情報処理学会論文誌　Vol. 49　No. 9　3157–3164 (Sep. 2008)

# IP トレースバックのための出国印方式の試作と評価

潘　　博　文[†1]　　佐々木　良一[†1]

インターネットの普及にともない，不正アクセスによる被害が問題になっている．その中でも，発信源 IP アドレスの詐称を用いた DoS/DDoS（サービス不能）攻撃は大きな問題となっており，このような問題を解決できる IP トレースバック技術が従来から望まれていた．しかし，従来の方式は，ネットワークやルータにおける負荷の増大など，様々な問題をかかえていた．そこで，著者らは攻撃者をより短時間で特定するため，エッジルータを通過するパケットにエッジルータ自身の IP アドレスなどの情報を書き込み，被害者に送る方式（出国印方式）を提案してきた．本論文では，提案方式である出国印方式の実装方法の検討を行い，試作したプログラムに基づき，機能，性能の評価結果を報告する．

# Trial Development and the Evaluation of the Departure Point Marked Method for IP Trace Back

Hakubun Han[†1] and Ryoichi Sasaki[†1]

Recently, damages by illegal access are increasing with the spread of the Internet. Among then, there is a case of the DoS/DDoS attack used “spoofed” source IP address for in that. Therefore, the technique that can solve such a problem was expected. However, the conventional methods had various problems such as the increase of the packet or increase of the load in the router. Therefore we proposed the method named as “Syutugokuin Housiki”, which wrote in an IP address of edge router oneself to a packet passing on the router before sending it to the victim side. In this paper, after explaining the method in some detail, we describe the trial development program based on the method. After then the evaluated results applying the program to the Internet is described.

†1 東京電機大学
Tokyo Denki University

## 1. はじめに

近年インターネットの普及にともない，安価で高速である常時接続環境の普及が進み，同時にインターネットへの攻撃数は年々増加を続け，ウィルスの感染，不正アクセスなどの脅威が多くなっている．なかでもサービスを不能に追いやる脅威，DoS（Denial of service）攻撃や DDoS（Distributed DoS）攻撃と呼ばれる攻撃が問題になってきている．

DoS 攻撃とは標的とされたサーバに対し大量な不正データを送信することで，過剰な負荷をかけ，サービスを提供できなくするような攻撃である．DDoS 攻撃はこのような攻撃を並行していろいろなところから実施するものである．これらの攻撃によりネットワークのトラフィックを増大させ，ネットワーク自体の機能を麻痺させてしまうなど深刻な問題となっている．

様々なセキュリティ対策を導入しているが DoS 攻撃や DDoS 攻撃を仕掛ける不正者は後を絶たない．なぜならばこれらの攻撃自体の実装は容易であり，特に最近では，ボットネットを利用した DoS 攻撃がネットワークセキュリティへの脅威となってきている．また，これらの攻撃の際に使用される送信元 IP アドレスは偽装されることがあり，攻撃者の特定は困難なものであった．このような問題を解決するため，いくつかの IP トレースバック方式が提案されてきたが[1)–4)]，従来の方式はネットワークやルータにおける負荷の増大などの問題をかかえていた．

これに対し，Vijairagbavan らは 2007 年 2 月に IEEE ジャーナル誌の中で SIPT（Speedy IP Traceback）[6)] と呼ばれるエッジルータでパケットに IP アドレスなどの情報を挿入する方式が探索スピードなど多くの面において最も良いことを示した．しかし，ここでは具体的な実装の検討は行っていない．著者らはこれとは独立に，出国印方式と名付けた SPIT と同様な方式を開発してきた[7)]．今回，この方式の実装方法の検討を行い，システムの試作を行うとともに機能，性能の評価を行ったので，報告する[8)]．

## 2. 既存方式

今日の DoS 攻撃や DDoS 攻撃などのセキュリティ脅威の打開策としてインターネットセキュリティの分野に IP トレースバックと呼ばれる技術がある．

IP トレースバックとは，一般に IP パケットの送信元アドレスが詐称されたとしても，発信源を特定できるようにする技術の総称であり，いろいろな方式があるが[6)]，ここでは，よく知られており，本論文と関連の深い次のような 3 つの方式を紹介する．

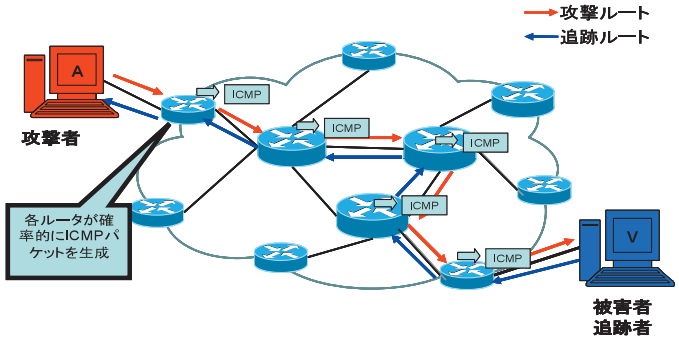


**図 1**　ICMP トレースバック方式
Fig. 1　ICMP trace back method.

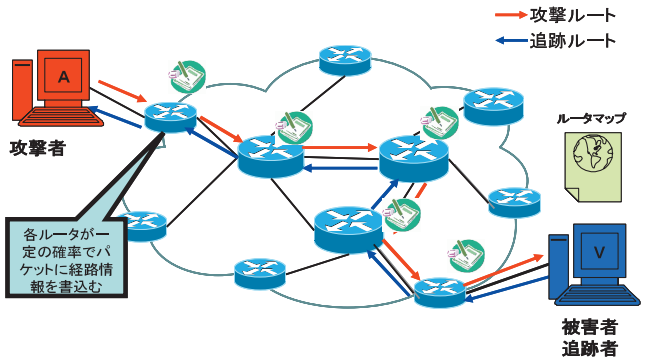


**図 2**　IPPM トレースバック方式
Fig. 2　IPPM trace back method.

### 2.1　ICMP 方式

ICMP 方式（**図 1** 参照）は，ルータがある一定の確率でパケットのサンプリングを行う．サンプリングしたパケット情報，ルータ自身のリンク情報を，ICMP パケットに載せて追跡者側へ送信する[1]．

追跡のために新たに ICMP パケットが生成されるため，ネットワークに余計なトラフィックが増えることになるという欠点があり，そのためサンプリングレートは追跡の有利性とネットワーク負荷の両方面を考慮した値が推奨される．

### 2.2　IPPM 方式

IPPM 方式（**図 2** 参照）は，ICPM 方式と異なり，追跡情報を生成するのではなく，サンプリングしたパケット本体に追跡情報を書き込むマーキングプロトコルという手法を用いている[2),3)]．

ICMP 方式と比較した場合，余計なトラフィックを増加させないのでサンプリングレートを上げることが可能であり，追跡性能を向上できるという利点がある．しかし上流ルータの書き込みに対して下流ルータによる上書きが発生する可能性がある．

また，情報を書き込むフィールドはわずかなものであり，その情報不足を補う手段として正確なルータマップが必要となってしまう．

### 2.3　Hash 方式

Hash 方式（**図 3** 参照）は，ICMP，IPPM 方式とは本質的に異なる手法である．

ルータによる機能は確率的なサンプリングは必要なく，通過パケットをすべて記録することにより，追跡を可能としている．したがってこの方式は，大量パケットによる攻撃やたった 1 つのパケットによる攻撃の発信源探査が行える[4]．

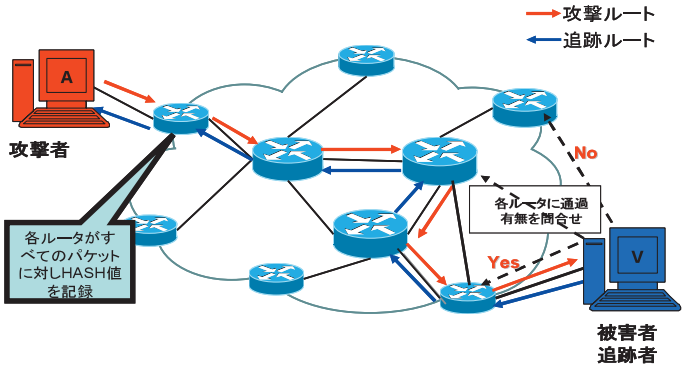


**図 3**　Hash トレースバック方式
Fig. 3　Hash trace back method.

しかし現実では，パケットを記録することは大量のストレージが必要である，保存するにはコストをかけて大きな記憶装置を導入しなければならない．

以上述べた既存の方式は，それぞれ問題点をかかえており，より良い方式の開発が望まれていた．

## 3.　出国印方式

### 3.1　概　　要

提案方式は，エッジルータで，その IP アドレスを書き込んでおけば，ネットワーク上どの地点へ行こうとも，そのエッジルータから来たものであることが確認できるだろうという発想に基づいている．

ここで，エッジルータとは，企業や大学のネットワークとインターネットの境界にあるルータを表している．なお，家庭などからのインターネットへの接続はひとまず今回の提案方式の対象外とした．

エッジルータの IP アドレス以外に発信元 PC の MAC アドレスや，IP アドレスも書き込む方法が考えられるが，この点の検討結果は，3.2.2 項に示す．

情報をパケットに書き込むマーキングプロトコルを用いるという点では，IPPM 方式と同じであるが，1 回だけの書き込みですむという特徴がある．

エッジルータでパケットにたった 1 度書き込みをすることによりネットワーク上のどの地点へ行こうとも，出発元を突き止めることができ，出国の際にパスポートに出国印を押すのと似ていることから，我々はこの提案方式を出国印方式と呼ぶことにした（**図 4**）．

### 3.2　実装方式の検討

#### 3.2.1　書き込み領域の検討

発信元側では，エッジルータで情報の書き込みを行う．書き込み領域の候補としては**図 5** に示すように TOS，Option，Identification の 3 フィールドが考えられる．

TOS と Option フィールドは Strayer らも指摘したとおり[5]，パケットのマーキングプロトコルによって，変わりやすいため，使わないことにした．

Identification フィールドはフラグメント化されたパケットを結合する際の識別子として用いられており，フラグメント化されたパケットはインターネットを流れるトラフィック全体からみても 0.25%で[10]，ごくわずかな量であると考えられるからである．

この Identification フィールドに，追跡のためのエッジルータの IP アドレス情報などを格納するが，Identification フィールドは長さが 16 ビットと短く，1 度に入れることはできない．そこで，**図 6** に示すように発信元情報という名で 8 ビットに分割して各パケットに挿入することとし，後で結合するために，ルータ識別子情報とシーケンス番号を表す index 情報を追加することとした．今，エッジルータの IP アドレスだけを送るとすると，そのアドレス長 32 bit を 8 bit で割ると 4 となり，4 回に分けて送ることになる．一方，受信先で

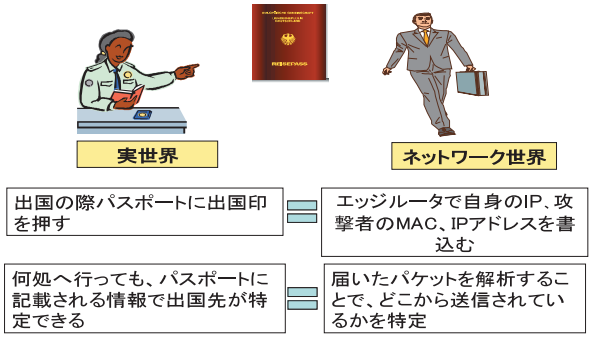


**図 4**　出国印方式
Fig. 4　Outline of Proposal method.

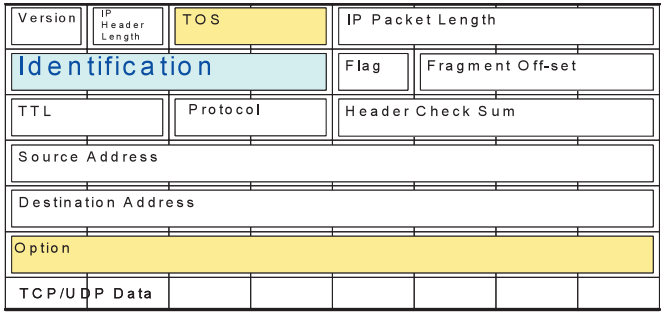


**図 5**　IPv4 パケットの構造
Fig. 5　Structure of IPv4 packet.

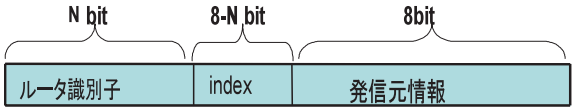


**図 6**　分割後の Identification
Fig. 6　Division plan of Identification field.

はいろいろな発信元からパケットが飛んでくるとどの 4 つが 1 つのエッジルータの IP アドレスを表しているのか分からなくなるので，ルータ識別子をつけることにした．また，パケットの到着が前後する場合に備えて情報の前後関係を示す Index 番号を用いている．図 6 では，エッジルータの IP アドレス以外も送る場合に備えて，ルータ識別子と Index 番号の長さを一般的な書き方で表現している．

### 3.2.2　書き込みデータの検討

次に書き込むべき情報の検討を行った．書き込む発信元情報の重要性は ①，②，③ の順であると考えられる．

① エッジルータ IP アドレスは，管理者に不正パケットがそのルータ経由で送られてきていることを連絡するうえで，不可欠な情報である．

② 発信元の MAC アドレスは，不正者を特定するのに重要な情報である．しかし，最近では攻撃者の PC の MAC アドレスではなく，プロキシサーバの MAC アドレスが入っている場合もあり，また改ざんできるため，直接に利用できない場合もある．

③ 発信元の IP アドレスは通常書き換えており，重要性が低い．

したがって，発信元情報として 4 つの案が考えられる（**図 7** 参照）：

①　エッジルータ IP アドレス；

②　エッジルータ IP アドレス＋攻撃ホスト MAC アドレス；

③　エッジルータ IP アドレス＋攻撃ホスト IP アドレス；

④　エッジルータ IP アドレス＋攻撃ホスト IP アドレス＋攻撃ホストの MAC アドレス；

Identification field

| 書込情報 | | 送信回数 | ルータ識別子（ビット長） | INDEX番号（ビット長） | 発信元情報（ビット/回） |
|---|---|---|---|---|---|
| 1 | ルータIPのみ（32ビット） | 4 | 6 | 2 | 8 |
| 2 | ルータIP+攻撃者MAC（80ビット） | 10 | 4 | 4 | 8 |
| 3 | ルータIP+攻撃者IP（64ビット） | 8 | 5 | 3 | 8 |
| 4 | ルータIP+攻撃者IP+MAC（112ビット） | 14 | 4 | 4 | 8 |

**図 7**　Identification フィールドの設計
Fig. 7　Design of the Identification field.

不正者を検出するためには，データは多ければ多いほど望ましいが，

(1)　データが多くなると送信回数が増え，送信回数が増えると復元が困難になる可能性がある，

(2)　しかも，すでに述べたように発信元の MAC アドレスや IP アドレスは正しくない場合がある，

(3)　エッジルータの IP アドレスが分かればそのエッジルータを管理する組織の管理者に連絡することは比較的容易であり，その管理者さえ分かれば，その組織の LAN 上のどこからそのパケットが発信されているのかを探索するのが比較的容易であるといわれている（たとえば，LAN 内においては，一般的にネットワークのモニタリングが可能であることから，発信先アドレスに対するパケットを調査・追跡することで，特定が可能と考えられる），

などの理由から，今回は案 ① を採用した．

## 4.　試作システム

提案の有効性を示すために，今回，案 ① の設計に基づきシステムを試作した．

（ア）構成

試作システムは攻撃者側（発信側）と被害者側（受信側）で構成している（**図 8** 参照）．

攻撃者側では，カーネルを改造した FreeBSD5.4 をルータとして利用し，パケットの書

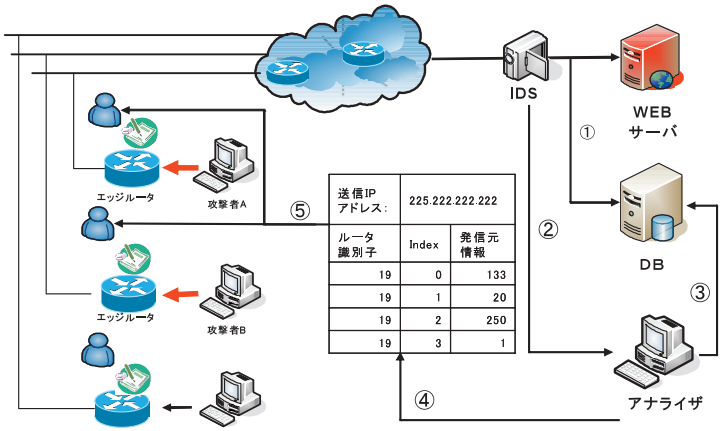


**図 8**　出国印方式構成
Fig. 8　Structure of Proposed method.

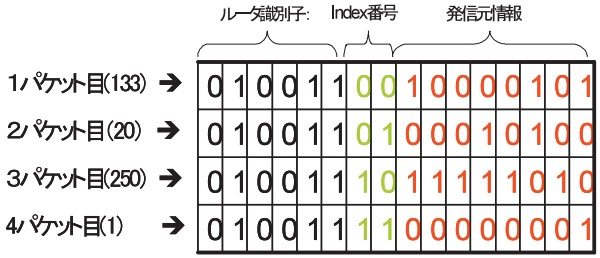


**図 9**　Identification フィールドに書き込むデータ
Fig. 9　Data written in Identification field.

き込み機能を持たせた．

被害者側では次の構成となっている．

① キャプチャ：WinPcap を使い，パケットをキャプチャする．ID 識別子フィールド分解し，データベースに出力機能を持つ．

② データベース：PostgreSQL 8.1 を使用する．キャップチャからのパケットのヘッダ情報を格納する．

③ アナライザ：探索条件に従い，データベースのヘッダ情報を抽出し，攻撃情報を復元する．

（イ）攻撃者側の処理

エッジルータでパケットの Identification フィールドに書き込む情報としては，今回はエッジルータの IP アドレスだけ送ることにしている．この場合，ルータ識別子は 6 ビット，Index 番号は 2 ビットとなり，たとえば IP アドレス 133.20.250.1 を送る場合は，**図 9** に示すようになる．なお，ルータ識別子は，エッジルータの IP アドレスを sha-1 で 160 ビットのハッシュを生成し，先頭から 6 ビットをとって使っている．

（ウ）被害者側の処理

被害者側（受信者側であり追跡者側でもある）の処理手順は以下のとおりである（以下の ①，② などは図 8 の ①，② などに対応）．

① つねに受信したパケットのヘッダ部分（含む Identification フィールドの情報）だけをデータベースに保存する．

② IDS を用いパケットを監視し，DoS 攻撃（含む DDoS 攻撃）であるかどうかを判断する．この部分は既存の方式を採用する．たとえば，パケットをシグニチャベースで照合し，あてはまったパケットの単位時間あたりの数がしきい値を超えていれば DoS 攻撃が発生と判断する．

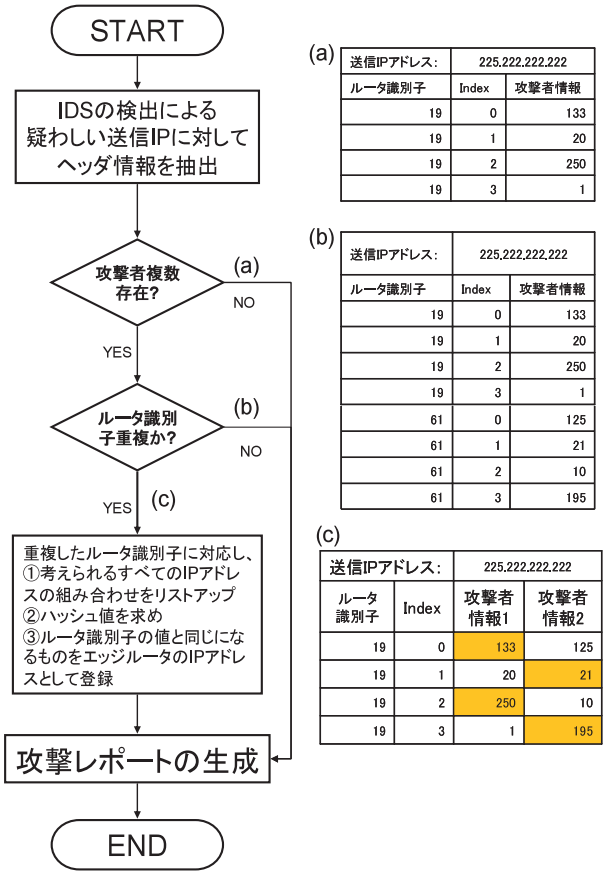


**図 10**　IP アドレス復元手順
Fig. 10　IP address restoration procedure.

③ 自動的にデータベースに保存していたパケットのうち，IDS の時間帯情報と，IDS からの情報により疑わしい発信元 IP アドレスの情報などから攻撃に関連すると考えられる部分を取り出し**図 10** に示すような方法でパケットの解析を行う．

すなわち，同じルータ識別子ごとに Index 番号順に送信元 IP アドレスを表す後ろ

8 ビット分を取り出す．

(i) もしも，図 10 の (a) や (b) に示すように，それぞれのルータ識別子に対応する値が 1 種類ならば，それを組み合わせたものが，エッジルータの IP アドレスになる．すなわち，(a) の場合は 133.20.250.1 であり，(b) の場合は，133.20.250.1 と 125.21.10.195 である．

(ii) そうではなく図 10 の (c) に示すように，同じルータ識別子に対し複数のデータが存在する場合もある．同じルータ識別子に対し複数のデータが存在するのは，エッジルータの IP アドレスのハッシュ値がたまたま同じであるような場合である．

この場合は，エッジルータの IP アドレスは 2 つあることは分かるが，それぞれが 133.20.250.1 かもしれないし，133.21.250.195 かもしれないし，125.20.10.1 かもしれないし，もっと別の組合せかもしれない．すなわち全部で 2 の 4 乗の組合せが考えられる．そこで以下に示したようにすることによって 2 つの IP アドレスを推定することができる．

重複したルータ識別子や INDEX 番号に基づいて，ルータ IP アドレスを組み合わせながら，ハッシュを生成し，ルータ識別子と比較する，等しければ，それが 1 つの発信元エッジルータの IP アドレスになる．違っていればそれらは，発信元 IP アドレスの対象ではないことが明らかになる．

④ このようにして攻撃パケットが通過したと識別されたエッジルータに対し，被害を受けているということや自分の IP アドレスなどをつけて現状ではメールなどでエッジルータの管理元に送る．

## 5. 実験と検討

### 5.1 攻撃実験

4 章で述べたように実装したシステムを用いて有用性を確認する次のような実験を行った．なお，有用であることをいうためには，(a) 攻撃元のエッジルータを正しく確認できる，(b) その処理時間が十分小さいということを示す必要がある．

(1) 利用者：攻撃者 2 名，正規ユーザ 1 名

ここで，利用者はインターネットに接続された自宅の PC を利用する．これらの PC には Identification フィールドに，情報を書き込む機能が実装されている．

(2) 攻撃先サーバ：大学（研究室）のサーバ

このサーバには 4 章で述べたキャプチャ，データベース，アナライザの機能が組み込まれている．

**表 1**　実験結果
Table 1　Experiment result.

| 攻撃ケース | 総パケット数 | 攻撃パケット数 | 結果 | 解析時間 |
|---|---|---|---|---|
| ① | 58482 | 13801 | 成功 | 769ms |
| ② | 39648 | 21372 | 成功 | 790ms |
| ③ | 65136 | 25829 | 成功 | 962ms |

(3) DDoS 攻撃種類：

(a) PING，(b) SYN Flood

1 人の攻撃者が (a) を行い，別の攻撃者が (b) を行った．

(4) 攻撃ケース

実験は次の 3 つのケースについて実施した．

① 攻撃者らは送信元 IP アドレスを詐称しない．

② 攻撃者らは送信元 IP アドレスを詐称する（2 つの IP アドレスは異なる）．

③ 攻撃者らは送信元 IP アドレスを詐称する（2 つの IP アドレスは同じ）．

この実験の結果は以下のとおりである．

(1) ①–③ については，いずれもエッジルータの IP アドレスの抽出に成功した．

(2) また，それぞれ 1 回だけの実験結果であるが，**表 1** に示すように，いずれも 1 秒以内と十分小さいものであった．

今回の実験では DDoS の攻撃元（より正確には攻撃パケットが通るエッジルータ）を 2 カ所とした．解析時間が攻撃元数に比例すると仮定すると，この数が 100 カ所の場合でも，数十秒となり実用上問題ない時間であると考えられる．今後より大規模の実験を行うことにより本当にそうか確認していきたいと考えている．

### 5.2 ルータ識別子が重複する場合の処理の検討

4 章の ③ で述べたようにルータ識別子が重複する場合は，どの組合せが正しいものかチェックする必要がある．ここでは，そのチェックの時間が現実的な時間で実施可能かどうか検討を行った．

そこで，重複が 2 つの場合は，$2^4$ 回のケースについてハッシュ値などの計算が必要であり，6 の場合は $6^4 = 1.296 \times 10^3$ 回の計算が必要となる．ここで，ハッシュの演算は，100 MIPS（$10^8$ IPS）は十分あるといわれている．32 ビットのハッシュ演算を $10^4$ 回しても，その計算時間は 1 秒以下となることが予想され十分小さいことが明らかである．重複がたとえ 10 個であってもこの計算のための処理時間は十分小さいといえる．

一方，ルータの識別子は 6 ビットで，その状態は $2^6 = 64$ 通りある．たとえば 6 回以上重複する確率を多項分布の式を用い，攻撃元が 100 カ所の場合，次のように表現される[12]．

$$\sum_{\#} \frac{100!}{k_1!\,k_2!\,k_3!\cdots k_{64}!}\left(\frac{1}{64}\right)^{100}$$

ここでの $\#$ は以下の条件である：

$$\begin{cases} k_1 + k_2 + k_3 + \cdots + k_{64} = 100 \\ (k_1 \geq 6) \text{ または } (k_2 \geq 6) \text{ または} \cdots \text{ または } (k_{64} \geq 6) \end{cases}$$

この場合の確率 $P_6$ は約 1.28%となり，非常に小さい．したがって，この方式で性能がネックになることは考えられず，提案方式は実用性があると考えられる．

### 5.3　他方式との比較

提案方式と関連するものに，Vijairaghavan らが提案した SPIT 方式がある[6]．この方式はすでに述べたように出国印方式と基本的に同じであるが，実装方式についてはほとんど言及していない．

Identification フィールドに IP アドレスを入れる方式に，Belenky らが提案した DPM 方式[9] がある．DPM 方式は，パケットのヘッダ部 17 ビットを使って，2 回に分けて書き込みをしており，1 つの IP アドレス以外を入れることはできず拡張性に乏しい．一方，提案方式では，図 7 に示したようにエッジルータの IP アドレスだけではなく，発信元の MAC アドレス情報なども書き込むことも可能である．

また，IP トレースバック方式ではないが同じ目的を達成しようとするものにエグレスフィルタ方式がある．この方式は 2000 年に RFC2827 として標準化されたものであり，ISP がエッジルータで，すべてのパケットが管理範囲内の発信元 IP アドレスであるかどうかをチェックし，管理範囲外の IP パケットを通過させないという方式である．これにより，IP スプーフィングに対応することができる．この方式はネットワークに負荷が少ないなどのメリットがあり，仮にすべてにわたりこの方式が実現していればトレースバックの必要性がなくなるともいえる．しかし，エッジルータに多くの負荷がかかるなどの理由から，現実にはこの方式が実現されてこなかったため，多くの IP トレースバック方式が提案されてきたのである．

著者らの提案方式もエッジルータに負荷がかかることが予想されるが，文献 6) によると著者らの提案方式と同様の SPIT はエグレスフィルタ方式に比べルータのオーバヘッドが小さいと記述されている．この点も今後，実験などによって確認していく必要がある．

## 6. 運用方法の検討

既存方式では IP トレースバックを運用するため，ISP 側が一斉導入する必要があり，またトレースバックシステムのサービス開始後，設備の投資や運用コストの回収，法律など様々な問題が指摘されている[11]．

本提案方式においても，導入方法などをあらかじめ考えておく必要がある．本提案方式の導入方法としては次の 2 つが考えられる．

（1）ISP を中心とした解決策

ISP が提供するエッジルータに強制的に提案方式のモジュールを実装する．これにより，本方式を急速に普及させることが可能となる．しかも，ここでは，被害が発生した場合，被害者側が ISP 側に直接問い合わせる必要がない．すなわち ISP 側から不正発信源を特定する必要がなく，ユーザ間で解決できる．また，ISP は，エッジルータを導入後，運営コストがかからないというメリットがある．法律面の問題も避けられるではないかと考えているがこれは今後の課題である．

（2）ISP ではなく企業などの組織からの解決策

ISP が提供するエッジルータに強制的に提案方式のモジュールを実装できない場合には，企業側や組織を中心とした解決法が考えられる．この場合，攻撃者が企業や組織の IP を詐称したとしても，被害が発生後，攻撃パケットの解析で，エッジルータの書き込みがないので，企業や組織は自らの攻撃ではないと主張できる．法律的に問題はないと考えられるが，普及に時間がかかる可能性がある．

したがって，（1）が法的に問題ないときは（1）で，問題が残る場合は（2）で徐々に普及させていくというのが良いと考えられる．

## 7. ま と め

以上，出国印方式の提案と評価を行い，提案方式の運用まで検討してきた．

実際の小規模の攻撃実験により，提案が有効であるという見通しを得た．提案方式は複雑

な攻撃でも探査可能であり，ネットワークとルータの負荷問題も考慮に入れた実用性の高い方式であると考えられる．

今後は，提案した手法の評価を，理論解析を精緻化することにより実施するとともに，大規模な環境において，実用的なパフォーマンスを得られるかどうかや使い勝手も検証する必要があると考えられる．

また，3.2.2 項で述べた方式 ② の実装評価も実施していきたいと考えている．

**謝辞**　本研究を進めるにあたり，ご指導たまわったコンピュータ疫学研究会の小山覚氏，高橋正和氏，東京電機大学の入江博先生に謹んで感謝する．

## 参 考 文 献

1) Bellovin, S.M.: ICMP Traceback Message, InternetDraft: draft-vellovin-itrace-00.txt (submitted Mar. 2000).
2) Song, D., et al.: Advanced and Authenticated Marking Schemes for IP Trace back, *Proc. IEEE INFO-COM* (Apr. 2001).
3) Savage, S., et al.: Practical Network Support for IP Traceback, *Proc. ACM SIGCOMM Conference*, Stockholm, Sweden (Aug. 2000).
4) Snoeren, A.C., et al.: Hash-Based IP Traceback, *ACM SIGCOMM 2001*, San Diego (Aug. 2001).
5) Strayer, W.T., Jones, C.E., Tchakountio, F., Snoeren, A.C., Schwartz, B., Clements, R.C., Condell, M. and Partridge, C.: Traceback of single IP packets using SPIE, *Proc. DARPA Information Survivability Conference and Exposition 2003*, Vol.2, Issue 22-24, pp.266–270 (Apr. 2003).
6) Vijairaghavan, V. and Shah, D.: Marking Technique to Isolate Boundary Router and Attacker, *IEEE Computer* (Feb. 2007).
7) 潘　博文，佐々木良一：IP トレースバックの為の出国印方式の提案，コンピューターセキュリティシンポジュウム 2006 (2006).
8) 潘　博文，佐々木良一：IP トレースバックのための出国印方式の試作と評価，コンピューターセキュリティシンポジュウム 2007 (2007).
9) Belenky, S. and Ansari, N.: IP Traceback With Deterministic Packet Marking, *IEEE Communications Letters*, Vol.7, No.4, pp.162–164 (2003).
10) Stoica, I. and Zhang, H.: Providing Guaranteed Services Without Per Flow Management, *Proc. 1999 ACM SIGCOMM Conference*, Boston, MA, pp.81–94 (Aug. 1999).
11) 木村道弘ほか：インターネットにおけるトレースバック運用に係る ISP 間連携の取り決め事項の整理，コンピューターセキュリティシンポジュウム 2006 (2006).
12) 河野光雄，友知政樹：統計学の基礎，牧野書店 (2003).

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

**潘　　博文**（正会員）

平成 18 年 3 月東京電機大学情報メディア学科卒業．平成 20 年 3 月同大学院工学研究科情報メディア学専攻博士前期課程修了．同年ソフトバンク BB（株）入社．現在，高度ネットワーク部勤務．バックボーンネットワークの設計に従事．

**佐々木良一**（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．平成 13 年 4 月より東京電機大学工学部教授，平成 19 年 4 月より未来科学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．平成 19 年総務大臣表彰（情報セキュリティ促進部門）．平成 19 年度「情報セキュリティの日」功労者表彰．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『IT リスクの考え方』（岩波新書，2008 年）等．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネージメント学会会長，情報ネットワーク法学会理事長，日本学術会議連携会員，日本ネットワークセキュリティ協会会長．