ディペンダブルな安心安全環境を提供するセキュリティエンジン技術

神谷 聡史・上野 洋史
山田 憲晋・西原 基夫

要　旨

次世代ネットワークでは、トランスポート、ネットワークサーバ、ネットワークサービス、企業網ネットワークにおいてそれぞれ異なるセキュリティ対応が求められます。特に10Gbps以上のブロードバンド環境において高度なセキュリティ機能を実現するためには、ネットワークプロトコル処理、コンテンツチェック処理、大容量通信セッションの同時監視機能などにおけるブレークスルーが必要になります。これらを実現する技術として、セキュリティエンジン技術および付随するAPI/ドライバ技術を開発したので報告します。またAPI/ドライバを活用したシステムソリューションとして、10Gbpsの侵入検知システム(IDS/IPS)と高性能な迷惑メール対策システムを紹介します。

キーワード

●ネットワークセキュリティ　●ハードウェアエンジン

1. はじめに

次世代ネットワークセキュリティにおいては、トラヒック規模、障害時の波及性、秘匿要件などの点で、一般のエンドユーザセキュリティを大きく上回る性能や柔軟性が求められます。特に、ブロードバンド回線適用に向けた高速処理技術や、セキュリティ対処方式の進化に対応できる柔軟性が必要です。これらの要求に対応する技術が、セキュリティエンジン技術です。本稿ではセキュリティエンジン技術とセキュリティエンジンを活用したセキュリティシステムを紹介します。

2. 安心安全なネットワークに向けたセキュリティ

次世代ネットワークの構成と必要なセキュリティ機能の対応を**図1**に示します。次世代ネットワークにおけるセキュリティ対象は、トランスポート網、ネットワークサーバ群、ネットワークサービス、企業ネットワークに分類されます。

①トランスポート網におけるセキュリティ

音声、データなどのトラヒックを転送するトランスポート網において必要とされるセキュリティは、万人の共有リソースであるネットワーク帯域の保護です。DDoS(分散型サービス妨害)攻撃や悪質なコンピュータウイルスの一種であるボッ

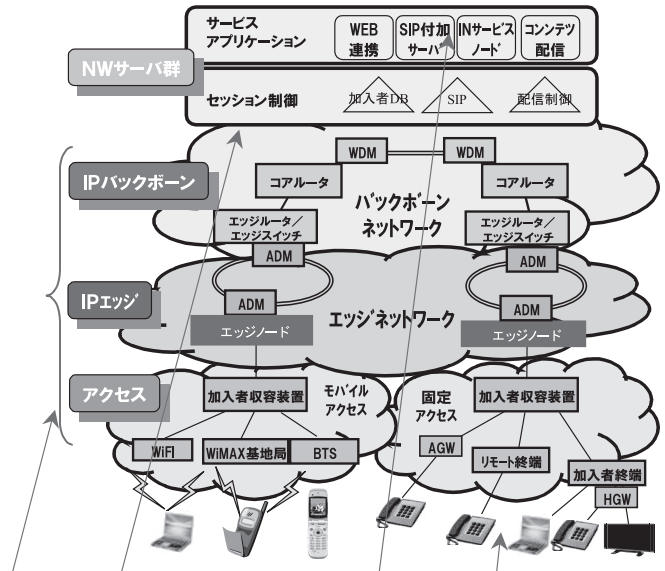

図1　次世代ネットワーク構成と必要なセキュリティ機能

トなどによる異常トラヒックの発生や、一部ユーザのヘビートラヒック(P2P(ピアツーピア)サービス、動画転送などの帯域を占有するアプリケーション)によりネットワークの帯域が占有され、他のユーザトラヒックの転送に支障が発生するのを防ぎます。

②ネットワークサーバ群および企業ネットワークにおけるセキュリティ

次世代ネットワークにおいては、IMS (IP Multimedia Subsystem)を活用したネットワークサービスや、外部のサービスベンダーによる多様なサービス展開が期待されています。本領域においては、サービス提供者・享受者の正当性を保証する認証機能、各種ネットワークサーバの保護(不正アクセス防止・トラヒック流量制限・アクセス制御など)がセキュリティとして必要になります。

③ネットワークサービスに関するセキュリティ

従来の電話・電信・Faxなどのインフラサービスに加え、インターネットの出現により同一IP網の上において多様なサービスの構築が可能になりました。現状の主要キャリアサービスとして、音声、携帯メール、IM(Instant Messenger)などが挙げられます。特に携帯メールは電話に次ぐサービスとなっており、迷惑メール、フィッシング詐欺、メールウイルスに対する防御が社会的な要請になっています。

3. 高性能セキュリティエンジン技術

3.1 実現に向けた課題

第2章に挙げたセキュリティ要件を満たすためには、セキュリティエンジンとして解決すべき以下の課題があります。

(1) 10Gbps超の高速ネットワークプロトコル処理

アプリケーションレベルの検査処理を行うためには、TCPセッションのステートフル監視技術ならびにTCPリアセンブリ技術が要求されます。数100Mbpsのトラヒックにおいてはは CPUの高速化によりソフトウェア処理が可能になりましたが、それを超えるトラヒックに対してはハードウェアエンジン処理が必須です。10Gbps超の大容量処理かつ100万を超える多数TCPセッションを監視するための性能を実現するTCP処理技術の実現が課題となります。

(2) コンテンツチェック処理

アプリケーションレイヤのプロトコル解釈やペイロードデータのコンテンツに対する攻撃パターン文字列比較処理は処理負荷が高く、ハードウェアエンジン処理が有効です。本技術においては、セキュリティ処理に有効なオフロード機能の分析と10Gbps超トラヒックを実現するハードウェア処理に適したアルゴリズム確立が課題です。

(3) ソフトウェアとハードウェアエンジンの連携技術

新規プロトコルの出現や新規の検知手法への対応などを考慮すると、ハードウェアエンジンによるオフロード処理とソフトウェアとの連携機能が重要になります。共通性が高くかつ処理負荷の高い機能をハードウェアエンジンで実現し、それ以外はプロセッサベースで処理できるプラットフォームが必要です。ハードウェアとソフトウェアの間で効率的な連携を行うためには、データコピーやエンジン呼び出しのコストを考慮したプロセッサ連携技術とプログラミングモデルの確立が課題になります。

3.2 セキュリティエンジンの実現

NECではすでに1Gbpsクラスの各種エンジン技術[1)]を開発し製品適用していますが、今回、さらに前記の課題を解決した10Gbps性能のセキュリティエンジン群と、それらを稼働させるプラットフォームを開発しました[2)]。

(1) TCPモニタリングエンジン

上位のアプリケーションプロトコルを識別しつつ10GbpsでのTCPモニタ処理を行うエンジンです(**図2**)。TCPモニタリングエンジンでは平均TCPペイロード長が250Byteのショートパケット条件で10Gbps処理を実現しました。また、セッション開設、切断に対して毎秒70万セッションの開設・切断処理を実現しました。さらに同時処理セッション数は1Mセッションを実現しました。

(2) セッションマネージメントエンジン

セッションマネージメントエンジンでは、10Gbps性能の速度

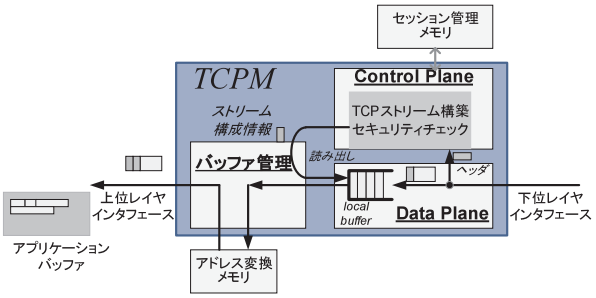

図2 TCPモニタエンジン ブロック概略図

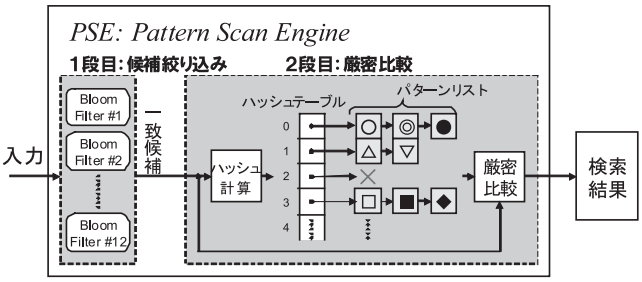

図3　パターンスキャンエンジン ブロック概略図

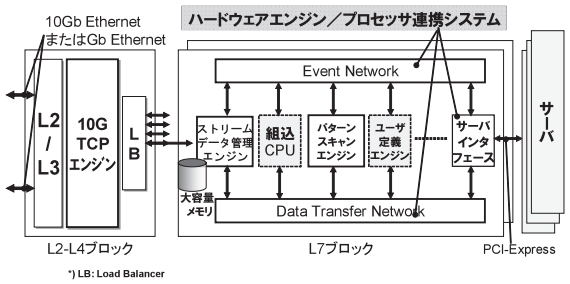

図4　セキュリティエンジンプラットフォーム概略図

でステートフルなTCP/IPセッションおよびUDPフローの管理を実現しました。アクセス制限リスト(Access Control List: ACL)によるパケットフィルタリング機能も搭載しており、本エンジンを使用してファイアウォールが実現できます。

(3) パターンスキャンエンジン

パターンスキャンエンジンは、入力データに対してあらかじめ登録されたキーワード/文字列パターンと比較を行って一致判定を行う機能を備えています(**図3**)。通常のトラヒックモデルにおいてエンジン1基当たり2.5Gbps～4Gbpsの処理性能があり、複数基による10Gbps性能達成を可能としています。

(4) ハードウェアエンジン/プロセッサ連携基盤

前述の複数の各種ハードウェアエンジンとプロセッサの連携を実現するために必要な基盤ソフトウェアとして、高速タスクスイッチング機能とデバイスドライバ群、さらに高速タスクスイッチング機能を補助するハードウェア機構であるイベントコントローラを開発しました。本開発によりソフトウェアからのハードウェア利用機構が実現され、性能面ではソフトウェアタスク処理切り替えにおいて既存OS性能に比べ100倍程度の高速化を図ることができました。

3.3 セキュリティエンジンプラットフォーム

図4に10Gbpsセキュリティエンジンプラットフォームの構成を示します。L2-L4ブロックはL2/L3部と10G TCPエンジン部から構成され、10Gbpsのトラヒック処理能力を有します。L2/L3部はイーサネット終端、IPパケット処理、ファイアウォール処理、セッション管理を行い、10G TCPエンジン部はTCP処理を行います。L7ブロックは、10G TCPエンジン部で構築されたストリームデータをストリーム管理エンジンで収容・管理し、パターンスキャンエンジンで検索処理を実行します。L7ブロックは、装置外部のサーバや組込CPUと連携可能です。また、組込CPUをソフトウェアベースのオフロードエンジンとして使用することも可能です。**写真**は共通プラットフォームカードの外観です。

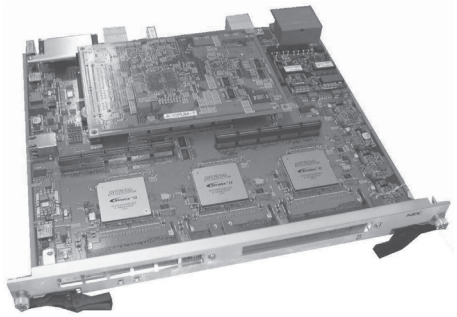

写真　共通プラットフォームカード外観

4. 10Gbps 高速侵入検知システム(IDS/IPS)への適用

アプリケーションレイヤのモニタリングを含むファイアウォールおよび侵入検知システム(Intrusion Detection System: IDS) は、データペイロードのコンテンツチェックを伴うために処理負荷が高く、高速ネットワークにおいてはその処理性能が問題になります。そこでNECではセキュリティエンジンプラットフォームを応用して、10Gbps処理を実現するSnort[3]の高速処理を実現しました。Snortは、マルチレイヤ検査が可能な、オープンソースソフトウェアのIDS の1つで、既知の攻撃パターン文字列(シグネチャ)と入力データを比較することにより侵入検知を行います。また侵入検知機能と通信セッションマネージメントのセッション切断機能を組み合わせることにより、アプリケーションファイアウォールとして動作させることが可能です。

処理の概略図を**図5**に示します。セッションマネージメントエンジン、TCPモニタリングエンジンにより、入力セッションの管理とTCPデータの再構成を行い、L7フィルタ処理部に置かれたパターンスキャンエンジンにより入力トラヒックに対するシグネチャ一致検査を行います。さらに、被疑トラヒックにつ

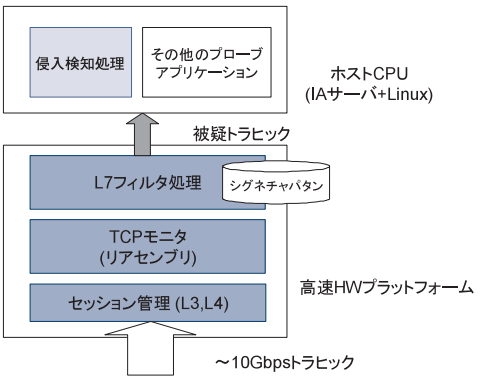

図5　高速IDS処理概略図

いてプロセッサ上のソフトウェアで詳細な検査を行います。ハードウェア性能としてはTCPモニタ部が10Gbps処理対応であり、L7フィルタ部は1カード当たり2.5Gbps～4Gbpsの処理性能を持ち、複数ごとのカード構成により10Gbps処理を実現します。

5. 迷惑メール対策ソリューションへの適用: SLIMIT

SLIMITシリーズ[4]は、ハードウェアエンジンによる高性能処理を特徴とした迷惑メール対策装置であり、帯域制御機能を持つSLIMIT-LとURLフィルタ機能を持つSLIMIT-Cがあります。

図6に示すように、SLIMIT-Lはメールサーバの前段に置かれるメールトラフィック制御装置で、メールの統計情報に基づいてアプリケーションレベルでの規制をかける機能を備えます。TCP処理、セッション単位の帯域規制処理において1Gbps処理の各種エンジン技術を利用することにより、秒間1,000通のメールトランザクションの性能を有しています。また、SLIMIT-Cはメールサーバからの迷惑メール判定要求を処理する装置で、メールペイロードに含まれるURL文字列をブラックリストデータベースと照合するURLフィルタ機能を備えます。ペイロードデータ解析処理、URLデータベース照合処理をエンジン技術で実行することにより、最大秒間5,000通のメールに対する判定処理を低遅延で実現します。

6. おわりに

広範囲なネットワークセキュリティに適用可能なセキュリティエンジンの紹介をしました。セキュリティソリューションの展開に向けては、高性能検知を目的とするセキュリティエンジン以外に、個別セキュリティシステムとの連携や検知データの配信・同期などのシステム技術も必要になります。セキュリティエンジン技術の改善とともに、今後はシステム技術との連携も強化していく所存です。

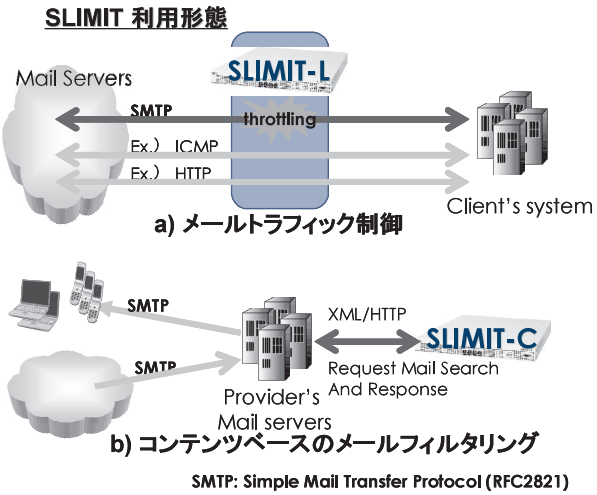

図6　SLIMITの利用形態

本内容の一部は総務省委託研究「次世代バックボーンに関する研究開発」の成果です。

* SnortはSourcefire社の登録商標です。

参考文献

1) Motoo Nishihara et. al., "Broadband Service Gateway Platform for Readily Available and Reliable Business Applications and Services," NEC Journal of Advanced Technology,Vol.1, No.2, Spring 2004.
2) 神谷、他「10Gbps高性能セキュリティエンジンプラットフォームの開発」, 2006年電子情報通信学会総合大会, BS-5-13, 2006-3
3) Snort:http: //www.snort.org/
4) SLIMIT:http: //www.nec-mobilesolutions.com/application/jcontents/slimit/index.html

執筆者プロフィール

神谷 聡史
中央研究所
システムプラットフォーム研究所
主任研究員

上野 洋史
中央研究所
システムプラットフォーム研究所
主任研究員

山田 憲晋
中央研究所
システムプラットフォーム研究所
主任

西原 基夫
中央研究所
システムプラットフォーム研究所
研究部長