ファイアウォール専用装置

GeoStream NetShelter/FW-L

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-L の特長

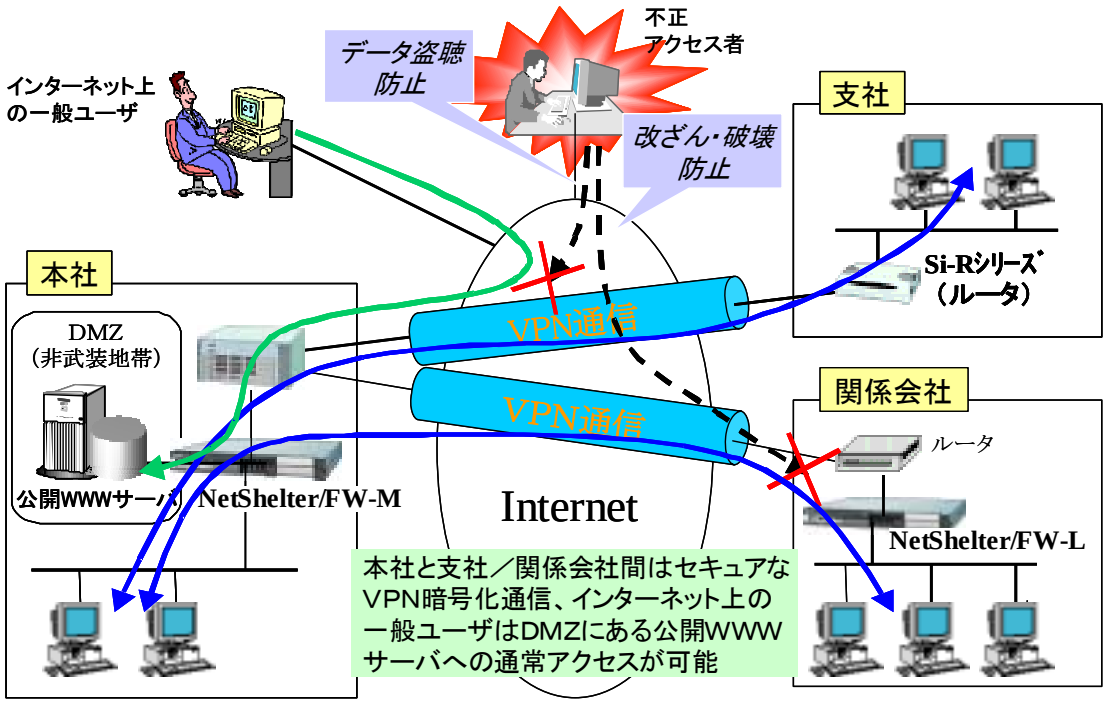
本装置は、NetShelter/FW の上位機種で、NetShelter/FW-M の下位機種に位置し、専用回線などを利用したインターネット常時接続環境のセキュリティ対策としてファイアウォールを構築するための中小規模事業所向け専用装置（1U ラックマウント型）である。

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、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、SYN Attack や DoS（Denial of Service）攻撃などの不正アクセスを検知し、防御する IDP（Intrusion Detection and Prevention）機能や、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、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、フラシュメモリを使用したディスクレスを実現し、装置自身の信頼度を向上させ、UPS 装置でのバックアップを必要としないシステム構築を可能とする。



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、中小規模事業所で運用できるように、コネクション管理機能、アクセス制御機能、アドレス変換機能、VPN 通信機能、リモート端末機能、不正アクセスの検知・防御機能、フィルタリング条件検証機能を提供。

(2) 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 の 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と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 サーバ機能を提供。

(3) 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）、ログサーバ、稼動監視機能、時刻同期起動を提供。

(4) 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、ファイアウォール停止機能を提供。

特に、NetShelter/FW-L は、NetShelter/FW の特長を継続し、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) ステートフルインスペクションによるセキュリティ強化

TCP コネクション／UDP セッションを追跡し、不正なパケットをブロック。
アプリケーションを意識した動的な TCP/UDP ポートの穴あけと閉塞を制御。

(2) 不正アクセスの検知・防御機能

ターゲット検索、ターゲット情報の取得、攻撃（侵入、サービス運用妨害、盗聴）といった不正アクセスに対し、パケット、および、コネクションの監視による検知を行い、検知後パケット破棄による防御を行う。さらに、不正アクセス発生後、一定期間、監視を行い、ブラックサービス制御やブラックリスト制御による同一不正アクセスの防御を実現。

(3) 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）。

(4) VPN 暗号通信機能の強化

VPN 通信で IPsec を利用した暗号化を行っている場合に、通信速度の低下を防ぐため、基本機能での暗号処理を強化し、VPN 暗号通信性能を最大スループット 40Mbps（3DES）に向上。さらに、オプションの VPN 強化モジュールを搭載した暗号処理のハードウェア化により、VPN 暗号通信性能を最大スループット 100Mbps（3DES）に向上。

(5) 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。

(6) ディスクレスによる装置信頼度の向上

フラシュメモリを利用したディスクレスを実現。
UPS 装置によるバックアップを必要としないシステム構築が可能。

3　機能

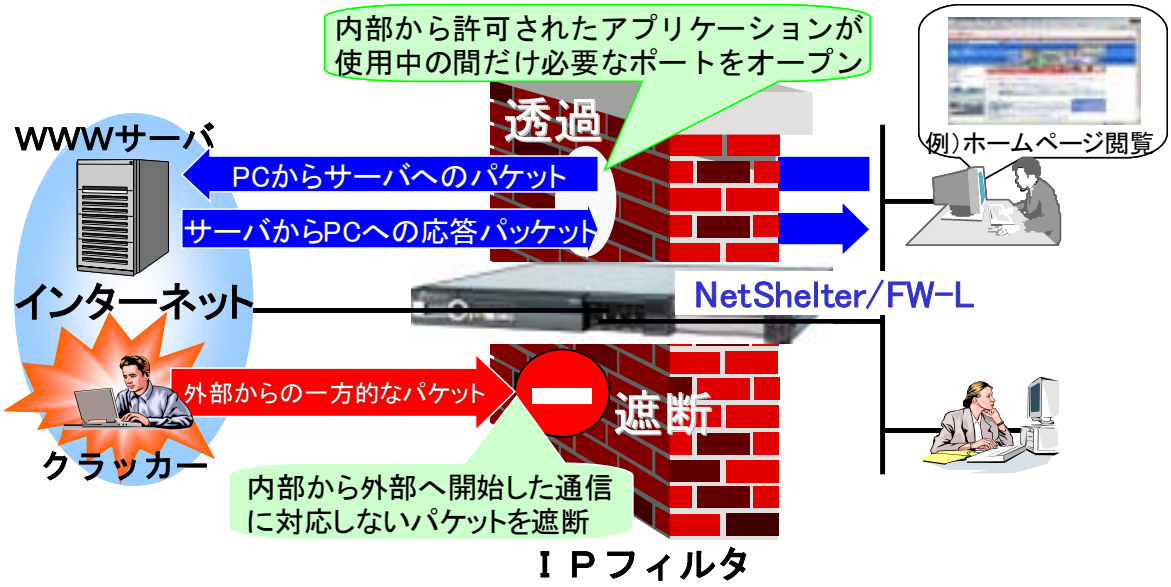
本装置の主な機能を以下に示す。

3.1　ファイアウォール機能

通過する IP パケットを対象に、送信先 IP アドレスと送信元 IP アドレス、プロトコル、サービスなどの情報をもとにパケットを通過または破棄し、外部からの不正アクセスを防御する機能である。

ファイアウォール機能では、「フィルタリング条件」に基づき、「コネクション管理機能」により、ステートフルインスペクション機能を提供している。なお、「フィルタリング条件」とは、ファイアウォール機能の動作を規定するフィルタリングルールの集合である。

フィルタリング条件が設定されていない場合は、内部ネットワークへのすべてのパケットは、破棄（ブロック）される（図－２参照）。



図－２　IP フィルタリング機能（ステートフルインスペクション）の概念

本装置では、ファイアウォール機能として、アクセス制御機能、アドレス変換機能、VPN 暗号通信機能、リモート端末接続機能、不正アクセス防御機能などを提供する。

3.1.1　フィルタリング条件

フィルタリング条件は、セキュリティポリシーに従い、個々の送受信パケットの動作を既定するフィルタリングルールの集合であり、以下の情報から構成される。

- 管理情報
  フィルタリング条件の管理情報を保持する。
  また、個々のフィルタリング条件の優先順位情報を含む。
- 条件
  ファイアウォール機能を適用する送受信データを識別する情報。

表　「条件」として設定できる属性情報

分類	説明
送信元アドレス情報	受信インタフェース、送信元IPアドレス
送信先アドレス情報	送信インタフェース、送信先IPアドレス
サービス	IPプロトコル（TCP、UDP等）、送信元ポート番号／送信先ポート番号（TCP、UDPの場合）、ICMPメッセージタイプ（ICMPの場合）
ユーザ情報	本条件が関連付けられるユーザ情報を識別。 本条件は、ここで関連付けられたユーザの認証が許可された時点で、はじめて有効となる条件であることを示す。

- 動作
  「条件」に合致したパケットに適用するファイアウォール機能を識別する情報。
  なお、VPN 通信条件もフィルタリングルールとして一元的に管理する。

表　「動作」として設定できる情報

分類	説明
通過（PASS）	データを通過させます。
破棄（BLOCK）	データを破棄します。
拒否（REJECT）	データを破棄します。送信元に拒否応答を行います。
送信元NAT	送信元IPアドレスのアドレス変換を行います。
送信元NAPT	送信元IPアドレス、送信元ポート番号のアドレス変換を行います。
送信先NAT	送信先IPアドレスのアドレス変換を行います。
IPsec暗号	マニュアルIPsec方式によるVPN 通信を行います。
IKE暗号	IKE方式によるVPN 通信を行います。
独自暗号	独自暗号方式によるVPN 通信を行います。

- 監査
  「条件」に合致したパケットに適用した「動作」の実施結果を監査情報として保存。

フィルタリングルールの設定簡略化のため、個々のサービスそれぞれに対してフィルタリングルールを設定する方法に代え、IP プロトコル上の全てのサービスや、TCP/UDP/ICMP のサービスを総称したフィルタリグルールを設定することが可能である。

表　総称サービスとして設定できる情報

総称サービス名	意味
ALL	すべての IP パケット
TCP-ALL	すべての TCP プロトコルパケット
UDP-ALL	すべての UDP プロトコルパケット
ICMP-ALL	すべての ICMP プロトコルパケット

3.1.2　コネクション管理機能

アクセス制御機能、および、アドレス変換機能で、送受信されるそれぞれの IP パケットは、「コネクション情報」として、その通信が終了するまで維持・管理される。

このコネクション情報を利用し、それぞれのコネクション上の通信状況を捕捉／監視することで、ステートフルインスペクション機能を実現する。

- コネクション情報
  送受信される IP パケットを捕捉し、「コネクション情報」として管理する。コネクション情報は、新たなコネクションの検出時に生成し、コネクションの終了時に解放する。

表　プロトコル毎のコネクション情報の管理

プロトコル名	コネクション情報の管理
TCP	エンドシステム上のTCPは、TCPコネクションの確立、切断といった状態遷移を行いながら、TCPコネクション状態を維持している。 TCPヘッダに含まれるTCP 状態遷移事象を捕捉し、送信元、及び送信先システム上のTCPコネクション状態をエミュレートしている。
UDP	エンドシステム上のUDPは、コネクション状態を管理することはないが、アクセス制御機能やアドレス変換機能などを適用する処理方法をTCP に合わせるため、擬似的なコネクション情報として管理する。
ICMP	ICMPにはTCPのようなコネクションの概念はないが、ICMPのエラー通知と要求／応答といった２つの通信方式のうち、要求／応答方式の場合には、送信元からの要求があってはじめて送信先から応答が行われる。ICMPのこのような通信方式にも対応するため、擬似的なコネクション情報として管理する。

- 最大コネクション数
  不正アクセスでの DoS 攻撃に対応するため、本装置を介して通信可能なコネクション数に上限値を設け、メモリ資源の枯渇や枯渇にともなうシステム運用への悪影響を未然に防止する。なお、最大コネクション数以上のコネクション確立要求は破棄する。最大コネクション数は、40,000 である。

- コネクション監視タイマ
  不正アクセスやクライアント／サーバの状態（不慮の電源断など）により、正常に終了できない場合や、正常終了時でも、ネットワーク上を浮遊している再送パケットを回収する必要がある場合は、コネクション状態に応じてタイマを使用する。各タイマのタイムアウト時に、当該コネクションを無効とし、コネクション情報を解放する。

- ブロックコネクション解放タイマ
  フィルタリング条件で「破棄」、または、「拒否」が設定されたパケットを受信した場合、一旦、ブロックコネクションが作成され、継続する同様なパケットによる「破棄」、または、「拒否」イベントの発生を削減し、負荷上昇を抑止する。
  ブロックコネクション解放タイマは、ブロックコネクション上の最後のパケットを処理してから本コネクション情報を解放するまでの時間を設定する。本タイマのタイムアウト時に、ブロックコネクションは開放される。

- 監査情報
  本装置の稼働監視を効率化するために、監査情報を通知する。

表　稼動監視で通知する監査情報

分類		説明	出力先
コネクションの確立・解放	コネクション確立	新たなコネクションの検出時に生成。	コネクションログ
	コネクション解放	タイムアウトによるコネクション情報解放のタイミングで生成。通信データ量などを出力する。	
コネクション数の監視	最大コネクション数に到達	処理可能は最大コネクションに到達したことを通知する（エラー）。	Syslog
	警告コネクション数に到達（初期値は最大コネクション数の80%）	使用中のコネクション数が警告コネクション数に到達したことを通知する（警告）。	

3.1.3 アクセス制御機能

管理者により指定されたフィルタリング条件にしたがい、IP パケットの「通過（PASS）」、「破棄（BLOCK）」、および、「拒否（REJECT）」の処理を行う。

本機能により、内部ネットワークからインターネットなどの外部ネットワークを利用するユーザや利用可能なアプリケーションを制限したり、インターネットからの不正な侵入を遮断したりする。

アクセス制御機能は、以下のトラフィックに対して適用できる。

- 通過可能なトラフィック

表　通過可能なトラフィックに対するアクセス制御

通過可能なトラフィック	アクセス制御
IPアドレスのみの場合	IPプロトコルが省略されたサービスのフィルタリングルールの場合（ALL）、送受信IPアドレスにのみ特化したアクセス制御を行う。
特定IPプロトコルのみの場合	ポート番号、メッセージタイプが省略されたサービスのフィルタリングルールの場合（TCP-ALL、UDP-ALL、ICMP-ALL）、送受信IPアドレス、およびIPプロトコルにのみ特化したアクセス制御を行う。
TCP/UDPポート番号を含めた場合	TCP/UDPポート番号を含めたアクセス制御を行う。
ICMPメッセージタイプを含めた場合	ICMPメッセージタイプを含めたアクセス制御を行う。なお、適用可能なICMPメッセージは、ICMP ECHO /Reply（ping）のみである。

- アプリケーション

  FTP プロトコルやマルチメディア系サービスなどのように、一つの機能を利用する場合に複数のコネクションが確立され、それらのコネクションの相関関係自体が、送受信データ領域に明示されている場合は、TCP/IP ヘッダに加え、各プロトコルのデータ領域までを評価する必要があり、一つのフィルタリング条件でサポートする。

  FTP（PORT、Passive、EPSV）、Windows Media Player、RealAudio、CUSeeMe、RTSP や SIP/SDP を利用したアプリケーション

  また、一つのフィルタリング条件では表現できない以下のサービスは、ステートフルインスペクション機能を利用できない。

  －あるサービスに呼応して、サービスの要求元に対して別のサービス用のコネクションを確立するサービス（例：SMTP に対する Authentication Service など）。

  －NFS 系のマウントやロックなどの RPC ベースのサービス。

3.1.4 アドレス変換機能

アドレス変換機能では、本装置にて接続された異なるネットワーク間で送受信されるデータのアドレス情報を変換して中継する機能を提供する。

本機能により、内部ネットワークの IP アドレス情報を外部ネットワークから保護する。

接続するサービスに対するフィルタリング条件で、「アドレス変換」動作が設定されている場合は、アドレス変換処理が行われる。

(1) アドレス変換

送受信される IP パケットの IP アドレス情報、または、ポート番号を変換し、以下の変換方式を提供する。

- NAT 方式
  中継するパケットの送信元 IP アドレス、または、送信先 IP アドレスを変換する。
  一般に、NAT（Network Address Transfer）と呼ばれる方式であり、本装置では、変換前後の IP アドレスを、事前に１対１の静的な対応をつけて定義しておく必要がある。
  本方式では、変換する IP アドレスによって、「送信元 NAT」と「送信先 NAT」の２つの方法があり、「送信元 NAT」では、送信元 IP アドレスを変換し、「送信先 NAT」では、送信先の IP アドレスを変換する。

- 送信元 NAPT（IP マスカレード方式）
  中継するパケットの送信元 IP アドレスおよび送信元ポート番号を変換する。
  一般に、送信元 NAPT、または IP マスカレード方式 と呼ばれる方式であり、変換前後の IP アドレスの対応付けは不要であるが、中継後の IP アドレスはパケットを送信するインタフェースの IP アドレスに変換されため、送信先ホストでは、送信元ホストを一意に識別することはできない。

さらに、アドレス変換機能では、内部ネットワークの IP アドレスを、外部ネットワークで利用する IP アドレスに変換する。外部ネットワークの利用者に公開される内部ネットワークの実 IP アドレスに対応付ける変換後の IP アドレスを「仮想アドレス」といい、以下の用途で使用する。

- 外部ネットワークから内部ネットワークへの通信
  外部ネットワークに公開する内部ネットワーク上の特定ホストに割り当てる IP アドレスであり、外部ネットワーク上の利用者から、送信先 NAT での「送信先 IP アドレス」として見える。外部ネットワークから内部ネットワーク上のホストにアクセスする場合、設定した仮想アドレス宛てのパケットは、内部ネットワーク上の実 IP アドレスに変換される。

- 内部ネットワークから外部ネットワークへの通信
  外部ネットワークと通信するための内部ネットワーク上のホストに割り当てる IP アドレスであり、外部ネットワーク上の利用者からは、送信元 NAT、送信元 NAPT での「送信元 IP アドレス」として見える。内部ネットワーク上のホストから外部ネットワークにアクセスする場合、設定した仮想アドレスは、IP パケットの送信元アドレスに変換される。

なお、仮想アドレスとして設定する IP アドレスは、外部ネットワーク上で通信可能な IP アドレスである必要があるため、グローバルアドレスを使用する必要がある。

また、アドレス変換機能は、アクセス制御機能と同様のトラフィックに対して、適用できる（「3.1.3　アクセス制御」を参照）。

(2)　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。

3.1.5 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。

(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出来ないので、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。

(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
プロトコル	RFC2401,2403,2405,2406準拠	独自（Safegate方式）
暗号アルゴリズム	DES-CBC（56bit）, ES-CBC（168bit）	DES-CBC（56bit）
パケット認証	HMAC-MD5, HMAC-SHA1	HMAC-MD5
通信パケット	トンネルモードの認証付ESP	IP in UDP（元パケットをIPからUDP/IPでカプセル化）
鍵配布	マニュアル、IKE（自動鍵交換）	マニュアル
鍵更新	マニュアル、IKE（自動鍵交換）	自動更新（更新間隔固定）
相手暗号GW数	最大1284	最大128
相手暗号GW毎の条件数	最大4条件	最大4条件

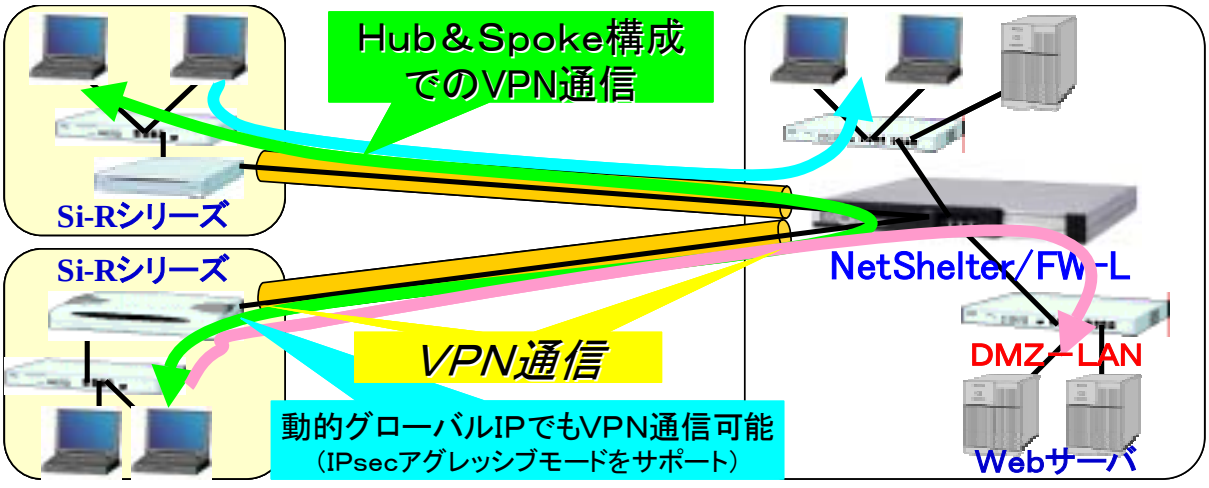
(4)　IPsec アグレッシブモード

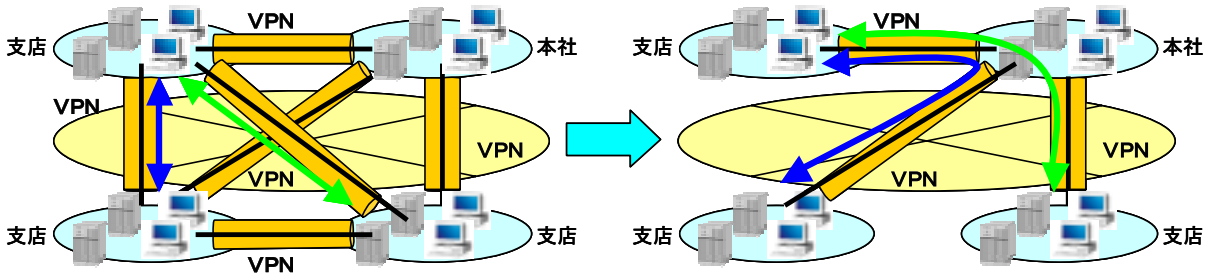
Si-R シリーズルータと組合せて、フレッツサービスなどの動的な IP 取得契約においても VPN 通信が可能になる。発信側を識別する方法では、装置固定の ID を使用するため、発信側の IP アドレスが不定でも使用可能である。本装置には、固定 IP アドレスが必要となる。

(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－３参照）。

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－３　**Hub & Spoke 接続機能の利用概念**

3.1.6　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。同時に接続できる Safegate client は最大 128 台まであり、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

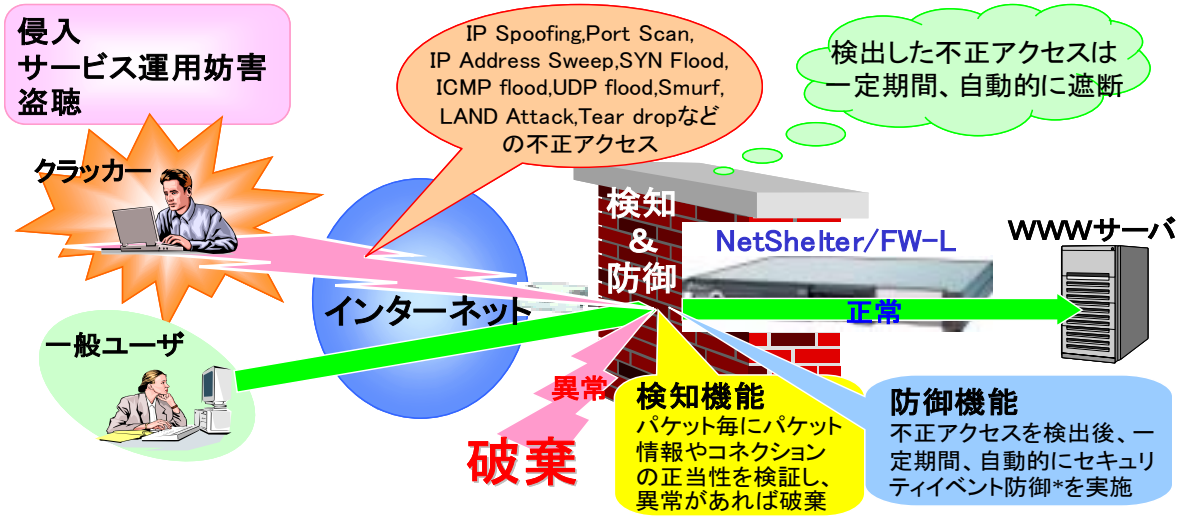
ローカル認証とリモート認証のどちらか一方の方式を選択することができる。

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 128 ユーザ、同時接続数は最大 128 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。

3.1.7　不正アクセスの検知・防御機能

不正アクセスに対する検知と防御機能を提供する（図－４参照）。



図－４　攻撃防御機能の概念

(1)　不正アクセスとは

一般に、不正アクセスの方法は、大きく以下のように分類することができる。

- ターゲット探索
  不正アクセスの対象となるターゲットに関するあらゆる情報が収集される。
  収集される情報には、ネットワーク情報（ドメイン名、IP アドレス）などがある。

- ターゲット情報の取得
  不正アクセスの対象となるターゲットが絞り込まれると、ターゲットに関する情報が収集される。収集情報は、OS 種別や稼動中サービス（ポート番号）など。

- 攻撃
  ターゲットとなる対象ホストに対する不正アクセス（攻撃）が行われる。
  攻撃方法には、以下のようなものがある。
  －侵入：パスワードクラックやアプリケーションのセキュリティホール（バッファオーバフローなど）を攻撃し、ターゲットシステムに侵入する。侵入の結果、システムの破壊や改ざん、運用妨害などが簡単に行えるようになる。
  －サービス運用妨害（DoS：Denial of Service）
  ターゲットへの侵入をともなわずに、ターゲットが提供しているサービスの運用を妨害する。ターゲット上で実行されている TCP/IP 実装やアプリケーションなどを攻撃し、ターゲットが提供しているサービスの運用を妨害する。
  －盗聴：ネットワークで送受信されるデータを盗聴し、機密データが漏洩する。

(2) 不正アクセスの検知

前述のような不正アクセスに対し、パケットおよびコネクションの監視から検知を行う。

- パケット監視機能
  それぞれのパケットごとに、パケット情報の正当性を検証。
- コネクション監視機能
  あるコネクション上で送受信されるパケットを監視し、当該コネクションの正当性を検証。

(3) 不正アクセスの通知

不正アクセスとして、疑わしいアクセスや代表的な DoS/DDoS 攻撃を検出し、セキュリティアラートとして管理者に通知する。不正アクセスとして、以下の攻撃を検知する。

不正 IP パケット、不正 TCP パケット、不正 UDP パケット、不正 ICMP パケット、不正チェクサムパケット、パケットシーケンス検証、FTP コマンド検証、コネクション数の制御、ポートスキャン、SYN Flood Attack、UDP Flood attack、ICMP Flood attack、IP Spoofing attack、Too Many IP Fragment attack、Very Small IP attack 、LAND attack、UDP Bomb attack 、Smurf attack 、Tear Drop attack、FTP Bounce attack など

(4) 不正アクセスの防御

異常パケットや異常通信を検出した場合、それ以降の同様な攻撃を未然に防止するため、監視機能と防御機能を行う。

監視機能では、疑わしき不正アクセスを検知後、アクセス監視を行い、不正アクセスと判断すると、以下の制御を自動的に有効とし、以降の不正アクセスを未然に防止する。

- ブラックサービス制御
  本制御は、ブラックリスト制御から起動され、特定サーバへのアクセス集中のイベントが発生した場合、それ以降も当該送信先へセキュリティアタックが仕掛けられる可能性があると判断し、一定期間、同一の送信先 IP アドレス、送信先ポートへのパケットを破棄する。
  不正アクセスを仕掛けられていると判断した送信先 IP アドレスと送信先ポートのリストを「ブラックサービスリスト」という。
- ブラックリスト制御
  本制御は、不正なアクセスと判断した送信元 IP アドレスからのパケットは、それ以降も攻撃が仕掛けられる可能性があると判断し、一定期間、同一の送信元 IP アドレスからのパケットを破棄する。
  不正アクセスを仕掛けていると判断した送信元 IP アドレスのリストを「ブラックリスト」という。
- ルール当たりのリミッタ制御
  １ルール当たりのコネクション数の過負荷状態を検出した場合に起動される。
  本制御では、コネクション数過負荷状態からのリカバリを図るため、１ルール当たりの最大コネクション数を超えるコネクション確立要求が発生した場合に起動され、リミッタ制御を解除するコネクション数になるまで、コネクション確立要求パケットを破棄する。
  リミッタ制御が適用された送信先サーバを保護するため、ブラックリスト制御とブラックサービス制御も同時に起動する。
- 単位時間当たりのリミッタ制御
  単位時間当たりのコネクション数の過負荷状態を検出した場合に起動される。

本制御では、コネクション数の急激な過負荷状態への遷移を防止するため、単位時間内に最大確立コネクション数を超えるコネクション確立要求が発生した場合に起動され、当該コネクション確立要求パケットを破棄する。リミッタ制御が適用された送信先サーバを保護するため、ブラックリスト制御とブラックサービス制御も同時に起動する。

また、ブラックサービス制御、および、ブラックリスト制御の対象外とするサービス（送信先 IP アドレスとサービスの組み合わせ）や送信元 IP アドレスをブラックサービス対象外エントリ、および、ブラックアドレス対象外エントリに設定することにより、動的なリストへの追加が除外される。なお、ブラックサービス対象外エントリ一覧、および、ブラックアドレス対象外エントリ一覧の最大エントリ数は、256 である。

(5) 強制ブロック機能

ネットワークの稼動状況を監視し、動的にフィルタリング条件の追加・解除が必要となった場合に、管理者は以下のフィルタリング条件を追加・解除することができる。

- 送信元 IP アドレス
- サービス（送信先 IP アドレス、送信先ポート番号）

強制ブロックの追加で、動作は「破棄（Block）」、ログ採取は「ログ採取する」となる。
本機能で追加される動的フィルタリング条件が、設定されているすべてのフィルタリング条件より優先される。

3.1.8 フィルタリング条件検証機能

本機能は、指定されたフィルタリング条件を対象に、指定されたデータを擬似的に生成し、どのフィルタリング条件にヒットするかをシミュレートする機能を提供する。本機能を利用して、環境設定情報の正当性の事前検証や当該データがヒットしているフィルタリング条件を具体的に確認ができ、効率的なトラブルなどの解析ができる。なお、擬似パケットに対するファイアウォール機能の動作は行わないし、ネットワーク上にも送出しない。
検証は、擬似パケットを動作しているファイアウォール機能へ入力し、入力された擬似パケットに対して送受信されているフィルタリング条件を検索して行い、検索の結果、ヒットした有効なフィルタリング条件の情報を応答する。なお、「フィルタリング条件の検証」設定で、特定パケット検証、または、一括検証を選択し、必要な情報を設定後に実行される。検証結果には、擬似パケット情報とヒットしたフィルタリング条件の内容が表示され、予期せぬフィルタリングルールでヒットした場合は、フィルタリングルールの設定が不適切なことを示している。

- 特定パケット検証
  入力したデータがどのフィルタリング条件にヒットするかを検証する。管理者は、画面上から生成する擬似 IP パケットの情報を設定する。なお、無効なフィルタリング条件にヒットしても、有効なフィルタリング条件にヒットするまで検索は継続される。
- 一括検証
  すべてのフィルタリング条件から、それぞれのフィルタリング条件にあったデータを自動作成し、そのフィルタリング条件にヒットするか否かを検証する。なお、無効なフィルタリング条件は検索対象に含めない。

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、URL フィルタリング条件に直接設定する。本機能を利用する場合、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。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。ロギング情報は、URL フィルタログで表示することができる。

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。

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

DHCP サーバを起動する場合は、DHCP 基本情報の基本設定で『DHCP サーバを使用する』を選択し、設定終了後に環境定義情報を反映させる。停止する場合は、DHCP 基本情報の基本設定で『DHCP サーバを使用する』を無効にし、設定終了後に環境定義情報を反映させる。

3.3 運用支援機能

3.3.1 ロギング機能

ロギング機能は、ファイアウォール機能を経由した通信状況を、ログファイルに記録する。

表　ファイアウォール機能のサービスとログ情報

ログ情報	説明
コネクションログ	IPパケットフィルタリング機能の処理結果に関する情報。 すべての処理（PASS、BLOCK、REJECT、SNAT、DNAT、SNAPT、ENC、IPSEC、IKE）のコネクション情報が記録。
アラートログ	警告イベント、セキュリティアラート情報。
IPsec暗号エラーログ	IPsec暗号通信時に発生したエラー情報。
IKE通信エラーログ	IKE通信時に発生したエラー情報。
独自方式暗号エラーログ	独自暗号通信時に発生したエラー情報。
認証ログ	Safegate client連携、Safegate集中管理連携を利用した場合の認証処理情報。

ログ情報が格納されるログファイル容量は、通信トラフィック量に応じて可変である。

本装置に格納できるログ容量に制約があるため、すべてのログ情報は規定された最大容量の範囲内で最新のログ情報を管理する。

表　ログ情報の容量

ログ情報	説明
コネクションログ／アラートログ	１ファイルサイズは、16Mbyte。 コネクションログ、アラートログ合わせて最大4ファイルまで保持。
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	１ファイルサイズは、1Mbyte。 最大3ファイルまで、当日のファイルは最大2ファイルまで保持。

ログ情報の保存には、本装置への保存と他システムへの保存の方法を提供し、コンソール端末上でログ情報を解析する機能を提供する。

表　ログ情報の保存方法

保存方法	説明
装置保存	本装置にだけログ情報を保存。本装置に格納できる最大容量は、メモリ容量に制約され、本装置の電源断にて、格納されていたログ情報は消失。
ログサーバ保存	採取したログ情報、フィルタリング条件を、ログサーバに保存。ログサーバに格納できる容量の制約はなく、本装置の電源断にて、格納されていたログ情報は消失しない。ログサーバへの格納結果は、イベント情報として通知。 ログサーバに保存されたログ情報は、Webブラウザ画面から解析が可能。

Web ブラウザのログ表示機能では、以下の操作でログ解析が実行できる。

表　Webブラウザのログ表示機能

表示機能	説明
ログ情報表示	Webブラウザから、ログ情報を参照。Webブラウザは、装置保存の場合は本装置へ、ログサーバ保存の場合はログサーバへ、接続する。
統計情報表示	Webブラウザから、統計情報を参照。
CSV出力	ログ情報の表示結果を、テキスト形式（CSV形式）に出力。

3.3.2　イベント監視機能

本装置が稼動中に発生したイベント情報を監視する。

- エラーイベント（ERROR）
  本装置の正常動作を阻害するイベント（リトライ不能エラー）であり、本装置の正常動作を保持できなくなったイベントを監視する。
  イベントには、「システムイベント」と「その他」がある。

- セキュリティイベント（ALERT）
  不正アクセスに関するセキュリティアラートの検出に伴って発生するイベントであり、不正アクセスの兆候を監視し、必要な措置を実施する。
  イベントには「異常パケット」と「異常通信」がある。

- 警告イベント（WARN）
  ファイアウォール機能が動作する上で必要なリソース不足等の兆候（リトライ可能エラー）や暗号通信機能の破棄パケットの検出に伴って発生するイベントであり、ファイアウォール機能の正常動作を維持するために必要な措置を実施する。
  イベントには、「セキュリティイベント」、「システムイベント」、「その他」がある。

- 情報イベント（INFO）
  本装置の動作状態に伴って発生するイベントであり、管理者が意図した通りに本装置が動作しているか否かを判断することができる。
  イベントには、「装置起動終了」、「機能起動終了」、「接続切断」、「システム操作」、「動作環境操作」、「その他」がある。

検出したイベントに対する処置（アクション）は、「管理者通知」と「無視」のいずれかを選択することができる。

イベント情報には、本装置の稼動状況や不正アクセス状況など、本装置の運用管理を行う上で有用な情報が保持されており、本装置で検出したイベント情報は、装置に保存する方法とログサーバに保存する方法があり、コンソール端末上でイベント情報を解析する機能も提供する。

保存したイベント情報の解析は、Web ブラウザのイベント表示機能を利用して行う。

イベント表示機能では、Web ブラウザから、装置格納の場合は本装置へ、ログサーバ格納の場合はログサーバへ、接続して、イベント情報を参照する。

3.3.3 イベント通知機能

イベントアクションで、「管理者通知」を選択したイベントは、以下のいずれかの方法で管理者に通知する。以下に、検出するイベントの種別を示す。

表　通知イベントの種別

種別	説明
異常	異常イベントを通知。
セキュリティ	異常、セキュリティイベントを通知。
警告	異常、警告イベントを通知。
情報	異常、警告、情報イベントを通知。

- システムログ（syslog）通知
  本装置で検出したイベントは、システムログに通知される。管理者は、システムログを解析することで、本装置で検出したイベントを参照でき、どのイベントをシステムログに通知するかを設定できる。下表のとおり、通知情報を編集できる。

表　システムログ通知情報の編集内容

分類	説明	デフォルト
システム	イベントを検出したシステム情報。	かんたん設定「基本設定」の「システム名」
送信元IPアドレス	syslogサーバに通知する場合の送信元IPアドレスを設定。設定されていない場合、syslogサーバが接続されているインタフェースのIPアドレスを使用。	syslogサーバが接続されているインタフェースのIPアドレス
機能	イベントを検出した機能情報。変更できない。 syslogの「ident」に相当する。	変更不可
検出分類	イベントを検出した分類情報。 syslogの「facility」に相当する。	Daemon

システムログは、ログ情報と同様な保存方法を選択することができる。

表　システムログの保存方法

保存方法	説明
装置格納	本装置にだけシステムログを格納。本装置に格納できる最大容量はフラシュメモリ容量に制約され、容量分の最新システムログしか格納されない。 本装置の電源断にて、格納されていたシステムログは消失。
ログサーバ保存	採取したシステムログを、ログサーバに転送し、保存。格納できる最大容量の制約はなく、本装置の電源断にて、格納されていたシステムログは消失しない。 なお、ログサーバへの格納結果は、イベント情報で通知。
syslogサーバ通知	採取したシステムログを、syslogサーバに通知。

システムログは、以下のいずれかの方法で解析することができる。

表　システムログの解析方法

解析方法	説明
Webブラウザ	Webブラウザ経由の場合、本装置に接続したWebブラウザから、システムログが格納されている場所を自動的に認識し、格納されているシステムログをWeb ブラウザ上に表示。システムログの保存で、装置格納、または、ログサーバ保存を選択した場合に利用。
syslogサーバ機能	syslogサーバの表示機能を利用して参照。

- SNMP マネージャ（SNMP）通知
  発生したイベントを、SNMP プロトコルの trap オペレーションを使用して、SNMP マネージャ経由で管理者に通知する場合は、SNMP マネージャの通知を行うよう動作環境を設定し、検出したイベントのうち、どのイベントを SNMP マネージャに通知するかを設定する。以下のとおり、SNMP 通知情報を編集することができる。

表　SNMP通知情報の編集内容

分類	説明	デフォルト
管理者名	管理者名を設定。	設定なし
設置場所	本装置の設置場所を設定。	設定なし
SNMPコミュニティ名	SNMPコミュニティ名を設定。	Public
送信元IPアドレス	SNMPマネージャに通知する場合の送信元IPアドレスを設定。設定されていない場合、SNMPマネージャが接続されているインタフェースのIPアドレスを使用。	SNMPマネージャが接続されているインタフェースのIPアドレス

- メール（SMTP）通知
  発生したイベントを、メール送信機能を利用して、メールサーバ経由で管理者に通知する。

本機能を利用する場合は、メール通知を行えるよう動作環境を設定する必要がある。
検出したイベントのうち、どのイベントをメール通知するかを設定する。
デフォルトは、「情報」（すべての異常、警告、情報イベントの通知）である。選択されていない種別のイベントは、イベントを検出しても通知されない。
下表のように、メール通知する情報を編集することができる。

表　SNMP通知情報の編集内容

分類	説明	デフォルト
メール表題	メール表題（Subject）に設定する情報を設定する。	NetShelter Event
送信先メールアドレス	メールを送信する送信先メールアドレスを設定する。	設定なし
送信元メールアドレス	送信メールの送信元メールアドレスを設定する。	設定なし
暗号化	イベント情報を暗号化することができる。	暗号化なし
送信元IPアドレス	メールサーバに通知する場合の送信元IPアドレスを設定する。設定されていない場合、メールサーバが接続されているインタフェースのIPアドレスを使用する。	メールサーバが接続されているインタフェースのIPアドレス

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り、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。

- 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、トラップ情報（アラート情報）や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。
  SNMPマネージャとして動作する製品は、NetEyeManager、および、SystemWalkerがある。

- 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

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 ・手動登録	・手動登録
	監視内容	・システム起動有無 ・ネットワークトラフィック －systemグループ －interfacesグループ －address translationグループ －ipグループ －tcpグループ －udpグループ －icmpグループ －snmpグループ	・システム稼働有無 ・稼働機能種別 ・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

3.3.5　稼動監視機能

本装置の稼動状況を監視することができる。以下の情報を参照可能。

- システム負荷情報
- ネットワーク負荷状況
- トラフィック状況
- コネクション状況
- サービス状況

これらの情報は、本装置にのみ格納される。所定時間（1 時間／2 時間／4 時間／8 時間／1 日／1 週間／1 ヶ月／1 年）の稼動履歴グラフを Web ブラウザから参照できる。

3.3.6　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。

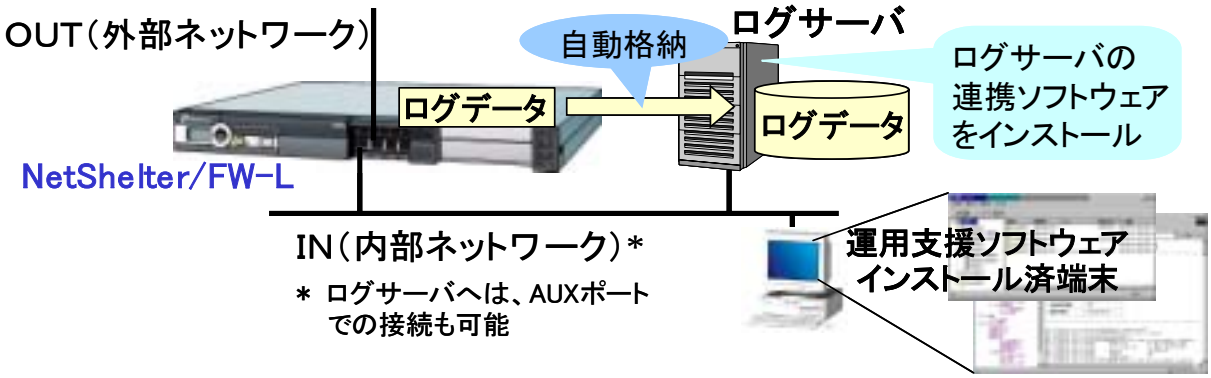
- 手動設定
  手動設定では、設定したい時刻を手動で設定する。
- 自動同期
  自動同期では、上位タイムサーバに時刻を問合せ、タイムサーバと本装置の時刻を一致させ、同期をとる機能をサポートする。

(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。

3.3.7　ログサーバ

本装置は、ディスクレスであり、採取・検出したログ情報やイベント情報を保存できる容量には制約があるため、ログデータを外部装置に格納することで、この制約を解除する。
このログデータを格納する外部装置をログサーバという（図－５参照）。



図－５　ログサーバの利用概念

「ログサーバ」との連携環境を設定することで、本装置のハード制約に縛られずに、これまでと同様なログ、イベント監視運用が可能となり、以下の情報を格納することができる。

- ログ情報
  コネクションログ、認証ログ、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、URL フィルタログ
- syslog 情報
  エラー、アラート、警告、情報
- フィルタリング条件
  ログ情報には、フィルタリングルールの優先順位が格納されており、ログ情報を解析する場合、当該ログ情報が出力された時点のフィルタリング条件と合わせて解析することで、確実なログ解析が可能となる。

ログサーバへ転送するタイミングを示す。

表　ログ情報の転送タイミング

分類	項目	転送タイミング
ログ情報	コネクションログ	・設定したログレコード数を超えた場合 ・フィルタリング条件が更新された場合
	syslog、認証ログ、マニュアルIPsecエラーログ、IKEIPsecエラーログ、独自暗号エラーログ、URLフィルタログ	・毎日1回定時 ・ログファイルサイズを超えた場合
イベント情報		・ログファイルサイズを超えた場合
フィルタリング条件		・フィルタリング条件が更新された場合

ログサーバ上では、装置ごとにアップロードを許容できる最大格納ファイル数により、ディスク資源を管理することが可能である。
最大格納ファイル数を超えてアップロードされた場合は、当該装置の最も古いログファイルから自動的に削除される。デフォルトは、1000 ファイルである。たとえば、5 台の本装置と接続する場合には、全体で 5000（1000×5 台）ファイルの格納が可能である。

ログサーバへの最大格納容量は、装置ごとの最大格納ファイル数をもとに見積もる。
それぞれのログ種別について、一つのログファイル容量の最大値を見積もり、最大格納ファイル数と装置台数を掛け合わせることで、ログサーバ上で必要なディスク容量が算出できる。

（一つのログファイル容量の最大値）×（最大格納ファイル数）×（装置台数）

たとえば、以下の場合であれば、ログサーバでは 80Gbyte のディスク容量が必要となる。
－ログファイル容量の最大値：16Mbyte
－最大格納ファイル：1000
－本装置：5 台

また、ログサーバは、Windows 版と Linux 版を提供する。
ログサーバを動作させるために必要なシステム構成を示す。

表　ログサーバのシステム構成

項目	条件
パソコン本体	下記OSが動作するPCでCD-ROMドライブとLANコントローラが必要
CPU	PentiumIII450MHz相当以上
実装メモリ	256MB以上
ハードディスクの空き容量	プログラム：55Mbyte以上 登録するロギング情報ファイルのサイズと保存期間に依存する。
対象OS	・WindowsのIIS4.0が動作するOS Windows 2000 Server(Service Pack2以上)を推奨 Windows Server 2003 ・RedHat Linux 7.2以降
Webサーバ	Microsoft Internet Information Server4.0以降を推奨 Apache 1.3.x/Apache 2.x
暗号ソフト（別売り）	SecureBOX V1.0L10以降（ログデータの暗号化を行う場合） お問い合わせ先：株式会社富士通北陸システムズ

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。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。

(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。

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-Lハードウェア仕様

LANインタフェース	LANポート	10/100BASE-T×3
	保守／二重化	10/100BASE-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
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）		422mm×380mm×44mm（ゴム足、突起物を除いて）
重量		9.0Kg（レールを含む）
消費電力		80 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－６参照）。

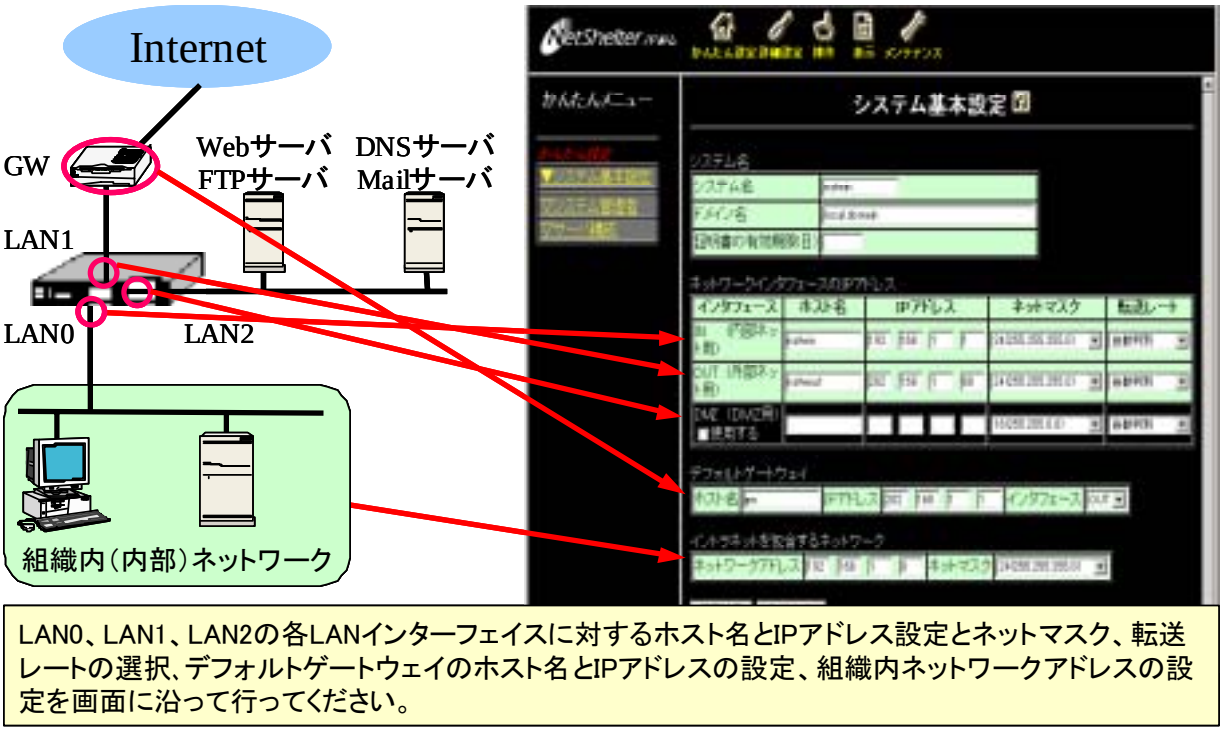
図－６　**NetShelter/FW-L 装置の前面**

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－７参照)。



図－７　NetShelter/FW-L の簡易設定メニュー画面

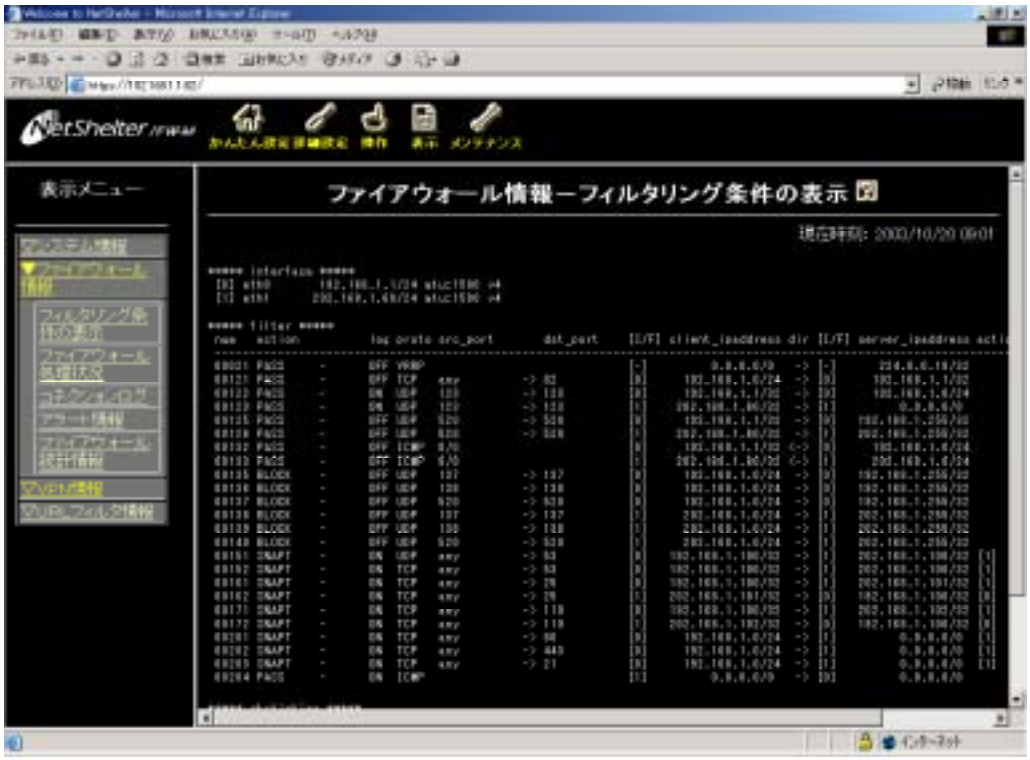
かんたん設定は、本装置に対する装置情報と公開サーバの情報を設定するだけで、基本的な運用に入れるようになる。

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－８参照)。

－ 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

パケットフィルタリング機能の統計情報



図－８　**NetShelter/FW-L 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

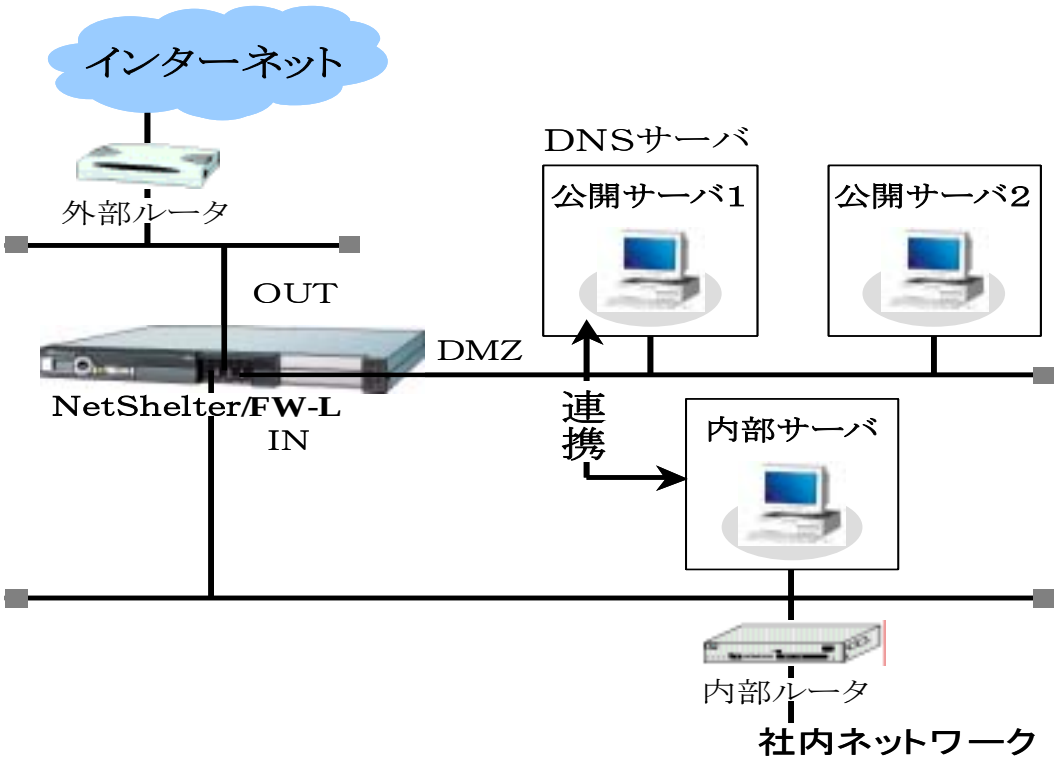
以下に、本装置の代表的な設置パターンについて説明する。

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－９参照）。

- 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



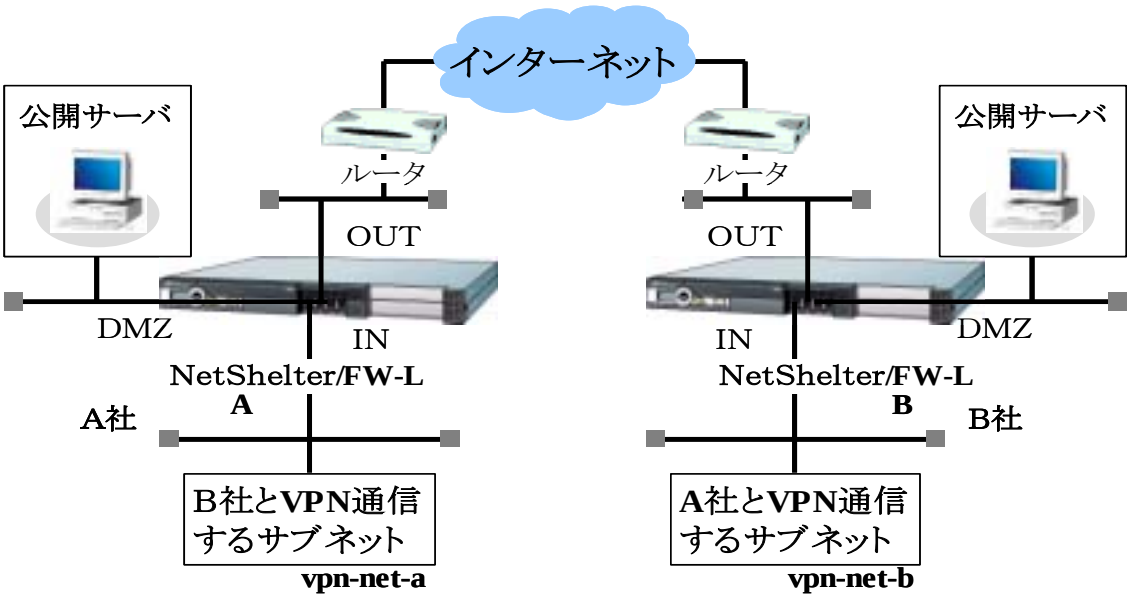
図－９　**DMZ に公開サーバを設置した形態**

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－１０参照）。

- 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。

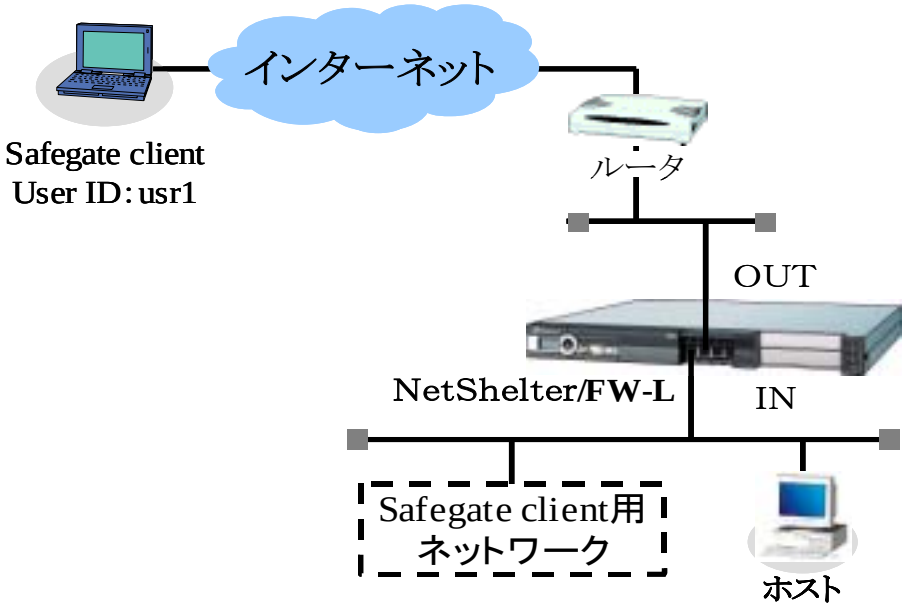


図－１０　VPN（IKE を使った Ipsec 通信）形態

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－１１参照）。

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