WEBGUARDIAN 導入事前準備

*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。

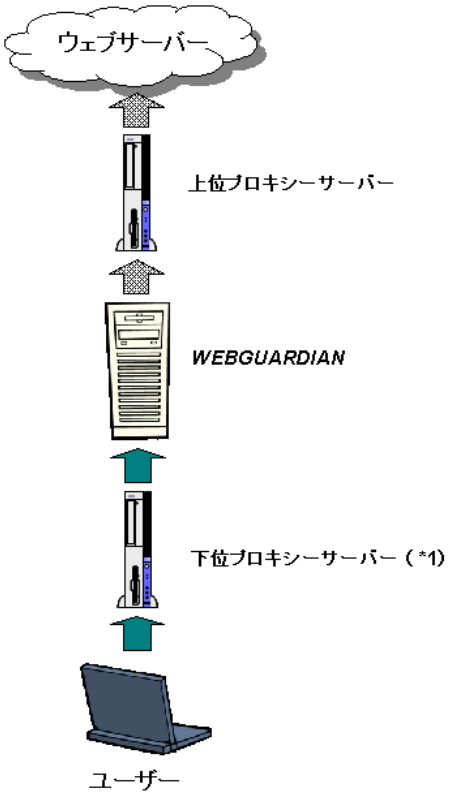
※*WEBGUARDIAN*システムはウェブリクエスト検査を実施する**「検査サーバー」**と検査サーバーの設定操作やログ閲覧操作を受け付ける**「管理サーバー（*SUITE*）」**から構成されています。以降の文中で特に明示されていない場合は、**「***WEBGUARDIAN***」**は**「***WEBGUARDIAN* の検査サーバー」**を意味します。

1 システム構成の設計

1-1 プロキシーサーバー構成

*WEBGUARDIAN*は、HTTP、HTTPS、FTP プロトコルをサポートするプロキシー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。

● **基本プロキシー構成図**



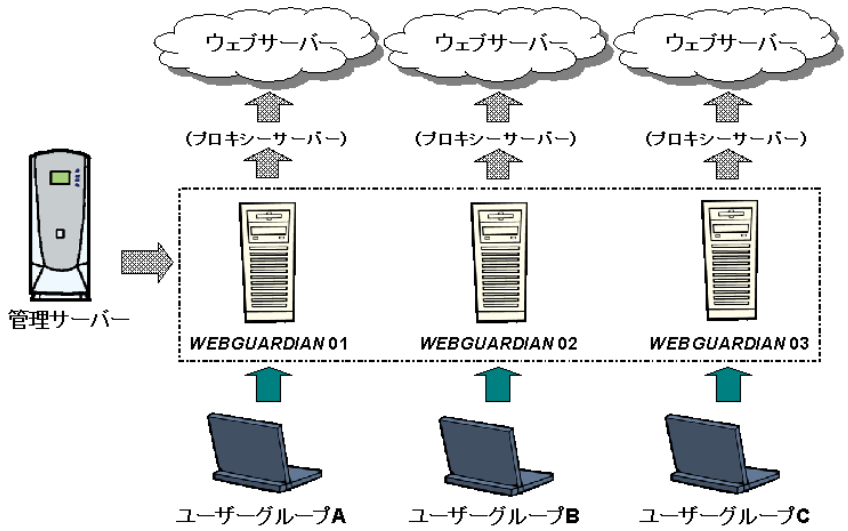
（*1）のように *WEBGUARDIAN* の下位にプロキシーサーバーが存在する場合は、*WEBGUARDIAN*が認識するクライアントIPアドレスは下位プロキシーサーバーのIPアドレスになりますのでご注意ください。ユーザーの利用端末の IP アドレスをポリシー制御の条件にしたい場合は、ユーザー端末が*WEBGUARDIAN*へ直接アクセスする構成にする必要があります。

下位プロキシーサーバーが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、下位プロキシー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* V3.6編（ウェブ）～**』の**「5-6 プロキシー多段構成時の設定」-「(1) WEBGUARDIANの下位にプロキシー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

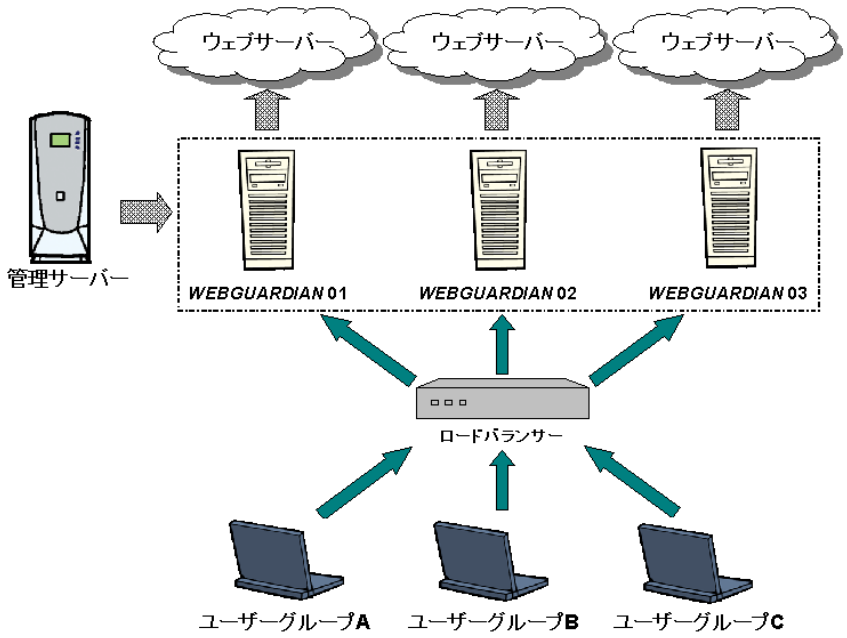
ウェブアクセスが大量にある環境に対応するために、*WEBGUARDIAN*を複数台構成にすることが可能です。
またすでにプロキシーサーバーを複数台並列配置されている場合などには、並列配置されている各々のプロキシーサーバーの下位プロキシーとして、それぞれ*WEBGUARDIAN*1 台を配置することを推奨します。

● **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*のプロキシー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そ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ヵ月（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 プロキシー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**
- **上位プロキシーサーバーホストの IP アドレスとポート番号**
- **上位プロキシー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
- 下位プロキシーやレイヤー 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

3-4 ライセンスについて

パッケージインストール時には、試用版ライセンスが設定されています。
試用版ライセンスの有効期間は以下のとおりです。

・パッケージをインストールした日が1日から15日までの場合、有効期間はその月の最終日になります。
・パッケージをインストールした日が16日以降の場合、有効期間はその翌月の最終日になります。

試用版ライセンスの有効期限内に、正式版ライセンスをインストールしてください。
試用版ライセンスが有効期限を過ぎると、*WEBGUARDIAN*のあらゆるポリシー管理機能は動作しませんのでご注意ください。

3-5 OSパラメータの調整(Solaris9のみ)

Solaris9上で*WEBGUARDIAN*検査サーバーを稼動させる場合、以下の手順でOSパラメータの調整を行ってください。

① /etc/systemファイルに以下の行を追加します

```
set semsys:seminfo_semmnu=20030
```

② システムをリブートします

```
# reboot
```