ネットワーク・セキュリティ・ソリューション

～「SecApPlat™」コンポーネントからソリューションへ ～

濱田　恒生　　鈴木　友泰
芝　修吾　　濱　隆二

近年，ネットワークで自己増殖を繰り返しながら破壊活動を続けるワームや，複数の感染端末で構築されたネットワークから組織的な攻撃を仕掛けるボットネット*1)によるネットワークを悪用した攻撃の被害が多数報告されており，ネットワークのセキュリティ対策として各種対策ソフトウェアや専用アプライアンス製品の導入が進んでいる。

また，個人情報保護法の施行により注目される情報漏えいでは，ネットワークを悪用し，故意または過失による機密情報の流出事例が報告されており，その対策が急務である。

一方，急速に通信とコンピュータの融合が進む中，ソフトフォンのように音声，映像，データを連携させて付加価値を向上させるアプリケーションへの要求が高まっている。ネットワークは，この3種類のトラフィックを効率的に扱う，トリプルプレー・ネットワークへの進化が必要である。なお，本稿では，音声，映像，データの3種類のトラフィックを単一のネットワークで提供，運用する形態のことをトリプルプレー・ネットワークと呼ぶ。

これらを背景とし，ネットワーク・セキュリティ対策には，ネットワークのセキュリティ確保と，トリプルプレー・ネットワークの実現を両立するソリューションが求められている。

沖テクノクリエーションは，ネットワーク・セキュリティ対策に必要とされる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「SecApPlat™*2)」[1)]を開発した。「SecApPlat」は，ネットワークプロセッサを採用し，高速なパケット処理が可能であり，かつファームウェアを入れ替えることで異なるソリューションに柔軟に適応するEngineを中核とし，統合管理機能を提供するManager，レイヤ7のサービスを提供するGatewayの3つのコンポーネントで構成される。本稿では，「SecApPlat」をベースとした，ネットワークのセキュリティ確保とトリプルプレー・ネットワークを実現する，3つのソリューションを紹介する。

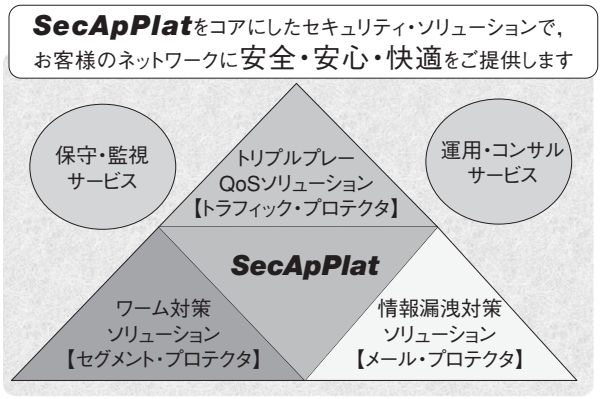

図1 「SecApPlat」セキュリティ・ソリューション

ネットワーク・セキュリティ・ソリューション

ネットワーク・セキュリティ・ソリューションは，**図1**に示す3つのソリューションで構成する。

第1のソリューションは，ワームの感染拡大を未然に防止するワーム対策ソリューション「セグメント・プロテクタ」である。

第2のソリューションは，電子メールによる情報漏えいを防止する情報漏えい対策ソリューション「メール・コンフィデンス・プロテクタ」である。

第3のソリューションは，音声，映像，データのトラフィックを統合するトリプルプレー・ネットワークの効率的な運用を実現するトリプルプレーQoS（Quality of Service）ソリューション「トラフィック・プロテクタ」である。

以降，3つのソリューションの特徴，システム構成，適用例を，ソリューションごとに述べる。

セグメント・プロテクタ

セグメント・プロテクタは，ワームの感染拡大を未然に防止するワーム対策ソリューションである。既存種，新種に関わらず，ワームの自己増殖活動を検出し，感染端末のトラフィックを隔離することで，感染拡大を防止することができる。

*1)ウィルスの1種で，感染すると遠隔操作が可能になり，攻撃者によって悪用されるコンピュータ群
*2)SecApPlatは(株)沖テクノクリエーション社の商標です。

(1) 特徴

■ ワーム感染拡大を防止

社員のうっかりミスで，ワームに感染した端末が社内に持ち込まれ感染が拡大する等，ウィルス対策ソフトの導入だけではワームの自己増殖活動を完全に防止することができない。これは，ウィルス対策ソフトが，基本的にパターンマッチングを用いた仕組みによりワーム感染を検出するため，新種のワームには，パターンが更新されるまで，無力であることに起因する。

セグメント･プロテクタは，既存種，新種に関わらずワームの自己増殖活動（ワームがネットワーク上の感染対象を見つけ出すためのトラフィックの挙動）を検出し，感染端末のトラフィックを自動的に隔離する。さらに，**図2**に示すように，プロテクションセグメントで社内ネットワークを組織ごとに最大64分割することで，感染した端末が存在する組織から，他の組織への感染拡大を防止することができる。なお，プロテクションセグメントは，物理的なファイヤウォールと同等な機能を後述するEngineの内部に論理的なファイヤウォールとして，閉域空間を構成するものである。

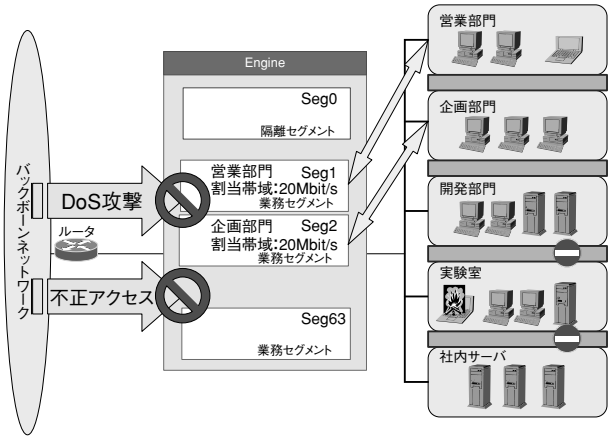

図2 プロテクションセグメント

■ 導入が容易

一般に，新しいネットワーク･セキュリティ製品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の対策ソフトウェアをインストールする必要があり，導入に手間がかかってしまう。

セグメント･プロテクタは，端末に専用の対策ソフトウェアをインストールする必要がなく，防衛するネットワークへ専用ハードウェア（Engine）とPCサーバ（Manager，IDS，WFS）を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ーを変更することなく，容易に既存のネットワークに設置できる。さらに，最小構成でも1,000台以上の端末を監視することができ，端末1台当りの導入コストを劇的に低減できる。

■ 効率よくトラフィックを転送

DoS攻撃や不正アクセス等の異常トラフィックにより，業務のトラフィックが悪影響を受ける場合がある。また，ブリッジ型のネットワーク･セキュリティ製品の導入は，ネットワークの転送能力を劣化させ，ネットミーティング中に音声が途切れる等，アプリケーションの運用の障害になることがある。

セグメント･プロテクタは，専用ハードウェアを用いたQoS制御機能を搭載しており，プロテクションセグメントで分割した組織ごとの利用帯域や特定アプリケーションごとのQoSを制御できるために，リアルタイム性の高い音声や映像トラフィックを劣化させることなく，スムーズに転送できる。

(2) システム構成

セグメント･プロテクタは，4種類のコンポーネントで構成し，各コンポーネントを相互に連携することで，既存種，新種に関わらず，ワームに感染した端末のトラフィック（ワーム･トラフィック）を隔離する。

●Engine（専用ハードウェア）

透過的にイーサネット･フレームを転送する専用ハードウェアであり，最大64個のプロテクションセグメントを業務セグメントや隔離セグメントとして設定し，ワーム･トラフィックの隔離を実行する。

●Manager（PCサーバ）

最大10台のEngineを管理するソフトウェアである。管理者は，Web画面を操作することで，ワーム検出状態やモニタグラフによる統計情報の監視を実行する。

●IDS:Intrusion Detection System（PCサーバ）

Engineから複製されたトラフィックを受信し，その挙動を解析することで，ワームの自己増殖活動を検出する。

●WFS:Work Flow Server（PCサーバ）

隔離された端末を利用するユーザへ感染を通知するために，警告Web画面を強制的に表示する。

図3に4種類のコンポーネント（最小構成の4台）が連携し，感染端末を隔離する動作の概要を示す。

① IDSでワームの自己増殖活動を検出
② Managerにワーム検出を通知
③ Managerは，感染端末の隔離を指示し，Engineが感染端末を隔離セグメントへ移転
④ ユーザが感染端末のブラウザを起動，WFSは警告Web画面を送信し，ブラウザに表示

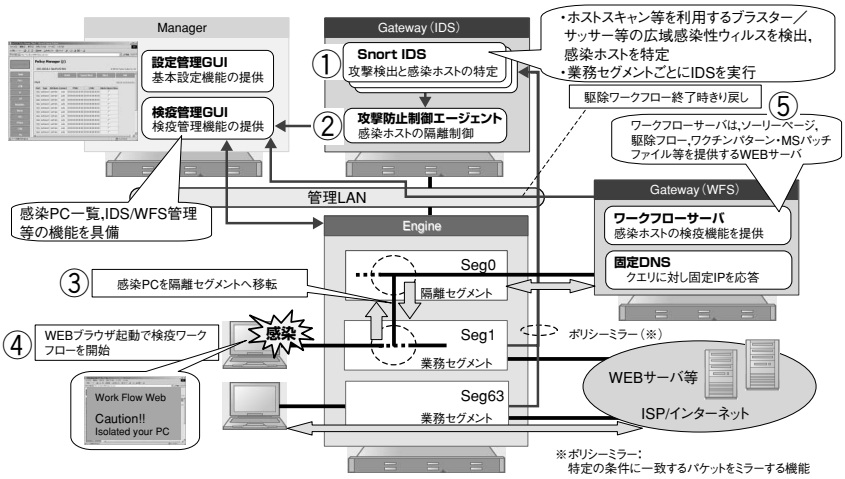

図 3　隔離動作の概要

⑤ ユーザは，WFSに配備したワーム除去ソフトウェアや，
許可された特定サーバへアクセスし，復旧作業を実施
以上の動作によりワームの感染拡大を最小限に防止することができる。

(3) 適用例

1,000端末を越える大規模ネットワークでは，4種類のコンポーネントを最適な数だけ配置することで，導入コストおよび運用コストを削減することができる。**図4**は，管理エリアにManagerとWFSを1台ずつ配置し，運用エリアそれぞれにEngineとIDSを配置した例である。

各運用エリアは，たとえば，企業における支社拠点や工場拠点が相当する。1つの運用エリアは，最大1,000端末を収容し，運用エリア内はプロテクションセグメントにより組織ごとやフロアごとにファイヤウォールを設置する。これにより，組織･フロアごとにセキュリティポリシーを柔軟に管理できる。

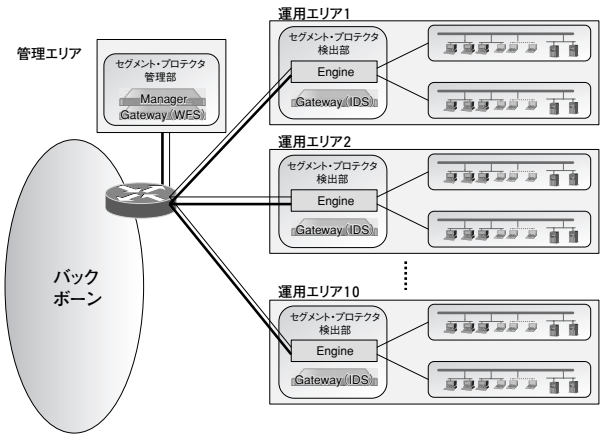

図4　大規模ネットワークにおける分散配置の例

メール･コンフィデンス･プロテクタ

メール･コンフィデンス･プロテクタは，電子メールによる情報漏えいを防止する，情報漏えい対策ソリューションである。

2005年4月の個人情報保護法施行に伴い，情報漏えい対策は企業の必須課題となっている。電子メールは，情報を共有するツールとして極めて利用頻度が高いために，簡単に情報漏えい経路となる代表的なツールである。

(1) 特徴

電子メールによる情報漏えい対策は，a）ユーザの操作ミス等の過失によるもの，b）悪意を持ったユーザが情報漏えいを起こす故意によるもの，の2つを防止する必要がある。

■ 過失による情報漏えいを防止

類似電子メールアドレスによる宛先の打ち間違いや，返信や転送時の宛先の消し忘れ等，操作ミスにより簡単に情報漏えいが発生する電子メールシステムは，リスク管理として最優先で対策すべきである。

メール･コンフィデンス･プロテクタは，予め指定した不正キーワードが電子メールに含まれるかを検査し，不正な電子メールを判定，送信を規制する。これにより，ユーザの過失による情報漏えいを防止できる。さらに，Webメールにも対応しており，万全の対策ができる。

■ 故意による情報漏えいを防止

電子メールシステムでは，暗号を用いた電子メールや，Webメールによる外部へのファイル送信により，顧客情報等の機密情報を売買目的で外部に持ち出すことができる。

メール･コンフィデンス･プロテクタは，電子メール送受信をロギングすることで，情報漏えいが発生した際に，情報を持ち出した者を特定でき，故意による情報漏えい犯罪への抑制効果を発揮できる。また，管理者の操作自体もロギングでき，完全に情報漏えいの経路を監視できる。

■ 常時監視の実現

情報漏えいは，いつ発生するか予測できないため，24時間365日，常に電子メールを監視する情報漏えい対策が必要である。

メール･コンフィデンス･プロテクタは，コンポーネントの1つである電子メール情報漏えいゲートウェイ（MP-GW）を冗長配置することで，ゲートウェイの装置故障やファイルアップデート時でも電子メールシステムの監視

を中断しない。

(2) システム構成

メール･コンフィデンス･プロテクタは，3種類のコンポーネントで構成する。

●Engine（専用ハードウェア）

透過的にイーサネット･フレームを転送する専用ハードウェアであり，冗長配置されたMP-GW間をロードバランスすることで，情報漏えい対策としてノンストップサービスを実現する。

●MP-GW（PCサーバ）

透過型のゲートウェイであり，クライアントやメールサーバの設定を変更する必要はない。電子メールの不正キーワード検索および遮断処理を実行する。

●管理端末

MP-GW管理用の専用ソフトウェアをインストールした端末であり，電子メール遮断やロギングの不正キーワードポリシーの設定やロギング情報の検索，参照を行う。

次に，メール･コンフィデンス･プロテクタの主な機能を示す。

■ 電子メール遮断機能

電子メール遮断機能は，SMTPとHTTP（Webメール）に対応し，**図5**に示すような外部への電子メール情報漏えいを防止する。

主な機能を以下に示す。

- 電子メールのヘッダおよび本文，添付ファイル内の不正キーワードの検索が可能
- 電子メールのサイズや添付ファイル数を制限し，電子メールサーバの負荷を軽減
- マイクロソフト･オフィス･データファイルやPDFのファイル形式をサポートしており，通常の業務で使用されるファイルが検査可能
- LZH，TGZ，ZIP等のファイル圧縮形式をサポートしており，通常の業務で使用されるファイル圧縮形式で圧縮されたファイルが検査可能
- 管理者に対して警告を発することで，インシデント発生時に迅速な対処が可能
- 送信者への警告メール通知によって，ユーザは自ら検知，対処が可能

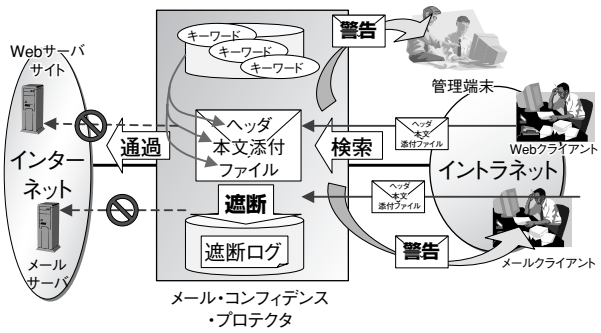

図 5　電子メール遮断機能

■ ロギング機能

ロギング機能には，2種類の機能があり，いずれも電子メールの本文，添付ファイルの全てをログとして蓄積することができ，管理者は必要に応じて参照できる。

2種類のロギング機能の1つは，電子メール遮断時に蓄積する機能であり，これは，管理者の承認により，一旦ログとして蓄積された電子メールをそのまま再送させることもできる。

もう1つは，通過する電子メールを全てロギングする機能であり，過去ログとして蓄積された電子メールは，遮断機能と同様の操作で，ヘッダおよび本文，添付ファイル内の不正キーワードを検索することができる。

■ 高可用性機能

高可用性機能は，**図6**に示すように，a）障害発生時のMP-GWの自動切り替え，b）MP-GW復旧前にログを故障前の状態へ完全復旧，の2つを行う。これらは，転送レイヤレベルとアプリケーション（APL）レベルの2種類の障害検出により実現し，同様のゲートウェイ型のシステムよりも，高い可用性を確保できる。

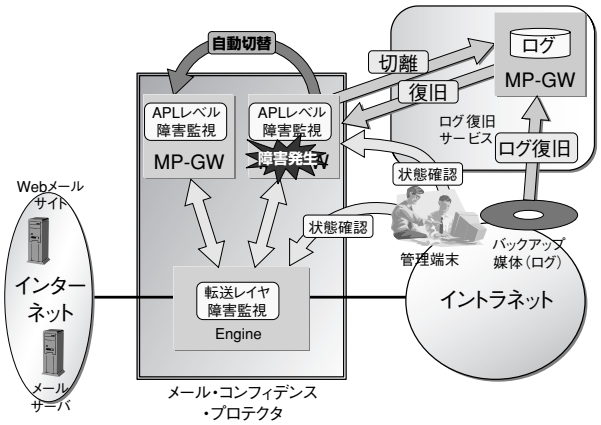

図 6　高可用性機能

(3) 適用例

メール･コンフィデンス･プロテクタは，**図7**に示すように，設置位置により情報漏えい防止の目的が異なる。

①の設置位置では，ユーザの電子メールクライアントの操作ミスによる情報漏えい防止と，悪意を持ったユーザの電子メール送信をロギングする。

②の設置位置では，グループ企業等で電子メールシス

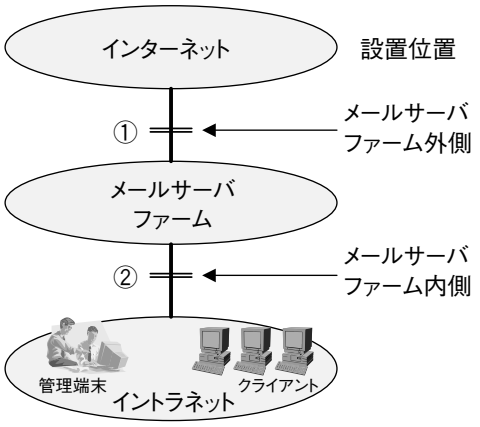

図 7　目的別の設置位置

テムを共用している場合等，内部ネットワークへの情報漏えいを防止する。

トラフィック･プロテクタ

トラフィック･プロテクタは，音声，映像，データのトラフィックが単一のネットワークに混在するトリプルプレー･ネットワークの効率的な運用を実現する，トリプルプレーQoSソリューションである。また，通信品質を確保することで，セキュリティ対策としても有効なソリューションとなる。

企業内のネットワークでは，今後，IP電話だけでなく，PC上で動作する映像やデータを連携することで付加価値を向上させるアプリケーションが普及すると予測される。このようなアプリケーションの普及により，ネットワークは，IP電話，映像，データといった，3種のトラフィックが複雑に交じり合うことになる。現状のネットワークでは，音声，映像，データのそれぞれの通信品質を確保することができない。

(1) 特徴

■ 通信品質劣化の要因を分析

トリプルプレー･ネットワーク上の音声，映像のトラフィックは，ワーム感染拡大による輻輳や，大容量ファイル転送による影響を受けやすく，通信品質の劣化による音声のエコーや途切れや映像の乱れが生じる。

トラフィック･プロテクタは，レイヤ4までのパケットヘッダ情報とRTPヘッダ情報を識別し，トラフィックを音声，映像，データに分類することができる。分類したトラフィック状態を監視し，流入するトラフィックの統計情報を収集，収集した統計情報のグラフ化により，通信品質劣化の要因をリアルタイムに監視，分析できる。

■ 通信品質の確保

接続する拠点が多いネットワークは，アクセス回線の帯域幅やトラフィック量が異なり，全拠点における通信品質を均一に保つことが困難である。

トラフィック･プロテクタは，帯域規制，バースト吸収，優先転送が可能な階層型QoS制御機能で，各トラフィックの通信品質を確保する。

(2) システム構成

トラフィック･プロテクタは，2種類のコンポーネントで構成する。Engineを各分散拠点のネットワーク境界部分に配置し，Engineを統合管理するManagerを管理拠点に配置する。

●Engine（専用ハードウェア）

透過的にイーサネット･フレームを転送する専用ハードウェアであり，パケット分析およびトラフィック制御を実行する。

●Manager（PCサーバ）

最大10台のEngineを管理するソフトウェアである。管理者は，Web画面を操作することで，映像，音声，データトラフィックを監視する。

次に，トラフィック･プロテクタの主な機能を示す。

■ トラフィック分析機能

トラフィック分析機能は，**図8**に示すように，a）パケットヘッダ情報からトラフィックの種別を分析するパケット分析，b）RTPヘッダ情報からリアルタイムトラフィックの種別を分析するトリプルプレー分析，の2つのトラフィック分析機構を持つ。これら2つの分析機構により，音声，映像，データトラフィックを，さらに細かく分類できる。また，ネットワークを構成するIP機器（スイッチ，ルータ）と連携したQoSを制御するために，分類結果から，イーサネットヘッダ上の優先度（Priority）と，IPヘッダ上のToS（Type of Service）を付与できる。これによりネットワーク上で，より高い通信品質を確保することができる。

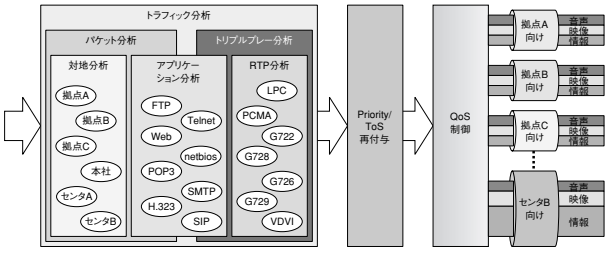

図 8　トラフィック分析機能

■ トラフィック制御機能

トラフィック制御機能は，CBQ（Class Based Queueing）方式による帯域制御機構により，一定の帯域幅にトラフィックを制限できる。これにより，Webアクセス等の利用帯域を規制し，業務アプリケーションが利用する帯域を保証するといった制御ができる。また，パケット送信の優先制御機構により，IP電話やビデオ会議等のリアルタイムアプリケーションのトラフィックを，非リアルタイムアプリケーショントラフィックより優先して転送できるため，内部遅延が少ないスムーズな到達性を保証できる。

図9にトラフィック制御の実施前と実施後の帯域利用状況の比較を示す。トリプルプレー分析により音声，映像のトラフィック量を把握しつつ，トラフィック制御によりバーストするトラフィックから音声･映像のトラフィックを守ることで，エコーや映像の揺らぎを抑えることができる。

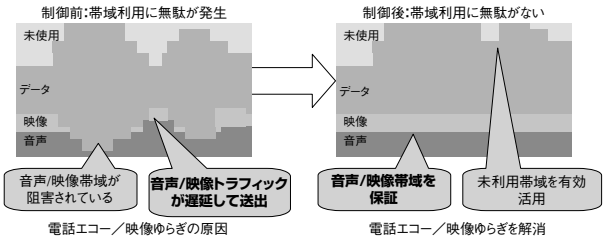

図 9　品質制御の効果

(3) 適用例

図10にトラフィック･プロテクタの適用例として，ソフトスイッチを用いたIP電話システムへの適用を示す。

本適用例では，次の効果を得ることができる。

- センタ側に配置したEngineによりDoS攻撃や突発的な輻輳から，呼制御トラフィックを防御
- 拠点ごとに配置したEngineにより音声トラフィックの通信品質を確保
- ブリッジ型の接続により，ネットワークトポロジに依存しない配置が可能

ま と め

「SecApPlat」をベースとした，ネットワークのセキュリティ確保とトリプルプレー･ネットワークを実現する，3つのソリューションを紹介した。

ワームやボットネットによるネットワークを悪用した攻撃や，ネットワークを媒体とした情報漏えいによる被害は後を絶たず，ネットワークのセキュリティ対策は，必ずしも十分とは言えない状況である。

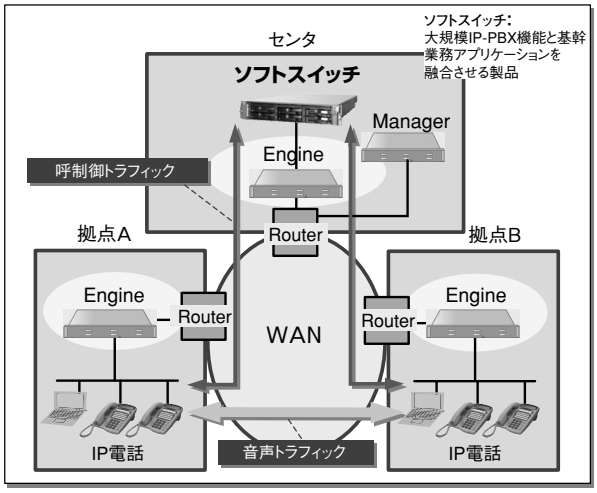

図 10　IP電話システムへの適用

このような状況に対して，今回，紹介した3つのソリューションは，未知のワームの感染拡大防止や，透過型の電子メール情報漏えい防止，さらに，音声，映像，データの通信品質の確保を実現し，お客様のネットワーク･セキュリティ対策の強化に貢献できる。

今後は，お客様への提案の中から新たな課題を掘り起こし，よりよいネットワーク･セキュリティ･ソリューションの開発と展開を進めていく。 ◆◆

■参考文献

1）鈴木友泰，吉田守男，濱田恒生，青木裕樹：セキュリティ･アプライアンス･プラットフォーム，沖テクニカルレビュー202 号，Vol.72 No.2，pp.50–pp.55，2005年

●筆者紹介

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
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
芝修吾：Shugo Shiba. 株式会社沖テクノクリエーション システム開発部
濱隆二：Ryuji Hama. 株式会社沖テクノクリエーション　システム開発部