ファイアウォール専用装置

# GeoStream NetShelter/FW-P

プロダクトレポート

富士通株式会社

2003年8月

# 目次

# 1　はじめに

## 1.1　ファイアウォールの必要性

インターネット上には、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。これらはインターネット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、悪意を持ったものがあり、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
- 内部侵入
- 別サーバ（他社を含む）へアタックの踏み台とされる。

などの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も、

- 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。

インターネットに接続されている装置には、攻撃に対する防御が必要であり、これらの対策を行うために、ファイアウォールを用いるのが一般的である。

ファイアウォール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

などが可能となる。

# 2　NetShelter/FW-P の特長

本装置は、NetShelter/FW の上位機種であり、専用回線などを利用したインターネット常時接続環境のセキュリティ対策として、ファイアウォールを構築するための中小規模事業所向け専用装置（1U ハーフサイズのラックマウント型）である。

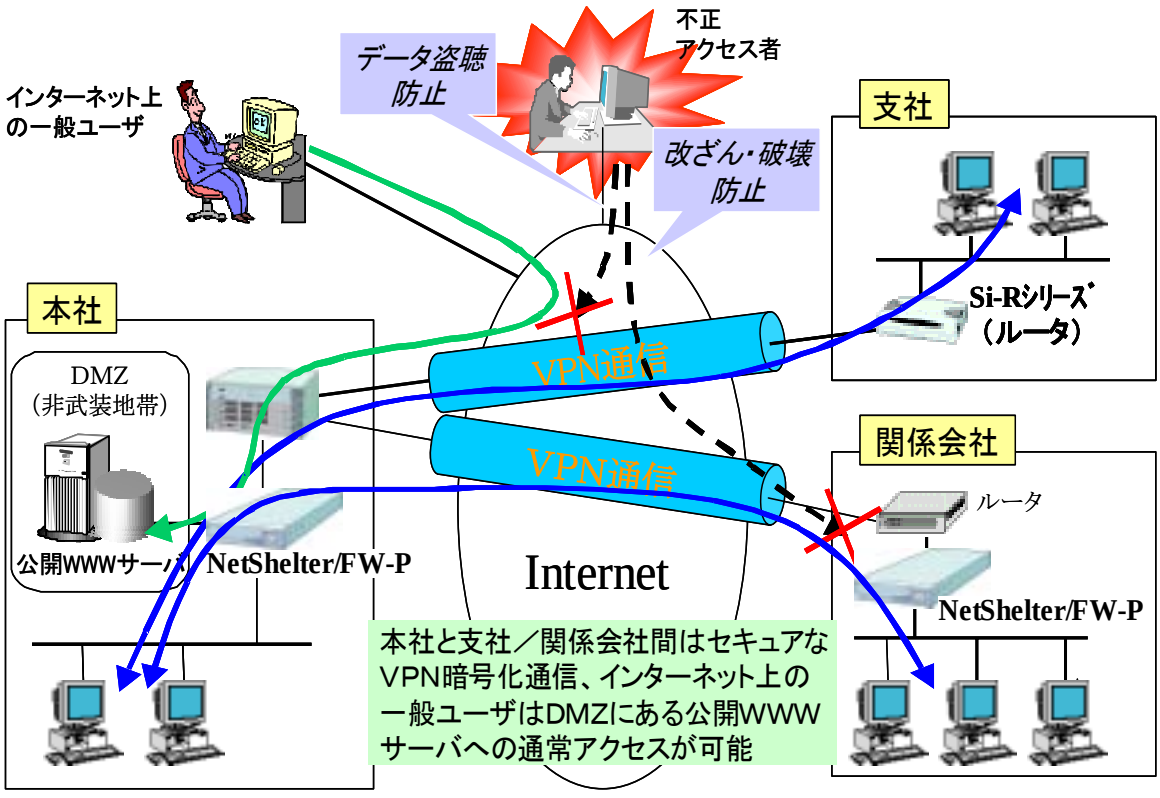
ファイアウォール機能としては、外部からの不正侵入を防ぐ IP パケットフィルタリング機能、外部から内部のホストやネットワークの情報（IP アドレス）を隠すアドレス変換機能、有害なサイトへのアクセスを禁止する URL フィルタ機能などがある。

また、インターネットを介したエクストラネット構築に対応するため業界標準の VPN（Virtual Private Network）方式に準拠した VPN 通信機能を提供する。

さらに、Web キャシュ機能、DNS キャシュ機能、メール中継機能、DHCP サーバ機能および、時刻同期機能といったネットワーク運用支援機能も提供する（図－1 参照）。

本装置は、1U サイズラックに２台、搭載が可能である。

また、IN、OUT、DMZ 用の LAN インタフェースの他に、二重化連携/保守用監視用の LAN インタフェースを装備している。




図－１　**NetShelter/FW-P の利用概念**

主な機能概要を以下に説明する。

(1) ファイアウォール機能

高セキュアなファイアウォール機能を持った専用装置として、中小規模事業所で運用できるように、アドレス変換機能、IP フィルタリング機能、VPN 通信機能、リモート端末機能を提供。

(2) 100Mbps-LAN をターゲットとした高性能

ワイヤー性能に近いパケット処理を実現（180Mbps）。

(3) ネットワークサービス機能

ネットワークを有効に利用するサービス機能として、本装置では、事前に登録した URL も Web サーバ、または、サイトへのアクセスを禁止する URL フィルタリング機能、中小事業所などの環境で IP アドレスを有効利用し、環境設定の簡易化を図るために有効な DHCP サーバ機能、および、中小事業所などの環境でキャッシュサーバの代替を行う Web キャッシュ機能や DNS キャッシュ機能を提供。

(4) ＵＲＬフィルタ規制リストのサポート

手入力による URL フィルタ機能に加え、自動更新に対応し、22 カテゴリから指定が可能な URL フィルタ規制リストを使用する機能を提供。

※ 「NetShelter/FW バージョンアップオプション」サービス契約によるライセンス付与が必要。

(5) 運用支援機能

管理者が、本装置が意図した通信制御を行っているか否かを監視したり、各サービスの利用状況を把握し、解析し、通知したりするために、ロギング機能、アラート機能、syslog、ネットワーク管理機能（SNMP マネージャ連携機能、Safegate 集中管理連携機能）、および、時刻同期起動を提供。

(6) 保守監視機能

遠隔操作による運用や保守を可能にするために、AUX インタフェースにて制御する機能、プログラムアップデート機能、および、ダンプ収集機能を提供。

(7) 二重化連携機能＋経路監視機能

本装置を 2 台利用して冗長構成のシステムを構築し、運用・待機として相手装置の動作状態、および、装置に接続されたネットワークの隣接機器や配線の状態を監視する機能を提供。

また、二重化連携のために、前面パネルオペレーションで 1 操作を行うだけの簡単な導入機能も提供。

# 3　機能

本装置の主な機能を以下に示す。

## 3.1　ファイアウォール機能

ファイアウォール機能としては、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
- URL フィルタリング機能
- ログ管理、アラート通知機能

### 3.1.1　アドレス変換機能

NAT（Network　Address　Translations）機能とは、アドレス変換を行う機能である。

本装置では、通常のアドレス変換に加えて、ポート番号も変換を行う。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

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。

#### (1)　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、40,000 である。

本装置は、送信元の 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、本装置の 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、本装置宛の IP アドレスとポート番号を、内部宛の 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
- CU-SeeMe

### (2) 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（たとえば、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指定したりすることが可能となる。

外部ネットワークへアクセスもしくは、外部ネットワークから内部の特定のホストへ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 へ広視する。

## 3.1.2 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ことにより、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御等が可能となる。

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／プロトコルなど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、取扱説明書を参照のこと。

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 上の全てのサービスを意味する。
－UDP-ALL　　：UDP 上の全てのサービスを意味する。
－ICMP-ALL　　：ICMP 上の全てのサービスを意味する。
－ALL　　：全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 などの総称サービス名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。

※ AUX インタフェースは二重化運用時の系間パス及び保守専用のポートであるため、任意のフィルタリング条件を設定することはできない。

## 3.1.3 VPN 通信機能

Virtual Private Network（VPN）とは、インターネットなどの公共のネットワークを利用し、仮想的に通信環境を構築し、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。
VPN 通信では、VPN 通信機能を装備した装置間でデータをカプセリングし、相手の装置に送信する。その際、データの盗聴、改ざんを防止するため、認証や暗号化などのセキュリティ機能でデータを保護する。VPN 通信機能では、IP のみサポートしており、IP 以外は中継されない。
なお、VPN 機能では NAT 等の特別なアドレス変化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。

### (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、本装置で登録可能な暗号化通信相手先は、最大 128 までで、同一暗号化通信相手先に対しては、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。
暗号化の方式は、業界標準に準拠した RFC 規定の IPsec 方式と当社の独自暗号方式（Safegate 方式）を提供している。

### (2) 暗号化の条件（アドレス指定方法）

暗号化してパケットを送信するか否かは、オリジナルの IP パケットの送信元アドレスと送信先アドレスをもとに制御する。暗号化の条件は、128 サイトまで登録可能であるが、相手ゲートウェイを重複させることはできないので、相手ゲートウェイ 1 つに対し、最大 4 ネットワークまたはホスト定義までが可能となる。

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、対で指定される。なお、本装置の複数インタフェースをまた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) 暗号方式の仕様

IPsec 方式と独自暗号方式の概要を示す。なお、サイト間の暗号化方式は、装置単位で一つの方式のみとなるので、相手によっては一台の装置だけでは対向できない。ただし、Safegate client は、前述の設定に関係なく利用可能である。

**表　IPsec方式と独自暗号方式の概要**

| | | IPsec方式 | 独自暗号方式 |
|---|---|---|---|
| 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（健長 56bit）<br>3-DES（健長 168bit） | DES-CBC（健長 56bit） |
| 認証アルゴリズム | | HMAC-MD5-96<br>HMAC-SHAI-90 | MID5 |
| 暗号鍵 | DES-CBC | 送信と受信で別々である16桁の16進数 | 64文字以内の英数字 |
| | 3-DES | 送信と受信が別々である48の16進数 | — |
| 認証鍵 | DES-CBC | 送信と受信が別々である32桁の16進数 | — |
| | 3-DES | 送信と受信が別々である40桁の16進数 | — |
| 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<br>IKE（Pre-Shared Key 方式） | 通信中の1時間（固定）毎に更新 |
| 鍵管理 | | オフライン<br>IKEPre-Shared Key | オフライン |
| 暗号通信 | | 認証付き　ESP(ESP_AUTH)<br>(IPのプロトコル番号は50) | UDPて暗号パケットをカプセル化<br>(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<br>(IPアドレス、ネットマスク) | 送信先/送信元アドレス<br>(IPアドレス、ネットマスク) |
| 相手暗号GW数 | | 最大128 | 最大128 |
| 相手暗号GW毎の条件数 | | 最大4条件 | 最大4条件 |

IPsec は以下の標準仕様に準拠している。

RFC2401：ecurity Arehitecture for Internet Protocol
RFC2403：The Use of HMAC-MD5-96 within ESP and AH
RFC2406：IP Encapsulating Security PayLoad（ESP）

- IPsec 方式

  IPsec は、秘匿性を主に提供する IP Encapsulating Security Payload（ESP）と、完全性と認証を提供する IP Authentication Header（AH）の２つのセキュリティプロトコルからなり、以下の２つの方式がある。

－IPsec 暗号方式

2 つのプロトコルのパラメタ（SA：Security Association）をあらかじめ、送信元と送信先で利用者が設定しておいて、通信する方式である。

なお、複数拠点と VPN 通信を行う場合は、該当する拠点数分の暗号設定が必要となる。

－IKE 暗号方式

IPsec 暗号方式では、利用者が事前に設定しておく必要のあった暗号鍵や SPI など IPsec 通信に必要な情報を、相手と通信し、自動的に作成する IKE（Internet Key Exchange）機能をサポートした方式である。

- 独自暗号方式

独自暗号方式は、当社独自のプロトコルを使用して VPN 通信を行う方式である。

指定されたクライアント（自局）アドレスからサーバ（他局）アドレスに送信されるすべてのパケットに対して暗号化を行う。

#### (4) IPsec アグレッシブモード

Si-R シリーズルータと組合せて、フレッツサービスなどの動的な IP 取得契約においても VPN 通信が可能になる。

発信側を識別する方法では、装置固定の ID を使用するため、発信側の IP アドレスが不定でも使用可能である。本装置には、固定 IP アドレスが必要となる。

### 3.1.4 リモート端末接続（Safegate client）機能

リモート端末接続機能は、自宅や出張先のホテルなどから内部ネットワークのホストに安全にアクセスするための機能である。Safegate client をインストールした端末から VPN 暗号通信機能（独自暗号方式）を利用し、本装置経由で、内部ネットワークへのアクセスが可能。

#### (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、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 との間で暗号通信を行うことができ、同時に接続できる Safegate client は最大 256 台までである。

モバイルで利用できる暗号化方式は、独自暗号方式のみである。

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 と本装置の間の通信は、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 と本装置との通信は、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パケットのカプセル化により、Safegate client と本装置の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。

本装置は、ネットワーク上の任意の装置から受信した ICMP パケットを送信元に中継することができるため、本装置で暗号化するパケットについて管理者は特に意識する必要はない。ただし、本装置に暗号データを送信する Safegate client については、MTU 長を短くするなどの対処が必要となる場合がある。

---

(2) ローカル認証とリモート認証

ローカル認証とリモート認証のどちらか一方の方式を選択することができる。

ローカル認証は、本装置自身で認証を行う方式で、登録ユーザ数は最大 256 ユーザ、同時接続数は最大 256 ユーザである。ユーザ情報とアクセス記録は、本装置に保管・管理される。

リモート認証は、RADIUS サーバを使用して認証を行う方式で、ユーザからの接続要求に対し、本装置が RADIUS サーバに認証を依頼し、認証可否を処理する。登録ユーザ数は、RADIUS サーバしだいで、同時接続数は最大 256 ユーザである。ユーザ情報とアクセス状況は、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ことができる。リモート認証の対象 RADIUS サーバは、SafeauthorV2.0 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。

## 3.2 ネットワークサービス機能

### 3.2.1 URL フィルタリング機能

URL フィルタリング機能は、登録した URL の Web サーバまたはサイトへのアクセスを禁止する機能であり、HTTP プロキシを経由して利用するすべてのクライアントからのアクセスを一括して制限することができ、特定のサイトへのアクセスを禁止することできる。

本機能では、Web コンテンツをフィルタリングする方式としてリスト方式を採っており、制限するサイトの URL をリストアップし、直接設定する URL フィルタリング条件機能と規制リストをインターネット上からダウンロードし、規制リストをもとに有害サイトを制限する規制リスト機能を利用することができる。なお、規制リスト機能はオプション機能である。

本機能を利用する場合は、Web ブラウザの HTTP のプロキシ設定で、本装置の IN ポートの IP アドレスを指定するか、IN 側のプロキシサーバの上位プロキシサーバとして本装置の IN の IP アドレスを指定するかして利用する。URL フィルタリング機能で、不正アクセスとして検出された場合は、クライアントの Web ブラウザにエラーページが表示される。

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。

本機能を使用すると、公序良俗に反するサイトなどへのアクセスを禁止することができる。

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、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。

(1) URL フィルタ規制リスト

URL フィルタ規制リストとは、SurfContril 社が提供する公序良俗に反するサイトへのアクセスを禁止した URL ダウンロードできるようにしたオプションである。

規制リストには、22 カテゴリ、280 万件（2002 年 4 月時点）が登録されており、自動更新によって規制リストを常に最新の状態に保っている。

### 3.2.2 DHCP サーバ機能

本装置の IN ポート直下の LAN に接続される DHCP クライアント端末に対し、アドレスの割り振りサービスを行う DHCP サーバ機能を提供する。アドレス割り振り方式は、DHCP クライアントからの要求順に割当範囲内で空いている IP アドレスを割り当てる「動的割割り当て方式」と、特定のホストに特定の IP アドレスを割り当てる「静的割り当て方式」の２通りがある。

DHCP サーバにより割り当てられるアドレスの範囲は、本装置の IN ポートと同じセグメントのネットワークに限られ、割り当てできる IP アドレスの個数は、動的割り当てと静的割り当てを含めて 253 個である。なお、動的割り当てに指定した範囲内の IP アドレスを静的割り当ての割当 IP アドレスとして割り当てることはできない。ただし、静的割り当ては 32 までである。

割り当てられた IP アドレスの割当期間（リース期間）は、次の通りである。

- 指定可能範囲 － 10 分 ～ 525600 分（365 日）
- 初期値 － 60 分

静的割当を行う場合は、次の値を GUI で登録する。

- ホスト名 － 割当を要求するホスト名
- IP アドレス － 割当を希望する IP アドレス
- MAC アドレス － 割当を要求するホストの MAC アドレス

なお、本装置では、動的に割当可能なアドレス範囲の登録は、1 範囲のみに限られる。
この範囲には、次のアドレスを除外した範囲を設定する必要がある。

- 本装置の IN ポートの IP アドレス
- 本装置の IN ポート直下のネットワークアドレス、ブロードキャストアドレス
- 静的割当を行う場合、静的に割当を行う IP アドレス

### 3.2.3 Web キャッシュ機能

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ことである。

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。

#### (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、http1.1 の keep-alive にも対応しています。

### (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 ICMP 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。

本装置が上位 proxy となる形態の場合は、本装置の http ポート番号でのアクセスが可能。

## 3.8 DNS キャッシュ機能

DNS キャッシュ機能とは、（インターネット上の不特定多数の）外部 DNS サーバと（社内の）内部端末との名前解決を仲介する機能である。一般的には、内部セグメントを守るために、外部との通信を受ける DMZ というセグメントを用意し、一旦、DMZ にて通信を受ける構成を取る。

しかし、外部と内部が直接通信する場合よりも、セキュリティ強度を高めることができる。

また、キャッシュ機能があるため、不要なトラフィックの削減も可能である。

本装置にキャッシュされたデータの有効期限は、検索情報の SOA レコードの最小 TTL にしたがうが、通常は 1～7 日の範囲である。なお、DNS キャッシュ機能を停止した場合は、キャッシュは無効となる。

### (1) メール中継機能

メール中継機能とは、（インターネット上の不特定多数の）外部メールサーバと、（社内の）内部メールサーバとの通信を仲介する機能である。一般的には、内部セグメントを守る為に、外部との通信を受ける DMZ というセグメントを用意し、一旦、DMZ にて通信を受ける構成を取る。

しかし、DMZ にサーバを用意できない場合に、メール中継機能にて通信を仲介することによって、外部と内部が直接通信するよりも、セキュリティ強度を高めることができる。

### (2) 不正リレー対策

不正リレー対策は、メールアドレス／IP アドレスにり SMTP アクセスに制限をかける機能である。SPAM メールなどに代表される迷惑メールの発信元として、本装置を不正利用されないようにするために使用する。

### (3) メールキューに関して

受信したメールは装置なのキューに保存され、メール再送が完了すると削除される。配送が正常に完了していない場合、一旦キューに保存する。キューに保存されたメールは、一時間毎に再送を試みる。また、一日後に未配送通知をメール発信者に返信する。キューは最大 5 日間保存される。二重化連携時は、メール中継機能に必要な情報が待機系システムに引き継がれるがログとメールキューの内容は引き継がれない為、NetShelter/FW-P がダウンした時キューにメールが存在した時に復旧するまでメールは配信されない。

**表　メールキュー仕様**

| 項目 | 値 | 備考 |
|---|---|---|
| 再送間隔 | 1時間 | 変更不可 |
| キュー最大保存股間 | 5日間 | 変更不可 |

- メール配送設定
  内部ネットワークへ配送されるメールは特定のメールサーバに配送される。

外部ネットワークに送信されるメールは、DNS を参照して適切なメールサーバに配送する方法と、特定のメールサーバに配送する方法を選択することが可能である。

**表　メール配送機能設定項目**

| 項目 | | 内容 |
|---|---|---|
| 管理者メールアドレス | | トラブル発生時に通知するメールアドレス。 |
| 内部受信 | 受信ドメイン | メールの受信を許可するドメイン名もしくはホスト名＋ドメイン名。複数指定可。 |
| | 受信メールサーバ | 配送する内部特定サーバ。 |
| 外部受信 | DNS（MX）配送 | DNSを参照し、適切なメールサーバへ配送する。 |
| | メールサーバ配送 | 外部ネットワーク宛の全てのメールを特定のメールサーバに配送する。 |
| | 送信メールサーバ | 配送する外部特定サーバ。 |
| メールの最大受信可能サイズ | | 受信できるメールの最大サイズ。 |

# 3.3　運用支援機能

## 3.3.1　ロギング機能

本装置のファイアウォール機能およびWeb キャッシュ機能について、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 通信機器、Web キャッシュ）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、表の通りである。

**表　ログ一覧**

| フィルタリング種類 | 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キャッシュ | 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できるが、Web キャッシュログ、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もと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条件は syslog に記録することが可能で、設定によりリモートの syslog サーバにも情報を送ることができる。

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、ファイアウォール機能のログおよびWeb キャッシュ機能のログ、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できる。

## 3.3.2 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 アラートイベントとしきい値**

| 項目 | アラートイベントのしきい値 |
|---|---|
| 同一送信元からのアタック | 単位時間当たりの破棄パケット数 |
| 同一宛先へのアタック | 単位時間当たりの破棄パケット数 |
| 暗号パケット改竄検出 | 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 |

## 3.3.3 syslog

syslog は、システムのメッセージログのことであり、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 サーバに記録することが可能である。本装置は、syslog をサポートし、エラーメッセージなどを sysylog 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憶しておくことができないため、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（本装置においても、記録量に限りがある）。古い情報が消去されるということは、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ことであるため、必要であれば、外部 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など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ことが可能だが、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 syslog仕様**

| 項目 | 内容 |
|---|---|
| Webによるログ閲覧可能件数 | 1,000件 |
| ファシリティ | Kern（0）、deamon（3） |
| プライオリティ | Warm、err、crit、alert、emerg |

**表 プライオリティの割当て**

| プライオリティ | メッセージ種別 |
|---|---|
| LOG_WARNING | 警告メッセージ |
| LOG_ERR | エラーメッセージ |
| LOG_CRIT | クリティカルメッセージ |
| LOG_ALERT | アラートメッセージ |
| LOG_EMERG | エマージュンメッセージ |

## 3.3.4 ネットワーク管理機能

本装置では、環境設定や稼動状況の監視を Web ブラウザによるリモートから行うことが可能である。

ネットワーク経由での監視機能として、SystemWalker、NetEyeManager などの SNMP マネージャによる管理と Safegate 集中管理による管理の 2 つ方式がある。

以下に、SNMP マネージャと Safegate 集中管理各々と連携してできる機能を示す。

**表　Safegate集中管理とSNMPマネージャの機能一覧**

| | | SNMPマネージャ | Safegate集中管理 |
|---|---|---|---|
| 稼働監視 | 機器認識 | ・オートマップ機能による自動登録<br>・手動登録 | ・手動登録 |
| | 監視内容 | ・システム起動有無<br>・ネットワークトラフィック<br>－systemグループ<br>－interfacesグループ<br>－address translationグループ<br>－ipグループ<br>－tcpグループ<br>－udpグループ<br>－icmpグループ<br>－snmpグループ | ・システム稼働有無<br>・稼働機能種別<br>・適用ポリシーの作成日時 |
| アラート監視 | | SNMP-Trap（Firewallアラート、Coldstartトラップ、Link Up/Down） | syslog内容（Firewallアラート、RASアラート） |
| リモート操作 | | Web ブラウザの併用により、リモート操作可能 | Web ブラウザの併用により、リモート操作可能 |

一般的には、ネットワーク全体を監視する場合は、SNMP マネージャ連携による管理を行い、Safegate が導入済みの場合は、Safegate 集中管理を使用する。なお、SNMP による監視では、本装置との通信は暗号化されないので、VPN 暗号通信を使用したエクストラネットを構築し、セキュリティを確保した上で、センタから拠点側の本装置を監視する必要がある。

Safegate 集中管理では、本装置との通信が暗号化されるため、暗号化を意識する必要はない。

## (1)　SNMP マネージャ連携

SNMP マネージャから本装置のイベント監視、稼働状況監視が可能となる。

SNMP の手順にしたがい、MIB 情報（稼働状況）をユーザ指定の SNMP マネージャに送信する。

SNMP マネージャでは、受け取った MIB 情報を元にネットワークおよび本装置の状態を監視することができる。本装置でサポートしている MIB は、MIB-II の範囲全てである。

## (2)　Safegate 集中管理

Safegate 集中管理とは、Safegate や本装置を集中管理するソフトであり、本装置の運用監視を一元管理できる。Safegate 集中管理は、Windows NT のソフトであり、UNIX がなくても本装置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 ゲートウェイアラートイベント監視
- 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

### 3.3.5 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。指定する項目は、

- メールによるログの採取を使用する
- 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間
- ログ採取メール再送期間

### 3.3.6 時刻同期機能

上位タイムサーバと同期をとる機能をサポートする。また、内部ネットワーク上にあるタイムサーバやNTP クライアントからの時刻問い合わせに応答する。

一般的には、内部セグメントを守るために、外部との通信を受ける DMZ というセグメントを用意し、一旦、DMZ にて通信を受け取る構成を取る。しかし、DMZ にサーバを用意できない場合に、NTP サーバ／クライアント機能にて通信を仲介することによって、外部と内部が直接通信する場合よりも、セキュリティ強度を高めることができる。

#### (1) NTP クライアント機能

本装置では、上位タイムサーバから取得した時刻により同期をとる。上位サーバに対して定期的に時刻の問い合わせを行う。上位タイムサーバは最大 10 まで指定する事が可能。複数サーバを設定した場合、全てサーバに対して問い合わせを行い、最も精度の高いサーバと同期をとる。

## 3.4 保守監視機能

保守監視機能は、遠隔操作による運用や守を可能にする機能である。

本装置では、運用系 LAN（IN、OUT、DMZ）とは別系統の保守監視用 LAN（AUX）を利用して、運用及び保守監視を行うことが可能である。

AUX ポートに接続した保守監視用ネットワークを使用することで、運用系 LAN とは切り離されたネットワークを使用することとなり、保守監視用 LAN のネットワーク負荷の影響を運用系 LAN に与えないネットワーク構築が可能となる。

また、インターネットとは物理的に独立した保守監視ネットワークを使用することで、セキュリティの高い保守監視を行うことができる。

AUX ポートからブラウザで以下の保守監視を行う。

#### (1) AUX インタフェースにてサポートする機能

AUX インタフェースを通じて制御可能なものを以下に示す。

- 保守監視パスワード
- プログラムアップデート機能

- ダンプ収集機能
- AUX インタフェースでの保守監視設定
- ファイアウォール停止機能

### (2)　プログラムアップデート機能

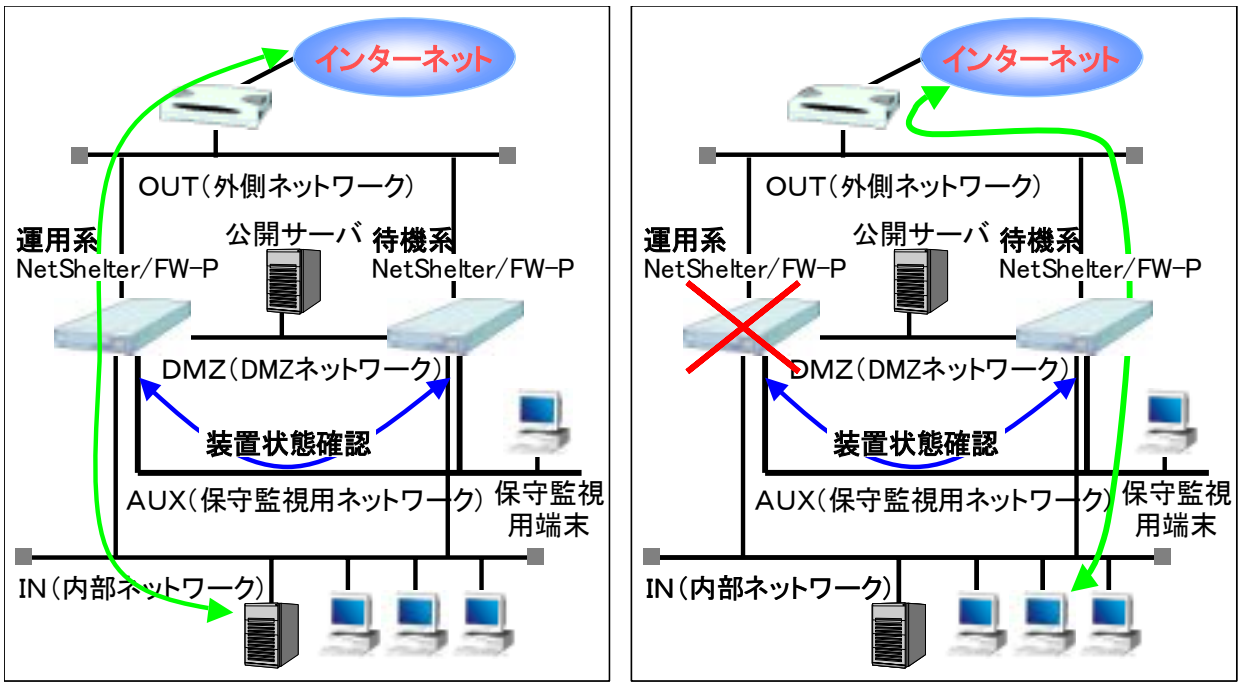
本機能は、装置内のプログラムを更新するものである。
通常、レベルアップは CD-ROM により全モジュール置き換えで行うが、プログラムアップデート機能では、修正されるモジュールのみ置き換える。また、不具合があった場合は、レベルアップ前（一世代前のみ）に戻す事も可能である。なお、この機能では、プログラム全体を更新することはできない。

### (3)　ダンプ収集機能

障害発生時に原因を追究するため、本装置のメモリダンプおよびプロセスダンプの採取を行う機能である。
ファイルサイズは、最大 128MB となる。
対象となるダンプファイルは、メモリダンプと Core ダンプである。

## 3.5　二重化連携機能

二重化連携機能は、2 台の装置による冗長構成（二重化構成）をとる機能である（図－２参照）。




二重化構成をとる場合は、各インタフェース同士は同一セグメントにしなければならないので注意しなければならない。

図－２　二重化連携図の概要

それぞれの装置が他方の動作状態を監視し、1 台の装置が故障などで停止した場合、もう一方の装置で運用を継続することができる。運用を継続した装置は、AUX 以外の MAC アドレス及び IP アドレスを引き継いで運用する。

二重化連携の導入作業は、装置前面の操作スイッチのみで可能（設定不要）。

## 3.5.1 障害発生切り替え時間

障害発生切り替え時間時間

異常検出時間＋切り替え時間＋α

－異常検出時間：4～600 秒の範囲で設定可能。デフォルト値は 30 秒

－切り替え時間：約 30 秒

－α：周辺機器への影響など

## 3.5.2 切り替え時の通信の影響

二重化連携機能では、運用系の環境定義情報に変化があった場合、その内容を速やかに待機系に反映させることで、両方装置の環境が常に同一となるようにしている。運用系の停止時には、待機系が新運用系として処理を継続する。但し、メール中継機能は引き継ぎができない。

**表　インタフェースごとのアドレス引継ぎ可否**

| インタフェース | 運用形態 |
|---|---|
| IN（内部ネットワーク） | IPアドレス、および、MACアドレスの引き継ぎ |
| OUT（外部ネットワーク） | IPアドレス、および、MACアドレスの引き継ぎ |
| DMZ（DMZネットワーク、ノード間通信パス） | IPアドレス、および、MACアドレスの引き継ぎ |
| AUX（リモート保守、ノード間通信パス） | IPアドレス、および、MACアドレスは引き継がない |

本装置の各機能における引継ぎは、以下の通り。

**表　環境情報の引継ぎの可否**

| 機能 | | 通信への影響 |
|---|---|---|
| IPパケットフィルタリング機能 | | 制限なし（フィルタ引き継ぎ）。 |
| アドレス変換機能（NAT機能） | 動的NAT | NATテーブルを引き継がないため、TCPはセッション確立中のものは通信が切断される。UDPは、外部からの応答待ちであった場合、その応答が受け取れずタイムアウトとなる。 |
| | 静的NAT | ftp、RealAudio、StreamWork、VDOLiveは再接続が必要。<br>それ以外は必要なし。 |
| URLフィルタリング機能 | | 制限なし（フィルタ条件引き継ぎ）。 |
| VPN 通信機能 | | IKEの鍵情報は引き継がれないため、切り替え後の最初のアクセスで鍵交換処理が行われる。切り替え後の最初のアクセスが受信処理後の場合、再接続が行われる。 |
| リモート端末接続機能 | | 通信接続不可、再接続が必要。（注1） |
| Webキャッシュ機能 | | キャッシュ情報は引き継がない。<br>切り替え後は実サイトへアクセスとなる。 |
| DHCPサーバ機能 | | 制限なし（リソースアドレス引き継ぎ）。 |
| ネットワーク管理エージェント機能 | NetEyeManager連携 | 制限なし（注2） |
| | SystemWalker連携 | 制限なし（注2） |
| | Safegate集中管理連携 | 再接続が必要。（注1）。<br>（クライアント用暗号キー引き継ぎ）（注2） |

表　環境情報の引継ぎの可否（続き）

| 機能 | | 通信への影響 |
|---|---|---|
| 運用支援機能 | 環境設定 | 制限なし |
| | アラート | 制限なし |
| | ログギング | ログの引継は行わない。 |
| メール通知 | | 制限なし |
| 退避／復元 | | 制限なし |
| 停電対策 | | 制限なし |
| メール中継機能 | | ロギングとメールキューの引き継ぎは行わない。<br>メール装置内に蓄積される。 |
| DNSキャッシュ機能 | | キャッシュ情報の引き継ぎは行わない |
| タイムサーバ機能 | | 制限なし |

注１）認証情報の引き継ぎは行わない。切り替え発生後は、認証セションが切断され、再接続が必要。なお、Safegate client は、セション確立中にサーバの生存確認を行っていないため、認証セションが切断されたことを認識できないので、暗号通信路を使用してシステムと通信しているアプリ側のタイムアウトで、検出する必要がある。

注２）二重化連携を行っている場合、AUX では運用系/待機系の両系が見える。
IN/OUT からは運用系のみが見える。

## 3.5.3　MAC アドレスの引き継ぎ

運用系装置（以下：装置 A）に障害が発生し、待機系装置（以下：B）に切り替わる場合、装置 B は装置 A の MAC アドレスを引き継いで運用を行う。

さらに、装置 A を別装置（以下：装置 C）に置き換え、装置 C が運用系に切り替わった場合、装置 C は装置 B の使用していた装置 A の MAC アドレスを引き継いで運用を行う。つまり、二重化連携にて装置が使用している MAC アドレスは、syslog にて確認することが可能である。

MAC アドレスを引き継いでの運用は、装置の電源断によって終了する。

装置の再起動時は、装置自身の MAC アドレスに戻る。

## 3.5.4　機能動作

二重化連携機能を使用した場合の動作は以下のようになる。

### (1)　初期導入

2 台の本装置の AUX、および、DMZ インタフェースをノード間通信パスとして接続し、装置前面の装置スイッチの操作により、二重化連携構成となる。

二重化連携を行う場合は、AUX インタフェース同士は必ず接続しなければならないので注意すること。

また、AUX インタフェース同士の監視が出来なくなった場合、二重化連携が正常に行われないため、DMZ インタフェース同士も接続することを推奨する。

### (2)　二重化連携時（正常時動作）

二重化連携時は、AUX、および、DMZ インタフェースのノード間通信パスを利用して、運用系と待機系の間で相互に定期周期診断を行っている。

監視パケットは、MAC アドレスによる通信にて行う。監視パケットは、1 秒間隔で送信され、監視パケットが一定時間（デフォルト 30 秒、変更可能）途絶えた時、相手装置に障害が発生したとみなす。

運用系装置に障害が発生した場合、待機系装置へ切り替えを行う。また待機系装置に障害が発生した場合、運用系装置は待機系装置を切り捨てて、片側運用状態となる。

二重化連携の状態では、連携装置のインタフェースが全て活性化されているが、待機系装置のインタフェースに関しては IN、OUT、DMZ インタフェースが非活性状態となっている。したがって、待機系装置の IN、OUT、DMZ インタフェースにはアクセスすることはできない。

運用系装置に設置したネットワークアドレスやフィルタリング条件などの環境情報を待機系装置にコピーするため、待機系でのファイアウォール機能に関する環境情報設定は不要である。

運用系装置の環境定義情報に変化があった場合、その内容を速やかに待機系に反映し、2 台の装置の環境が常に同一となるような処理を装置間で行う。

環境引継ぎは以下の条件で自動的に行われる。

- 二重化連携機能立ち上げ時に、運用系の環境定義情報を待機系に転送する。
- 待機系装置の組み込み時に、運用系の環境定義情報を待機系に転送する。
- 運用系で「環境定義情報の反映」の操作を行った時、変更された情報を待機系に反映する。
- 運用系で環境定義情報の復元をした時、アップロードされた定義情報を待機系に転送する。

### (3) 運用系装置障害時

運用系装置に障害が発生した場合は、待機系装置はノード間通信パスの監視により、運用系装置の障害を検出する。相手装置が障害であるとみなすタイミングは、以下の場合がある。

- 装置間の監視パケットが一定時間（変更可能、デフォルト 30 秒）途絶えたとき
- 相手装置より、シャットダウン開始メッセージを受信したとき

新運用系装置は、障害が発生した装置に対して電源強制切断の指示をした後、自装置インタフェースの活性化とファイアウォールサービスの起動を行い、新運用系として動作を始める。

### (4) 待機系装置障害時

二重化運用に待機系装置で障害が発生した場合、運用系装置は待機系装置をシャットダウンさせた後、そのまま運用を継続する。

### (5) 旧運用系復旧時

二重化連携時の障害が発生した旧運用系装置を復旧させる場合、一旦待機系として動作させ、その後、組み込み処理を行った」時点で自動的に切り離し処理が行われる。

# 4　ハードウェア仕様

本装置のハードウェアは､19インチラックの1Uサイズに2台搭載する事が可能な筐体であり、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ー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ドライブに本装置専用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。

下表に、ハードウェア仕様を示す。

**表　NetShelter/FW-Pハードウェア仕様**

| | | |
|---|---|---|
| LANインタフェース | LANポート | 10/100BASE-T×3（自動／手動切替え） |
| | 保守／二重化 | 10/100BASE-T×1（自動／手動切替え） |
| シリアルポート | コンソール接続用 | RS-232C（9,600Kbps,D-SUB9ピン）×1 |
| | UPS接続用 | RS-232C（9,600Kbps,D-SUB9ピン）×1 |
| LCDパネル | | ASCII8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 | | CD-ROM、ハードディスク（インストール、アップデート用） |
| 外形寸法（幅×奥行×高さ） | | 195 mm × 560 mm × 38 mm（ゴム足、突起物を除いて） |
| 重量 | | 4.3 Kg以下 |
| 消費電力 | | 40 W（最大） |

# 5　かんたん導入/設定/運用

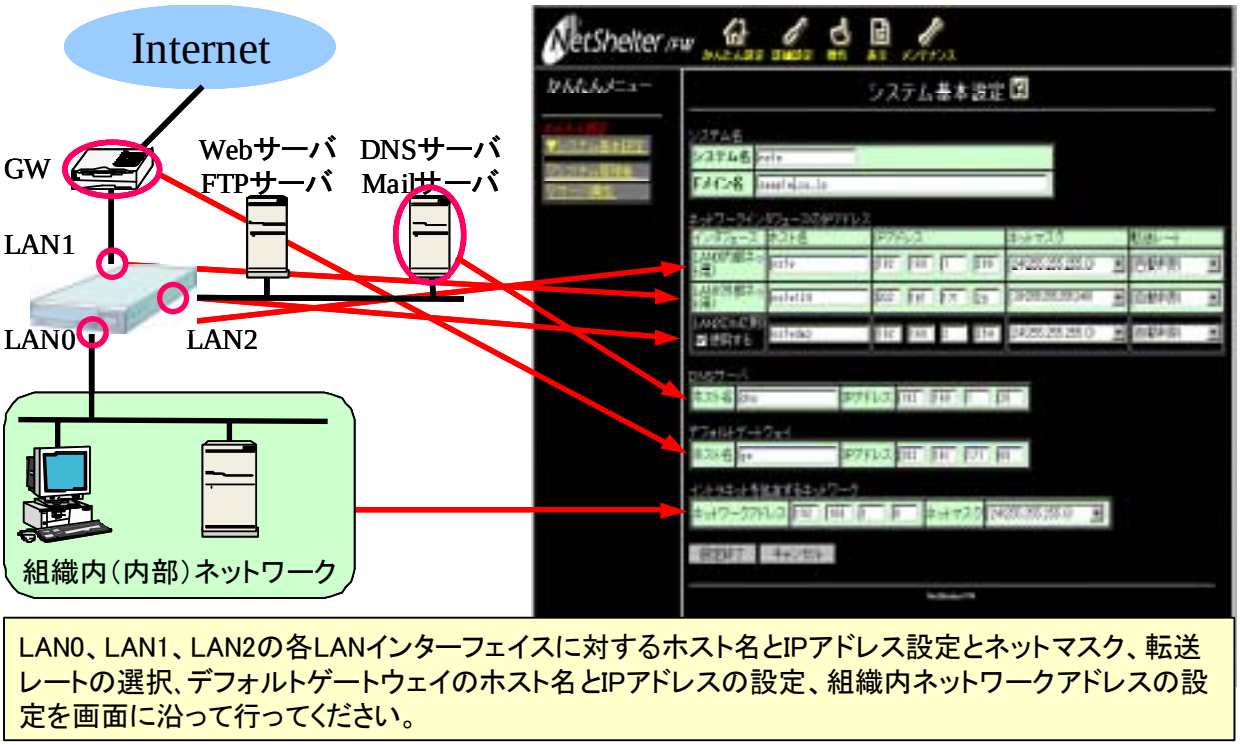
## 5.1　導入/設定の容易さ

### (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。

### (2)　設定の容易さ

本装置は、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。設定内容も短期間で導入から運用に入れるように「かんたん設定」メニューを用意する（図－３参照）。




**図－３　NetShelter/FW-P の簡易設定メニュー画面**

かんたん設定は、本装置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なる。

## 5.2　運用の容易さ

### (1)　状況表示、ログ表示機能

本装置では、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－４参照）。

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 ネットサーク状況表示
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確認状況
サマリ、アラート機能、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。
集計単位としてヒット率、URL 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－４　**NetShelter/FW-P 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、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出来る。

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、本体直前にあるアラーム 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、システムの機能運転が困難な場合は、直ちに安全に装置を停止する機能を備えている。

# 6　導入事例

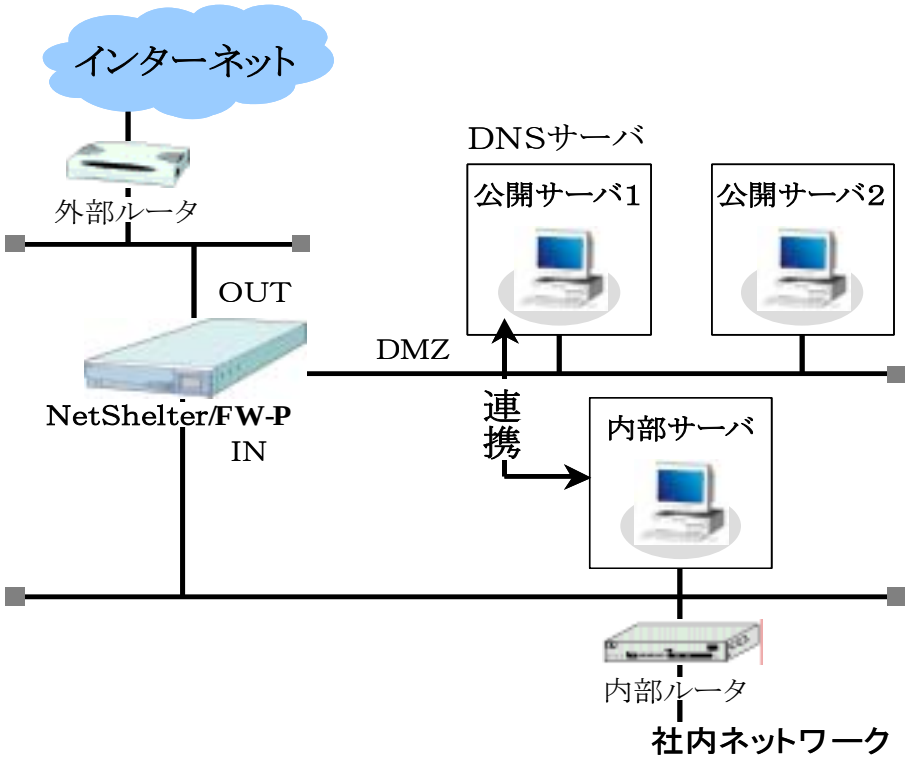
以下に、本装置の代表的な設置パターンについて説明する。

## 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、環境を構築する（図－５参照）。

- 新規にインターネットアクセスとインターネットへ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、FTP サーバ、ニュースサーバを同一マシンに設置
- 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



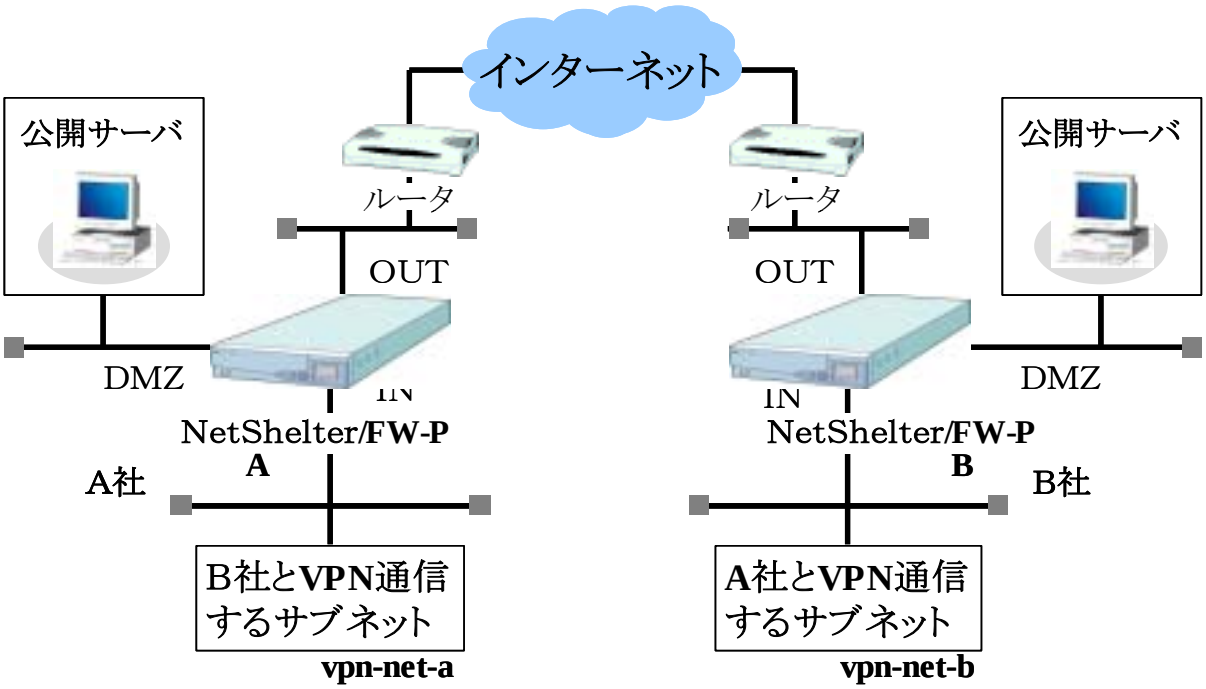

**図－５　DMZ に公開サーバを設置した形態**

## 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、環境を構築する（図－６参照）。

- 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。

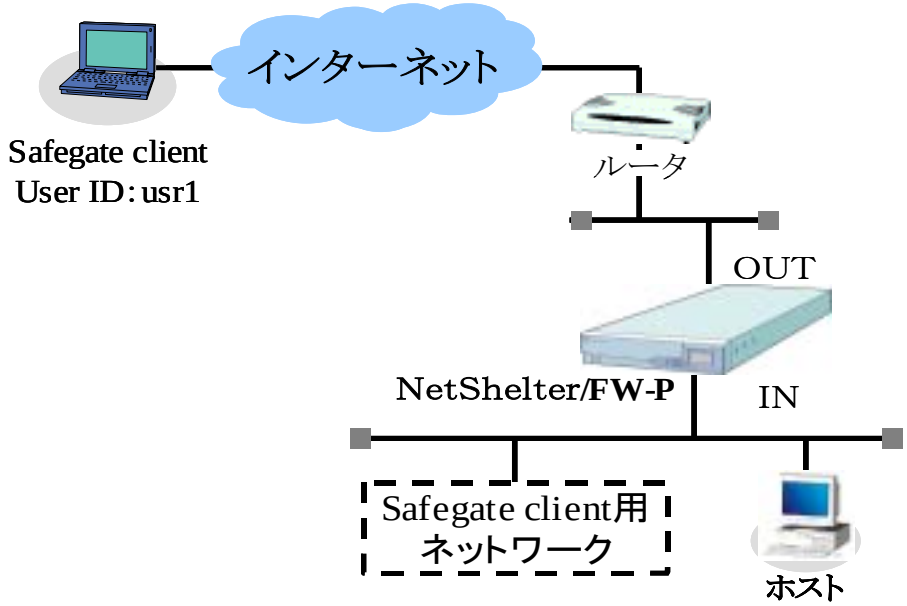



図－６　VPN（IKE を使った IPsec 通信）形態

## 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、本装置を経由して社内にアクセスする際の設定例を示す。Safegate client からのアクセスは、事前に登録されたユーザ情報よってユーザ認証をした後、社内へアクセスする。以下の条件を想定し、環境を構築する（図－７参照）。

- 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 を使って社内に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－７　モバイル PC（Safegate client を利用した通信）形態