

# GUARDIANSUITE

---

## 検査サーバー 導入の手引き

～GUARDIANWALL 導入事前準備～

© Canon IT Solutions Inc. 2017

本マニュアルの一部あるいは全部について、キヤノン I T ソリューションズ株式会社の事前の承認なく、複製、転載することを禁止します。

<https://www.canon-its.co.jp/>

2017-Apr-28 GUARDIANSUITE V5.1  
GUARDIANWALL V8.1

---

MEMO

GUARDIANWALL をご利用いただくために、必要な準備について以下に説明します。  
GUARDIANSUITE の導入作業を行う前にご用意ください。

## 1 インストールプラン

本システムはファイアウォールの内側のネットワークにすでに設置されている SMTP ゲートウェイへのインストールを推奨します。既存の SMTP ゲートウェイではなく新規ハードウェアにインストールする場合は、事前に SMTP トラフィックを正しく中継し、メール送信が正しく行われるよう各種ネットワーク設定と MTA (Mail Transfer Agent) ソフトウェアのセットアップが完了している必要があります。

本システムは、SMTP トラフィックを処理するようなアプリケーション（グループウェアの SMTP ゲートウェイ、ウィルス検査ソフト等）がすでにインストールされている環境での動作は保証していません。また、本システムをインストールするサーバーで利用できる MTA ソフトウェアは sendmail、もしくは、sendmail 互換インタフェースを持つ qmail、Postfix だけになります。



- 本システムはファイアウォールの内部側ネットワークに設置してください。インターネットと直接つながれたネットワークセグメントや DMZ (DeMilitarized Zone) には、そこに設置しなければならない積極的な理由がない限り、無用なサーバーは設置すべきではありません。そのような場所には、SMTP トラフィックの中継だけを行う SMTP ゲートウェイを設置してください。本システムは、通常のメールサーバーより詳細なログ情報を保存し、メールのメッセージデータを保存します（保留機能、メール保存機能使用時）。したがって、DMZ やインターネットと直接つながれたネットワークセグメントへの設置は推奨しません。内部側ネットワークへの設置を強く推奨します。
  - Ver5.1 よりメール中継時に sendmail、qmail、Postfix 以外の外部コマンドを経由して送信したり、指定した外部サーバーに直接送信することができます。ただし、本システムで生成、送信する通知メールなどの送信には上記 MTA ソフトウェアを使用します。
  - GUARDIANWALL Ver8.1 に対応する管理サーバーのバージョンは、GUARDIANSUITE Ver5.1 および 5.2 です。
-

---

## 2 データ保存用ディスク領域

GUARDIANWALL が使用するキュー領域や、ログファイルを保管する領域を用意してください。メール保存機能を使用する場合は、メール本文データを保存する専用のディスク領域を準備する必要があります。

領域	内容
一時キュー	処理中のメッセージデータを一時キューに（一時的に）保存し検査を行います。メールの検査や処理が終わればメッセージデータは削除されます。
保留キュー	検査の結果、配送を保留するメールは保留キューに保存されます。管理者が、保留されたメールの送付、削除処置を行えば、保留キューから削除されます。管理者による処置が行われなくても、指定保存期間を過ぎた保留メールは自動的に削除されます。
ログディレクトリ	処理したメールのヘッダ情報などを含むログファイルを保管します。指定期間を過ぎた古いログファイルは自動的に削除されます。
メール保存ディレクトリ	メール保存機能を利用した場合、処理したメールのメッセージを保存します。ログデータに比較して大量の領域を使用します。保存専用の領域にデータを保存し、領域が不足すると自動的に古いデータを順に削除します。

### ■ 一時キュー、保留キュー

初期状態では、GUARDIANWALL をインストールしたディレクトリのサブディレクトリが指定されています。一度に多くのメールを保留させるような運用を行う場合は、十分な空き領域のあるディスク領域が必要です。



NFS（Network File System）マウントしたディレクトリは指定しないでください（ファイルロックが正常に動作しないため運用上障害が発生します）。

---

### ■ ログディレクトリ

初期状態では、GUARDIANWALL をインストールしたディレクトリのサブディレクトリが指定されています。ログファイルの容量の目安としては、メール 1 件につき約 1200 バイト使用します。これはログディレクトリに保存される全てのログを考慮しています。

メール流量、保存期間を考慮して十分な領域を準備してください。保留メールの閲覧や送付、削除操作、保存メールの内容閲覧などの操作もログに記録されますので、運用状態によってはより多くの領域が必要になります。

インストール後システム管理画面より、ログディレクトリ、各ログの保存期間を変更することができます。詳細については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』の「3-2-2-2 個別設定」-「(3) サーバーの詳細設定」-【データ保存】(86 ページ)をご参照ください。



NFS マウントしたディレクトリは指定しないでください（ファイルロックが正常に動作しないため運用上障害が発生します）。

---



本システムでは、メールの発信者アドレス、受信者アドレス、標題などのデータを「ログ」と呼び、ログディレクトリ以下にはこれらのログデータのみを保存します。メールのメッセージ（本文、添付ファイルなど含む RFC2822 形式メッセージ）を保存したものを「アーカイブ」と呼び、次のメール保存ディレクトリに保存します。

---

## ■ メール保存ディレクトリ

メール保存機能を使用する場合は、メール保存ディレクトリにメールのメッセージデータを圧縮（平均圧縮率は、約 50%）しながら保存します。メール流量にあわせて、十分な領域を準備してください。

初期状態ではメール保存機能は OFF です。また、メール保存ディレクトリも未設定です。同機能を使用する際は、インストール後、システム管理画面より設定します。詳細については、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「3-2-2-2 個別設定」-「(3) サーバーの詳細設定」-【データ保存】(86 ページ) をご参照ください。

---



メール保存ディレクトリは、複数指定できますが、必ず、以下の条件を満たすように設定してください。

- 1 つのメール保存ディレクトリは、1 つのディスクパーティション、ファイルシステムから構成してください（同一のファイルシステムから複数のメール保存ディレクトリは指定しないでください）。
  - メール保存ディレクトリはメール保存領域専用で準備してください（ログ保存領域、他のアプリケーションや OS が使用する領域とは共有しないでください）。
  - NFS マウントしたディレクトリは指定しないでください（ファイルロックが正常に動作しないので、障害が発生します）。
- 



ソフトウェア RAID で構成されたファイルシステムは、ディスクの書き込み処理パフォーマンスが著しく低下しますので、メール流量の多い環境では、キューやメール保存領域に使用しないでください。

---



遅延書き込み (write-behind) を有効にしたファイルシステムでは、使用スペースを解放しても実際に使用可能になるまで大きく遅延する場合があります。メール保存ディレクトリでは、ディスクフル後の容量管理処理で古いアーカイブデータファイルを削除して新データを保存できる空きスペースを確保します。

ディスクフルに達した状態で、古いアーカイブファイルの削除、使用可能スペースの確保を実施している時に遅延の影響により必要以上にアーカイブデータファイル、全文検索用インデックスファイルの削除が発生することがあります。

また、アーカイブデータファイルの転送や全文検索用インデックスの作成処理が失敗する場合があります。ファイルシステムや仮想ボリュームソフト、ディスク装置のキャッシュコントローラ等の遅延書き込み機構を無効にしてください。

---

#### ■ログ、メールアーカイブ転送一時作業ディレクトリ

管理サーバーと検査サーバーが異なるマシンにインストールされている場合、ログ、メールアーカイブを転送する必要があります。

このためのデータを一時的に格納する領域 (/opt/Guardian/Admin/tmp) は、転送するデータ (1 検査サーバーの 1 日分のデータ量) の 3 倍以上のディスク領域が、管理サーバーと検査サーバーのどちらにも必要になります。

## 3 OS 設定

GUARDIANWALL の運用に必要な OS の導入例を説明します。

導入環境や運用ポリシーにより必要な設定や手順を追加してください。詳細については、『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』をご参照ください。

### 3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）

Red Hat Enterprise Linux 5.5 がインストールされたサーバーへ GUARDIANWALL（管理サーバー）を導入するために必要な準備を例に、Red Hat Enterprise Linux への設定手順例を説明します。以下に説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口にてご確認ください。

#### (1) 必要パッケージのインストール確認

- ① サーバーへ管理者権限を持つユーザーでログインしてください。
- ② 必要パッケージ **compat-db** (32bit パッケージ) がインストールされているかご確認ください。

確認例 1) **compat-db** がインストールされている場合

```
# rpm -qa | grep compat-db
compat-db-4.2.52-5.1      ←パッケージ名が表示される
#
```

確認例 2) **compat-db** がインストールされていない場合

```
# rpm -qa | grep compat-db
#      ←パッケージ名が表示されず終了する
```

- ③ パッケージがインストールされていない場合、OS のインストール CD を利用してインストールを実施してください。
- ④ 同様に以下のパッケージがインストールされているかご確認ください。  
ed, tcl, compat-libstdc++-33 (32bit パッケージ) , mt-st,at



32bit パッケージはパッケージ名末尾が「.i686」となっているパッケージです。

---

#### (2) IPv6 設定の解除

GUARDIANWALL（管理サーバー／検査サーバ）は IPv6 に対応しておりません。以下に IPv6 設定の解除手順を説明します。

- ① vi エディタなどのテキストエディタで設定ファイル **/etc/modprobe.conf** を開いてください。

```
# vi /etc/modprobe.conf
```



---

② 設定ファイルを以下の通り編集してください。

- ・「alias net-pf-10 ipv6」と記述された行があれば、削除します。
- ・「alias net-pf-10 off」と記述された行が無ければ、追加します。
- ・「alias ipv6 off」と記述された行が無ければ、追加します。

変更前表示例)

```
alias eth0 e1000
alias net-pf-10 ipv6      # (存在すれば) この行をコメントアウト
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptspi
alias scsi_hostadapter2 ata_piix
                        # alias net-pf-10 off を追加
                        # alias ipv6 off を追加
```

変更後表示例)

```
alias eth0 e1000
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptspi
alias scsi_hostadapter2 ata_piix
alias net-pf-10 off      # 追加を実施
alias ipv6 off           # 追加を実施
```

変更をしたら、保存して終了します。

③ vi エディタなどのテキストエディタにて設定ファイル /etc/sysconfig/network を開いてください。

```
# vi /etc/sysconfig/network
```

④ 設定ファイルを以下の通り編集してください。

- ・「NETWORKING\_IPV6=yes」と記述された行があれば、「NETWORKING\_IPV6=no」と変更します。
- ・「NETWORKING\_IPV6=no」と記述された行がなければ、追加します。

変更前表示例)

```
NETWORKING=Yes
HOSTNAME=gwtest.canon-its.local
GATEWAY=192.168.1.2
                        # NETWORKING_IPV6=no を追加
```

変更後表示例)

```
NETWORKING=Yes
HOSTNAME=gwtest.canon-its.local
GATEWAY=192.168.1.2
NETWORKING_IPV6=no # 追加を実施
```

変更をしたら、保存して終了します。

⑤ システムの再起動を実施してください。

### (3) hosts ファイルの設定

- ① vi エディタなどのテキストエディタにて設定ファイル /etc/hosts を開いてください。

```
# vi /etc/hosts
```

- ② 設定ファイルを以下の通り編集してください。

- ・ IPv6 の設定は「#」でコメントアウトしてください。
- ・ 自サーバーの IP アドレスとホスト名を登録してください。

<IP アドレス> <FQDN> <ホスト名>

※各項目は tab 区切りでご記入ください。

参考) 自サーバー IP アドレス: 192.168.1.1、FQDN: gwtest.canon-its.local、ホスト名: gwtest の場合

変更前表示例)

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
::1 localhost6.localdomain6 localhost6
# ( 存在すれば ) この行をコメントアウト
127.0.0.1 localhost.localdomain localhost
# 最終行に自サーバー設定を追加
```

変更後表示例)

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
:::1 localhost6.localdomain6 localhost6      # コメントアウトを実施
127.0.0.1 localhost.localdomain localhost
192.168.1.1 gwtest.canon-its.local gwtest      # 追加を実施
```

変更をしたら、保存して終了します。

- ③ システムの再起動を実施してください。
- ④ hostid コマンドで出力結果を確認してください。

確認例 1) hosts に正しく設定できた場合

```
# hostid
a8c08100      ← hostid が出力される
```

確認例 2) hosts が正しく設定できていない場合

```
# hostid
00000000 ← 「0」「00000000」「007f0100」など正常ではない hostid が出力されている
```

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

#### (4) ポート 5432 確認

※本項目は **GUARDIANWALL**（管理サーバー）をインストールするサーバーにのみ実施してください。

① **netstat** コマンドで出力結果を確認してください。

確認例 1) ポート 5432 を利用しているサービスがない（(5)へ進んでください）

```
# netstat -na | grep 5432
#                               ←出力がない
```

確認例 2) ポート 5432 を利用しているサービスがある（(4)-②へ進んでください）

```
# netstat -na | grep 5432
tcp 0 0 127.0.0.1:5432 0.0.0.0:* LISTEN
unix 2 [ ACC ] STREAM LISTENING 343193 /tmp/.s.PGSQL.5432
```

※上記は出力例です。ポート 5432 を利用しているサービスにより表示は異なります。

② ポート 5432 を利用しているサービスがある場合該当サービスを停止してください。

※停止手順については該当サービスを提供しているソフトウェアのサポート窓口にてご確認ください。

#### (5) 言語環境

① **vi** エディタなどのテキストエディタにて設定ファイル **/etc/sysconfig/i18n** を開いてください。

```
# vi /etc/sysconfig/i18n
```

② 設定ファイルを以下の通り編集してください。

- ・EUCJP（英語の場合 C）以外の言語環境の設定値についてはコメントアウトしてください。
- ・EUCJP（英語の場合 C）を登録してください。

参考）言語環境を UTF-8 から EUC-JP に変更する

変更前表示例）

```
LANG="ja_JP.UTF-8"           # この行をコメントアウト
SUPPORTED="ja_JP.UTF-8:ja_JP:ja" # この行をコメントアウト
SYSFONT="latarcyrheb-sun16"
                                # 最終行以降に EUC-JP 設定を追加
```

変更後表示例）

```
#LANG="ja_JP.UTF-8"           # この行をコメントアウト
#SUPPORTED="ja_JP.UTF-8:ja_JP:ja" # この行をコメントアウト
SYSFONT="latarcyrheb-sun16"
LANG="ja_JP.eucJP"           # 追加を実施
LC_ALL="ja_JP.eucJP"         # 追加を実施
LANGUAGE="ja"                 # 追加を実施
SUPPORTED="ja_JP.eucJP:ja_JP:ja" # 追加を実施
```

変更をしたら、「:wq!」と入力して保存して終了します。

- ③ システムの再起動を実施してください。
- ④ echo コマンドで出力結果を確認してください。

確認例 1) 言語環境が正しく設定できた場合

```
# echo $LANG
ja_JP.eucJP      ← EUC-JP 環境に変更されている
```

確認例 2) 言語環境が正しく設定できていない場合

```
# echo $LANG
ja_JP.UTF-8      ← EUC-JP 環境に変更できていない
```

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (6) umask の設定

- ① umask コマンドで出力結果を確認してください。

確認例 1) umask の設定が 0022 に設定されている場合 ((7) へ進んでください)

```
# umask
0022 ← 0022 または 022 と出力される
```

確認例 2) umask の設定が 0022 以外に設定されている場合 ((6) へ進んでください)

```
# umask
0027      ← 0022 または 022 以外の数字が出力される
```

- ② vi エディタなどのテキストエディタにて設定ファイル/etc/bashrc を開いてください。

```
# vi /etc/bashrc
```

- ③ 設定ファイルを以下の通り編集してください。

- ・ umask を 022 に設定してください。

参考) umask を 022 にする

変更前表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 027 # 022 へ変更
fi
(後略)
```

変更後表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 022 # 022 へ変更を実施
fi
(後略)
```

---

変更をしたら、「:wq!」と入力して保存して終了します。

④ システムの再起動を実施してください。

※①から②で変更を実施せず、確認のみ実施した場合、再起動は不要です。

⑤ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (7) 時刻同期

① date コマンドで出力結果を確認し、以下の点を確認してください。

- ・管理サーバーと検査サーバーで時計にずれがないこと。
- ・極端に現在時刻と差異がないこと。

確認例 1) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示される場合

(8) へ進んでください)

```
# date
2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている
```

確認例 2) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示されない場合

(2)へ進んでください)

```
# date
1970 年 1 月 1 日 木曜日 00:00:30 JST ←実行時の日付と極端に差異がある表示になっている
```

② date コマンドで時刻を設定します。

設定例 1) 2012 年 6 月 1 日 14:00 に変更する場合

```
# date 060114002012
2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている
```

③ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (8) MTA 設定

後述する「4 MTA 設定」をご参照いただき、GUARDIANWALL（管理サーバー）をインストールするサーバーからメールが送信できるよう設定してください。

## (9) ディレクトリの作成

『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「1-5 データ保存用ディスク領域」（13 ページ）をご参照いただき、必要なディレクトリを作成してください。

## 3-2 Red Hat Enterprise Linux 5 への導入準備（検査サーバー）

Red Hat Enterprise Linux5.5 がインストールされたサーバーへ GUARDIANWALL（検査サーバー）を導入するために必要な準備について説明します。以下に説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口にてご確認ください。

### (1) 必要パッケージのインストール確認

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(1) 必要パッケージのインストール確認」をご確認ください。

### (2) IPv6 設定の解除

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(2) IPv6 設定の解除」をご確認ください。

### (3) hosts ファイルの設定

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(3) hosts ファイルの設定」をご確認ください。

### (4) 言語環境

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(5) 言語環境」をご確認ください。

### (5) umask の設定

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(6) umask の設定」をご確認ください。

### (6) 時刻同期

前述の「3-1 Red Hat Enterprise Linux 5 への導入準備（管理サーバー）」- 「(7) 時刻同期」をご確認ください。

### (7) ディレクトリの作成

『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「1-5 データ保存用ディスク領域」（13 ページ）をご参照いただき、必要なディレクトリを作成してください。

---

### 3-3 Red Hat Enterprise Linux 6への導入準備(管理サーバー／検査サーバー)

Red Hat Enterprise Linux 6.5 がインストールされたサーバーへ GUARDIANWALL (管理サーバー／検査サーバー) を導入するために必要な準備を例に、Red Hat Enterprise Linux への設定手順例を説明します。以下に説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口にてご確認ください。

#### (1) 必要パッケージのインストール確認

- ① サーバーへ管理者権限を持つユーザーでログインしてください。
- ② 必要パッケージ `compat-db` (32bit パッケージ) がインストールされているかご確認ください。

確認例 1) `compat-db` がインストールされている場合

```
# rpm -qa | grep compat-db
compat-db-4.6.21-15      ←パッケージ名が表示される
#
```

確認例 2) `compat-db` がインストールされていない場合

```
# rpm -qa | grep compat-db
#                        ←パッケージ名が表示されず終了する
```

- ③ パッケージがインストールされていない場合、OS のインストール CD を利用してインストールを実施してください。インストール方法については OS の保守担当窓口へご確認ください。
- ④ 同様に以下のパッケージがインストールされているかご確認ください。  
`compat-expat1` (32bit パッケージ) ,`compat-libstdc++-33` (32bit パッケージ) ,  
`cyrus-sasl-lib` (32bit パッケージ) ,`libuuid` (32bit パッケージ) ,`mt-st`,  
`ncurses-libs` (32bit パッケージ) ,`tcl`,`at`



32bit パッケージはパッケージ名末尾が「.i686」となっているパッケージです。

---

#### (2) IPv6 設定の解除

GUARDIANWALL (管理サーバー／検査サーバ) は IPv6 に対応しておりません。ここでは IPv6 設定の解除手順を説明します。

- ① `vi` エディタなどのテキストエディタにて設定ファイル `/etc/modprobe.d/ipv6.conf` を開いてください。ファイルが存在しない場合、新規に作成します。

```
# vi /etc/modprobe.d/ipv6.conf
```

- ② 設定ファイルを以下の通り編集してください。
  - ・「`options ipv6 disable=1`」と記述された行が無ければ、追加します。

変更後表示例)

```
options ipv6 disable=1 # 追加を実施
```

変更をしたら、保存して終了します。

- ③ vi エディタなどのテキストエディタにて設定ファイル `/etc/sysconfig/networkscripts/ifcfg-eth0` を開いてください。

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- ④ 設定ファイルを以下の通り編集してください。

- ・「`IPV6INIT=yes`」と記述された行があれば、削除します。
- ・「`IPV6INIT=no`」と記述された行が無ければ、追加します。

変更前表示例)

```
IPV6INIT=yes # (存在すれば) この行をコメントアウト
```

変更後表示例)

```
#IPV6INIT=yes  
IPV6INIT=no # 追加を実施
```

変更をしたら、保存して終了します。

### (3) ファイヤーウォール設定の解除

- ① iptables のサービスが起動していれば、停止します。

```
# service iptables stop
```

- ② ip6tables のサービスが起動していれば、停止します。

```
# service ip6tables stop
```

- ③ iptables のサービスが自動起動しないよう、停止します。

```
# chkconfig iptables off
```

- ④ ip6tables のサービスが自動起動しないよう、停止します。

```
# chkconfig ip6tables off
```

### (4) SELinux 設定の解除

- ① vi エディタなどのテキストエディタにて設定ファイル `/etc/selinux/conf` を開いてください。

- ② 設定ファイルを以下の通り編集してください。

- ・「`SELINUX=enforcing`」と記述された行があれば、削除します。
- ・「`SELINUX=disabled`」と記述された行が無ければ、追加します。



変更前表示例)

```
SELINUX=enforcing # (存在すれば) この行をコメントアウト  
SELINUXTYPE=targeted
```

変更後表示例)

```
#SELINUX=enforcing  
SELINUX=disabled # 追加を実施  
SELINUXTYPE=targeted
```

変更をしたら、保存して終了します。

## (5) hosts ファイルの設定

① vi エディタなどのテキストエディタにて設定ファイル /etc/hosts を開いてください。

```
# vi /etc/hosts
```

② 設定ファイルを以下の通り編集してください。

- ・ IPv6 の設定は「#」でコメントアウトしてください。
- ・ 自サーバーの IP アドレスとホスト名を登録してください。

<IP アドレス> <FQDN> <ホスト名>

※各項目は tab 区切りでご記入ください。

参考) 自サーバー IP アドレス: 192.168.1.1、FQDN: gwtest.canon-its.local、ホスト名: gwtest の場合

変更前表示例)

```
# Do not remove the following line, or various programs  
# that require network functionality will fail.  
::1 localhost6.localdomain6 localhost6 # (存在すれば) この行をコメントアウト  
127.0.0.1 localhost.localdomain localhost  
# 最終行に自サーバー設定を追加
```

変更後表示例)

```
# Do not remove the following line, or various programs  
# that require network functionality will fail.  
::1 localhost6.localdomain6 localhost6  
127.0.0.1 localhost.localdomain localhost  
192.168.1.1 gwtest.canon-its.local gwtest # 追加を実施
```

変更をしたら、保存して終了します。

③ システムの再起動を実施してください。

④ hostid コマンドで出力結果を確認してください。

確認例 1) hosts に正しく設定できた場合

```
# hostid  
a8c08100 ← hostid が出力される
```

確認例 2) hosts が正しく設定できていない場合

```
# hostid
00000000 ← 「0」「00000000」「007f0100」など正常ではない hostid が出力されている
```

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (6) ポート 5432 確認

※本項目は **GUARDIANWALL**（管理サーバー）をインストールするサーバーにのみ実施してください。

① netstat コマンドで出力結果を確認してください。

確認例 1) ポート 5432 を利用しているサービスがない (7) へ進んでください)

```
# netstat -na | grep 5432
#                               ←出力がない
```

確認例 2) ポート 5432 を利用しているサービスがある (2) へ進んでください)

```
# netstat -na | grep 5432
tcp 0 0 127.0.0.1:5432 0.0.0.0:* LISTEN
unix 2 [ ACC ] STREAM LISTENING 343193 /tmp/.s.PGSQL.5432
```

※上記は出力例です。ポート 5432 を利用しているサービスにより表示は異なります。

② ポート 5432 を利用しているサービスがある場合該当サービスを停止してください。  
※停止手順については該当サービスを提供しているソフトウェアのサポート窓口にてご確認ください。

## (7) 言語環境

① vi エディタなどのテキストエディタで設定ファイル /etc/sysconfig/i18n を開いてください。

```
# vi /etc/sysconfig/i18n
```

② 設定ファイルを以下の通り編集してください。

- ・EUCJP（英語の場合 C）以外の言語環境の設定値についてはコメントアウトしてください。
- ・EUCJP（英語の場合 C）を登録してください。

参考) 言語環境を UTF-8 から C に変更する

変更前表示例)

```
LANG="ja_JP.UTF-8"      # (存在すれば) この行をコメントアウト
```

変更後表示例)

```
#LANG="ja_JP.UTF-8"
LANG="C"                # 追加を実施
```

変更をしたら、保存して終了します。

- 
- ③ システムの再起動を実施してください。
- ④ `echo` コマンドで出力結果を確認してください。

確認例 1) 言語環境が正しく設定できた場合

```
# echo $LANG
C          ← C 環境に変更されている
```

確認例 2) 言語環境が正しく設定できていない場合

```
# echo $LANG
ja_JP.UTF-8    ← C 環境に変更できていない
```

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (8) `umask` の設定

- ① `umask` コマンドで出力結果を確認してください。

確認例 1) `umask` の設定が `0022` に設定されている場合 (⑨) へ進んでください)

```
# umask
0022          ← 0022 または 022 と出力される
```

確認例 2) `umask` の設定が `0022` 以外に設定されている場合 (②) へ進んでください)

```
# umask
0027          ← 0022 または 022 以外の数字が出力される
```

- ② `vi` エディタなどのテキストエディタにて設定ファイル `/etc/bashrc` を開いてください。

```
# vi /etc/bashrc
```

- ③ 設定ファイルを以下の通り編集してください。

- `umask` を `022` に設定してください。

参考) `umask` を `022` にする

変更前表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 027 # 022 へ変更
fi
(後略)
```

変更後表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 022 # 022 へ変更を実施
fi
(後略)
```

変更をしたら、「:wq!」と入力して保存して終了します。

④ システムの再起動を実施してください。

※①から②で変更を実施せず、確認のみ実施した場合、再起動は不要です。

⑤ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (9) 時刻同期

① `date` コマンドで出力結果を確認し、以下の点を確認してください。

- ・ 管理サーバーと検査サーバーで時計にずれがないこと
- ・ 極端に現在時刻と差異がないこと

確認例 1) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示される場合 ((10) へ進んでください)

```
# date
2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている
```

確認例 2) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示されない場合 ((2)へ進んでください)

```
# date
1970 年 1 月 1 日 木曜日 00:00:30 JST ←実行時の日付と極端に差異がある表示になっている
```

② `date` コマンドで時刻を設定します。

設定例 1) 2012 年 6 月 1 日 14:00 に変更する場合

```
# date 060114002012
2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている
```

③ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (10) MTA 設定

後述する「4 MTA 設定」をご参照いただき、GUARDIANWALL (管理サーバー) をインストールするサーバーからメールが送信できるよう設定してください。

## (11) ディレクトリの作成

『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「1-5 データ保存用ディスク領域」(13 ページ)をご参照いただき、必要なディレクトリを作成してください。

---

### 3-4 Red Hat Enterprise Linux 7への導入準備(管理サーバー／検査サーバー)

Red Hat Enterprise Linux 7.1 がインストールされたサーバーへ GUARDIANWALL (管理サーバー／検査サーバー) を導入するために必要な準備を例に、Red Hat EnterpriseLinux への設定手順例を説明します。以下に説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口にてご確認ください。

#### (1) 必要パッケージのインストール確認

① サーバーへ管理者権限を持つユーザーでログインしてください。

② 必要パッケージ `compat-db` (32bit パッケージ) がインストールされているかご確認ください。

確認例 1) `compat-db` がインストールされている場合

```
# rpm -qa | grep compat-db
compat-db47-4.7.25-28.el7.i686 ←パッケージ名が表示される
#
```

確認例 2) `compat-db` がインストールされていない場合

```
# rpm -qa | grep compat-db
# ←パッケージ名が表示されず終了する
```

③ パッケージがインストールされていない場合、OS のインストール CD を利用してインストールを実施してください。インストール方法については OS の保守担当窓口へご確認ください。

④ 同様に以下のパッケージがインストールされているかご確認ください。

`compat-db-headers`, `nss-softokn-freebl` (32bit パッケージ) , `glibc` (32bit パッケージ) , `libstdc++` (32bit パッケージ) , `libgcc` (32bit パッケージ) , `expat` (32bit パッケージ) , `libdb` (32bit パッケージ) , `libuuid` (32bit パッケージ) , `ncurses-libs` (32bit パッケージ) , `bzip2-libs` (32bit パッケージ) (※1), `mt-st`, `tcl`, `at` (※2)

(※1) 添付ファイル ZIP 暗号化機能で「暗号化 ZIP +パスワード」をご利用される場合にのみ必要です。

(※2) 管理サーバーをインストールされる場合に必要です。



32bit パッケージはパッケージ名末尾が「`i686`」となっているパッケージです。

---

#### (2) IPv6 設定の解除

GUARDIANWALL (管理サーバー／検査サーバ) は IPv6 に対応していません。ここでは IPv6 設定の解除手順を説明します。

- ① vi エディタなどのテキストエディタにて設定ファイル /etc/sysctl.conf を開いてください。ファイルが存在しない場合、新規に作成します。

```
# vi /etc/sysctl.conf
```

- ② 設定ファイルを以下の通り編集してください。

「net.ipv6.conf.all.disable\_ipv6=1」と記述された行が無ければ、追加します  
変更後表示例)

```
net.ipv6.conf.all.disable_ipv6=1 # 追加を実施
```

- ③ システムの再起動を実施してください。

### (3) ファイヤーウォール設定の解除

- ① firewalld のサービスが起動していれば、停止します。

```
# systemctl stop firewalld.service
```

- ② firewalld のサービスが自動起動しないよう、停止します。

```
# systemctl disable firewalld.service
```

### (4) SELinux 設定の解除

- ① vi エディタなどのテキストエディタにて設定ファイル /etc/selinux/config を開いてください。

```
# vi /etc/selinux/config
```

- ② 設定ファイルを以下の通り編集してください。

- ・「SELINUX=enforcing」と記述された行があれば、削除します。
- ・「SELINUX=disabled」と記述された行が無ければ、追加します。

変更前表示例)

```
SELINUX=enforcing # ( 存在すれば ) この行をコメントアウト  
SELINUXTYPE=targeted
```

変更後表示例)

```
#SELINUX=enforcing  
SELINUX=disabled # 追加を実施  
SELINUXTYPE=targeted
```

変更をしたら、保存して終了します。

- ③ システムの再起動を実施してください。

---

## (5) hosts ファイルの設定

- ① vi エディタなどのテキストエディタにて設定ファイル/etc/hosts を開いてください。

```
# vi /etc/hosts
```

- ② 設定ファイルを以下の通り編集してください。

- IPv6 の設定は「#」でコメントアウトしてください。
- 自サーバーの IP アドレスとホスト名を登録してください。

＜IP アドレス＞ ＜FQDN＞ ＜ホスト名＞

※各項目は tab 区切りでご記入ください。

参考) 自サーバー IP アドレス:192.168.1.1、FQDN:gwtest.canon-its.local、ホスト名:  
gwtest の場合

変更前表示例)

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
# ( 存在すれば ) この行をコメントアウト
# 最終行に自サーバー設定を追加
```

変更後表示例)

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
#::1        localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.1.1 gwtest.canon-its.local gwtest # 追加を実施
```

変更をしたら、保存して終了します。

- ③ システムの再起動を実施してください。
- ④ hostid コマンドで出力結果を確認してください。

確認例 1) hosts に正しく設定できた場合

```
# hostid
a8c08100 ← hostid が出力される
```

確認例 2) hosts が正しく設定できていない場合

```
# hostid
00000000 ← 「0」「00000000」「007f0100」など正常ではない hostid が出力されている
```

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (6) ポート 5432 確認

※本項目は GUARDIANWALL (管理サーバー) をインストールするサーバーにのみ実施してください。

- ① ss コマンドで出力結果を確認してください。

確認例 1) ポート 5432 を利用しているサービスがない (7) へ進んでください)

```
# ss -na | grep 5432
#          ←出力がない
```

確認例 2) ポート 5432 を利用しているサービスがある (2) へ進んでください)

```
# ss -na | grep 5432
u_str LISTEN  0    128   /var/run/postgresql/.s.PGSQL.5432 22054972      * 0
u_str LISTEN  0    128   /tmp/.s.PGSQL.5432 22054974      * 0
tcp   LISTEN  0    128   127.0.0.1:5432      *.*
```

※上記は出力例です。ポート 5432 を利用しているサービスにより表示は異なります。

② ポート 5432 を利用しているサービスがある場合該当サービスを停止してください。

※停止手順については該当サービスを提供しているソフトウェアのサポート窓口にてご確認ください。

## (7) 言語環境

① 言語環境が EUCJP (英語の場合 C) であることを確認してください。

確認例 1) 言語環境が EUCJP (英語の場合 C) である (8) へ進んでください)

```
# localectl status
System Locale: LANG=ja_JP.EUC-JP ←システムロケールが EUCJP である
```

確認例 2) 言語環境が EUCJP (英語の場合 C) でない

```
# localectl status
System Locale: LANG=ja_JP.UTF-8 ←システムロケールが EUCJP でない
```

② 言語環境が EUCJP (英語の場合 C) に変更してください。

```
# localectl set-locale LANG=ja_JP.EUC-JP ← EUCJP に変更する場合
# localectl set-locale LANG=C ← C に変更する場合
```

③ ①を実施し、言語環境が変更されたことを確認してください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (8) umask の設定

① umask コマンドで出力結果を確認してください。

確認例 1) umask の設定が 0022 に設定されている場合 (9) へ進んでください)

```
# umask
0022 ← 0022 または 022 と出力される
```

確認例 2) umask の設定が 0022 以外に設定されている場合 (2) へ進んでください)

```
# umask
0027 ← 0022 または 022 以外の数字が出力される
```



- ② vi エディタなどのテキストエディタにて設定ファイル `/etc/bashrc` を開いてください。

```
# vi /etc/bashrc
```

- ③ 設定ファイルを以下の通り編集してください。

- `umask` を `022` に設定してください。

変更前表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 027 # 022 へ変更
fi
(後略)
```

変更後表示例)

```
(前略)
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 022 # 022 へ変更を実施
fi
(後略)
```

変更をしたら、「`:wq!`」と入力して保存して終了します。

- ④ システムの再起動を実施してください。

※①から②で変更を実施せず、確認のみ実施した場合、再起動は不要です。

- ⑤ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

## (9) 時刻同期

- ① `date` コマンドで出力結果を確認し、以下の点を確認してください。

- 管理サーバーと検査サーバーで時計にずれがないこと
- 極端に現在時刻と差異がないこと

確認例 1) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示される場合 ((10) へ進んでください)

```
# date
2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている
```

確認例 2) 2012 年 6 月 1 日 14:00 に確認し、時刻が正しく表示されない場合 ((2) へ進んでください)

```
# date
1970 年 1 月 1 日 木曜日 00:00:30 JST ←実行時の日付と極端に差異がある表示になっている
```

② **date** コマンドで時刻を設定します。

設定例 1) 2012 年 6 月 1 日 14:00 に変更する場合

<pre># date 060114002012 2012 年 6 月 1 日 木曜日 14:00:18 JST ←実行時の日付が正しく表示されている</pre>
---

③ ①を実施し、正しく設定されたことをご確認ください。

※設定後も正しく変更ができていない場合、OS の保守担当窓口へご相談ください。

#### (10) MTA 設定

後述する「4 MTA 設定」をご参照いただき、GUARDIANWALL（管理サーバー）をインストールするサーバーからメールが送信できるよう設定してください。

#### (11) ディレクトリの作成

『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「1-5 データ保存用ディスク領域」（13 ページ）をご参照いただき、必要なディレクトリを作成してください。

## 4 MTA 設定

GUARDIANWALL の運用に必要な MTA の導入例を説明します。

GUARDIANWALL は sendmail、postfix、qmail に対応していますが、本章では、3 つの MTA のうち sendmail、postfix の導入例を説明します。これより説明する導入例は GUARDIANWALL をインストールするために必要な最低限の項目ですので、導入環境や運用ポリシーにより必要な設定や手順を追加してください。詳細については『**管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』をご参照ください。

また、GUARDIANWALL での受信メールサイズ制限について、MTA 側でサイズ制限を行うと正常に配送できない場合がありますので、MTA 側ではサイズを無制限に設定し、GUARDIANWALL 側でサイズ制限を設定してください。

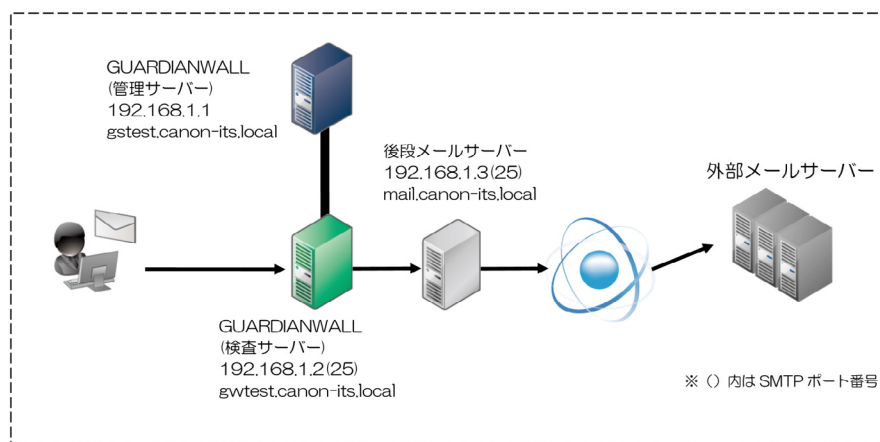
GUARDIANWALL 側でのサイズ制限の設定については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』の「3-3-5-1 基本設定」-【拡張】の「最大メッセージ受信サイズ」(254 ページ)をご参照ください。

### 4-1 sendmail

sendmail を MTA とする環境に GUARDIANWALL を導入するために必要な準備について、以下の環境への導入を例に説明します。

sendmail-8.13.8 (Red Hat Enterprise Linux 5.5 同梱版)

※ Red Hat Enterprise Linux 6.5 をご利用の場合、sendmail のバージョンは sendmail-8.14.4 です。設定は sendmail-8.13.8 と同様になります。



本項目で説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口にてご確認ください。

## (1) 設定ファイル /etc/mail/sendmail.mc を編集

(vi エディタなどのテキストエディタで編集してください)

- ・サーバーのホスト名、ドメイン名を設定してください。
- ・変更後表示例に記載がなく、お客様環境の sendmail.mc に記載のある行は文頭に「dn!」と追加しコメントアウトしてください。
- ・変更後表示例に記載があるが、お客様環境の sendmail.mc に記載のない行は新たに追加してください。

参考) 自サーバーの FQDN : gwtest.canon-its.local、ホスト名 : gwtest、後段メールサーバーの IP : 192.168.1.3 の場合

変更後表示例)

```
divert(-1)dn!
include(`/usr/share/sendmail-cf/m4/cf.m4')dn!
VERSIONID(`setup for linux')dn!
OSTYPE(`linux')dn!
Dwgtest # 追記、自サーバーのホスト名を設定してください。
Dmexample.co.jp # 追記、自サーバーのドメイン名を設定してください。
define(`confDOMAIN_NAME', `$. $m')dn! # 追記
define(`SMART_HOST', `smtp:[192.168.1.3]')dn!
# ↑ 追記、メールの中継先 IP アドレスを設定してください。
define(`confDEF_USER_ID', ``8:12'')dn!
define(`PROCMAIL_MAILER_PATH', `/usr/bin/procmail')dn!
define(`ALIAS_FILE', `/etc/aliases')dn!
define(`STATUS_FILE', `/var/log/mail/statistics')dn!
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dn!
define(`confPRIVACY_FLAGS', `authwarnings, novrfy, noexpn, restrictqrun')dn!
define(`confAUTH_OPTIONS', `A')dn!
define(`confTO_IDENT', `0')dn!
define(`confSERVICE_SWITCH_FILE', `/etc/mail/service.switch')dn! # 追記
FEATURE(`no_default_msa', `dn!')dn!
FEATURE(`smrsh', `/usr/sbin/smrsh')dn!
FEATURE(`mailertable', `hash -o /etc/mail/mailertable.db')dn!
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dn!
FEATURE(redirect)dn!
FEATURE(always_add_domain)dn!
FEATURE(use_cw_file)dn!
FEATURE(use_ct_file)dn!
FEATURE(`nocanonify')dn! # 追記
FEATURE(local_procmail, ``', `procmail -t -Y -a $h -d $u')dn!
EXPOSED_USER(`root')dn!
dn! DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dn! # (※1)
FEATURE(`accept_unqualified_senders')dn!
FEATURE(`accept_unresolvable_domains')dn!
MAILER(smtp)dn!
MAILER(procmail)dn!
```

(※1)「DAEMON\_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dn!」がある場合は上記変更後表示例と同様に文頭に「dn!」を挿入し、無い場合は上記記入例と同様に文頭に「dn!」が挿入された状態で追記します。

※詳細な記述方法については sendmail のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

---

## (2) cf ファイルの作成

```
# make -C /etc/mail
```

## (3) sendmail の再起動

```
# /etc/init.d/sendmail stop
```

※ sendmail サービスが停止します

```
# /etc/init.d/sendmail start
```

※ sendmail サービスが起動します

## (4) 中継を許可するドメイン / ネットワークの設定

- ① vi エディタなどのテキストエディタにて設定ファイル `/etc/mail/ relay-domains` を作成し、開いてください。

```
# vi /etc/mail/ relay-domains
```

- ② 設定ファイルを以下の通り編集してください。

- ・ 自サーバーがメールの中継を許可するドメイン名またはネットワークを設定します。

参考) `canon-its.local` ドメインのメール及び `192.168.1.0/24` からのメールの中継を許可する場合

変更前表示例)

```
# ドメイン名を追加  
# ネットワークを追加
```

変更後表示例)

```
canon-its.local # 追加を実施  
192.168.1      # 追加を実施
```

※詳細な記述方法については `sendmail` のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

## (5) 中継先の設定

- ① vi エディタなどのテキストエディタにて設定ファイル `/etc/mail/mailertable` を開いてください。

```
# vi /etc/mail/mailertable
```

② 設定ファイルを以下の通り編集してください。

- ・ GUARDIANWALL を中継後、送付先となる MTA を設定してください。

参考) GUARDIANWALL でのフィルタリング後、後段 MTA (IP アドレス 192.168.1.3) へ中継する場合

変更前表示例)

```
# ドメイン名、送付先 MTA を追加
```

変更後表示例)

```
canon-its.local smtp:[192.168.1.3] # 追加を実施
```

※詳細な記述方法については sendmail のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

③ db ファイルの作成

```
#usr/sbin/makemap hash /etc/mail/mailertable.db < /etc/mail/mailertable
```

④ 「(3) sendmail の再起動」を参照し sendmail の再起動を実施してください。

## (6) DNS 非参照の設定

① vi エディタなどのテキストエディタにて設定ファイル /etc/mail/service.switch を開いてください。

```
# vi /etc/mail/service.switch
```

② 設定ファイルを以下の通り編集してください。

- ・ 名前解決の際、DNS を参照しない設定を追加してください。

参考)

変更前表示例)

```
# 参照先に hosts、files を追加
```

変更後表示例)

```
hosts files # 追加を実施
```

※詳細な記述方法については sendmail のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

③ 「(3) sendmail の再起動」を参照し sendmail の再起動を実施してください。

---

## (7) root 宛てメールの配送先の設定

- ① vi エディタなどのテキストエディタにて設定ファイル `/etc/mail/aliases` を開いてください。

```
# vi /etc/mail/aliases
```

- ② 設定ファイルを以下の通り編集してください。

- root 宛てのメールを管理者へ送付する設定を追加してください。

参考)

変更前表示例)

```
# Person who should get root's mail
# root: marc      ←コメントアウトを外し「marc」を管理者メールアドレスへ変更
```

変更後表示例)

```
# Person who should get root's mail
root: admin@canon-its.local    ←管理者メールアドレスへの変更を実施
```

※詳細な記述方法については `sendmail` のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

- ③ `aliases` ファイルの作成

```
# /usr/bin/newaliases
```

- ④ 「(3) `sendmail` の再起動」を参照し `sendmail` の再起動を実施してください。

## (8) 動作確認

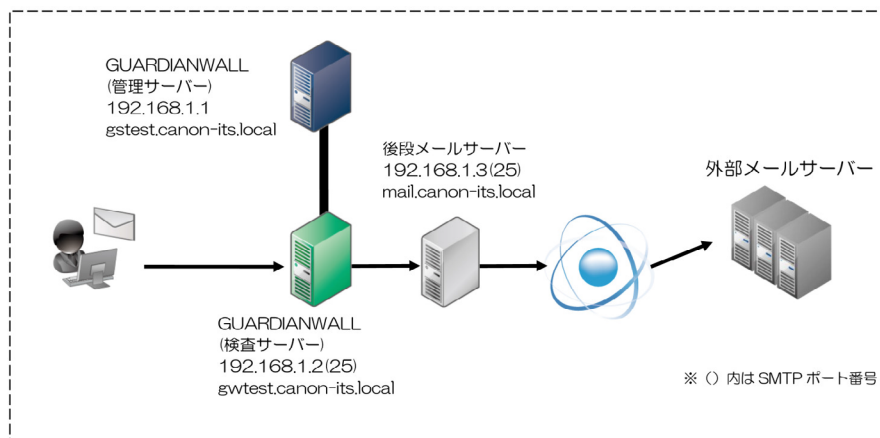
**GUARDIANWALL** インストール前に、メーラーからメールが送付できることをご確認ください。

## 4-2 postfix

postfix を MTA とする環境に GUARDIANWALL（検査サーバー）を導入するために必要な準備について、以下の環境への導入を例に説明します。

postfix 2.3.3-2.1.el5\_2（Red Hat Enterprise Linux 5.5 同梱版）

※ Red Hat Enterprise Linux 6.5 をご利用の場合、postfix のバージョンは postfix 2.6.6-2.2.el6\_1 です。設定は postfix 2.3.3-2.1.el5\_2 と同様になります。



本項目で説明する手順についてはお客様環境によりそのままご利用いただけない場合があります。設定方法の詳細については OS の保守担当窓口へご確認ください。

### (1) 設定ファイル /etc/postfix/main.cf を編集

(vi エディタなどのテキストエディタで編集してください)

- ・サーバーのホスト名、ドメイン名を設定してください。
- ・変更後表示例に記載がなく、お客様環境の main.cf に記載のある行は文頭に「#」と追加しコメントアウトしてください。
- ・変更後表示例に記載があるが、お客様環境の main.cf に記載のない行は新たに追加してください。



参考) 自サーバーの FQDN : gwtest.canon-its.local、後段メールサーバーの IP : 192.168.1.3 の場合  
変更後表示例)

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
mail_owner = postfix
myhostname = gwtest.canon-its.local
mydomain = canon-its.local
myorigin = $myhostname
inet_interfaces = localhost
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
mynetworks_style = host
relayhost = [192.168.1.3]
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
debug_peer_level = 2
debugger_command =
PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.3.3/samples
readme_directory = /usr/share/doc/postfix-2.3.3/README_FILE
disable_dns_lookups = yes
message_size_limit = 0    ←メールサイズを無制限に設定する
mailbox_size_limit = 0    ←メールサイズを無制限に設定する
```

※詳細な記述方法については postfix のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

## (2) postfix の再起動

```
# /etc/init.d/postfix stop
```

※ postfix サービスが停止します

```
# /etc/init.d/postfix start
```

※ postfix サービスが起動します

### (3) デフォルト MTA の変更

- ① alternatives コマンドを以下の通り実行してください。

```
# alternatives --config mta
```

- ② 以下の表示が出力されたら「2」を選択し、Enter を押下してください。

```
2 プログラムがあり 'mta' を提供します。
選択 コマンド
-----
* 1 /usr/sbin/sendmail.sendmail
+ 2 /usr/sbin/sendmail.postfix
Enter を押して現在の選択 [+] を保持するか、選択番号を入力します：
```

- ③ chkconfig コマンドにて設定確認

- 確認例 1) postfix が on になっている場合 (⑥ へ進んでください)

```
# chkconfig --list | grep postfix
postfix 0:off 1:off 2:on 3:on 4:on 5:on ← 3 と 5 で on になっている
```

- 確認例 2) postfix が on になっていない場合 (④ へ進んでください)

```
# chkconfig --list | grep postfix
postfix 0:off 1:off 2:off 3:off 4:off 5:off ← すべて off になっている
```

- ④ postfix の起動設定

```
# chkconfig postfix on
```

- ⑤ ③を実施し postfix が on になったことを確認してください。

- ⑥ sendmail の停止設定

```
# chkconfig sendmail off
```

- ⑦ chkconfig コマンドにて設定確認

- 確認例 1) sendmail が on になっている場合 (⑥へ進んでください)

```
# chkconfig --list | grep sendmail
sendmail 0:off 1:off 2:on 3:on 4:on 5:on ← 3 と 5 で on になっている
```

- 確認例 2) sendmail が on になっていない場合 (⑧へ進んでください)

```
# chkconfig --list | grep sendmail
sendmail 0:off 1:off 2:off 3:off 4:off 5:off ← すべて off になっている
```

- ⑧ sendmail の停止

```
# /etc/init.d/sendmail stop
```

---

#### (4) root 宛てメールの配送先の設定

- ① vi エディタなどのテキストエディタにて設定ファイル `/etc/mail/aliases` を開いてください。

```
# vi /etc/mail/aliases
```

- ② 設定ファイルを以下の通り編集してください。

・名前解決の際、DNS を参照しない設定を追加してください。

参考)

変更前表示例)

```
# Person who should get root's mail
# root: marc      ←コメントアウトを外し「marc」を管理者メールアドレスへ変更
```

変更後表示例)

```
# Person who should get root's mail
root: admin@canon-its.local      # 追加を実施
```

※詳細な記述方法については `sendmail` のマニュアル及び各種リファレンスをご確認ください。

変更をしたら、「:wq!」と入力して保存して終了します。

- ③ `aliases` ファイルの作成

```
# /usr/bin/newaliases
```

- ④ 「(2) postfix の再起動」を参照し Postfix の再起動を実施してください。

#### (5) 動作確認

GUARDIANWALL インストール前に、メーラーからメールが送付できることをご確認ください。

#### (6) master.cf の設定

※本項目は GUARDIANWALL (検査サーバー) をインストールするサーバーにのみ実施してください。

『管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「2-8 Postfix がインストールされている場合」(36 ページ) をご参照いただき、`master.cf` の編集をしてください。

## 5 暗号化モジュール導入の手引き

添付ファイル暗号化設定で「暗号化 ZIP+ パスワード」を使用可能にする暗号化モジュールのインストール手順を説明します。暗号化モジュールをインストールすることによって、強固な AES256bit の暗号化による添付ファイル送信が可能になります。

### (1) ライセンスについて

暗号化モジュールの SecureZIP のライセンスには、評価版と製品版の 2 種類があります。評価版はインストールから 30 日間、使用することが可能となっています。製品版は評価版に製品ライセンスを登録することによって、継続して使用可能になりますので、まずは評価版にて動作をご評価いただいてから製品版をご使用いただくことを推奨します。

### (2) インストール準備

暗号化モジュールを検査サーバー上に用意してください。

暗号化モジュールをお持ちでない場合は、ダウンロード URL をご案内致しますので、サポート窓口へお問い合わせください。

なお、ダウンロードには以下の情報が必要になりますので事前にご準備ください。

- ・ダウンロード申請者情報
  - 会社名 / 組織名 (必須)
  - 部署名
  - 担当者名 (必須)
  - Email (必須)
  - 電話番号

### (3) インストール方法

#### ① インストール

root ユーザーで以下のコマンドを実行して用意したプログラムをインストールします。

```
# rpm -i <filename>.rpm
```

#### ② パッケージの確認

以下のコマンドを実行してパッケージが正常にインストールされていることを確認できます。

```
# rpm -q PKZIP_Server  
PKZIP_Server-12.50.0016-1  
#
```

以上で、モジュールのインストールは完了です。次に使用するライセンスに合わせて、ライセンス登録を実施してください。

---

#### (4) ライセンス登録

##### ・ 評価版

root ユーザーで、以下のコマンドを実行すると、使用許諾が表示されますので、スペースキーで全てを表示させ、最後に同意（Yes を入力）すると評価版を使用できます。

※評価期間（インストールから 30 日）を経過した場合、暗号化メール送信ができなくなり、エラーメールが送信者へ返信されるのでご注意ください。

```
# pkzipc -license
```

##### ・ 製品版

※評価版から製品版へ変更時も同じ操作になります。

※ライセンスキーは暗号化モジュールをご購入後弊社よりご案内させていただきます。

root ユーザーで、以下のコマンドを実行してライセンスキーを登録します。

評価版の使用許諾登録同様にして、使用許諾へ同意の後、ライセンスキーを登録してください。

```
# pkzipc -enterlicense
```

以上で、ライセンス登録は完了となります。特にサービスの再起動は発生しません。

#### (5) アンインストール方法

root ユーザーで、以下のコマンドを実行してアンインストールをします。

```
# rpm -e PKZIP_Server
```

以上で、暗号化モジュールのアンインストールが完了となります。