大規模ネットワークセキュリティの確保に向けた研究開発

福田尚弘*　清水　弘　（松下電工株式会社）
箱田貴久　神尾政和　（安川情報システム株式会社）
井上文範　鈴木彩子　（NTT アドバンステクノロジ株式会社）
塚本克治　（工学院大学）

*fukuda@trc.mew.co.jp

あらまし

より安全性や信頼性の高い大規模ネットワークシステムを構築するために、セキュリティ侵害への対処方法や再発防止などの対策を行うことを目的としたセキュリティ運用の仕組みの研究開発は不可欠である。本論文ではセキュリティ侵害の例としてサービス拒否(DoS/DDoS)攻撃を取り上げ、これまでの調査・検討状況を報告する。具体的には、開発中の発信源の探査システム、ログの収集・分析システム、および以上のシステムを検証するための大規模検証用ネットワークシステムについて、これまで行ってきた調査・検討状況を報告する。

１　はじめに

インターネットを利用した情報通信システムは社会のインフラストラクチャとなっているが、最近の不正アクセス件数の増加などに見られるように、システムのセキュリティ問題が極めて重要になってきている。電子政府や電子自治体（LGWAN）[1][2][3]等の公共システム、インターネットプロバイダ、データセンタ、大企業、病院、学校等の大規模ネットワークシステムにおいては、不正アクセスを防御するなんらかの技術がすでに導入されている。しかし、これらのシステムでは発信源探査や法的根拠を持つログ収集解析の機能が不十分であり、これらの機能を持つ仕組みやシステムの研究開発が急務となっている。

このような背景から、通信・放送機構（TAO）より、「大規模ネットワークセキュリティの確保に向けた研究開発」をテーマとしたインフラストラクチャ・セキュリティに関する受託研究(期間：平成 14 年度～16 年度)の公募が行われ、今回、松下電工、工学院大学、安川情報システムおよび NTT アドバンステクノロジからなる 3 社 1 大学が受託した。

本研究開発では分散化・階層化された様々なネットワーク機器等の情報の集中的な管理と不正データの発信源探査を基盤とする統合的なセキュリティ運用の仕組みを研究開発し、大規模な実験ネットワーク環境により、その実効性を検証する。

２　課題と目標

情報通信システムへの攻撃や被害の実態は必ずしも明らかではない。企業にとって被害にあうことは、恥ずべき事態と考えられ、また信用を低下させる懸念があるため、被害が公表されることは少なく、その実態は捕捉しにくいのが現状である。

CERT（Computer Security Incident Team）によると、インシデントと脆弱性の数の推移は表１のようになっている[4]。これをみると、脆弱性報告数とインシデント数は関連性をもって著しく増加していると思われる。

表 1　脆弱性とインシデントの増加

	1998	1999	2000	2001	2002	2003
インシデント(件)	3734	9859	21756	52658	92094	42586
脆弱性(件)	262	417	1090	2437	4129	959

また、頻度と被害額については母数が少ないが CSI-FBI の調査がある（図１、図２）[5]。

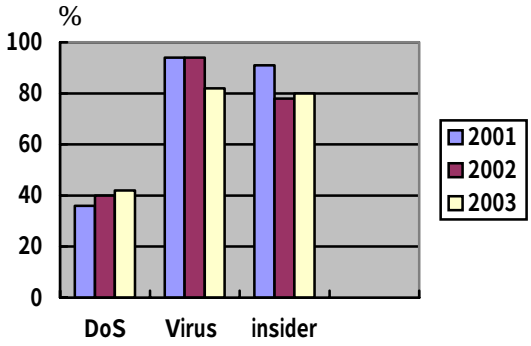

図１　被害件数
（重複解答ありの比率）

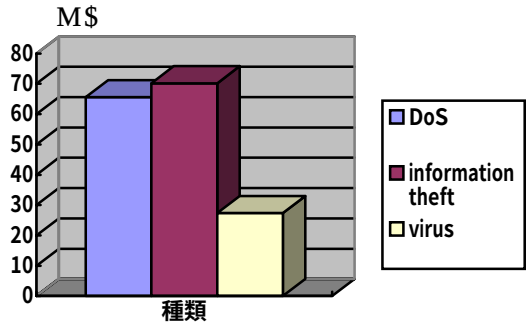

図２　被害額

攻撃数だけをみると DoS 攻撃の比率はそれほど高くないが、被害金額でみるとその比率は高いことがわかる。また、DoS 攻撃は、ネットワークシステム、ノードの設計、仕様、性能等に深く依存する。他の攻撃と異なり、システムの脆弱部分（システムのバグや、管理上の不備）を修復することで防御できるものではない。DoS 攻撃は、ネットワークを構築する上で、不正アクセスの中で最も対処が困難な課題のひとつである[3]。また、近年の不正アクセスにおいて DoS 攻撃は単なるサービス妨害に止まらず、ウイルスやワームとの連携によって対象のネットワークや OS やワクチンのアップデートサーバや企業のプロキシサーバを麻痺させ、復旧を遅らせるだけでなく、ウイルスやワームの感染や発症のための時間稼ぎにも利用されている[6]。

我々は、このような観点から今後も増加するであろう DoS 攻撃対策を最も重要な課題と考え、このような不正アクセスに対する対策技術として、下記の課題と目標値を設定した。

(1) 不正アクセスの探査技術

ネットワークの内部からの不正アクセス（IP アドレス詐称を含む）の場合にはエンドノードまで、また外部からの不正アクセスの場合には踏み台ホストのレベルまでを、誤り率 5%以内で 2 分以内に発信源を探査できること。ここで、誤り率は、「間違った探査結果」を得る「探査の失敗」を含むとする。

(2) 様々な機器のログ管理技術

分散・階層化された複数のネットワーク機器を制御してアクセスログ情報を収集し、その情報を解析して異常状態を検出する一連の処理を 1 分以内に完了すること。

(3) 大規模な検証用ネットワークの構築技術

大規模な分散化・階層化ネットワークのモデルとして LGWAN を考え、数千規模のサーバを接続する様々なネットワーク機器等で構成した大規模実験ネットワークの構築と実証実験を行う。すなわち、当該ネットワークの内、外部から擬似的な不正アクセス（IP アドレス詐称を含む）を発生させ、当該ネットワーク環境をフィールドとして実効性を検証する。

３　不正アクセスの発信源探査技術

本章では発信源探査（トレースバック）技術に注目し、現在提案されているトレースバック方式の現状、DoS/DDoS 攻撃の分類と探査方法、探査精度向上技術および発信源探査システムの設計と実装について述べる。

３．１　発信源探査技術の現状

ここでは、現段階での技術動向を把握するために現状の発信源探査方式[6]の調査結果について述べる。
トレースバック方式は次のように大別される。

(1)　Input　debugging を利用する方式（リンクトレースバック方式）

ルータのデバッグ機能を利用する。被害者（victim）は攻撃を受けた時点で、パケット群を分析し、プロトコル種別やポート番号などの特徴を抽出して、管理者に通知する。通知を受けたネットワーク管理者は、ルータの出力ポートでフィルタを設定して、パケットの入力ポートを特定する。入力ポート情報から、隣接ルータを特定する。これを繰り返して、発信源を特定する。この Input　debugging 方式は、攻撃ツールの発達によってパケットの特徴抽出が難しくなりつつある、複数の管理主体（ISP）にわたって隣接ルータへのアクセスを繰り返すことが難しいという問題がある。

(2)　逆探知パケットを使用する方式（ICMP トレースバック方式）

ルータが、逆探知のための情報として ICMP（Internet Control Message Protocol）パケットを用いて通知する方式である。ICMP パケットには経路情報として、攻撃を経由したルータ自身およびその前後のルータの IP アドレスや MAC アドレスが含まれる。DoS 攻撃によって被害者が多数のパケットを受信した場合､それらと並行して受け取った ICMP パケットの内容から、攻撃パケットが通過したリンクやインタフェース名を特定する。

この方式には、ルータに付加する機能が軽くて済むという利点がある。また、PKI 技術を用いて ICMP パケットを認証して、発信源探査パケットの偽造攻撃を防止できる。一方、追跡する側のファイアウォールに ICMP パケットを通過させる設定をしておく必要があり、また、１つの攻撃サイトから送信するパケット数が少ない場合には、発信源を特定できない可能性が有る。現在 IETF（Internet Engineer Task Force）において、iTrace という名称で標準化が進められている。

（3）ある確率でパケットにマークをつける方式（IP マーキング方式）

逆探知のための情報を IPv4 ヘッダ内の Identification フィールドに入れる方式で､いくつかの方式が提案されている。ここでは代表的な次の 2 つの方式について述べる。

①　Savage 他が提案している方式[7]

最初に提案されたマーキング方式で、隣接する 2 つのルータの IP アドレスの組（Rs、Re）によってリンクを表現し､これをいくつかに分割して IP ヘッダの Identification フィールドに入れる。隣接する 2 つのルータの IP アドレスの排他的論理和を簡潔に表現したものをエッジ ID と呼ぶ。エッジ ID からルータの IP アドレスを復元するためには、個々のエッジ ID について観測点からのホップ数がわかっていればよい。

②　Song 他が提案している方式[8]

Savage の方式を改良して、ルータの IP アドレスのハッシュ値の排他的論理和を計算する。ハッシュ値からルータの IP アドレスを復元しなくてはならないので、上流のルータのマップ情報が必要になる。

IP マーキング方式には、ICMP トレースバック方式と同様にルータに付加する機能が軽くて済むという利点がある。一方、1 つの攻撃サイトから送信するパケット数が少ない場合には、発信源を特定できない可能性がある。また、IP アドレスのハッシュ部分を偽造して、発信源を撹乱する攻撃も論文として報告されている[9]。

(4) パケットのダイジェストを利用する方式（Hash トレースバック方式）

IP ヘッダの中で、経路中で不変な部分とペイロードの先頭 8 バイトについて、k 個の独立なハッシュ関数を適用した結果を 2n ビットのビットマップとして保持する。ビットマップは一定の時間間隔でゼロクリアされ、そのときに期間と期間中に使用したハッシュ関数を一緒にダイジェストテーブルに保管する。

大きな記憶容量や高いハッシュ処理能力などが要求されるため、他方式よりもコスト面で不利になる可能性があるが、この方式には、攻撃パケットが 1 個さえあれば、発信源を特定できるという利点がある[10]。

表 2 にこれらのトレースバック方式を比較した結果を示す。

表 2　主なトレースバック方式の比較

	管理のオーバーヘッド	ネットワーク負荷	ルータの負荷	攻撃後の追跡性	必要なパケット数
リンクトレースバック方式	中	多	多	×	多
ICMP トレースバック方式	少	少	少	○	多
IP マーキング方式	少	少	少	○	中
Hash トレースバック方式	多	少	多	○	少（1 個）

3．2　DoS/DDoS 攻撃の調査分類

(1) DoS/DDoS 攻撃のパターン

DoS/DDoS 攻撃のパターンを表 3 に示す。

DoS(Denial of Service)攻撃は、単一のパスでの攻撃である。DoS 攻撃は、攻撃者から見ると、十分な負荷がかけられない、追跡され経路をたどられる恐れがあるという欠点がある。そこで、攻撃拠点を分散することが考えられた。それが分散 DoS 攻撃(DDoS、Distributed Denial of Service)である。また、DDoS 攻撃にもいくつかの手法が存在する。

表 3　DoS/DDoS 攻撃のパターン

攻撃のパターン	内　容
DoS 攻撃	単一のパスでの攻撃。
直接攻撃 DDoS	ハンドラとエージェント間、エージェントと victim 間の通信が共に直接通信の DoS 攻撃。
間接 DDoS	ハンドラとエージェント間を間接通信にしたものである。IRC(Internet Relay Chat)を利用するのが典型的な方法である。
反射攻撃 (reflector attack)	エージェントと victim の間にリフレクタを設定する。エージェントからリフレクタに向けて、送信先が victim のパケットを送信する。多数のリフレクタから victim に向けて応答パケットを送信する。

(2) DoS/DDoS 攻撃の仕組み

表４に、DoS/DDoS 攻撃の仕組みを、起動方法と特徴について整理した結果を示す。表５に、起動方法の概要を示す[11]。

表4　DoS/DDoS 攻撃の仕組み

特徴 ＼ 起動方法	直接性			走査方式					コード伝播機構		
	直接	間接		ランダム	ヒットリスト	トポロジ	置換	ローカルサブネット	セントラル	バックチェイニング	自律
		Master-agent	Agent-victim								
手動	○	－	－	○	○	○	○	○	－	－	－
準自動	○	○	－	○	○	○	○	○	○	○	○
自動	－	○	○	○	○	○	○	○	○	○	○

○：該当あり、　－：該当分類なし

表5　起動方法の概要

方式	内容
手動	現在はほとんど使われない。 遠隔計算機の弱点を走査し、それらを中に入り込み、攻撃のコードをインストールし、攻撃を開始するコマンドを出すという一連の作業を手動で行う。
準自動	準自動攻撃では、DDoS ネットワークはハンドラ(master)とエージェント(slave または daemon、zombie)からなる。攻撃者はハンドラやエージェントとなるマシンを走査(scan)し、それらのマシンに損傷を与え、攻撃コードをインストールするのに自動的 script(automated　script)を使う。そして、攻撃者はハンドラを利用し、攻撃タイプと victim のアドレスを設定し、エージェントに攻撃開始のコマンドを送る。これを受けてエージェントはパケットを victim に送る。
自動攻撃	自動 DDoS 攻撃はさらに攻撃フェーズを自動化するので、攻撃者とエージェント・マシンの通信も必要でなくなる。攻撃を仕掛けるタイミング、攻撃タイプ、攻撃時間と victim のアドレスは attack　code の中に事前にプログラムされている。

(3) DoS/DDoS 攻撃の経路

DoS 攻撃は比較的近いネットワークから手動の攻撃であり、時間も攻撃源を探査しにくくするために数分程度と短く、また DDoS 攻撃はワームやウイルスの発症機能によって引き起こされるため、比較的遠いネットワークから長時間の攻撃を受けるという報告がある[12]。

表６に、攻撃の経路と TTL(Time To Live)、RTT(Round-trip Time)の値との関係を示す。

表６　攻撃の経路と TTL、RTT の値との関係

攻撃の経路	TTL の値	RTT の値	トラフィックの大きさ	攻撃時間
DoS 攻撃	大きい	小さい(例：最大 120ms)	小さい	短い(数分)
DDoS 攻撃	小さい	大きい(例：最大 3000ms)	大きい	長い

３．３　DoS/DDoS 攻撃の探査手法

3.2 (3)で述べたとおり、TTL、RTT、トラフィック量、攻撃時間の特徴（図３)から、DoS/DDoS 攻

撃を判断し、それぞれの攻撃にあわせた追跡の手法が考えられる。

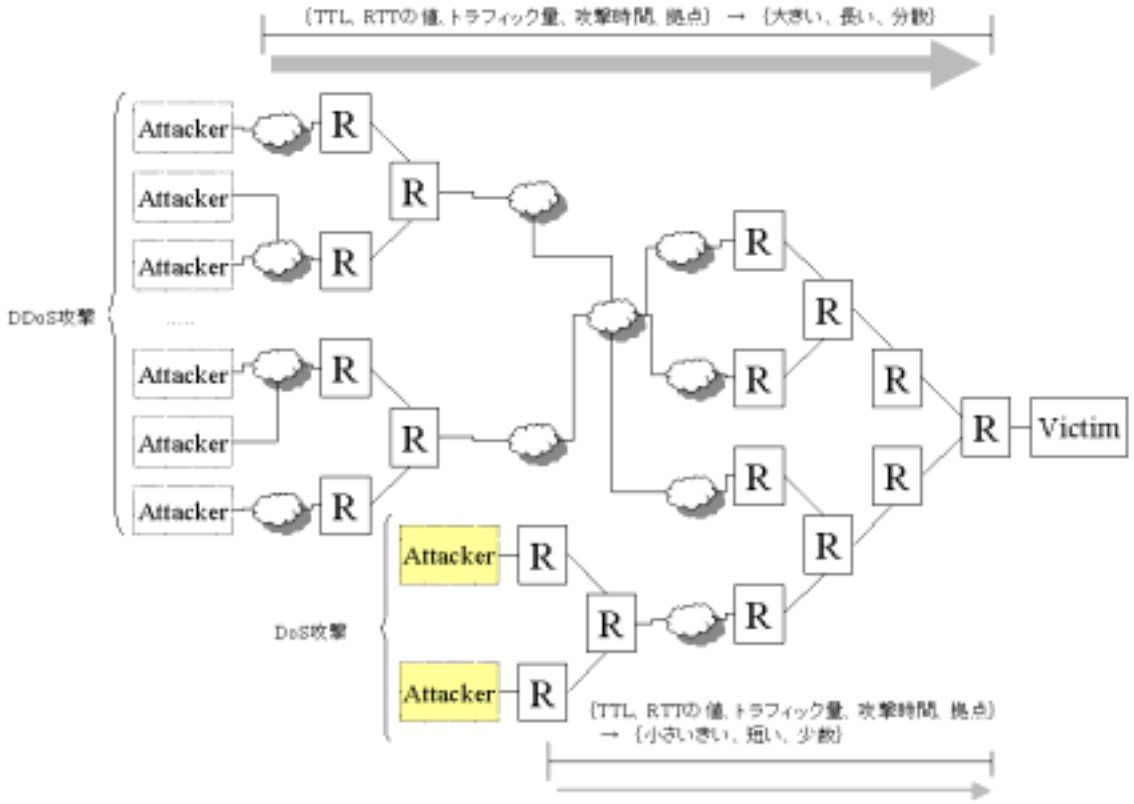

図3　DoS/DDoS 攻撃の特徴

ここでは、ICMP トレースバック(iTrace)方式に絞って、DoS、DDoS を分類し、追跡する方法を検討した結果を表７に示す[13]。

表７　ICMP 方式による DoS、DDoS 攻撃の探査手法

DoS 攻撃の場合	ICMP パケットの TTL 値およびルータまでの RTT 値が比較的小さく、攻撃のトラフィック量も比較的少なく、また攻撃時間も短い場合で拠点数が少ない場合、DoS 攻撃と判断する。 この場合、比較的短時間の ICMP パケットの収集により追跡結果の判断をおこなう事ができる。攻撃者（attacker）に近いルータまでのリンク情報が早期に確立する。なお、各ルータの確率の設定を小さくすることでより検出速度を向上させることができる。
DDoS 攻撃の場合	ICMP パケットの TTL 値およびルータまでの RTT 値が大きく、攻撃のトラフィック量も膨大で、また攻撃時間も長く拠点数も分散する場合、DDoS 攻撃と判断する。 この場合、誤検知率を抑える目的と、エンド側までのリンク情報の収集を十分行うために長時間の ICMP パケットの収集により追跡結果の判断を行わないといけない。

特に、DDoS の場合、どの程度のトラフィックでどのように対処を行っていくかの閾値（パラメータ等）の決定が今後の検討課題であり、検証実験を通して最適な閾値を明らかにする予定である。

３．４　探査精度向上技術

前節の探査の基本情報の付加情報を用いてその発信源探査の精度を向上できないかを検討した。ここでは、付加情報としてディレクトリ情報（DNS、LDAP）、位置情報（地図、GPS）、ネットワークトポロジーやトラフィックの状態、時間情報等を取上げ、トレースバック情報と連携させることを想定した。

表８に、付加情報の評価結果を示す。

表8 付加情報の評価結果

項目	必要性	内 容
①時刻情報 ・検出時刻 ・到着時刻	高	不正アクセスが行われた時刻。トレース技術において証拠性および原因の解析には欠かせない項目である。時刻設定は統一されていることが必須。
②トポロジ情報 ・ネットワークのルートマップ	中	静的ネットワークであればネットワークマップは重要となる。トレースバックシステムの方式によってはネットワークのルートマップを取得できればトレースバック結果が十分得られない場合でも情報を補完することが可能。
③トラフィック情報 ・トラフィック量・種類・状態	中	トレースバックシステムの方式に依存。トラフィックの状態が不正アクセスの検知やシステム検知能力に影響する。この情報によってトレースバック結果の補完が可能。
④イベント情報 ・障害情報 ・他リンク情報等	中	トレースバックシステムの方式、実装、イベント内容に依存。障害情報、不正アクセスの情報（アドレス偽造の通知等）、他のトレースバックシステムからのリンク情報のなど。相手の実装（ラップトップパソコン等）まで把握できれば経験的推測によりトレースバック結果を補足できる。
⑤物理的位置情報 ・住所、場所 ・地図、ＧＰＳ情報等	中～低	位置情報が判るため場合によって迅速な判断または対応が可能になる。相手が想定外の場所からのアクセス等、検知判断の材料として利用すれば効果がある。
⑥ディレクトリ情報 ・組織名、管理者名 ・地域、電話番号等	中～低	ここでのディレクトリ情報は機器管理者の属性情報とする。情報は必ず得られるとは限らない、また得られても対策・対応できるとは限らない。逆にこの情報からオフラインでの対応の方法が決定される。想定外の情報の場合など検知判断の材料として利用すれば効果がある。

３．５　発信源探査システムの設計と実装

本研究開発では、現時点で公開されている実装が存在しない ICMP トレースバック方式について実装した。本方式に関しては、IETF(Internet Engineer Task Force)において iTrace として標準化活動が行われているが、まだ詳細な仕様が固まっていない。（現状ではこの方式はインターネットドラフトの段階である:ietf-draft-itrace-04.txt）

ここでは発信源探査システムの設計と実装を行った内容について述べる。

(1) 探査システムの構成

ICMP トレースバック基礎部分構築のための構成要素を以下の構成とする。構成要素は、発信源探査パケットである ICMP トレースバックパケットを発生させる Generator、Generator によって発生した ICMP トレースバックパケットを収集する Collector、Collector によって収集した探査データを表示・保存する Viewer の 3 つの構成要素からなるシステムとした（表９、図４）。

表9　機能実装に必要な構成要素

No.	構成要素	内容
①	Generator	ネットワークを構成する各ルータに追加実装される発信源探査パケットを発生させる機能を持つ。ルータを通過するパケットをある確率（デフォルトは 2 万分の１）でサンプリングし、そのパケットの内容、およびそのパケットがルータを通過した経路情報、時刻、その他の情報を ICMP パケットのフィールドに記述し、そのパケットのあて先に対して送信する。
②	Collector	攻撃が想定されるネットワークセグメント（IDS が配置される DMZ 等）に配置し、Generator によって送信された ICMP トレースバックパケットを収集し、収集した情報を Viewer に提供する。
③	Viewer	Collector と同一システム内に存在し、Collector が収集・保存した情報を発信源探査のために有効な形式に情報を加工し表示、保存する機能。

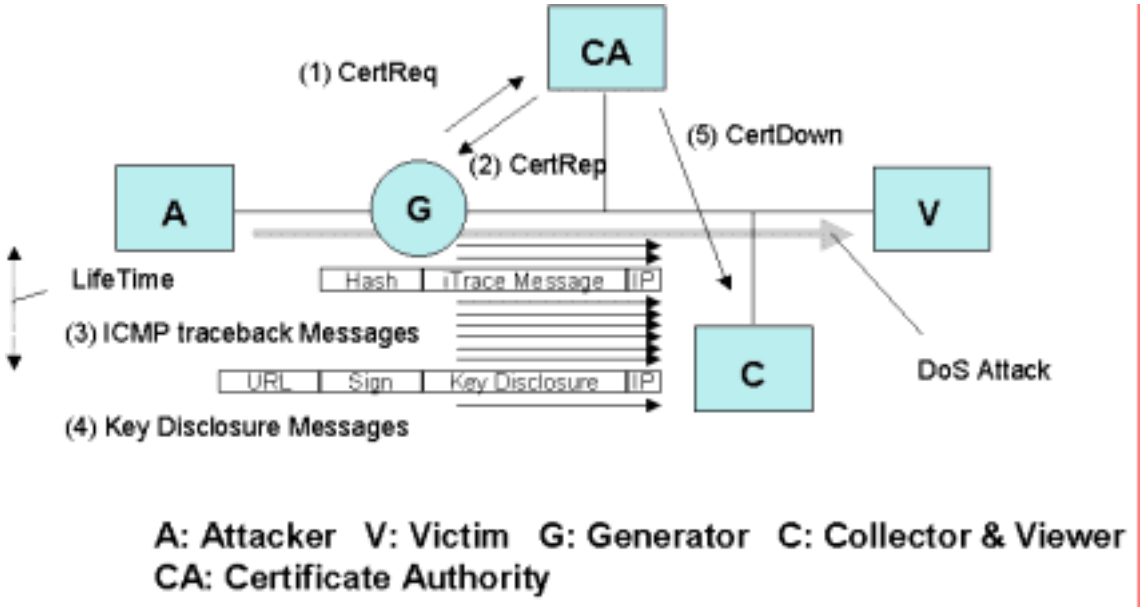

図4　システム構成

図４において、A は攻撃者（attacker)、V は犠牲者（victim)、G は ICMP パケットの Generator、C は ICMP パケットの Collector、CA は認証局および証明書のレポジトリを示す。

「A」の攻撃者より「V」の犠牲者宛に DoS 攻撃が実行された場合、攻撃経路上の各ルータ「G」に ICMP トレースバック（iTrace）の Generator 機構が存在すると、各ルータ上の Generator「G」は設定された確率（デフォルトでは 2 万分の１の確率）で犠牲者（V）宛に発信源探査のための追跡パケットである ICMP トレースバックメッセージを送信する。

犠牲者（V）側のネットワークセグメント上に配置された Collector「C」は、各ルータからの ICMP トレースバックメッセージを複数受信し、各ルータのリンク情報を結合することで、攻撃者側のルータまでの経路を探査（特定）することができる。

完全な探査（ルータまでの完全な経路の特定）のためには、経路上の全ての Generator が ICMP トレースバックを送信（全発火）する必要がある。そのためには、攻撃がバースト的に連続した状態、かつ一定以上のパケット量が必要となる。リンク情報としては、主に各ルータのフォワードリンクおよびバックワードリンク（IP アドレスと MAC アドレスのペア）を用いる。

ICMP トレースバックでは、追跡情報は ICMP トレースバックパケットで運ばれる、つまり通常の通信路と同じ経路を介して流れるため、攻撃者がその探査システムに気づき、ICMP トレースバックパケットを偽造する恐れがある。このため、PKI（パブリック・キー・インフラストラクチャ）の技術

を用いて ICMP トレースバックパケット自体を認証することとした。

なお、鍵公開リスト（Key Disclosure List）自体の偽造も考えられることから、鍵公開リストを搬送するパケットに電子署名（Sign）を行い、その証明書をパケットに添付する代わりに証明書(Certificate)のレポジトリを URL で指示する方式をとっている。Collector「C」は鍵公開リストを含むパケットの到着までハッシュ認証された複数の ICMP トレースバックパケットを保持し、到着後、そのパケットの URL より証明書を取得し、電子署名（Sign）を確認した後、保持していた複数の ICMP トレースバックパケットの認証を行う。その前準備として Generator「G」は証明書の発行作業（CertReq/CertRep）を事前に行い、Generator の証明書を認証局（CA：Certificate Authority）またはレポジトリに置く作業を必要とする。

今回の実装では証明書の発行作業（CertReq/CertRep）はオフライン処理としている。また簡便のため証明書の失効の確認（CRL の確認）は行っていない。なお、Viewer は Collector と同じ位置に存在し、Collector の提供するリンク情報を表示または保存する機能がある。

リフレクタを用いた複数の拠点からの同一犠牲者（V）への DDoS 攻撃の場合、Viewer は複数の Generator（G）を表示する。

(2) 実用化に向けての今後の課題

今回、設計と実装を行うことにより、次のような課題が明らかになった。

①IETF のドラフトに記載されている提案レベルの仕様はあくまで必要最低限の情報にすぎない。また、現状の様々なネットワーク環境（NAT、2 重化、高速ネットワークなど）に対応した仕様とはいえない部分も存在する。
②トレースバックパケットが攻撃者側にも通知される可能性がある。
③最適なトレースバックパケットの発生確率を明らかにする必要がある。
④イングレスフィルタリングとの有効性を対比する必要がある。
⑤PKI を用いる仕様では偽造した認証つきのトレースバックパケット自体が、PKI の計算が遅いことを利用したコレクタへの DoS 攻撃になるおそれがある。

４．様々な機器のログ管理技術

４．１ ログ調査の現状

不正アクセスの調査（異常検出・解析）ではサーバ、ネットワーク機器などのノードが出力したログからの異常と考えられる記録やパターンを探索することが基本的手段となる。しかし、ログの調査及びその扱いに関して多くの問題がある。

ネットワークに接続されたノードは Unix をはじめとする多くのコンピュータで利用されている syslog[14]、Microsoft 社の WindowsNT 系列の OS（Operating System）で使用される Event Log、ルータやスイッチングハブなどのネットワーク機器で利用されることの多い SNMP（Simple Network Management Protocol）[15]情報、アプリケーションごとのアクセスログ、IDS(Intrusion Detection System)のアラートなど様々なログによって状態通知や異常の通知を行う。これらは個別にログを出力するだけか同種の仕組みの間でのみ連携できる。このため、不正アクセスなどの異常が発見された場合、管理者は複数のノードを個別に調査しなければならない。加えて、不正アクセスは様々なセキュリティホールを利用し、複数のコンピュータを踏み台とするためノード横断的、ネットワーク横断的な調査が必要となり、ネットワーク規模の拡大に伴って調査の複雑さも爆発的に増大する結果となる。

そして、様々な形式のログをノード横断的に調査し、異常の原因を発見するためには高度な技術が必要となる。したがって、次の問題、人間-機械インタフェースの問題が起こる。syslog をはじめとしてほとんどのログ情報はテキストベースの出力であり調査しやすいものではない。

この状況を改善するため、いくつかの製品で統計情報を用いるなど視覚的に判りやすく表示する手段は提供されているが、最終的には高度な判断ができる管理者の人手に頼らざるをえないというのが現状である。

４．２ ログの集中管理手法

様々なログのうち特に広く利用されている、syslog、Event Log および SNMP についてログ収集、管理機能に関する調査を行った結果を以下に述べる。

(1) syslog（The BSD syslog protocol）

syslog では device、relay、collector（トレースバックで使用する collector と区別するため以降"collector†"と表記）といった仕組みが定義されておりネットワークを通してログを収集することが考慮されている。syslog でログを収集する場合、図５のように device から collector にログを送信する。また、relay は device と collector†の間を中継する。collector†は device から送信されたログをすべて集積する。

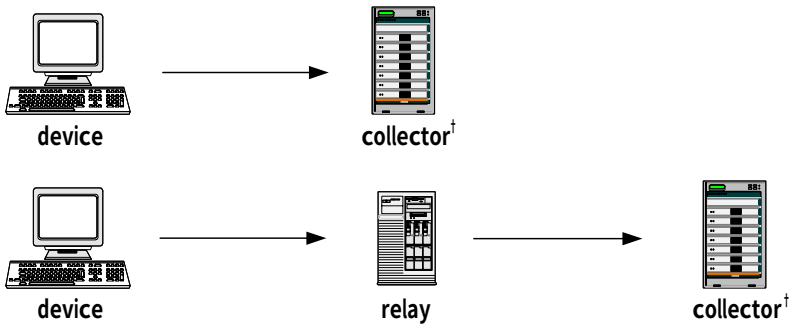

図５　syslog 転送の形態

(2) Event Log

Event Log は Microsoft 社の WindowsNT 系列の OS で利用されているログである。Event Log は Event Viewer というアプリケーションを利用して閲覧可能である。また、Event Viewer では他の Windows マシンを指定することによってリモートマシンから別のマシンのログを閲覧することができる。

(3) SNMP（Simple Network Management Protocol）

SNMP は「マネージャ」からの要求に対して「エージェント」が管理情報データベース MIB（Management Information Base）[16]に蓄積されている情報を通知する、というマネージャ/エージェントシステム・モデルを用いている。この仕組みを利用することによってマネージャから管理対象の機器の情報を集中管理することが可能である。

上記の 3 種類のログは互換性がない。したがって、それぞれの形式では集中管理が可能であっても異なる形式で出力されるログをいずれか一つの方式で管理することは不可能である。このため、現在市販されているログ収集システムでは、下記のいずれかで異なる形式のログの収集を可能としている。

① ログを管理システムに送信する時点で形式を変換する
② 管理システム側で複数のプロトコルに対応する

４．３ 異常検出の方法

ログの異常検出、解析機能を提供するソフトウェア製品はいくつか存在する。これらの製品の異常検出、解析機能は大きく、パターンに基づくログのチェックおよびログの統計処理・視覚化に集約できる。前者は特定の文字列を検査し、それに合致するものがあった場合管理者に警告するといったもので、これは管理者のログの検査作業を一部自動化し、分担する。後者はログ検査作業を主として人間-機械インタフェースを高度化し、作業効率を上げるもので、異常性の判断は人間が行う。不正なアクセスなどの特徴を、図形として認識しやすいグラフなどの統計情報として、ログを検査する管理者に顕著に表示するものである。表１０にログ解析ソフトと主な機能の一覧を示す。

表１０ ログ解析ソフト

製品名	収集	解析	視覚化	解析方法
ShowTOC	○	○	○	パターンマッチング
IP Tables logs analyzer v0.1			○	
LogRep	○	○	○	統計的解析 グラフ化
The Logging Project		○	○	パターンマッチング grep、awk、perl の利用
Swatch			○	パターンマッチング
Logsurfer			○	パターンマッチング
Arcsight	○	○	○	不明
Method for Visualizing Log Information			○	
LogWatch			○	パターンマッチング
fwLogWatch			○	パターンマッチング
Lire		○	○	パターンマッチング

市中のログの解析ツールとしては見当たらなかったが、一般的な情報解析の手法としては Fuzzy 理論や Artificial Neural Network（以下 ANN)、統計的解析手法があり、これらの手法をログの解析に応用することは可能であろう[17]。

４．４ ネットワーク犯罪に対する法整備状況

近年のコンピュータ犯罪の増加[18][4][19]、プライバシーや著作権保護と関連して国内外において急速に法整備が進められている。国内におけるネットワーク関連法案としては「不正アクセス禁止法」、「不正競争防止法」、「電子署名法」、「電子契約法」、「個人情報保護法」、「刑法（コンピュータ犯罪防止法)」および「プロバイダ責任法」が存在する。また、国際条約としては「サイバー犯罪条約」が存在し、ネットワーク犯罪に対して国家間の連携ができるような取り決めがなされつつある。

ログはセキュリティの面からみると、アカウンタビリティの上で必須であり、ログ、post-mortem（事後分析）による DoS その他のアタックの解明にも重要である。しかし、国内に

おいては警察の捜査においてログの提出を要求されるなどの例は存在するが、ログが裁判における法判断の証拠となったことはない。これはコンピュータが出力するログが、必ずしも原本製、改ざんなどに対する正真性を保証するものではなかったためであろう。近年これらの問題は電子証明書を中心とした暗号、認証技術の進歩や、前出の「電子署名法」の整備に伴い解決されるものであると考えられており、それを視野に入れて開発している。

４．５ 実現すべき技術

ネットワーク犯罪の増加に伴いネットワーク上のノードが出力するログを元にした調査、異常検出は必須の技術である。また、ネットワーク犯罪に対する法整備は国内外を問わず急速に進められており、近い将来ログが犯罪の証拠として利用されるようになることは間違いないと思われる。しかし、ログの管理、調査の現状はネットワーク管理者の技量に依存している。

このような現状から、我々はログを統合的に管理し、調査、異常検出を効率的に行えるログシステムが必要であると判断した。

以下では我々が考えるログシステムの基本構想と実現手段について述べる。

(1) 法的根拠性の実現

現在の法律などをもとにログがネットワーク犯罪などの証拠となるために必要と考えられる要件は、①可視性があること、②原本性を保証できること、③同一性を保証できること、④正真性を保証できること、⑤違法性がないこと、⑥必要な内容が記述されていること、および、⑦法律が定める期間保存されること、である。表１１はこれらをまとめたものである。現在、これらの要件を満たすシステムの設計を行っている。

表１１　ログの証拠性に要求される項目と内容

項目	内　容
可視性	電子媒体の他に印刷物か閲覧ソフトが必要
原本製	印刷物の場合、コピーではないこと
同一性	印刷作業に関する証言が得られること
正真性	公的認証機関による証明があること システム全体のログが得られること ログ発生の経緯が提示できること ログの改ざんや不整合の無いことが証明できること
違法性	個人情報保護が考慮されること ソフトウェアのライセンス管理
内容	発信元、宛先、日時、通信サイズ、通信時間、プロトコル
保存期間	最低 90 日

(2) 多種のログ収集の実現

我々は syslog、Event Log、SNMP をはじめとして IDS（Intrusion Detection System）などアプリケーションのログも収集できるシステムを構築する予定である。また、既存の機器に対して可能な限りアプリケーションを追加せずにログの収集機能を実現し､異なるフォーマット、プロトコルを利用した装置への拡張性を実現するため、これらは、ログの受信部分をプロトコル、ログのフォーマットごとにモジュール化することによって実現できると考えている。

また、元のログメッセージとそれに対する電子署名を行った後フォーマットを統一し、異なる種類のログに対して異常検出やログの集積を効率的に行えるような仕組みを考えている。

(3)拡張性の実現

我々の考えるシステムでは①対象ノードの種類、②対象ノード数の拡大の両方に対して拡張性を実現したいと考えている。

まず、①に対する拡張性は収集、解析対象となるログ、プロトコルの増大への柔軟性を意味している。したがって、これは前述の「多種のログ収集の実現」に記述した内容を実現できればよい。

次に②に関しては(a)単体システムの能力の拡大による方法と、(b)システムの分散による方法、が考えられる。現在の、市場のログ収集システムでは規模の拡大に対しては(a) の単体システムの能力の拡大による方法をとるものしかない。この方法の利点は一箇所に複数のノードからのログを集積するためノード横断的なログの検査を行いやすいという点にある。しかし、この方法は規模の拡大に対してハードウェアを置き換えるしか増強の手段がなくコスト面での問題が多い。また、多数のノードからのログを集積しようとした場合、ログ転送のトラフィックが一箇所に集中してしまうという問題もある。そこで我々は数ノードから十数ノード程度のログは一ヶ所に集積し、それ以上の規模に対してはログ収集システムをメッセージのやり取りによって複数連携させる方法を検討している。これにより、規模の増大に対してはシステムの追加を行えばよいため既存のシステムは無駄にならない。また、メッセージの連携によってネットワークトラフィックを減少させることが可能であると考えている。

(4) ログの異常検出

現在のログ解析システムは主にパターンマッチングの手法を利用して異常検出を行うか、統計的手法を用いてログを視覚化し、調査しやすくするというものがほとんどである。しかし、近年、Fuzzy や ANN といった手法を用いた特徴抽出、傾向分析はデータマイニングとして利用されるようになってきている。経済調査などいくつかの分野では実用化されている。我々はログの解析にもこれらの技術を応用可能であると考えており、これらの手法によるログの解析機能を実装したいと考えている。さらに、①異なる解析手法による結果を組み合わせる、②異なる情報源からの結果を照合する、ことによって解析精度を向上させることが可能であると考えており、これらの手法の実装を行いその効果についての検証を行う予定である。

また、我々のログ収集システムでは既述のように複数ノードからのログの収集、ログ収集システム同士の連携によって多数のノードおよびネットワークにわたってログの調査を行う機能を実現することを目的としている。この機能と、②の機能により、広範囲なネットワークおよびノード横断的な異常検出を実現できると考えている。

５．大規模検証用ネットワークの構築技術

本章では、3 および 4 章で述べた IP トレースバック技術及びログ収集・解析技術を実ネットワーク環境に近い環境で検証するための大規模検証用ネットワークの構成方法について述べる。

５．１　大規模検証用ネットワークの必要性

ここで大規模ネットワークとは、その構成ノード数が数百～数千になるネットワークを指すこととする。大規模ネットワークの具体的な例としては、世界的な規模のものとしては The Internet[20]、日本国内のものとしては LGWAN[2]及びそこに接続される自治体ネットワーク等がある。

大規模ネットワークでの利用を想定したシステムの機能および大規模ネットワークそのものの機能を検証するためには、次の理由より実際に実サービスの利用に供されるネットワークではなく、これと独立な大規模検証用のネットワークが必要である。

① 本プロジェクトで開発するログ管理技術とトレースバック技術を評価するには、Dos/DDoS、スパムメールなどの攻撃を実際に実施する必要がある。しかし、これらの攻撃をインターネットなどの現在使用されているネットワークで実施することは不可能である。

② インターネットに関するシステムの場合、これまであまりにも小さな実験システムが利用されてきた。このため、スケールアップしたときの挙動が必ずしも十分に把握できていない恐れがあった。

③ 本プロジェクトで開発するログ収集解析技術とトレースバック技術を実ネットワークに近い状態で特性を把握せずに導入した場合、想定外の動作により実ネットワークを撹乱し想定した効果が大規模システムでは発揮できない恐れがある。この問題は実ネットワークの規模が大きいほど深刻になる。

④ 現在提案されている主要なトレースバックの中には、ルータのホップ数や攻撃者の数によって、攻撃者の特定にかかる時間や攻撃者の特定精度が大きく変わるものがある。シミュレーションではいくつかの報告がなされているが、大規模な実験システムでの評価はほとんどなされていない。本プロジェクトで開発する予定の新しいトレースバック方式の信頼性を高めるためにも、大規模なネットワークでの性能検証が不可欠である。
⑤ DDoS は理論的解析が困難である。

⑥ 本論文が対象としている DoS/DDoS、スパムメール等の不正アクセスは、現実には複数の ISP（AS）にまたがって実行されることが多く、発信源探査システムの検証も複数の AS が含まれるようなネットワーク環境で行われなければならない。このような環境は多数のネットワークノード含む大規模なネットワーク検証環境を必要とする。本研究での検証用ネットワークの要求条件については 5.3 で述べる。

５．２　検証用ネットワークの現状

ここでは、現在利用されている検証用ネットワークについて概観する。現在、様々な研究・開発機関で用いられている検証用ネットワークは以下のように大別できる。

① 小規模の独立した実験用ネットワーク
② 実運用中の（主として研究用）ネットワークを結合したネットワーク
③ シミュレーションソフトウエアで模擬したネットワーク

以下に、それぞれについて詳述する。

(1) 小規模の独立した実験用ネットワーク

小規模の独立した実ネットワーク環境では、ファイアウォール（FW）やルータなどの実際のネットワークで利用される機器を組み合せて検証環境を構築する。そのため、検証の目的に応じた機器の選定やネットワーク構成を組むことができる。また、外部と接続せずに閉じたネットワークとするため、実運用中のネットワークやサービスへの影響を与えることはない。

但し、接続する機器類は多くとも数十台のため、実運用環境下での特性や挙動までは再現することは困難である。

この検証環境は主に、個々のネットワーク機器の動作検証や、ネットワーク管理システムの動作検証に用いられる。

(2)実運用中のネットワークを結合したネットワーク

例えば、JGN(Japan Gigabit Network)[21]は e-Japan 重点計画に基づき全国 10 ヶ所の ATM 交換設備及び 56 ヶ所の接続装置を超高速光ファイバで結んだ研究開発用のネットワークであり、超高速ネットワーク技術、次世代インターネット技術、高度アプリケーション技術等の先端技術の研究開発を推進することを目的としている。しかし、このような特殊な実験には有効ではあるが､特にセキュリティの実験の場合は､完全なコントロール下で行えない場合が多く、極めて大きな危険が伴う。

(3) シミュレーションソフトウエアで模擬したネットワーク

小規模検証環境では測定することのできない大規模なネットワークでの特性を計測するために用いられる。ソフトウェアによる実現であるため、論理的にはいかなる大規模なネットワークでも構成可能であるが、性能（計算時間）や設定の複雑さなどから、数十から数百に至るノード規模の検証に用いることが多い。

シミュレーションソフトウェアには市販製品の OPNET[22]、オープンソースソフトの ns-2 [23]などがある。

ネットワーク製品の検証は、当該製品の機能を検証するための最低限のノード構成を持つ小規模検証用ネットワークによっている場合が多い。当該製品の大規模ネットワークで挙動を検証するときはソフトウェアシミュレータを用いる場合がほとんどである。シミュレーションソフトウエアでは規模の大きいネットワークをシミュレーションすることは困難である。

大規模な研究開発用のネットワークは、かなり将来の実用を目指した先端技術の研究開発を目的として構築されるため、ネットワーク構成や構成要素がその時点で利用されているネットワークとは異なっていることが多い。このため、比較的近い将来の利用に供するネットワーク製品の検証には向いていないことが多く、また、利用目的や利用者が限定されるため利用しづらいという側面もある。

５．３　検証用大規模ネットワークの実現方式

ここでは、検証用大規模ネットワークに対する要求条件を整理し、その要求条件を満たす検証用大規模ネットワーク構成法について述べる。

(1) 検証用大規模ネットワークに対する要求条件

本論文では､不正アクセスの一種である DoS/DDoS の防止(抑止)を狙いとした効率の良い「発信源探査機能」と「ログ管理機能」を提案している。これらは、実ネットワークに近い環境でその機能・性能を確認（検証）しなければならない。ここでは､「発信源探査機能」と「ログ集中管理機能」から検証用大規模ネットワークに対する要求条件を述べる。要求条件を表１２に示す。

表１２　検証用大規模ネットワークに対する要求条件

項目		要求条件
発信源探査機能からの要求条件	機能	ICMP パケットジェネレータを搭載したルータが設置できること
		設置される機器でルータの機能を持つ機器は、新規のトレースバック方式の実装が可能なこと
		設置される機器でサーバの機能を持つ機器は、新規のトレースバック方式の実装が可能なこと
		動的ルーティングが実装できること
		NAT の機能を提供できること
		PKI（CA 機能）を実装できること
		IPv6 ネットワークの実現もできること
	攻撃関連	DoS/DDoS 攻撃が実施できること
		上記以外の攻撃を含めて、多様な攻撃を設定できること
ログ管理機能からの要求条件	ログ関連	syslog の収集ができること
		eventlog の収集ができること
		Apache ログ、 Squid ログの収集ができること
		Alert の収集ができること
		SNMP（MIB、トラップ）の収集ができること
	攻撃関連	DoS/DDoS 攻撃が実施できること
検証環境としての要求条件	サーバ機能	クライアントからの要求に対し、サーバが応答を返せること
	実網への影響	実運用中の NW に影響を与えないこと
	大規模検証	大規模な実際のネットワークでの挙動を予測できること

(2) 検証ネットワークの比較

ここでは 5.2 で述べた 3 つの検証用ネットワークに対して前記ツールからの要求条件に対する満足度を比較した。この結果を表１３に示す。

表１３からわかるように、本論文で提案している「発信源探査機能」と「ログ管理機能」を検証するためには、5.2 で述べた現在広く利用されている方式だけでは全ての項目を満足することはできない。

本論文では、小規模の独立した実験用ネットワーク方式を拡張し、多数の PC を利用して実際に近い環境を構築する方法を提案する。この方式を大規模実験用ネットワーク方式と呼ぶ。この方式はさまざまな物理的制約から現在は利用されていない。この制約が解消されれば本方式は大規模検証用ネットワークを構成する方式として有望になる。本方式の詳細については次節で述べる。

表１３　検証用ネットワークの満足度の比較

要求条件	小規模の独立した実験用ネットワーク	実運用中のネットワークを結合したネットワーク	シミュレーションソフトウエアで模擬したネットワーク
ICMP トレースバック用ルータの設置	○	○	○
動的ルーチング	○	○	○
NAT 機能	○	○	×
PKI（CA 機能）	○	○	×
syslog の収集	○	○	○
eventlog の収集	○	○	○
Apache ログ、Squid ログの収集	○	○	×
Alert の収集	○	○	×
SNMP（MIB、トラップ）の収集	○	○	×
サーバからの応答	○	○	×
DoS/DDoS 攻撃	○	△	○
実運用中のネットワークに影響を与えないこと	○	×	○
大規模な実際のネットワークでの挙動を予測できること	×	○	○

○：実現可能／×：実現不可能／△攻撃は可能だが、実施すべきではない

５．４　大規模ネットワークの構成

(1) 実現方式

数百台､数千台のノードで構成される大規模検証用ネットワークを実際のルータや PC をそのノード台数だけ用意して実現する場合において、以下の問題がある。

① 収容スペース
② コスト
③ 電力

そこで１台のサーバに複数のサーバやルータ端末の役割を集約させるための仮想化技術である仮想 OS、仮想マシン技術を用いて実現することとした。

仮想化する手段としては、jail/chroot によるファイル空間の隔離、仮想 OS および仮想マシンがある。これらの比較を表１４に示す。

表１４　仮想化の手段の比較

仮想化技術	概要	製品名など
jail/chroot	ファイルシステムの root を変更し、ファイル空間を隔離する技術	
仮想 OS	OS の上で仮想的な OS を複数動かす技術	UML[24]
仮想マシン	OS の上でハードウェアをエミュレートし、その上で OS を動かす技術	VMware[25]、VirtualPC[26]

今回はこれらを以下のように用いることとした。

① 攻撃パケットが通るルートは仮想化せずに、実 OS 上に PC ルータを配置する。
② 攻撃パケットが通らないルートは仮想化を行う。
③ サーバとクライアント端末は仮想化を行う。

④ 性能があまり問題にならない機器には、仮想化を適用する。

仮想化技術の適用による､サーバ 3000 台のネットワークを実現した場合の効果の予測を表１５に示す｡表１５では PC 上に Linux ルータを実装し､ネットワークを構築することとして計算している。

表１５　仮想化による効果の予測

	PC 数	PC に係る費用	消費電力	スペース
仮想化しない場合(a)	6,000 台	約 300 百万円	約 1,200KW	約 1,000 ㎡
仮想化技術を適用した場合(b)	1,500 台	約 75 百万円	約 300KW	約 250 ㎡
効果(a/b)	4	4	4	4

表１５から、大規模検証用ネットワークに仮想化技術を適用することにより約 4 倍の効果が得られると予想されることがわかる。

(2) ネットワークトポロジ

今回実現した大規模検証用ネットワークのネットワークトポロジを図６に示す。このトポロジは、ツールからの要求およびできる限り実ネットワークに近い構成となるように LGWAN 等の現実に利用されているネットワークを参考にして決定した。

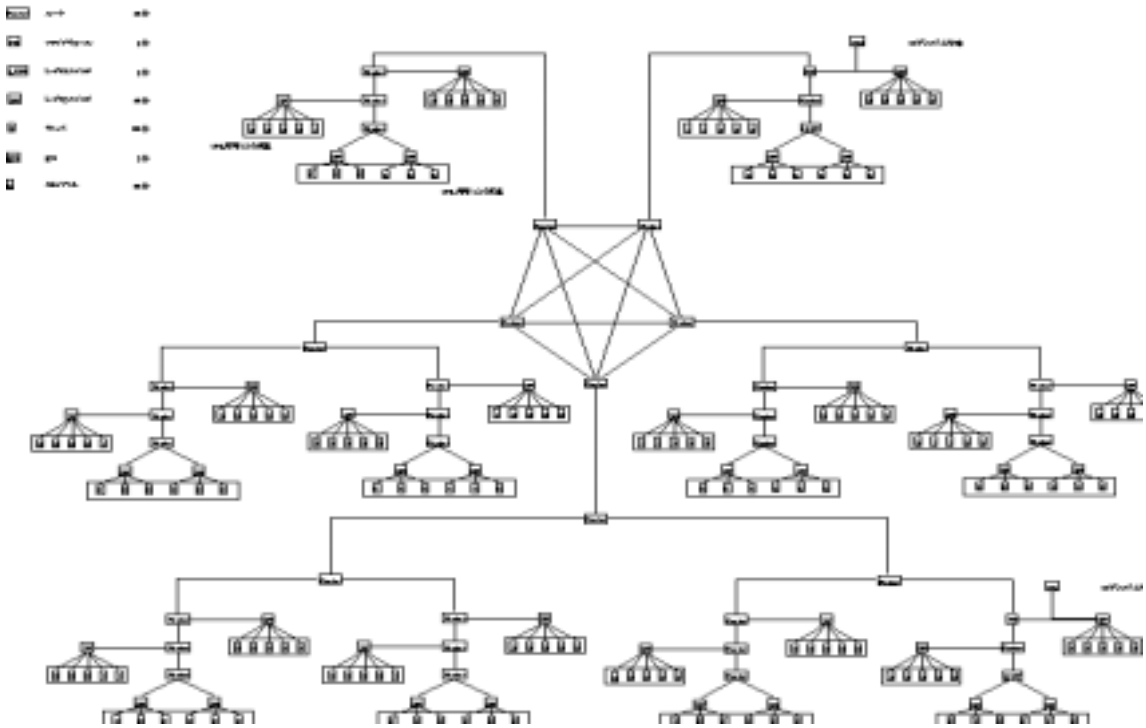

図６　大規模検証用ネットワークのトポロジ

6　おわりに

下記にそれぞれの課題ごとに行った検討内容と今後の方向を簡単にまとめた。

① 発信源探査に関しては、トレースバック方式の調査、DoS/DDoS 攻撃の調査・検討、ICMP トレースバック方式の基礎部分の設計・実装を行った。平成 15 年度以降は、本技術を応用し、セキュリティ侵害のパターン検出ロジックを独自に追加することにより、不正アクセスの検出と発信源の特定が誤り率 5%以内で 2 分以内の目標の達成に向けてさらに研究開発を進める予定である。

② ログシステムに関しては、今回の基本設計ではネットワーク上でのログシステム、データベースの配置、連携方法に関して考察を行った。平成 15 年度以降では、個々のログ・システムの機能実装に必要な要素を洗い出し、その結果を踏まえてプロトタイプの作成を行う。最終的にアクセスログの収集と異常検出が 1 分以内の目標の達成に向けてさらに研究開発を進める予定である。

③ 検証実験については、検証用ネットワークの実現方式の調査を行い、大規模検証用ネットワークの実現方式とトポロジについて検討を行った。平成 15 年度以降は、数百台のサーバによるネットワークでの検証方法に関する検討、検証に必要なネットワーク環境の設計と構築、検証に必要な不正アクセスを行うツールの検討と開発を行う予定である。また、平成 16 年度は数千台のサーバ環境を構築し、本プロジェクトで開発するログ管理技術とトレースバック技術を実ネットワークに近い状態で確認する予定である。

参考文献

[1] 門林雄基, 大江将史“IP トレースバック技術”In 情報処理 Vol.12, No.42(2001)

[2] LGWAN(総合行政ネットワーク)全国センターホームページ, http://www.lasdec.nippon-net.ne.jp/lgw/lgwan.htm

[3] Vadim Kuznetsov, Helena Sandstrom, and Andrei Simkin“An Evaluation of different IP Traceback approaches”In ICICS 2002 Singapore(2002)

[4] CERT/CC Statistics 1988-2003, http://www. Cert.org

[5] CSI-FBI Computer Crime and Security Survey 2003

[6] CenterTrack: An IP Overlay Network for Tracking DoS Floods, Robert Stone, UUNET Technologies, Inc. USENIX, Security Symposium 2000

[7] Savage S.,Wetherall D, Karlin A and Anderson T“Practical Network Support IP Traceback“In Proceedings of SIGCOMM’00 pp295-306(2000)

[8] Song D and Perrig A“Advanced and Authenticated Marking Schemes for IP Traceback”In Proceeding of NDSS’01(2001)

[9] GOSSIB vs. IP Traceback Rumors - Waldvogel (2002)

[10] Hash-Based IP Traceback, Alex C. Snoeren†, Craig Partridge, Luis A. Sanchez‡, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, BBN Technologies

[11] A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms, Jelena Mirkovic, Janice Martin and Peter Reiher,Computer Science Department, University of California, Los Angeles, Technical report #020018

[12] Effect of Malicious Traffic on the Network, Kun-chan Lan, Alefiya Hussain, Debojyoti Dutta,USC/ISI

[13] Steve Bellovin, Marcus Leech, Tom Taylor: ICMP Traceback Messages, Internet Draft Document: draft-ietf-itrace-04.txt, Feb 2003
[14] C. Lonvick, The BSD Syslog Protocol, RFC3164, 2001.8
[15] J. Case, M. Fedor, M. Schoffstall, J. Davin, Simple Network Management Protocol (SNMP), RFC1157, 1990.5
[16] M. Rose, Management Information base for network management to TCP/IP-based internets: MIB-II, RFC1158, 1990.5
[17] J. P. Bigus, Data Mining with Neural Networks, 1996
[18] 平成 14 年上半期の不正アクセス行為の発生状況等について, 警察庁 広報資料, 平成 14 年 8 月 22 日
[19] コンピュータウイルス・不正アクセスの届出状況について［要旨］, 情報処理振興事業協会セキュリティセンター(IPA/ISEC)(http://www.ipa.go.jp/), 2003.1.10
[20] FYI 20/RFC 1462 "FYI on `What is the Internet?'"
[21] JGN ホームページ　http://www.jgn.tao.go.jp/index.html
[22] OPNET Technologies, Inc. Home Page　http://www.opnet.com
[23] ns-2 homepage http://www.isi.edu/nsnam/ns/
[24] The User-mode Linux Kernel Home Page　http://user-mode-linux.sourceforge.net/
[25] VMware,inc. Home Page　http://www.vmware.com/
[26] Microsoft Virtual PC Home Page　http://www.microsoft.com/windowsxp/virtualpc/