ギデオン ゲートウェイセキュリティ インストール手順

概 要

このドキュメントでは「ギデオン ゲートウェイセキュリティ」(以下、「ゲートウェイセキュリティ」と表記します) を新規にインストールする方法について説明します。

1 インストール

1.1 前提条件

「ゲートウェイセキュリティ」はすでにゲートウェイサーバとして動作している Linux サーバにインストールする事ができます。

1.2 インストーラについて

主に RedHat 系のディストリビューションで利用されている RPM パッケージに対応したインストーラが用意されています。

```
RPM-gav-gproxy-antispamplus
```

1.3 インストール方法

ご利用の Linux サーバにインストーラをダウンロード後、展開してインストーラを実行します。

インストーラをダウンロードしてインストールするには以下のコマンドを実行します。インストーラのサイズは約 170MB ありますのでダウンロードに時間がかかります。またインストーラを展開して実行するには十分なディスク容量を必要としますのでご注意下さい。

以下の実行例中の '#' はシェルのプロンプトを示しますので入力は不要です。(環境によっては '#' プロンプトは異なる場合があります。)

```
# wget http://download.gideon.co.jp/RPM-gav-gproxy-antispamplus.tgz
# tar zxvf RPM-gav-gproxy-antispamplus.tgz
# ./RPM-gav-gproxy-antispamplus install
```

CD からのインストールをご希望の場合はお手数ですが弊社 Web Site よりお試し版の CD をご請求ください。
http://www.gideon.co.jp/support/trial/

1.4 インストール時の注意事項

インストール途中でソフトウェアを最新の状態に更新するために、コンソールに

```
Now, update?  [Y/n]
```

と表示されますので、必ず “y” を入力してください。
上記表示に “y” を入力しますとソフトウェアを最新版に更新する処理が実行されますので、終了までに 10 分程度の時間がかかります。

コンソール画面に上記メッセージが表示されずにインストール動作が終了してしまった場合は、弊社までお問合せ下さい。

2 インストール時のシステム変更

「ゲートウェイセキュリティ」をインストールする際に以下に示すシステムの変更、およびファイルの変更などが生じます。

1. mailflt3 ユーザ、および mailflt3 グループがシステムに追加されます。
2. /etc/cron.d ディレクトリに「ゲートウェイセキュリティ」用の設定ファイルが追加されます。
3. /etc/logrotate.d ディレクトリに「ゲートウェイセキュリティ」用の設定ファイルが追加されます。
4. syslog の設定ファイルに「ゲートウェイセキュリティ」用の設定項目が追加されます。
5. Kaspersky 社の AntiVirus エンジンで利用するデーモンを起動し、システムの起動時の自動起動項目に追加されます。
6. Kaspersky 社の AntiSpam エンジンで利用するデーモンを起動し、システムの起動時の自動起動項目に追加されます。

3　ゲートウェイセキュリティ機能動作までの手順

「ゲートウェイセキュリティ」を導入後、アンチウイルス アンチスパム機能を正しく動作させるために以下の手順に従い設定してください。

3.1　管理画面のアクセス

「ゲートウェイセキュリティ」の設定は管理画面より行いますが、管理画面を利用するためにはインストール後に一度だけ以下の操作を実行する必要があります。

```
# /usr/local/gwav/gwav-gui-control
```

上記コマンドを実行すると、コンソールに

```
Use web-interface for anti-virus Yes/No [No]:
```

と表示されますので、“y” を入力してください。

管理画面用のサービスが起動されましたら、クライアント PC から Web ブラウザを利用して管理画面にアクセスします。

Web ブラウザのアドレスバーに「ゲートウェイセキュリティ」をインストールしたサーバのホスト名、もしくは IP アドレスに続けてポート番号の 777 を指定します。

```
http://ゲートウェイサーバのホスト名:777/
```

3.2　アンチウイルス機能

1. アンチウイルス設定画面
   管理・設定画面の左上「アンチウイルス」タブをクリックすると、『アンチウイルス設定画面』が表示されます。この画面からアンチウイルスの各種設定を行います。
2. ウイルス定義ファイルの手動更新
   『アンチウイルス設定画面』上部「更新状況」タブをクリックすると『更新状況画面』が表示されます。
   この画面の 手動更新 ボタンをクリックして、最新の定義ファイルを取得します。通信速度にもよりますが、初回の更新には約 10 分程度時間がかかります。
3. 管理用のメールアドレス設定
   『アンチウイルス設定画面』上部「共通設定」タブをクリックすると、『共通設定画面』が表示されます。

この画面の「基本設定」タブをクリックして表示される画面で保守管理のための報告メールやウイルス検出時の警告メールの宛先となるメールアドレス、および、警告メールやスパム検出メールを転送する場合の送信元メールアドレスを設定します。

4. メール送信で使用するサーバ設定
『共通設定画面』の「詳細設定」タブをクリックして表示される画面でシステムが各種メールを送信する際に使用する SMTP サーバを設定します。

> ※デフォルトでは 127.0.0.1 が設定されます。

5. 更新環境設定
本製品は、常に最新版のウイルス定義ファイルやプログラムモジュールを利用するために、弊社が設置するアップデート情報提供用のサーバに HTTP プロトコルを利用して定期的にアクセスしています。
外部サーバへの HTTP アクセスが制限されていてプロキシーサーバを経由してのアクセスが必要な場合は、『共通設定画面』の「更新環境設定」タブをクリックして表示される画面にて「更新のために HTTP プロキシーを使用する」を選択してください。
「プロキシーの IP アドレス」、「ポート」項目は入力が必須てすので、利用するプロキシーサーバの IP アドレス、およびポート番号を入力して下さい。ご利用のプロキシーサーバに「ID」、「パスワード」が設定されている場合には、それらの項目も入力して下さい。

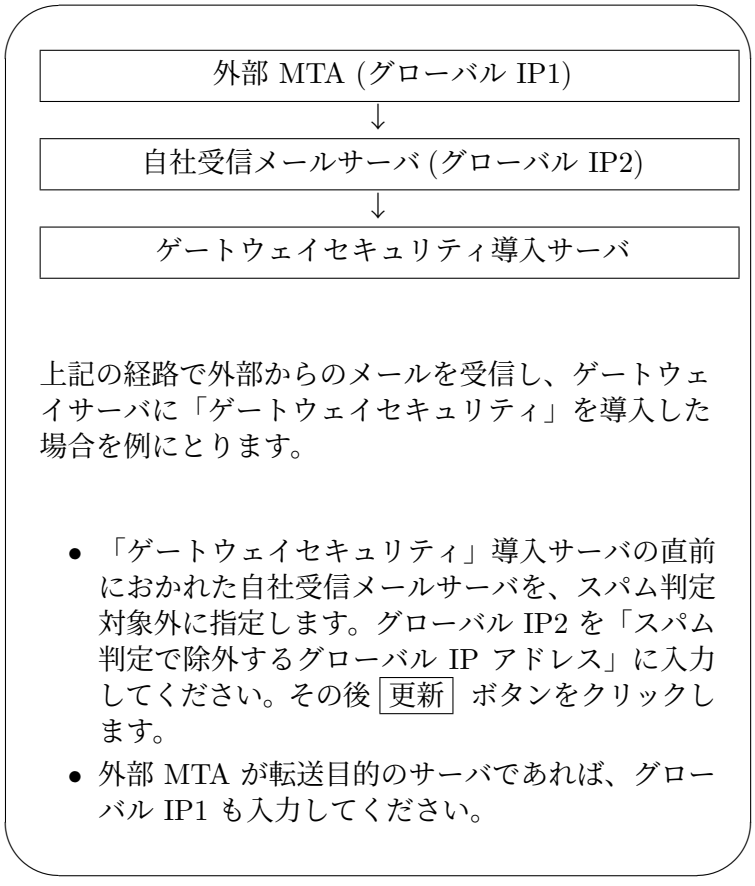
6. メール設定
アンチウイルス設定画面上部「メール設定」タブをクリックすると、『メール設定画面』か表示されます。
この画面の上部に表示されるボタンをクリックすることで、アンチウイルス機能の有効/無効の切替が行えます。
ボタン下部のタブを選択すると表示される画面で各種機能の確認、設定が行えます。
設定内容について詳しくは「ギデオン ゲートウェイセキュリティ」ユーザーズガイド「第 3 章 アンチウイルス設定」を参照してください。

3.3 アンチスパム機能

1. アンチスパム設定画面
管理・設定画面の左上「アンチスパム」タブをクリックすると、『アンチスパム設定画面』が表示されます。この画面からアンチスパムの各種設定を行います。

2. データベースの手動更新
『アンチスパム設定画面』上部「更新状況」タブをクリックすると『更新状況画面』が表示されます。
この画面の 手動更新 ボタンをクリックして、最新の定義ファイルを取得します。通信速度にもよりますが、初回の更新には約 10 分程度時間がかかります。

3. スパム判定方法の設定
   アンチスパム設定画面上部「メール設定」タブをクリックすると、『メール設定画面』が表示されます。
   この画面の上部に表示されるボタンをクリックすることで、アンチスパム機能の有効/無効の切替が行えます。
   ボタン下部のタブを選択すると表示される画面で各種機能の確認、設定が行えます。
   設定内容について詳しくは「ギデオン ゲートウェイセキュリティ」ユーザーズガイド「第 3 章 アンチウイルス設定」を参照してください。
4. スパム判定で除外するグローバル IP アドレスの設定
   「ゲートウェイセキュリティ」では受信したメールの直前のグローバル IP アドレスをチェックしてスパム判定を行います。したがって本製品を導入したサーバと外部との間に転送用その他のサーバが接続されている場合には、それらのグローバル IP アドレスをスパム判定対象から除外する指定が必要です。
   『アンチスパム設定画面』の「メール設定」タブをクリックし、この画面の「詳細設定 2 」タブをクリックします。
   「スパム判定で除外するグローバル IP アドレス」欄に、本製品を導入したメールサーバでメールを受信する経路上においてスパム判定しないグローバルな IP を指定します。



上記の経路で外部からのメールを受信し、ゲートウェイサーバに「ゲートウェイセキュリティ」を導入した場合を例にとります。

- 「ゲートウェイセキュリティ」導入サーバの直前におかれた自社受信メールサーバを、スパム判定対象外に指定します。グローバル IP2 を「スパム判定で除外するグローバル IP アドレス」に入力してください。その後 更新 ボタンをクリックします。
- 外部 MTA が転送目的のサーバであれば、グローバル IP1 も入力してください。

5. ユーザにスパムを配信しないようにする設定
『アンチスパム設定画面』上部「メール設定」タブをクリックし、この画面の「転送メール」タブをクリックします。この画面で以下の設定をすることで、ユーザにスパムメールが配信されないように指定できます。
   - 「転送下限スコアに達していたら転送」を選択
   - 「受信先への配信を停止する」にチェックマークをつける
   - テキストボックスに転送対象アドレスと転送先アドレスを記述

> `@example.com` が付くメールアドレスへのスパムメールを配信停止させたい場合は以下のように記述します。
>
> `@example.com spam@example.co.jp`
>
> 上記設定を行うことにより、`@example.com` 宛のスパムは `spam@example.com` に転送され、実際のユーザへの配信は停止します。

4 アンインストール

「ゲートウェイセキュリティ」をアンインストールする場合、以下のコマンドを実行します。

```
# /etc/GwAV/uninst/RPM-gav-gproxy-antispamplus uninstall
```

5 マニュアルのダウンロード

マニュアルは弊社の Web Site よりダウンロードできます。詳細はマニュアルを参照してください。

`http://www.gideon.co.jp/support/download/`