THE POSSIBILITIES ARE INFINITE FUJITSU

コンピュータウイルスを検出・駆除する専用装置

GeoStream NetShelter/VW

E10L31

プロダクトレポート

富士通株式会社

2003 年 1 月

― 目次 ―

本レポートは，NetShelter/VW E10L31 を対象としています.

1.はじめに

近年，バッドトランス(BADTRANS.B)やクレズ(KLEZ)に代表されるコンピュータウイルスによる感染被害が増加しており，ネットワークシステムの安全性を維持するためには，ファイアウォール装置とともに，メールや Web などに対するウイルスチェックを行うための装置の導入が必要不可欠なものとなっている.

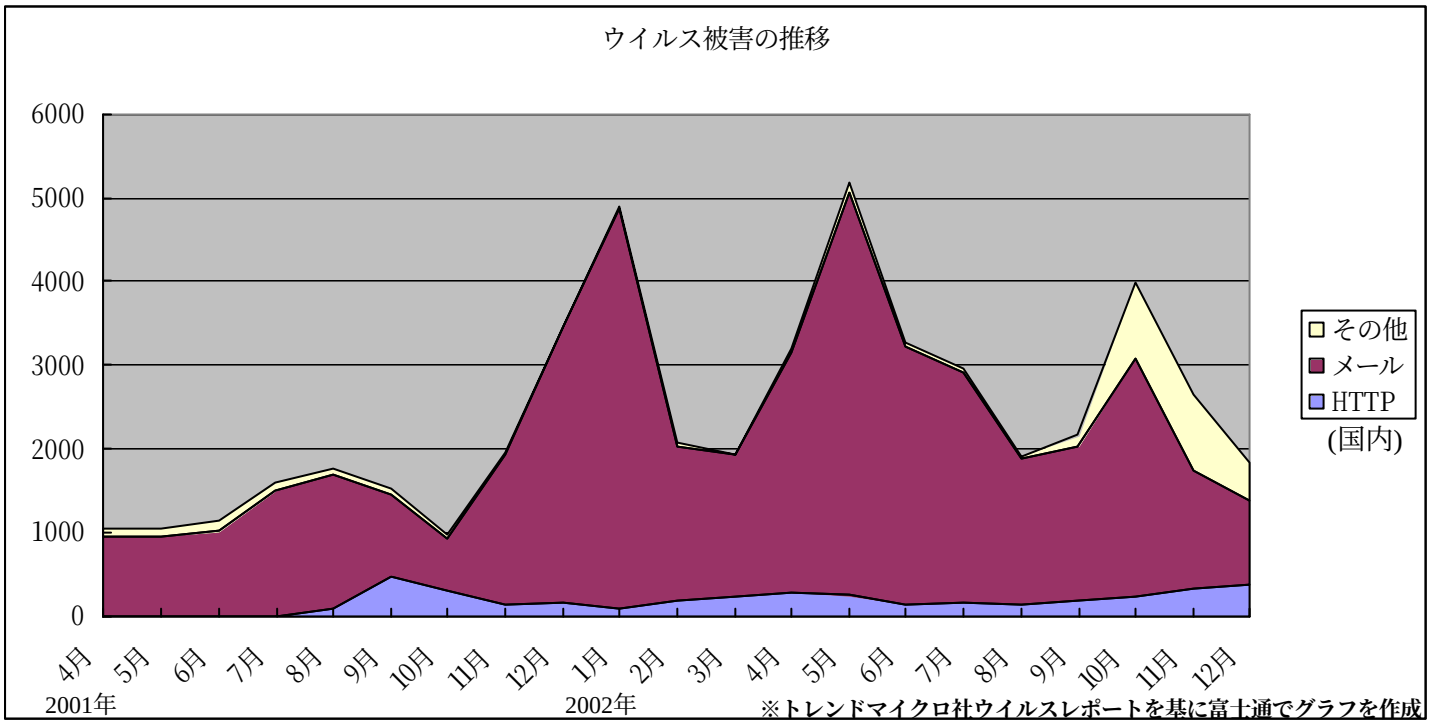


図-1　トレンドマイクロ社が受けたウイルス感染被害報告件数の推移

2002 年のトレンドマイクロ社の発表によると，ウイルス被害報告数は増加傾向にあり，前年度の倍以上の件数に昇っている．また，ニムダ(NIMDA)の大流行以降，HTTP による被害が増加傾向にあり，感染被害は常に全体の 5%以上を占めるようになっている（図-1）.

ブロードバンドの普及に伴い，中小企業や家庭でのインターネット接続が長時間化しつつあるため，ウイルスに遭遇する確立が高まっていると考えられる．このような状況下において，安全なネットワーク環境を維持するためには，メールや HTTP の通信に対して適切なウイルス対策が必須である.

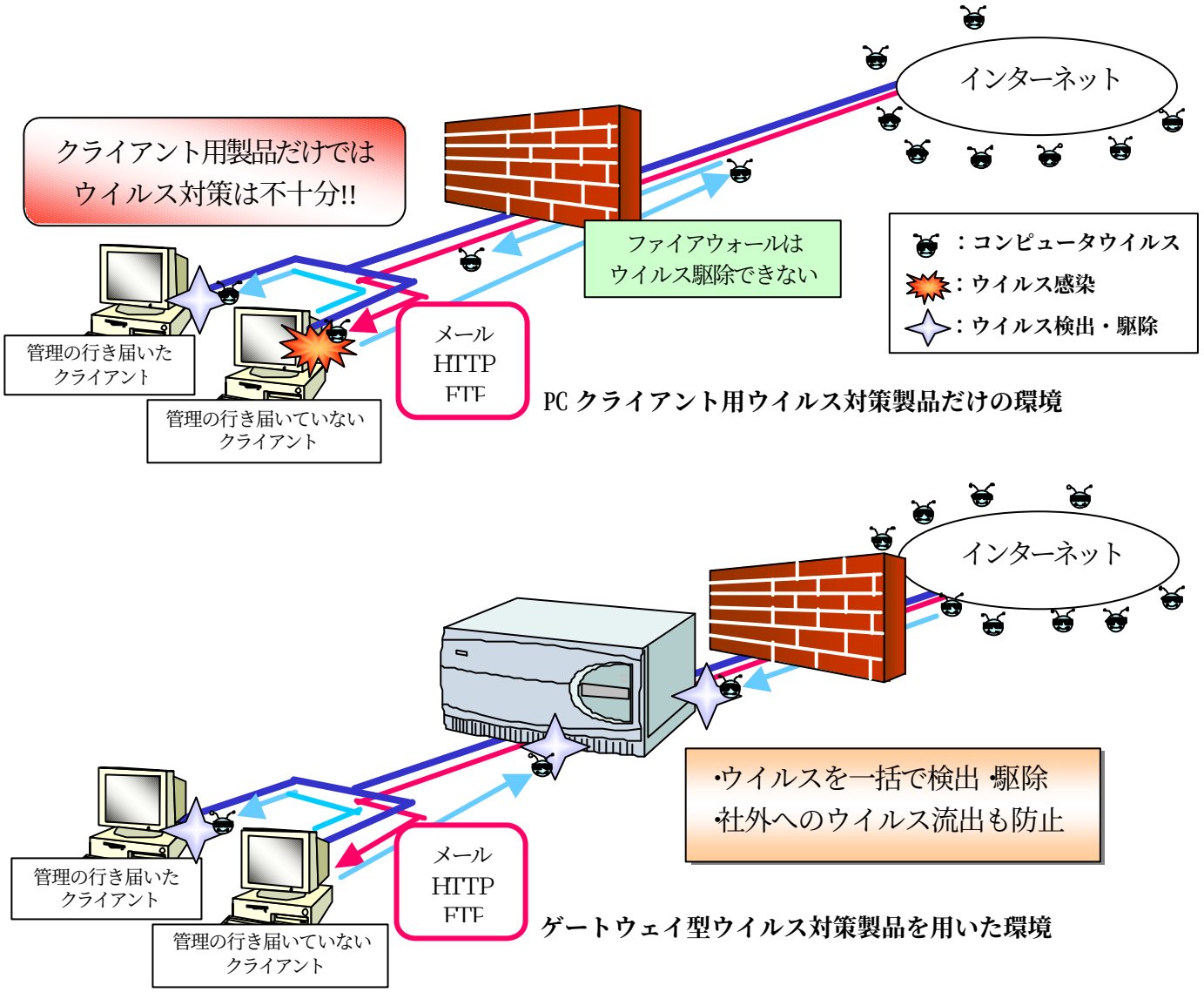


図-2　PC 用ウイルス対策製品とゲートウェイ型ウイルス対策製品の違い

また，企業の 95%が PC クライアント用ウイルス対策製品を使用している．しかし，その 10%がウイルスに感染している(2002 年 5 月の英国 MessageLabs の発表)．これは，PC クライアント用ウイルス対策製品だけでは，パターンファイルの更新やプログラムのアップデートなどの管理が行き届かずウイルスによる感染被害を防ぎきれないことが原因と言われている．

これに対して，ゲートウェイ型ウイルス対策製品におけるウイルス検索は，メールの送受信や Web コンテンツの閲覧を一括してウイルスチェックすることができる．

このことから，個々のパソコンにインストールされたウイルス対策製品とゲートウェイ型ウイルス対策製品を併用することで，より確実なウイルス対策を行うことができる(図-2 参照)．

2.NetShelter/VW の概要

2.1 対象ユーザ

NetShelter/VW は，中小企業や学校，地方自治体などをターゲットとし，サポートするユーザ数は最大 200 ユーザである．

2.2 コンセプト

導入・運用が簡単に行えるゲートウェイ型ウイルス対策専用装置(アプライアンス)である．

導入においては，ソフトウェア製品と比較して，ハードウェアや OS，アプリケーションについての専門知識を必要とせず，ネットワークに接続し Web ブラウザを使って簡単な設定を行うだけで運用を開始できる．そのため，専任の管理者がいない環境にも適している．

また，ファームウェアの更新については，アップデート用の CD をセットするだけで適用できる．

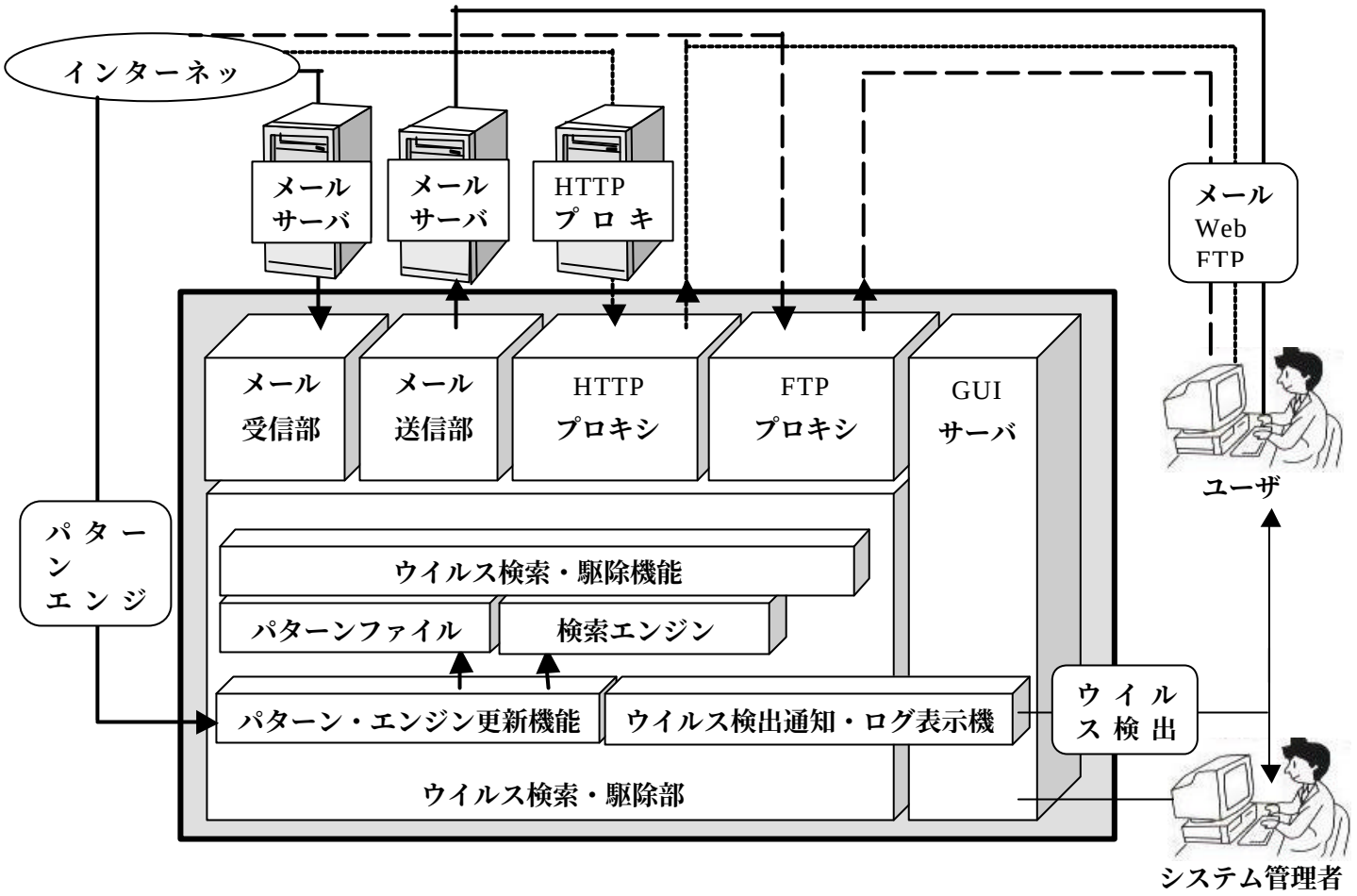


図-3　システム構成図

2.3 主要機能

ここでは，本装置のシステム構成図を図-3 に示すと共に本装置の主要機能であるウイルス検出・駆除機能について説明する．

(1) ウイルス検索・駆除機能

NetShelter/VW が中継する電子メール，Web コンテンツ，FTP 転送ファイルに対してウイルス検索を行い，ウイルスを検出した場合，それを削除する機能を持つ．

ウイルス検索にはウイルス情報データベースであるウイルスパターンファイルと，ウイルス検索を行うためのプログラムであるウイルス検索エンジンを使用する．

(2) ウイルス検出通知・ログ表示機能

NetShelter/VW がウイルスを検出した場合，あらかじめユーザによって指定された管理者に，ウイルス感染を通知する電子メールを送信する．また，NetShelter/VW が中継する電子メールからウイルスを検出した場合は，その受信者と送信者に対しても，ウイルス感染を通知することが可能である．

さらに，管理者が Web ブラウザからウイルス検出ログを確認することもできる．

(3) パターン・エンジン更新機能

最新のウイルスに対応するためには，ウイルスパターンファイルとウイルス検索エンジンを常に最新に保つ必要がある．NetShelter/VW では，これら二つのファイルの自動更新を行う機能をもつ．更新作業はユーザの指定した間隔，時間帯にインターネット経由で実施する．

3.NetShelter/VW の特長

3.1　実績ある InterScan のウイルス検索・駆除

NetShelter/VW のウイルス検索・駆除部には，Gateway 型ウイルス対策製品の 41.3%もの世界シェアを持つ[注1)]トレンドマイクロ社の InterScan VirusWall の技術を使用している．NetShelter/VW が中継する電子メール，Web コンテンツ，FTP 転送ファイルの各データを，ウイルスパターンファイルのウイルス情報と比較することでウイルス検索を実施し，ウイルスを検出した場合は，あらかじめユーザによって指定されている方法に従いウイルスに感染したファイルを処理する(図-4 参照)．処理方法には，「自動駆除」「削除」「放置」の 3 種類がある．

HTTP や FTP のウイルス検索は，ユーザがデータのダウンロードを要求してから，実際にダウンロードを開始するまでの間にウイルス検索を行う．このウイルス検索にかかる時間がユーザの負担にならないように，一般的なアクセス頻度やデータ量の調査・分析，性能測定を実施し，最大同時コネクション数など InterScan VirusWall のパラメタを最適な値に設定している．

注１）　出展:IDC："Antivirus Software 2002: A Segmentation of the market" Aug 2002

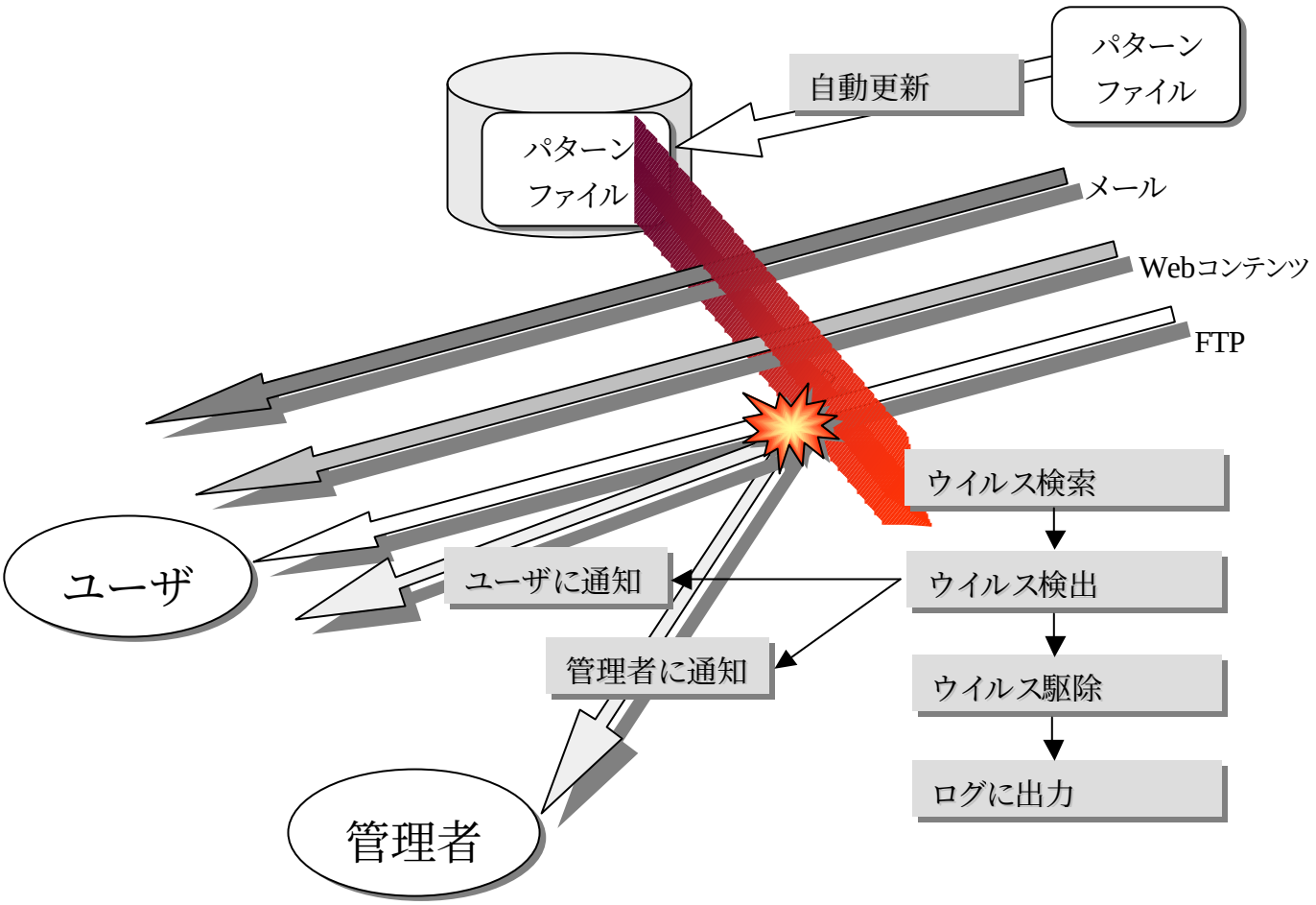


図-4　ウイルス検索のイメージ図

3.2 高信頼，コンパクトな専用ハードウェア

NetShelter/VW のハードウェアは，装置の小型化(当社製ワークステーションとの体積比 51%，表 -1参照)と，ネットワーク製品として 24 時間運転に耐えうる高信頼性を実現している．

ハードディスク，電源などの寿命部品を冷却するため 80mm 角の装置ファンは，低速度回転による静寂性(稼動時 42.5dB(A)以下を実現)と高冷却性能を実現した．

メモリは ECC(1 ビット誤り訂正，2 ビット誤り検出)を装備しており，ソフトウェアエラーによる異常動作を排除し，安定した動作を保証する．

表-1　ハードウェア仕様

項　　目		仕　様
インタフェース	LAN	10/100BASE-TX×1
	UPS接続ポート	RS-232C×1
諸元	外形寸法	278×240.5×135mm
	重量	6.0Kg
	消費電力	45W

3.3 簡単導入

(1) 選定・手配が容易

単機能かつハード・ソフト一体型であるため，ハードウェアや OS，アプリケーションの選定が不要であり，手配も容易になる．エンドユーザや販社，ベンダーにとって扱いやすい製品である．

(2) インストールが不要

NetShelter/VW は出荷状態でソフトウェアが組み込まれているため，インストール作業は不要である．

(3) Web ブラウザを使ったかんたん設定

初期導入時の設定を Web ブラウザから行うことができる．Web ブラウザでアクセスする NetShelter/VW の設定画面は，全て日本語で表示し，簡単に設定できる構成にしている．また，設定後はネットワークに接続し，すぐに運用を開始することができる．

3.4 簡単運用

(1) 検索エンジンの自動更新

NetShelter/VW は，トレンドマイクロ社が Web 上で公開する最新のウイルス検索エンジンを自動的に更新する独自の機能を搭載している．

ウイルス検索エンジンが自動更新された際には，システム管理者に更新の完了を通知するメールが送信されるため，ユーザは新しいウイルス検索エンジンのリリース状況などを気にすることなく運用を続けることができる．

(2) 専用 CD-ROM によるファームウェア更新

システム管理者は，ゲートウェイ型ウイルス対策ソフトがプレインストールされた製品などを利用する場合，OS や InterScan VirusWall の更新プログラムがリリースされるとダウンロードサイトからプログラムを取得し，適用・再設定を行う必要がある．一方 NetShelter/VW は，全登録ユーザ[注2)]に配布されるアップデート用の CD を装置にセットして再起動するだけで更新プログラムを適用する．また，設定内容を自動的に引き継ぐため，アップデート後の再設定も不要である．

注2） NetShelter/VW をご使用の際は，必ずユーザ登録をしていただく必要があります．

3.5 高信頼性

(1) SNMP [注3)] エージェント機能

SNMP エージェント機能を搭載しており，ネットワーク管理ソフトによる装置の状態監視が可能である．また，ファン異常や CPU の温度異常などを始めとするハードウェアの障害や，ウイルス検出時の Trap 通知にも対応している．

(2) SSL [注4)] による GUI との通信の暗号化

SSL により，管理者の端末と NetShelter/VW の設定画面との通信の暗号化を実現した．これにより設定画面との通信の安全を確保することができる．

(3) 管理者用端末の指定

管理者用の端末を指定することで設定画面へのアクセスを制限できるため，第 3 者による不正な設定変更などを防止できる．

(4) UPS [注5)] との連携

停電や瞬電への対応として，UPS との連携機能を備えており，オプションの UPS を接続することで電源異常時に安全にシステムを停止することができる．

注3） Simple Network Management Protocol の略．ネットワーク上に接続された通信機器をネットワーク経由で監視・管理するためのプロトコル．

注4） Secure Sockets Layer の略．Web ブラウザと Web サーバ間で安全な通信を行うために Netscape Communications が開発した技術．

注5） 無停電電源装置．

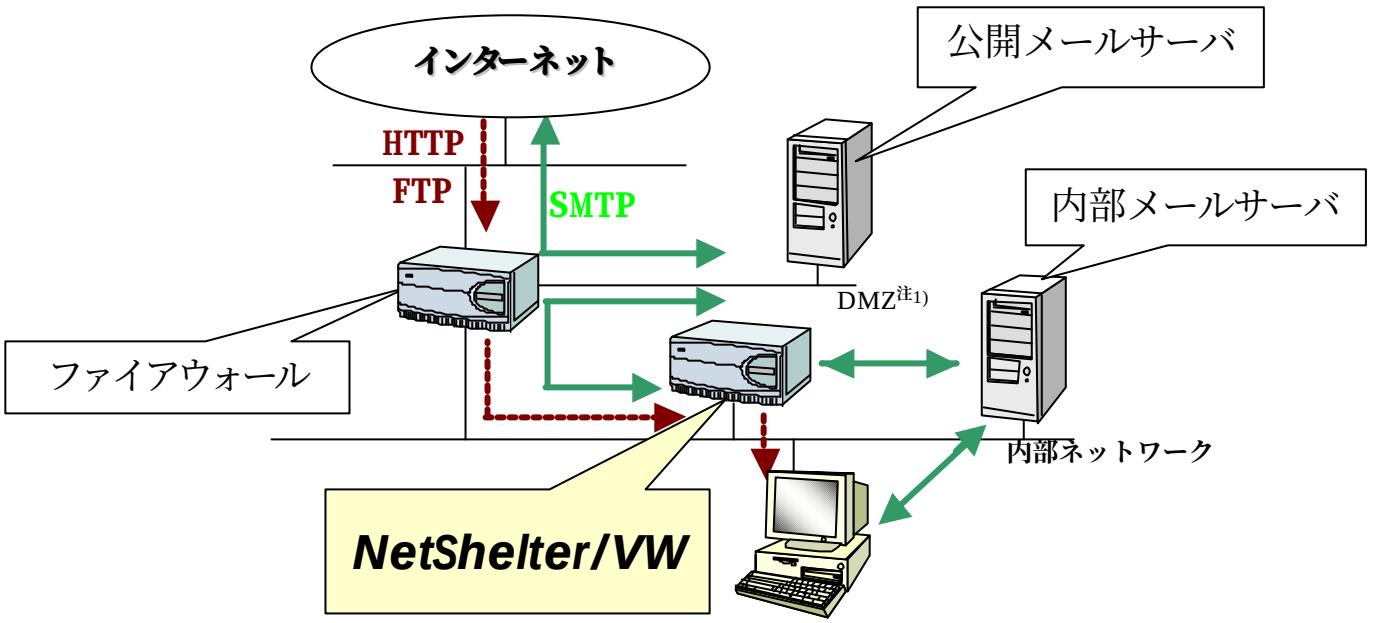
4.設置例

NetShelter/VW の設置位置について，ファイアウォールとの位置関係で示した場合，以下のパターンが考えられる．

4.1 ファイアウォールの内側に設置する場合

NetShelter/VW をファイアウォールの内側に設置する場合の構成例を図 5 に示す．

ファイアウォールの内側に設置することにより外部のネットワークから NetShelter/VW の存在が完全に見えなくなるため，より安全な構成である．また，クライアントのメールソフトの設定変更を行わずに NetShelter/VW の導入が可能である．



注1） De-Militarized Zone(非武装地帯)の略. DMZポートにはWebサーバやメールサーバなどの公開サーバを接続し，セキュリティを高めた上で外部からのアクセスも可能にする.

図-5　ファイアウォールの内側に設置する場合

4.2 ファイアウォールの DMZ に設置する場合

NetShelter/VW をファイアウォールの DMZ 上に設置する場合の構成例を図 6 に示す.

ファイアウォールの DMZ 上に設置する場合は, NetShelter/VW を最上位プロキシとすることでウイルス検索済みのコンテンツを配下のプロキシサーバにキャッシュすることができる. そのため, HTTP のリクエストがあるたびにウイルスチェックを行う必要がなくなり, ネットワークの負荷を軽減させることができる.

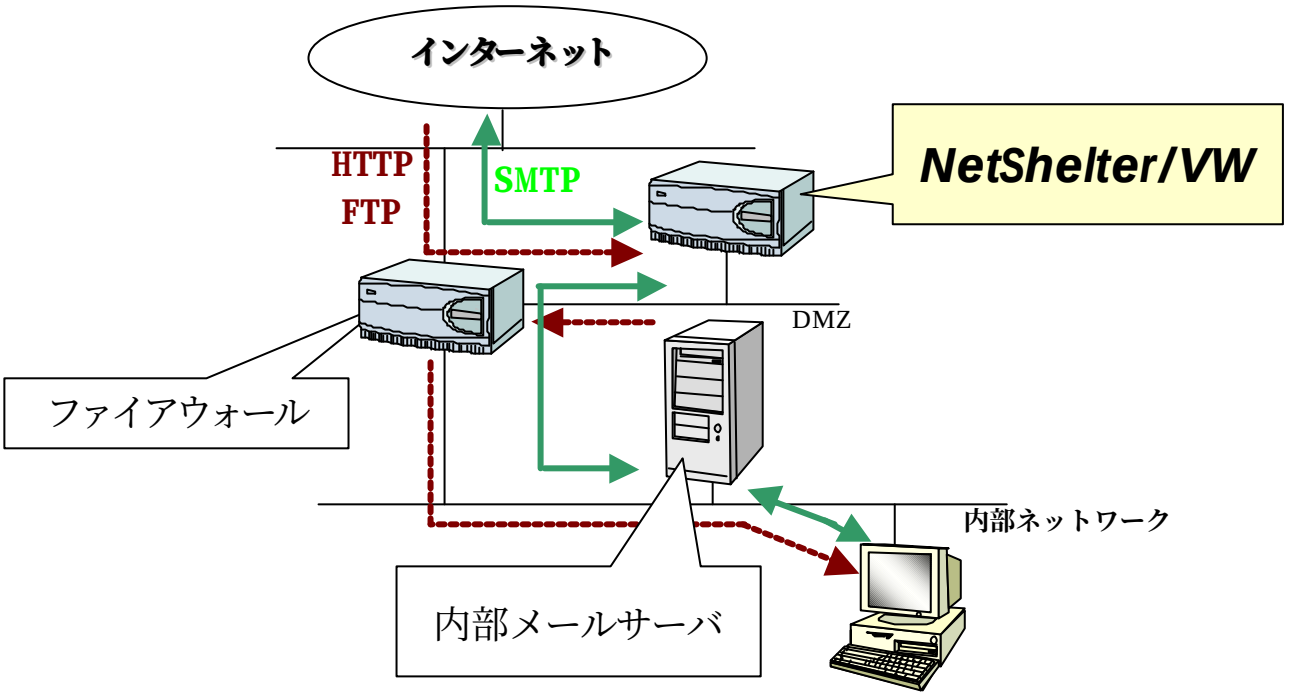


図-6　ファイアウォールの DMZ に設置する場合

5.適用ユーザ数、環境

5.1 適用ユーザ数の考え方

使用する中継機能の組み合わせやデータ量，データの種類などにより処理性能が変化するため正確な指針を示すのは困難であるが，目安として以下のような指標値を持っている．

(1)ユーザ数が 200 ユーザ以下であること

NetShelter/VW は，本体装置 1 台あたりの最大ユーザ数が 200 ユーザである．
200 ユーザ以上の環境の場合は，InterScan VirusWall 等のソフトウェア製品の導入か，NetShelter/VW 複数台の導入を検討する必要がある．

(2)200 ユーザで想定した負荷以下であること

導入する環境が下記に示す 200 ユーザを想定した負荷以下である必要がある．

SMTP:8 時間あたり 40,000 通 (1 通あたり 40KB)
HTTP:ピーク時の最大リクエスト数が 1 分あたり 180 ページ (1 ページあたり 5KB×10 ファイル=50KB)
FTP：8 時間あたり 200 ファイル (1 ファイルあたり 30MB)

HTTP の値は，あくまでピーク時の最大値．上記の値に相当するリクエストを継続して受けつづけた場合，中継処理に遅延が生じる可能性がある．
また，上記の値以上のリクエストを受けた場合，中継処理が遅延する可能性がある．

(3)ユーザ環境に応じたライセンスモデルを使用すること

ユーザは 50，100，200 ユーザモデルからユーザ環境にあったモデルを購入する．
購入したモデルのユーザ数以上のユーザでは利用できない．

5.2 複数台での運用

ユーザ数が 200 ユーザ以上の環境で使用する場合や, ネットワークの負荷が高い場合に NetShelter/VW を複数台使って運用することができる．運用形態として以下のような対応が考えられる．

(1)ユーザごとに分けて使用する

200 ユーザ以上の環境で使用する場合やウイルス検索のパフォーマンス向上を図りたい場合,
使用する NetShelter/VW をユーザ数ごとに割り振り，運用する．

(2)プロトコルごとに分けて使用する

200 ユーザ以下の環境で, ウイルス検索のパフォーマンス向上を図りたい場合, 処理を担当する NetShelter/VW をメール用や Web ページ用，FTP 用などプロトコルごとに割り振り，運用する．