

IPCOM EX シリーズの統合セキュリティ管理機能の強化 —シグネチャー型 IPS 機能—

Reinforcement of the Integrated Security Management Function of the IPCOM EX Series
- Signature-type IPS Function -

道根慶治 * 山下康一 * 阿久津 寛 * 中臣国雄 * 越智昭喜 * 早川 明 * 小出和弘 *
Keiji Michine Koichi Yamashita Kan Akutsu Kunio Nakatomi Akiyoshi Ochi Akira Hayakawa Kazuhiro Koide

* ソフト・アプライアンスグループ アプライアンスソフトウェア事業部 第四開発部

IPCOM EX シリーズの統合セキュリティ管理機能の機能強化として、2007 年 10 月に「シグネチャー型 IPS」機能の提供を開始した。本稿では、シグネチャー型 IPS 機能を開発する上での課題と対策、シグネチャー型 IPS 機能の概要とその特長および、IPCOM EX シリーズの統合セキュリティ管理機能の優位性と導入効果について紹介する。

To reinforce the integrated security management function of the IPCOM EX series, PFU started to provide the "signature-type IPS function" in October 2007. This paper introduces the challenges faced in the development of the signature-type IPS function and their solutions; the overview and features of the signature-type IPS function; and the advantages of and the benefits after implementation of the integrated security management function of the IPCOM EX series.

1 まえがき

昨今のネットワークシステムは、様々な新たなセキュリティ脅威にさらされ、機密情報の漏洩、システムの停止などの被害が発生しており、これらの複雑化、高度化するセキュリティ脅威に対抗する対策の実施が緊急の課題となっている。

IPCOM EX シリーズは、2007 年 4 月に、アプリケーション・ファイアウォール機能（アプリケーションレベルのアクセス制御機能）、アノマリ型侵入検知・防御（IPS：Intrusion Prevention System）機能、アンチウイルス機能および Web コンテンツ・フィルタリング機能を集約、一元化した統合セキュリティ管理機能の第一弾を提供した^{※1）、※2）}。

統合セキュリティ管理機能は、1 台のハードウェアで多種多様なセキュリティ管理機能を集約、一元化できるため、管理・運用負荷と導入コストの低減を実現するベストソリューションを提供する。

本稿では、統合セキュリティ管理機能の強化として、

2007 年 10 月に提供を開始した、多様化する様々なシステム上の脆弱性やアプリケーションの脆弱性を突いたセキュリティ脅威からネットワークシステムを保護する「シグネチャー型 IPS」機能の提供機能とその特長、他社機能比較にもとづいた IPCOM EX シリーズの優位性と IPCOM EX シリーズのセキュリティ管理機能を使用したセキュリティソリューションおよび、今後の取り組みを紹介する。

2 開発背景と狙い

2.1 シグネチャー型 IPS 機能の開発背景

IPCOM EX シリーズは、ネットワークセキュリティ管理機能、アプリケーション配信の最適化（サーバ負荷分散）機能および、ネットワークの最適化（QoS 制御）機能の三つの機能を柱に、ネットワークシステムの安全（セキュリティ脅威の排除）、安心（ネットワークシステムの高信頼化）、高速化（サーバアクセラレーシ

ョン) を提供する。

IPCOM EX シリーズは、ネットワークシステムの安全、安心を制御する機能の一つとして、アプリケーションに対する不正アクセスや許可されないアクセスからシステムを保護する「アプリケーション・ファイアウォール機能」、異常な形式のパケットや異常なアプリケーションコンテンツを使用したサービス妨害攻撃からシステムを保護する「アノマリ型の IPS 機能」および、ウイルス感染や許可されないサイトへのアクセスを防御する「アンチウイルス機能」と「Web コンテンツ・フィルタリング機能」を提供している。しかし、これらの機能では、昨今急速に増加している Web アプリケーションやオペレーティングシステム (OS) の脆弱性を狙った攻撃や機密情報の搾取を目的としたシステムへの不正侵入などの新たなセキュリティ脅威からネットワークシステムを完全に保護することが難しく、これらのセキュリティ脅威に対抗する機能の早期提供が求められている。

2.2 シグネチャー型 IPS 機能の狙い

近年、クライアント PC に専用のソフトウェアをインストールする必要がないこと、管理コストが大幅に削減できるなどの理由で、社内システムや情報公開システム、商取引システムに Web アプリケーションを利用することが定着している。特に、企業活動の中心となる情報発信のためのシステムや商取引システムは、その性格上、インターネットへの接続が前提となるため、これらの Web アプリケーションシステムは、世界中のあらゆる場所から攻撃対象となり、常にセキュリティ脅威に晒されることになる。独立行政法人 情報処理推進機構 (IPA) の情報セキュリティ白書 2006 年版^{※3)} および、情報セキュリティ白書 2007 年版^{※4)} によると、2006 年から引き続き、情報漏洩の被害は増加傾向にあること、安易なパスワードを狙った Web システムへの不正侵入や Web アプリケーションの脆弱性に起因したインジェクション攻撃、オペレーティングシステム (OS) の脆弱性を悪用したコマンドインジェクション攻撃や Web アプリケーションのバッファオーバーフローの脆弱性を悪用した攻撃が 2006 年から 2007 年になって急増していることが報告されている。主な攻撃手法としては、ソフトウェアの脆弱性を悪用してシステムに侵入する手法とフィッシング詐欺によって人間の心理の脆弱性を狙う手法を組み合わせた巧妙な攻撃が増加し、特に、金銭を目的とした機密情報漏洩被害が増加していることが報

告されている。

また、IPA は、最近の攻撃の傾向として、攻撃を受けたことに気づきにくい巧妙な手口が増加し、ネットワーク管理者やシステム管理者であっても事前の対策なしには気がつくことすらできない脅威が多くなっていると警告している。

表-1 に、Web アプリケーションの主な脆弱性の種類と想定される脅威を示す。

情報セキュリティ白書 2007 年版の「付録 C 2006 年のソフトウェア等の脆弱性関連情報に関する届出状況」^{※4)} によると、2006 年 12 月末までに IPA に届出があった 704 件の Web アプリケーション脆弱性被

●表-1 Web アプリケーションの主な脆弱性と脅威●

脆弱性の種類	想定される脅威
クロスサイトスクリプティング	<ul style="list-style-type: none"> Cookie 情報の漏洩 個人情報の漏洩 データの改竄、消去 なりすまし 本物サイト上への偽情報の表示
インジェクション <ul style="list-style-type: none"> SQL インジェクション コマンドインジェクション LDAP インジェクション XPath インジェクション HTML/XML インジェクション 	<ul style="list-style-type: none"> 情報漏洩 データの改竄、消去 任意コマンドの実行 システムの乗っ取り なりすまし
バッファオーバーフロー	<ul style="list-style-type: none"> データの漏洩 データの改竄、消去 任意コマンドの実行 システムの乗っ取り
クロスサイトリクエストフォージェリ	<ul style="list-style-type: none"> データの改竄、消去
URL へのアクセス制限の不備 <ul style="list-style-type: none"> ディレクトリトラバース ファイルの誤った公開 	<ul style="list-style-type: none"> 個人情報の漏洩 サーバ内ファイルの漏洩 データの改竄、消去
パス名 / 入力パラメーター検査不良	<ul style="list-style-type: none"> データの漏洩
不適切な認証、セッション管理、エラーハンドリング	<ul style="list-style-type: none"> Cookie 情報の漏洩 個人情報の漏洩 データの改竄、消去 なりすまし
HTTP レスポンス分割	<ul style="list-style-type: none"> キャッシュ情報のすり替え
オープンプロキシ	<ul style="list-style-type: none"> 踏み台 中継システムの不正利用
DNS 情報の設定不備	<ul style="list-style-type: none"> ドメイン情報の挿入

害の内訳は、クロスサイトスクリプティング、インジェクション、バッファオーバーフロー脆弱性が約 7 割と大半を占める結果となっている。

表-1 に示す Web アプリケーションの脆弱性の脅威を根本的に解消するには、Web アプリケーションやオペレーティングシステム (OS) の脆弱箇所の修正や適切な動作環境のパラメーター設定を行う必要があるが、修正やパラメーター変更を実施するには、修正方法の検討と修正後の十分なテスト期間の確保、運用中システムの停止が必要となるため、脆弱性の情報を入手してから対処を完了するまでを短期間で行うことは難しい。特に、インターネットに公開されているシステムの場合、24 時間 365 日の稼働が前提となっているため、定期的な保守期間以外に対処することが難しくなっている。

このような事情から、Web アプリケーションやオペレーティングシステム (OS) の修正やパラメーター変更を行うまでの間、何らかの手段で脆弱性の脅威を回避するセキュリティ管理機能が必要になっていた。

現状の IPCOM EX シリーズが提供するアプリケーションレベルのアクセス制御機能やアノマリ型 IPS 機能を使用することで、表-1 に示す Web アプリケーションの脆弱性を突いた攻撃の一部には対処できるものの、十分に對抗できないことが判っており、脆弱性攻撃からシステムを保護するセキュリティ管理機能の早期提供を要望されていた。

一般に、表-1 に示す Web アプリケーションの脆弱性の内、クロスサイトスクリプティング、インジェクション、ディレクトリトラバーサル、コマンドインジェクション、バッファオーバーフローなどの脆弱性攻撃には、特定の通信パターンが存在する。ネットワーク上を流れるパケットをリアルタイムに検査して、特定の通信パターンに一致するトラフィックを検出し、ブロックする手法の一つに「シグネチャー型 IPS」と呼ばれるセキュリティ管理方式がある。

シグネチャー型 IPS は、脆弱性攻撃の通信パターンを「シグネチャー」と呼ばれるパターンリストとして持ち、パターンリストのいずれかに一致するパケットを検出した場合にパケットを遮断、破棄する機能を提供する。

IPCOM EX シリーズが提供しているセキュリティ管理機能にシグネチャー型 IPS 機能を追加することで、右記の 4 種類のセキュリティ制御ブロックが順番に働き、低レイヤーのネットワーク攻撃からアプリケーションレベルの高レイヤーにわたる、システムの正常稼働を脅かす様々なセキュリティ脅威に対抗して、万全な保護

機能を提供することが可能になる。

- ① アノマリ型の IPS 機能 - 異常な形式のパケットやアプリケーションコンテンツを使用したサービス妨害攻撃や不正アクセスを防御する。
- ② アプリケーション・ファイアウォール機能 - 許可されないアクセスやアプリケーションへの要求を防御する。
- ③ シグネチャー型 IPS 機能 - アプリケーションやオペレーティングシステム (OS) の脆弱性を狙った攻撃からシステムを保護する。
- ④ アンチウィルス機能 - ウィルス、ワーム、トロイの木馬などの有害なコンテンツをブロックする。

図-1 に、4 種類のセキュリティ管理機能の制御ブロックが連携して動作することで、様々なセキュリティ脅威を排除して、最終的に、正常なアクセスだけを通わせる様子を示す。

3 課題と対策

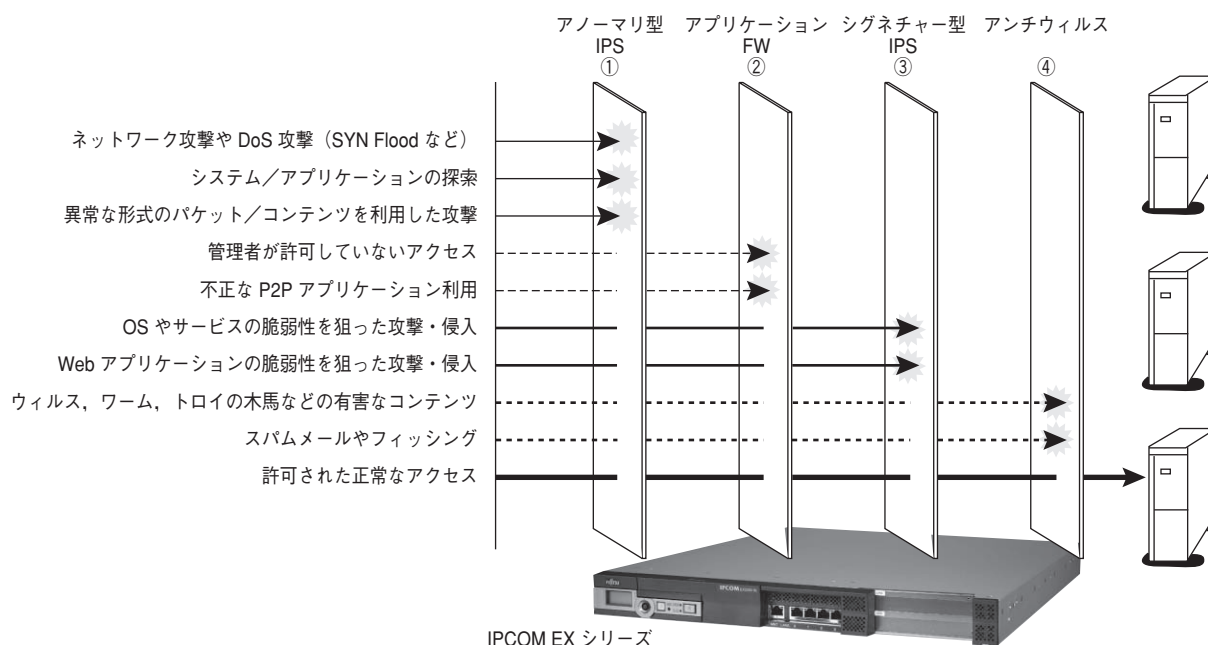
IPCOM EX シリーズにシグネチャー型 IPS 機能を実装するに当たっての課題と対策を示す。

3.1 シグネチャー供給ベンダーの選定

シグネチャー型 IPS 機能は、「シグネチャー」と呼ばれるシステムの脆弱性を狙った侵入や攻撃の通信パターンが記述されたパターンファイルを使用して、侵入・攻撃を検知、防御する。

したがって、脆弱性攻撃に対抗する防御能力は、シグネチャーの正確さと脆弱性が発見されてからシグネチャーが作成、適用されるまでの迅速性に依存する。脆弱性攻撃に対抗するシグネチャーが正確でないと、脆弱性攻撃ではない正常な通信を遮断してしまい、業務に多大な影響を与えてしまう弊害が発生する。この弊害は、シグネチャー型 IPS の「誤検知 (False Positive)」として知られている。また、脆弱性攻撃を検知した場合に、ネットワーク管理者やシステム管理者が運用システムにどのような対処を行うべきかの情報提供も重要になる。

正確なシグネチャーを迅速に作成するには、日々発生、検出される脆弱性情報をワールドワイドに監視して、新たに検出された脆弱性情報にもついで侵入や攻撃の通信パターンを特定し、侵入・攻撃通信パターンを記述したシグネチャーを迅速に作成、検証できなければならない。さらに、作成したシグネチャーを対象装置にタイ



●図-1 セキュリティ管理機能の4層制御ブロック●
(Fig.1-Security management function's control blocks composed of 4 layers)

ムリーに配信することが要求される。

これらの作業は、高い専門性が要求され、専用の監視センターと専任のセキュリティスタッフが必要となるが、短期に実現することは難しい問題であった。

この課題に対して、シグネチャーの作成と配信は自社で行わず、専門のセキュリティスタッフを擁するソフトウェア・ベンダーと協業することを選択した。

シグネチャー供給ソフトウェア・ベンダーは、表-2に示す選定ポイントにもとづいて評価した。

シグネチャー型 IPS 専業ベンダーを中心に、数社のベンダーを選定し、表-2の評価ポイントに沿って評価した結果、(株)セキュアソフトを選択した。

セキュアソフト社は、シグネチャー型 IPS 専用アプリケーション装置「SNIPER IPS シリーズ」を日本国内で販売しており、同装置は、韓国でトップシェアを誇る製品である。

セキュアソフト社は、表-2の評価ポイントをすべて満たしており、特に、誤検知が非常に少ない高品質なシグネチャーが供給できることと、新たな脆弱性に対応したシグネチャーを短期間で公開、配信できる専門スタッフを有していることが選択の大きな理由である。

3.2 高いスループット (検知性能)

シグネチャー型 IPS 機能は、ネットワーク上を流れるすべてのパケットを検査して、正常なパケットだけを

通過させる制御を行う。したがって、一般に、他のネットワーク機器より処理負荷が高く、ネットワーク上のボトルネックポイントになり易い。特に、シグネチャーの数に比例してスループットが低下する。

この問題に対処するために、シグネチャー型 IPS 機能を IPCOM EX シリーズに搭載するに当たり、以下の点を設計上の最重要課題として取り組んだ。

- ① シグネチャーの数が増加してもスループット低下を最小限に留める。
- ② IPCOM EX シリーズが提供する複数のセキュリティ管理機能を同時に動作させた場合のスループット低下を最小限に留める。

個々のパケットに対して、シグネチャーの一つ一つを順番に評価していくと、シグネチャーの数に比例して処理時間が増加してスループットの低下を招く。この解決策として、シグネチャー情報の効率的な階層管理とハッシュ制御方式を採用して、シグネチャーを高速に効率的に検索できるようにした。また、複数のセキュリティ管理機能を同時動作させた場合のスループット低下の課題は、個々のセキュリティ管理機能で共通に行っている個々の検査ロジックを極力集約することで、個々のセキュリティ管理機能が重複した検査を行わないように対処することで解決した。

図-2に、IPCOM EX1200 SC のシグネチャー型 IPS 機能を動作させた場合と動作させなかった場合の

●表-2 協業ベンダーの選定ポイントと要件●

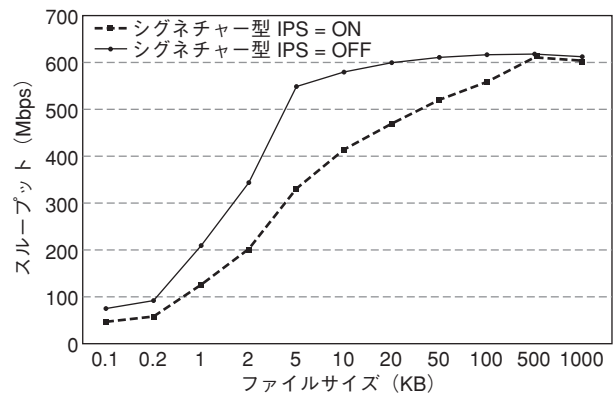
選定ポイント	要件
セキュリティ専門スタッフの能力が優れていること	高いセキュリティ専門能力を有し、脆弱性攻撃手法を正確に理解し、その攻撃の影響度と対策情報を提供できること。
専用の監視センターを有すること	監視センターを有し、ワールドワイドに脆弱性情報を収集する専門スタッフを抱えていること。また、シグネチャーをタイムリーに配信する設備を有していること。
シグネチャーだけを供給できること	IPCOM EX シリーズは、様々なセキュリティ管理機能が組み込まれており、相互に連携して制御することで、高度な独自のセキュリティ機能を提供している。したがって、シグネチャー供給ベンダーの制御エンジンを組み込むのではなく、制御エンジンは自社開発できることが必要であった。
シグネチャーの品質が高いこと	シグネチャー型 IPS 機能の課題の一つに、「誤検知」問題がある。供給シグネチャー数が多くても、誤検知が多ければ、システム管理者の負荷が増加するだけで意味がない。誤検知の少ない品質の高いシグネチャーが供給できることが重要な要件となる。
新たな脆弱性に対応するシグネチャーの供給期間がタイムリー（短期）であること	シグネチャー型 IPS 機能の最重要視点。新たな脆弱性が検出、報告された場合に、その脆弱性に対応するシグネチャーをタイムリーに供給する必要がある。リスクの高い脆弱性に対するシグネチャーは、短期間で提供が求められる。
脆弱性の説明や対処方法などの情報が日本語で提供されること	IPCOM EX シリーズの販売ターゲットは日本国内であるため、脆弱性情報や対処方法等の情報を日本語で提供することが求められる。

スループット比較を示す。

図-2から、シグネチャー型 IPS 機能を動作させた場合、最大 20 数%程度のスループットの劣化に留まっていることが判る。この性能は、他社装置に比べて格段に小さい値であり、IPCOM EX シリーズのシグネチャー型 IPS 性能の高さを示している。

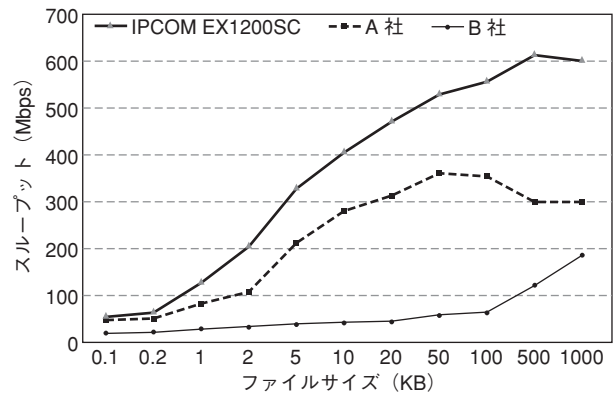
また、図-3に、アノマリ型 IPS 機能、ファイアーウォール機能、シグネチャー型 IPS 機能が同時に動作した場合の他社装置とのスループット比較（当社実測結果）を示す。

図-3から、IPCOM EX シリーズは、他社の同一価格レンジの製品に比べ、非常に高いスループットを達



●図-2 シグネチャー型 IPS 機能の動作有無によるスループット比較●

(Fig.2-Comparison of throughput depending on whether the signature-type IPS function operates)



●図-3 他社装置スループット比較（同一価格レンジ）●

(Fig.3-Comparison of throughput with other manufacturers' devices (in the same price range))

成し、価格性能比が他社製品よりも優れている結果となった。

3.3 セキュリティ診断情報

シグネチャー型 IPS 機能は、導入しただけでは何の意味も無い。システム管理者は、外部からの侵入、攻撃からシステムを保護、維持するために、システムで使用しているソフトウェアやネットワーク機器に影響を与えるセキュリティ脅威が漸次に報告されていないか、常日頃から情報を収集しておくことが重要となる。

シグネチャー型 IPS 機能は、シグネチャーに一致するパケットを検出すると、該当パケットを破棄すると同時に、システム管理者に侵入・攻撃があったことを通知する。システム管理者は、侵入・攻撃が実際に発生したのか、誤検知によるものなのかの判断、さらに、実際に

侵入・攻撃が発生していた場合は、どのシステムが標的になったのか、システムにどのような影響があり、どう対処すべきかの早急な判断が必要になる。

IPCOM EX シリーズにシグネチャー型 IPS 機能を実装するに当たり、システム管理者が判断、分析を行う際に必要な情報は何かの見極めが課題であった。

システム管理者が侵入・攻撃を的確に判断、分析するには、侵入・攻撃と判断された結果情報だけでなく、該当パケット情報も採取しておく必要があると考え、「いつ」、「誰が」、「どこから」、「どこに」、「どのような攻撃」を、「どのようにして」行ったかの詳細なイベントログと侵入・攻撃として検出した実パケットデータをリアルタイムに確実に採取、保存することにした。また、アノマリ型 IPS 機能やファイアーウォール機能のログと時系列に参照できるように、これらの機能のログと同じ形式で保存することにした。

さらに、攻撃統計情報（今日、1 週間、1 ヶ月ごとの攻撃種別、攻撃者や被害者 IP アドレス、検回数、検知データ量など）を採取することで、攻撃の傾向分析、誤検知の判断ができるように対処した。

4 特長

IPCOM EX シリーズのシグネチャー型 IPS 機能の概要と特長を示す。

4.1 IPCOM EX シリーズのシグネチャー型 IPS 機能

表-3 に、IPCOM EX シリーズのシグネチャー型 IPS 機能の提供機能を示す。

IPCOM EX シリーズのシグネチャー型 IPS 機能は、配置形態として、インライン形態（通過型）とパッシブ形態（スイッチの SPAM ポートまたは、タップに接続して利用）の両方に対応できる。また、ブリッジモードとルーティングモードの両方のモードで動作することができるため、あらゆるネットワークに配置できる特長を有する。

防御アクションとして、検知だけのモードと検知および防御のモードを有する。防御を行う場合は、防御時間を指定でき、指定された時間の間、侵入・攻撃パケットを破棄できる。なお、防御アクションは、個々のシグネチャー単位に指定できるため、「誤検知」問題に柔軟に対処できるようになっている。IPCOM EX シリーズのシグネチャー型 IPS 機能は、シグネチャー毎に、

攻撃の説明、攻撃を検出した場合のシステムへの影響と対処方法などの情報を記載したヘルプファイルを提供している。ヘルプファイルは装置に格納されているため、攻撃を受けてネットワークが使用できない状況でも参照できるようにしている。

4.2 真の統合セキュリティ管理システム

(1) 集約された高度なセキュリティ管理機能

IPCOM EX シリーズは、これまでに提供した 3 種類のセキュリティ管理機能に、シグネチャー型 IPS 機能を加え、基本的な 4 種類のセキュリティ管理機能を搭載することで、ネットワーク攻撃やサービス妨害攻撃などのネットワークやサーバを麻痺させる低レイヤーの攻撃から、一見正常なトラフィックに見えるアプリケーションレイヤーの脆弱性を狙った攻撃やウイルス、ワームなどの悪質なコンテンツなどの高レイヤーの攻撃まで、様々なセキュリティ脅威に対抗できる。

さらに、IPCOM EX シリーズは、オプション機能として、暗号通信を行うための IPsec-VPN 機能や SSL アクセラレータ機能、SSL-VPN 機能を搭載している。一般のファイアーウォール装置や UTM (Unified Threat Management : 統合脅威管理) 装置は、暗号通信によるセキュリティ脅威に対抗できないが、IPCOM EX シリーズでは、これらの暗号通信機能を使用することで、暗号通信を復号した後のパケットに対して、4 種類のセキュリティ管理機能が働くため、暗号通信によるセキュリティ脅威からシステムを保護することができる。この連携機能により、特に、ショッピングサイトなどで使用されている SSL 暗号通信による脆弱性攻撃に対する防御が可能になる。

また、最近では、ボットネットワークからの一斉攻撃を受けて、ネットワークが麻痺してしまう被害が増加しているが、IPCOM EX シリーズに搭載されている QoS (帯域) 制御機能を利用することで、悪質なトラフィックによる帯域消費を抑制することができる。

図-4 に、4 種類のセキュリティ管理機能と他の機能の連携イメージを示す。IPCOM EX シリーズは、4 種類のセキュリティ管理機能を中心に、IPsec-VPN 機能、SSL アクセラレータ機能、SSL-VPN 機能、QoS (帯域) 制御機能などの他の機能と密に連携し、多種多様なトラフィックを厳密に評価、制御することで、高度、複雑化するセキュリティ脅威から運用システムを保護できるように設計している。

集約されたセキュリティ管理機能を利用することの

●表-3 提供機能と概要●

機能		概要
配置形態	インライン形態	通過（中継）型形態
	バッシブ形態	スイッチの SPAN ポートやタップに接続する形態
動作形態	ブリッジ	ブリッジ構成で動作する。
	ルーティング	ルーティング構成で動作する。
インラインバイパス		装置故障時に LAN 間を直結して、パケットをスルーする。
シグネチャーに基づいた検知と防御		シグネチャーを使用して、セキュリティ脆弱性を狙った侵入や攻撃の検知と防御が可能。プロトコル脆弱性攻撃、バッファオーバーフロー攻撃、Web CGI 攻撃、バックドア、ワームなどの検知と防御に対応している。
検知ポリシーの作成・編集	セキュリティゾーンの策定（仮想 IPS）	シグネチャー型 IPS 機能を適用するネットワークやホストの集合（＝セキュリティゾーン）を定義することができる。1 台の装置に独立した複数のセキュリティゾーンを定義（＝仮想 IPS）できる。
	シグネチャーの選択と編集	セキュリティゾーンに適用するシグネチャーを選択し、編集し、ゾーンに最適な検知ポリシーの作成を行うことができる。
	シグネチャーのカスタマイズ	シグネチャーの各種パラメーターや有効／無効をチューニングすることができる。
	ユーザー定義のシグネチャーの作成	利用者自身で独自のシグネチャーを作成することができる。
アクション	検知（DETECT）	攻撃検知だけを行い、防御を実行しない。（IDS モード動作）
	破棄（DROP）	攻撃検知と防御を実行する。（IPS モード動作）
シグネチャーの更新	自動更新	スケジュールに従って自動で最新のシグネチャーを取得する。
	手動更新	コマンドを投入することで最新のシグネチャーを取得する。
更新シグネチャーの適用プロセスの選択		自動または手動で取得した最新のシグネチャーの適用方法を選択（自動又は手動）できる。
検知ポリシーのインポートとエクスポート		検知ポリシーを装置外部に移出し、外部で編集後、装置に移入することができる。検知ポリシーは、XML 形式で移入できる。
セキュリティ診断情報	イベントログ	攻撃の検知、攻撃の継続、攻撃の終了イベントを記録、保存する。
	検知パケット	イベントログを記録すると同時に、攻撃と判断した該当パケットのパケットデータを採取して PCAP 形式で保存する。
	攻撃統計情報	長期的な脅威分析、脆弱性問題に対する保守計画の立案時に役立つ攻撃統計情報を採取する。
	攻撃状態情報	現時点の侵入防御に関する状態情報を参照することができる。
通報	シスログ転送	攻撃を検知した場合に、システム管理者に通知する手段として、Syslog 転送、メール送信、SNMP トラップをサポートしている。メール送信では、攻撃検知パケットを添付することもできる。
	メール送信	
	SNMP トラップ	
日本語シグネチャーヘルプ		対象脆弱性攻撃の説明、攻撃を受けた場合の影響、影響を受ける OS やアプリケーション、攻撃に対する対策、処置方法、誤検知の可能性情報、システムへの影響と対策、CVE 識別番号などの日本語情報をシグネチャーごとに HTML 形式ファイルで提供する。

もう一つの利点は、セキュリティ監査が容易に行えることである。不正アクセスや攻撃が検出された場合、影響調査、対策の立案と実行が要求されるが、セキュリティ管理機能が集約されていることで、いつ、どこから、ど

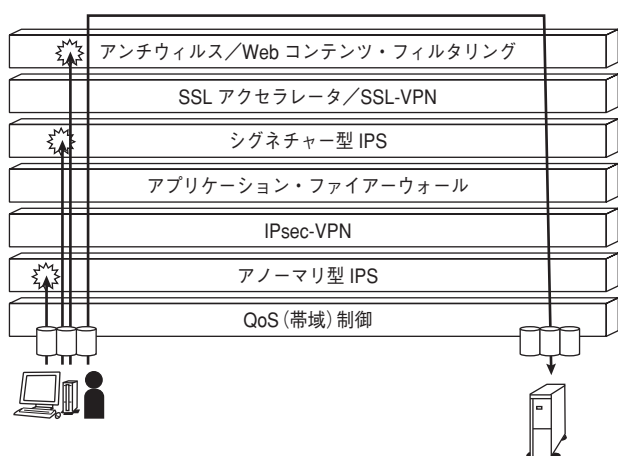
こに、どのような攻撃が、どのように実行されたかの情報が統一された形式で時系列に参照できるため、分析が非常に容易に行える利点があり、運用管理コストの低減につながる。

(2) ネットワークトポロジの簡略化と導入/運用コストの削減

IPCOM EX シリーズは、ネットワークシステムの安全（セキュリティ脅威の排除）、安心（ネットワークシステムの高信頼化）、高速化（サーバアクセラレーション）に要求される機能群を1台の装置で提供する。

例えば、センターネットワークに、高信頼でセキュアな Web アプリケーションシステムを構築する場合、単一機能のネットワーク機器で構築すると、図-5に示すネットワーク機器群が必要になる。さらに、セキュリティ脅威への対抗とネットワーク性能を考慮し、パケットの処理順番を意識したネットワーク設計を行う必要がある。導入コストがかかる。また、複数のネットワーク機器を管理する手間が増え、運用コストが高くなる結果になる。

IPCOM EX シリーズを使用して構築する場合は、



●図-4 集約された統合セキュリティ管理機能●
(Fig.4-Integrated security management function concentrated on a single machine)

必要な機能が1台に集約されているため、導入コストおよび運用コストを大幅に削減できる。また、IPCOM EX に順次機能を追加してシステムを強化する方法で導入することもできる。

サーバアクセス時のレスポンス性能面では、各パケットの処理を1台の装置内で効率的に処理するため、単一機能のネットワーク機器を配置する場合に比べ、総パケット遅延時間が削減され、良好なレスポンス時間が保証される。

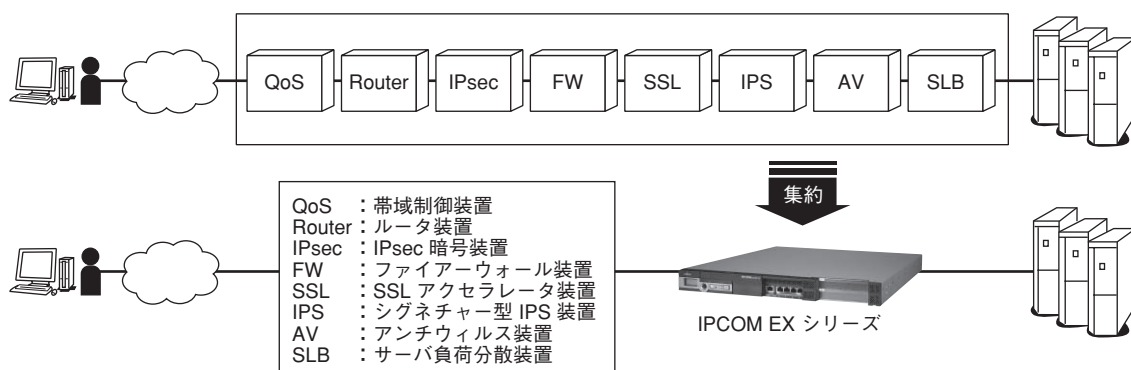
5 むすび

IPCOM EX シリーズにシグネチャー型 IPS 機能を搭載したことで、アプリケーションやオペレーティングシステム（OS）の脆弱性を狙った攻撃に対処できるようになった。しかし、一方で、セキュリティ脅威は日々進化しており、セキュリティ管理の網にかからない正常な通信を装った巧妙な手法が出現しはじめている。

IPCOM EX シリーズは、これらの高度化、複雑化するセキュリティ脅威に対抗できるセキュリティ管理機能を更に充実、強化し、タイムリーに提供していく。

参考文献

- 参1) 新井, 遠藤: 進化した統合型ネットワークサーバ
IPCOM EX シリーズ, *PFU Tech. Rev.*, **18**, 1, pp. 15-22 (2007).
- 参2) 伴野ほか: IPCOM EX シリーズの統合脅威管理 (UTM) 機能, *PFU Tech. Rev.*, **18**, 2, pp. 37-44 (2007).
- 参3) 情報セキュリティ白書 2006 年版
http://www.ipa.go.jp/security/vuln/20060322_ISwhitepaper.html
- 参4) 情報セキュリティ白書 2007 年版
http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html



●図-5 センターネットワークの機器構成●
(Fig.5-Device configuration of the center network)