

GUARDIANSUITE

検査サーバー 導入の手引き

～WEBGUARDIAN 導入事前準備～

Copyright©2015 Canon IT Solutions Inc.

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。

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

2015-Mar-01 WEBGUARDIAN V4.0

MEMO

WEBGUARDIAN をご利用いただくために、準備していただくことを以下に説明します。
GUARDIANSUITE の導入作業を行う前にご用意ください。

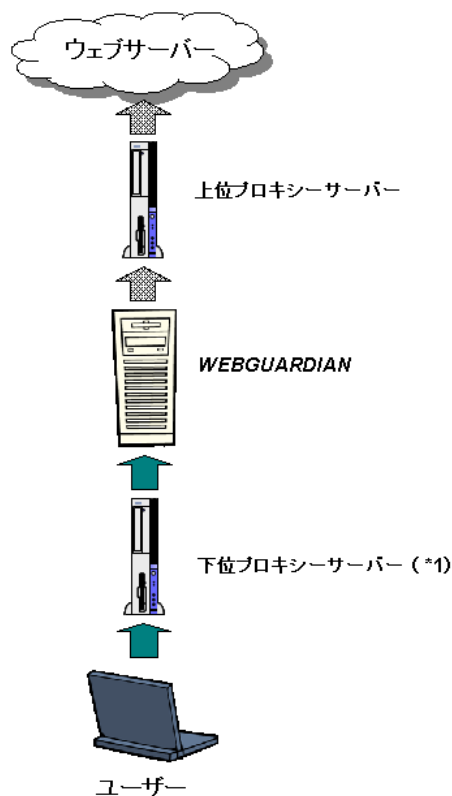
※ WEBGUARDIAN システムはウェブリクエスト検査を実施する「**検査サーバー**」と検査サーバーの設定操作やログ閲覧操作を受け付ける「**管理サーバー (SUITE)**」から構成されています。以降の文中で特に明示されていない場合は、「WEBGUARDIAN」は「WEBGUARDIAN の検査サーバー」を意味します。

1 システム構成の設計

1-1 プロキシサーバー構成

WEBGUARDIAN は、HTTP、HTTPS、FTP プロトコルをサポートするプロキシサーバーとして動作します。ポリシー制御機能を適用したいユーザーのウェブアクセスが WEBGUARDIAN を経由するように、WEBGUARDIAN を組織内ネットワークで適切に設置する必要があります。

● 基本プロキシ構成図



(*1) のように WEBGUARDIAN の下位にプロキシサーバーが存在する場合は、WEBGUARDIAN が認識するクライアント IP アドレスは下位プロキシサーバーの IP アドレスになりますのでご注意ください。ユーザーの利用端末の IP アドレスをポリシー制御の条件にしたい場合は、ユーザー端末が WEBGUARDIAN へ直接アクセスする構成にする必要があります。



下位プロキシサーバーが X-Forwarded-For ヘッダーでユーザーの利用端末の IP アドレスを WEBGUARDIAN に送信することで、下位プロキシサーバーが存在する場合にも WEBGUARDIAN でユーザーの利用端末の IP アドレスをポリシー制御の条件にすることが可能です。

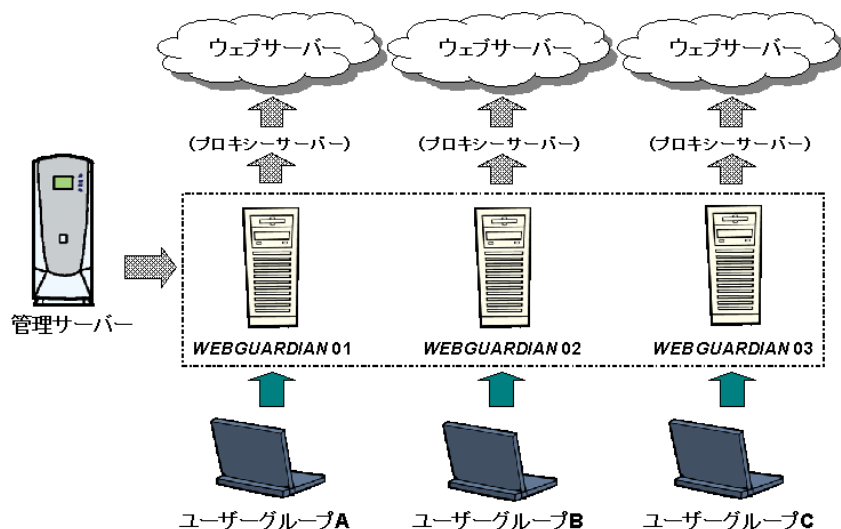
詳細については、『検査サーバー 利用の手引き ～ WEBGUARDIAN V4.0 編 (ウェブ) ～』の「5-6 プロキシ多段構成時の設定」-「(1) WEBGUARDIAN の下位にプロキシサーバーが存在する場合」(78 ページ) をご参照ください。

1-2 複数台構成のケース

ウェブアクセスが大量にある環境に対応するために、WEBGUARDIAN を複数台構成にすることが可能です。

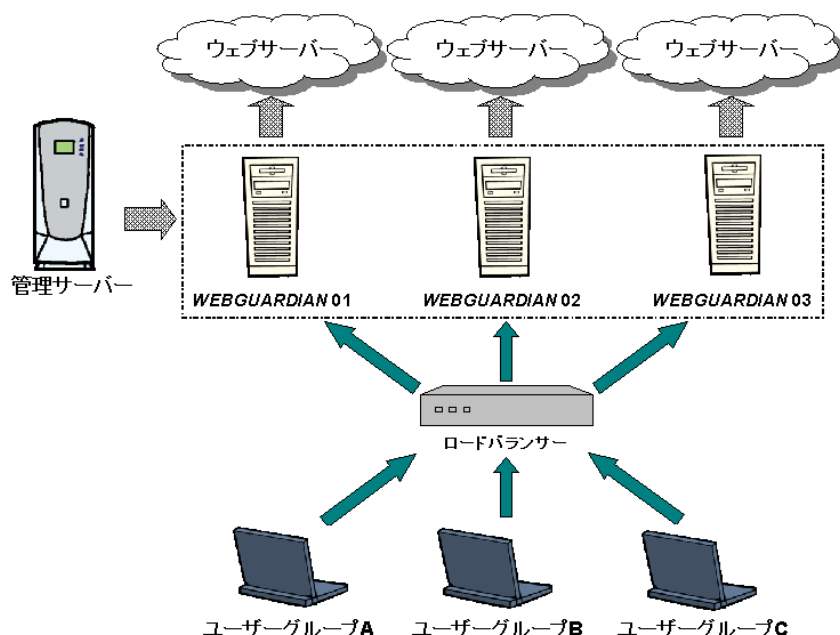
またすでにプロキシサーバーを複数台並列配置されている場合などには、並列配置されている各々のプロキシサーバーの下位プロキシとして、それぞれ WEBGUARDIAN1 台を配置することを推奨します。

● 複数台時の構成図



このように WEBGUARDIAN の複数台を並列配置した場合でも、SUITE 管理サーバーホスト 1 台を導入すれば、ポリシー適用やログ閲覧などの管理操作は一箇所で行うことが可能です。この場合、同じポリシーが全ての WEBGUARDIAN へ適用されます。

● 複数台時の構成図（ロードバランサー利用時）



また、上図のようにロードバランサー（負荷分散装置）を設置することで利用者のユーザー端末に対して透過的に WEBGUARDIAN を複数台構成にすることができ、全体のスループットを向上させることが可能です。

1-3 アクセス許可ホストの決定

特に前述の「1-2 複数台構成のケース」の最初に示した図のような複数台構成にした場合に、各 WEBGUARDIAN のプロキシポートにどの範囲の端末をアクセス可能とするかを決定してください。

WEBGUARDIAN は、検査サーバー個別にアクセス許可ホストの範囲を設定できます。

2 運用の設計

2-1 ログ保存領域の見積り

WEBGUARDIAN を経由して行われたウェブアクセスに関するログは、各検査サーバーにて一次記録されます。次に管理サーバーが各検査サーバー上の一次ログを定期的に収集し、マージして保存します。

管理サーバーにて収集され、マージが行われた結果のログに対して管理者が閲覧・検索することができるようになります。

そのため全体でどれぐらいのウェブアクセスが対象環境で発生するのか、また各検査サーバーにおよどれぐらいのディスク空き領域が必要なのか、あらかじめ見積りを実施してください。

<容量見積り例>

1 トランザクション当たりのログ容量の目安 : 1 KB	
10 万トランザクション	→ 100 MB
10 万トランザクション × 1 カ月 (30 日)	→ 3 GB

2-2 ログ収集スケジュール

管理サーバーからログ収集するタイミング・時間間隔を決定してください。

管理者が管理サーバーの画面から確認できるログ情報は、検査サーバーから管理サーバーへ収集されたものしか対象になりません。

ユーザーのアクセスが記録された時間とその記録情報を管理者が閲覧できる時間には、ログ収集処理の時間間隔だけ遅延が生じます。

また、ログ収集の時間間隔が大きいと、1 度の収集で転送されるデータサイズが大きくなり、マージ処理に大きな計算リソースが消費される場合がありますのでご注意ください。

3 インストールの準備

3-1 ディスク空き容量の確認

WEBGUARDIAN 検査サーバーでは以下のディスク空き容量が必要です。

- ・ パッケージ導入領域

対象ディレクトリ : /opt

最低 : 1.0 GB

- ・ ログ保存領域

対象ディレクトリ (変更可能) : /var/opt

最低 : 100 MB

推奨 : 2.0 GB

3-2 メールサーバーのセットアップ

WEBGUARDIAN でのルール適合イベントを電子メールで管理者へ通知する機能があります。このため WEBGUARDIAN が稼働するホストにおいて sendmail 等の MTA を適切に設定して稼働させておいてください。または、別ホストの MTA を使用することも可能です。

3-3 プロキシサーバー基本設定事項

前述の、「1 システム構成の設計」において決定した方針に従ってあらかじめ以下の項目の値を準備しておいてください。

- ・ WEBGUARDIAN のポート番号

- ・ 上位プロキシサーバーホストの IP アドレスとポート番号

- ・ 上位プロキシサーバーを経由しない宛先ホスト範囲

- ・ アクセス可能なクライアントホストアドレス範囲

- ユーザーから直接アクセスされる場合はユーザー端末の IP アドレス範囲

- 下位プロキシやレイヤー 4 以上のロードバランサーを利用する場合はそれらの IP アドレス

4 OS 設定

WEBGUARDIAN 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。詳しくは『**管理サーバー 導入の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』をご参照ください。

4-1 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 WEBGUARDIAN（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ございます。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) 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。

※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。

ed, tcl, compat-libstdc++-33（32bit パッケージ）, mt-st

(2) IPv6 設定の解除

WEBGUARDIAN（管理サーバー／検査サーバー）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.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」と記述された行がなければ、追加します。
- ・「alias ipv6 off」と記述された行がなければ、追加します。

変更前表示例)

```
alias eth0 e1000
alias net-pf-10 ipv6          # (存在すれば) この行を削除
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、「:wq!」と入力して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、「:wq!」と入力して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、「: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 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 **WEBGUARDIAN**（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（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へご確認ください。

(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削除してください。
- ・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" # この行を削除
SUPPORTED="ja_JP.UTF-8:ja_JP:ja" # この行を削除
SYSFONT="latarcyrheb-sun16"
# 最終行以降に EUC-JP 設定を追加
```

変更後表示例）

```
SYSFONT="latarcyrheb-sun16" # この行をコメントアウト
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確認ください。

(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 ((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

文字挿入コマンド : i 入力を完了する時は Esc キー

文字削除コマンド : x

変更前表示例)

```
(前略)
if [ "`id -gn`" = "`id -un`" -a `id -u` -gt 99 ]; then
umask 002
else
umask 027 #022 へ変更
fi
(後略)
```

変更後表示例)

```
(前略)
if [ "`id -gn`" = "`id -un`" -a `id -u` -gt 99 ]; 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る場合

((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「5 MTA 設定」をご参照いただき、WEBGUARDIAN (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。

4-2 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 WEBGUARDIAN (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ございます。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) 必要パッケージのインストール確認

前述の「4-1 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「4-1 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「4-1 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「4-1 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「4-1 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「4-1 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) MTA 設定

後述する「5 MTA 設定」をご参照いただき、WEBGUARDIAN (検査サーバー) 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。

(8) 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。

4-3 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 WEBGUARDIAN (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ございます。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) 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

(2) IPv6 設定の解除

WEBGUARDIAN (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」と記述された行がなければ、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」と記述された行がなければ、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 off
```

② ip6tables のサービスが起動していれば、停止します。

```
# service ip6tables off
```

③ iptables のサービスが自動起動しないよう、停止します。

```
# chkconfig iptables stop
```

④ ip6tables のサービスが自動起動しないよう、停止します。

```
# chkconfig ip6tables stop
```

(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」と記述された行がなければ、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 # 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。

(6) ポート 5432 確認

※本項目は **WEBGUARDIAN**（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 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="en_US.UTF-8"      # 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
en_US.UTF-8      ← 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 [ "`id -gn`" = "`id -un`" -a `id -u` -gt 99 ]; then
umask 002
else
umask 027      #022 へ変更
fi
( 後略 )
```

変更後表示例)

```
( 前略 )
if [ "`id -gn`" = "`id -un`" -a `id -u` -gt 99 ]; 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る場合
(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「5 MTA 設定」をご参照いただき、WEBGUARDIAN (管理サーバー／検査サーバー) 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。

5 MTA 設定

本章では、sendmail、postfix の設定例を説明します。

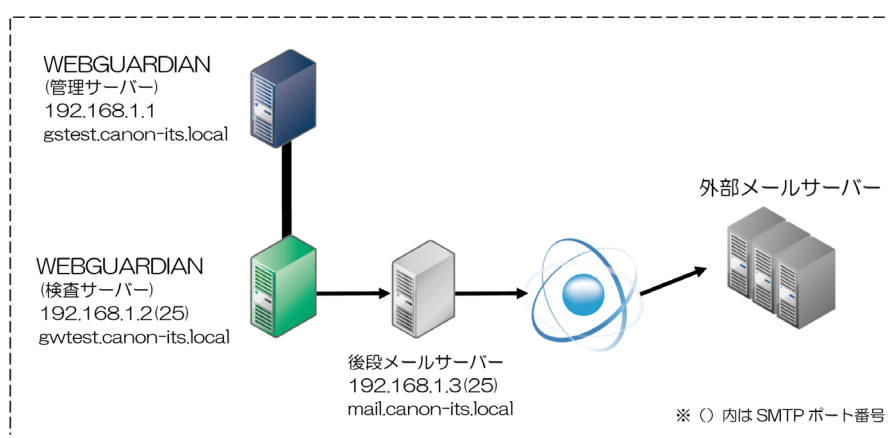
WEBGUARDIAN からの通知メールを送信するための設定です。

5-1 sendmail

sendmail を MTA とするために必要な準備について、以下の環境への設定を例に説明します。

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「dnl」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)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for linux')dnl
OSTYPE(`linux')dnl
Dwgwtst # 追記、自サーバーのホスト名を設定してください。
Dmcanon-its.local # 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')dnl # 追記
define(`SMART_HOST', `smtp:[192.168.1.3]')dnl
# ↑ 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'')dnl
define(`PROCMAIL_MAILER_PATH', `/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/mail/statistics')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings, novrfy, noexpn, restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
define(`confTO_IDENT', `O')dnl
define(`confSERVICE_SWITCH_FILE', `/etc/mail/service.switch')dnl # 追記
FEATURE(`no_default_msa', `dnl')dnl
FEATURE(`smrsh', `/usr/sbin/smrsh')dnl
FEATURE(`mailertable', `hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable', `hash -o /etc/mail/virtusertable.db')dnl
FEATURE(reirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(`nocanonify')dnl # 追記
FEATURE(local_procmail, `', `procmail -t -Y -a $h -d $u')dnl
EXPOSED_USER(`root')dnl
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl # (※1)
FEATURE(`accept_unqualified_senders')dnl
FEATURE(`accept_unresolvable_domains')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl

```

(※1)「DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl」がある場合は上記変更後表示例と同様に文頭に「dnl」を挿入し、無い場合は上記記入例と同様に文頭に「dnl」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。

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

参考) **WEBGUARDIAN** 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

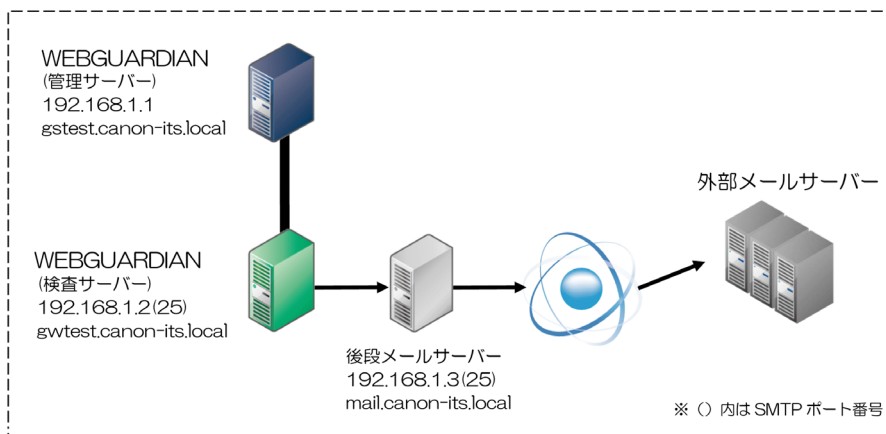
WEBGUARDIAN インストール前に、メーラーからメールが送付できることをご確認ください。

5-2 postfix

postfix を MTA とするために必要な準備について、以下の環境への設定を例に説明します。

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
```

※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) 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

WEBGUARDIAN 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。

MEMO