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

TLAS対応

はじめに

この度は、製品を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 アンチスパム Plus TLAS 対応』および『ギデオン アンチウイルス メールサーバ Turbolinux AS 対応』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 TLAS 対応』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「メールサーバー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』は、ウイルス、スパイウェアをメールサーバー上で確実に検出・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 TLAS 対応』は『ギデオン アンチウイルス メールサーバ』にアンチスパム機能を追加した製品です。
両製品ともに Turbolinux Server Desktop の管理ツールと共通化することにより運用コストを削減し、使いやすい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を行う
「2.2 初期画面」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 バージョン情報メニュー」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
「3.3 ウイルス検出ログメニュー」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
- OS デフォルトの Turbolinux Server Desktop 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、ウイルスを完全に検出、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（2006 年 9 月現在）

『ギデオン アンチウイルス アンチスパム Plus TLAS 対応』は、メールサーバ上でのスパムメール対策、ウイルス対策のソフトウェアです。

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

- Linux カーネルインテルアーキテクチャ

- メールサーバー

  sendmail8.9.3 以降 8.x
  sendmail.cf は「Mlocal,M*smtp*,Mrelay」定義を含むこと
  (デフォルトでは通常含まれます）

- 対応 Linux ディストリビューション

  Turbolinux Appliance Server Hosting Edition 1.0
  Turbolinux Appliance Server Workgroup Edition 1.0
  Turbolinux Appliance Server 2.0

- 物理空きメモリ容量 128MB 以上

- /usr/local ディレクトリ以下に200MB 以上の空き容量

注意

本マニュアル記載の Turbolinux Server Desktop 画面は Turbolinux Appliance Server 2.0　をベースにしています。他のバージョンでは画面のデザインなどが多少異なりますのでご了承ください。

1.5 インストール対象サーバ環境

『ギデオン アンチウイルス アンチスパム Plus TLAS 対応』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。

● OS デフォルトの sendmail メールサーバが正常に稼動していること

手動で postfix, qmail など、sendmail 以外の MTA をインストールして稼動している場合、本製品は動作いたしません。その場合、「ギデオン アンチウイルス アンチスパム Plus」をご利用ください。

● 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（スパム検出でも同様）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 , およびスパム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 空きメモリ容量 128MB 以上です。

1.6 インストール前の注意事項［重要］

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。

「ギデオン アンチウイルス アンチスパム Plus TLAS 対応」は、gantispamplus.rpm パッケージ（rpm 形式）から成ります。パッケージサイズはおよそ50MB 程度です。

OS の設定で必要なファイルサイズをアップロードできるように設定してください。/etc/admserv/php.ini ファイル内で、

```
post_max_size = 50M
upload_max_filesize = 50M
```

のように記述し、`service admserv restart` と管理ウェブサービスを再起動してください。

上記を行わない場合、「2.1 インストール」< 手順 4 >がうまく動作しません。

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。

注意

「Turbopkg」→「自動アップデートの設定」の設定方法によっては、ユーザが気づかないうちにメールサーバがバージョンアップされてしまい、sendmail.cf の記述が入れ替わりアンチウイルスが動作しない設定になってしまう場合がありますので、ご注意ください。

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、管理メニューから定義ファイルの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など、システムの資源が不足する場合、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、スパム判定・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 の速度を向上させることをお勧めします。

● 大量のメールなどで過負荷となった場合、メールサーバが停止する可能性があります。日常の運用・管理にご注意ください。

● 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の有効なソフトです。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

ここでは、本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、以下の手順で本製品をサーバにインストールします。
メールサーバを停止し、メール処理が行われない状態でインストールを実行することをお勧めします。

注意

すでに従来製品「アンチウイルス for Linux」がインストールされている場合、いったんアンインストールしてから本製品をインストールしてください。

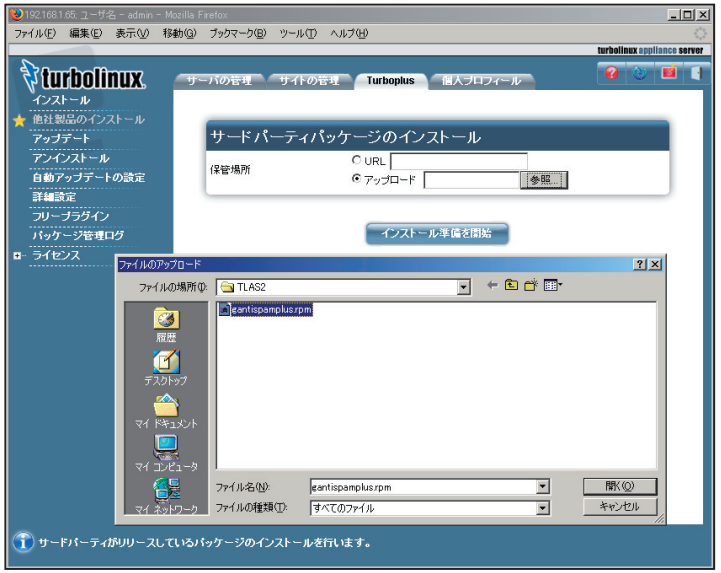
2.1 インストール

《手順1》製品CD をCD ドライブに挿入
製品CD をお使いのデスクトップPC のCD ドライブに入れてください。

《手順2》TLAS のGUI 管理画面にログイン

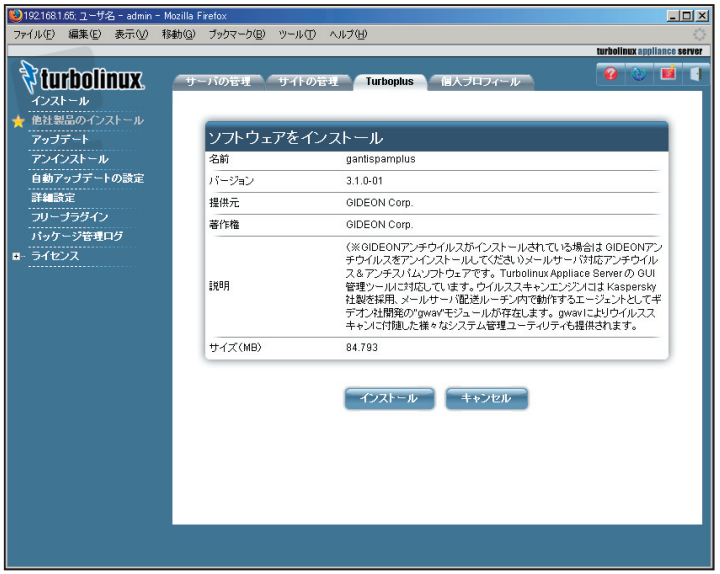
《手順3》パッケージのインストール
画面上部「Turbopkg」タブをクリックし、左側「サードパーティパッケージのインストール」または「他社製品のインストール」メニューをクリックします。

《手順4》インストール準備を開始
画面2.1.1 でアップロードするファイルを指定し、「インストール準備を開始」ボタンをクリックします。 ルートディレクトリには、 TLAS1 とTLAS2 のディレクトリがあります。TLAS1 にはTurbolinux Appliance Server 1.0 用のインストールパッケージ(rpm) があり、 TLAS2 にはTurbolinux Appliance Server 2.0 用のインストールパッケージ(rpm) があります。パッケージファイル名は、どちらもgantispamplus.rpm です。



画面2.1.1

《手順5》「インストール」ボタンをクリック
アップロードが完了して画面2.1.2 のようにパッケージの説明が表示されたら「インストール」ボタンをクリックします。



画面2.1.2

画面2.1.3

《手順6》「パッケージをインストールしています...」の表示

しばらくの間、画面2.1.3 のように表示されます。

《手順7》インストールが終了

10 分程度で、ステータスバーが100% となりインストールが終了します。

インストール終了後、2～3分以内にGUI 管理ツールのサービスが自動的に再起動されますので、しばらくお待ちください。

インストール直後に「アンチウイルス」初期画面を開くと、チェックボックスのチェックがすべて空欄になっている場合があります。これはまだGUI 管理ツールのサービスが再起動されておらず、インストール処理が途中であることを示唆しますので、2～3分おいてから、ブラウザをリロードして再度アクセスしてください。

注意

インストール途中で何らかの管理作業によりGUI 管理ツールサービスが再起動されると、画面2.1.3 が表示されないことがあります。また、システム環境によっては、稀にインストールに数十分かかる場合があります。いずれの場合にも、十分に時間を置いた後に後述の画面を見て正常にインストールされているか確認してください。

《手順8》インストールの確認

インストール終了後、「Turbopkg」タブ→「パッケージ管理ログ」メニューを見ると、次のように表示されます。

```
パッケージ情報の読み込...
依存関係の確認...
解決。
パッケージのアップデート...
Preparing... [>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>] 100%
gantispamplus-3.1.0-01 [****************************************]
100%
```

あるいは次のように表示される場合もあります。

```
Reading installed packages...
Dependency check...
fixed.
Update packages...
Install gantispamplus-3.1.0-01.
Complete.
```

2.2 初期画面

インストール後、画面上部「サーバの管理」タブをクリックし、左側「セキュリティ」メニューをクリックすると、「アンチウイルス」「アンチスパム」というメニューが新規に追加されます。

画面2.2

注意

画面2.2 が表示されない場合、一旦ブラウザをリロードしてください。またはインストール終了後すぐにこの画面を開くと、メニューがなかったり、デフォルトで画面内のチェックがない、あるいはメニューの日本語表記が英語になっている等の場合があります。数分待ってブラウザをリロードすると正常に表示されます。

「アンチウイルス」以下には、次の４つのメニューが存在します。

- 基本設定
- 詳細設定
- ウイルス検出ログ
- バージョン情報

「アンチスパム」以下には、次の４つのメニューが存在します。

- 基本設定
- 詳細設定
- スパム検出ログ
- バージョン情報

初めてインストールした場合、画面2.2 で「使用開始」ボタンを押してください。

2.2.1 評価ユーザ

画面が遷移すると、評価ユーザ登録の状態でアンチウイルス機能が動作するようになります。

評価ユーザの場合は、「評価ライセンス試用中」と表示され、インストールした日から3ヶ月間、正規ユーザと同じように最新の定義ファイルを更新し、アンチウイルス機能をご試用いただけます。

試用期間が終わると最新の定義ファイルの更新ができなくなり、その後発生した新種のウイルスには対応しなくなります。
後で正式なライセンス契約をしていただき、「お客様登録No.」「パスワード」を入力し直すことで、試用期間以降も継続してお使いいただけます。
ユーザ情報が正しくない場合、アンチウイルス機能は動作しません（ウイルスを検出しません）。

2.2.2 正規ライセンスユーザ

正規にライセンスをご購入いただいたお客様は、「お客様登録No.」および「パスワード」の欄に正しい文字列を入力し、「保存」ボタンを押してください。
ユーザ情報の入力が正しければ、初期画面が「正規ライセンス使用中」（画面2.2.2）に遷移します。

画面2.2.2

ご契約いただいた期間中、アンチウイルス機能が有効になります。
契約期間はシステム側で管理していませんので、製品購入時の契約書類で期間をご確認ください。期間満了で契約更新がない場合、アップデートサーバ側で定義ファイルのアップデートができなくなります。
契約満了日が近くなりましたら販売会社よりご案内をお送りします。

2.3 アンインストール

《手順1》管理画面にログイン

《手順2》「アンインストール」メニューをクリック
画面上部「Turbopkg」タブをクリックし、左側「アンインストール」メニューを

クリックします。

《手順3》"gantispamplus" にチェック

画面2.3 のように、"gantispamplus" にチェックをつけます。

画面2.3

《手順4》アンインストール完了

画面2.3 最下部の「アンインストール」ボタンを押します。1 分ほどでアンインストールは完了します。

《手順5》「パッケージ管理ログ」メニュー

「Turbopkg」タブ→「パッケージ管理ログ」メニューを見て以下のようなメッセージが表示されていればOK です。

```
rpm -e gwantivirus
Shutting down sendmail MTA:
Shutting down sendmail MSP:
.....
Stopping GIDEON Anti-Virus daemon.
saved /etc/mail/sendmail.cf.diff
etc/mail/sendmail.cf was returned.
Stopping Kaspersky Anti-Virus server.
error: removal of /usr/sausalito/ui/web/gideon/antivirus/
antivirus _ regular.php failed: No such file or directory
....
Setup sendmail:
Starting sendmail MTA:
Starting sendmail MSP:
```

あるいは以下のように表示される場合もあります

```
Remove packages...
Uninstall gantispamplus-3.1.0-01.
Complete.
```

第３章 アンチウイルス設定

3.1 アンチウイルス基本設定メニュー

本メニューでは、ウイルスチェックの稼動 / 停止、ウイルス検出時の動作、ユーザ情報などを設定します。

3.1.1 基本

画面 3.1.1

【ウイルスチェックを有効にする】

ウイルスチェック機能の有効 / 無効を設定できます。ウイルスチェックを有効にすると、メールに添付ファイルがある場合、ウイルスチェックします。添付ファイルがない場合、ウイルスチェックせずにそのまま送信します。

ウイルスチェックを無効にするか、ユーザアカウントが正しくないか、評価ユーザで期限が切れた場合、添付ファイルについてもウイルスチェックせずにそのまま送信します。

3.1.2 警告メール

画面 3.1.2

【全体に適用される設定】
ウイルスを検出した場合に、管理者に警告メールを送ることができますが、その際に送信元アドレスとして書かれるメールアドレスを記述します。

【管理者宛警告メールの設定】
ウイルス検出した場合、管理者に警告メールを送信する場合にチェックします。管理者のメールアドレス（複数指定する場合は半角スペースで区切ってください）を記述します。

【ウイルス検知時の管理者への警告メール Subject 設定】
管理者に届く警告メールの表題（サブジェクト）の記述に、元のメールのサブジェクトを後半部に付ける場合、感染メール Subject の付加にチェックします。

【受信者宛警告メールの設定】
ウイルス検出した場合、受信者に警告メールを送信する場合にチェックします。受信者に届く警告メールの表題（サブジェクト）を選択します。また、検出したウイルスを含む添付ファイルの扱いをここで決定します。
−添付ファイルを削除し詳しいヘッダ情報を記載した内容を知らせる
−添付ファイルを削除して警告メールとしてだけ送る
−ウイルスファイルを削除せずそのまま添付して送る
上記から選択できます。

【ウイルス検知時の受信者への警告メール Subject 設定】
受信者に届く警告メールの表題（サブジェクト）の記述に、元のメールのサブジェクトを後半部に付ける場合、感染メール Subject の付加にチェックします。

【送信者宛警告メールの設定】
ウイルスメールの送信者に、警告メールが届いた旨を知らせたい場合にチェックします。
ただし、ウイルス発信元に見えても、実際は存在しないアドレスであったり詐称されていることがほとんどですので、ウイルスを送信した心当たりのないユーザに警告メールを送ることになる場合があります。逆に迷惑メールを送ることにもなりかねないので、この設定は**通常オフにする**ことをお勧めします。

【ウイルス検知時の送信者への警告メール Subject 設定】
送信者に届く警告メールの表題（サブジェクト）の記述に、元のメールのサブジェクトを後半部に付ける場合、感染メール Subject の付加にチェックします。

3.1.3　通知メール

画面 3.1.3

【通知メール送信先設定】

前記警告メール以外の、本製品に関する通知メールを管理者に送ることができます。

ユーザ認証がアップデートサーバで正しく行われるかチェックするメール、定義ファイルのステータスを確認するメール、ディレクトリチェックした場合に結果を通知するメールなどが該当します。管理者としては、警告メールと同じアドレスか、または別アドレスを指定することができます。

通知メール用に別の管理者アドレスを指定したい場合、テキストフィールドに記述してください（複数指定する場合は、半角スペースで区切って入力してください）。

【ウイルス定義ファイル ステータス確認】

現在のウイルス定義ファイルの状態を定期的にチェックし（デフォルトは毎時 20 分）、必要であれば管理者宛に通知メールを送ります。

すべてにチェックすると、1 時間おきに必ず何かしらの通知メールが届きます。通常は「過去 3 日間更新されていなければ通知する」だけをオンにすることをお勧めします。

定義ファイルの状態は、ギデオン社のウェブサーバである www.gideon.co.jp とユーザが利用しているサーバ間の定義ファイルを比較します。どちらもウイルス検出エンジン供給元のアップデートサーバから定期的に定義ファイルをダウンロードするため、タイミングによっては、ユーザのサーバの定義ファイルの方が新しい場合があります。

ユーザのサーバの定義ファイルと、エンジン供給元のアップデートサーバとを直接比較することは行っておりません。

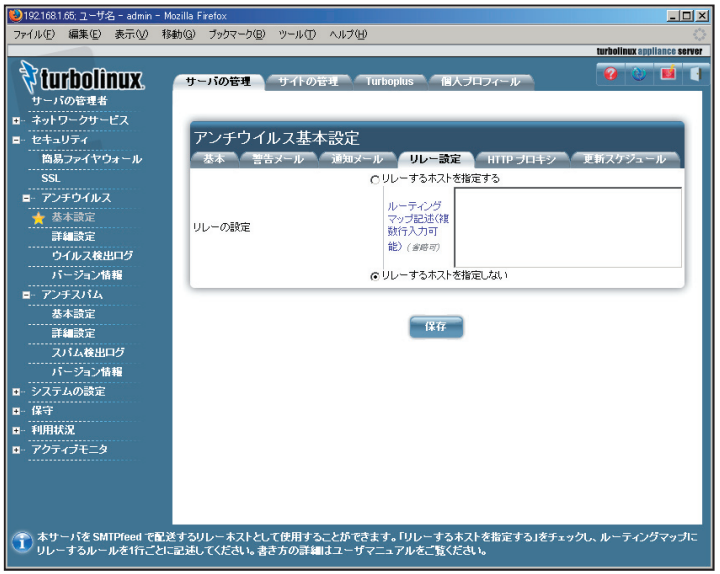
最新の定義ファイルの情報につきましては、以下のギデオン社ウェブサイトをご覧ください。

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

最新の定義ファイルのリリース時間を確認するには、以下の検出エンジン供給元のウェブサイト（表示はロシア時間）をご確認ください。

http://www.kaspersky.com/avupdates

3.1.4 リレー設定



画面 3.1.4

【リレーするホストを指定する】

本サーバをリレーホストとして使用する場合、「リレーするホストを指定する」にチェックしてください。チェックした場合、記述があるルーティングマップ行にしたがって SMTP 配送を行います。
特別にリレーの設定等がなければ、チェックは必要ありません。

【ルーティングマップ記述】

ルーティングマップ行（テキストボックス）には、smtpfeed マップファイルの書式に従って記述します。

ドメイン部　宛先ホスト 1: 宛先ホスト 2:…

ドメイン部と宛先ホスト 1 は、半角スペースで区切って入力します。
宛先ホストが複数ある場合は、コロン（:）で区切って入力します。

宛先ホストには、hostname、[hostname]、A、MX などが指定できます。

hostname	ホスト名に対する MX を検索する
[hostname]	ホスト名に対する A を検索する
[IPaddress]	IP アドレスを利用する
MX	メールアドレスのドメイン部に対する MX
MX?	MX と同様（DNS が引けなかった場合は、後続する宛先ホストについても試行する）
A	メールアドレスのドメイン部に対する A
=domain	エイリアスを適用した MX を検索

ドメイン部に対しては、メールアドレスのドメイン部に対して完全一致で比較するか、または部分一致で比較するかを選択できます。
以下は記述例です。

----- 例 -----

（例 1） sub.my.domain　A:[backup.server]
宛先ホストが、ドメイン部で指定した「sub.my.domain」に完全に一致した場合、例えば「username@sub.my.domain」へのメールは、「sub.my.domain」というサーバまたは「backup.server」というサーバへ送ります。

（例 2） .co.jp　quick.relay.server:MX
「co.jp」のように、サブドメインに部分一致した場合、
例えば「co.jp」のサブドメイン名をもつメールで「username@xxx.yyy.co.jp」へのメールは、「quick.relay.server」というサーバまたは「.co.jp」

のサブドメインに一致するメールサーバへ送ります。

（例 3） .bitnet =.bitnet.ad.jp
エイリアスの場合、例えば「bitnet」のサブドメイン名をもつメールで、「username@xxx.yyy.bitnet」へのメールは、「bitnet.ad.jp」というメールサーバへ送ります。

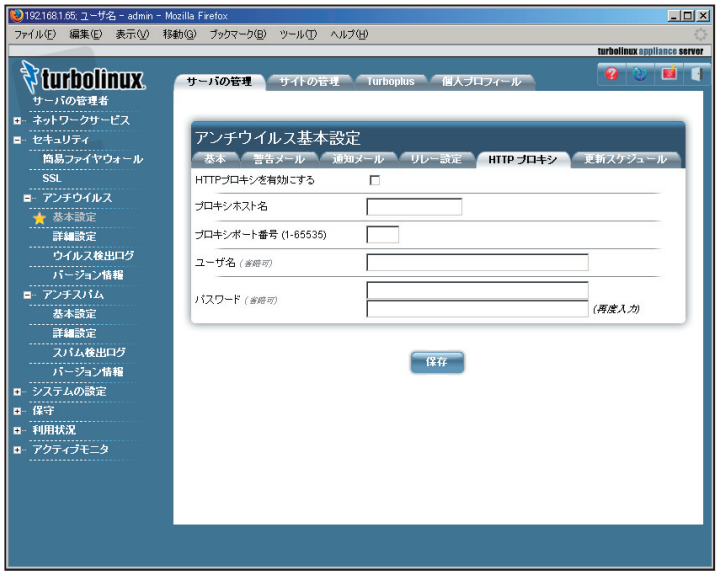
（例 4） .jp MX?:[fallback.mx]
メールサーバへの送信が失敗した場合、
例えば「.jp」のサブドメイン名をもつメールで、「username@xxx.yyy.co.jp」へのメールは「.jp」のサブドメインに一致するメールサーバに送ります。また、そのメールサーバへの送信に失敗した場合、「fallback.mx」サーバへ送ります。

（例 5） . MX #default
マップファイルで以下のように設定すると、特定のドメイン名や宛先ホストを指定しない場合と同じ意味になります。

注意

テキストボックスは空欄にできませんので、何も必要なければ #... 行を入力してください。# 以降はコメントなので設定には何ら影響しません。

3.1.5 HTTP プロキシ



画面 3.1.5

定義ファイルおよびモジュールの更新は、HTTPでインターネット上のアップデートサーバにアクセスして行われるため、本サーバからHTTPによる外部アクセスができることが必須です。
お使いのネットワーク環境によってはプロキシサーバを経由してウェブアクセスしている場合があります。その場合、本画面でプロキシ設定を行います。

注意

プロキシの有無やプロキシの設定詳細については、ネットワーク管理者に確認してください。

【プロキシを有効にする】
チェックマークを付けると、「アンチウイルス」の更新時、外部に HTTP アクセスをする際に、すでに正常に稼動しているプロキシサーバを経由します。
プロキシを有効にした場合、以下の項目の設定が必要です。

【プロキシホスト名】
プロキシサーバの「ホスト名」または「IP アドレス」を入力します。

【プロキシポート番号】
プロキシにアクセスする際の「ポート番号」を指定します。
現在お使いのポート番号については、ネットワーク管理者に確認してください。

【ユーザ名】および【パスワード】
プロキシサーバでユーザ認証を行っている場合、有効な「ユーザ名」とその「パスワード」を入力してください。

注意

ユーザ名を入力せずに、パスワードだけを入力しても無効です。
ユーザ名およびパスワードについては、ネットワーク管理者に確認してください。

3.1.6 更新スケジュール

画面 3.1.6

【更新するタイミング】
1 時間おき、2 時間おき、3 時間おき、6 時間おき、に定義ファイルを更新します。
「保存」ボタンを押すと、更新するタイミング設定が保存されます。

【アンチウイルスのアップデート】
「アップデートの実行」ボタンを押すと、アンチウイルスの定義ファイルが更新されます。場合によっては終了まで数分かかります。アップデートが完了すると自動的に基本画面に戻ります。アップデートが実際に終了したかどうかは、後述の「3.4 バージョン情報メニュー」で確認できます。

3.2 詳細設定メニュー

3.2.1 ホワイトリスト

画面 3.2.1

【ホワイトリストの設定】
通常、デフォルトではすべての SMTP 配送がウイルスチェックの対象となりますが、例外的に「ホワイトリスト」を設定することで、指定した送信者・受信者（どちらかまたは両方）について「ウイルスチェックしない」ようにできます。

以下のように、from=<Envelope の From アドレス >、to=<Envelope の To アドレス > として指定できます。1 行にあるものはすべて "AND" として扱われます（行中すべてマッチした場合に適用）。

from=aaa@bbb.co.jp
to=ccc@ddd.com
from=eee@fff.ne.jp to=ggg@hhh.net

「保存」ボタンを押すと、テキストボックスに記載した内容が /etc/GwAV/mta/whitelist ファイルに反映されます。

3.2.2 チェックリスト

画面 3.2.2

【チェックリストの設定】
通常、デフォルトではすべての SMTP 配送がウイルスチェックの対象となりま

すが、「チェックリスト」を設定すると、チェックリストで指定したエントリに対してのみウイルスチェックし、その他マッチングしないものはすべてウイルスチェックしない、という設定にすることができます。

チェックリストに一つでもエントリが記載されると、「指定したものだけ、ウイルスチェックする」実装に変わります。またチェックリストに一つでも記載があると、ホワイトリストの内容はすべて無効になります。

以下のように、単一メールアドレスまたは @ 以下のドメインを指定できます。

aaa@bbb.co.jp
ccc@ddd.com
@eee.fff.ne.jp

「保存」ボタンを押すと、テキストボックスで記載した内容が
/etc/GwAV/mta/checklist ファイルに反映されます。

注意

ホワイトリスト、チェックリストともに設定ファイルは /etc/GwAV/mta/whitelist,checklist ですが、実際にプログラムに読み込まれるファイルは /etc/GwAV/mta/whitelist.sm, checklist.sm です。*.sm ファイルは自動生成されるファイルですので直接編集しないでください。

3.2.3 ディレクトリチェック

本製品は、ファイルサーバの用途に準じたディレクトリチェックを実行することができます。リアルタイムスキャンには対応していませんが、スケジューリングにより指定したディレクトリを指定した日時にウイルススキャンします。スキャン結果は「通知メール」で指定した管理者宛にメールされます。

画面 3.2.3

「チェックするディレクトリ」テキストボックスでは、/home/aaa、/home/bbb などウイルスファイルが含まれている可能性がある読み書き可の一般的なユーザディレクトリを指定してください。"/"（ルート）を指定したり、"/proc" や "/dev" などシステムで使われる読み込み専用の不正なディレクトリを指定すると、ウイルスチェックプログラムが長時間完了せずに、システム負荷が増大するなど問題が発生する場合がありますのでご注意ください。

「ディレクトリスキャンの実行」ボタンを押すと、テキストボックスで指定したディレクトリについて即座にウイルスチェックが実行されます。指定したディレクトリサイズが大きいと、しばらく時間を要する場合があります。

3.3 ウイルス検出ログメニュー

画面 3.3

ウイルスに関するログについて説明します。

ウイルス検知ログの読込みを有効にする

デフォルト設定では、ログファイルのパーミッションにより GUI 管理画面から読み込みできません。チェックマークを付けると、GUI 管理画面でもログを表示

することができます。
この際、ログファイルがシステム管理者以外にも読み込み可能になりますが、セキュリティ上問題がある場合には、この機能を有効にしないことをお勧めします。また、ログファイルのサイズが大きい場合、該当行の抽出に時間がかかり表示までしばらくかかる場合があります。

ウイルスに関係する履歴があると、「ウイルスに関するログ一覧」に以下の情報が表示されます。

日付	：	ウイルスが検出された日時
From アドレス	：	メール送信者
To アドレス	：	メール受信者
ウイルス名	：	ウイルス名

過去にウイルスが検知されたことがないか、ログファイルに情報が何もない場合は特に何も表示されません。

通知メールの管理者宛に月次レポートを毎月送信する

「基本設定」で設定された、通知メールを送る管理者のメールアドレス宛に、ウイルス検知の月次レポートが送信されます。通知メールの管理者が指定されていない場合は、警告メールで指定した管理者宛に届きます。前月検知されたウイルスの種類と数の集計が記載されています。
送信されるタイミングについては、システムの monthly cron 設定をご確認ください。

【今すぐ月次レポートを送信する場合の設定】

● 今すぐ送信する
「送信実行」ボタンを押すと、ただちに月次レポートを指定したアドレス宛に送信することができます。年・月、アドレスを下記で指定してください。

● 年
「 2005 」など今年以前の西暦年を 4 桁で指定します。2000 - 2100 まで入力可能です。
● 月
月は「 1 」「 2 」....「 12 」の形式で指定します。1 -12 まで入力可能です。当月以前を指定します。
ログに記載がない月については、「集計 0」としてメールが届きます。将来の年・月を指定すると集計メールは送信されません。

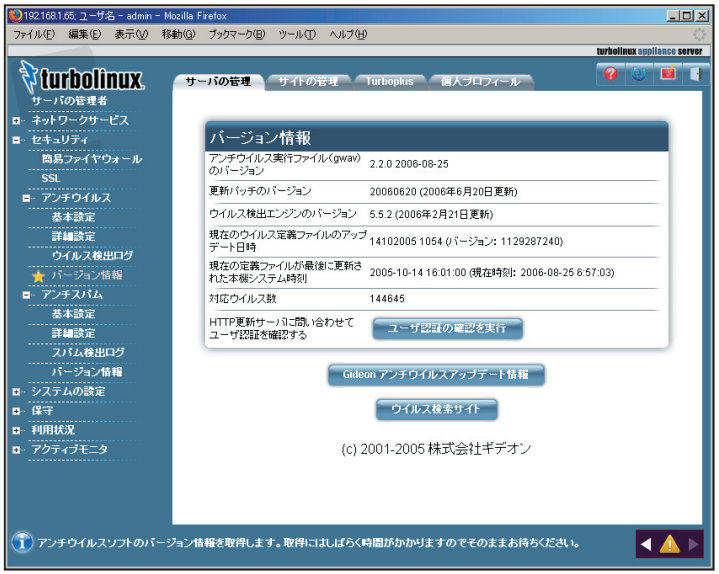
【今すぐ月次レポートを送るメールアドレス】

デフォルトでは、「基本設定」で指定した通知メールを送る管理者のメールアドレス宛に送信します。通知メールの管理者が指定されていない場合は、警告メールで指定した管理者宛に届きます。
別のアドレスを指定したい場合、「メールアドレスを指定する」ラジオボタンにチェックをつけて、アドレステキストボックスにメールアドレスを指定してください。@ を含むアドレス、またはローカルユーザ名の指定が可能です。複数入力する場合は、スペースで区切ってください。

注意

従来製品「アンチウイルス for Linux」から本製品にアップグレードした場合、アップグレード後に検知されたウイルスのみ表示・集計の対象となります。

3.4 バージョン情報メニュー



画面 3.4.1

現在使用しているアンチウイルスソフトのバージョン情報を確認できます。
本製品のプログラムは、「アンチウイルスのモジュール」 各種コマンド類)」、および「定義ファイル（パターンファイル）」の二つに分類できます。アップデートが発生すると、モジュールはギデオン社のモジュールアップデートサーバから、定義ファイルはウイルス検出エンジン供給元のアップデートサーバから自動でダウンロードします。アップデート状況については常に注意して、モジュール、定義ファイルともに最新のバージョンにしておく必要があります（モジュール更新頻度は年間数回程度です）。

以下の 3 項目は「アンチウイルスのモジュール」に属するものです。

- アンチウイルス実行ファイル（gwav）のバージョン
- 更新パッチのバージョン
- ウイルス検出エンジンのバージョン

「Gideon アンチウイルスアップデート情報」 ボタンをクリックすると http://www.gideon.co.jp/updates サイトにハイパーリンクされます。サイトの情報と比較して、各々が最新バージョンであれば問題ありません。
これらモジュール群では、プログラムのバグフィックスや機能拡張を含む、各種コマンド類のバージョンアップデートが含まれます。

●「現在のウイルス定義ファイルのアップデート日時」
本サーバ上に存在する定義ファイルのアップデート日時（ロシア時間）およびバージョンです。アップデート日時がバージョン代わりに扱われることがあります。

●「現在の定義ファイルが最後に更新された本機システム時刻」
「基本設定」 メニューの「更新スケジュール」 タブで、「アップデートの実行」おこなった後、アップデートされたかどうか、システム時刻と照らし合わせて確認してください（システム時刻は常に正しい状態にしてください）。アップデートされていない場合、ネットワーク接続に問題がないか確認してください。また、定義ファイルがすでに最新の場合にはアップデートされません。

●「対応ウイルス数」
本サーバ上に存在する定義ファイルで対応済みのウイルス総数です。
どのウイルスに対応しているか詳細を知りたいときは、「ウイルス検索サイト」ボタンをクリックして、ハイパーリンクされたサイト（http://www.viruslist.com）の右上のテキストフィールドにウイルス名などの検索文字列を入力し、"Viruses" ラジオボタンにチェックして "Go" ボタンを押してください。
対応済みのウイルスであればその一覧と説明を見ることができます（英語）。

ユーザ情報の入力が間違っていたり、本サーバが正常にアップデートサーバに HTTP アクセスできない場合、アップデートが行われません。「ユーザ認証の確認」ボタンを押すと、アップデートサーバへの認証テストを実行します。しばらく待って画面 3.4.2 のように［OK］が表示されれば認証は OK です。外部インターネットにつながらなかったり、認証に失敗するなどのエラーが発生するとその旨表示されますので、お使いの環境を確認して問題を修正してください。

画面 3.4.2

なお、このオプションにチェックをつけたままの場合、毎回バージョンを確認するたびに認証テストを実行します。したがってバージョン情報表示までに時間がかかるので、必要な場合以外はチェックをオフにしておくことをお勧めいたします。

注意

外部インターネットにつながらない場合には、結果が表示されるまで数分かかることがありますのでしばらくお待ちください。

注意

評価試用ユーザの場合、評価期限が過ぎても認証は [OK] と表示されます。評価期限を過ぎると、アップデートを実行しても定義ファイルが最新の状態になりませんので、ご了承ください。
評価ユーザの期限が過ぎたか否かは、画面 2.7 のインジケータで確認できます。

3.5 動作確認

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。

3.5.1 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。

----- 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。

(3) (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。

第 4 章 アンチスパム設定

4.1 基本設定メニュー

本メニューでは、スパムチェックの稼働 / 停止、スパム検出時の動作、ユーザ情報などを設定します。『ギデオン アンチウイルス メールサーバ』には本章で説明するアンチスパム機能は搭載されていません。

4.1.1 基本

画面4.1.1

【基本システム設定】

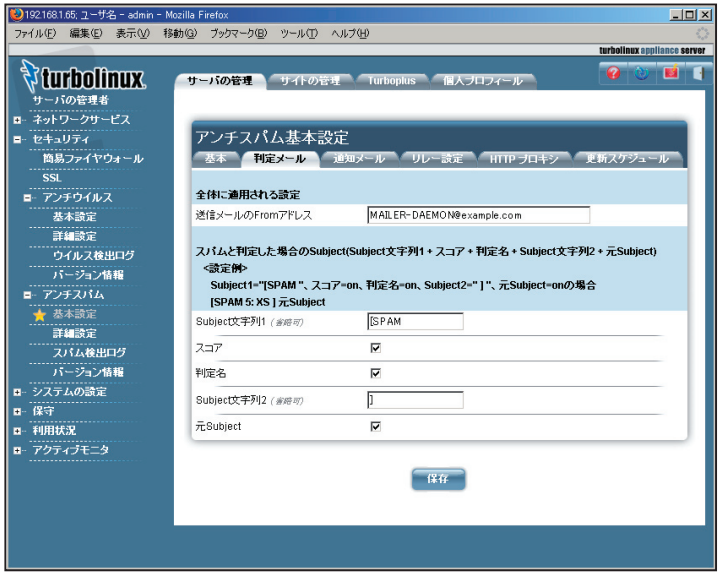
●スパムチェックを有効にする

スパムチェック機能の有効 / 無効を設定できます。

【ユーザアカウント設定】

「2.1 インストール」で設定された項目を引き継ぎます。

4.1.2 判定メール



画面4.1.2

【全体に適用される設定】

●送信メールのFrom アドレス

スパムを検出した場合、管理者に警告メールを送ることができますが、その際に送信元アドレスとして書かれるメールアドレスを記述します。

【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。

例えば、

Subject1="[SPAM "、スコア=on、判定名=on、Subject2="] "、

元Subject=on の場合, ユーザは以下のSubject を受信します。

[SPAM 5: XS] 元Subject

●Subject 文字列1

Subject の最初の文字列を記述できます。

●スコア

スコアにチェックすると、スパム判定の合計値を表示できます。

●判定名

判定名にチェックすると、スパムの判定名を表示できます。

●Subject 文字列2

判定名に続く文字列を記述できます。

●元Subject

元Subject にチェックすると、Subject 行の最後に送信元のSunbject が表示されます。

4.1.3 通知メール

画面4.1.3

【通知メール送信先設定】

●通知メールを送る管理者のメールアドレス

通知メール用の管理者アドレスを指定したい場合、テキストフィールドに記述してください（複数指定する場合、半角スペースで区切って入力してください）。

【スパム定義ファイル ステータス確認】

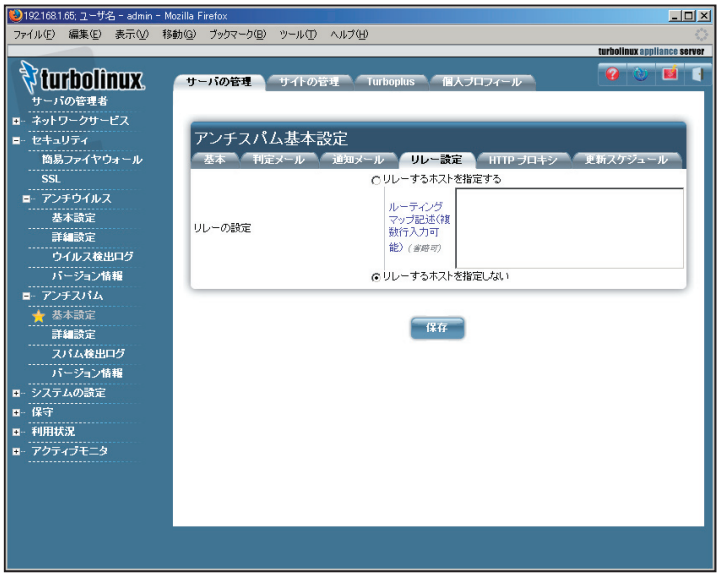
●過去3 日間更新されていなければ通知する（通常オン）

スパムの本文解析などにスパムのデータベースを使っています。このデータベースが過去3 日以上更新されていない場合、前述の通知メールが送信されます。

●システム上の定義ファイルとアップデートサーバの定義ファイルが違う場合に通知する（推奨オフ）

スパムのデータベース更新がギデオン社のサイトにある定義ファイルのバージョンが異なる場合に通知します。

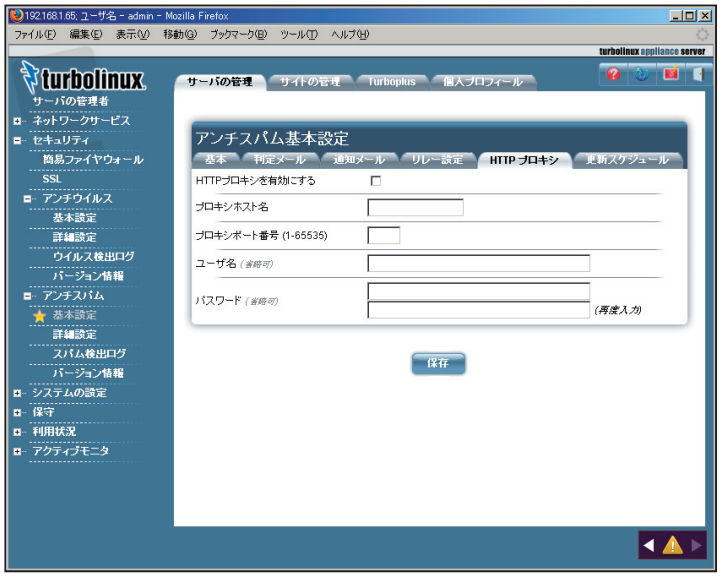
4.1.4 リレー設定



画面4.1.4

アンチウイルスのリレー設定と全く同じ機能です。設定の解説は「3.1.4 リレー設定」を参照してください。

4.1.5 HTTP プロキシ



画面4.1.5

アンチウイルスのHTTP プロキシと全く同じ機能です。設定の解説は「3.1.5 HTTP プロキシ」を参照してください。

4.1.6 更新スケジュール

画面4.1.6

【更新するタイミング】

1時間おき、3時間おき、6時間おき、12時間おき、24時間おきの中からインターバルを選択し、スパム定義データベースを更新します。初期設定は3時間おきに設定されています。

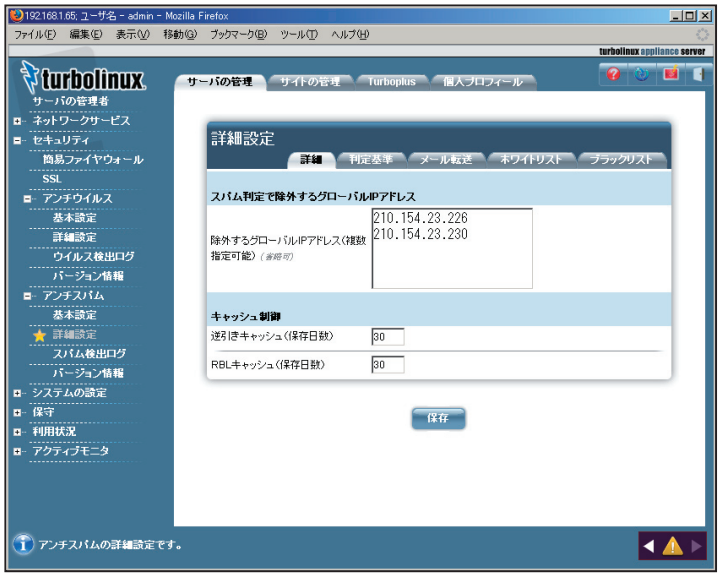
「保存」ボタンを押すと、上記の設定が保存されます。

【アンチスパムのアップデート】

「アップデートの実行」ボタンを押すと、スパム定義データベースを更新します。アップデートが実際に終了したかどうかは、後述の「4.4 バージョン情報メニュー」で確認できます。

4.2 詳細設定

4.2.1 詳細



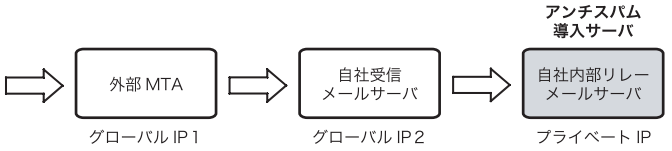
画面4.2.1

【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おこないます。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でメールを受信する経路上において、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自社受信メールサーバを、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が転送用のサーバであれば、グローバルIP 1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

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。

【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。
保存期間（日数）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。
キャッシュを有効にすることで、より高速にチェックすることができます。初期設定ではキャッシュできる容量は約2000 件程度です。このリスト容量を超えた場合、もっとも古いリストを除外し、新規に追加する仕組みになっています。したがって、有効期間内でも古いリストは上限を超えると保持されないことがあります。

4.2.2 判定基準

画面4.2.2

カスタマイズを利用する場合は設定項目に注意して行ってください。特に、アクションの「POP3 のみ本文変更」「SMTP のみ受信拒否」に関しては、慎重に行ってください。

【スパム判定基準の設定】

スパム判定基準として、初期設定は「推奨設定を利用する」になっています。

「カスタマイズを利用する」 をチェックすると、判定方法のスコア値を変更できます。

【判定方法のスコア設定】

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。

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。

【アクションのスコア設定】

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。

何もしない：

設定したスコアでは通常のメールとして扱います。

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。

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。

【追加ヘッダのスコア設定】

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。

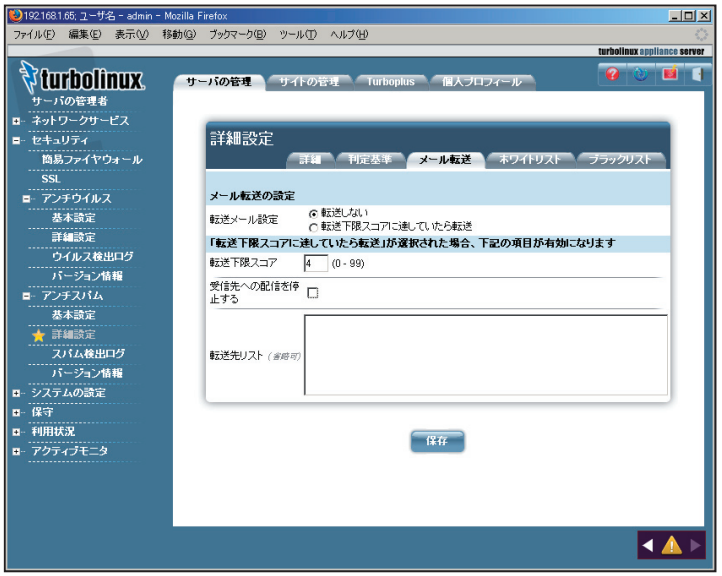
（ヘッダ表示）	（内容）
X-Spam-Status: NONE	スパムに該当せず
X-Spam-Status: SUSPICION	スパムと疑わしい
X-Spam-Status: SPAM	スパムに該当

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

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。

4.2.3 メール転送



画面 4.2.3

【メール転送の設定】

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。

【「転送下限スコアに達していたら転送」が選択された場合、下記の項目が有効になります】

● 転送下限スコア

転送下限スコア値以上になると、転送先リストの設定でメール転送します。

● 受信先への配信を停止する

受信先への配信を停止するをチェックすると、転送先にはメールを送信はしましが、受信先には配信されません。

● 転送先リスト

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。

注意

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。

4.2.4 ホワイトリスト

画面4.2.4

【ホワイトリストの設定】
スパムチェックを無効にする条件を指定できます。
1 行内に指定した条件は全て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、実際に逆引き等を行うグローバルIP アドレスを指します。必ずしもSTMP 接続元のIP アドレスではありません。メールヘッダのReceivedに記述されたIP アドレスの可能性もあります。

----- 例 1-----
127.0.0.2 から送信されてきて、from がsender@example.net の場合にスパムチェック無効

host=127.0.0.2 from=sender@example.net

----- 例 2-----
127.0.0.0 ～127.0.0.255 から送信されてきた場合、スパムチェック無効

host=127.0.0.0/255.255.255.0

4.2.5 ブラックリスト

画面4.2.5

【ブラックリストの設定】

ブラックリストはスパム判定方法の1 つという扱いです。ブラックリストの判定に適合した場合のスコアは、基本設定のスパム判定方法で指定できます。
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、実際に逆引き等を行うグローバルIP アドレスを指します。必ずしもSTMP 接続元のIP アドレスではありません。メールヘッダのReceived に記述されたIP アドレスの可能性もあります。

----- 例 -----

from がsender@example.com でto がuser-one@example.com のみの場合にブラックリスト適合

from=sender@example.com to=user-one@example.com

4.3 スパム検出ログ

画面4.3

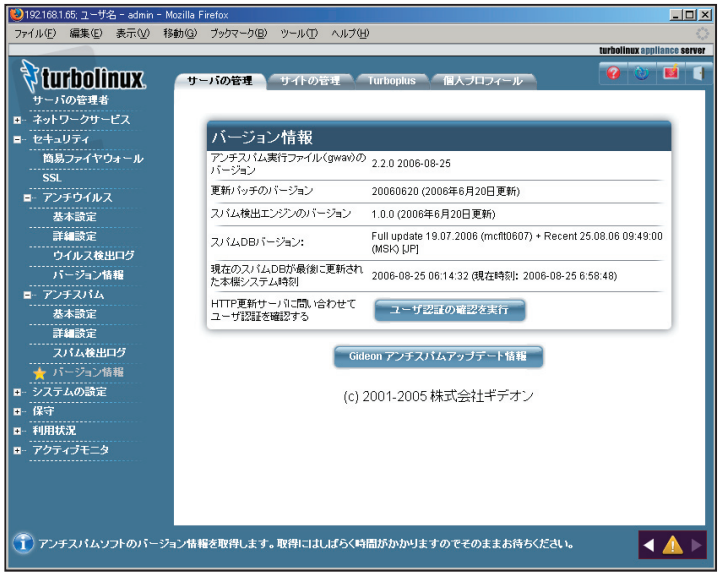
【スパム検出ログ】

スパム検出ログの読み込みを有効にするにチェックし、「保存」ボタンを実行するとログが表示されます。

ログのリストは、検出日時、検出方法、スコア、サブジェクト、From アドレス、To アドレスが表示されます。

4.4 バージョン情報

4.4.1 バージョン情報



画面 4.4.1

【バージョン情報】

アンチスパムの各種モジュールのバージョン情報を表示します。

アンチスパムの実行ファイル(gwav) のバージョン、更新パッチのバージョン、スパム検出エンジンのバージョン、スパムDB バージョン、現在のスパムDBが最後に更新された本機システム時刻等が表示されます。

【ユーザ認証の確認を実行】

ユーザ情報の入力が間違っていたり、本サーバが正常にアップデートサーバにHTTP アクセスできない場合、アップデートが行われません。「合わせてユーザ認証の確認を実行」ボタンを押すと、アップデートサーバへの認証テストを

実行します。しばらく待って画面 4.4.2 のように［OK］が表示されれば認証は OK です。ネットワークにつながっていなかったり、認証に失敗するなどのエラーが発生するとその旨表示されますので、お使いの環境を確認して問題を修正してください。

画面4.4.2

「Gideon アンチスパムアップデート情報」ボタンをクリックすると、http://www.gideon.co.jp/updates サイトにハイパーリンクされます。サイトの情報と比較して、最新に更新されているかご確認ください。

5.1 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。

5.2 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。

5.3 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 バージョン情報」を参照してください。

5.4 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 経由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/ ディレクトリ以下）
・メールサーバ設定ファイル（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 3448-4
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 /
アンチスパム Plus TLAS 対応
共通ユーザーズガイド

2007 年 1 月 9 日　第 3 刷発行

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 3448-4
http://www.gideon.co.jp/