セキュリティ・アプライアンス・プラットフォーム

鈴木　友泰　　吉田　守男
濱田　恒生　　青木　裕樹

沖テクノクリエーションは，沖電気工業株式会社の通信分野のハード系技術者を中心に2002年10月に設立した会社であり，通信，情報処理等の機器に関する開発，設計および販売，さらには，上記機器のコンサル，システムインテグレーション，運用支援までの幅広いプロセスに対応できる，高スキル保有者の集団である。

近年市場では，セキュリティに関する被害が広がる中で企業等の情報漏洩問題は少なくなく，企業内部のネットワークのセキュリティ対策として，情報漏洩防止ツールや専用のアプライアンス製品が注目されつつある。また，ネットワークで自己増殖し続けるワーム被害は収束には至らず，感染被害時のトラヒック輻輳は無視することはできない。こういった背景で通信とコンピュータの融合が急速に進む中，音声，画像，データをいかに最適に保護するかが現状の課題とも言える。

沖テクノクリエーションは，これらの課題を解決するために，初の自社製品として，セキュリティ対策の基本的な機能をコンポーネントとして提供する，セキュリティ・アプライアンス・プラットフォーム（以下，SecPLAT：Security Appliance Platformと呼ぶ）を開発した。本稿ではSecPLATの「アーキテクチャ」，「セキュリティソリューション」，SecPLATを利用した商品である「ワーム対策ソリューション」，および，SecPLATの要素技術を「ハードウェア」「プラットフォームソフトウェア」「管理ソフトウェア」の順で紹介する。

アーキテクチャ

SecPLATのアーキテクチャを**図1**に示す。SecPLATは，SecPLAT-Engine，SecPLAT-Gateway，SecPLAT-Managerの3つのコンポーネントで構成する。

■ SecPLAT-Engine

SecPLAT-Engineはネットワークプロセッサをコアとした高性能パケット・ハンドリング・プラットフォームである。レイヤ2から4までのパケットを処理し，セキュリティ対策として必要と考えた，パケットフィルタリング機能，QoS機能，ロードバランス機能，および，仮想ファイアウォール機能を標準で提供するセキュリティ専用のアプライアンス装置である。仮想ファイアウォール機能

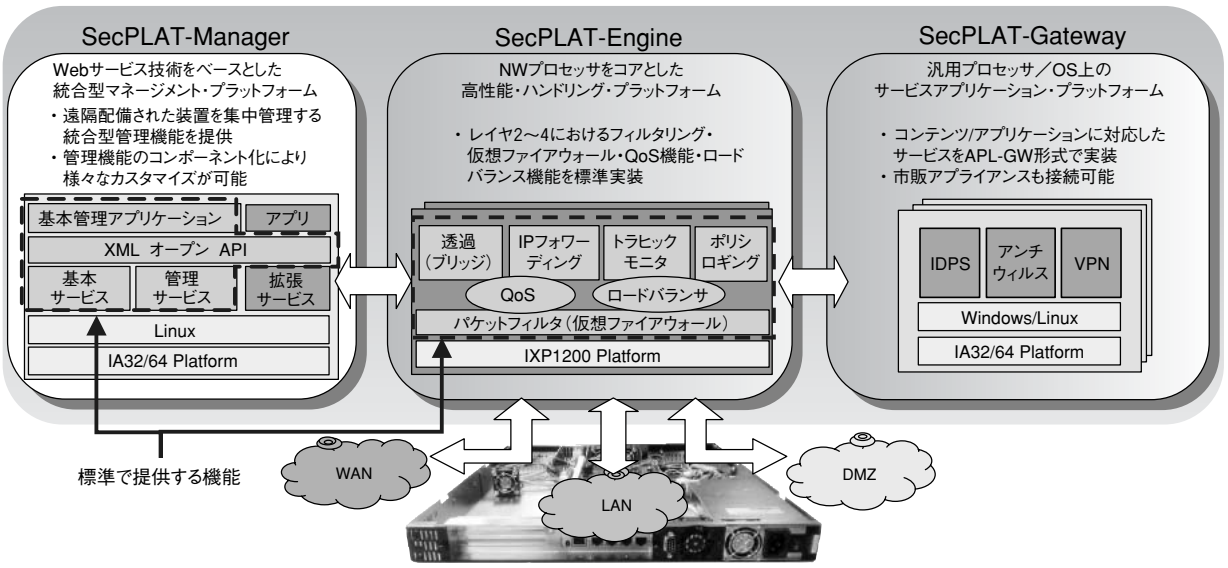

図1　SecPLATアーキテクチャ

は，VLAN（Virtual LAN）単位あるいはVLANの集合等でネットワークを仮想的かつセキュアなセグメント（以下セグメントと呼ぶ）で区分する機能であり，セグメントごとでのパケットフィルタやQoSの制御を可能にした，内部ネットワークのセキュリティ強化に向けた機能である。

■ SecPLAT-Manager

SecPLAT-Managerは遠隔配備された装置を集中管理する統合型管理機能，SecPLAT-Engineで収集するトラヒック情報をグラフィカルに表示，通知するレポート機能等を提供する。

■ SecPLAT-Gateway

SecPLAT-Gatewayは顧客のニーズに応じて，コンテンツ・アプリケーションに対応するレイヤ7のサービスをAPL-GW方式で実装するコンポーネントである。

SecPLATの特徴を以下に示す。

①セキュアな障壁を部門ごとに設置可能

SecPLAT-Engineの仮想ファイアウォール機能により，SecPLAT1台で最大64個の仮想的なセグメントを構築できる。これは，ネットワークの内部にファイアウォール装置を64台設置する時と同様の効果およびパフォーマンスが得られる。このセグメントが作り出す仮想的な障壁を越えた通信は原則として不可能なため，部門間で情報が流出することを防ぐことができる。さらに，ワームに感染した端末による影響を端末が所属する部門に局所化できる。

②きめ細かな帯域制御（QoS）が可能

SecPLAT-EngineのQoS機能が同パケットフィルタリング機能および同仮想ファイウォール機能と連携して動作することで，他部門で発生したトラヒック輻輳から影響を受けずに，リアルタイム性の高い画像とVoIPパケットおよびバースト性の高いストリームパケットをネットワーク上に最適な状態で転送できる。

③イントラネット上のトラヒック情報収集が可能

SecPLAT-Managerのレポート機能により，セグメントごと，アプリケーションごとにトラヒック状態を監視でき，ネットワークのボトルネック検出やトラヒック輻輳の対策効果をグラフィカルに確認できる。

④新たなセキュリティソリューションを迅速に提供

SecPLATが提供する標準機能を最大限に利用し，顧客ニーズに応じたアプリケーションをSecPLAT-Gatewayで実装することで，顧客ニーズに応じたセキュリティシステムを短期間で開発し，提供できる。

セキュリティソリューション

SecPLATをシステムのベースプラットフォームとして採用することで，以下のようなセキュリティソリューションを容易に開発できる。

①ワーム対策ソリューション

社内ネットワークに持込んだPCによるウィルス被害拡大・盗聴を防ぐために，トラヒックを部門ごとに規制する必要がある企業/官公庁向けのソリューションである。

②セキュアなデータセンタ構築ソリューション

企業ネットワークのアウトソーシングで，企業ごとのネットワークを安価に分離できるISP/データセンタ向けのソリューションである。

③特定アプリ向けセキュリティソリューション

市販セキュリティ装置では対応できない独自のAPLあるいはVoIPでのセキュリティを強化したい企業/官公庁向けのソリューションである。

次は，自社がSecPLATを利用し，セキュリティソリューションの1つとして商品化した「ワーム対策ソリューション」を紹介する。

ワーム対策ソリューション

SecPLATを応用した商品であるワーム対策ソリューションは，イントラネット内でワームの感染拡大を防止するソリューションである。**図2**に概要図を示す。ワーム対策ソリューションは，SecPLATに標準搭載されている機能のうち，仮想ファイアウォール機能，パケットフィルタ機能およびQoS機能を主要機能として用いることで，容易かつ短期間に開発した。独自に追加した機能は，SecPLAT-Gatewayにワーム検出機能を搭載したのみである。

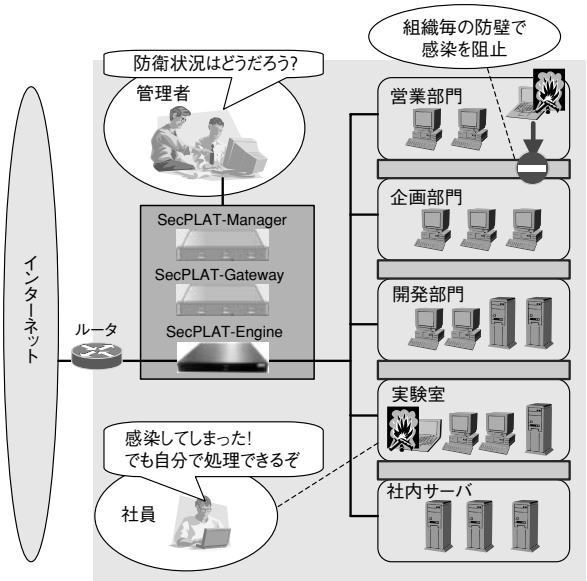

図2　ワーム対策ソリューションの概要

近年，企業ではIP電話導入等でネットワーク再構成を控えており，次のようなイントラネットの脅威への対応が最大の課題である。

●ワーム感染拡大の防止が困難

社員のうっかりミスでワーム感染端末が社内に持ち込まれ，感染が拡大するなど，アンチウィルスソフトの導入だけではワーム感染拡大を防止することができない。

●設置コスト高で導入困難

新しいセキュリティ装置を導入するためには，ネットワーク構成の変更や端末に専用ソフトウェアをインストールする必要があるなど，導入が困難である。

●ネットワークパフォーマンスに影響

セキュリティ製品を導入したことによって，ネットワークパフォーマンスの劣化やネットミーティング中に音声が途切れるといった問題が発生する可能性がある。

これらの課題は，ワーム対策ソリューションで解決できる。

●ワーム感染拡大を防止

組織ごとに最大64個の仮想的な障壁を設置することで，他の組織への感染拡大を防止できる。また，ワーム感染の予兆活動を検出し，感染端末に対して，特定のサーバを除き，自動的にネットワークへのアクセスを制限（隔離）する。特定のサーバは，最新OSパッチをダウンロードできるサーバなどが該当する。

●導入が容易

端末に専用ソフトをインストールする必要はなく，防衛するネットワークへ接続するだけで利用できる。また，ネットワークトポロジやセキュリティポリシを変更することなく，既存のネットワークに容易に設置できる。なお，最小構成でも1000台以上の端末を監視可能であり，端末1台当りの導入コストを低減できる。

●効率良くトラヒックを転送

QoS機能で，防壁ごとに帯域を分離させることが可能である。また，特定アプリケーションごとのQoS制御も可能であり，リアルタイム性の高い音声や画像トラヒックをスムーズに通過させることができる。

SecPLATを用いることで，ワーム対策ソリューションのように，現状の課題を解決する新しいセキュリティソリューションを容易に開発できた。具体的には，デモ機の開発に要した期間は1ヶ月程度と非常に短い期間であった。

以降では，SecPLATの要素技術を「ハードウェア」「プラットフォームソフトウェア」「管理ソフトウェア」の順に紹介する。

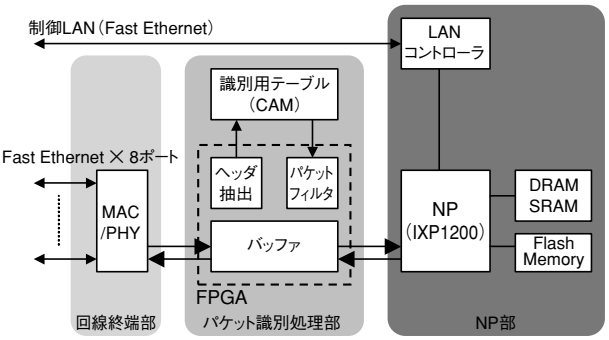

図3　SecPLAT-Engineハードウェア構成図

ハードウェア

SecPLAT-Engineのハードウェア（SecPLAT-Engineハードウェア）は，SecPLATアーキテクチャの中核に位置し，高速にパケットを識別し，転送するハードウェアである。「高速かつ柔軟なパケットハンドリング・プラットフォーム」として各種アプリケーションに容易に適用するため，**図3**に示すように，Intel社のIXP1200 Network Processor（以下NP）*1) を採用した構成である。NPにはプラットフォームソフトウェアを内蔵し，「プラットフォームソフトウェア」で述べる，入力パケットのフィルタリング，仮想ファイアウォール，QoS等の機能が提供される。

回線終端部とNP部の間には高速にパケットを識別するためのパケット識別処理部がある。このパケット識別処理部で入力パケットの識別処理をプラットフォームソフトウェアと分担，連携したことで，SecPLAT-Engineは，L4レベルまでのトラヒックフローの識別を高速に実現できた。SecPLAT-Engineハードウェアが担当するパケットの識別対象は**図4**に示す。

各ポートより受信したMAC（Media Access Control）フレームに対して，レイヤ2～4のヘッダ情報を抽出し，CAM（Content Addressable Memory）を用いて高速にパケットを識別する。ヘッダ抽出，CAM検索，識別結果によるフィルタリング，NPへの識別結果通知といった一連の動作をパイプラインで処理するこで，パケット識別処理部は，最小パケットサイズ（64Byte）で1Gbit/sのスループットを実現した。このパケットを識別するハードウェアをFPGAで構成することで，各種アプリケーションに応じて容易にカスタマイズ可能な構成となっている。SecPLAT-EngineボードはPIGMG*2) 規格に準拠し，汎用の1Uシャーシへ搭載が可能である。各種アプリケーション向けに，拡張PCIインタフェースを介した拡張ドライブ等の機能追加が可能である。**写真1**に開発した

＊1）IXP1200はIntel社の登録商標です。　＊2）PCIベースの産業用組込ボードの標準化団体（Advanced TCA,Compact PCI他）

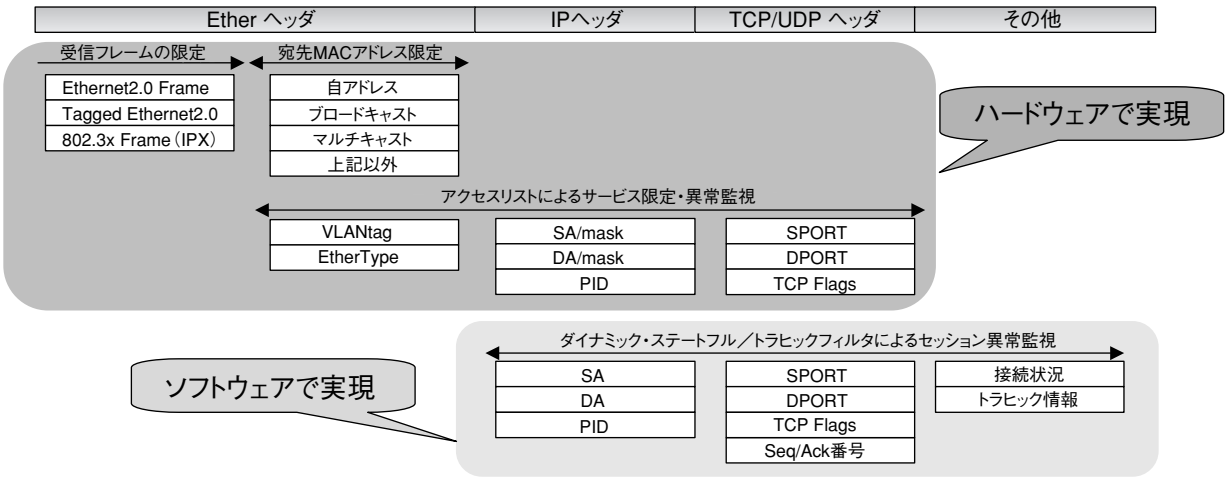

図4　パケット識別の分担

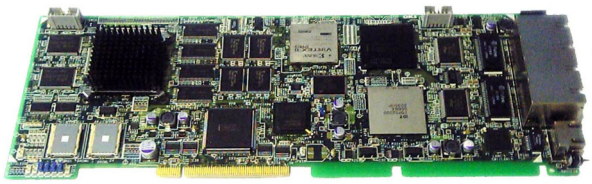

写真1　SecPLAT-Engineボード外観

写真2　SecPLAT-Engine装置外観

SecPLAT-Engineボードの外観，**写真2**にSecPLAT-Engine装置の外観を示す。

以上，SecPLAT-Engineハードウェアは，レイヤ2～4のパケットを高速に識別し，転送するプラットフォームを実現したことを述べた。このようなSecPLAT-Engineハードウェアにより，次に述べる「プラットフォームソフトウェア」は，ハイパフォーマンスを維持しつつ，セキュリティ対策の標準機能を提供できた。

プラットフォームソフトウェア

プラットフォームソフトウェアは，SecPLAT-EngineハードウェアのNP上のマイクロエンジンソフトウェアであり，SecPLATの標準機能である，仮想ファイアウォール機能，QoS機能，ロードバランス機能等を実現する。特にSecPLATの特徴的な機能である，仮想ファイアウォール機能とQoS機能を説明する。

①仮想ファイアウォール機能

図5に仮想ファイアウォール（VFW:Virtual FireWall）機能のイメージ図を示す。VFWは，物理的なファイアウォール装置と同等な機能をSecPLAT-Engineの内部に論理的なファイアウォールとして構成する機能である。たとえば，ファイアウォールサービスを提供するデータセンタなどで，新規にサービスを提供する際に新たなファイアウォール装置を追加する必要がなく，サービスの追加・削除が容易になる。

仮想ファイアウォール機能の特徴を以下に示す。

- 最大64個のVFWを構成可能。
- VFWごとに独立したパケットフィルタをポリシーとして設定可能。

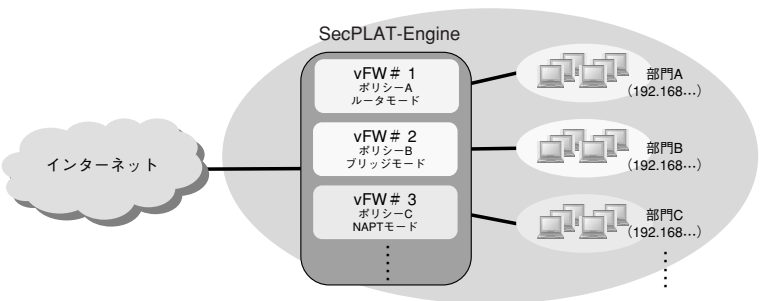

図5　仮想ファイアウォール（VFW）機能

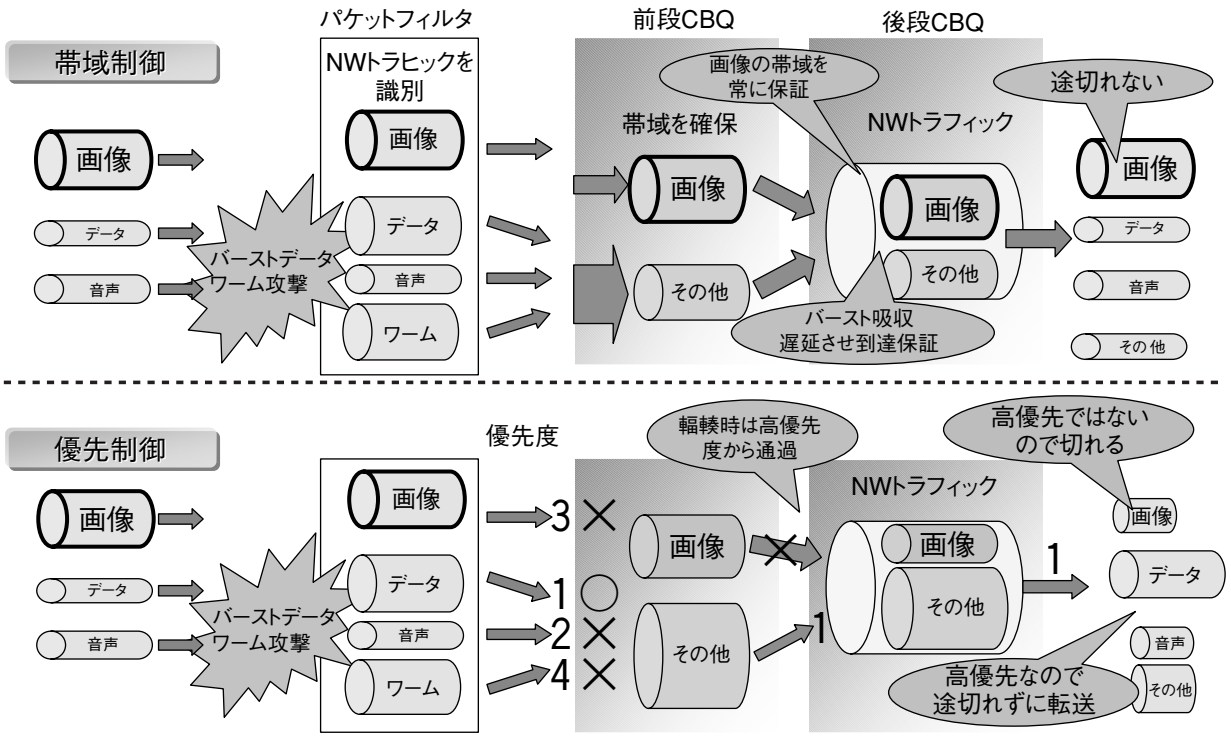

図6　品質制御（QoS）

- 各VFWの動作はルータ，ブリッジ，NAPT（Network Address Port Translation, IP masquerade）のいずれかを選択できる。
- VFWごとに独立したアドレス空間を割当可能で，IPアドレスを重複して利用できる。
- VLANにVFWを関連付けることができる。イントラネット内部の部門がVLANで区分されていれば，VFWが部門間に仮想的な障壁を設け部門間の情報流出を防止できる。
- VFW間でのフォワーディングが可能で，イントラネット内部の部門をまたがるP2Pアプリケーション（たとえばVoIP）も問題なく利用できる。

②品質制御（QoS）機能

QoS機能の概要を**図6**に示す。QoS機能は帯域制御と優先制御で実現する。帯域制御は，トークンバケット方式のCBQ（Class-Based Queueing）を前段と後段で階層的に配置する。前段のCBQはパケットフィルタで識別されたアプリケーションごとに帯域を保証する。後段のCBQはバッファを持ち，トラヒックのバーストを吸収しながら遅延転送することで，到達性を保証する。帯域制御と優先制御を組み合わせて利用することで，バースト性の高いビデオストリームパケット，リアルタイム性の高いVoIPパケットなどをネットワーク上で最適な状態で転送できる。さらに，後段のCBQを各VFWに割当てることで，パケットの到達性がVFWごとに確保され，VFWごとの可用性を保証できる。また，各VFW内を導通する各トラフィックフローを前段のCBQに割当てることで，VFWごとでかつアプリケーションごとに帯域を保証できる。

以上，プラットフォームソフトウェアはSecPLATの特徴となる仮想ファイアウォール機能とQoS機能を実現したことを述べた。次は，これまで述べたSecPLAT-Engineを統合管理する管理ソフトウェアの技術を述べる。

管理ソフトウェア

SecPLAT-Managerに搭載する管理ソフトウェアは，遠隔配備された装置を集中管理する統合型管理機能，SecPLAT-Engineで収集するトラヒック情報をグラフィカルに表示，通知するレポート機能等を提供するソフトウェアである。管理ソフトウェアが提供する管理機能の中から，レポート機能とアラート機能を紹介する。機能の概要図を**図7**に示す。

①レポート機能

レポート機能は，SecPLAT-Engineから定期的に収集し蓄積したパケット統計情報に基づき，時間・日・週・月を単位として，トラヒックの状況をグラフィカルに表示し，通知する機能である。管理者は，Webブラウザま

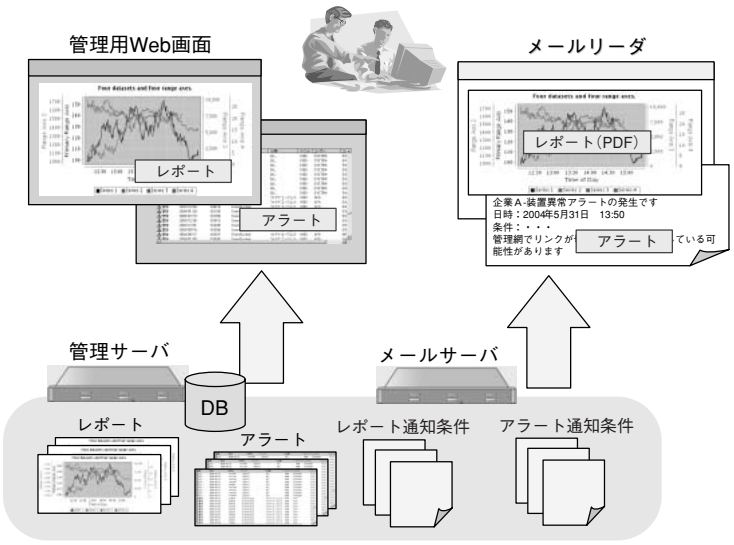

図7　レポート機能とアラート機能

たはメールに添付したPDFファイルを見ることでトラヒックの状況を確認できる。

レポート機能の特徴は，仮想ファイアウォール機能で構成されるセグメントごとやアプリケーションごとにトラヒック情報をまとめることができるために，ネットワーク管理者が監視し易い情報を提供できる点にある。たとえば，イントラネットの部門ごとのトラヒック利用状況や，データセンタの企業ごとのトラヒック利用状況をグラフィカルに監視できる。

②アラート機能

アラート機能は，装置障害や設定した通知条件（統計カウンタの閾値超過等）に一致する条件が発生した時，アラートを送信する機能である。アラートはメールでリアルタイムに通知する方法とWebブラウザにより過去発生アラートを表示する方法の2つの形態を提供する。

アラート機能の特徴は，レポート機能と同様に，セグメントごとやアプリケーションごとにトラヒック異常を監視できる点にある。

この他，管理ソフトウェアは，SecPLATが他のアプライアンス装置／アプリケーションと容易に連携するために,Webサービス技術を採用した。管理機能は,SOAP（Simple Object Access Protocol）over HTTPS（Hyper Text Transfer Protocol over SSL）で外部アプリケーションから利用でき,複数のアプリケーションが連携動作することで，新たなセキュリティソリューションを早期に開発できる枠組みを設けた。

今後の展開

弊社は今までSecPLATを開発し，SecPLATを利用したワーム対策ソリューションを商品化した。今後は，SecPLATをベースにしたセキュリティソリューションを創出していきたい。IT資産管理，スパムメール対策などの新たなセキュリティソリューションの創出により，新しい市場を開拓する。ソリューション創出のキーとなるSecPLAT-Gatewayでの機能については，沖電気グループ内の資産のみでなく，他社のセキュリティ・アプライアンスおよび各種セキュリティ関連ソフトウェアとの連携による実現も視野に入れていく予定である。

また，現在のSecPLATは，総スループットが1Gbit/s未満であるような，中規模のイントラネットであるのに対し，今後は小規模のイントラネット／SOHOをターゲットにした，低価格で顧客のニーズに応じたセキュリティプラットフォームを開発していく予定である。

あ と が き

以上，簡単ではあるが，SecPLATの概要，SecPLATを利用したワーム対策ソリューションを紹介し，SecPLATの要素技術である，ハードウェア，プラットフォームソフトウェア，管理ソフトウェアを説明するとともに，今後のSecPLATを展望した。SecPLATの開発を通して，沖電気グループとして取り組んでいる「情報通信融合ソリューションの創出」に貢献していきたいと考える。◆◆

●筆者紹介

鈴木友泰：Tomoyasu Suzuki. 株式会社沖テクノクリエーション システム開発部
吉田守男：Kamio Yoshida. 株式会社沖テクノクリエーション 設計開発1部
濱田恒生：Tsuneo Hamada. 株式会社沖テクノクリエーション システム開発部
青木裕樹：Yuki Aoki. 株式会社沖テクノクリエーション システム開発部