MAC アドレス情報に基づく IP トレースバック技術の提案

播磨　宏和　　竹尾　大輔　　渡邊　晃
名城大学大学院理工学研究科

A proposal of IP trace back technology based on MAC Address information

Hirokazu Harima　　Daisuke Takeo　Akira Watanabe
Graduate School of Science and Technology，Meijo University

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を介した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．中でもサービス不能攻撃（DoS 攻撃）は対応策が困難であることから大きな問題となりつつある．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る攻撃である．DoS 攻撃を阻止する有効な手段はいまだに確立されてないのが現状である．DoS 攻撃では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．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 IP トレースバック技術[1]は重要である．

既存の IP トレースバック技術としては，ルータのデバッグ機能を利用するリンク検査方式，逆探知パケットを使用する ICMP 方式[2]，ある確率でパケットにマークをつけるマーキング方式[3][4]，パケットのダイジェストを利用する Hash-Based 方式[5]などが有名である．これらの既存の研究は IP レイヤ機能を用いたものがほとんどで，MAC レイヤに着目したものはほとんど存在しない．本研究では，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 MAC-Based IP トレースバックを提案する．DoS 攻撃では大量の攻撃パケットが攻撃対象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．このとき，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．

以下に 2 章で既存のトレースバック技術と課題を述べ，3 章で提案方式の概要，4 章で実装について述べ，5 章でまとめる．

2.　既存のトレースバック技術とその課題

2.1. IP トレースバック技術

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．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，図 1 に示すように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を行う．以下に代表的な IP トレースバック技術であるマーキング方式と Hash-based 方式について概要と指摘されている課題を述べる．

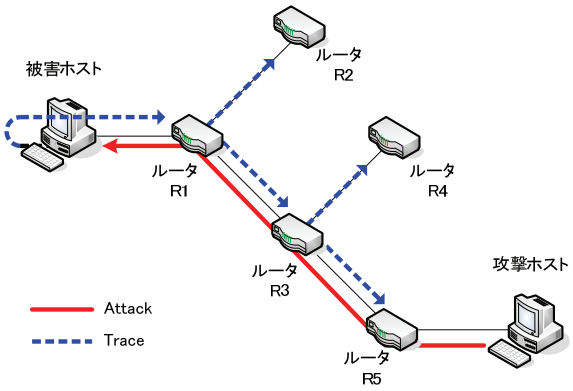


図 1．IP トレースバック技術の概要

2.2. マーキング方式

マーキング方式はある確率で逆探知のための情報をパケットの特定のフィールドにマーキングと呼ばれる追跡のための情報を分割して挿入し，被害ホストへと送り届ける方式である．初めにマーキングを行ったルータと下流のルータの 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 ヘッダの IP identification フィールドに埋め込む．マーキングされたパケット（マーキングパケット）を受け取った被害ホストは，分割されていたマーキングを元通りに復元し，攻撃経路を再構築する．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，追跡のためにルータからあたら他情報を収集する必要がないという利点がある．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で莫大な計算量を要するという課題がある．

2.3. Hash-based 方式

Hash-based 方式は各ルータでパケットを転送する際にログを記録する方式である．すべての受信パケットの先頭部分から計算した複数のハッシュ値を内部メモリに記録する．パケットの記録を効率よく保持することができれば，IP ヘッダに情報を埋め込んだり拡張することがなく逆探知が可能となるという考えに基づいている． IP ヘッダの中で，経路中で不変な部分とペイロードについてハッシュ関数を適用した結果を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，そのときに使用したハッシュ関数と共に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，攻撃パケットのパケットシグニチャをダイジェストテーブルのハッシュ関数に通し，記録されている

MACアドレス情報に基づく IPトレースバック技術の提案

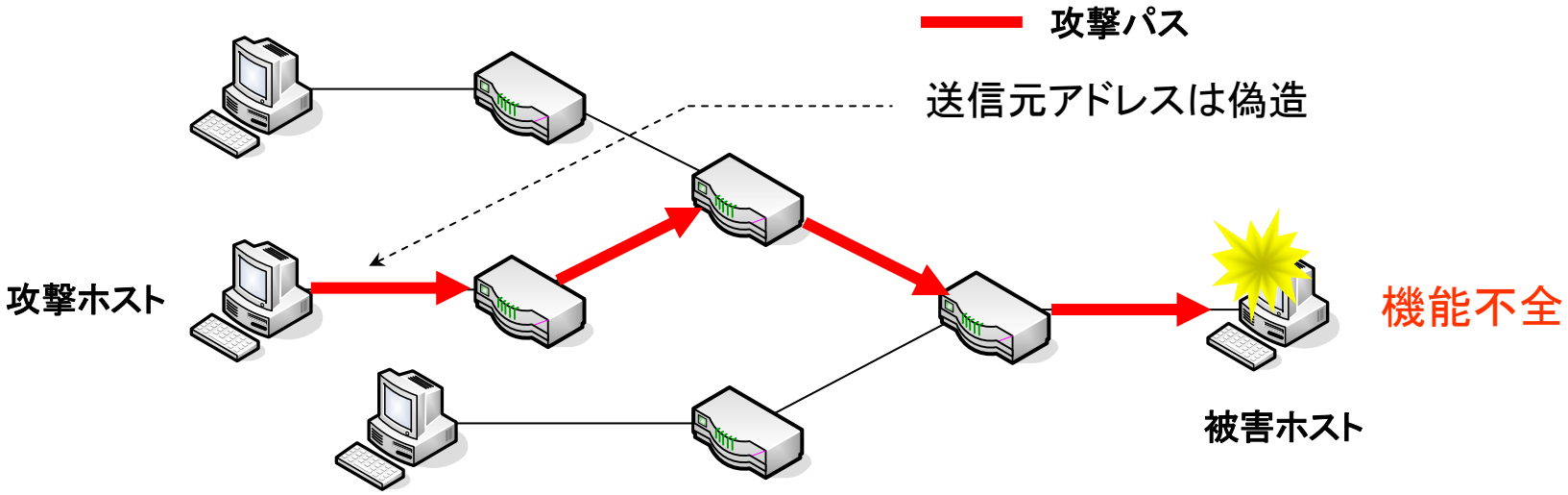
A proposal of IP trace back technology based on MAC Address information

名城大学大学院理工学研究科

播磨　宏和，竹尾　大輔，渡邊　晃

研究の背景

- セキュリティに関わる被害規模の拡大
  - サービス不能攻撃（DoS攻撃）
    - 大量のパケットを送信
    - 身元の特定は困難

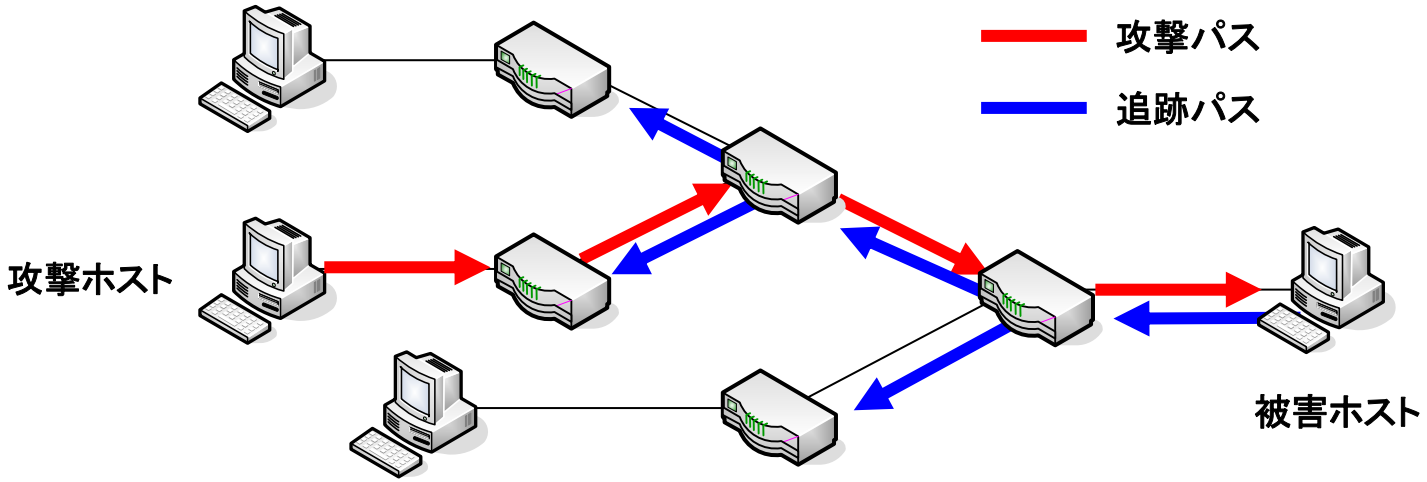


- 攻撃パケットの発信源を特定する手段が必要

IPトレースバック技術

IPトレースバック技術とは

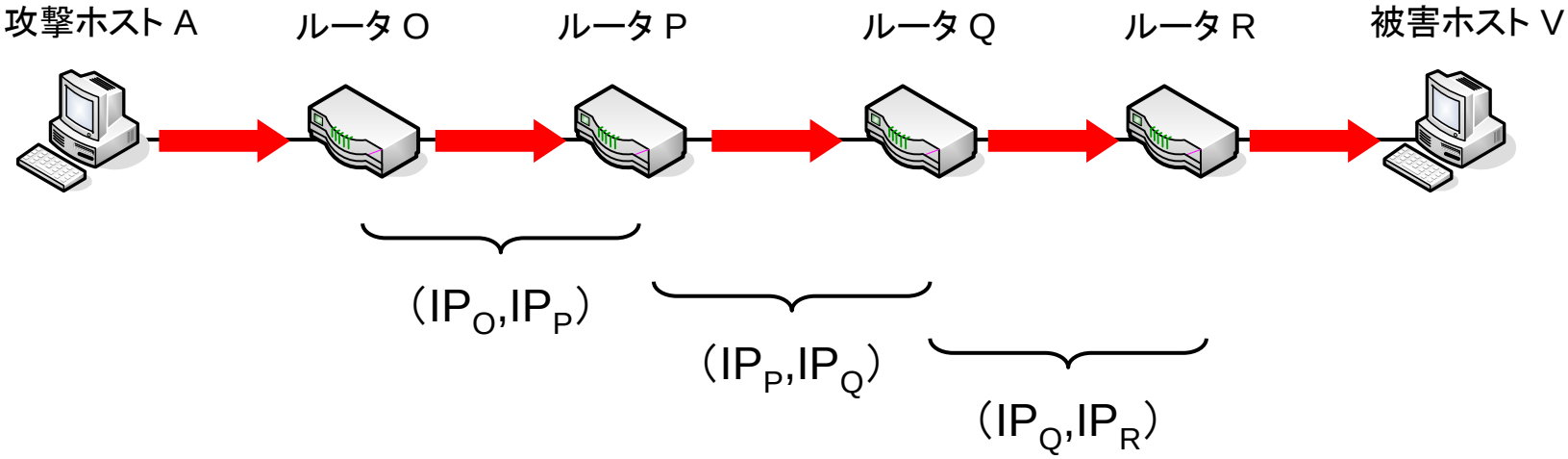
- IPトレースバック技術
  - ルータ機能の追加



- 既存技術
  - 受動型
    - マーキング方式 ….. Savageらの方式
    - メッセージ方式 …… ICMPトレースバック方式
  - 能動型
    - リンクテスト方式 …. Input-debugging方式
    - ログ方式 …….. Hash-Based方式

既存技術
マーキング(Savageらの)方式

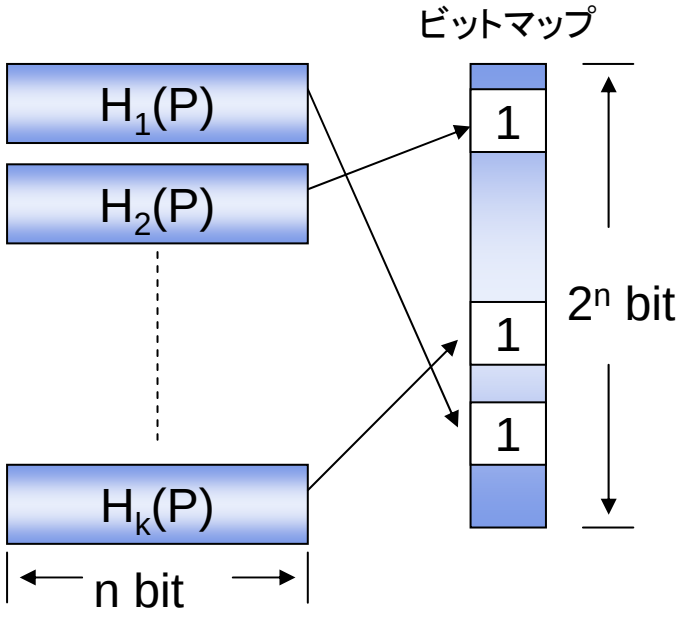
- IPヘッダ内の未使用ビットにマーキング
  - IPヘッダ（Identificationフィールド）
  - 2つのルータのアドレス
- 収集したマーキングパケットから攻撃経路を再構築



- 欠点
  - 攻撃経路の構築に膨大な時間が必要
  - 既存の通信に影響を及ぼす

既存技術
ログ(Hash-Based)方式

- ハッシュ関数を用いてビットマップを生成、通過記録を保存
- ビットマップがルータに保存されているかを1ホップずつ検証することで攻撃経路を追跡



K個のハッシュ関数($H_1,H_2,\ldots,H_k$)

IPヘッダ

不変な部分(P)

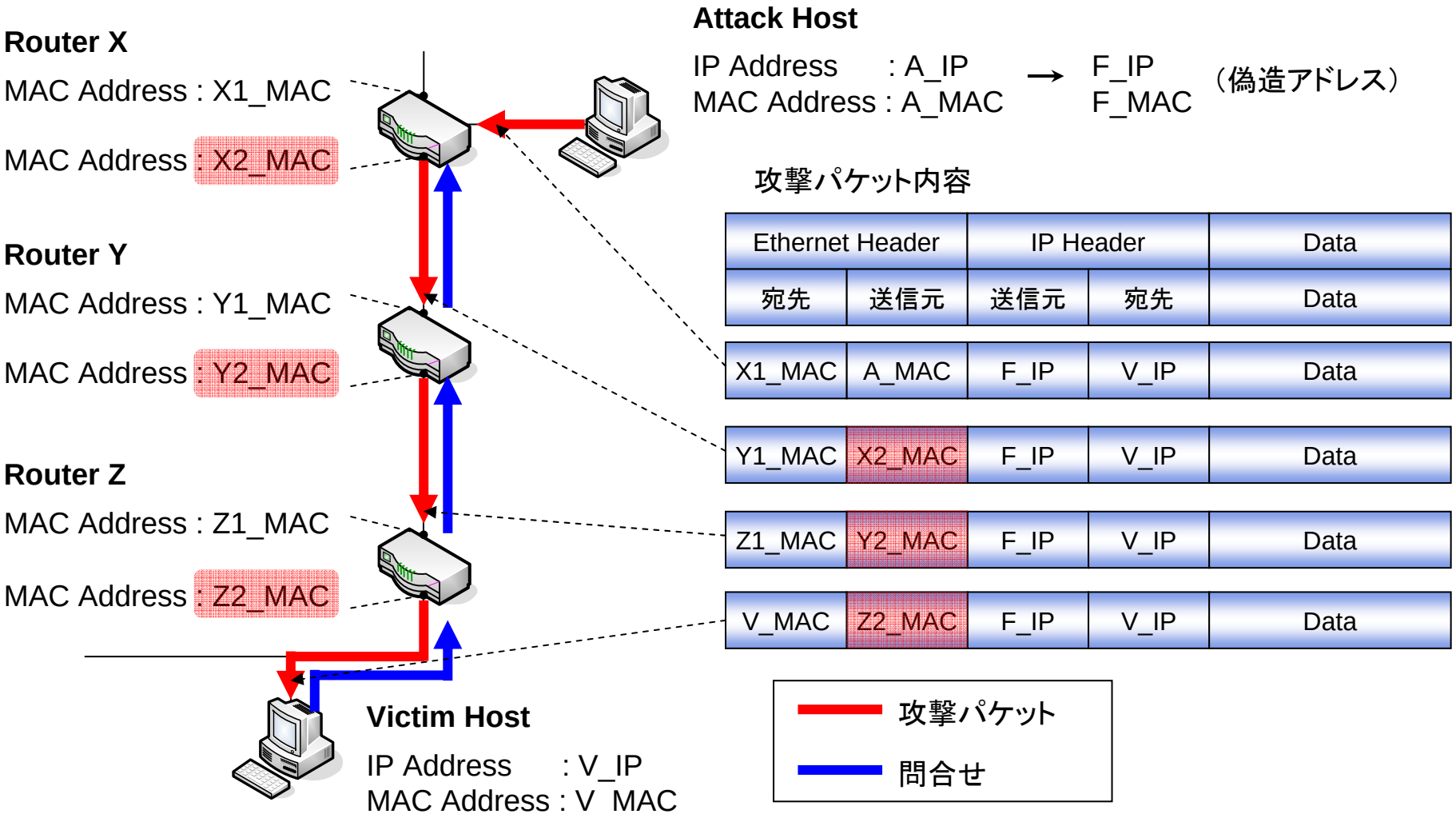
Ver	H L	TOS	Total Length
Identification			Fragment Offset
TTL		Protocol	Checksum
Source Address			
Destination Address			
Options			
Payload			

- 欠点
  - 大きな記憶容量や高いハッシュ処理能力が必要

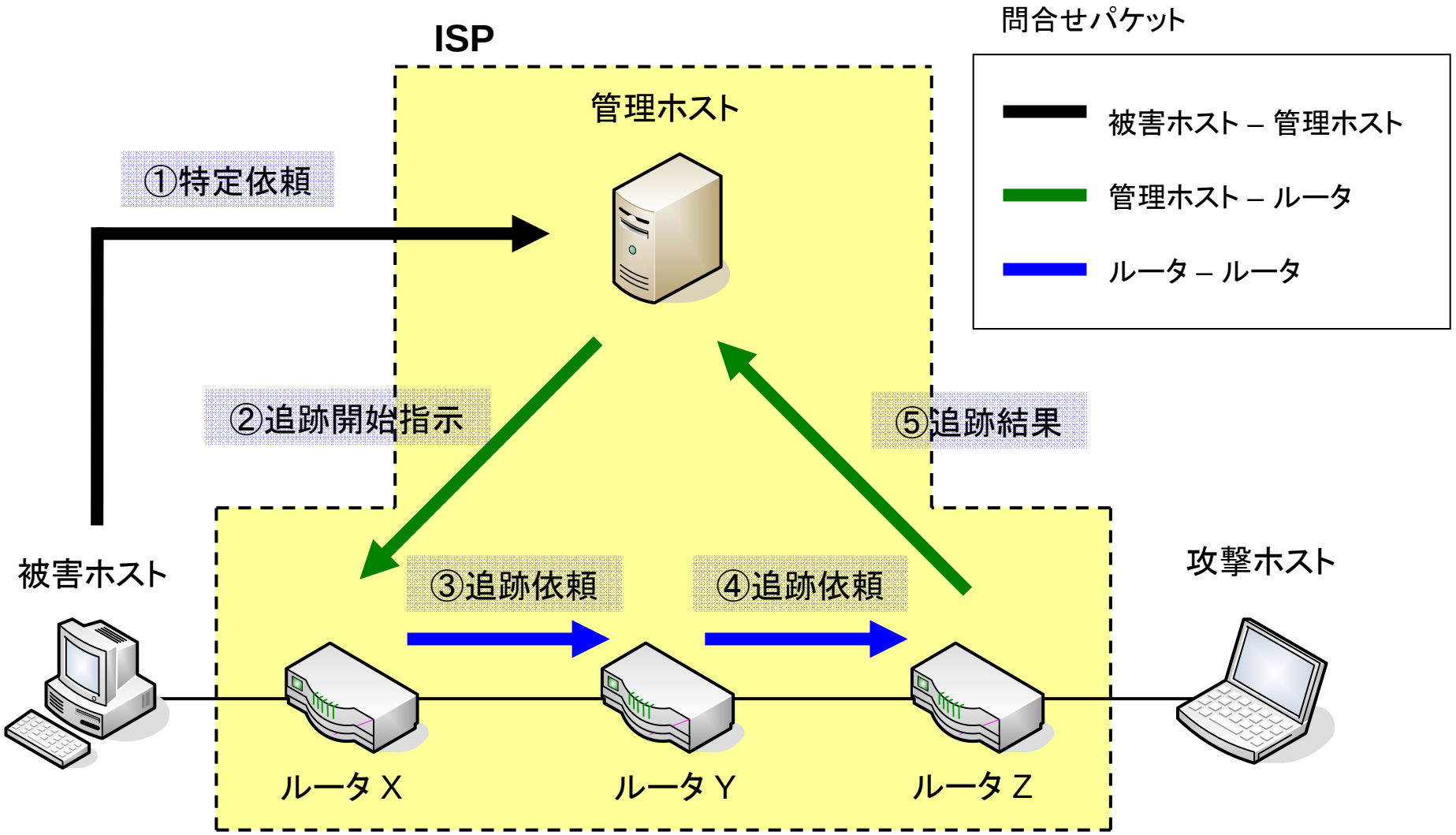
提案方式
MAC-Based方式の概要

- DoS攻撃の可能性のあるパケットから送信元MACアドレスを記録
- 記録されたMACアドレスにより上位のノードを特定し発信元を追跡する

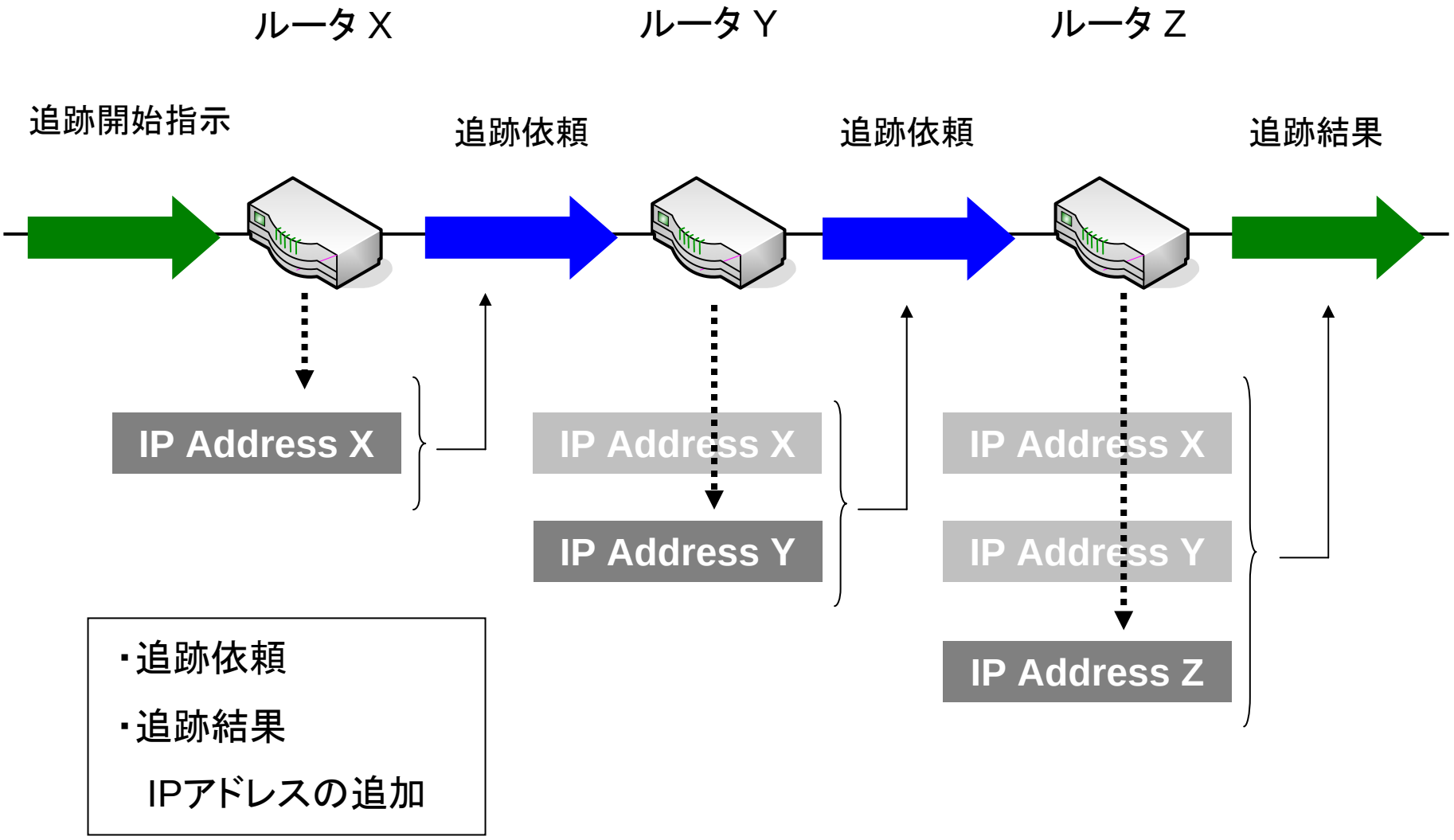
動作原理


Router X
MAC Address : X1_MAC
MAC Address : X2_MAC
Router Y
MAC Address : Y1_MAC
MAC Address : Y2_MAC
Router Z
MAC Address : Z1_MAC
MAC Address : Z2_MAC
Victim Host
IP Address : V_IP
MAC Address : V_MAC
Attack Host
IP Address : A_IP
MAC Address : A_MAC
→
F_IP
F_MAC
（偽造アドレス）
攻撃パケット内容
Ethernet Header
IP Header
Data
宛先
送信元
送信元
宛先
Data
X1_MAC
A_MAC
F_IP
V_IP
Data
Y1_MAC
X2_MAC
F_IP
V_IP
Data
Z1_MAC
Y2_MAC
F_IP
V_IP
Data
V_MAC
Z2_MAC
F_IP
V_IP
Data
攻撃パケット
問合せ

ネットワーク構成


問合せパケット
被害ホスト – 管理ホスト
管理ホスト – ルータ
ルータ – ルータ
ISP
管理ホスト
①特定依頼
②追跡開始指示
③追跡依頼
④追跡依頼
⑤追跡結果
被害ホスト
攻撃ホスト
ルータ X
ルータ Y
ルータ Z

経路情報の格納


ルータ X
ルータ Y
ルータ Z
追跡開始指示
追跡依頼
追跡依頼
追跡結果
IP Address X
IP Address X
IP Address Y
IP Address X
IP Address Y
IP Address Z
・追跡依頼
・追跡結果
IPアドレスの追加

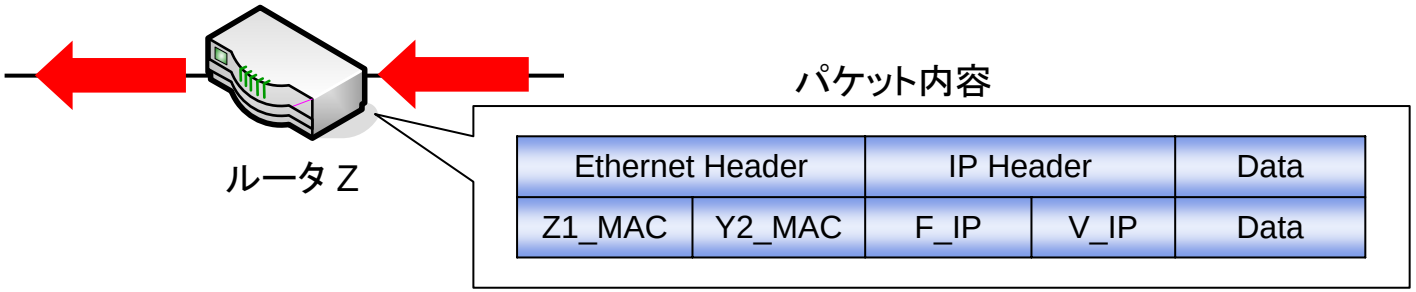
アドレスの記録

- テーブル1
  1. 宛先IPアドレスを記録
  2. カウント値の加算
  3. 時間単位で消去
  4. 閾値を超えたらテーブル2に保存*

  *攻撃経路の判断材料

- テーブル2
  1. 組アドレス*を記録
  2. 長期保存

  *組アドレス
  - ✓ 送信元MACアドレス
  - ✓ 宛先IPアドレス



テーブル1

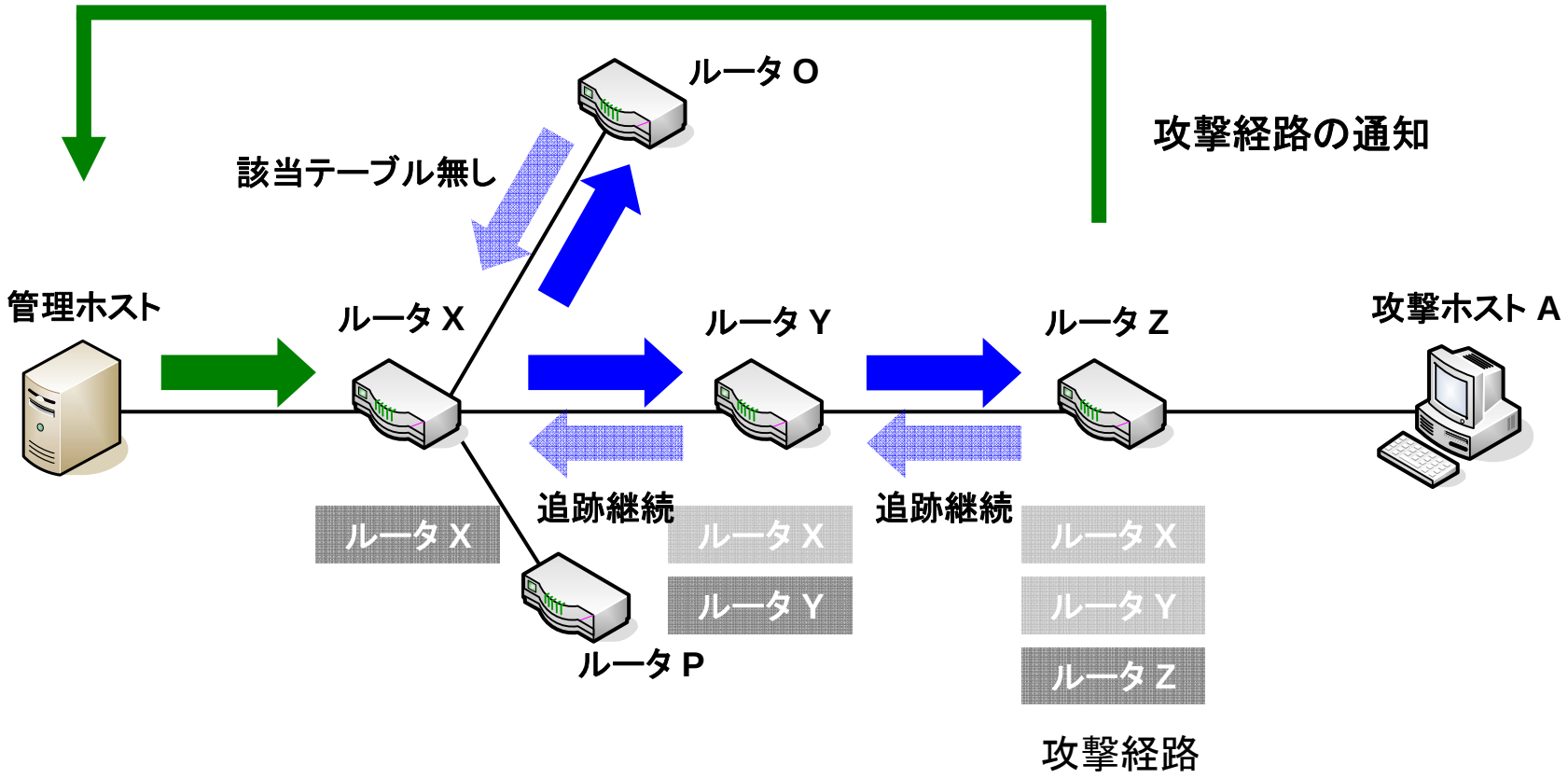
Destination IP Address	COUNT値
·····	·····
V_IP	1001
H_IP	73

閾値:1000

テーブル2

Destination IP Address	Source MAC Address
V_IP	Y2_MAC
·····	·····
V_IP	O2_MAC

攻撃経路の追跡

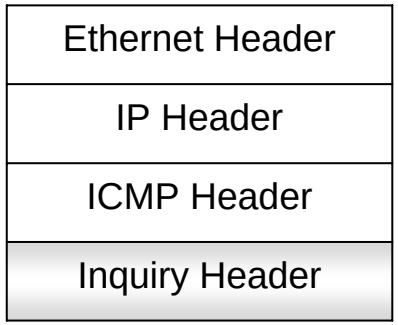


追跡依頼パケットに自分自身のIPアドレスを追加

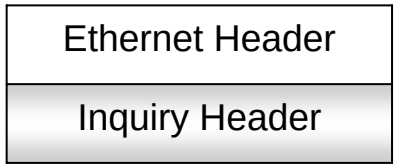
自分自身がエッジルータであれば管理ホストに攻撃経路を通知する

パケットフォーマット

MTC



MTI



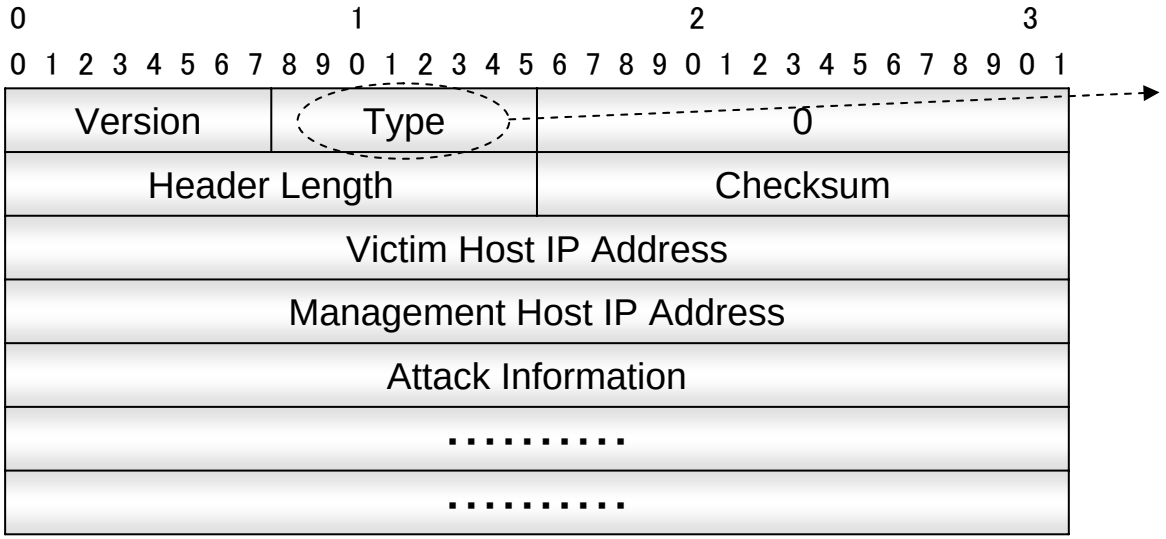
MTC（MAC Traceback Control）

管理ホスト - ルータ間

MTI（MAC Traceback Information）

ルータ - ルータ間

Inquiry Header



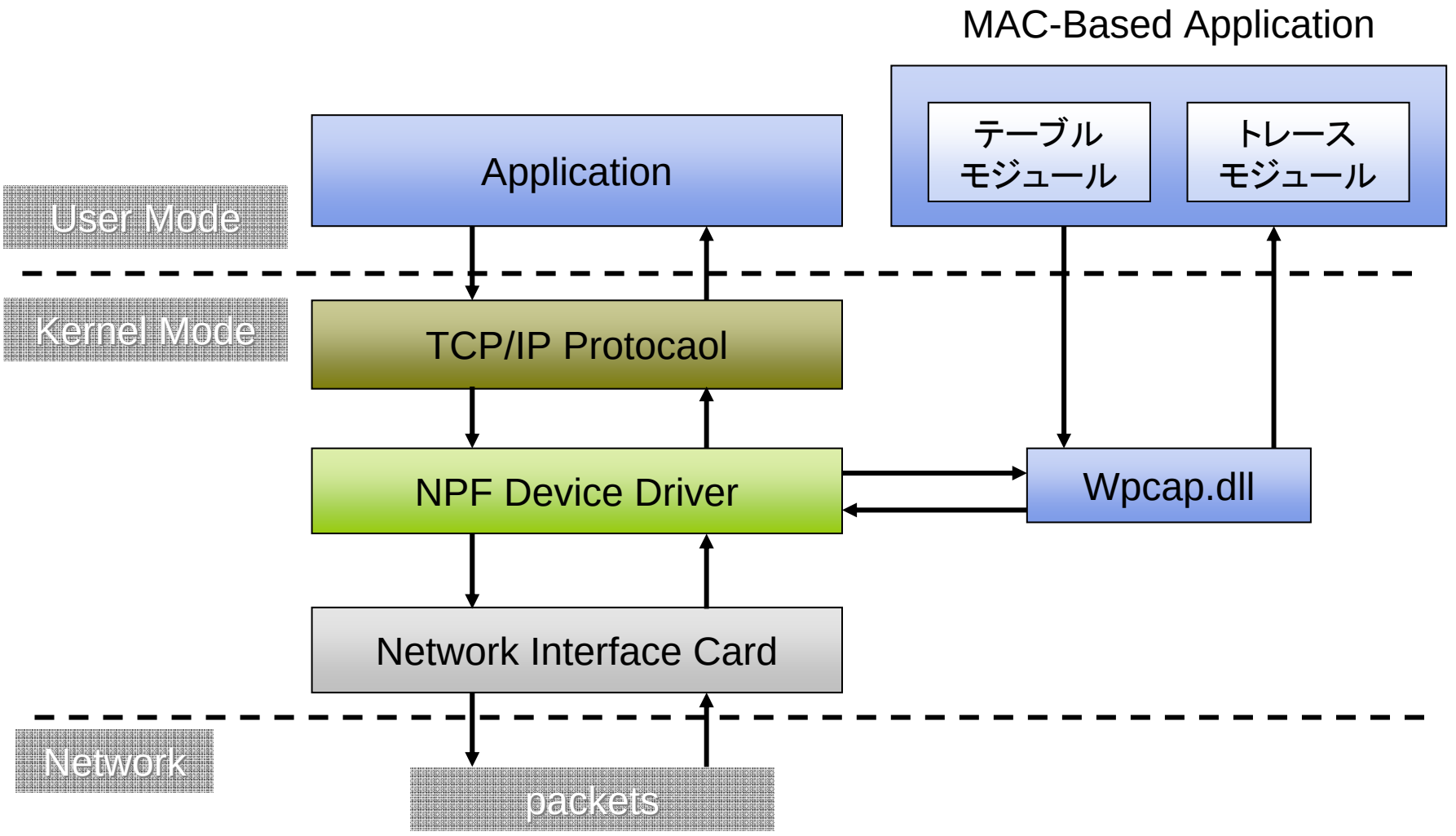
Type Field

- 追跡開始指示
- 追跡結果
- 追跡依頼
- 該当テーブル無し
- 追跡継続

MAC-Basedプログラムの実装 [1/2]

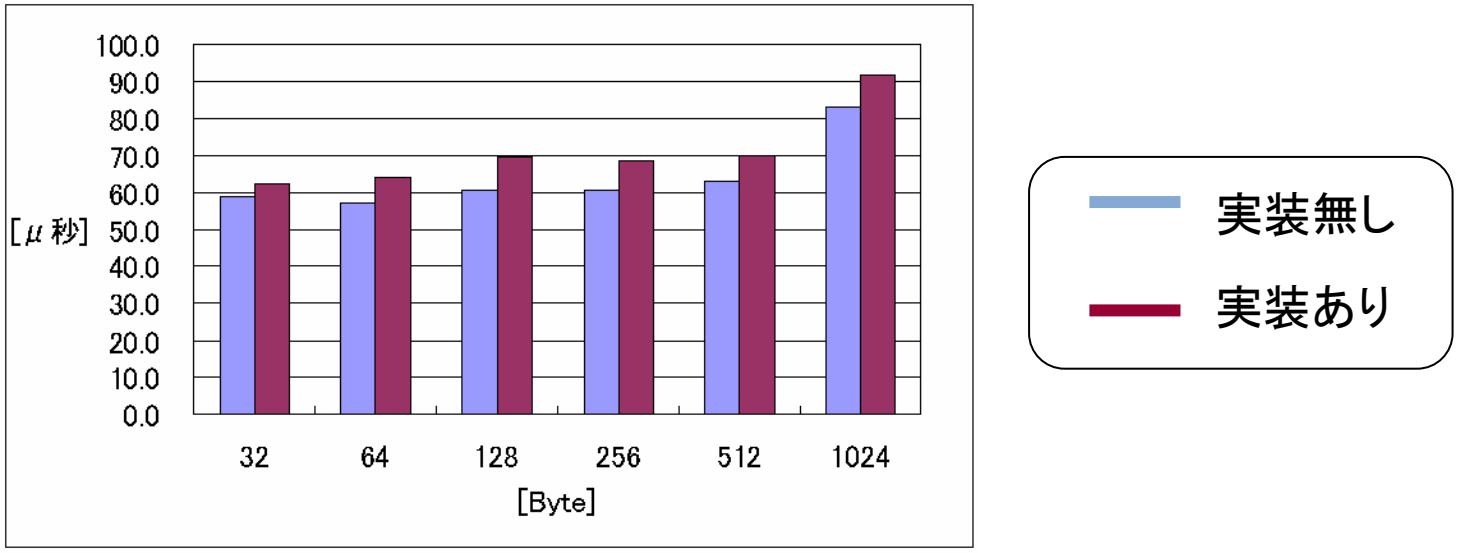
- 試作システムをWindows 2000上に実装
  - 管理ホスト
  - ルータ
- パケットキャプチャライブラリ
  - Winpcap
    - オープンソースである
    - UNIX用キャプチャライブラリ「libpcap」と互換性あり

MAC-Basedプログラムの実装 [2/2]



スループット測定

- ルータの中継処理に与える影響
  - 1つのUDPパケットの中継時間



- パケットキャプチャ機能
  - ルータのスループット低下等の問題が発生

既存技術と提案方式との比較

	ハードウェアコスト	解析量	パケット変更	プロトコル定義
マーキング方式	○	×	△	○
Hash-based方式	×	○	○	△
提案方式	○	○	○	△

- **ハードウェアコスト**
  - Hash-based方式：高い処理能力、高記憶容量
- **解析量**
  - マーキング方式：攻撃者の数が増えるほど増大
- **パケット変更**
  - マーキング方式：既存の通信への影響
- **プロトコル定義**
  - 信頼性や定義の難しさ
  - マーキング方式：追跡情報の送信

むすび

- まとめ
  - MACアドレスを用いたIPトレースバック技術の手法について提案した
- 現在の状況
  - Windows OSにて試作プログラムを開発
  - 攻撃者側のエッジルータの特定を確認
- 今後の課題
  - スループット向上のため、モジュールをFreeBSDのカーネルに組込み、より実践的な開発を行う
  - 提案システムを実装して有効性を確認するとともに最適な閾値決定方法を検討する

おわり

かどうかを検査することで確認できる．この方式では，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が，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，他の方式よりもコスト面で不利になる可能性がある．

3. MAC-Based IP トレースバック

3.1. 概要

MAC-Based 方式はルータに残された攻撃パケットの送信元 MAC アドレスと宛先 IP アドレスを手がかりとして，ルータを順にたどることで攻撃側のエッジルータまでを追跡する．

攻撃ホストから被害ホストに DoS 攻撃が仕掛けられた場合においてパケットのアドレスが変化する様子を図 2 に示す．攻撃ホストから送信されたパケットの送信元 IP アドレスは一般に詐称されており，送信元 MAC アドレスも詐称されている可能性が大きい．攻撃パケットの内容は図 2 のように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が，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は変わることがない．攻撃パケットには被害ホストの IP アドレスと上流ルータの正しい MAC アドレスが必ず含まれている．

MAC-Based 方式はルータにパケットの送信元 MAC アドレスと宛先 IP アドレスをペアにして記録させておき，この情報を元にトレースバックを行う．

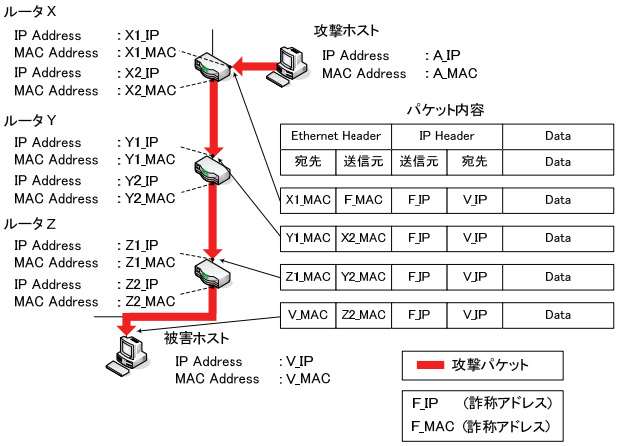


図 2．パケットのアドレスが変化する様子

図 3 に想定するネットワーク構成を示す．DoS 攻撃を仕掛ける攻撃ホスト，その攻撃を受ける被害ホストがユーザサイドに存在し，プロバイダが提供するルータは MAC-Based 方式の機能を搭載しているものとする．プロバイダ内には管理ホストが存在し，DoS 攻撃が発生したときは管理ホストの指示に従いトレースバックを開始する．点線内がプロバイダに相当し，被害ホストは特殊な機能を持たない一般端末である．

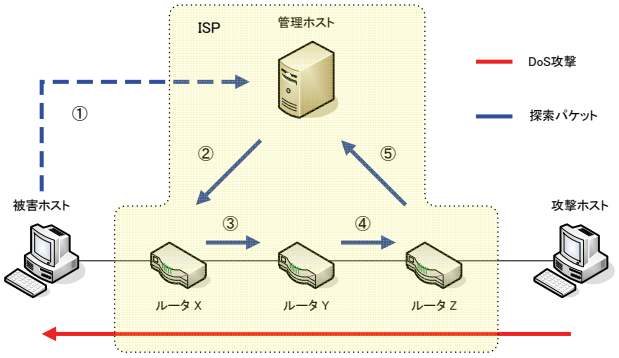


図 3．想定するネットワーク構成

被害ホストが DoS 攻撃を受けたと知ると，被害者側のユーザはプロバイダに対して攻撃ホスト特定の依頼を行う（①）．依頼を受けたプロバイダは管理ホストから被害ホスト側のエッジルータに攻撃経路追跡のための指示パケットを送信する（②）．指示パケットを受信したルータは記録されたアドレス情報から上位のルータを特定し，攻撃パケットが通過したルータを順にたどり攻撃経路を構築していく（③,④）．最後に攻撃ホスト側のエッジルータは管理ホストへ攻撃経路の情報を通知する（⑤）．なお，②,⑤は通常の IP パケット，③,④は MAC-Based 方式特有のイーサネットパケットにより追跡が行われる．

3.2. 組アドレス情報の記録

攻撃経路の情報を交換するにあたり，ルータは図 4 に示すように宛先 IP アドレスと送信元 MAC アドレスの情報を記録するためのテーブル 1，テーブル 2 を保持している．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 に記録する．テーブル 1 の内容は短い一定間隔で消去する．転送回数のカウント値には閾値を設け，カウント値が上記一定時間内にこの閾値を超えた場合，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送信元 MAC アドレスと宛先 IP アドレスの 2 つのアドレス（以降，組アドレスと呼ぶ）を記録する．カウンタの閾値は，ルータの起動時に管理ホストの管理者によって決定される．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長期的に保持する．

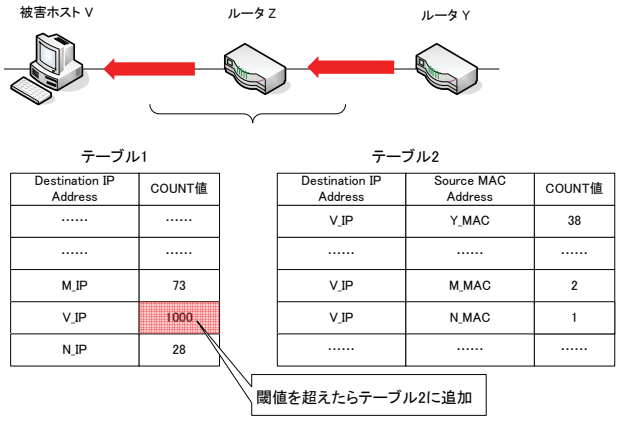


図 4．組アドレスの記録

3.3. 追跡動作

追跡時においては各ルータがテーブル 2 に記録されている組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．

管理ホストは被害ホストの IP アドレスを格納した問合せパケットを被害者側のエッジルータ Z に対して送信する．受信したルータ Z は自身のテーブル 2 を用いて被害ホストに対応した送信元 MAC アドレスすべてを割り出す．次に図 5 のように自分自身の IP アドレス情報を加え，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．問合せパケットはイーサネットヘッダ後に直接追跡情報がのる．問合せパケットを処理するためにはルータにこのパケットをイーサネットレベルで解析し処理を行う機能が必要である．ルータがこれらの操作を同様に行うことで，攻撃ホスト側のエッジルータまで問合わせていく．

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，つまりテーブル 2 に情報がない場合，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．

図 6 に問合せの要求と応答の様子を示す．攻撃ホストに最も近いエッジルータは上流に問合せを行っても応答は返ってこないので，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，最終的に攻撃ホストの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．最後にこのエッジルータは管理ホストに攻撃経路の情報を報告する．

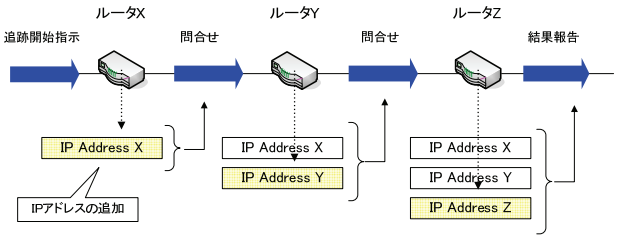


図 5. 経路情報の格納

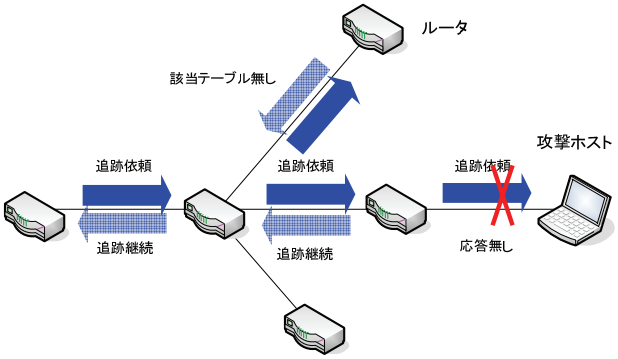


図 6. 問合せの要求と応答

3.4. パケットフォーマット

トレースバックパケットは，管理ホストとルータ間の通信で使われる MTC（MAC Traceback Control）メッセージと，ルータ間で使われる MTI（MAC Traceback Information）メッセージがある．前者は ICMP Echo Request をベースに定義されており，後者はイーサネットヘッダの上に独自に定義した問合せパケットを用いる．パケットフォーマットとメッセージ内容を図 7 に示す．

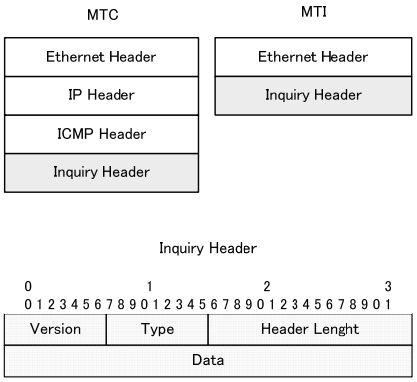


図 7. パケットフォーマット

MTI メッセージは MAC-Based 方式の特徴的な構成を持つパケットである，Inquiry の Type フィールドには以下のメッセージが格納されており，これを受信したルータは下記の情報を元に経路探索のための処理を行う．

1). 追跡依頼（Trace Request）
追跡経路上のルータが上位のルータに対してトレースバックを要求する．

2). 追跡継続（Trace Continue）
追跡依頼を受信したルータがテーブルに被害ホストの IP アドレスが存在した場合に下流ルータに送信する．これを受信したルータは上流のルータが攻撃経路ではないことを確認する．

3). 該当テーブル無し（No Pertinent Table）
追跡継続を受信したルータがテーブルに該当する被害ホストの IP アドレスが存在しない場合に，下流のルータに対してその旨を伝える．

4. 提案方式の実装と評価

MAC-Based 方式の有効性を示すために試作の実装と評価を行った．

4.1. 試作の実装

試作システムとして，Windows PC をルータとして利用し，MAC-Based 方式を実装した．Windows 用汎用パケットキャプチャライブラリ「Winpcap」[6]を用いてテーブルの作成と各ノードとの相互通信を実現させた．

テーブルのアドレス情報においても閾値を超えたパケットの情報が格納され，管理ホストからの追跡開始指示に対してルータは自律的にトレースバックを実行し，管理ホストはエッジルータからの結果報告を受信したことを確認した．

試作システムがルータの中継処理に与える影響がどの程度あるのか，1 パケットの転送時間を比較した．提案方式を実装した状態と実装していない状態で様々なデータ長の UDP パケットを中継させて測定した結果を図 8 に示す．図 8 から確認できるように試作のパケットキャプチャ機能を使用した実装ではルータのスループット低下等の問題が発生する．これはパケットキャプチャライブラリがデータをムーブしているためと考えられる．実運用ではこのようなスループットの低下は無視できないため，今後は MAC-Based 方式を OS に組み込むことを検討する必要がある．

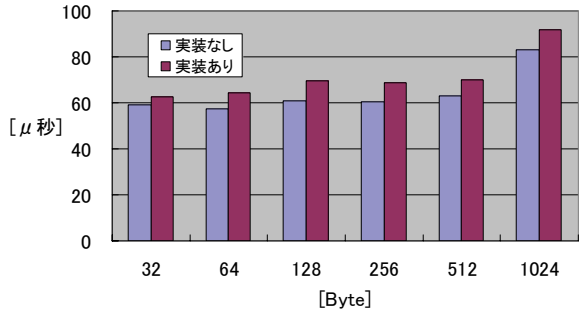


図 8. スループット測定結果

4.2. 既存のトレースバック方式との比較

既存方式と MAC-Based 方式を比較した結果を表 1 に示す. ハードウェアコストの面においては，Hash-based 方式はルータに処理能力や記憶容量の高いコストが求められる．解析量の面においては，マーキング方式は膨大なマーキングパケットから攻撃経路の情報を確かめなければならないことから攻撃ホスト特定に時間がかかる．Hash-based 方式もマーキング方式ほどではないが，解析に時間を要する．パケット変更に関しては，マーキング方式はパケットそのものを改良するため既存の通信に影響を与えるといった問題が指摘されている．プロトコル定義に関しては，独自のシーケンスを適用する Hash-based 方式と MAC-Based 方式はルータ間の連携が必要になることからエラーの発生を考慮した設計が必要である．

提案方式では，与えられた閾値によってはトレースが行われない場合の出ることが考えられる．SOHO や中規模なネットワークと ISP や企業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量は大きく異なってくる．閾値の設定によっては通常のパケットが攻撃パケットととられてしまう可能性があり，この誤認知をさけるためには各テーブルに設ける閾値の決定が特に重要となる．

表 1. 既存方式と MAC-Based 方式の比較

	ハードウェアコスト	解析量	パケット変更	プロトコル定義
マーキング方式	○	×	×	○
Hash-based方式	×	○	○	△
MAC-Based方式	○	○	○	△

5. 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について検討した．MAC-Based 方式を実装させ，動作確認と既存方式との比較を行った．今後は，さまざまなネットワーク環境において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実用性を確認する．また，経路を撹乱させる分散型 DoS 攻撃（DDoS 攻撃）にも対応させるための検討を行う予定である．

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 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] WinPcap http://winpcap.polito.it/

[7] Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, B. Schwartz, S. Kent, and W. Strayer. Single-Packet IP Traceback. In ACM/IEEE Transactions on Networking, vol.10, no.6, December 2002.

[8] 三輪信雄，白井雄一郎，白濱直哉，又江原恭彦，柳岡裕美,「不正アクセスの手法と防御」, ソフトバンクパブリッシング株式会社，2001 年

[9] 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

[10] 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

[11] 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

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