MAC アドレスを用いた IP トレースバック技術の提案

01j078　播磨 宏和
渡邊研究室

1. はじめに

インターネット人口の増大に伴い，セキュリティにかかわる被害規模が拡大している．その中でもサービス不能攻撃（DoS 攻撃）は防御が難しく，巧妙に身元を隠してシステムを機能不全にしてしまう．この攻撃に対して攻撃者の身元を探索する技術として IP トレースバックが盛んに研究されている[1]．しかし，これまでの IP トレースバックは大量の攻撃パケットを会席する必要があったり，高性能な CPU が必要となるなどの課題がある．

本研究ではルータに残された攻撃パケットの MAC アドレス情報から攻撃ルートの上位ルータを特定し，攻撃源までの経路を追跡するトレースバック方式を提案する．

2. 既存の IP トレースバック技術とその課題

Input-debugging 方式はルータのデバッグ機能を利用したものであるが，近年攻撃ツールの発達により攻撃パケットの特徴抽出が困難になっている．

逆探知パケットおよび，マーキング方式は各ルータにおいて，通過するパケットについてある確率で経路情報の一部をのせる方式であるが，攻撃パケット数が少ない場合には，発信源を特定できない．

Hash トレースバック方式はパケットのダイジェストを利用するので攻撃パケットが 1 個あれば発信源を特定できるが，大きな記憶容量や高いハッシュ処理能力が必要とされるため，コスト面において不利になる．

3. 提案方式

提案方式は既存のトレースバック技術とは異なり，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．

DoS 攻撃では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 アドレスの組アドレス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．

提案方式では図 1 のように情報を記録するテーブル 1，テーブル 2 を保持しており，それぞれカウント値が設けられている．

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．このテーブルは一定間隔で消去する．カウント値が一定時間内にある閾値を超えた場合，その時のパケットの IP アドレスと MAC アドレスの組をテーブル 2 へと記録する．

テーブル 1

Destination IP Address	COUNT値
……	……
……	……
M_ip	73
V_ip	1015
……	……
N_ip	28

テーブル 2

Destination IP Address	Source MAC Address	COUNT値
……	……	……
V_ip	P_mac	25
V_ip	X_mac	34
……	……	……
……	……	……
V_ip	O_mac	4

図 1．テーブルの保持

このようにしてテーブル 2 には上流ルータの MAC アドレスが記録される．テーブル 2 は長時間保持する．

被害ホストは攻撃を受けると，MAC アドレスを頼りに上流ルータに対して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，受信したルータはテーブル 2 を用いて被害ホストの IP アドレスから送信元 MAC アドレスを割り出す．

次にルータは自分自身の IP アドレス情報を加え，割り出した MAC アドレスのうちカウント値が最も大きなルータに対して問い合わせを行う．各ルータが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問合わせていく．

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(図 2).

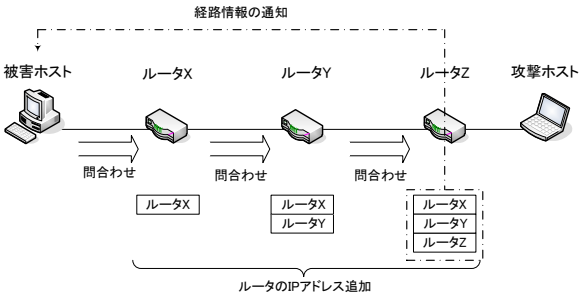


図 2．問合せパケット

4. むすび

本研究では，MAC アドレスを用いた IP トレースバックの提案を行った．今後は本方式を実装することにより本方式の有効性やルータにかかる負荷などについて既存技術と比較していく．

参考文献

[1]門森 雄基，大江 将史：IP トレースバック技術，IPSJ Magazine Vol.42(Dec.2001)

[2]岡崎 直宣，河村 栄寿，朴 美娘：サービス不能攻撃の経路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,No12(Dec.2003)

MACアドレスを用いた IPトレースバック技術の提案

The proposal of IP trace back technology using MAC Address

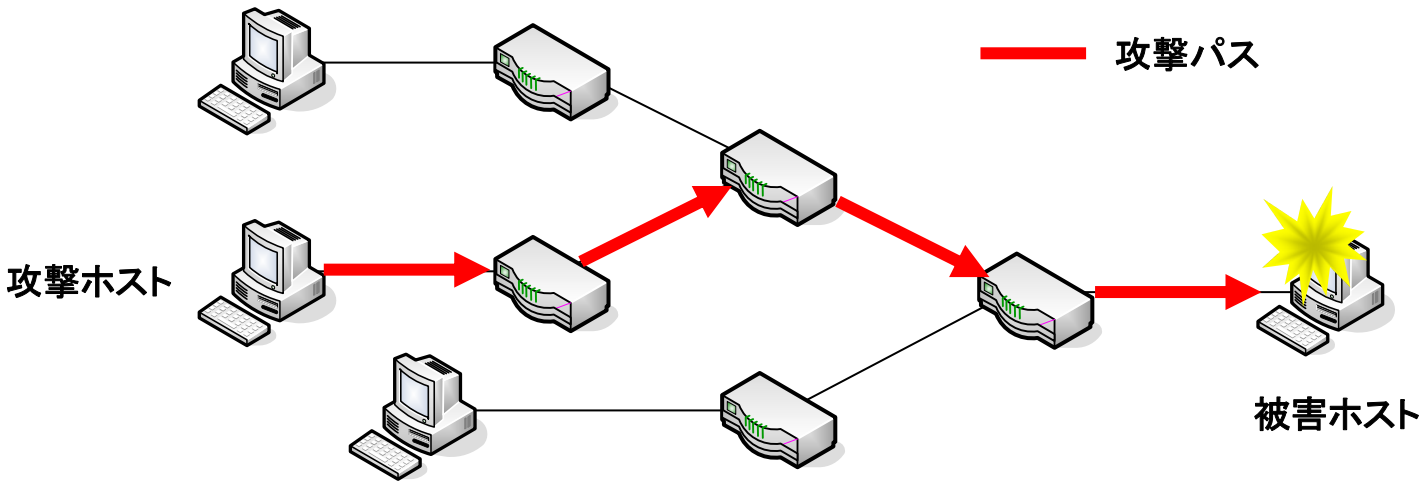
名城大学理工学部

渡邊研究室

01J078　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

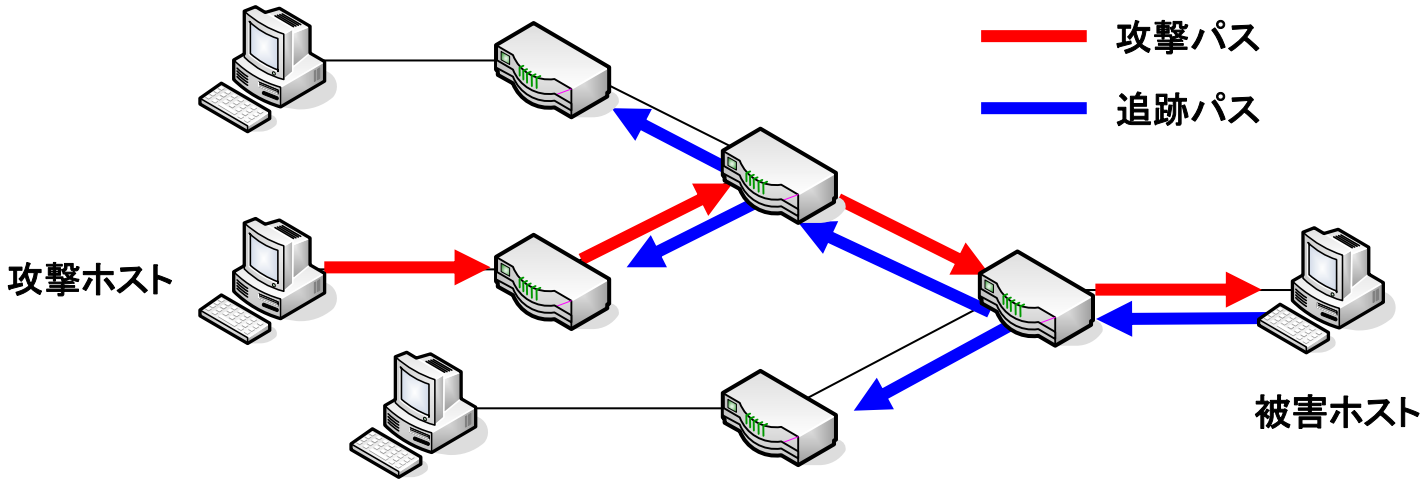


- 攻撃パケットの発信源を特定する手段が必要

IPトレースバック技術

IPトレースバック技術とは

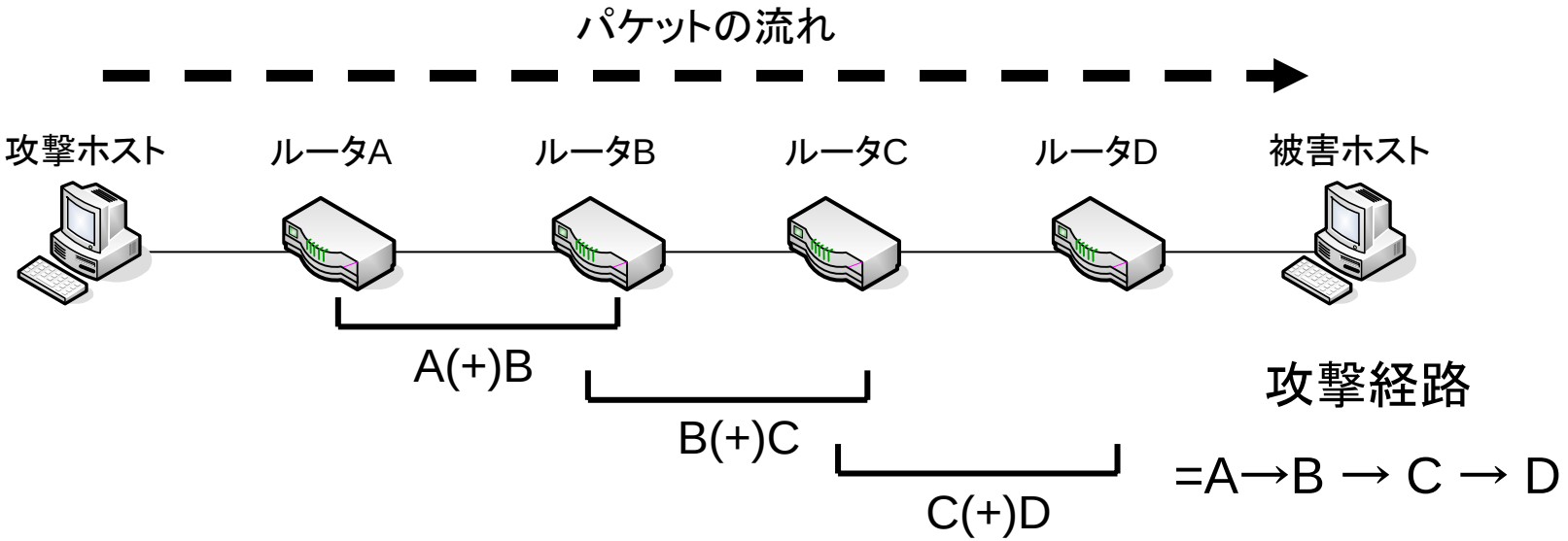
- IPトレースバック技術
  - ルータ機能の追加



- 既存技術
  - Input-debugging方式
  - ICMPトレースバック方式
  - マーキング方式
  - Hash-based方式

既存技術　～マーキング方式～

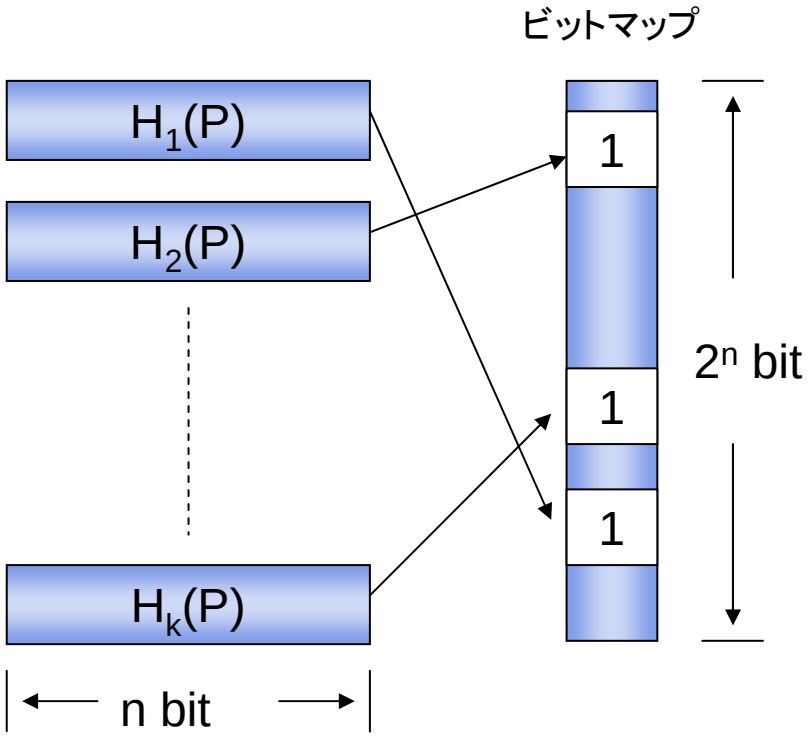
- IPヘッダ内の未使用ビットにマーキング
  - IPヘッダ（Identificationフィールド）
  - 2つのルータのアドレス
- 収集したマーキングパケットから攻撃経路を再構築



- 欠点
  - 攻撃経路の構築に膨大な時間が必要
  - アプリケーションとの親和性が低い

既存技術　～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確認することで攻撃経路を再構築



IPヘッダ

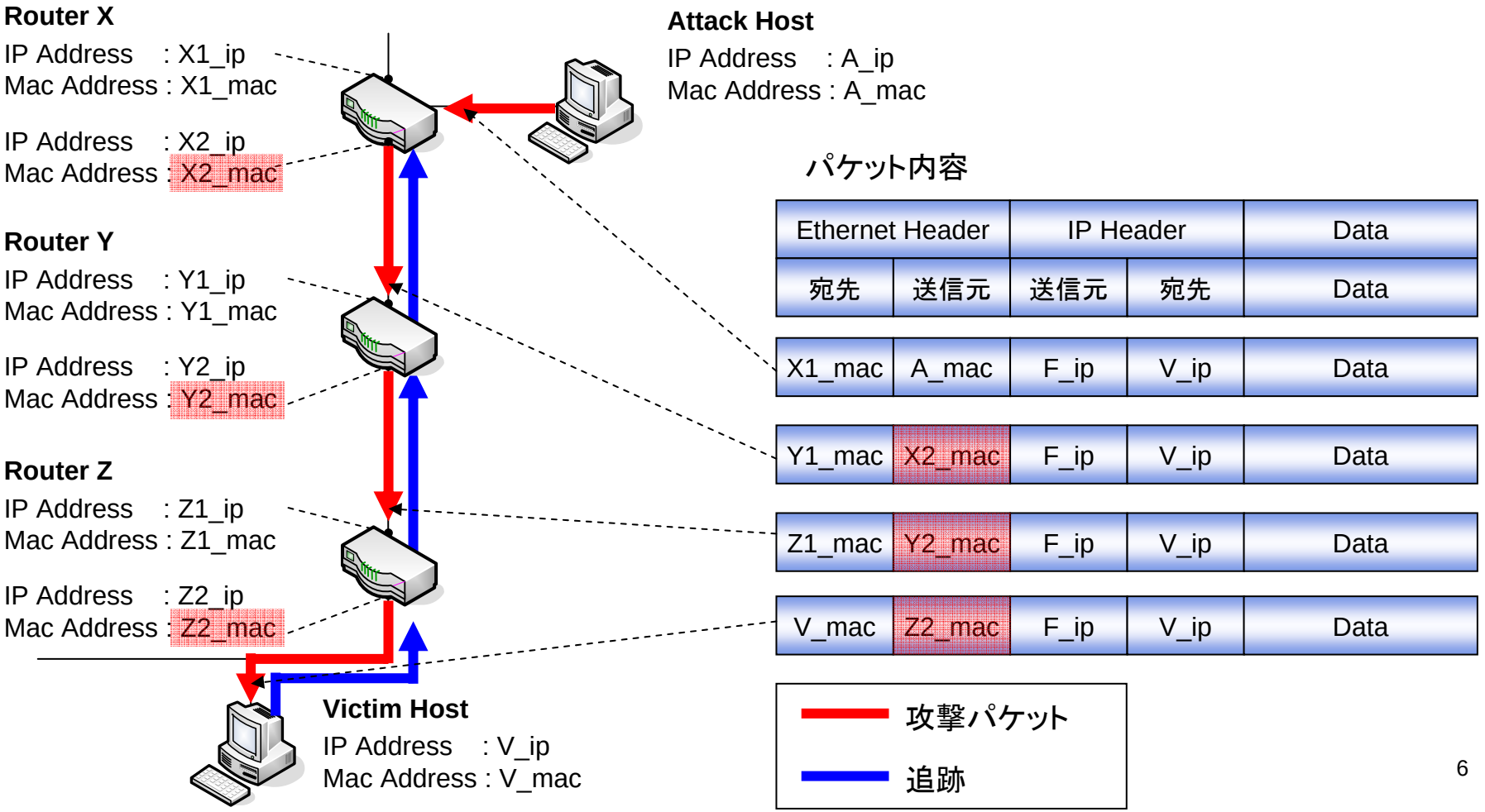
不変な部分

Version	Header Lenght	TOS	Total Lenght
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

提案技術の原理

- これまでのIPトレースバック技術とは異なる手法
- ルータに記録された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



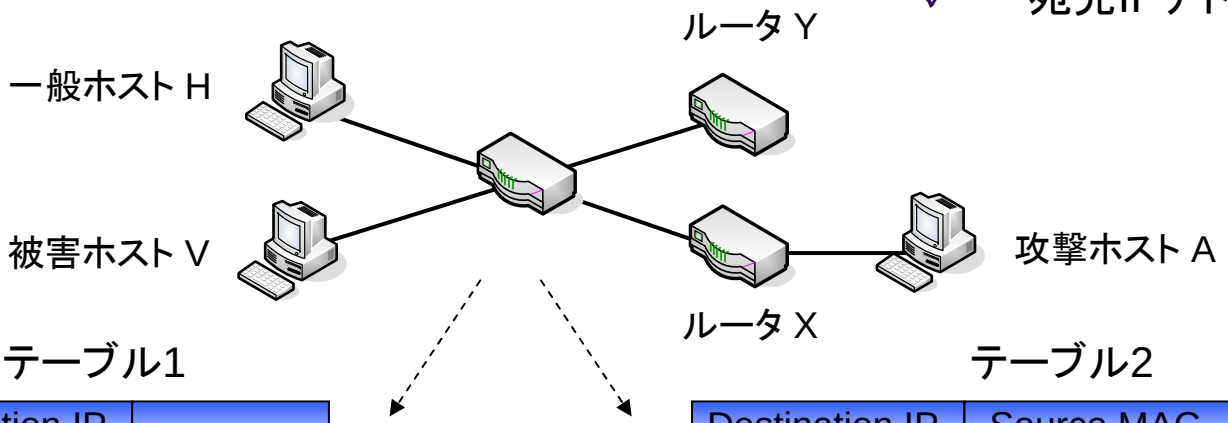
動作概要

- 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. カウント値の加算
  3. 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

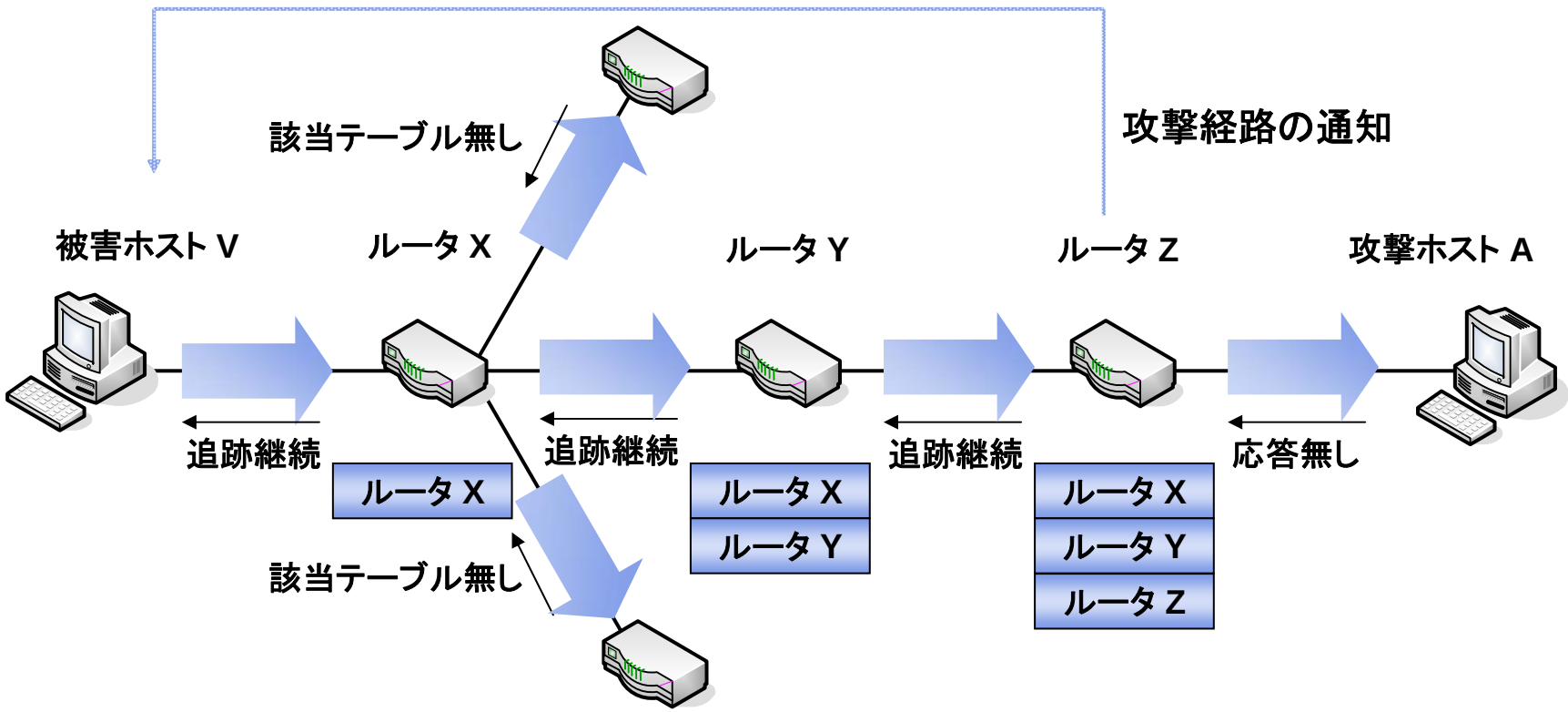
Destination IP Address	COUNT値
·····	·····
V_IP	1001
H_IP	
·····	·····

閾値:1000

テーブル2

Destination IP Address	Source MAC Address	COUNT値
V_IP	Y_MAC	3
·····	·····	·····
V_IP	X_MAC	716
·····	·····	·····

攻撃経路の追跡



問合せパケットに自分自身のIPアドレスを追加

攻撃ホストからは応答が無い

エッジルータは被害ホストに攻撃経路を通知する

評価

- 利点
  - ルータが自律的に動作 → 管理コストは低い
  - パケットに改良を加えない → 親和性問題が発生しない
  - 複雑な動作を行わない → ルータに掛かる負担は軽い

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
  - 今後は、提案システムを実装して有効性を確認するとともに既存技術との比較を行う
- 現在の状況
  - Windows OSにて擬似的なテーブル作成プログラムを開発
  - 情報の格納、上位ルータの特定を確認した
- 今後の課題
  - 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

おわり