

アンチウイルス for Linux RedHat 対応
Sendmail 版/Qmail 版/Postfix 版

アンチウイルス for Sun Cobalt™
Sun Cobalt RaQ™ /Sun LX™ 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製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。

RedHat は RedHat, Inc. の登録商標です。

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.

Sun Cobalt RaQ/XTR および Sun LX はサン・マイクロシステムズ社の登録商標です。

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
前提条件	iii
テスト用ウイルスファイルについて	iii
著作権など	iii
表記など	iv
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
2 利用環境	4
2-1 使用条件（2005年5月現在）	4
2-2 インストール対象マシン環境	5
2-3 インストール後のシステム環境	6
2-4 メールサーバのバージョンアップによる更新の注意	7
2-5 インターネット接続による更新の注意	7
3 ご利用上の注意	8
4 インストール	9
4-1 CD-ROM ドライブ付マシンへのインストール	9
4-2 CD-ROM ドライブがないマシンへのインストール	12
5 バージョンアップデート	16
6 基本設定手順	18
7 ユーザ情報の設定	23
8 詳細情報設定	25
8-1 設定項目とパラメータの説明	25
8-2 スキャンコード一覧	32

9	メールリレーホストの設定 (Sendmail 版のみ)	33
9-1	設定ファイルの記述.....	33
9-2	マップファイルの記述	33
10	アンインストール.....	36
11	定義ファイルおよびモジュールの更新	38
11-1	現モジュールのバージョン及び HTTP 更新可否確認	38
11-2	自動更新ファイルと起動スクリプト	44
11-3	自動更新スケジュール	44
11-4	更新ログの確認.....	45
12	動作確認	46
12-1	ウイルス検出機能の動作確認テスト	46
12-2	メールログでの確認.....	47
12-3	トラブルシューティング.....	48
12-4	動作しない場合.....	49
13	運用・管理.....	50
13-1	メールによる各種情報の通知.....	50
13-2	更新ログの確認.....	53
13-3	システム運用上の確認	53
14	ファイルチェック機能.....	54
14-1	概要	54
14-2	ディレクトリリストの記述	54
14-3	実行結果の報告.....	56
14-4	ファイルチェックの設定方法.....	57
14-5	samba によるファイル共有に関する情報取得方法	58
14-6	コマンドの使い方について	58
付録	サポートサービス.....	59

サービス内容	59
製品のサポート情報.....	60
サポート依頼フォーム	60
ユーザサポート窓口.....	61

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。

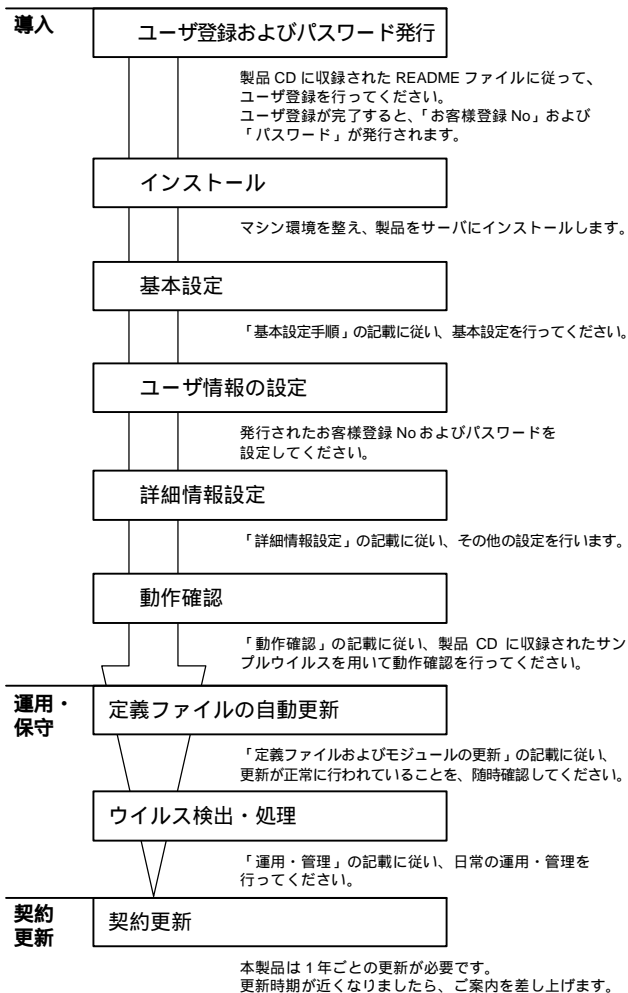
ウイルス感染経路の90%近くが電子メールによるものと言われています。

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

すでに稼働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浸入を防ぐには、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。

2 利用環境

『アンチウイルス for Linux/Sun Cobalt』は、RedHat 系 Linux および Sun Cobalt/Sun LX に対応したメールサーバのウイルス検出・駆除ソフトです。

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/products/>

2-1 使用条件（2005 年 5 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**
(glibc 2.1.2 およびそれ以前では動作しません。Redhat 6.1、Turbolinux Server 6.0 などでは glibc のアップデートが必要です)
- メールサーバ
 - 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）
 - qmail 1.03
 - postfix 0.0.20000529 以降
- 対応 Linux ディストリビューション
 - RedHat 6.2/7.0.x/7.1/7.2/7.3/8.0/9.0 AdvancedServer2.1
 - Red Hat Enterprise Linux AS/ES/WS(Version 2.1)
 - Red Hat Enterprise Linux AS/ES/WS(Version 3)
 - Fedora Core 1,2
 - LASER5 Linux 6.2/6.4/6.5/6.9/7.2
 - Turbolinux 6.1/6.5/7/8 Turbolinux7/8/10 Server
 - Turbolinux Enterprise Server 8
 - Vine Linux 2.1/2.1.5/2.5/2.6
 - Miracle Linux 2.0/2.1

OpenLinux eServer 2.3 Server 3.1.1

など、主要な RedHat 互換 OS (インテルアーキテクチャ)。

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

- Sun Cobalt RaQ3 / RaQ4/RaQXTR/RaQ550 / Sun LX50
- 物理メモリ空き容量 64MB 以上 スワップ (swap) 容量 64MB 以上
- 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
- ハードディスク空領域 100MB 程度 (インストール直後は 100MB 必要ありませんが、定義ファイルやログなど、運用上将来的な使用率増加を見積もってください)

2-2 インストール対象マシン環境

- RedHat 系 Linux または Sun Cobalt で、メールサーバが正常に稼働していること

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。メモリ使用量は約 64MB です。

2-3 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せん。

Sendmail 版の場合

既存の `sendmail.cf` が、「アンチウイルス」対応用に変更されません。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。

Qmail 版の場合

`/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.gwav
```

Postfix 版の場合

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.gwav
```

```
/etc/postfix/main.cf.org.gwav
```

2-4 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。

2-5 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 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、逐次バージョンを確認いただき、最新のバージョンになっているかご確認ください。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は後述します。更新は手動で行うこともできます。

- 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、すぐにサポートデスク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、正しくメールが配送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引っかかって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。システム管理者様にご相談ください。
- メール 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。

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。

4 インストール

ここでは、本製品のインストール方法について説明します。

CD-ROM ドライブの有無により、インストールの手順が異なります。

注意

インストール前の確認

メールサーバが正しく稼働しており、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。

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。

4-1 CD-ROM ドライブ付マシンへのインストール

CD-ROM ドライブが付いているマシンへのインストール手順について説明します。

《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。画面 4-1 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 -
```

画面 4-1

《手順 3》 製品 CD をマウント（読み可能に）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、画面 4-2 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
```

画面 4-2

《手順 4》 アプリケーションをインストールする

- Sendmail 版の場合、画面 4-3 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:~#rpm -ihv /mnt/cdrom/gwantivirus.i386.rpm
```

画面 4-3

- Qmail 版の場合、画面 4-4 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。

```
#/mnt/cdrom/gwav-qmail-installer install
```

画面 4-4

(注) /usr/local/gwav ディレクトリの権限が、正しく設定されていない事があります。このディレクトリの権限が “0755” に設定されていることを以下で確認してください。

```
ls -ld /usr/local/gwav
```

権限が “0755” 以外である場合には、次のコマンドで設定変更してください。

```
chmod 0755 /usr/local/gwav
```

- Postfix 版の場合、画面 4-5 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。

```
#rpm -ihv /mnt/cdrom/gwantivirus-postfix.i386.rpm
```

画面 4-5

コンソールにメッセージが表示され、これでインストールは完了です。

《手順 5》 製品 CD をアンマウントし (CD から切離し) 取出す

CD の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、画面 4-6 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。

製品 CD をドライブから取り出してください。

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

画面 4-6

4-2 CD-ROM ドライブがないマシンへのインストール

Sun Cobalt RaQ3/RaQ4/RaQXTR/RaQ550、Sun LX50 など、CD-ROM ドライブが付いていないマシンへのインストール手順について説明します。

ここでは、Windows クライアントから RaQ にインストールする場合を例に、説明します。インストール先のサーバ名は「raq」とします。

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

《手順 1》 DOS プロンプトを表示する

Windows のスタートメニューをクリックして、[ファイル名を指定して実行] を選択します。「ファイル名を指定して実行」画面の「名前」に「command」と入力して、[OK] ボタンをクリックします。

または「アクセサリ」から「コマンドプロンプト」を開いてください。表示された画面に、CD が入っている「ドライブ名:」（例えば、E:）を入力します。

《手順 2》 製品 CD のインストール用ファイルを確認

CD の内容を参照し、以下のファイル名および 0 バイトでないことを確認します。

- Sendmail 版および Postfix 版の場合、`gwantivirus-xxxxxxx.i386.rpm`

（Postfix 版の場合具体的には
`gwantivirus-postfix-xxxxxxx.rpm`

に置き換えてください）

xxxxxxx には、`gwantivirus-2.1-4.i386.rpm` のように半角英数字が入っています。

- Qmail 版の場合、gwav-qmail-installer、gwav-qmail.tgz の 2 ファイル

《手順 3》 ファイルを raq に転送

画面 4-7 のようにイタリックの部分を入力して、《手順 2》で確認したファイルを ftp で raq に転送します。

```
E:¥>ftp raq
```

画面 4-7

続いて、「ユーザアカウント」および「パスワード」を入力後、

- Sendmail 版および Postfix 版の場合、画面 4-8 のようにイタリックの部分を入力します。

```
ftp>binary
200 Type set to I.
ftp>cd /tmp
ftp>put gwantivirus-xxxxxxxx.rpm
ftp>ls
ftp>quit
```

画面 4-8

- Qmail 版の場合、以下のようにイタリックの部分を入力します。

```
ftp>put gwav-qmail-installer
ftp>put gwav-qmail.tgz
```

《手順 4》 telnet でログインしてインストール

画面 4-9 のようにイタリックの部分を入力します。

```
E:¥>telnet raq
```

画面 4-9

raq に telnet でログインしてインストールします。

続いて、「ユーザアカウント」および「パスワード」を入力後、

- Sendmail 版および Postfix 版の場合、画面 4-10 のようにイタリックの部分を入力します。

```
$su
Password:*****
#cd /tmp
#rpm -ihv gwantivirus-xxxxxxx.rpm
```

画面 4-10

- Qmail 版の場合、同じディレクトリに gwav-qmail.tgz ファイルがあることを確認の上、以下のようにイタリックの部分を入力します。

```
# cd /tmp
# ./gwav-qmail-installer install
```

《手順 5》 パッケージファイルを削除

- Sendmail 版および Postfix 版の場合、画面 4-11 のようにイタリックの部分を入力して、rpm パッケージファイルを削除します。

```
#cd /tmp
#rm -f gwantivirus-xxxxxxx.rpm
```

画面 4-11

- Qmail 版の場合、以下のようにイタリックの部分を入力します。

```
#cd /tmp
#rm -f gwav-qmail-installer
(/tmp ディレクトリ以下で作業した場合、gwav-qmail.tgz
ファイルはインストールスクリプトにより削除されます)
```

5 バージョンアップデート

ここでは、本製品のプログラムのバージョンアップデート方法について説明します。

プログラムファイル (rpm) をサーバに置くまでの手順は、前章を参照してください。

注意

バージョンアップデートは 2.1-4 から対応しました。例えば、2.0-x のシステムを 2.1-4 より古い 2.1-x へアップデートする場合には本章の記載は適用されません。また **qmail 対応版** については rpm 形式を採用していないため適用されません。

Sendmail, postfix 対応版をお使いで、2.1-1 以前のシステムを 2.1-4 にアップデートする場合に、本章をご参照ください。

すでに「アンチウイルス for Linux」の旧バージョンがインストールされたシステムに、2.1-4 またはそれ以降のバージョンの rpm ファイルを置き(本マニュアル出稿時点 06/01/2005 の最新バージョンは 2.1-4 です)、root またはスーパーユーザ (su-) でログインしてください。

《手順》

- Sendmail 版および Postfix 版の場合、画面 5-1 のようにイタリックの部分を入力します。rpm ファイルを/tmp 以下に置いた場合は以下になります。

```
#cd /tmp
#rpm -Uhv gwantivirus-xxxxxxx.rpm
```

画面 5-1

注意

バージョンアップデートは、定義ファイル更新と同じように自動更新（後述）でも行われます。``rpm -q gwantivirus`` コマンドで現在インストールされている rpm のバージョンが表示されますが、“2.1-0”というバージョンが表示される場合であっても、``/usr/local/gwav/gwav-checker`` コマンドで “GWAV version: Engine 2.1-4” と表示されていれば最新のプログラムにすでにアップデートされていますので、本章の操作は必要ありません。

6 基本設定手順

インストールが完了したら、基本設定を行います。

《手順 1》 root 権限で設定プログラムを実行する

root 権限でログインします。

画面 6-1 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:~# /usr/local/gwav/gwav_conf
```

画面 6-1

《手順 2》 基本設定を行う

画面 6-1 のコマンドを実行すると、コンソールに、画面 6-2 のような基本設定情報が表示されます。

ここで、y キーまたは Enter キーを押すと、表示された情報が保存されます。

n キーを押すと、基本設定情報を個別に設定できます。

```
Current setting:
VIRUS_CHECK=YES
OUTGOING_CHECK=YES
SUBJECT_METHOD=*** Virus warning ***
INFECTION_FILE_ACTION=H
WARN_SENDER=YES
VIRUS_REPORT_TO=postmaster

OK?(Y/n)
```

画面 6-2

(1) メールのウイルスチェック

画面 6-3 で、y キーまたは Enter キーを押すと、受信メールのウイルスチェックをします。

n キーを押すと、ウイルス検出機能が停止します。

```
Do virus check?(Y/n)_
```

画面 6-3

注意

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。

(2) 送付 (Outgoing : 本サーバから外部へ出て行く) メール

のウイルスチェック

画面 6-4 で、y キーまたは Enter キーを押すと、送付メールのウイルスチェックをします。

n キーを押すと、送付メールのウイルスチェックをしません。

ただし、Qmail 版および Postfix 版では、「n (送付メールのウイルスチェックをしない)」を設定できません。

```
Also check outgoing mails?(y/N)_
```

画面 6-4

(3) ウイルスを検出した受信者メールのサブジェクト表示方法

以下の 3 通りの表示方法が選択できます。

- 1) 警告メッセージ「*** Virus Warning ***」と表示
- 2) オリジナルのサブジェクトのまま表示
- 3) オリジナルのサブジェクトに警告メッセージを付加して表示

画面 6-5 で、「1」「2」「3」の中から 1 つを選択して入力し、

Enter キーを押します。

```
Select one from the following 3 subject
methods:
  1) *** Virus warning ***
  2) ORIGINAL_SUBJECT
  3) Virus warning:ORIGINAL_SUBJECT
which one?(1/2/3)_
```

画面 6-5

例

オリジナルのサブジェクトが「第 10 回定期講演会開催のお知らせ」である場合、受信者メールのサブジェクトは、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

(4) 検出されたウイルスの処理方法

ウイルスが検出された場合、受信者へ警告メールを送信します。警告メールの形式で、以下の 4 つの処理方法が選択できます。

- A: ウイルス感染ファイルを別添付形式で送信します。
- D: 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。ただし、完全に削除できない場合がありますので、以下の「H」または「W」の選択を推奨します。
- H: ウイルスメールそのものを削除し、ヘッダ情報を別添付形式にして送信します。
- W: 警告メッセージのみ送信します。

画面 6-6 で、「A」「D」「H」「W」の中から 1 つを選択して入力し、Enter キーを押します。

```
Select one from the following 4 handling:
  A) Attach virus files
  D) Delete them (make virus files be 0 byte)
  H) Delete virus-mail & attach mail-header
  W) Warning message only
which one?(A/D/H/W)
```

画面 6-6

(5) ウイルスが検出された場合の送信者への警告

画面 6-7 で、y キーまたは Enter キーを押すと、ウイルス検出時に、送信者へ警告メールを送信します。

n キーを押すと、ウイルス検出時に、送信者へ警告メールを送信しません。

```
Send warning message to sender?(y/N)
```

画面 6-7

(6) ウイルスが検出された場合に報告する宛先（管理者）メールアドレス

ウイルスを検出した場合の通知先に、管理者のメールアドレスを指定します。

例

「postmaster」「tanaka」の 2 人に通知する場合、画面 6-8 のようにイタリックの部分を入力します。複数の人へ報告する場合は、「ユーザ名」や「メールアドレス」を、半角スペースで区切って入力します。

導入されたサーバ以外のユーザに送信する場合は、正式なメールアドレスを指定する必要があります。

```
Report virus info. to [postmaster]:postmaster tanaka
```

画面 6-8

最初の確認画面に戻ります。

これで基本設定は完了です。

7 ユーザ情報の設定

基本設定が完了したら、ユーザ情報の設定を行います。

ユーザ情報とは、製品購入時、ユーザ登録をしたときに発行された「お客様登録 No.」と「パスワード」のことです。

注意

ユーザ情報を必ず設定してください。
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が自動更新されません。
定義ファイルおよびモジュールの更新については、「11 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。

ここでは、お客様登録 No.が「AVR12345」、パスワードが「password」の場合を例に、説明します。

- (1) root 権限でログインします。
画面 7-1 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。

```
# /usr/local/gwav/regist
```

画面 7-1

- (2) 画面 7-2 のように、イタリックの部分に「お客様登録 No.」と「パスワード」を入力します。

「お客様登録 No.」と「パスワード」は、サポートサービス証書に記載されています。

- お客様登録 No. :
AVR12345 の部分に、お客様登録 No.を入力して Enter キーを押します。
確認のため、再度入力して Enter キーを押します。

- パスワード：
password の部分に、お客様のパスワードを入力して、Enter キーを押します。
確認のため、再度入力して Enter キーを押します。

```
User-number: AVR12345
Retype user-number: AVR12345
Password: password
Retype password: password
-----
User-number: AVR12345
Password: password
-----
```

画面 7-2

- (3) (2)で入力した「お客様登録 No.」と「パスワード」が、ユーザ情報として設定されます。

ユーザ情報は、画面 7-2 の破線の下に表示されますので、正しく設定されているかを確認してください。

誤って入力した場合は、再度(1)、(2)の操作を行ってください。

8 詳細情報設定

「アンチウイルス」の詳細情報は、リスト 8-1 のように設定ファイルに記載されています。設定ファイルは、`/etc/GwAV/GWAV.conf` です。

システム管理者が、詳細情報を確認するための参考にしてください。

注意

追加機能などの最新情報については、以下の URL を参照してください。

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

```
#####
## Config file for GIDEON WHITEBOX Anti-Virus system ##
##      copyright(C) 1999,2000 GIDEON Corp.  ##
##      http://www.gideon.co.jp/  ##

#####
### Site options
*1 VIRUS_CHECK=YES
*2 OUTGOING_CHECK=YES
*3 SUBJECT_METHOD=*** Virus warning ***
*4 INFECTION_FILE_ACTION=H
*5 WARN_SENDER=NO
*6 VIRUS_REPORT_TO=postmaster
*7 VARTmp_DIR=/var/tmp
*8 MAIL_LOG=/var/log/maillog
```

リスト 8-1

8-1 設定項目とパラメータの説明

設定可能な項目（「=」の左側の値）とそのパラメータ（「=」の右側の値）について説明します。

注) 「=」の前後にスペースなどの文字は入れないでください。

*1: VIRUS_CHECK=YES

設定項目： ウイルスチェックをするかどうかの設定

パラメータ： YES / NO

初期値： YES

*2: `OUTGOING_CHECK=YES`

設定項目： 送出メールもチェックするかどうかの設定

パラメータ：`YES / NO`

初期値：`YES`

前述の通り、Qmail 版、Postfix 版は「`YES`」のみ有効。

*3: `SUBJECT_METHOD=*** Virus warning ***`

設定項目： ウイルスを検出した受信者メールの、サブジェクト表示方法の設定

パラメータ：以下の3通りの表示方法

- (1) `*** Virus warning ***`
- (2) `Virus warning: ORIGINAL_SUBJECT`
- (3) `ORIGINAL_SUBJECT`

例

オリジナルのサブジェクトが「第10回定期講演会のお知らせ」である場合、受信者メールのサブジェクトは、それぞれ以下のように表示されます。

- `*** Virus warning ***`
- `Virus warning: 第10回定期講演会のお知らせ`
- `第10回定期講演会のお知らせ`

初期値：`*** Virus warning ***`

注意

例えば、「`*** Virus warning ***`」の文字列は「`**** VIRUS REPORT ****`」のように英数半角文字での表記または `ISO-2022-JP` のエンコード文字列(1行のみ)でも表記できます。

(2)の仕様の場合、`ORIGINAL_SUBJECT` の前に半角スペースが必要です。

- 送信者への警告メールのサブジェクトの表示方法は、以下の設定項目で設定できます。

SUBJECT_METHOD_SENDER=

パラメータは「ウイルスを検出した受信者メールの、サブジェクト表示方法の設定」と同様

- 管理者への警告メールのサブジェクトの表示方法は、以下の設定項目で設定できます。

SUBJECT_METHOD_VIRUS_REPORT_TO=

パラメータは「ウイルスを検出した受信者メールの、サブジェクト表示方法の設定」と同様

***4: INFECTION_FILE_ACTION=H**

設定項目： ウイルス検出ファイルをそのまま添付するか削除するかの設定

パラメータ： **A** (添付) / **D** (削除) / **W** (警告メールのみ) / **H** (警告メールにヘッダ情報を添付)

初期値： **H**

***5: WARN_SENDER=NO**

設定項目： ウイルスが検出された場合、送信者に警告メールを送信するかどうかの設定

パラメータ： **YES** / **NO**

初期値： **NO**

***6: VIRUS_REPORT_TO=postmaster**

設定項目： ウイルスが検出された場合に報告する、宛先メールアドレスを指定

パラメータ： メールアドレスまたは指定なし

指定なし (空欄) にすると、報告メールが配信されません。

複数の人に報告する場合は、半角スペースで区切る

例) `postmaster tanaka yoshida@nihon.virus.co.jp`

初期値： `postmaster`

*7: `VARTmp_DIR=/var/tmp`

設定項目： GWAV がウイルススキャンをするときに使うディスク領域

パラメータ：ディレクトリ名

初期値： `/var/tmp`

*8: `MAIL_LOG=/var/log/maillog`

設定項目： システムの mail に関するログファイル
(`/etc/syslog.conf` に定義されている)

パラメータ：ログファイル名

初期値： `/var/log/maillog`

- ウイルスが検出された場合、受信者に警告メールを送信するかどうかの設定できます。

`WARN_RECEIVER=NO`

初期値： デフォルトでは `GWAV.conf` には存在しません。行がない場合は `YES` と同義です。

メールログに記載されるウイルススキャンのメッセージフォーマットについて：

ログフォーマット

日付時刻ホスト名 `gwav[PID]:SCANNED:Scan_code:<Message-ID>`

ウイルスが検出されたら、さらに以下の情報を記録

日付時刻ホスト名 `gwav[PID]:VIRUS FOUND --`
FROM: 送信者 TO: 受信者

日付時刻ホスト名 `gwav[PID]:VIRUS type --`
ファイル名 infection: TYPE

- 例) ウイルスが検出された場合、リスト 8-2 のように表示されます。
 行末の「¥」は行が継続していることを示しています。
 実際のログファイルは 1 行で記述され、「¥」は表示されません。

```
Dec 21 11:27:25 intra gwav[27966]: ¥
      SCANNED:3:<200012210227.eBL2RGB27941@mail.gideon.co.jp>
Dec 21 11:27:25 intra gwav[27966]: ¥
      VIRUS FOUND -- FROM: owner-info@gideon.co.jp TO:yamada
Dec 21 11:27:25 intra gwav[27966]: ¥
      VIRUS type -- KDEDPCCK.EXE infection: W95/Hybris.worm
```

リスト 8-2

- 例) ウイルスが検出されなかった場合、リスト 8-3 のように表示されます。

```
Jan 5 09:56:38 intra gwav[16156]: ¥
      SCANNED:0:<200101050056.f050uaK16147@mail.gideon.co.jp>
```

リスト 8-3

- 注) 行末の「¥」は行が継続していることを示しています。
 実際のログファイルは 1 行で記述され、「¥」は表示されません。

スキャンコードについては後述します。

Sendmail 版の場合は、リスト 8-4 の 2 項目の設定が有効です。

```
*1 SMTPFEED=/usr/sbin/smtpfeed
*2 LOCALmailer=/usr/sbin/mail.local
```

リスト 8-4

***1: SMTPFEED=/usr/sbin/smtpfeed**

設定項目： ほかのメールサーバにメールを送るとき（relay ではない）に使用する `smtpfeed` のパスの指定

パラメータ：実行ファイル名とオプション
システムに存在しなければ、
`/usr/local/gwaw/smtpfeed` を使用する

初期値： `/usr/sbin/smtpfeed`

メールリレーの指定については、「9 メールリレーホストの設定（Sendmail 版のみ）」を参照してください。

***2: LOCALmailer=/usr/sbin/mail.local**

設定項目： ローカルメールプールに、メールを配信するときに使う配信エージェントのパスの指定

パラメータ：ファイル名+ [オプション指定]
インストール時に、ローカルメール配信エージェントを自動選択して設定します。例えば、`procmail` が `/usr/bin` に存在する場合、以下のように設定されます。
`LOCALmailer=/usr/bin/procmail -f $from -d $to`
システムにローカルメール配信エージェントが存在しない場合（`/usr/bin` または `/usr/sbin` に存在しない場合）
`/usr/local/gwaw/mail.local` を使用します。

初期値： `/usr/sbin/mail.local`

Qmail 版の場合は、リスト 8-5 の 3 項目の設定が有効です。

```
*1  MODE=qmail
*2  MAILER=/var/qmail/bin/qmail-inject
*3  REPLACED_COMMAND=/var/qmail/bin/qmail-queue.org.gwaw
```

リスト 8-5

- ```

*1: MODE=qmail
 設定項目： メールサーバの動作モード指定
 パラメータ： qmail
 初期値： qmail

*2: MAILER=/var/qmail/bin/qmail-inject
 設定項目： 警告メールを送信する際に使用するコマンドを指定
 パラメータ： ファイル名
 初期値： /var/qmail/bin/qmail-inject

*3: REPLACED_COMMAND=/var/qmail/bin/qmail-queue.org.gwav
 設定項目： インストール時の qmail-queue の変更後のファイル名
 パラメータ： ファイル名
 初期値： /var/qmail/bin/qmail-queue.org.gwav

```

Postfix 版の場合は、リスト 8-6 の 2 項目の設定が有効です。

- |                                                                        |
|------------------------------------------------------------------------|
| <pre> *1  MODE=postfix-pipe *2  MAILER=/usr/sbin/sendmail -i -t </pre> |
|------------------------------------------------------------------------|

リスト 8-6

- ```

*1: MODE=postfix-pipe
    設定項目： メールサーバの動作モード指定
    パラメータ： postfix-pipe
    初期値：    postfix-pipe

*2: MAILER=/usr/sbin/sendmail -i -t
    設定項目： 警告メールを送信する際に使用するコマンドを指定
    パラメータ： ファイル名
    初期値：    /usr/sbin/sendmail -i -t

```

8-2 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	対応
0	スキャンしたがウイルスに感染されていないかった	対応無用です
3	スキャンしたところ、定義ファイルにマッチしており、ウイルスに感染していた	/etc/GwAV/GWAV.conf 設定ファイルの “INFECTION_FILE_ACTION=” 行でウイルスが削除される設定 (“A”以外)になっていれば、メール受信者にはウイルスは届きません。
8	ウイルスである疑いがある	
9	ウイルスチェックできないファイル (暗号化されたファイルなど)	対応無用です
-2,-1,1,2,141 その他	システムエラーが発生している可能性あり。ウイルススキャンおよびメールの配信が正常に行われていない可能性がある	様々なケースが考えられます。 ギデオン サポートセンターにお問い合わせください。

リスト 8-7

上記スキャンコードは、受信者宛の元メールに“**Virus Check ERROR (X)**”という記述が付されます。0,9の場合は、元のメールをそのまま配信します。

9 メールリレーホストの設定 (Sendmail 版のみ)

本製品を導入したサーバから、外部メールサーバにリレーするときは、以下のように指定します。この章の設定は Sendmail 版のみ有効です。

9-1 設定ファイル (/etc/GwAV/GWAV.conf) の記述

この設定ファイルに、以下のように 1 行を追加します。

- /usr/sbin/smtpfeed が存在する場合、以下の記述を追加
SMTPFEED=/usr/sbin/smtpfeed -M /usr/local/gwav/SMTPFEEDmapfile

- /usr/sbin/smtpfeed が存在しない場合、以下の記述を追加
SMTPFEED=/usr/local/gwav/smtpfeed -M /usr/local/gwav/SMTPFEEDmapfile

9-2 マップファイル

(/usr/local/gwav/SMTPFEEDmapfile) の記述

マップファイルは、以下の書式に従って記述します。

ドメイン名 宛先ホスト 1:宛先ホスト 2:...

「宛先ホスト 1」「宛先ホスト 2」... それぞれの箇所には、ホスト名、[ホスト名]、A、MX などが指定できます。この記述により、左部「ドメイン名」で指定したメールアドレスへリレー配送する場合、右部「宛先ホスト 1」「宛先ホスト 2」... で記述した形式を参照して、その内容に従い配送ルールを決定します。

ホスト名	指定したホスト名に対する MX レコード (DNS を参照) を検索する
[ホスト名]	四角カッコでくくる。指定したホスト名に対する A レコード (DNS を参照) を検索する
[IP アドレス]	四角カッコでくくる。指定した 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、DNS の MX レコードを参照する

MX?	上記 MX と同じだが、DNS で指定された fallback MX レコードも参照する
A	メールアドレスのドメイン部に該当する、DNS の A レコード (ホスト名) を参照する
=domain	エイリアスを適用した後、MX を検索する

で始まる箇所は「コメント」とみなされ、設定上関係ありません。

マップファイル内のスペースで区切られた左側に記載する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指定できます。

次ページに記述例を示します。

例

- `. MX`

すべてのリレー配送について、特定のドメイン名や先ホストを指定しない場合に参照するメールサーバを経由しようとしません(デフォルト)。

- `sub.my.domain A:[backup.server]`

`sub.my.domain` ドメインをもつメールアドレスへリレーする場合に「`sub.my.domain`」のように完全に一致したならば「`username@sub.my.domain`」へのメールは、「`sub.my.domain`」というホスト("A"で指定)を最初に DNS で参照し配送を試みます。DNS で `sub.my.domain` が名前解決されずに失敗した場合は、次いで「`backup.server`」というホストへ配送しようとしします。

ここで例として示すドメイン名やホスト名はご使用の環境に応じて書き換えてください(以下の説明でも同様です)。

- `.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、「`.co.jp`」のサブドメイン名をもつメール例えば「`username@xxx.co.jp`」へのメールは、最初に「`quick.relay.server`」というホストに対する MX レコードを引き、そこで指定されたメールサーバへ配送を試みます。失敗した場合、次いで「`co.jp`」というサブドメインに一致する、DNS の MX レコードで指定されたメールサーバへ送ります。

- `.bitnet =.bitnet.ad.jp`

例えば、エイリアスで「`bitnet`」のサブドメイン名をもつメールで、「`username@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。

10 アンインストール

本製品のアンインストールは、以下の手順で行います。

まず、root 権限でログインします。

- Sendmail 版の場合、画面 10-1 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。

```
# rpm -e gwantivirus
```

画面 10-1

Sendmail 版では、「アンチウイルス for Linux」をアンインストールすると、あらかじめインストール時に保存したオリジナルの `sendmail.cf`（「アンチウイルス for Linux」インストール時に `sendmail.cf.org.gwav` として保存されます）からファイルを上書きして戻すため、「アンチウイルス for Linux」インストール後にユーザ自身で編集した内容が消去されます。

編集内容がまったく分からなくなる事を回避するため、「アンチウイルス for Linux」バージョン 2.1-4 からは、アンインストール時に「アンチウイルス for Linux」インストール後に編集した `sendmail.cf` の内容とオリジナルの `sendmail.cf.org.gwav` の内容との差分を抽出して別ファイル (`sendmail.cf.diff`) として保存するようにしました。アンインストール後、編集内容の確認は上記ファイルを参照してください。設定を改めて記述したいときは、diff ファイルを参照しつつ、必要な箇所を取り出して `vi` コマンドなどで `sendmail.cf` を編集してください。

- Postfix 版の場合、画面 10-2 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。

```
# rpm -e gwantivirus-postfix
```

画面 10-2

- Qmail 版の場合、第 4 章を参照してインストール CD-ROM をマウントしてください。CD-ROM 内の `gwav-qmail-install` コマンドをサーバ上の任意のディレクトリ(下記例では `/tmp`)に置き、画面 10-3 のように実行してください。

```
# cd /tmp  
#/gwav-qmail-installer uninstall
```

画面 10-3

注意

アンインストールは、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。

11 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。

11-1 現モジュールバージョン及び HTTP 更新可否確認

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 11-1 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、「12 動作確認」の「12-3 トラブルシューティング」を参照してください。

```

< VERSION >
*1  GWAV version:
*2  -r-sr-xr-x 1 root root 127236 Apr 7 11:10 /usr/local/gwav/gwav
*3  Engine: 2.1.4 2005-04-06
*4  Patch: Proserver with AntiVirus version 2.1.1 20040506
*5  RPM: gwantivirus-2.1-0
*6  FSAV version:
*7  FSAV database version: 2005-04-04_02
*8  F-Secure Anti-Virus for Linux Servers version 4.61 build 3215
   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: 2005-04-04_02

Scanner Engine versions:
*9  F-Secure Corporation Libra engine version 2.1 build 11
*10 F-Secure Corporation Libra database version 2005-04-03

*11 F-Secure Corporation Orion engine version 1.2 build 33
*12 F-Secure Corporation Orion database version 2005-03-29

*13 Kaspersky Labs. AVP FPI Engine engine version 4.0 build 164
*14 Kaspersky Labs. AVP FPI Engine database version 2005-04-04

*15 libfm.so: /usr/local/fsav/4.61/lib/libfm.so: symbolic link to
   libfm.1.4.3050.so
*16 Daemon: Daemon process 28959 exists.

< USER >
*17 user-number: AVLXXXXX

< HTTP >
*18 HTTP proxy server: 192.168.1.70:8080
*19 ==== avupdate.f-secure.com ====
*20 http connect [ OK ]
*21 user-number & password [ OK ]
*22 get file [ OK ]
*23 ==== ns3.gideon.co.jp ====
   http connect [ OK ]
   user-number & password [ OK ]
   get file [ OK ]
*24 ==== www.gideon.co.jp ====

```

リスト 11-1

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/updates/>

***2: -r-sr-xr-x 1 root root 120694 Oct 30 16:56 /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: 2.1.4 2005-04-06**

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-2.1-0**

RPM パッケージのバージョン表示
「アンチウイルス」をインストールした `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「2.1-0」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。
<http://www.gideon.co.jp/updates/>

***7: FSAV database version: 2005-04-04_02**

定義ファイルのバージョン表示。

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

ウイルス検出 fsav モジュールのバージョン表示 (表面上ウイルススキャンエンジンは fsav ですが、内部的には3つのエンジン Libra、Orion、AVP から構成されています)

***9: F-Secure Corporation Libra engine version 2.1 build 11**

ウイルス検出エンジン Libra のバージョン表示

***10: F-Secure Corporation Libra database version 2005-04-03**

ウイルス検出エンジン Libra の定義ファイル更新日の表示

***11: F-Secure Corporation Orion engine version 1.2 build 33**

ウイルス検出エンジン Orion のバージョン表示

***12: F-Secure Corporation Orion database version 2005-03-29**

ウイルス検出エンジン Orion の定義ファイル更新日の表示

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

ウイルス検出エンジン AVP のバージョン表示

***14: Kaspersky Labs. AVP FPI Engine database version 2005-04-04**

ウイルス検出エンジン AVP の定義ファイル更新日の表示

*15: **libfm.so: /usr/local/fsav/4.61/lib/libfm.so:
symbolic link to libfm.1.4.3050.so**

ウイルス検出エンジンに用いられるライブラリ libfm のファイル名
(バージョン) 表示

*16: **Daemon: Daemon process 28959 exists.**

fsavd デーモンが起動している場合、そのプロセス ID を表示します。「アンチウイルス for Linux」バージョン 2.1-4 以降ではデフォルトでデーモン起動を推奨しています。デーモン起動により、スキャン速度の向上、システム負荷の軽減が見込まれます。デーモンが常駐起動していなくても、ウイルススキャンは実行されます。

< USER > セクション

*17: **user-number: AVLXXXXX**

「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

*18: **HTTP proxy server: 192.168.1.70:8080**

サーバがプロキシを経由してインターネットに接続している場合、プロキシホストとポート番号を表示 (/usr/local/gwav/myhttpproxy ファイルに記述した設定)

*19: **==== avupdate.f-secure.com ====**

定義ファイルダウンロード先サーバ名

*20: **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による制御やデフォルトルートの設定で http の外部への接続ができない可能性があります。

ファイアウォール等で接続先を指定する必要がある場合、定義ファイルダウンロード先サーバについては、IP アドレスではなくホスト名を指定してください(アップデートサイトのラウンドロビン機能により毎回異なる任意の IP アドレスに接続に行きます)。ポートは HTTP (80 番) を開けてください。

*21: `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。

*22: `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

*23: `==== ns3.gideon.co.jp ====`

モジュールダウンロード先サーバ名 (第 1 サイト)

*24: `==== www.gideon.co.jp ====`

モジュールダウンロード先サーバ名 (第 2 サイト)

ファイアウォール等で接続先を指定する必要がある場合、第 1・第 2 モジュールダウンロード先サーバについては、HTTP (80 番) ポートを開けてください。

11-2 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
```

11-3 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
```

したがってデフォルトは1日に1回定義ファイルのダウンロードを試みます。クーロンの設定を編集して、1時間に1回もしくは好みの時間に設定することも可能です。ただし、アップデートサーバ側での定義ファイルの更新は1日に2~3回(全くない日もあります)なので、最短でも3時間に1回程度のクーロン設定で十分です。

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を参照してください。

11-4 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/updatedlog.txt
```

リスト 11-2 は表示の一部です。

```
[Header]
Timestamp=1112623822
Engines=avp,f-prot,general,orion,libra
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=2005-04-04_02

----- (以下省略) -----
```

リスト 11-2

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 11-3 は表示例です。

```
Proserver with AntiVirus version 2.1.4 20050406
Proserver with AntiVirus version 2.1.4 20050323
```

リスト 11-3

12 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。

12-1 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。

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 版の場合は、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。

例えば、本製品を導入したメールサーバに、「sato」というメールアドレスが存在する場合、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
```

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。

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ドレスで、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。

12-2 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。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
```

ログファイル内で、“SCANNED:X (X はスキャンコード数値)” という記載があるかご確認ください(スキャンコードについては第 8 章をご覧ください)。

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。

12-3 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。

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、「6 基本設定手順」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。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。

12-4 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/updates/>

「アンチウイルス」のよくあるご質問 (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/>

13 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。

13-1 メールによる各種情報の通知

本製品をインストールすると、月次処理の実行時 (crontab で設定された日時) に管理レポートが毎月送信されます。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 13-1 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
               (2005/06/01 - 2005/06/30)
To : postmaster@redhat7.gideon.co.jp
```

リスト 13-1

リスト 13-2 は、月次管理レポートのメール本文の表示例です。

2005-06-01 から 2005-06-30 までの統計情報

送受信メール数: 28
 ウイルス添付メール: 4
 ウイルス: 12

=====
 ウイルス添付メール数の詳細
 (説明文略)

 4 mail: (EICAR-Test-File [AVP]
 EICAR_Test_File [Libra]
 EICAR Test File [Orion])

4 mail: ALL

=====
 ウイルス数の詳細
 [中略]

ウイルス数 virus: ウイルス名

 4 virus: EICAR-Test-File [AVP]
 4 virus: EICAR_Test_File [Libra]
 4 virus: EICAR Test File [Orion]

12 virus: ALL

リスト 13-2

管理レポートでは、メール送受信の総件数(システムのエラーメールやリターンメールも含まれます)、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総数、種類などが報告されます。

「送受信メール数」は、デフォルトでは表示されませんが、
 /etc/GwAV/GWAV.conf ファイルに下記一行を追加することで表示されるようになります。

```
GWMVW_COUNT=/var/log/GWMVW.count
```

注意

統計情報では、ウィルスの種類、ウィルス名、エンジン名が表示されます。「アンチウイルス for Linux」では、fsav というウィルススキャンエンジンが動作しますが、fsav は内部的に [AVP]、 [Libra]、 [orion] という異なる 3 種類のエンジンから構成されます。それぞれの内部エンジンが独立してウィルス検出します。そのため、通常同じ 1 つのウィルスに対して、それぞれの内部エンジンがもつ定義ファイルで検出し、それぞれの定義ファイルに登録されているウィルス名で表示します。一つのウィルスについてどれか一つのエンジン、どれか二つのエンジン、もしくは 3 つすべてのエンジンで検出する場合などあります。同じファイルでも、表示するウィルス名は内部エンジンにより大抵異なります。

したがって、表示された各ウィルス数を単純に足せば総数として集計されるわけではありませんので、参考としてご利用ください。もしウィルスがすべての内部エンジンで検出された場合、

「ウィルス添付メール数」 × 3 = 「ウィルス数」
になります。

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ので、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。

13-2 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、「11 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。

13-3 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。

「アンチウイルス for Linux」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。

「アンチウイルス for Linux」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様にご相談ください。

14 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。そしてその結果をメールで報告します。

14-1 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、/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。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。

14-2 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
```

14-3 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` 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 14-1 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 14-1

14-4 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 (現在の仕様では “No” と同じです)

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
```

14-5 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 14-3 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 14-3

14-6 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
```

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: A V L34567、A V R 23456)
(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 サポートセンター

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

- * 営業時間

9:00 ~ 17:00 土・日・祝祭日・年末年始を除きます。

技術サポート以外の一般的なお問い合わせは、インフォメーションセンターまでお願いいたします。

E-Mail : info@gideon.co.jp

GIDEON 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（技術のお問合せ）

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

アンチウイルス for Linux RedHat 対応
Sendmail 版/Qmail 版/Postfix 版

アンチウイルス for Sun Cobalt
Sun Cobalt RaQ/Sun LX 対応

ユーザーズガイド

2001 年 4 月 27 日 初版発行
2005 年 6 月 1 日 第 13 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

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ください。

Copyright(c)2001-2005 GIDEON Co.,Ltd

Printed in Japan