ブロードバンド・ユビキタス社会を支えるネットワークセキュリティ技術

加藤　圭　　五十嵐　譲

ネットワークのブロードバンド化に伴い，コアネットワーク上を流れるトラフィックは増大の一途をたどっている。一方で，ユビキタスネットワークの進展により，ネットワーク上のトラフィックの種別も多種多様になってきている。これらのトラフィックは，人々の生活に欠くべからざるものを多様に含み，インターネットのライフラインとしての重要性が増加していることを示している。したがって，何らかの形でこれらのトラフィックの送受信に支障が生じると，社会生活への影響は甚大なものとなる。インターネットへの人為的な攻撃によるセキュリティの脅威は，その最たるものである。2003年2月のSQL/SLAMMERによるインターネットへの攻撃をはじめとして，数々の攻撃による被害が各種機関から報告されている。2005年3月には，携帯電話に感染する初のウィルス「Cabir」が日本にも上陸し，セキュリティの脅威が携帯網にも及んでいることを如実に物語っている。本稿では，来るべきユビキタス社会のセキュリティの脅威を明らかにし，その解決手段としての沖電気のネットワークセキュリティ技術を紹介する。

現状のセキュリティ脅威と対策について

インターネット上におけるセキュリティ脅威に対しては，対策をいくつかのフェーズに分けて実施することが1つの手法として提案されている（参考文献1）。参考文献では，①予兆フェーズ　②インシデント発生・検出フェーズ　③原因箇所切り分けフェーズ　④ネットワーク遮断フェーズ　⑤原因特定　の5つのフェーズに分けた対策を提案している。各フェーズでは，以下のような対策が現在講じられている。

①予兆フェーズ

ポートスキャンなどを含む，攻撃の前段階での調査プロセスを指す。攻撃コード，ツールの情報公開にあわせ，パターンをダウンロードすることで，予兆検知を行うアプライアンス装置などが市場に出始めている。

②インシデント発生・検出フェーズ

実際のインシデントの活動状態を検出するフェーズである。これも①と同様，攻撃パターンのダウンロードにより，インシデントの発生検出を行う装置の開発が進められている。

③原因箇所切り分けフェーズ

②の検出情報を複数箇所から取得することで，原因がどこであるかを分析するフェーズである。これは，トラフィック分析を行う監視システムとの連携で実現されるものが多い。

④ネットワーク遮断フェーズ

③の原因箇所切り分け作業に基づき，しかるべき場所にて，攻撃パターンのトラフィックを絞り込み，あるいは遮断を実施する。一般的にはファイアウォールがその役割をなす。

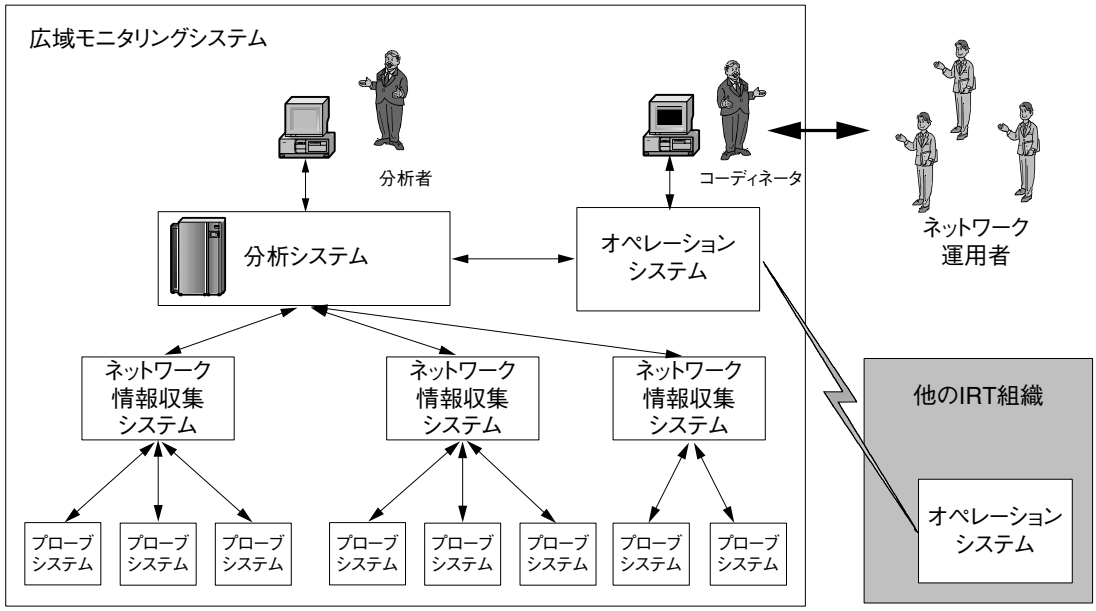
⑤原因特定フェーズ

原因が何であったかを特定するフェーズである。主な対策としては，トレースバック技術を用い，攻撃者を特定するものが提案されている。

委託研究「広域モニタリングシステムに関する基盤技術の研究開発」

前述のように，対策としては5つのフェーズに分けられるが，これらを総合的に実現するためのシステムが望まれている。こうした背景を踏まえ，独立行政法人情報通信研究機構（以下NiCT）より平成16年度「広域モニタリングシステムに関する基盤技術の研究開発」という委託研究が開始された。本研究開発では，沖電気を含め4社が委託研究という形で平成16年度より3年間，研究が進められている。

本研究は，**図1**の通りインターネット上の多地点で，トラフィックログ情報とセキュリティログ情報を収集して，その大規模情報を効率的に統合管理し，多地点・複数レ



IRT：Incident Response Teamの略。セキュリティインシデント（事象）に対応し支援する組織。公的な性格のIRTとして、CERT/CCやJPCERT/CCがある。

図１　広域モニタリングシステム概要

イヤにまたがる分析を行うことで，広域ネットワークに影響を及ぼす異常なインシデントの早期発見を実現する基礎技術を確立することが目的である。また，異常が検出されてからの迅速な対応を促すために，セキュリティオペレーションおよびそのための情報交換を円滑にする基盤システムを開発する。

広域モニタリングシステムは，プローブシステム，情報収集システム，分析システム，オペレーションシステムから構成される。

このうち，沖電気はプローブシステムの一部（超高速トラフィックプローブシステム）及び情報収集システムの一部を担務している。本プローブシステムは，各対策フェーズを実現するにあたり必要不可欠なものである。

沖電気のネットワークセキュリティに対する取り組み

本稿では，広域モニタリングシステムにおける取り組みのうち，超高速トラフィックプローブシステムについて説明する。

超高速トラフィックプローブシステムの開発では，ネットワークに広く設置するプローブシステムの中で，インターネット環境におけるバックボーンあるいはAS（Autonomous System）間での高速大容量トラフィックのモニタリングおよび弁別を行い，セキュリティインシデント検出に有効な情報を収集するシステムを開発する。

サーバやエンドユーザ直近で要求されるようなアプリケーションを意識した高レイヤ処理よりも，ネットワーク層付近での高速トラフィック観測が必要条件となる。高速トラフィックの監視に関して，運用者が随時きめ細かく全ての情報を参照し判断することは不可能であり，データ量の削減と運用のしやすさの観点からトラフィック情報のアグリゲートや簡易な絞り込み手法や手続きが必要となる。すなわち，大容量トラフィックの挙動を監視するための効率的なトラフィックの監視と絞り込み・弁別手法が解決すべき課題である。

加えて，日々進歩するトラフィック分析技術に対応するべく，トラフィック弁別・分析手法の改変や追加が必要に応じて可能となる柔軟なシステムアーキテクチャが必要となる（**図2**）。

このような背景や課題のもとで，超高速トラフィックプローブシステムの開発を実施した。

【研究開発成果】

超高速トラフィックプローブシステムの開発として，システム機能要件の抽出およびシステム概要設計を行い，さらに高速トラフィックプローブ評価システムを構築し，評価を実施した。

本システムでは，高速トラフィックのモニタリングを実現するためにレイヤ4までのフローを識別しながらフローごとに統計情報を持ち，パケット情報を収集するIPパケットエンジン部の開発を行うとともに，これらの収

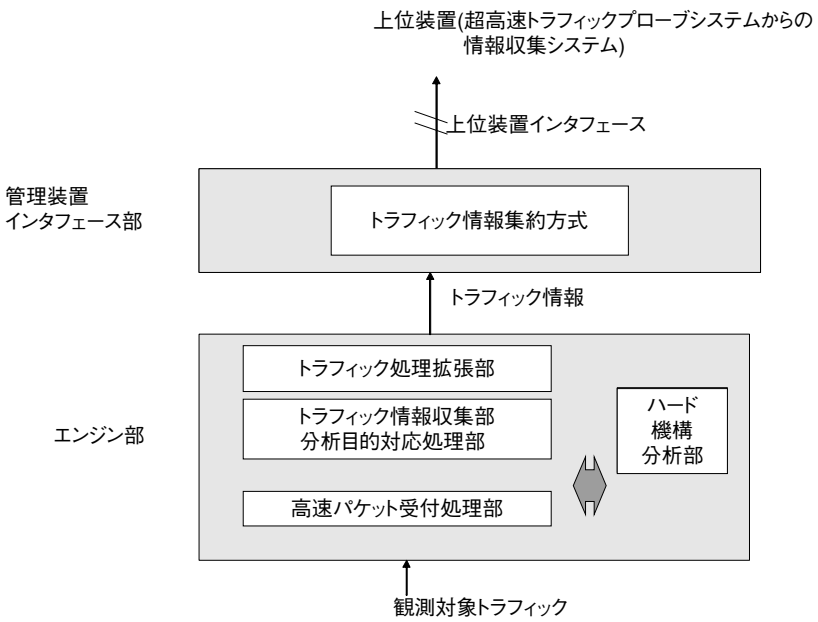


図２　超高速トラフィックプローブシステム概要図

集情報とパケット情報を集約する管理装置インタフェース部の基本設計を行った。

【ハードウェア構成】

10Gbit/sトラフィックを処理する，トラフィック処理モジュールのハードウェア構成を示す。入力された高速トラフィックをCAMを用いたハードウェア検索機能で初期検索を行い，その結果を元にNPU（ネットワークプロセッサ）で継続的なトラフィックの識別と情報収集および後処理を行う。ハードウェアでの検索はあくまで基本的な機能にとどめ，分類・分析のための高度な，かつ将来追加や変更が想定される処理はNPUで実施することで，全体の高速化を図るとともにフレキシブルなシステムとしている（**図3**）。

【トラフィック監視機能】

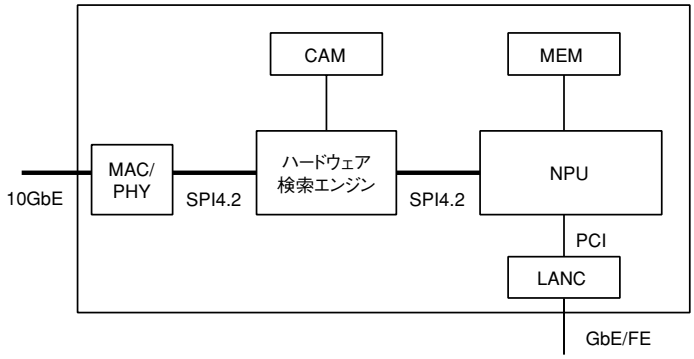
本システムの主要な機能であるトラフィック監視について示す。

機能的にポート毎トラフィック常時監視，ポートとIPアドレス毎トラフィック常時監視，パケットサイズ閾値監視とレイヤ4フロー（サンプリングおよびフロー情報指定）による詳細監視機能を具備する。

CAM（ハード機構）による高速検索とそれを補充するファームウェアによる検索処理を組み合わせ，処理を分担しながらお互いの検索情報をフィードバックし調整する。また，出現するFirstパケットの処理と情報収集目的別のトラフィック処理を段階的に実現することで，高速なトラフィック検索と情報収集を可能とした。また，本処理により，統計情報収集のために必要なメモリ資源が節約可能となる。

トラフィックを観測するために到着したパケット全体に関してデスティネーション-ポートおよびデスティネーションIPアドレスに着目して統計情報を収集する（First Packet処理）。この統計情報から送信先情報に着目したトラフィック情報がどのようになっているかを把握することが可能になる。統計情報を分析することで，トラフィック量やサイズに関しての上位に関するパケットが何であるかを判別し，次検索機能の設定情報を抽出する（宛先レベル統計情報処理）。ここで抽出した設定情報と送信元情報に関しても分類できるように，ソースポート，ソースIPアドレス，プロトコル情報に関しても着目し，かつ高速分析できるようにハード処理（CAM）にて行う。最終的には5 tuplesに関してのトラフィック量やサイズに関する統計情報を収集することが可能となる（5 tuplesサンプリングレベル処理，5 tuples統計情報処理）。

このような手順によって，トラフィック情報は徐々に詳細化されるため，ネットワークに異常が発生した場合などに，保守者は異常トラフィックを抽出・特定するこ



名称	機能概要
NPU、MEM	トラフィック統計情報を分析/収集するネットワークプロセッサとメモリ。
ハードウェア検索エンジン	パケットヘッダから必要なフィールドを抽出したのち、CAMへ照合を行い照合結果をパケットに追加したのちNPUへ送る。送受信はSPI4.2形式で行う
MAC/PHY	10Gb Ethernetからのパケットを受信したのち、エラーチェックを行いSPI4.2形式でハードウェア検索エンジンへ送る
LANC	管理網へのLAN接続を提供する
CAM	Content Addressable Memoryの略。メモリ内に格納されているデータ列と、外部から入力されたデータ列が一致するかの比較を高速に行い、一致した結果を出力するメモリ。

図３　ハードウェア構成図と機能概要

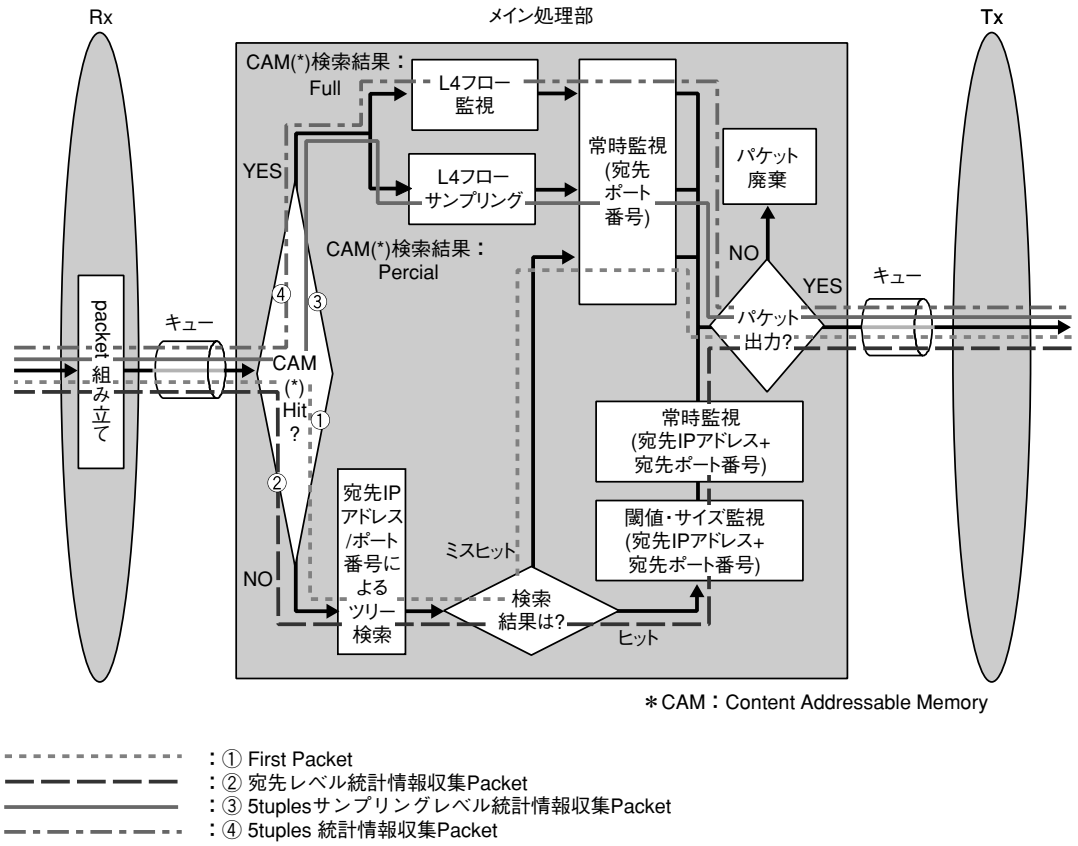


図 4　超高速トラフィックプローブ　トラフィック処理部ブロック構成図

とが可能になる（**図4** ①〜④）。

これらを評価システム上で構築し，IPパケットの観測と基本情報の収集において1Gbit/s超のトラフィック量を遅滞無く扱えることを実証するとともに，分析プログラムの変更が容易なネットワークプロセッサを適用した基本アーキテクチャを確立したことで，将来2.4〜10Gbit/sの高速トラフィックを処理するためのプローブシステムが十分実現可能であるとの見通しを得ることができた。

今後の課題

本稿では，超高速トラフィックプローブのトラフィック処理部について詳細を説明したが，トラフィック情報集約部にて，複数のトラフィック処理部を集約し，上位分析部へ情報を転送することが必要となる。今後，トラフィックが増大する中で，この情報集約部分のスケーラビリティが，市場展開への重要な鍵を握るものであるため，今後の課題として重要である。

ま と め

本年度は，超高速トラフィックプローブ装置の基礎部分となる設計，試作，評価を行った。プローブ評価システムによる高速トラフィック動作の検証を行い，また，要件抽出に基づいた基本機能のシステム設計を実施した。

今後は，2.4〜10Gbit/sのトラフィック観測と分析が可能な装置の開発・実装を行い，10Gbit/s回線への適用を睨んだ評価を行う。また，上位システムとのインタフェース（情報集約部）を実現し，システム化の研究を行う。 ◆◆

■参考文献

1）武智，坂本，加藤，中尾：“広域モニタリングシステムの構築に関する一考察”，SCIS2004，2004年

●筆者紹介

加藤圭：Kei Kato. ネットワークシステムカンパニー ネットワークシステム開発本部 システム開発部
五十嵐譲：Yuzuru Igarashi. ネットワークシステムカンパニー メガキャリアビジネス本部 ソリューションSE第三部 SE第二チームリーダ