

アンチウイルス for Linux
Turbolinux AS 対応

ユーザーズガイド

はじめに

■ 前提条件

本ユーザーズガイドは、本製品の概要、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。

■ 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

本ユーザーズガイドの著作権は、株式会社ギデオンに帰属します。

本ユーザーズガイドの一部または全部を、株式会社ギデオンに無断で複写することはできません。

GIDEON、ギデオンの名称およびロゴは株式会社ギデオンの商標または登録商標です。

F-SECURE Anti-Virus Linux はエフセキュア社の登録商標です。

The Linux kernel is Copyright 1991,1992,1993,1994,1995,1996 Linus Torvalds (others hold copyrights on some of the drivers, filesystems, and other parts of the kernel) and is licensed under the terms of the GNU General Public License.

Turbolinux はターボリナックス株式会社の登録商標です。
sendmail その他、記載されている会社名、製品名は各社の商標および登録商標です。

■ 表記など

本ユーザーズガイド内では、画面で入力する文字を、イタリック体 (例：*password*) で表示してあります。

目 次

はじめに.....	iii
1 概要.....	1
1-1 導入から契約更新の流れ.....	2
1-2 本製品の特徴・機能.....	3
1-3 ご利用上の注意.....	4
2 利用環境.....	5
3 インストールと初期画面.....	9
3-1. インストール.....	9
3-2. 初期画面.....	14
4 アンインストールと再インストール.....	19
4-1 アンインストール.....	19
4-2 再インストール.....	20
5 ウイルス検出方針についての基本設定.....	22
5-1 基本の設定.....	23
5-2 SMTPfeed の設定.....	27
5-3 プロキシの設定.....	30
5-4 更新スケジュールの設定.....	32
6 ウイルス検出ログ.....	35
7 バージョン情報.....	38
8 定義ファイルおよびモジュールの更新.....	45
9 動作確認.....	54
10 運用・管理.....	58
11 ファイルチェック機能.....	60
付録 サポートサービス.....	66

1 概要

このたびは、本製品をお買い上げいただき、誠にありがとうございます。

コンピュータウイルスは、データのセキュリティを脅かす危険なものです。近年、特にウイルス感染の被害が増大しており、すでに数万種類のウイルスが発見されています。ウイルスに感染すると、データが破壊されたり、コンピュータの機器そのものが動作しなくなる可能性もあります。

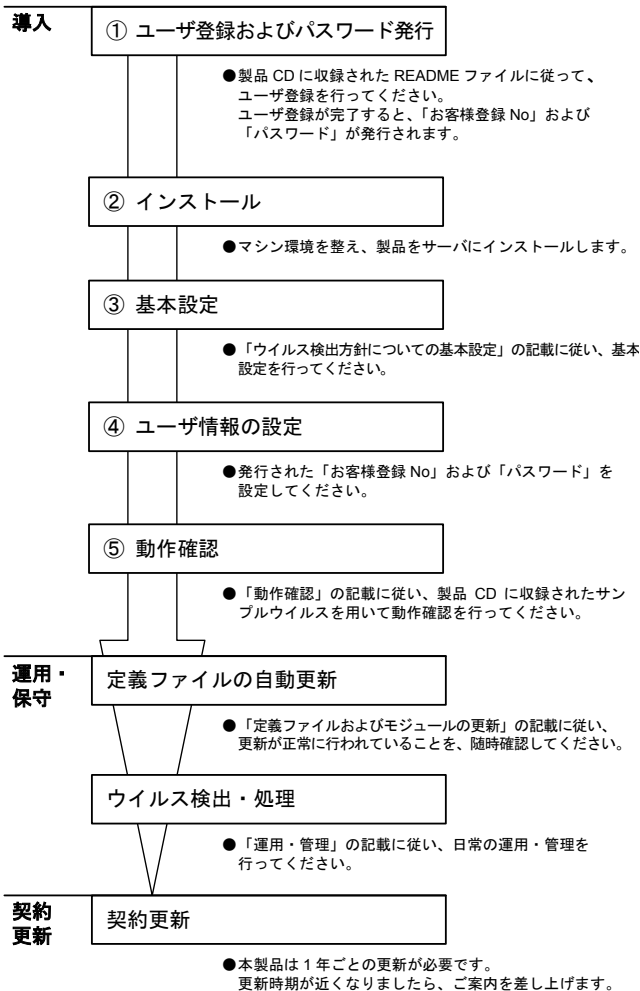
ウイルス感染経路の90%近くが電子メールによるものと言われています。

したがって、「電子メールからのウイルス感染を防ぐこと」が、最も有効な防御といえます。

本製品は、サーバでメール文書をチェックすることで、管理コストの削減およびより安全なウイルスチェックを実現します。

1-1 導入から契約更新の流れ

本製品の導入から運用・保守、契約更新までの流れは、以下のとおりです。



1-2 本製品の特徴・機能

本製品には、以下のような特徴があります。

■ メール送受信時のウイルス検出を一台のサーバ機で実現

すでに稼動しているメールサーバへスムーズにインストールでき、新たなサーバ投資が不要です。ご利用のユーザアカウントをそのままお使いいただけますので、たいへん便利です。メールサーバでの設定ルールもそのまま引き継がれます。

また、「アンチウイルス」専用サーバを、ゲートウェイサーバとしてご利用いただけます。この場合、「アンチウイルス」専用サーバをメールの送受信先に指定し、メールサーバを別途設置することができます。

■ メールサーバのセキュリティを確保するニューテクノロジー

従来のメールスキャン方式では、SPAM、リレー、DoS 攻撃などに対するセキュリティの脆弱性が課題でした。本製品は、ニューテクノロジーによってセキュリティの脆弱性を克服しました。

■ ウイルス検出は、エフセキュア社製 FSAV Linux を採用

近年、新種のウイルスが頻繁に出現しています。これらのウイルスの侵入を防ぐには、新しいパターンに対応した定義ファイルの更新に加え、検索ロジックも更新する必要があります。すなわち、絶えず新種のウイルスに対応するための技術やサービスが不可欠となります。

本製品は、世界的に実績を誇るウイルス対策用ソフト「FSAV Linux」を採用し、新種のウイルスにいち早く対応します。

■ ウイルス定義ファイル・エンジンの自動更新をスケジュール化

頻繁に更新される定義ファイル・検出エンジンのアップデートをスケジュール化しました。手間が省けるとともに、更新忘れもないので安心です。

■ インストールと設定が簡単

本製品は、簡単にインストールできます。また、ウイルスが検出された場合は、メールにその旨のメッセージを付加して通知し、あらかじめ設定された方針（削除または添付）に従って処理します。

1-3 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、1 週間以上も更新されていない場合には、http サイトを確認するか、または再度更新プログラムを起動して、定義ファイルの更新状況を確認してください。

- 容量管理

ディスク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。

- 不正ファイル

不正なファイルの場合、ファイルを削除する指示があっても削除できない場合があります。ウイルス検出の警告があった場合は、不用意にファイルを開かないことをお勧めします。

以下のような場合には、「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。

- サーバがウイルスに感染していたり、システムが正常に動作しないような環境では、ウイルスの検出に失敗することがあります。システムに異常がないことをご確認ください。
- メールの SPAM（スパム）攻撃などで、外部から、不正なメールを大量に受信した場合、メールサーバが停止して、ウイルスが検出できなくなる可能性があります。日常の運用・管理にご注意ください。
- 新種のウイルスに対応した定義ファイルが更新されるまでは、そのウイルスを検出することはできません。

本製品は、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、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。

2 利用環境

『アンチウイルス for Linux Turbolinux AS 対応』は、Turbolinux Appliance Server に対応したメールサーバのアンチウイルスソフトです。

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、以下の URL を参照してください。

URL: <http://www.gideon.co.jp/>

■ 使用条件 (2004 年 4 月現在)

- Linux カーネルインテルアーキテクチャ glibc 2.1.3 以降
- メールサーバ
sendmail8.9.3 以降 8.x
sendmail.cf は「**Mlocal, Msmtp*, Mrelay**」定義を含むこと
- 物理メモリ空き容量 64MB 以上 スワップ (swap) 容量 64MB 以上
- Turbolinux Appliance Server において、下記のパッケージについて表記したバージョン以降のものがインストールされている

Hosting edition:

```
base-services-capstone-1.1.0u-122TL8.noarch.rpm  
base-services-glue-1.1.0u-122TL8.noarch.rpm  
base-services-locale-en-1.1.0u-122TL8.noarch.rpm  
base-services-locale-ja-1.1.0u-122TL8.noarch.rpm  
base-services-ui-1.1.0u-122TL8.noarch.rpm
```

Workgroup edition:

```
base-services-capstone-1.0.1-42TL17.noarch.rpm  
base-services-glue-1.0.1-42TL17.noarch.rpm
```

base-services-locale-en-1.0.1-42TL17.noarch.rpm

base-services-locale-ja-1.0.1-42TL17.noarch.rpm

表記されたバージョンより古い場合、Turbolinux Appliance Server をアップデートしてください。アップデートしない場合、「3-1. インストール」で説明するファイルのアップロードが正常に動作しません。アップデートパッケージの詳細は

<http://www.turbolinux.co.jp/security/indexas10he.html>

の“TLEA-2004-30”を確認してください。

インストール対象マシン環境

- Turbolinux Appliance Server がインストールされたマシンで、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
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。メモリ使用量として約 64MB 確保すれば問題ありません。但しメール量やシステム環境にも左右されるため、十分な大きさのメモリを搭載することを推奨します。

■ 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、以下のようにメールサーバのシステム環境が変更されます。

- 既存の **sendmail.cf** が、「アンチウイルス」対応用に変更され
ず。
元のファイルは、以下の名前で保存されます。
sendmail.cf.org.gwav
- 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
信エージェントを使います。例えば、システムに **procmail** が存在
している場合、その **procmail** を使います。
同様に、システムに **mail.local** が存在している場合、その
mail.local を使います。
両方とも存在している場合は、**mail.local** を使います。
- 他のメールサーバへのメール配信に **smtpfeed** を使います。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。

■ メールサーバのバージョンアップなどによる更新に関する注 意事項

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。

サーバを更新すると、本製品のインストール時に設定した環境が置き
換えられ、ウイルス検出機能が無効になる可能性があります。

メールサーバの更新は、本製品を一旦アンインストールしてから行っ
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

メールサーバの設定（例えば、**sendmail.cf**）を変更する場合な
ども同様の手順になります。

■ インターネット接続による更新に関する注意事項

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アウォールの設定(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。

3 インストールと初期画面

ここでは、本製品のインストール方法とインストール直後の初期画面設定について説明します。

3-1 インストール

《手順 1》 管理画面にログインする

管理者権限のあるユーザ(**admin** など)で管理画面にログインします。

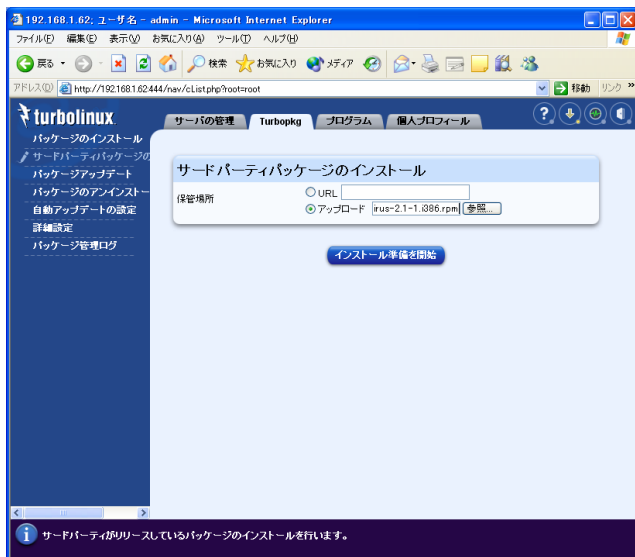
《手順 2》 インストール準備を開始する

画面上部の「Turbopkg」タブをクリックします。

注) OS のバージョン、エディションによっては、画面のタブ位置や文字表記、チェックマークのデザインなどが異なる場合があります。

次に、画面左側のメニューから [サードパーティパッケージのインストール](#) をクリックすると、画面 3-1 が表示されます。

3 インストールと初期画面



画面 3-1

画面 3-1 で、アップロードするファイルを指定します。

「アップロード」のラジオボタンにチェックマークを付けて、[参照] ボタンをクリックします。

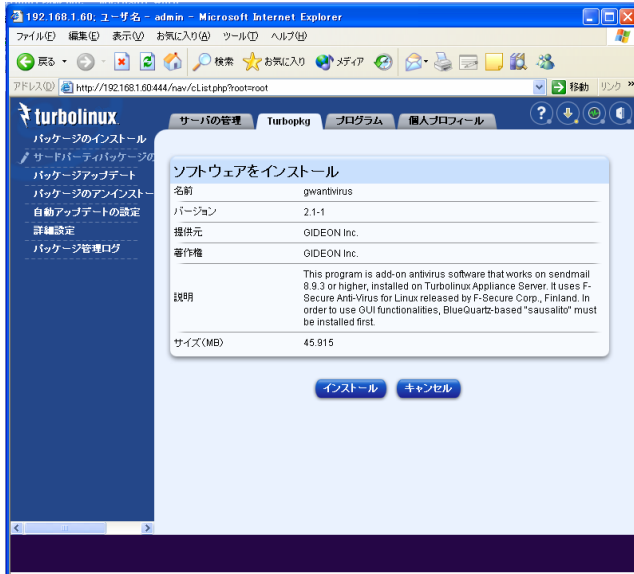
ファイル選択画面が表示されますので、インストール CD の **gwantivirus-xxxx.rpm** (xxxx はバージョン表記) を指定します。

「アップロード」の右側に表示されたファイル名を確認し、[インストール準備を開始] ボタンをクリックします。

《手順 3》 インストールを行う

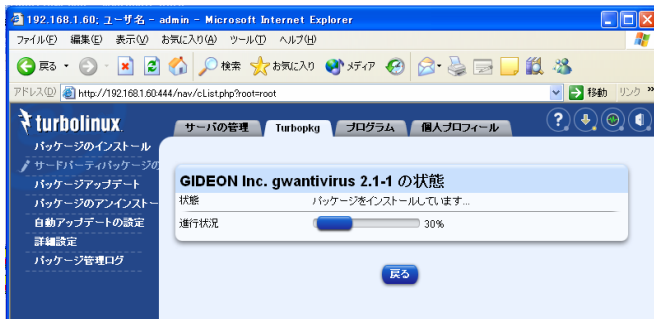
画面 3-2 のようなパッケージ情報が表示されます。

内容を確認して、[インストール] ボタンをクリックします。



画面 3-2

インストールが開始され、画面 3-3 で進捗状況をお知らせします。



画面 3-3

画面 3-4 のように、進捗状況に「100%」と表示されたらインストールは完了です。

インストールには長い場合数十分かかることがあります。数十分が経過しても 100%にならない場合、手順 4 で説明する「パッケージ管理ログ」をクリックしてインストールの状況を確認してください。「gwantivirus-xxxx 100% 完了」のような記述があれば、「アンチウイルス」は正常にインストールされています。



画面 3-4

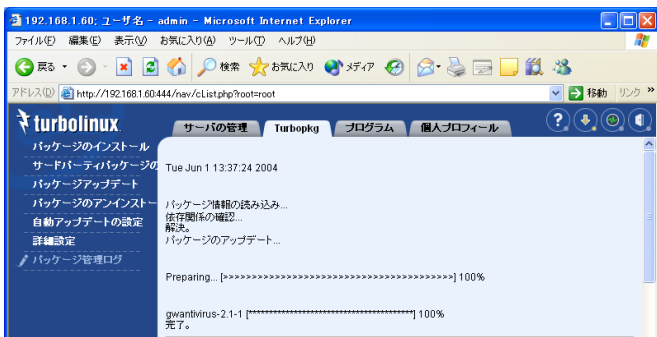
《手順 4》 インストールされたことを確認する

「アンチウイルス」が正常にインストールされたことを確認します。

(1) パッケージ管理ログを確認します。

画面左側のメニューから [パッケージ管理ログ](#) をクリックします。画面 3-5 パッケージ管理ログ画面が表示されます。

画面上に、「gwantivirus-xxxx 100% 完了」のような記述があれば、「アンチウイルス」は正常にインストールされています。



画面 3-5

注) [パッケージ管理ログ](#) をクリックしても表示されない場合、インストールは完了していませんので、しばらくお待ちください。

(2) 「セキュリティ」メニューに、アンチウイルス固有のメニューが追加されたかどうかを確認します。

画面上部の「サーバの管理」タブをクリックし、画面左側のメニューから [セキュリティ](#) をクリックします。

「アンチウイルス」が正常にインストールされると、「セキュリティ」メニューの中に、「アンチウイルス設定」「アンチウイルスログ」「アンチウイルスバージョン情報」の3つのサブメニューが表示されます。

注) 「セキュリティ」メニューの位置やサブメニューの表示は、OSのバージョンによって異なります。

注) 3つのサブメニューが表示されないなど、正常に表示されない場合は、しばらくしてから、ブラウザの[更新]ボタンをクリックして再読み込みを行ってください。

3-2 初期画面

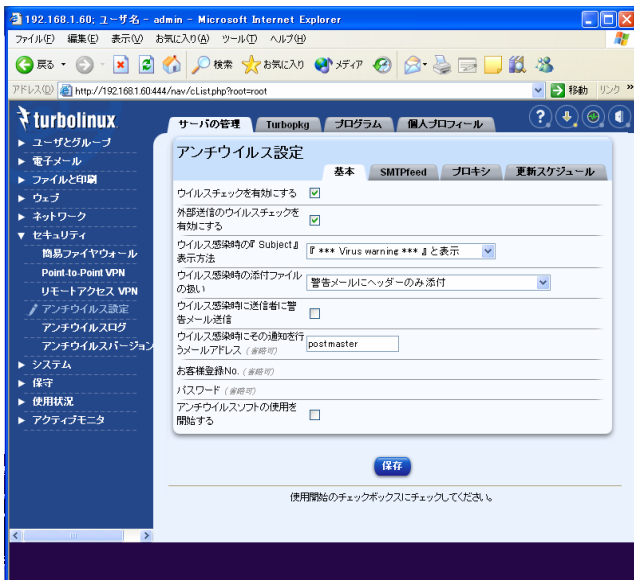
《手順 1》 管理画面にログインする

管理者権限のあるユーザ(**admin** など)で管理画面にログインします。前述の「3-1 インストール」から引き続き行う場合は、直接手順 2 に進んで下さい。

《手順 2》 アンチウイルスソフトウェアの使用を開始する

画面上部の「サーバの管理」タブをクリックし、画面左側のメニューから [セキュリティ](#) → [アンチウイルス設定](#) をクリックします。

画面 3-6 「アンチウイルス設定」画面が表示されます。



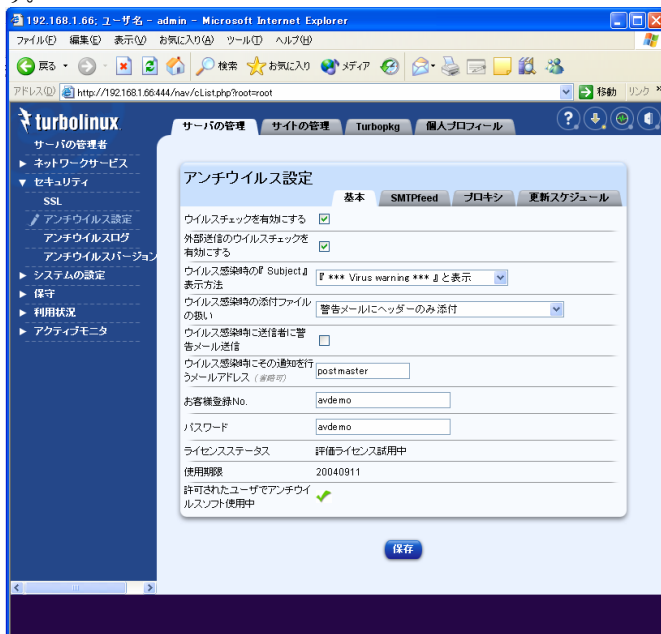
画面 3-6

注意

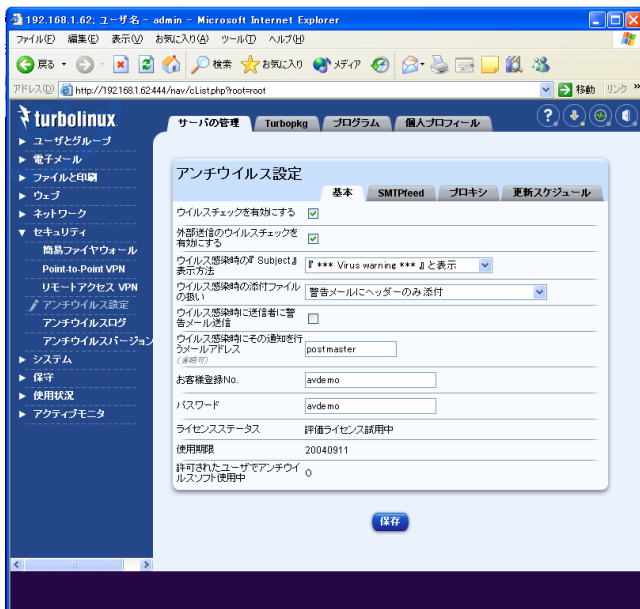
インストール直後に、管理画面の**アンチウイルス設定**メニューをクリックすると、「基本」設定画面でチェックボックスがチェックされず、フィールドがすべて空欄になることがあります。この場合しばらく待ってからブラウザをリロードし、再度画面左側のメニューから **セキュリティ** → **アンチウイルス設定** をクリックしてください。それによりデフォルトで有効な設定が表示されます。

最初の段階では、「お客様登録 No.」「パスワード」に表記がありません。その状態で「アンチウイルスソフトを使用開始する」にチェックをつけて [保存] ボタンを押します。

画面 3-7 または、画面 3-8「アンチウイルス設定」画面が表示されます。



画面 3-7 (Hosting edition)



画面 3-8 (Workgroup edition)

この画面では評価試用ユーザのお客様登録 No.、パスワード、ライセンスステータス、評価試用の使用期限などが表示されます。

- 評価試用の場合：

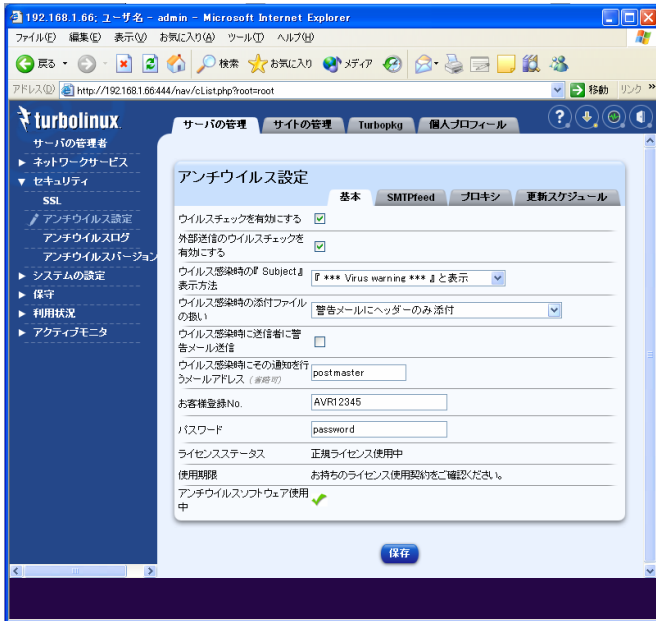
評価試用の場合、開始後 3 ヶ月間に限り、アンチウイルス機能の最新定義ファイル・モジュール等を随時更新します。3 ヶ月を超えると更新が停止し、新しいウイルスに対応できなくなります。

- 製品版を購入されている場合：

ユーザ登録の際に発行された「お客様登録 No.」と「パスワード」を該当フィールドに入力して [保存] ボタンを押してください。

「お客様登録 No.」と「パスワード」について詳しくは「5-1. 基本の設定」を参照してください。

画面 3-9 が表示されます。



画面 3-9 (Hosting edition)

正規ライセンスユーザとしての使用期限は契約内容によって異なりますので、お持ちの書類等をご確認ください。

注意

誤った「お客様登録 No.」「パスワード」を入力しても GUI 画面ではチェックされません。文字列を正しく入力してください。正しい「お客様登録 No.」と「パスワード」を入力して初めて、HTTP 経由の定義ファイル等の更新が可能になります。

「お客様登録 No.」「パスワード」の確認方法は「7. バージョン情報」を参照してください。

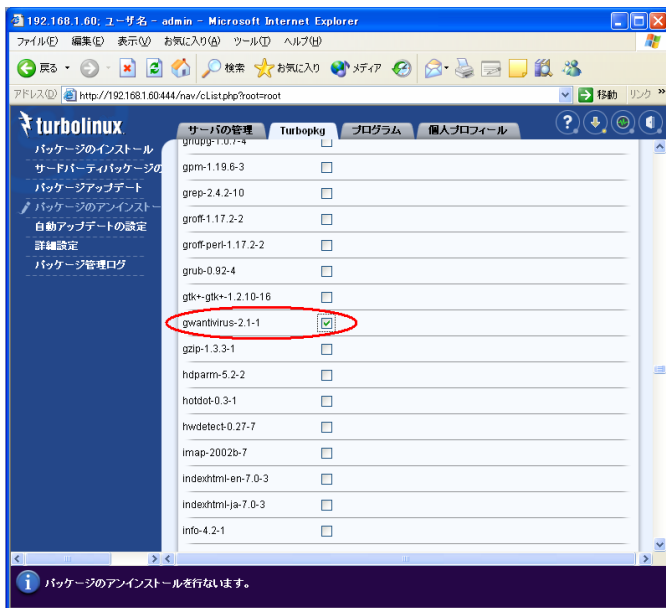
4 アンインストールと再インストール

ここでは、本製品のアンインストールと再インストール方法について説明します。

4-1 アンインストール

《手順 1》 管理画面にログインする

管理者権限のあるユーザ(**admin** など)で管理画面にログインします。



画面 4-1

《手順 2》 アンインストールを行う

画面上部の「Turbopkg」タブをクリックします。

次に、画面左側のメニューから [パッケージのアンインストール](#) をクリックすると、現在システムにインストールされているパッケージの一覧が表示されます。

画面 4-1 のように、`gwantivirus-xxxx` (`xxxx` はバージョン表記) にチェックマークを付けて、[アンインストール] ボタンを押します。

注) [アンインストール] ボタンは画面の下部にありますのでスクロールしてください。

これでアンインストールは完了です。

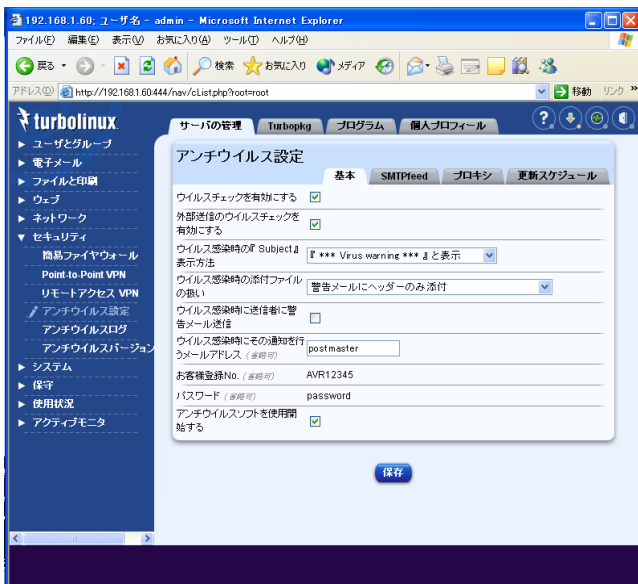
4-2 再インストール

アンチウイルスソフトをアンインストール後、再度アンチウイルスソフトをインストールする場合 (再インストール)、まずは「3. インストール」で説明した手順でアンチウイルスソフトの rpm をインストールし、その後、以下の操作を必ず行ってください。

《手順 1》 管理画面を開く

再インストール後「3-2 初期画面」の管理画面を開きます (画面 4-2)。

管理画面では、アンインストールする以前に有効であった設定情報が表示されます。ただし、この時点では、表示される情報と実際のシステム設定情報は一致していません。



画面 4-2

注意

再インストール直後に管理画面の[アンチウイルス設定](#)メニューをクリックすると、「基本」設定画面でチェックボックスがチェックされず、フィールドがすべて空欄になることがあります。この場合しばらく待ってからブラウザをリロードし、再度画面左側のメニューから[セキュリティ](#) → [アンチウイルス設定](#)をクリックしてください。それによりアンインストール前の設定が表示されます。

《手順 2》 管理画面の設定で上書きする

表示された状態で [保存] ボタンを押します。これにより画面に表示された設定内容を、実際のシステム設定に上書きすることができます。

注意

[保存] ボタンを改めて押さない限り、再インストール後のシステムで以前の設定項目が反映されませんのでご注意ください。

5 ウイルス検出方針についての基本設定

ここでは、ウイルス検出方針の基本設定について説明します。

「アンチウイルス設定」画面の、「基本」「SMTPfeed」「プロキシ」「更新スケジュール」の4つタブで画面を切り替えて、「アンチウイルス」の基本設定を行います。

タブ名	説明	参照先
基本	ウイルス検出時の動作やユーザ情報などの基本的な設定を行います。	5-1 基本の設定
SMTPfeed	リレーホストの設定を行います。sendmail版を使用しているときのみ設定可能です。	5-2 SMTPfeed の設定
プロキシ	プロキシサーバを経由して外部にアクセスしている場合に、プロキシの設定を行います。	5-3 プロキシの設定
更新スケジュール	定義ファイルおよびモジュールの自動更新スケジュールの設定を行います。	5-4 更新スケジュールの設定

注) 「アンチウイルス設定」画面の項目に文字を入力する場合、半角英数字を使用してください。全角文字を使用すると、正しく動作しなくなりますのでご注意ください。

5-1 基本の設定

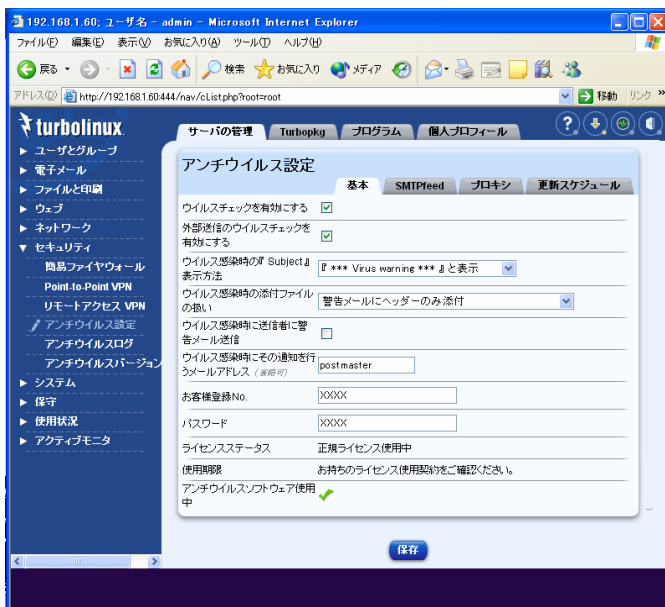
「基本」画面で、ウイルスチェックの稼動/停止、ウイルス検出時の動作、ユーザ情報などを設定します。

《手順 1》 「基本」画面を表示する

管理者権限のあるユーザ(admin など)で管理画面にログインします。

画面上部の「サーバの管理」タブをクリックし、画面左側のメニューから [セキュリティ](#) → [アンチウイルス設定](#) をクリックします。

画面 5-1 「アンチウイルス設定」画面が表示されます。



画面 5-1

《手順2》 基本設定を行う

【ウイルスチェックを有効にする】

チェックマークを付けると、ウイルス検出機能が稼働します。
チェックマークをはずすと、ウイルス検出機能が停止します。

注) ウイルス検出機能が停止した状態では、以下の機能はすべて無効になります。

【外部送信のウイルスチェックを有効にする】

チェックマークを付けて有効にすると、受信メールだけでなく、送信 (Outgoing) メールもウイルスチェックされます。

【ウイルス感染時の『Subject』表示方法】

ウイルスが検出された受信者メールの表題 (サブジェクト) の表示方法を選択します。以下の3通りの表示方法があります。

- ① 『*** Virus Warning ***』と表示
受信したメールの表題を変更して、「*** Virus Warning ***」と表示します。
- ② 元のサブジェクトのまま表示
受信したメールの表題を特に変更しません。
- ③ 『Virus Warning: 元のサブジェクト』と表示
受信したメールの表題の先頭に「Virus Warning」と書き添えます。

例

オリジナルの表題が「第10回定期講演会開催のお知らせ」の場合、受信者メールの表題は、それぞれ以下のように表示されます。

- ① *** Virus Warning ***
- ② 第10回定期講演会開催のお知らせ
- ③ Virus Warning: 第10回定期講演会開催のお知らせ

【ウイルス感染時の添付ファイルの扱い】

ウイルスが検出された場合の、添付ファイルの扱いについて設定します。以下の4通りの方法があります。

- ① ウイルスファイルを削除する
ウイルス感染した部分を削除し、メール本文を別添付形式で送信します（ウイルスファイルを0バイトで添付して送信します）。ただし、完全に削除できない場合がありますので、③または④の選択を推奨します。
- ② ウイルスを添付したまま送信
ウイルスファイルを別添付形式にして送信します。
- ③ 警告メールにヘッダーのみ添付
ウイルスメールそのものを削除し、ヘッダー情報を別添付形式にして送信します。
- ④ ウイルスメールはすべて削除し警告メールのみ送信
警告メッセージのみ送信します。

【ウイルス感染時に送信者に警告メール送信】

チェックマークを付けると、ウイルス検出時に送信者へ警告メールを送信します。

【ウイルス感染時にその通知を行うメールアドレス】

ウイルスが検出された場合の通知先メールアドレスを指定します。

例

「postmaster」「tanaka」「admin@gideon.co.jp」の3人に通知する場合

```
postmaster tanaka admin@gideon.co.jp
```

のように、1行で、半角スペースで区切って入力します。

【お客様登録 No.】

製品購入時、ユーザ登録をした際に発行された「お客様登録 No.」を入力します。使用開始の状態では、自動的に評価試用ユーザが表示されます。

【パスワード】

製品購入時、ユーザ登録をした際に発行された「パスワード」を入力します。使用開始の状態では、自動的に評価試用ユーザが表示されません。

重要

「お客様登録 No.」および「パスワード」は、インターネット経由の自動更新に使用する重要なユーザ情報です。ユーザ情報を設定しないと、定義ファイルおよびモジュールの更新が行われません。

定義ファイルおよびモジュールの更新については、「8 定義ファイルおよびモジュールの更新」を参照してください。

《手順 3》 基本設定を保存する

各項目の設定内容を確認し、[保存] ボタンをクリックします。
「基本」画面の設定が保存されます。

5-2 SMTPfeed の設定

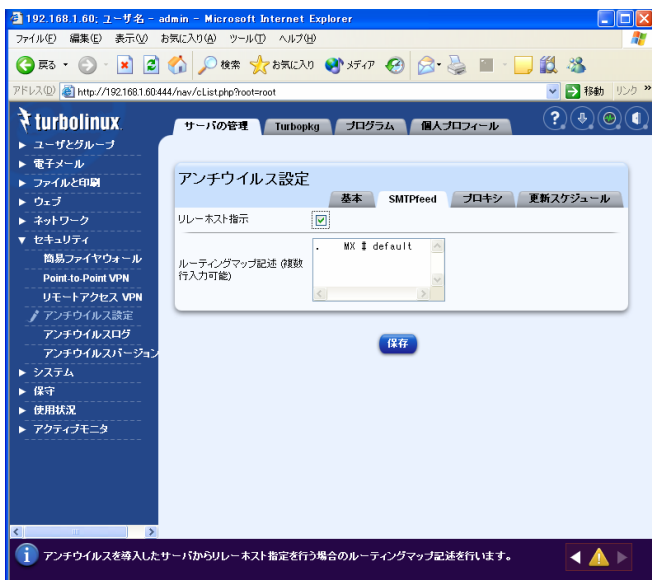
本サーバをリレーホストとして利用する場合は、「SMTPfeed」画面で、リレーホストの設定を行います。

注) この設定は、メールサーバソフトとして sendmail を使用しているときのみ有効です。

《手順 1》 「SMTPfeed」画面を表示する

以下の「アンチウイルス設定」画面で「SMTPfeed」タブをクリックします。

「アンチウイルス設定」画面を表示する手順については、「5-1 基本の設定」の《手順 1》を参照してください。



画面 5-2

《手順2》 リレーホストの設定を行う

【リレーホスト指示】

チェックマークを付けると、本サーバをリレーホストとして利用し、外部メールサーバにリレーするように設定できます。

【ルーティングマップ記述】

「リレーホスト指示」を有効にした場合、ルーティングマップの記述が必要です。

ルーティングマップは、以下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** などが指定できません。

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

- `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。
- `.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。
- `.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。
- `.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。
- `. 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) #以降はコメントなので設定には何ら影響しません。

《手順3》 SMTPfeed の設定を保存する

各項目の設定内容を確認し、[保存] ボタンをクリックします。
「SMTPfeed」画面の設定が保存され、「基本」画面に戻ります。

5-3 プロキシの設定

定義ファイルおよびモジュールの更新は、HTTP で外部のアップデートダウンロード用サーバにアクセスして行われます。したがって本サーバから HTTP による外部アクセスができることが必須です。

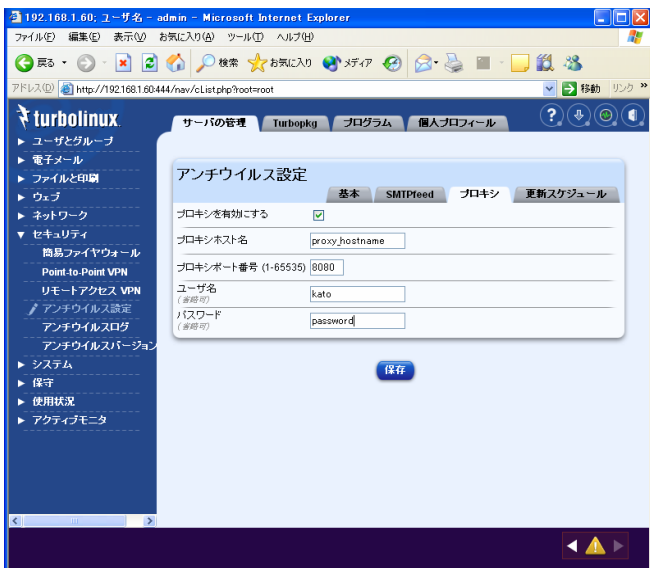
ネットワーク環境によっては、クライアントが社内プロキシサーバを経由して外部にアクセスしている場合があります。その場合は「プロキシ」画面でプロキシ設定を行ってください。

注) 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。

《手順 1》 「プロキシ」画面を表示する

「アンチウイルス設定」画面で「プロキシ」タブをクリックします。

「アンチウイルス設定」画面を表示する手順については、「5-1 基本の設定」の《手順 1》を参照してください。



画面 5-3

《手順2》 プロキシの設定を行う

【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」のアップデート時、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) ユーザ名を入力せずに、パスワードだけ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。

《手順3》 プロキシの設定を保存する

各項目の設定内容を確認し、[保存] ボタンをクリックします。「プロキシ」画面の設定が保存され、「基本」画面に戻ります。

5-4 更新スケジュールの設定

定義ファイルおよびモジュールは、デフォルトでは、HTTP 経由で外部サーバに 1 日 1 回アクセスし、更新する必要がある場合に更新されます。

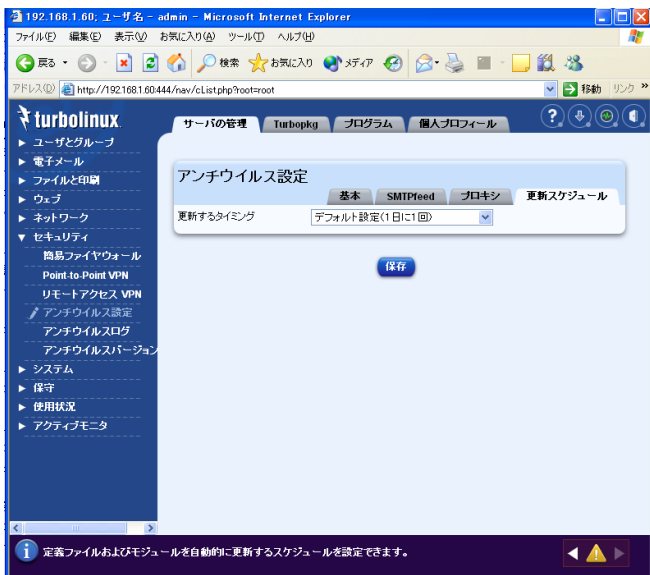
「更新スケジュール」画面では、このアクセスのタイミングを変更することができます。

また、ユーザが、任意にアクセスタイミングを指定したい場合、直接コマンドラインから設定する方法もあります。

《手順 1》 「更新スケジュール」画面を表示する

「アンチウイルス設定」画面で「更新スケジュール」タブをクリックします。

「アンチウイルス設定」画面を表示する手順については、「5-1 基本の設定」の《手順 1》を参照してください。



画面 5-4

《手順2》 更新スケジュールの設定を行う

【更新するタイミング】

更新するタイミングは、「1日1回」「3時間おき」「6時間おき」「12時間おき」から選択できます。指定した時間ごとにHTTP外部アクセスを行い、定義ファイルおよびモジュールが自動更新されます。

更新スケジュールを任意に設定したい場合は、「ユーザが自分で設定する」を選択します。この場合、直接コマンドラインから、更新スケジュールを設定する必要があります。

設定については、後述の「・更新スケジュールを任意に設定する場合」を参考にしてください。

注) 「ユーザが自分で設定する」を利用するには、スケジュール設定機能「クーロン」についての知識が必要です。

「クーロン」の詳しい使い方は、本ユーザーズガイドの範囲外となりますので、他の参考文献またはマニュアルなどを参照してください。

また、「1日1回」を選択した場合で、更新時刻のみ変更したいときも、コマンドラインからの設定が必要です。

設定については、後述の「・更新頻度は1日1回で、更新時刻だけ変更する場合」を参考にしてください。

《手順3》 更新スケジュールの設定を保存する

各項目の設定内容を確認し、[保存] ボタンをクリックします。「更新スケジュール」画面の設定が保存され、「基本」画面に戻ります。

- 更新スケジュールを任意に設定する場合

この操作を行う前に、「更新スケジュール」画面の「更新のタイミング」で、「ユーザが自分で設定する」を設定しておく必要があります。

システムには「クーロン」というスケジュール設定機能が装備されていて、設定したスケジュールに従い特定のプログラムが実行されます。

この「クローン」を利用して更新スケジュールを設定します。

/etc/cron.d/pavupdate.user の下にファイルを作成し、以下のように記述します。

```
<分> <時> <日> <月> <曜日> root /usr/local/gwav/pavupdate
```

その後、crond を再起動します。

crond を再起動するには、以下のどちらかのコマンドを入力してください。

```
#service crond restart
```

または

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

注意

上記のファイル (/etc/cron.d/pavupdate.user) は、アンインストール時には削除してください。再インストールした場合「ユーザが自分で設定する」を選択し、このファイル名を再度作成してください。

- 更新頻度は1日1回で、更新時刻だけ変更する場合

この操作を行う前に、「更新スケジュール」画面の「更新のタイミング」で、「デフォルト設定 (1日1回)」を設定しておく必要があります。

コマンドラインから、/etc/crontab ファイルの下線部を、任意の時刻に変更します。

```
02 4 * * * root run-parts /etc/cron.daily
```

その後、crond を再起動します。

crond の再起動については、前述の「更新スケジュールを任意に設定する場合」を参照してください。

6 ウィルス検出ログ

ここでは、ウイルスに関するログを閲覧する方法について説明します。

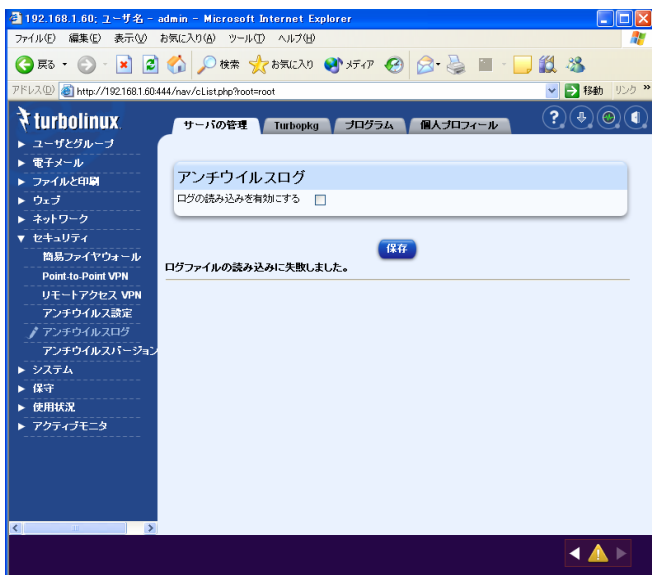
デフォルトでは、GUI 管理画面からはメールログにアクセスできませんが、画面 6-1「アンチウイルスログ」画面で、ログの読み込みを有効にすると、GUI 管理画面でもログを表示することができます。この際、メールログファイルが管理者以外にも読み込み可能になります。セキュリティ上問題がある場合には、この機能を有効にしないことをお勧めします。

《手順 1》 「アンチウイルスログ」画面を表示する

画面上部の「サーバの管理」タブをクリックし、画面左側のメニューから [セキュリティ](#) → [アンチウイルスログ](#) をクリックします。

画面 6-1「アンチウイルスログ」画面が表示されます。

「ログの読み込みを有効にする」にチェックマークを付け、[保存] ボタンをクリックします。



画面 6-1

《手順2》 ログを確認する

メールログが読み込まれ、画面 6-2 のように「ウイルスに関するログ一覧」が表示されます。

ログのサイズが大きい場合、ログ一覧の表示にしばらく時間がかかることがあります。

注) ログローテートした古いファイルは読み込まれません。

ログローテートの設定については、システム設定に依存しますので、管理者に確認してください。

192.168.1.60: ユーザ名 - admin - Microsoft Internet Explorer

アドレス http://192.168.1.60:444/nav/c/List.php?root=root

サーバの管理 Turbokpg プログラム 個人プロフィール

アンチウイルスログ

ログの読み込みを有効にする

保存

ウイルスに関するログ一覧

2004年4月日13時56分現在

Apr 20 13:56:28 atom gwaw[21417]: VIRUS FOUND -- FROM: root@atom.mydomain TO: admin
Apr 20 13:56:28 atom gwaw[21417]: VIRUS type -- eicar.com\infection: EICAR_Test_File [F-Prot]
Apr 20 13:56:28 atom gwaw[21417]: VIRUS type -- eicar.com\infection: EICAR-Test-File [AVP]
Apr 20 13:56:28 atom gwaw[21417]: VIRUS type -- eicar.com\infection: EICAR Test File [Onion]

メールログに記録されているウイルス感染履歴を表示します。ログのサイズが大きい場合取得に時間がかかることがありますのでしばらくお待ちください。

画面 6-2

ウイルスに関する履歴があると、「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。

- 日時：ウイルスが検出された日時
- ファイル名：ウイルスに感染したファイル名
- ウイルスタイプ：感染ウイルスの種類
- FROM：メール送信者
- TO：メール受信者

例

ログ表示の例

```
Apr 20 13:56:28 atom gwav[PID]: VIRUS FOUND -- FROM:
aaaa@gideonanonymous.co.jp TO: bbbb@gideon.co.jp
```

```
Apr 20 13:56:28 atom gwav[PID]: VIRUS type ?
cccc.xlsinfection: DDDDD
```

このログ表示は、以下のことを示しています。

- ウイルスに感染したファイル： ccccc.xls
- ウイルスタイプ： DDDDD
- FROM（送信者）： aaaa@gideonanonymous.co.jp
- TO（受信者）： bbbb@gideon.co.jp

7 バージョン情報

ここでは、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する方法について説明します。

「アンチウイルスバージョン情報」画面で、「アンチウイルスの実行ファイル」「更新パッチ」「ウイルス検出エンジン」「ウイルス定義ファイル」の各バージョンを確認できます。

これらは、常に最新のバージョンにしておく必要があります。

また HTTP 更新が正しく行われるか否かを確認することができます。

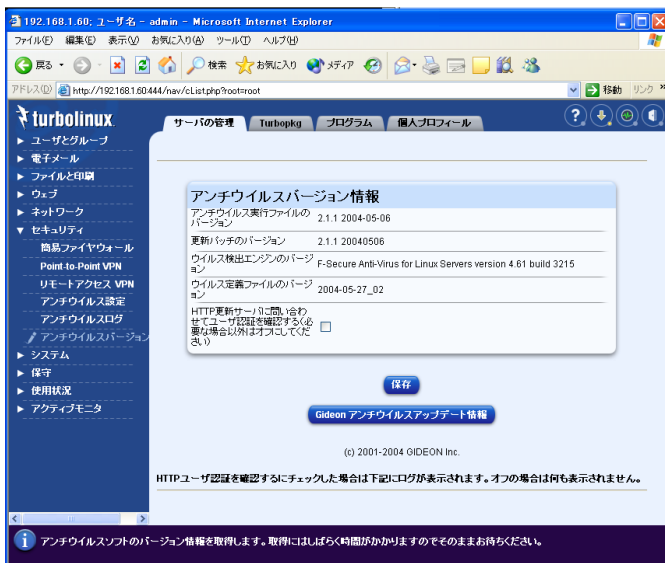
定義ファイルおよびモジュールの更新については、「8 定義ファイルおよびモジュールの更新」を参照してください。

《手順 1》 「アンチウイルスバージョン情報」画面を表示する

画面上部の「サーバの管理」タブをクリックし、画面左側のメニューから [セキュリティ](#) → [アンチウイルスバージョン情報](#) をクリックします。

画面 7-1 「アンチウイルスバージョン情報」画面が表示されます。

注) 画面を表示するまでにしばらく時間がかかります。



画面 7-1

《手順 2》 バージョン情報を確認する

【アンチウイルス実行ファイルのバージョン】

アンチウイルスの実行ファイルを含むモジュールのバージョンです。

【更新パッチのバージョン】

上記モジュールを含む更新パッチを、アップデートサイトからダウンロードしたときのバージョンです。

【ウイルス検出エンジンのバージョン】

ウイルス検出モジュールのバージョンです。

【ウイルス定義ファイルのバージョン】

ウイルス定義ファイルのバージョンです。

【HTTP 更新サーバに問い合わせさせてユーザ認証を確認する】

アンチウイルス基本設定画面で入力した「お客様登録 No.」「パスワード」で正しく最新ウイルス定義ファイルやモジュールのアップデートができるかどうかを確認することができます。

チェックボックスにチェックして [保存] ボタンを押すと、HTTP サーバへの問い合わせ結果ログが表示されます。(画面 7-2)

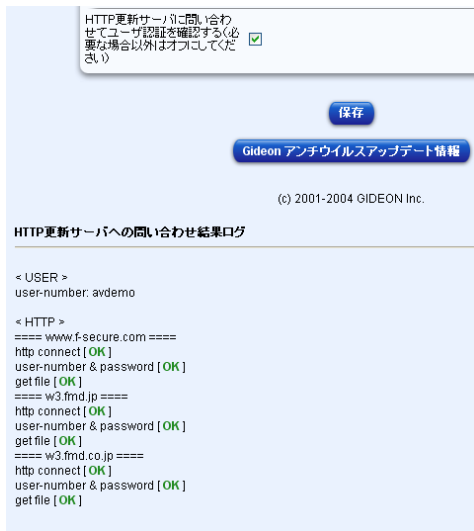
注意

チェックボックスにチェックして [保存] ボタンを押した後、画面が表示されるまでに数分かかります。

HTTP 接続を確認する場合を除き、通常はチェックボックスをオフにしておくことをお勧めします。

また、コマンド操作による確認も可能です。詳しくは、「8. 定義ファイルおよびモジュールの更新」を参照してください。

正しく認証された場合、以下のように各種サーバへの接続と認証の状況が[OK]と表示されます。



画面 7-2

注意

評価試用ユーザで HTTP 認証を行った場合、評価期限が過ぎても認証は成功するので[OK]と表示されます。評価期限が過ぎると最新定義ファイル・モジュールの更新ができなくなりますが、更新の可否はここではチェックしません。

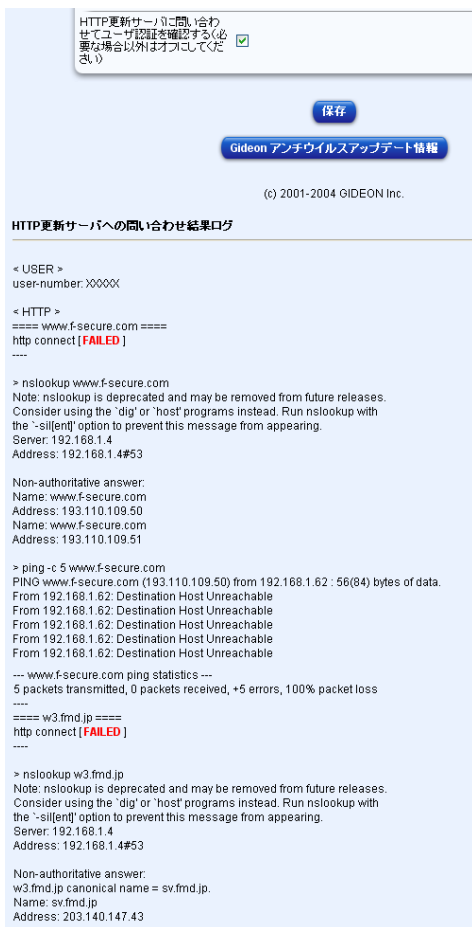
最新定義ファイル・実行ファイルの状態はバージョン表示で確認してください。バージョンが古い場合、アップデートは実際には行われていません。

正しく認証されない場合、以下のようにいずれかの“user-number & password”情報に[FAILED]が表示されます。



画面 7-3

ネットワークが接続していないか HTTP サーバに接続できない場合、“http connect” に [FAILED] が表示されます (画面 7-4)。



画面 7-4

具体的にチェックすべき点は以下になります。

- 「nslookup xxxx Connection time out」 および 「ping xxxx Unknown host」と表示される場合、正しく DNS サーバを指定していること、および DNS が正しく解決されることを確認してください。
- 「ping xxxx Destination Host Unreachable」と表示される場合、ゲートウェイの指定や物理ネットワークの状態など、ネットワークが正しく接続していることを確認してください。
- 「http connect」のみ問題がある場合、ご使用のファイアウォール等で HTTP ポートを開いているか、またはプロキシサーバの有無、ポート番号の指定、プロキシでのユーザ認証等を確認してください（アンチウイルスでプロキシを指定する場合は「5-3. プロキシの設定」を参照してください。）

【HTTP 更新サーバに問い合わせるユーザ認証を確認する】

[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、株式会社ギデオンの URL にアクセスし、アップデートの最新情報や各種ご案内を確認していただけます。

8 定義ファイルおよびモジュールの更新

本製品では、ウイルス検出のために用いる定義ファイルおよびモジュールは、インターネット経由で自動更新する仕組みになっています。

注意

インストール、基本設定、およびユーザ設定が完了した後、以下のモジュールなどの更新コマンドを必ず実行してください。最新のモジュールと定義ファイルを適用することで、より安全な対策になります。

注意

この章のコマンド操作は、GUI 管理画面とは別に、管理者がシステムにログインして行います。クライアント PC から telnet でリモートログインする方法などがあります。

Windows クライアントで DOS プロンプトを起動して以下を実行します。次ページの「**■**現モジュールのバージョンおよび HTTP 更新可否の確認」のコマンドを実行する前に、以下のコマンドを実行してください。

例

以下のイタリック部分を入力してください。

```
> telnet <サーバ名または IP アドレス>
```

```
login: admin
```

```
Password: <ユーザ「admin」のパスワード>
```

```
[admin@サーバ名]$          ログインすると、プロンプトが表示  
                           されます。
```

```
[admin@サーバ名]$ su -    「su (スペース) -」と入力すると、  
                           root ユーザに切り替わります。
```

```
Password: <「root」ユーザのパスワード>
```

```
[root@サーバ名]#          root 権限でログインすると、  
                           「#」プロンプトが表示されます。
```

■ 現モジュールのバージョンおよび HTTP 更新可否の確認

現在使われているモジュールのバージョンなどの確認、およびサーバから HTTP による更新が可能かどうかを確認します。前述の「ユーザ情報の設定」完了後、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
```

コマンドを実行すると、リスト 8-1 のメッセージが表示されます。

表示内容は、バージョンにより異なる場合があります。

日本語詳細情報をメールで取得する方法については、「9 動作確認」の「■トラブルシューティング」を参照してください。

```
< VERSION >
GWAV version:
*1 -r-sr-xr-x 1 root root 132656 May 20 15:09 /usr/local/gwav/gwav
*2 Engine: 2.1.1 2004-05-06
*3 Patch: Proserver with AntiVirus version 2.1.1 20040506
*4 RPM: gwantivirus-2.1-1
*5 FSAV version:
*6 F-Secure Anti-Virus for Linux Servers version 4.61 build 3215
*7
*8 Copyright (c) 1999-2004 F-Secure Corporation. All Rights Reserved.

F-Secure Anti-Virus Copyright (c) 1993-2004, F-Secure Corp.
Portions:
Copyright (c) 1991-2004 Kaspersky Labs, Ltd.

F-Secure Anti-Virus for Linux Servers Command line client version:
F-Secure Anti-Virus for Linux Servers version 4.61 build 3215

F-Secure Anti-Virus for Linux Servers Daemon version:
F-Secure Anti-Virus for Linux Servers version 4.61 build 3215

Database version: 2004-05-27_02

*9
*10 Scanner Engine versions:
*11 F-Secure Corporation Libra engine version 2.1 build 11
*12 F-Secure Corporation Libra database version 2004-05-26

F-Secure Corporation Orion engine version 1.2 build 33
F-Secure Corporation Orion database version 2004-05-21

Kaspersky Labs. AVP FPI Engine engine version 4.0 build 164
Kaspersky Labs. AVP FPI Engine database version 2004-05-27

*13

< USER >
*14 user-number: xxxxx
*15
*16 < HTTP >
*17 ===== www.f-secure.com =====
*18 http connect [ OK ]
user-number & password [ OK ]
get file [ OK ]
===== w3.fmd.jp =====
*19 http connect [ OK ]
user-number & password [ OK ]
get file [ OK ]
===== w3.fmd.co.jp =====
http connect [ OK ]
user-number & password [ OK ]
get file [ OK ]
```

リスト 8-1

説明

<VERSION> セクション

*1: **GWAV version:**

「アンチウイルス」実行ファイル (**gwav**) に関する情報
以下の URL に最新の **gwav** モジュール更新情報が掲載されています。
*3 および *4 に表示されたバージョンが、最新のものであるかどうか
を確認してください。

<http://www.gideon.co.jp/antivirus/update.html>

*2: **-r-sr-xr-x 1 root root 132656 May 20 15:09 /usr/local/gwav/gwav**

現在の **gwav** ファイル情報
現在サーバにある **gwav** 実行ファイルに関するアクセス権限、更新日
などを表示します。

*3: **Engine: 2.1.1 2004-05-06**

現在使用している **gwav** モジュールのバージョン表示
更新が正常に行われている場合、*4 と同じ情報を表示します。
*4 とバージョン番号または更新日付が異なる場合は、**gwav** モジュール
以外の更新が行われたことを意味します。

*4: **Patch: Proserver with AntiVirus version 2.1.1 20040506**

gwav モジュールを含む更新パッチを、サイトからダウンロードした
時のバージョン表示

*5: **RPM: gwantivirus-2.1-1**

RPM パッケージのバージョン表示
「アンチウイルス」を導入した **rpm** パッケージのバージョン情報を表
示します。この例では、**rpm** パッケージ名「**gwantivirus**」で、バ
ージョンが「2.1-1」であることを意味します。

***6: FSAV version:**

ウイルス検出 **fsav** モジュールおよび定義ファイルに関する情報
以下の URL に最新の **fsav** モジュール更新情報が掲載されています。
*4 に表示されたバージョンが、最新のものであるかどうかを確認して
ください。

<http://www.gideon.co.jp/antivirus/update.html>

***7: F-Secure Anti-Virus for Linux Servers version 4.61
build 3215**

ウイルス検出エンジンのバージョン表示

***8: Database version: 2004-05-27_02**

定義ファイルのバージョン表示

***11: Scanner Engine versions:**

F-Secure Corporation Libra engine version 2.1 build 11

F-Secure Corporation Libra database version 2004-05-26

F-Secure Corporation Orion engine version 1.2 build 33

F-Secure Corporation Orion database version 2004-05-21

**Kaspersky Labs. AVP FPI Engine engine version 4.0 build
164**

**Kaspersky Labs. AVP FPI Engine database version
2004-05-27**

ウイルス検出エンジン Libra、Orion、AVP のバージョンおよび定義
ファイル最終更新日の表示

< USER > セクション

***13: user-number: XXXXXX**

「ユーザ情報の設定」で入力された「お客様登録 No.」を表示

< HTTP > セクション

*14: ===== **www.f-secure.com** =====

定義ファイルダウンロード先サーバ名

*15: **http connect [OK]**

上記サイトへ http 接続ができたかどうかをチェックした結果表示

[OK]ではなく[FAILED]となっている場合は、このマシンから外部のサイトへ http 接続ができなかったことを意味します。

この場合の原因はさまざまですが、DNS で解消できない場合は、ネットワーク上から外部所定のサイトに接続できません。またファイアウォールなどの設定で http の外部への接続ができない可能性があります。

手動による外部の http サイトへの接続が可能かどうかを確認してください。

*16: **user-number & password [OK]**

サイトアクセスした場合に、認証されたかどうかをチェック

[OK]ではなく[FAILED]となっている場合は、登録されたユーザ情報が間違っているか、またはすでに更新切れの期間になっており、アクセスできない状態であることを意味します。

*17: **get file [OK]**

http サイトからファイルのダウンロードができるかどうかをチェック

*18: ===== **w3.fmd.jp** =====

モジュールダウンロード先サーバ名 (第1サイト)

*19: ===== **w3.fmd.co.jp** =====

モジュールダウンロード先サーバ名 (第2サイト)

■ 自動更新ファイルと起動スクリプト

自動更新の対象となるのは、以下の2種類のファイルです。

1) モジュールなどの更新ファイル

最新の検出エンジン、システムの更新に伴うモジュール、およびバグフィックスされたモジュールなどを更新します。更新対象ファイルは以下のディレクトリ下に展開されます。

```
/usr/local/gwav
```

2) ウイルス検出に用いられる定義ファイルなどの更新ファイル

新種ウイルス検出のために、最新の定義ファイルを http サイトより更新します。更新ファイルは、以下のディレクトリに展開されます。

```
/usr/local/fsav
```

定義ファイルおよびモジュールを手動で更新する場合、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/pavupdate
```

■ 自動更新スケジュール

本製品をインストールすると、以下のファイルが追加されます。このスクリプトにより定義ファイルおよびモジュールが更新されます。

```
/etc/cron.daily/pavupdate
```

更新時刻の設定などは、以下のファイルに記述されています。

```
/etc/crontab
```

crontab の設定については、各 Linux のディストリビューションに同梱されたマニュアルまたは「**man crontab**」を参照してください。

■ 更新ログの確認

更新されたログは、以下の方法で確認できます。

1) 定義ファイルの更新ログの確認

最新の定義ファイルの更新ログは、以下のコマンドで確認できます。

```
#cat /usr/local/fsav/updatelog.txt
```

リスト 8-2 は表示の一部です。

```
[Header]
Timestamp=1067706390
Engines=avp,f-prot,general,orion
Packetformat=1
Product_version=Compatible with FSAV 4.03 or later
Title=FSAV Virus Signature Database Update
Message=Database Update Package

[FSAV_Database_Version]
Version=2003-11-01_02

----- (途中省略) -----

[f-prot]
Files=fsmacro.def,sign.def,fssign2.def
Dates=2003-11-01,2003-11-01,2003-11-01
Message=F-PROT scanner database files

[avp]
Files=avp.klb,avp.set,avp.vnd,avp0310.avc,backdoor.avc,ca.avc,daily.
avc,eicar.av
c,extra-cab.avc,extract.avc,fsav.set,kernel.avc,krndos.avc,krnengn.avc,
krnexe.avc

----- (以下省略) -----
```

リスト 8-2

2) モジュール更新ログの確認

最新のモジュールの更新ログは、以下のコマンドで確認できます。

(最新の更新ログ 2 件を表示する場合)

```
#head -n 2 /usr/local/gwav/.PAVver
```

リスト 8-3 は表示例です。

```
Proserver with AntiVirus version 2.0.9 20021015  
Proserver with AntiVirus version 2.0.9 20020905
```

リスト 8-3

9 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。

注意

この章のコマンド操作は、GUI 管理画面とは別に、管理者がシステムにログインして行います。クライアント PC から telnet でリモートログインする方法などがあります。

Windows クライアントで DOS プロンプトを起動して以下を実行します。

次ページの「■ウイルス検出機能の動作確認テスト」のコマンドを実行する前に、以下のコマンドを実行してください。

例

以下のイタリック部分を入力してください。

```
> telnet <サーバ名または IP アドレス>
login: admin
Password: <ユーザ「admin」のパスワード>
[admin@サーバ名]$          ログインすると、プロンプトが表示
                           されます。
[admin@サーバ名]$ su -    「su (スペース) -」と入力すると、
                           root ユーザに切り替わります。
Password: <「root」ユーザのパスワード>
[root@サーバ名]$          root 権限でログインすると、
                           「#」プロンプトが表示されます。
```

■ 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。

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メールアカウント、「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を指定します。

例えば、本製品を導入したメールサーバに、「mori」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 mori
```

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（「mori」）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、sendmail パッケージに含まれる `sendmail.cf` を変更すると、本製品が正常に動作しない可能性があります。

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ル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となります。

■ 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。以下のメールログを参照してください。

(ただし、ディストリビューションによってメールログファイルのある場所が異なる場合があります。)

```
#tail -f /var/log/maillog
```

メッセージ表示を終了するには、Ctrl キー+c キーを押します。

■ 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。

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、「5 ウイルス検出方針についての基本設定」を参照してください。

さらに、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
```

サポート窓口へのお問い合わせの際、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。

■ 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、当該バージョンでのバグ情報や最新の更新情報などを確認してください。

「アンチウイルス」の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/antivirus/update.html>

10 運用・管理

日常の運用・管理を行うための留意点について説明します。

■ メールによるウイルス情報の通知

本製品を導入すると、月次処理の実行時 (crontab で設定された日時) に管理レポートが送信されます。この管理レポートは、ウイルスが検出された場合に報告する宛先へ送信されます。

リスト 10-1 は、月次管理レポートのメールヘッダの表示例です。

```
From: MAILER-DAEMON@redhat7.gideon.co.jp
日時: 2001/10/05 11:56:33
サブジェクト: [AntiVirus for Linux] monthly report
              (2001/09/05 - 2001/10/04)
To: postmaster@redhat7.gideon.co.jp
```

リスト 10-1

リスト 10-2 は、月次管理レポートのメール本文の表示例です。

```
2003/10/01 から 2003/10/31 までの統計情報
送受信メール数: 3209
ウイルス添付メール: 137 <-----ウイルス感染検出のメール総数
EICAR-Test-File [AVP]: 26 <-----AVP が発見したテストウイルス (eicar)
EICAR_Test_File [F-Prot]: 26 <-----F-PROT が発見したテストウイルス (eicar)
I-Worm.Klez.h [AVP]: 7 <-----AVP が発見した Klez の命名
                          (下の F-PROT とは命名が異なる)
I-Worm.Sobig.c [AVP]: 96
Macro.Excel.Laroux.a [AVP]: 8
W32/Klez.H@mm [F-Prot]: 7 <-----F-PROT が発見した Klez の命名
W32/Sobig.C@mm [F-Prot]: 96
XM/Laroux.A [F-Prot]: 8
```

リスト 10-2

管理レポートでは、メール送受信の総件数、その内ウイルスを検出したメールの数、および検出したウイルスの種類などが報告されます。

■ 更新ログの確認

定期的に、更新ログ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。

更新ログの確認については、「8 定義ファイルおよびモジュールの更新」の「■更新ログの確認」を参照してください。

■ 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。

11 ファイルチェック機能

本製品では、ウイルスに感染したファイルをチェックする機能があります。指定したディレクトリのファイルに対して、定期的にウイルスチェックを行い、その結果をメールで報告します。

注意

この章のコマンド操作は、GUI 管理画面とは別に、管理者がシステムにログインして行います。クライアント PC から telnet でリモートログインする方法などがあります。

Windows クライアントで DOS プロンプトを起動して以下を実行します。

例

以下のイタリック部分を入力してください。

```
> telnet <サーバ名または IP アドレス>
```

```
login: admin
```

```
Password: <ユーザ「admin」のパスワード>
```

```
[admin@サーバ名]$          ログインすると、プロンプトが表示  
                           されます。
```

```
[admin@サーバ名]$ su -    「su (スペース) -」と入力すると、  
                           root ユーザに切り替わります。
```

```
Password: <「root」ユーザのパスワード>
```

```
[root@サーバ名]#          root 権限でログインすると、  
                           「#」プロンプトが表示されます。
```

■ 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、`/home/samba` および`/home/hoge` ディレクトリをチェックする場合、`root` 権限で以下のコマンドを実行します。

```
# echo "/home/samba" > /etc/GwAV/checkdir
# echo "/home/hoge" >> /etc/GwAV/checkdir
# /usr/local/gwav/gwav-file-control --daily
```

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。

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。

■ 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
```

■ 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` 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 11-1 は、`/etc/GwAV/checkdir` に `/home/share` が記述されている場合の、ウイルスチェックの実行結果を報告するメールです。

```
From: VirusReportFromIntra@gideon.co.jp
Subject: [AntiVirus for Linux] directory report(2003-11-14 11:28:48)
```

※圧縮ファイル形式はチェックしてません。

```
START: 2003-11-14 11:28:48
END: 2003-11-14 11:29:50
```

```
Directory list:
/var/spool/* EUC-JP
```

```
Result message:
/var/spool/cron
/var/spool/fax
/var/spool/lintian
/var/spool/lpd
/var/spool/mail
/var/spool/mqueue
/var/spool/pop
/var/spool/popbull
/var/spool/squid
```

ウイルスに感染しているファイルはありません。

```
-----
F-Secure Anti-Virus for Linux version 4.50 build 2111
Copyright (c) 1999-2003 F-Secure Corporation. All Rights Reserved.
```

```
3635 files scanned
-----
```

リスト 11-1

■ 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、毎日、定期的にチェックする場合、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
Cycle (None/Daily/Weekly/Monthly) [none] :d
CheckArchive (Yes/No/Recommend) [Recommend] :r
```

周期 (Cycle) 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

圧縮・書庫ファイルチェック (CheckArchive) 設定：

Yes	圧縮・書庫ファイルをチェックする
No	圧縮・書庫ファイルをチェックしない
Reccomend	推奨する方法に従う

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
```

リスト 11-2 は、このコマンド実行結果を表示した例です。

```
Cycle : daily
Archive-file : recommend (no check)
Directory-list:
/home/share
```

リスト 11-2

■ samba によるファイル共有に関する情報取得方法

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 11-3 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 11-3

■ 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
```

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（*）（**）（***）

* 回数：3 インシデントまで

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。

*** 導入・運用の請負は別契約となります。

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。ただし、製品 CD から再インストールした場合など、旧バージョンから更新を行うと、バージョンによっては正常に動作しない可能性があります。その場合は、「ユーザサポート窓口」までお問い合わせください。
- c. 更新は、1 年ごとの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/>

■ 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: AVL34567、A VR23456)
(製品シリアル No. 例: GR-12345、GC-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下さい。

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`）
- 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。

■ ユーザサポート窓口

株式会社ギデオン アンチウイルスサポート係

E-Mail： sp@gideon.co.jp

- * 電子メールをご利用になれない場合は直接お電話ください。
受付電話番号：045-590-3655
- * サポート窓口営業時間
9:00～17:00 ※土・日・祝祭日・年末年始を除きます。

■コメントシート

本ユーザーズガイドについてのご意見、あるいは誤記などを発見された場合は、下の欄にご記入の上 Fax いただければ幸いです。

宛先：株式会社ギデオン Fax 045-590-1217

該当箇所	コメント

アンチウイルス for Linux
Turbolinux AS 対応
ユーザーズガイド

2004 年 5 月 15 日 初版発行
2005 年 5 月 1 日 第 3 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 3448-4

本誌からの無断転載を禁じます。
乱丁、落丁はお取替え致します。上記発行所までご連絡下さい。

Copyright© 2004 GIDEON Inc
Printed in Japan