MAC-based IP トレースバック方式の提案と実装

m0532017　播磨　宏和
渡邊研究室

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．その中でもサービス不能攻撃（DoS 攻撃）と呼ばれる攻撃は，標的に対して大量のパケットを送りつけることでシステムを停止させる悪質な攻撃である．防御策としては，攻撃者を特定し，攻撃ホストと接続しているルータから遮断させる方法がある．しかし，DoS 攻撃の多くは送信されるパケットの送信元 IP アドレスが詐称されている場合がほとんどであり，攻撃者の特定が困難という課題がある．

DoS 攻撃のパケットから送信元を特定する方法として IP トレースバック技術がある[1]．IP トレースバック技術とはルータに機能を追加することにより，攻撃パケットが通過したルータを割り出し，攻撃者までの経路をつきとめる技術である．

しかし，既存の研究では IP レイヤに機能を追加したものがほとんどで，攻撃経路を正確に追跡できなかったり，ルータの処理負荷が増大し，スループットが低下するなどの点が指摘されている．我々は偽造が困難な MAC アドレスに着目した MAC-based IP トレースバックを提案する．実装と評価を行い，その効果を確認したので報告する．

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の概要を示す．

2.1 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，ある確率で攻撃経路の情報をパケットの一部に付加する方式である． IP ヘッダ内の 16 ビットの識別子である identification フィールドにルータの IP アドレスを分割して挿入する．被害を受けた被害ホストは，マーキングされた受信パケットから，ルータの IP アドレスを復元して攻撃経路を再構築する．追跡のためのパケットを新たに発生しないので，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，確実に経路を再構築するには大量のパケットが必要である．また，経路構築の計算量が膨大である．IP ヘッダに情報を埋め込むことにより既存の通信への影響が出る可能性がある．

2.2 Hash-based 方式

Hash-based 方式は，ルータが転送するすべてのパケットに対してログを記録する方式である．IP ヘッダの中でも，ルータを経由してもフィールド値が変化しない不変部分 20 バイトとペイロードの先頭 8 バイトのハッシュを適応し記録する．攻撃を受けた場合，ルータが攻撃パケットと一致するログを記録しているかどうか調べることにより攻撃経路を構築する．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，ルータにハッシュ計算のための高い処理能力が必要である．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ている可能性があり，限られた時間で追跡を完了させる必要がある．

3. MAC-based IP トレースバック

3.1 MAC-based IP トレースバックの概要

図 1 のようなネットワーク環境において，攻撃ホストが被害ホストに DoS 攻撃を仕掛けたとする．このとき，攻撃ホストから送信された攻撃パケットの送信元 IP アドレスは詐称されているものとする．図 1 に示すように，撃パケットはルータを経由するごとに，MAC アドレスが入れ替わるが，この部分を攻撃者が偽造することはできない．つまり，攻撃パケットには必ず被害ホストの IP アドレスとパケットを転送した上位ルータの正しい MAC アドレスが含まれている．

MAC-based IP トレースバックでは，攻撃パケットの送信元 MAC アドレスから上位ルータの IP アドレスを割り出し，その IP アドレスを記録しておくことにより，攻撃経路の構築を可能とする．

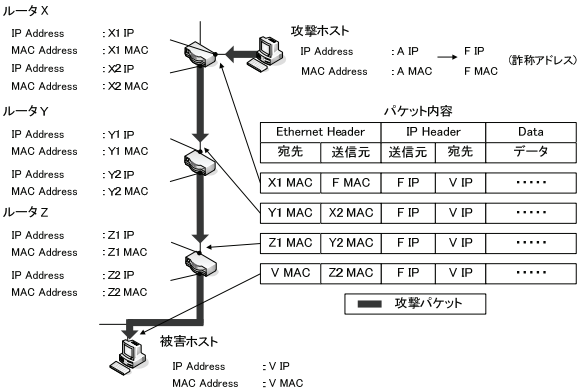


図 1. MAC－based IP トレースバックの概要

3.2 MAC-based IP トレースバックの動作

MAC-based IP トレースバックでは単位時間における各種パケットの転送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転送回数が，設けられた閾値を超えると DoS 攻撃パケットの可能性があると判断する．DoS 攻撃と判断されたパケットの送信元

MAC アドレスを基に 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，経路構築用の情報として記録する．

DoS 攻撃の種類によっては少量のパケットを送信しただけでも被害ホストを停止させることができる．そこで，DoS 攻撃の種類に応じて閾値を決定できるようにするため，ルータは DoS 攻撃の種類を判別させるためのシグネチャを保持する．個々のシグネチャと閾値を関連付け，パケット転送時にそれらを照らし合わせることにより，経路構築用の情報を蓄積することができる．

MAC-based IP トレースバックが動作する環境としては図 2 のようなネットワーク構成を想定する．点線内はプロバイダに相当する．被害ホストが攻撃を受けると被害者はプロバイダの管理者に電話等により攻撃者追跡の依頼をする．依頼を受けた管理者は，管理ホストを用いてルータに，被害ホスト宛の攻撃パケットを転送していないかを問合せて行くことにより，攻撃経路を構築していく．

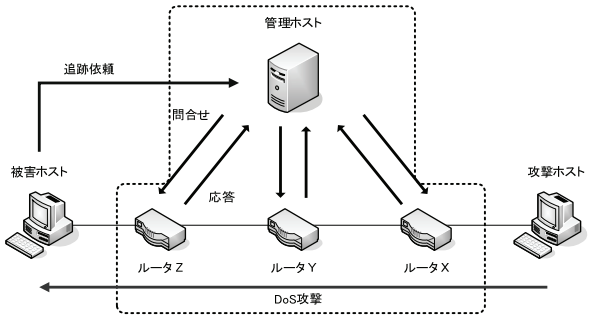


図 2. 想定するネットワーク構成

4. 評価

MAC-based IP トレースバックを評価するため，FreeBSD 上で動作するルータのカーネル内に本機能を実装した．管理ホストはアプリケーションプログラムとして動作させた．

4.1 スループット測定

MAC-based システムを実装させたルータにおいて処理能力にどの程度影響を与えるかスループット測定を行った．その結果，本機能を実装しない場合のスループットは 72.221Mbps，実装した場合のスループットは 72.178Mbps であった．スループット低下は約 0.06%であり，本システムの実装におけるスループット低下はほとんどみられなかった．この結果は，ルータへの追加機能が転送パケットとシグネチャを照らし合わせ，カウントを計るだけの単純な処理でよいためである．

4.2 閾値の決定

各種の DoS 攻撃に対して最適な閾値を決定させるための実験を行った．被害ホストの仕様は CPU Intel Celeron 2.66 Ghz，メモリ 512 MB，OS は Fedora Core 4 を使用し，ネットワークに 100base で接続した．被害ホストに WEB サーバを起動させ，クライアントから一定の HTTP 要求に対する応答時間を測定した．攻撃ホストが SYN-Flood 攻撃を仕掛けた場合における応答時間と CPU 負荷の変化を図 3 に示す．攻撃ホストからの攻撃レートが 6500[pps]を境に急激なシステム低下が見られる．このことから，SYN-Flood 攻撃においては 6500[pps]の攻撃レートが閾値ということができる．

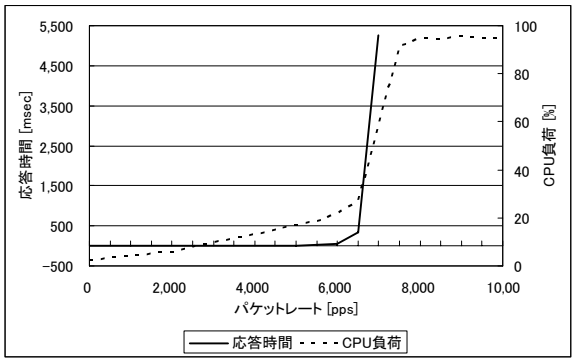


図 3. SYN Flood 実験による閾値の決定

4.3 既存技術との比較

表 1 に提案方式と既存技術の比較を示す．本方式はルータの処理負荷が少なく，記憶容量も少なくてよいことからルータに掛かるコストが少ない．経路構築情報は長く保存できるので，DoS 攻撃後でも追跡を行うことができる．DoS 攻撃の種類ごとにシグネチャを保持させるので，あらゆる DoS 攻撃に対して効率よく経路の構築情報を蓄積できる．管理ホストがルータに問合せて行くことにより容易に経路の構築ができる．しかし，本方式は問合せのためのプロトコル定義を行う必要があり，通信プロトコルを悪用した攻撃に注意する必要がある．

表 1.提案方式と既存技術との比較

	ルータコスト	事後追跡	経路生成	経路構築	プロトコル定義
マーキング方式	○	○	×	×	○
Hash-based方式	×	△	○	△	△
提案方式	○	○	△	○	△

5. まとめ

パケットの MAC アドレスを利用することにより上位ルータを特定し，攻撃経路を構築できる MAC-based IP トレースバックについて提案した．本方式は上位ルータを確実に特定することが可能である．ルータはパケットの転送回数を計測するだけであり，処理コストが少ない．閾値を DoS 攻撃ごとに設定させることにより,あらゆる DoS 攻撃に対しても対応可能である．

MAC-based 方式を実装し，動作検証と性能測定を実施した結果，有効な方式であることが実証できた．

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.

MAC-based IPトレースバック方式の提案と実装

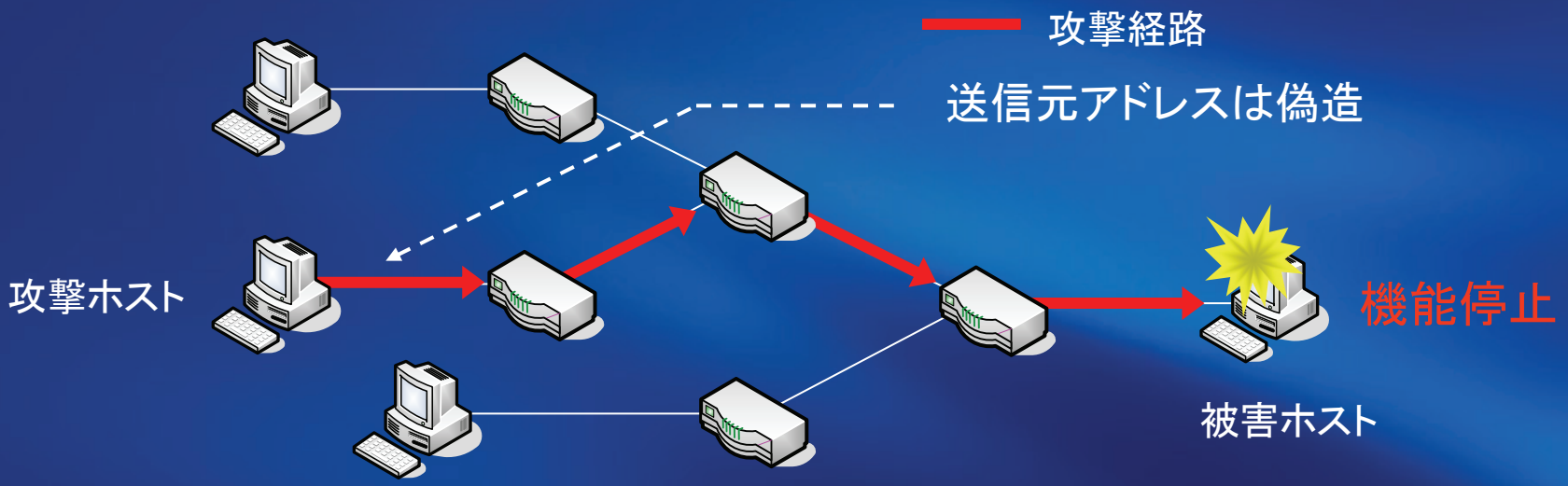
A Proposal of MAC-based IP Traceback and its Implementation

渡邊研究室

053432017　播磨　宏和

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：Denial of Service 攻撃）
    - 大量のパケットを送信
    - 身元の特定は困難

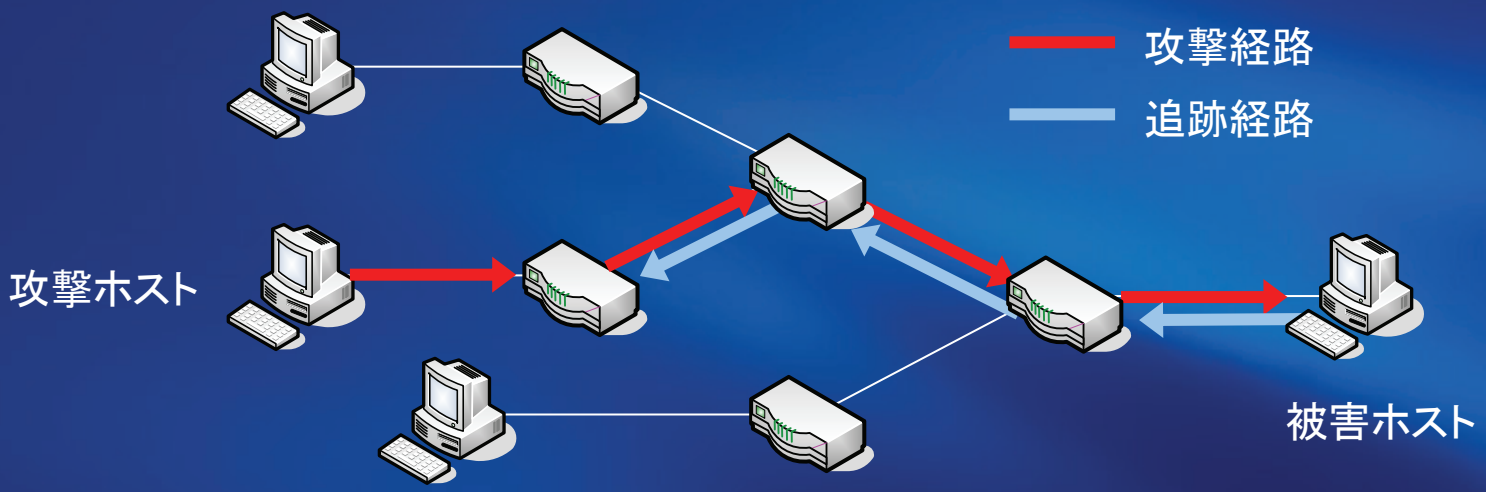


- 攻撃パケットの発信源を特定する技術

IPトレースバック技術

IPトレースバック技術とは

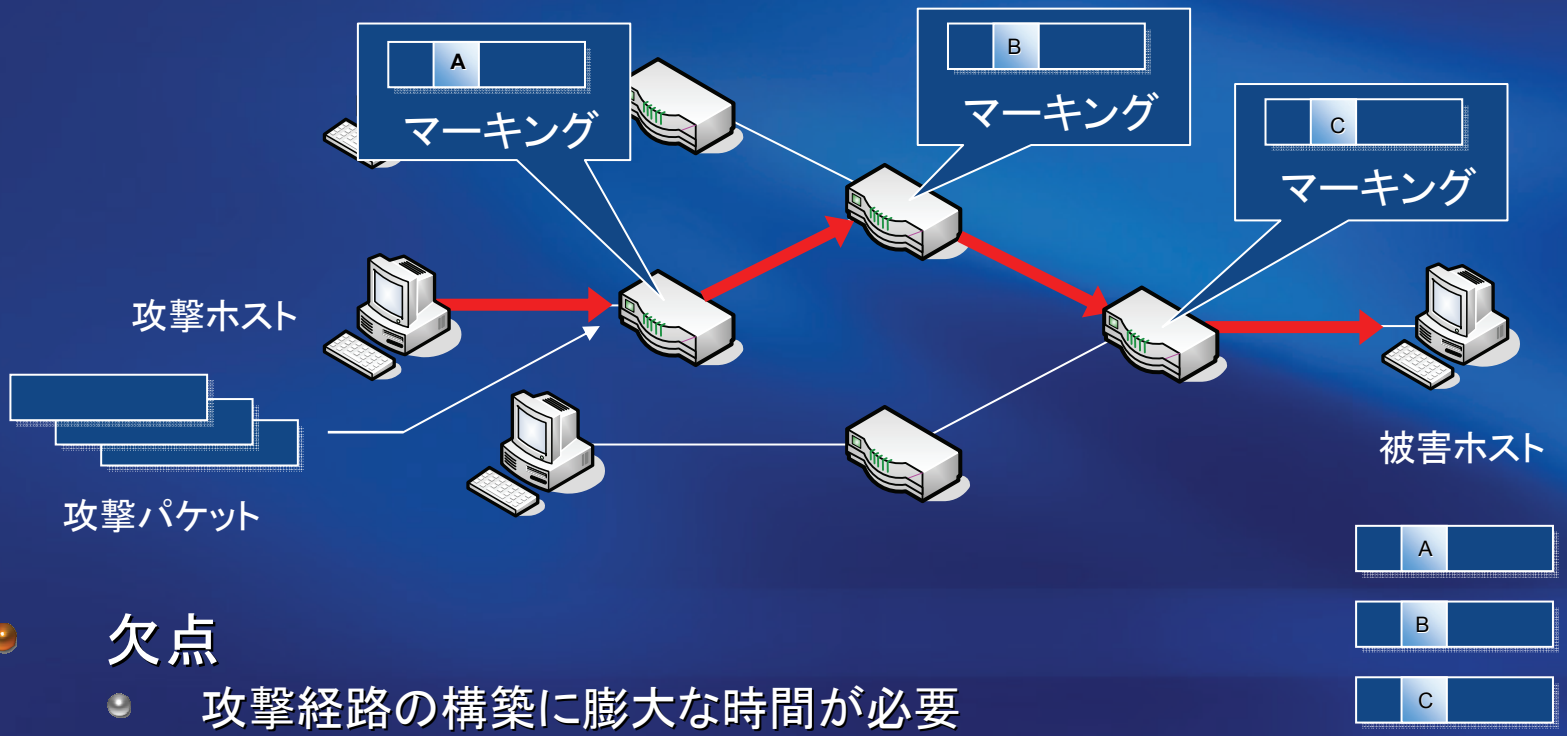
- IPトレースバック技術
  - ルータ機能の追加
  - 攻撃経路をさかのぼる



- 既存技術
  - マーキング方式
  - Hash-based方式

既存技術 マーキング方式

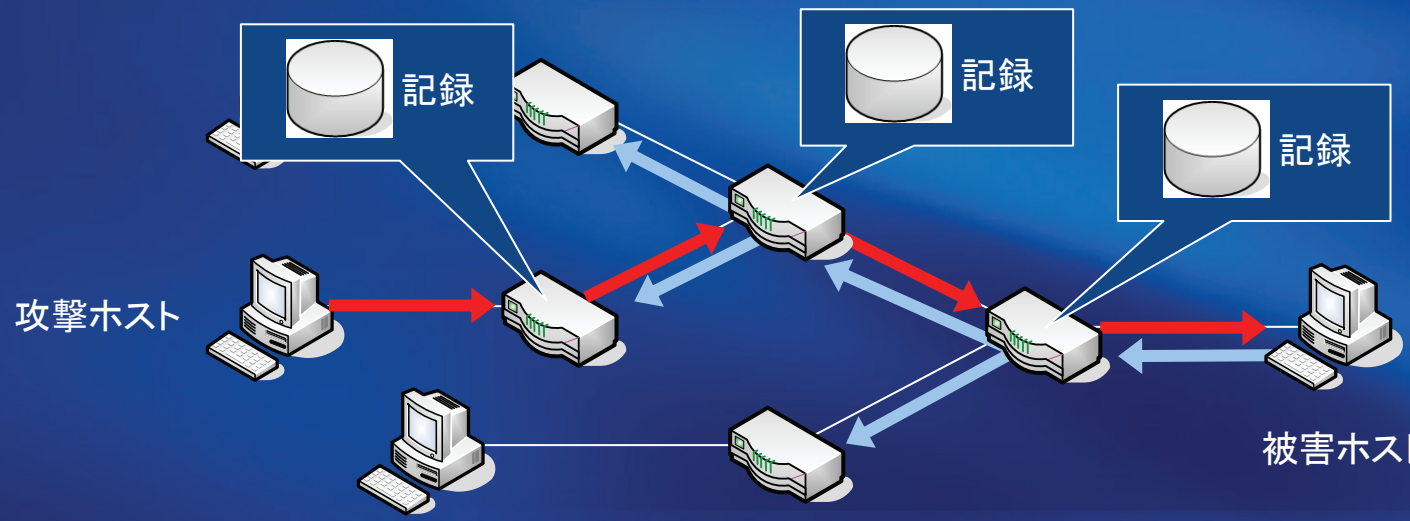
- 特定の確率でIPヘッダ内の未使用フィールドにマーキング
  - IPヘッダのIdentificationフィールド（16bit）
  - ルータのIPアドレス(32bit)を分割して挿入
- 収集したマーキングパケットから攻撃経路を再構築



- 欠点
  - 攻撃経路の構築に膨大な時間が必要
  - 偽造マーキングされる可能性がある

既存技術 Hash-based方式

- 全てのパケットに対し，ハッシュ関数を用いて
  パケットのログ（通過記録）を保存
  - IPヘッダの不変な部分
- ログ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

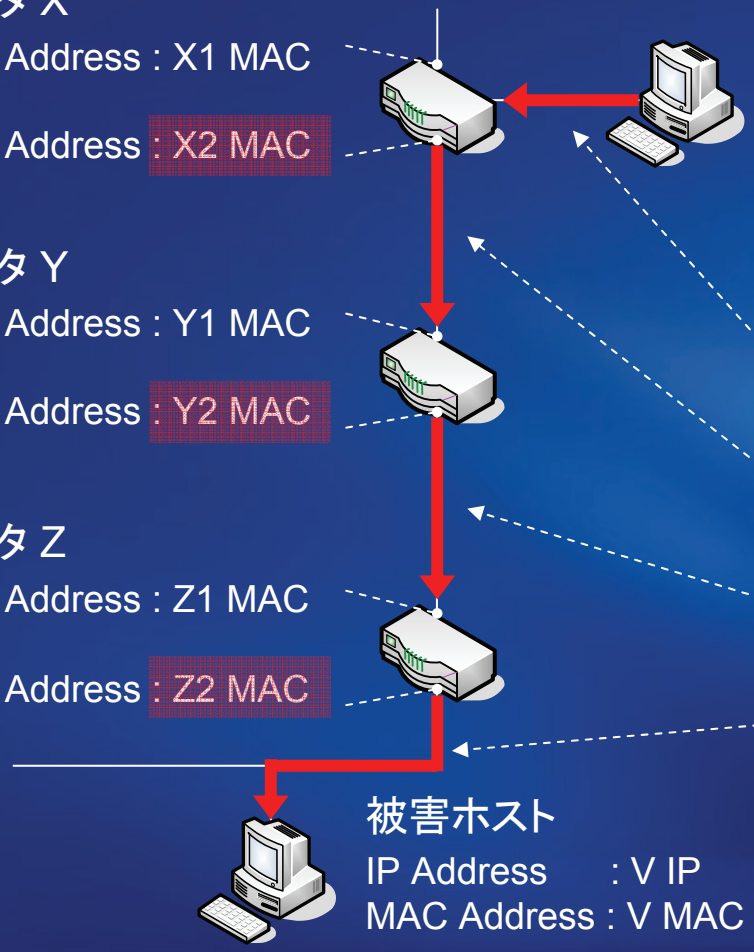


- 欠点
  - ルータに大きな記憶容量や高いハッシュ処理能力が必要

提案方式 MAC-based方式の特徴

- 偽造が困難なルータのMACアドレスに注目
  - 攻撃パケットを転送した上流ルータを確実に特定
- DoS攻撃の可能性がある場合にのみ経路情報を生成
  - 記憶容量・処理負荷の少ないトレースバック

MAC情報の利用方法



攻撃ホスト

IP Address : A IP → F IP
MAC Address : A MAC → 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	F MAC	F IP	V IP	・・・・・
Y1 MAC	X2 MAC	F IP	V IP	・・・・・
Z1 MAC	Y2 MAC	F IP	V IP	・・・・・
V MAC	Z2 MAC	F IP	V IP	・・・・・

攻撃経路

提案方式のルータ動作

- 単位時間あたりにおけるパケット転送回数をリアルタイムに計測
- 転送回数に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
  - MACアドレスを利用して上位ルータを特定
- DoS攻撃パケットを判別するシグネチャと閾値を関連付けて定義
  - 様々なDoS攻撃に対応

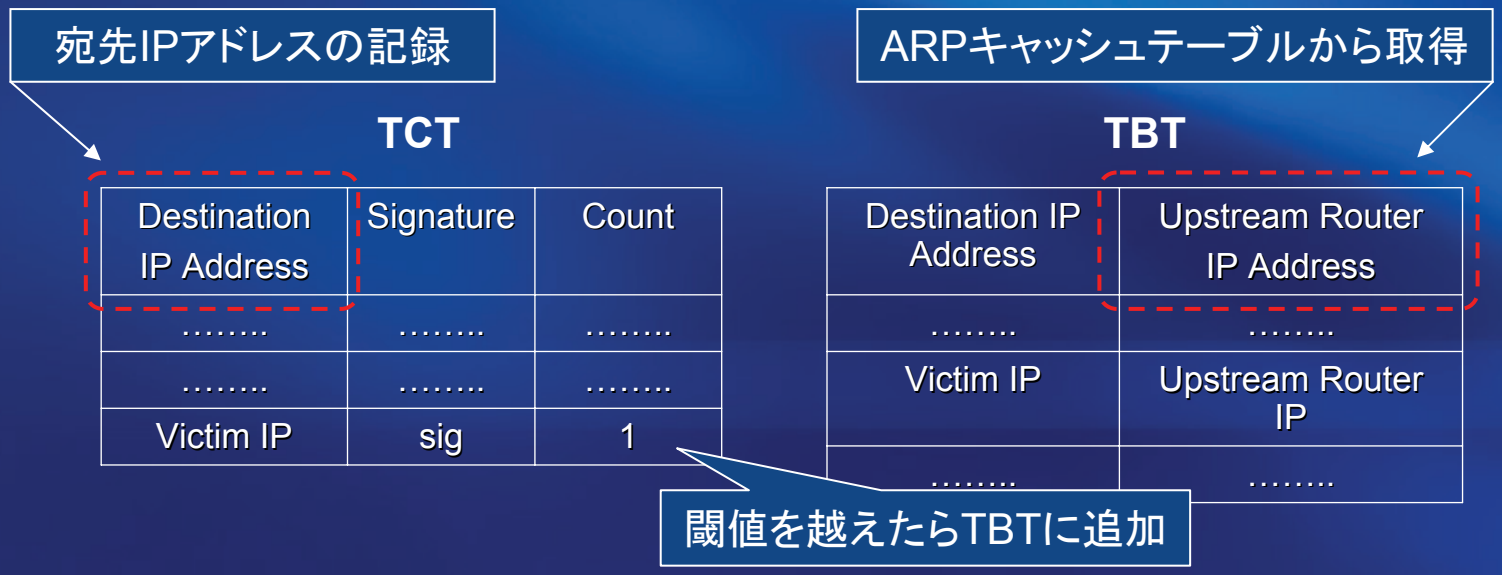
アドレス情報の記録

一時カウンタテーブル（TCT：Temporary Counter Table）

1. 宛先IPアドレスとシグネチャごとにカウント値を加算
2. 1秒単位の短い時間で消去
3. 特定の閾値を超えたらTBTにアドレスを転記

トレースバックテーブル（TBT：Trace Back Table）

1. 送信元MACアドレスから上位ルータのIPを取得
2. 宛先IPと上位ルータのIPを記録
3. 長期保存（数日単位）



閾値の設定

- DoS攻撃の種類で閾値は異なる
  - DoS攻撃ごとにシグネチャと閾値が定義されているリストを保持
  - シグネチャリストに従い、TCTの内容を記述

1. パケット検査
2. Signature List参照
3. DoS攻撃パケットと一致（pac = sig）
4. TCT記述

Signature List

Signature	Threshold
……..	
sig	1000
……..	

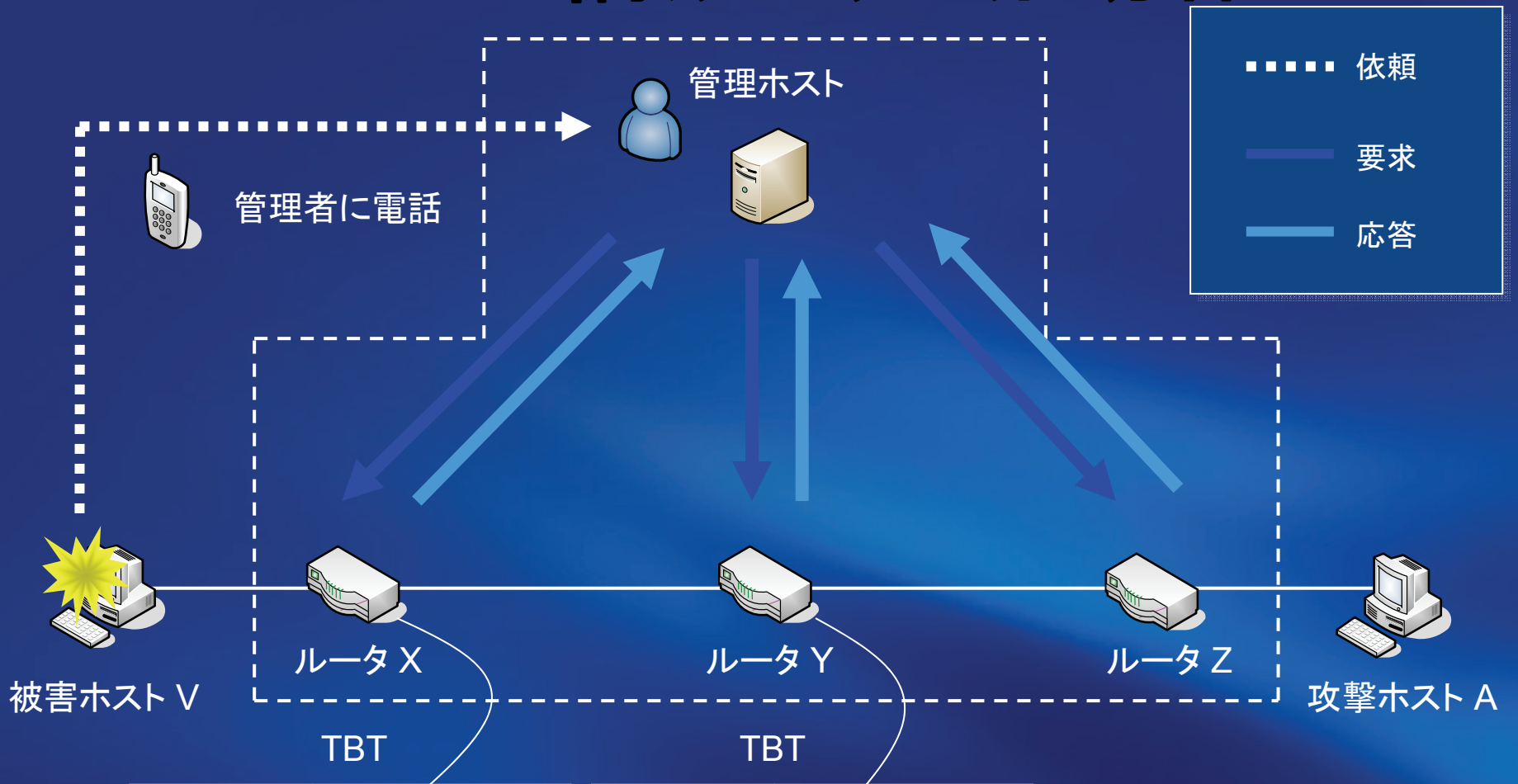
TCT

Destination IP Address	Signature	Count
……..	……..	……..
……..	……..	……..
Victim IP	sig	1

DoS攻撃を判別するシグネチャ

DoS攻撃	シグネチャ
SYN Flood	プロトコルタイプ：TCP，TCPフラグ：SYN
ACK Flood	プロトコルタイプ：TCP，TCPフラグ：ACK
Land	プロトコルタイプ：TCP， IPアドレス：宛先 = 送信元，ポート番号：宛先 = 送信元
HTTP GET Flood	プロトコルタイプ：TCP，宛先ポート番号：80，ペイロード：”GET”
UDP Flood	プロトコルタイプ：UDP
IKE DoS	プロトコルタイプ：UDP，宛先ポート番号：500
ICMP Flood	プロトコルタイプ：ICMP，ICMPタイプ：要求
Ping of Death	プロトコルタイプ：ICMP， IPフラグメント：IPオフセット * 8 + IPデータ長 > 65535

システムの構成と追跡動作



TBT

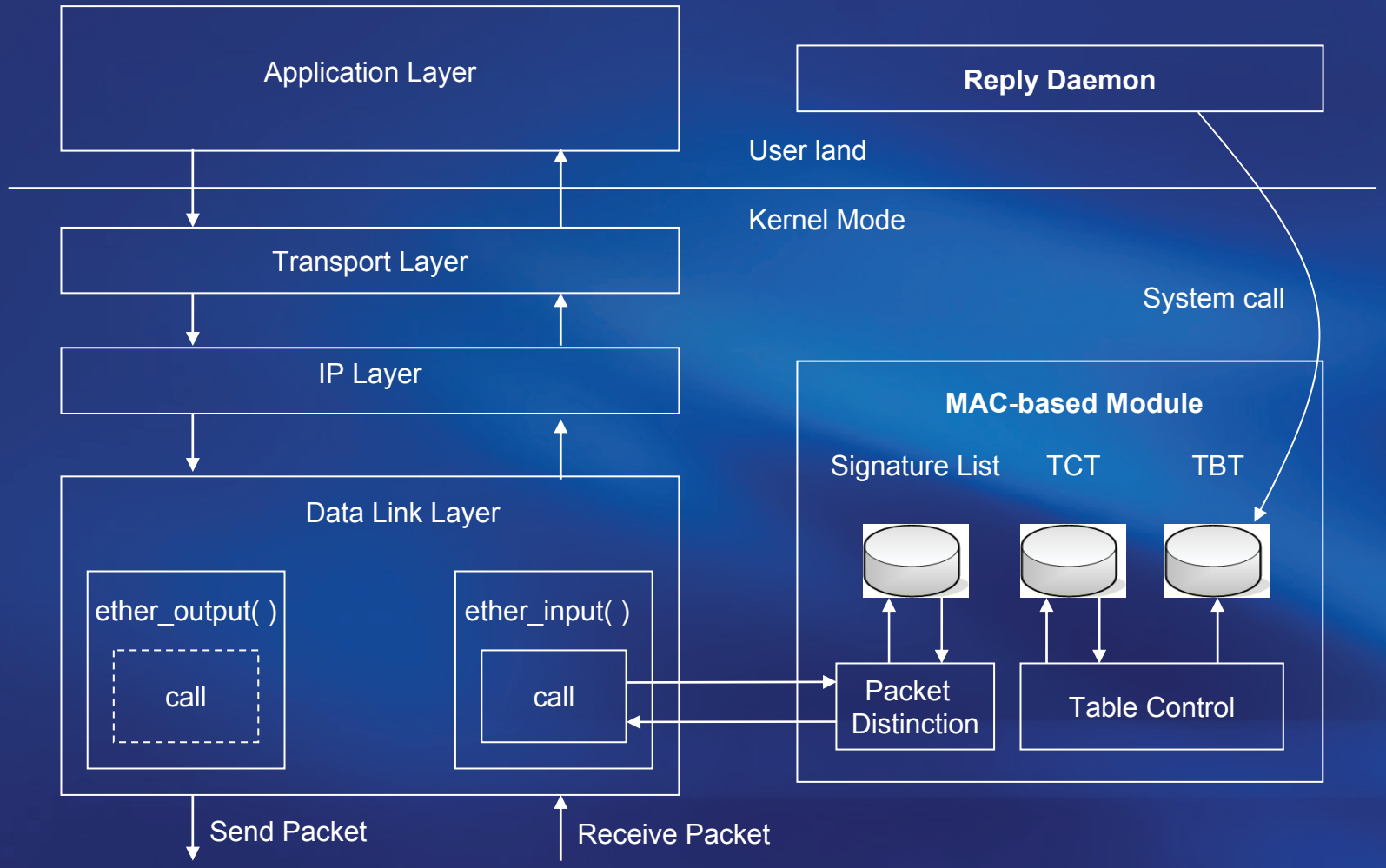
Destination IP Address	Upstream Router IP Address
V IP	Y IP
……..	……..
……..	……..

TBT

Destination IP Address	Upstream Router IP Address
……..	……..
V IP	Z IP
……..	……..

MAC-Basedプログラムの実装

- FreeBSD 5.3に実装



性能測定

- ルータの中継処理に与える影響
  - FTPを利用したスループット測定
    - 200MByteのデータ 転送
  - netperfを利用したパケット中継処理測定
    - 18～1,472ByteサイズのUDPパケット

測定構成

100base-TX接続

性能測定 結果

FTPを利用したスループット測定

	スループット値
実装なし	72.22 Mbps
実装あり	72.18 Mbps
減少比	0.06 %

パケット処理能力

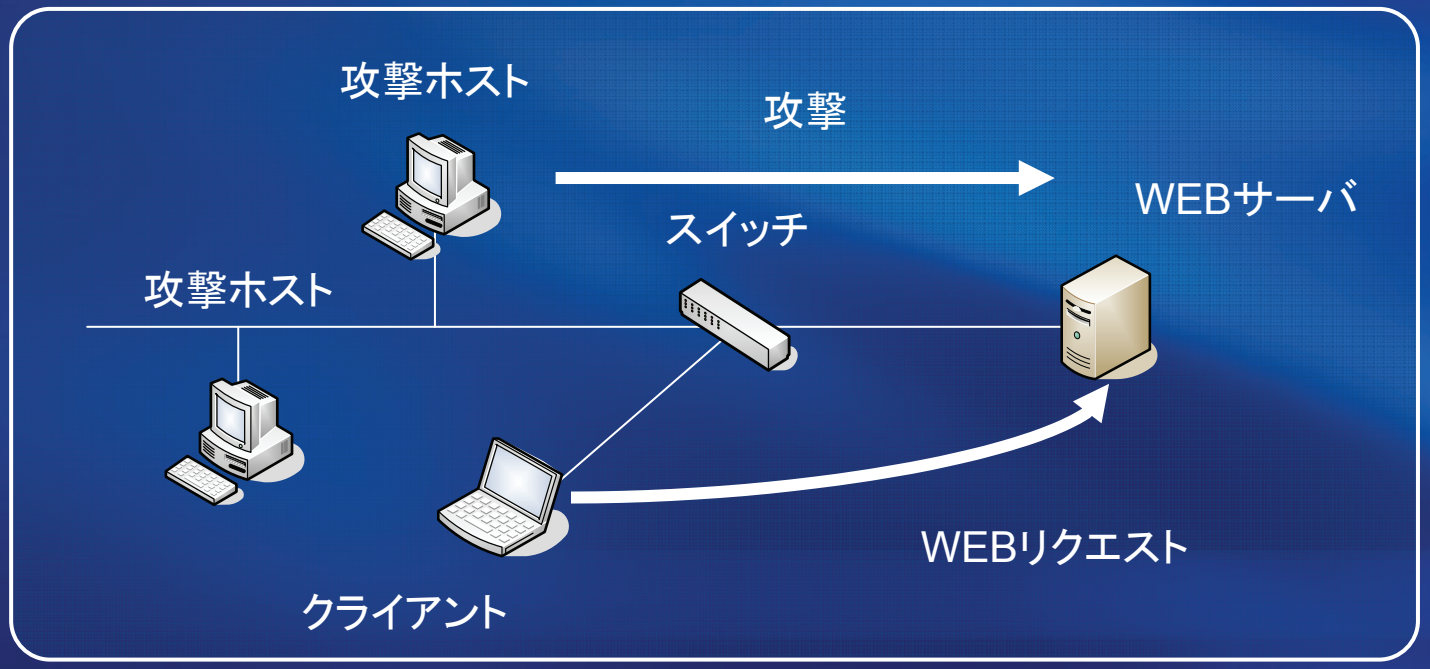
データサイズ [byte]	18	512	1024	1472
実装なし [PPS]	75755	21624	11466	8126
実装あり [PPS]	75109	21623	11463	8120
劣化率 [%]	0.85	0.05	0.03	0.07

- 性能劣化は1%未満
- MAC-basedシステムを実装させても、
  性能の低下きわめて小さい

閾値の調査

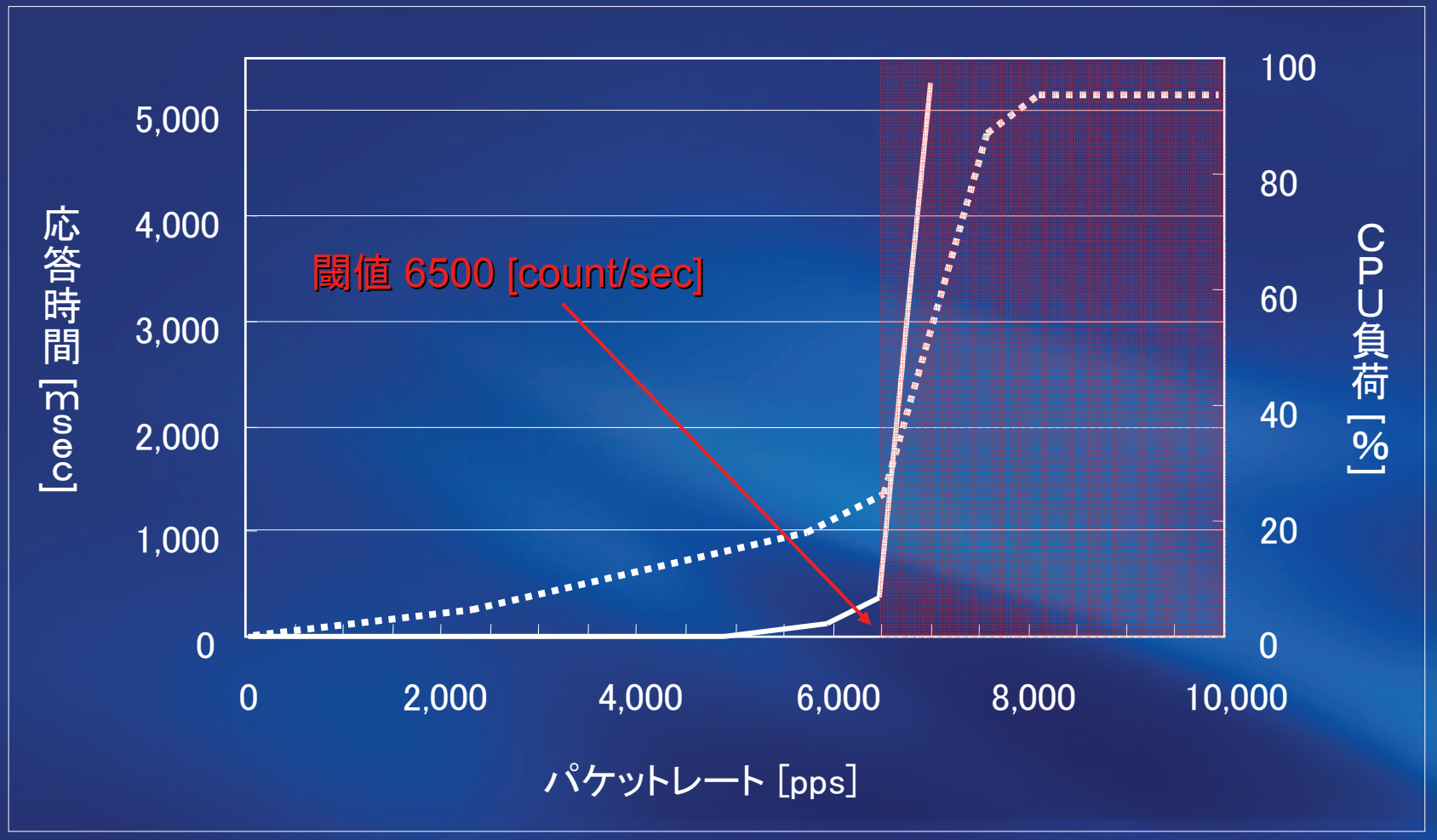
- DoS攻撃配下においてサーバが使用不可になる閾値
- WEBサーバにリクエスト要求
- 攻撃レートを増加
  - 応答時間，CPU負荷を測定

測定構成



100base-TX接続

SYN Flood攻撃に対する閾値



閾値の一覧

DoS攻撃名	閾値 [count/sec]
SYN Flood	6500
ICMP Flood	8100
HTTP GET	1250
Ping of Death	1
WinNuke	1

既存技術と提案方式の比較

	ルータコスト	解析量	DoS識別
マーキング方式	○	×	×
Hash-based方式	×	○	○
提案方式	○	○	○

提案方式の特徴

- **ルータコスト**
  - 高いハッシュ計算能力，大きな記憶容量を必要としない
- **解析量**
  - 上流ルータを確実に特定しているため，経路構築が容易
- **DoS識別**
  - シグネチャにより，様々なDoS攻撃の識別が可能

むすび

- まとめ
  - MAC-based IPトレースバック方式について提案
    - MAC情報を利用して上位ルータを特定
    - シグネチャを定義することで様々なDoS攻撃に対応
  - MAC-basedモジュールを実装、性能測定を行った
    - モジュール追加による性能劣化は極めて小さい
- 今後の課題
  - 攻撃者が多数存在するDDoS（Distributed DoS）攻撃の対応について検討

おわり

参考

警察庁

「平成17年上半期（1～6月）におけるbotnet観測システム観測結果」

平成17年10月25日

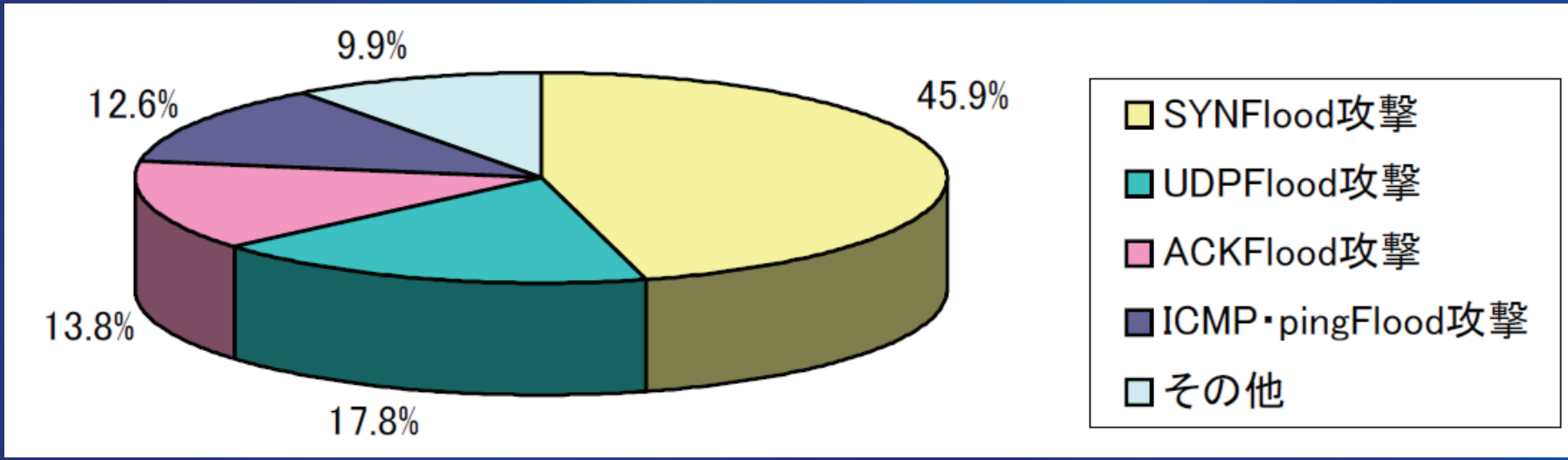


図8. 攻撃活動命令手段別比率

（P. 8 ）