

GIDEON

ユーザーズ
ガイド

AntiVirus

for Linux

ギデオン

リアルタイムスキャン

はじめに

この度は、製品をご利用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 リアルタイムスキャン』ユーザーズガイドとなっています。

対象読者は、システムのインストールを行う方、システム管理者、ネットワーク管理者です。本製品の運用・管理を行うには、Linuxの基礎知識およびシステム管理の経験が必要になります。

ご使用前に必ずご一読いただきますようお願いいたします。

■テスト用ウイルスファイルについて

本製品CD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。

このファイルをチェックすることで、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。

GIDEON、ギデオン、GIDEON AntiVirus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。

Kaspersky Lab、カスペルスキーラボの名称およびロゴはカスペルスキー社の商標または登録商標です。

The Linux kernel is Copyright 1991-1996 Lius Torvalds and is licensed under the term of the GNU General Public License.

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。

目次

第1章 製品の使用に関して	6
1.1 製品の概要	6
1.2 本製品の特長・機能	7
1.3 推奨動作環境	8
1.4 インストール対象サーバ環境	10
1.5 インターネット接続による更新の注意	11
1.6 ご利用上の注意	12
第2章 インストール・アンインストール	14
2.1 インストール準備	14
2.2 インストール	15
2.3 アンインストール	15
第3章 管理GUI操作	16
3.1 管理GUI用サービス起動と停止	16
3.2 管理・設定画面のアクセス方法	16
3.3 初回のログイン	17
3.4 ログイン	19
3.5 TOP画面	20
3.5.1 全体設定	22
3.5.1.1 基本動作の設定	23
3.5.1.2 セキュリティポリシー自動適用	28
3.5.1.3 ライセンス登録	31
3.5.1.4 SMTPサーバの設定	32
3.5.1.5 更新環境の設定	33
3.5.1.6 その他の設定	34
3.5.2 ディレクトリの追加	35
3.5.3 ディレクトリの設定変更	37
3.6 サポート画面	39
3.7 ウイルス検出機能の動作確認テスト	41

第4章 ファイルチェック機能	42
4.1 概要	42
4.2 ディレクトリリストの記述	43
4.3 実行結果の報告	45
4.4 ファイルチェックの設定方法	47
4.5 sambaによるファイル共有に関する情報	48
4.6 コマンドの使い方について	49
付録 サポートサービス	50
■ サービス内容	50
■ 製品のサポート情報	51
■ サポート依頼フォーム	51
■ お問い合わせ	52

1.1 製品の概要

近年、ウェブサーバに対するサイバー攻撃などにより、ウェブの改ざんや改ざんされたサイトからのウイルスの流布、さらにはサーバ上に保持していた情報の漏洩など、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。

このようなサイトの改ざんやウイルス被害を防ぎ、安心した環境にするには、「ウェブサーバ上で対策をすること」が、最も有効な方法といえます。

『ギデオン リアルタイムスキャン』は、サーバ上に置かれたサイトを構成するファイルやシステムリソースのファイルの改ざん検知、及び修復を行うとともにウイルス、スパイウェアをサーバ上で検出・隔離します。このことによりウェブサイトを安心して利用・管理できる環境を提供します。

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

1.2 本製品の特長・機能

■ 本製品の特長

- ウェブサーバの改ざん対策、ウイルス対策の統合ソフトウェア
- 使いやすいGUI管理画面から設定可能
- ウイルス定義ファイル、モジュールの自動更新機能でメンテナンスフリー
- Kaspersky社製のコアエンジンを組み込み、ウイルスを検出、駆除
(約15万種のウイルスパターン、新種ウイルスに数分間隔で対応)



■ 本製品の機能

指定されたディレクトリ以下を監視して、ファイルやディレクトリの新規作成、ファイルの削除、ファイルの内容変更をリアルタイムに検出し、新規作成や変更されたファイルの隔離処理やウイルススキャン処理、削除されたファイルの復帰処理、セキュリティポリシーの適用などの処理等を全て自動で実行します。

1.3 推奨動作環境

注意

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

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

■ 推奨動作環境

● 対応OS:

Linux Kernel 2.6.13 以降 (*1)

● 対応CPU:

インテル社製及びインテル互換CPU
Pentium4 2GHz 以上

● 対応ディストリビューション:

Red Hat Enterprise Linux 5/6、Cent OS 5/6、Debian 4/5/6、SUSE 10/11、Turbolinux 11 (TLAS3.0)、Miracle Linux v5/6
そのほか、ディストリビュータがサポートを継続しているLinuxディストリビューション (*2)

● メモリ:

空きメモリ容量 512MB 以上

● ハードディスク:

最低 50MB (インストールに必要な容量)

運用するにはログなどのディスク容量が別途必要になります(*3)。

*1) SELINUX が有効になっている環境では動作保証できません。

また、本製品は32bitで動作するソフトウェアのため、64bit版OSをご利用の場合は32bit互換ライブラリ (glibc/zlib/ncurses) を追加して頂く必要がございます

*2) 上記に含まれていないディストリビューションでも動作実績がある場合があります。弊社インフォメーションセンターにお問い合わせ下さい。

*3) 必要とするディスク容量は運用形態によって異なります。

1.4 インストール対象サーバ環境

本製品をインストールするサーバでは以下の要件を備えている必要があります。

- ウェブサーバとして正常に動作する容量、処理能力を備えていること
ウイルス検出のため一時的に文書の容量が必要になります。ディスクまたはメモリに、プロセス同時起動分の容量を確保してください。また、ウイルス検出のための処理負荷が増えます。
推奨メモリサイズは、約1GB以上 空きメモリ容量512MB以上です。

1.5 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。

1.6 ご利用上の注意

本製品をご利用いただく上で、以下の点にご注意ください。

● 定義ファイルの更新

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

● 容量管理

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

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

● スペックが低いマシンでは、サーバ負荷が異常に上がったとき、ウイルススキャン後、正しくメールが配信されない場合があります。CPUのスペックアップとディスクI/Oの転送速度を向上させることをお勧めします。

● 本製品はウイルス感染の危険を最小限にとどめるために有効なソフトです。しかし、これまでに述べたような理由や予期できない原因により、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。

2.1 インストール準備

試用版ソフトウェアはCD からサーバにインストールします。

《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。

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

```
server~>su -
```

《手順3》製品CD をマウント (読み可能に)する

CD のマウントについては、システムのコマンドを参照してください。

例えば、以下のようにイタリックの部分を入力して、Enter キーを押します。

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

インストール終了後、CD をアンマウントしてください。アンマウントについては、システムのコマンドを参照してください。

例えば、以下のようにイタリックの部分を入力して、Enter キーを押します。

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

2.2 インストール

一旦、CD-ROMをマウントしたディレクトリに移動してからインストールを実行します。

```
# cd /mnt/cdrom
# ./ginstall -F -M N -P RTV
```

『Installation SUCCEEDED.』というメッセージが表示されたらインストールは完了です。

2.3 アンインストール

root 権限でログインし、次のコマンドを入力し、Enter キーを押します。

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

3.1 管理GUI用サービス起動と停止

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

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

このサービスを停止するには、上記「*y*」に替わり「*n*」を入力します。

3.2 管理・設定画面のアクセス方法

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

<http://antivirus.gideon.co.jp:777/rtscan/>

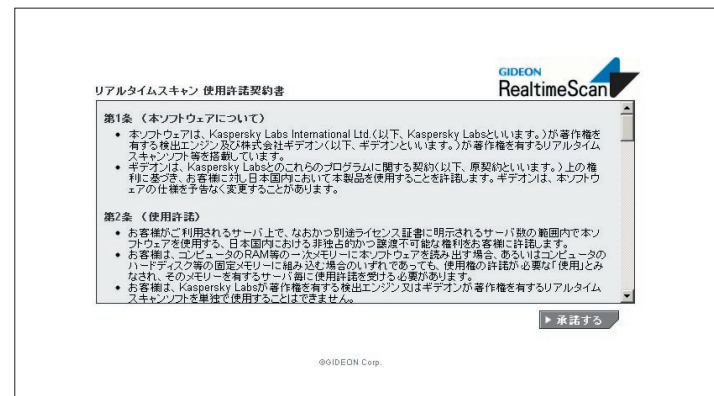
セキュリティが気になる場合は、HTTPSでポート番号(999)を指定します。

<https://antivirus.gideon.co.jp:999/rtscan/>

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

3.3 初回のログイン

本製品をサーバにインストールした後、はじめて管理・設定画面にアクセスすると、画面3.1のような本製品の使用許諾契約書が表示されますので、ご一読ください。



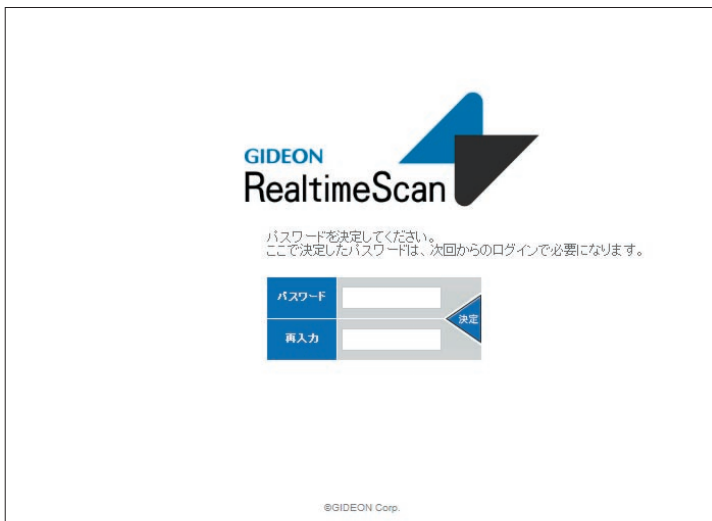
画面3.1

注意

ここに記載された諸条件をご承諾いただける場合は「承諾する」ボタンをクリックすることで、以降の本製品ご利用操作を開始いただけます。

「承諾する」ボタンをクリックすると、続いて画面3.2 パスワード設定画面が表示されます。この画面で任意のパスワードを入力します。(半角英数20文字以内)

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



画面3.2

3.4 ログイン

前項で説明した初回のログイン以後は、管理・設定画面にアクセスすると、画面3.3 ログイン画面が表示されます。

初回のログインで設定したパスワードを入力します。パスワード入力後 [ログイン] ボタンをクリックします。

パスワードの変更

画面3.3 ログイン画面で既存のパスワードを入力して [変更] ボタンをクリックすると、画面3.2 パスワード入力画面が表示されます。

初回のログインと同様にパスワードを再設定します。(半角英数20文字以内)



画面3.3

3.5 TOP画面

「TOP」タブをクリックすると、画面3.4が表示されます。



画面3.4

[再読み込み]ボタン：

監視ログ、状況や監視イベントの表示を最新にする場合にクリックします。

[ログアウト]ボタン：

管理GUIから再度ログイン画面に戻る場合にクリックします。

動作状況：

ONはサービス稼働中、OFFはサービス停止中です。動作状況表示ボタンをクリックすると、動作切り替えウインドウがポップアップし、サービスのON/OFFを切り替え可能です。

最新24時間の監視状況：

最新24時間の発生イベント数を時間別のグラフで表示します。

最新1週間の監視状況：

最新1週間の発生イベント数を日別のグラフで表示します。

●リアルタイム監視ログ (画面3.4 上段部分)


指定されたディレクトリ以下で発生する以下のイベントを検出し、発生した日時、アクションの種類、ファイル名などの情報をログに出力します。

- ファイルの変更(作成、移動を含む)
- ファイルの削除
- フォルダ(ディレクトリ)の作成
- フォルダ(ディレクトリ)の削除
- ウイルス感染
- ウイルス未感染

なお、表の各項目名(No.、日時、ファイルパス、イベント)の部分をクリックすると、項目別に表をソートすることが可能です。

また、右上部に設置されたプルダウンメニューによりイベント種類を選択すると、イベント種類を限定したログ表示が可能です。

[自動更新]ボタン：

このボタンをクリックすると、ボタンの色が  と変化し、10秒ごとにログ表示を更新します。

[ダウンロード]ボタン：

このボタンをクリックすると、リアルタイム監視ログをcsv形式でダウンロードすることができます。

●ディレクトリリスト (画面3.4 下段部分)

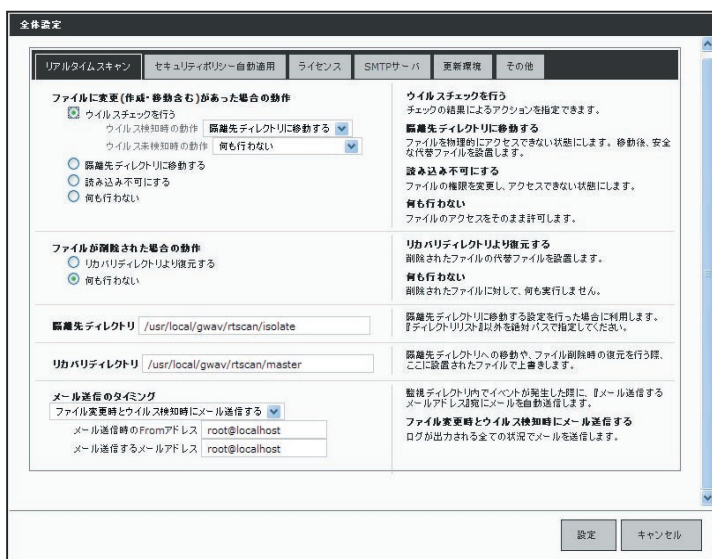
ここでは監視対象となるディレクトリの指定、指定されたディレクトリに対する設定やディレクトリごとのイベント数グラフの表示、発生イベントに対するアクションなどを指定します。

なお、リスト右上にウイルスチェックとセキュリティポリシーのステータス(有効/無効)が表示されます。

3.5.1 全体設定

画面3.4下段のディレクトリリストにて、[全体設定]ボタンをクリックすると、画面3.5がポップアップウィンドウとして表示されます。

この画面では検出したイベントに対する変更されたファイルの隔離処理やウイルススキャン処理、削除されたファイルの復帰処理、セキュリティポリシーの適用などの処理等のアクションを設定します。



画面3.5

設定項目の詳細を以下にご案内します。

3.5.1.1 基本動作の設定

[全体設定]ボタンをクリックした直後、あるいは[リアルタイムスキャン]タブを選択することにより表示される画面3.5上で、ファイル変更検知時の動作、隔離先/リカバリディレクトリやメール通知の設定が行えます。

3.5.1.1.1 ファイルに変更(作成)があった場合の動作

ラジオボタンにより、以下(1)~(4)の動作を選択します。

(1) 隔離先ディレクトリに移動する

変更されたファイルを指定された隔離先ディレクトリに移動して、他のプログラムからのアクセスを物理的に遮断します。移動が成功した場合は作成されたファイルの代替ファイルを設置します。

代替ファイルは以下の方法で決定します。

- 1) 信頼できるファイル(⇒3.5.1.4 注記)がある場合はそのファイル
- 2) 1)のファイルがない場合はサイズ 0 のファイル

何らかの理由で隔離できなかった場合は、事後策として 次項(2)の動作を試みます。

(2) 読み込み不可にする

ファイルの所有者情報、アクセス権限を変更して、他のプログラムからの不意なアクセスを防止します。変更されるモードを以下に示します。

- ・所有者情報: root, root (オーナー、グループ)
- ・アクセス権限: 000 (全てのユーザからのアクセスを拒否します)

(3) 何も行わない

変更されたファイルのアクセスをそのまま許可します。

(4) ウイルスチェックを行う

変更されたファイルを当社の提供するアンチウイルスエンジンによりスキャンし、スキャン結果によるアクションを指定することができます。

[ウイルス検知時]

ウイルススキャンの結果ウイルスに感染していると判断された場合に指定できるアクションは次の通りです。

- ・ 隔離先ディレクトリに移動する[(1)と同じアクション]
- ・ 読み込み不可にする[(2)と同じアクション]

[ウイルス未検知時]

ウイルススキャンの結果ウイルスに感染していないと判断された場合に指定できるアクションは次の通りです。

- ・ 隔離先ディレクトリに移動する[(1)と同じアクション]
- ・ 何も行わない[(3)と同じアクション]

3.5.1.1.2 ファイルが削除された場合の動作

ラジオボタンにより、以下(1)～(2)の動作を選択します。

(1) リカバリディレクトリより復元する

削除されたファイルの代替ファイルを設置します。

代替ファイルは以下の方法で決定します。

- 1) 信頼できるファイル(⇒3.7.1.4 注記)がある場合はそのファイル
- 2) 1)のファイルがない場合はサイズ 0 のファイル

(2) 何も行わない

削除されたファイルに対して、何も実行しません。

3.5.1.1.3 隔離先ディレクトリ

変更されたファイルやウイルスチェックされたファイルを隔離するアクションを選択した場合に移動先のディレクトリをフルパスで指定します。

インストール時のデフォルト設定では「/usr/local/gwav/rtscan/isolate」が指定されています。

※ 隔離先ディレクトリには次のようにファイルパスをURLエンコードして変更日時を付加したファイル名を持つ隔離ファイルが作成されます。

[隔離ファイル作成例]

「/var/www/html」を監視ディレクトリとして設定していて、そのディレクトリ直下のファイル「index.html」に変更があった場合の隔離ファイル名

```
%2fvar%2fwww%2fhtml%2findex.html.2011-11-21-17-32-08
```

URLエンコードされた部分
変更日時

3.5.1.1.4 リカバリディレクトリ

変更されたファイルを隔離先に移動した後、代替ファイルを設置する場合やファイルが削除された際に復元するアクションを選択した場合に使用する代替ファイルの設置ディレクトリをフルパスで指定します。

インストール時のデフォルト設定では「/usr/local/gwav/rtscan/master」が指定されています。

※ 復元するアクションを実施するためには、リカバリディレクトリ以下に予め監視するディレクトリ構造を保持した形で、ファイルのコピーを置いておく必要があります。

[リカバリディレクトリ作成例]

「/var/www/html」を監視ディレクトリ、「/usr/local/gwav/rtscan/master」をリカバリディレクトリとして設定している場合、監視ディレクトリ直下のファイルを全てコピーする。

```
# cd /var/tmp
□ ⇒テンポラリディレクトリに移動する
# tar czvf org.egz /var/www/html/*
□ ⇒監視ディレクトリを構造ごと圧縮ファイルにする
# tar xzvf org.egz -c /usr/local/gwav/master/
⇒圧縮ファイルをリカバリディレクトリに構造をそのままにして解凍する
```

注) 信頼できるファイル

ターゲット指定されたディレクトリでファイルの作成や変更、削除が発生した際に、代替ファイルとして使用するファイルを指定することができますが、代替ファイルとして使用するファイルのうち、安全性が検証されたファイルを“信頼できるファイル”と表現します。

代替ファイルとして使用するファイルはリカバリディレクトリ以下にターゲット指定したディレクトリと同じ構成でファイルを設置する事で指定します。

本製品では起動時に指定されたディレクトリ以下に含まれる全てのファイルのハッシュ値を取得してプログラム中に保存しておきます。

イベント発生時に代替ファイルとして利用するファイルのハッシュ値を再計算し、起動時に取得した値と等しい場合は信頼できるファイルとして使用します。

ハッシュ値が異っていた場合は本コマンドの起動後に改ざんされているので、代替ファイルとして利用しません。

3.5.1.1.5 メール通知機能

ターゲット指定されたディレクトリでイベントが発生した際に、指定したメールアドレスにメールを自動送信する機能があります。

「メール送信のタイミング」の項目ではメール送信するタイミングを次の3つからプルダウンで選択できます。

- 1) ファイル変更時とウイルス検知時
- 2) ウイルス検知時のみ
- 3) メール送信しない

なお、送信されるメールのテンプレートはデフォルトでは次のようになっています。

```
Date: (日時)
From: (メール送信時のFromアドレス) ←GUIから設定
To: (メール送信時のToアドレス) ←GUIから設定
Subject: ### GIDEON rtscan notification mail ###
Content-Type: text/plain; charset=iso-2022-jp
```

以下のファイルに対するアクセスを検知しました。

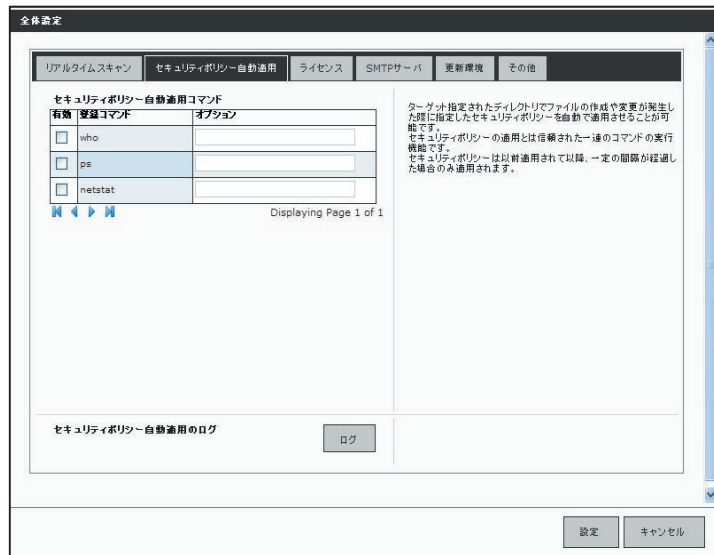
```
日時: (検知日時)
ホスト名: (ホストのFQDN)
イベント: (発生したイベント)
動作: (実施したアクション)
ファイル: (変更されたファイル名) (ファイルのモード)(ファイルサイズ)
(ウイルス名などの追加情報)
```

3.5.1.2 セキュリティポリシー自動適用

画面3.5上で、[セキュリティポリシー自動適用]タブを選択すると、画面3.6が表示されます。画面3.6上で、GUI操作によって指定された監視ディレクトリにおいて、ファイルの作成や変更が発生した場合、予め登録したセキュリティポリシーを自動で適用させることが可能です。

なお、インストール後のデフォルトではwho、ps、netstatがコマンドとして登録されています。(各コマンドにはオプション設定も可能です。)

また、コマンド実行結果は同画面下部にある「セキュリティポリシー自動適用のログ」の項目の[ログ]ボタンをクリックすると表示されます。



画面3.6

[実施例]

psコマンドを選択して、/var/www/html/index.htmlを改変したときのログ

```

2011/12/19 00:00:00 [ /var/www/html/index.html ]
2011/12/19 00:00:00 execute: /usr/local/gwaw/rtscan/trust/ps
PID TTY          TIME CMD
  1 ?            00:00:00 init
  2 ?            00:00:00 kthreadd
  3 ?            00:00:00 migration/0
  4 ?            00:00:00 ksoftirqd/0
  5 ?            00:00:00 watchdog/0
  6 ?            00:00:00 events/0
  7 ?            00:00:00 khelper
 42 ?           00:00:00 kblockd/0
 45 ?           00:00:00 kacpid
 46 ?           00:00:00 kacpi_notify
111 ?          00:00:00 ksuspend_usbd
117 ?          00:00:00 khubd
120 ?          00:00:00 kseriod
154 ?          00:00:00 pdflush
155 ?          00:00:01 pdflush
156 ?          00:00:00 kswaped0
157 ?          00:00:00 aio/0
 814 ?         00:00:00 ata/0
 815 ?         00:00:00 ata_aux
 820 ?         00:00:00 scsi_eh_0
 822 ?         00:00:00 scsi_eh_1
 842 ?         00:00:00 scsi_eh_2
 886 ?         00:00:01 kjournald
 938 ?         00:00:00 kauditd
 960 ?         00:00:00 kpsmoused
1348 ?        00:00:02 acpid
1663 ?        00:00:00 auditd
1665 ?        00:00:00 audispd
1729 ?        00:00:00 netplugd
1802 ?        00:00:00 cced
2149 ?        00:00:00 master
2280 ?        00:00:25 aisexec
2330 ?        00:00:00 ccsd
2393 ?        00:00:00 syslog-ng
2426 ?        00:00:00 udevd
3593 ?        00:00:01 snmpd
3609 ?        00:00:00 snmptrapd
3625 ?        00:00:00 xinetd
3638 ?        00:00:00 sshd
3671 ?        00:00:00 slapd
3689 ?        00:00:00 httpd.admsrv
3808 ?        00:00:00 gpm
3825 ?        00:00:00 httpd
3870 ?        00:00:00 crond
3905 ?        00:00:00 squid
3965 ?        00:00:00 cupsd
4247 ?        00:00:00 login
8559 ?        00:00:00 rtscan
8850 ?        00:00:00 ps

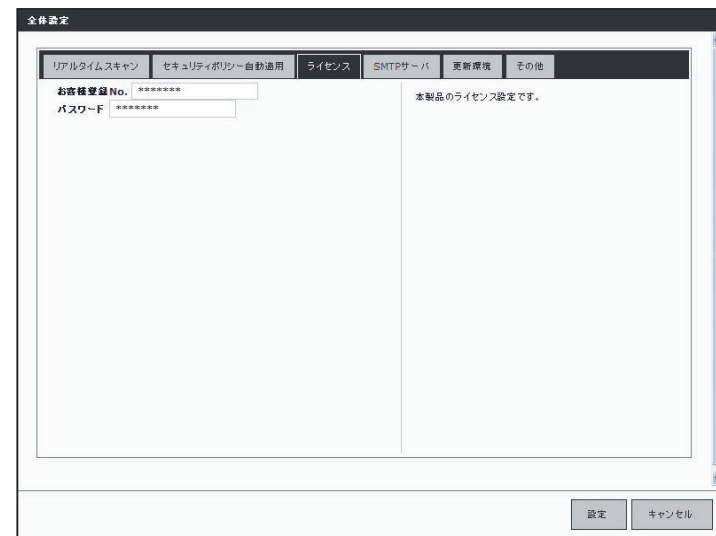
```

[コマンドの追加]

GUIから選択できるコマンドを追加する場合は登録したいコマンドを登録ディレクトリ(/usr/local/gwav/rtscan/trust)配下にコピーします。

3.5.1.3 ライセンス登録

画面3.5上で、[ライセンス]タブを選択することにより表示される画面3.7上で、ユーザ登録時に発行された「お客様登録No.」と「パスワード」を入力します。



画面3.7

3.5.1.4 SMTPサーバの設定

画面3.5上で、[SMTPサーバ]タブを選択することにより表示される画面3.8上で、通知メールなどを送信するために使うメール(SMTP)サーバを指定します。

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

画面3.8

3.5.1.5 更新環境の設定

画面3.5上で、[更新環境]タブをクリックすると、画面3.9が表示されます。

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

「プロキシのIPアドレス」「ポート番号」は必須項目です。

「ID」「パスワード」が設定されている場合には、それぞれ入力が必要です。

画面3.9

3.5.1.6 その他の設定

画面3.5上で、[その他]タブをクリックすると、画面3.10が表示されます。



画面3.10

設定の初期化

リアルタイムスキャンに関する設定を初期化します。監視ディレクトリリストは初期化されませんが、ホワイトリストはクリアします。

3.5.2 ディレクトリの追加

画面3.4下段の監視ディレクトリリストの項目において、[追加]ボタンをクリックすると、画面3.11がポップアップウインドウとして表示されます。

この画面では監視対象とするディレクトリを指定します。



画面3.11

ラベル名

ディレクトリリスト上で判別のつくような名称を記載してください。

ディレクトリパス

監視対象とするディレクトリをフルパスで記載してください。

文字コード

指定するディレクトリ内のファイル名の文字コードをプルダウンから以下の4つより選択します。

- 1) us-ascii
- 2) UTF-8
- 3) euc-jp
- 4) SHIFT_JIS

ホワイトリスト

監視対象とするディレクトリ配下で監視対象から除外するファイル、およびディレクトリを監視ディレクトリからの相対パスで指定できます。

[設定例 (監視対象ディレクトリ: /var/www/html)]

- (1) ファイル/var/www/html/dir1/fooを監視対象から除外する場合
→「dir1/foo」と記載します。
- (2) ディレクトリ/var/www/html/dir1/foo/を監視対象から除外する場合
→「dir1/foo/」と記載します。

注意

ホワイトリストでディレクトリを指定する場合はファイルと区別するために最後にスラッシュ(/)で閉じてください。

3.5.3 ディレクトリの設定変更

画面3.4下段の監視ディレクトリリストの項目において、各指定ディレクトリ左側に表示される設定ボタンをクリックすると、画面3.12がポップアップウィンドウとして表示されます。

この画面では先に指定した監視対象ディレクトリのラベル名、ファイル名の文字コード、ホワイトリストを変更できます。



画面3.12

ラベル名

ディレクトリリスト上で判別のつくような名称を記載してください。

文字コード

指定するディレクトリ内のファイル名の文字コードをプルダウンから以下の4つより選択します。

- 1) us-ascii
- 2) UTF-8
- 3) euc-jp
- 4) SHIFT_JIS

ホワイトリスト

監視対象とするディレクトリ配下で監視対象から除外するファイル、およびディレクトリを監視ディレクトリからの相対パスで指定できます。

[設定例 (監視対象ディレクトリ: /var/www/html)]

- (1) ファイル/var/www/html/dir1/fooを監視対象から除外する場合
→「dir1/foo」と記載します。
- (2) ディレクトリ/var/www/html/dir1/foo/を監視対象から除外する場合
→「dir1/foo/」と記載します。

注意

ホワイトリストでディレクトリを指定する場合はファイルと区別するために最後にスラッシュ(/)で閉じてください。

注意

ディレクトリパスの指定変更はこの画面上からはできません。
違うディレクトリパスに監視対象を変更される場合は、ご面倒でも画面3.12上の[削除]ボタンで一旦削除したのち、変更先ディレクトリ指定を追加設定してください。

3.6 サポート画面

「サポート」タブをクリックすると、画面3.13 が表示されます。



画面3.13

[再読み込み]ボタン :

稼働状況やウイルス定義ファイル更新ログの表示を最新にする場合にクリックします。

[ログアウト]ボタン :

管理GUIから再度ログイン画面に戻る場合にクリックします。

最新のバージョン情報

製品モジュールとアンチウイルスエンジンの定義ファイルの現在のバージョンが表示されます。

製品モジュールの[手動更新]ボタン :

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

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

稼働状況

1時間おきに実施される製品稼働チェックの結果が表示されます。

ウイルス定義ファイル更新ログ履歴

1時間おきにウイルス定義ファイル更新動作の結果が表示されます。但し、配布元サーバが更新されていないなどの理由で定義ファイル配布元サーバと製品内にダウンロードされている定義ファイルが同一の場合の更新動作については表示されませんのでご了承下さい。

ウイルス定義ファイルの[手動更新]ボタン :

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

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

3.7 ウィルス検出機能の動作確認テスト

以下にウイルス検出機能の動作確認テスト方法を示します。

※テストは製品インストールCDに収録されている無害なウイルスファイル「eicar.com」を利用します。

- (1) 製品インストールCDをCDドライブに挿入します。
- (2) root権限でログインして、製品インストールCDをマウントします。

```
# mount -r -t iso9660 /dev/cdrom /mnt/cdrom
```

- (3) 製品インストールCDから監視対象のディレクトリにウイルスファイル「eicar.com」をコピーします。

```
# cp /mnt/cdrom/sample/eicar.com /var/www/html/.
```

※監視対象ディレクトリが/var/www/htmlと設定されている場合

- (4) ウィルス検出機能が動作している場合、図3.14のように管理GUIのリアルタイム監視ログに「感染」というイベントが記録されます。

No.	日時	ファイルパス	イベント
0001	2011/12/15 20:05:12	/var/www/html/eicar.com	感染

図3.14

本製品の主機能はLinuxサーバ向けリアルタイムの改ざん検知、修復、およびウイルス検知ですが、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ファイルチェック機能があります。またその結果をメールで報告します。

4.1 概要

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

----例----

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

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

注意

ウイルス検出時には、処理負荷が大きくなりますので、特定のディレクトリに限り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。

4.2 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
```

4.3 実行結果の報告

指定されたディレクトリのウイルスチェックが完了すると、その実行結果がメールで報告されます。

報告先は、/etc/GwAV/GWAV.confの中のINFO_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4-3は、/etc/GwAV/checkdirに/var/spool/* EUC-JPが記述されている場合の、ウイルスチェック実行結果の報告メールです。

```

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

```

リスト4-3

4.4 ファイルチェックの設定方法

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

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

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

```

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

```

周期(Interval)設定:

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

ファイルチェックの設定内容を確認する場合、以下のコマンドを実行します。

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

4.5 sambaによるファイル共有に関する情報

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

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

リスト4-5は、このコマンド実行結果を表示した例です。

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

リスト4-5

4.6 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
```

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おります。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、発現象

できるだけ具体的に記述してください。

- ・ 発生頻度
- ・ ログの記録などの具体的な情報
- ・ 再現テスト手順(特に再現性がある場合)

問題解決のため、おわかりになる範囲で以下の項目等をお知らせください。

4. サーバ機種名

5. サーバ設定の変更等

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

6. ソフトの利用環境

例えば、以下のような情報が判断材料になります。

- ・ インストールしたサーバOSとそのバージョン
- ・ 設定ファイル

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。

■ お問い合わせ

株式会社 ギデオン

〒223-0056横浜市港北区新吉田町3382-7

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

●サポートセンター(技術のお問合せ)

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

受付時間/9:00～17:00(祝祭日を除く、月～金)

ギデオン リアルタイムスキャン
ユーザーズガイド

2012年2月27日 第2版発行

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

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(c)2012 GIDEON Corp.
Printed in Japan