対象とする場合:
envelope-from="*.gideon.co.jp"

エンベロップToのメールアドレスを記述する場合:
envelope-to="*.to_address_domain"　の後方一致のマッチング
もしくは
envelope-to="to_address"　完全一致

-----例3-----
エンベロップToが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストに　おけるアカウントを対象とする場合:
envelope-to="*.gideon.co.jp"

From フィールドのアドレス部を記述する場合:
from="*.from_address_domain"　の後方一致のマッチング
もしくは
from="from_address"　完全一致

-----例4-----
Fromが@△.example.com(△はh2～h9、k2～k9、m2～m9)の
アカウントの場合:
from="*.example.com"

From フィールドのアドレス部を記述する場合:
from-name="name"
※from-name,subjectにおいて日本語を指定したい場合はRFC2047形式で記述。

-----例4-----
送信元名が「GIDEON」の場合:　from-name="GIDEON"
送信元名が「ギデオン」の場合:
from-name="=?ISO-2022-JP?B?GyRCJS4lRyUqJXMbKEIA?="

x-mailer フィールドのメーラ名を記述する場合(前方一致)
x-mailer="mailer name *"

-----例5-----
Outlook　Express5:　x-mailer =" Microsoft Outlook Express 5.* "

・Outlook　Express6:　x-mailer =" Microsoft Outlook Express 6.* "
・Outlook2000:　x-mailer =" Microsoft Outlook IMO, Build 9.*"
・Outlook2002:　x-mailer =" Microsoft Outlook, Build 10.*"
・Outlook2003:　x-mailer =" Microsoft Office Outlook, Build 11.*"

すべてAND条件の場合、以下のように半角スペースにて区切る。
from="address" from-name="from name" x-mailer="mailer name"

6.5.7 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、「6.5.2基本設定」の「BL ユーザ定義ブラックリスト」で指定します。

画面6.5.7

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「6.5.4 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。
この指定の場合、example.net の該当メールアドレスは全てブラックリスト適用となります。

```
host=192.168.1.2 from=@example.net
```

拡張ブラックリスト設定

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「ブラックリスト」タブ「拡張」タブをクリックします。拡張ブラックリスト設定では従来の画面では設定できなかった部分一致による設定やエンベロップ情報とヘッダ情報を区別した設定が可能となっています。

管理GUI上で新たに表示される以下のタブ画面から設定を行います。

画面6.5.7-2

拡張ブラックリスト記入上の注意

(1)設定の際は、従来のブラックリストとは異なり、
from-name="GIDEON"
などのように『"』(ダブルクォーテーション)で囲うようにしてください。

(2)sendmailの場合でのエンベロップToは自サーバのFQDN(ホスト名)に対応していません。
これは自サーバ上で管理しているバーチャルドメインのFQDNも含みます。
自サーバのFQDNを指定する場合は、envelope-to="*localhost"というようにFQDNをlocalhostに変更してください

(3)拡張ブラックリストに記述する書式は以下の通りです。
ホストのIPアドレスを記述する場合:
host="ip_address" もしくは　host="ip_address/mask"

-----例1-----
ホストのIPアドレスが127.0.0.0～127.0.0.255の範囲にある場合:
host="127.0.0.0/255.255.255.0"

エンベロップFromのメールアドレスを記述する場合:
envelope-from="*.from_address_domain"　の後方一致のマッチング
もしくは
envelope-from="from_address"　完全一致

-----例2-----
エンベロップfromが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストにおけるアカウントを対象とする場合:
envelope-from="*.gideon.co.jp"

エンベロップToのメールアドレスを記述する場合:

envelope-to="*.to_address_domain"　の後方一致のマッチング
もしくは
envelope-to="to_address"　完全一致

-----例3-----

エンベロップToが@mail.gideon.co.jpや@mail2.gideon.co.jpなど、同じドメイン内の複数ホストに　おけるアカウントを対象とする場合:
envelope-to="*.gideon.co.jp"

From フィールドのアドレス部を記述する場合:
from="*.from_address_domain"　　の後方一致のマッチング
もしくは
from="from_address"　　完全一致

-----例4-----

Fromが@△.example.com(△はh2～h9、k2～k9、m2～m9)の
アカウントの場合:
from="*.example.com"

From フィールドのアドレス部を記述する場合:
from-name="name"
※from-name,subjectにおいて日本語を指定したい場合はRFC2047形式で記述。

-----例5-----

送信元名が「GIDEON」の場合:　from-name="GIDEON"
送信元名が「ギデオン」の場合:
from-name="=?ISO-2022-JP?B?GyRCJS4lRyUqJXMbKEIA?="

x-mailer フィールドのメーラ名を記述する場合(前方一致)

x-mailer="mailer name *"

-----例6-----

・Outlook　Express5:　x-mailer =" Microsoft Outlook Express 5.* "
・Outlook　Express6:　x-mailer =" Microsoft Outlook Express 6.* "
・Outlook2000:　x-mailer =" Microsoft Outlook IMO, Build 9.*"
・Outlook2002:　x-mailer =" Microsoft Outlook, Build 10.*"
・Outlook2003:　x-mailer =" Microsoft Office Outlook, Build 11.*"

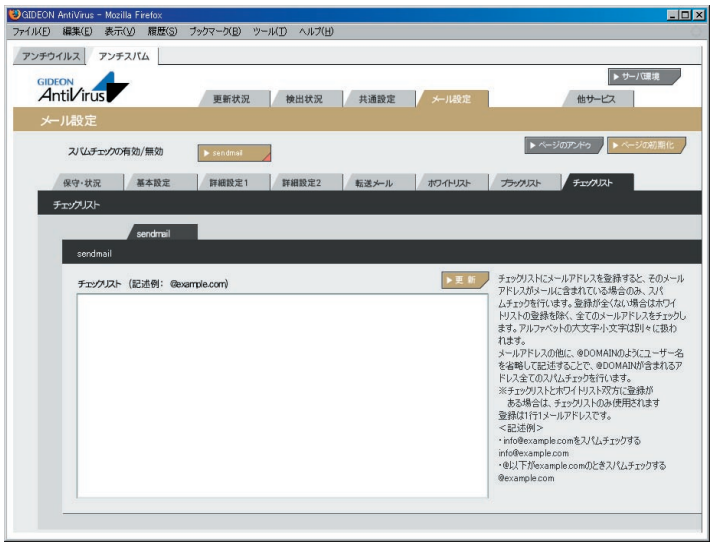
すべてAND条件の場合、以下のように半角スペースにて区切る。
from="address" from-name="from name" x-mailer="mailer name"

6.5.8 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6.5.8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受信時に検出対象となります。

チェックリストに1件でも登録がある場合、ホワイトリストの内容は無効になりますのでご注意ください。



画面6.5.8

6.5.9 ヘッダーチェック(HC)機能

最近の迷惑メールでは直接送信されるメールとは別に、不特定のサーバへ向けて特定のメールアドレスを差出人と偽って宛先不明メールを大量に送信することにより、差出人とされたメールアドレス宛に大量のエラーメールが届くという手法も増えています。
そのようなエラーメールによる迷惑メールをサーバでの受信の段階で食い止める手法として、メールヘッダー部の特徴的記述を迷惑メール判定に用いる手法がこの「ヘッダーチェック」です。

以下のエラーメールのヘッダー部をサンプルとして、この手法を説明します。

----- 例 -----

エラーメールのヘッダー部

Received: from ******.***.ne.jp (******.***.ne.jp [**.***.***.***])by *******.***.co.jp (8.11.6p2/3.7W) with SMTP id h6FMD4Y08675　for <********　@******.co.jp>; Wed, 16 Jul 2003 07:13:04 +0900 (JST)

Received: (qmail 11787 invoked from network); 16 Jul 2003 07:13:03 +0900

Received: from unknown (HELO *********.***.ne.jp) (***.***.***.***)　by ********.***.co.jp with SMTP; 16 Jul 2003 07:13:03 +0900

Received: from wfilter18-a0 (wsmtprv0.********.***.ne.jp [***.***.***.***])　by wsmtpr01.********.***.ne.jp with SMTP id 35988831　for <********** @*****.co.jp>; Wed, 16 Jul 2003 07:13:02 +0900 (JST)

MIME-Version: 1.0

Content-Type: text/plain; charset="iso-2022-jp"

From: Postmaster @*****.ne.jp

To: info @*****.co.jp

Subject: Mail System Error - Returned Mail

このようにエラーメールなどの迷惑メールには特徴的な書式があるので、これを迷惑メールとして判定するためのヘッダーチェック(HC) 設定方法を次に説明します。
なお、HC の適用にはGUI からではなく、コマンドラインからvi などのエディタを利用して設定ファイルを記述します。

(1)HC のスコア設定
/etc/GwAV/GWAV.conf において

SPAM_METHOD_SCORE=BL 4,XS 3,R1 3,S25 1,RES 1,KAS 3,R2 3,HC 0

となっている行があります。この行中[HC] の設定スコアを0 以外の正数にすることにより、判定が可能となります。

----- 例 -----
HC のスコアを3 とする設定

SPAM_METHOD_SCORE=BL 4,XS 3,R1 3,S25 1,RES 1,KAS 3,R2 3,HC 3
---

(2) エラーメール判定ルール設定
エラーメール判定するための特徴的なルールを以下のファイルに記載します。
/usr/local/gwav/ase/HC

----- 例 -----
(先のエラーメールサンプルを題材にした設定)
3:ToEmailAddress1:To:info@*******.co.jp
3:ToEmailAddress2:To:sales@********.co.jp

7:ErrorFromMailerDaemon:From:[Mm][Aa][Ii][Ll][Ee][Rr]-[Dd][Aa][Ee][Mm][Oo][Nn]@
7:ErrorFromAdministrator:From:[Aa][Dd][Mm][Ii][Nn][Ii][Ss][Tt][Rr][Aa][Tt][Oo][Rr]@
7:ErrorFromPostoffice:From:[Pp][Oo][Ss][Tt][Oo][Ff][Ff][Ii][Cc][Ee]@
3:ErrorSubjectUndelivered:Subject:Undelivered Mail Returned to Sender
3:ErrorSubjectReturnedMail:Subject:Returned mail
3:ErrorSubjectFailureNotice:Subject:failure notice
3:ErrorSubjectDeliveryFailure:Subject:Delivery Failure

このサンプルでは
info@ かsales@ 宛に来るメールに対して、差出人が
Postmaster、MAILER-DAEMON、administrator、Postoffice
(大文字、小文字は問わない) の何れかで、件名に
Undelivered Mail Returned to Sender、Returned mail、failure notice、Delivery Failure の何れかの言葉を含む
というメールを対象としたルールとなります。
なお、各行の先頭の数字はHC におけるスコアを意味し、適合ルールのスコア合計が10 点を越えるとエラーメールとして判定され、先の/etc/GwAV/GWAV.conf にて設定されたHC スコアがスパム判定スコアとして、加算されます。

※先のエラーメールサンプルを例に取れば、このサンプルルールでは
3:ToEmailAddress1:To:info@*******.co.jp
7:ErrorFromPostoffice:From:[Pp][Oo][Ss][Tt][Oo][Ff][Ff][Ii][Cc][Ee]@
3:ErrorSubjectReturnedMail:Subject:Returned mail
という3 つのルールが該当し、適合ルールのスコア合計は13 点となりますので、エラーメールと判断します。さらにエラーメールと判断された場合、迷惑メール判定スコアとして、HC 設定スコアが他の判定方式(R1、XS、KAS、

RES など) で得た判定スコアに加算されます。

参考として、次ページに弊社が作成した一般的なHC ルール設定を以下に記載しておきますのでご活用下さい。

----- 例 -----

(一般的なHC ルール設定)

3:ToEmailAddress1:To: エラーメールアドレスが届くメールアドレス1
3:ToEmailAddress2:To: エラーメールアドレスが届くメールアドレス2
3:ToEmailAddress3:To: エラーメールアドレスが届くメールアドレス3
3:ToEmailAddress4:To: エラーメールアドレスが届くメールアドレス4
7:ErrorFromPostmaster:From:[Pp][Oo][Ss][Tt][Mm][Aa][Ss][Tt][Ee][Rr]@
7:ErrorFromMailerDaemon:From:[Mm][Aa][Ii][Ll][Ee][Rr]-[Dd][Aa][Ee][Mm][Oo][Nn]@
7:ErrorFromAdministrator:From:[Aa][Dd][Mm][Ii][Nn][Ii][Ss][Tt][Rr][Aa][Tt][Oo][Rr]@
7:ErrorFromPostoffice:From:[Pp][Oo][Ss][Tt][Oo][Ff][Ff][Ii][Cc][Ee]@
7:ErrorFromDevNull:From:devnull@
7:ErrorFromYahooGroups:From:notify@yahoogroups\.com
7:ErrorFromYahooGroups:From:noreply@googlegroups\.com
7:ErrorFromYahooJpGroups:From:notify@yahoogroups.jp
7:ErrorFromMailmanBounces:From:mailman-bounces@
7:ErrorContentType:Content-Type:delivery-status
4:ErrorFromNameSystemAdministrator:From:System Administrator
4:ErrorFromAdmin:From:[Aa][Dd][Mm][Ii][Nn]@
4:ErrorFromMailer:From:MAILER@
4:ErrorFromDisnVscan:From:disn-vscan1@
4:ErrorFromNoReply:From:no-reply@

4:ErrorFromSymantec:From:Symantec_AntiVirus_for_SMTP_Gateways@
4:ErrorFromMailFilter:From:mailfilter@
4:ErrorFromBounce:From:bounces?@
3:ErrorSubjectUndelivered:Subject:Undelivered Mail Returned to Sender
3:ErrorSubjectReturnedMail:Subject:Returned mail
3:ErrorSubjectFailureNotice:Subject:failure notice
3:ErrorSubjectDeliveryFailure:Subject:Delivery Failure
3:ErrorSubjectDeliveryStatus:Subject:Delivery Status

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、「3.8.1 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、「3.6 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

メールサーバ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。

付録 サポートサービス

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
   - メール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. メールサーバ設定の変更等
   お客様がメール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およびメールサーバとそのバージョン
- メールを中心としたネットワーク構成
- 上記ネットワーク構成中、どのサーバに「アンチウイルス」を導入したか
- メール送信の経路（例えば、導入サーバでメールリレーを行っている場合、その方法など）

・実際に送信したメールスプール（/var/spool/mail/アカウント名）
・クライアントのメーラの情報
・メール送信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）
・メールサーバ設定ファイル（例えば、sendmailの場合sendmail.cf）
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 アンチウイルス メールサーバ Ver.3
ギデオン アンチウイルス アンチスパムPlus
共通ユーザーズガイド

2012年8月15日　第8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/