MACアドレスを用いたIPトレースバック技術の提案

播磨　宏和

近年，インターネットの普及に伴いセキュリティに関する問題が多発している．その中でも外部からの攻撃であるサービス不能攻撃（DoS 攻撃）は，大量のパケットをターゲットに送信することでシステムを機能不全にしてしまう．一般的に，これらの攻撃の送信元IPアドレスは偽造されており，本当の発信源の特定は困難とされている．この攻撃に対して発信源の身元を特定する手法として IP トレースバック技術が存在する．しかしながら，既存技術の中でもいくつかの問題点が指摘されている．本論文では既存の技術とは別に，ルータに記録されたMACアドレスから上流のノードを特定し，攻撃の発信源までを追跡する手法を提案する．

The proposal of IP Traceback technology using MAC Address

Hirokazu Harima

Recently, the security happens are often causing by Internet spreads. It makes system crash by transmitting a too much packet to the target especially for Denial of Service attack that is attack from the outside. In general, these attacks that source IP address is impersonated and determines the true source of attacking packets to be difficult. The IP trace backing technology exists as a technique for determining the sending source for this attack. However, several problems are pointed out with existing technology. This paper proposes the technique that tracing sending source for this attack besides an existing technology. The upstream node is specified from the MAC address recorded in the router.

1. はじめに

近年、インターネットが普及し、安価で高速な常時接続環境の普及が進むにつれ、サービスを提供するために企業や個人でも手軽にサーバを構築するようになってきた. それに伴いインターネットセキュリティへの攻撃数は増加し、ウイルスの感染や外部からの不正侵入等の脅威が多発している. 中でもサービスに対する脅威が懸念され、サービス不能攻撃（DoS 攻撃）とよばれる攻撃が問題となっている．DoS 攻撃とは目標のサーバに対して大量のデータを送信することで、サーバの資源を使い尽くしてサービスを妨害してしまう. またネットワークのトラフィ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る攻撃である. DoS 攻撃を阻止する有効な手段としてはいまだに確立されてないのが現状であり、これらを防ぐ実践的な方法としては Firewall 及びフィルタリングなどのセキュリティ製品の導入が挙げられている. イントラネットに対するアクセスを制限し、セキュリティ侵害の発生する可能性を低くする対策方法である．しかしながら、これらの予防策は一般的に広く知られており、今や常識として対策を施している. これらのようなセキュリティ対策を導入しても DoS 攻撃を仕掛けるハッカーが後を絶たない．なぜなら DoS 攻撃自体の実装は容易であり、インターネットでこれらのツールが大量に出回っているため、スキルの低いハッカーでも使用することができてしまうからである．また、DoS 攻撃で送信されるパケットの送信元アドレスは偽造されていることがほとんどであり、攻撃者の特定は非常に困難とされている. つまり従来の Firewall やフィルタリングといった特定のアドレスをはじく対策をとってもあまり有効とは考えられない．したがって、このような状況においても正確な発信源を特定する技術が必要となってくる.

送信元アドレスが偽造されている DoS 攻撃の発信源を特定する手法としては IP トレースバックと呼ばれる技術が存在し、攻撃パケットが通過した経路を発信元までさかのぼる行為のことをいう．近年，IP トレースバック技術は盛んに研究がなされており, さまざまな方式が提案されている. ルータのデバッグ機能である Input debugging を利用する方式（リンク検査方式）[1]や逆探知パケットを使用する方

式（ICMP トレースバック方式）[2]，ある確立でパケットにマークをつける方式（マーキング方式）[3][4]、パケットのダイジェストを利用する方式（Hash-Based 方式）[5]などが存在する．しかしこれらの方式はどれも改善の余地が多く残されると考えられている．

そこで、本論文では新たな IP トレースバック技術として、ルータに残されたパケットの MAC アドレス情報を記録することで上位のノードを特定する手法について提案する．

まず、2 章では既存の IP トレース技術を取り上げ、攻撃経路を特定する上での問題点を述べる．3 章で MAC アドレスを用いた IP トレースバック技術について紹介する．4 章においては提案方式を実装させるために機能の設計を行い、実現方法を述べる．そして、5 章では既存技術との比較を行う．最後に、6 章において本研究のまとめ、今後の課題について述べる．

2. 既存技術とその課題

現在，一般的に知られている IP トレースバック技術を紹介し，その課題について述べる．

2.1.IP トレースバック技術

はじめに，パケットがどのような振る舞いをして，どのような経路を通過したかということを順にたどっていく行為をトレーシングと表現する．特にトレーシングの中でも攻撃の発信元までさかのぼるシステムを自動化したものをトレースバックシステムと呼び，それらの技術を IP トレースバックという．IP トレースバック技術とは、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手法の総称である．ルータに機能を追加することにより，パケットが通過した手がかりを調べることによって発信源の特定が可能となる．図 1 に IP トレースバック技術の概要を示す．IP トレースバック技術は、近年，アドレス詐称問題に対して盛んに研究がなされており、さまざまな方式が提案されている． IP トレースバックは以下のように分類できる．

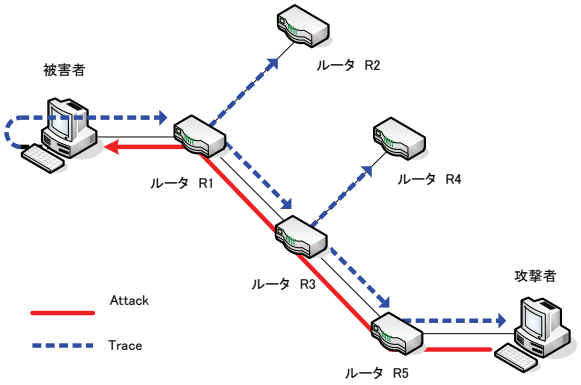

図 1．IP トレースバック技術の概要

2.1.1 リンク検査方式

リンク検査手法は古くから用いられている方式であり，手動で発信源までの経路を追跡する．被害者の最寄のルータから DoS 攻撃の上流となるリンクを特定し，隣接ルータへと順になどって行くことで攻撃経路を特定していく手法である．そのための手法として input debugging が知られており，ルータのデバッグ機能を利用したものである．DoS 攻撃を受けた被害者は攻撃トラフィックを分析し，特徴を抽出する．抽出する特徴としては，プロトコルの種別やポート番号などが挙げられる．次に被害者からの以来を受けたネットワーク管理者が，ルータの出力ポートにおいて DoS パケットを判別するフィルタを設定することで，DoS パケットの入力ポートを知ることができる．入力ポートを特定することで接続されている隣接ルータを割り出し，そのルータに同様の操作を行うことで発信源まで特定することができる．たとえば Cisco 社のルータでは，アクセスリストといった DoS を識別する設定を行い攻撃トラフィックの特徴を抽出し，次に log-input を適応させることで通過しているインターフェースを識別することができる[6]．しかしながら，リンク検査方式では攻撃が行われている間でしか追跡が行えないことや，ルータの管理者に大きな負担をかけてしまうという管理コストの問題がある．また，攻撃ツールの発達によって攻撃パケットからの特徴抽出が困難になっている．

2.1.2 ICMP トレースバック方式

ルータを通過するパケットに何らかの方法で逆探知のための情報を付与できれば，被害者の近傍でそれらを収拾し発信源を特定することができる．この方法として，ICMP に新たなメッセージ種別 Traceback を定義し，被害者

まで届ける手法が提案されている. ICMP トレースバック方式では, すべてのルータは通過するパケットに ICMP Traceback メッセージを 2 万分の 1 という低い確率で生成することで通信料のオーバーヘッドを抑えている. 被害者は DoS 攻撃を受けると，それらと平行して受け取った ICMP Traceback メッセージから，攻撃トラフィックが通過した情報を得る. 追跡のための情報としては, ICMP Traceback メッセージ内に各リンクの IP アドレスやインターフェース名, 公開鍵などを収める手法が提案されている. この方式の利点はルータに付加する機能が軽く, 手がかりとなる情報を多く伝えることができる．しかし逆探知に ICMP を用いるので，攻撃経路に ICMP を拒否しているルータや，Firewall が存在していると正常に動作しない．また，DoS 攻撃のパケット数が少ない場合，ルータは ICMP Traceback メッセージを生成しないので攻撃の発信源を特定できない可能性がある.

2.1.3 マーキング方式

マーキング方式は逆探知のための情報を特定のエリアに追跡のための情報を分割して挿入し, 攻撃対象へと送り届ける方式である．マーキングされたパケット（マーキングパケット）を受け取った攻撃対象は, 分割されたマーキングパケットを元通りに復元し, 攻撃経路を再構築する．Savage らの論文[3]では，マーキング方式に関する最初の論文である. 隣接する 2 つのルータの IP アドレスの組（R s，Re）によって各リンクを表現し, これを細分化して IP identification フィールドに埋め込むとで逆探知を提案している. マーキング方式は流れているパケットそのものに追跡のための情報を付与する方法であり，ICMP トレースバック方式とは異なり追加のパケットを必要としないことから, ネットワークのオーバーヘッドは生まれないのでネットワークに負荷をかけずに追跡を実行できる利点がある. しかしながら, 複数の攻撃経路を再構築する際には必要な数のパケットを収集するために一定の時間が必要で, 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課題がある. 経路情報を IP identification フィールドに書き込むため，IPsec などの比較的新しいアプリケーションとの親和性が低い. また, ICMP トレースバック方式と同様に, ルータがある確率でパケットにマーキングを行うので, 攻撃者からのパケットが少ない場合は攻撃経路を構築できない可能性がある.

2.1.4 Hash-Base トレースバック方式

パケットの記録を効率よく保持することができれば，IP ヘッダを流用あるいは拡張することがなく逆探知が可能となるという考え方である．しかし, パケットそのものを記録しているのでは記録容量の問題が起きてくる. そこで Snoeren らの論文によるとパケットを記録する代わりに, パケットの先頭部分から計算した複数のハッシュ値を記録する方式を提案している[5].

IP ヘッダの中で，経路中で不変な部分とペイロードの先頭 8 バイトについて, k 個の独立なハッシュ関数を適用した結果を 2n ビットのビットマップとして保存する. ビットマップは一定の時間間隔でゼロクリアされ, その更新時に使用された k 個のハッシュ値と時間をダイジェストテーブルに保管する.

あるパケットが通過したかどうかは, パケットの先頭部分を用いて k 個のハッシュ関数を計算することで検査することができる. 計算結果と 2n ビットのビットマップを比較し，すべてのビットが 1 であれば高い確率でパケットが通過したといえる.

大きな記憶容量や高いハッシュ処理能力などが要求されるため, 高の方式よりもコスト面で不利になる可能性があるが，この方式には, 攻撃パケットが 1 個さえあれば, 発信源を特定できるという利点がある.

3. MAC アドレスを用いた IP トレースバック

本章では 2 章で述べた方式とは異なる手法の一つである MAC アドレスを用いた IP トレースバック技術について提案する. 以下 3.1 では MAC に基づいたトレースについての基本原理を述べ，3.2 では提案方式の動作を具体的に示す.

3.1 基本原理

2 章で紹介した既存技術は IP レイヤの機能を用いた IP トレースバックであり，MAC レイヤに着目した技術はほとんど存在しない.

攻撃者の発見において MAC アドレスを用いる理由としては，送信元 IP アドレスを詐称する攻撃を受けても攻撃経路を構築することが可能であると考えられる．一般的な DoS 攻撃は送信元 IP アドレスを詐称することが多く, また, 仮に攻撃パケットの送信元 MAC アドレ

スが詐称されていたとしても，ルータ間とのパケット転送では正常なアドレスが用いられているので，攻撃者の隣接ルータまで追跡が可能と考えられる（図 2）．

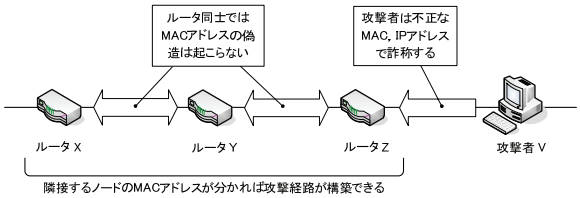

図 2. ノード間における MAC アドレスの詐称

3.2 提案技術の概要

3.3.1. 動作概要

提案方式は既存のトレースバック技術とは異なる一方式であり，ルータに残された攻撃パケットの送信元 MAC アドレスを手がかりとして攻撃側のエッジルータまでを追跡する．エッジルータとは攻撃ホストに最も近いルータのことであり，このルータに DoS パケットが流入していることが分かれば，同じサブネット内に存在するホストに攻撃者が含まれていると考えられる．

図 3 が示しているように，DoS 攻撃では一般ホストが送信するパケットと比べ，大量の攻撃パケットが被害ホストへと送信されることから，ルータは特定の上位ルータから同じ宛先 IP アドレスのパケットを大量に受信することになる．ことのき，上流ルータから受信した攻撃パケットの送信元 MAC アドレスと宛先 IP アドレスの組をルータに記録しておくことで，攻撃対象ホストに対する攻撃の経路を推測する手がかりを得る．以降，パケットの送信元 MAC アドレスと宛先 IP アドレスを組アドレスと呼ぶ．

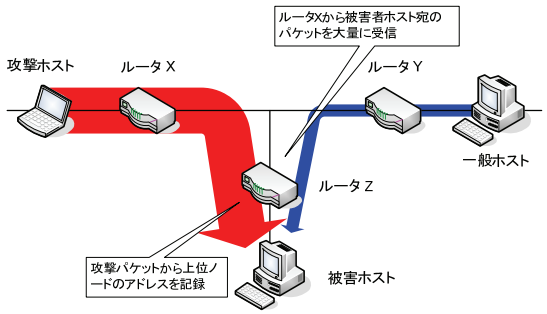

図 3. パケット数とアドレス記録の関係

図 4 のようなネットワークにおいて，攻撃ホストが被害ホストに攻撃を仕掛けるとする．このとき攻撃パケットの内容を見てみると送信元 IP アドレスは偽造されており，パケットがルータを経由するごとに MAC アドレスの内容が入れ替わっていく様子が分かる．このとき，各ルータはパケット転送時に組アドレスを記録していくことで攻撃対象ホストに対する攻撃の経路を推測する手がかりを得る．

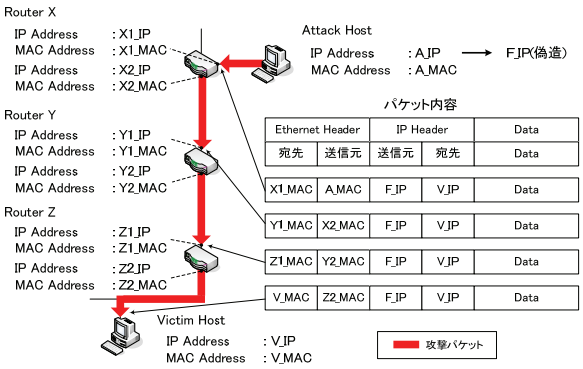

図 4. 提案方式の概要

提案方式では追跡情報を記録するためテーブル 1，テーブル 2 の 2 種類のテーブルを保持する．ルータはパケット転送時にパケットの宛先 IP アドレスとその転送回数をテーブル 1 に記録し，記録の内容は短い一定間隔で消去する．DoS 攻撃のような大量なパケットを転送すると，通常のパケットと比べ閾値は極端に増大していく．転送回数のカウント値にはある閾値を設けておき，カウント値が一定時間内に閾値を超えた場合，その宛先を攻撃対象とした DoS 攻撃が行われている可能性があると判断し，この時のパケットの組アドレスをテーブル 2 へと記録する．つまりテーブル 2 には攻撃パケットが通過した上位のルータの MAC アドレスが記録されることになる．テーブル 2 は攻撃の可能性があった場合のみ生成されるものであり，攻撃経路の判断材料となるため長期的に保持する（図 5）．

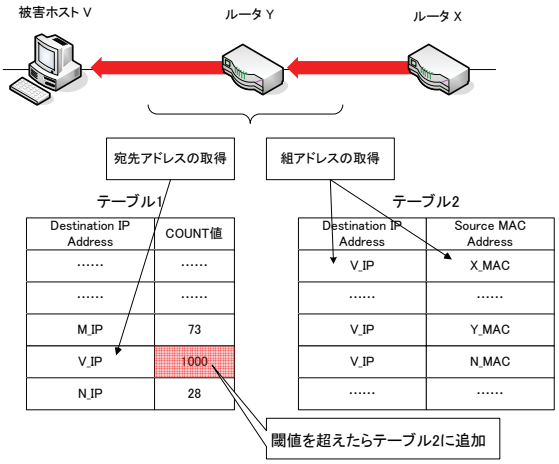

図 5. 組アドレスの保存

発信源を特定するためのトレースバック概要を図 6 に示す. 追跡時においては各ルータがテーブル 2 に記録されている MAC アドレスを参照することで, 攻撃パケットが通過した上位ノードを特定する. まず, 被害ホストは攻撃を受けた時点で受信した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, 逆探知のための問合せパケットを送信する. 問合せパケットには被害ホストの IP アドレスが含まれており, 受信した上流ルータは自身のテーブル 2 を参照して被害ホストの IP アドレスを基に組アドレスの送信元 MAC アドレスすべてを割り出す. 次にルータは自分自身の IP アドレス情報を問合せパケットに格納していくことで、攻撃の経路を構成する. 割り出した MAC アドレスを持つ更に上流のルータに対して問合せパケットを送信する. これらの操作を同様に行うことで攻撃ホストのエッジルータまでさかのぼることができる.

しかし, 問い合わせパケットを受信したルータが上位ノードの特定ができない場合が存在する. それはルータが保持しているテーブル 2 に被害ホストの IP アドレスを含む組アドレスが存在しない場合, すなわちカウントの増加が閾値に達しておらず, 組アドレスがテーブル 2 へと記録されない場合である. そこで, この旨の応答を下流ルータへ返すことで, この経路は攻撃経路でないと知らせる. 一方, エッジルータが攻撃ホストに問合せを行っても応答は返ってこない（図 7）. この場合は, 自身がエッジルータである可能性が高い. 問合せパケットには, 最終的に被害ホストからエッジルータまでの IP アドレスが書き込まれることから, このルータまでが発信源までの攻撃経路となる. エッジルータは攻撃経路の情報を被害ホストに知らせることでトレースバックを完了させる.

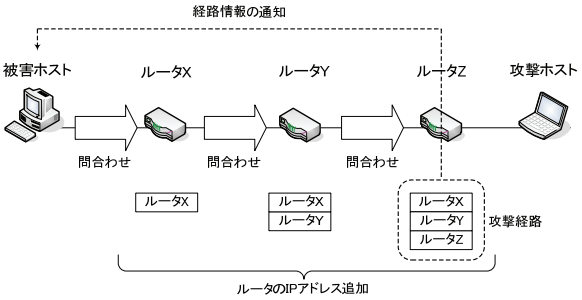

図 6. トレースバック概要

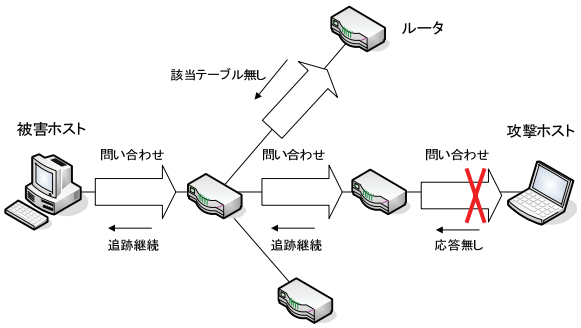

図 7. 問合せの返信と応答

3.3. パケットフォーマット

問合わせパケットのフォーマットを図 8 に示す. フォーマットはデータリンクに続いて送信される.

図 8. パケットフォーマット

パケットフォーマットの説明は以下のとおり.

- バージョン
- タイプ
- ヘッダ長
- チェックサム
- 被害ホスト IP アドレス
- 経路情報

バージョンは送信する問合せメッセージのバージョンを表す.

タイプは問合せの応答, 要求を種別するもので, 追跡依頼, 追跡継続, 該当テーブル無し, 追跡結果の 4 つが含まれる.

ヘッダ長は問合せパケット全体の長さをオクテットで表す.

チェックサムはヘッダのチェックサムを表す.

被害ホストアドレスは被害ホストの IP アドレスを格納する.

経路情報はルータの IP アドレスを順に格納する.

4. 実装

本提案によるトレースバック技術を実装するにあたり実装の詳細について述べる. まずシステムを構築するにあたり開発環境を述べ, 次に実装概要について説明する.

4.1. 開発環境

現在はシステムの開発段階であり, 開発言語に C 言語を利用する. システムの安定性やネットワークに関連する情報が豊富なこと, カーネルを容易に変更できる点を考慮し, FreeBSD OS を利用する.

4.2. 実装概要

パケットの扱いに関してはデータリンク層を改良し, カーネルレベルで動作するトレース機能を持たせた FreeBSD OS をルータとして確認を行う. データリンク層から渡された受信パケットを参照し, 開発した独自のモジュールにより各テーブルを生成する. 問合せのパケットを受信, または返信・応答を返す場合においてもモジュールにより下位層に渡される.

5. 比較・評価

ここでは, 2 章で紹介した既存技術と提案方式を比較した結果を表 1 に示す.

表 1. 既存技術の比較

評価項目	リンク検査方式	ICMP方式	マーキング方式	Hash-based方式	提案方式
管理コスト	中	小	小	多	小
ネットワーク負荷	多	小	小	小	小
ルータ負荷	多	小	小	多	小
必要パケット数	多	中	多	小	中
攻撃後の追跡	×	○	○	○	○

管理コストでは, リンク検査方式は手動でトレースを行うことや, Hash-based トレースバック方式ではシステムの保守・管理が難しく管理者に大きな負担が掛かる. それに比べて ICMP トレースバック方式やマーキング方式, 提案方式はルータ同士が同様の機能を持ち, 個々が独立して動作するのでコストに対するオーバーヘッドは少ない.

ネットワーク負荷では, 追跡のための情報を余分に被害者へとパケットを流すため, ネットワークに余分なトラフィックを生成してしまうことになる. 提案方式は追跡のための情報は生成しないことからネットワークトラフィックに影響は与えない.

ルータ負荷では, Hash-based トレースバック方式はハッシュを計算する高性能な処理能力が要求され, パケットを記録する膨大なディスク容量を必要とする. また, リンク検査方式はフィルタリングを行うことでルータのパフォーマンスに影響を合える. 提案方式は複雑な処理を行わないので動作は比較的軽い.

攻撃経路を特定するに当たり, より多くのパケット数を必要とするのがリンク検査方式と ICMP トレースバック方式である. 逆に Hash-based トレースバック方式は攻撃数にとらわれずに逆探知を行うことができる.

攻撃後の追跡においては, 4 つの技術のうちリンク検査方式を除く方式は攻撃者が DoS 攻撃を終了した後でも追跡が行える. しかしリンク検査方式は DoS 攻撃が発生している最中にしか追跡を行うことはできない.

以上のことからこれまでの既存のトレースバック技術と提案方式との比較を行った. それぞれの利点はあるものの, 各評価をみると課題点が残されていることが分かる. 提案方式の問題点としては与えられた閾値によりトレースが行われないことが考えられる. SOHO のような中規模なネットワークと ISP や学校などの大規模なネットワークでは, ルータが転送するパケット数は大きく異なってくる. 閾値が小さければ通常のパケットが攻撃パケットととらわれてしまう. この誤認知をさけるためには各テーブルに設けられた閾値が特に重要となる.

6. まとめ

本研究では MAC アドレスを用いた IP トレースバック技術の提案について検討した. 章のはじめに既存技術を紹介し, それらが持ついくつかの問題点を指摘した. 次に, 既存技術とは異なる一方式として提案した本方式は開発段階であり, 今後は提案方式を実装して動作確認を行うことで, どの程度まで正確に攻撃経路をさかのぼることが可能か確認する. また, 実際に DoS 攻撃からデータを収集することで閾値の決定方法を考えていく.

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, Vol.12, No.42, Aug, 2001.

[2] Steve Bellovin, et al, “ICMP Traceback Messages”, Internet-Draft, Expires August, 2003.

[3] S. Savege, D. Wetherall, A. Karlin, T. Anderson, “Practical Network Support for IP Traceback”, In Proceedings of SIGCOMM ‘00, pp.295-306, 2000.

[4] 岡崎直宣, 河村栄寿, 朴美娘, “サービス不能攻撃の追跡手法の効率化に関する検討”, 情報処理

学会論文誌，Vol.44，No.12，Dec.2003.

[5] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, “HashBased IP Traceback”, Proceedings of ACM SIGCOMM 2001，San Diego，CA，USA，August 2001.

[6] Cisco ルータを使用したパケットフラッドの識別とトレース
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/22-j.html

[7] Stephen Northcutt，Mark Cooper，Matt Fearnow，Karen Frederik，クイープ，ネットワーク侵入解析ガイド 侵入検知のためのトラフィック解析法，株式会社ピアソン・エデュケーション，2001/12/01

[8] 竹尾大輔, Telnet による渡り歩きの検出方法の検討，渡邊研究室卒業論文集，Vol.1，No.9，2004/3

[9] Stefan Savage, David Watcherall, Anna Karlin, and Tom Anderson, “Network Support for IP Traceback，IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.9，NO.3 JUNE，2001.

[10] 池田竜朗，山田竜也，“発信源追跡のためのハイブリッドトレースバック方式”東芝レビュー，Vol.58，No.8，2003.

[11] Dos/DDoS 対策について，警察庁，http://www.cyberpolice.go.jp/server/rd_env/pdf/DDoS_Inspection.pdf, June 2003.

[12] Stefan Savage，David Wetherall，Anna Karlin and Tom Anderson，“Network support for IP traceback”，IEEE/ACM Transactions on Networking，Vol.9，No.3，pp.226-237，2001.

[13] R. Stone, “CenterTrack : an IP overlay network for tracking DoS floods” in Proceedings of 9th USENIX Security Symposium ‘00，Den-ver，USA，Aug．2000.

[14] D．Turk，“Configuring BGP to Block Denial-of-Service Attacks”RFC 3882，Sep 2004.

[15] 武田　圭史，“ネットワークセキュリティ：4.侵入検知システムに関する研究の現状”, 情報処理，Vol.12，No.42，Aug，2001.

謝辞

本研究を行うにあたり，多大なるご指導，ご鞭撻を賜りました渡邊明教授に心より感謝致します．有益なご助言，ご検討頂きました渡邊研究室の学部生，学院生の皆様方に深く感謝いたします．特に学院生の皆様方には私からの度重なる質問や疑問に対し丁寧に答えて頂き，誠に感謝いたします．

また，宮崎大学の岡崎氏には，私の原稿について貴重な意見を頂きました．厚くお礼申し上げます．