Vol. 49 No. 6 情報処理学会論文誌 June 2008

L2-based IP トレースバック方式の提案と実装

播磨宏和[†] 伊藤将志[†] 鈴木秀和[†]
岡崎直宣[††] 渡邊晃[†]

インターネット利用人口の増大に伴い，悪意ある利用者による DoS 攻撃が多発している．DoS 攻撃は正常なアクセスとの区別ができず，ファイアウォールの設置や，ルータのフィルタリングといった方法で防ぐことは難しい．また，送信元の IP アドレスが偽造されていることがほとんどで，攻撃者の特定は困難とされている．これまで様々な IP トレースバック技術が研究されているが，攻撃経路を正確に追跡できないことや，ルータの処理負荷が大きくなる等の問題が指摘されている．そこで我々は偽造が困難なルータのレイヤ 2 アドレスに着目した L2-based IP トレースバックを提案する．提案方式は特定のルータにおける同一宛先パケットの中継回数が閾値を超えた場合のみ，DoS 攻撃の可能性があると判断し，攻撃経路の追跡情報を生成する．また，様々な DoS 攻撃に対応するため，シグネチャを利用して DoS 攻撃ごとに閾値を決定する．提案方式を実装して評価を行った結果，ルータに与える負荷は十分に小さく，様々な DoS 攻撃を検出できることを確認した．

Proposal and Its Implementation of L2-based IP Trace Back Method

Hirokazu Harima,[†] Masashi Ito,[†] Hidekazu Suzuki,[†]
Naonobu Okazaki,[††] Akira Watanabe[†] and

With the increase of population who use the Internet, DoS attacks by malicious users are becoming serious problems. It is difficalt to prevent DoS attacks by setting up Firewalls or using router's filtering functions, because it is difficult to distinguish DoS attacks from normal accesses. It is said that identifying the attacker is quite difficult, because source IP addresses of packets are always forged. Though there have been several studies on IP trace back technologies, there still remain problems that tracing mechanism is not so accurate, and the loads of routers are so high. In this paper, we propose L2-based IP trace back method noting that layer2 addresses of routers are impossible to forge. The proposed method generates the information that identifies the attacking route only when the number of forwarded packets exceeds the predetermined threshold value. Threshold values are determined according to each Dos attack using signature, in order to detect several types of DoS attacks. We have implemented and evaluationed the proposed method, and it has been confirmed that the loads of routers are sufficiently small and it can detect several types of DoS attacks effectively.

1. はじめに

インターネット技術は情報交換手段における社会基盤のひとつとして定着し，電子商取引や有料コンテンツ配信など，様々なサービスが展開されている．しかし，これらのサービスを妨害する攻撃が脅威となっている．中でも，サービス不能攻撃（DoS 攻撃）は，ターゲットホストに対して大量の接続要求やデータを送りつけることにより，ホストを機能不全にしたり，ネットワークのトラヒックを増大させるなどしてネットワークの機能を麻痺させたりする攻撃であり，防御が極めて困難な攻撃として問題になっている．

DoS 攻撃は正当な通信との区別が困難なため，ファイアウォールの設置やルータのフィルタリングといった方法で防ぐことは難しい．ソフトウェアの脆弱性をついた攻撃においては，少量の攻撃パケットでホストが麻痺する場合もある．これに対しては，セキュリティ更新プログラムをサーバに適応することで回避できるが，攻撃者はセキュリティホールの検出を続けるため，一時的な防御法にしかならない場合が多い．

DoS 攻撃を回避するには，攻撃ホストと接続されているルータを発見し，接続を切断したり，通信のトラヒックを制御したりする必要がある．しかし，送信

† 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
†† 宮崎大学工学部
Faculty of Engineering, University of Miyazaki

元アドレスは偽造されている場合がほとんどであり，攻撃者を特定するのが難しいという特徴がある．このような DoS 攻撃に対して，攻撃ホストを特定できる技術として，IP トレースバック技術が盛んに研究されている[1)]．IP トレースバック技術は，主にルータに機能を追加し，攻撃パケットが通過した経路をさかのぼる．

IP トレースバックは一般にルータの改造を伴うので，全プロバイダが同一手法を採用することを想定するのは非現実的である．プロバイダ内で責任を持って送信元ルータを検出し，プロバイダ間は互いに協力して最終的な送信源を検出する必要がある[2)]．我々はプロバイダ間が連携する前に，各プロバイダが自ネットワーク内の攻撃元を迅速に追跡できることが先決と考え，同一プロバイダ，または同一組織内での IP トレースバックの方式に着目した．

既存の IP トレースバック技術として，ルータのデバッグ機能を利用したリンクテスト方式[3)4)]，ICMP パケットに追跡のための情報をのせてエンドホストに送信する ICMP 方式[5)]，通信パケット自体に追跡のための情報を埋め込むマーキング方式[6)~9)]，全ての中継パケットをログとして記憶するログ方式[10)~13)] が提案されている．リンクテスト方式は管理者のマニュアル操作が必要で負担が大きい．ICMP 方式およびマーキング方式は Flood 系の攻撃に対してのみ有効で，少数のパケットで攻撃が成り立つような場合には対応できない．ログ方式はルータの処理負荷が大きく，通常時のルータ性能に影響を与えるなどの課題がある．

本研究では，攻撃者による偽造が困難なルータのレイヤ 2 アドレスに注目し，かつ DoS 攻撃の可能性がある場合のみ必要な情報を記録する L2-based IP トレースバックを提案する．提案方式では，ルーティング処理時に特定のルータにおける同一宛先パケットの中継回数を計測し，一定の閾値を超えると攻撃の可能性があると判断する．攻撃の種類によっては閾値が異なることがあるため，DoS 攻撃ごとにシグネチャを定義し，DoS 攻撃の可能性があるかどうかを判断する．これにより，提案方式は様々な DoS 攻撃に対応でき，ルータの処理負荷も少ない．提案システムを実装した結果，攻撃ホストまでの経路を迅速に追跡できることを確認するとともに，ルータの性能劣化はほとんど無いことを確認した．

2 章で既存技術と課題を述べ，3 章で L2-based IP トレースバック，4 章で実装，5 章で評価を述べ．6 章でまとめを行う．

2. 既存技術とその課題

以下に代表的な IP トレースバック技術を取り上げ，概要とその課題について述べる．

2.1 リンクテスト方式

リンクテスト方式はルータが本来持っている機能を利用して，攻撃ルートを割り出す．代表的な手法として input debugging が知られており，ルータのデバッグ機能を利用する．攻撃トラヒックの特徴を抽出してアクセスリストを作成し，一致する攻撃トラヒックについてアクセスログを保存する．次に，ログ内容から攻撃パケットが入ってきた入力ポートを特定し，上流ルータを割り出す．手作業で上流のルータをさかのぼる必要があり，追跡に時間が掛かり，人的労力が膨大になる．また，攻撃が行われている間しか追跡が行えないという課題がある．

2.2 ICMP 方式

ICMP 方式は，パケットの通過情報をルータからエンド端末に対して ICMP により通知する方式である．文献 5) ではパケット通過時に 2 万分の 1 などの低い確率で，ルータ自身の IP アドレス等の情報を格納した ICMP パケットを宛先に対して送信する．DoS 攻撃によって被害ホストは攻撃パケットと同時に上記 ICMP パケットを受信することになる．受信した ICMP パケットの内容から，攻撃パケットが通過したルータを特定することができる．しかし，攻撃経路中に ICMP を拒否しているルータやファイアウォールが存在していると，情報が被害ホストに届かないことがある．

2.3 マーキング方式

マーキング方式は，ルータがパケット転送時に，ある一定の確率で攻撃経路の情報を生成する方式である．文献 6) では，IP ヘッダの identification フィールドに中継ルータの IP アドレスを分割して挿入し，被害ホストへ送り届ける．被害ホストはマーキングされたパケットを収集し，分割する前の IP アドレス情報を復元して攻撃経路を再構築することができる．しかし，追跡にはマーキングしたパケットが大量に必要で，経路構築の計算量が膨大になるという課題がある．また，攻撃者がマーキング情報を偽造するような攻撃への対処が難しい．

2.4 ロ グ 方 式

ログ方式は，ルータが転送する全てのパケットに対してログを記録する．IP ヘッダの一部とペイロードの先頭部分を圧縮して記録する．追跡においては，探査装置が被害ホストに隣接するすべてのルータに対して，攻撃パケットのログが記録されているかどうか調

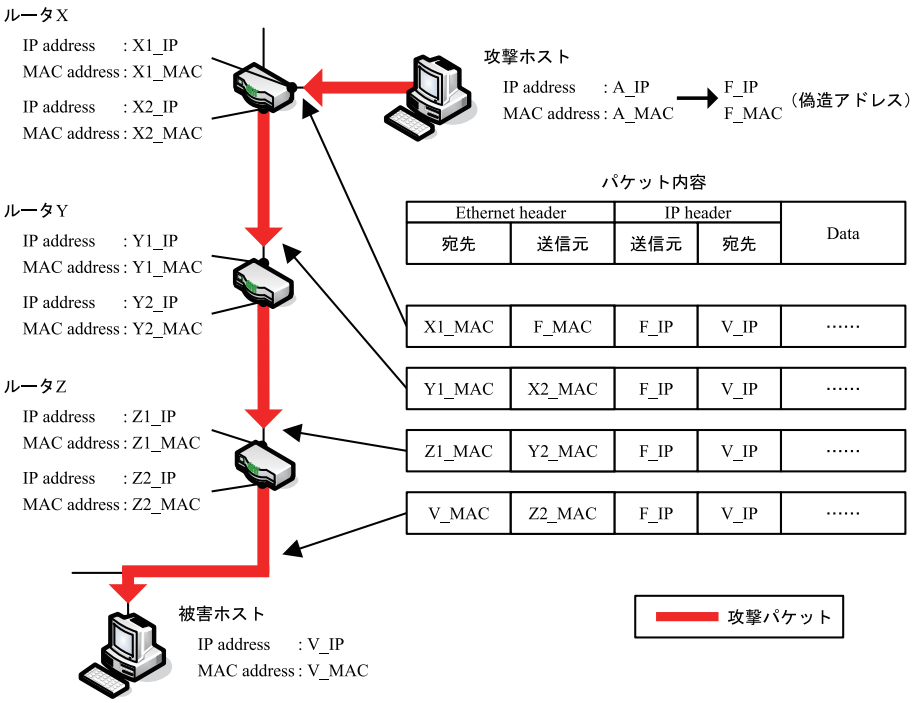


図 1 攻撃パケットのアドレスが変化する様子
Fig. 1 The state of address changes in an attacking packet.

査する．該当するログ情報が記録されていれば，そのルータに隣接する上位ルータに対しても同様に判定を繰り返す．攻撃パケットの情報が 1 つだけでも記録されていれば，発信源を特定できるという利点があるが，パケットごとにハッシュ計算をするための高い処理能力がルータに求められる．また，随時パケットのログを記録し続けなければいけないため，ルータが保持する記憶容量によっては攻撃追跡のためのログ情報が失われる可能性があり，限られた時間で追跡を完了させる必要がある．パケットのログを記録する際に，同時に LAN の MAC アドレスの情報も含める方式が提案されている[13]．これにより上位ルータの特定が容易かつ確実にできるという利点があるが，ルータに高い処理能力を必要とする点は変わっていない．

3. L2-based IP トレースバック

L2-based IP トレースバックはレイヤ 2 の情報を利用して攻撃者の追跡を行う．レイヤ 2 がイーサネットの場合は MAC アドレスを使用するが，レイヤ 2 を抽象化し，様々なデータリンクに対応できるようにしている．追跡情報が最小限となるよう，2 種のテーブルを生成する．また，様々なタイプの DoS 攻撃にも対応できるようにシグネチャリストを定義している．

3.1 レイヤ 2 情報の利用方法

攻撃ホストから被害ホストに DoS 攻撃が仕掛けられたときのパケットの内容が変化する様子を**図 1** に示す．代表的な例としてレイヤ 2 は LAN とし，レイヤ 2 ヘッダは MAC アドレスであるものとする．攻撃ホストから送信されたパケットの送信元 IP アドレスは一般に偽造されており，送信元 MAC アドレスも偽造されている可能性が大きい． IP アドレス“ A_IP ”を持つ攻撃ホストが，IP アドレス“ V_IP ”を持つ被害ホストに攻撃を仕掛けたとき，ルータを通過するごとに MAC アドレスが入れ替わっていく．このとき攻撃ホストが送信する攻撃パケットの送信元 IP アドレスは“ A_IP ”から“ F_IP ”に，MAC アドレスは“ A_MAC ”から“ F_MAC ”に偽造されているものとする．宛先 IP アドレスは被害ホストのアドレスであり，ルータを通過してもその内容が変わることはない．また，MAC アドレスは中継されるルータの MAC アドレスであり，この部分を偽造することはできない．つまり，攻撃パケットには被害ホストの IP アドレスと，上位ルータの正しい送信元 MAC アドレスが必ず含まれている．

L2-based IP トレースバックでは，ルータが攻撃経路の構築において，攻撃パケットの送信元 MAC アドレスから上位のルータを特定して記録しておく．この情報をもとにトレースバックを行う．

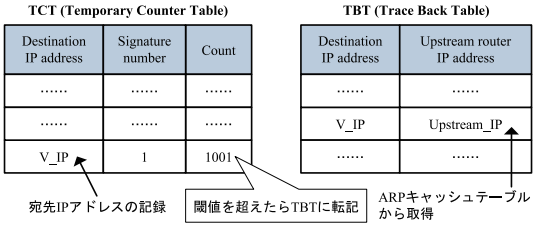


図 2 テーブルの種類とその内容
Fig. 2 Table types and its contents.

3.2 アドレス情報の記録

ルータはパケット種別ごとに，単位時間あたりにおけるパケット中継回数をリアルタイムで計測する．ある宛先に対するパケットの中継回数が設けられた閾値を超えると，DoS 攻撃の可能性があると判断する．DoS 攻撃には様々な種類があるため，DoS 攻撃ごとにシグネチャを定義し，閾値を設定する．

ルータはシグネチャごとにパケット中継数を数える一時カウンタテーブル（TCT: Temporary Counter Table），及び経路構築時に参照するトレースバックテーブル（TBT: Trace Back Table）の 2 つを保持する（**図 2**）．パケット中継時に宛先 IP アドレスとシグネチャリストを参照して，パケット種別ごとに中継回数を TCT に記録する．シグネチャ番号欄には DoS 攻撃に対応した番号を記述する．TCT の内容は 1 秒程度の短い一定間隔で消去する．シグネチャごとに閾値が設けられており，カウント値が上記一定時間内に閾値を超えた場合，宛先 IP アドレスを攻撃対象とした DoS 攻撃が行われている可能性があると判断する．この時のパケットの送信元 MAC アドレスを利用して，上位ルータを特定し，TBT に転記する．実際に TBT に記録する内容としては，ARP キャッシュテーブルから上位ルータの IP アドレスを取得し，この内容を記録する．

このように上位ルータを特定するために MAC アドレスを利用するが，TBT に記憶するときは IP アドレスを用いる．これは，管理ホストからの追跡を行いやすくするためと，レイヤ 2 を抽象化するためである．プロバイダネットワークのレイヤ 2 は LAN とは限らず，ATM や専用線を利用しているところもある．このような場合においても，TBT のフォーマットは変える必要はない．レイヤ 2 がイーサネットの場合は MAC アドレスを使用するが，ATM の場合は VPI/VCI アドレスを入力値として ARP キャッシュテーブルを参照し，上位ルータの IP アドレスを取得する．また，専用線の場合はインタフェース名を入力値としてルーティングテーブルを参照し，IP アドレスを取得する．TBT は攻撃の可能性があった場合のみ生成されるもので，数日単位の期間で保持する．

3.3 シグネチャリスト

カウント値に設けられる閾値は，ネットワーク管理者によって決定される．処理の重いプロトコルでは，少量のパケットでもシステムの機能を低下させ，OS の脆弱性をついた攻撃では単発のパケットでも機能不全となることがある．このような少量のパケットによる攻撃も，本論文では DoS 攻撃の対象としている．あらゆる DoS 攻撃に対応可能とするため，ルータは DoS 攻撃を判別するためのシグネチャリストを保持する．シグネチャは DoS 攻撃の種類を一意に特定するシグネチャ番号と関連付けられている．シグネチャには Snort[14] のシグネチャルールを参考にし，独自の形式として定義した．**表 1** に代表的な DoS 攻撃とそのシグネチャを示す．DoS 攻撃のタイプとしては，Flood 系のものと，OS の脆弱性をついたものに分類できる．UDP Flood と ICMP Flood においてはパケット長が長い場合と短い場合があり，長い場合はネットワーク帯域を埋めつくし，短い場合はターゲットの CPU を攻撃する．シグネチャ欄の括弧内は実際のプログラムで用いられる書式を記述した．

3.4 必要メモリサイズの見積もり

プロバイダの基幹ネットワークは，コアルータとエッジルータで構成されるが，コアルータは MPLS などのラベル処理であるため，本提案方式の対象外である．エッジルータにおいて，ラベルから対応する相手のエッジルータのアドレスを判別できるためである．従って，基幹に設置される場合の TCT の所要メモリ量については，ハイエンドエッジルータでの見積もりを示す．

TCT は宛先 IP アドレスと DoS 攻撃シグネチャのペアごとに作成されなければならない．しかし，TCT の更新周期が 1 秒程度であるため，同時に多くのメモリを必要とはしない．具体的な方法については 5.1 節のモジュール構成にて記述する．

ルータの最大処理性能を P[パケット/秒]，TCT レコードサイズを S[バイト]，処理パケットのうち集約可能なパケット数の平均値を F[パケット] とすると，TCT の必要メモリサイズ Q[バイト] は下記の式で表すことができる．

$$Q = P \div F \times S \quad (1)$$

ここで，レコードサイズ S は 28 バイトとする．内訳は，宛先 IP アドレス：16 バイト（IPv6 を想定），シグネチャ：1 バイト，中継カウンタ：3 バイト，その他（時刻情報など）：4 バイト，リンク情報（ハッシュ衝突

表 1 DoS 攻撃の種類とシグネチャ
Table 1 Types of DoS attacks and signatures.

番号	DoS 攻撃名	プロトコルタイプ	攻撃タイプ	シグネチャ
1	SYN Flood	TCP	Flood 系	TCP フラグ:SYN (ip_p=IPPROTO_TCP,th_flags_a=TH_SYN)
2	Tear-Drop	TCP	脆弱性	IP フラグメントオフセット: フラグメントオフセット<受信 IP データ長の合計 (ip_p=IPPROTO_TCP,ip_flag_off < total_flag_len)
3	WinNuke	TCP	脆弱性	宛先ポート番号:139,TCP フラグ:URG (ip_p=IPPROTO_TCP,th_dport=139,TH_URG=1)
4	HTTP GET	TCP	Flood 系	宛先ポート番号:80, ペイロード:GET (ip_p=IPPROTO_TCP,th_dport=80,data=GET)
5	Land	TCP	脆弱性	IP アドレス:宛先=送信元, ポート番号:宛先=送信元 (ip_p=IPPROTO_TCP,ip_src=ip_dst,th_sport=th_dport)
6	UDP Flood (帯域攻撃)	UDP	Flood 系	IP データ長:データ長> 1K バイト (ip_p=IPPROTO_UDP,ip_len > 128)
7	UDP Flood (機器攻撃)	UDP	Flood 系	IP データ長:データ長< 128 バイト (ip_p=IPPROTO_UDP,ip_len < 128)
8	IKE-DoS	UDP	脆弱性	宛先ポート番号:500 (ip_p=IPPROTO_UDP,th_dport=500)
9	Smurf	ICMP	Flood 系	ICMP タイプ:要求, 宛先 IP アドレス:ブロードキャスト (ip_p=IPPROTO_ICMP,icmp_type=ICMP_ECHO,ip_dst=BROADCAST)
10	Ping-of-Death	ICMP	脆弱性	IP オフセット× 8+IP データ長> 65535 (ip_p=IPPROTO_ICMP,ip_flag_off+ip_len > 65535)
11	ICMP Flood (帯域攻撃)	ICMP	Flood 系	ICMP タイプ:要求,IP データ長:データ長> 1K バイト (ip_p=IPPROTO_ICMP,icmp_type=ICMP_ECHO,ip_len > 1024)
12	ICMP Flood (機器攻撃)	ICMP	Flood 系	ICMP タイプ:要求,IP データ長:データ長> 128 バイト (ip_p=IPPROTO_ICMP,icmp_type=ICMP_ECHO,ip_len > 128)

時の次 TCT へのリンク情報)：4 バイトである．P は現時点におけるハイエンドエッジルータ[15] の最大パケット処理性能を適用し，30Mpkt/s とする．F は本提案方式特有の値で，推測が困難である．そこで具体的なデータのある，1 通信フロー当たりの平均パケット数で代用する．通信フローとは，送信元 IP アドレス，宛先 IP アドレス，プロトコルにより識別できる通信として定義され，F の値と比較すると送信元 IP アドレスの違いも識別する分小さい値となり，メモリの見積もりとしては厳しい方向の条件となる．通信フローとルータの中継パケット数の関係に着目すると，文献 16) より 1 通信フローあたり平均 15 中継パケットという観測結果が提示されているので，この結果を適用することとする．

以上の値を式 (1) に適用すると，ハイエンドエッジルータで必要となる TCT メモリサイズ Q は，56MB となる．この値は，上記ハイエンドエッジルータにメモリオプションとして追加できる 512MB に収まっており，十分許容できる範囲と考えられる．実際には，送信元 IP アドレスが異なっていても同一の TCT に登録されるため，メモリサイズは更に少なくて済む．

4. 閾値の最適化と運用方法

4.1 閾値の最適化

閾値は提案方式を実装するうえで重要なパラメータとなる．そこで閾値の目安を得るための基礎実験を行った．ターゲットとなる WEB サーバを構築し，DoS 攻撃ごとにサーバが使用不可となるトラヒック量を調査した．DoS 攻撃ツールとして，公開されているソースコード[17] を実験用に改造したものを用いた．ここでは，代表的な DoS 攻撃として SYN Flood，長パケットによる ICMP Flood，HTTP GET Flood を選定した．

実験で用いたネットワーク構成を**図 3** に示す．クライアントが WEB サーバに対して繰り返し所定のアクセス要求を行っている状態において，攻撃ホストから WEB サーバに DoS 攻撃を仕掛けた．**表 2** に実験機の構成を示す．WEB サーバソフトウェアには Apache 1.6.2 を利用し，OS の設定を含め全てデフォルトとした．

(1) **SYN Flood 攻撃**

SYN Flood 攻撃は TCP の 3 ウェイハンドシェイクを利用した攻撃であり，送信元 IP アドレスを偽造した大量の SYN パケットをターゲットに送信する．ター

表 2 実験器の構成
Table 2 Structure of experimental devices.

	攻撃ホスト	WEB サーバ	WEB クライアント
CPU	Intel Pentium 4 3.2GHz	Intel Celeron 2.66GHz	Mobile Intel Pentium 3 M 800MHz
メモリ	1.0GB	512MB	256MB
OS	WindowsXP Professional	Fedora Core 4	WindowsXP Professional

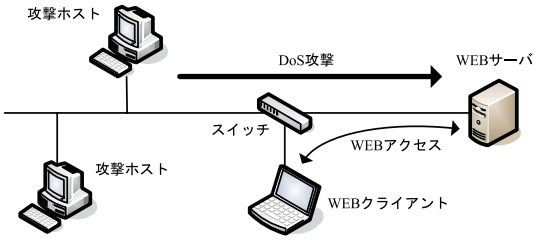


図 3 実験ネットワークの構成
Fig. 3 Structure of the experimental network.

ゲットは TCP コネクションにおけるハーフオープン状態となり，ACK 応答を受信するためにハーフオープン状態をバッファに記録する．ACK 応答が返ってこないまま攻撃者からの新たな SYN パケットを受信し続ける結果，バッファが埋め尽くされ，システム機能低下および通信不能状態になる．

攻撃ホストを 2 台使用し，WEB サーバに対して同時に攻撃を仕掛けた．攻撃パケットレートを徐々に増加させたときの WEB サーバの CPU 負荷と，アクセス応答時間，および WEB サーバ内簡易プログラム完了時間を測定した．使用した簡易プログラムは以下のとおりであり，正常時には約 100[msec] で終了する．

$$for\ (i = 0; i < 14000000; i++)\ \{\} \qquad (2)$$

図 4 に SYN Flood 攻撃におけるアクセス応答時間と WEB サーバの CPU 負荷を，**図 5** に SYN Flood 攻撃における CPU 負荷と簡易プログラム完了時間を示す．図 4 および図 5 から，SYN Flood の攻撃パケットレートが 6,500[PPS] を境に CPU 負荷が急激に増加し始め，これに伴ってアクセス応答時間および簡易プログラム完了時間が大きく増加していることが確認できる．アクセス応答時間においては，攻撃パケットレートが 7,000[PPS] を超えると，TCP コネクションがタイムアウトし，通信の開始すらできなくなる．この結果から，実験環境と同等なネットワーク構成であれば，SYN Flood 攻撃では 6,500[PPS] で WEB サーバが使用不可状態となる．

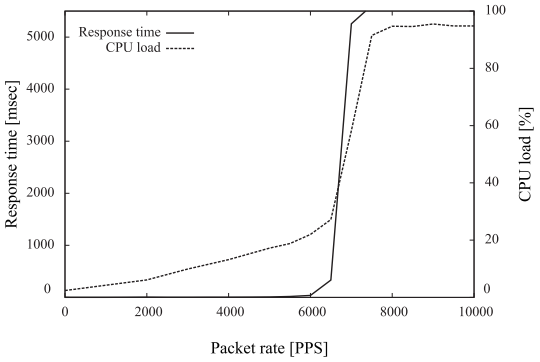


図 4 SYN Flood 攻撃におけるサーバのアクセス応答時間と CPU 負荷
Fig. 4 Response time from the server and CPU loads with SYN Flood attack.

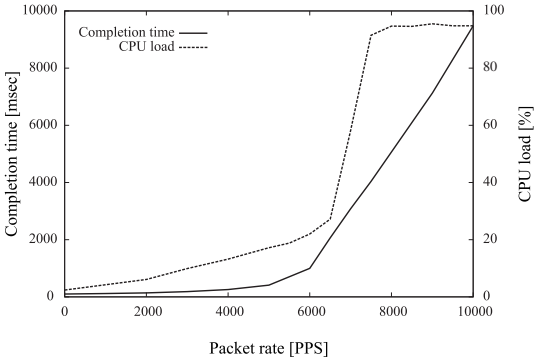


図 5 SYN Flood 攻撃におけるサーバのプログラム完了時間と CPU 負荷
Fig. 5 Program completion time and CPU loads in the server with SYN Flood attack.

(2) **長パケットによる ICMP Flood 攻撃**

長パケットによる ICMP Flood 攻撃は大量の ICMP 要求を送信し，ネットワークを機能不全にする攻撃である．ICMP 要求を受け取ったターゲットは偽造 IP アドレスに対して ICMP 応答を送信し，ネットワーク帯域が埋め尽くされる．

攻撃ホストを 2 台使用し，WEB サーバに対して同時に ICMP Flood 攻撃を仕掛けた．パケットサイズはイーサネットの最大長 1,500 バイトとした．**図 6** に ICMP Flood 攻撃におけるアクセス応答時間とパケットロス率を示す．攻撃パケットが，最大理論パケットレート値 8,127［PPS］を超えてからパケットロス率が急激に上昇している．パケットロス率の増加に伴い TCP コネクションのタイムアウトが発生するため，アクセス応答時間も増加している．これは，パケットロ

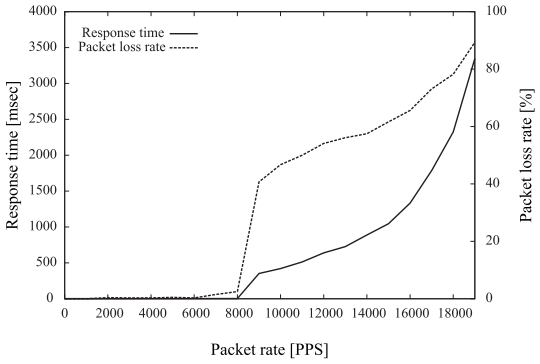


図 6 ICMP Flood 攻撃におけるアクセス応答時間とパケットロス率
Fig. 6 Response time and packet loss rates with ICMP Flood attack.

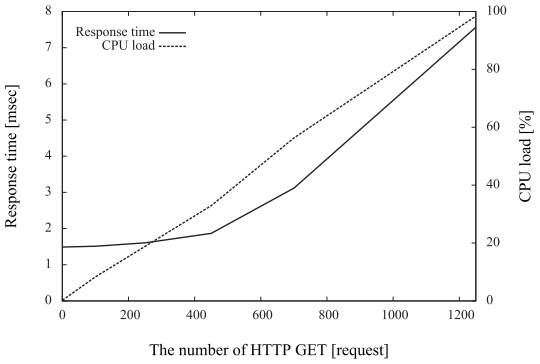


図 7 HTTP GET Flood 攻撃におけるサーバのアクセス応答時間と CPU 負荷
Fig. 7 Response time from the server and CPU loads with HTTP GET Flood attack.

スによる再送制御が発生するためである．攻撃のパケットレートが 20,000[PPS] を超えると，WEB サーバとの通信は不能状態となった．このときのサーバの CPU 負荷は，いずれのパケットレートにおいても 1% 前後の値であり, 本攻撃に対しては CPU リソースには余裕があることがわかる．この結果から，実験環境と同等なネットワーク構成であれば，長パケットによる ICMP Flood 攻撃では 8,100[PPS] でネットワークが使用不可となる．

(3) HTTP GET Flood 攻撃

HTTP GET Flood 攻撃は WEB サーバをターゲットにした攻撃であり， WEB ブラウザでターゲットとなる WEB ページを表示させ，更新を何度も行う．多数の攻撃者から一斉に HTTP 要求を行うことにより，サーバに大きな処理負荷を与える．

攻撃ホストを 10 台使用し，WEB サーバに対して同時に HTTP GET Flood 攻撃を仕掛けた．**図 7** に HTTP GET Flood 攻撃における CPU 負荷とアクセス応答時間，**図 8** に HTTP GET Flood 攻撃における CPU 負荷とプログラム完了時間を示す．CPU 負荷はリクエスト数に比例した形で増加した．プログラム完了時間は 1,000[PPS] 程度から急激に上昇し始め，1,250[PPS] では正常時より 30 倍の時間を要した．アクセス応答時間は最大でも 10[msec] 以下であった．この結果から，実験環境と同等なネットワーク構成であれば，HTTP GET Flood 攻撃では 1,000[PPS] 程度で WEB サーバの処理負荷が非常に重くなる．

以上の実験結果を**表 3** にまとめる．DoS 攻撃の種類により，攻撃に必要となるパケット数が大きく異なることがわかる．実際にはこれらのデータを参考にして，システムごとに閾値を決定する必要がある．また，脆弱性を狙った攻撃は，OS のバージョンによっては 1

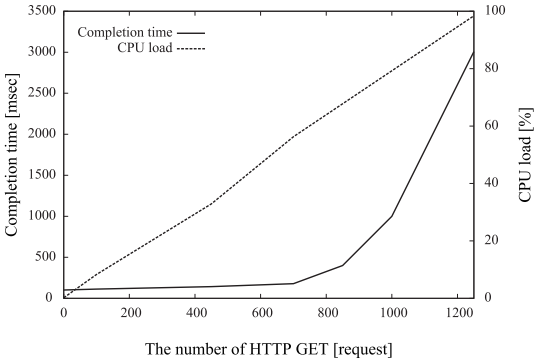


図 8 HTTP GET Flood 攻撃におけるサーバのプログラム完了時間と CPU 負荷
Fig. 8 Program completion time and CPU loads in the server with HTTP GET Flood attack.

表 3 実験から得られた処理限界値
Table 3 Processing limits of packets.

DoS 攻撃名	処理限界値 [PPS]	攻撃対象
SYN Flood	6500	CPU
ICMP Flood (長パケット)	8100	ネットワーク
HTTP GET Attack	1000	CPU

つのパケットを送りつけるだけでターゲットのシステムを停止させる．このような攻撃に対しての閾値を 1 と定義しておけば，パケットが 1 回通過しただけで TBT に転記されるため，攻撃経路を知ることが可能である．

4.2 運 用 方 法

閾値の設定は DoS 攻撃に対して行う．閾値は管理装置からの指示により変更することができる．DoS 攻撃が仕掛けられている間に，閾値の設定を管理装置からダイナミックに変えながら上流に追跡していくことが可能である．閾値をオーバすると TBT に転記され

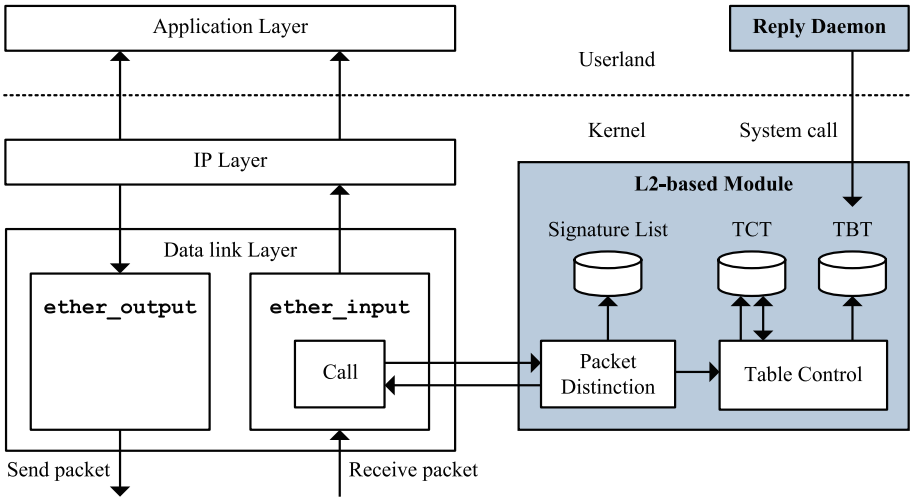


図 9 ルータのモジュール構成
Fig. 9 Module structure of a router.

るが，これは DoS 攻撃の可能性を示唆するものであり，余分に転記されたとしても問題にはならない．

L2-based トレースバックの運用方式は，例えば以下のような方法が考えられる．4 章で述べた調査結果からもわかるように，DoS 攻撃の内容によって閾値が大きく異なる．この値を参考にして，シグネチャごとの閾値を暫定的に決定する．例えば，SYN Flood 攻撃であれば，閾値を 6,500 回/秒と設定する．これだけの負荷がかかったとしても，ハイエンドサーバでは動作が可能であるかもしれないが，TBT への転記は発生する．しかし，TBT は追跡時に使用するものであるため，転記されていても特に問題にはならない．逆にローエンドサーバでは，上記閾値以下の攻撃でもダウンする可能性がある．この場合は，ユーザからの連絡により追跡を開始することになる．この時点で TBT に追跡情報が存在しない場合は，対応する DoS 攻撃に対するシグネチャの閾値を下げるよう，管理装置から指示し，TBT に情報が転記されるのを待つ．転記にかかる時間は TCT 更新時間（約 1 秒）でよいため，多くの時間を要することはない．このようにして運用を継続しながら上流にリンクをたどることにより，攻撃者が存在するネットワークを特定することができる．このような方法では DoS 攻撃が継続している間でないと追跡ができないが，既存のログ方式であってもログ情報が新しい内容に上書きされる前に追跡を終える必要があることを考えると，特に大きな欠点とは言えないと考えられる．

5. 実　　装

5.1 モジュール構成

レイヤ 2 が LAN の場合を想定し，L2-based IP トレースバックを実装して評価を行った．**図 9** にルータのモジュール構成を示す．OS には FreeBSD 5.3-Release を選択した．データリンク層の入力関数である `ether_input()` から L2-based モジュールを呼び出し，入力パケットの内容を参照して TCT，TBT を更新する．既存の通信処理には一切影響を与えない．

パケットを受信すると，L2-based モジュールが呼び出される．IP ヘッダのプロトコルタイプの値から対応するシグネチャグループを判別し，次にポート番号や TCP フラグといったフィールドを参照する．もし該当する DoS 攻撃のシグネチャと一致すれば，TCT の対応するカウント値の増加を行う．カウント値の増加後にシグネチャの閾値を超えていた場合は，その情報を TBT へ転記する．

管理ホストと通信を行う応答デーモンはアプリケーション層で動作させた．応答デーモンは，管理ホストからの問合せがあった場合，L2-based モジュールで生成した TBT をシステムコールで呼び出し，要求された宛先 IP アドレスと上位ルータの IP アドレスを抽出する．その後， Socket を利用して管理ホストへ返答する．なお，管理ホストの機能は全てアプリケーション層にて実装した．

L2-based トレースバックでは，通常のパケット受信処理に加え，概略以下のような処理を実行する．

(1) 受信パケットの宛先 IP アドレスと対応するシ

表 4 測定環境
Table 4 Measurement environment.

	ルータ	サーバ	クライアント
CPU	Intel Pentium 4 2.4GHz	Intel Pentium 4 3.2GHz	Intel Pentium 4 3.2GHz
メモリ	512MB	1.0GB	1.0GB
OS	FreeBSD 5.3-Release	WindowsXP Professional	WindowsXP Professional

グネチャのハッシュ値を生成する．

(2) ハッシュ値よりハッシュテーブルを参照し，該当 TCT のアドレスを求める．

(3) 該当 TCT の内容からハッシュ値が衝突していないことを確認する．

(4) TCT が生成された時刻から 1 秒間以上経過しているものは中継カウンタをクリアする．

(5) 1秒経過していないものはカウンタ値をアップし，設定された閾値と比較する．閾値に達していたら TBT へ内容を転記する．

(6) ハッシュテーブルが衝突していた場合，TCT 内の次チェイン情報からチェインをたどる．

(7) チェインをたどる過程で 1 秒間以上経過している TCT は削除し，チェインを張り直す．

(6)(7) の処理はハッシュ値が衝突したときのみ発生する処理である．TCT のエントリ数が増してもハッシュの衝突確率を低く抑えられれば，処理時間が増加することはない．これには，TCT のエントリ数に応じてハッシュテーブルのサイズを大きくすることで対応できる．

5.2 追跡の手順

図 10 にシステム構成と追跡動作を示す．攻撃ホストと被害ホストはプロバイダの外部ネットワークに存在し，プロバイダが提供するルータには本提案方式の機能が搭載されている．点線内がプロバイダに相当し，プロバイダ内には管理ホストが存在する．被害ホストは特殊な機能を持たない一般端末である．

被害ホストが DoS 攻撃を受けたことを知ると，被害者側のユーザはプロバイダに対して，電話等により攻撃ホスト特定の依頼を行う．追跡時においては，管理ホストがルータに対して順次問合せを行い，攻撃経路を構築していく．

問合せを受けたルータは被害ホストの IP アドレスをキーに，TBT から上位ルータの IP アドレスをすべて割り出して，管理ホストに返答する．管理ホストは返答結果から，次の上位ルータに問合せを行う．これらの操作を繰り返し，攻撃経路を構築する．

5.3 動作確認

SYN flood，HTTP GET Flood，WinNuke，UDP Flood，IKE DoS，ICMP Flood に対して動作確認を行ったところ，シグネチャリストの閾値に従って TBT が生成されることを確認した．また，管理ホストから各ルータの TBT を参照することにより，攻撃経路を正しく割り出すことを確認した．

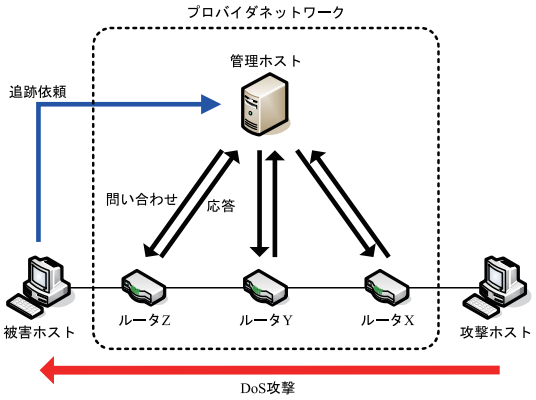


図 10 システムの構成と追跡動作
Fig. 10 System configuration and trace back operation.

表 5 FTP スループット測定結果
Table 5 Measurement results of FTP throughput.

	スループット値 [Mbps]
実装なし	72.22
実装あり	72.12
減少比 [%]	0.06

6. 評価

6.1 中継性能の測定

提案方式がルータの処理に与える影響がどの程度であるか評価するため，パケットの中継性能の測定を行った．測定にあたっては，シグネチャリストとして表 1 に示す 12 種類のシグネチャをそのまま準備した．

FTP スループット測定では，FTP サーバと FTP クライアントの間にルータを 1 段挟み，ルータに L2-based モジュールを実装した場合と，そうでない場合を比較した．実験器の構成は**表 4** のとおりであり，LAN は 100BASE-TX で接続した．データは 200MB のバイナリデータとした．**表 5** に 50 回測定を行ったときのスループット測定結果を示す．L2-based モジュー

表 6 パケット処理能力の測定結果
Table 6 Measurement results of packet processing performance.

データサイズ [byte]	18	512	1024	1472
実装なし [PPS]	75,755	21,624	11,466	8,126
実装あり [PPS]	75,109	21,623	11,463	8,120
減少比 [%]	0.853	0.051	0.026	0.074

ルを実装した場合と実装していない場合はスループットの違いが 0.06 % であり，ほとんど影響がないことがわかった．

次に netperf を使用して，クライアントからサーバに対して UDP による一方向転送を行い，ルータ処理能力の測定を行った．UDP のデータサイズを変化させ，それぞれ 20 秒間の測定を 10 回行った．**表 6** に測定結果を示す．L2-based モジュールを実装した場合のパケット処理能力の低下は，実装していない場合に比べ，どのデータサイズにおいても 1 % 以下であり，ほとんど劣化のないことがわかる．L2-based モジュールがパケットごとに行う処理は，プロトコルタイプやポート番号の値がシグネチャと一致するかどうかをチェックし，カウンタ値を更新するだけである．また，シグネチャはプロトコルタイプごとにグループ分けされており，余分な処理が発生しないようにしている．このため，ほとんど性能が劣化しないという結果が得られた．測定ではシグネチャを 12 種類としたが，今後この数が増えても大きな劣化はないと考えられる．

表 6 に示す試作機の実測値より，ルータ処理のパケット転送にかかるソフトウエア処理時間を逆算することができる．試作機ではハッシュ衝突時の処理は含まれていないが，衝突の確率が低いことを考えると，性能に与える影響はほとんどない．長パケットの場合は，中継性能はパケット伝送時間で決まるため，パケット処理時間が増加しても中継性能はほとんど変化しない．しかし，短パケットの場合，中継性能ネックはソフトウエア処理となる．表 6 に示す減少比がデータサイズ 18 のときだけ大きくなっているのはこのためである．このときのパケット処理時間を表 6 の中継性能から逆算すると，提案方式を実装しなかった場合は 13.200[μsec]（受信してから送信するまでの処理，及び送信完了処理を含む），提案方式を実装した場合は 13.314[μsec] となる．両者の差となる 0.114[μsec] が上記提案方式の追加処理にかかった時間となる．このように，パケット中継処理全体に対する L2-based トレースバックのソフトウエア処理による劣化率は 0.853% と極めて小さいことがわかる．ハッシュ方式では TCT エントリ数が増加しても処理内容は同じであり，処理時間の劣化率はどのようなルータであっても同等であるといえる．従って，本提案方式は CPU 負荷量についてはほとんど問題になることはないと考えられる．

6.2 追跡時間の測定

管理ホストとルータ間における問合せ，および応答の時間を測定した．事前に攻撃ホストは SYN Flood 攻撃をターゲットに仕掛けており，それぞれのルータが保持する TBT テーブルには，被害ホストの IP アドレスと，上位ルータの IP アドレスが記録されているものとした．管理ホストが問合せを行ってから，ルータからの応答が返るまでの時間を測定した．試行回数を 50 回としたときの平均値は 1.2[msec] となった．ルータ台数を n とすると，追跡にかかる時間は約 $1.2 \times n$[msec] となる．この結果から，いくつかのルータをまたがった追跡でも，十分短い時間で攻撃経路を構築できることがわかる．

6.3 既存技術との比較

表 7 に既存技術と提案方式の比較を示す．リンクテスト方式は手動での操作が必要となるため，比較表から省略した．ICMP 方式とマーキング方式は，大量の攻撃パケットを使用する Flood 系の攻撃にのみ有効な方式であり，攻撃パケットが少ない場合には適用できない．また，マーキング方式は解析に膨大な計算を必要とする．ログ方式は様々な攻撃方法への対処が可能であるが，ルータの処理負荷が大きく，ログを格納するメモリ消費が大きい．また，時間が経過するとログが消えてしまう可能性があるため DoS 攻撃終了後の解析ができない場合がある．提案方式は，ルータの処理負荷が軽く，様々な DoS 攻撃にも対応でき，既存技術の課題をバランスよく解決していると言える．

ログ方式と提案方式は，リンクを上流にたどる方式であるため，全ルータに機能を実装する必要がある．ログ方式は単パケットであってもその攻撃経路を追跡できるというメリットがある．L2-based トレースバックでは，特定の DoS 攻撃に対する閾値を 1 と置くことにより，ログ方式と同様に単パケットの追跡が可能である．ルータの処理性能をログ方式ほど犠牲にしないという点で，本提案方式は大きな利点を持っている．

TBT に実際のトラヒック量がわかる情報（閾値に達するまでの時間など）を一緒に保存しておけば，追跡の手がかりが増える．たとえば，上流と下流で TBT に記憶されているトラヒック量が一致しない場合は，分散型 Dos 攻撃（DDoS 攻撃）により複数の上流から攻撃を受けている可能性がある．この場合はさらに

表 7 既存技術と提案方式との比較
Table 7 Comparison of existing methods and the proposed method.

	ルータの処理負荷	攻撃終了後の追跡	様々な DoS 攻撃の識別	解析時間
ICMP 方式	○ (低い)	○ (可)	× (Flood 系のみ)	○ (短い)
マーキング方式	○ (低い)	○ (可)	× (Flood 系のみ)	× (長い)
ログ方式	× (高い)	△ (困難な場合あり)	○ (可)	○ (短い)
提案方式	○ (低い)	○ (可)	○ (可)	○ (短い)

閾値を下げることにより，さらに上流のルータを特定することが可能である．

L2-based トレースバックには検討を要する点がいくつか残されている．たとえば，帯域攻撃の場合には，攻撃パケットの宛先 IP アドレスが同一サブネット内の複数のアドレスに渡る場合も考えられる．このような攻撃には，現在のままの実装では対応できない．このような攻撃にも対応するには，TCT の作成時に，宛先ネットワークアドレスごとに記録するような機能が必要になる．この機能は個別ユーザからの要求があって，その場所のネットワークアドレスが具体的にわかる必要がある．また TBT に転記する際に，上記トラヒック量がわかる情報の他にも，どのような情報を格納するのが有効であるかも検討が必要と思われる．これらの情報は TBT を定期的に参照することによって，DoS 攻撃の兆候を監視できる可能性がある．

7. ま と め

本研究ではパケットのレイヤ 2 の情報を利用することにより，上位ルータを特定し，攻撃経路を構築する L2-based IP トレースバックを提案した．ルータは中継パケットをシグネチャリストと比較して，中継回数を計測するだけなので，ルータにかかる負荷は小さい．閾値を DoS 攻撃ごとに定義できるため Flood 系の攻撃だけでなく，様々な攻撃に対しても対応可能である．

L2-based 方式を実装し，動作検証と性能測定を実施した．その結果，ルータの性能劣化はほとんどないことを示した．

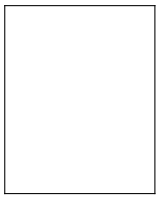
今後は，プロバイダ間の連携や DDoS 攻撃への対応方法について検討を行う必要がある．

参 考 文 献

1) 門森雄基，大江将史：IP トレースバック技術，情報処理学会論文誌，Vol.12, No.42, pp.1175–1180 (2001).
2) 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，電子情報通信学会論文誌 B，Vol.J85-B, No.8, pp.1313–1322 (2002).
3) Stone, R.: CenterTrack: An IP overlay network for tracking DoS floods, *Proceedings of 9th USENIX Security Symposium* (2000).
4) Burch, H. and Cheswick, B.: Tracing Anonymous Packets to Their Approximate Source, *Proceedings of the 14th USENIX conference on System administration*, pp.313–322 (2000).
5) Bellovin, S., Leech, M. and Taylor, T.: ICMP Traceback Messages, *IETF Internet-Draft* (2003).
6) Savage, S., Wetherall, D., Karlin, A. and Anderson, T.: Practical network support for IP traceback, Proceedings of ACM SIGCOMM ' 00，pp.295–306 (2000).
7) Song, D. X. and Perrig, A.: Advanced and authenticated marking schemes for IP traceback, *Proceedings of IEEESPINFOCOM 2001* (2001).
8) Nishio, N., Harashima, N. and Tokuda, H.: Reflective Probabilistic Packet Marking Scheme for IP Traceback, *IPSJ Journal*, Vol.44, No.8, pp.1848–1860 (2003).
9) Belenky, A. and Ansari, N.: IP Traceback With Deterministic Packet Marking, *IEEESP-Communications Letters*, Vol.7, No.4, pp.162–164 (2003-04).
10) Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C.E., Tchakountio, F., Kent, S.T. and Strayer, W.T.: HashBased IP Traceback, *Proceedings of ACM SIGCOMM 2001* (2001).
11) Snoeren, A.C., Partridge, C., Sanchez, L.A., Jones, C. E., Tchakountio, F., Schwartz, B., Kent, S.T. and Strayer, W.T.: Single-Packet IP Traceback, *ACM/IEEE Transactions on Networking*, Vol.10, No.6 (2002).
12) Hazeyama, H., Oe, M. and Kadobayashi, Y.: A Layer-2 Extension to Hash-Based IP Traceback, *IEICE TRANSACTIONS on Information and Systems*, Vol.E86-D, No.11, pp.2325–2333 (2003).
13) Matsuda, S., Baba, T., Hayakawa, A. and Nakamura, T.: Design and Implementation of Unauthorized Access Tracing System, *Proceedings of the 2002 Symposium on Applications and the Internet*, pp.74–81 (2002).
14) Snort: http://www.snort.org/.
15) Cisco: Cisco 7600 シリーズルータ (2007).

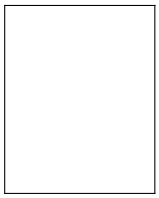
http://www.cisco.com/jp/product/hs/routers/c7600/index.shtml.
16) Cisco: NetFlow Services Solutions Guide (2007).
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/netflsol/nfwhite.pdf.
17) PacketStorm:
http://packetstormsecurity.org/.

(平成 19 年 8 月 3 日受付)
(平成 20 年 3 月 5 日採録)



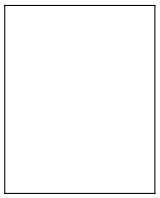
鈴木　秀和（学生会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．現在，同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程に在学中．2008 年日本学術振興会特別研究員．ネットワークセキュリティ，モバイルネットワーク等の研究に従事．修士（工学）．2006 年 IEEE 名古屋支部学生奨励賞受賞．2006 年 DICOMO2006 松下温賞受賞．2007 年 DICOMO2007 ヤングリサーチャー賞受賞．電子情報通信学会所属．



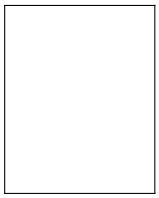
播磨　宏和（学生会員）

2005 年名城大学理工学部情報科学科卒業．2007 年同大学大学院理工学研究科情報科学専攻修了．同年アイホン株式会社入社。ソフトウェア開発部に所属．修士（工学）．



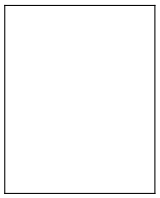
岡崎　直宣（正会員）

1986 年東北大学工学部通信工学科卒．1991 年東北大学大学院工学研究科電気及び通信工学専攻博士後期課程了．同年，三菱電機（株）入社．2002 年宮崎大学工学部助教授．2007 年同準教授．通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事．博士（工学）．電子情報通信学会，電気学会，IEEE 各会員．



伊藤　将志（学生会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．現在，同大学院理工学研究科電気電子・情報・材料工学専攻博士後期過程に在学中．VoIP，無線ネットワーク等の研究に従事．修士（工学）．2007 年 DICOMO ヤングリサーチャー賞受賞．電子情報通信学会所属．



渡邊　　晃（正会員）

1974 年慶応義塾大学工学部電気工科学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年名城大学理工学部教授，現在に至る．博士（工学）．電子情報通信学会，IEEE 各会員．