

GUARDIANSUITE

検査サーバー 導入の手引き

～ GUARDIANWALL 導入事前準備～

Copyright©2013 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/>

2013-Aug-30 GUARDIANWALL V7.5

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。
-

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出、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出、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】（78 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】（78 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。

MEMO