

# ファイアウォール専用装置 NetShelter/FW-L および NetShelter/FW-M

Dedicated FireWall Device NetShelter/FW-L and NetShelter/FW-M

青木 弘 \*  
Hiroshi Aoki

向井哲也 \*\*  
Tetsuya Mukai

中村美樹 \*\*  
Yoshiki Nakamura

多幡明人 \*\*  
Akihito Tabata

\* プロダクト本部 ProDes 事業部 第三技術部

\*\* プロダクト本部 アプライアンス事業部 第一開発部

NetShelter/FW シリーズは、ネットワークセキュリティの構築を簡単に、しかも低コストで実現できる富士通のファイアウォール専用装置として、2000年にシリーズ最初の装置を出荷後、一定の新市場を開拓してきた。NetShelter/FW-L および NetShelter/FW-M は、装置信頼度の向上を目的としてディスクレスを実現したシリーズ最初の装置である。また、不正アクセス検知および防御機能強化や、VPN 機能強化など従来機種にない様々な取り組みを実施した製品である。本製品の技術的特長と、今後の展開について紹介する。

The NetShelter/FW series was introduced in 2000 as a dedicated firewall device which provides an inexpensive and simple network security solution from Fujitsu, and has accomplished a new stable market. The NetShelter/FW-L and NetShelter/FW-M are the first diskless devices aiming at improvement of device reliability. The products are the result of various unprecedented challenges for the series such as reinforcement of illegal access detection, defense facilities, and VPN facilities. This chapter introduces the product's technical features and development.

## 1 まえがき

NetShelter/FW シリーズは、2000年2月より販売を開始し、ファイアウォール専用用途のセキュリティ装置として、数多くの導入実績を持つ製品である<sup>1), 2)</sup>。今回、NetShelter/FW-L (以降 FW-L と略す) および、NetShelter/FW-M (以降 FW-M と略す) の追加によるラインナップ拡充に当たり、機能向上およびセキュリティ強化と共に、更なる装置信頼性の向上を一つのテーマとして取り組んだ。

図-1にFW-L, FW-Mの概観を示す。

## 2 開発の狙いと技術的課題

FW-L および FW-M 以前の既出荷装置においては、ハードディスクという駆動系を内蔵しており、ハードトラブルの大半がハードディスクと言う実情があった。

NetShelter においては、内蔵ハードディスクはファームウェアの格納先であるばかりか、ファイアウォール

(1) FW-L



(2) FW-M



図 1 装置外観  
( Fig.1-Device appearance )

にとって重要なログ情報の格納先でもあり、重要な役割を担っている。しかし、唯一の駆動系であるハードディスクを廃することが装置稼動信頼度の更なる向上となることは確かであり、FW-L および FW-M 開発において、ハードディスクレス化とそれに伴う幾つかのテーマに取り組んだ。

### 3 ディスクレス

#### 3.1 ハードウェアとしての取り組み

シリーズ最初のディスクレス装置として、ハードウェア面での取り組みについて紹介する。

ハードウェアとしてディスクレスとすると、新規開発装置の FW-L としてはスペースメリットが発生し、そのメリットを最大限に活かすことが取り組みとなる。従来製品をベースに一部変更による開発を目指した FW-M としては、従来製品に対していかに変更量を少なくして、効率よく開発するかが課題となった。

まず、新規開発した FW-L のメリットを活かした取り組みについて以下に述べる。ディスクレスとすると、以下のメリットが発生する。

##### (1) 省スペース、省発熱

ハードディスクを採用すると、3.5 インチディスクで 101.6 mm × 146.0 mm × 25.4 mm (幅, 奥行き, 高さ) の体積を持ち、さらに放熱を考慮した間隔として側面に 2.5 mm、底面に 2.5 mm が必要となるため、装置全体としては 106.6 mm × 146.0 mm × 27.9 mm の容量が失われる。

これは、3.5 インチハードディスクの短面を 1 U ラックマウントサイズ装置の正面と併せて実装した場合、25% を占める。また、1 U サイズとした場合、ディスク上にはほとんど何も重ねられないことを示しており、装置を小型化する上でネックとなっていた。今回 FW-L ではディスクに代わり、半導体記憶素子を使用したため、容積比で 98.8% の削減となった。

##### (2) 省電力

3.5 インチハードディスクは 12 V と 5 V 電源を持ち、その消費電力は最大で 9.4 W となる。一方、代替の半導体記憶素子では 0.2 W ですみ、9.2 W の電力を削減できる。この変更は、省電力化と共に、電源容量の削減に伴う電源ユニットの小型化を可能とし、結果として従来比で約 50% の設置容量を削減できた。

上記で述べた通り、ハードディスクレス化により、大幅にスペースを削減することが可能となり、その削減し

たスペースを有効活用することが課題となった。FW-L はラックマウントと平置き用の両用設置をセールスポイントとしているため、平置きした場合に設置面積を取らないように、従来装置とのデザインの互換を保ちながら、奥行きを短くすることを新たな課題とした。

図 - 2 に従来装置の内部レイアウトを、図 - 3 に上記課題を解決して新規開発した FW-L の内部レイアウトを示し、以降に、その設計の取り組みを説明する。

従来機種とデザインの共通化を図るために、正面パネルは既存機種と同一とした。正面パネルを既存機種と同一とすることにより、CD-ROM ドライブと LAN コネクタの位置が決定した。移動できるユニットは電源ユニットと PCI スロットとなるが、奥行きを短くすることが課題であるため、従来装置で正面から見て左奥に配

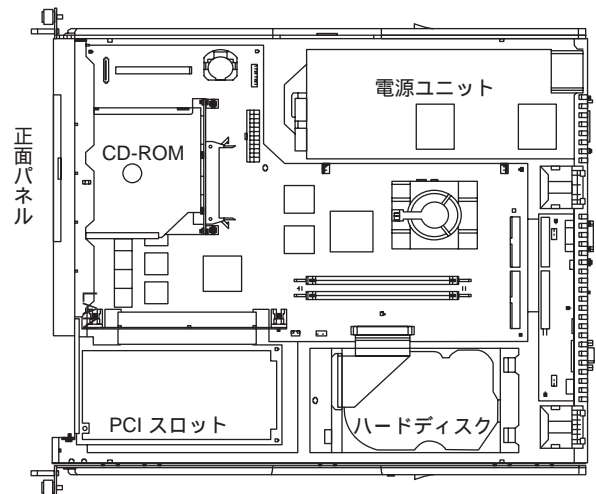


図 2 従来装置の内部レイアウト  
( Fig.2-Internal layout of the existing devices )

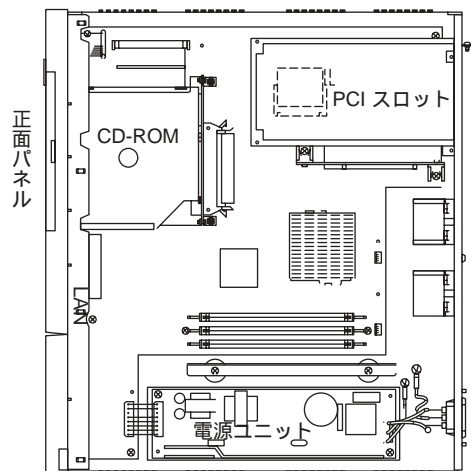


図 3 FW-L の内部レイアウト  
( Fig.3-Internal layout of FW-L )

置いていた電源ユニットを右奥に移し、右手前にあった PCI スロットを左奥に配置換えした。

このレイアウト変更により、従来機の奥行きが 498 mm であったものを、FW-L では 380 mm とし、従来機種比 24 %の短縮が図れた。

次に FW-M の設計取り組みについて、以下に述べる。

FW-M の設計課題は、新規開発の FW-L と平行開発する中で、いかに効率よく開発し、ハードディスクレス化を実現するかであった。そのために、従来装置をベースに、ハードディスクの取り付けスペースに合わせた大きさで、代替の半導体記憶素子を実装したアダプタカードを開発して、全体の開発工数を削減した。

図 - 4 に今回開発したアダプタカードを実装した FW-M の内部レイアウト図を示す。

従来装置のハードディスク設置場所に収まるように、ハードディスクの代替の半導体記憶素子を実装したアダプタカードを開発することにより、わずかな開発期間で新製品投入を果たすことができた。

### 3.2 ファームウェアとしての取り組み

装置信頼度の向上対策としてのディスクレス化に対して、これまで NetShelter シリーズが提供してきた顧客運用を犠牲にすることなく、また、これまで以上の「かんたん運用」に向けて、以下の対策を行った。

#### (1) ログサーバ機能の搭載

他社製品などにも見られるように、一般にディスクレス装置における稼動イベント監視機構は、採取した稼動イベントをログ情報と合わせて即座に外部 syslog サー

バに通知し、外部 syslog サーバ上で稼動イベントやログ情報を監視または、解析する方法を採っている。しかしながら、このような方法を採った場合、NetShelter シリーズのこれまでの顧客殿での稼動イベント監視やログ解析などの運用管理作業のシームレスな移行を阻害する恐れがある。

これへの対策として、図 - 5 に示すように稼動イベントやログ情報の格納庫としてのサーバ（外部 syslog サーバに相当）設置に加え、格納した情報を、これまでと同様な操作性で運用できるログサーバ機能を搭載し、既存顧客に対するアップグレード時の安心感を維持するようにした。さらに、通信プロトコルには http/https を採用し、ログサーバとの接続に柔軟性を持たせている。

これにより、NetShelter の運用管理形態は、従来までの顧客殿独自運用に加え、顧客殿以外のネットワーク上に設置されたログサーバでの稼動監視サービスやログ解析サービスなど、顧客密着型セキュリティ運用管理サービスの利用も可能となっている。

#### (2) 大量トラフィックへの対処

ネットワークトラフィックが増大の一途を辿るなか、ディスクレス化により、NetShelter 上で保持できる稼動イベントやログ情報の格納領域は最大 64 M バイトに制限されている。このような相反する実行環境のなかで、「不正なトラフィック情報を管理者に確実に通知する」といったセキュリティ運用を保証するため、稼動イベントやログ情報の採取機構を全面的に見直している。具体的には、採取するログ情報の絞込み、およびファームウェア内部でのセキュリティイベント検出機構の実装

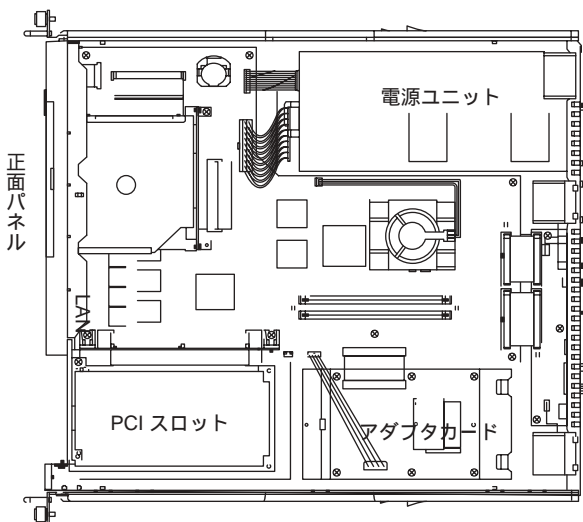


図 4 FW-M の内部レイアウト  
( Fig.4-Internal layout of FW-M )

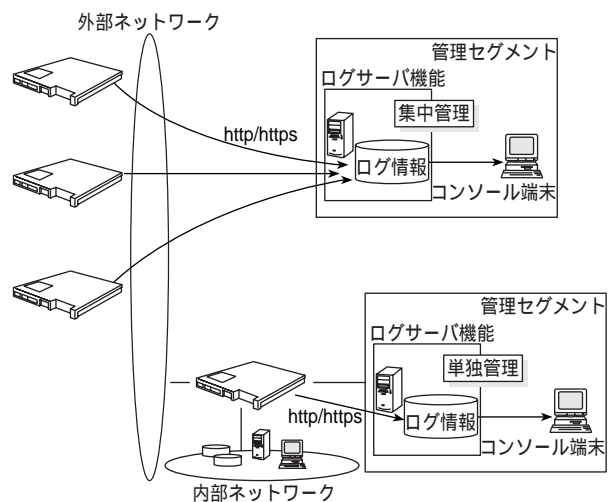


図 5 ログサーバ構成例  
( Fig.5-Structure example for the log server )

である。

これにより、ログ格納領域の削減（1 コネクションにつき約 600 バイト削減）を達成するとともに、不正なトラフィックを確実に管理者に通知できるようになっている。

## 4 二重化連携機能

一般にファイアウォール機器は、インターネットと社内ネットワークの境界に設置され、通常 24 時間稼動が前提となる。NetShelter では、ファイアウォール専用機器として、先に述べたようなハードウェアレベルでの高信頼性に加え、装置を二重化し冗長性を持たせることで、24 時間の連続稼動に十分耐えうる信頼性を確保している。

FW-M の二重化連携機能では、従来からの「簡単に導入」でき、「装置障害発生時にも短時間で復旧できる」という利点を引き継ぎ、さらなる「復旧処理の高速化」と「ネットワークの冗長化」を実現し、ネットワークシステム全体の信頼性向上を図った。

### 4.1 高速な異常検出と復旧

従来機種である NetShelter/FW-P の二重化連携機能では、装置の障害発生時からネットワーク復旧までに、約 1 分程度の時間がかかっていた。

FW-M では、この復旧時間を FW-M の TCP コネクション確立タイムデフォルト値である 30 秒以内を目標として、システムの見直しを行った。

二重化連携機能の復旧処理時間は、「障害検出時間」+「装置の切り替え起動時間」で決定される。

#### (1) 障害検出時間の短縮

NetShelter の障害検出方法は、2 台の装置間に等間隔で Keep-Alive パケットを送信し合う生存監視制御を行っている。運用系装置からのパケットが待機系装置に届かなかった場合、待機系装置は、運用系装置に異常が発生したと判断する。しかし、この Keep-Alive パケットの間隔をあまり短くすると、システム負荷等の影響により誤検出する可能性が高くなる。

FW-M では、生存監視制御のシステム内での処理優先度をできるだけ高くすることで、誤検出の可能性を低くしたまま、監視間隔の短縮を図った。

これにより、従来機種のデフォルト 30 秒を 5 秒にまで短縮することができた。

#### (2) 装置切替え起動時間の短縮

待機系装置は異常を検出すると、運用系装置から処理を引き継ぐため、ネットワーク制御の初期化と各サービスプロセスの起動を行う必要がある。

FW-M では、切り替え処理時に必要となる処理をあらかじめ実施しておき、切り替え処理時に実施する処理を削減するように改善を行った。

これにより、従来機種では約 30 秒かかっていた処理を 10 秒以内に完了することができるようになった。

以上のような改善により、FW-M の切り替え処理時間は約 15 秒で完了するようになり、NetShelter の二重化切り替え処理が発生した場合でも、アプリケーションには影響を与えず、ネットワークの復旧ができるようになった。

### 4.2 ネットワークの冗長化

本体装置の冗長化により、NetShelter 装置に異常が発生した場合でも、速やかな復旧が可能になったが、ネットワークシステム全体の信頼性向上を図るためには、ネットワーク自体を冗長化し、異常発生時には正常な経路を経由し通信を行えることが要求される。

FW-M では、この要求に応えるためにネットワークの冗長化を可能とする「経路監視機能」を新たにサポートした。

#### (1) 経路監視機能

経路監視機能は、NetShelter 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。監視ホストからのパケットが届かなくなった場合、ネットワークに異常が発生したものと判断し、システム管理者に異常発生を通知し、ネットワークの復旧処理を行う。

#### (2) ネットワークの二重化

FW-M では、運用系装置に接続されたネットワークを運用系ネットワーク、待機系装置に接続されたネットワークを待機系ネットワークとして使用し、通常は運用系ネットワークで処理を行う。

経路監視機能で、ネットワーク異常を検出した場合には、装置の二重化連携機能の切り替え処理を行い、待機系ネットワークへの切り替えを行う。図 - 6 に NetShelter の二重化連携の運用例を示す。

これらの処理により、ネットワークシステム自体を冗長化することが可能となり、システム全体の信頼性向上を図ることができるようになった。

## 5 不正アクセス検知と防御機能

TCP/IP レベルの不正アクセスから内部サーバを保護する不正アクセス検知機能、および検知した不正アクセスを契機に内部サーバを自動的に保護する不正アクセス防御機能について説明する。特に、不正アクセス防御機能における「ブラックサービス制御」は、他社製品には見られない特長を持っている。

### (1) Statefull なパケットフィルタ

エンドシステム間で送受信されるデータは、ネットワークの下位レベルでは「IP パケット」として認識され、しかも、その接続情報（各エンドシステムの IP アドレス、ポート番号の組合せ）は、個々のパケットごとに識別することができる。本装置のパケットフィルタは、エンドシステム間の通信開始から終了を捕捉しながら（Statefull）、通信可否を動的に判断している。

今回、この Statefull なパケットフィルタ機能を、不正アクセス検知及び不正アクセス防御の基盤機能とし

て実装し、不正アクセスと接続情報との相関関係をファームウェア内部で動的に管理できるようにしている。

### (2) 検知機能

TCP/UDP、IP レベルの個々の IP パケット情報に基づく不正アクセスの検知に加え、IP フィルタリングルール<sup>注1)</sup>や単位時間当たりの最大多重接続の過負荷など、トラフィックに関する不正アクセスについても検知することができる。これにより、より実運用上問題となる DoS (Denial of Service : サービス不能) 攻撃や DDoS (Distributed Denial of Service : 分散サービス妨害) 攻撃の検知も可能であり、単に個々の IP パケット情報に基づく他社のパケットフィルタエンジンとは一線を画している<sup>注2)</sup>。

### (3) 監視機能

不正アクセスを仕掛けてきた送信元 IP は、ファームウェア内部に自動的に記録され、誤操作やパケット異常などの偶発的な誤動作による突発性の不正なパケットを不正アクセスと判断しないよう、一定期間、疑わしき送信元 IP を監視している。最終的に疑わしき送信元 IP からのアクセスを不正アクセスと判断すると、防御機能が起動される。

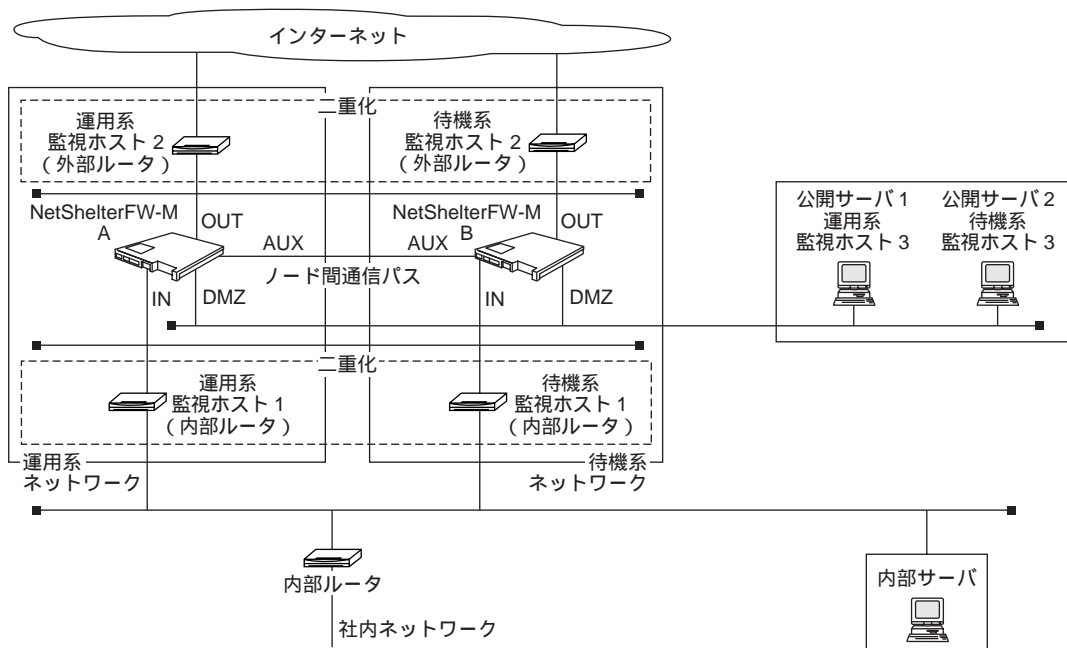


図 6 NetShelter 二重化連携の運用例  
( Fig.6-Example of linked duplex NetShelter operation )

注 1 ) 送信元アドレスや送信先アドレス、サービスなどの条件に応じて該当パケットの通過、破棄、加工を行う条件をフィルタルールと呼ぶ。  
注 2 ) TCP/UDP などプロトコル上不当なパケットは勿論、Spoofing などの成りすまし、Flood などの大量なパケット送信など 60 種類以上の攻撃に対応。

#### (4) 防御機能

不正アクセスと判断した場合、以下の防御機能が自動的に起動される。

- 1) ブラックサービス制御
- 2) ブラックリスト制御
- 3) リミッタ制御

ブラックサービス制御は、不正アクセスを仕掛けられた送信先 IP、送信先ポート（Web サーバなどのサービス）へのアクセスを一定期間遮断する。送信元 IP が不定となる DDoS 攻撃に対して特に有効である。

ブラックリスト制御は、不正アクセスを仕掛けた送信元 IP からのアクセスを一定期間遮断する。ブラックサービス制御が内部サーバを保護するのに対して、ブラックリスト制御は送信元 IP からのアクセスを遮断する。

リミッタ制御は、最大多重コネクション過負荷となったとき、ある一定の多重度に落ち着くまで、当該フィルタールール上のコネクション確立要求を破棄する。

これらの防御機能により、不正な送信元からの継続する攻撃を防御するとともに、安定稼動が必要な内部サーバを自動的に保護することができ、これまで以上の安心感を提案できたものと考えている。

## 6 VPN 通信機能

NetShelter シリーズでは、従来機種より VPN (Virtual Private Network) 通信機能をサポートしており、TCP/IP の IP 層で暗号化や認証を行う IPsec (IP Security) を利用して、暗号化された安全性の高い通信を提供してきた。

ブロードバンドの普及に伴い、安価なインターネット上に VPN 通信を行うインターネット VPN の利用がますます増加するものと予想される。

NetShelter では、インターネット環境での適応範囲を広げ、さまざまな利用シーンに導入可能なように、次のような改善を行っている。

#### (1) 高性能化

IPsec 通信は、一般に高度な暗号化処理を必要とするため、通常の通信に比べると処理負荷が増え性能が出にくいという特性がある。

NetShelter では、専用装置であるということのメリットを生かし、カーネルレベルでの優先度制御のチューニングやプログラムロジックの最適化を実施し、FW-L の場合、ソフトウェア処理でも 40 Mbps (3DES/MD5) を超える性能を実現した。また、暗号

化処理をハードウェアで処理する<sup>注3)</sup>ことにより、FW-L で 100 Mbps、FW-M で 150 Mbps を超える VPN 性能を実現した。

このことにより、企業の拠点での VPN 通信利用はもちろんのこと、企業のセンタ運用でも耐えうるだけの性能を確保した。

#### (2) VPN 環境構築を簡易化する Hub&Spoke

VPN 通信は、通信相手との間に暗号化された論理的な伝送路を作成し、伝送路上にデータを通すことで安全な通信を実現している。複数の拠点間で VPN 通信を行おうとすると、一般的には複数の拠点間同士で伝送路を作成するメッシュ型のネットワークが必要となる。この場合、拠点数×拠点数分の伝送路設定が必要となり、拠点数が増えるに従って設定する数が大きく増大する。また、それに伴い各拠点に配置する装置に対しても、複数の伝送路を作成できるようスペックの高い装置が要求される。

Hub&Spoke 機能は、1 つのセンタに複数の拠点から接続し、センタ側の装置が VPN 通信の中継を行うことで、複数の通信相手と VPN 通信を行う機能である (図 - 7 参照)。

各拠点に配置された装置からは、センタとの間に伝送路を設定するのみで、他拠点との通信が可能であるため、適切なスペックの装置を配置することができるほか、拠点の追加、削除などの変更においても、変更対象となる拠点とセンタ装置の設定変更のみで、従来必要であった各拠点の変更は不要となる。

本機能も、前記(1)項で述べた高速な VPN 通信により、十分運用に耐えうるサービスとなっている。

#### (3) アグレッシブモードによる動的 IP 割り当て

VPN 通信の伝送路を作成する場合、通信相手との間で、お互いの IP アドレスや使用するセキュリティプロトコルなどを定義した SA (Security Association) を設定する必要がある。設定された SA を元に暗号化のための鍵を作成し、通信相手と鍵交換を行い暗号通信を行う。

IP アドレスが不定な相手との間でこの SA を確立するためには、通信毎に IP アドレス以外の項目で通信相手と鍵交換を行う必要がある。

NetShelter では、従来から鍵交換を自動で行う IKE (Internet Key Exchange) 機構をサポートしているが、今回、IKE の処理モードの一つであるアグレ

注3) FW-L は「VPN オプションカード」使用、FW-M は標準実装。

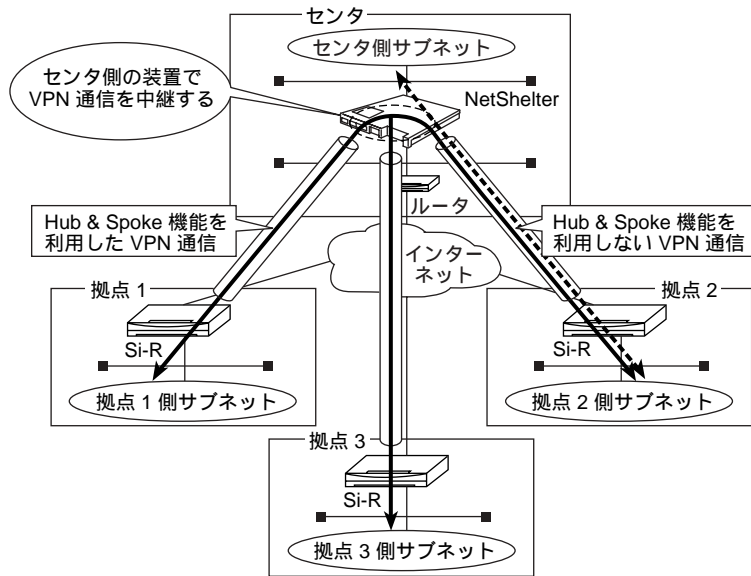


図 7 Hub & Spoke 機能を使った VPN 通信例  
( Fig.7-Example of VPN communications with Hub&Spoke functions )

ッシブモードを使用して、通信相手の IP アドレスが不定な場合でも鍵交換処理が可能となるような処理を追加した。

具体的には、通信相手を特定する ID を項目に追加し、この ID により相手を認証した後、実際に通信に使用する IP アドレスを特定して、VPN 通信を行う処理を行っている。この機能により、ブロードバンドやモバイル通信など、IP アドレスが接続毎に変化するような環境においても、VPN 通信を行えるようになった。

(4) 復旧処理を早める IKE セッション監視

IKE 方式の VPN 通信では、新規にデータが流れた時に、双方の装置で SA が確立され、その情報に従って暗号通信が行われる。そのため、相手側の装置でなんらかの異常が発生した場合、相手装置の SA は削除されてしまうが、自装置では SA を保持したままの状態となり、双方の装置間で SA の情報に矛盾が発生し、通信ができなくなってしまう。

また、自装置側の SA の削除のタイミングは、SA 有効期限が切れるまで無いため、その期間は新たな通信もできない状態になる。

このような状態を回避し、異常発生時にできるだけ早く復旧処理ができるように、IKE セッション監視機能をサポートした。

IKE セッション監視は、IKE 方式で接続された VPN 通信相手と定期的に通信を行い、VPN 通信路の生存監視を行う機能である。具体的には、相手装置から応答が

帰ってこない場合、異常が発生したと判断し、システム管理者にアラート通知すると共に、自装置の SA 情報を削除する。この機能により、相手装置が復旧した場合、速やかに VPN 通信を再開することが可能となった。

7 運用管理機能

情報セキュリティは、セキュリティ装置の導入がすべてではなく、導入したセキュリティ装置を運用して初めてその効果が得られるものと考えている。このような設計方針のもと、運用管理機能についても既存機種に比べ、大幅な機能強化を行っている。

以下に主な機能強化の概要を示す。

特に、フィルタリング条件の検証機能は、他社製品に見られない機能であり、設定したフィルタリング条件の検証作業を大幅に効率化することができる。

(1) フィルタリング条件の検証

設定したフィルタリング条件を擬似 IP パケットにより検証することができる。これまでフィルタリング条件の検証を行う場合、実際に構築したネットワーク環境で実際に IP パケットを送信し、現場でフィルタリング条件の正当性を検証する必要があった。このため、事前にフィルタリング条件を設計しても、その正当性は現地へ搬入してからでないと検証できず、また、運用変更/運用拡張の度に現場で検証する必要があった。

フィルタリング条件の検証機能により、上記問題は解

決される。さらに、ある拠点で一括してフィルタリング条件の設計～検証が可能となり、セキュリティ管理者、導入担当者、運用担当者すべての作業効率向上に大きく寄与できるものと考えている。

図 - 8 にフィルタリング条件検証画面例を示す。

なお、本機能は本製品と GUI 端末との構成でのみ実行できる。

(2) 稼働監視を容易とするグラフィカルな稼働履歴

本装置のシステム負荷、ネットワーク負荷、トラフィック状況、コネクション状況、サービス状況といった稼働状況を時系列に、しかも視覚的に参照することができる(参照する時間範囲は、直近 1 時間、2 時間、4 時間、8 時間、1 日、1 週間、1 ケ月、1 年から選択できる)。また、画面は 5 分ごとに自動的に最新状況に更新される。

これにより、負荷状況や定常状態、定常状態からの変動状況、及び変動タイミングなどを、短時間に、しかも直感的に確認することができる。また、異常が検出された場合でも、調査すべきトラフィックが発生した時刻は直ちに把握できるようになっている。

図 - 9 に直近 1 日のコネクション数の推移例を示す。



図 8 フィルタリング条件検証画面例  
( Fig.8-Example of the filtering condition monitor screen )

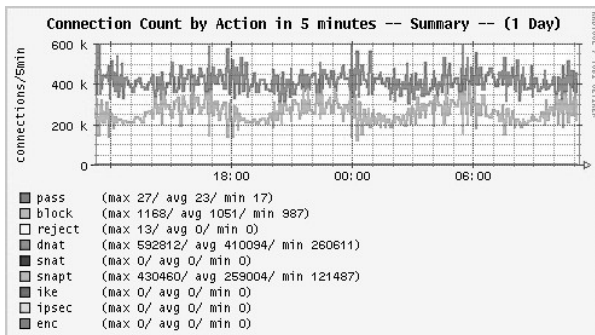


図 9 稼働履歴例 (直近 1 日のコネクション推移)  
( Fig.9-Example of an operation history ( previous 24 hours connection transition ) )

このように、特別なスキルはなくても稼働監視ができるため、運用管理者の負荷軽減ができるとともに、万一の異常事象についても調査対象を直ちに割り出せるため、運用管理工数についても大幅に削減できるものと考えている。

なお、本機能は本製品と GUI 端末との構成でのみ実行できる。

(3) 多面的な解析を可能とするファイアウォール統計情報

コネクションログ情報から、時系列統計、トラフィック統計、サービス統計、送信元統計、送信先統計といった 5 つの統計情報を参照することができる。

これらの統計情報を横断的に分析することで、NetShelter を経由したトラフィックの特性や不正アクセス状況等を詳細に分析することができる。

図 - 10 にファイアウォール統計情報の例を示す。

また、本機能は、本製品と GUI 端末との組合せのみならず、ログサーバ上でも利用できるようにしており、統計情報の分析スキルを蓄積することで新たなサービスビジネスへの展開も可能である。

## 8 むすび

以上ご紹介したとおり、今回ラインナップ追加した FW-L および FW-M の両装置は、他社製品に見られない斬新な機能を取り入れつつ、従来装置に勝る高信頼を実現している。今回の開発で取り組んだ様々なテーマの成果をもとに、従来装置の機能強化も継続的に実施し、更なるラインナップ強化と機能の充実を図っていく。

参考文献

- 1) 武田ほか：セキュリティ専用装置 NetShelter，PFU Tech.Rev.,11,1, pp.16-25 (2000)。
- 2) 青木ほか：高性能 / 高信頼セキュリティ専用装置 NetShelter / FW-P，PFU Tech.Rev.,12,2, pp.1-8 (2001)。

1) 時系列のコネクション統計

```
### パケット数 (Packet Count by Date & Hour)
03-10-05 00:00-01:00 pass 0 snat 0 snapt 0 ipsec 0 ipa 0 enc 0 block 0 reject 0
03-10-05 01:00-02:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 02:00-03:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 03:00-04:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 04:00-05:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 05:00-06:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 06:00-07:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 07:00-08:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 08:00-09:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 09:00-10:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 10:00-11:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 11:00-12:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 12:00-13:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 13:00-14:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 14:00-15:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 15:00-16:00 1244 0 0 0 0 0 0 0 0 0 0
03-10-05 16:00-17:00 105 0 0 0 0 0 0 0 0 0 0
03-10-05 17:00-18:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 18:00-19:00 271 0 0 0 0 0 0 0 0 0 0
03-10-05 19:00-20:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 20:00-21:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 21:00-22:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 22:00-23:00 0 0 0 0 0 0 0 0 0 0 0
03-10-05 23:00-24:00 0 0 0 0 0 0 0 0 0 0 0
Day 1720 0 0 0 0 0 0 0 0 0 0
Total 1720 0 0 0 0 0 0 0 0 0 0
```

2) トラフィック (パケット数とデータサイズ) に着目したコネクション統計

```
### パケット数 (Traffic by Packet-Count)
Packet-Count SrcIP DstIP IPProto DstPort Data-size
488 10.234.47.16 10.234.47.244 tcp 80 114278
488 10.234.47.244 10.234.47.16 tcp 82 197877
406 10.234.47.30 10.234.47.16 tcp 23 25301
332 10.234.47.16 10.234.47.30 tcp 1522 116431
23 10.234.47.16 10.234.47.244 tcp 1707 6700
3 10.234.47.16 10.234.47.244 tcp 1708 120

### データサイズ (Traffic by Data-size)
Data-size SrcIP DstIP IPProto DstPort Packet-Count
197877 10.234.47.244 10.234.47.16 tcp 82 488
116431 10.234.47.16 10.234.47.30 tcp 1522 332
114278 10.234.47.16 10.234.47.244 tcp 80 488
25301 10.234.47.30 10.234.47.16 tcp 23 406
6700 10.234.47.16 10.234.47.244 tcp 1707 23
120 10.234.47.16 10.234.47.244 tcp 1708 3

( 解析ログレコード数: 63 )
```

3) サービス種に着目したコネクション統計

```
### サービス (IPプロトコル/送信先ポート番号: Traffic by protocol & service)
IF IPProto DstPort Action Packet-Count Data-size
1 tcp 23 PASS 406 25301
1 tcp 80 PASS 488 114278
1 tcp 82 PASS 488 197877
1 tcp 1522 PASS 332 116431
1 tcp 1707 PASS 23 6700
1 tcp 1708 PASS 3 120

( 解析ログレコード数: 63 )
```

4) 送信先ホストに着目したコネクション統計

```
### 送信先IPアドレス (Traffic by Destination address)
# DstIP
IF IPProto DstPort Action Packet-Count Data-size SrcIP
10.234.47.16
1 tcp 23 PASS 406 25301 10.234.47.30
1 tcp 82 PASS 488 197877 10.234.47.244
10.234.47.30
1 tcp 1522 PASS 332 116431 10.234.47.16
10.234.47.244
1 tcp 80 PASS 488 114278 10.234.47.16
1 tcp 1707 PASS 23 6700 10.234.47.16
1 tcp 1708 PASS 3 120 10.234.47.16
```

5) 送信元ホストに着目したコネクション統計

```
### 送信元IPアドレス (Traffic by Source address)
# SrcIP
IF IPProto DstPort Action Packet-Count Data-size DstIP
10.234.47.16
1 tcp 80 PASS 488 114278 10.234.47.244
1 tcp 1522 PASS 332 116431 10.234.47.30
1 tcp 1707 PASS 23 6700 10.234.47.244
1 tcp 1708 PASS 3 120 10.234.47.244
10.234.47.30
1 tcp 23 PASS 406 25301 10.234.47.16
10.234.47.244
1 tcp 82 PASS 488 197877 10.234.47.16

( 解析ログレコード数: 63 )
```

図 10 ファイアウォール統計情報例  
( Fig.10-Example of the firewall statistical information )