GUARDIANSUITE

管理サーバー 導入の手引き

～GUARDIANWALL、WEBGUARDIAN 共通～

Canon キヤノン IT ソリューションズ株式会社

* Internet Explorer、Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

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

2015-Mar-01　GUARDIANSUITE V5.0
GUARDIANWALL V8.0
WEBGUARDIAN V4.0

GUARDIANSUITE V5.0 ライセンス控

販売会社より発行された本システムのライセンスキーの情報を控えておいてください。

ライセンスキー	:
製品種類	:
登録済みライセンス	:

ライセンスの詳細については、本マニュアルの「4 ライセンス登録」（48 ページ）をご参照ください。

はじめに

この度は、GUARDIANSUITE をご導入いただき誠にありがとうございます。
本章では本マニュアル『**管理サーバー　導入の手引き ～ GUARDIANWALL、WEB-GUARDIAN 共通～**』の使い方について説明します。
導入の前に、別冊の『**GUARDIANWALL 導入事前準備**』、『**WEBGUARDIAN 導入事前準備**』をそれぞれご覧ください。
また、本システムの詳しい使用方法については、『**管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～**』をご覧ください。

(1) 本マニュアルの使い方

本マニュアルは、GUARDIANSUITE の導入に必要な設定作業などについて説明します。
必ず、本マニュアルをお読みいただいたうえで、本システムの導入を行ってください。
以下に各章の概要を説明します。

1 準備（10 ページ）
本システムをご利用いただくために準備していただくことを説明します。

2 インストール（24 ページ）
本システムのインストール方法について説明します。また、インストール時の諸設定についても説明します。

3 動作確認（42 ページ）
GUARDIANSUITE のインストールが正しく行われたかを確認するための動作確認方法を説明します。

4 ライセンス登録（48 ページ）
本製品のライセンス登録の方法について説明します。
ライセンス未登録の状態では、検査サーバーの検査機能が無効になっています。必ず、ライセンス登録を行ってください。

5 パスワード設定（52 ページ）
本システムを安全にご使用いただくために必要となるパスワードの設定方法を説明します。

6 アンインストール（58 ページ）
GUARDIANSUITE のアンインストール方法を説明します。

7 トラブルシューティング（60 ページ）
本システムのインストール時のトラブルへの対処方法を説明します。

(2) 表記ルールについて

本マニュアルで使用している表記ルールについて説明します。

書体について

画面やファイル中のテキストは枠で囲い、以下のような書体で記述します。

書体	意味	使用例
あいう ABCabc123	画面上のコンピュータ出力	GUARDIANSUITE インストーラ Linux 版
あいう ABCabc123	ユーザーが入力する文字	# mv /usr/sbin/sendmail /usr/sbin/sendmail.OFF
あいう *ABCabc123*	コマンド行の可変部分	# rm filename # rm < **ファイル** >
あいう ABCabc123	ファイルやシステム中のテキスト	Top 5 **合計メール数順** (total: 64)

マークについて

本システムを安全にご使用いただくため、守っていただきたい事項に次のマークを使用しています。必ずお読みください。

マーク	意味
	注意： システムの停止やデータの消去など、重大なトラブルを発生させる可能性があることを示しています。十分注意してください。
	情報： 操作や運用に関連した情報です。参考にお読みください。

記号について

本マニュアルでは以下のような記号を使用しています。

記号	意味	使用例
『』	参照するマニュアル名を表します。 ※ただし、同じマニュアル内では省略します。	・『**利用の手引き**』の「**1-1 機能**」（**22 ページ**）をご参照ください。 ・「**新規インストール**」を選択します。 ・MTA（Mail Transfer Agent）
「」	参照する章、節の番号と名称、 または、システム内のメニュー、項目、値、強調する語等を表します。	
()	ページ番号、または、補足内容を表します。	
[]	システム中のボタン名、リンク名等を表します。	・［**設定**］ボタンをクリックします。
【】	システム内のトップレベルメニュー、 タブメニュー名を表します。	・「**状況確認**」-【**稼動状況**】
\	画面例などで、テキストがページ行幅を超える場合に、継続を示します。	・Enter your domain name \ [your.domain]: example.co.jp

設定例について

本マニュアルに記載されている IP アドレスやドメイン名、URL アドレスなどの設定例は、説明のためのものです。実際はそれぞれの環境に合わせた設定を行ってください。

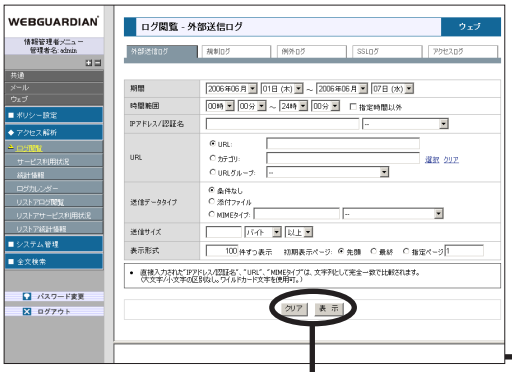
(3) 管理画面名称

本システムは、ウェブブラウザー経由で操作できます。ウェブブラウザーより本システムにアクセスした際、表示される画面を管理画面と総称します。
本節では各管理画面の名称について説明します。

ログイン画面：
ウェブブラウザーより本システムにアクセスすると、この画面が表示されます。この画面から、各利用者別にログインします。

メニューフレーム：
各利用者が行うことのできる操作が表示されます。

利用者別トップページ：
ログインすると、各利用者別のトップページが表示されます。



操作画面：
各操作を行います。

表示（設定）/ クリアボタン：
操作を実行、もしくはクリアするボタンは主に操作画面下中央に配置しています。

MEMO

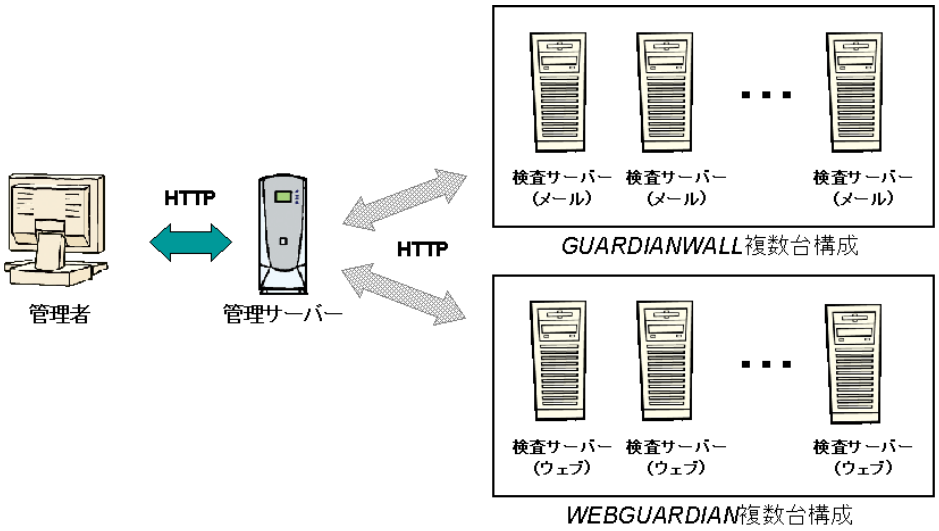
目次

1 準備

本システム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。
本システムの導入作業を行う前にご用意ください。

1-1 インストールプラン

本システムは、GUARDIANWALL と WEBGUARDIAN を統合管理するシステムです。
GUARDIANWALL や WEBGUARDIAN 自体のインストールプランは、それぞれ、『GUARDIANWALL 導入事前準備』、『WEBGUARDIAN 導入事前準備』をご覧ください。
GUARDIANSUITE は各インストールプランによって設置された検査サーバー（GUARDIANWALL もしくは WEBGUARDIAN）と HTTP プロトコルで直接通信可能な場所に設置される必要があります。
GUARDIANSUITE と GUARDIANWALL、WEBGUARDIAN は、通信用に TCP ポート 8080 番を利用します。また、GUARDIANSUITE は、データベースアクセス用に TCP ポート 5432 番を利用します。インストール予定のホストでこれらのポートがすでに使用されていないことを確認してください。



1-2 ウェブブラウザー及びウェブブラウザーを起動するコンピュータ

本システムは、このマニュアルで説明する初期設定以外の通常の管理操作をウェブブラウザー経由で行います。ウェブブラウザーから行う操作には、保留メールの管理、本システムの各種設定作業などがあります。したがって、ウェブブラウザーとウェブブラウザーを起動するコンピュータが必要です。

対応ウェブブラウザーは、Windows Vista SP1,SP2/7 SP1/8/8.1 上の Windows Internet Explorer Ver7.0、Windows Internet Explorer Ver8.0、Windows Internet Explorer Ver9.0、Windows Internet Explorer Ver10.0、Windows Internet Explorer Ver11.0 です。

また、Javascript を有効にする必要があります。

JIS2004 対応環境についてのご注意

Windows Vista の環境では、ウェブブラウザーから管理画面へ JIS2004 文字を入力することができます。しかしながら GUARDIANSUITE 管理サーバーは JIS2004 文字に対応していないため、設定情報を入力後に該当文字が文字化けし、入力情報を各種設定へ正常に反映させることができません。

Windows については、32 ビットおよび、64 ビットバージョン共に対応しています。

Windows7 の Windows XP モードは対応していません。

弊社の検証環境については、上記の環境（インストール後のデフォルトパラメータ）で検証しています。

1-3 利用者の決定

本システムをインストールするハードウェアの root 権限者の他に、本システムが定義する利用者には、情報管理者、部門情報管理者、システム管理者があり、それぞれ複数設定可能です。これらの利用者を何方にするか事前に協議しておく必要があります。各利用者の役割及び権限は以下のとおりです。

利用者	役割・権限
root 権限者	本システムをインストールするハードウェアの root 権限を持つ利用者です。 本システムの導入・設定など、コンピュータ自体の設定を行います。
情報管理者	システム管理全般、ポリシー設定、ログ閲覧など利用者管理以外の全ての項目に対して操作権限を持つ管理クラスです。 メニューの以下の項目を管理することが可能です。 共通　：管理サーバー管理、検査サーバー管理、データ管理、運用監査 メール　：ポリシー管理、保留メール管理、保存メール管理、ログ閲覧、システム管理 ウェブ　：ポリシー設定、アクセス解析、システム管理
部門情報管理者	メールに関しては、特定のユーザーグループが送信するメッセージに対する管理権限を持つ管理クラスです。ウェブに関しては、ログ参照のみを許可する管理クラスです。 メニューの以下の項目を管理することが可能です。 共通　：なし メール　：保留メール管理、保存メール管理、ログ閲覧 ウェブ　：アクセス解析
システム管理者	管理サーバー、検査サーバーのシステム管理項目全般に対する管理権限を持つ管理クラスです。 メニューの以下の項目を管理することが可能です。 共通　：管理サーバー管理、検査サーバー管理、データ管理 メール　：システム管理 ウェブ　：システム管理
利用者管理	情報管理者、部門情報管理者、システム管理者のアカウント作成、詳細管理権限設定、アカウントの削除や、アカウントセキュリティの設定を行う管理クラスです。 メニューの以下の項目を管理することが可能です。 共通　：利用者管理、セキュリティ メール　：ポリシー管理（グループのみ） ウェブ　：ポリシー管理（グループのみ）

1-4 管理者のメールアドレス

本システムの稼働状況の監視ジョブや各種統計情報のレポート通知などの機能は、システム組込みのスケジューラーサービスにより定期実行され、処理結果を管理者へ電子メールで通知します。このため通知メールを受ける管理者のメールアドレスをあらかじめ設定しておく必要があります。メールアドレスはパッケージインストール後にインストーラを使い設定します。

1-5 データ保存用ディスク領域

本システムは、管理対象の GUARDIANWALL や WEBGUARDIAN において、各々記録されたログファイルを収集して保管するディスク領域が必要になります。以下で説明します各ログデータの有無を確認して、保存ディレクトリに十分な空き記憶領域があることを確認してください。

(1) システムログ保存ディレクトリ

デフォルトパス　　：/opt/Guardian/Admin/logs
設定による変更　　：不可

本システムの管理システムが生成するログを保存する領域です。
必ず使用されます。50 MB 程の領域を必要とします。
ディレクトリパスを変更することはできません。

(2) 監査データ保存ディレクトリ

デフォルトパス　　：/var/opt/Guardian/Admin/kansa
設定による変更　　：可

本システムの利用者が操作した各種設定変更の履歴を記録した設定アーカイブファイルや、メールやウェブメールのメッセージ閲覧及び監査に関する情報を記録したメール監査統計情報ファイルやウェブ監査統計情報ファイルを保存する領域です。
設定アーカイブファイルは、監査機能の操作ログ記録と設定保存機能を共にオンにした場合に記録します。
メール監査統計情報ファイルは、検査サーバーとしてメール（GUARDIANWALL）が登録されている場合で、監査機能の操作ログ記録をオンにし、さらにメール監査統計レポートをスケジューラーに登録した場合に記録します。
ウェブ監査統計情報ファイルは、検査サーバーとしてウェブ（WEBGUARDIAN）が登録されている場合で、監査機能の操作ログ記録をオンにし、さらにウェブ監査統計レポートをスケジューラーに登録した場合に記録します。

(3) メールログ保存ディレクトリ

デフォルトパス　　：/var/opt/Guardian/Admin/mail
設定による変更　　：可

検査サーバーとして、メール（GUARDIANWALL）が登録される場合に必要となる領域です。
管理対象の GUARDIANWALL が保存している配送ログや情報検査ログなどの各種ログファイルがこの領域に収集・保存されます。複数の GUARDIANWALL を管理している場合は、各ログはマージされた状態で保存されます。
空き容量の目安は、管理対象の検査サーバーごとに見積りされた「メールログ保存ディレクトリ」の容量を全て足し合わせた容量です。
ディレクトリパスはインストール終了後変更することができます。

管理サーバーと検査サーバーを同一筐体に一括インストールする場合は、インストーラによって検査サーバーのログ保存ディレクトリの値（デフォルトパス：/opt/Guardian/WALL/logs）が設定されます。その場合は、管理サーバーによるログの収集・保存は実施せず、ログ閲覧時には検査サーバーが出力したログファイルが直接参照されることになります。
なお、複数台の検査サーバーを管理する場合は、検査サーバーのログ保存ディレクトリとは、別のディレクトリを必ず指定ください。

(4) メールアーカイブ保存ディレクトリ

デフォルトパス　　：なし
設定による変更　　：可

検査サーバーとして、メール（GUARDIANWALL）が登録される場合で、さらに GUARDIANWALL のメール保存機能を有効にする場合に必要な領域です。
GUARDIANWALL で処理されたメールメッセージがアーカイブ形式で保存されます。
複数の GUARDIANWALL を管理している場合は、メールメッセージは検査サーバーごとに 1 日 1 ファイルで保存されます。
メールメッセージは圧縮（平均圧縮率 約 50 %）した状態で保存されますが、メール流量にあわせて十分な領域を準備してください。
空き容量の目安は、管理対象の検査サーバーごとに見積りされた**「メールアーカイブ保存ディレクトリ」**の容量を全て足し合わせた容量です。

GUARDIANWALL のメール保存機能は初期状態では有効になっていません。メール保存機能を有効にする場合は、保存ディレクトリパス名を必ず設定してください。
メールアーカイブ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 つのメールアーカイブ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）。
なお、複数台の検査サーバーを管理する場合は、検査サーバーのメール保存ディレクトリとは、別のディレクトリを必ず指定ください。

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される場合があります。メールアーカイブ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。

(5) ウェブログ保存ディレクトリ

デフォルトパス　　：/var/opt/Guardian/Admin/web
設定による変更　　：可

検査サーバーとして、ウェブ（WEBGUARDIAN）が登録される場合に必要となる領域です。
管理対象の WEBGUARDIAN が保存しているアクセスログや外部送信ログ、送信メッセージデータが、この領域に収集・保存されます。複数の WEBGUARDIAN を管理している場合は、各ログはマージされた状態で保存されます。
空き容量の目安は、管理対象の検査サーバーごとに見積りされた**「ログ保存ディレクトリ」**の容量を全て足し合わせた容量です。
ディレクトリパスはインストール終了後変更することができます。

管理サーバーと検査サーバーを同一筐体に一括インストールする場合は、インストーラによって検査サーバーのログ保存ディレクトリの値（デフォルトパス:/var/opt/Guardian/WG）が設定されます。その場合は、管理サーバーによるログの収集・保存は実施せず、ログ閲覧時には検査サーバーが出力したログファイルが直接参照されることになります。

(6) データベースディレクトリ

デフォルトパス　　：/var/opt/Guardian/Admin/database/pgsql
設定による変更　　：不可
※インストール時のみ変更可

管理サーバーの監査機能を有効にする場合に必要となるデータベースを格納する領域です。
管理サーバーを利用した記録を操作ログとしてデータベースに保存します。
管理サーバーの操作ログを保存するのに十分な空き容量を準備する必要があります。

データベースを保存するディスク装置のコントローラーに書き込みキャッシュ 機能がある場合は、書き込みモードを write-through に設定することを推奨します。

(7) バックアップ用ディレクトリ

デフォルトパス　　：なし
設定による変更　　：可

上記の各種ログデータをテープなどの外部記憶メディア以外に、任意のディレクトリへバックアップすることができます。
ログのバックアップ処理を実施する前に、システムにディレクトリを作成し、作成したディレクトリパスを設定しておいてください。

(8) リストア用ディレクトリ

デフォルトパス　　：なし
設定による変更　　：可

GUARDIANWALL や WEBGUARDIAN などの各種ログデータをテープなどの外部記憶メディアや任意のディレクトリへバックアップすることができますが、それらのバックアップデータを本システムのログ検索機能を使って閲覧する場合には、別途復元用のディスク領域が必要になります。
ログデータのリストア処理を実施する前に、システムにディレクトリを作成し、作成したディレクトリパスを設定しておいてください。

(9) リストアデータベース用ディレクトリ

デフォルトパス　　：なし
設定による変更　　：可

データベースに格納されている管理サーバーの操作ログをテープなどの外部記憶メディアや任意のディレクトリへバックアップすることができますが、それらのバックアップデータをリストアするためには､別途復元用のディスク領域が必要になります。ログデータのリストア処理を実施する前に、システムにディレクトリを作成し、作成したディレクトリパスを設定しておいてください。

(10) ログ、メールアーカイブ転送一時作業ディレクトリ

デフォルトパス　　：/opt/Guardian/Admin/tmp
設定による変更　　：設定ファイルの変更でのみ可能

検査サーバーから取得してくる各種ログ、メールアーカイブを一時的に格納する領域です。取得するデータの 3 倍以上の容量を必要とします。
※実際に必要な領域は、実データの 2 倍＋予備領域（30 MB 程度）ですが、3 倍以上の空きを確保しておくことを推奨します。
変更する場合は、root 権限で管理・検査サーバーの設定ファイルに以下の設定を登録してください。
・設定ファイル
　管理サーバー　　：/opt/Guardian/Admin/etc/admin/admin.conf
　検査サーバー　　：/opt/Guardian/Admin/etc/cserv/admin.conf
・設定項目（例：デフォルト）

```
[Directories]
GatWorkDirectory=/opt/Guardian/Admin/tmp/
```

1-6 カーネルチューニング

本システム（管理サーバー）は、一部のデータ保存用に、データベースソフトウェアの PostgreSQL を利用します。PostgreSQL では OS の共有メモリとセマフォを利用するため、本システムをインストールする前にカーネルの設定値を本システムの PostgreSQL の稼動に必要な値より大きく設定する必要があります。これらの設定が本システムで利用する PostgreSQL が要求する値よりも小さい場合は、本システムのインストール時に行うデータベースの初期化に失敗します。
ご使用する OS の共有メモリやセマフォの設定が以下に示す本システムの稼動に必要な共有メモリとセマフォの値より大きくなるよう設定をしてください。

■ 本システムの稼動に必要な共有メモリとセマフォの設定

名前	説明	稼動に必要な値
SHMMAX	共有メモリセグメントの最大サイズ	16 MB 以上
SEMMNS	システム全体のセマフォの最大数	250 以上

共有メモリとセマフォの設定の確認及び変更方法はご使用の OS のマニュアルをご覧ください。

1-7 ハードウェアの時刻設定

本システムをインストールして運用を開始する前に、ハードウェアの時刻の設定を確認してください。極端に現在時刻と差異がある場合はその時計を正確に合わせてください。また、管理サーバーと検査サーバーとで時計にずれがある場合についても双方の時計を合わせるようにしてください。

本システム運用中にハードウェアの時刻設定を変更した場合、一時的に検査サーバーのログ収集が正確に機能しない場合があります。
特に検査サーバー側の時計を現設定より大幅に過去に戻した場合にはしばらくログ収集が行われないことがあります。

1-8 OS 言語環境の選択

OS のシステムロケール環境を、英語（C ロケール）以外にする場合は、必ず日本語 EUC-JP 環境を選択してください。

1-9 umask 設定

本システムをインストールする前に、umask 設定を「0022」に設定しておく必要があります。
umask 設定を「0022」以外で設定した状態でインストールを行った場合、本システムが正常に動作しません。

1-10 Red Hat Enterprise Linux 6 で使用する際の注意事項

本システムを Red Hat Enterprise Linux 6（以下、RHEL6）でご使用いただくための意事項について説明します。

(1) OS に必要な設定

① /etc/hosts ファイルの設定

/etc/hosts ファイルが正しく記述されているか確認する必要があります。以下はホスト名が mailwall、サーバーの IP アドレスが 192.168.0.1 であった場合の例となります。

[/etc/hosts の正しい記述例]

```
127.0.0.1 localhost.localdomain localhost
192.168.0.1 mailwall.xx.co.jp mailwall
yy.yy.yy.yy ......
```

[/etc/hosts が正しく記述されていない例]

・IPv6 の記述がある

```
127.0.0.1   localhost   localhost.localdomain
192.168.0.1   mailwall.xx.co.jp   mailwall
::1   localhost   localhost.localdomain
yy.yy.yy.yy ......
```

・ホスト名の記述がない

```
127.0.0.1 localhost.localdomain localhost
yy.yy.yy.yy ......
```

・ループバックアドレスにホスト名が記述されている

```
127.0.0.1 mailwall localhost.localdomain localhost
yy.yy.yy.yy ......
```

② IPv6 の無効化

RHEL6 では IPv6 がデフォルトで有効になっております。本システムでは IPv6 を無効化してください。

/etc/modprobe.d ディレクトリ以下に ipv6.conf のようなファイルを作成し、下記を記述してください。

[/etc/modprobe.d/ipv6.conf の記述例]

```
options ipv6 disable=1
```

③ システムロケールの設定

本システムではCロケール（英語）もしくはそれ以外のシステムロケールを使用する場合は日本語EUCを使用してください。

Cロケールへの設定方法

[/etc/sysconfig/i18nの記述例]

```
#LANG=" ja_JP.UTF-8"
LANG=" C"
```

(2) 必要なソフトウェアの導入

RHEL6では、**「基本パッケージ」**及び、下記パッケージがインストールされている必要があります。

必要なパッケージ名

- compat-db （32bitパッケージ）
- 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

確認方法

以下のコマンドを実行し、パッケージ名が表示されれば、インストールされています。インストールされていない場合は、「package （パッケージ名） is not installed」と表示されます。

```
# rpm -q 〈確認を行うパッケージ名〉
```

(3) Red Hat Enterprise Linux 6の各種機能について

RHEL6は、インストール時にさまざまな機能を選択することができますが、その使用には十分な注意を必要とするものがあります。

① LVM（Logical Volume Manager）の使用に関して

システムのパーティション設定を行う画面ではLVMを選択することができますが、LVMの使用経験があるお客様のみご使用ください。

パーティション構成時に自動設定を使用されますと、LVMが選択されますのでご注意ください。

② ファイヤーウォールの設定に関して

ファイヤーウォールを有効にすると、システムは明確に指定されていない接続（デフォルト設定以外）を受け付けません。システム上で稼動しているサービスへのアクセスが必要な場合には、ファイヤーウォールを通じて特定のサービスのみが許可されるように選択する必要があります（管理サーバーと検査サーバー間、管理サーバーと PC 間等）。この機能をご使用になる場合は、お客様の責任の下にお願いします。

RHEL6 で本機能はデフォルトで有効になります。停止方法は下記の通りです。

② -1. サービス自動起動の停止

```
# chkconfig iptables off
# chkconfig ip6tables off
```

② -2. サービスの停止

```
# service iptables stop
# service ip6tables stop
```

③ SELinux（Security Enhanced Linux）の使用に関して

SELinux ではあらゆる対象（ユーザー、プログラム、プロセス）及び対象物（ファイルやデバイス）に対して詳細なパーミッションを設定します。あるアプリケーションが機能するために必要となるパーミッションだけをそのアプリケーションに安全に許可することができます。システム全体の総合的な理解が必要不可欠となるため、この機能をご使用になる場合はお客様の責任の下にお願い致します（2015 年 2 月時点での、本機能を使用した導入実績はございません）。

RHEL6 で本機能はデフォルトで有効になります。停止方法は下記の通りです。

③ -1. 設定ファイルの更新

［/etc/selinux/config の変更例］

```
#SELINUX=enforcing        ←コメントアウト
SELINUX=disabled          ←追記
```

③ -2. サーバー再起動を実施して設定を有効化します。

(4) 本システムで必要な設定

RHEL6 上で本システムを使用する場合は、下記の通り設定いただく必要がございます。

① 管理サーバーの設定ファイルへの記述

RHEL6 ではデフォルトでは Postfix のみ導入されます。その場合、管理サーバー上の設定ファイル（/opt/Guardian/Admin/etc/admin/admin.conf）に設定を追記いただく必要がございます。

[/opt/Guardian/Admin/etc/admin/admin.conf への追記例]

```
[SMTP]
MailSubmissionProgram = postfix
PostfixQueueDirectory = /var/spool/postfix
```

② 本システムで Sendmail を使用した際の注意事項

RHEL6 での Sendmail のバージョンは 8.14.x となります。本システムが使用する MSP を Sendmail とする場合は、「8.12/8.13」のオプションスイッチを ON としてご利用ください。

MEMO

2 インストール

本章では、GUARDIANSUITE をインストールする方法を説明します。以下の手順に従って本システムのインストールを行ってください。

GUARDIANWALL のみをインストールする場合、インストールの前に以下をご参照ください。

- qmail が動作している環境へインストールする方法「2-7 qmail がインストールされている場合」(35 ページ)
- Postfix が動作している環境へインストールする方法「2-8 Postfix がインストールされている場合」(37 ページ)

2-1 導入ソフトウェアの選択

管理サーバーと検査サーバーの構成を決定してください。
サーバー構成に関する説明は、『管理サーバー 利用の手引き ～ GUARDIANWALL、WEBGUARDIAN 共通～』の「1 概要」(22 ページ) の章をご参照ください。

管理サーバーと検査サーバーにはそれぞれ以下のソフトウェアが必要です。

管理サーバー	: GUARDIANSUITE ソフトウェア
検査サーバー（メール）	: GUARDIANWALL ソフトウェア
検査サーバー（ウェブ）	: WEBGUARDIAN ソフトウェア

また、インストール CD には以下の 2 種類があります。

(A) GUARDIANWALL インストール CD
GUARDIANSUITE ソフトウェア、GUARDIANWALL ソフトウェアが含まれているメディアです。
※ GUARDIANWALL を単体構成で導入する場合の一括インストレーションを含みます。

(B) WEBGUARDIAN インストール CD
GUARDIANSUITE ソフトウェア、WEBGUARDIAN ソフトウェアが含まれているメディアです。
※ WEBGUARDIAN を単体構成で導入する場合の一括インストレーションを含みます。

実現するサーバー構成・サーバー種別に合わせて各ソフトウェアをインストールしてください。利用するインストール CD については以下を参考にしてください。

① GUARDIANWALL のみをインストールする場合
インストール CD（A）を用いて対象ホストにソフトウェアをインストールします。

② WEBGUARDIAN のみをインストールする場合
インストール CD（B）を用いて対象ホストにソフトウェアをインストールします。

③ 全てをインストールする場合
インストール CD（A）、（B）を用いて対象ホストにソフトウェアをインストールします。

2-2 インストールプログラムの実行

コンソールより、root 権限でログインします。
製品の CD-ROM をドライブにセットし、マウントします。
CD-ROM をマウントしたディレクトリに移動し、インストールプログラム inst をシェル（sh）で実行します。

```
# cd <CD-ROM をマウントしたディレクトリ >
# sh inst
```

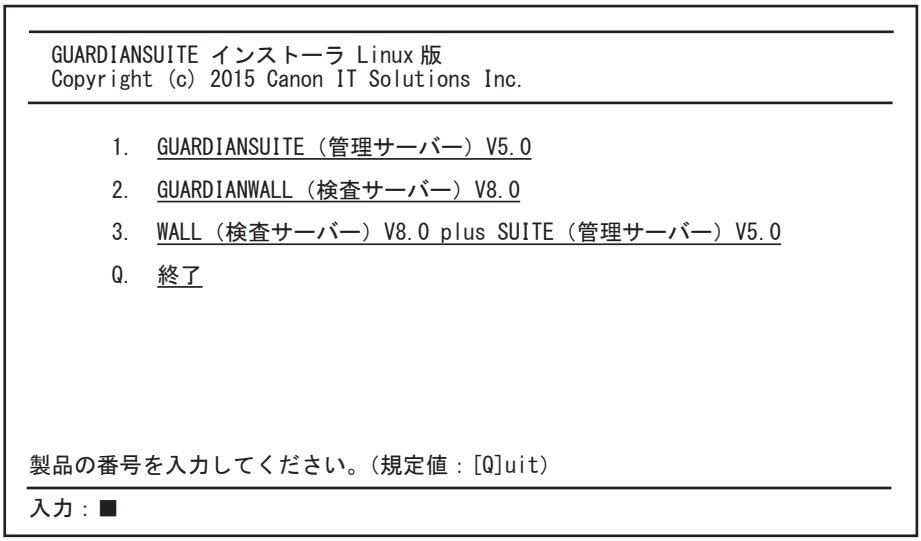
インストールプログラム実行後は、インストールプログラムの表示に従い、ソフトウェアのインストール作業を進めてください。

日本語表示できないコンソールの場合、英語メッセージが表示されます。EUC コードの表示可能なコンソール、端末エミュレータソフトをご利用ください。
コンソール画面の表示領域が狭い場合、正常に表示できない場合があります。コンソール推奨サイズは 80 桁× 25 行以上です。
画面表示が正常にできない場合は、TERMCAP などの設定をご確認ください。

2-3 製品の選択

提供される製品のメディアによってメニューに表示される項目が異なります。

■ GUARDIANWALL インストール CD の場合



上記画面図のように表示された製品メニューの内、1 ～ 3 のいずれかの番号を選択します。

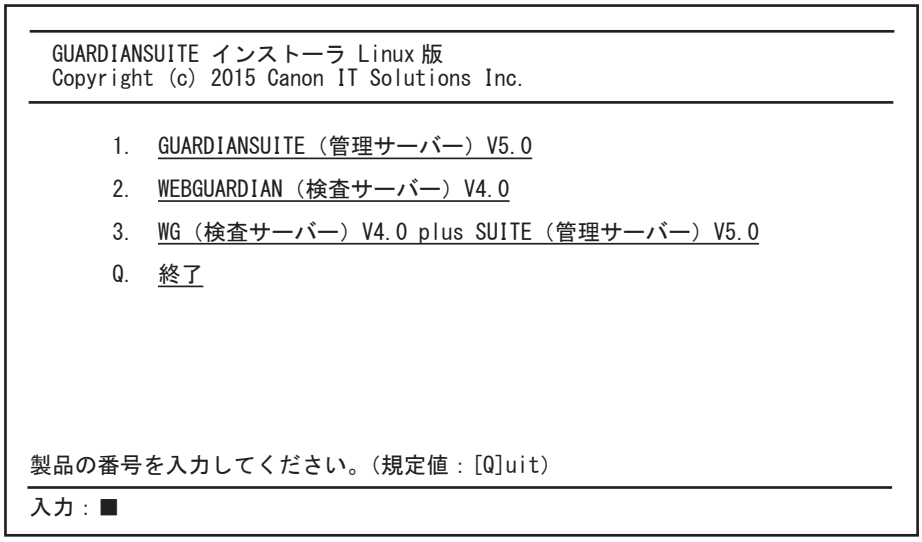
「1. GUARDIANSUITE（管理サーバー）V5.0」
- 運用管理に使用するための管理サーバーのソフトウェアをインストールします。

「2. GUARDIANWALL（検査サーバー）V8.0」
- 検査サーバー（メール）のソフトウェアをインストールします。

「3. WALL（検査サーバー）V8.0 plus SUITE（管理サーバー）V5.0」
- 管理サーバーと検査サーバー（メール）のソフトウェアを、まとめて同一筐体にインストールします。

GUARDIANSUITE（管理サーバー）ソフトウェアをインストールすると、データベースソフトウェアとして PostgreSQL がインストールされます。また、データベース管理用アカウントとして grdndb ユーザーとグループが OS に追加されます。
データベースソフトウェアは、管理サーバーの各利用者が管理画面（GUI）を通じて利用した記録を操作ログとして保存するために使用されます。

■ WEBGUARDIAN インストール CD の場合



上記画面図のように表示された製品メニューの内、1 ～ 3 のいずれかの番号を選択します。

「1. GUARDIANSUITE（管理サーバー）V5.0」

- 運用管理に使用するための管理サーバーのソフトウェアをインストールします。

「2. WEBGUARDIAN（検査サーバー）V4.0」

- 検査サーバー（ウェブ）のソフトウェアをインストールします。

「3. WG（検査サーバー）V4.0 plus SUITE（管理サーバー）V5.0」

- 管理サーバーと検査サーバー（ウェブ）のソフトウェアを、まとめて同一筐体にインストールします。

2-4 インストール方法の選択

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

GUARDIANSUITE（管理サーバー）のインストール

    1.  新規インストール
    2.  アップグレードインストール
    3.  アンインストール
    4.  GUARDIANWALL（V6.0 未満）からのアップグレードインストール
    B.  戻る


実行したい項目の番号を入力してください。(規定値：[B]ack)
入力：■
```

最初にインストールする場合は**「新規インストール」**を選択します。
すでにインストールされた旧バージョンからアップグレードする場合は**「アップグレードインストール」**を選択します。

※ WEBGUARDIAN の旧バージョン（Ver2.3 以前）からのアップグレードには対応しておりません。

GUARDIANWALL Ver6.0 未満のバージョンを、管理サーバーのみにアップグレードする場合は、**「GUARDIANWALL（V6.0 未満）からのアップグレードインストール」**を選択してください（GUARDIANSUITE インストール CD ／ GUARDIANWALL インストール CD において**「GUARDIANSUITE（管理サーバー）」**を選択した画面のみ選択可）。この場合は、GUARDIANWALL で使用している各種キューディレクトリに保存されている下記のメッセージは、アップグレード後は全て削除されてしまいますのでご注意ください。

・保留中のメッセージ（pqueue）
・未保存のメッセージ（aqueue）

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

インストールに必要なディレクトリ情報...

        ディレクトリ名    : /opt
        必須ディスク容量  : 1024MB
        現在の空き容量    : 1944MB

        このディレクトリにパッケージがインストールされます。


システム環境をチェックしています...

続行しますか？ [y/n] ■
```

インストール方法の選択後、システム環境のチェックを行い、/opt や /var ディレクトリの空き容量が少ない場合は、エラーメッセージや警告メッセージが表示される場合があります。その場合は、インストールを中止して、必要なディスク空き容量を確保してください。インストールを続行すると導入するパッケージを表示します。

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

以下のパッケージがインストールされます。
        GRDNcore        : GUARDIANSUITE Core Package V5.0.00-000
        GRDNlocal       : GUARDIANSUITE Tools Package V2.1.05-000
        GRDNperl        : GUARDIANSUITE Perl Package V5.6.1-011
        GRDNjre         : GUARDIANSUITE J2RE Package V1.4.2-010
        GRDNadmin       : GUARDIANSUITE Admin Package V5.0.00-000
        GRDNdb          : GUARDIANSUITE Database Package V8.1.23-001


インストールを続行しますか？ [y/n] ■
```

ご使用のインストールメディアによっては、上記表示と異なるパッケージ名やバージョン番号が表示されます。

導入パッケージ名の確認を求めるプロンプトを表示します。インストールを続行するとパッケージの導入を行います（アップグレードインストール時は、旧パッケージの削除を行ってから新パッケージの導入を行います)。

アップグレードインストール時、旧パッケージの削除を行う前にインストーラはスケジューラー JOB の実行確認を行います。JOB 実行中の場合はエラーメッセージを出力し、インストールを中止します。この場合はスケジューラー JOB の完了後、再度インストールプログラムを実行し、アップグレードインストールを行ってください。

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

        0% ************************************------- 100%

パッケージ<GRDNcore> をインストールしています...
```

ソフトウェアのインストールには、OS のパッケージ管理システムを使用しています。別のホストに導入したファイル一式をコピーした場合や、OS の再インストール後にファイルだけリストアした場合など、OS 上のパッケージ管理情報が失われている場合は、本処理でアップグレードインストールやアンインストールが実行できない場合があります。

2-5 初期設定（新規インストール選択時のみ）

パッケージの導入が終わると、続いて初期設定を行います（アップグレードインストール時は、旧バージョンの設定情報を引き継ぎますので初期設定作業はありません）。

(1) GUARDIANSUITE の場合

■ 管理者メールアドレス

管理者のメールアドレスを設定します。リターンキーのみを押すと、[ ] 内に表示されている値が設定されます。
本システムにより送信される各種通知メールのデフォルトの宛先に、この管理者メールアドレスが使用されます。

■ データベース格納ディレクトリ

データベースを格納するディレクトリを設定します。リターンキーのみを押すと、[ ] 内に表示されている値が設定されます。
GUARDIANSUITE（管理サーバー）で使用するデータベースがこのディレクトリに作成されます。

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

初期設定を開始します...


AdminMailAddress        : admin@example.co.jp
DatabaseDirectory       : /var/opt/Guardian/Admin/database/pgsql/




上記内容で良ければ [y] を、変更したければ [n] を入力してください

入力 : ■
```

表示された内容で設定を実行する場合には「y」を、再入力するには「n」を入力します。「y」を入力すると初期設定の後、データベースの初期化が行われ、データベース格納ディレクトリにデータベースが作成されます。

(2) GUARDIANWALL の場合

■ MSP（Mail Submission Program）

メールを送信するために使う MSP を選択します。リターンキーのみを押すと、[ ] 内に表示されている値が設定されます。MSP には、sendmail、qmail、Postfix を使用することができます。

MSP として、qmail もしくは Postfix をご使用になる場合は、これらソフトウェアが SMTP デーモンとして起動しないように設定する必要があります。設定方法については、それぞれ「2-7 qmail がインストールされている場合」（35 ページ）、「2-8 Postfix がインストールされている場合」（37 ページ）をご参照ください。

MSP として、sendmail を選択した場合は、sendmail のバージョンを調べて表示します。

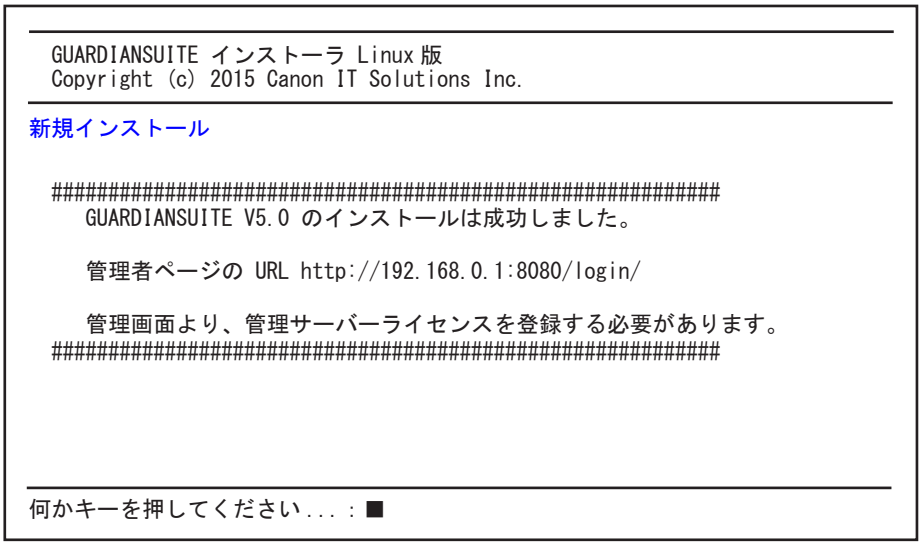
```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

初期設定を開始します...


Msp                    : sendmail
sendmail version       : 8.13.8



上記内容で良ければ [y] を、変更したければ [n] を入力してください

入力：■
```

表示された内容で設定を実行する場合には「y」を、再入力するには「n」を入力します。

2-6 インストール完了

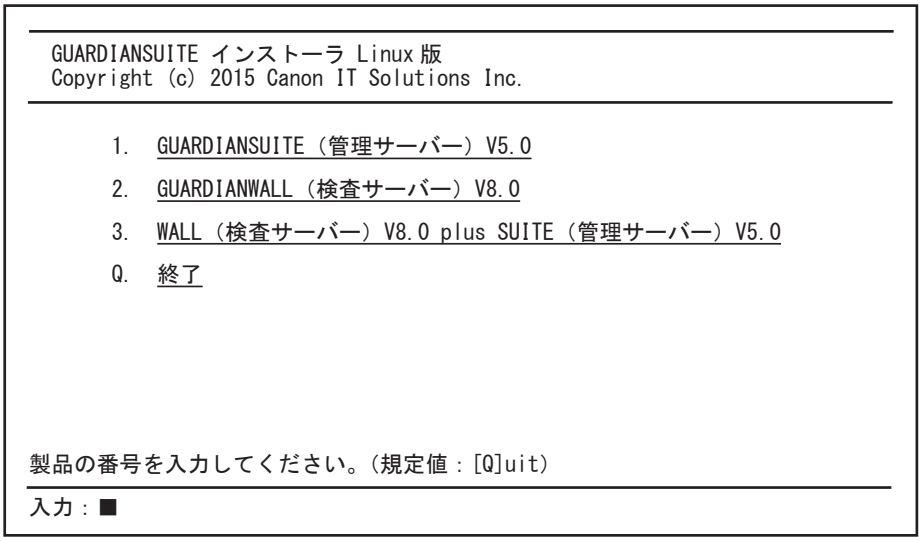
本システムに必要な各種設定やサービスの起動を行います。

下記内容が表示されれば、インストール完了です。製品選択メニューに戻り、インストールプログラムを終了してください。



何かキーを押します。

インストール完了時の表示内容は、前述の**「2-3 製品の選択」**(22 ページ)のところで選択した項目により異なります。



「終了」を選択して、インストールプログラムを終了します。

引き続き、**「3 動作確認」（42 ページ）**を行ってください。

2-7 qmail がインストールされている場合

■ 前提条件

すでに、qmail がインストールされている環境に、GUARDIANWALL を新規インストールする場合は、qmail の sendmail 互換インタフェースを使用しますので、あらかじめ、qmail をインストールしておいてください。

■ qmail の設定変更

qmail の SMTP サーバーの代わりに GUARDIANWALL が SMTP サーバーとして動作することになります。そのため、qmail の SMTP サーバーを止め、起動しないように設定を変更する必要があります。以下は変更手順の一例ですが、ご使用の環境に合わせて実行してください。

- qmail の停止
- qmail の smtpd の停止

  inetd、tcpwrapper、tcpserver 経由の起動になっている場合は、それらの設定変更と再起動
- qmail 起動

■ GUARDIANWALL のインストール

インストールプログラムを実行し、パッケージ導入後の初期設定で MSP に qmail を選択します。

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

初期設定を開始します...

MSP                    : qmail

上記内容で良ければ [y] を、変更したければ [n] を入力してください
入力：■
```

■ GUARDIANWALL の設定変更（必要な場合）

GUARDIANWALL は、qmail のデフォルトインストール時のパス名で qmail 関連プログラムを呼び出し、キューディレクトリの空き容量を検査します。
qmail のデフォルトインストール以外の場所に qmail コマンドやキューディレクトリを設定している場合は、管理サーバーにて検査サーバー（メール）を追加した後、管理サーバーの GUARDIANWALL の設定ファイルに以下の内容を追記し、検査サーバーの設定ファイルの更新、GUARDIANWALL の再起動を行ってください。

管理サーバーでの作業

・検査サーバーの追加

管理画面の**【共通】-「検査サーバー管理」-「個別設定」**にて、検査サーバーを追加します。詳細な操作方法については、**『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」（77 ページ）**をご参照ください。
※すでに検査サーバーが登録されている場合はこの作業は不要です。

・GUARDIANWALL の設定ファイルを編集

上記で追加した検査サーバーの個別設定ファイルを編集します。

```
# vi /opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf
```

・上記設定ファイルに以下内容を追記

```
[SMTP]
MailSubmissionProgram = qmail
QmailProgram = <sendmail 互換プログラムパス名>
                                （デフォルト　/usr/lib/sendmail）
QmailQueueDirectory = <キューディレクトリ>
                                （デフォルト　/var/qmail/queue）
QmailQueueListProgram = <キューリスト表示プログラムパス名><引数>
                                （デフォルト　/var/qmail/bin/qmail-qstat）
```

・GUARDIANWALL の設定ファイル更新

```
# /opt/Guardian/Admin/support/pushMailWall [-s <server_id>] conf
```

※特定の GUARDIANWALL のみ行う場合は、-s オプションで検査サーバー ID を指定して実行してください。

検査サーバーでの作業

・GUARDIANWALL の再起動

```
# /etc/init.d/Guardian.mail restart
```

※ QmailProgram は、オリジナル sendmail ではなく、qmail の sendmail 互換インタフェース用 sendmail プログラムを指定してください。
※ qmail の起動／停止スクリプトは、ご使用の環境に合わせて準備してください。GUARDIANWALL の起動 / 停止スクリプト（/etc/rc2.d/S99Guardian.mail 等）では qmail の起動 / 停止は行いません。

2-8 Postfix がインストールされている場合

■ 前提条件

すでに、Postfix がインストールされている環境に、GUARDIANWALL を新規インストールする場合は、Postfix の sendmail 互換インタフェースを使用しますので、あらかじめ、Postfix をインストールしておいてください。

■ Postfix の設定変更

Postfix の SMTP サーバーの代わりに GUARDIANWALL が SMTP サーバーとして動作することになります。そのため、Postfix の SMTP サーバーを止め、起動しないように設定を変更する必要があります。以下は変更内容の一例ですが、コマンドパス名、設定ファイルパス名は、ご使用の環境に合わせて実行してください。

・Postfix の停止

```
# postfix stop
```

・Postfix 設定ファイル master.cf の smtp inet で始まる行をコメントアウト
（/etc/postfix/master.cf：Postfix デフォルトインストール時の設定ファイルパス名）

```
#smtp      inet  n       -       n       -       -       smtpd
```

・Postfix 起動

```
# postfix start
```

■ GUARDIANWALL のインストール

インストールプログラムを実行し、パッケージ導入後の初期設定で MSP に Postfix を選択します。

```
GUARDIANSUITE インストーラ Linux 版
Copyright (c) 2015 Canon IT Solutions Inc.

新規インストール

初期設定を開始します...

                                                                    ...
MSP                     : postfix



上記内容で良ければ [y] を、変更したければ [n] を入力してください
入力：■
```

■ GUARDIANWALL の設定変更（必要な場合）

GUARDIANWALL は、Postfix のデフォルトインストール時のパス名で Postfix 関連プログラムを呼び出し、キューディレクトリの空き容量を検査します。
Postfix のデフォルトインストール以外の場所に Postfix コマンドやキューディレクトリを設定している場合は、管理サーバーにて検査サーバー（メール）を追加した後、管理サーバーの GUARDIANWALL の設定ファイルに以下の内容を追記し、検査サーバーの設定ファイルの更新、GUARDIANWALL の再起動を行ってください。

管理サーバーでの作業

・検査サーバーの追加

管理画面の**【共通】-「検査サーバー管理」-「個別設定」**にて、検査サーバーを追加します。詳細な操作方法については、**『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」（77 ページ）**をご参照ください。
※すでに検査サーバーが登録されている場合はこの作業は不要です。

・GUARDIANWALL の設定ファイルを編集

上記で追加した検査サーバーの個別設定ファイルを編集します。

```
# vi /opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf
```

・上記設定ファイルに以下内容を追記

```
[SMTP]
MailSubmissionProgram = postfix
PostfixProgram = <sendmail 互換プログラムパス名>
                                （デフォルト　/usr/lib/sendmail）
PostfixQueueDirectory = <キューディレクトリ>
                                （デフォルト　/var/spool/postfix）
PostfixQueueListProgram = <キューリスト表示プログラムパス名><引数>
                                （デフォルト　/usr/sbin/postqueue -p）
```

・GUARDIANWALL の設定ファイル更新

```
# /opt/Guardian/Admin/support/pushMailWall [-s <server_id>] conf
```

※特定の GUARDIANWALL のみ行う場合は、-s オプションで検査サーバー ID を指定して実行してください。

検査サーバーでの作業

・GUARDIANWALL の再起動

```
# /etc/init.d/Guardian.mail restart
```

※ PostfixProgram は、オリジナル sendmail ではなく、Postfix の sendmail 互換インタフェース用 sendmail プログラムを指定してください。

※ Postfix の起動 / 停止スクリプトは、ご使用の環境に合わせて準備してください。GUARDIANWALL の起動 / 停止スクリプト（/etc/rc2.d/S99Guardian.mail 等）では Postfix の起動 / 停止は行いません。

2-9 sendmail Ver8.12 以降を利用になる場合のご注意

GUARDIANWALL は、受信したメールの送信時に sendmail を MSP（Mail Submission Program）として呼び出します。Ver8.12 以降の sendmail は、MSP として起動された場合は、設定ファイルとして submit.cf を参照します。特に設定されることなくデフォルトのままインストールされた submit.cf の設定は、localhost の SMTP ポートにメールを送信します。したがって、GUARDIANWALL を導入した環境では、メールがループすることになり正常に送信できません。

sendmail Ver8.12 以降をご利用になる場合は、sendmail 実行時に submit.cf 設定ファイルを用いないようにするために、sendmail に -Am を付与します。本インストーラの初期設定時に sendmail のバージョンを確認し、Ver8.12 以上であると判別できれば下記内容を設定します。なんらかの事情でバージョンが判別できなかった場合や、GUARDIANWALL インストール後に sendmail のバージョンアップを行う場合は下記内容の設定、再起動を行ってください。

管理サーバーでの作業

・検査サーバーの追加

管理画面の**【共通】-「検査サーバー管理」-「個別設定」**にて、検査サーバーを追加します。詳細な操作方法については、**『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」（77 ページ）**をご参照ください。

※すでに検査サーバーが登録されている場合はこの作業は不要です。

・GUARDIANWALL の設定ファイルを編集

上記で追加した検査サーバーの個別設定ファイルを編集します。

```
# vi /opt/Guardian/Admin/etc/admin/server/<server_id>/server.conf
```

・上記設定ファイルに以下内容を追記

```
[SMTP]
SendmailOption = -Am
```

・GUARDIANWALL の設定ファイル更新

```
# /opt/Guardian/Admin/support/pushMailWall [-s <server_id>] conf
```

※特定の GUARDIANWALL のみ行う場合は、-s オプションで検査サーバー ID を指定して実行してください。

・GUARDIANWALL の再起動

```
# /etc/init.d/Guardian.mail restart
```

※本設定により、GUARDIANWALL は、メールの送信時に -Am オプションをつけて sendmail を呼び出します。本オプションを使用して sendmail を MSP として起動した場合は、submit.cf を使用しません。詳しくは、sendmail のドキュメントをご覧ください。

2-10 添付ファイル暗号化機能を利用になる場合のご注意

添付ファイル暗号化機能において、暗号化方式を暗号化 ZIP+ パスワードとする場合は、別途暗号化モジュールをインストールする必要がございます。

暗号化モジュールのインストールは別紙**「暗号化モジュール　導入の手引き」**をご覧ください。

MEMO

3 動作確認

本章では、「2 インストール」が正しく行われたかを確認する手順を説明します。
本システムが正常に起動されている場合は、以下の手順で動作確認を行います。

(1) ウェブブラウザーの起動
↓
(2) 本システムへのアクセス

3-1 ウェブブラウザーの起動

「1 準備」で用意したコンピュータとウェブブラウザーを起動してください。
次に、ウェブブラウザーのプロキシーの設定を確認します。本システムへのアクセスにはプロキシーを使用しないでください。プロキシー未使用の場合、もしくは、プロキシー使用でかつローカルネットワークへのアクセスにプロキシーを使用しないように設定されている場合は、設定を変更する必要はありません。
本システムへのアクセスにはプロキシーを使用しないように、ウェブブラウザーの設定を変更してください。ウェブブラウザーの詳しい使用方法については、ウェブブラウザーの付属マニュアルをご覧ください。

アップグレードインストールを行った場合は、ブラウザーの一時ファイルなどを削除してください。旧バージョンの管理画面をアクセスした際のキャッシュが残っている場合は、新バージョンの管理画面の表示が正常に行えない場合があります。ウェブブラウザーの一時ファイルの削除方法については、ウェブブラウザーの付属マニュアルをご覧ください。

3-2 本システムへのアクセス

ウェブブラウザーの起動・設定が完了しましたら、続いて実際に本システムへアクセスできるかを確認します。
本システムへアクセスするには、ウェブブラウザーの URL 入力欄に管理サーバーの IP アドレスとポート番号を「http://<**管理サーバーの IP アドレス**>:8080/login」のように入力します。
例） http://192.168.0.1:8080/login/

ウェブブラウザーで URL を設定し、本システムに正しくアクセスができると、以下のようなログイン画面が表示されます。

ここまで表示できましたら、引き続き、**「4 ライセンス登録」（48 ページ）**を行ってください。

3-3 ウェブサーバーの SSL 対応について

管理サーバーのウェブサーバーを SSL 対応する方法について説明します。
管理サーバーへのアクセスを暗号化通信で行いたい場合は、以下の設定を実施してください。

(1) 設定方法

以下の設定ファイルの有無で、SSL 対応を切り替えます。
よって、touch コマンドを用い、ファイルを作成してください。

```
# touch /opt/Guardian/Admin/SSL
```

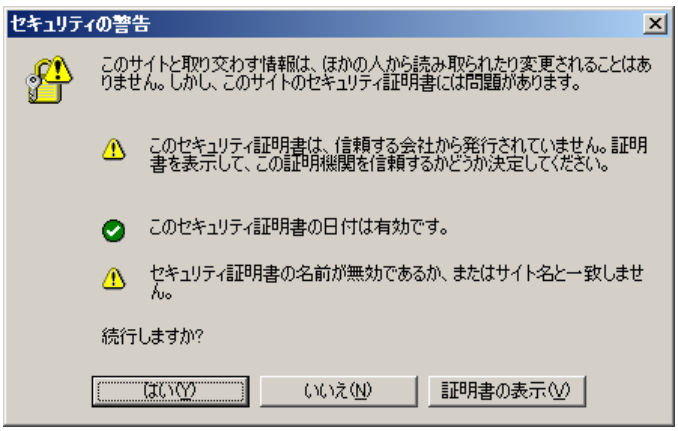
ファイルを作成後、管理サーバーを再起動してください。

```
# /etc/init.d/Guardian.admin stop
# /etc/init.d/Guardian.admin start
```

(2) アクセスについて

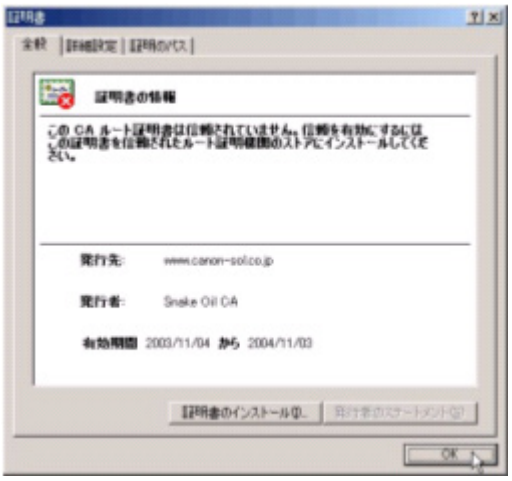
ウェブブラウザーより「https://<**管理サーバーの IP アドレス**>:8443/login」へアクセスして、ウェブ管理画面へ SSL でアクセスできることを確認してください。
例）https://192.168.0.1:8443/login/

なお、標準で用意している証明書は SSL で通信を実施するためだけのダミーの証明書となるため、以下のようにセキュリティの警告が表示されます。



入力した URL が管理サーバーの IP であることを確認後、[**はい (Y)**] をクリックして通信を継続してください。

> 標準で用意される証明書は SSL で通信をするためだけの証明書になりますので、決して「証明書のインストール」は実施しないでください。



※セキュリティの警告を表示させたくない場合は、適切な CA より適切な証明書をご購入ください。

(3) 設定の解除について

/opt/Guardian/Admin/SSL ファイルにて SSL 対応の有無を切り替えております。SSL 対応を非対応とされる場合は、設定ファイルの削除を実施してください。

```
# rm /opt/Guardian/Admin/SSL
```

(4) サーバー証明書の設定方法

CA などから正規のサーバー証明書を購入された場合には以下の手順に従って設定してください。

登録するサーバー証明書ファイル（PEM エンコード形式）と秘密鍵ファイル（PEM エンコード形式）をそれぞれ以下のディレクトリに配置してください。

証明書ファイル：/opt/Guardian/Admin/httpd/conf/ssl.crt
秘密鍵ファイル：/opt/Guardian/Admin/httpd/conf/ssl.key

各ファイルのオーナー、グループ、パーミッション、拡張子は以下のように設定してください。

ファイル	オーナー	グループ	パーミッション	拡張子
証明書ファイル	root	root	644	.crt
秘密鍵ファイル	root	root	400	.key

次に設定ファイル（/opt/Guardian/Admin/httpd/conf/httpd.conf）の次のディレクティブを設置したファイルのパスに変更してください。

証明書ファイル：SSLCertificateFile
秘密鍵ファイル：SSLCertificateKeyFile

最後に管理サーバーを再起動してください。

```
# /etc/init.d/Guardian.admin stop
# /etc/init.d/Guardian.admin start
```

MEMO

4 ライセンス登録

本章では、本製品のライセンス登録を行います。
ライセンス未登録の状態では、検査サーバーの検査機能が無効になっています。メールは中継動作のみを行い、ウェブは単なるプロキシーサーバーとして稼動します。正規ライセンスの登録を行ってください。
なお、ライセンスキーは管理サーバーと検査サーバーで共通です。
※ URLDB ライセンスを除く

■ ライセンスキーの種類

ライセンスキーには、以下の種類がありそれぞれ適切な場所に登録する必要があります。ライセンスキーの登録については、後述の**「4-1　本システムへのログイン」**以降をご参照ください。

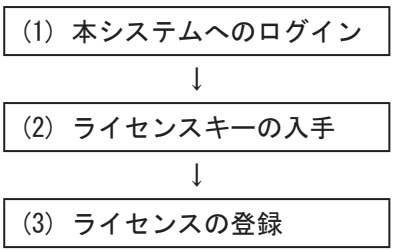
・管理サーバー、検査サーバー（メール、ウェブ）ライセンス

以下の機能を提供するためのライセンスキーです。

- 本システムの各種設定やログ閲覧などの管理機能（管理サーバー）
- 電子メールに関する配送制御などの検査機能（メール検査サーバー）
- ウェブ閲覧に関するアクセス制御などの検査機能（ウェブ検査サーバー）

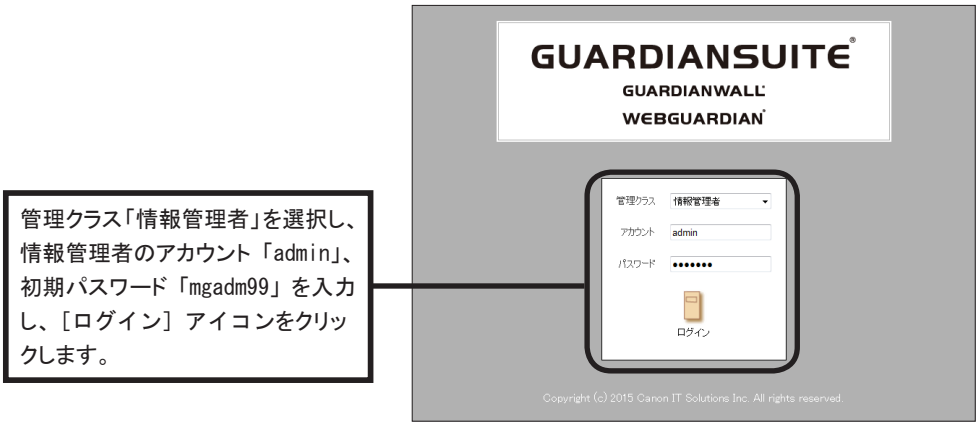
・URLDB ライセンス

ウェブ検査サーバーで稼動する URLDB の更新のためのライセンスキーです。



4-1 本システムへのログイン

本システムに**「情報管理者」**としてログインします。
ログイン画面の管理クラスで**「情報管理者」**を選択、情報管理者のアカウント「admin」を入力します。初期状態ではパスワードは「mgadm99」に設定されています。入力後、**[ログイン]** アイコンをクリックしてください。ログインすると、情報管理者のトップページが表示されます。

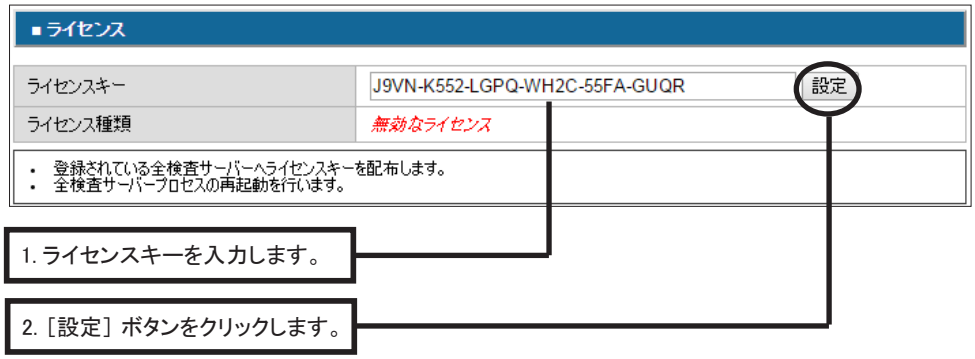


ユーザーの認証が正しく行われると、情報管理者トップページが表示されます。

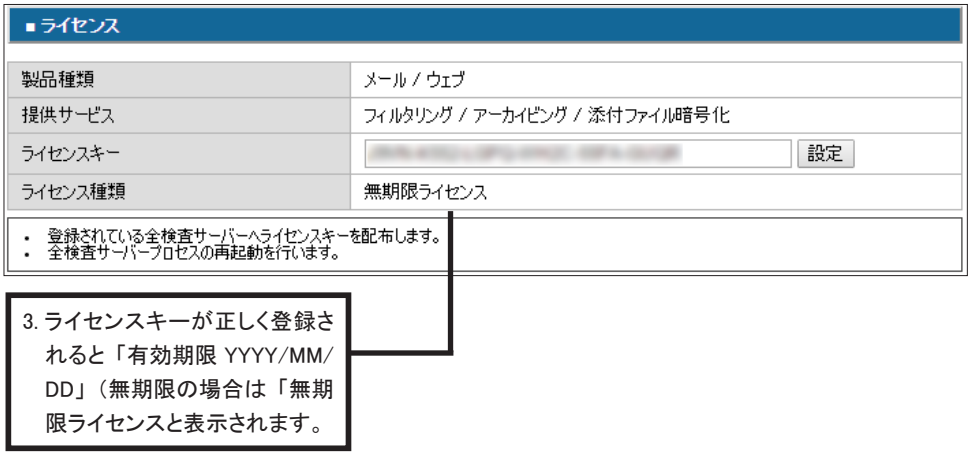
4-2 ライセンスの登録

【共通】-「管理サーバー管理」-「基本設定」-【ライセンス】画面の**「■ライセンス項目」**で、発行されたライセンスキーを入力し、入力ボックス右の［**設定**］ボタンをクリックすると登録されます。

※ URLDB ライセンス（**【共通】-「検査サーバー管理」-「個別設定」-【ライセンス】**）の場合、ユーザーアカウント欄に、DB ダウンロードサイトへログインする際のアカウントが表示されます。



正しくライセンスが登録されると、ライセンス種類欄に有効期限（無期限の場合は**「無期限ライセンス」**）が表示されます。



ライセンスの登録が完了しましたら、引き続き、**「5　パスワード設定」（52 ページ）**を行ってください。

MEMO

5 パスワード設定

電子メールやウェブのアクセス情報は、機密情報や個人のプライバシーにも関わりかねない非常にデリケートな情報です。本システムはそのデリケートな情報を取り扱うため、監査結果の取扱い等には十分慎重であることが必要です。
そのため、本システムではあらかじめ決められた一部の方だけがアクセスできるよう、アクセスする際に利用者の認証を行います。これにより、外部の方や、権限のない一般の方が本システムに無断でアクセスすることを回避します。
本システムは、利用者の認証にパスワードによる認証方式を採用しています。
本システムを安全にご利用いただくために、必ず、パスワードの設定を行ってください。

5-1 利用者の種類

本システムのインストールを行う root 権限者の他、本システムへアクセスが許可される利用者には、以下の 4 種類があります。

- **情報管理者**
- **部門情報管理者**
- **システム管理者（情報管理者のシステム管理系機能のみ利用できる）**
- **利用者管理（上記 3 種類のアカウントの管理用）**

以下に各利用者の役割とパスワードの変更方法を簡単に説明します。

(1) 情報管理者

情報管理者は、共通メニューの管理サーバーの管理、検査サーバーの管理、データの管理、運用監査を行います。また、メールメニューのポリシー設定、保留メール管理、保存メール管理、ログ閲覧、システム管理、ウェブメニューのポリシー設定、アクセス解析、システム管理を行います。
初期状態で情報管理者のアカウントを「admin」で登録しています。必要に応じて利用者管理画面からアカウントを追加、削除できます。

(2) 部門情報管理者

部門情報管理者は、メールメニューの保留メール管理、保存メール管理、ログ閲覧、ウェブメニューのアクセス解析を行います。
必要に応じて利用者管理画面からアカウントを追加、削除できます。

(3) システム管理者

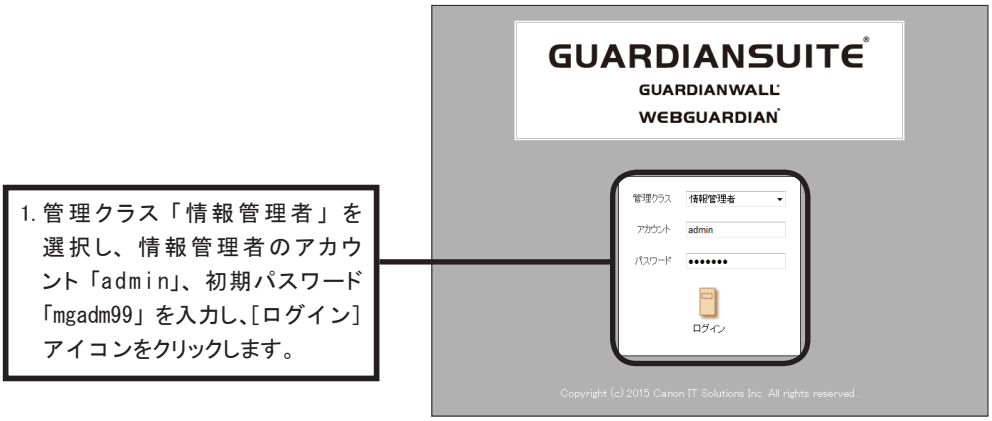
システム管理者は、本共通メニューの管理サーバーの管理、検査サーバーの管理、データの管理を行います。また、メールメニューのシステム管理、ウェブメニューのシステム管理を行います。
必要に応じて利用者管理画面からアカウントを追加、削除できます。

(4) 利用者管理

必要に応じて、上記の情報管理者、部門情報管理者、システム管理者のアカウントを追加、削除するための管理用アカウントです。管理画面よりそれぞれの管理者アカウントの作成、削除を行えます。また、本システム利用者のための運用セキュリティの設定及び管理が行えます。初期状態で利用者管理用のアカウントを「usradm」で登録しています。

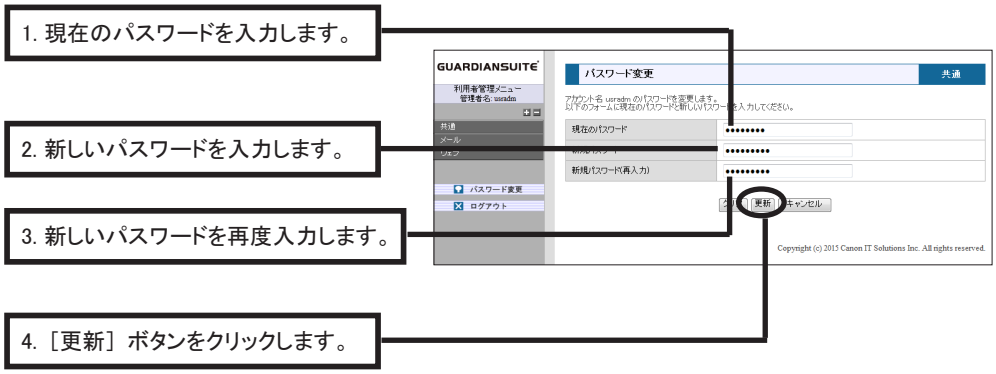
5-2 情報管理者パスワード設定

情報管理者のパスワードは、ウェブブラウザーから変更します。
まず、ウェブブラウザーを起動し、本システムにアクセスしてください。本システムのログイン画面が表示されたら、管理クラスで**「情報管理者」**を選択、情報管理者のアカウント「admin」を入力します。初期状態ではパスワードは「mgadm99」に設定されています。入力後、**[ログイン]**アイコンをクリックしてください。



ユーザーの認証が正しく行われると、情報管理者トップページが表示されます。
画面左側のメニューフレームより、**[パスワード変更]**アイコンをクリックしてください。

「パスワード変更」画面が表示されます。
現在のパスワード、新しいパスワードを入力し、下の入力欄に上と同じ新しいパスワードを再入力してください。入力した文字は**「*」**などで表示されます。パスワード無しの設定にすることはできません。

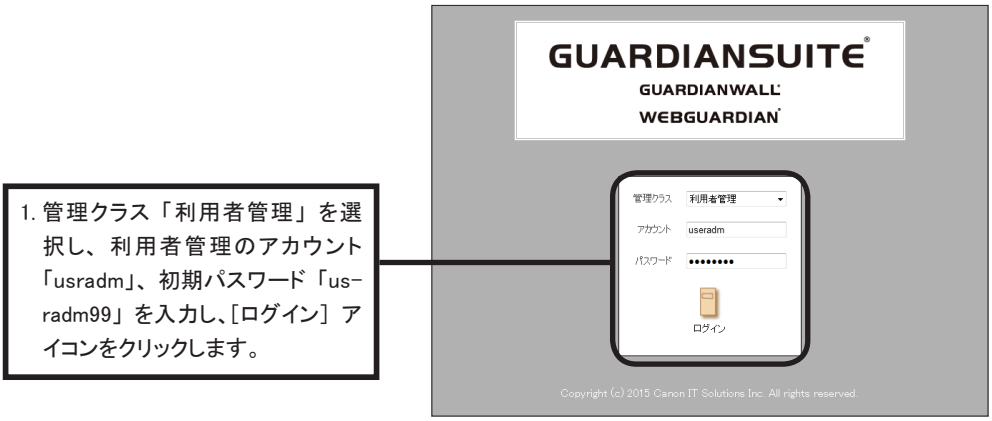


パスワード入力後、［**更新**］ボタンをクリックすると、パスワードが更新されます。［**キャンセル**］ボタンをクリックすると、トップ画面に戻ります。パスワードが正しく入力されると、パスワードが変更された旨のメッセージが表示されます。

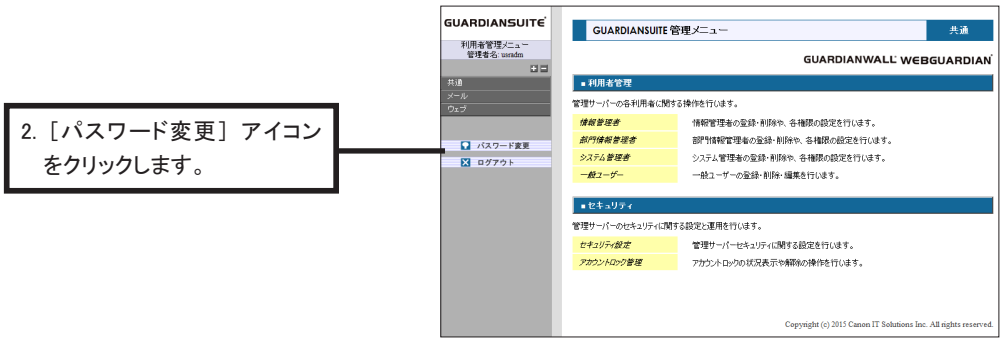
パスワード変更後、一旦ログアウトしてください。
その後、再び本システムにログインします。更新したパスワードによるユーザー認証が行われます。パスワードが確実に変更されたことを確認してください。

5-3 利用者管理パスワード設定

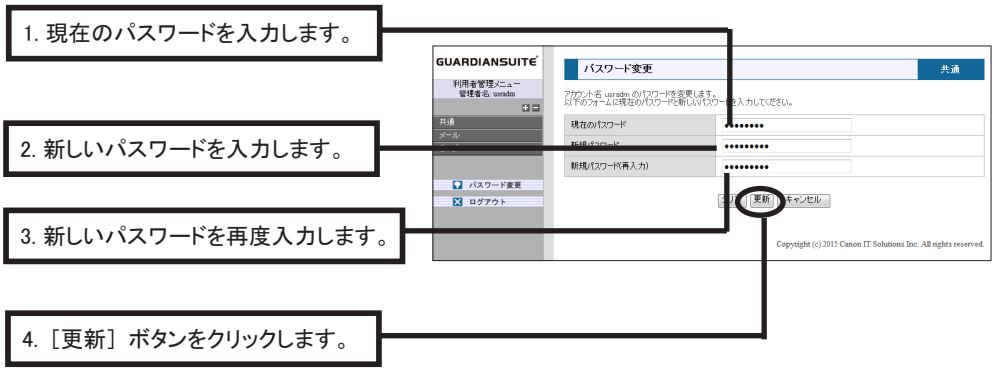
利用者管理のパスワードは、ウェブブラウザーから変更します。
まず、ウェブブラウザーを起動し、本システムにアクセスしてください。本システムのログイン画面が表示されたら、管理クラスで**「利用者管理」**を選択、情報管理者のアカウント**「usradm」**を入力します。初期状態ではパスワードは**「usradm99」**に設定されています。入力後、**［ログイン］**アイコンをクリックしてください。



ユーザーの認証が正しく行われると、利用者管理トップページが表示されます。画面左側のメニューフレームより、**［パスワード変更］**アイコンをクリックしてください。



「パスワード変更」画面が表示されます。
現在のパスワード、新しいパスワードを入力し、下の入力欄に上と同じ新しいパスワードを再入力してください。入力した文字は**「*」**などで表示されます。パスワードを無しの設定にすることはできません。



パスワード入力後、**［更新］**ボタンをクリックすると、パスワードが更新されます。**［キャンセル］**ボタンをクリックすると、トップ画面に戻ります。パスワードが正しく入力されると、パスワードが変更された旨のメッセージが表示されます。

パスワード変更後、一旦ログアウトしてください。
その後、再び本システムにログインします。更新したパスワードによるユーザー認証が行われます。パスワードが確実に変更されたことを確認してください。

6 アンインストール

6-1 GUARDIANSUITE のアンインストール

以下の手順に従って本システムのアンインストールを行ってください。

コンソールより、root 権限でログインします。
GUARDIANSUITE CD-ROM をドライブにセットし、マウントします。
CD-ROM をマウントしたディレクトリに移動し、inst をシェル（sh）で実行します。

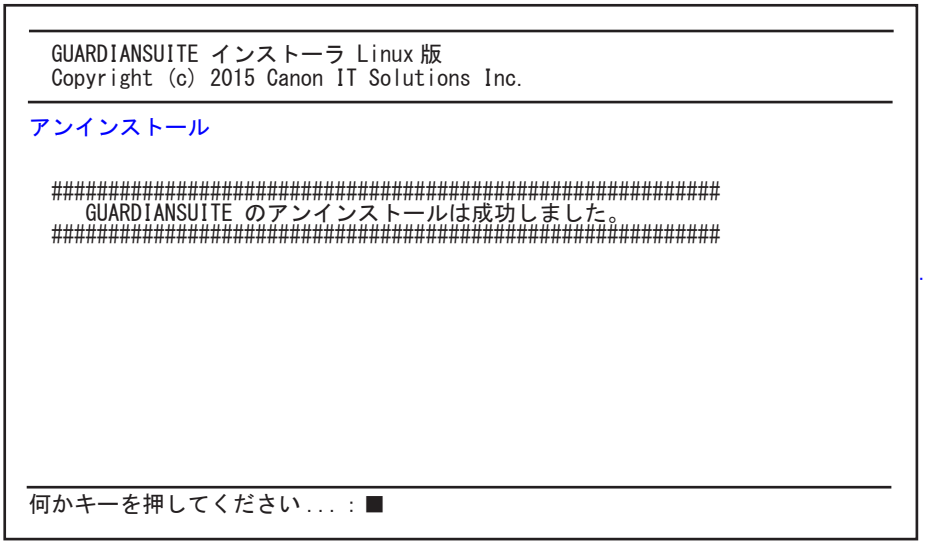
```
# cd（CD-ROM をマウントしたディレクトリ）
# sh inst
```

画面表示に従い、ソフトウェアのアンインストール作業を進めてください。

- 「GUARDIANSUITE V5.0」「GUARDIANWALL V8.0」「WEBGUARDIAN V4.0」など、表示されたメニューからアンインストールしたい製品項目を選択します。
- 「**アンインストール**」を選択します。

パッケージの削除後、ログファイルと未処置の保留メッセージ、データベースファイルを削除するかどうか確認を求めますので、必要な場合は残します。

下記内容が表示されればアンインストール完了です。



・管理サーバーをアンインストールする場合は、管理画面の**【共通】－「検査サーバー」－「個別設定」**メニューで、登録されている検査サーバーを全て削除してから、アンインストールを行ってください。
・検査サーバーをアンインストールする場合は、管理画面の**【共通】－「検査サーバー」－「個別設定」**メニューで、アンインストールする検査サーバーを削除してから、アンインストールを行ってください。
・GUARDIANSUITE（管理サーバー）ソフトウェアをインストールすると、データベース管理用カウントとして grdndb ユーザーとグループが OS に追加されます。このユーザーアカウントは同ソフトウェアをアンインストールした場合も削除されませんので、不要な場合は、手動で削除してください。

7 トラブルシューティング

本章では、障害時の対策について解説します。

(1) 管理画面が表示されない

管理サーバーは、インストール時に 8080 番ポートを使用して起動するように設定されています。すでに、同ポートを他アプリケーションが使用している場合はこのポート番号を変更してください。ポート番号の変更方法については、**『管理サーバー　利用の手引き～ GUARDIANWALL、WEBGUARDIAN 共通～』**の**「12 ポート番号の変更方法」（490 ページ）**をご参照ください。

(2) バージョンアップしたのに、画面が旧バージョンのまま変わらない

ウェブブラウザー、プロキシーのキャッシュデータを表示している可能性があります。ご使用のウェブブラウザーのキャッシュをクリアしてください。また、プロキシー経由で管理サーバーにアクセスしている場合は、プロキシーを使用しない設定に変更してください。

ウェブブラウザーの詳しい使用方法については、ウェブブラウザーの付属マニュアルをご覧ください。

(3) バージョンアップ後、管理画面の操作で通信エラーが発生する

ウェブブラウザー、プロキシーのキャッシュデータが使用されている可能性があります。ご使用のウェブブラウザーのキャッシュをクリアしてください。また、プロキシー経由で管理サーバーにアクセスしている場合は、プロキシーを使用しない設定に変更してください。

ウェブブラウザーの詳しい使用方法については、ウェブブラウザーの付属マニュアルをご覧ください。

(4) sendmai Verl8.12 以降を使用するとメールがループする

sendmail Ver8.12 以降を使用する場合は、以下の点に注意して設定を確認してください。

sendmail Ver8.12 より sendmail を MSP（Mail Submission Program）として起動してメール送信する場合の動作が変更されています。
sendmail を MSP として起動した場合は、submit.cf を参照します。特に設定することなくデフォルトのままインストールされた submit.cf の設定は、localhost の SMTP ポートに接続してメールを送信する設定になっています。
Ver8.12 以降の sendmail だけがインストールされた環境では問題になりませんが、GUARDIANWALL をインストールした環境ではメールがループすることになり、正常にメールの送信ができません。必ず、以下の設定を行ってください。
GUARDIANWALL からメール送信のために sendmail を起動する際に、submit.cf を使用しないようにする sendmail 起動オプションを追加する（**「2-9 sendmail Ver8.12 以降を利用になる場合のご注意」(39 ページ)**）をご参照ください。

sendmail Ver8.12 以降をご利用になる場合の設定方法の詳細については、**『検査サーバー利用の手引き～ GUARDIANWALL V8.0 編（メール）～』**をご参照ください。また、sendmail Ver8.12 以降の機能、Ver8.11 以前との変更点の詳細については、sendmail のマニュアル、ドキュメントをご参照ください。

(5) データベースの初期化に失敗する

GUARDIANSUITE（管理サーバー）ソフトウェアのインストール中の画面に以下の内容が表示される場合はデータベースの初期化処理に失敗しています。

```
データベースの初期化に失敗しました（/var/guardian-install-err.log）
```

エラーログ（/var/guardian-install-err.log）に下記内容が記載されている場合は、OS に設定されている共有メモリセグメントの最大サイズが小さいことが原因です。

```
FATAL: could not create shared memory segment: Invalid argument
DETAIL: Failed system call was shmget(key=1, size=1327104,03600).
```

OS の共有メモリセグメントの最大サイズを変更し、手動でデータベースの初期化処理を行った後データベースと管理サーバーの両サービスを再起動してください。
サービスの起動後、ウェブブラウザーから管理サーバーにアクセスして起動を確認してください。

・データベースの初期化

```
# sh /opt/Guardian/pgsql/share/SUITE_initutil.sh
```

・データベースと管理サーバーの再起動

```
# /etc/init.d/Guardian.db restart
# /etc/init.d/Guardian.admin restart
```

共有メモリセグメントの最大サイズの変更方法についてはご使用の OS のマニュアルをご覧ください。

MEMO