本資料について

- 本資料は下記論文を基に作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文、参考資料を参照してください。

- 題目：IP Traceback Using DNS Logs against Bots
- 著者：Keisuke Takemori
  Masahiro Fujinaga
  Toshiya Sayama
  Masakatsu Nishigaki

IP Traceback Using DNS Logs against Bots

名城大学　理工学部
渡邊研究室
080425210　戸田尚希

背景

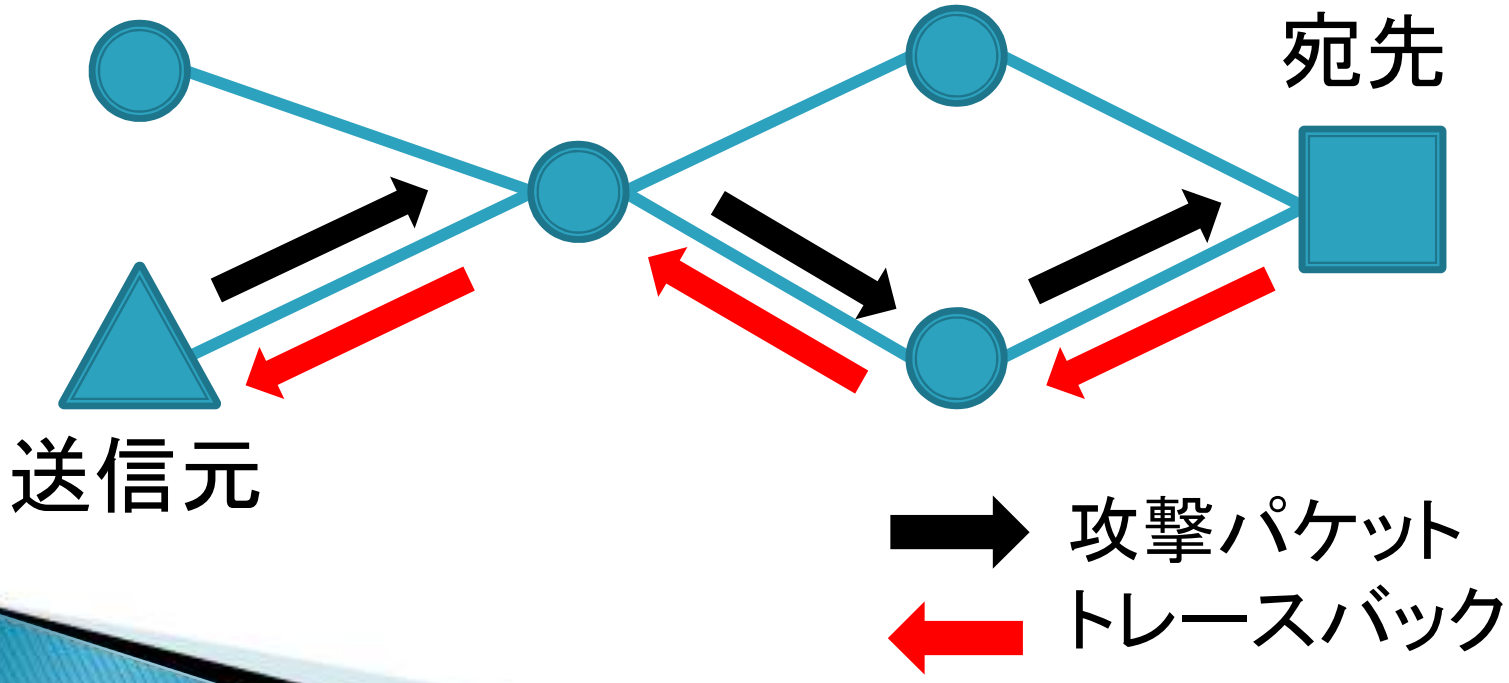
- IPスプーフィング攻撃がインターネットにおける重要な問題になっている

- IPスプーフィングとは？
  - 攻撃元を隠ぺいするために、偽の送信元IPアドレスを持ったパケットを作成し送ること
  - 近年では、DoS攻撃の際に併用

パケットの送信元を突き止めたい

IPトレースバック

- 送信元IPアドレスが詐称された通信の送信元を突き止める技術

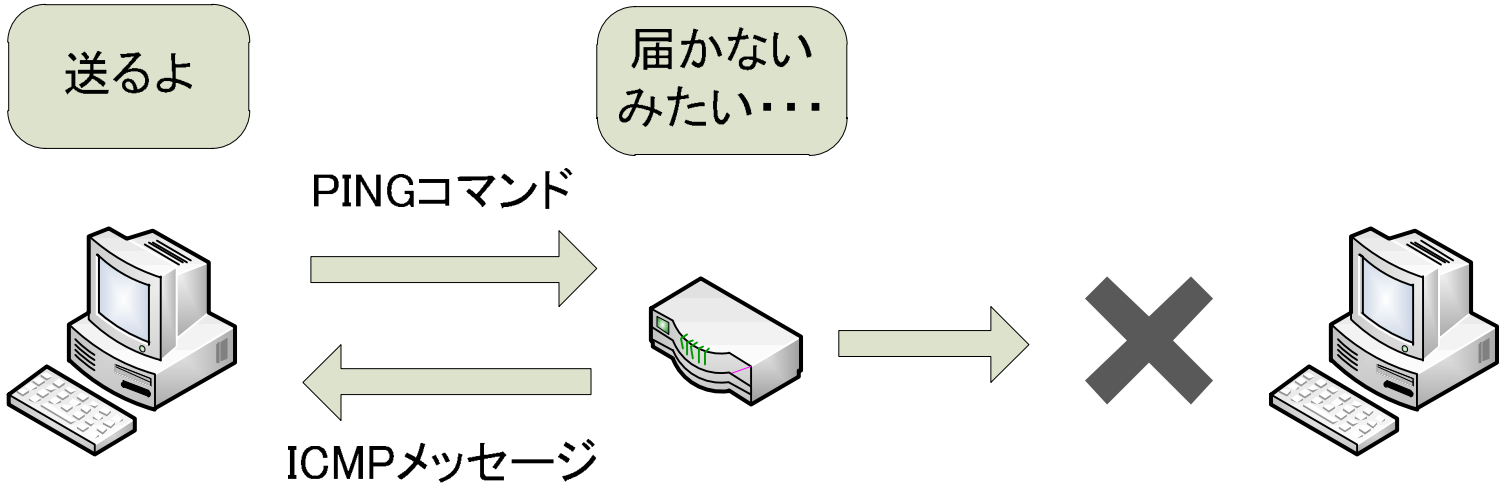


IPトレースバックの既存技術

- ICMPトレースバック方式
- パケットマーキング方式
- ハッシュベーストレース方式

ICMPトレースバック方式(1)

- ICMPとは？
  - インターネット制御通知プロトコル
  - Pingが利用しているプロトコル



ICMPトレースバック方式(2)

- 全てのルータは、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

- 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

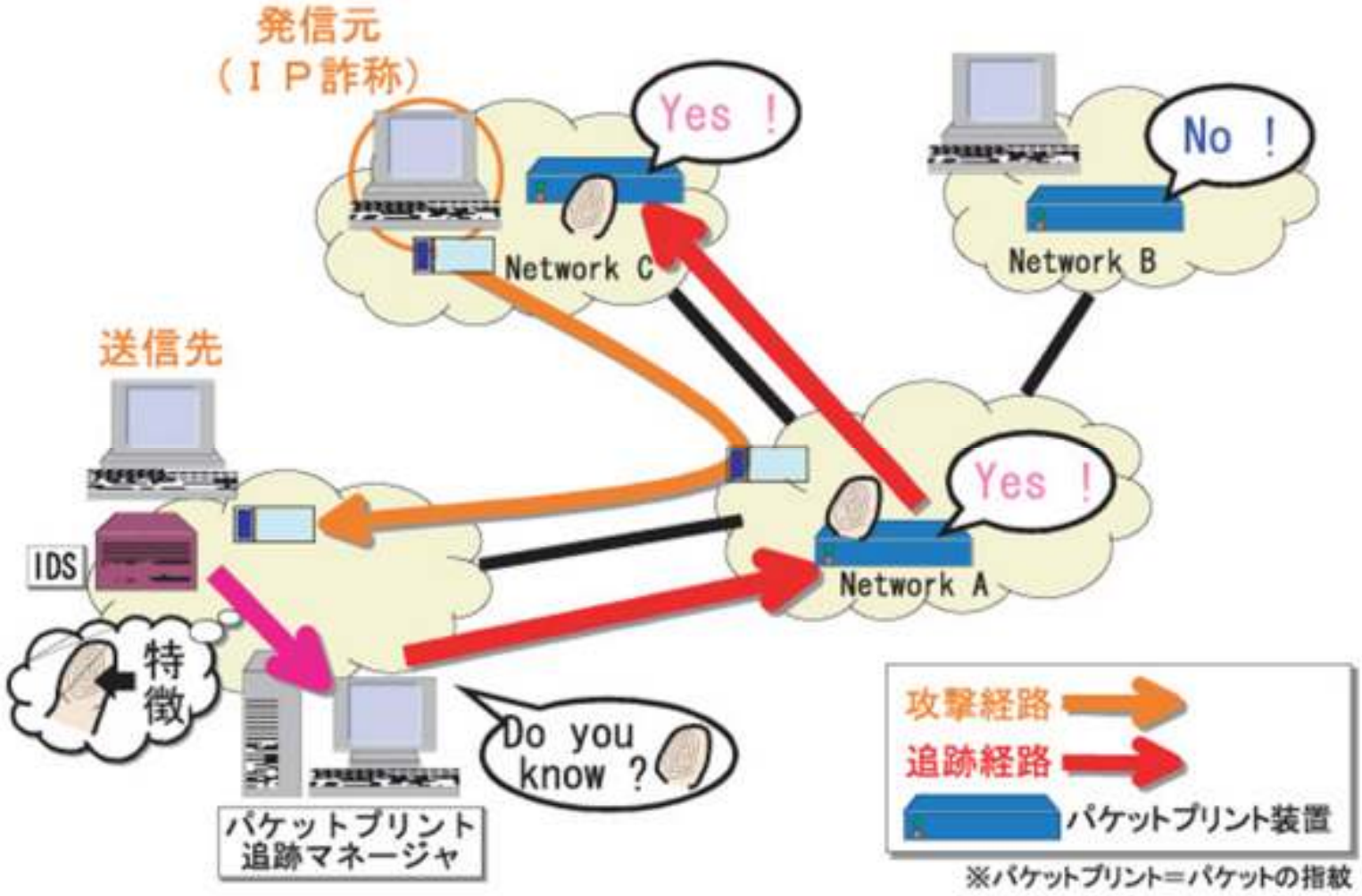
ICMPトレースバック方式(3)

- メリット
  - 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
- デメリット
  - ICMPを拒否しているルータやFirewallの存在により、情報が被害ホストに届かない
  - 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

パケットマーキング方式

- ルータがある一定の確率で、IPヘッダ内の未使用ビットにマーキングを行い、収集したパケットから攻撃経路を再構築する
- メリット
  - 追加のパケットを必要としないので、ネットワークに負荷をかけずに追跡を実行できる
- デメリット
  - 追跡にはマーキングしたパケットが大量に必要
  - 経路構築の計算量が膨大になる

ハッシュベーストレース方式(1)



ハッシュベーストレース方式(2)

- メリット
  - ルータが転送する全てのパケットに対して、ハッシュ値を記録するため、攻撃パケットが1個さえあれば、発信源を特定可能
  - パケットを加工しないため、既存のネットワークプロトコルや設備がそのまま利用可能
- デメリット
  - 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

本論文の提案

- タイトル
  - 「IP Traceback Using DNS Logs against Bots」

「ボットに対するDNSログを利用した
IPトレースバック」を提案

- DNSログとは？

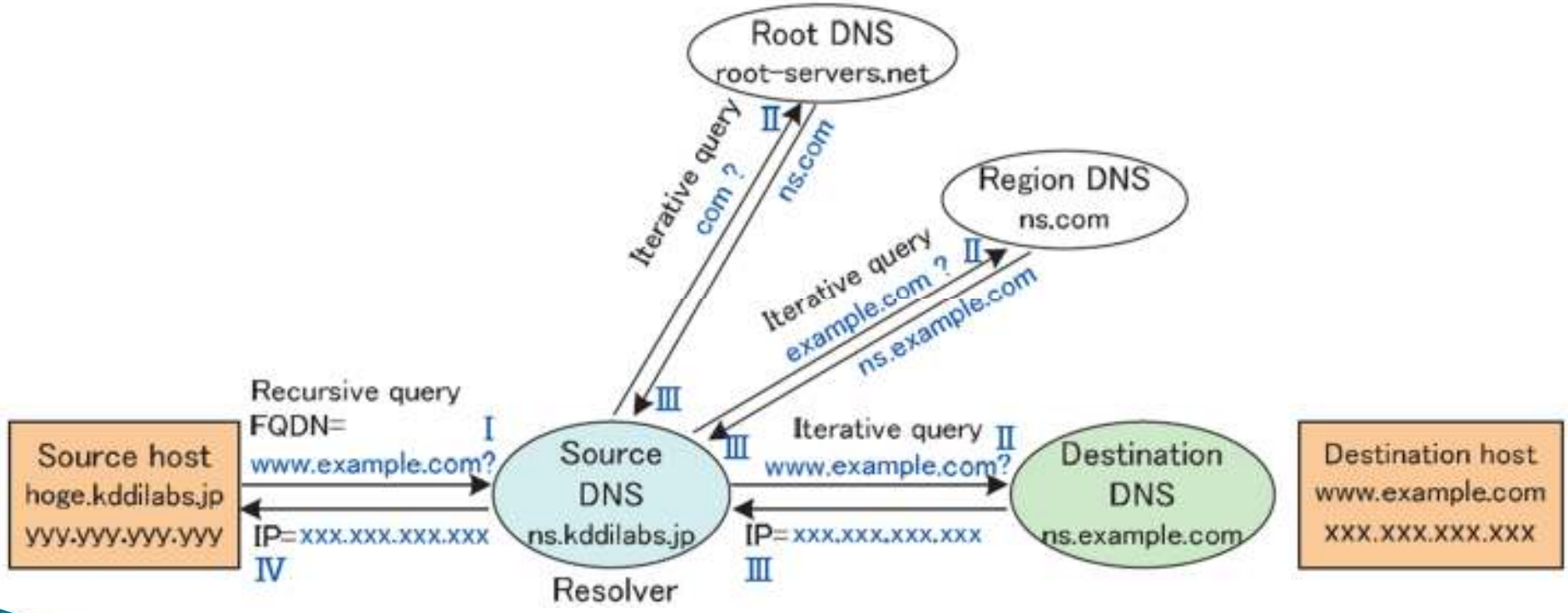
DNSログ

- DNS(Domain Name System)とは？
  - インターネットにおけるドメイン名とIPアドレスの対応づけを管理する役割

- DNSログとは？
  - DNSクエリの記録
  - クライアントからサーバへの「FQDN→IPアドレス」、「IPアドレス→FQDN」の問い合わせの記録

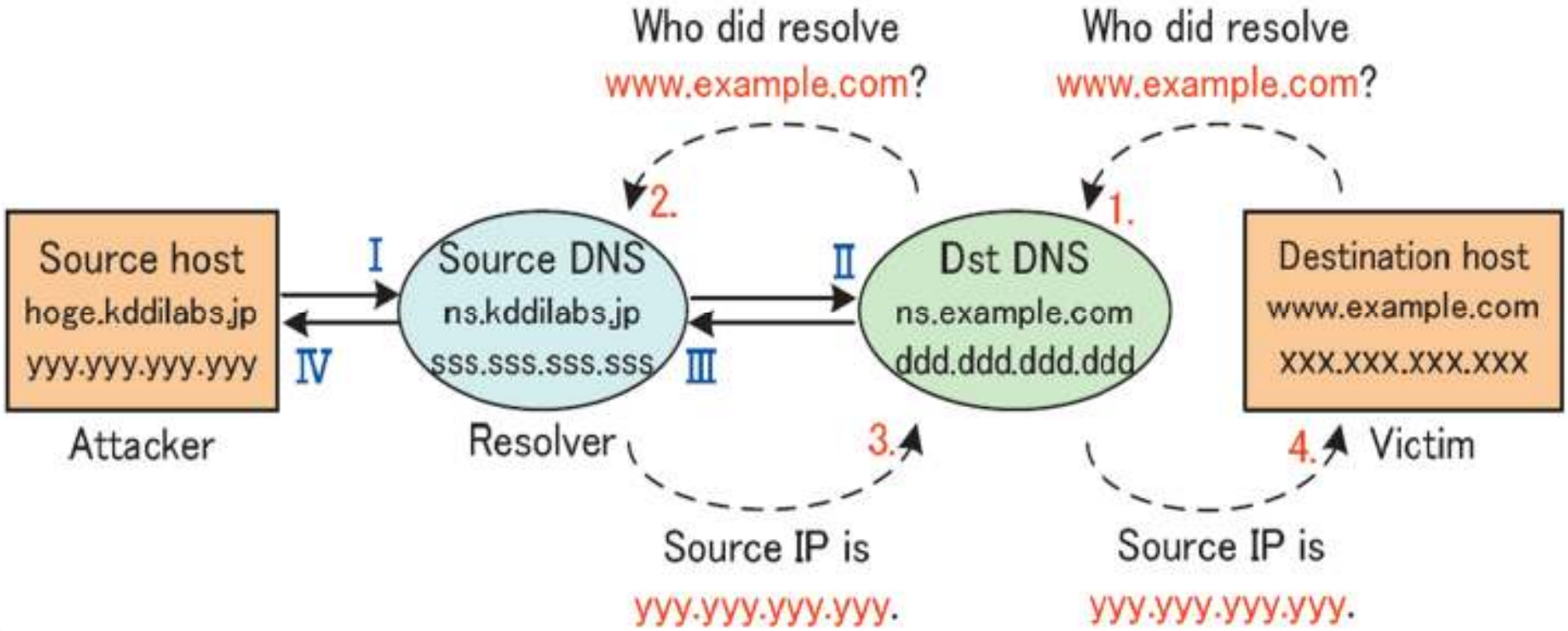
典型的なDNSクエリモデル

- 宛先DNSは被害ホストである宛先ホストの情報が登録されている

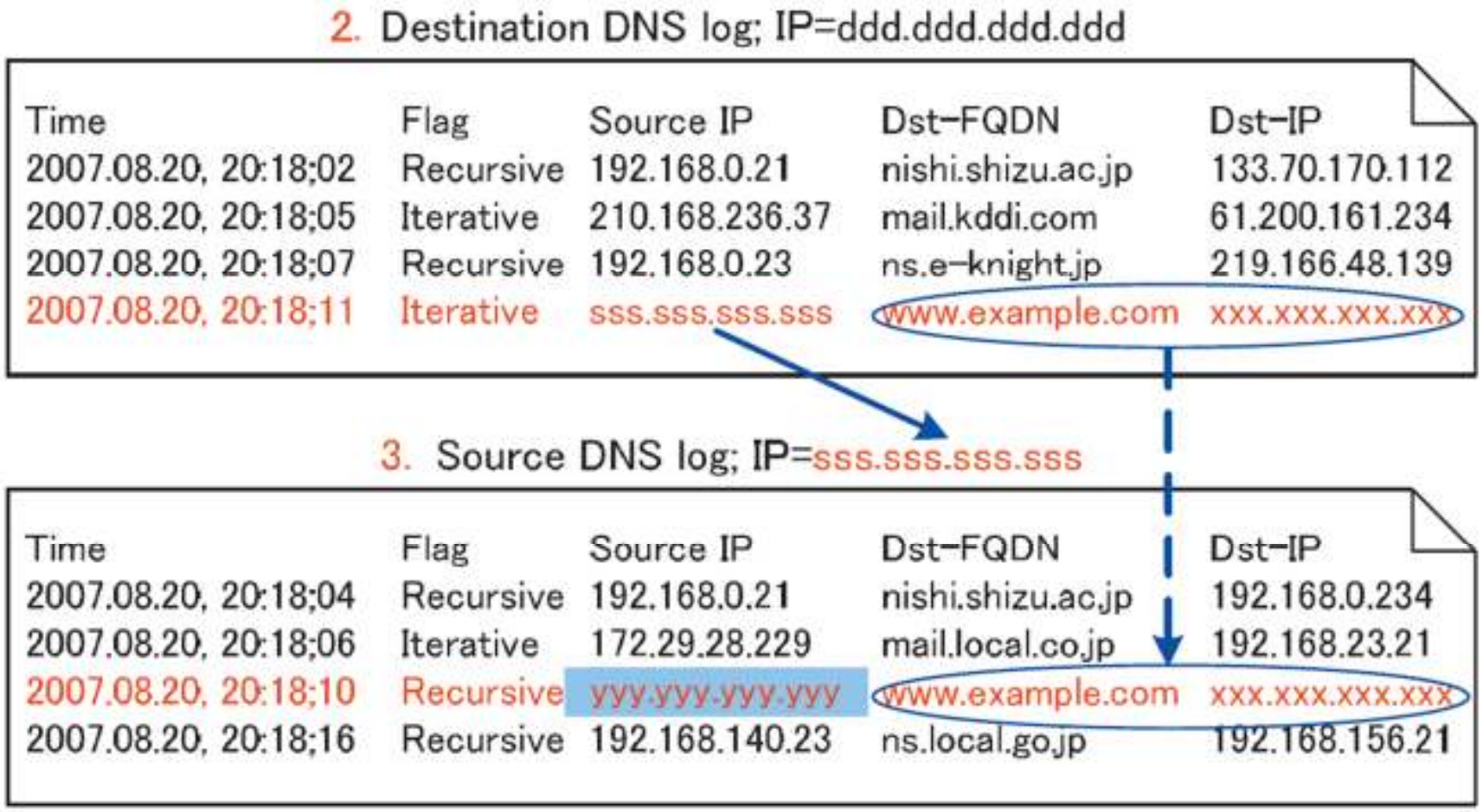


提案方式

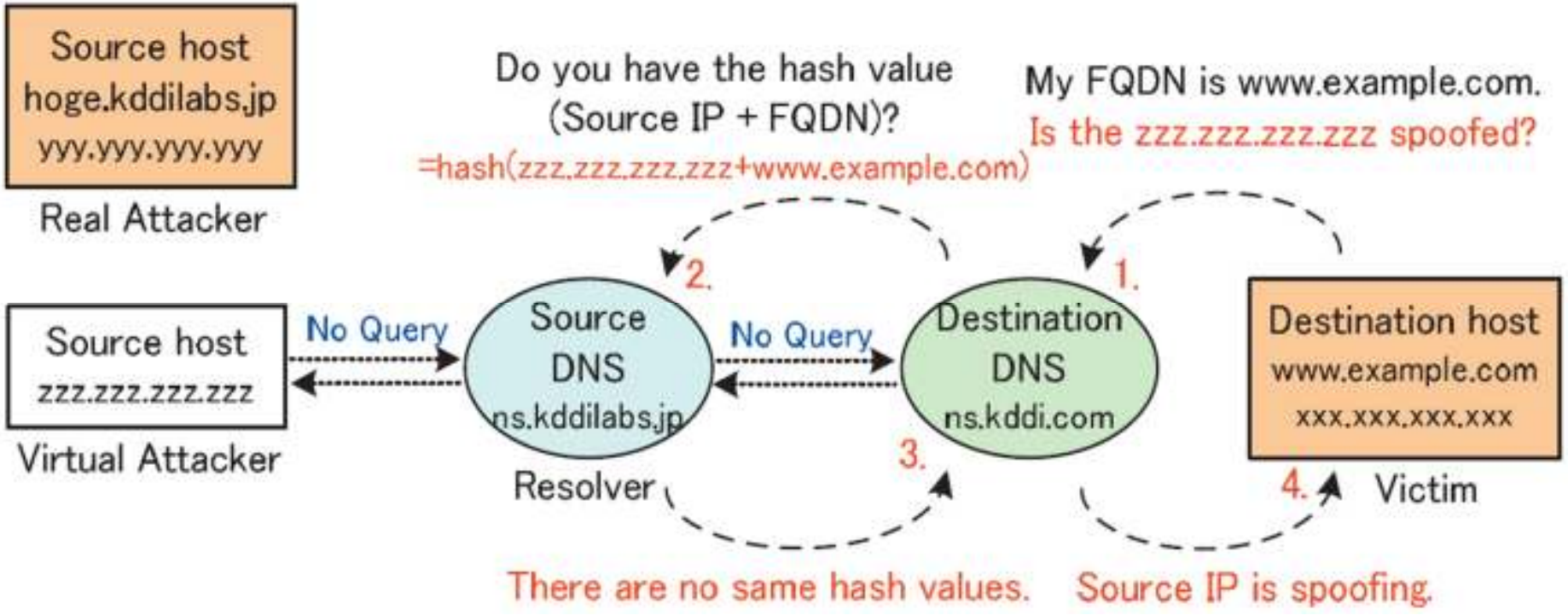
- 送信元DNS、宛先DNS共に利用する



DNSログの内容


2. Destination DNS log; IP=ddd.ddd.ddd.ddd
Time Flag Source IP Dst-FQDN Dst-IP
2007.08.20, 20:18;02 Recursive 192.168.0.21 nishi.shizu.ac.jp 133.70.170.112
2007.08.20, 20:18;05 Iterative 210.168.236.37 mail.kddi.com 61.200.161.234
2007.08.20, 20:18;07 Recursive 192.168.0.23 ns.e-knight.jp 219.166.48.139
2007.08.20, 20:18;11 Iterative sss.sss.sss.sss www.example.com xxx.xxx.xxx.xxx
3. Source DNS log; IP=sss.sss.sss.sss
Time Flag Source IP Dst-FQDN Dst-IP
2007.08.20, 20:18;04 Recursive 192.168.0.21 nishi.shizu.ac.jp 192.168.0.234
2007.08.20, 20:18;06 Iterative 172.29.28.229 mail.local.co.jp 192.168.23.21
2007.08.20, 20:18;10 Recursive yyy.yyy.yyy.yyy www.example.com xxx.xxx.xxx.xxx
2007.08.20, 20:18;16 Recursive 192.168.140.23 ns.local.go.jp 192.168.156.21

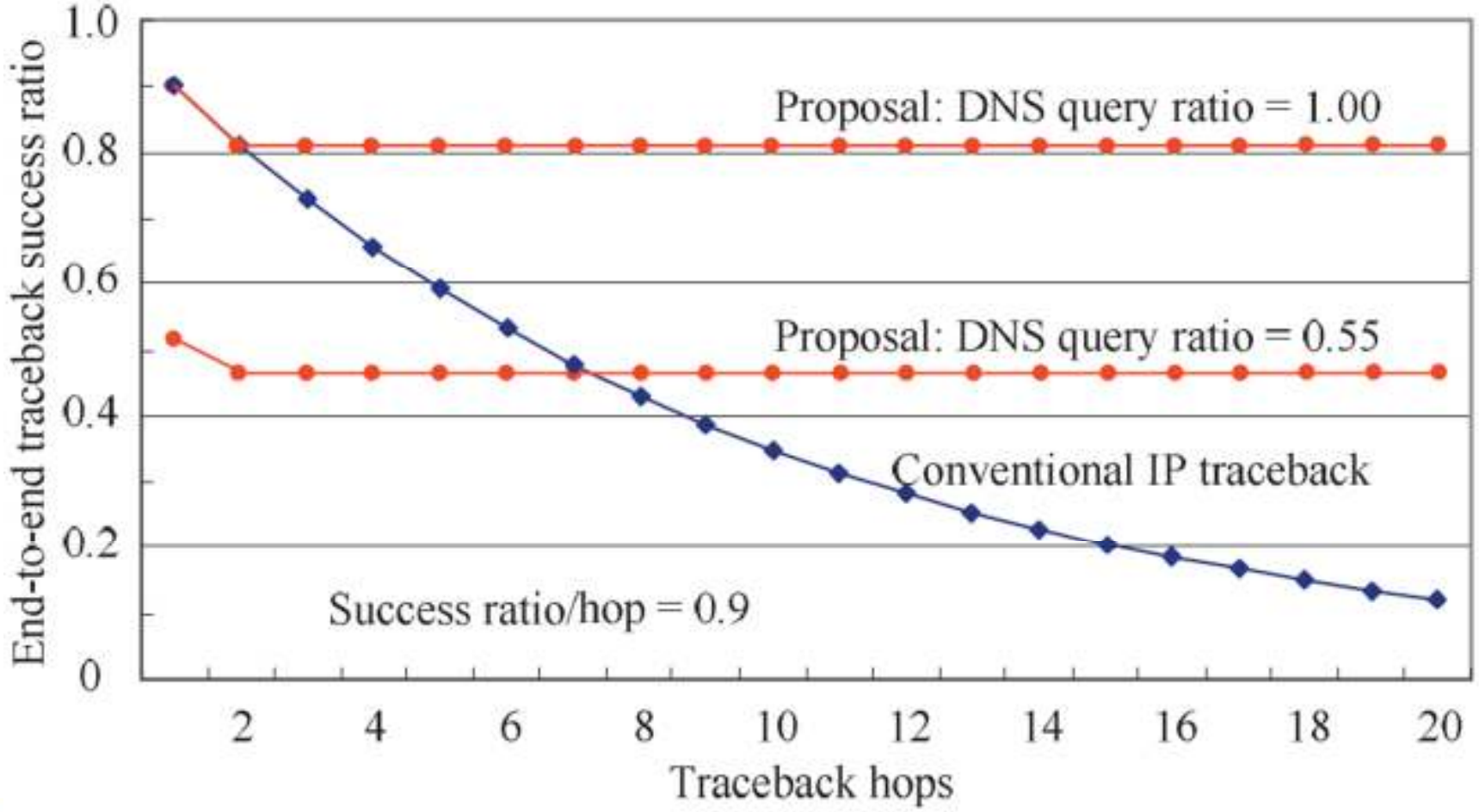
IPスプーフィングに対する判断(1)



IPスプーフィングに対する判断(2)

- 宛先ホストはハッシュ値を計算
  - 送信元IPと宛先FQDNを利用
- IPトレースバック要求と共にハッシュ値を送信
- 送信元DNSサーバはDNSログを利用して
  ハッシュ値を計算
- ハッシュ値の一致・不一致の確認
  - 一致・・・偽装IPではない、不一致・・・偽装IP

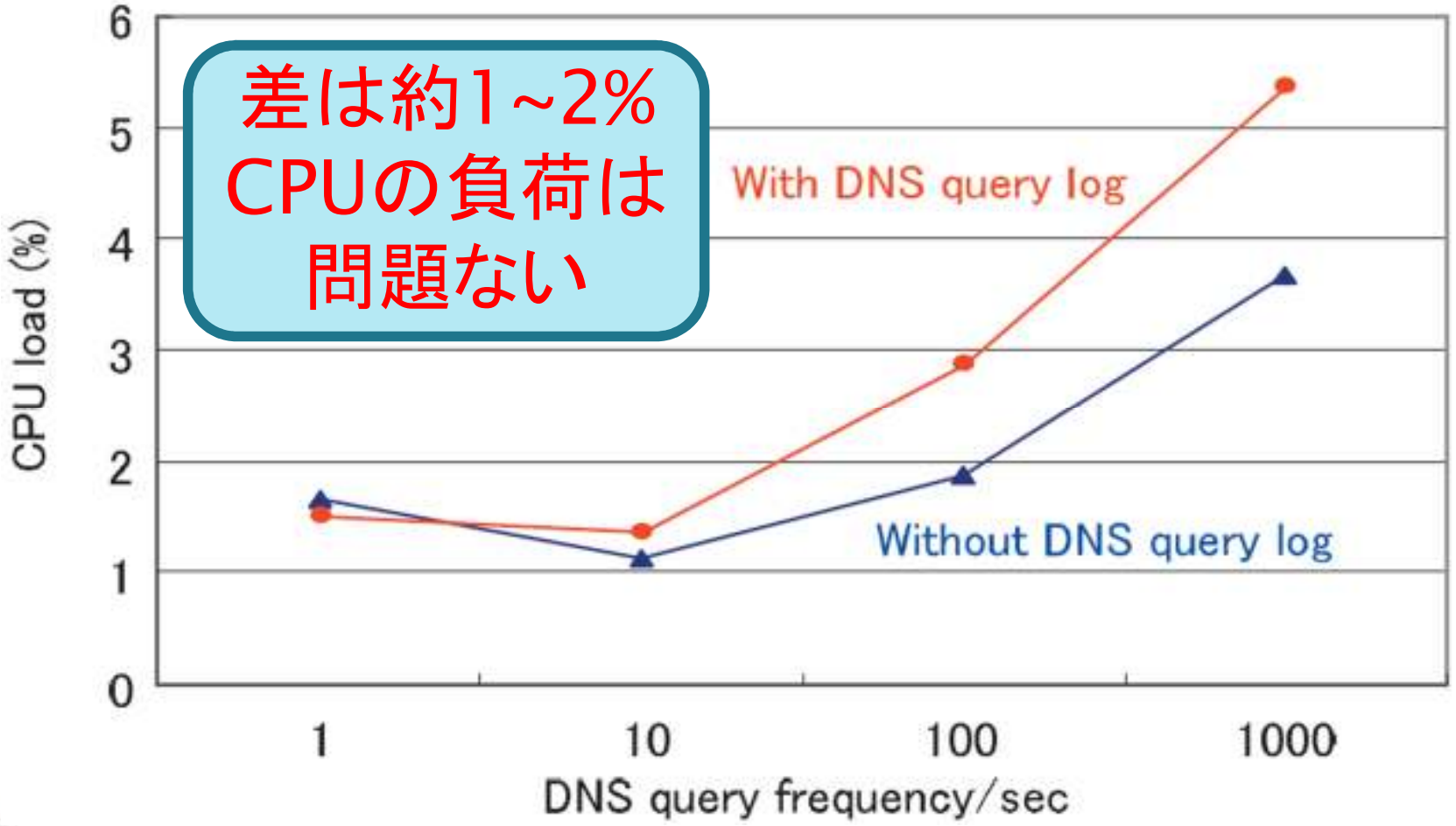
トレースバック成功率


End-to-end traceback success ratio
1.0
0.8
0.6
0.4
0.2
0
Proposal: DNS query ratio = 1.00
Proposal: DNS query ratio = 0.55
Conventional IP traceback
Success ratio/hop = 0.9
2
4
6
8
10
12
14
16
18
20
Traceback hops

DNSサーバのCPU負荷(1)

- 特別な動作
  - DNSログを出力
- サーバの仕様
  - Intel Xeon 3.6 GHzデュアルCPU
  - メモリは4GB
  - Linux 2.4.21.27.0.1.Elamp
  - BIND 9.2.4-5 EL3 DNS

DNSサーバのCPU負荷(2)



まとめ

- 既存技術の紹介
  - ICMPトレースバック方式
  - パケットマーキング方式
  - ハッシュベーストレース方式
- 提案方式の紹介
  - DNSサーバに注目した提案
  - パケット自体に手を加えない
  - IPスプーフィング問題に対応
  - 既存技術よりトレースバック成功率が高い
  - DNSサーバのCPU負荷は問題ない

参考資料

- 「最新技術トレンドIPアドレス詐称パケットの追跡技術」 http://www.bcm.co.jp/site/2003/2003Sep/techo-trend3/techo-trend3.htm (2011年4月19日アクセス)
- 「RBBTODAY」 http://dictionary.rbbtoday.com/Details/term179.html (2011年4月19日アクセス)
- 「IPトレースバックとその応用 JANOG19」 www.janog.gr.jp/meeting/janog19/files/iptraceback.pdf (2011年4月19日アクセス)
- 「L2-based IP トレースバック方式の提案と実装」 http://www.wata-lab.meijo-u.ac.jp/file/journal/2008/200806-IPSJ-Hirokazu_Harima.pdf (2011年4月20日アクセス)
- 「MAC-Based トレースバック方式の実装」 http://www.wata-lab.meijo-u.ac.jp/file/convention/2005/200509-Tokai-Hirokazu_Harima.pdf (2011年4月20日アクセス)

以上