ファイアウォール専用装置

GeoStream NetShelter/FW

プロダクトレポート

富士通株式会社

２００１年４月

目次

1 はじめに ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1

1.1 ファイアウオールの必要性 1

2 NetShelter/FW の特長 ・・・・・・・・・・・・・・・・・・・・・・ 2

3 機能 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3

3.1 Firewall 機能 3

3.1.1 アドレス変換機能 3

3.1.2 動的 NAT 3

3.1.3 静的 NAT 4

3.2 IP フィルタリング 4

3.3 URL フィルタリング 5

3.4 VPN 機能 5

3.4.1 暗号通信機能 6

3.5 Safegate client 機能 7

3.5.1 ユーザ認証機能 (モバイル PC 接続機能) 7

3.5.2 ローカル認証とリモート認証 8

3.6 W eb キャッシュ 8

3.6.1 対応プロトコル 8

3.6.2 システム形態 9

3.7 DHCP サーバ機能 9

3.8 ロギング機能 9

3.9 アラート機能 10

3.10 syslog 10

3.11 ネットワーク管理機能 11

3.11.1 SNMP エージェント機能 11

3.11.2 Safegate 集中管理 11

3.12 メール通知 12

4 ハードウェア仕様 12

5. かんたん導入/設定/運用 ・・・・・・・・・・・・・・・・・・・・・・ 13
5.1 導入/設定の容易さ.....13
5.2 運用の容易さ.....14
5.3 高信頼性・運用性.....15
6 導入例 ・・ 15
6.1 DMZ に公開サーバを設置した形態 ・・・・・・・・ 16
6.2 VPN(IKE を使った IPsec 通信)形態 ・・・・・・・ 16
6.3 リモート端末（モバイル PC）形態 ・・・・・・・ 17

1 はじめに

1.1 ファイアウオールの必要性

Internet に接続される装置は、悪意を持ったものから攻撃を受ける可能性があり、Firewall が必要である。Internet 上には、WWW や FTP サーバといったサーバ群、サーバへアクセスするクライアント端末等がある。これらは Internet 上の不特定多数の端末/サーバとの通信が可能となっている。不特定多数の相手の中には、悪意を持ったものもあり、攻撃を受ける可能性が出てくる。

その結果、

- データの盗聴
- データの改ざん
- サービス不可 DOS(Denial Of Service)
- 内部侵入
- 別サーバ(他社を含む)へのアタックの踏み台

とされる

等の被害を受ける可能性がある。

Internet に接続されている装置は、攻撃に対する防御が必要である。Internet に接続していると、不特定多数より自由にアクセスされる。万が一、サーバ(および端末)にセキュリティホールがあると、上記の様な被害を受ける可能性がある。

この様な被害を受けないようにするために、

- 提供サービスのセキュリティ確保
- 提供サービス以外のセキュリティを確保

といった処置が必要である。

これらの対策を行うために、Firewall を用いるのが一般的である。

Firewall を導入することにより、

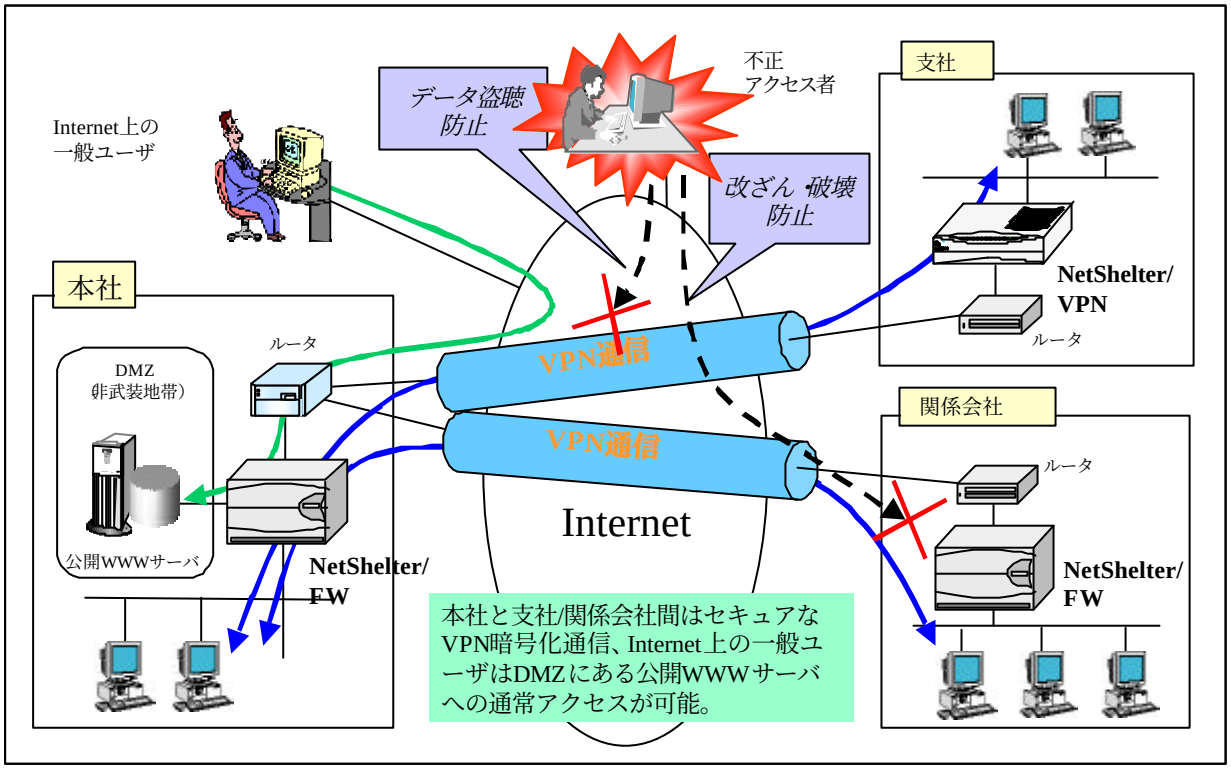
- 提供サービス以外のセキュリティを確保
- 通過させるべきパケットを選別
- ログ管理
- 不正なアクセスの検知

等が可能となる。

2 NetShelter/FW の特長

NetShelter/FW はファイアウォールの他に VPN機能とおよびキャッシュ機能を搭載したセキュリティ専用装置である（図－1 参照）.

NetShelter/FW では， IP フィルタや[sano1]URL フィルタなどのファイアウォール機能，業界標準の VPN 規格である IPsec 準拠の暗号化機能，インターネットアクセスの高速化に向けた WEB キャッシュ機能，さらに公開サーバの設置に適した DMZ 構築用に LAN インタフェースを 3 ポート標準装備する.



図－１ NetShelter／FWの利用概念

(1)国際認定が証明する高いセキュリティ

ISO15408 を取得（国内初）した Safegate ベースの装置
セキュリティ製品認定として世界的に認知されている ICSA 認定を取得（予定）

(2)VPN を標準搭載したファイアウォール専用装置

多彩な機能（NAT、DMZ 対応、VPN、Web キャッシュ）を標準装備したオールインワン

(3)100Mbps-LAN をターゲットとした高性能

パケット処理能力は 1 万 pps を実現

3 機能

NetShelter/FW の主な機能を以下に示す。

3.1 Firewall 機能

Firewall 機能としては、次のような機能を有する。

・ アドレス変換機能
・ IP フィルタ機能

3.1.1 アドレス変換機能

NAT(Network Address Translation)機能とは、アドレス変換をおこなう機能である。

NetShelter/FW では通常のアドレス変換に加えて、ポート番号も変換をおこなう。これにより、複数のアドレスを 1 つのアドレスへ変換する事も可能である。

NAT 機能を使用する事により、外部から内部ネットワークのアドレスを隠蔽し、外部からの直接の攻撃を防ぐ他に、内部ネットワークとしてプライベートアドレスを使ったネットワーク構成が可能となる。

変換方式としては、動的 NAT と静的 NAT の 2 つの方式をサポートしており、変換は

・ LAN0 と LAN1(注 1)
・ LAN2 と LAN1
・ LAN0 と LAN2 (E11L10 より)

との間で可能である。

(注 1) LAN0 は内部ネットワーク、LAN1 は外部ネットワーク、LAN2 は DMZ ネットワークを示す。

3.1.2 動的 NAT

動的 NAT とは、内部ネットワークからのコネクションを管理し、許可されたサービス／コネクションを中断する際に、動的にアドレスとポート番号を変換するものである。内部ネットワークから、外部ネットワークへアクセスする際にのみ使用可能であり、変換後のアドレスは LAN1 のアドレスとなる。(同時に利用可能なコネクション数は、400 となる)

NetShelter は、送信元IP アドレス(内部ネットワークの IP アドレス)と送信元ポート番号を NetShelter/FW の IP アドレスとポート番号に変換して外部ネットワークに送信する。当該パケットの応答パケットに関しては、NetShelter/FW 宛の IP アドレスとポート番号を、内部ホスト宛の IP アドレスとポート番号に戻して、内部ホストに送信する。

外部ネットワークから内部ネットワークに対して異なる接続を要求するサービスや、ホスト間通信において、IP アドレス、ポート番号の情報を交換するサービスについては、下記サービスを除いてサポート範囲外とする。

・ FTP(port/pasv)
・ RealAudio/RealVideo
・ StreamWorks
・ VDOLive
・ CU-SeeMe

3.1.3 静的 NAT

静的 NAT とは、アドレス変換のルールをあらかじめ設定しておき、ルールに合ったパケットのアドレスを変換する方式である。これにより、特定の内部ホストアドレス（例えば、DMZ上の公開サーバ）を固定的に変換する指定をしたり、外部ネットワークからのコネクション確立要求や、ストリーム系アプリケーションを使用する事が可能となる。

外部ネットワークへのアクセスもしくは、外部ネットワークから内部の特定ホストへのアクセスの際に用いられる特定内部ホストのアドレスは、32 個まで定義可能である。

なお、静的 NAT では複数アドレスを同一アドレスに変換させることはできない。また、変換後のアドレスを LAN1 と同一ネットワーク内のひとつとした場合、LAN1側ネットワークに対して ARP の擬似応答を行ない、LAN1と異なるネットワークのアドレスとした場合、RIP を LAN1 へ広報する。

3.2 IP フィルタリング

IP フィルタリングとは、
・ 送信 IP アドレス
・ 受信 IP アドレス
・ ポート番号
といった条件によってアクセス制御を行うものである。また、対象パケットは、
・ TCP
・ UDP
・ ICMP
・ ESP パケット
のパケットとなり、アクセス制御には
・ 通過(pass)
・ 破棄(block)
・ NAT(trans)
といった指定が可能である。

この機能を利用する事により、意図していないプロトコルの遮断(使用プロトコルの限定)、外部からのアクセスの制限等が可能となる。

出荷時のデフォルトでは、
・ 環境設定のための Web ブラウザアクセス
・ 疎通確認用 ping
などが通過可能となっている。これら以外は、全てのパケットを遮断する設定になっているため、使用する際には、通過させるアドレス/プロトコル等を設定する必要がある。

なお、簡単設定で設定されるフィルタに関しては、取扱説明書を参照ください。

また、フィルタリング条件を設定する際に以下の総称サービス名を指定することができる。

TCP-ALL　　TCP 上のすべてのサービスを意味する。

UDP-ALL　　UDP 上のすべてのサービスを意味する。
ICMP-ALL　　ICMP 上のすべてのサービスを意味する。
ALL　　すべてのサービスを意味する。
ただし、ICMP-ALL と ALL 指定時は NAT(trans)を指定することはできない。

ORACLE 使用時の注意事項
ORACLE のサーバ・クライアントの通信では、次の 2 通りの方式がある。
- シングルサーバモード(SQL*Net V1 互換)
- マルチサーバモード

シングルサーバモードでは、サーバ側のサービスポートが固定の運用となるため、厳しいフィルタリングが可能であるが、マルチサーバモードではサーバ側ポート番号が不定となるため、広範囲のフィルタリング条件の設定が必要となる。

顧客とのセキュリティポリシーの立案において、同意が得られるならば、特定のクライアント、サーバ間で TCP-ALL、UDP-ALL などの層証明サービスを使ったフィルタリング条件を設定することで、通信させることが出来る。

3.3　URL フィルタリング

URL フィルタリングとは、アクセス先 URL 単位でアクセス制限をかける機能である。アクセス制限は禁止する URL のみ指定可能で、許可をする URL は指定できない。本機能を使用する事により、公序良俗に反するサイトなどへのアクセスを禁止する事が出来る。
URL の指定は
・ URL そのもの
・ URL 内のキーワードによる条件組み合わせ
によって、指定可能である。
ただし、特定の IP アドレスからのアクセスのみは、URL フィルタリングを迂回させるという指定も可能である。
なおこの機能は、NetShelter/FW を proxy としたアクセスのみ対象となるので、URL フィルタリングを使用する場合は、クライアント側の proxy の設定が必要となる。

3.4　VPN 機能

Virtual Private Network(VPN)とは、インターネット等の公共のネットワークを利用し、低コストで専用線相当のセキュリティを持ったネットワークを実現するものである。
インターネット等の公共のネットワークでは、容易にパケットを盗み見る事が出来、データの盗聴、改ざんが可能である。したがって、VPN を実現するために、暗号化、認証機能等を行っている。
VPN 機能では、IP のみサポートしており、IP 以外は中継されない以外は中継されない以外は中継されない。
なお、VPN 機能では NAT 等の特別なアドレス変換を行っていないため、マルチメディア系などクライアントがコネクション接続後､サーバ側より別コネクションを接続するサービスに対しても対応可能である。

3.4.1 暗号通信機能

暗号通信機能とは、VPN 装置間のデータを暗号化する機能であり、NetShelter/FW で登録可能な暗号通信相手先は最大 128 までである。また、同一暗号通信相手先に対して、登録可能なホストもしくはネットワークは４つまでである。

NetShelter/FW は暗号化の手法として、独自方式(Safegate 方式)と RFC で規定されている IPsec 方式を提供している。この機能を利用する事により、NetShelter/FW 間で接続するネットワークを VPN 化する事が出来、セキュリティを確保する事が可能となる。

NetShelter/FW での暗号化の動作は、受信したポートによって処理が異なる。内部ネットワークから受信したパケットは、暗号化しカプセル化して外部ネットワークへ送信する。また、外部ネットワークから受信した暗号データは、復号化して内部ネットワークへ送信する。

3.4.1.1 暗号化の条件(アドレス指定方法)

NetShelter/FW が暗号化してパケットを送信するかどうかは、オリジナルの IP パケットの送信元アドレスおよび、送信先アドレスを元に制御している。暗号化の条件は、128 サイトまで登録可能である。

なお、相手ゲートウェイを重複させる事は出来ないので、相手ゲートウェイ 1 つに対して、最大 4 ネットワークまたはホスト定義までとなる。一つのネットワーク定義には、「通信クライアント」と「通信サーバ」の二つがあり、これが対で指定される。

暗号化対象とするアドレスの指定は、アドレスとマスクで指定を行う。その際、クラス A やクラス B/C といったクラスは関係なく、マスク指定が可能であるので、複数のネットワークをまとめて指定可能である。ただし、NetShelter/FW の複数のインタフェースを跨いだ指定はできない、

また、同一ゲートウェイに対して、複数のネットワークを暗号化の対象としたい場合は、マスクを調整するか、通信クライアント/サーバを追加する必要がある。また、マルチキャストやブロードキャストパケットは、暗号化できない。

3.4.1.2 暗号方式の仕様

独自方式、IPsec 方式の仕様を以下に示す。NetShelter/FW では、サイト間の暗号化方式は装置単位で 2 つの暗号方式のうち、どちらか一方のみの選択となるので、対向相手によっては、一台の NetShelter/FW では対向できない。ただし、Safegate client は、上記の設定に関係なく利用可能である。通常は IPsec を使用すれば良い。

IPsec 方式には、IPsec 方式に必要な情報である暗号鍵や SPI （Security Parameter Index ）などを手動で設定して行うマニュアル方式と、システムが定期的に更新を行う IKE (Internet Key Exchange ）方式の 2 種類の方式があります。

・ IPsec （IKE ：リリース 1 ）方式(E11L10 より)
NetShelter/FW E11L10 と IPsec （IKE ）接続する場合に使用します。
・ IPsec （IKE ：リリース 2 ）方式（E11L11 より）
NetShelter/FW E11L11 以降、または LR-X シリーズと IPsec （IKE ）接続する場合に使用します。

表－１ 暗号通信方式

	IPsec 方式(マニアル/IKE)	独自方式(Safegate 独自)
パケット暗号方式	ESP(暗号ペイロード)	独自方式
パケット認証方式	認証付き ESP(AH 無し)	独自方式
暗号アルゴリズム	DES-CBC(鍵長 56bit)	DES-CBC(鍵長 56bit)

	3-DES-CBC(鍵長 168bit)	
認証アルゴリズム	HMAC-MD5-96 HMAC-SHA1-96	―
暗号鍵	送信と受信で別々である 16 桁の 16 進数(MD5)、 送信と受信で別々である 48 桁の 16 進数(SHA1)、	64 文字以内の英数字
認証鍵	送信と受信で別々である 32 桁の 16 進数(MD5)、 送信と受信で別々である 40 桁の 16 進数(SHA1)、	―
送信 SPI	値変更可能	―
受信 SPI	値変更可能	―
鍵更新.	マニュアル設定 IKE(Pre-Shared KEY)	1 時間単位で更新間隔指定可能
鍵管理	オフライン IKE(Pre-Shared KEY)	オフライン
自動鍵交換	ＩＫＥ	なし
暗号通信相手	NetShelter シリーズ Safegate V2.0, LR-X シリーズ	NetShelter シリーズ Safegate V2.0 Safegate client V2.0
暗号通信	認証付き ESP(ESP_AUTH)	UDP にて暗号パケットをカプセル化(ポート番号は 9337: 変更可能)
暗号化条件単位	送信先/送信元アドレス (IP アドレス、ネットマスク)	送信先/送信元アドレス (IP アドレス、ネットマスク)

IPsec は以下の標準仕様に準拠している。

- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406: IP Encapsulating Security Payload (ESP)

3.5 Safegate client 機能

3.5.1 ユーザ認証機能 (モバイル PC 接続機能)

ユーザ認証とは、IP アドレスを認証に使用せず、ユーザ ID とパスワードを用いて行う認証であり、IP アドレスが不定なモバイル PC との認証に使用する。なお、使用可能な Safegate client のバージョンは V2.0 以降であり、モバイル PC に Safegate client をインストールしておく必要がある。

NetShelter/FW は Safegate client を用いる事により、モバイル PC との間で暗号通信を行う事が出来、同時に接続できる Safegate client は最大 32 台までである。なお、モバイルで利用できる暗号方式は独自方式(Safegate 方式)のみである。

認証には、以下の情報が使用される。

・ ユーザ ID
・ パスワード(固定パスワード:CHAP 、S/Key 、SecurID リモート認証時)

Safegate client と NetShelter/FW 間の通信は、オリジナルパケットを暗号化したあとカプセル化通信を行なうもので、途中経路に NAT 装置が存在しても通信は可能である。

注意！----------

Safegate client と NetShelter/FW との通信は、途中経路に NAT 装置が介在した場合、パケットのサイズ(MTU 長)に留意する必要がある。

- 通信に先立って暗号化とパケットのカプセル化により、Safegate client と NetShelter/FW 間で送受信されるパケットは、オリジナルのパケットより大きくなる。
- NAT 装置あるいは、廉価なルータ機器では、分割されたパケットを正常に中継できない場合がある。

対処方法としては End-End 間で MTU 長を短くする等調整を行なう。

3.5.2 ローカル認証とリモート認証

NetShelter/FW では、ローカル認証とリモート認証のどちらか一方を選択する事が出来る。ローカル認証とは、NetShelter/FW 自身で認証を行う方式であり、リモート認証は、RADIUS サーバを使用して認証を行う方式である。

ローカル認証を用いた場合は、登録できるユーザ数は最大 32 ユーザまでで、同時接続数は最大 32 ユーザまでである。ローカル認証では、認証するためのユーザ情報とアクセス記録は NetShelter/FW に保管・管理される。

リモート認証(RADIUS サーバ連携)は、ユーザからの接続要求に対し、NetShelter/FW が RADIUS サーバにユーザ認証を依頼し、承認可否を処理する機能である。登録できるユーザ数は RADIUS サーバ次第で、同時接続数は最大 32 ユーザまでである。また、リモート認証では、ユーザ情報とアクセス状況が RADIUS サーバ側に保管・管理され、複数のアクセスポイントが存在する場合は、ユーザ管理、アクセス状況を一元管理する事が可能である。

リモート認証の対象 RADIUS サーバは Safeauthor V2.0 である。

また、Safeauthor と ACE/Server を使用することにより、SecurID も利用可能である。

3.6 Web キャッシュ

Web キャッシュとは、http 、https 、gopher プロトコルに対応したキャッシュ機能の事である。Web キャッシュは、キャッシュ容量は約 2GB で、URL フィルタを使用することが可能である。

Web キャッシュの動作は proxy モードで動作し、Web キャッシュが利用可能なコネクション数は最大 240 である。

Web キャッシュを使用可能なポートは LAN0 のみであり、LAN1,LAN2 からは使用できない。

3.6.1 対応プロトコル

次のサービスに対する代理アクセスとデータキャッシュ機能を提供する。

・ http
・ https

・gopher

HTTP プロトコルについては、CGI の出力、cookie 、SSL などは透過する。また、http 1.1 の keep-alive にも対応している。

3.6.2 システム形態

インターネット上の Web サーバへの中継、および、上位/下位の proxy サーバとの中継が可能である。Web サーバ/proxy サーバへは http ポート番号への中継で、キャッシュで使用される ICP 連携はサポートしない。また、上位 proxy サーバを指定した場合、上位 proxy サーバを経由しないドメインの指定も可能である。

NetShelter/FW が上位 proxy となる形態の場合は、本機の http ポート番号でのアクセスが可能。

3.7 DHCP サーバ機能

DHCP サーバ機能とは、DHCP クライアントへ IP アドレスの自動割当を行う機能である。NetShelter/FW の DHCP サーバ機能は RFC1541 に準拠している。

小規模サイトでのネットワークアドレスの割り振りの簡易化や、モバイル PC など移動端末のアドレスの有効利用を目的に DHCP サーバ機能を提供する。

IP アドレスの割り当ては、DHCP クライアントの要求に対して割当範囲内のアドレスを動的に割り当てていく方法と、特定の MAC アドレスに対し、特定の IP アドレスを静的に割り当てる方法の 2 種類をサポートしており、動的および静的を合わせて 253 個のアドレスを管理できる。ただし、静的割り当ては 32 までである。また、DHCP サーバより、DHCP クライアントへ通知可能な情報は、DHCP クライアントへ割り当てる IP アドレス／リース期間／デフォルトルータの IP アドレス／ DNS サーバの IP アドレス／ドメイン名 である。

3.8 ロギング機能

NetShelter/FW の Firewall 機能および web-cache 機能について、各々動作状況ログと統計情報ログを記録管理する。また、VPN 通信機能において、処理状況ログを記録する。記録単位は、機能単位(IP フィルタ、URL フィルタ、VPN 通信機能、Web-cache)毎に 1 日単位で、保存方法は、保存日数の間サイクリックに保存していく（ログの量が多く格納領域をオーバする場合は、保存日数が指定の日数未満となる）。

記録内容は、表３の通りである。

表 2 ログ一覧

フィルタリング種別	ロギング項目	備考
IP フィルタ	ロギング日時	
	処理パケット情報	IP アドレス、プロトコル、サービス
	処理結果	通過, 破棄, NAT, 暗号
URL フィルタ	ロギング日時	
	処理 URL 情報	URL 、キーワード
	要求元クライアント情報	
VPN 通信機能	ロギング日時	
	VPN 通信処理パケット情報	IP アドレス、暗号、

Web-cache	ロギング日時	
	処理データ情報	IP アドレス、ポート番号

IP フィルタ、VPN 通信エラーなどのログ情報は、その必要性からリアルタイムに検索表示することが出来るが、Web-cache ログ、URL フィルタログは、統計情報として扱い、1 日前までのデータを基に編集処理を行って、日報、週報、月報として表示する。

また、システムとしての動作状況は syslog に記録する事が可能で、設定によりリモートの syslog サーバにも情報を送ることが出来る。リモートの syslog サーバに情報を送る場合も、ローカルには情報を残すものとし、最大確認可能行数は 1000 行とする。

なお、Firewall 機能のログおよび Web-cache 機能のログ、syslog の各情報は、Web ブラウザ経由により管理者の元に取り出すことが出来る。

3.9 アラート機能

アラート機能とは、次のようなイベント発生を契機としたアラートを通知する機能である。検出したアラート事象を syslog に記録すると共に、SNMP マネージャに SNMP トラップ情報として通知する。

表 3 アラートイベントと閾値

項目	ア ラートイベントとしきい値
同一送信元からのアタック	単位時間あたりの破棄パケット数
同一宛先へのアタック	単位時間あたりの破棄パケット数
暗号パケット改ざん検出	1 パケット検出
認証アラート	1 イベント単位
DiskFull(ロギング領域)	検出時

3.10 syslog

syslog は、システムのメッセージログの事であり、設定によりエラーメッセージやログ情報をネットワーク上の syslog サーバに記録する事が可能である。

NetShelter/FW は、syslog をサポートしエラーメッセージ等を syslog サーバに転送できる。また、転送するメッセージを装置内に保存しておく事も可能で、Web により 1000 件のログが閲覧可能である。

一般的に、ルータの様な補助記憶装置を持たない機器では、情報を記録する領域が少なく、装置に関する様々な情報をそれほど多く記録しておく事が出来ないため、最新の記録を残すために、古い情報を順に消去することが一般的である。(NetShelter/FW においても、記録量に限りがある) 古い情報が消去されるという事は、トラブルの解析やアクセス状況等を解析することは難しくなるという事であるため、必要であれば、外部の syslog サーバ(たとえば UNIX)に情報を送り、syslog サーバでハードディスク等の補助記憶装置に記録し、ログの管理を行うこと。

UNIX では標準の syslogd というデーモンでロギングする事が可能だが、Windows 等では標準でサポートされていないため、syslogd ソフトを導入する必要がある。

表 4 ｓｙｓｌｏｇ仕様

項目	内容
Web によるログ閲覧可能件数	1000 件
ファシリティ	kern(0), daemon(3)
プライオリティ	warn, err, crit, alert, emerg

3.11 ネットワーク管理機能

NetShelter/FW では、環境設定および稼動状況の監視は Web ブラウザによりリモートからの監視となる。ネットワーク管理機能として、SystemWalker 、NetEyeManager 等の SNMP マネージャによる管理と、Safegate 集中管理による管理の２ つの方式がある。

下記に Safegate 集中管理と SNMP マネージャ各々と連携して出来る機能を示す。

表５　Safegate 集中管理と SNMP マネージャの機能一覧

		Safegate 集中管理	SNMP マネージャ	備考
稼動監視	機器認識	手動登録	オートマップ機能により自動登録もしくは、手動登録	
	監視内容	システム稼動有無 稼動機能種別 適用ポリシーの作成日時	ネットワークトラフィック ・System グループ ・Interface グループ ・Address Translation グループ ・IP グループ ・icmp グループ ・tcp グループ ・udp グループ ・snmp グループ	SNMP マネージャでの統計的数字は、リモート操作での Web ブラウザからの確認可能
アラート監視		Syslog 内容	SNMP-Trap(内容は左に同等)	
リモート操作		Web ブラウザ起動によりリモート操作可能	同左	

一般的には、ネットワーク全体を監視する場合は SNMP による管理を行い、Safegate 等が入っている場合は、Safegate 集中管理を使用する。

但し、SNMP による監視では、NetShelter との通信は暗号化されないため、SNMP マネージャを用いて監視する場合は、ローカルでの監視を行うか、NetShelter 等で暗号通信を行って、セキュリティを確保すること。Safegate 集中管理に関しては、NetShelter との通信が暗号化されているため、暗号化を意識する必要が無い。

3.11.1　SNMP エージェント機能

NetShelter/FW では、SNMP の手順に従い MIB を特定ホストに送出する。

情報を受け取ったホスト(SNMP マネージャ)は、情報を元にネットワークの状態を監視する。

NetShelter/FW でサポートしている MIB は、MIB-II の範囲全てである。

3.11.2　Safegate 集中管理

Safegate 集中管理とは、Safegate や NetShelter を集中管理するソフトであり、NetShelter の運用監視を一元管理できる。Safegate 集中管理は、WindowsNT のソフトであり、これを利用する事によって UNIX が無くても NetShelter/FW のアラート情報や稼動状況を監視する事が可能となる。

Safegate 集中管理では、以下のものが管理可能である。

・ Safegate 集中管理連携機能

・暗号ゲートウェイ稼動状況監視
・認証ゲートウェイ稼動状況監視
・IPsec ゲートウェイ稼動状況監視
・暗号ゲートウェイアラートイベント監視
・IPsec 暗号ゲートウェイアラートイベント監視
・ 認証アラートイベント監視

3.12 メール通知

環境設定で設定された情報をもとに、メールでアラート通知やログの採取を行うことができる。(E11L10 より)
指定する項目は、
・メールによるログ採取を使用する
・メールを暗号化する
・メールサーバ
・アラートメール表題
・ログ採取表題
・送信先メールアドレス
・送信元メールアドレス
・ログ採取メール送信時刻
・ ログ採取メール再送期間

4 ハードウェア仕様

表 6 NetShelter/FW ハードウェア仕様

LAN インタフェース	10/100BASE-TX × 3(10M/100M 自動および手動切替え)
シリアルポート	RS--232C D-SUB9 ピン × 1(UPS 接続/保守用)
LCD パネル	16 桁 × 2 行
LED	電源(緑/アンバー)、アラーム(アンバー)
操作キー	4 方向+押し込み、
内蔵 I/O 装置	ハードディスク、CD-ROM(インストール、アップデート用)
外形寸法(幅×奥行×高さ)	278mm × 240.5mm × 135mm
重量	6Kg

NetShelter/FW のハードウェアは、コンパクトな筐体でありながらハードディスクドライブと CD-ROM ドライブを内蔵し、前面には LCD パネル、LED と操作キーを備え、専用装置として必要十分なユーザインタフェースを提供している。
前面の LED と LCD パネルにハードウェアの動作状態(通常時は IP アドレスや LAN インタフェースの接続モードを、ハードウェア異常時には異常要因など)を表示する。また操作キーと LCD パネルによるメニュー操作では、UPS 運用の切り替え、システムの停止など、基本的な設定、操作を行うことができるようになっている。
CD-ROM ドライブに NetShelter/FW 専用 CD-ROM をセットして装置を再起動すると、自動的に CD-ROM からシステムが起動される。この機能により、ソフトウェアのインストールやアップデートが容易に行えるようになっている。

5. かんたん導入/設定/運用

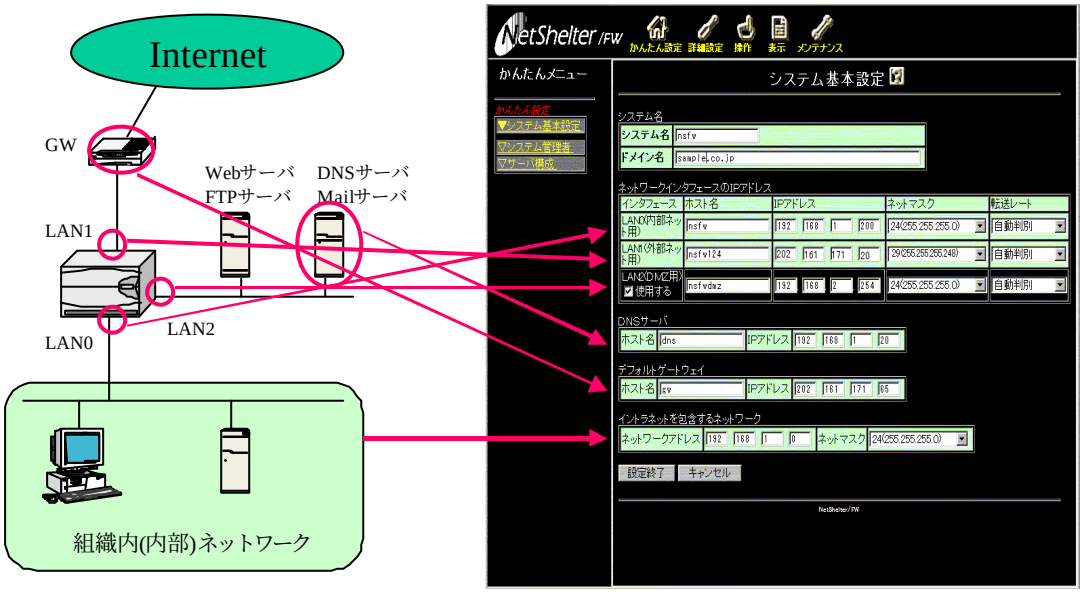
5.1 導入/設定の容易さ

(1) 選定・手配の容易さ

単機能かつハードソフト一体型であることから、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。このことは、エンドユーザとともに販社やベンダーにとっての扱いやすさにもつながる。

(2) 設定の容易さ

NetShelter/FW は，かんたん導入，かんたん設定を製品コンセプトとしており，広く普及した WWW ブラウザを GUI として採用している. 設定内容も短時間で導入から運用に入れるように，「かんたん設定」メニュー（図－2 参照）を用意する.



LAN0、LAN1,LAN2の各LANインタフェースに対するホスト名とIPアドレス設定とネットマスク、転送レートの選択、外部DNSサーバのホスト名、IPアドレスの設定、デフォルトゲートウェイのホスト名とIPアドレスの設定、組織内ネットワークアドレスの設定を画面に沿って行なって下さい。

図－２ NetShelter/FWの簡単設定メニュー画面

かんたん設定は，NetShelter/FW に対する装置情報と公開サーバの情報を設定するだけで，基本的な運用に入れるようにしている.

5.2 運用の容易さ

(1)状況表示、ログ表示機能

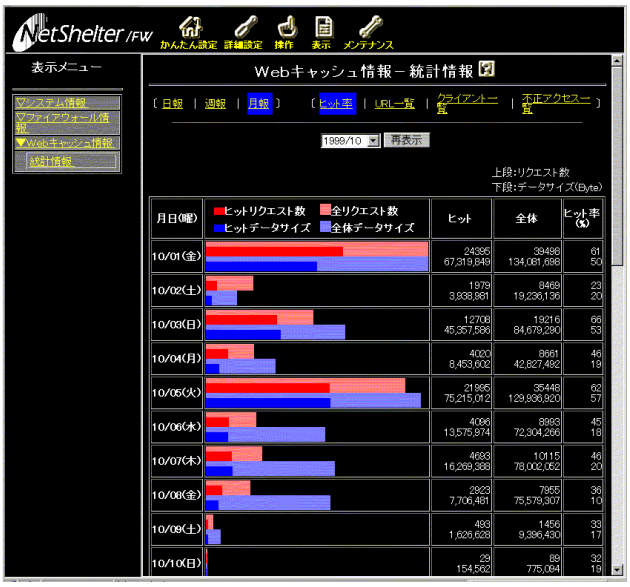
NetShelter/FW では、インストール後の動作状態の監視も WWW ブラウザから行うことができる。設定メニューから以下の情報、ログが参照可能である。また，統計情報表示にグラフを使うなど，操作および視認性に優れている（図－3 参照)．：

① システム稼動状況表示
　現在のソフトウェア版数、システム起動日、負荷状態、プロセス数、syslog など

② ネットワーク状況表示
　LAN ポートの情報（パケットの処理状況)、ネットワーク情報（LAN アダプタの MAC アドレス、ARP テーブル、ルーティングテーブル、ネットワーク統計情報）など

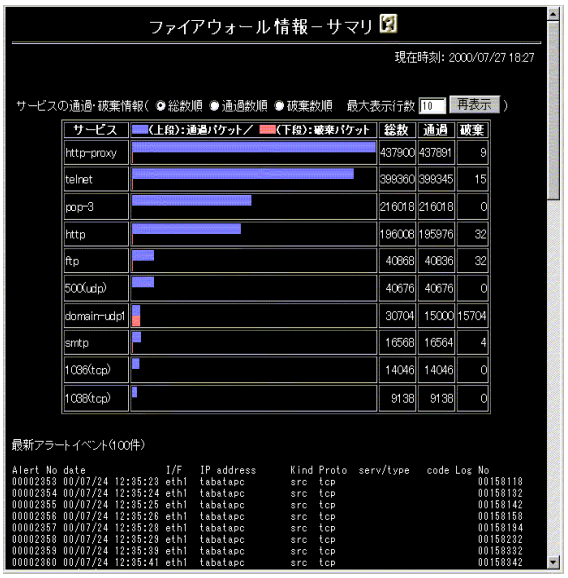
③ ファイアウォール機能の動作状況
　サマリ、アラート情報、パケットフィルタログ、SA 状態表示、IPsec 暗号エラーログ、IKE 通信エラーログ、独自方式暗号エラーログ、認証ログ、URL フィルタログなど

④ Web キャッシュ機能における統計情報
対象となる統計データは、現在日を除く過去 1 年間を対象としている。集計単位として日報（1 日単位)、週報（1 週間単位)、月報（1 カ月単位）がある。それぞれに対してヒット率、URL 一覧、クライアント一覧、不正アクセス一覧の情報が統計データとして表示



Webキャッシュ機能の統計情報

パケットフィルタリング機能の統計情報



図－３ NetShelter/FWの統計情報表示例

5.3 高信頼性・運用性

停電や瞬電への対応として、UPS（無停電電源装置）との連携機能を備えており、GP5SUP103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。

また、内部温度異常やファン動作異常、ハードディスク異常などのハードウェア障害を監視し、本体前面にあるアラームLEDの点灯やLCDパネルへのメッセージ出力、ロギングなどを行うとともに、システムの継続運転が困難な場合は、ただちに安全に装置を停止する機能を備えている。

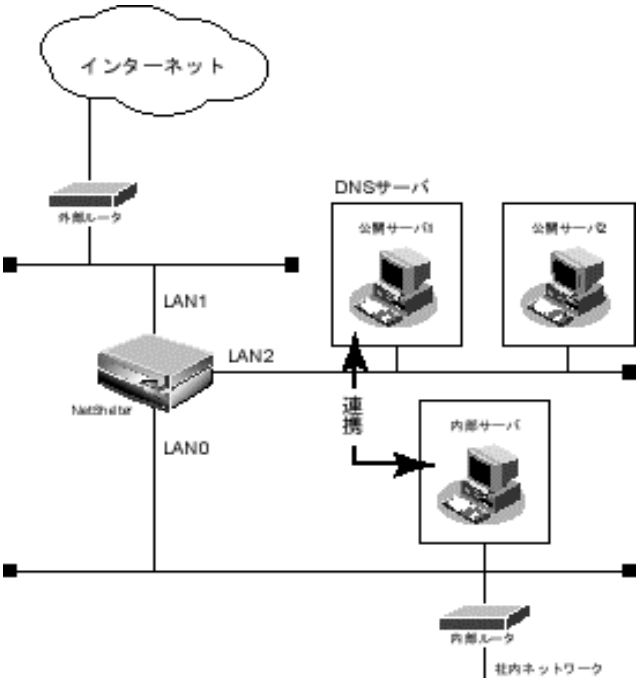
6 導入例

以下にNetShelter/FWの代表的な設置パターンについて説明する。

6.1 DMZ に公開サーバを設置した形態

インターネット接続において、第 3 のネットワークである DMZ に公開サーバを設置した形態の例について説明する。

以下の条件を想定し、環境を構築。
- ●新規にインターネットアクセスとインターネットへの情報公開をできるようにする。
- ●公開サーバ 1 として DNS サーバとメールサーバ、ニュースサーバを同一マシン上に設置
- ●公開サーバ 2 として Web サーバと FTP サーバを同一マシン上に設置
- ● 公開サーバ 1 と連携する内部サーバを 1 台設置



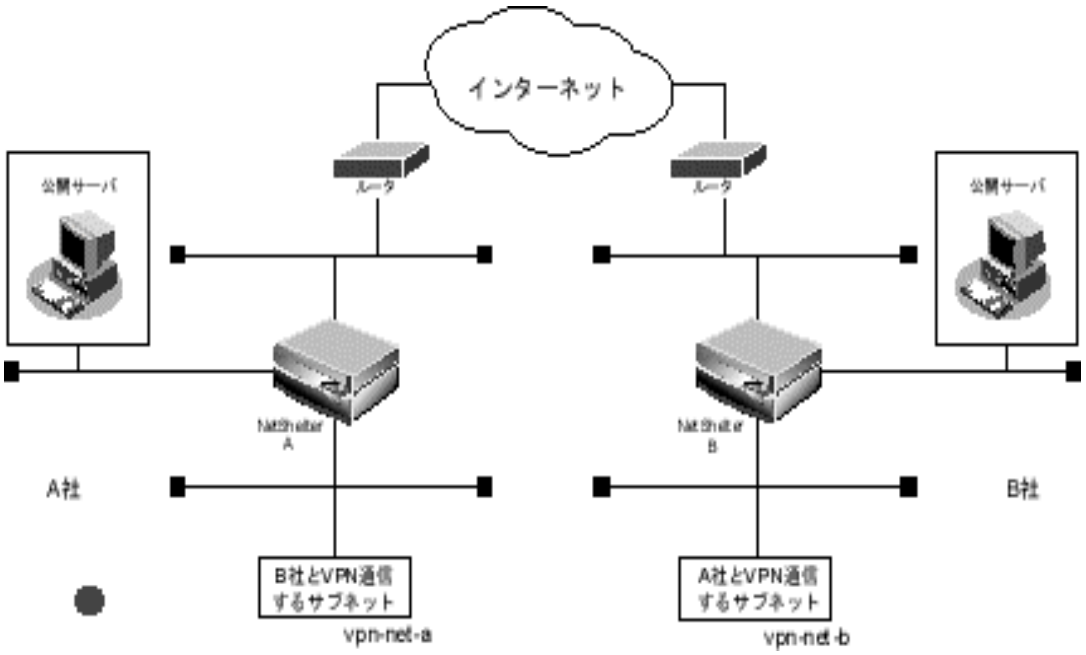
図－4 DMZ に公開サーバを設置した形態

6.2 VPN(IKE を使った IPsec 通信)形態

インターネット上で、VPN 通信を利用してエキストラネットワークを構築する場合の運用例として、以下の場合について説明する。

以下の条件を想定し、環境を構築。

●A 社と B 社との間でお互い特定のサブネットを VPN 通信できるようにする。
●A 社も B 社もインターネット接続環境は構築済みである。
●VPN 通信のプロトコルは、IKE を使った IPsec を使用する。



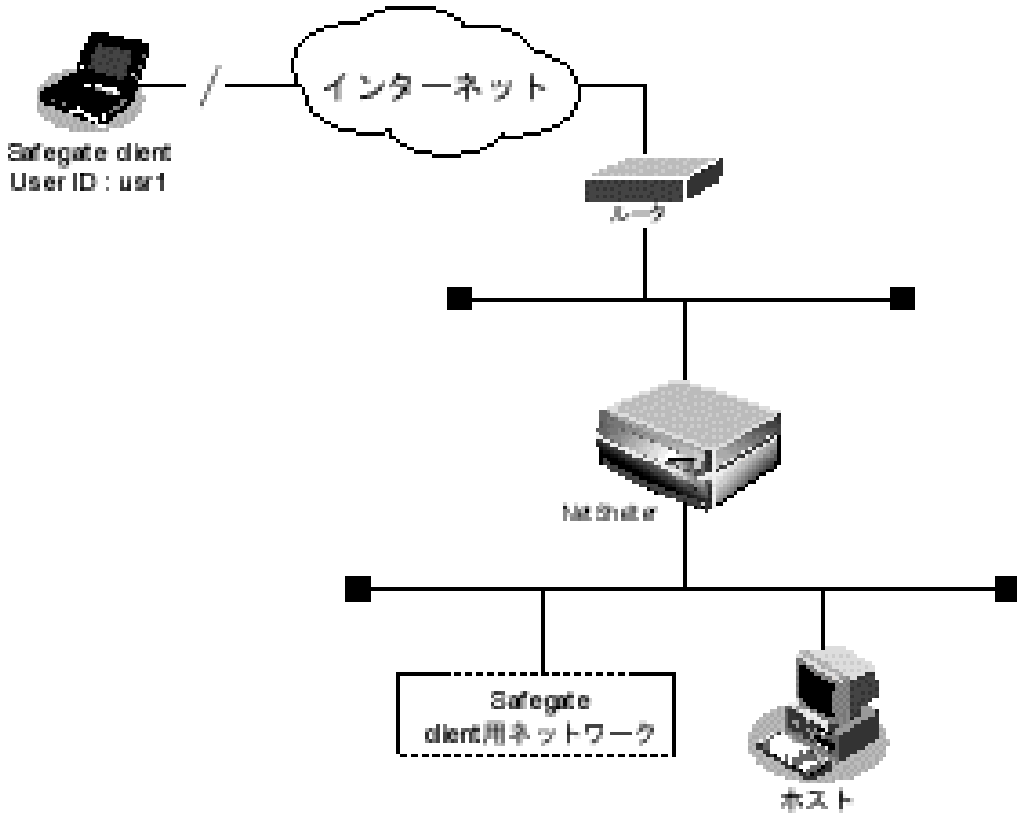
図－5 VPN（IKEを利用したIPsec通信）形態

6.3 リモート端末（モバイル PC）形態

Safegate client をインストールした PC から、NetShelter を経由して社内にアクセスする際の設定例を示す。Safegate client からのアクセスの場合、事前に登録されたユーザ情報によってユーザ認証を行った後で社内へアクセスする。

以下の条件を想定し、環境を構築。

●インターネットへの接続環境は既に構築済みである。
●Safegate client を使って社内アクセスするユーザに対しては、社内アクセスに関する制限は設けない。



図－6 モバイルPC Safegate clientを利用した通信形態