2004－CSEC－27　(6)
2004／12／20

DDoS 攻撃に対する高性能発信源探査方式の提案

甲斐 俊文*　　中谷 浩茂*　　清水 弘*　　鈴木 彩子**　　塚本 克治***

あらまし インターネットの普及に伴って、不正アクセスによる被害が増加傾向にある。特に、送信元アドレスを偽装した DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃は、システムを停止に追いやることもあり、社会生活への影響が出始めている。その対策のために、幾つかの発信源探査方式（トレースバック方式）が提案されている。本稿では、既存方式の問題点を解決したハイブリッドトレースバック方式を提案する。また、探査性能および導入（実装）の容易さの点から既存技術との比較を行い、かつテストベッドにおける性能検証も実施し、提案する新方式の優位性を示す。

Efficient Traceback Method for Detecting DDoS Attacks

Toshifumi KAI*　Hiroshige NAKATANI*　Hiroshi SHIMIZU*　Ayako SUZUKI**
Katsuji TSUKAMOTO***

Abstract　The amount of damage by illegal access is increasing with the spread of the Internet. Especially the DoS (Denial of Service) and DDoS (Distributed DoS) attacks cause system down and often have serious impacts on the society. Various attacker detection techniques have been proposed until now, of which characteristics in performance and easiness of implementation are discussed in this paper. Based on the discussion, we propose hybrid traceback method that solves the drawbacks of the exiting techniques. Advantages of this proposed scheme to the exiting ones are clarified by some numerical models and experiment.

1.　はじめに

ネットワークが社会的インフラとして定着した今日、これを用いたサービスの提供は当然のものと認識されている。一方で、それを停止させようとする妨害も増加の一途を辿っている。このような「攻撃」と呼ばれる妨害行為の代表的なものに DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃がある。これらの攻撃は一般的に送信元 IP アドレスを偽装したパケットを用いていることが多く、被害者側には真の発信源が特定できないため対策が困難なものとなっている。

攻撃の信源を探査する手法として、不正パケットの経路を基に探査を行うトレースバック（図 1）がある。

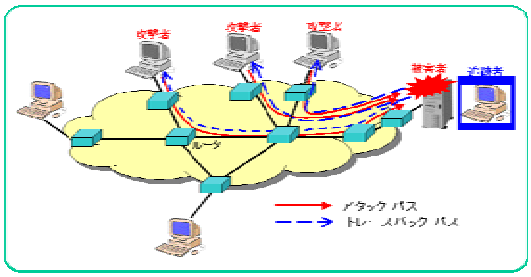

図 1　トレースバック

ただし、インターネットは、プロバイダネット、行政ネットなど固有のポリシーによって管理された AS（Autonomous System）の集合体で構成されているため、複数の AS にわたって同じ方法で探査することは不可能に近い。そこで、AS 間のトレースバックと AS 内のトレースバックを階層的に行う必要があると言われている[1][2]。

AS 内のトレースバック方式については、現在までにさまざまな方式が提案されているが[3][4][5][6][7]、それぞれに一長一短があり、どれも絶対的なものとは言えない。また、複数の方式を併用する手法も提案さ

*松下電工株式会社　システム技術研究所
Matsusita Electric Works, Ltd.　Systems Technology Research Laboratory
**NTT アドバンステクノロジ株式会社コアネットワーク事業本部システム開発ユニット
NTT Advanced Technology Corp, Core Networks Bussiness Headquarters System Development Unit
***工学院大学　情報工学科
Kogakuin University　Dept. of Computer Engineering

れているが[8][9]、有効性は明らかになっていない。

今回我々は、AS 内のトレースバック方式を対象として、既存方式の長所を生かしながら、それらが持つ短所を補完する組み合わせの手段とその実現方法について検討し[9][10]、性能面および実用面で既存方式を上回る独自の方式を考案した。さらに、この方式を用いて既存の課題を抜本的に解決した AS 内トレースバック方式を考案した。

本稿ではまず、既存トレースバック方式の中でも最も有効と言われる３つの方式（ICMP 方式、マーキング方式、Hash 方式）に着目して評価を行うことで、各方式の特性を明らかにする。次に、既存の方式では困難とされる DDoS 攻撃を高速に探査するために考案した独自方式（連動方式、uTrace）を示し、さらに独自方式と Hash 方式を組み合わせたものを新方式（ハイブリッドⅠ、Ⅱ）として提案する。特に、新方式の核となる独自方式については、探査時間に対する成功率、および実ネットワークへの導入の容易さという２つの視点から既存方式との比較を行い、優位性を示す。

2. 既存方式

IP トレースバック技術の代表的な３つの既存方式とそれぞれの実装例を表 1に示す。いずれの方式も全てのルータ上（または外付け）の探査情報取得用モジュールと、各モジュールから集めた探査情報を基にパケットの通過した経路を構築する探査端末から成る。

表 1　既存のトレースバック方式

方式名	実装例
ICMP 方式	iTrace **iTrace-II ＊**
マーキング方式	FMS AMS **AMS-II ＊**
Hash 方式	Paffi **SPIE ＊**

2.1 ICMP 方式

(1) 方式概要

ICMP 方式では、確率的にサンプリングしたパケットの探査情報を探査端末に送るために、iTrace パケットと呼ばれる特別な ICMP パケットを生成する。

ここでは ICMP 方式の具体的な実装方式として iTrace[3]に我々独自の改良を加えた iTrace-II について説明する。iTrace-II では複数のサンプリングパケットを一つの iTrace パケットにまとめて送ることで、ネットワーク負荷を抑えたまま iTrace よりもサンプリングレートを上げられるようにした。iTrace-II の動作手順を表 2に示す。iTrace-II では攻撃経路上の全てのルータから指定された個数の iTrace パケットを集めることができた時点で探査成功となる。

表 2　iTrace-II の動作

ルータ上のモジュールの動作
(i) フォワーディングされるパケットを無作為に確率 P でサンプリングする
(ii) サンプリングしたパケットについて、以下の情報を iTrace パケットに書き込む ・ IP ヘッダ＋ペイロード数バイト ・ 一つ前のルータ＋自ルータ＋一つ先のルータの IP アドレス ・ サンプリング時刻など
(iii) iTrace パケットに書きこまれたサンプリングパケットが定数 L 個を超えたら発信源探査端末宛に iTrace パケットを送信する
(iv) (i)から繰返す(探査時に特別な動作はしない)

(2) 特徴

探査情報を送るために新たにパケットを生成するため、一度に十分大きな探査情報を送信できる。

2.2 マーキング方式

(1) 方式概要

マーキング方式の ICMP 方式との大きな違いは特別に探査用のパケットを生成せず、サンプリングしたパケットに直接、探査情報を書き込む点である。

ここでは代表的な実装例として AMS-II[5]を取り上げる。その動作を表 3に示す。AMS-II では発信源探査端末（ルータマップ所有）に、攻撃経路上の全ルータからハッシュ値（フラグメントを集めて再生したもの）が全て経路確定閾値以上集まれば発信源探査が成功したことになる。

表 3　AMS-II の動作

ルータ上のモジュールの動作
(i) フォワーディングされるパケットを無作為に確率 P でサンプリングする
(ii) 自身の IP アドレスから 64bit のハッシュ値を算出し、8bit 単位で 8 分割(フラグメント)して、そのいずれかをランダムにサンプリングしたパケットの ID フィールド(16bit)に書き込む
(iii) ID フィールドの残り 8bit にフラグメント番号（0～7）と被害端末からのホップ数の値を書き込む（そしてサンプリングパケットを送信）
(iv) (i) から繰返す(探査時に特別な動作はしない)

(2) 特徴

マーキング方式は探査のために新たなパケットを生成しないためネットワークに負荷をかけず、DDoS 攻撃のように一台の攻撃端末からのパケット流量が少ない場合でもある程度高速に探査できる。

2.3 Hash 方式

(1) 方式概要

Hash 方式は前出の２つの方式とは異なり、発信源探査端末から各ルータに対して能動的に問合せを行なう。この方式の代表的な実装例として SPIE[6]があり、

ルータが全ての通過パケットについて Hash 値を保存しておき、探査端末は１パケット単位でルータに通過の有無を問い合わせる。

(2) 特徴

ルータが全てのパケットについてハッシュ値を記録しておくため、１パケット攻撃に対する探査が可能であり、精度も高い。

2.4 既存方式の問題点

既存方式について、探査可能な攻撃パケット流量の範囲と問題点を表 4にまとめた。

表 4 既存方式の比較

方式名		ICMP (iTrace-II)	マーキング (AMS-II)	Hash (SPIE)
攻撃端末一台辺りのパケット流量	大量（DoS）	○	○	―
	少量 (DDoS)	×	△	―
	単発	―	―	○
導入時の問題		ほぼ問題なし	要ルータマップ／ヘッダ改変	コスト(必要メモリ量やや大)

○:性能高 △:性能中 ×:性能低 ー:非対応

ICMP 方式はネットワークにかける負荷を考慮してサンプリング確率を低く(1/20000)設定することが推奨されており、数万個以上の攻撃パケットが送信されなければ探査できない。

マーキング方式は発信源探査端末が常に正確なルータマップを持っていなければならない点と、IP ヘッダの ID フィールドを書き換えてしまうためフラグメントが発生する環境には適応できないという点で、現実のネットワークに導入する際の障壁が高い。

Hash 方式は探査するパケット 1 つにつき数十個の問合せパケットがやり取りされるため、被害端末に大量のパケットが送られてくるような攻撃の探査には向かない。また、ハッシュ値を保存しておくためにルータにはある程度大きなメモリが必要になる。

3. 考案した新方式（ハイブリッド方式）

論文[10]で我々は、ICMP 方式と Hash 方式を連動させることにより、複数パケット攻撃に対してマーキング方式と同等の性能を持つ連動方式を考案し、それを通常の Hash 方式と組み合わせたハイブリッド I 方式を提案した。その後新たに、マーキング方式よりも単独で性能の良い UDP 方式（uTrace）を作り出し、それを Hash 方式と組み合わせたハイブリッド II 方式を考案したのでここに報告する。

3.1 ハイブリッド I 方式

3.1.1 ハイブリッド I 方式の構成

ハイブリッド I 方式は、複数パケット攻撃に対しては ICMP（iTrace-Ⅱ）方式と Hash(SPIE)方式の技術を組合せた連動方式で探査を行い、単発パケット攻撃は Hash 方式のみで探査を行う。攻撃によって双方の方式を切り替えて利用するため、それぞれ独立して動作する。Hash 方式単体の特徴、動作については前述の通りであるため、以下では我々の考案した連動方式について概要と特徴を述べる。

3.1.2 連動方式の概要

各ルータには iTrace-II と SPIE のモジュールを実装する。ただし、ルータ内で双方のモジュールが干渉し合うことはない。また、特に既存のモジュールからの機能変更もない。探査端末側も iTrace-II の受信機能と SPIE の問合せ機能を持つ。

攻撃が発生し、IDS(Intrusion Detection System)もしくはネットワーク管理者から探査要求を受け取ると、探査端末は各ルータから送られてくる iTrace パケットについて攻撃パケットがサンプリングされていないかをチェックする。そしてもし攻撃パケットが書き込まれていれば、SPIE を用いて直ちにその発信源を探査する。

3.1.3 連動方式の特徴

連動方式では iTrace パケットをトリガーにして SPIE による探査を行うため、攻撃経路上のルータのどれか一台が攻撃パケットをサンプリングすれば経路を発見できる。したがって、経路上の全てのルータでサンプリングされるまで経路を構築できない iTrace-II と比べると、高速に探査可能である。

3.2 ハイブリッド II 方式

3.2.1 ハイブリッド II 方式の構成

ハイブリッド II 方式では、複数パケット攻撃に対して我々が新たに考案した uTrace（UDP 方式）を用いる。なお、ハイブリッド II 方式においても、単発パケット攻撃の探査には Hash 方式のみを使用する。このため、以下では uTrace のみについて説明を行う。

3.2.2 uTrace の構成

各ルータには uTrace のモジュールを実装する。このモジュールは通過パケットの中から探査したいパケットの特徴にマッチするものを選択し、iTrace-II と同様の探査情報を uTrace パケットと名付けた UDP パケットに書き込み、探査端末に送信する機能を持つ。一方、探査端末は各ルータに探査したいパケットの特徴

を含んだ探査要求メッセージを送信する機能と、各ルータから送信された uTrace パケットを受信する機能を持つ。さらに、探査端末は収集した uTrace パケットに書き込まれた探査情報を元にして、次に探査要求メッセージを送信すべきルータを判断する機能も持つ。

3.2.3 uTrace の動作

図 2に uTrace の動作概要を示す。探査を開始する際に、探査したいパケットの特徴情報および被害端末最寄りのルータの IP アドレスが必要である。探査したいパケットの特徴情報とは、プロトコル番号や上位プロトコルのポート番号などである。探査端末は IDS やネットワーク管理者からこれらの情報を受け取り、下記のステップで探査を行う。

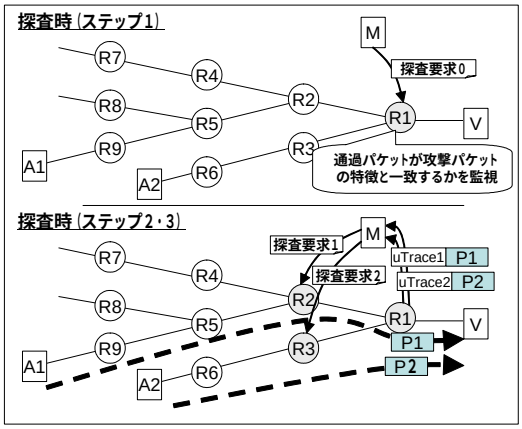

図 2 uTrace の動作概要

（ステップ１）探査要求メッセージの送信

探査端末は指定されたルータに探査要求メッセージ（探査要求０）を送信する。メッセージの内容は、探査したいパケットの特徴情報、探査端末の IP アドレス、要求 ID、uTrace パケットの要求数、要求の有効期間、である。

（ステップ２）uTrace パケットの送信

探査端末から探査要求メッセージを受けたルータは、要求の有効期間が過ぎるまで、通過パケットを全て監視し、探査したいパケットの特徴にマッチするパケット（Ｐ１、Ｐ２）を選択する。そして選択したパケットの探査情報を書き込んだ uTrace パケットを探査端末に送信する。

（ステップ３）次のルータの選択

探査端末は uTrace パケットを受信し、そのパケットに含まれている一つ攻撃端末寄りのルータの IP アドレス（Ｒ２、Ｒ３）を探査リストに加える。もし、探査リストにまだ登録されていないアドレスであったら、そのアドレスについて探査要求メッセージ（探査要求１、探査要求２）を送信する。

以上を繰り返すことで、攻撃パケットが通過するたびに、被害端末側のルータから攻撃端末に最寄りのルータまで、順番に探査要求メッセージが送信され、探査端末は各ルータから探査情報を集めることができる。

4. 性能評価

ここでは方式毎に性能についての数学モデルを求め、既存方式と考案した独自方式の比較を行う。

4.1 評価モデル

定量的に各トレースバック方式の性能を比較するために、4.1.1 節から 4.1.5 節で示す評価モデルを用いた。

4.1.1 発信源探査

コンピュータフォレンジックの観点から、発信源探査は、攻撃端末（攻撃者）に加え、攻撃パケットが通過した経路も併せて突き止めることが望ましい。このため本稿では、攻撃端末と攻撃パケット通過経路の両方を見つけ出すことを発信源探査と定義した。

4.1.2 環境条件

評価については、理想的な IDS と理想的なネットワークを用いた環境下を前提とする。ここで言う理想的な IDS とは攻撃パケットと非攻撃パケットの正確な切り分けと、攻撃発生と同時にアラート生成ができるものであり、理想的なネットワークとは通信遅延・輻輳・パケットロスが発生しないものである。

また、通常トラフィックの流量は iTrace-II や連動方式においてサンプリングしたパケットが探査端末に送られる遅延時間を無視できる程度に大きいものとする。

4.1.3 攻撃

本稿で評価した各方式では、パケットの中身が動作に影響を与えることはない。よって攻撃について変化させるパラメータは、流量(packets/sec)のみとする。

4.1.4 ネットワーク

今回は評価をシンプルにするために、攻撃経路を S 分木として扱うことにした。パラメータはツリー分岐数 S と攻撃端末と被害端末間のホップ数である。攻撃端末は S 分木の末端のノード全てとする。

4.1.5 経路確定閾値

探査端末はこの値を超えて集まった探査情報のみを信頼する。高く設定するほど間違いが少なくなり精度は良くなるが、探査完了までにかかる時間は長くなる。

4.2 数学モデル

数学モデルを扱うにあたって、各方式共通に用いる値と記号を表 5にまとめた。また、二項分布関数とし

て *fb*(成功数,試行回数,成功率)を用いる。

表 5　数学モデルに用いる記号一覧

パラメータ	記号	単位
サンプリングレート	P	－
経路確定閾値	B※	個
攻撃端末１台当りの攻撃パケット流量	A	packets/sec
探査時間	T	Sec
ホップ数	H	Hops
ツリーの分岐数	S	－
探査成功率	Q	－

※方式によって定義が異なる

4.2.1　既存方式の数学モデル

２章で説明したICMP方式とマーキング方式について発信源探査時間と探査精度の関係を表す式を以下に示す。式１は iTrace-II、式２は AMS-II の式である。但し､式１では iTrace-II がサンプリングパケットをまとめて送信する際の遅延時間は考慮していない。

$$Q=\prod_{d=0}^{H-1}(1-\sum_{k=0}^{B-1} fb(k, ATS^d, P)) \quad \cdots \quad 式1$$

$$Q=\prod_{d=0}^{H-1}(1-\sum_{k=0}^{B-1} fb(k, ATS^d, P(1-P)^{H-d-1}/8))^8 \quad \cdots \quad 式2$$

4.2.2　連動方式の数学モデル

連動方式では攻撃経路上のルータのどれか一つが iTrace パケットを送信すれば、後は SPIE を使って全経路を明らかにできる。このため、探査成功率は式３で表される。これは攻撃端末数やネットワークトポロジに依存しない。

$$Q=1-\sum_{k=0}^{B-1} fb(k, ATH, P) \quad \cdots \quad 式3$$

4.2.3　uTrace の数学モデル

uTrace は確率に依存しないため、探査に必要な情報が取得できるだけの時間が経過すれば探査は成功する。これは探査開始後、ホップ数Hに経路確定閾値－１を加えた数の攻撃パケットが通過するまでの時間である。よって発信源探査時間と探査精度の関係は式４になる。

$$Q=\begin{cases} 0 & 但し \quad T<\dfrac{H+(B-1)}{A} \\ 1 & 但し \quad T\geq\dfrac{H+(B-1)}{A} \end{cases} \quad \cdots \quad 式4$$

4.2.4　数学モデルによる比較

DDoS攻撃に対する探査性能を比較するために、探査時間を 10 秒とした場合、方式毎に探査可能な攻撃者一台当りの攻撃パケット流量(packet/sec)の最低値を求めた。なおここでは、探査成功率が 95%以上になることを「探査可能」とした。また、攻撃パケット流量以外の条件は表 6の通りである。これは攻撃端末数Ｓ^{H}＝1024 台、総パケット流量ＡＳ^{H}＝10240 packet/sec のDDoS攻撃に相当する。この条件下で数学モデルから求めた結果を表 7に示す。

この条件下で各方式の性能を比較すると、iTrace-II よりも連動方式と AMS-II は 1/10 以下の攻撃パケット流量まで探査可能であり、uTrace はさらにその 1/100 以下の攻撃パケット流量まで探査可能であることが分かる。追跡可能な一台あたりの攻撃パケット流量の上限については、各方式とも制限がなくどんなに流量の大きな攻撃でも追跡可能であるから､uTrace は他の方式よりも広い範囲の攻撃を探査可能であると言える。

表 6　評価モデルのパラメータ

パラメータ	値
ホップ数H	**10**
分岐数Ｓ	**2**
一台あたりの攻撃パケット流量Ａ	**10[packet/sec]**
経路確定閾値Ｂ	**2**
サンプリングレート	(iTrace-II,連動方式)1/4000 (AMS-II)　1/20
サンプリングパケット集約数Ｌ	**5**

表 7　探査可能な攻撃パケット流量

方式名	10 秒間で探査可能な最低攻撃パケット流量[packet/sec]
ICMP 方式 (iTrace-Ⅱ)	**1904.5**
マーキング方式 (AMS-Ⅱ)	**181.3**
連動方式 (iTrace-Ⅱ+SPIE)	**189.8**
UDP方式 (uTrace)	**1.1**

4.3　テストベッドでの実験

4.3.1　実験方法

uTrace の性能を検証するために表 8に示す構成のテストベッド上で実験を行った。このテストベッド上で攻撃端末数１台あたりの攻撃パケット流量を一定（50packet/sec）にし、攻撃端末から被害端末までのホップ数を 3, 5, 10, 15, 20 と変化させて、探査が完了する時間を測定した。攻撃の種類は syn flood とし、経路確定閾値は２とした｡試験はそれぞれ 60 回行い、探査時間の平均値と理論値を比較した。

4.3.2　実験結果

ホップ数変更試験の結果を表 9に示す。この結果により、攻撃端末単体では実測値と理論値がほぼ一致することを確認できた。実測値の方が早く攻撃端末を発見されているのは､理論計算では理想的な IDS を前提

としているため、１個目のパケットが探査開始直後に通過するような場合を考慮せず、必ず探査開始から 1/50(0.02)sec 後に通過するものとして計算しているためである。ちなみに、数学モデルとテストベッドでの実験とのその他の違いは、ネットワーク遅延時間、ルータと探査端末の処理時間、syn flood を受けた被害端末からの TCP ACK 応答、といった点である。この実験では、これらの要素は特に探査時間に大きな影響を与えていないことが分かる。

表 8　テストベッドの構成

機器・環境	項目	内容
ネットワーク	ＰＣルータ数	40 台
	エンドノード数	160 台（実 PC30 台）
	ネットワークタイプ	Ethernet (100base)
ＰＣルータ	OS	Reahat Linux 7.3
	CPU	Celeron2.0GHz
	メモリ	512Mbytes

表 9　ホップ数変更試験の結果

ホップ数	理論値 [sec]	実測値 [sec]	標準偏差
3	0.080	0.077	0.0072
5	0.120	0.118	0.0077
10	0.220	0.217	0.0077
15	0.320	0.320	0.0107
20	0.420	0.419	0.0156

5. 考察

4.2.4 節で述べたように、uTrace は AMS-II や連動方式よりも高い性能を持つ。また、uTrace は ICMP 方式同様、特に導入時に問題になる特性は持たない。これをまとめると、表 10のようになる。

表 10　既存方式と考案した方式の比較

方式名		ICMP (iTrace-II)	マーキング (AMS-II)	Hash (SPIE)	連動方式 (iTrace-II + SPIE)	UDP (uTrace)
攻撃端末一台あたりのパケット流量	大量 (DoS)	○	○	―	○	○
	少量 (DDoS)	×	△	―	△	○
	単発	―	―	○	―	―
導入時の問題		ほぼ問題なし	要ルータマップ/ヘッダ改変	コスト(必要メモリ量やや大)	コスト(必要メモリ量やや大)	ほぼ問題なし

○:性能高　△:性能中　×:性能低　－:非対応

また、我々の提案するハイブリッド II 方式は UDP 方式（uTrace）と Hash 方式を組み合わせるため、さまざまなタイプの攻撃に対して高い探査性能を持つことがこの表から分かる。

6. おわりに

我々は、トレースバックの代表的な既存方式の評価を行い、その結果を基にハイブリッド方式を考案し、優位性を示した。また、ＰＣルータを用いたテストベッドでの実機試験も行い、性能を確認した。

なお、本稿では AS 内のトレースバック方式について述べたが、複数 AS での探査を連携させるための AS 間トレースバックに関しても並行して研究中である。

(注)本研究は独立行政法人 情報通信研究機構からの委託(H14～H16 年度)による。

参考文献

[1] 塚本克治他”AS 間のトレースバックに関する一考察”,電子情報通信学会 2004 総合大会,Mar.2004

[2] 大江将史他”階層型ＩＰトレースバック機構の実装と検証”, 電子情報通信学会インターネットアーキテクチャ技術論文特集 Aug,2003

[3] S.Bellovin, "ICMP Traceback Message", InternetDraft:draft-bellovin-itrace-00.txt, submitted Mar. 2000,

[4] S.Savege, D.Wtherall, A.Karlin, T.Anderson, "Practical Network Support for IP Traceback", Proceedings of Sigcomm 2000, Aug 2000, Stockholm, Sweden,

[5] D.Song and A.Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” Proc. IEEE INFO-COM, April 2001.

[6] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Kent ST, Strayer T, "Hash-Based IP Traceback", Proc. of the ACM SIGCOMM 2001 Conf. San Diego, Aug 2001,

[7] 早川晃弘他”不正アクセス発信源追跡システムにおける追跡時間の評価”,情報処理学会第 64 回全大, Mar.2002

[8] 山田竜也他”発信源追跡のためのハイブリッドトレースバック方式の設計と実装”, 情報処理学会分散システム／インターネット運用技術シンポジウム Jan,2003

[9] 福田尚弘他”発信源探査システムの研究開発”,電子情報通信学会 2004 総合大会,Mar.2004

[10] 甲斐俊文他”送信元アドレスを偽装した不正パケットの発信源探査方式”,情報処理学会第 12 回マルチメディア通信と分散処理ワークショップ,Dec.2004