社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＳＬＤＭ－129／2007－ＥＭＢ－4（１）
2007／3／15

［招待講演］高速ネットワークにおけるセキュリティ監視の現状と課題

三宅 優†

† （株）KDDI研究所 〒356-8502 埼玉県ふじみ野市大原2-1-15
E-mail: †miyake@kddilabs.jp

あらまし インターネットの普及により、オンラインショッピングやインターネットバンキング等の取引、会社間の取引等、ネットワーク上において様々なサービスやアプリケーションが展開されている。インターネットは社会の重要な基盤となり、その停止やセキュリティ上の問題は、社会を混乱させる要因となっている。しかし、インターネット自体はセキュリティ的な機能がそれほど重要視されずに研究開発が進められ、そのまま利用されることとなったため、セキュリティ上の問題からネットワークの障害や利用者から重要な情報を引き出す詐欺的な行為、情報漏洩等が発生している。そこで、ネットワーク側においてもセキュリティを確保するために監視を強化する試みが進められている。本稿では、高速ネットワークを対象としたセキュリティ監視の現状と課題について述べる。
キーワード 高速ネットワーク、セキュリティ、ネットワーク監視、DoS/DDoS攻撃、攻撃検知

Security monitoring for high speed networks

Yutaka MIYAKE†

† KDDI R&D Laboratories Inc. 2-1-15, Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan
E-mail: †miyake@kddilabs.jp

Abstract Many people use the Internet for on-line shopping, network banking, etc., and such critical applications that handle important information are expanded rapidly. Because the Internet becomes the important social infrastructure, its failure causes confusion in many situations. However, because the Internet had been developed to connect many networks easily, security issues were not so considered at the first stage of the Internet researches. Therefore, network malfunction, phishing, information leaking, etc. have been occurred on the Internet. In order to resolve these problems, researches on network monitoring and control for security have become important. This paper describes the current status and problems of security monitoring for high speed networks.
Key words High speed Network, Security, Network monitoring, DoS/DDoS Attack, Intrusion detection

1. まえがき

インターネットでのサービスやアプリケーションの増加、および、アクセス回線の高速化・多様化等により、インターネット利用者は急激に増加している。日本国内では、2005年末で8529万人が何らかの形でインターネットにアクセスし、その人口普及率は66.8%となっていると報告されている[1]。アクセス回線の高速化、大容量データ転送を前提としたマルチメディア系アプリケーションやコンテンツの増加、利用者数の増加により、インターネットの総トラヒック量も急激に増加しており、国内主要IX（Internet Exchange）のトラヒック総量に占める当該インターネットサービスプロバイダー（ISP）7社のシェアから我が国ブロードバンド契約者のトラヒック総量を試算すると、およそ468.0Gbpsのトラヒックがインターネット上を流通していると試算されている[1]。

トラヒックの増加に伴い、ISPは高速な回線をバックボーンに利用しており、拠点間で10Gbpsの速度を持つ回線を複数本引くことも珍しくは無くなっている。このような状況下で、ネットワーク監視によるセキュリティ対策が困難になってきている。回線の高速化により、解析の対象となるデータが急激に増え、従来の解析手法では処理が滞ることになる。また、対象となるデータ量が増えることにより、重要な情報を見落とす可能性も高くなる。さらに、近年は攻撃手法が巧妙化しており、セキュリティの観点からの監視が従来と比較して困難になってきている。

一方、インターネットの技術に詳しくない、または、興味がないネットワーク利用者が増加し、セキュリティ対策が十分でない端末や、セキュリティに関わる情報に乏しい利用者が増加してきており、このような人々を対象とした犯罪が増加している。ネットワークが危険なものであるとの認識が広まることに

より、利用者の減少やサービス／アプリケーションの利用が控えられることも予想されており、通信事業者やサービス提供者としても安全・安心なネットワーク環境を提供することが重要な課題となっている。また、インターネット自体が重要な社会インフラの１つとなっており、ネットワークが停止すると社会的な活動に大きな影響を与えるようになった。これらを背景に、高速なネットワークを対象としたセキュリティ対策のための監視技術の研究が行われるとともに、事業者間の連携による取り組みも進められている。本稿では、高速なネットワークを対象として、そのセキュリティ監視に関わる課題や取り組み等を解説する。

2. インターネットとセキュリティ

インターネットは、ネットワークを相互接続して自律的に動作することを主目的として研究が開始されており、この研究成果が基盤となって一般の人々に利用されるようになってきた。そのため、研究初期の段階ではセキュリティ面からの検討は後回しとなってきた側面があり、既存の電話網等のネットワークと比較してセキュリティ的に弱い面があると言われている。

ネットワークを前提とした攻撃として、世界で最初のワームは、ゼロックス社パロアルトリサーチセンターで作成されたネットワークインストールプログラムであると言われている。これは、ネットワーク上に接続された 100 台以上のコンピュータにプログラムを効率的にロードすることを目的としていた。しかし、作成したプログラムにバグがあり、ネットワーク上のコンピュータが停止する事態となった。これにより、ネットワーク経由で多くのコンピュータに対して被害を発生させることが可能になることが実証された。これは、1979 年頃の出来事である。

インターネットで最初に影響を与えたワームは、1988 年の Morris ワームである。これは、メール送受信用プログラムである sendmail のデバッグコマンドや fingerd のバッファオーバフローを利用して次々と感染するプログラムであり、インターネットの機能が麻痺した。これにより、多くの人々にワームの危険性が認識されるとともに、セキュリティ対策の重要性が高まってきた。しかし、逆にインターネットやコンピュータの脆弱性が知れ渡ることにもなり、ここから、ウイルスやワーム等のセキュリティ上問題となるプログラムが数多く作られることとなった。

1980 年後半から 1990 年代後半にかけての期間は、数多くのウイルスやワームが作られてきたが、そのほとんどは、感染を楽しむ、または、被害者を混乱させるという愉快犯的なものが多かった。しかし、インターネット上で多くのサービスやアプリケーションが利用できるようになり、オンラインバンキング、ネットショッピング等の金銭のやりとりを伴うサービスが増加すると、利用者のパスワードやクレジットカード番号等を盗み出して金銭的な収入を得る犯罪的な傾向が強い攻撃が急激に増加してきた。また、これらの活動が徐々に表に出にくくなってきており、不正なソフトウェアに感染していたとしても、利用者が気がつきにくくなっている。

これまでにも、ウイルス等の不正なソフトウェアの感染防止策や、インターネット経由の攻撃を防ぐための仕組みは次々と提供されてきたが、新たな攻撃方法の出現や利用者の拡大によるセキュリティ対策が弱い端末の増加により、被害は拡大している。

3. 近年のセキュリティ上の脅威

新しい攻撃手法が次々と開発され、セキュリティ上の脅威は年々変化している。本節では、近年特に問題となっているセキュリティ上の脅威について述べる。

3.1 DoS/DDoS 攻撃

DoS (Denial of Services) 攻撃は、連続してパケットを送ることにより、受信側のサーバが提供するサービスを停止させたり、ネットワーク回線の帯域を消費することにより他の利用者の通信速度を低下させる攻撃である。DDoS (Distributed DoS) 攻撃は、複数の攻撃者が１つのターゲットに対してパケットを送る場合を指す。

アクセス回線の高速化により、一般家庭の利用者が大量にパケットを送出することが可能となり、DoS 攻撃は以前に比べて簡単に引き起こせるようになった。この攻撃により、ルータ等の通信機器に対する障害も発生しているとともに、著名なオンラインショッピングや検索サイト、掲示板等でアクセスがしにくくなる現象も多発している。

3.2 スパムメール、フィッシング

いわゆる迷惑メールであるスパムメールは、インターネット上の電子メールの 2/3 を超え、一日あたり数十億通が送られていると言われている。これにより、スパムメール自身がメールの送受信に関わる帯域の多くを利用することになり、ネットワークに対する負荷の一因となっている。また、メールを中継するサーバにとっても、スパムメールの送受信により増強する必要に迫られている。

スパムメールは、ネットワーク設備に影響を与えるだけではなく、不正請求サイトへの誘導や、パスワードや個人情報の収集を目的としたフィッシングサイトへの誘導といった手段にも用いられており、利用者に対する金銭的な被害も発生している。このような犯罪行為は、利用者側の対策に対応して手段を変更しているため、いたちごっこの様相を呈している。

3.3 マルウェア（ウイルス、ワーム、スパイウェア等）

パソコンの利用者に対して被害を与えることを目的としたソフトウェアは、一般的にマルウェア（悪意あるソフトウェア）と呼ばれている。前述のように、以前のマルウェアは、感染の広がりや利用者へのダメージ（ファイルの消去、OS の破壊、ファイルの配布（情報漏洩）、等）が目的のものが多かったが、近年は、金銭奪取等を目的とした犯罪傾向の強いものが増えている。そのため、パスワードやクレジットカード番号等の個人情報をを盗むスパイウェアや、悪意ある第３者に遠隔操作によりコンピュータが利用されてしまうボットプログラムが多くなってきている。また、このようなマルウェアは、いわゆるウイルス検知ソフトウェアより検出・削除されてきたが、元のプログラムに対してウイルス検知エンジンで検知できないように

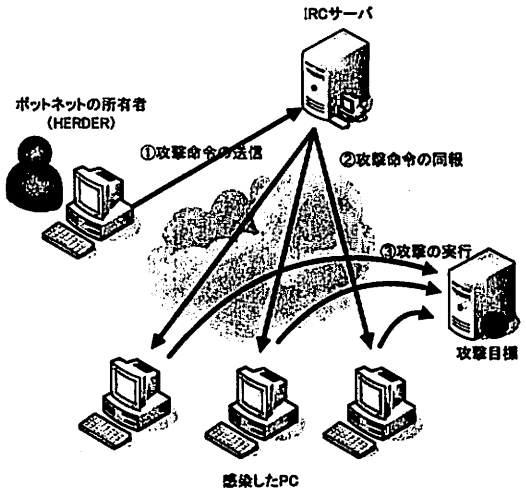

図 1 ボットネットワークによる攻撃手順
Fig. 1 Attacking procedures using bot network

変更したプログラム（亜種）が氾濫するとともに、感染する毎にプログラムの形状を変化させて、マルウェアの特徴との比較によるパターンマッチング方式の検出方法では検知されにくくするものも出現している。さらに、感染しても発症しない、または、潜伏期間が長いマルウェアも増加しており、マルウェアの検出が困難になってきている。

3.4 ボットネット

ネットワーク上で攻撃や侵入行為を行う場合には、その行為の実行者が特定されないために、ターゲットとなるホストとは別のコンピュータに侵入し、そこから攻撃・侵入行為が行われることが多い。このような発信源を特定しにくくするために使用されるコンピュータは「踏み台」と呼ばれ、インターネット上に数多く存在している。

2002 年頃より、このようなマルウェアに感染して外部からの制御が可能となるコンピュータを数万台規模で操作可能とするボットネットが増加してきた。ボットネットは、Herder と呼ばれるボットネットの所有者が IRC サーバ等に命令を書き込むと、その命令を読み込んだ感染したコンピュータが命令に従って様々な行動を起こす。（図 1）行動としては、特定のサーバに対する DoS/DDoS 攻撃、スパムメールの送信、感染者の行動把握（個人情報の収集）、フィッシングサイトの開設等がある。

Telecom-ISAC と JPCERT/CC が共同で実施した実態調査において、2005 年 4 月の時点で日本国内だけでネットワーク利用者の 2〜2.5%がボットに感染していると推測されており、これは、40〜50 万台に相当している。多くの利用者が自分のコンピュータが感染していることを気がつかずにネットワークを利用しており、これらのコンピュータによりスパムメールの発信特定がより困難な状況にある。また、ボットネットワークを時間貸しするビジネスがいわゆる裏社会で存在しており、ボットネットの構築、スパムメールの送信、フィッシングによる個人情報収集、ワンクリック詐欺、等の一連の活動が組織化されて行われている。

4. 高速ネットワークを対象としたセキュリティ監視の研究

本節では、特に高速なネットワークを対象としてセキュリティ監視を行うための研究について紹介を行う。

4.1 ストリーミングアルゴリズムを利用した Superspreader の検出

高速なネットワークのトラヒックを解析するためにストリーミングアルゴリズムを利用した研究が行われている。文献 [2] では、別々の接続先に大量にアクセスする Superspreader を検出するために、メモリの消費量を低くして高速なネットワークに対応したストリーミングアルゴリズムを提案している。Superspreader は、ウイルスやワームの感染源となっている可能性があり、検出により感染者や感染の広がりを把握できることになる。

侵入検知システム（IDS: Intrusion Detection System）等によるシグネチャベースの検出ではパケット単位で攻撃の有無を判断するため、パケットを蓄積して解析する必要は無かった。しかし、Superspreader のようなネットワーク内のある挙動を検出するには、パケット単位での処理は難しく、複数のパケットから抽出したデータを比較・解析して検出を行う必要がある。高速ネットワークでは、処理すべきパケット量が膨大になることから、パケットを蓄積してからまとめて解析する手法では、メモリ資源や処理能力を大幅に消費してしまう。ストリーミングアルゴリズムを利用することにより、高速なネットワークの監視で大量のトラヒックデータを処理する場合でも、実用的な時間内に目的となる事象を発見することが可能となっている。

4.2 DoS/DDoS 攻撃検知

DoS/DDoS 攻撃を検知する場合、バックボーン回線の監視では末端で影響がある攻撃がトラヒック量全体に影響しにくくなるため発見しにくくなり、アクセス回線付近の監視では、監視装置が多くなることと、トラヒックの変動が激しくなることから攻撃と通常のトラヒックの区別が難しくなるという問題がある。KDDI 研究所では、この問題に対処するために、高速バックボーン回線で DoS/DDoS 攻撃を検知可能とするシステムを開発した [3]。

本システムでは、10Gbps の回線に対応するために、インタフェースのパケット破棄率を考慮したサンプリングを行っている。DoS/DDoS 攻撃の検知に関しては、全てのトラヒックの内容を確認する必要が無く、特に通信量が多いパケットを把握すればよいため、サンプリングレートが適切であれば問題がない。回線から収集したパケットは、IP ヘッダ情報から動的にグループ分けが行われ、各グループ単位でトラヒックの変化を把握して攻撃の検知を行う。図 2 は、トラヒックが各グループに分類されて推移する様子を示している。トラヒックをグループ化することにより、全体の推移からでは発見が困難なトラヒックの変化を発見し、DoS/DDoS 攻撃の判定が可能となっている。攻撃発生から検知までの時間を短くする必要があり、IP アドレスやポート番号、プロトコルの種類による適切なサイズで

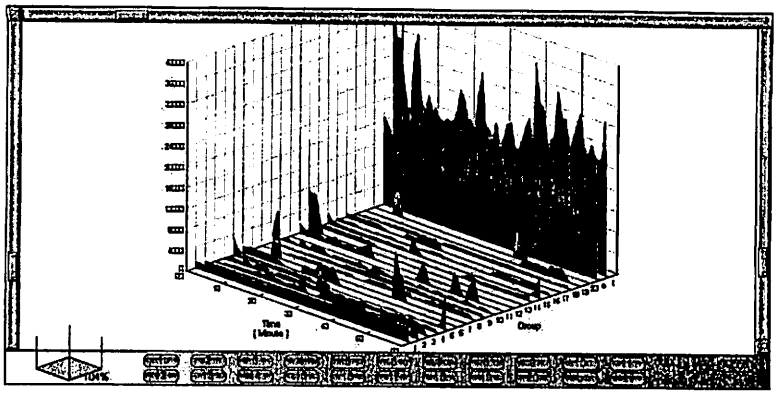

図 2 DoS/DDoS 攻撃検知システムにおけるグループ化されたトラヒックごとの通信量の推移
Fig. 2 Behavior of each grouped traffic in DoS/DDoS attack detection system

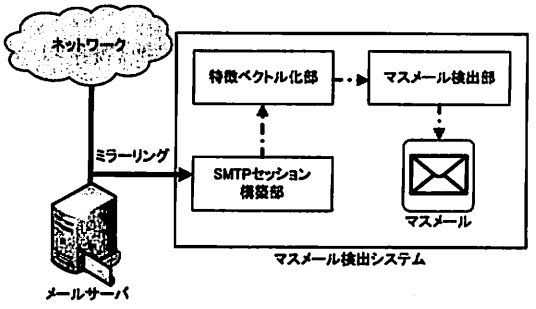

図 3 マスメール検知システムの構成
Fig. 3 Architecture of mass mail detection system

のグループ化を、ネットワークの速度に適応させて行うことが重要となっている。

4.3 スパムフィルター

文献[4]では、高速ネットワークを対象としたスパムメールのフィルタリング対策を提案している。一般的なスパムメールフィルターは、メールの内容やヘッダ情報からスパムメールの判定を行うものがあるが、これらは利用者側での適用を前提としており、高速回線における大規模なメールサーバへの適用には必ずしも適していない。そこで、メールの内容を特徴ベクトル化してハッシュデータベースに格納し、特徴ベクトル集合(メールの内容)が90%類似しているものが100件以上存在するものをマスメールと判断し、スパムメールの候補としている。すなわち、内容的に類似のメールが大量に送られている場合を検出する。図3に検出システムの構成を示す。この手法により、約12,500通/秒の処理速度でマスメールを検出することが確認された。この手法では、メールマガジンやメーリングリストのメール等もマスメール判定されてしまうが、ホワイトリストにより対応可能としている。

4.4 広域セキュリティ監視

インターネット上の攻撃やウイルス/ワーム感染の拡大により、ネットワークに障害が発生する事件がこれまでに何度も発生してきた。インターネットは社会的基盤として広く利用されており、ネットワーク停止に伴う影響度が急激に高まりつつある中で、インターネットでのセキュリティに関わる監視を強化する動きがある。そこで、ネットワーク上の多くのポイントに監視ポイントを設けて情報を収集、解析するとともに、それらの情報を統合して、広域でのセキュリティ上の挙動を把握するシステムの検討が進められている[5]。

図4は、広域でセキュリティを監視する場合の構成例である。各地のNOC (Network Operation Center) に設置された監視装置である攻撃検知エージェント、および、情報収集用のおとり網においてトラヒックの解析が行われ、解析結果がSOC (Security Operation Center) にあるネットワーク全体の状況を解析する統合解析マネージャに送られる。統合解析マネージャでは、各地から送られてきた情報をさらに解析し、ネットワークの異常の発生やその広がり具合を検出する。また、攻撃発生源等の追跡も行われることになる。データの解析においては、大量の情報から的確に異常を検知するために、適切な処理能力と処理速度を持つ解析方法が求められる[6]。

4.5 ハードウェアを利用したモニタリングシステム

ネットワークの高速化により、IDS等のパケットのペイロードをチェックするアプリケーションの対応が困難となってきている。そこで、パケットのペイロードチェックをハードウェア処理で行うことを目的とした研究が行われている。

文献[7]では、ウイルスチェックをFPGA (Field Programmable Gate Array) を用いて行う方法を提案している。FPGAにウイルス検知を行うためのパターンマッチング回路を実装し、パターンマッチングに使用するシグネチャ情報からマッチングロジックのHDLコードを生成して、最新のウイルス情報に対応したFPGAの再構成が行えるようになっている。パターンマッチング回路のスループットは10Gbps以上であることが確認されたとしており、高速ネットワークでのすべてのパケットを対象としたリアルタイム検出が期待される。

また、[8]では、侵入防止システム (IPS: Intrusion Prevention System) で使われることを想定したFPGAのアクセラレータを試作している。IPSは、攻撃を検知するIDSに攻撃を防御する機能を追加したものであり、検知能力とともに、攻撃

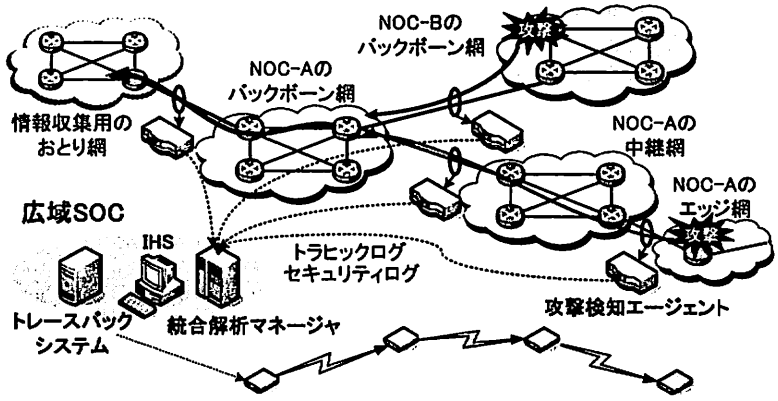

図 4　広域セキュリティ監視システムの構成例

Fig. 4　Example framework of wide area security monitoring system

パケットのみの高速フィルタリング機能が要求される。処理能力を向上させるために、キャッシュを管理するためのメモリ量を 2MB の SRAM とする小さいサイズで実現し、評価において 480Mbps で処理することが確認されている。ただし、この性能は実装においてバグが混入したために低くなっており、パケットサイズの平均が 80 バイト以上であれば、1Gbps の回線（処理的には双方向で 2Gbps）をフルレートで処理可能としている。

5. 高速ネットワークにおけるセキュリティ監視と組み込み技術

本節では、著者の私見として、高速ネットワークのセキュリティ監視における組み込み技術活用の要件について述べる。

5.1 高速回線への対応

これまでに述べてきたように、バックボーン回線、アクセス回線とも急激に回線速度が増加するとともに、そのトラヒックも増えている。このような状況で、サンプリングによるセキュリティ監視では十分な情報が得られない監視対象も存在し、1Gbps や 10Gbps の回線速度に対応したシステムの開発が求められている。そのため、セキュリティ監視を目的とした特別なネットワークインタフェースが必要とされ、そのための研究開発も行われている。また、ネットワークインタフェース自体で高速化処理が可能となったとしても、キャプチャしたパケットをすべてハードディスク等の記憶装置に蓄積し、CPU により処理することは困難であると考えられるため、セキュリティ監視を目的としたインタフェースではインタフェース上である程度の解析処理を行い、その結果に基づいてデータの蓄積やホスト計算機上での CPU の処理を行えることとする能力が必要とされると考えられる。

5.2 複雑化する処理の高速実行

ネットワーク上での攻撃は、既存の攻撃検知システムやウイルス検知システムによる検出を回避し、さらに、利用者に気づかれないような方法により行われるようになってきているため、より高度な検出方法が必要とされてきている。パソコンで使用されている各種ウイルス検知ソフトウェアも、攻撃の特徴を含むパターンを利用して検出する方法から、ウイルスの行動パターンを推論して検知する手法も併用されるようになっており、より複雑な処理が行われている。高速ネットワークでのセキュリティ監視においても、攻撃の検出や情報の収集において、パケット単位の単純な処理だけでは対応できなくなると考えられ、通信のセッション単位の処理や、過去に受信したトラヒック情報を反映したデータの解析処理が可能となる仕組みが必要になると考えられる。

5.3 ハードウェア処理に対応したアルゴリズムの開発

高速ネットワークにおけるセキュリティ監視、セキュリティ対策に関しては、特定のホストへの攻撃を検知する「侵入検知システム（IDS: Intrusion Detection System）」、トラヒック情報全体を監視することよりネットワーク上での挙動から問題を発見する「トラヒック解析による異常検知、攻撃検知」、検出した攻撃のブロックや問題があるサイトへのアクセス制御等を実現する「高速フィルタリング」等があるが、高速化に対応して少ないメモリ容量で連続的にパケットを処理することにより、これらの仕組みを実現するためのアルゴリズムが提案されてきた。これまでのアルゴリズムは、主にコンピュータ上でプログラムにより処理させることを念頭に置いて開発されてきたが、ハードウェアにより処理を行う場合には、ハードウェアに適したアルゴリズムや実装方法があると考えられる。より高速化したネットワーク、および、複雑化する各種の処理に対してハードウェアによる高速な実行が必要とされており、その対応が求められる。

6. ま と め

本稿では、高速ネットワークに対応したセキュリティ監視の現状と課題について述べた。ネットワークの高速化と攻撃の複雑化により、セキュリティ的な面からのネットワーク監視は困難となっており、処理の高速化や効率化が求められている。これまでに、プログラムでの処理を前提として高速なネットワークでのセキュリティ監視を行う方法が提案されており、今後も、

このような研究開発が進められていく必要がある。また、処理の高速化のためには、ハードウェア化による処理の高速化と、ハードウェアに適した処理方式、アルゴリズムの検討も重要である。

ネットワークのトラヒックのかなりの割合で攻撃や侵入を目的としたパケットややspamメール等で占められており、利用者への負担となっているとともに、通信機器、サービス提供機器への負担も大きくなっている。このような攻撃や不必要なメール等が送られないような仕組みを早期に確立する必要もあるが、不正な行動もセキュリティ対策を回避するような手法を次々と展開しており、ネットワーク監視における行動把握とその対応は、今後さらに重要になってくると考えられる。そのためにも、高速なネットワーク下で適切にセキュリティ監視をできる仕組みを確立することが早急な課題であると言える。

文　献

[1] 情報通信白書、総務省、2005.

[2] Shobha Venkataraman, Dawn Song, Phil Gibbons, and Avrim Blum, New Streaming Algorithms for Superspreader Detection, Network and Distributed Systems Security Symposium, 2005.

[3] 山田明、三宅優、竹森敬祐、田中俊昭、属性指向帰納によるネットワークログの特徴抽出と異常検知、情報処理学会論文誌、Vol.47-No.8、2006.

[4] Kenichi Yoshida, Fuminori Adachi, Takashi Washio, Hiroshi Motoda, Teruaki Homma, Akihiro Nakashima, Hiromitsu Fujikawa, and Katsuyuki Yamazaki, Density-based spam detector, 電子情報通信学会誌（D）, Vol.E87-D, 2004.

[5] 竹森敬祐、中尾康二、広域セキュリティ監視技術について、電子情報通信学会誌、Vol.89、No.4、2006.

[6] 竹森敬祐、三宅優、中尾康二、菅谷史昭、笹瀬巌、Security Operation Center のための IDS ログ分析支援システム、電子情報通信学会論文誌（A）、vol.J87-A、No.6、2004.

[7] 石田由香里、飯島洋祐、高橋栄一、古谷立美、樋口哲也、FPGA を用いたウイルスチェックシステムの構築と評価、情学技法、RECONF2006-45(2006-11)、2006.

[8] Nicholas Weaver, Vern Paxson, and Jose Gonzalez, The Shunt: An FPGA-Based Accelerator for Network Intrusion Prevention, Proc. of FPGA '07, 2007.