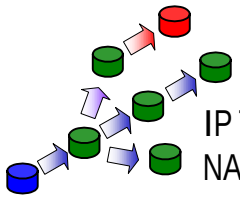
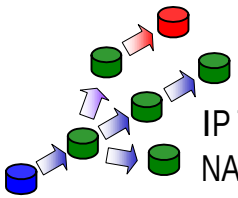


IP TRACEBACK TEAM
NAIST, JAPAN

# DDoS防御にむけて
## ～IP Tracebackの現状と課題～

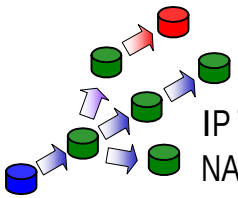
おおえまさふみ <masa@fumi.org>
奈良先端科学技術大学院大学
情報科学研究科





# はじめるまえに

- 率直な意見が聞きたい
  - 現場(ISP)はどう思っているのか？
    - 学術側の人間の考え
    - 現場と仲良く研究開発を進めたい.
  - 今ないもの何か？
    - IETFの標準化に向けて
    - 対策網の構築



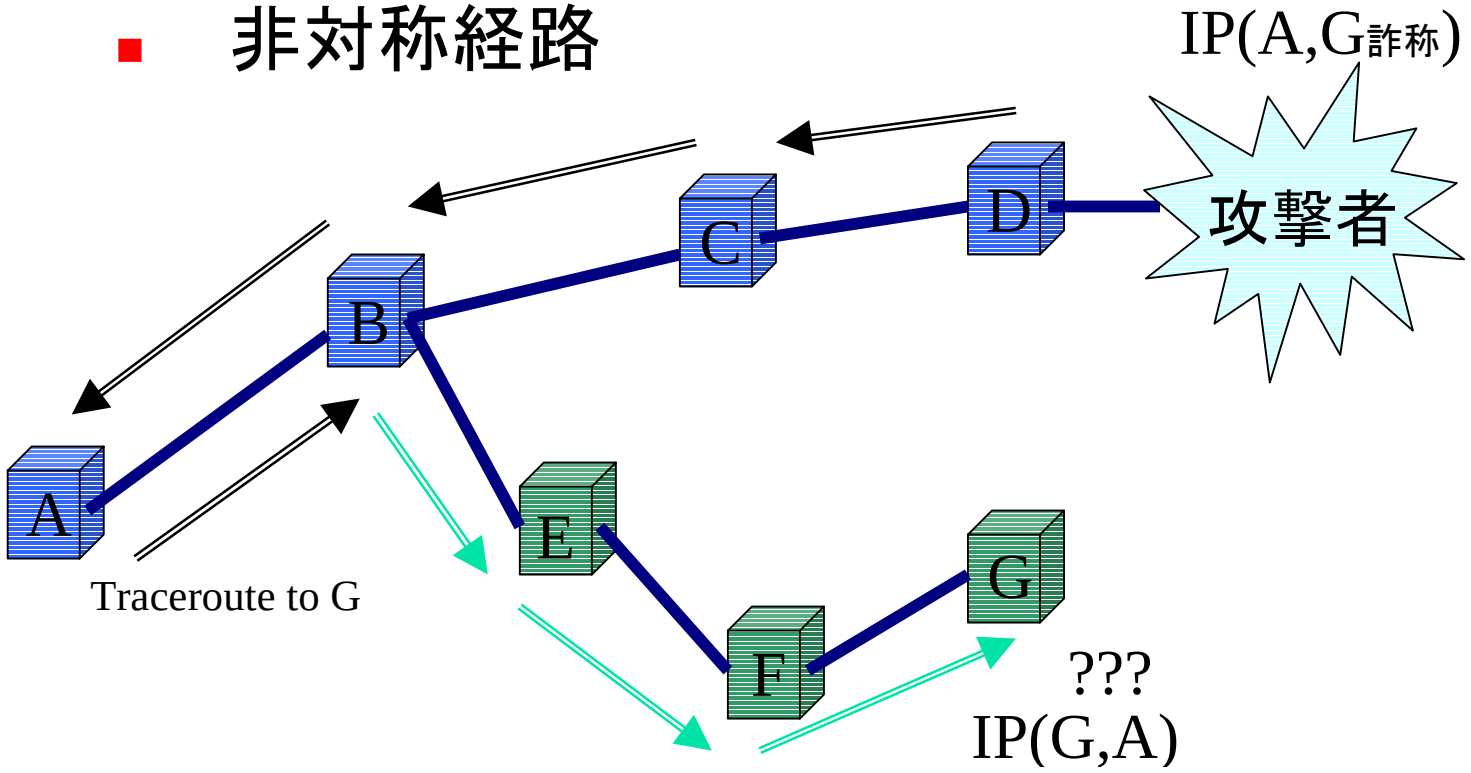


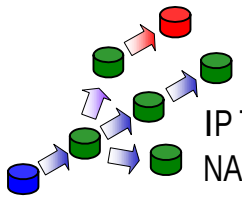
# DoS攻撃と対策

- 脆弱性をつくもの
  - Code Red等
  - システムへの対策
    - ベンダー提供によるパッチ
    - 該当サービスの停止 etc.
- トラフィック集中によるもの　(対象)
  - 分散型DoS攻撃(DDoS attack)
  - トラフィック（攻撃フロー）の特定と遮断

# トラフィック集中型DoS（特徴）

- 発信元アドレスが詐称
  - 経路特定にtracerouteは使えない
  - 非対称経路







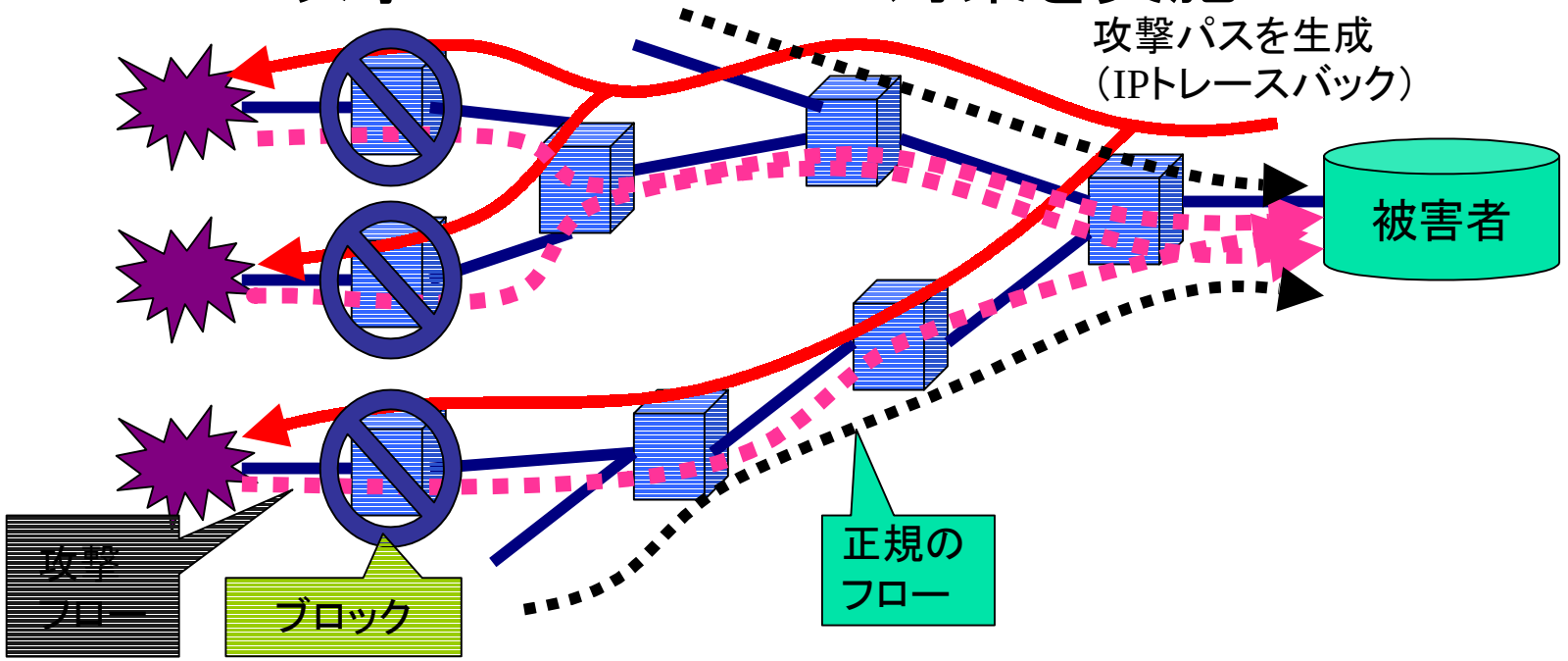
# 対策 トラフィック集中型DoS

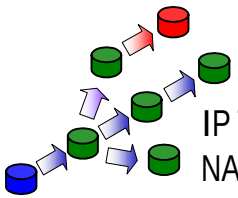
- 攻撃フローの経路特定
  - ISPや，企業，研究・学術機関をまたがる追跡
  - 境界を越える追跡における時間・労力コスト
    - ポリシーの違い・国・時差 etc.
- 対策時間を必要とする
  - 対策時間の増加＝被害量(額)の増加

# IPトレースバック

- 攻撃パス/攻撃ノードの探索手法
  - ネットワーク上の付加機能

  →攻撃パス上でDDoS対策を実施

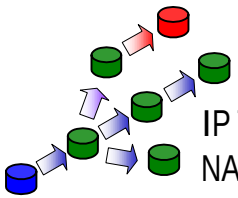






# 関連研究

- 手法の分類
  - リンク追跡型
  - 逆探知パケット型
  - マーキング型
  - ダイジェスト型

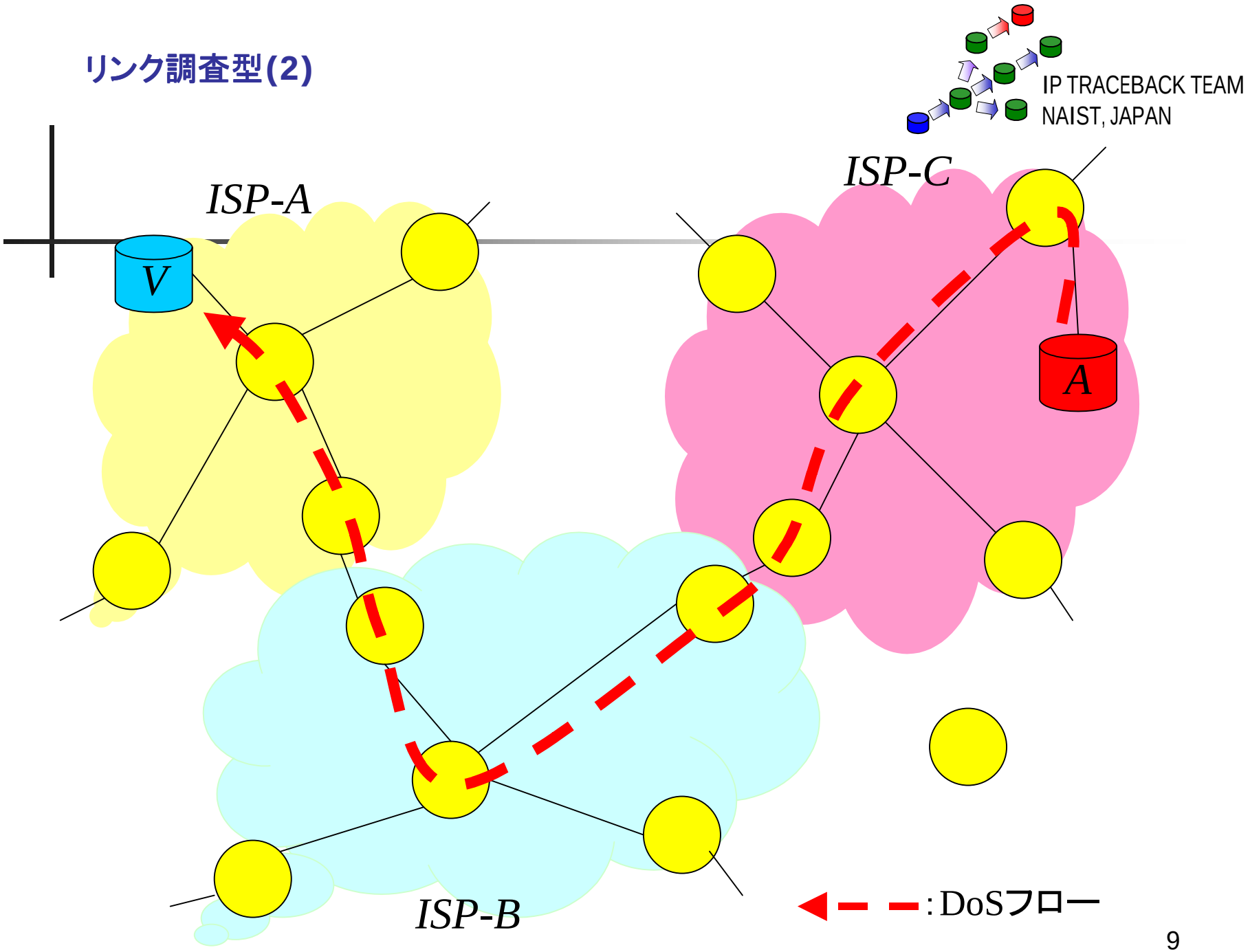




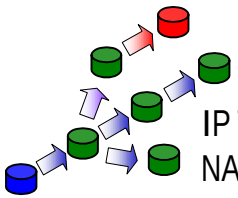
# リンク調査型

- 攻撃フローのモニタリング(従来型)
  - 流入・流出インターフェースの特定
  - ルータ毎に繰り返す事で攻撃フローを追跡

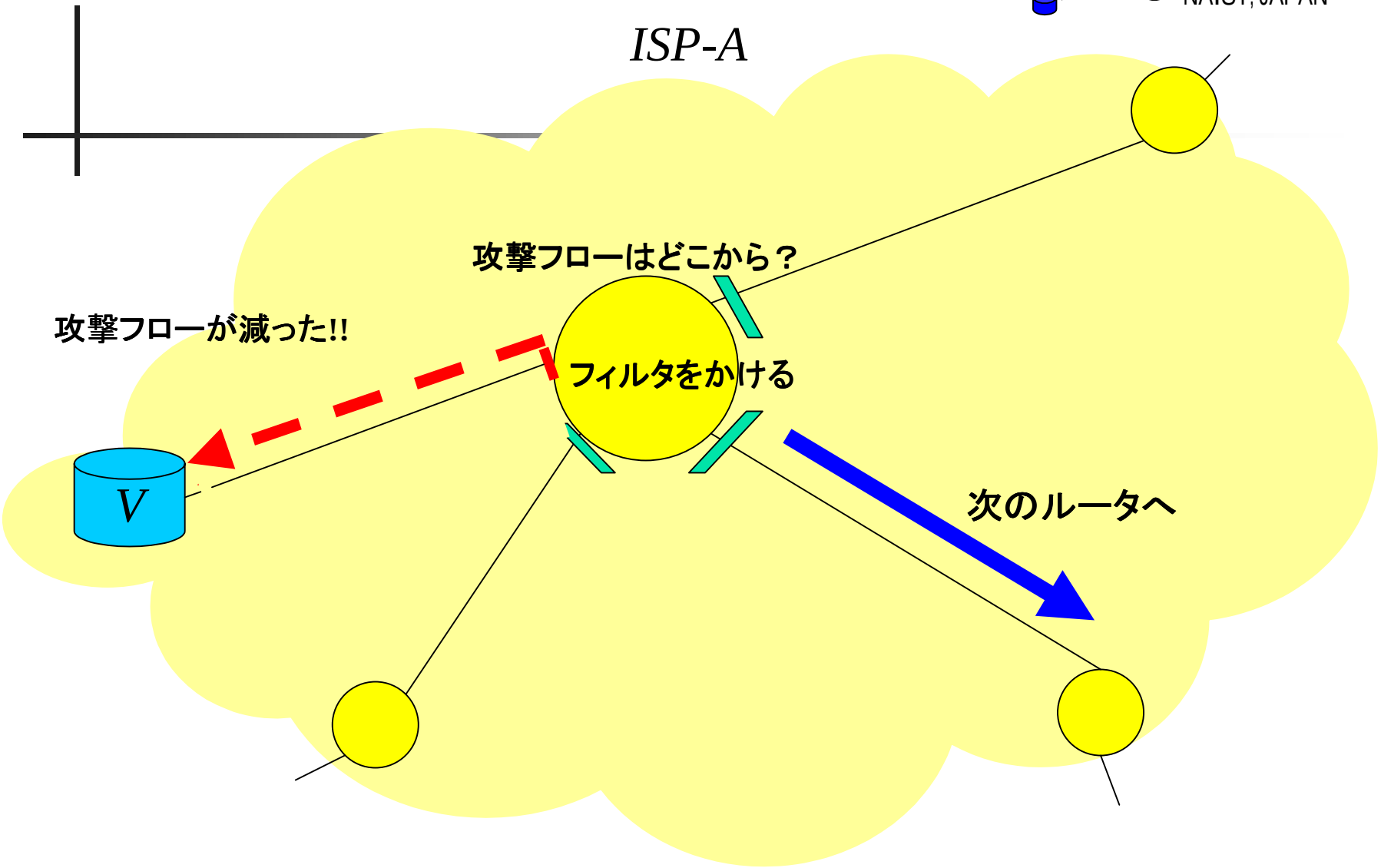
## リンク調査型(2)



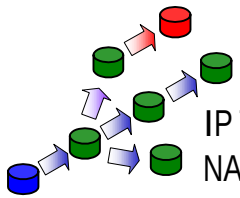
# リンク調査型(3)



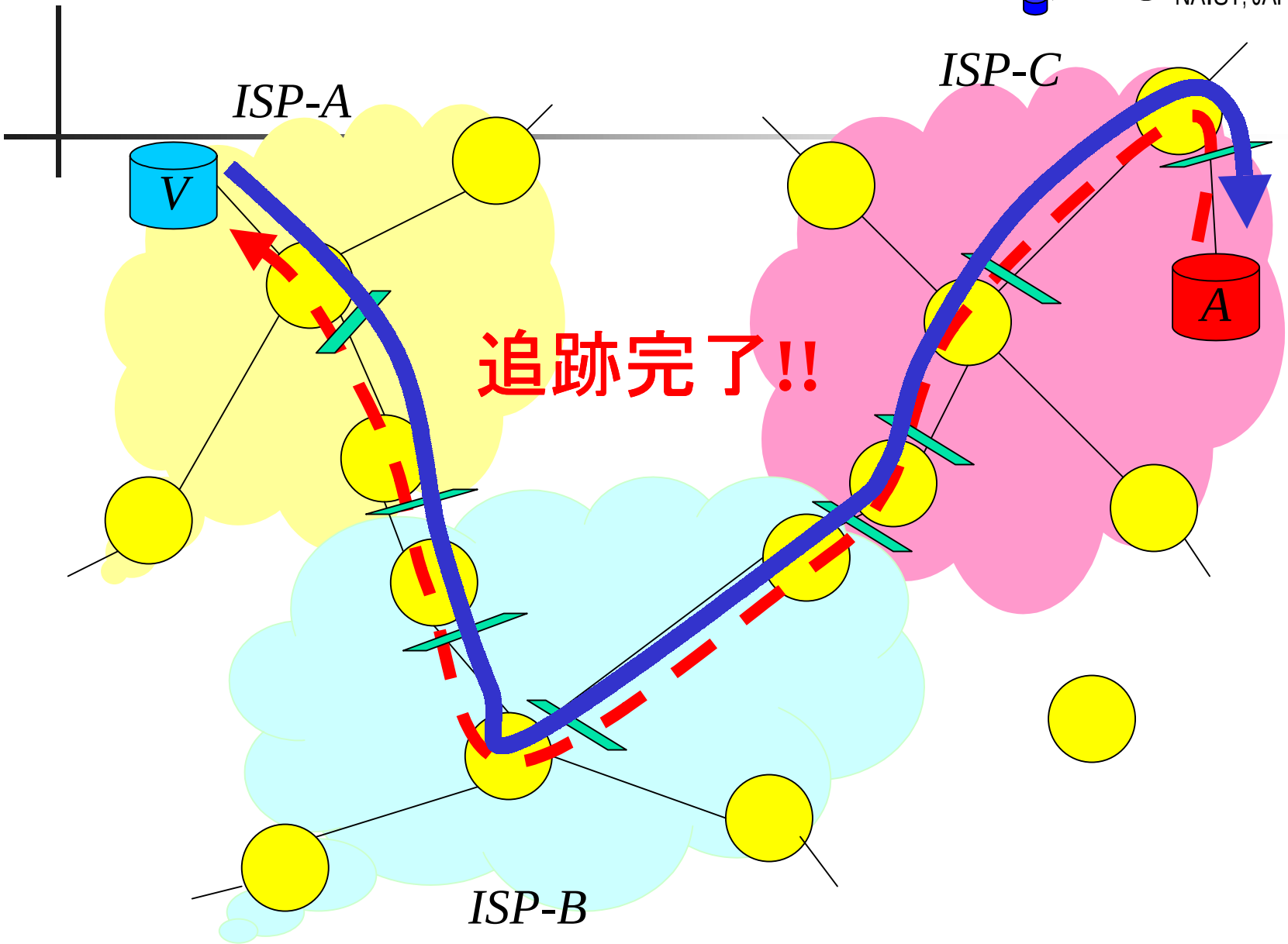


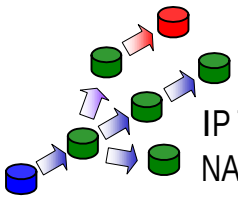


## リンク調査型(4)



IP TRACEBACK TEAM
NAIST, JAPAN

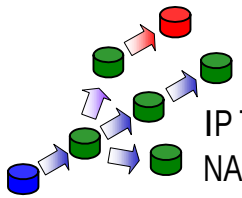






# リンク調査型(5)

- 改善手法(Stoneら)
  - 境界ルータから追跡ルータへのトンネル構築
    - 攻撃フローを1点に集約化して調査
  - 短時間で追跡可能
  - 他組織と連携が必要
  - 攻撃フローの特徴抽出が重要

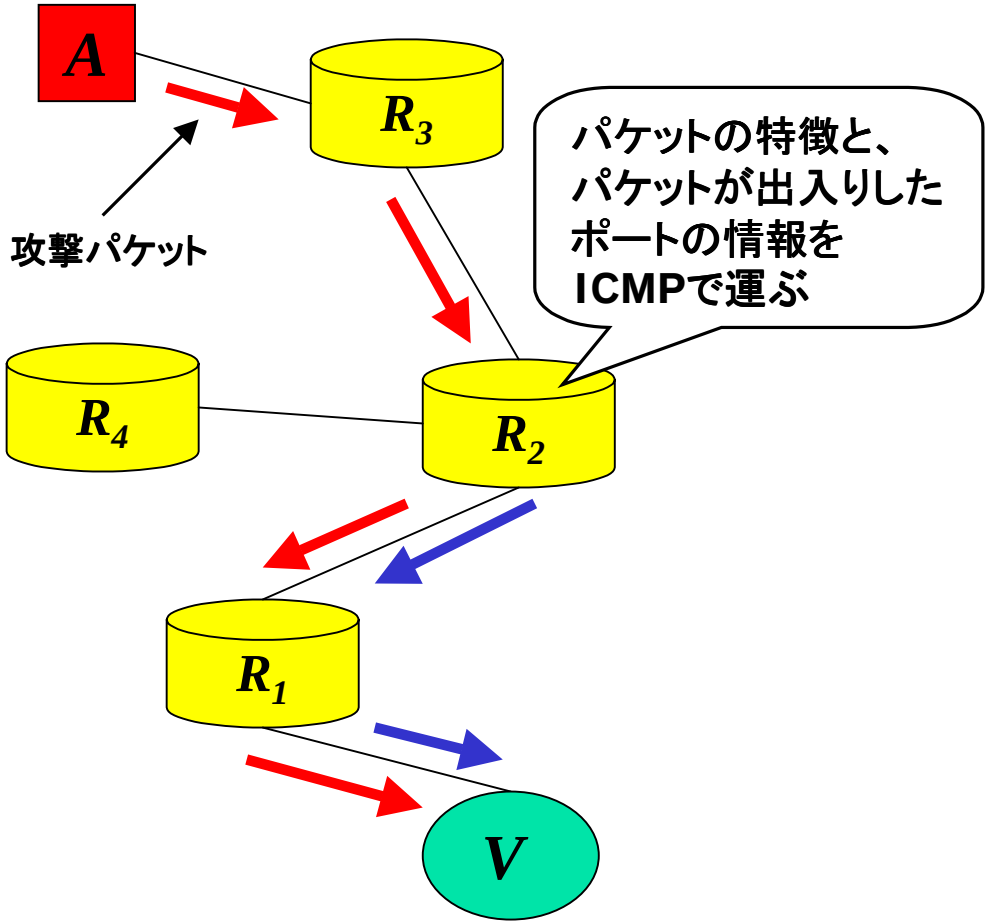


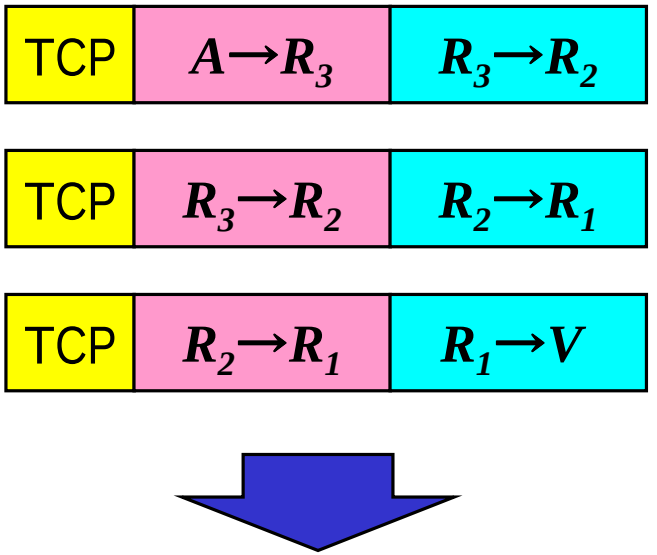


# 逆探知パケット型

- 攻撃フロー特定に専用パケットを使用
- ICMPトレースバック(IETF-ITRACE-WG提案)
  - 各ルータが確立Pに従ってパケットを選定
  - 通過ルータのアドレス等記録したiTraceメッセージ(ICMP)を「確定された」パケットのDstアドレスへ送出
  - iTraceメッセージから攻撃パスを生成
- 追跡用トラフィックが生成
  - 0.1%以内に押さえる (internet-draft)

# ICMP Traceback Message




特徴がTCPのパケットの
アタックパスは

$< A , R_1, R_2, R_3, V >$

# マーキング型

- IPトレースバックに必要な情報を記録
  - Savageらの手法
    - 識別子フィールドへ記録
      - 前後のルータ関係等
      - 距離(ルータ毎に加算)
  - Songらの手法
    - Savageらの脆弱性を改善
    - 同一距離における攻撃ノードの把握能力

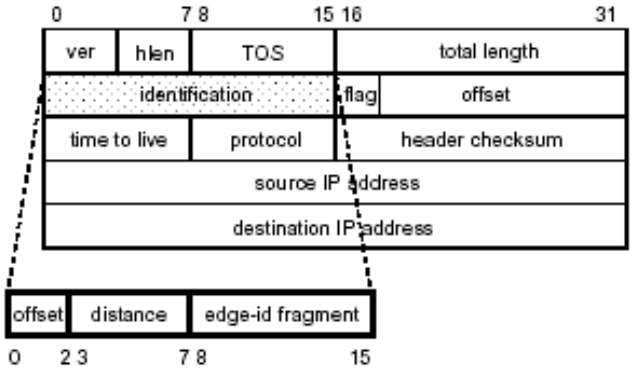
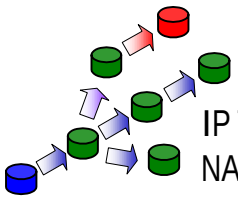
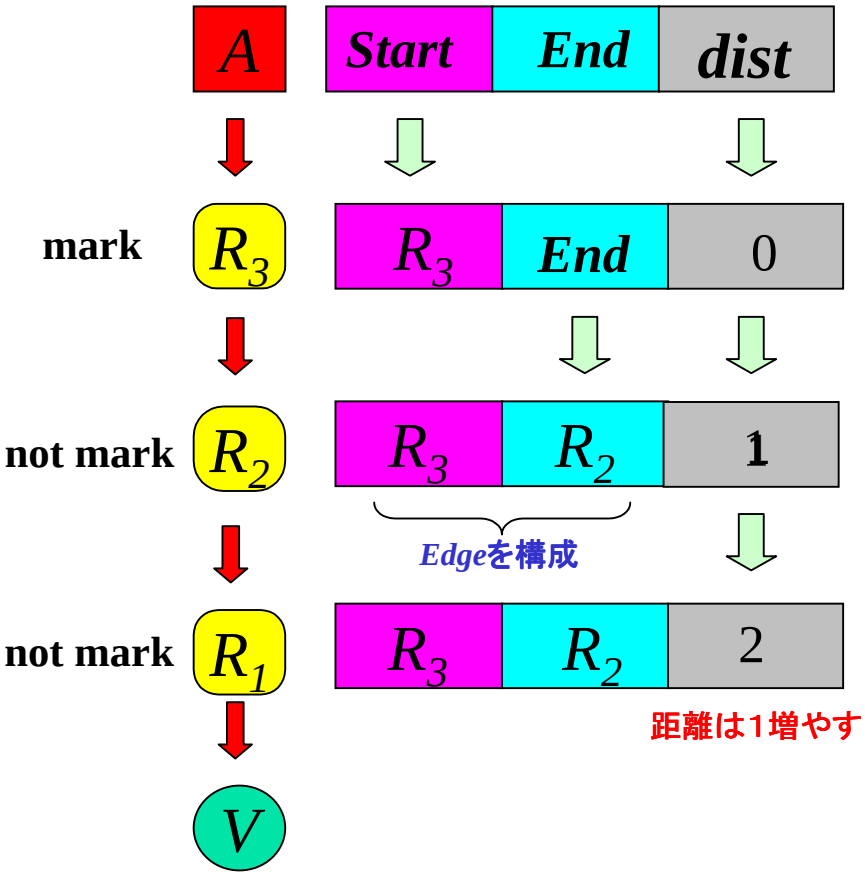



図 2　識別子フィールドを利用したマーキング

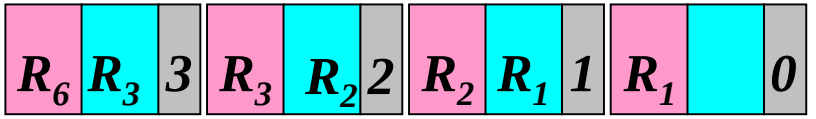


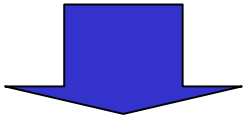
IP TRACEBACK TEAM
NAIST, JAPAN

# マーキング(Savageら)




集まったエッジサンプルを並べる



$Attack\ path = <V, R_1, R_2, R_3, R_6, A>$

# ダイジェスト型

- BBN社がSPIE（Source Path Isolation Engine）として提案
- 効率よくパケットの通過ログを記録
  - 通過するパケット（ダイジェスト化）の特徴を記録
- 攻撃フローのパケットを元に記録を照合し，攻撃フローの経路を特定
- 1パケットでも追跡可能
  - ログ記録システムへの攻撃
  - 組織内追跡

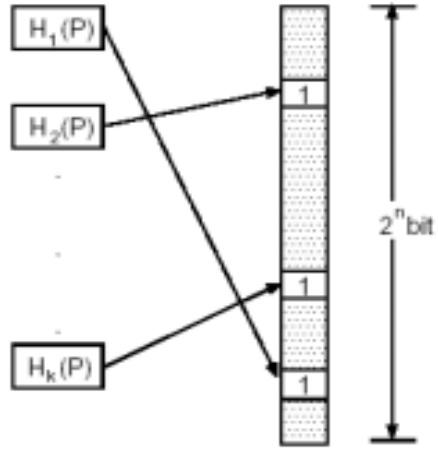
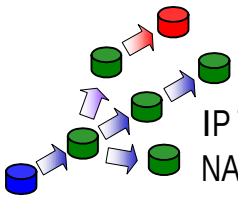
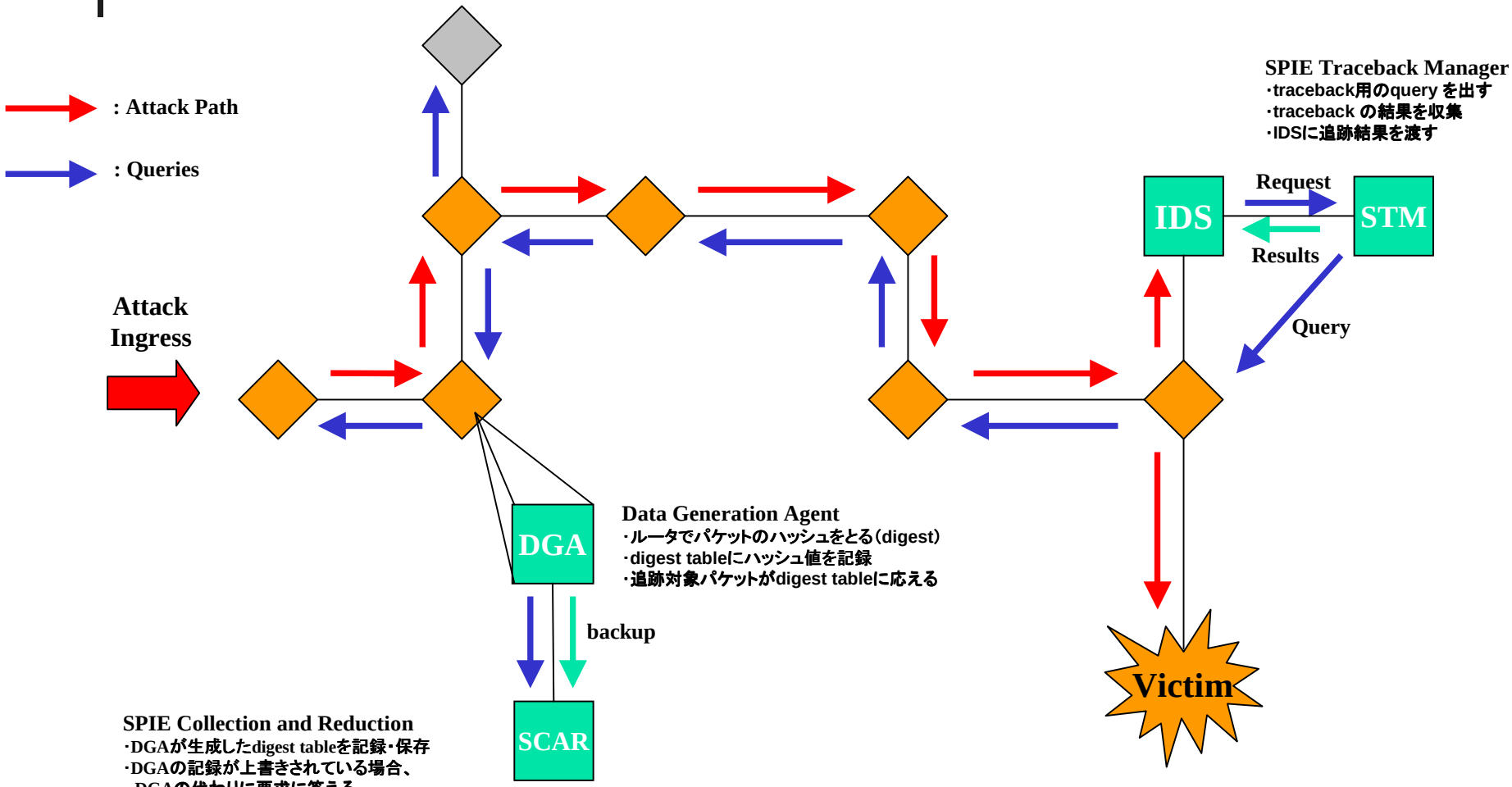


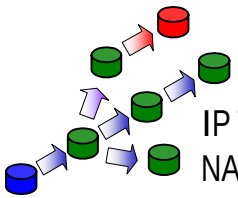

図 3　パケット P とハッシュ関数 H からのビットマップの生成



IP TRACEBACK TEAM
NAIST, JAPAN

# SPIE (Source Path Isolation Engine)

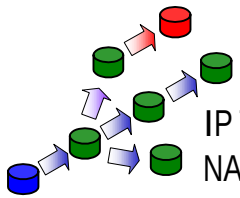






# 比較(欠点)

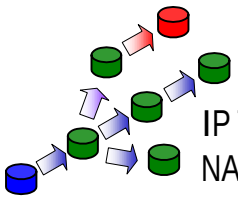
- ICMP トレースバック
  - メッセージの正しさの証明が難しい
- Marking
  - フラグメントやIP sec、IPv6と互換性がない
  - 情報理論駆使・抗トレースバック攻撃への弱さ
  - 精度を上げるには上流ルータのマップが必要
- SPIE
  - 実時間追跡に制約がかかる
    - ルータのメモリ量
  - IP secなど変形パケットの記録がルータでボトルネックに
  - ログ収集用のホストSCARへの攻撃に脆弱
  - 大規模な追跡機構





# 共通する問題点

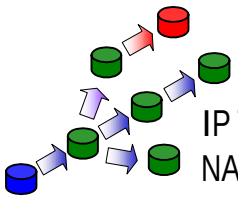
- ISP間の密接な協力体制が必要
- トポロジーなどの秘密情報の漏洩
  - ICMPとマーキングは勝手にトポロジー情報が流出
- 大規模な認証機構
  - 認証が必要な対象：被害者、パケット、エージェント間、ISP間





# 共通する問題点(2)

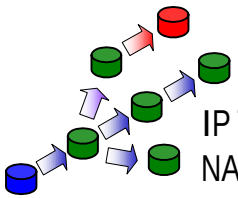
- スケーラビリティ
  - 配備されていないISPからの攻撃は特定にまで至らない
- 攻撃手法の進化
  - 抗IPトレースバック攻撃
- 各手法の適応対象
  - ネットワークの規模や費用
- 単一手法による世界制覇を前提





# 提案手法(奈良先端)

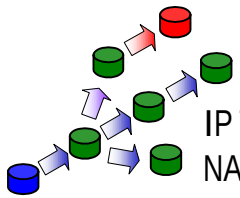
- 階層型IPトレースバック手法(概念)
  - ネットワーク規模に分けてトレース範囲を分離
  - iIP(Interior)トレースバック
    - 組織内(AS内)トレースバック
  - eIP(Exterior)トレースバック
    - 組織間(AS間)トレースバック
  - iIP/eIPトレースバックの手段は問わない
    - 追跡対象の規模に依存
    - iIP/eIP間の連携APIを定義するのみ





# eIPトレースバック

- 攻撃ノードの存在するASを特定する
  - ASを特定するためのIPトレースバック
- 大まかな攻撃ノードの特定
  - 大まかに攻撃トラフィックを遮断
  - 早期に被害を緩和





# iIPトレースバック

- 攻撃ノードのIPアドレスを特定
- 攻撃フロー(ノード)を通過ルータ特定
  - お金が無ければリンク検査型？
  - ダイジェスト方式でもよいでしょう.
  - eIPトレースバックからの情報を元に追跡
    - APIを経由→ iIPトレースバック駆動

# ITMネットワーク

- eIP/iIPトレースバック間の連携用
- EGP(BGP)信頼関係に基づく構築
  - peerを関係のお隣ASはお友達

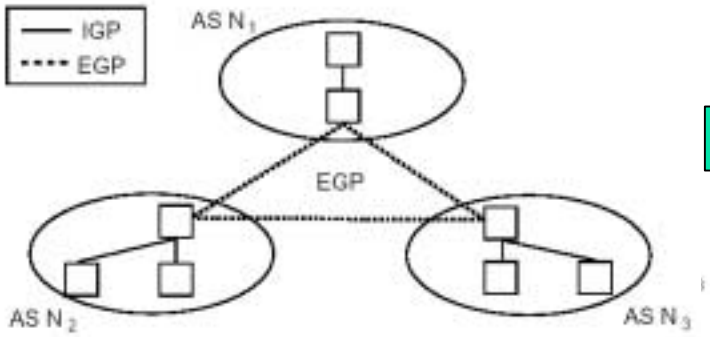



図 4　IGP と EGP の階層関係

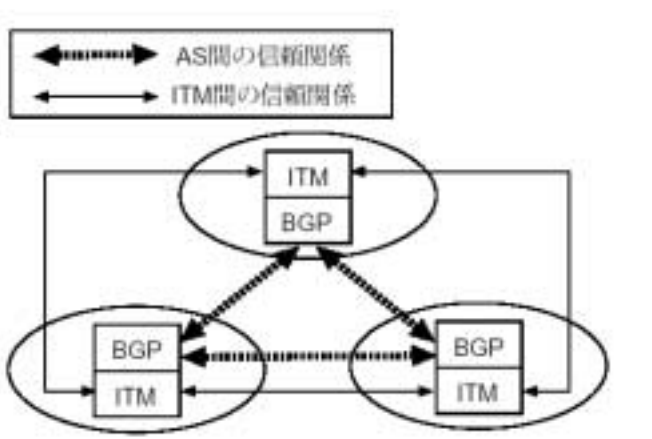
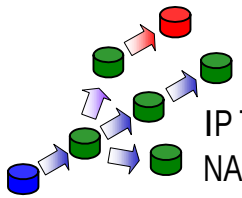


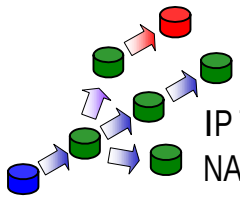

図 7　ITM ネットワーク: ITM の相互接続による形成





# IPオプション・トレースバック

- eIPトレースバックの1手法
- IPv6での設計(v4も計画中)
- ITMネットワークを利用して攻撃パスを構成
- 逆探知パケット方式
  - ASから流出するパケットを対象
    - 確立Pに従って抽出
    - DUPパケット生成し，IPオプションを付加(ICMPではない)
    - AS番号を記録
    - 抽出パケットを元に逆探知パケット生成



IP TRACEBACK TEAM
NAIST, JAPAN

# IPオプション・トレースバック(2)

- IPv6終点オプションヘッダ(記録)
  - ルータアドレス・抽出パケットの送信元アドレス・鍵識別番号(Key_No)・HMACデータ
  - HMACデータ
    =(Key(Key_No)+
    通過AS番号)


図 6　終点オプションヘッダにおけるトレースバックオプションの構成

# 追跡シナリオ

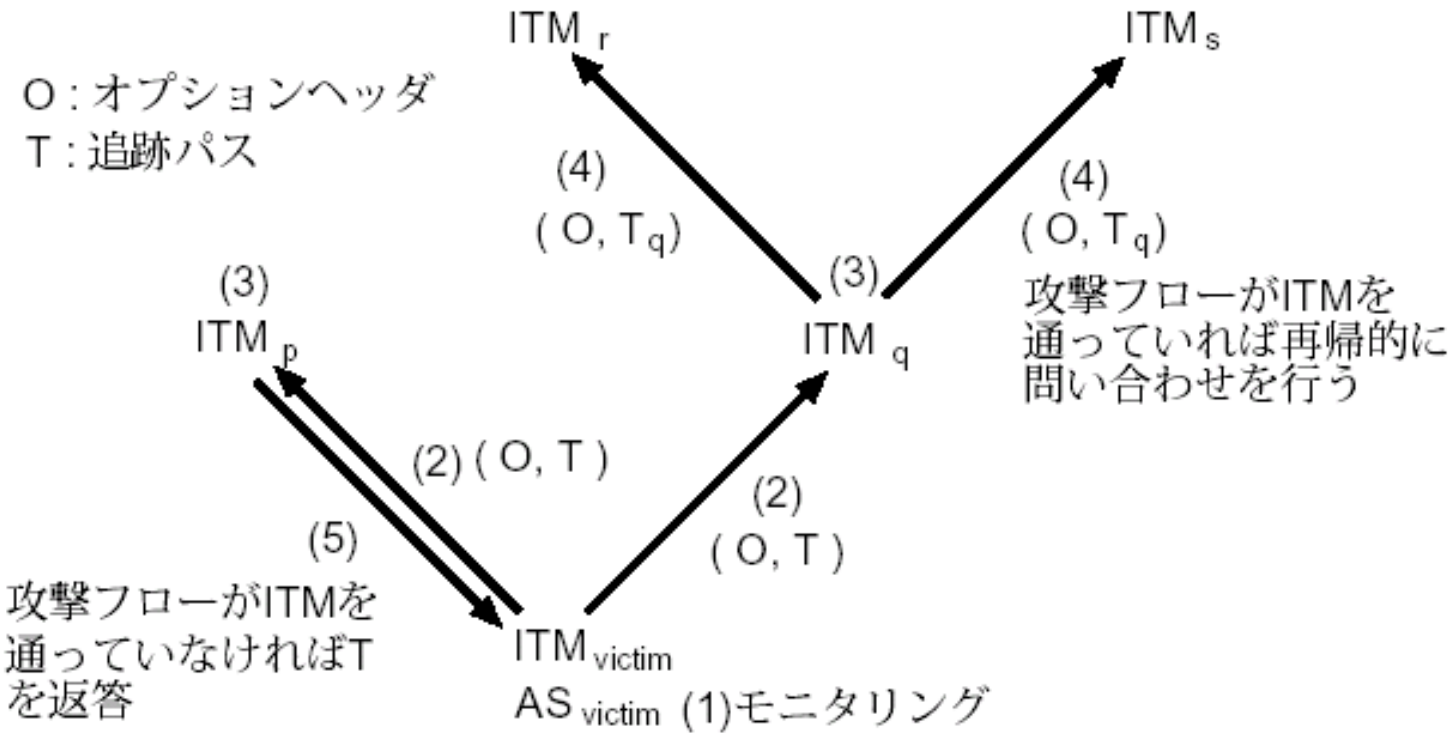
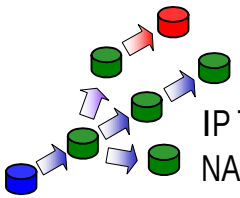


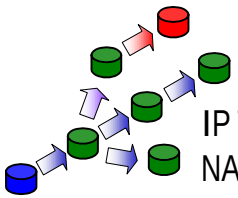

図 8　追跡 (攻撃) パス T の生成過程





# 標準化動向

- IPPT-BOF(ops)
  - チェア: C.Partridge (BBN.COM)
  - BBN.COM主体によるトレースバック連携プロトコルの標準化(Message Exchange の標準化)
    - BBN提案のダイジェスト方式を前提
    - WGへの昇格を考えている.
- iTrace-WG(int)
  - チェア: S.Bellovin
  - ICMP Traceback方式/Intention ICMP Traceback方式
    - 実用的方向性が弱い.

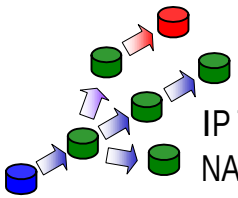




# 今後の計画

- IPオプショントレースバックの改良
  - IPv4対応
  - 流入トラフィックへの逆探知パケットの生成
    - 隣ASが対応していない場合の対策
- ITM間連携プロトコルの設計
  - eIP/iIP間のAPI
  - 追跡対象フローの特徴通知
  - 追跡依頼・返答

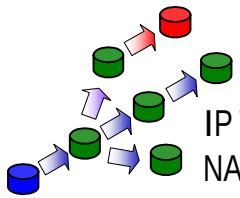
  等々





# 今後の計画(2)

- 実装
  - プロトタイプ実装(eIP)
    - 公開(IETF-53前(2末)を予定)
  - Network Processor ベースのハードウエア
    - 横河電機(iIP)
- 公開情報＆連絡先
  - http://iplab.aist-nara.ac.jp/

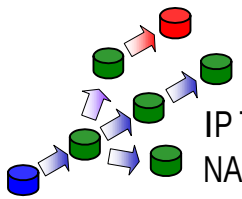


IP TRACEBACK TEAM
NAIST, JAPAN

# パケット追跡システム

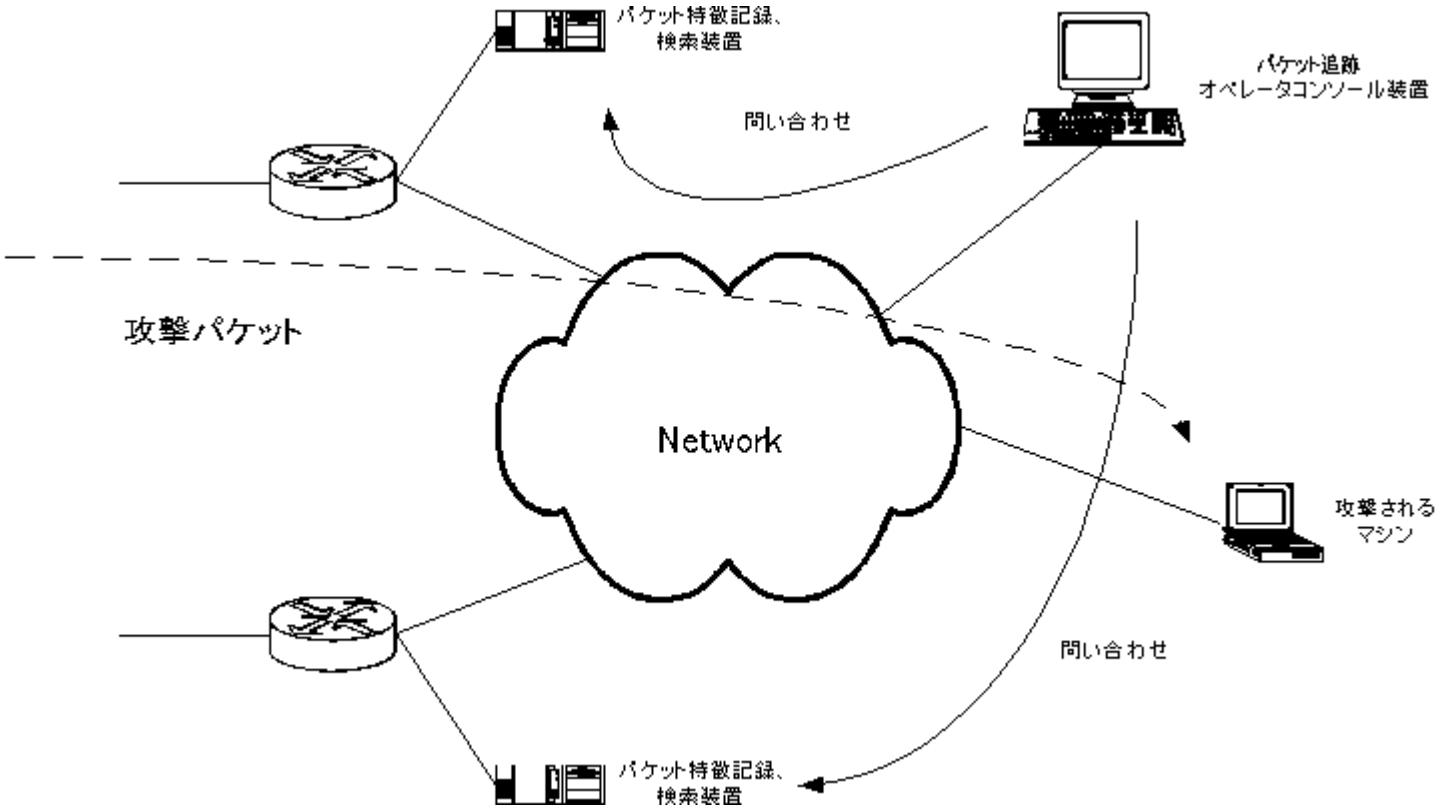
- 横河電機との共同研究
- ソースアドレス偽造したパケットが、どこを通ったかを追跡する
- Hash Based IP Traceback 手法に基づく
- 複数のパケット記録Box と、コンソール
  - SWのミラーポートに接続

YOKOGAWA

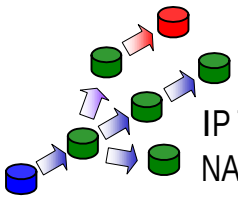


IP TRACEBACK TEAM
NAIST, JAPAN

# パケット追跡システム概要




YOKOGAWA

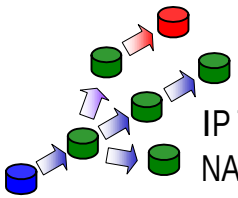


IP TRACEBACK TEAM
NAIST, JAPAN

# 特長

- ソースアドレス偽造された、IP パケットを追跡可能
- 既存のネットワークにアドオンして監視
  - ⇨ ネットワークトポロジを変更しない
- パケットを書き換えない
  - ⇨ 既存の通信に影響を与えない
- 必ず記録する（確率的記録ではない）
  - ⇨ 少量の攻撃パケットも追跡可能

YOKOGAWA



IP TRACEBACK TEAM
NAIST, JAPAN

# ステータス

- 現在開発中
  - 奈良先端科学技術大学院大学と共同研究
- Welcome
  - ニーズをお持ちのバックボーン管理者の方
  - ともに仕様を考え悩んでくれる方
  - フィールドテストの場を提供してもよい方
- 連絡先（開発メンバー）

  Traceback@rant.jp

YOKOGAWA