NAIST-IS-DT9961007

博士論文

分散型サービス妨害攻撃における攻撃ノード追跡手法に関する研究

大江 将史

2003年3月10日

奈良先端科学技術大学院大学
情報科学研究科 情報処理学専攻

本論文は奈良先端科学技術大学院大学情報科学研究科に
博士 (工学) 授与の要件として提出した博士論文である。

大江 将史

審査委員：　山口 英 教授
砂原 秀樹教授
門林 雄基助教授

分散型サービス妨害攻撃における攻撃ノード追跡手法に関する研究*

大江 将史

内容梗概

インターネットにおける脅威の一つである分散型サービス妨害攻撃への被害を最小限にするためには，可能な限り短時間に攻撃パケットが通過した経路を特定し，攻撃ノードの位置を明らかにする技術が必要である．現在は，送信元アドレスが擬装された攻撃パケットの追跡を各ルータ毎にモニタリング機能などを使用して手作業でおこなっている．このために，攻撃フローと攻撃ノードの特定には時間を要する点が問題となっている．

この問題の解決策として，IP トレースバック技術が提案されている．IP トレースバックは，攻撃フローの真の送信元を特定する技術である．しかしながら，既存の手法は，インターネット全体での同一手法が適用されることを前提としているため，さまざま運用ポリシーを持った組織の集合で成り立っているインターネット上での運用を考慮していない．

そこで，本研究では，さまざまな組織で構成されるインターネット上での運用を前提とした「階層型トレースバック機構」を提案した．本提案手法は，インターネットでの経路制御が，AS (Autonomous System) 間と AS 内にわけて EGP (Exterior Gateway Protocol) と IGP (Interior Gateway Protocol) の二つに階層化されている点に着目し，攻撃フローの通過する AS の特定を行う「Exterior IP

* 奈良先端科学技術大学院大学 情報科学研究科 情報処理学専攻 博士論文, NAIST-IS-DT9961007, 2003 年 3 月 10 日.

(eIP) トレースバック機構」と AS 内部において攻撃フローが通過するルータの特定を行う「Interior IP(iIP) トレースバック機構」の 2 つに分離したアーキテクチャとなっている．eIP トレースバックは，攻撃フローの AS を短時間に特定することを目的とする．AS の特定は，フィルタリングなどによる大まかな分散型サービス妨害攻撃への対策を可能とする．また，iIP トレースバックは，AS 内における攻撃ノードの特定を目的とする．攻撃ノードの特定によって，攻撃ノードの分離や遮断等の対策が可能となる．提案手法は，既存の手法では出来なかった実インターネット上での分散型サービス妨害攻撃に対する効果的な対策を実現する．

本研究では，本提案手法の実現可能性を明らかにするために，1. アーキテクチャの定義と必要な技術の特定と評価，2. 実インターネットでの提案手法の実現可能性を明らかにするために実装を用いた検証を行った．1. では，実インターネットでの本提案手法を用いた追跡過程とその目標条件を定めた．2. では，実証実験に向けてのプロトタイプ実装についてのアーキテクチャ設計，通信プロトコルの定義，連携に必要な API を定め提案手法の実装を行った．そして，本実装は，50 程度の AS 規模をエミュレートした環境上で十分な追跡性能を有することを確認した．

以上の結果より，本提案手法は，分散型サービス妨害攻撃に対して有効な手法であることが明らかになった．

キーワード

IP トレースバック，分散型サービス妨害攻撃，セキュリティ，インターネット

Studies on technique for tracing attack nodes under Distributed Denial of Service Attack*

Masafumi OE

Abstract

Distributed Denial of Service (DDoS) attacks are one of the threats on the Internet. In DDoS attacks, the attack nodes are widely set up in the Internet, and transmit a large number of packets to the victim's node. These packets consume network resources and server resources, and obstruct network services like World-Wide-Web in the victim's node. In order to keep this damage to a minimum, the technology that identifies attack nodes and the paths of attack packets is required to be as fast as possible.

However, the source address of the IP packet for DDoS attack is spoofed to a random address. Therefore, investigating an attack node using TRACEROUTE, which depends on a source address, is not effective. For this reason, tracking the attack flow is done by hand using a monitoring function, a DDoS attack detection function, (which each router has), etc. The Internet, as an international communications infrastructure, is constructed by various organizations connecting each other with various policies, such as ISPs, companies, research institutes, universities, etc. When tracking attack flows, a lot of time is wasted getting cooperation between organizations on attack paths. Tracking by hand is a big barrier to the

* Doctor's Thesis, Department of Information Processing, Graduate School of Information Science, Nara Institute of Science and Technology, NAIST-IS-DT9961007, March 10, 2003 .

reduction of time. IP traceback methods are proposed as solution to this issue. IP traceback detects the attack paths and specifes the true origin of an attack flow with a spoofed source address.

In this paper, we propose a hierarchical IP traceback architecture, which decomposes Internet-wide traceback procedure into interdomain traceback and intradomain traceback. Our proposed method is different from existing approaches in that our method is independent from single IP traceback mechanisms, and domain decomposition is based on the existing operational model of the Internet.

The proposed architecture is made up of a construct with two components: eIP traceback and iIP traceback. Each control area of eIP and iIP traceback is the same as each control area of EGP and IGP, which are the routing control protocols. "Exterior IP (eIP) traceback architecture" designates each AS that the attack flow passed. eIP traceback should have the capability for finding attack paths within 30 minutes. "Interior IP(iIP) traceback architecture" designates the router's IP address that the attack flow has passed in the AS.

We investigated existing IP traceback and described implementation architecture of the ITM network which was used to make an association between eIP and iIP traceback. Then we brushed up our implementation and carried out experiments on the StarBED which has 50 physical nodes and is a fully programmable the Internet simulator.

From this result of experimentation, we cleared that our proposal is an effective method for Distributed Denial of Service attack.

Keywords:

Internet, Security, IP traceback, IPv6

目 次

図 目 次

表 目 次

1. まえがき

本章では,「分散型サービス妨害攻撃」がインターネットに与える脅威，その発生する背景，しくみについて述べ，その対抗策である「IP トレースバック技術」について述べる.

1.1 インターネットに対する脅威の出現

2000 年 2 月，米 Yahoo!，Amazon.com，CNN 等のポータルサイトへのアクセスが不能となる事件が発生した.

この事件は,「分散型サービス妨害攻撃 (Distributed Denial of Service:DDoS)」と呼ばれる攻撃手法によって，米国内の商用サイトが攻撃された結果であった.この攻撃手法は，悪意ある者 (攻撃者) がインターネット・プロトコルのもつ弱点を利用した不正な攻撃パケットを，被害サイトに対して意図的に送信する方法である.

この攻撃は，次に示す過程に従って行われた．まず，攻撃者は，インターネット上の各所のサーバやホストに不正アクセスを行い．攻撃パケットの生成を行うスレーブ・ノードと攻撃指令するマスター・ノードを準備した．このような準備には，サーバやホストのシステムの持つ「脆弱性」を利用して行われる.

脆弱性は，システムのオペレーティング・システム (Operating System:OS)や，アプリケーションの設計ミスやプログラム・ミス等のヒューマン・エラーが原因である．悪意ある者は，プログラムの予期しない入出力を与えることによって，管理者権限や任意のアプリケーションの実行を行うことができる.

コンピュータ・システムが人間によって開発されている以上脆弱性が，なくなることはない．そして，インターネット上でさまざまなシステムが常時接続され，ネットワークが高機能になるにつれて，コンピュータ・システムの脆弱性が与える影響は大きなものとなっている．例えば，2001 年 4 月 CordRed ワーム [1] は,

米 Microsoft 社の ISS の脆弱性を利用し，爆発的に感染を引き起こす結果となった．そして，2003 年 2 月，同じく米 Microsoft 社の MS-SQL サーバの脆弱性を利用した SQL Slammer ワーム [2][3] は，世界各地でインターネットへの接続障害を引き起こした．

次に，マスター・ノードからインターネット各所に設置したスレーブ・ノードに対して，米 Yahoo!等のポータルサイトを目標とする攻撃指令を行った．各スレーブ・ノードは，攻撃指令にしたがって，攻撃用の通信パケットを攻撃対象に対して送信する．全スレーブノードからの不正な通信パケットは，被害ノード (Victim node) に近づくにつれて，集約化され，被害ノードに配送される．

この結果，被害ノードは，大量の不正な通信パケットの受信によって，ネットワークやコンピュータのリソースが消費させられる．そして，被害ノードは，リソースの不足によって，ユーザーへの正常なサービス提供が不可能となる．

米 Yahoo!は，この攻撃によって正常なサービス運用が不可能となり，その被害額は，米国調査会社の報告によると，米 Yahoo!単体で数百万ドルに達したとされている [4]．

この事例が示す用に，インターネットがインフラストラクチャとして，なくてはならない物となった今，分散型サービス妨害攻撃が与える脅威は非常に大きなものなっている．

1.2 分散型サービス妨害攻撃とは

分散型サービス妨害攻撃とは，インターネット上に分散した攻撃ノードから被害ノードに対して大量のパケットを送ることによって，ネットワーク帯域やサーバなどのリソースを奪い WWW や FTP といった正規のサービスを妨害する攻撃手法である．

本研究では，スレーブ・ノードといった攻撃パケットを送信するノードを「攻撃ノード (Attack node)」と呼び，攻撃ノードから被害ノードへ送信された攻撃

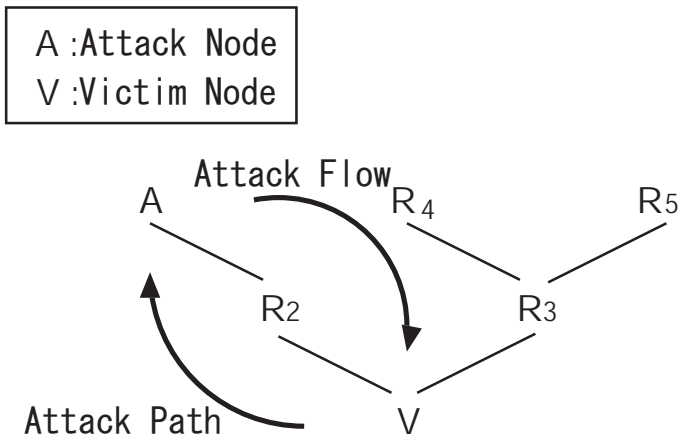

図 1 攻撃フローと攻撃パス

パケットの流れを「攻撃フロー (Attack Flow)」とし，その攻撃フローが通過した経路を「攻撃パス (Attack Path)」とする (図 1)

この攻撃手法は，公衆回線交換ネットワーク (Public Switched Telephone Network:PSTN) でたとえるならば，いたずら電話といえる．事務所の電話に対していたずら電話が何度もかかってくれば，業務電話の着信や発信を妨害することとなり，その電話の利用が出来なくなる．その結果，事務所の業務運用に大きな影響を与えることになる．つまり，インターネットにおいて，大量の接続要求や不正なパケットをノードへ送信し続けることは，そのノードにおけるインターネットの利用を妨害することになる．

分散型サービス妨害攻撃の被害は，攻撃時間を T_v，被害ノードにおける単位時間あたりの攻撃パケット数 P_v とすると，被害ノードにおける被害量 D_v は，

$$D_v = T_v \times P_v \tag{1}$$

となる．

分散型サービス妨害攻撃は，この T_v と P_v のパラメータが双方ともに大きくな

る攻撃手法である．つまり，複数の地点に設置した攻撃ノードからの攻撃パケットを送信 (P_v が大) と，送信元アドレスの擬装した攻撃パケットを利用することによる困難な攻撃ノードの特定 (T_v が大) の組み合わせたものだからである．

分散した攻撃ノードから攻撃することによって，1 ノードからの攻撃パケットの送信よりより多くの攻撃パケットが送信でき，かつその対策も困難にする．1 ノードから送信できる攻撃パケットの数は，そのノードがインターネットに対してもっているネットワーク帯域幅に依存した結果になり，また，帯域を使い切るような攻撃は，攻撃ノードの存在が目立ち，結果として攻撃ノードの特定につながってしまう．一方，インターネット上に分散した複数ノードからの攻撃は，各攻撃ノードごとに利用可能な帯域が存在し，また，その帯域を使い切ることなく一部を利用することによって，攻撃ノードの存在を目立たなくすることができる．

そして，攻撃ノードの特定を困難とするために，攻撃パケットに用いる IP パケットの送信元アドレスは擬装したものを使用する．従って，例えば，traceroute のように，攻撃パケットの送信元アドレスを利用した攻撃ノードの追跡は不可能である．

分散配置された攻撃ノードと追跡困難な攻撃パケットの利用という 2 点を組み合わせた分散型サービス妨害攻撃は，非常に効果の高い攻撃方法であることがいえる．

1.3 送信元アドレスに依存しないパケット転送

先に分散型サービス妨害攻撃で用いるパケットは，送信元アドレスを擬装したものとなっていることを述べた．これは，インターネットが，送信元アドレスに依存しないパケット転送アーキテクチャを持っていることから，擬装したパケットの転送が可能となっている．

インターネット・プロトコル [5] は，1980 年 J.Postel 博士によって提案され，さまざまな拡張やアプリケーションが研究・開発され続けてきた．そして，基本的

な要素は変わることなく利用され続けてきた.

近年は，爆発的なインターネットの普及に伴い，インターネット上に接続されたノードを識別するために用いられるIPアドレスの枯渇が問題となっている．この問題への対策として，IPv6の研究開発が行われ，すでに，さまざまな商用製品が開発され，実用化の段階にきている[6][7].

現用のIP(IPv4)，次のIPv6の双方において，インターネット・プロトコルは，ベスト・エフォートなプロトコルである．これは，信頼性を保証しないプロトコルであり，信頼性は，上位層のプロトコルで確保することとしている．例えば，OSI7階層のトランスポートプロトコルであるTCP[8]は，再送制御や，フローコントロール制御などの高機能な機能をエンド・ノード間で提供することによって，信頼性の高い通信を可能としている.

信頼性のある通信の実現を上位層に依託し，信頼性の保証をネットワークで行わないことによって，単純なシステムとなった点が，インターネットの今日までの成功につながっている.

インターネットプロトコルにおいて，パケットの転送(フォワーディング: Forwarding)は，送信先アドレスに基づいて行われる．ホストから送信されたパケットは，インターネット上のルータを経由して転送される．経路上の各ルータは，パケットの送信先アドレスを元に自身の経路表を参照し，適切な次ルータ，もしくは，ホストへの転送を行う．このように，インターネットにおけるパケット転送の過程において送信元アドレスは利用されない.

従って，送信元アドレスの内容に関わらずパケットの転送は送信先アドレスへ行われる．同様に，擬装されたアドレスをもつ攻撃パケットも送信先アドレスへ転送される.

1.4 分散型サービス妨害攻撃の歴史と要因

ここでは，分散型サービス妨害攻撃手法の進化の歴史とその発生要因について述べる．

インターネット・プロトコルにおける攻撃の可能性については，Morris ら [9][10] が指摘しているように，インターネットの普及以前から把握されていた．その攻撃の可能性が現実となり被害を出すようになったのは，インターネットの普及が始まりだした 1996 年を迎えてからであった [11][12].

そして，その攻撃手法は，進化をし続けており，被害量は，インターネットに常時接続するノードの種類やその数が増えるにしたがって，大きくなってきている [13].

例えば，TFN2K(Tribe Flood Network 2000) は，1998 年頃に公開された TFN(Tribe Flood Network) をベースに，攻撃ノード秘匿性の向上や，攻撃パターンの追加等の改良がおこなれた [14]．この結果，TFN2K は，TFN に比べて，より高い破壊力と，より高い攻撃ノードの秘匿性を持つようになった．

各攻撃者は，自らの能力の誇示や脆弱性の啓蒙活動等の目的として，さまざまな手法を考え，そして，その手法は，ソースファイルという形で誰もが見て改変が可能な形でインターネット上で提供された．公開された手法は，他の多くの攻撃者によってさらなる改良が加えられ，同様にソースファイルが公開された．このように，手法に対する改良によって新たな手法の登場が繰り返されることにより，攻撃ツールは日々進化しつづけている．

一方，攻撃が行われる要因は，クラッカーと呼ばれるシステムの破壊を目的とした者が，インターネットの世界において自らの力を誇示するためや，IRC や WWW の掲示板上などで，攻撃者にとって不都合な発言や行動がなされた際に，その報復として攻撃を行うといった短絡的で稚拙なものがある [15].

さらに，最近は，サイバーテロや戦争の兵器として用いられる事件が発生するようになった．文献 [16] によれば，その道具として用いられる理由として，(1) 攻

撃に要するコストが低い．(2) 専門的な技術者さえいれば，大人数の部隊は必要ない．(3) 犯人の特定が困難である．(4) 地理的・時間的制約がなく，いつでもどこからでも攻撃が可能である．(5) いったん攻撃が成功すれば，経済・社会に大きなダメージを与えることができる．という点を指摘している．

被害の実例としては，中東方面におけるイスラエル-パレスチナ暫定政府間での緊張が高まり，軍事衝突が発生しているが，この際，アラブ諸国からユダヤ諸国に対しての分散型サービス妨害攻撃が行われるといった事件が発生している [17]．

このように，分散型サービス妨害攻撃は，短絡的で稚拙な目的の攻撃から，戦争の兵器として相手国の通信・経済システムの破壊を目的とした攻撃まで，さまざまな要因によって発生している．

1.5 分散型サービス妨害攻撃のしくみ

ここでは，以上に述べた分散型サービス妨害攻撃の具体的な方法を実在する攻撃ツールを元に説明をおこなう．

分散型サービス妨害攻撃をおこなうためのツールは，ざまざまなものが存在する．攻撃手法やその管理手法は異なっているが，多くのツールにおいて攻撃システム自体の基本的な構成は同じである．ここでは，そのツールの中でも Trinoo を例に分散型サービス妨害攻撃のシステムについて述べる [18]．

攻撃ツールは，図 2 に示すように大まかに 3 つのコンポーネントで構成されている．それらは，攻撃の指令を行う「マスター (Master)」，攻撃パケットの生成を行う「スレーブ (Slave)」，そして，攻撃パケット数の増加や送信元の隠蔽を行う「リフレクタ (Reflector)」である．

マスターは，各スレーブを把握・操作することによって，攻撃の管理を行う．具体的には，各スレーブからの存在の報告や被害ノードの指定や攻撃パケットの量，時間などといった攻撃指令をスレーブへ行う．

スレーブとマスター間の通信は，送信元アドレスの擬装，ICMP エコー・リプ

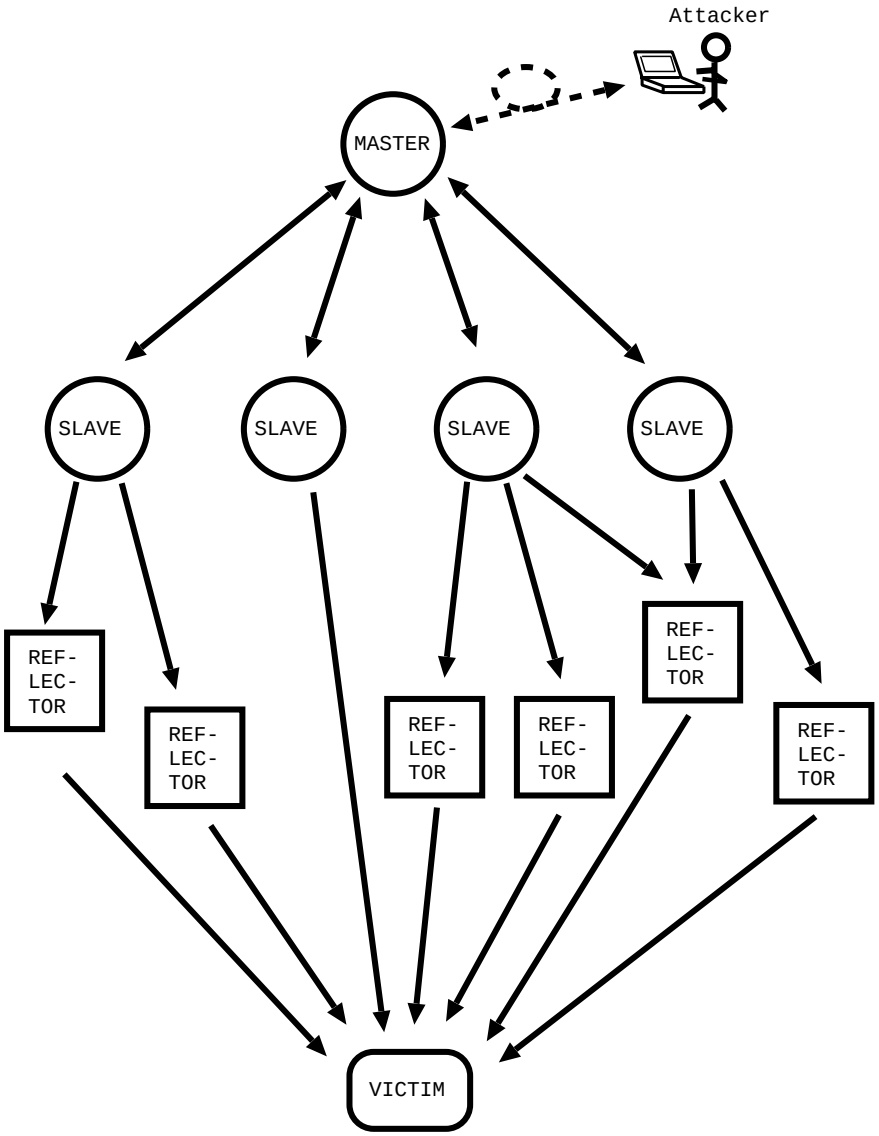

図 2 分散型サービス妨害攻撃ツールの構成要素

ライ/リクエストや，HTTP リクエスト・リプライ，IRC などを利用し，通信の特徴を目立たなくし，かつ，内容を暗号化している．これによって，トラフィック観測からのスレーブとマスターノードの存在を隠蔽し，それらの存在が発見困難となるように設計されている．

次に，スレーブについて述べる．スレーブは，マスターからの指令に従って，攻撃ノードとして攻撃パケットの送信を行う場合と，リフレクタを攻撃ノードとして使用するための攻撃パケットを送信する場合がある．なお，スレーブの呼称は攻撃ツールによって異なり，Trinoo ではエージェント (Agents)，TFN ではデーモン (Deamons) となっている．

攻撃パケットに用いる送信元アドレス・送信先アドレスの組み合わせは 2 種類ある．スレーブが攻撃ノードとして被害ノードを直接攻撃する場合は，被害ノードのアドレスを送信先アドレスとし，送信元アドレスをランダムなアドレスによって擬装した攻撃パケットを使用する．一方，スレーブが直接被害ノードへパケットを送らずに，リフレクタを攻撃ノードとして，攻撃を行う場合は，攻撃パケットの送信元アドレスを被害ノードのアドレスとした攻撃パケットを使用する．

また，スレーブはインターネット上の複数の地点に設置され，スレーブの設置数が多ければ多いほど，被害は大きなものとなる．その設置方法は，大きく分けて 3 つある．

1. 攻撃者自身による設置

   攻撃者がシステムの脆弱性を利用した不正アクセスによって，スレーブをホストに設置する．なお，スレーブに同じく，マスターの設置も同様の手法で行われる．設置ホストごとに作業が伴うために，手間がかかるが，アクセス・ログからの痕跡の除去等によってその発見を困難することができる．

2. 自己増殖による設置

   先に示した CordRed ワームのように，ワームによって，スレーブの設置を行う方法である．大量に設置することが可能である．しかし，ワームの活

動結果によっては，その発見につながり，そのスレーブの除去が迅速に行われる場合がある．

3. 一般ユーザによる設置

スレーブ機能をトロイの木馬として組み込んだアプリケーションを公開し，無意識のうちに，一般ユーザが自らスレーブを設置する方法である．これには，政治・思想的，または，興味本位の攻撃のために，自らスレーブを設置する場合も含まれる．

リフレクタは，攻撃ツールの一部ではなく攻撃の際に踏み台として利用する一般のノードのことである．その目的は，攻撃パケットの増加目的に利用する場合もしくは，攻撃パケットの送信元をかく乱する場合がある．しかし，どちらの場合においても特別なシステム設置などはせずに，インターネット・プロトコルやその上位層の仕様をリフレクタとして利用する．攻撃パケットの増加をリフレクタで行う場合は，ICMP のエコーリクエスト/リプライ・メッセージとブロードキャスト・アドレスを組み合わせて行う方法や，DNS の要求と応答を利用する方法などがある．

例えば，TFN は，ICMP エコーリクエスト・リプライとリフレクタを組み合わせて，攻撃パケットの増加をおこなっている．この場合，リフレクタは，ネットワーク・セグメント上の全ノードである (図 3 の (1))．スレーブは，攻撃パケットとして，送信元アドレスを被害ノードのアドレスとし，送信先アドレスをリフレクタのネットワーク・セグメントのブロードキャスト・アドレスとした ICMP エコーリクエスト・パケットを送信する (図 3 の (2))．このパケットは，リフレクタのセグメントに転送され，そこで，全ノードがそのブロードキャスト・アドレスに対して，ICMP エコーリプライパケットを被害ノードに対して送信する (図 3 の (3))．

もし，リフレクタが n ノード存在する場合，攻撃パケット 1 パケットに対して，n 倍のパケットとなって，被害ノードに向かって送信されることになる．

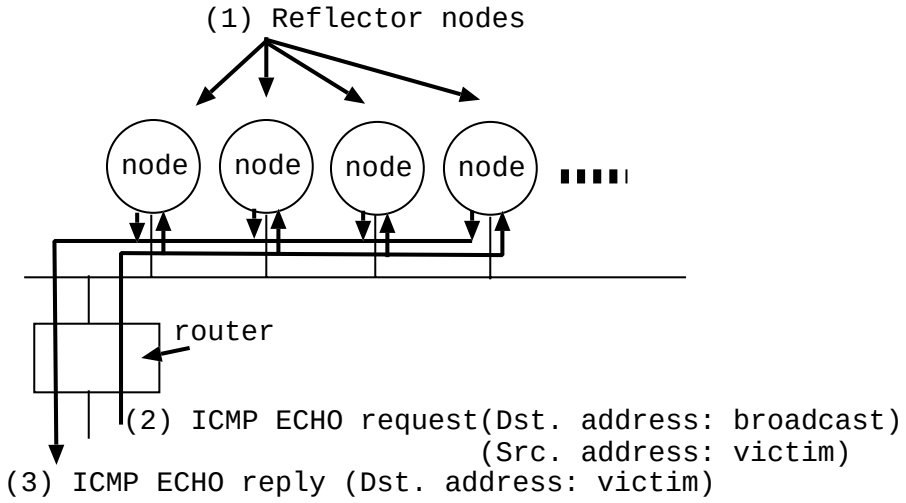

図 3 ICMP エコーリプライ・メッセージを利用した攻撃パケットの増大

一方，送信元を擬装する目的であれば，ICMP TTL(Time to Live) エクスパイア・メッセージや，ICMP ポートアンリーチ・メッセージなど利用する手法がある．

例えば，ICMP TTL エクスパイアを利用する場合は，スレーブが送信元アドレスを被害ノードとして，送信先アドレスを適当なアドレス，TTL 値を n とした攻撃パケットを送信する (図 4 の (1))．この結果，n ホップ目のルータにおいて，TTL が 0 となり，パケットの送信元アドレスすなわち被害ノードに向けて，ICMP TTL エクスパイア・メッセージが送信される (図 4 の (2))．被害ノードは，予期しないノードからの ICMP TTL エクスパイア・メッセージを受信する (図 4 の (3))．

このように，設置されたマスター，スレーブそして，リフレクタを組み合わせて，攻撃者は，追跡困難な攻撃パケットを大量に生成し被害ノードを攻撃する．

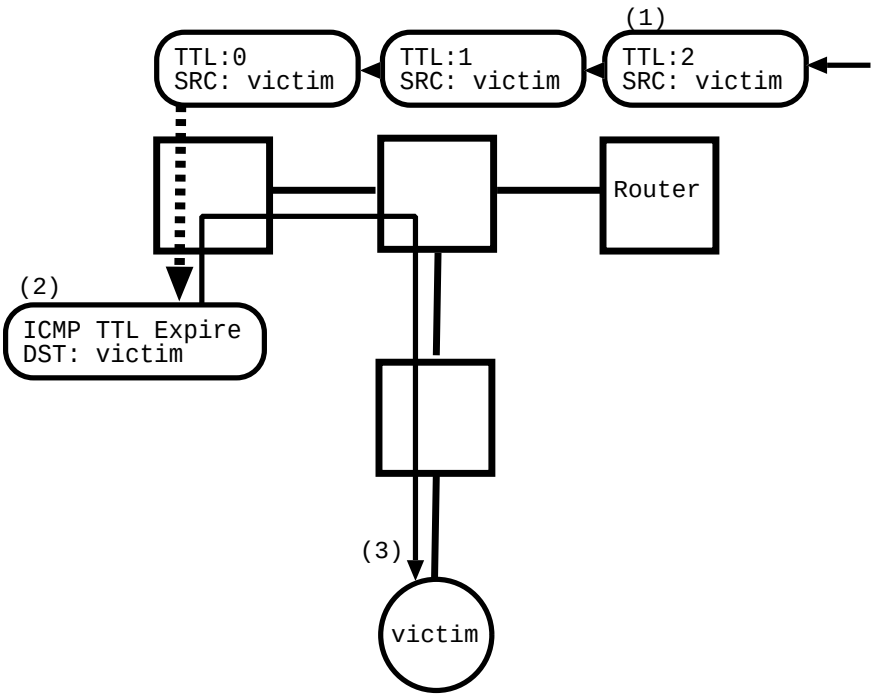

図 4 ICMP TTL エクスパイア・メッセージを利用した送信元アドレスの擬装

1.6 分散型サービス妨害攻撃への対策

ここでは，以上に述べた分散型サービス妨害攻撃に対する対策手法について述べる．

分散型サービス妨害攻撃への対策は，事前対策と事後対策がある．事前対策とは，マスターやスレーブなどの攻撃ツール設置の阻止とその除去である．先に述べた通り，マスターやスレーブの設置は，システムのもつ脆弱性を利用した不正アクセスを通して行われたり，ワームやトロイの木馬など用いて行なわれる．よって，脆弱性に対するベンダーなどから提供される修正プログラムの適用によって，脆弱性への対応は可能である．また，マスターやスレーブが設置されてしまった場合でも，ウイルス対策ベンダーなどの走査ツール・対策ツールによって，攻撃ノードの発見は可能であり，システムの分離など未然に攻撃の発生を防ぐことができる．

しかしながら，CERT などの各インシデント機関を通して脆弱性に関する情報提供は広く行われている点や，各種ベンダーや団体による走査ツール・対策ツールが有償・無償を問わず手に入る点にも関わらず，未然に攻撃の発生を防ぐことはできていない．

これは，ベンダーの脆弱性対策に対する姿勢や，システム運用に必要な予算の問題，システム管理者のセキュリティに対する意識の低さが問題となっているからである．ここで示した問題点の解決を図ることが重要であはあるが，これらは，容易に解決できる問題ではない．

よって，事前対策のみで分散型サービス妨害攻撃を根絶することは困難である．

事後対策とは，起こってしまった分散型サービス妨害攻撃を収束させることを目的とした対策である．

これには，2 段階の対策過程がある．第 1 段階目は，発生した分散型サービス妨害攻撃の攻撃ノードと攻撃フローの特定である．第 2 段階目は，攻撃ノードと攻撃フローへの対策である．これは，攻撃ノードのインターネットから隔離や攻

撃フローを攻撃パス上のルータでフィルタリングによって，攻撃パケットの遮断を行うことである．

第 1 段階における特定に要する時間 T_f と第 2 段階の対策に要する時間 T_m の合計が攻撃時間 T_v となる．

$$T_v \quad = \quad T_f + T_m \tag{2}$$

したがって，T_f と T_m の双方を最小化することが，被害量 D_v を最小化することとなる．

本研究において着目する IP トレースバック技術は，分散型サービス妨害攻撃における攻撃フローのパス（攻撃パス）を求める技術であり，第 1 段階における対策手法の一つである．

現在，もっとも用いられている IP トレースバック手法は手動追跡手法である．これは，ルータのモニタリング機能やサービス妨害攻撃検知機能などを使い，各ルータ毎に手作業によって，攻撃パスと攻撃ノードの特定をおこなう方法である．この手法は，ルータに有する機能を使うため，IP トレースバックに伴う新たな機器やインフラの整備を準備する必要がない [19].

しかし，手動追跡手法を用いた攻撃パスの特定は，非常に時間を要する点が問題である．この要因は，インターネットがさまざまな組織が接続した国際的な通信インフラである点にある．インターネットは，商用 ISP や，企業，研究・学術機関といった様々なポリシーをもった機関が相互に接続して成り立っている．従って，その境界を越えた追跡を行う際の協力が必要となり，追跡時間の短縮に対する大きな障壁となっている．

そこで，手動追跡手法に比べて短時間に攻撃パスの特定が可能な技術について，活発に研究・開発が行われている．攻撃パス構築に要する時間短縮は，その分散型サービス妨害の被害量の低減につながる．

1.7 本研究の展開

本研究では，IP トレースバックの先行研究について概観し，その問題点の指摘を行う．そして，問題点の解決策として，階層型IP トレースバック機構を提案しその概要を述べ，インターネットでの運用の可能性について論ずる．そして，提案手法の実装アーキテクチャや各種プロトコルについて述べ，その動作検証結果と考察を述べる．

以後，2 章では既存の IP トレースバック技術の概観を行い，3 章にて，提案手法である階層型IP トレースバック機構の説明する．そして，5 章にて，提案手法のプロトタイプ実装とインターネット・エミュレーション環境上での実験とその結果について述べ，6 章では，提案手法の考察，7 章にて，本研究における成果と今後の展開について述べる．

2. IP トレースバック技術

先行研究として，種々の IP トレースバック技術が提案されている．本章では，既存の IP トレースバック技術をその特徴を元に分類し，各手法の概観とその問題点を指摘する．

2.1 IP トレースバック技術に関する既存研究

IP トレースバック技術に関する研究は，さまざまな手法が提案されている．本研究では，その各手法の内容に従って，IP トレースバック手法を「リンク検査手法」「逆探知パケット手法」「マーキング手法」「ダイジェスト手法」の 4 種類に分類した．

リンク検査手法は，各ルータにおける攻撃フローの流れるリンク (ネットワーク・インターフェース) を特定する方法である．これには，手動追跡手法も含まれる．

逆探知・マーキング・ダイジェスト手法は，攻撃パケットの通過したルータの情報を記録し，その記録から攻撃パスの特定を行う手法である．それぞれ記録領域として，逆探知手法は，攻撃パス特定用のパケットに記録，マーキング手法は，パケット自体の未使用領域に記録，ダイジェスト手法は，ルータ上に記録する．

次に，分類した各手法毎にその特徴と提案研究をまとめる．

2.2 リンク検査手法

本手法は，ルータ毎にモニタリングによる攻撃フローの流入方向を特定を繰り返すことによって，攻撃パスの特定を行う．この特定には，攻撃パケットの特徴 (送信先アドレスや上位層プロトコル等) からルータに実装されているトラフィックモニタ機能などを利用する．

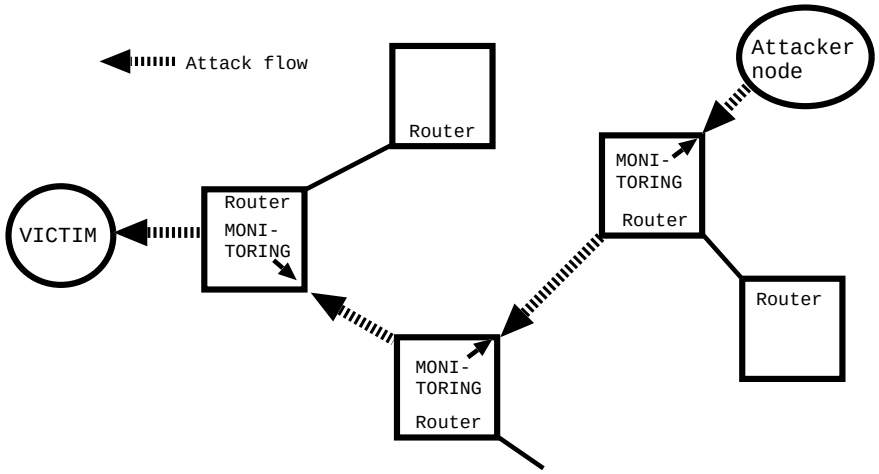

図 5　リンク検査手法における追跡過程

攻撃フローが流入するネットワーク・インターフェースが特定できれば，そのネットワーク・インターフェースの接続されたリンク上に存在する対向のルータにおいて同様のトラフィックモニタを実施する．図 5 に示すように，被害ノードから順次攻撃フローの発生源に向かって，各ルータ上でモニタリングを繰り返すことによって，攻撃パスの特定が可能となる．

この手法を発展したものとして Stone らは，攻撃フローの追跡を専用に行うネットワークをバックボーン上に構築する方法を提案している [20]．この手法では，AS (Autonomous System) 間に設置される境界ルータから追跡ルータと呼ばれるルータへ IP トンネルを設定する．この追跡ルータ上に攻撃フローを一元化することで被害ノード向きの IP パケットを集約し，モニタリングから各境界ルータにおける攻撃フローが通過するインターフェースを特定することができる．この追跡ルータ上の攻撃フローの一元化によって，効率よく攻撃パスの特定が可能となる．

リンク検査手法の問題は，攻撃フローをモニタリングしながら攻撃パスの特定を行うため，攻撃フローが無ければ追跡出来ない点にある．

2.3 逆探知パケット手法

本手法は，ルータなどが攻撃パスを構成するために必要な情報を逆探知パケット (Passive detection packet) と呼ばれる専用の IP パケットに記録し送信する．図 6 に示すように，各ルータが生成した逆探知パケットを元に攻撃パスの構築を行う．

IETF iTrace 分科会によって，検討が進められている ICMP Traceback では，あるルータで交換される全 IP パケットに対して極めて低い確率 $P(=1/20000)$ に従って IP パケットを抽出する．抽出された全 IP パケットについて追跡に必要な情報を集め，ICMP Traceback メッセージとしてその情報をその IP パケットの最終的な送信先ホストアドレスに指定されたホストへ送信する [21].

この方法に対する拡張として Wu らの提案 [22][23] は，被害ノードに対する ICMP Traceback メッセージの生成要求を可能としている．この提案では，元々提案されている ICMP トレースバックに比べてより短期間に攻撃パスの構築が可能であることが示されている．

しかし，逆探知パケット手法は，IP トレースバックを必要としないノードに対してもルータの情報が平文で含まれた逆探知パケットが生成されるため，ネットワークトポロジといったネットワーク構成に係る情報の漏洩が発生する．また，ICMP Traceback は逆探知パケットとして ICMP を使用しているため，抽出した追跡対象パケットと逆探知パケットは異なる種類のパケットとなる．そして，コンテンツ・ルーティングと呼ばれる TCP や UDP 等の上位層プロトコルの内容によって，IP パケットのルーティングを行う機構がある．したがって，攻撃フローに対してコンテンツ・ルーティングが行われた場合，逆探知パケットは攻撃フローと同一のルーティングが行われないために，攻撃パスを正しく構成することはできない．

また，生成される逆探知パケットのトラフィック量と攻撃パスの構成に必要な時間は，トレードオフの関係にあるので逆探知パケット手法においては，確率 P

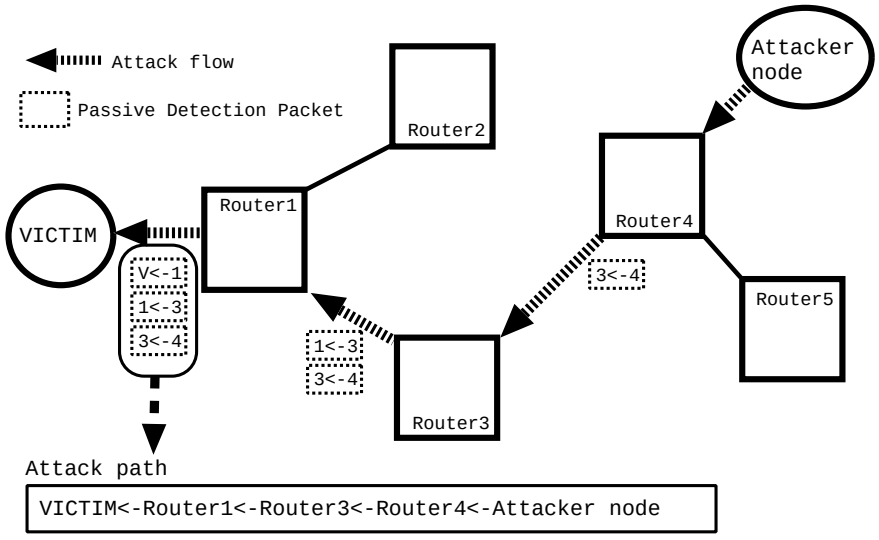

図 6 逆探知パケット手法における攻撃パス特定

を適切に設定する必要がある.

2.4 マーキング手法

この手法は，IPv4 ヘッダ中に IP トレースバックに必要な情報を記録することで，攻撃パスを特定する方法である．逆探知パケット手法と異なり，IP トレースバックに伴う追加のトラフィックが一切発生しない.

この手法の代表例として Savage[24] らの手法では，IPv4 ヘッダ中にある識別子フィールド (Identification Field, 16bit) を利用してマーキングを行い IP トレースバックを実現している．図 7 は，本手法に基づく識別子フィールドの使用法である．これは，オフセット (Offset, 3bit)，距離 (Distance, 5bit)，エッジ ID (Edge-id fragment, 8bit) の 3 つのパラメータで構成されている．このフィールドは，フラグメント化する際に利用されるが，パケット当たりのフラグメント率は 0.07〜0.14%と少ないため，このフィールドを IP トレースバックのために利用しても問

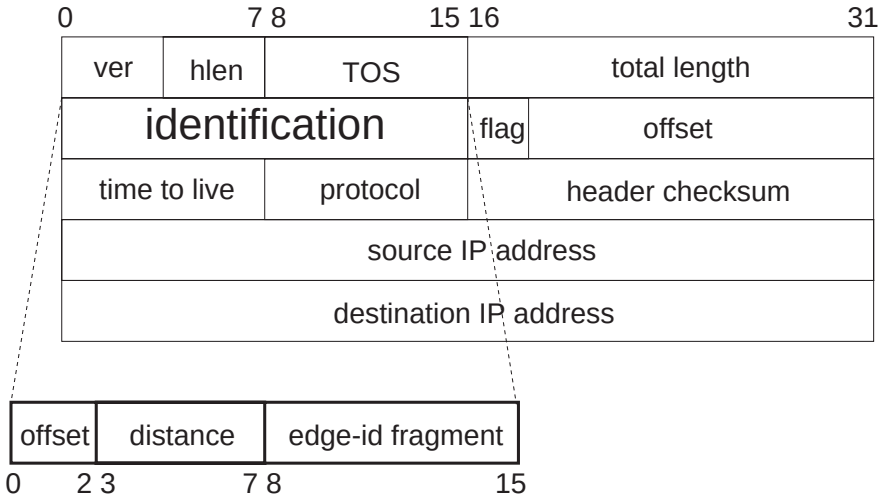

図 7 識別子フィールドを利用したマーキング

題は無いとしている．Savage らの提案では，IP パケットが通過するルータ間をリンクと呼び．リンクは，両端のルータ S および E の組によって識別することができる．ルータ S および E のアドレスを R_S，および R_E とすると，あるリンクは，(R_S, R_E) と表現できる．R_S と R_E の排他的論理和 $(\oplus)$ である $R_S \oplus R_E$ をここで R_{link} とし，R_{link} と，被害ノードと R_{link} 間の距離（ホップ数）d をマーキングに用いる．

一方，攻撃パスの構成は，被害ノード上のルータ IP アドレス R_0 と距離 1 の R_{link} を元に $A \oplus (A \oplus B) = B$ を利用して，$R_0 \oplus R_{link} = R_E$ より，R_0 の次のルータ R_E を特定することができる．これを繰り返すことより，攻撃パスの構築が可能となる．

Savage らの手法は，同一距離のルータが多く存在する時，攻撃パスの構成が失敗する場合がある．これを改良した IP トレースバック手法を，Song[25] らが提案している．この手法では，マーキングにルータの IP アドレスを用いる代わりにそのハッシュ値を用いている．シミュレーションでは，1500 地点からのサービ

ス妨害攻撃においても攻撃パスの構成が可能であるとしている．しかし，この手法では，攻撃パスの構成には予めネットワークトポロジが必要となり，その入手方法が問題となる．

CAIDA の報告によると，フラグメントパケットの主な原因として，トンネリング (GRE，L2TP，IPsec，PPPoE) があり全体の 15%を占めている [26]．また，RealAudio や Windows Media 等においてもフラグメントパケットが発生するとしている．このほかに，IPsec AH[27] においては，ICV (Integrity Check Value) の計算に，識別子フィールドを使用している．以上より，マーキング手法は，VPN，IPsec，ストリーミング・メディアといった新しいアプリケーションとの親和性が低いといえる．また，IP トレースバック情報を組み込むためのマーキング領域は小さい．この点を情報理論の応用によって IP トレースバックに必要な情報を断片化し，マーキングすることでによって対処している．そのため，攻撃ノードが偽造マーキングを生成した場合，攻撃パスの構築に必要な計算量が増大する点や，短期間の攻撃や数万ホストに分散した攻撃ノードからの攻撃フローの追跡は困難である．よって，攻撃者の抗トレースバック攻撃に対して無力であるという点は否めない．

さらに，IPv6 においては，IPv4 に比べ IP ヘッダの効率化が行われており，マーキング手法において利用する 16bit の識別子フィールドは廃止されている．そのため同様の手法は利用できない．また，記録すべきルータ間のリンク情報は，IP アドレスが 32bit から 128bit へと増えているため，Savage らの手法において記録しなければならない情報は 96bit 増加することになる．従ってより多くの断片化を伴ったマーキングをしなければならず，抗トレースバック攻撃に対する防御はより難しいものとなる．

2.5 ダイジェスト手法

Snoeren[28] らは，ルーター上を通過するパケットの記録を効率よく行うことによって，攻撃フローの特定を行う手法を提案している．この手法では，経路上で IP ヘッダ中の不変な部分 (20byte) とペイロード先頭部分 (8byte) である P を k 個の独立なハッシュ関数 H を用いて，図 8 に示すように 2^nbit のビットマップに変換し保管するというものである．保管されたビットマップは，一定期間毎にハッシュ関数とともにダイジェスト・テーブル (digest table) へ保管される．各ルータにおける異なるハッシュ関数と，定期的なハッシュ関数の更新によって，IP パケットのハッシュ衝突をできる限り防ぐ工夫がなされている．

あるパケットが通過したルータの特定は，対象となるパケットを k 個のハッシュ関数を通し，2^n 個のビットマップテーブルと比較することで，通過したルータのパスを特定することができる．また，これと併せて，Snoeren らは，このデータ収集と問い合わせのアーキテクチャSPIE (Source Path Isolation Engine) の提案をおこなっている．

この手法では，AS 間でのダイジェスト・テーブル等のやりとりに先に示した通り連携の障壁が予想される．また，監視対象のインターフェース毎に記録データの転送のために必要なネットワーク帯域と保存のためのストレージ，そしてそれらの管理コストが必要となる点が問題である．

2.6 既存研究が抱える共通の問題

以上の既存研究をふまえた結果，現実のインターネット上で IP トレースバックを実現するには，次に述べる 3 つの問題が既存研究には存在する．

1. 完全な攻撃パスの特定が目的

   既存の研究では，完全な攻撃パスの特定を目的とした研究が行われている．この考え方は,「犯人探し (=攻撃ノード) のスタンス」であり，被害者保護

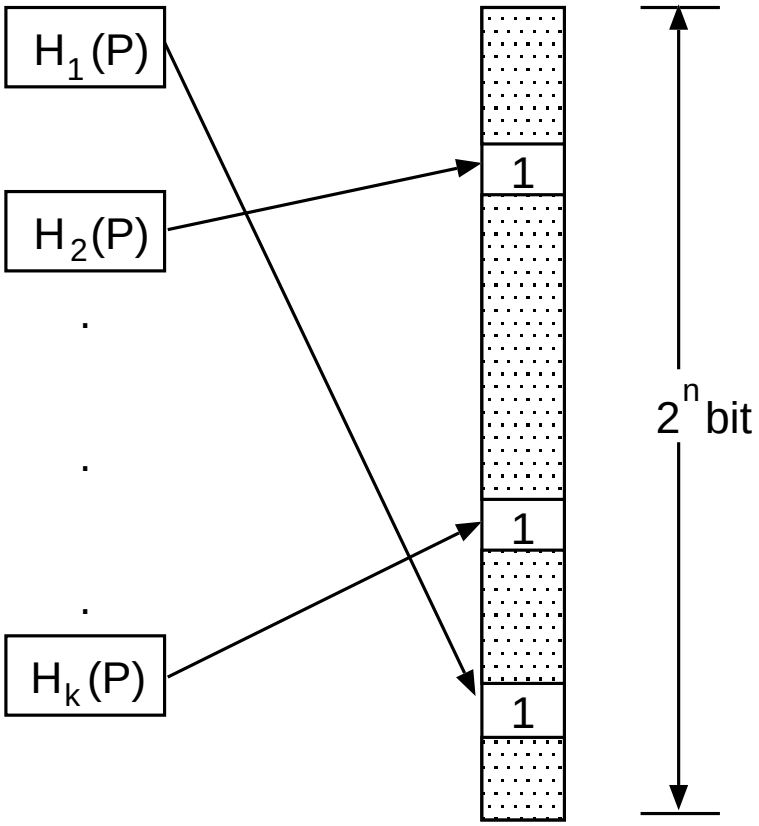

図 8 パケット P とハッシュ関数 H からのビットマップの生成

の技術とはなっていない．分散型サービス妨害攻撃の事後対策としてのIPトレースバック技術という観点では，被害ノードへの対策が可能な限り早く実行できる技術であることが重要である．

したがって，IPトレースバック技術が優先すべき目標は，被害ノードにおける早急な被害緩和対策を行うために，早急に攻撃パスを特定する技術を実現することである．

2. 単一手法による全体運用を想定

インターネットは， AS毎に独立した管理・運用が行われている．このため，特定手法による単一的なIPトレースバックの運用は，困難である．したがって，IPトレースバックには，AS毎に独立した運用可能であることが求められる

また，IPトレースバック・システムの運用コストは，各手法毎に異なる．例えば，ダイジェスト手法の場合は，各ルータ毎にパケットのモニタリング機構や，記録情報のストレージ領域が必須であり，その維持コストも大きくなることが考えられる．逆に，逆探知手法は，ネットワーク負荷の問題があるが，ストレージ領域は不要であるため，その維持コストは，ダイジェスト手法に比べて低いと考えられる．

このように，すべてのルータに対する改変を必要とするIPトレースバック手法やIPトレースバック用の情報を保管するためシステムの運用と保守を必要とする手法など，種々の提案手法毎に運用コストは異なる．よって，ISP等の予算や運用規模に応じて異なるIPトレースバック手法を運用する必要がある．

3. IPトレースバックに対する攻撃

日々分散型サービス妨害攻撃の手法が進化する状況を考えれば，攻撃者は，種々のIPトレースバック手法を分析しその弱点を狙った攻撃手法を開発す

ると予想される．我々は，攻撃者の抗IP トレースバック攻撃に対するIP トレースバックの改良や変更を行わなければならない．

したがって，柔軟にIP トレースバック手法の変更が可能な運用機構でなければならない．

既存の各研究は，理論・シミュレーションなどによる性能検証は行われている．しかし，インターネットという複雑なポリシーが絡んだ上で運用を行う上では，構造的な問題を持っており，現時点では，その運用の実現は困難であると考える．

そこで，これらの問題点を解決するために，本研究では，階層型IP トレースバック手法を提案した．

3. 階層型IPトレースバック手法

既存研究におけるIPトレースバック手法は，インターネットで運用する上で3つの大きな問題を持っていることを述べた．本章では，この問題点の解決したIPトレースバック技術である階層型IPトレースバック手法を提案する．本提案手法は，インターネットの経路制御機構を元に設計され，そして，IPトレースバックをインターネット上に展開可能なアーキテクチャを有している．

本章では，まず提案手法のアーキテクチャについて説明し，そして，その各構成要素の説明をする．

3.1 階層型IPトレースバックのアーキテクチャ

インターネットでの運用を前提としたIPトレースバック手法のアーキテクチャを設計するあたって，本研究では，現在のインターネット上での経路制御機構に着目した．

インターネットの経路制御は，単一の経路制御プロトコルによって行われているのではなく，ネットワークの規模もしくは管理ドメインに応じて，EGP (Exterior Gateway Protocol) と IGP (Interior Gateway Protocol) の二つに階層化されている．ASドメイン間での経路制御プロトコルには，EGPが用いられ，EGPに分類されるプロトコルとして，IPv4用はBGP (Boarder Gateway Protocol)4[29]，そして， IPv6用はBGP4+[30]がある．一方，ASドメイン内の経路制御プロトコルには，IGPが用いられ，IGPに分類されるプロトコルとして，OSPF (Open Shortest Path First) やIS-IS (Intermediate System-to-Intermediate System) が用いられている．

EGP運用では，図9に示すようにAS間において契約に基づいた相互接続 (ピアリング: peering) によって，経路の交換を行っている．各ASがEGPによって，相互接続し経路交換を行うことによって，インターネット上でのエンドツーエン

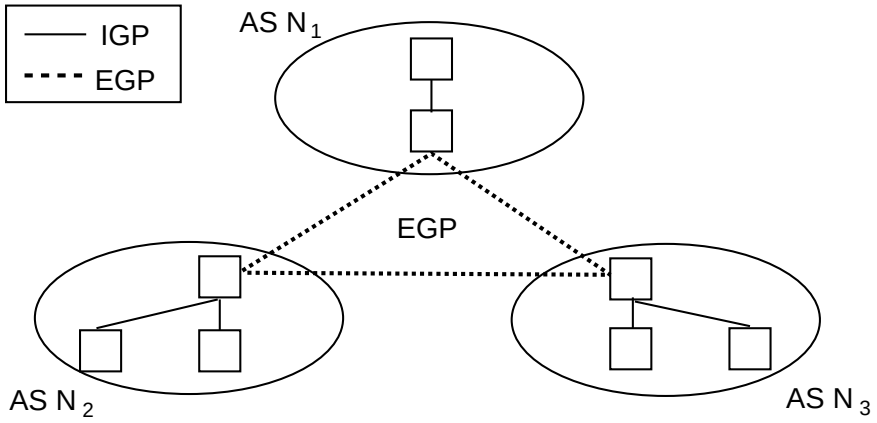

図 9 IGP と EGP の階層関係

ドの通信が可能となる.

この経路制御機構における「階層」の概念を IP トレースバックに適応した「階層型 IP トレースバック機構」の提案を行う.

本機構は,「ITM (IP traceback Manager) ネットワーク」,「Exterior IP (eIP) トレースバック機構」,「Interior IP (iIP) トレースバック機構」の 3 つの要素で構成されている.

ITM は，各 AS 上に一つ存在し，eIP トレースバックと iIP トレースバック間で IP トレースバックを行うために必要な情報を交換するために用いられる．各 AS 上の ITM は，ITM プロトコル (ITM Protocol, ITMP) を用いて各 AS の ITM と相互接続し情報交換を行う．この相互接続することによって構築されたネットワークを ITM ネットワークと呼ぶ.

そして，各 eIP/iIP トレースバックの対象となるネットワークの範囲は，図 10 に示すように経路制御の EGP/IGP の制御ドメインと同一である．eIP トレースバック機構は，AS ドメイン間の IP トレースバックを行う際に用いられる機構であり，iIP トレースバック機構は，AS ドメイン内において IP トレースバックを

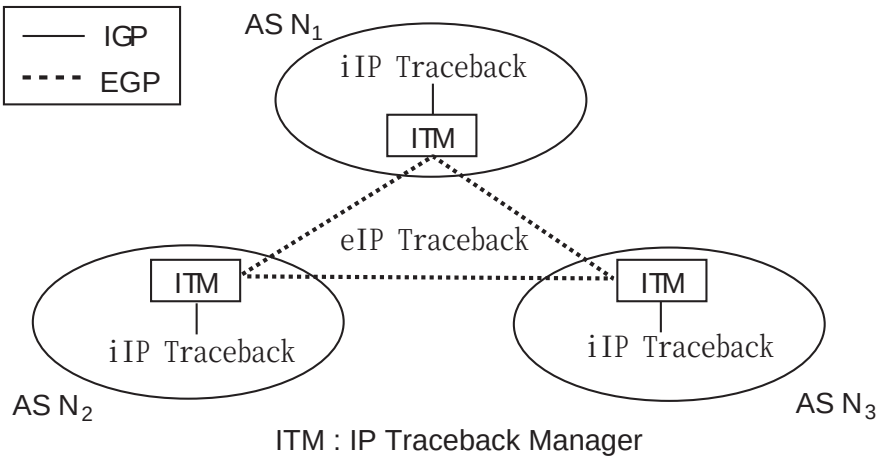

図 10 階層型 IP トレースバック機構

行う際に用いられる機構である．

eIP トレースバックによって，攻撃パスを AS 単位で高速に特定し，次に，iIP トレースバックによって，攻撃パスを IP アドレス単位で特定する．その過程における eIP から iIP トレースバックへの攻撃パス追跡のための情報移管は，ITM ネットワークを用いて行われる．

つまり，本提案手法は， AS 単位という大まかな情報であるが，短時間に攻撃パスの特定が可能である eIP トレースバックと時間はかかるが攻撃パスの IP アドレスまでを特定する iIP トレースバックの連携を ITM ネットワークを用いて行うという仕組みである．

この提案は，先に示した 3 つの問題を解決している．

- 完全な攻撃パスの特定が目的とする点に対して

  eIP トレースバックは，iIP トレースバックに比べて，短時間に攻撃パスの特定を AS 単位でおこなう．得られた AS 攻撃パス上の AS で，フィルタリングなど行うことによって，被害ノードにおける被害緩和を行うことがで

きる．そして，その後に，iIP トレースバック機構を用いて，完全な攻撃パスの特定を行う．

- 単一手法による全体運用を想定とする点と IP トレースバックに対する攻撃の脅威に対して

  本提案手法は，eIP/iIP トレースバックを ITM の管理下に納め，入出力情報の共通化をおこなっている．従って，eIP/iIP トレースバックの仕様に従った手法であれば，eIP と iIP トレースバックは，分離独立して行うことができる．

  よって，ドメイン毎に独立した iIP トレースバック機構の運用と，ドメイン間では，共通の eIP トレースバックを行うことによって，単一手法による全体運用は不要である．また，IP トレースバックに対する攻撃に対しても脆弱性のある IP トレースバックの切りはずしや仕様変更などを局所的に行うことができるため，IP トレースバックの攻撃に対して柔軟な対処が可能となる．

以上に述べるように，本提案手法は，既存の IP トレースバックがもつ問題点が解決可能なアーキテクチャとなっている．次に，本提案手法のアーキテクチャを実現するための各機構の技術的説明を述べる．

3.2 ITM ネットワーク

ITM は，本提案手法における eIP トレースバックと iIP トレースバック間の連携を行う上で非常に重要な機構である．これは，ITM 間のピアリングを行うために用いるプロトコル ITMP と各 eIP トレースバック，iIP トレースバックが ITM 間でやり取りする情報を共通化した ITM-API の 2 つで構成されている．

ITMP は，ITM 間で用いたれる通信プロトコルである．各 ITM 間で ITMP を用いて通信を行うことによって，ITM ネットワークが構築される．そして，ITM

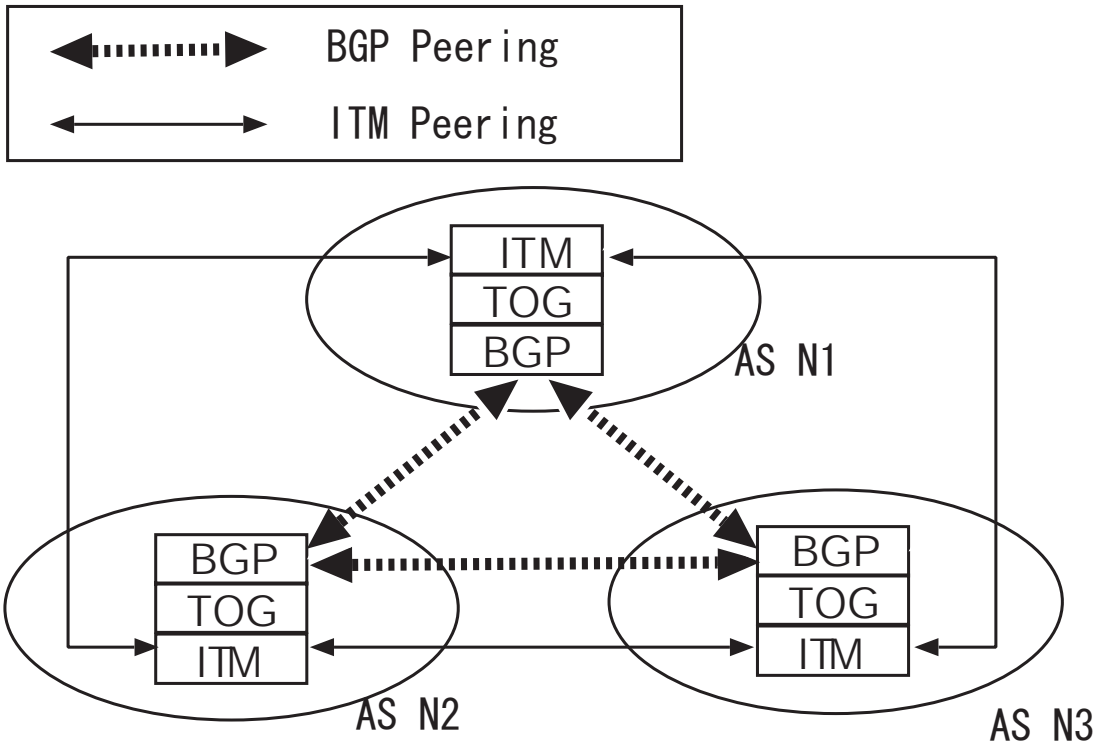

図 11 BGP ピアリングの AS に対して，ITM ピアリングも行う

のピアリング・パートナーは，BGP ピアリングにおけるパートナーと同様である．つまり，図 11 に示すように，ある AS_{N1} が，BGP のピアリングを AS_{N2} と AS_{N3} に対して確立している場合，ITM のピアリングも同様に，AS_{N2} と AS_{N3} に対して行う．したがって，ITM ネットワークのトポロジは，AS ネットワークのトポロジと同一となる．

各 ITM 上の eIP/iIP トレースバック機構は，ITM-API を利用することによって，ITM ネットワークを介したデータ転送が可能である．例えば，AS_x 上の eIP トレースバック機構が，隣接する AS_y の eIP トレースバック機構に対して，ITM-API を介して，データの送受信が可能である．また，eIP トレースバックから iIP トレースバックといった異なるエリアをカバーするトレースバック間の情報伝達

も可能な機能を有している．

3.3 ITM-API の定義

ここでは，eIP と iIP トレースバック間での連携を行うための ITM-API 定義について述べる．eIP トレースバックおよび iIP トレースバックと ITM 間はこの API を経由して，IP トレースバックを実行するための情報や，実行結果についての情報を交換をしなければならない．

eIP/iIP トレースバック機構と ITM の関係構成を図 12 に示す．各トレースバック機構は，図 12 に示すように ITM-API を介して ITM と接続されている．これにより，手法の異なる IP トレースバック手法が，各システム毎に独立したモジュールとして，ITM に接続することが可能である．先に述べた通り，各 AS の eIP/iIP トレースバック機構は，ITM-API と ITM を経由して，隣接の ITM 上の iIP/eIP トレースバック機構とのデータ交換が可能である．

また，本実装における ITM-API の設計は，既存研究におけるアルゴリズム解析や，実在する実装モデルの解析を行い，そのデータ交換すべき情報と制御するための機構の定義を行う．

参照する実装として，iIP トレースバックとしては，Hash-based IP トレースバックを NP (Network Processor) へ実装した横河電機 PAFFI[31] を使用する．PAFFI は，現在，IP トレースバックをための入出力インターフェースとして WEB を利用している．本研究では，その WEB インターフェース上で入出力される情報元に ITM 上に用いる ITM-API の設計を行う．

関連研究の調査結果から，既存の IP トレースバックを eIP/iIP トレースバックとして利用するために ITM と IP トレースバック間で交換する情報は次の項目となった．

1. **攻撃フローのパケットダンプ記録 (ITM から e/iIP へ入力)**

攻撃フローを構成するパケットの記録

2. **記録タイムスタンプ (ITM から e/iIP へ入力)**

   パケットを記録した際のタイムスタンプ

3. **記録ノード情報 (AS 番号/IP アドレス)(ITM から e/iIP へ入力)**

   記録を行ったノードの所属する AS 番号と IP アドレス

4. **攻撃パス情報 (e/iIP から ITM へ入力)**

   攻撃パスの検索結果

以上の 4 種類の情報を各 IP トレースバックと ITM 間で交換することによって，実在する実装を iIP もしくは eIP トレースバック・モジュールとして ITM と連携させることが可能となっている．

また，eIP トレースバックとして，本研究で提案・開発した IP オプション・トレースバック実装を利用し，同様に，ITM-API の設計に反映した．

以上の結果をまとめ ITM-API を定めた．それは，大きく分けて 3 種類の API に分類できる．

- **ITM 情報交換 API:**

  この API は，各 eIP/iIP トレースバック機構がその接続している ITM および，ITM ネットワークの情報を入手するために用いる．その情報は，接続を確立している近隣 ITM の AS 番号，接続状態，サポートする eIP/iIP トレースバックである．

- **データ交換 API:**

  この API は，隣接する ITM の eIP/iIP トレースバックモジュールと通信を行うために用いられる．この API を介して，隣接 ITM の eIP/iIP トレース

バック・システム同士でのデータ交換 (ITM はデータ中継を行うパイプとなる) や，同 IP トレースバック・システムの状態を入出力する．

- **トレースバック要求と応答 API**:

  この API は，各 eIP/iIP トレースバックシステムの実行やその中断といった制御を行うために用いられる API である．この API によって，攻撃フローのパケットダンプ情報 (記録タイムスタンプ，記録ノード AS 番号/IP アドレス) 入力，攻撃パス情報出力，IP トレースバックの制御 (中断，状況報告など) を行うことができる．

各 IP トレースバックが ITM-API を利用することにより，他 AS の IP トレースバックシステムとのデータ交換や連携が容易に行うことができる．そして，各 eIP/iIP トレースバック機構へのアクセス制御や利用記録といった管理機構を ITM の元に一元化することができる．

また，ITM-API は，既存実装における入出力項目の調査結果を元に設計されている．このため，ITM との連携部分の実装は，既存の実装と独立して行うことができる．したがって，既存の各 IP トレースバックは，その機能の制約を受けることなく，IP トレースバックと iIP トレースバック間の連携性を得ることができる．

よって，ITM 上の IP トレースバックは，各 AS との連携を ITM ネットワークを用いて行うプロトコル・デザインが可能となる．本提案手法である IP オプション・トレースバックは，ITM-API を介して ITM ネットワーク利用し，隣接 AS と連携し攻撃パスの構築を行う．

以上が ITM-API の説明である．本 API は，既存研究の手法をベースに定義されているが，将来登場しうる新たな IP トレースバック手法によっては，下位互換性を残しつつ拡張を順次行う予定である．

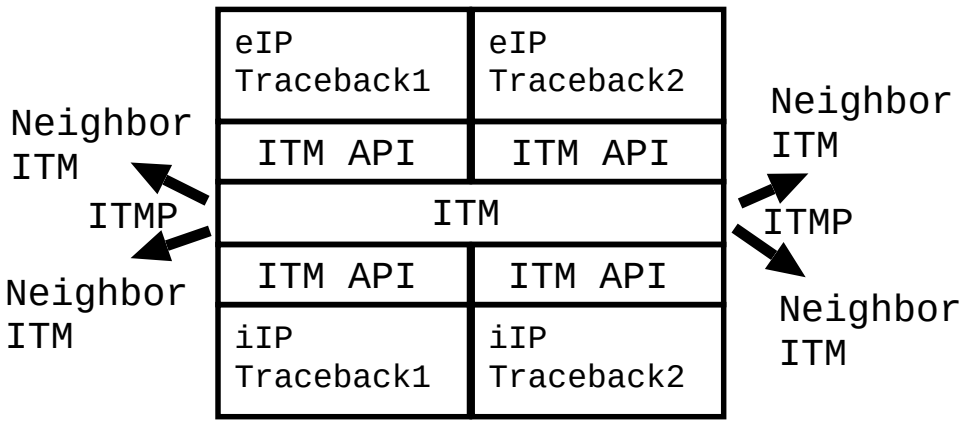

図 12 ITM におけるモジュール構成

3.4 ITMP: ITM Protocol の定義

ITMP は，ITM 間の通信に用いられるプロトコルである．BGP によってピアリングを行っている AS 間で，ITM についても同様に ITMP を用いてピアリングを行うことで ITM ネットワークは構築される．この ITM ネットワークを構築するために，近接 ITM 間で認証や IP トレースバック制御といったデータ交換が必要である．ITMP は，ITM 間の認証や制御を行うために定義された状態遷移を伴う通信プロトコルである．ITMP は，TCP プロトコルをトランスポート層プロトコルとして使用する．そのポート番号は，IANA への申請はしていないが 13000 を使用する．

図 13 は，ITMP における状態遷移を示している．ITMP は，認証フェーズ (authentication phase) と接続確立フェーズ (connected phase) がある．

認証フェーズは，隣接する ITM 間でピアリングを確立するに当たって，ピアリング相手のユーザとパスワードを元にしたアクセス制御を行う．この認証には，一方向性ハッシュ関数である MD5[32] を用いて，チャレンジング認証をおこなっている．この認証機構によって，クリアパスワード交換によるパスワード漏洩を

防止している．

認証は，相互にユーザ名とパスワードを検証することによって完了する．具体的には，ITM_A がピアリングを行う ITM_B に対して TCP/13000 番ポートに対して，TCP コネクションを確立する．そして，まず，ITM_B が，ITM_A からのユーザ認証を行う．その後，次に，ITM_B がユーザ名とパスワードを提出し，ITM_A が ITM_B のユーザ認証という過程となる．

双方の認証完了後，双方の ITM が，近隣情報 (AS 番号，利用可能な eIP トレースバックと iIP トレースバック) の交換を行う．以上で認証フェーズは終了である，その後，接続確立フェーズに移行する．

接続確立フェーズにおいては，各 eIP/iIP トレースバック機構の実行や，ITM モジュールによる隣接する AS の IP トレースバック・モジュール同士での ITM ネットワークを介したデータ交換を実行する．

そのプロトコルは，ITM 自体の基本制御を行うため (ピアリング切断や，隣接 ITM の状況確認など) 基本プロトコルと各 eIP/iIP トレースバック機構が独自に ITMP を利用して行う拡張プロトコルに分かれている．

基本プロトコルのコマンドは，各 eIP/iIP トレースバック機構が ITM-API を通して実行することができる．拡張プロトコルは，前者の基本プロトコルにおいて呼び出すコマンドが定められており，そして，各 eIP/iIP トレースバック毎に定めなければならない．

3.5 eIP トレースバック機構と iIP トレースバック機構の技術要件

ここでは，eIP トレースバック機構と iIP トレースバック機構の技術要件を述べる．

eIP トレースバック機構は，短時間に攻撃パスの AS を特定することを目的とする．本研究では，eIP トレースバックにおける攻撃パスの探索時間の目標は，追跡開始から 30 分以内と定めた．この値は，CAIDA[33] の分散型サービス妨害攻

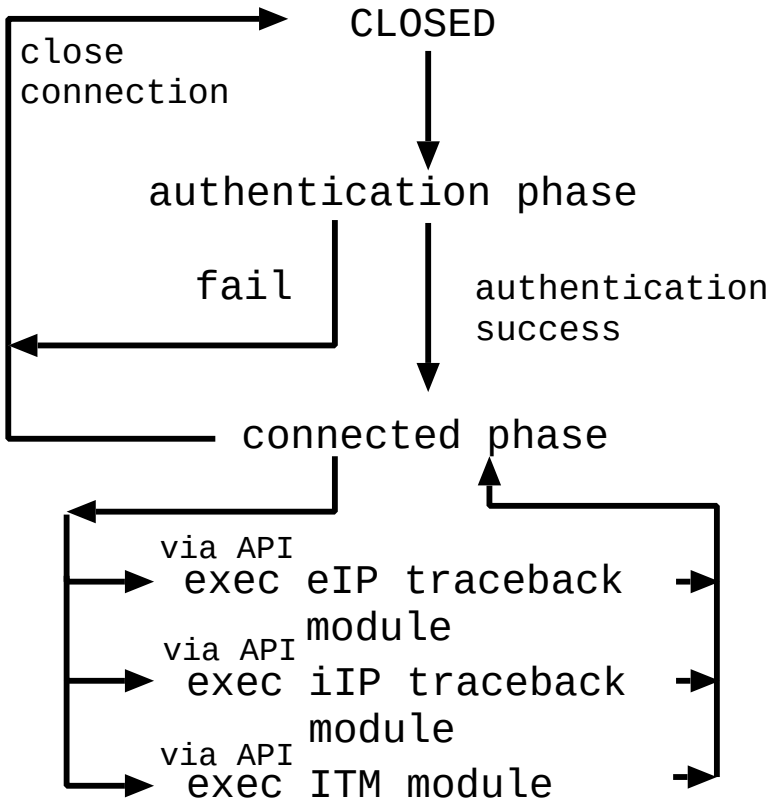

図 13 ITMP の状態遷移

撃の活動に関する研究報告において，分散型サービス妨害攻撃は，攻撃開始から約 30 分で一旦終了し，その後は，断続的に発生する状態となっている活動報告から定めた．

攻撃パスの AS が特定によって，その経路上で被害ノードに対するフィルタリングなどの対策を行うことができる．その着手にかかれる時間は，短いほど被害量の軽減につながる．

以上のように，攻撃パスが AS 単位で特定可能であり，かつ，30 分以内での攻撃パスの特定が可能な IP トレースバック手法は既存手法として提案されていない．そこで，本研究では,「IP オプショント・レースバック」を提案した．本手法は，先に紹介した iTrace 等が分類されてる逆探知パケット手法である．

AS 間の特定は，ポリシーの異なる AS 間をまたがる追跡が必要であるために，IP トレースバック手法として，システムの負担がもっとも小さい逆探知パケット手法を利用した．このプロトコルのより詳しい説明は，後に述べる．

一方，iIP トレースバック機構は，攻撃パスのルータ (IP アドレス) を特定することを目的とする．つまり，既存の研究における IP トレースバック技術が iIP トレースバックとして利用できることとなる．

したがって，iIP トレースバック機構の技術要件は，既存のルータが特定可能な IP トレースバック機構に ITM との連携するための機構 (ITM-API) を組み合わせたものを満たさなければならない．

以上が，eIP トレースバックと iIP トレースバックの技術要件である．

3.6 本提案手法おける攻撃パス特定までのシナリオ

本手法による分散型サービス妨害攻撃への対策は，次に示す過程を経て行われる．

1. **攻撃フローの記録**: 被害ノードの管理者は，所属する AS の管理者へ攻撃フローに対する対策を要求する．AS 管理者は，被害ノードにおいて攻撃フ

ローのモニタリングと記録を行う．

2. **eIP トレースバックの実行**: 記録から eIP トレースバックによって攻撃フローが通過した AS で構成された攻撃パスを求める．

3. **初期対策の実行**: 攻撃パス上の AS は，フィルタリングや帯域のシェーピング等の対策を行い被害者に対する早急な被害の緩和を行う．

4. **iIP トレースバックの実行**: 各攻撃ノードの存在する AS 上で iIP トレースバックを行い，攻撃ノードの IP アドレスを特定しネットワークから遮断する．

5. **攻撃の収束**: 攻撃ノードのネットワークからの分離により，攻撃フローは収束し，分散型サービス妨害攻撃は終了する．

上記に示す過程のように，eIP トレースバックによる AS 単位の大まか攻撃ノードの位置特定によって，被害ノードにおける被害の緩和を行い．そして，iIP トレースバックによって，攻撃ノードの特定による攻撃フローの収束を行う．

4. IP オプション・トレースバック手法

本研究では，IP オプション・トレースバックを eIP トレースバックの 1 手法として提案する．本章では提案手法の説明を行う．

4.1 IP オプション・トレースバックの構成

本研究で提案する IP オプショントレースバックは，eIP トレースバック手法の一つである．その逆探知パケット用のパケットには，IPv4 の場合，IP オプション・パケット，そして，IPv6 の場合，拡張オプションヘッダの終点オプションヘッダ (2) を利用する．

本手法は，PM (Packet Monitor) と TOG (Traceback Option Generator) の 2 つの機構で構成されている (図 14)．PM は，AS 上の各 BGP 境界ルータ (Border Router) 上に存在し，AS 外へフォワーディングされる IP パケットの観測とサンプリングを行う．TOG は，各 AS 上に 1 つ存在しその AS 内の PM の管理と IP オプションを用いた逆探知パケットの生成と解析を行う．

PM は，次に示す 2 つの機能で構成されている．

1. **パケットの選択**: ルータの各インターフェース出力から，確率 P でパケットを選択しコピーする．

2. **TOG との連携**: PM は，TOG から要求に応じた確率 P の設定や選択したパケットの TOG への転送を行う．

次に，TOG の機能について述べる．TOG は，5 つの機能で構成されている．

1. **IP トレースバック・オプションの生成**: TOG は，選択されたパケットとパラメータ (AS 番号，擬装防止用ハッシュ情報) から IP トレースバック・オプションを生成し送信する．

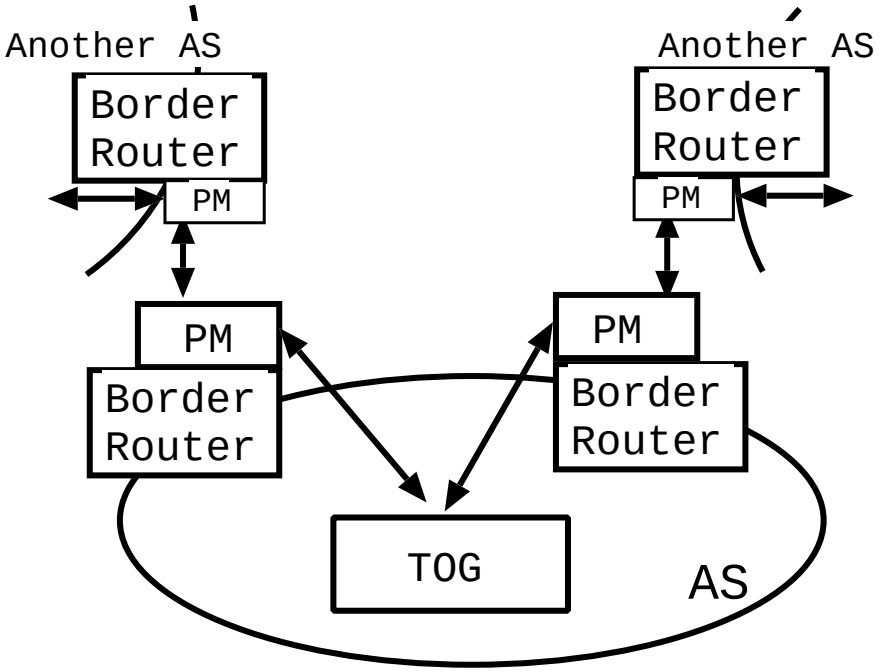

図 14 IP オプション・トレースバックの構成

2. **オプション管理**: TOG は，AS メッセージ鍵 X と鍵識別番号 Z を生成し管理する．ハッシュ情報は，AS メッセージ鍵 X の鍵識別番号 Z から HMAC (Keyed-Hash Message Authentication Code)[34] を用いて生成される．

3. **PM との連携**: TOG は，PM でパケットを選択する際に用いる確率 P を各 PM へ送信する．

4. **パケットの検証**: TOG は，IP トレースバック・オプション中の HMAC 認証を検証し，攻撃パスの構築を行う．

5. **ITM 間の連携**: 攻撃パスの構築のために，TOG は，近隣の TOG との間で，攻撃パスや IP トレースバック・オプションを ITM ネットワークを用いて交換する．TOG は，ITM ネットワークを利用して iIP トレースバックの実行と結果の取得を行う．

上記の過程で生成される IP トレースバック情報は，オプションヘッダに収容される．IPv6 の場合，終点オプションヘッダの構成は，図 15 になっており，各項目の内容を次に示す．

- **HMAC タグ番号 (HMAC Tag Number) (16bit)**: HMAC で使用した HMAC アルゴリズム識別子
- **ルータアドレス (Router Address) (v4: 32bit/ v6:128bit)**: PM のアドレス
- **送信元アドレス (Source Address) (v4: 32bit/ v6:128bit)**: 追跡対象パケットのソースアドレス
- **鍵識別番号 (Identify Number) (64bit)**: HMAC で使用した AS メッセージ鍵 X の鍵識別番号 Z

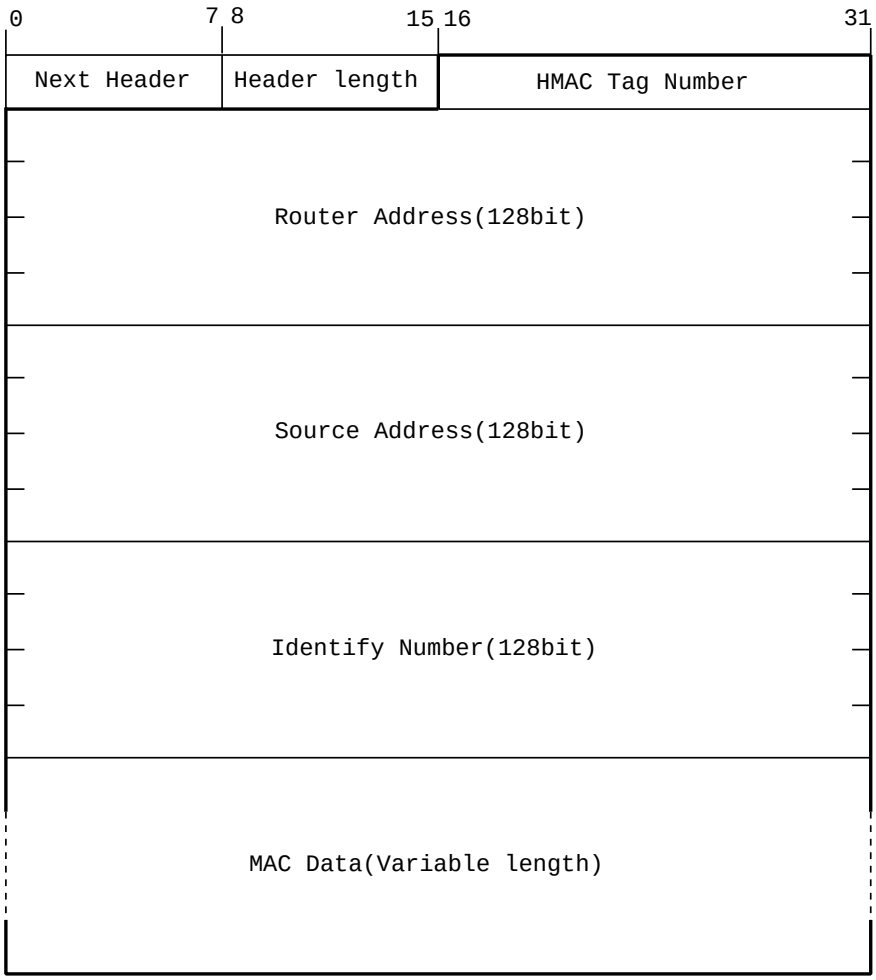

図 15 終点オプションヘッダにおける IP オプションの構成

- **MAC データ (MAC Data) (アルゴリズム依存，可変長)**: 自 AS 番号と次 AS 番号，AS のメッセージ鍵 X から生成した HMAC 認証データ H

本手法では，AS 番号を HMAC 認証によって MAC データにすることによって，IP トレースバック・オプションに AS 番号をクリアテキスト形式で保持しないようにしている．これは，ICMP トレースバックの持つ逆探知パケットからのネットワークトポロジー情報が流出するという問題点を解決している．

ここでは，自 AS 番号を AS，次 AS 番号を AS_{NEXT}，鍵識別番号 Z と一意に対応するメッセージ鍵 X_Z，HMAC 認証で用いるハッシュ関数 H とした場合，MAC データは，

$$MAC = H(AS, AS_{NEXT}, X_Z) \tag{3}$$

となる．よって，IP トレースバック・オプション O は，

$$\begin{aligned} O \quad = \quad & (HMAC_{tag}, \text{生成元アドレス}, \\ & \text{送信元アドレス}, Z, MAC) \end{aligned} \tag{4}$$

となる．なお，メッセージ鍵 X や鍵識別番号 Z 等のパラメータ管理は，TOG が一元管理を行う．

本手法では，通過した AS の前後関係や距離を逆探知パケットに組み込むのではなく，通過した自 AS 番号と次 AS 番号のみを記録する．そのため，攻撃パスの構成には，AS 間のつながりを示したネットワーク・トポロジ情報が必要となる．これらは，各 AS 上に 1 つ存在する ITM 同士が相互接続された ITM ネットワークから入手できる．

ITM ネットワークのトポロジは，トラフィックが通過する AS パスを示している．よって，各ITM 上の TOG は，攻撃フローに含まれる IP トレースバック・オプション中の MAC データが自 TOG から生成したものであるかどうかを HMAC 認証によって検証することで，攻撃フローが自 AS を通過したかどうかを判断で

きる．攻撃パスは，攻撃フローが通過しているAS同士をITMネットワーク上のパスに従って接続することで入手できる．

そして，より詳細な検証過程を次に述べる．

4.2 IPオプション・トレースバックの動作

定常的にTOGは，攻撃パス構成の際に必要な逆探知パケットを次にに示す過程に従って送出する．まず各境界ルータ上のTOGが，自AS外へ交換される全IPパケットの中から確率Pに従って追跡対象のIPパケットを抽出しコピーを行う．コピーされた全IPパケットには，自ASを通過したことを示す情報が入ったIPトレースバック・オプションが挿入される．送信元アドレスは逆探知パケットを送出するノードのアドレスに書き換えられて送出される．

そして，送出された逆探知パケットからの攻撃パスの構成は，次のステップを踏んで行われる

1. 分散型サービス妨害攻撃による被害ノードの発生
2. 被害ノードの管理者から属するASの管理者への分散型サービス妨害攻撃の被害報告と攻撃フローの調査・停止要求
3. AS管理者は，IPトレースバック・オプションの取得のためにAS_V上の被害ノードVにおいて，攻撃フローのトラフィックの記録を行う（図16の(1)）．
4. 記録結果からIPトレースバック・オプションの付加されたIPパケットを抽出し，IPトレースバック・オプションの集合Oを生成する．
5. Oと攻撃パスT，探索深度HをTOG_VがITM_Vを経由して，隣接AS_nのTOG_nへ入力する（図16の(2)）．
6. TOG_nは，経路表から被害ノードを宛先とする場合の次ホップのAS_{next}を検索する．そのAS_{next}が前TOGであるTOG_{n-1}のAS_{n-1}と一致するかど

うかを判定する．一致するなら，被害ノードへの経路上に AS_n-AS_{n-1} というパスが存在するため，7. へ，そうでなければ，11. へ

7. AS メッセージ鍵 X_n と識別番号 Z_n から自 AS の MAC データ $HMAC_n$ を求め，IP トレースバック・オプション O の中の MAC データ $HMAC$ と鍵識別番号 Z から，MAC データの比較を行う．一致する場合は，攻撃フローが AS_n を通過したことを示すため，8．へ，ない場合は，11．へ（図 16 の (3)）．

8. 攻撃パス T_n に自 AS 番号 n を加え，探索深度 H を 1 減らす．もし，H=0 の場合は，11. へ

9. O から AS_n で一致したオプションをのぞいた O' とする．O' = 空集合 の場合は，11. へ．

10. O' と T_n と H' を TOG_n の隣接 AS の TOG へ ITM を経由し出力し，6．へ（図 16 の (4)）．

11. O を入力した TOG に対して攻撃パス T を返答する（図 16 の (5)）．

これによって，攻撃パス T が求められ，攻撃フロー発生源の AS が特定できる．

以上が本手法の提案内容である．次に，本手法の IP オプションを用いた逆探知パケットがインターネットのトラフィックに与える影響について述べる．

4.3 IP オプション・トレースバックにおける帯域負担と攻撃パスの特定時間

ここでは，生成確率とネットワークに与える負荷の関係について，実トラフィックを元におこなった考察を述べる．IP オプション・トレースバックは，逆探知パケット手法を使用する．このため，本提案手法を運用するためには，攻撃パス探

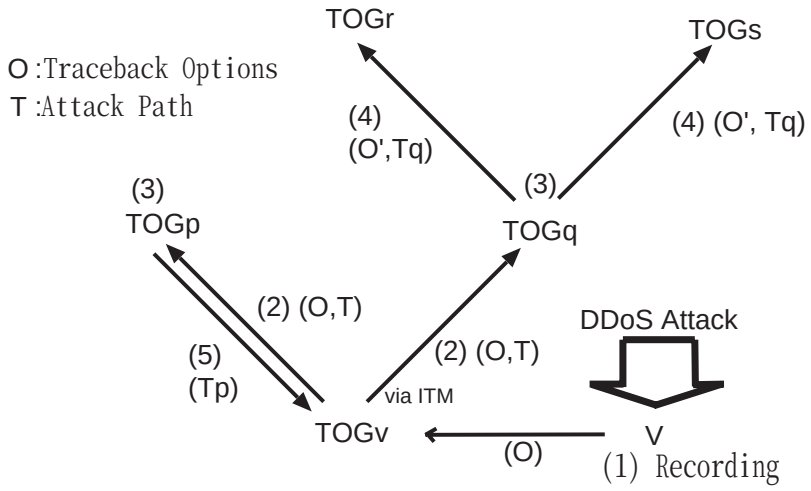

図 16　攻撃パス T の構築過程

索に要する時間とネットワークへの負担の双方を考慮した生成確率のパラメータを定めるための指針が必要である．そこで，生成確率とネットワーク与える負荷の関係にトレードオフを明らかにすることにした．

まず，確率 P でオプションパケットの生成を行った場合，パケットの複製に対してオプションパケットが組み込まれるため，各 AS におけるトラフィックの増加率 D は，

$$D = P \tag{5}$$

となる．また，AS から流出する IP パケット数を R[pkt/s] とし，R に含まれる攻撃フローの割合を A とすると，被害ノードに AS からのオプションパケットが到達する間隔 T[s] は，

$$T = \frac{1}{PRA} \text{ [s]} \tag{6}$$

となる．

ここで， WIDE プロジェクト (AS 2500)[35] の AS 境界ルータにおける AS 外

への流出トラフィックを計測した結果，流出バイト数O[byte/s]，および，Rは，

$$O = 1134 \text{ [Kbit/s]} = 141 \text{ [Kbyte/s]} \tag{7}$$

$$R = 415 \text{ [pkt/s]} \tag{8}$$

であった．確率Pは，BellovinがiTraceで提唱する$P = \frac{1}{20000}$を中心に，その前後である$P = \frac{1}{10000}$，$P = \frac{1}{30000}$の3点を選択した．本AS上の攻撃ノードからの攻撃フローの量F [byte/s]と被害ノードが当ASのオプションパケットを確認するまでの時間Tの関係を図17に示す．例えば，$P = \frac{1}{20000}$，攻撃フロー$F = 8$[Kbyte/s]のときは，

$$\begin{aligned} A &= \frac{F}{O} = \frac{8.0 \times 10^3}{141 \times 10^3} \\ &= 56.7 \times 10^{-3} \end{aligned} \tag{9}$$

$$\begin{aligned} T &= \frac{1}{PRA} = \frac{1}{\frac{1}{20000} \times 415 \times 56.7 \times 10^{-3}} \\ &= 850\text{[s]} \end{aligned} \tag{10}$$

となる．

トラフィックがn個のASを通過した後のオプションパケットによるトラフィックの増加がd倍となるとすると，

$$d = (1+P)^n \tag{11}$$

となる．トラフィック増加率$P = 5 \times 10^{-3}\%$の時，WIDEプロジェクトにおける最大ASパス長は$n = 16$であることから，終端ノードにおいて増加トラフィックは，$(1+P)^{16} - 1 = 0.8 \times 10^{-3}$倍である．なお，Huston[36]は，2001年における平均ASパス長の変動が3〜5.5であるとしていることから，$(1+P)^n$における$n = 16$の値は十分大きな値である．そして，その値は十分に実用になる範囲に収まっており，インターネットにおける増加トラフィックの問題はないと考察できる．

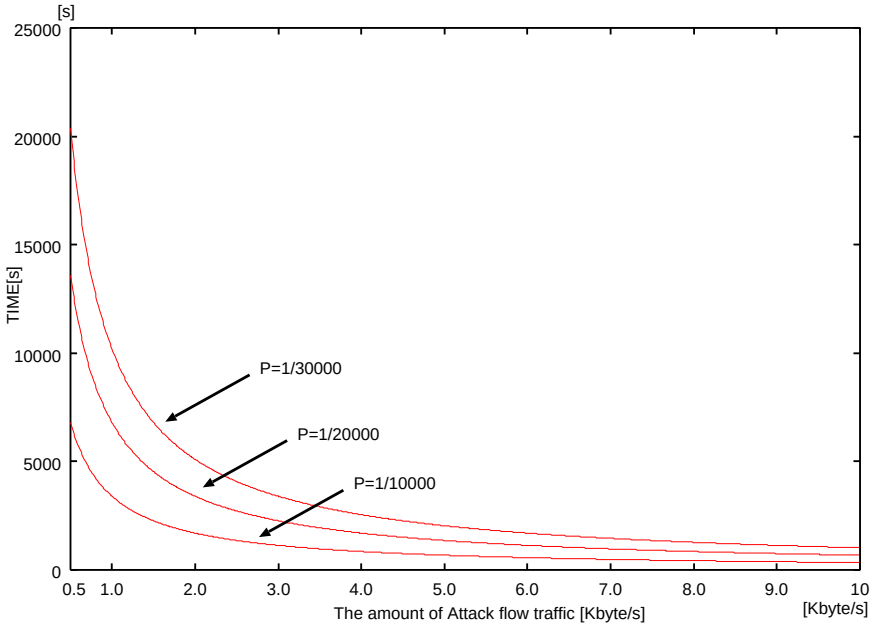

図 17 確率 $P = 1/10000$，$1/20000$，$1/30000$ における攻撃フロー F と T の関係: WIDE Project の境界ルータより

また，トラフィック被害ノードは約 14 分のモニタリング結果で本 AS が攻撃フローに係わっていることが特定が可能であり，目標としているサービス妨害攻撃の収束時間である 30 分から考えれば十分短いと結論できる．図 17 より攻撃フローが少ない (より攻撃ノードに近い) 場合，確率 P を高めることで攻撃ノードの AS からのオプションパケットを短時間で拾うことが分かる．したがって，固定的に確率 P を運用するのではなく，外部の IDS(Intrusion Detection System) システムによる攻撃検知や ITM からの近隣の IP オプション・トレースバックの稼動状況など情報によって，動的に確率 P を変化させる事によって，より短時間に IP オプション・トレースバックによる攻撃パス特定が可能となる．

5. インターネット・エミュレーション環境での検証

本提案手法の有効性は，実インターネット環境のエミュレーション上で実装を用いた性能検証によって示す.

まず，提案手法の全体の検証過程について述べ，本研究における検証過程の範囲について述べる.

その範囲に従った検証は，1. 提案手法のプロトタイプ実装と動作検証を行い，そして，2. 大規模なシミュレーション設備を利用した性能検証という 2 段階を経ておこなった.

1 段階目において，プロトタイプの実装開発は，FreeBSD/NetBSD/Windows の 3 種類のプラットフォーム上で動作するように行った．そして，その動作検証を 5 台の PC 上で行った.

次に，2 段階目において，通信・放送機構北陸 IT 研究開発支援センター [37] におけるシミュレータ研究設備を用いたエミュレーション環境上で，本提案手法の性能評価を行った.

5.1 提案手法の検証過程

ここでは，提案手法を実現する上での全検証過程について考察し，本研究における検証の範囲を明らかにする.

本提案手法の実インターネット上での有効性を示すためには，次に示す過程に沿った検証が必要であると考える.

1. 提案手法を具体化するためのアーキテクチャ設計とその定性的考察.

2. アーキテクチャ設計に基づくプロトコルの仕様策定と実装の開発，および動作検証

3. 50 程度の小規模な AS 間に展開される ITM ネットワーク上での eIP トレー

スバック (IP オプション・トレースバック) の動作検証.

4. 各 ITM 上で eIP トレースバックから ITM を介した iIP トレースバックへの連携検証.

5. 100 を超える大規模な AS 間における ITM ネットワーク上での eIP トレースバックの動作検証.

6. 実インターネットでの実証実験.

本研究では，項目 (1)，項目 (2) および (3) までの実施を行う．

項目 (4) の実施は，本実装で用いるために準備を進めている PAFFI との連携部分の実装が不可欠である．しかしながら，現在は，API 設計のみで，実装は完成していない．PAFFI システム自体は，その動作検証が完了しているため，これまでに述べてきた ITM-API に従ったパラメータが入力されれば，IP トレースバックを行うことが可能と考えられる．したがって，本研究では，その iIP トレースバックとして動作する点までの検証は行わない事とした．

項目 (5) の実施は，そのコストと得られる効果を考え，今回は見送った．その理由は，項目 (5) の実施は，その規模に沿った機材の準備など項目 (3) に比べてそのコストが必要である．このため，項目 (3) における検証結果を基にその実験環境を含めた検証を行ない．その検証から得られた問題点とその改善を提案手法に対して行った上で，実施しなければいけないからである．

項目 (6) についても項目 (5) に同様であり，その実施は，さらなるコストを要するため，慎重を要する．

以上の事から，検証に要するコストを考慮した結果，本提案手法における性能評価は，項目 (3) までの時点で達成可能であると考えた．

項目 (1) に関しては，ここまでの時点において述べた．項目 (2) における実装プロトタイプの実装と動作検証そして，実インターネットでの運用規模を考慮し

た項目 (3) の検証は，本章において述べる．そして，その項目 (3) までの結果についてのまとめと考察を 6 章で述べる．

5.2 プロトタイプ実装の構成

本節では，FreeBSD 4.7 および，NetBSD 1.6 上で開発したプロトタイプ実装のアプリケーション構成について述べる．

本実行コードは，ITM 部，IP オプション・トレースバック (TOG/PM) 部で構成されている．ITM 部は，eIP トレースバックとして，IP オプション・トレースバックが組み込まれているが，現時点では，iIP トレースバックは組み込まれていない．これは，PAFFI を ITM と接続するための設計と検証は行なったが実装は完了していないからである．

すべての開発に用いたコードは C を用いた．また，ライブラリは標準ライブラリを用いたが，IP オプション・トレースバック PM 部においては，パケットのキャプチャを行うために libpcap ライブラリ [38] を使用し，また，TOG 部には，パケットの生成を行うために libnet ライブラリ [39] を外部ライブラリとしてそれぞれ利用した．

ITM 間や IP オプショントレースバックにおける TOG と PM 間の通信には，IPv4/v6 デュアルスタックを考慮した開発を行い，IPv4/IPv6 双方での利用が可能となっている．したがって，IPv4/IPv6 毎に独立した ITM ネットワークが構築可能となっている．なお，IPv6 上と IPv4 上での ITM および，その IP トレースバックは，インターネット・プロトコルのバージョン毎に，互いに独立して運用しなければならない．

IP オプション・トレースバック PM は，パケットのモニタリングをルータで行わなければならない．このため，既存インフラストラクチャへの影響を最小限にしつつ，ルータのトラヒック・モニタリングを行う必要がある．

本プロトタイプ実装では，図 18 に示す構成によって，PC 上のモニタリング用

に割り当てたネットワーク・インターフェース・カード (Network Interface Card: NIC) を流れるトラフィックを PM 部でモニタする．ルータの観測対象となるネットワーク・インターフェース・カードの出力をイーサーネット・スイッチングハブのミラーポート (Mirror port)(図 18 の (1)) や電気・光スプリッタ (Spliter)(図 18 の (2)) を利用して分岐し，PC のモニタリング用ネットワーク・インターフェース・カードに接続する．これによって，ルータから出力されるトラフィックが分岐され，PC のネットワーク・インターフェース・カードへ送信される．そして，そのトラフィックは，PM 上でモニタリングされ IP オプション・トレースバックのアルゴリズムにしたがって，パケットの抽出が行われる．

以上より，本プロトタイプ実装は，既存のインフラを用いた実証検証も十分可能な実装構成となっている．

5.3 プロトタイプ実装の動作検証

プロトタイプ実装の動作検証は，図 19 のように構成された小規模ネットワークテスト環境で行った．この環境は，ルータとなる 5 台の PC とそれらを収納する L2 スイッチ (L2 Switching HUB，Extremenetworks 社製 Summit48) および，トラヒック生成機 (Traffic Generator，Agilent 社製 Router Tester)，そして，これらのネットワーク構成変更やトラヒックの制御を行うコントローラ機 (Ctrl. Unit) で構成されている．各 PC は，2 つ以上のネットワーク・インターフェース・カードを持ち，すべてのネットワーク・インターフェース・カードは，L2 スイッチに収納されている．コントローラ上で，L2 スイッチハブのバーチャル LAN を設定する事によって，物理的な変更を行うことなく柔軟なトポロジ設計が可能となっている．また，トラヒック生成機とバーチャル LAN の組み合わせによって，数十ノード程度の攻撃ノードから生成される攻撃フローの生成と観測が可能となっている．

今回は，本システム上の各 PC を独立した AS と想定し，eIP トレースバックと

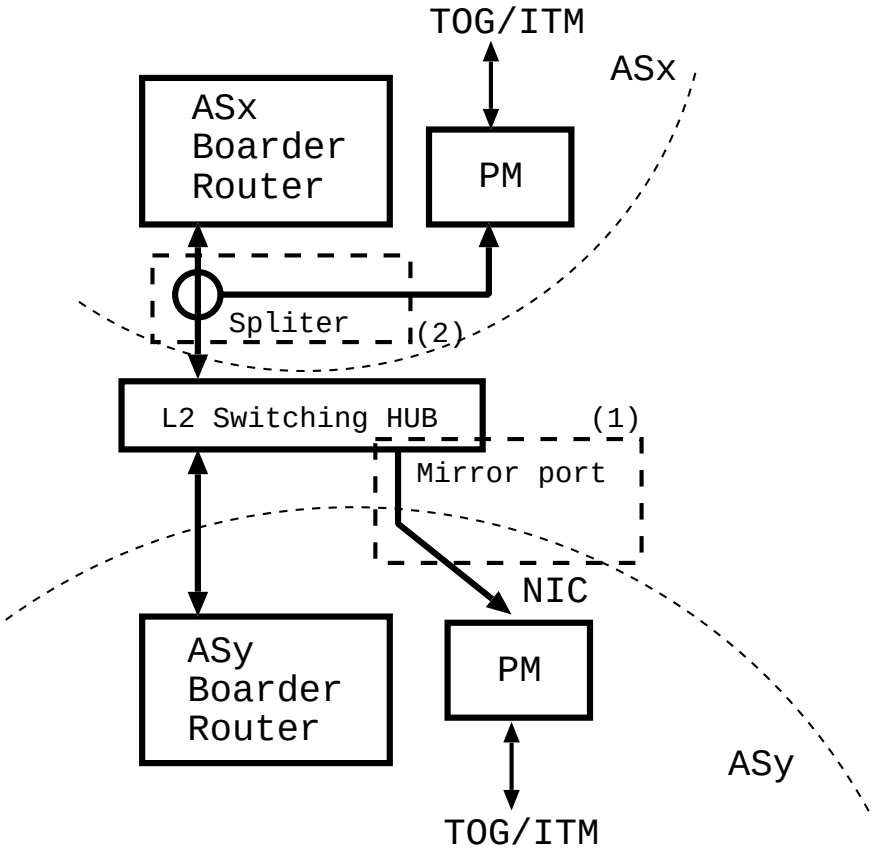

図 18 プロトタイプ実装におけるトラフィックのモニタリング構成

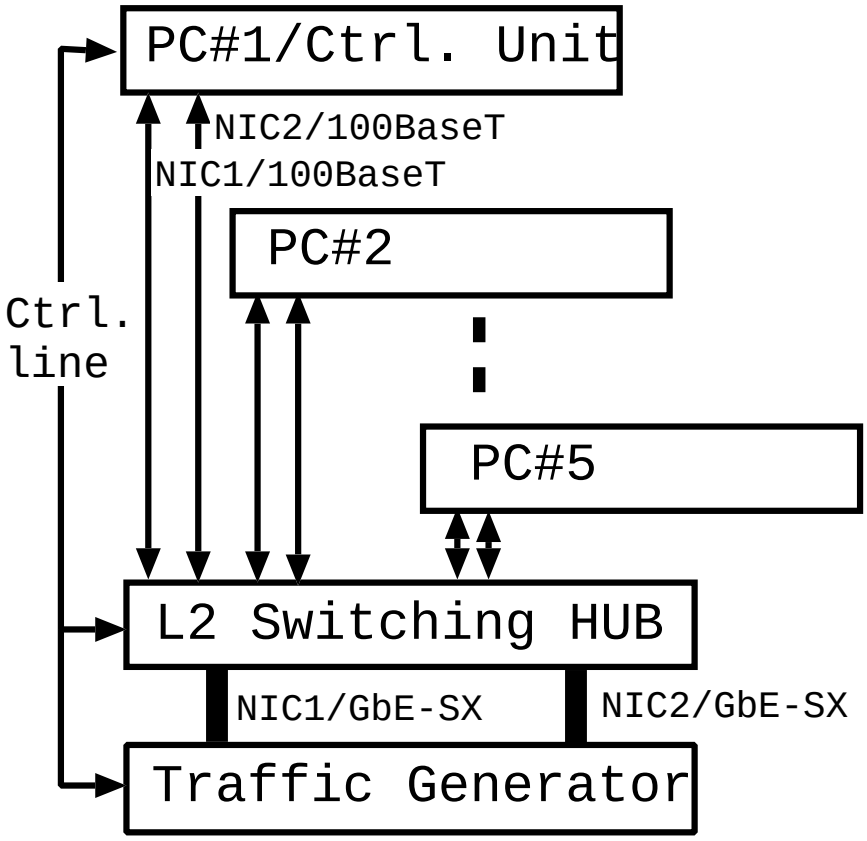

図 19 検証用システムの構成

ITM ネットワーク間の実装動作検証を行った．iIP トレースバックは，eIP トレースバックや ITM ネットワークとは独立に閉じた環境で実行される．また，先に示すように連携部分の実装が未完了である事から，ITM からの iIP トレースバックを行うための情報を受け取るのみのスタブ・モジュールとした．

以上の実験環境下で，プロトタイプ実装が設計に従った動作することを確認した．

5.4 インターネット・エミュレーション環境での実験

次に，本提案手法を通信・放送機構北陸 IT 研究開発支援センターにおけるシミュレータ研究設備を用いた実験を行った．この研究設備は，512 台の PC がイーサーネットや ATM を用いてネットワーク接続されており，これらの PC を用いたシミュレーション等の実験が可能な環境となっている．

本研究では，本設備のうち 64 台の PC を利用した実インターネットに基づく AS トポロジーを構築し，インターネットのエミュレーション (模倣) を行った．そして，3.6 節で述べた攻撃パス特定過程における eIP トレースバック (IP オプション・トレースバック) の動作結果までの実験をおこない．その性能評価を行った．

5.5 実験で用いたハードウエア構成

実験に用いた機器のハードウエア接続構成は，実験用 PC が 64 台，レイヤー 2 スイッチが 2 台，管理用 PC が 2 台で，その接続構成を図 20 に示す．

実験に用いた PC のハードウエア・スペックを表 1 に示す．これらの PC は，2 つのネットワーク・インターフェース・カードを持っている．一つは，PC への遠隔ログインによる管理を行うための管理用セグメントに接続されている．もう一方は，実験のために利用する実験用セグメントに接続されている．

今回は，管理用セグメント (図 20 の L2 Switch#1) を利用して，各 PC 上で

表 1 実験に用いた PC の構成

ハードウエア	構成
CPU	Intel PentimumIII-800Mhz
メモリ	512Mbyte
ハードディスク・ドライブ	60 Gbyte
ネットワーク・インターフェース・カード 1	100Mbps 管理用セグメントに接続
ネットワーク・インターフェース・カード 2	100Mbps 実験用セグメントに接続

のオペレーティングシステムのネットワークブートや遠隔ログインによる操作を行なった．管理用 PC は，各 PC をネットワーク・ブート (PreBoot Execution Environment:PXE ブート) の際にオペレーティングシステムの転送や，各種設定ファイルの転送を行う事を目的としている．

実験用セグメント (図 20 の L2 Switch#2) を利用して，各 PC 間の BGP ピアリングや，パケットのルーティング，分散型サービス妨害攻撃を行い実験を行った．

64 台の実験用 PC は，AS をエミュレーションする PC として 50 台，そして，攻撃ノードおよび被害ノード用として，14 台を割り当てた．

5.6 実験のネットワーク構成

本実験で用いた AS ネットワークには，RouteViews データベースを利用した．RouteViews は，米オレゴン大によって収集されている BGP の経路情報であり，また，Skitter プロジェクトは，各 AS の AS 間相互接続 (ピアリング) 数に基づく AS 規模の順位付けを行っている [40][41][42]．本実験では，RouteViews データベースから，次に示す 2 種類の AS 構成情報を作成し，実験をおこなった．

1. 上位 50 位までの AS によって構成された AS トポロジー

2. 上位 20 位までの AS と上位 20 位から AS 距離が 4 までの 30 の AS で構成さ

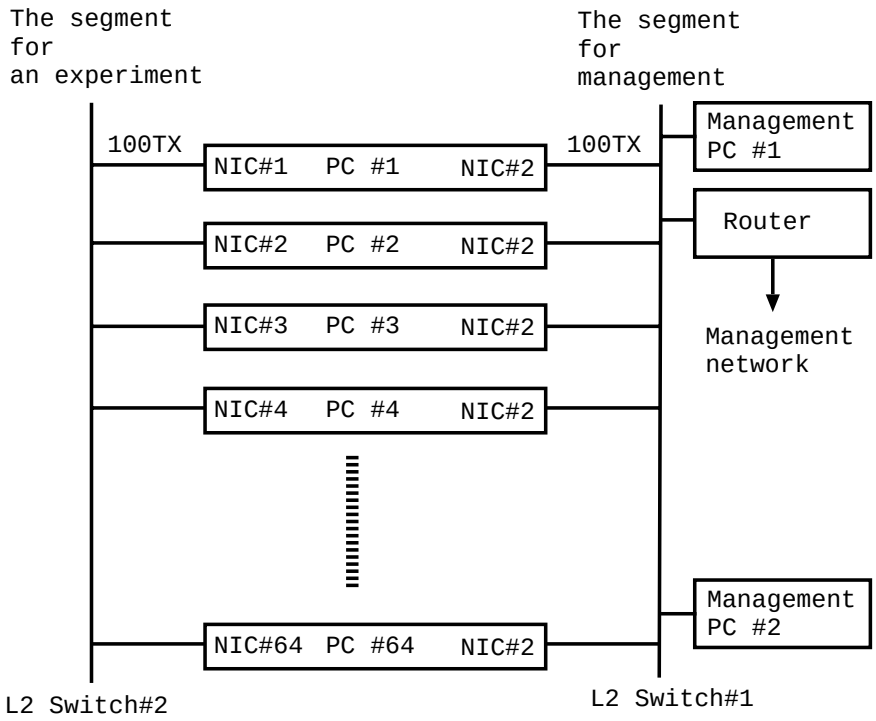

図 20 実験用システムのハードウエア構成

れた AS トポロジー

上位の AS を選定する理由は，次の通りである．RouteViews データベースから生成された Skitter グラフ [40] より，ピアリング数の上位 31AS は，アメリカを中心に，日本，アジア，ヨーロッパ等，地域的に分散して位置している．そして，それらの AS 群は，多くのピアリングを国内外を問わず行っている．従って，通常のトラフィックがこれらの AS 群を経由するのと同様に，分散型サービス妨害攻撃の攻撃フローもこれらの AS 群を通過する可能性が非常に高い．よって，これらの中心的な AS 群での運用を想定した AS トポロジーを用いた実験は，本提案の実運用における有効性を示すことができる．

なお，実験では，1 台の PC を 1 つの AS と想定した AS 用 PC を用意した．また，ハードウエア数の制約から，最大 AS 数は 50 となっている．AS 用 PC 上の実験用ネットワーク・インターフェースに対して，ピアリング毎にポイント・ツー・ポイント・アドレスをエイリアス・アドレスとして割り当てた．そして AS 間のピアリング接続は，このエイリアス・アドレスを使用したポイント・ツー・ポイント接続で行った．

5.7 実験のソフトウエア構成

ここでは，本実験で用いたソフトウエア環境について述べる．

AS をシミュレートするための PC に用いたオペレーティング・システムは，FreeBSD 4.7 である．各 AS 用 PC は，内蔵のハードディスク・ドライブから起動するのではなく，管理用 PC 経由からのネットワーク・ブートする．使用した FreeBSD 4.7 のカーネルは，フォワーディングされるパケットの選定と IP オプション・トレースバック・パケットの生成のために，バークレイ・パケット・フィルタ (Berkeley Packet Filter, bpf) とパケットロスや遅延をシミュレーションするためにダミーネット (Dummynet) が組み込まれている．

被害ノード，および攻撃ノード用PCのオペレーティング・システムは，シミュレータ研究設備の標準OSとして提供されている FreeBSD 4.6 を内蔵のハードディスク・ドライブからブートしたものを利用した．

AS用PCでのAS間のピアリングには，BGPが利用可能なルーティング・アプリケーションであるzebraを用いた．

そして，各AS用PC上に本研究において開発したシステム一式 (パケットモニター (PM) とトレースパケット・ジェネレータ (TOG)，ITM) をインストールし，AS毎に諸設定を行った．

被害ノードにおいては，攻撃パケットの保存とIPオプションパケットの抽出，その解析を行うためのシステムのインストールを行った．

攻撃ノードでは，分散型サービス妨害攻撃ツールの一つであるMstreamを本実験用に修正 (バグ修正，攻撃パケット数の記録など) した物を使用した．Mstreamは，攻撃パケットの送信を行う複数のスレーブ・ノードとスレーブへの攻撃指令や状況を管理するマスターノードの2部で構成されている．

攻撃パケットの送信は，マスターから各スレーブへの攻撃パケットの量や時間・攻撃パケットの種類をスレーブへ送信することで開始される．そして，送信後，送出した攻撃パケット数・時間がマスターに報告される．

AS用PC50台によって，ASネットワークを構成し，Mstreamによって，複数のスレーブから攻撃パケットの生成を行い，被害ノードに向けて攻撃パケットを送信し，攻撃パスの探索を行った．

5.8 本エミュレーションと実環境の相違

以上に示すように，本エミュレーション環境は，実インターネット環境下での提案手法の有効性を検証すること目標としている．このためのエミュレーション環境の要件として，以下の3点を示す．

1. 実インターネットのASトポロジーに基づくネットワーク構成

表 2 実験 1 で利用した攻撃ノード

攻撃ノードの	AS8342(ROSTELCOM), AS3269(IBSNAZ), AS3215(RAIN)
ある AS 番号	AS6517(YIPESCOM), AS4637 (HKT-NET-BORDER)
	AS16631(COGENT), AS5696 (WNST), AS7473 (SINGTEL)
	AS10910(INTERNAP)

本実験では，RouteViews によるデータを利用し，AS 規模上位 50 位までの AS ネットワークを再現することで，実インターネットをエミュレートしている．

2. インターネット・プロトコルのリッファレンス実装を用いたノードの構成

   ルーティングの構成は，IP フォワーディング実装のリッファレンスとなってきた BSD と市場シェアのもっとも高い米 Cisco 社の IOS-BGP との互換性を重視して設計されている zebra の BGP を組み合わせて行われている．

3. 実在する攻撃ツールによる分散型サービス妨害攻撃下での実験

   Mstream による攻撃パケットの生成を行い，その攻撃フローの IP トレースバックを行った．

以上の 3 点に基づく事によって，本エミュレーション環境は，実インターネットでの実験を想定した環境となっているといえる．

5.9 実験 1: 9 地点からの分散型サービス妨害攻撃

まず，AS トポロジー 1 番に基づく AS ネットワーク構成を行い，確率 $P = 1/10000$ として，表 2 に示す 9 カ所の攻撃ノード (スレーブ) からの分散型サービス妨害攻撃を行った．

表 3 実験 1 における IP オプションパケットの数

個数	IP オプション・パケットに含まれるリンク情報
2	AS701 〜 AS3561, AS6461 〜 AS5400, AS1239 〜 AS5696
2	AS701 〜 AS6461, AS701 〜 AS7018, AS701 〜 AS10910
3	AS701 〜 AS1239
5	AS701 〜 AS702, AS3561 〜 AS8342, AS702 〜 AS9057

被害ノードは AS701 に収容されており，攻撃パケットの送信は，各攻撃ノードから，500 パケット/秒，250 パケット/秒，125 パケット/秒，100 パケット/秒のパケット送信数で 60 秒間の攻撃を各 3 回実施した．

その結果は，次のようになった．500 パケット/秒の条件においては，図 21 に示すように，3 回の実験においてすべての攻撃ノードの特定を完了しているが，それ以下の条件においては，250 パケット/秒における 1 回の成功を除いて，十分な攻撃ノードの特定ができていない．したがって，攻撃ノードあたりの攻撃パケット数が減るに従って追跡が難しくなる傾向を示しており，また，この実験結果は，先に示した理論解析の結果と同等の傾向を示している．

図 22 は，500 パケット/秒の攻撃パケット数とした 3 回の実験において，攻撃パス上の各 AS から生成される IP オプション・パケットが，被害ノードにおいて到着した数 (同じ AS からの重複した IP オプション・パケットの数は省く) の推移をしめたものである．本実験の場合，攻撃パス上の AS(TOG) は 15 であるので，15 個の重複のない IP オプション・パケットを受信することによって攻撃パス構築が完了する．

これより，10 秒という攻撃時間全体における早期において，攻撃パスの半分が判明し，全体の判明には，38 秒を要していることがわかる．これは，各攻撃ノードからの集約された攻撃パケットが通過する AS では，通過する攻撃パケット数が多くなるため，確率 P によるパケット抽出も多くなり，その結果 IP オプション・パケットの生成も多くなった結果を示してる．

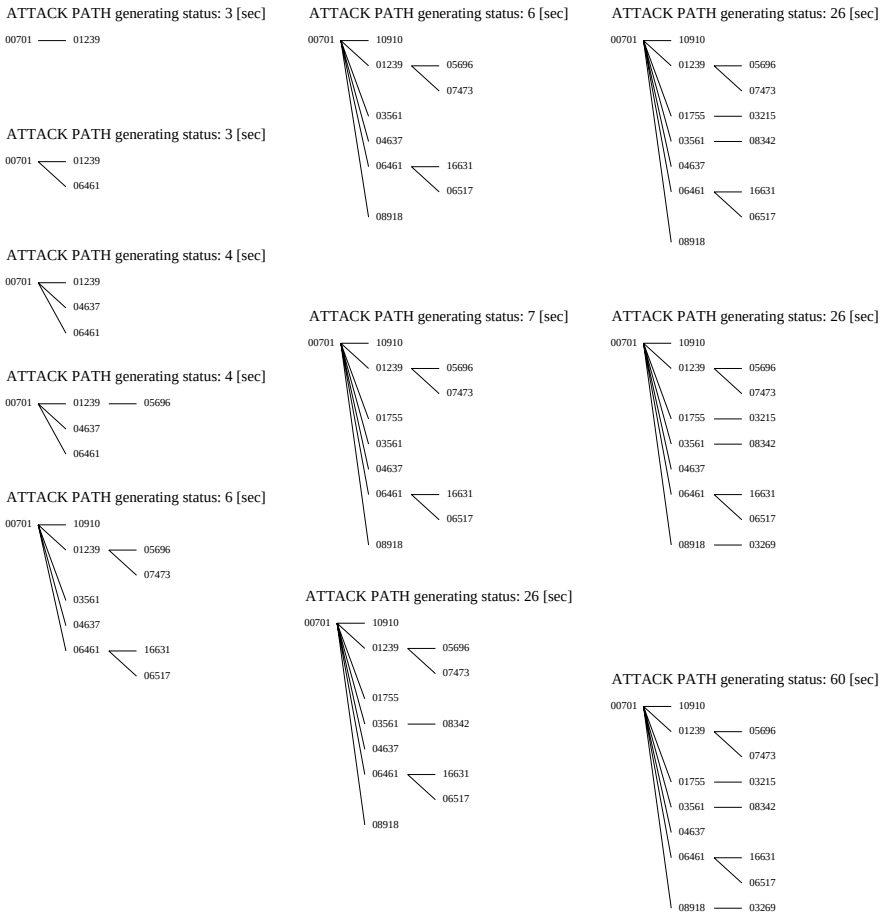

図 21 実験 1 における時系列に従った攻撃パス構築 (1 回目計測, 数値は AS 番号を示す)

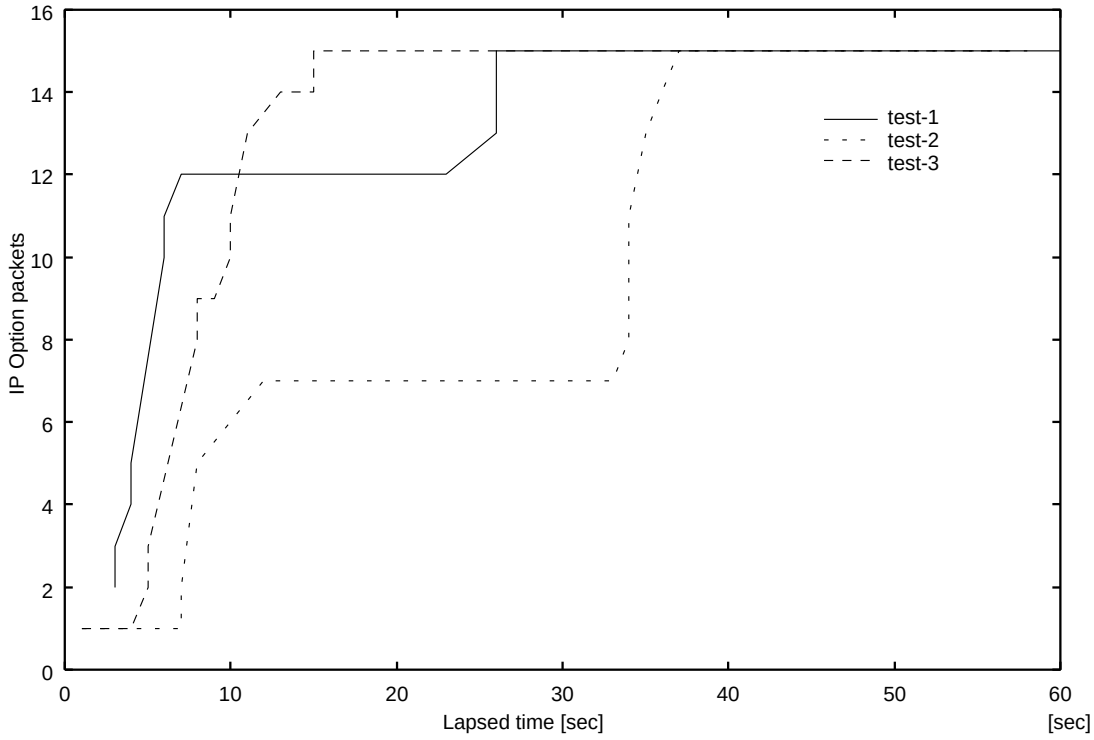

図 22 実験 1 500 パケット/秒における IP オプション・パケット収集数の推移

5.10 実験 2: パケットロス環境下における性能劣化

実験 1 の結果をふまえ，実験 2 においては，分散型サービス妨害攻撃によるトラフィック集中のために，被害ノードの AS においてパケットロスが発生することを想定した実験を行った．

この実験においては，実験 1 と同一のネットワーク・トポロジーを利用して，攻撃ノードの存在する AS を 20 地点追加し，合計 29 地点からの分散型サービス妨害攻撃を被害ノード (実験 1 と同様に AS701 配下) へ行った．攻撃は，攻撃パケット数 100 パケット/秒，攻撃時間 180 秒として，FreeBSD4.7 のダミーネットを用いて AS701 とその配下の被害ノード間のリンクにおいて，0%，10%，50%のパケットロスを発生させ，各 3 回づつ 9 回の実験をおこなった．

パケットロス 0%の場合，すべての実験において，攻撃パスの構築に成功した．攻撃地点が 20 地点増えたが，すべての攻撃ノードの特定に至っている．その特定できた攻撃パスは，3 回の実験共に図 23 に示す結果となり，IP オプション・パケット収集数の推移を図 24 に示す．

これらの結果より，実験 1 の場合と同様に，まず攻撃フローが集約されている AS からの IP オプション・パケットが集まるため，80 秒経過 (実験時間の 44

つぎに，パケットロス 10%の場合は，1，2 回目の実験では，すべての攻撃ノードの特定ができた．しかし，3 回目の実験では，図 25 に示す攻撃パスとなり，AS6461 〜AS5400 間の攻撃パスが特定できなかった．成功した場合 (1 回目) と失敗した場合 (3 回目) における IP オプション・パケット収集数の推移を図 26 に示す．

最後に，パケットロス 50%の場合における実験では，3 回の実験共に攻撃パスの構築ができなかった．その攻撃パスの構築結果は，それぞれ，図 27，図 28，図 29 に示す．また，実験における IP オプション・パケット収集数の推移を図 30 に示す．

10%パケットロス環境下での実験では，29 あるすべての攻撃ノードを特定することが出来ない場合があった．この原因は，次の事が考察できる．

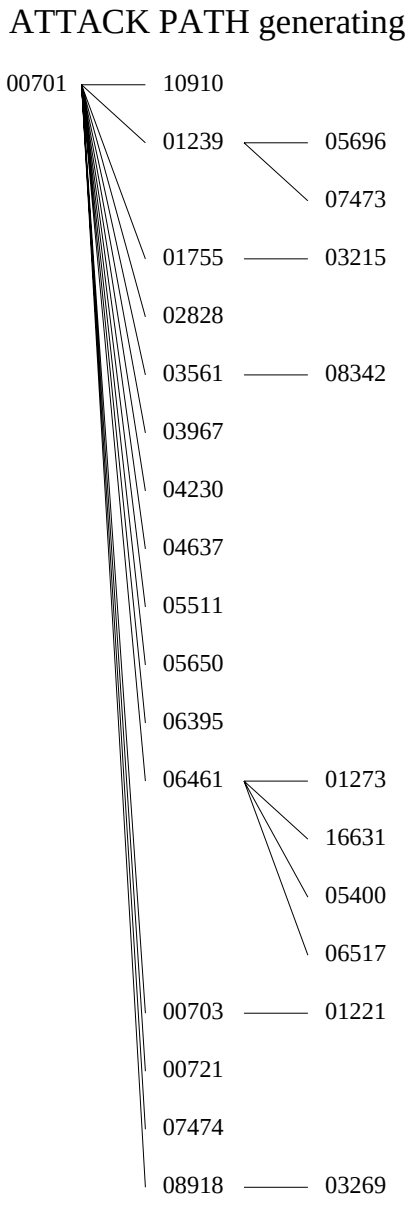

図 23　実験 2 パケットロス 0%における攻撃パス構築結果

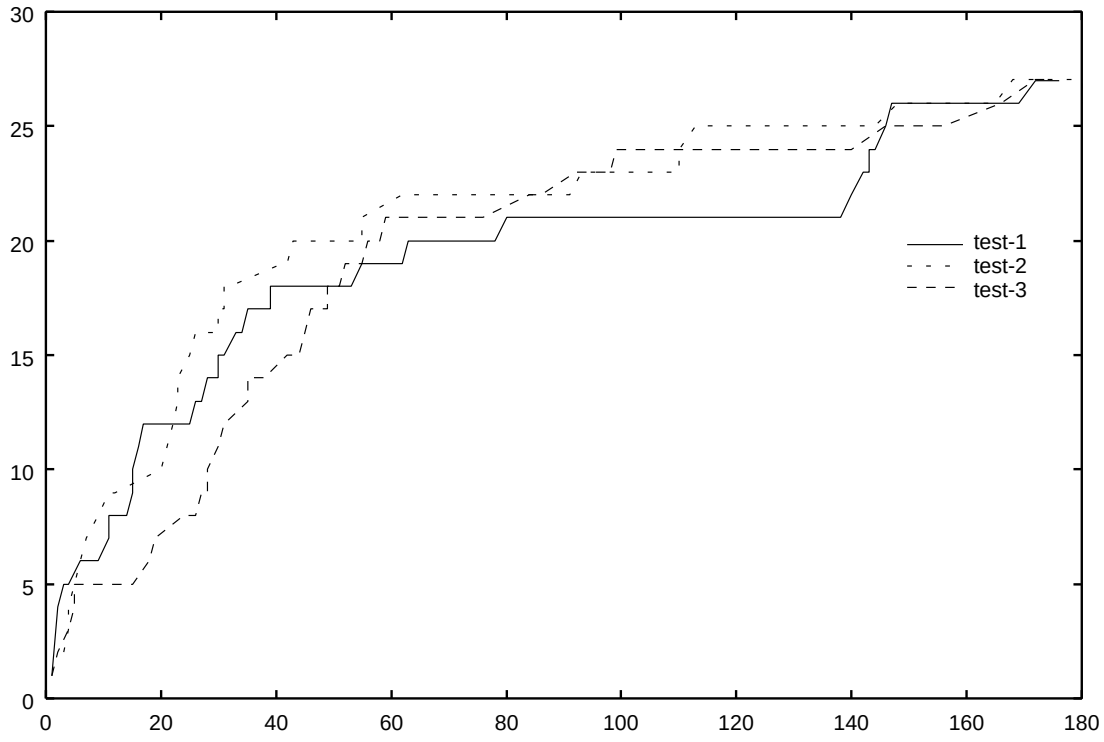

図 24 実験 2 パケットロス 0%における IP オプション・パケット収集数の推移

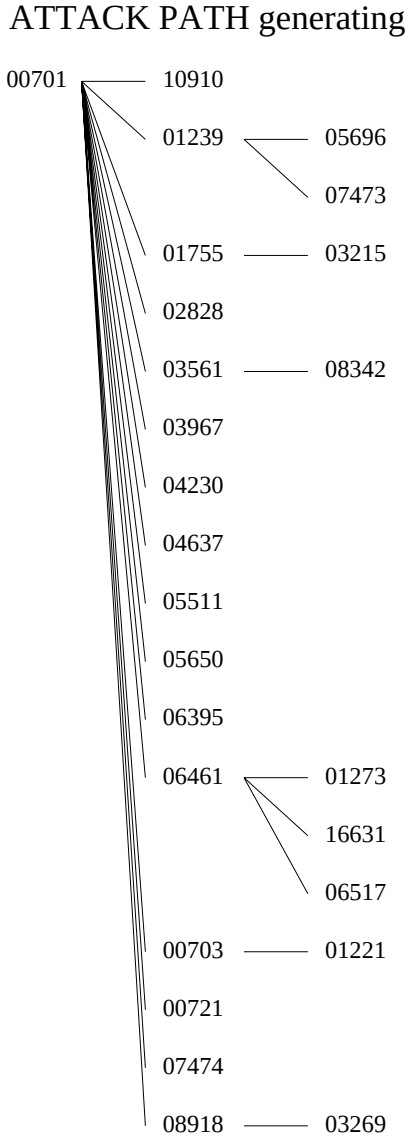

図 25　実験 2 パケットロス 10%における攻撃パス構築失敗の結果

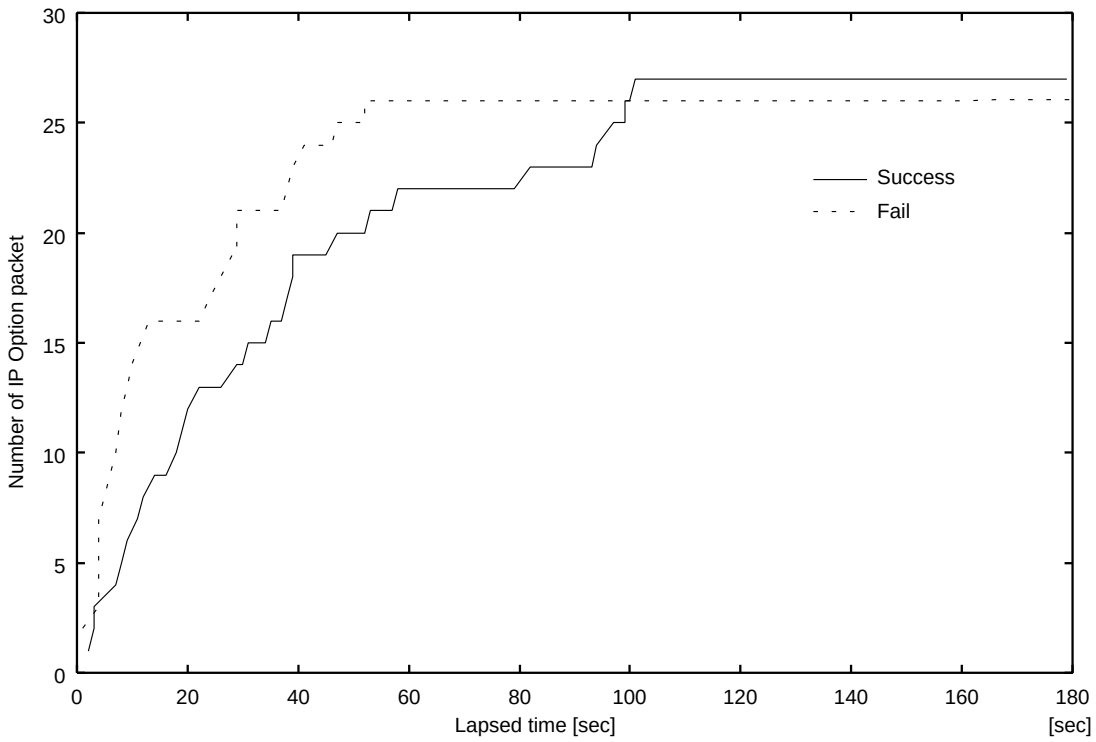

図 26 実験 2 パケットロス 10%における成功・失敗の各実験における IP オプション・パケット収集数の推移

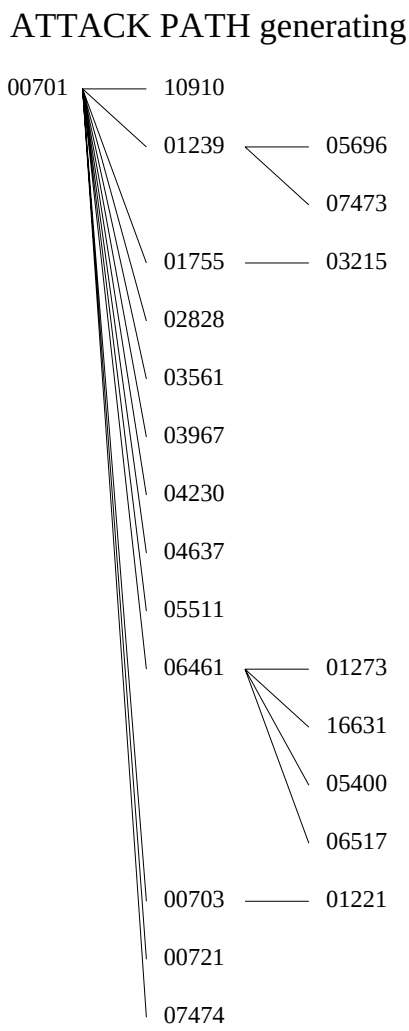

図 27　実験 2 パケットロス 50%における攻撃パス構築失敗 (1 回目) の結果

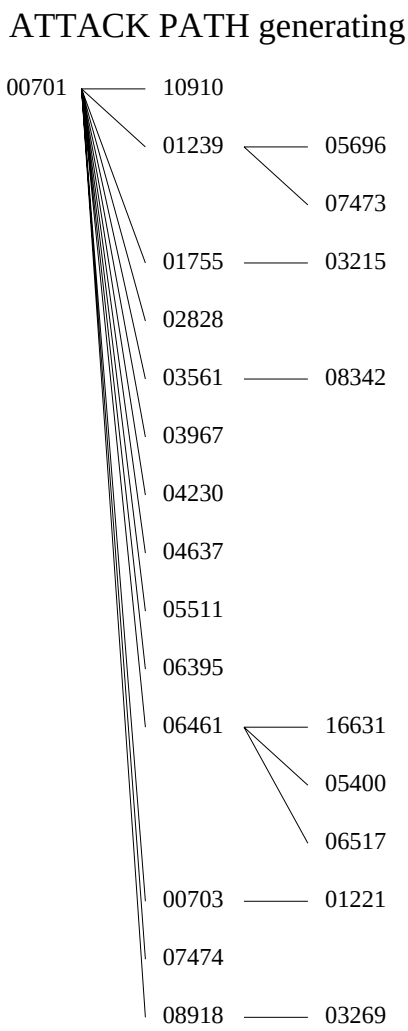

図 28 実験 2 パケットロス 50%における攻撃パス構築失敗 (2 回目) の結果

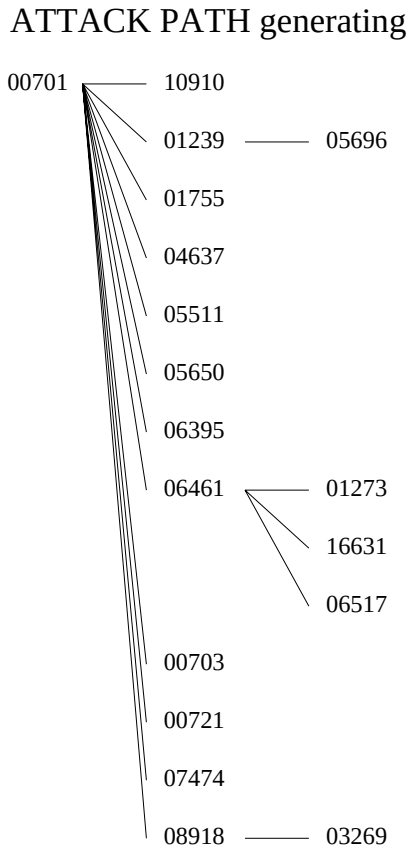

図 29 実験 2 パケットロス 50%における攻撃パス構築失敗 (3 回目) の結果

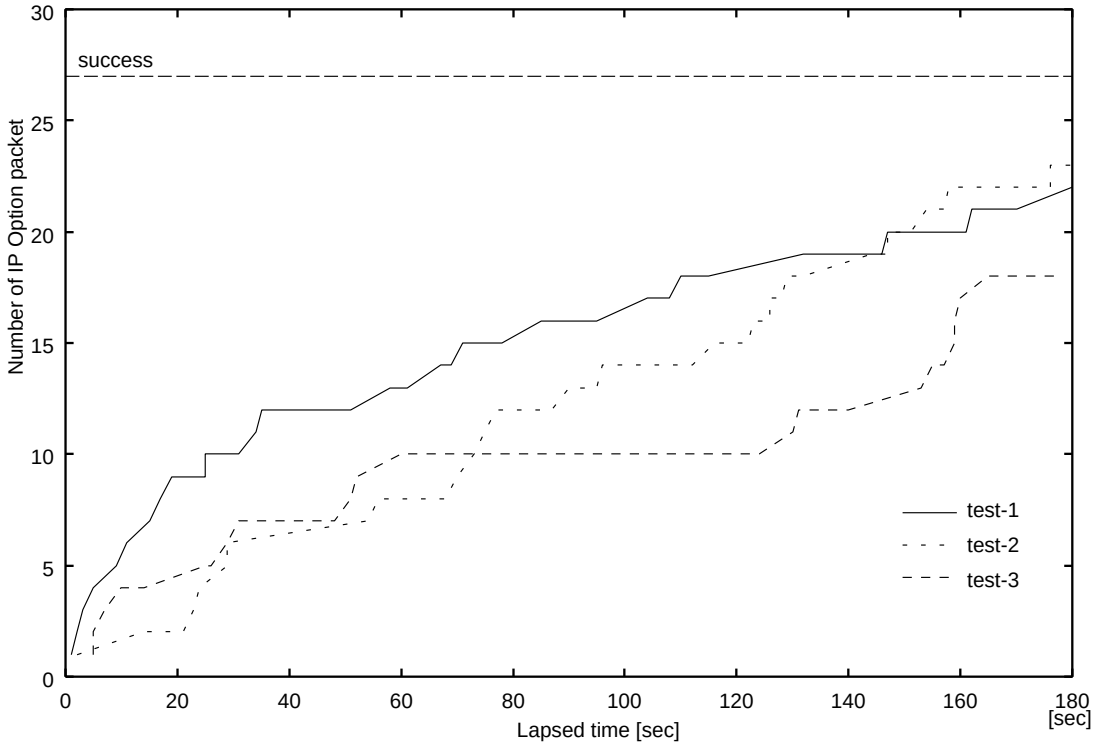

図 30 実験 2 パケットロス 50%における IP オプション・パケット収集数の推移

IP オプション・パケット収集数の推移 (図 24，図 26) は，同じ傾向を示している．つまり，攻撃フローが集約されている AS からの IP オプション・パケットは実験開始直後から到着し，攻撃ノードに近い末端の AS からは，なかなか到着しないということである．従って，3 つの異なる条件において，構築に失敗している原因は次に述べる共通したものであると考察する．

本手法は，攻撃パケットの量に比例して IP オプション・パケットが生成されるため，攻撃ノードに近いリンクの情報を含んだ IP オプション・パケットは，生成される数が少ない．

表 4 に IP オプション・パケットの受信数毎に IP オプション・パケットの内容をまとめた．これから解るように，AS6461 の用に複数の攻撃ノードからの攻撃フローが集約されるリンクに関する IP オプション・パケットは，13 個到着している．しかし，攻撃フローの集約されていない攻撃パスである AS1221-AS703-AS701 は，その IP オプション・パケットの数も 1 個 (AS703〜AS1221) と 2 個 (AS701〜AS703) となっており，その数は少なくなる．

そして，その少ない数の IP オプション・パケットがパケットロスよって，無くなる事により，この実験結果で特定できなかった AS6461〜AS5400 間のリンクのように短時間での検出は，不可能となる．

以上が，完全な攻撃パスもとめることが出来なかった原因の考察結果である．

しかしながら，一つのリンク損失のみで，ほぼ全体の攻撃パスを求めることができていることから，被害ノードにおける分散型サービス妨害攻撃状態において，10%のパケットロスが発生しても，分散型サービス妨害攻撃の被害を軽減することは十分可能であるといえる．

次にパケットロス 50%の結果について述べる．IP オプション・パケットに含まれるリンク毎の数を，表 5，表 6，表 7 に示す

これらの結果からわかるように，パケットロスのために IP オプション・パケットの数が半分になっている．しかしながら，攻撃パスの構築結果は，図 27，図 28，図 29 に示す通り，完全な攻撃パスの構築は出来ていないが，50%のパケットロス

表 4　リンク毎のオプションパケットの数

個数	該当リンク
1	AS703 〜 AS1221
1	AS701 〜 AS4230
2	AS701 〜 AS703, AS701 〜 AS2828, AS701 〜 AS3967
	AS6461 〜 AS6517, AS1239 〜 AS7473
3	AS6461 〜 AS1273, AS701 〜 AS3561, AS701 〜 AS4637
	AS701 〜 AS5650, AS1239 〜 AS5696 , AS701 〜 AS6395
	AS701 〜 AS10910 , AS6461 〜 AS16631
4	AS701 〜 AS721 , AS1755 〜 AS3215 , AS701 〜 AS5511
	AS3561 〜 AS8342
5	AS8918 〜 AS3269
6	AS701 〜 AS1755 , AS701 〜 AS8918
9	AS701 〜 AS1239
10	AS701 〜 AS7474
13	AS701 〜 AS6461

表 5 リンク毎のオプションパケットの数 (テスト 1 回目)

個数	該当リンク
1	AS701 〜 AS703 , AS703 〜 AS1221 , AS6461 〜 AS1273
	AS701 〜 AS1755 , AS701 〜 AS2828 , AS1755 〜 AS3215
	AS8918 〜 AS3269 , AS701 〜 AS3967 , AS6461 〜 AS6517
2	AS701 〜 AS4230 , AS701 〜 AS4637 , AS6461 〜 AS5400
	AS701 〜 AS5511 , AS701 〜 AS7474 , AS701 〜 AS10910
	AS6461 〜 AS16631
3	AS701 〜 AS721 , AS1239 〜 AS5696
4	AS701 〜 AS3561 , AS701 〜 AS6461 , AS1239 〜 AS7473
11	AS701 〜 AS1239

であるから，攻撃パスの構築も 50%という結果にはなっていない．これは，本手法が各リンク毎に 1 つのパケットがあれば攻撃パスの構築は可能であることと，全 IP オプションパケットを観測するまでの間に，攻撃トラフィックが集中する攻撃パス上の AS からは，複数個の IP オプション・パケットが送信されることから，大きな欠損をすることなく攻撃パスの構築が可能であることがわかる．

つまり，本手法は，分散型サービス妨害攻撃による帯域輻輳の状況においても，攻撃パスの構築が十分可能であることがわかる．

5.11 実験 3: 陽動攻撃における性能劣化

実験 3 では，実験 1，実験 2 と同一の AS トポロジーを用いて，陽動攻撃に対する本提案手法を用いた攻撃パスの構築実験をおこなった．

陽動攻撃とは，IP トレースバックによる追跡に対抗するための攻撃手法 (抗 IP トレースバック攻撃) である．これは，攻撃目標 (被害ノード) を主目標 (被害ノード 1) と副目標 (被害ノード 2) の 2 カ所設定し，その間に，主目標に対して，分散

表 6 リンク毎のオプションパケットの数 (テスト 2 回目)

個数	該当リンク
1	AS701 ～ AS703, AS703 ～ AS1221 , AS701 ～ AS1755
	AS701 ～ AS3561 , AS701 ～ AS3967 , AS6461 ～ AS5400
	AS701 ～ AS6395 , AS701 ～ AS8918
2	AS701 ～ AS1239 , AS1755 ～ AS3215 , AS701 ～ AS4230
	AS701 ～ AS7474 , AS6461 ～ AS16631
3	AS701 ～ AS2828 , AS1239 ～ AS5696 , AS701 ～ AS6461
4	AS6461 ～ AS6517 , AS3561 ～ AS8342 , AS701 ～ AS10910
5	AS701 ～ AS4637 , AS701 ～ AS5511 , AS1239 ～ AS7473
6	AS8918 ～ AS3269

表 7 リンク毎のオプションパケットの数 (テスト 3 回目)

個数	該当リンク
1	AS8918 ～ AS3269 , AS701 ～ AS4637 , AS1239 ～ AS5696
	AS3561 ～ AS8342 , AS701 ～ AS10910
2	AS701 ～ AS1755 , AS701 ～ AS5511 , AS6461 ～ AS6517
	AS6461 ～ AS16631
3	AS701 ～ AS703 , AS701 ～ AS721 , AS701 ～ AS1239
	AS701 ～ AS6395 , AS701 ～ AS7474 , AS6461 ～ AS1273
4	AS701 ～ AS5650 ,AS701 ～ AS8918
7	AS701 ～ AS6461

型サービス妨害攻撃を行い．そして，同時に，副目標に対しても主目標より規模の大きい分散型サービス妨害攻撃を行う．これによって，主目標を副目標の攻撃によって隠蔽し，主目標への攻撃パスの IP トレースバックを困難にすることを目的とする．

実験では，主目標を AS1 配下のノード，副目標を AS701 配下のノードとした．主目標への攻撃は，10 地点から行い，そして，副目標への攻撃は，18 地点から行った．確率 P は，全 AS において 10000 とし，各攻撃ノードから攻撃パケットは，100 パケット/秒を 600 秒間各攻撃ノードから送信した．

その結果，副目標とされた被害ノード 2 での攻撃パスの構築結果は，3 回の実験において，それぞれ，図 31，図 32，図 33 となり，IP オプションパケット収集数の推移を図 34 に併せて示す．

そして，主目標とされた被害ノード 1 での攻撃パスの構築結果は，図 35，図 36，図 37 となり，IP オプションパケット収集数の推移を図 38 に併せて示す．

以上の結果より，主目標 (被害ノード 1) における攻撃パスは，3 回の実験すべてにおいて構築することができた．しかし，副目標 (被害ノード 2) における攻撃パスは，2 回目の実験をのぞいて構築する事はできなかった．

この結果は，本提案手法が陽動攻撃に対する脆弱性のあることを示しており，原因の考察が必要である．

求めることが出来なかったリンクは，AS5400〜AS1755 である．これは，主目標の攻撃パスと副目標の攻撃パスが重なりあっているリンクでであった．そして，攻撃ノードをもつ AS のリンクであった．このため，AS5400 では，IP トレースバック・オプションが双方の目標に対して攻撃が流れたために，副目標に対する攻撃パケットの選択されるのに十分な時間がなかったのが原因なのではないかと考える．しかし，データの解析を行ったが十分な結論を得ることはできなかった．

この調査を行うためには，主目標と副目標への攻撃パスが重なる AS において，攻撃ノードが送出する攻撃パケットの実際の通過量を測定を行い．これより，本提案手法における陽動攻撃への対応についての対策を明らかにする必要であると

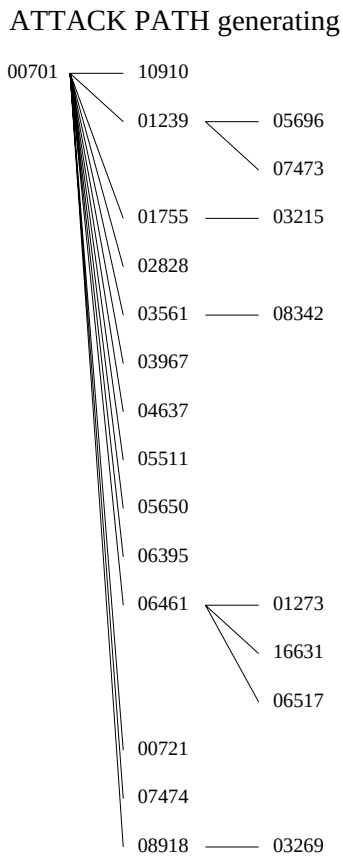

図 31　実験 3 副目標 (被害ノード 2) における攻撃パス構築結果 (失敗)(1 回目)

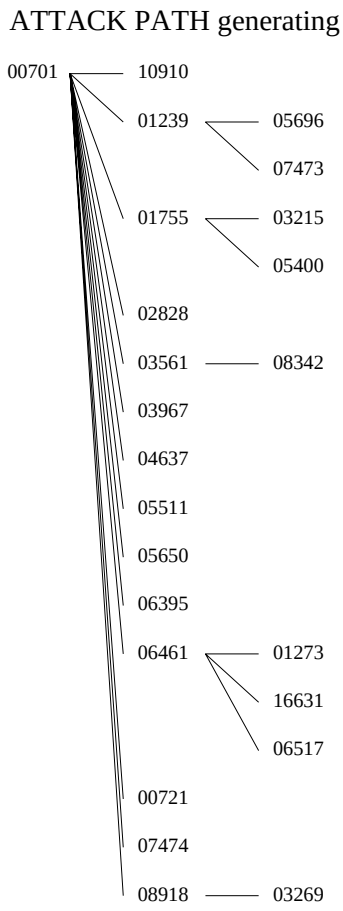

図 32　実験 3 副目標 (被害ノード 2) における攻撃パス構築結果 (成功)(2 回目)

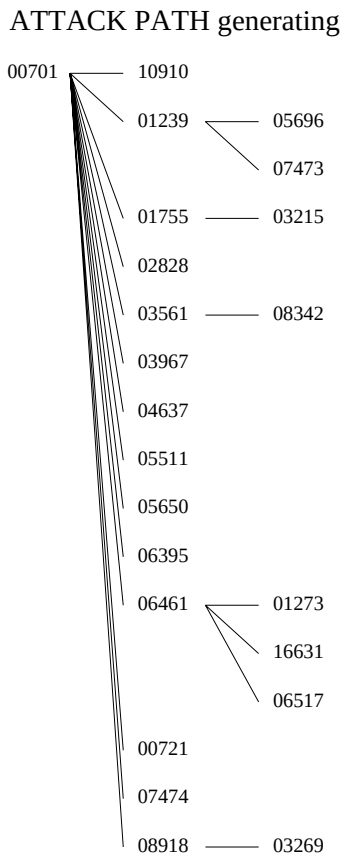

図 33 実験 3 副目標 (被害ノード 2) における攻撃パス構築結果 (失敗)(3 回目)

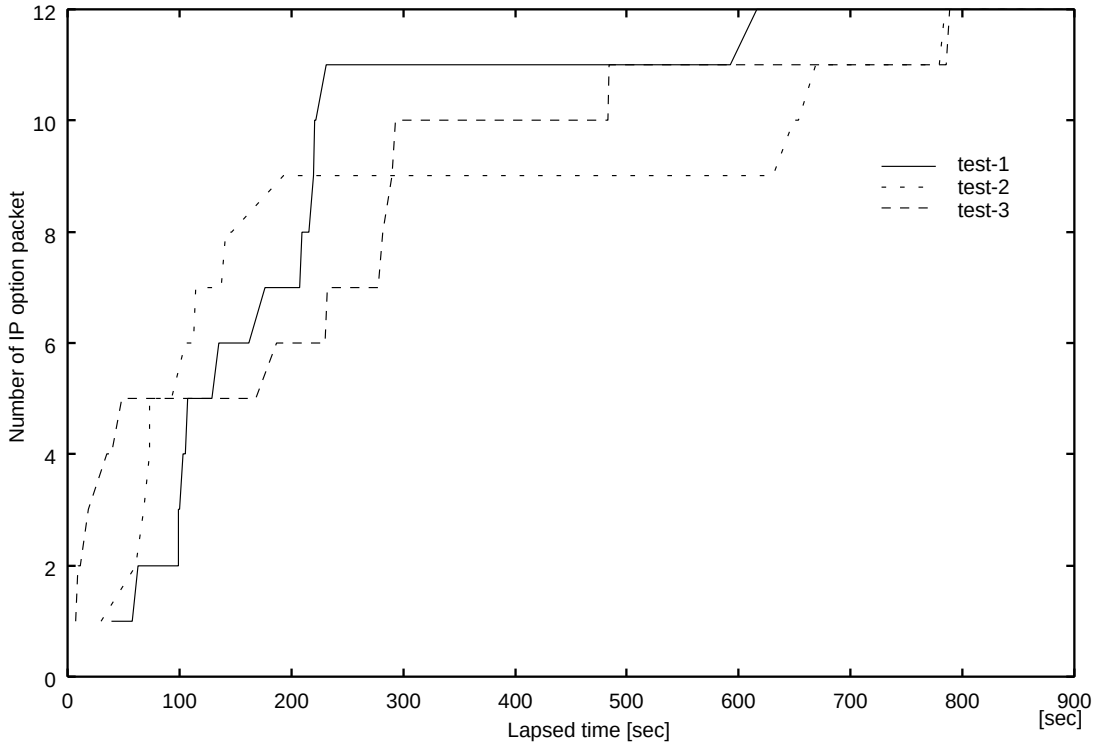

図 34 実験 3 副目標における IP オプション・パケット収集数の推移

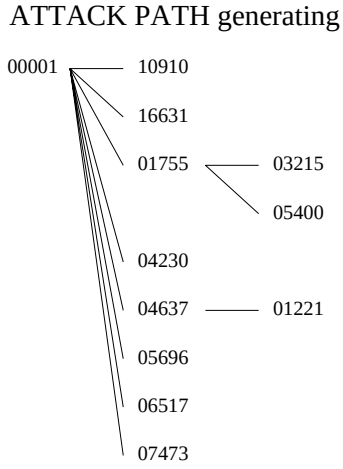

図 35　実験 3 主目標 (被害ノード 1) における攻撃パス構築結果 (成功)(1 回目)

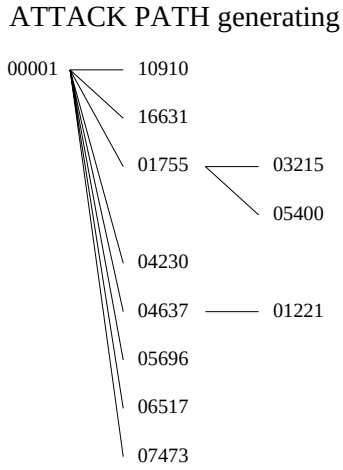

図 36　実験 3 主目標 (被害ノード 1) における攻撃パス構築結果 (成功)(2 回目)

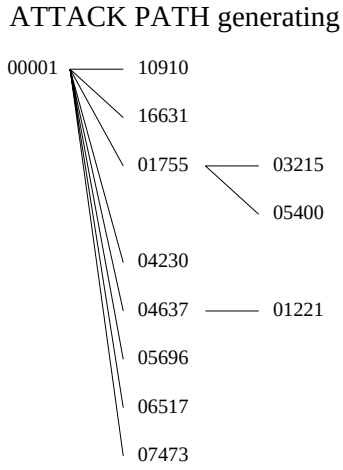

図 37 実験 3 主目標 (被害ノード 1) における攻撃パス構築結果 (成功)(3 回目)

考える.

5.12 実験 4: 確率 P を小さくした場合の性能劣化

実験 4 は，実験 2 と同一の AS トポロジーで確率 P を $1/10000$ から $1/20000$ として，実験 2 と同一である 29 地点の攻撃ノードから，100 パケット/秒を 360 秒間送信し，IP トレースバックを行う実験を 3 回おこなった.

その攻撃パス構築結果を図 39，図 40, 図 41 に，そして，IP オプション・パケット収集数の推移を図 42 に示す.

実験 2 のパケットロス 0% の場合では，三回すべての実験において攻撃パスの特定が可能であったの対して，確率 $P = 1/20000$ とした実験 4 で攻撃パスの特定が可能であったのは，1 回目のみであった．そして，図 40 と 図 41 から，末端の攻撃パスのみ特定ができていないことがわかる.

しかし，IP オプション・パケット収集数の推移傾向は，実験 4(図 42) と実験

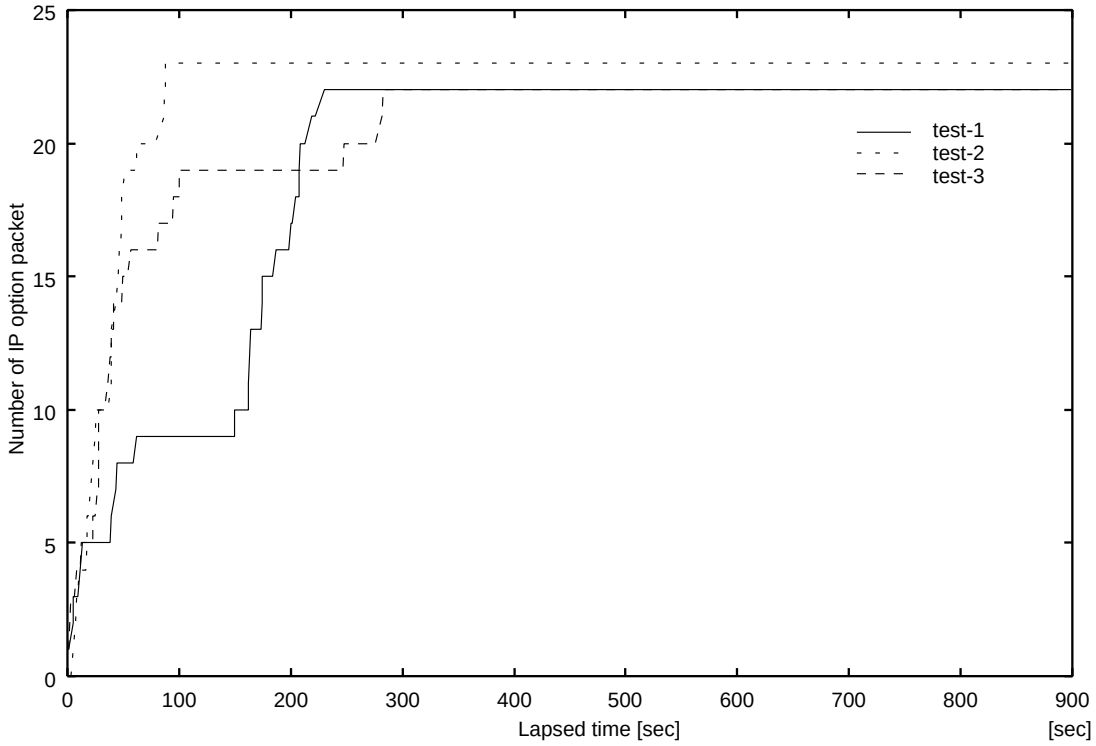

図 38 実験 3 主目標における IP オプション・パケット収集数の推移

表 8 実験 5 で利用した攻撃ノード

攻撃ノードのある AS 番号	AS5408, AS8756 , AS20965 , AS701
	AS1239, AS3561 , AS209 , AS702 , AS9010

2(図 24) において，時間範囲が倍違うグラフスケールにおいて，同じ傾向を示しているため，IP オプション・パケットの到着過程は，確率を 1/2 にしたことで 2 倍の 2 時間を要しているといえる．したがって，この特定の失敗に至ったのは，実験の試行回数が少ない点があるのではないかといえる．

5.13 実験 5: AS 距離が長い場合の性能評価

実験 5 では，AS トポロジーをトポロジーセット 2 とし実験を行った．被害ノードから攻撃ノードまでの距離は，実験 1〜4 において最大 2 ホップであった．そこで，実験 5 では，AS トポロジーセット 2 を使うことにより，最大のホップ数を 5 とし，距離に対する性能を明確にするための実験を行った．

攻撃パケットは，表 8 に示す攻撃ノードから，100 パケット/秒で 600 秒間送信し，5 回実験をおこなった．

そして，攻撃パスの構築結果は，成功した 1 回目，2 回目，3 回目，5 回目が図 43, 失敗した 4 回目が図 44 に示す結果となった．

これより，構築に失敗したのは，4 回目の実験のみでそれ以外においては成功した．また，4 回目の失敗した場合において，検出できなかった攻撃パスは，攻撃ノード近傍の末端部分であった．この結果は，今まで示したきた実験 1〜4 の実験と同一の傾向を示している．

しかしながら，実験の目的である攻撃パスが深さに対する追跡は，深さ 5 となる場合においても，攻撃パスの構築は可能である．これは，先に示した BGP ルーティングにおける平均 AS パス長の推移から実インターネットにおける追跡が可能なことを示している．

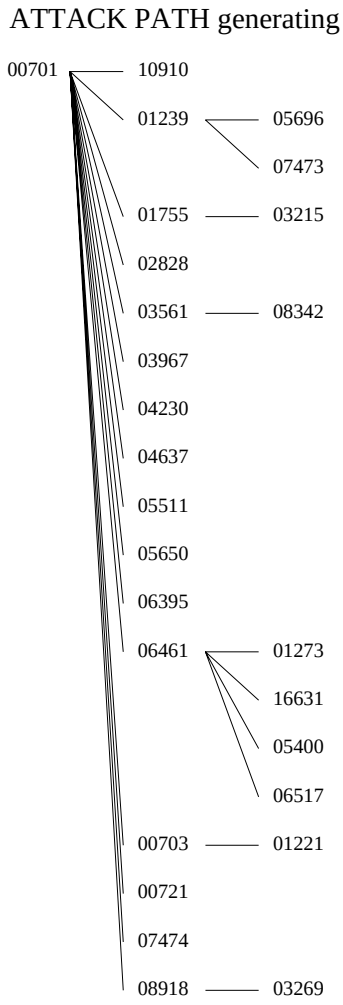

図 39　実験 4 確率 $P = 1/20000$ における攻撃パス構築結果 (成功)(1 回目)

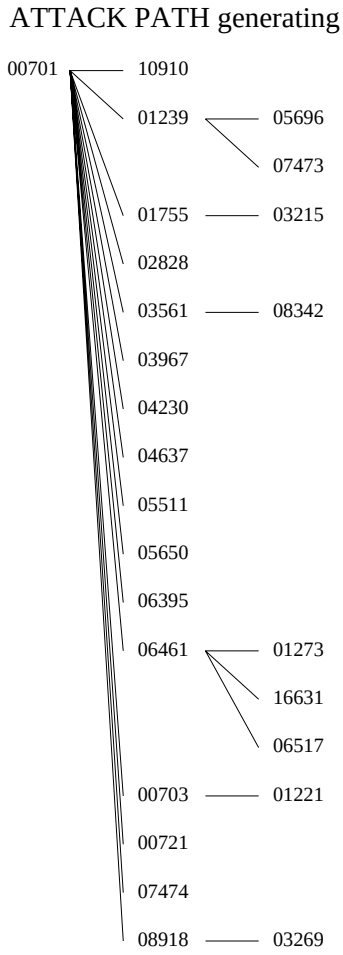

図 40　実験 4 確率 $P = 1/20000$ における攻撃パス構築結果 (失敗)(2 回目)

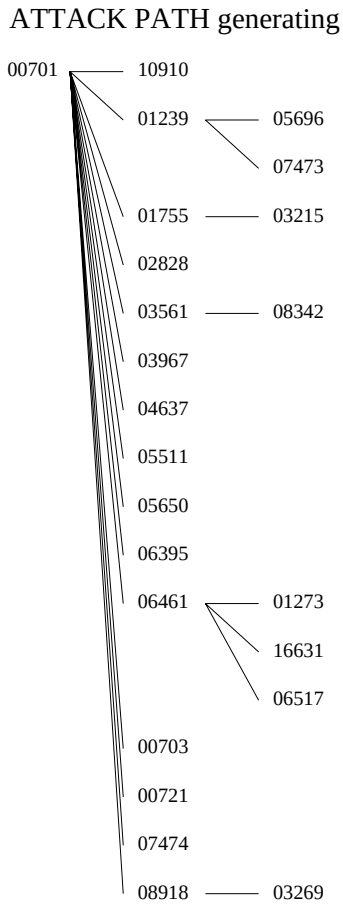

図 41　実験 4 確率 $P = 1/20000$ における攻撃パス構築結果 (失敗)(3 回目)

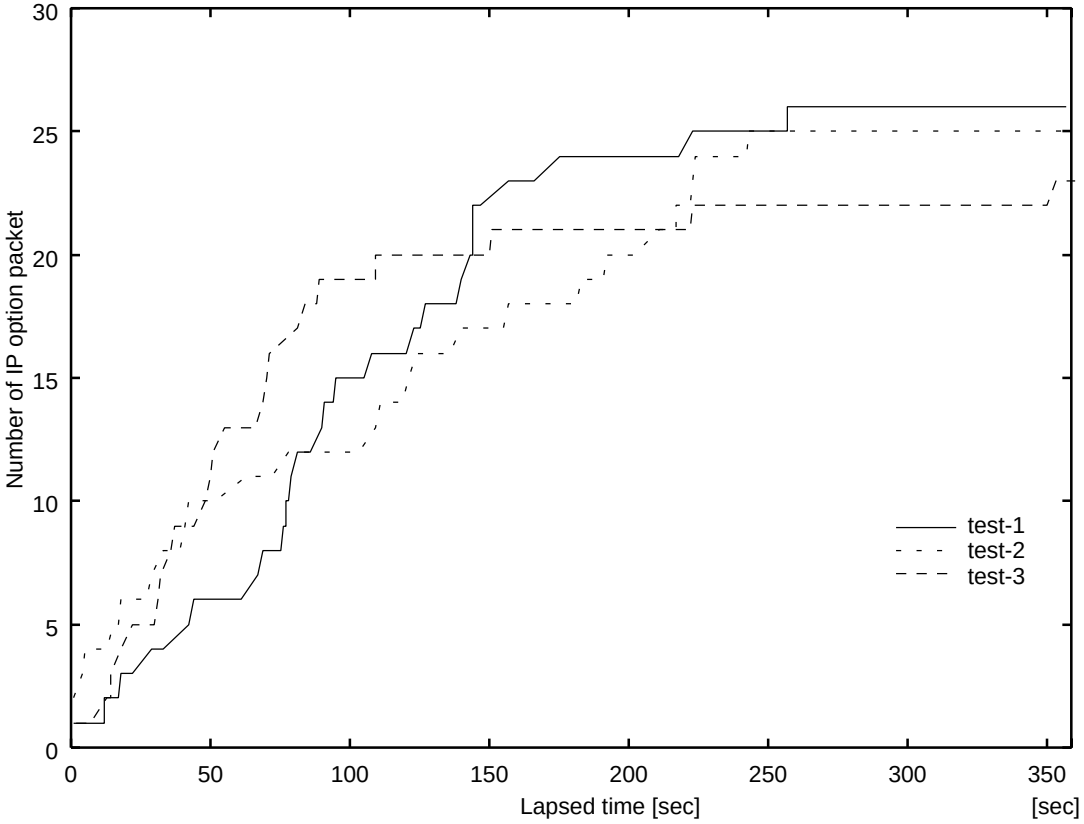

図 42 実験 4 被害ノードにおける IP オプション・パケット収集数の推移

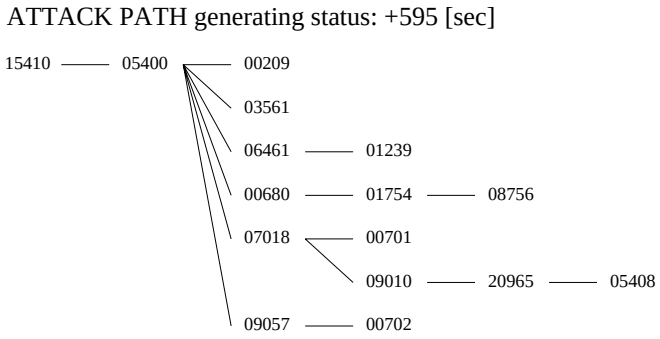

図 43　実験 5 攻撃パス構築結果 (成功)(1 回目，2 回目，3 回目，5 回目)

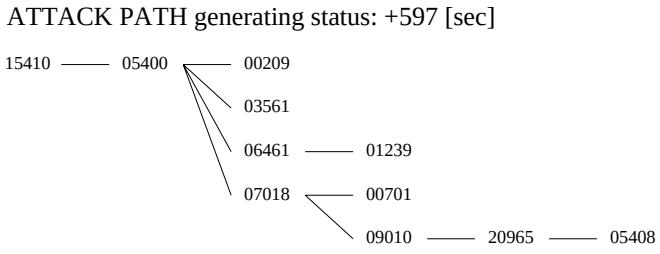

図 44　実験 5 攻撃パス構築結果 (失敗)(4 回目)

6. 実験結果の考察

本章では，以上のエミュレーション環境下における実験結果をふまえ，本手法の実現可能性についての考察を述べる．

6.1 実験結果について

実験から得られた結果として，攻撃トラフィック量が少ない場合，そのパスを通過する攻撃パスの構築必要な時間が大きくなることが判明した．これは，被害ノード近傍においては，分散された攻撃ノードからの攻撃パケットが集約化されいるため，そのパスを求めるのに必要な時間は少ない．

しかし，攻撃ノード近傍のトラフィックが集約されていないパスの特定には時間が必要であった．9 地点の攻撃ノードから，500 パケット/秒の攻撃トラフィックでの場合，完全な攻撃パス構築には，38 秒が必要であった．

しかし，末端部のパスを除いたトラフィックが集約された領域の攻撃パスは，早期の時点で特定できる．したがって，大まかな攻撃パスの特定から被害対策を行うことが可能である．

本実験で利用した攻撃パケット量と実インターネットにおける攻撃パケット量の差異については，実験で用いた攻撃パケット数の最大値 500 パケット/秒は，攻撃パケット長を 46 バイト (Mstream が用いる標準値) とするなら，

$$46 \times 500 \times 8 \quad = \quad 184k[bit/sec] \tag{12}$$

となり，184 キロビット/秒の帯域を利用した攻撃といえる．この攻撃量は，1.5Mbps の ADSL 回線の上り帯域の半分以下であり，ISP 等の AS から送信される攻撃量としては十分小さい値である．したがって，実験結果は，その設定した攻撃量が多いためによい結果となったいうわけではないことを示している．

以上の点から，IP オプション・トレースバックは，分散型サービス妨害攻撃に対する対策開始までに要する時間は目標の 30 分を達成しているといえる．

また，懸案の逆探知パケットがネットワークに与える負担はほぼない結果となった．29 地点の攻撃ノードから，100 パケット/秒の攻撃を 180 秒間行った場合，その攻撃パケット数は，617353 個であった．そして，IP オプションパケット数は，192 個であった．これは，$31 \times 10^{-3}\%$の増加でしかなく，ネットワークの負担は，ほぼないといえる．

また，分散型サービス分散攻撃のトラフィック集中によるパケットロスが発生した場合の攻撃パス構築に要する時間への影響は，少ない結果となった．29 地点の攻撃ノードからの 100 パケット/秒の攻撃をパケットロス率 50%の環境下において実験した結果，攻撃パスは，60〜80%の完成率となった．つまり，完全なパスは求められていないが，被害緩和のための対策は十分可能である．そして，対策により，パケットロス率が下がれば，完全な攻撃パスも構築可能となる．

主目標と副目標の 2 点への分散型サービス妨害攻撃を行った場合，その 2 点の被害ノードにおいて，攻撃パスの特定は可能であった．したがって，このように陽動を行った攻撃であっても，攻撃パスの特定は可能であるが，主目標における攻撃パスと副目標における攻撃パスが重なるリンクにおいて，かつ，攻撃パケット数が少ない場合，該当するリンクを攻撃パスとして特定することができない場合があった．この点に関して実験データの詳細な解析を行ったが，十分な結論を得るには取得したデータ数が少ないため，原因の特定には至らなかった．

被害ノードから攻撃ノード間のホップ数が 5 までの場合における攻撃パスの特定性能だが，9 地点の攻撃ノードからの 100 パケット/秒で 600 秒の攻撃を行った結果より，追跡はほぼ可能であることがわかった．したがって，距離に関わらず，攻撃パスの特定は可能であるといえる．

6.2 実現可能性に関する考察

階層型のトレースバック機構を実現するには，全 AS における導入を想定している ITM の運用が重要である．この点に関して，ITM ネットワークの構築の現

実性と攻撃者からの抗トレースバック攻撃に対する堅牢性の 2 点の考察が必要である．

最初の点に関して，ITM ネットワークの実現可能性は高いと考える．顧客の被る被害額を最小限にするために，ISP は早急な分散型サービス妨害攻撃への対策を行わなければならないが，攻撃パスの構築の為にリンク検査型の IP トレースバックを行なっている．これでは，AS 間の協調を行わなければならないため時間も人手も必要で高コストである．隣接 AS 間の ITM の存在は，eIP トレースバックによって攻撃フローの追跡を自動化でき，コストの削減を実現できる事を示している．さらに，各 AS は，ネットワーク規模や予算に応じた IP トレースバック手法を選択することから，本提案手法は柔軟性をもった IP トレースバック・システムの運用を実現する．

よって，AS が ITM を導入し階層型 IP トレースバック機構を運用することは十分なメリットがあるので，ITM ネットワークの実現可能性は高い．

6.3 ITM ネットワークの防御に関する考察

次に，抗トレースバック攻撃に対する堅牢性について述べる．本研究で提案した IP オプション・トレースバックは，ITM-API を介した ITM ネットワークを利用することで，攻撃パスの解析を行う．

したがって，既存のセキュリティ技術を利用し，ITM ネットワークをインターネットから分離することで，eIP/iIP トレースバックシステムの堅牢性を保たなければならない．ITM のピアリングは，BGP のピアリングの相手と同様であり，その相手先 ITM のアドレスは，不特定多数ではなく，各ピアリングごとに一意にきまる．よって，予め決められた各 AS の管理ネットワーク上にある ITM 間の通信しか行われない．

また，ITM ネットワークは，トレースバックを行うためのネットワークであり一般ユーザに対してサービスをオープンにしておく必要はない．以上から，既存

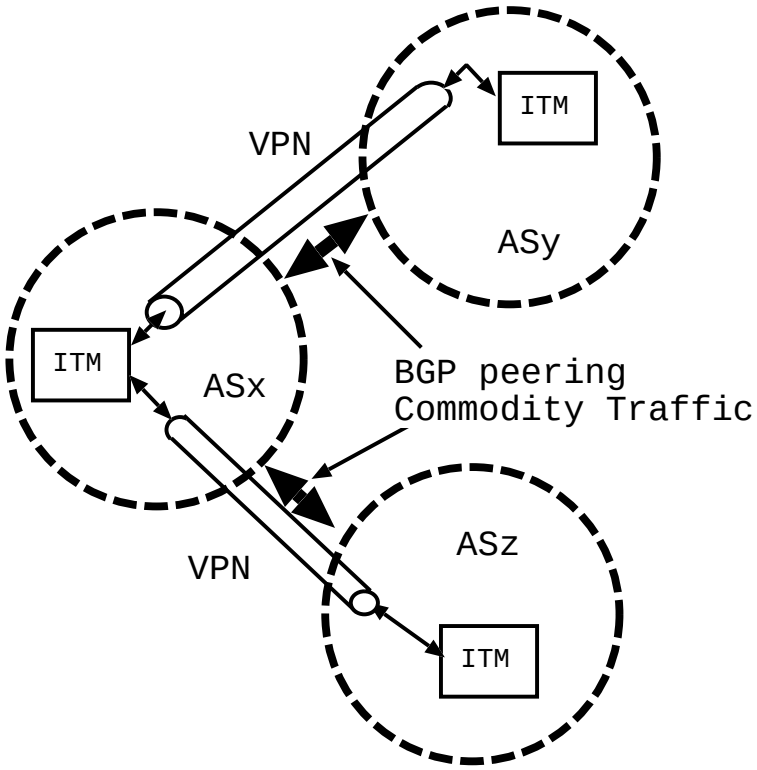

図 45 VPN を使用した ITM ネットワークの防御モデル例

セキュリティ技術の適用が容易であるといえる．

そして，強力な堅牢性を得るには，ITM ネットワークをインターネットから切りはずして運用するとよい．例えば，図 45 に示すようなピアリングを行う AS 間で，VPN や MPLS トンネルを利用したプライベート・ネットワークを構築し，その上でインターネットとは分離した ITM ネットワークを運用すれば，攻撃者から ITM ネットワークへの攻撃を不可能にすることができる．

しかしながら，ITM はコンピュータ・システムである以上，他のシステムと同様に，OS の脆弱性に対する対策など十分なシステム・セキュリティ対策が求められる．また，ITM ネットワークの防御対策が甘い AS があるとその 1 点から ITM

ネットワーク内に対して，悪意ある者が攻撃を行う可能性は否めない．また，悪意あるASからITMを利用した攻撃がある可能性も否めない．この隣接ITMからの攻撃への対応には，隣接ASのITMの運用環境を把握する機構や，運用ルール・チェック機関といった改善策や運用システムが必要であると考える．

6.4 本提案手法の導入費用対効果

次に，本提案の費用対効果について述べる．

本提案手法における費用は，導入費用と運用費用に分類することができる．導入費用は，本提案手法を実装した機器を設置するために必要な費用であり，運用費用は，その導入した機器を維持し，追跡を行うために必要な費用である．

まず，ITMおよび，IPオプション・トレースバックの導入費用は，非常に低いといえる．これは，トラフィックのモニタリング部分(PM)とIPトレースバック・オプションの生成部分(TOG)を分離するモデルとなっているため，既存のバックボーン・ルータ製品に対する改変を必要としない運用構成が組めるからである．

必要な機器は，TOG/ITMを動作させるためのPCハードウエア，各境界ルータごとにPMを動作させるためのPCハードウエア，そして，境界ルータのトラフィックをモニタリングするためのL2スイッチングハブのミラーポートかもしくはスプリッタである．

PCハードウエアは，信頼性や性能に依存するが1台辺りおおむね20万円程度，ミラーポートに関しては，IX等におけるリンクメディアがFastEthernetやGigabitEthernetとなっている点から，30万程度でL2のミラーリングポートを得ることができる．スプリッタの場合は，60万円程度である．

したがって，2箇所のIXに接続しているような場合，PCが3台，スプリッタが2台で，約180万円程度の投資でITMとIPオプション・トレースバックの導入が可能となる．この額は，一般にISPで利用されるハイエンド・ルータや，ファ

イヤーウオールやIDSといったセキュリティ製品への投資額から考えれば十分に低い額であり，本提案手法のコスト対効果は高いモデルとなっているといえる．

そして，本提案手法は，eIP トレースバックと iIP トレースバックの分離されたモデルとなっているため，独立して段階的に投資を行うことが可能であり，無駄のない投資が可能なモデルである．

また，その運用費用は，定常時の費用と非常時の費用に分類することができる．定常時は，運用作業とシステムの維持費用であり，これには，BGP ピアリング変更にともなうITM ピアリングの変更等である．これは，一般のルータ機材の運用作業と同じといえる．

非常時は，攻撃バスを特定するための人件費が必要となる．これは，本提案手法における攻撃パスの特定に要する時間は手動追跡に比べ短いために，非常時に必要な人件費は従来より圧縮することができる．

以上の費用の面に対する効果は，2 つある．1 つ目は，IP トレースバック作業の自動化によって，攻撃フロー特定に必要なコストの削減と攻撃パス特定に要する時間の削減によるネットワーク・サービス品質の向上が実現する点がある．2 つ目は，自 AS での投資が自 AS に閉じた投資となるのではなく，隣接 AS に対しても効果をもたらす点である．これは，各 AS における投資によってITM ネットワークが広域化すれば，攻撃フローの特定はより広範囲において行うことができ，きめ細かい攻撃への対策が可能となる．これは，普及に対する大きなバイアスとなるといえる．

以上のことから，本提案手法における費用対効果は高いといえる．

6.5 本提案手法の設置点について

本提案手法は，ITM の設置場所次第で効果的な IP トレースバックを行うことが可能となる．この点を考えればすべての AS にITM を設置することが，最大の効果を発揮することになる．しかし，段階的普及を考えれば，ITM の設置すべき

AS の優先度は決まってくる．ここでは，この点についての考察を述べる．

分散型サービス妨害攻撃は，国内に閉じた攻撃ではなく，国家といった地域とは関係なく世界中のノードから攻撃が行われる特徴がある．そして，その地域を超えた追跡こそがコストの増大につながっている．したがって，ITM 運用は，国外への BGP ピアリングを確保している運用規模が非常に大きい ISP を中心に行うことにより，限定的なエリアの IP トレースバックとなってしまうが，その追跡コストは大幅に削減できるといえる．

その運用するべき ISP は，各国の ISP で対外的な BGP ピアリングを多数有している ISP を中心に導入して行かなければならないと考える．すなわち，Route-Views/Skitter から得られる上位 31AS は，世界中に広く分散して存在しており，各地域の ISP と

例えば，インターネットの中心である米国におけるナショナル・バックボーンを構成しているといわれる AS 群，そして，実験のトポロジーで用いた Route-Views/Skitter の選定による上位 50 位の AS 群といった順序となる．また，ITM ネットワークは，AS 間のピアリングが連続になるように構築していく必要がある．なぜなら，連続した接続となっていない ITM ネットワーク，すなわち，分断された ITM ネットワークは，そのネットワーク毎の攻撃パスしか構築できないため，局所解となってしまうからである．

このような限定的な範囲における運用を行った場合であっても，手動追跡よりも短時間に攻撃パスの特定が可能となり，被害への対策実施が可能となる．したがって，その効果は，ITM ネットワークの展開規模次第ではあるが，被害者保護は十分可能である．

，本提案手法の実証実験を重ね．そして，実績を積むことによって，インターネットの BGP ピアリングが飛躍的に増加していったことと同じく，ITM ネットワークも成長し，より効果の高い IP トレースバックが可能となると考える．

6.6 非攻撃・攻撃パケットの識別が与える影響

ここでは，IP トレースバックにおける被害ノードにおける攻撃パケットと非攻撃パケットの識別が本提案手法に与える影響について述べる．

IP トレースバック技術全般に言えることであるが，攻撃フローの特定を被害ノードでおこなわなければ，IP トレースバックはできない．このためには，被害ノードにおける大量の受信パケットからの攻撃パケットと非攻撃パケットの識別が必要である．この識別によって，攻撃フローとして追跡する対象フローが決定されるからである．

本提案手法においては，IP オプション・トレースバックにおける IP トレースバック・オプションの選択がその識別に該当する．IP オプション・トレースバックでは，被害ノードでの受信パケットの中から IP トレースバック・オプションを含んだパケットを選択し，その中から攻撃フローの特定を行う．全 IP トレースバック・オプション群からその対象群を特定することが重要となる．

現時点では，一般的に攻撃パケットと非攻撃パケットの選別は困難であり，攻撃パケットの特徴を元に経験的に群を作成するしかないと考える．例えば，SYN-Flood のみを対象とする，ICMP ポートアンリーチ・メッセージを対象とするといった攻撃パケットのもつ特徴から群を作成するということである．

この攻撃パケットの特徴を利用した対象群の作成は，IP トレースバック・オプションの IP パケットに含まれる抽出したパケットのダンプ情報を利用すれば可能である．つまり，受信した攻撃パケット群と IP トレースバック・オプションに含まれるパケット・ダンプを比較し，攻撃パス構築のための対象群を作成するということである．

従って，技術的には，オペレータによる経験的な攻撃パケットの選定が可能であれば，IP オプション・トレースバックによって，攻撃トラフィックを対象とした攻撃パスの構築が可能である．

6.7 本提案手法の限界について

ここでは，米 Microsoft 社製 SQL サーバの脆弱性を利用した SQL Slammer ワーム [2] が，引き起こした多数ノードへの分散型サービス妨害攻撃対する本提案手法の有効性について論じ，本提案手法の限界について述べる．

このワームは，一意の被害ノードではなく無差別に被害ノードに対して，分散型サービス妨害攻撃を実施し，甚大な被害を与えた [43]．この被害量は，先に述べた CordRed ワームの被害に匹敵するとも言われている．

SQL Slammer ワームは，ランダムなアドレスを生成し脆弱性のもつ SQL サーバの探索を行う．SQL サーバが発見された場合，脆弱性を利用して感染する．探索と感染の繰り返すことによって，ワームは増殖し続ける．各ワームが探索の際に生成するトラフィックがネットワーク帯域を圧迫し，その結果，インターネット全体への分散型サービス妨害攻撃となる．

このような攻撃方式に対して，本提案手法による攻撃ノードの特定は，困難といえる．なぜならば，本提案手法による攻撃フローの特定には，一点の被害ノードへの攻撃が 30 分程度継続する事が必要である．しかし，SQL Slammer ワームのように被害ノードがランダムに変化し，かつ，脆弱性をもつ SQL サーバであるか否かを調べる間という短時間な攻撃時間であるため，本提案手法の IP オプション・トレースバックでは，攻撃パスの特定が困難であることがいえる．

この点を考え，攻撃トラフィックのパケット数が少数で，かつ，多数の被害ノードを対象とする攻撃形式において，攻撃ノード（ワーム）の特定が可能な eIP トレースバック手法提案が必要であるといえる．そこで，この新たな提案を行うためのベースとなる考え方について述べる．

IP オプショントレースバックは，攻撃フローが集中する被害ノードにおいては，逆探知パケットも集中する点を利用して，攻撃パスの特定を可能としている．しかし，ネットワーク上には攻撃トラフィックが存在するが，その攻撃フローの送信先が分散する場合は，逆探知パケットも分散してしまうために，十分な性能を

発揮することができない．

したがって，PM によるパケット記録を IP オプション・パケットとして送信するのではなく，ストレージ・サーバなどに蓄積することによって，蓄積された記録と攻撃トラフィックの特徴を比較することによって，攻撃パスの特定を行うようなアーキテクチャが有効であると考えられる．

このアルゴリズムの策定には，ストレージ容量や維持コスト，そして，その記録比較を行うために必要な計算コストといった点について，考察が必要だといえる．

SQL Slammer ワームによって明確となった「多数の被害ノードへの分散型サービス妨害攻撃」という攻撃方式に関しての対策手法の具体的な策定は，今後の課題とする．

次に，スケーラビリティにおける問題を述べる．RouteViews/Skitter によるとピアリング数がトップの AS においては，そのピアリング数が 1500 を超えており，増加し続けている．また，このような AS は，世界中の ISP とピアリングをおこなっており，隣接 AS との遅延 (距離) は大きくなる．したがって，1AS につき 1ITM のモデルである本手法では，この遅延の増加や信頼性の向上が問題となる．このため，AS 内での ITM の分散配置といったアーキテクチャが必要となる．

しかしながら，複数の ITM による運用は，複数の各 eIP/iIP トレースバックとの連携を困難とし，新たなアーキテクチャの考察が必要であると考える．この点に関しても，今後の課題とする．

7. 本研究における成果と今後の展開

IP トレースバック技術のもつ問題の解決策として階層型 IP トレースバック機構を提案した．これは，IP トレースバックをインターネットにおける経路制御アーキテクチャである EGP と IGP に従って，eIP トレースバックと iIP トレースバックの 2 つに分離し IP トレースバックを行うものである．

そして，本提案手法の実現可能性を明らかにするために既存研究の詳細な調査を行い，アーキテクチャの定義と必要な技術の特定と評価をおこなった．

実インターネットでの本提案手法を用いた追跡過程とその目標条件を定義し，既存技術を iIP トレースバック機構としての組み込むための要件を明確にした．そして，eIP トレースバック手法として IP オプション・トレースバックを新たに提案し，その性能解析を行なった．

そして，この結果を元に既存手法を iIP トレースバック機構として利用するために用いる ITM-API (ITM 情報交換 API，データ交換 API，トレースバック要求と応答 API) を定めた．また，ITM ネットワーク上で各 eIP と iIP トレースバック間の連携や制御をするための通信プロトコル ITMP を定めた．

そして，ITM-API と ITMP の設計に基づきプロトタイプの開発をおこなった．本提案手法の実インターネットにおける運用を目標とした検証過程を明確にし，まず，ITM と eIP トレースバック間の連携を検証をした．その結果，本提案手法のプロトコル設計や実装は，大規模エミュレーションを行うことが可能であることが明らかになった．

次に，放送通信機構北陸 IT 開発センターの大規模シミュレーション装置を利用し，インターネット環境のエミュレーション (模倣) を行い，eIP トレースバックとしての IP オプション・トレースバックの性能検証を行った．

この実験では，RouteViews/Skitter に基づく規模の上位 50 位までの AS 構成をエミュレーションし，実在する分散型サービス妨害攻撃ツールによる攻撃フローの生成を行い実験をおこなった．その結果，攻撃パス構成時間やネットワークへ

の負荷といった性能が明らかになり，本提案手法の eIP トレースバックは，IP トレースバック能力を十分有していることが明確になった．

また，本提案手法の費用対効果や導入過程，攻撃トラフィックの識別方法といった実インターネットにおける運用と展開に関する議論をおこなった．そして，本提案システム対するセキュリティに関する考察と防御モデルの提案を行い．ITM ネットワークをインターネット上のプライベートなネットワークとして運用する事によって，本システムの堅牢性を保つことが可能であることが明確となった．

今後の展開として，より規模の大きな実験，標準化活動，技術移転の 3 点を軸に研究を継続しなければならない．

今回の実験では，利用可能な PC の制約から AS 数 50 までのネットワークのエミュレーションしかできなかった．今後は，AS 数 100 を超えるエミュレーション環境での実験をおこない．実インターネットでの実証実験に向けての検証が必要である．

そして，得られた実験結果や定めたアーキテクチャ・プロトコル等の標準化を IETF を通じて，行なわなければならない．標準化活動に伴う成果は，IP トレースバック技術普及する大きな力となる．

また，学術研究機関の活動として得られた一連の技術・知見を開発企業や ISP などへ技術移転しなければならないといえる．これには，横河電気の NAPPI へのフィードバックや，ISP での本提案手法の運用などがある．

以上が，本研究活動を通して得られた結果と今後の展開である．

8. あとがき

分散型サービス妨害攻撃の対策として，既存の IP トレースバック技術では,「完璧な攻撃パス」の導出に重点を置いた研究がなされてきた．しかし，被害ノードでの経済的損失など被害を最小限にするスタンスに立てば,「犯人」探しの技術ではなく,「被害を緩和」する技術が必要である．

本研究では，eIP トレースバックによって，早急な攻撃パスの特定を大まかに AS レベルで行い．そして，iIP トレースバックへ連携することによって,「犯人」の特定に至ることができる．したがって，各 AS 管理者は，eIP トレースバックの結果の時点で，被害ノードに対する被害緩和処置を行うことが可能となる．

このように，本研究は，被害者保護の視点に立った考え方に基づき,「分散型サービス妨害攻撃による被害を最小化する技術」を IP トレースバックの枠組みで実現可能であることを示すことができた．

本研究の成果が，実インターネット上で展開されることによって，被害軽減化と攻撃ノードの特定に効果を出し，それが，分散型サービス妨害攻撃に対する「抑止力」となると考える．

これは，本提案手法が「分散型サービス妨害攻撃のないインターネット」を構築できる可能性をもっていることを示しており，本研究の成果が脅威のないインターネットの実現への糧となることを期待する．

謝辞

本研究，および本報告書作成における全過程を通じて，懇切なる御指導，御鞭撻を賜わりました本学情報科学研究科の山口 英教授，砂原 秀樹教授，および，門林 雄基助教授に厚く感謝の意を表します．

また，本研究を進めるにあたり，WIDE プロジェクトの皆様には，メーリングリストや研究会を通じ，様々な意見を頂き，お礼を申し上げます．

この博士後期課程の研究活動を通して，成長していく IP トレースバック技術に関われたことは，私にとって，言葉では表せ切れないほどの大きな経験でした．

最後になりましたが，様々な経験と機会を与えてくださった WIDE プロジェクトに深く感謝いたします．

参考文献

[1] Microsoft Technet, "Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise," Microsoft Security Bulletin, MS01-033
http://www.microsoft.com/technet/security/
bulletin/ms01-033.asp, 2001.

[2] Microsoft Technet, "Elevation of Privilege in SQL Server Web Tasks," Microsoft Security Bulletin, MS02-061
http://www.microsoft.com/technet/security/
bulletin/ms02-061.asp, Jan. 2003.

[3] PSS Security Response Team Alert, " PSS Security Response Team Alert - New Worm: W32.Slammer," Microsoft Technet
http://www.microsoft.com/technet/security/virus/alerts/slammer.asp,
Jan. 2003.

[4] J.Mack, "FBI talks with Yahoo! about attack," ZDnet NEWS, http://zdnet.com.com/2100-11-518359.html, Feb. 2000.

[5] J.Postel, "Internet Protocol," RFC791
http://www.ietf.org/rfc/rfc791.txt , 1981.

[6] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC2460
http://www.ietf.org/rfc/rfc2402.txt, 1998.

[7] O.Nakamura, S. Yamaguchi, N. Shigechika, N. Morishima and Y.Sekiya, " ShowNet on INTEROP Tokyo 2002 — First Largest demonstration network

of IPv4/IPv6 Dual Stack ," in Proceedings of SAINT'03, pp111-116, Florida, USA, Feb. 2003.

[8] J. Postel, "Transmission Control Protocol", RFC 793 http://www.ietf.org/rfc/rfc793.txt Sep. 1981.

[9] R. T. Morris, "A Weakness in the 4.2BSD Unix TCP/IP Software," Technical Report Computer Science No.117, AT&T, Bell Labs, Feb. 1985.

[10] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite, " ACM Computer Communications Review, 19(2):32-48, Apr. 1989.

[11] Computer Emergency Response Team, "CERT Advisory CA-96.26 Denial-of-Service Attack via pings, " http://www.cert.org/advisories/CA-96.26.ping.html, Dec. 1996.

[12] Computer Emergency Response Team, "CERT Advisory CA-97.28 IP Denial-of-Service Attacks," http://www.cert.org/advisories/CA-97.28.smurf.html, Dec. 1997.

[13] Computer Security Institute and Federal Bureau of Investigation, "1999 CSI/FBI Computer Crime and Security Survey," Computer Security Institute publication, Mar. 1999.

[14] Dittich, "TFN Analysis," http://staff.washington.edu/dittich/misc/tfn.analysis.txt.

[15] . M. Delio, "Davos Hack: 'Good' Sabotage ," WIRED NEWS http://www.wired.com/news/politics/0,1283,41760,00.html, Feb. 2001.

[16] . M.Takahashi, "サイバーテロの実態と被害状況をめぐって," Terra http://www.nttcom.co.jp/terra/terra11/terra11_06.html , Apr. 2002.

[17] . The National Infrastructure Protection Center (NIPC), "Increased Cyber Awareness,"
http://www.Nipc.gov/warnings/advisories/2001/01-020.htm, Sep. 2001.

[18] . Dittich, "Trinoo Analysis,"
http://staff.washington.edu/dittich/misc/tronoo.analysis.txt.

[19] Cisco Systems, "Configuring TCP Intercept (Prevent Denial-of-Service Attacks)," Cisco IOS Documentation, Dec.1997.

[20] R.Stone, "CenterTrack: an IP overlay network for tracking DoS floods," in Proceedings of 9th USENIX Security Symposium '00, Denver, USA, Aug. 2000.

[21] S.M.Bellovin, M.D Leech, and T.Taylor, "ICMP Traceback messages, "Internet-Draft, draft-ietf-itrace-01.txt, Oct. 2001.

[22] S.F.Wu, L.Zhang, D.Massey, and A.Mankin, "Intention-Driven ICMP Trace-Back," Internet-Draft, draft-wu-itrace-intention-01.txt, Jul. 2000.

[23] A.Mankin, D.Massey, C.L.Wu, S.F.Wu, and L.Zhang, "On Design and Evaluation of Intention-Driven ICMP Traceback," 10th International Conference on Computer Communications and Networks (IC3N'2001), Arizona, USA, Oct.2001.

[24] S.Savage, D.Wetherall, A.Kerlin, and T.Anderson, "Practical network support for IP traceback," in Proceedings of ACM 2000 SIGCOMM Conference,pp.295-306, Stockholm, Swiss, Aug. 2000.

[25] D.Song, and A.Perrig, "Advanced and authenticated techniques for IP traceback," in Proceedings of INFOCOMM2001, Apr. 2001.

[26] C.Shannon, D.Moore, and K.claffy, "Characteristics of fragmented IP traffic on Internet links," in Proceedings of PAM2001, Amsterdam, The Netherlands, Apr. 2001.

[27] S. Kent, and R. Atkinson, "IP Authentication Header," RFC2402 http://www.ietf.org/rfc/rfc2402.txt, 1998.

[28] A.C.Snoeren, C.Partridge, L.A.Sanches, C.E.Jones, F.Tchakountio, S.T.Kent, and W.T.Stayer, "Hash based IP Traceback," in Proceedings of SIGCOMM '01, San Diego, USA, Aug. 2001.

[29] Y. Rekhter, and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC1771 http://www.ietf.org/rfc/rfc1771.txt, 1995.

[30] T. Bates, R. Chandra, D. Karz, and Y. Rekhter, "Multiprotocol Extensions for BGP-4," RFC2283 http://www.ietf.org/rfc/rfc2283.txt, Feb. 1998.

[31] Yokogawa Electronic Corp., " PAFFI - PAcket Footmark FInder," http://www.netstar.co.jp/products/PAFFI/, Jul. 2002.

[32] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321 http://www.ietf.org/rfc/rfc1321.txt, Apr. 1992.

[33] D.Moore, G.M.Voelker, and S.Savage, "Inferring Internet Denial-of-Service Activity," in Proceedings of 10th USENIX Security Symposium '01, Washington, D.C, USA, Aug. 2001.

[34] H.Krawczyk, M.Bellare, R.Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104 http://www.ietf.org/rfc/rfc2104.txt, 1997.

[35] 村井, “WIDE プロジェクトとその研究活動, ” 情報処理, 39 巻 5 号, pp.401-407, May. 1998.

[36] G. Huston, “An Examination of the Internet’s BGP table Behaviour in 2001,” APRICOT 2002, Bangkok, Mar.2002.

[37] Telecommunications Advancement Organization of Japan (TAO), “Hokuriku IT open laboratory,”
http://www.hokuriku-it.tao.go.jp/english/, Sep. 2002.

[38] TCPDUMP.ORG, “The Libpcap library,”
http://www.tcpdump.org

[39] Mike D. Schiffman, “The Libnet library ,”
http://libnet.sourceforge.net

[40] the Cooperative Association for Internet Data Analysis (CAIDA), “Skitter,”
http://www.caida.org/tools/measurement/skitter/ , Jun. 2002.

[41] D. Meyer. “Lessons in Maintaining a Route Views Server,” ISMA 07, Dec. 2000.

[42] A. Broido, K. claffy, “Analysis of RouteViews BGP data: policy atoms,” Cooperative Association for Internet Data Analysis - CAIDA, San Diego Supercomputer Center, University of California, San Diego. Proceedings of network-related data management (NRDM) workshop Santa Barbara, May 2001.

[43] I. Nam, “Internet Worm Hits Korean Shares,”
http://www.washingtonpost.com/wp-dyn/articles/A48719-2003Jan27.html, Jan.2003.

付録

A. 業績リスト

A.1 論文誌

1. 大江将史, 門林雄基, 山口英, “階層型IP トレースバック機構の提案”, IEICE trans. commun., vol.J85-B, no.8, pp.1313-1322, Aug. 2002.

2. 大江将史, 門林雄基, “階層型IP トレースバック機構の実装と検証”, IEICE trans. commun., (条件付き採録).

A.2 国際会議 (審査あり)

1. M.Oe, S.Yamaguchi, “Implementation and Evaluation of IPv6 Anycast,” Proc. of INET2000, Yokohama, Japan, Jul. 2000.

2. M.Minami, K.Nagahashi, A.Kato, Y.Kadobayashi, M.Oe, H.Esaki, J.Murai, “Project JB: Advanced IP Version 6 Research and Educational Network,” Proc. of INET2000, Jul. 2000

3. M.Oe, Y.Kadobayashi and S.Yamaguchi, “An implementation of a hierarchical IP traceback architecture ,” Proc. of SAINT'03, Florida, USA, Feb. 2003.

4. H.Hazeyama, M.Oe, and Y.Kadobayashi, “A layer-2 extension to hash-based IP traceback,” Proc. of IFICT 2003, Hamamatu, Japan, Jan. 2003.

5. Y.Sawai, M.Oe, K.Iida, and Y.Kadobayashi, “Performance evaluation of intra-domain IP traceback,” to be presented at ICT'03, Tahiti, Feb. 2003.

A.3 国内会議 (査読あり)

1. 宮本大輔, 大江将史, 木村泰司, 門林雄基, “OS Fingerprint 対策手法の実装と評価,” 日本ソフトウエア学会 WIT2001, Aug. 2001.

2. 河野智彦, 大江将史, 門林雄基, 山口英, “圧縮 Proxy システムを用いた衛星回線帯域の有効利用,” 日本ソフトウエア学会 WIT2001, Aug. 2001.

A.4 研究会

1. 大江将史, 太田正哉, “8 パズルに対するカオスを用いたヒューリスティック探索法,” 信学会総合大会, Mar. 1997.

2. 篠田晃, 大江将史,“ダイアルアップ接続における IP マルチキャストパケットの受信,” 信学会 DPS, Nov. 1997

3. 宮本大輔, 久保聡之, 大江将史, 門林雄基, “侵入監視のための Honeypot の実装と評価,” 情報処理学会 CSS2001, Oct. 2001.

4. 久保聡之, 宮本大輔, 大江将史, 門林雄基,“隠しディスクデバイスの実装と評価,” 情報処理学会 CSS2001, Oct. 2001.

5. 澤井裕子, 大江将史, 飯田勝吉, 門林雄基, “ IP トレースバック逆探知パケット方式のトラヒック量と攻撃経路再構成時間の性能解析,” 情報処理学会 IA 研究会, Jul. 2002.

6. 櫨山寛章, 大江将史, 門林雄基, “MAC トレースバック：Hash-Based IP トレースバック拡張方式の提案,” 情報処理学会 IA 研究会, Jul. 2002.

A.5 解説論文

1. 大江将史, 藤澤慎一, 染川隆司, 藤枝俊輔, 三屋光史朗, “次世代インターネット研究開発の最前線：2．アドホック・ネットワーク構築技術－外部との接続－,” 情報処理, 41 巻 08 号, Aug. 2000.

2. 門林雄基，大江将史, “IP トレースバック技術,” 情報処理，42 巻 12 号，pp.1175-1180，Dec．2001.

A.6 標準化活動

1. M.Oe, “IP traceback mechanism using IPv6 Flowlabel,” Proc. of 50th IETF, itrace WG. Minneapolis, Mar. 2001.

2. M.Oe, “A hierarchical architecture for IP Traceback,” Proc. of 54th IETF, ippt BoF, Yokohama, Jul. 2002.