ファイアウォール専用装置

# GeoStream NetShelter/FW-G

プロダクトレポート

富士通株式会社

2003年11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-G の特長

本装置は、NetShelter/FW シリーズの最上位機種に位置し、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大規模事業所向け専用装置（1U ラックマウント型）である。

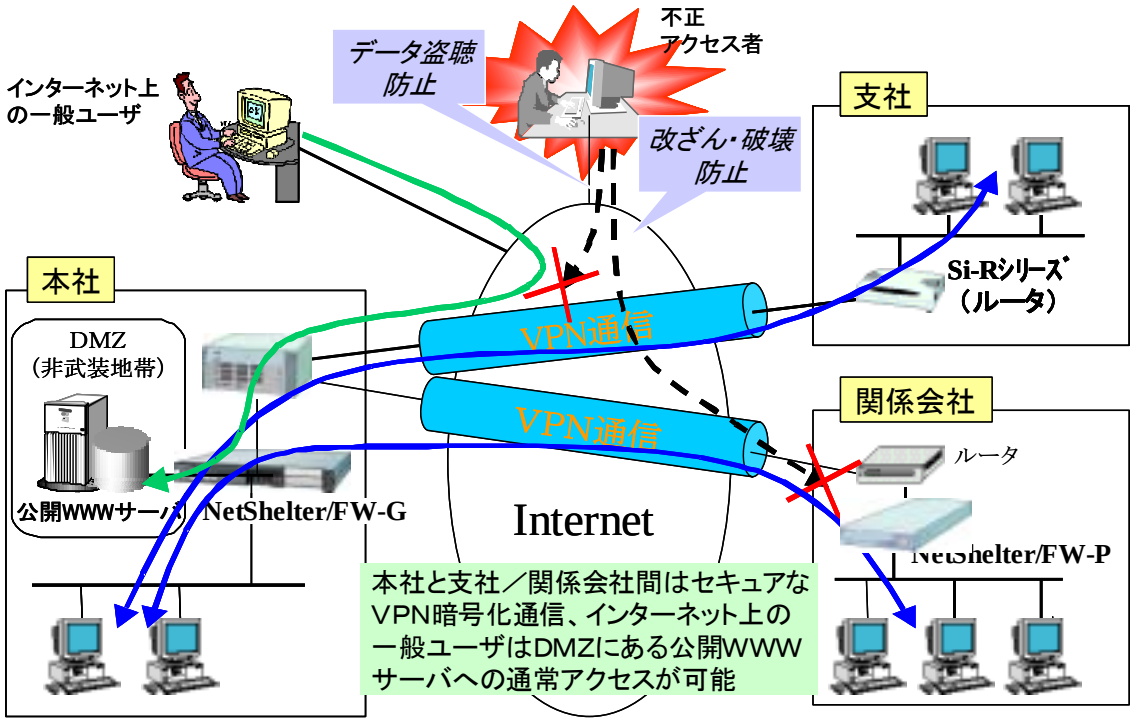
ファイアウォール機能としては、外部からの不正侵入を防ぐ IP パケットフィルタリング機能、外部から内部のホストやネットワークの情報（IP アドレス）を隠すアドレス変換機能などがある。

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、増大するネットワーク負荷に対応するため、ギガビットベースの LAN インタフェースや二重化連携機能、および、経路監視機能などによる高性能でかつ高信頼なネットワーク基盤を構築可能な機能を提供する。

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、VPN 通信用暗号化アクセラレータを搭載し、運用系 LAN（IN、OUT、DMZ）、および、保守監視系 LAN（AUX）はギガ対応 LAN インタフェースを装備している。




**図－１　NetShelter シリーズ・ファイアウォール製品の利用概念**

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、大規模事業所で運用できるように、アドレス変換機能、経路情報広報機能、VPN 通信機能、および、リモート端末機能を提供。

(2) 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、イベント監視機能、イベント通知機能、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）、時刻同期起動を提供。

(3) 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、ダンプ収集機能およびファイアウォール停止機能を提供。

(4) 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。

特に、NetShelter/FW-G は、NetShelter/FW-P の特長を継続しつつ、大規模事業所向けということで、以下の機能強化を行い、高セキュリティ、高性能、高信頼のユーザシステムの構築を可能とする。

(1) 動的 NAT 同時利用可能コネクション数の拡大

動的 NAT において、同時に利用可能なコネクション数を 500,000 に拡大し、大量の同時アクセス運用（５万人まで）を実現。

(2) 1Gbps-LAN をターゲットとした高性能

高いスループット性能 1.3 Gbps（双方向、パケットサイズ：1518byte）を実現。

(3) 高性能な VPN 暗号通信

IPsec を利用した暗号化を行っている場合、暗号化アクセラレータを標準搭載し、暗号処理のハードウェア化により、VPN 暗号通信性能は最大スループット 170Mbps（3DES）を実現。

(4) Hub&Spoke 接続機能

センタ装置に接続された各拠点間の VPN 通信を中継する機能。

本機能を利用することにより、各拠点に配置された VPN 装置は、センタ装置との間に１つトンネルを作成するだけで、簡単に他の拠点との VPN 通信を実現。

(5) ラック搭載状態でのメンテナンス性向上

前面ケーブリング、前面・背面にマークスイッチ、マーク LED を採用し、ラック搭載状態でのメンテナンス性を向上

# 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、500,000 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
- VDOLive
- 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。

また、静的 NAT 機能では、内部ネットワーク上のプライベートアドレスに対して、外部公開用のグローバルアドレスを仮想アドレスとして一対一でテーブル管理し、外部ネットワークから仮想アドレスに対してアクセスされた場合、対応するプライベートアドレスのホストに対してアクセスを行う。本装置では、この仮想アドレスを最大 64 個定義することができる。

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。

また、内部ホストからのアクセスに対して、外部ホストから内部ホストに対して異なる接続を要求するサービスやホスト間の通信は、動的 NAT と同様のサービスのみをサポート対象とする。

### (3) 経路情報広報機能

静的 NAT や Safegate client で使用する仮想アドレスに対する経路情報やデフォルトの経路情報を広報する機能を提供するが、Routed のようなルーティングデーモンによる動的な経路情報交換機能は提供しない。

- 仮想アドレス広報機能
  静的 NAT や Safegate client で使用する仮想アドレス宛のパケットが本装置に届くように、静的 NAT の仮想アドレスの場合は、外部（OUT）へ、Safegate client の仮想アドレスの場合は、内部（IN および DMZ）へ経路情報の広報を行う。

- デフォルト経路広報機能
  動的な経路情報交換機能はサポートしていないため、社内ネットワークのゲートウェイなどへ静的な経路情報の設定が必要となる。

  そこで、IN、または、DMZ 側へデフォルト経路（0.0.0.0）のゲートウェイアドレスとして、本装置のアドレスを設定した RIP1 パケットを定期的に送信する。

- 隣接機器の Arp テーブル更新機能
  隣接機器の Arp テーブルを更新するため、本装置の各インタフェースから Arp 広報を行う。

## 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 1024 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 32 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、1024 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出来ないので、相手ゲートウェイ 1 つに対し、最大 32 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。

- 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。

**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1024 | 最大128 |
| 相手暗号GW毎の条件数 | | 最大32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）

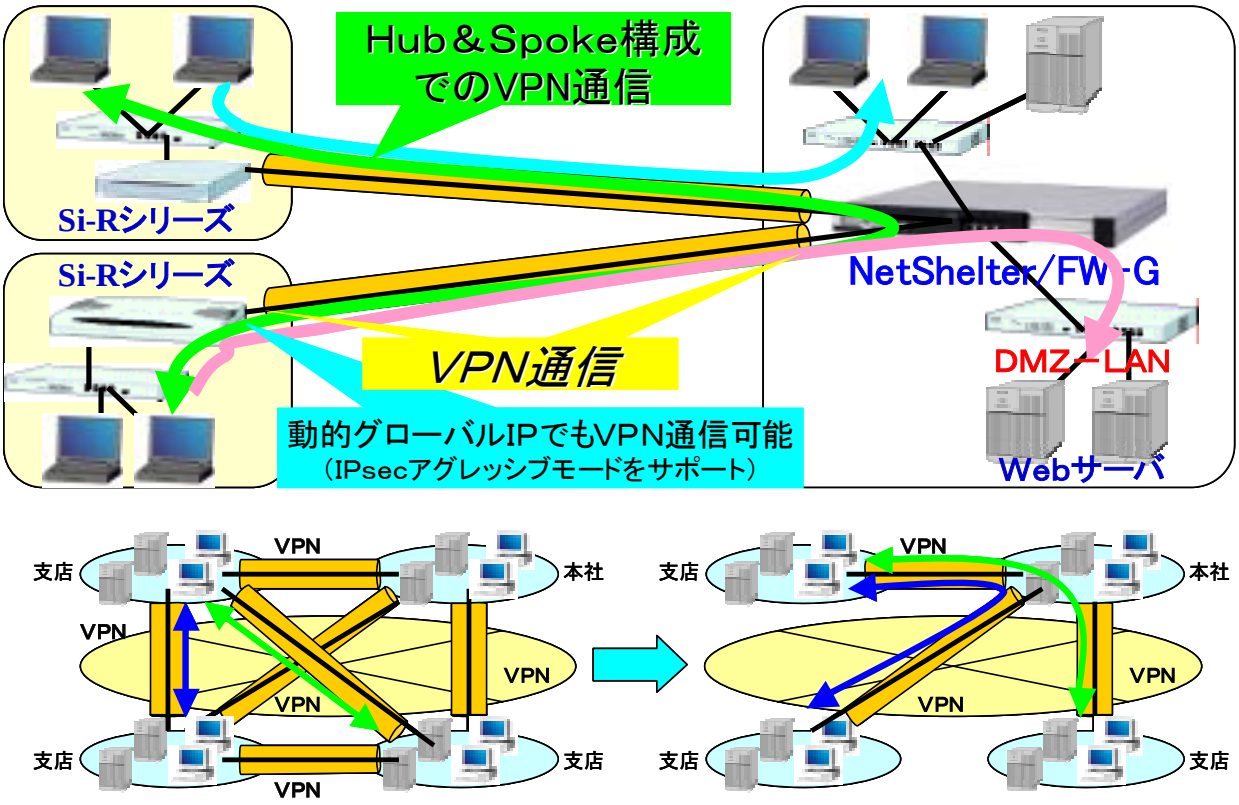
## (4)　IPsec アグレッシブモード

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。

### (5) Hub & Spoke 接続機能

Hub & Spoke 接続機能とは、複数の相手と VPN 通信を行う場合に、センタ側に Hub となる本装置を配置し、複数拠点間の仲介として VPN 通信を行う機能である（図－２参照）。

Hub & Spoke 構成を取ることにより、各拠点に配置された VPN 通信機能を装備した装置は、センタの本装置との間に 1 つのトンネルを作成するだけで、他の拠点との VPN 暗号通信を行うことができる。つまり、本接続機能では、送信元の拠点から届いたパケットを一旦復号し、再度、暗号化を行って送信先の拠点へ転送するので、各拠点とセンタ間の暗号条件は、トンネル毎に設定することができる。本機能は、IPsec 暗号方式、および、IKE 暗号方式で使用可能である。




図－２　**Hub & Spoke 接続機能の利用概念**

## 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 運用支援機能

### 3.2.1 ロギング機能

本装置を運用中に検出したさまざまな事象をログファイルとして、各々動作状況ログと統計情報ログを記録管理する。記録単位は、機能単位（IP フィルタ、IPsec、独自暗号、IKE、認証）毎に、１日単位で専用のログファイルを作成し、記録する。保存方法は、ログファイルの保存日数を 31 日とし、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）。

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。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。なお、同時にローカル syslog サーバにも同じログ情報が格納される。格納されたログ情報、および、syslog の各情報は、Web ブラウザ経由により環境設定用端末で管理者の元に取り出すことができる。また、任意のメールアドレスにメール送信することも可能である。

記録内容は、表の通りである。

**表　ログ情報一覧**

| ログ情報 | 説明 |
|---|---|
| パケットフィルタログ | IPフィルタリングによるパケットの通過､破棄などの処理結果を記録する。<br>ログ番号、ログ事象の検出日時、ログ事象検出LANレポート、送信元ホストIP、送信先ホストIP、プロトコル、送信先ポートまたはサービス、送信元ポートまたはサービス、および、処理結果を記録。 |
| パケットフィルタ統計ログ | IPフィルタリングによるパケットの通過､破棄などの処理結果を集計し､統計情報として記録する。サービス、総数、通過数、破棄数を記録 |
| パケットフィルタアラートログ | IPフィルタリングによる不当パケットの破棄数が､任意のしきい値を超える毎に１つのアラート情報を記録する。アラートログ番号、ロギング日時、検出インタフェース、検出パケット情報、種別、ログ番号を記録。 |
| IPsec暗号エラーログ | IPsec方式でのVPN通信で異常が発生した場合に、エラー情報を記録する。<br>ロギング番号、ログ事象検出日時、相手暗号ゲートウェイ名、処理種別、送信元の端末IPアドレスまたはホスト名、送信先の端末IPアドレスまたはホスト名、プロトコル、送信元ポート番号、送信先ポート番号、SPI値、処理結果を記録。 |
| IKE通信エラーログ | IKE通信で異常が発生した場合に、エラー情報を記録する。<br>ロギング番号、ログ事象検出日時、相手IKEゲートウェイ名、処理結果を記録。 |
| 独自方式暗号エラーログ | 独自方式暗号でのVPN通信で異常が発生した場合に、エラー情報を記録する。<br>ロギング番号、ログ事象検出日時、相手暗号ゲートウェイ名、処理種別、送信元の端末IPアドレスまたはホスト名、送信先の端末IPアドレスまたはホスト名、プロトコル、送信元ポート番号、送信先ポート番号、鍵ID、処理結果を記録。 |
| 認証ログ | Safegate clientからのユーザ認証要求における処理結果を記録する。<br>ロギング番号、ログ事象検出日時、認証ユーザID、認証ユーザIDがアクセスしてきたclientの仮想アドレス、処理結果、処理結果が認証拒否の場合に表示されるエラーコードを記録。 |

## 3.2.2　アラート機能

本装置が不正アタックやシステム動作異常などのアラート異常を検出すると､ロギング機能によるローカルのログファイルへの記録と共に､syslog､SNMP トラップ､またはメール送信を利用したリモートへのアラート通知を行うことができる。

**表　アラートイベントのしきい値**

| 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 | 同一送信元からの破棄パケットが､単位当たりの破棄パケット数で設定した値を超えた場合に通知。 |
| 同一宛先へのアタック | 同一宛先への破棄パケットが､単位当たりの破棄パケット数で設定した値を超えた場合に通知。 |
| IPsec暗号パケット改ざん | １パケットでも異常パケットを検出した場合に通知。 |
| IKE通信異常 | １ネゴシエーションでも通信異常を検出した場合に通知。 |
| 独自暗号パケット改ざん検出 | 1パケットでも異常パケットを検出した場合に通知。 |
| 認証拒否 | 認証が拒否された場合に通知。 |
| Disk Full（ロギング領域） | ロギング領域に空き領域が無くなった場合に通知。 |
| ディスク異常 | ディスク異常が発生した場合に通知。 |
| FAN異常 | ファン異常が発生した場合に通知。 |
| UPS異常 | UPS異常が発生した場合に通知。 |
| メモリ異常 | メモリ異常が発生した場合に通知。 |
| LANコントロール異常 | LANコントローラ異常が発生した場合に通知。 |

### 3.2.3 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 |

### 3.2.4 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。

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。

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 |

### (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

## 3.2.5　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

### 3.2.6 時刻同期機能

本装置の時刻を設定する方法には、以下の２通りがある。

- 手動設定
  手動設定では、設定したい時刻を手動で設定する。
- 自動同期
  自動同期では、上位タイムサーバに時刻を問合せ、タイムサーバと本装置の時刻を一致させ、同期をとる機能をサポートする。

#### (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 2 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。

## 3.3 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。なお、IN ポートを使用しても行える。

**表　保守監視の設定**

| 設定内容 | 説明 |
|---|---|
| 保守監視パスワードの設定 | 保守監視用のパスワードを設定。 |
| AUXポートの設定 | 保守監視用ネットワークをAUXポートに接続するための設定。 |
| 監視端末設定 | 保守監視ネットワーク上で保守監視端末を接続するための設定。 |
| syslog設定 | syslogサーバを保守監視用ネットワーク上で利用するための設定。 |
| SNMP設定 | SNMPマネージャを保守監視用ネットワーク上で利用するための設定。 |
| Safegate集中管理設定 | Safegate集中管理サーバを保守監視用ネットワーク上で利用するための設定。 |
| ロギング・アラート設定 | メールによるログ採取やアラートメール送信を保守監視用ネットワーク上で利用するための設定。 |
| 保守監視情報の反映 | 保守監視機能の各種設定をシステムに反映。 |

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。

本装置では、最大 2 個のメモリダンプと 1 個のプロセスダンプを採取することができる。

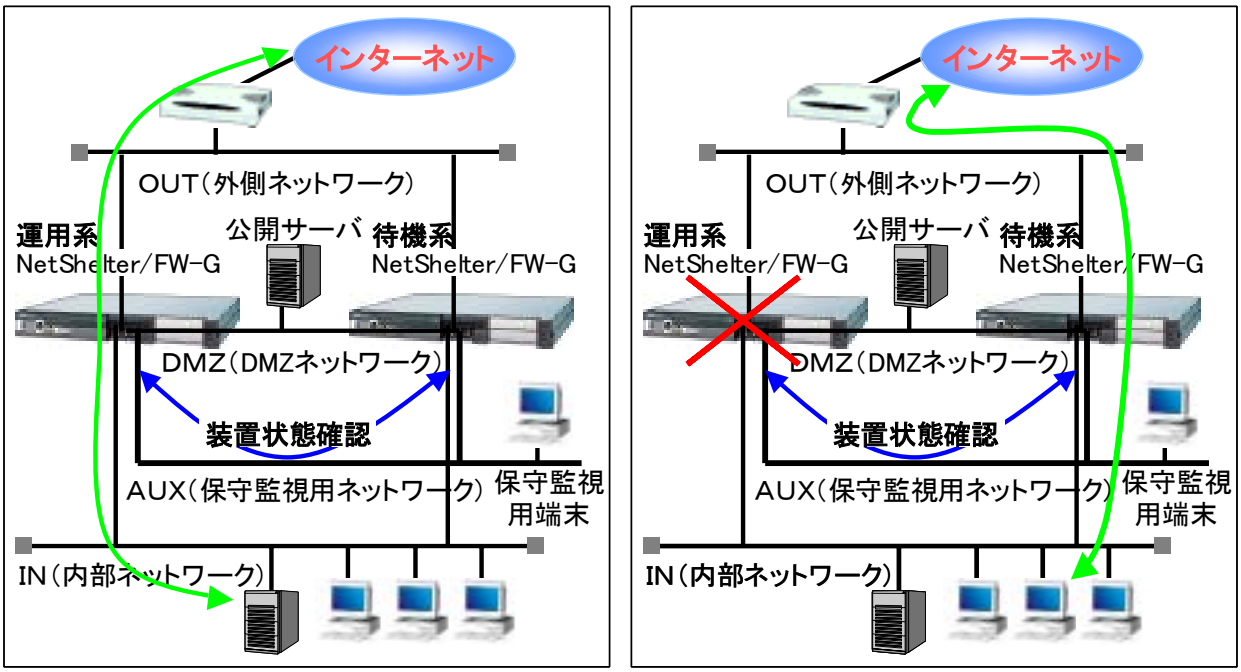
### (4) ファイアウォール停止

AUX ポート以外のネットワークを一時的に非活性にする機能である。

## 3.4 二重化制御

### 3.4.1 二重化連携機能

二重化連携機能は、2 台の本装置で冗長構成（二重化構成）をとる機能である（図－３参照）。




図－３　二重化連携図の概要

２台の装置を運用・待機とし、各々の装置で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、もう一方の装置がその状態を検知し、運用を継続する。
通常、運用系装置だけが動作しており、運用系装置が装置故障やファームウェア異常などでシステム停止した場合、待機系装置がその異常を検知し、自動的に処理を再開する。

- 相互監視機能
  メインパスとサブパスの 2 系統のノード間通信パスを利用して、二重化を構成する 2 つのノードを相互に監視する機能である。ノード間通信パス上には、一定間隔でハートビートパケットが送受信され、他ノードの生死監視を行い、規定時間内（ハートビート送信間隔（1 秒）×監視回数（3 回））に到達しなかった場合、ノード異常と判断する。また、ノード間通信パスは、メインパスとサブパスで冗長化されている。

- 状態遷移機能
  状態遷移機能は、二重化を構成する各ノードの状態により、本装置の二重化状態（二重化連携状態、片側運用状態、停止状態）を変化させる機能である。

- ファイル配布機能
  運用系の異常発生時に備えて、運用系と待機系の環境を一致させる機能である。
  運用系ノードの停止時は、待機系ノードが新運用系として動作し、処理の引き継ぐ。

  －立上げ処理時に、運用系の環境定義情報を待機系に反映する。
  －組込み処理時に、運用系の環境定義情報を待機系に反映する。
  －「環境定義情報の反映」時に、運用系で変更された情報を待機系に反映する。
  －環境定義情報の復元時に、復元された定義情報を待機系に反映する

- 時刻同期機能
  ノード間通信機能の定周期診断プロトコルを利用して、自ノードと他ノードの時刻を同期する機能である。

- 状態通知機能
  二重化連携動作時の各状態を通知する機能で、以下の手段で管理者に通知される。
  環境設定画面での状態表示、LCD 表示、Syslog 通知/Safegate 集中管理へのメッセージ通知、SNMPTrap 通知、メール通知

- 導入支援機能
  本装置の二重化機能導入を支援する機能で、液晶パネルと操作スイッチから簡単に導入ができる。最初に 1 台の装置で環境設定を行い、その後、二重化導入を行うと設定した内容が他装置にも複写される。

- パネル操作機能
  装置の液晶パネルと操作スイッチで二重化の機能を提供する。
  －両系停止機能：片方の装置で指定することで両方の装置を停止する。
  －切替え機能　：パネル操作で二重化の切替え処理を行うことができる。

### 3.4.2 状態と遷移

#### (1) 状態

- 二重化連携状態
  運用系と待機系が定周期で通信を行い、相手装置の状態を監視している状態である。
  二重化連携時には、運用系の設定環境に変更があった場合、待機系のその変更内容が通知され、常に運用系と同じ設定環境となり異常発生時の動作に備える。

- 片側運用状態
  運用系装置のみが動作している状態である。以下の場合に、片側運用状態で動作する。
  ー立上げ時に片方だけ電源を投入した。
  ー運用系装置が停止し、切替え処理が行われた。
  ー待機系装置が停止し、切捨て処理が行われた。

- 停止状態
  停止状態は、運用系装置と待機系装置の両方の電源が入っていない状態である。

#### (2) 遷移

- 立上げ処理
  立上げ処理は、電源投入により停止状態から二重化連携状態へ遷移する処理である。

- 切替え処理（運用系の異常停止）
  運用系装置に異常が発生した場合は、切替え処理が行われ二重化連携状態から片側運用状態へ状態遷移する。装置故障による切替えが発生した場合、運用系から待機系に処理が引き継がれる。

- 切替え処理（運用系のシステム停止）
  運用系のみシステム停止を行った場合は、切替え処理が行われ、二重化連携状態から片側運用状態へ状態遷移する。

- 組込み処理
  組込み処理は、片側運用状態から二重化連携状態へ遷移する処理である。組込み処理は、運用系処理には影響がないため、NetShelter は通常のサービスを継続する。

- 切捨て処理（待機系の異常停止）
  待機系装置に異常が発生した場合は、切捨て処理が行われ二重化連携状態から片側運用状態へ状態遷移する。

- 切捨て処理（待機系のシステム停止）
  待機系のみシステム停止を行った場合は、切替え処理が行われ、二重化連携状態から片側運用状態へ状態遷移する。

- 切戻し処理
  前回運用系で動作していた装置を組み込んだ場合、再び運用系として動作するように、組込みの後に切替えを行う処理である。切り戻し処理には、以下のモードがあり、各モードの切替えは、GUI で設定する。

－通常切り戻しモード（初期値）
装置を一旦待機系として組み込み、利用者がシャットダウンを行ったり、LCD メニュー操作により切替え処理を行うモードである。運用系で動作しているサービスの中断は発生しない。

－自動切り戻しモード
自動切り戻しモードは、装置を待機系として組み込んだあと、自動的に切替え処理を行うモードである。運用系で動作しているサービスの中断が発生する。

- 両系停止処理
LCD メニューでシャットダウンを行い、二重化連携状態から停止状態へ状態遷移を行う処理である。

### 3.4.3 環境の引継ぎ

二重化連携機能では、運用系の環境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、双方の環境が常に同一となるような処理を行う。運用系ノードの停止時には、待機系ノードが新運用系として動作し、処理の引き継ぎを行う。以下のタイミングで、環境の引き継ぎが行われる。

－立上げ処理時に、運用系の環境定義情報を待機系に反映する。
－組込み処理時に、運用系の環境定義情報を待機系に反映する。
－「環境定義情報の反映」時に、運用系で変更された情報を待機系に反映する。
－環境定義情報の復元時に、復元された定義情報を待機系に反映する。

通信処理中にメモリ上で展開している情報は引き継げない。また、UPS 情報や保守監視情報など、各装置固有情報の引き継ぎは行わない。各機能の環境引き継ぎの可否を示す。

**表　各機能の環境引継ぎ**

| 機能 | | | 引き継ぎの可否 |
|---|---|---|---|
| IPパケットフィルタリング機能 | | | 引継ぎ後の制限なし（フィルタ引継ぎ） |
| アドレス変換機能（NAT機能） | 動的NAT | | 中継情報を引き継がないため、TCPの再接続、および、UDPパケットの再送が必要（注1） |
| | 静的NAT | | |
| VPN通信機能 | | | 暗号キーは引き継ぐが、IKEの鍵情報は引き継がれない（注5）。 |
| リモート端末接続機能 | | | 引継ぎ後、再接続が必要（注2） |
| ネットワーク管理エージェント機能 | NetEyeManager連携 | | 引継ぎ後の制限なし（注3） |
| | SystemWalker連携 | | 引継ぎ後の制限なし（注3） |
| | Safegate集中管理連携 | | 引継ぎ後、再接続が必要（注2）<br>（クライアント用暗号キー引継ぎ）（注3） |
| 運用支援機能 | 環境設定 | | 引継ぎ後の制限なし |
| | アラート | | 引継ぎ後の制限なし |
| | ロギング | Syslog | ログの引継は行わない。（注4） |
| | | パケットフィルタログ | |
| | | 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 | |
| 退避／復元 | | | 引継ぎ後の制限なし |
| 停電対策 | | | 引継ぎ後の制限なし |
| 経路監視機能 | | | 引き継ぎ後の制限なし |

注１）NAT テーブルの引き継ぎは行わないため、切替え発生後は以下の状態となる。
－動的 NAT： TCP については、セション確立中のものは通信が切断される。
UDP については、外部からの応答待ちであった場合は、その応答が受け取れないため、応答待ちがタイムアウトする。
－静的 NAT： 二次コネクションの発生する以下のサービスは、再接続が必要。
ftp、RealAudio、StreamWorks、VDOLive、Cu-SeeMee
これ以外のサービスについては、セションが保持される。

注２）認証情報の引き継ぎは行わない。切替え発生後は、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３）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。

注４）下記の理由により、ログの引き継ぎは行わない。
－装置切替え発生時、切替え原因の特定を速やかに行うため。
－データ量が多いことから、運用時に性能への悪影響が懸念されるため。

注５）IKE 鍵情報の引き継ぎは行わない。切替え後の最初のアクセスで IKE の鍵交換処理が行われる。

### 3.4.4 経路監視機能

経路監視機能は、本装置の二重化連携機能が導入されている場合に動作し、本装置に接続されたネットワークの隣接機器および配線の異常を検知して、各ノードの状態によりネットワークの切替えやネットワークの停止を行う機能である。経路監視機能は、各ネットワークの終端に監視ホストを配置し、監視ホストからのパケットを監視することで行う。

監視ホストとは、本装置からの ICMP（Echo Request）に対して正常に ICMP（Echo Reply）の応答ができる環境を満足する PC またはルータをいい、監視するネットワークの終端に配置する。監視ホスト以遠のネットワークの監視は行わない。通常、経路監視機能を使用するためには、運用系ネットワークと待機系ネットワークの 2 系統のネットワーク環境を用意し、運用系で経路監視異常を検出した場合は、待機系に切り替える処理を行う。

また、待機系で経路監視異常を検出した場合は、その旨メッセージを通知する。なお、経路監視の対象となるネットワークは、IN/OUT/DMZ が対象となり AUX は経路監視の対象とはならない。

- 異常検出方法
  経路監視機能の異常検出は、監視するネットワークに接続された監視ホスト（IP アドレス）からのパケット有無を監視する。監視ホストからのパケット送信は不定期なため、ICMP（echo request）を定期的に送信し、ICMP（echo-reply）の受診を監視する。
  本装置の経路監視では、ICMP（echo-reply）を監視するのでは無く、単に監視対象の監視ホストからのデータパケットを受診したか否かの判定を行う。監視ホストから監視時間内にデータパケットを受信しなかった場合、経路異常と判断する。
  本体装置異常時と経路監視異常時の相違点について示す。

**表　装置異常時と経路監視異常時の相違点**

| | 装置故障 | LAN機器の異常（他の機器or LAN） |
|---|---|---|
| 運用系 | ・装置の異常を検出後切替え発生。新運用系による単独運用となる。<br>[動作]<br>運用系：システム停止<br>待機系：切替え発生後に単独運用 | ・運用系ネットワーク経路異常を検出後に切替えを行なう。<br>[操作]<br>運用系：経路異常を通知し、切替え発生後に待機系として動作する。また、ネットワークの修復後も待機系として動作する。<br>待機系：切替え発生後、新運用系として動作する。 |
| 待機系 | ・装置の異常を検出後切捨て発生。運用系による単独運用となる。<br>[動作]<br>運用系：切捨て発生後に単独運用。<br>待機系：システム停止 | ・待機系ネットワーク経路異常を検出後に異常を通知する。<br>[動作]<br>運用系：正常動作<br>待機系：経路異常を通知し、経路監視を継続<br>ネットワーク修復後は正常動作継続 |
| 運用系＋待機系 | ・両系の装置が異常を検出し、両系のシステムが停止する。<br>[動作]<br>運用系：システム停止<br>待機系：システム停止 | ・両系のネットワーク経路異常を検出後、経路異常を通知する。<br>[動作]<br>運用系：経路異常を通知し、経路監視継続。ネットワーク修復後は正常動作継続。<br>待機系：経路異常を通知し、経路監視継続。ネットワーク修復後は正常動作継続。 |

# 4　ハードウェア仕様

本装置のハードウェアは、ラックマウントタイプの 1U サイズの大きさで、前面に LAN ポートを配置し、ラック搭載状態での配線を容易にし、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）を表示するなど、メンテナンス性の向上を図っている。

さらに、ディスクレスによる装置信頼度の向上を図り、UPS 装置でのバックアップを必要としないシステムの構築を可能とする。

下表に、ハードウェア仕様を示す。

**表　NetShelter/FW-Gハードウェア仕様**

| | | |
|---|---|---|
| LANインタフェース | LANポート | 10/100/1000BASE-T×3 |
| | 保守／二重化 | 10/100/1000BASE-T×1 |
| 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（2,400Kbps,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（インストール、アップデート用） |
| 外形寸法（幅×奥行×高さ） | | 422 mm × 488 mm × 44 mm（ゴム足、突起物を除いて） |
| 重量 | | 10.0 Kg |
| 消費電力 | | 130 W（最大） |

また操作キーと LCD パネルによるメニュー操作では、システムの停止などの基本的な設定、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-L 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。

本装置の前面パネルを示す（図－４参照）。

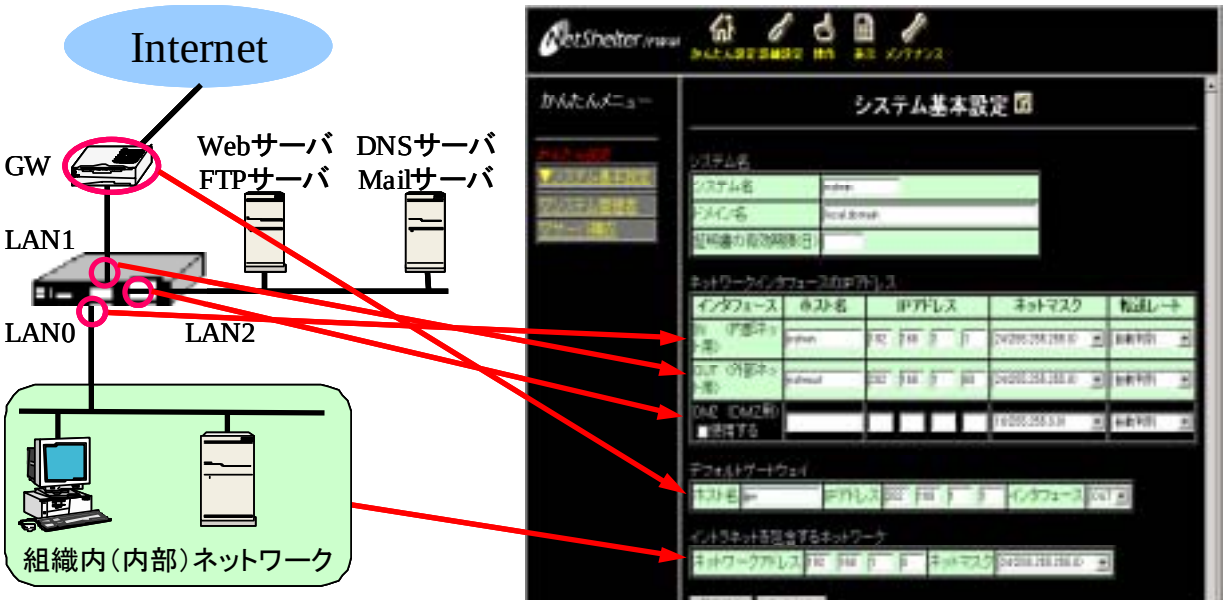

**図－４　NetShelter/FW-G 装置の前面**

# 5　かんたん導入/設定/運用

## 5.1　導入/設定の容易さ

- 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。

- 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。
  以下に簡単設定メニュー画面を示す（図－５参照）。




**図－５　NetShelter/FW-G 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

- 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－６参照）。

－ 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
－ 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）
－ 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、認証ログなど

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－６　**NetShelter/FW-G の統計情報表示例**

## 5.3　高信頼性・運用性

ディスクレスによる装置の信頼度を向上させることで、停電や瞬電などの電源異常が発生しても、UPS（無停電電源装置）に接続することなく、安全にシステムを停止することができる。なお、UPS 装置を接続することも可能である。

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

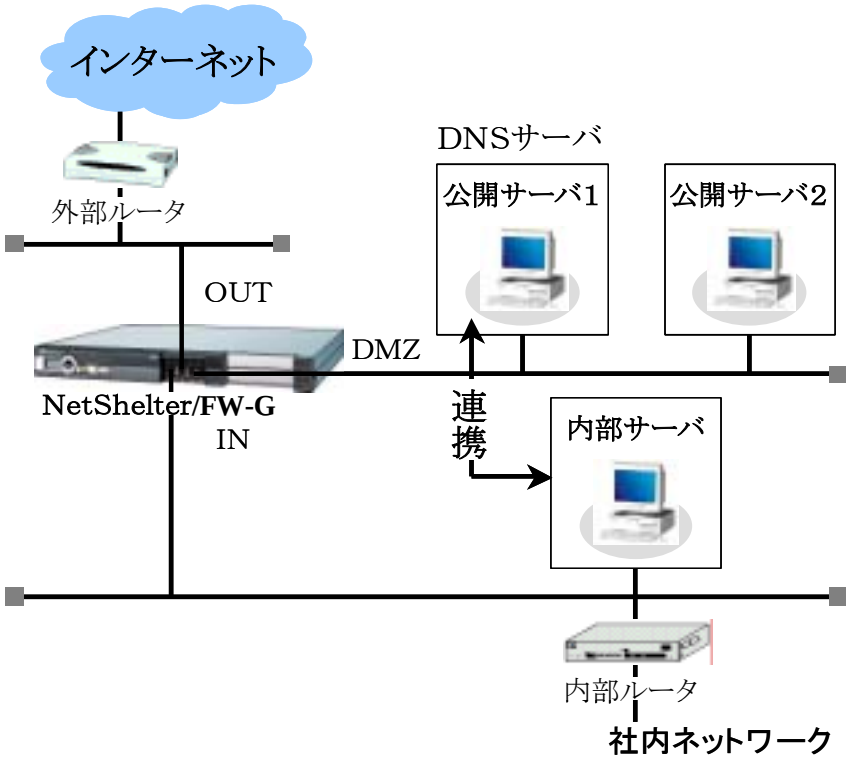
以下に、本装置の代表的な設置パターンについて説明する。

## 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－7 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



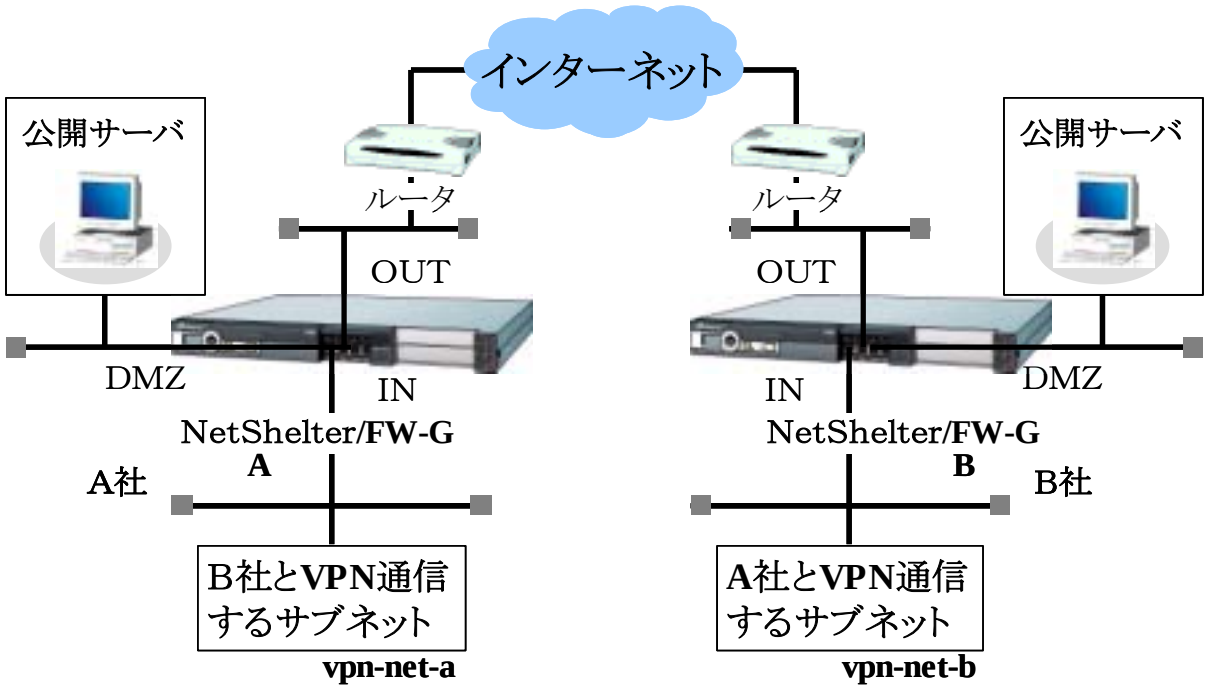

**図－7　DMZ に公開サーバを設置した形態**

## 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－8 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。

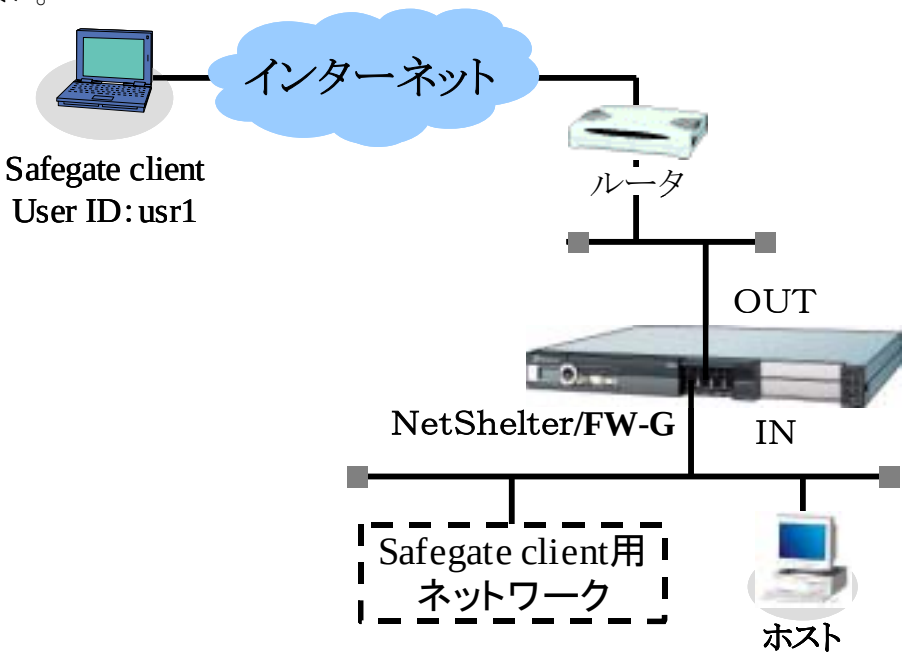



図－８　VPN（IKE を使った IPsec 通信）形態

## 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－９参照）。

- 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－９　モバイル PC（Safegate client を利用した通信）形態