情報処理学会論文誌　Vol. 51　No. 9　1610–1621 (Sep. 2010)

IP トレースバックにおける出国印方式の拡張と評価

村上真教[†1]　甲斐俊文[†1]
入江　博[†2]　佐々木良一[†1,†2]

インターネットの普及にともなって，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造した 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，いろいろな IP トレースバック方式が提案されているが，そのうちでは，既存方式の問題点を解決した出国印方式が最も有望であると考えられる．しかし，この方式にも欠点があり，本論文では，この出国印方式をさらに改良し，追跡性を向上させた 3 つの方式の提案とその評価結果の報告を行っている．

Extension and Evaluation of IP Trace Back Method Using Departure Stamp in Edge Router

Masanori Murakami,[†1] Toshifumi Kai,[†1]
Hiroshi Irie[†2] and Ryoichi Sasaki[†1,†2]

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 influence social life. To cope with the problem, many IP Trace back methods have been proposed. Among them, the method named departure stamp from mother land has most desirable functions. This paper proposes the three methods which improve the traceability compared with the above method, and evaluates these methods.

†1 東京電機大学大学院未来科学研究科
Graduate School of Science and Technology for Future, Tokyo Denki University
†2 東京電機大学未来科学部
School of Science and Technology for Future Life, 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不正アクセスによる被害が増加している．そのため，不正アクセスによる被害が今後も深刻な問題となることが予想できる．不正アクセスの中でも DoS（Denial of Service）攻撃や DDoS（Distributed DoS）攻撃が脅威になっている．DoS 攻撃とは，相手のコンピュータやルータなどに不正なデータを送信して使用不能にさせたり，トラフィックを増大させて相手のネットワークを麻痺させたりする攻撃のことをいい，DDoS 攻撃は複数のネットワークに分散する大量のコンピュータがいっせいに特定のサーバへパケットを送信し，通信路をあふれさせて機能を停止させる攻撃のことをいう[4),17)]．これらの攻撃は発信元 IP アドレスの偽造が可能であり，攻撃元の特定が困難になっている．

この問題に対し，現在攻撃元を特定する技術として IP トレースバックがある[1),5)–15)]．IP トレースバックについては，ハッシュ方式，マーキング方式，ICMP 方式，出国印方式などいろいろな方式が提案されているが決定的な方式がなく，試行錯誤の中でそれぞれの方式をベースにより良い方式を検討していっているのが現状である．著者らは，出国印方式[1)] が最も可能性がある方式であると考え出国印方式を改良し，攻撃ホストの追跡を可能にする方式の検討を行ってきた．出国印方式をベースにしたのは，他の方式がプロバイダが対応しなければ実現しない方式であるのに対し，出国印方式は，企業などの管理者が協力すれば実現できる方式だからである．

本論文では改良 3 方式の提案と評価を扱う．以下，2 章において既存方式の概要を述べる．3 章で提案方式について述べる．4 章に提案方式の運用方法，5 章に提案方式の比較と考察を述べる．6 章にまとめを述べる．

2. 既存方式

DoS 攻撃や DDoS 攻撃を受けた際に攻撃元を特定する技術に IP トレースバックというシステムがある．IP トレースバックとはパケットの送信元アドレスが詐称されたとしても，発信元を特定することができる技術の総称である（**図 1**）．本章では，既存の IP トレースバック技術の中で特に重要と思われる 4 つの方式について説明していく．

2.1 ICMP 方式

すべてのルータに，ある生成確率（例：1/20000）で通過するパケットに追跡のための情報である ICMP Traceback メッセージを新たに生成させ，攻撃対象へと送信する方式であ

© 2010 Information Processing Society of Japan

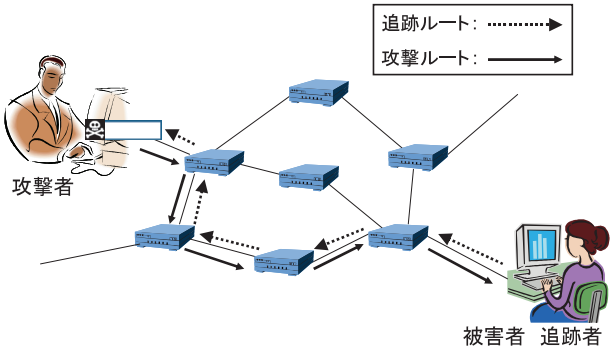


図 1　IP トレースバック
Fig. 1　IP traceback method.

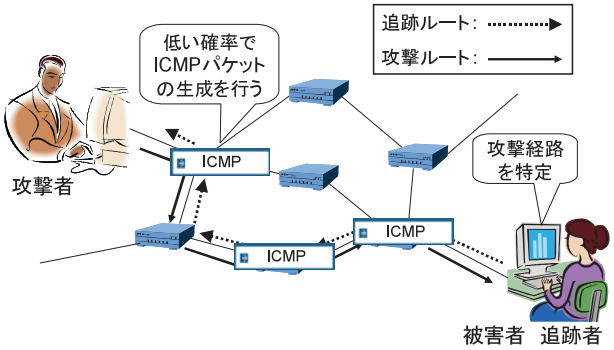


図 2　ICMP 方式
Fig. 2　ICMP method.

る（**図 2**）．

しかし，この生成確率でトレースバックを成功させるには攻撃ホスト 1 台あたり数万パケットも必要となる欠点がある．

2.2　マーキング方式

流れているパケットに直接，追跡情報を書き込む方式である．これは IP ヘッダの特定のエリアに追跡情報を分割して挿入し，攻撃対象へと送り届ける（**図 3**）．攻撃対象は，分割されたマーキングパケット（追跡情報が書かれたパケット）を元どおりに復元し攻撃経路を再構築する．

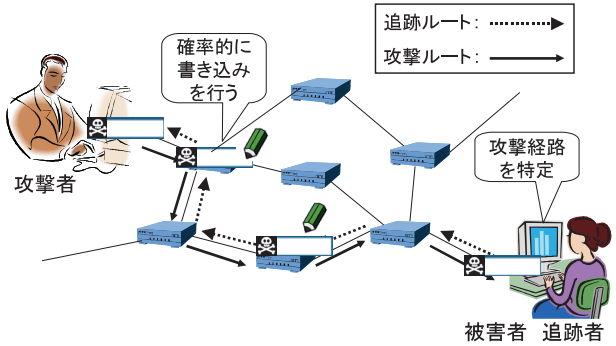


図 3　マーキング方式
Fig. 3　Marking method.

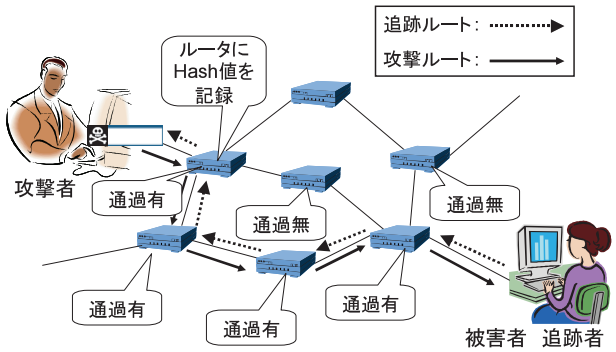


図 4　ハッシュ方式
Fig. 4　Hash method.

ネットワークに負荷をかけず追跡を実行できるという利点があるが，複数の攻撃経路を再構築する際に一定の時間が必要になる．また，分割されたデータを復元する過程において莫大な計算量を要するという問題がある．

2.3　ハッシュ方式

ルータでの確率的なサンプリングは必要なく，通過するパケットのハッシュ値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元探査が行える（**図 4**）．

© 2010 Information Processing Society of Japan

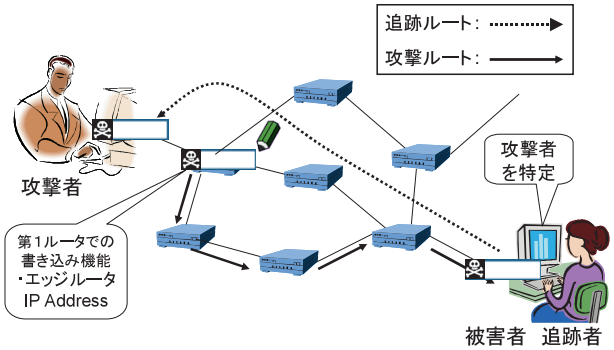


図 5　出国印方式
Fig. 5　IP traceback using departure stamps.

問題点としては，現実ではパケットをすべて記録することは大量のストレージが必要であったり，プライバシの問題が生じたりしてパケットをすべて保存することはできないという点があげられる．

2.4　出国印方式

出国印方式は，自組織から送出されるパケットに，企業や大学のネットワーク管理者が組織の出入り口のエッジルータで，自動的にそのエッジルータの IP アドレスを書き込む方式である（**図 5**）．ここでいうエッジルータとは，攻撃者側のネットワークの入り口に置かれたルータのことをいう．**図 6** で示している IP ヘッダ内の Identification フィールドにエッジルータ IP アドレスを埋め込むことを想定している．Identification フィールドが使われている可能性はあるが，文献 16) によるとその確率は 0.25%であり別のデータが入っている可能性は小さいと考えられる．また，そのようなものが入っていて，たとえ攻撃者を間違えてトレースバックしても相手サーバの管理者が再度調べることを想定できるので実用上は問題ないと考えている．ただし，Identification フィールドは 16 bit しかないので，IP アドレス 32 bit を埋め込むことができない．そこで，追跡情報を**図 7** のように分割して挿入し，攻撃対象へと送り届ける．図 7 でいうルータ識別子とは他のルータと区別をつけるためにある．ルータ識別子の値は，エッジルータ IP アドレスから sha256 で生成した 256 bit のハッシュ値の，先頭の 6 bit とする．Index 番号は何番目のパケットなのかを知るためのものである．印鑑は，エッジルータの IP アドレスが分割されて挿入される領域である[1]．

被害者側では複数の攻撃パケットの Identification フィールドを集め，同じルータ識別子を持つ印鑑を Index 番号順に並べることで，攻撃元のエッジルータの IP アドレスを取得することができる[1]．

なお，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見ても 0.25% [16] で，ごくわずかな量であると考えられるから Identification field を使うことにした[1]．

2.5　既存方式比較

出国印方式は組織の管理者が，組織内のパケットをキャプチャしたり，書き込みをしたりするので，プロバイダの人間がチェックする必要はなく，そのチェックの際に生じるプライバシの問題もクリアされている．しかし，出国印方式にも，(1) エッジルータまでしかトレースバックできない，(2) 異なるエッジルータで発信元識別子が偶然同一の値になった場

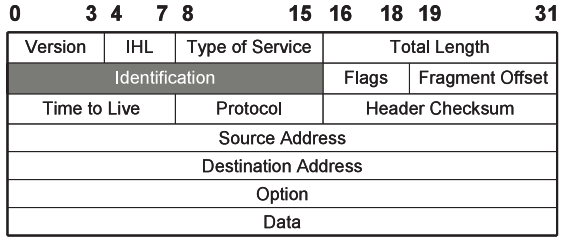


図 6　出国印の書き込み領域
Fig. 6　Fields in which departure stamps can be written.

	ルータ識別子 (6bit)	Index番号 (2bit)	印鑑 (8bit)
第1パケット	エッジルータIPのハッシュ値	00(0)	11000000(192)
第2パケット	〃	01(1)	10101000(168)
第3パケット	〃	10(2)	00000001(1)
第4パケット	〃	11(3)	00101101(45)

※エッジルータのIPアドレスが192．168．1．45の場合

図 7　出国印の押印方法
Fig. 7　Departure stamp formats.

© 2010 Information Processing Society of Japan

合には，正しくエッジルータ IP アドレスが再構築できないことがあり，誤検知が生じる可能性がある，(3) すべての Index 番号のついたパケットが集まらなければ，エッジルータ IP アドレスを復元することができないという 3 つの欠点がある[1)]．

3. 提案方式

今回著者らは，出国印方式をベースとして，攻撃ホストの追跡を可能にし，誤り確率の上昇をなるべく少なくした方式を提案する．提案方式は，エッジルータに ARP テーブルを利用して攻撃者などの発信元 MAC アドレスを書き込む機能を追加する．この追加により，攻撃元までのトレースバックが可能となる．

攻撃者 MAC アドレスの書き込み方により，トレースバック性能が異なってくるので，本章では単純に攻撃者 MAC アドレスをパケットに書き込む MAC 印鑑方式，効率化のために書き込む方法を工夫した MAC 挿入方式および芸名印方式の 3 つの提案方式について述べる．

3.1 MAC 印鑑方式

MAC 印鑑方式は，単に攻撃ホストの情報（エッジルータ IP アドレスと攻撃者 MAC アドレス 48 bit）を Identification Field に書き込む方式である（**図 8**）．エッジルータ IP アドレスと攻撃者 MAC アドレスの合計 80 bit を印鑑部分に 10 bit ずつ 8 回に分けて送信する．被害者側では，受信したパケットを Index 番号に従って組み立ててからエッジルータ IP アドレスと攻撃者 MAC アドレスを割り出してトレースバックを行う．

3.2 MAC 挿入方式

MAC 挿入方式ではエッジルータ IP アドレスと攻撃者 MAC アドレスからハッシュ値を生成して発信元識別子とする（**図 9** 左）．エッジルータ IP アドレスを印鑑部分に 8 bit ずつ 4 回に分けて送信する．被害者側では**表 1** に示すプロセスに従って攻撃元情報を割り出して，トレースバックを行う．

印鑑に攻撃者 MAC アドレスを使わない場合でも，攻撃側のエッジルータで発信元識別子と MAC アドレスの対応表を作っておけば，発信元識別子だけで攻撃者を割り出すことができる（**表 2**）．

3.3 芸名印方式

攻撃者 MAC アドレスに対応し，MAC アドレスよりも短い芸名印をつくり芸名印テーブルをエッジルータへ持たせる．芸名印方式は，本名とは別に芸名を用いて活動を行う芸能人と同様に，ネットワークにおける本名としての MAC アドレスと，トレースバックは行えるが端末の特定はできない芸名印を使用する．そのため，今回著者らはこの方式を「芸名

発信元識別子 (3bit)	Index番号 (3bit)	印鑑 (10bit)
エッジルータIP ＋ 攻撃者MAC から生成したハッシュ値	000(0)	1100000010
	001(1)	1010000000
	010(2)	0001001011
	011(3)	01+攻撃者MAC
	100(4)	攻撃者MAC
	101(5)	攻撃者MAC
	110(6)	攻撃者MAC
	111(7)	攻撃者MAC

図 8　MAC 印鑑方式の押印方法
Fig. 8　MAC stamping.

発信元識別子 (6bit)	Index番号 (2bit)	印鑑 (8bit)	
エッジルータIP ＋ 攻撃者MAC から生成したハッシュ値	00(0)	11000000(192)	エッジルータIP
	01(1)	10101000(168)	
	10(2)	00000001(1)	
	11(3)	00101101(45)	

MAC 挿入方式①

発信元識別子 (2bit)	Index番号 (2bit)	印鑑 (12bit)
エッジルータIP ＋ 芸名印 から生成したハッシュ値	00(0)	110000001010
	01(1)	100000000001
	10(2)	00101101+芸名印
	11(3)	芸名印

芸名印方式①

図 9　芸名印方式と MAC 挿入方式の押印方法
Fig. 9　MAC insertion 1 and alias stamping 1.

表 1　攻撃元情報の割出しプロセス
Table 1　Procedure for IP traceback.

MAC挿入方式	芸名印方式
(1)出国印方式と同様に、被害者側でパケットを集めて、エッジルータのIPアドレスを再構築	(1)出国印方式と同様に、被害者側でパケットを集めて、エッジルータの IPアドレスと芸名印を再構築
↓	↓
(2)得られたエッジルータのIPアドレスからWhoisなどでエッジルータの管理者を突き止め、連絡する。その際、発信元識別子も知らせる。	(2)得られたエッジルータのIPアドレスからWhoisなどでエッジルータの管理者を突き止め、連絡する。その際、芸名印も知らせる。
↓	↓
(3)エッジルータの管理者は被害者から知らされた発信元識別子で対応表を検索して攻撃ホストのMACアドレスを得る。	(3)エッジルータの管理者は被害者から知らされた芸名印で芸名印テーブルを検索して攻撃ホストのMACアドレスを得る。

© 2010 Information Processing Society of Japan

表 2　対応表
Table 2　Mapping.

発信元識別子のハッシュ値	MACアドレス
51	73-10-22-5B-AA-01
31	76-06-08-60-CD-02
10	86-04-08-63-D6-03
19	79-04-07-5B-D1-04

表 3　従業員者数が多い企業
Table 3　Japanese Companies with a large number of employees.

順位	企業名	従業員数(単独)
1	ヤマトホールディングス(株)	125043
2	トヨタ自動車(株)	65994
3	東日本旅客鉄道(株)	56219
4	松下電器産業(株)	46830
5	(株)日立製作所	41557

印方式」と名づけた．芸名印の数はエッジルータが管理する MAC アドレスの数だけあればよい．**表 3** に示すように最も大きな組織でも従業員の数は 12 万人程度であり，しかも，それらすべてを 1 つのエッジルータが 1 カ所で管理することはない．したがって，bit 数は 16 ビットもあれば，$2^{16} = 65536$ より十分であると考えられる．16 bit で芸名印を作ることにより，MAC アドレスよりも少ない bit 数で個々を表現することを可能にした．そして，芸名印は発信元識別子や印鑑に利用する（図 9 右）．エッジルータ IP アドレスと芸名印の合計 48 bit を印鑑部分に 12 bit ずつ 4 回に分けて送信する．被害者は，表 1 に示すプロセスに従って攻撃元情報を割り出してトレースバックを行う．

4. 提案方式の運用方法

3 章で，著者らは MAC 印鑑方式，MAC 挿入方式，芸名印方式の 3 方式を考案した（**表 4**）．表 4 中にある発信元識別子の内容と印鑑の内容はそれぞれ何を使うのかを示している．さらに著者らは発信元識別子 bit 数を減少させることによりできた，**表 5** の 8 方式を考案する．本章では，提案方式の運用方法について述べる．そして，運用する際の問題点について述べる．

表 4　各方式の識別子部内容と印鑑部内容
Table 4　Content of the router identifier and departure stamp for each proposed technique.

方式	識別子の内容	印鑑の内容
出国印	エッジルータIP	エッジルータIP
MAC印鑑	エッジルータIP 攻撃者MAC	エッジルータIP 攻撃者MAC
MAC挿入	エッジルータIP 攻撃者MAC	エッジルータIP
芸名印	エッジルータIP 芸名印	エッジルータIP 芸名印

表 5　各方式の構成
Table 5　Composition variations.

方式	発信元識別子	Index	印鑑	パケット数
出国印	6bit	2bit	8bit	4パケット
MAC印鑑①	3bit	3bit	10bit	8パケット
MAC印鑑②	7bit	4bit	5bit	16パケット
MAC挿入①	6bit	2bit	8bit	4パケット
MAC挿入②	9bit	3bit	4bit	8パケット
MAC挿入③	10bit	4bit	2bit	16パケット
芸名印①	2bit	2bit	12bit	4パケット
芸名印②	7bit	3bit	6bit	8パケット
芸名印③	9bit	4bit	3bit	16パケット

4.1 MAC 印鑑方式の運用方法

（ア）MAC 印鑑方式の攻撃者側処理

エッジルータが**図 10** でも示したとおりに，パケットの Identification フィールドに書き込みを行う．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見ても 0.25%で[16]，ごくわずかな量であると考えられるからである．そ

© 2010 Information Processing Society of Japan

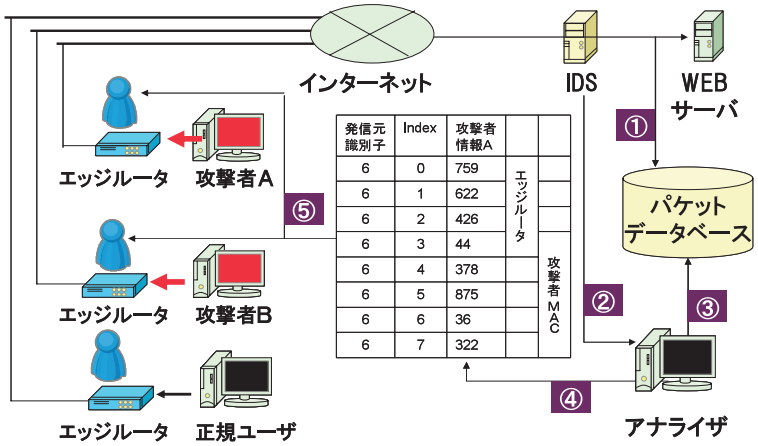


図 10　MAC 印鑑方式構成
Fig. 10　Flow chart of IP traceback using MAC stamping.

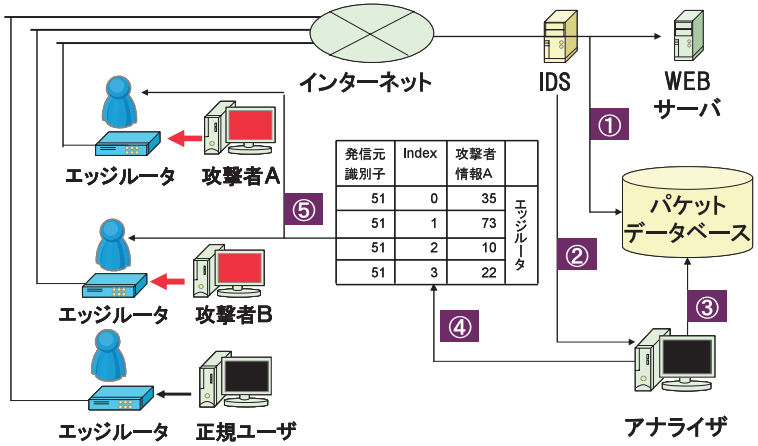


図 11　MAC 挿入方式構成
Fig. 11　Flow chart of IP traceback using MAC insertion.

して，エッジルータの管理者は発信元識別子と MAC アドレスの対応表を作成する．MAC アドレスは，ARP テーブルから情報を取得する．仮に ARP 解決をいっさい行わないで被害者にパケットが届いても，発信元識別子が重なっていなければエッジルータまではトレースバックできる．

（イ）MAC 印鑑方式の被害者側処理

追跡者側（被害者側）の処理手順は以下のとおりである（以下の ① ② などは図 10 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（Identification フィールドの情報を含む）だけをデータベースに保存する．

② IDS（侵入検知システム）がある場合は，IDS を用いパケットを監視し，DoS 攻撃や 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．

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，送信先 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パケットを取り出し，解析を行う．その後，送信先 IP アドレス，発信元識別子，Index ごとに Identification Filed の印鑑 bit を取り出す．それぞれに対応する値が 1 種類ならば，それを組み合わせたものが，エッジルータ IP アドレスや攻撃者 MAC アドレスになる．もしも，そうではなくハッシュ値が重なった場合は，正しい組合せを求める．

④ その際，届いたパケットの Identification フィールドのデータを結合し，攻撃側のエッジルータ IP アドレスと攻撃者 MAC アドレスを復元する．

⑤ そしてこれらの情報と，被害を受けていることならびに自分の IP アドレスなどを現状ではメールなどでエッジルータの管理者に送る．

4.2　MAC 挿入方式の運用方法

（ウ）MAC 挿入方式の攻撃者側処理

エッジルータが図 9 左でも示したとおりに，パケットの Identification フィールドに書き込みを行う．そして，エッジルータの管理者は発信元識別子と MAC アドレスの対応表を作成する．

（エ）MAC 挿入方式の被害者側処理

追跡者側（被害者側）の処理手順は以下のとおりである（以下の ① ② などは**図 11** 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（Identification フィールドの情報を含む）だけをデータベースに保存する．

© 2010 Information Processing Society of Japan

② IDS（侵入検知システム）がある場合は，IDS を用いてパケットを監視し，DoS 攻撃や 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．

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，送信先 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パケットを取り出し，解析を行う．その後，送信先 IP アドレス，発信元識別子，Index ごとに Identification Field の印鑑 bit を取り出す．それぞれに対応する値が 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．もしも，そうではなくハッシュ値が重なった場合は，正しい組合せを求める．

④ その際，届いたパケットの Identification フィールドのデータを結合し，攻撃側のエッジルータの IP アドレスを復元する．

⑤ そしてこれらの情報と，被害を受けていることならびに自分の IP アドレスなどを現状ではメールなどでエッジルータの管理者に送る．

⑥ 被害を受けていることを報告されたエッジルータの管理者は，対応表から攻撃元を特定する．

4.3　芸名印方式の運用方法

（オ）芸名印方式の攻撃者側処理

エッジルータが図 9 右でも示したとおりに，パケットの Identification フィールドに書き込みを行う．そして，エッジルータの管理者は MAC アドレスと芸名印の対応表を作成する．

（カ）芸名印方式の被害者側処理

追跡者側（被害者側）の処理手順は以下のとおりである（以下の ① ② などは**図 12** 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（Identification フィールドの情報を含む）だけをデータベースに保存する．

② IDS（侵入検知システム）がある場合は，IDS を用いてパケットを監視し，DoS 攻撃や 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．

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，送信先 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パケットを取り出し，解析を行う．

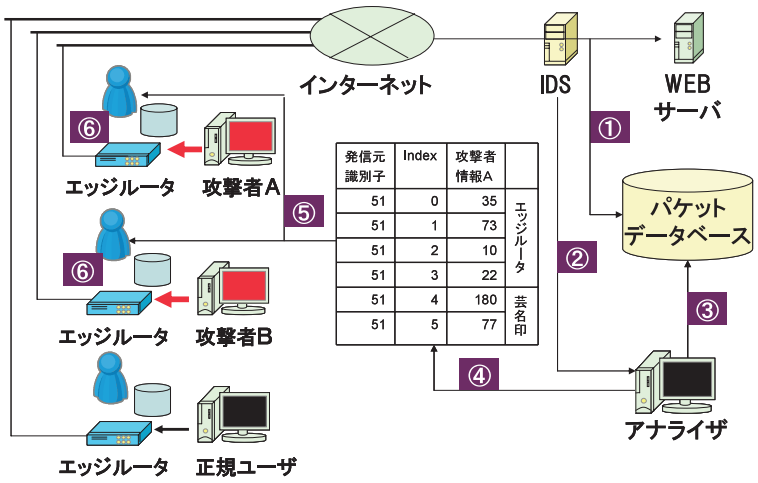


図 12　芸名印方式構成
Fig. 12　Flow chart of IP traceback using alias stamping.

その後，送信先 IP アドレス，発信元識別子，Index ごとに Identification Field の印鑑 bit を取り出す．それぞれに対応する値が 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．もしも，そうではなくハッシュ値が重なった場合は，正しい組合せを求める．

④ その際，届いたパケットの Identification フィールドのデータを結合し，攻撃側のエッジルータの IP アドレスを復元する．

⑤ そしてこれらの情報と，被害を受けていることならびに自分の IP アドレスなどを現状ではメールなどでエッジルータの管理者に送る．

⑥ 被害を受けていることを報告されたエッジルータの管理者は，対応表から攻撃元を特定する．

5.　提案方式の特徴と比較

ここで提案した 3 つの方式はすべての企業などの組織が 100%採用している状態になることが望ましいが，DDoS 攻撃の場合は部分的に採用されていてもその部分の攻撃者はトレースバックできる．そうすれば，(1) DDoS 攻撃はある割合で検知できそれらを抑えられるだけでも攻撃の集中を低減させることができ，(2) また，一部のボット PC が検知できれば

© 2010 Information Processing Society of Japan

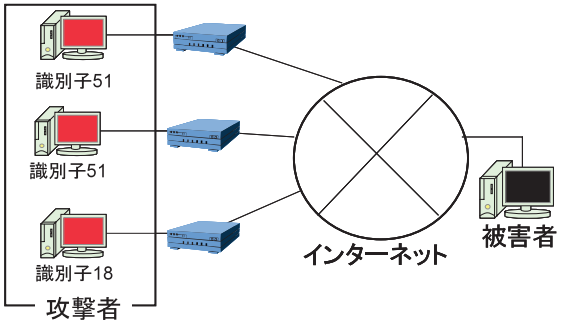


図 13　発信元識別子の衝突
Fig. 13　Multiple routers with duplicate router identifiers.

ハーダ PC などの検知につながる可能性があり，(3) さらに攻撃が自分たちの組織からのものでないことを証明できるというメリットもあるので，部分的な実装でも有効性のあるものとなっている．

著者らはこの誤り確率が最も低くなる方式を明らかにするために，数学の確率分布式により各方式の誤検知発生確率を求めて比較した．

5.1　発信元識別子に関する比較

DDoS 攻撃のように複数の攻撃元からパケットが送信されてくると，異なるエッジルータで発信元識別子が同一の値になることがある（**図 13**）．被害者側で印鑑を再構築する際，発信元識別子が重なっていると正しい組合せが分からず，誤検知が生じる．したがって複数の攻撃元がある場合に，発信元識別子が重複する確率が本節での誤り確率となる．ただし，MAC 印鑑方式と芸名印方式については，発信元識別子が重なっていても，重なる台数が少なければ，正しい印鑑の組合せを求めることができる可能性がある．

そこで，まず発信元識別子の衝突確率を求める方法を述べる．そして，MAC 印鑑方式と芸名印方式について何台まで発信元識別子が重なっても誤り確率が生じずにすむかを求める．最後に，識別可能台数を考慮して各方式について誤りが生じる確率を求める．

5.1.1　発信元識別子の衝突確率

発信元識別子のハッシュ値が衝突する可能性について考える．ある特定の識別子 C_i（$i = 1$〜2^z）に n 台以上重複する確率はルータの識別子 z bit，攻撃者と思われる利用者 Y 人とした場合，2 項分布の正規分布による近似を用いることにより次のように表現される．

表 6　発信元識別子が重なった場合
Table 6　Multiple routers with duplicate router identifiers.

ルータ識別子	Index	攻撃元情報A	攻撃元情報B		
51	0	A0	B0	エッジルータP	
51	1	A1	B1		
51	2	A2	B2		
51	3	A3	B3		
51	4	A4	B4		
51	5	A5	B5		芸名印
51	6	A6	B6		
51	7	A7	B7		

$$P(C_i) = P(X \geq n) = P\left(w \geq \frac{2^z \times n - Y}{\sqrt{Y \cdot (2^z - 1)}}\right) \tag{1}$$

式 (1) の w は標準正規分布に従う．よって 1〜2^z のどれか 1 つの値で衝突する確率は式 (2) である．

$$P(C_1 \cup C_2 \ldots \cup C_{2^z}) \tag{2}$$

$$P(C_1) + P(C_2) + \cdots + P(C_{2^z}) \tag{3}$$

式 (2) の計算は困難でありかつ C_i の発生確率は小さいと考えられるので，今回は式 (2) を近似した式 (3) で計算する．

5.1.2　発信元識別子重複時の識別機能

発信元識別子が同じでも別の発信元の可能性もある．発信元識別子が重なった場合 2 人以上の攻撃者を識別できるかが問題になってくる（**表 6**）．正しく発信元が識別できた場合は，各データを組み合わせた値のハッシュ値は，テーブルの中の発信元識別子の値（表 6 においては 51）に一致するはずである．このような場合は重なっていても識別能力があるので，いくつまで重なっても大丈夫か検討することにした．この結果は表 10 に示すとおりである．その過程をもう少し詳しく記述する．MAC 挿入方式で発信元識別子が重なった場合には，識別子の内容と印鑑の内容がことなっているため（表 4），正しい組合せを求めていたとしても被害者側で正しい発信元識別子を求めることができない（**図 14**）．したがって，

© 2010 Information Processing Society of Japan

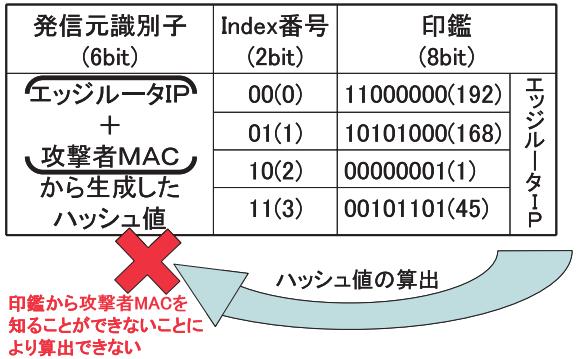


図 14　MAC 挿入方式のハッシュ値算出
Fig. 14　Calculation of hash value for MAC insertion.

表 7　情報の誤った組合せ A
Table 7　Incorrect reconstruction of data (A).

ルータ識別子	Index	発信元情報A	発信元情報B		
51	0	A0	B0	エッジルータIP	
51	1	A1	B1		
51	2	A2	B2		
51	3	A3	B3		
51	4	A4	B4		
51	5	A5	B5		芸名印
51	6	A6	B6		
51	7	A7	B7		
算出されるハッシュ値		18	11		

2 台重なると識別できなくなる．

次に，芸名印方式や MAC 印鑑方式で発信元識別子が重なった場合には，識別子の内容と印鑑の内容が同じため印鑑から発信元識別子を求めることができる．誤った組合せでは誤ったハッシュが算出され（**表 7**），正しい組合せを求めないと元の発信元識別子は算出されない（**表 8**）．しかし，これもある確率で間違った組合せで求めた発信元識別子の値と正しい

表 8　情報の正しい組合せ
Table 8　Correct reconstruction of data.

ルータ識別子	Index	発信元情報A	発信元情報B		
51	0	A0	B0	エッジルータIP	
51	1	A1	B1		
51	2	A2	B2		
51	3	A3	B3		
51	4	A4	B4		
51	5	A5	B5		芸名印
51	6	A6	B6		
51	7	A7	B7		
算出されるハッシュ値		51	51		

組合せで求めた発信元識別子の値が一致してしまうことがある（**表 9**）．この確率を求めるため，まず組合せの総数を求める．

表 9 のように芸名印方式 ② で 2 台の発信元識別子が重なった場合，パケットの組合せ総数は以下のようになる．

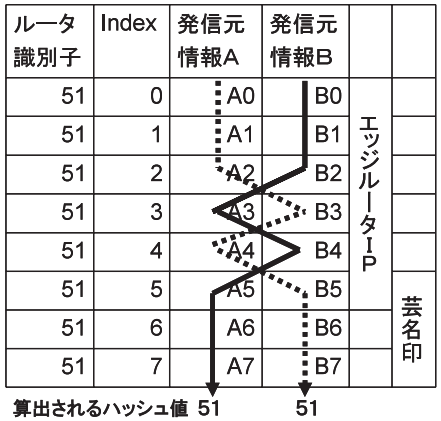
2 台の場合，Index が 0 のパケットは A0，B0 の 2 通り，Index が 1 のパケットは A1，B1 の 2 通り，Index が 2 のパケットは A2，B2 の 2 通り，Index が 3 のパケットは A3，B3 の 2 通り，Index が 4 のパケットは A4，B4 の 2 通り，Index が 5 のパケットは A5，B5 の 2 通り，Index が 6 のパケットは A6，B6 の 2 通り，Index が 7 のパケットは A7，B7 の 2 通り，よって 1 台目の組合せは $2\times2\times2\times2\times2\times2\times2\times2=2^8=256$ 通りとなる．2 台目の組合せは残ったパケットを組み合わせるだけなので $1\times1\times1\times1\times1\times1\times1\times1=1^8=1$ 通りとなる．1 台目と 2 台目の入れ違いもあるので 2! で割る必要がある．よって，2 台のときの組合せ総数は式 (4) に示すとおりとなる．

$$m_1=\left(\prod_{X=1}^{2}x^8\right)\div 2!=128 \tag{4}$$

$$m_2=\left(\frac{1}{2^7}\right)^2=\left(\frac{1}{128^2}\right) \tag{5}$$

© 2010 Information Processing Society of Japan

表 9　情報の誤った組合せ B
Table 9　Incorrect reconstruction of data (B).



$$m_3 = \left(\prod_{x=1}^{2} x^8\right) \div 2! \times \left(\frac{1}{128^2}\right) = 128 \div 128^2 = 0.0078125 \tag{6}$$

次に 2 台の発信元のハッシュ値が同じになる確率を考える．1 台目の攻撃者のハッシュ値が**表 10** のように 51 になるのは，ハッシュ値は 0 から 127 の 128 通りのハッシュ値が出るので 51 が出る確率は 1/128 となる．2 台目も同様にして 1/128 となる．2 台とも 51 が出る確率は式 (5) に示すとおりとなる．最後に式 (4) と式 (5) をかけることによって間違った組合せでも正しいハッシュ値が算出されてしまう確率を求めている．さらに，n 台の発信元識別子が重なった場合を式 (7)，(8)，(9) に示す．

$$m_1 = \left(\prod_{x=1}^{n} x^y\right) \div n! \tag{7}$$

$$m_2 = \left(\frac{1}{2^z}\right)^n \tag{8}$$

$$m_3 = \left(\prod_{x=1}^{n} x^y\right) \div n! \times \left(\frac{1}{2^z}\right)^n \tag{9}$$

表 10　識別不可能台数を求めた結果
Table 10　Number of attackers that can be undistinguished.

重なった台数	1台	2台	3台	4台
MAC印鑑①	0	0.125	識別不可能	識別不可能
MAC印鑑②	0	0.125	識別不可能	識別不可能
MAC挿入①	0	識別不可能	識別不可能	識別不可能
MAC挿入②	0	識別不可能	識別不可能	識別不可能
MAC挿入③	0	識別不可能	識別不可能	識別不可能
芸名印①	0	識別不可能	識別不可能	識別不可能
芸名印②	0	0.00781	0.13348	識別不可能
芸名印③	0	0.125	識別不可能	識別不可能

y：Index の数　z：識別子ビット数　n：衝突台数

そして，式 (9) を利用して 4 台までを求めた結果を表 10 に示す．ここでは，識別不可能確率は表 10 に示すようになる．ここで，この確率が 0.5 を超えるものを識別不可能と記述した．表 10 よりたとえば芸名印 ② は 3 台までは識別可能であるといえる．MAC 挿入 ① ② ③ は 2 台でも重なると識別できず，芸名印 ① と MAC 印鑑 ① ② は 2 台までならば識別できることが分かった．ただし，たとえば MAC 印鑑 ① の場合は識別できないことが 0.125 と小さいが存在する．しかし，トレースバックの際に攻撃者と思われる側の管理人に 1 度問い合わせる運用を想定できるので間違えても影響は小さい．

5.2　到着するパケットの調査・分析

攻撃パケットの到着間隔を求めるために最大規模の DDoS 攻撃と DoS 攻撃の過去事例から到着間隔を求めることにした．以下に攻撃パケット到着間隔を求めた計算プロセスを記す．

(1) DDoS 攻撃

最大規模の DDoS 攻撃は文献 4) によると，1 秒あたりの受信パケット数は事例より 1,200 万パケットであり，攻撃元は 3,000 台ぐらいであったという．これは最大規模のものであり，少ない台数の攻撃も多いと考えられる．

(2) DoS 攻撃

文献 3) によると，DoS の攻撃元は 1 カ所であり，総通信量は 1 Gbps であったという．1 秒あたりの受信パケット数は DDoS の事例より DoS 攻撃パケット間隔サイズも 62.5 byte とすると DoS の 1 秒間のパケット数は，

$1\,\mathrm{Gbps} \div 8 \div 62.5 = 200$ 万パケット

© 2010 Information Processing Society of Japan

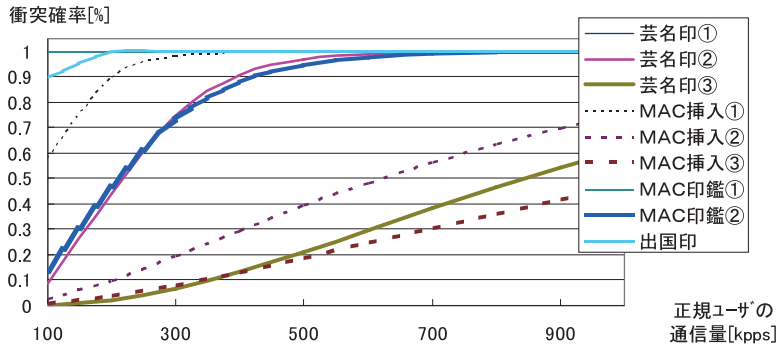


図 15　確率分布で求めた誤り確率
Fig. 15　Probability distribution.

であると推定できる．

(3) ノーマルパケット

約 8,000 人規模の大学のエッジルータへのパケットをキャプチャして 1 秒あたりのノーマルパケット受信数を求めたところ，1 番通信量が多い時間帯で 30 kpps の通信があった．また，このときの発信元は約 30 台であった．以上より，DDoS 攻撃時は最大 3,000 台ぐらいの発信源からパケットが到着することが分かる．

5.3 比　　較

式 (3) を用いて芸名印 ② は 4 台以上，MAC 印鑑 ① ② と芸名印 ③ は 3 台以上，MAC 挿入 ① ② ③ と芸名印 ① は 2 台以上重複する発信元識別子の割合を求めた結果を**図 15** に示す．図 15 から攻撃台数が増えるにつれて衝突確率（すなわち誤り確率）が上がっていくことが分かる．

5.4 考　　察

図 15 より発信元識別子のビット数が多い MAC 挿入 ③ の誤り確率が小さいことが分かる．したがって台数が多いときでも誤り確率の率が最も低い MAC 挿入方式 ③ が 8 つの候補の中では 1 番適しているといえる．

また，200 台でなら誤り確率は 1%，500 台程度であれば 3%ぐらいであるのが，800 台を超えると 10%を超えてしまうので，本方式は，DoS 攻撃と比較的規模の小さい DDoS 攻撃に適していることも分かった．

6. ま　と　め

本論文では出国印方式にホスト識別機能を追加した 3 つの提案方式を述べ，各提案方式の評価を行った．この結果，DDoS 攻撃に対しては MAC 挿入方式 ③ が最も適切な方式であることが明らかになった．

今後は，MAC 挿入方式 ③ を実装し，大規模なネットワーク環境下での実験を実施することにより，複数のネットワークに攻撃者が存在する場合でも，5 章と同様の結果が得られることを検証する．また，そのような場合に素早く攻撃者情報を復元できるように解析システムの自動化を実現してゆく．さらに，ハッシュ方式，マーキング方式，ICMP 方式などの改良方式との比較も今後の課題である．

参　考　文　献

1) 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，情報処理学会論文誌，Vol.49, No.9, pp.3157–3164 (2008).
2) 企業データ情報局，従業員者数リスト. http://company.multi-facet.org/rank/r1020000.htm (参照 2009 年 1 月 23 日)
3) 出雲教郎：DoS 攻撃の手口を知る．http://www.atmarkit.co.jp/fsecurity/special/58dos/dos01.html (参照 2009 年 1 月 23 日)
4) （株）インターネットイニシアティブ：DDoS の実体と対策．http://www.microsoft.com/japan/technet/security/secnews/columns/column060426.mspx (参照 2009 年 2 月 12 日)
5) Chao, G. and Kamil, S.: IP Traceback based on Packet Marking and Logging, *2005 IEEE International Conference on Communications* (*ICC2005*), Vol.2, pp.1043–1047 (2005).
6) Armoogum, S. and Mohamudally, N.: Mobile Agents and Packet Marking for Real-Time IP Traceback, *International Conference on Digital Society* (*ICDS2009*), pp.260–265 (2009).
7) Wei-Tsung, S., Yi-Hsun, C., Zong-Bing, W. and Yau-Hwang, K.: A table-driven approach for IP traceback based on network statistic analysis, *11th International Conference on Advanced Communication Technology* (*ICACT2009*), Vol.03, pp.1633–1637 (2009).
8) Zhaoyang, Q., Chunfeng, H. and Ningning, L.: A Novel Deterministic Packet Marking Scheme for IP Traceback, *Power Electronics and Intelligent Transportation System, 2008* (*PEITS '08*), pp.38–41 (2008).
9) Ashley, C., Wanlei, Z., Jaipal, S. and Yang, X.: Detecting and Tracing DDoS At-

© 2010 Information Processing Society of Japan

tacks by Intelligent Decision Prototype, *6th Annual IEEE International Conference on Pervasive Computing and Communications* (*PerCom 2008*), pp.578–583 (2008).
10) Vamsi, P., Arjan, D. and Sriram, C.: TTL Based Packet Marking for IP Traceback, *IEEE Global Telecommunications Conference* (*IEEE GLOBECOM 2008*), pp.1–5 (2008).
11) Stefanidis, K. and Serpanos, N.: Implementing filtering and traceback mechanism for packet-marking IP-traceback, *4th International IEEE Conference on Intelligent Systems* (*IS2008*), pp.14–28 (2008).
12) Shaoh-Chen, K. and Yen-Wen, C.: An edge router-based fast internet traceback, *IEEE Region 10 Conference on TENCON 2007* (*IRCT2007*), pp.1–4 (2007).
13) Cheol-Joo, C., Seoung-Hyeon, L. and Jae-Seung, L.: A Study of Defense DDoS Attacks Using IP Traceback, *Intelligent Pervasive Computing* (*IPC2007*), pp.402–408 (2007).
14) Syed Obaid, A. and Choong Seon, H.: On IPv6 traceback, *International Conference Advanced Communication Technology* (*ICACT2006*), Vol.3, pp.2138–2143 (2006).
15) Vijairaghavan, V. and Shah, D.: Marking Technique to Isolate Boundary Router and Attacker, *IEEE Computer*, Vol.40, No.2, pp.54–58 (2007).
16) Stoica, I. and Zhang, H.: Providing Guaranteed Services Without Per Flow Management, *Proc. 1999 ACM SIGCOMM Conference*, Boston, MA, pp.81–94 (Aug. 1999).
17) Arbor Networks: Worldwide Infrastructure Security Report, Vol.5.

(平成 21 年 11 月 30 日受付)
(平成 22 年 6 月 3 日採録)

村上　真教
平成 21 年 3 月東京電機大学工学部第一部情報メディア学科卒業．同年 4 月東京電機大学大学院未来科学研究科情報メディア学専攻入学．現在は IPv6 ネットワークセキュリティの研究に従事．

甲斐　俊文（正会員）
平成 12 年 3 月九州工業大学情報工学部知能工学科卒業．平成 14 年 3 月九州工業大学大学院情報工学研究科博士前期課程修了．同年 4 月松下電工株式会社（現パナソニック電工株式会社）入社．トレースバック技術をはじめとするネットワークセキュリティの研究開発に従事．

入江　博
平成 10 年 3 月東京都立大学理学部数学科卒業．平成 16 年 3 月東京都立大学大学院理学研究科博士課程修了．理学博士（東京都立大学）．同年 4 月より東京電機大学工学部講師，平成 19 年 4 月より東京電機大学未来科学部講師．専門は微分幾何学，特にハミルトン力学系の幾何学的な研究から発達したシンプレクティック幾何学，確率論的な考え方にも関連する積分幾何学を主に研究している．日本数学会会員．

佐々木良一（フェロー）
昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入社．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，平成 14 年情報処理学会論文賞，平成 19 年総務大臣表彰，平成 20 年情報処理学会功績賞等を受賞．著書に，『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，日本ネットワークセキュリティ協会会長．

© 2010 Information Processing Society of Japan