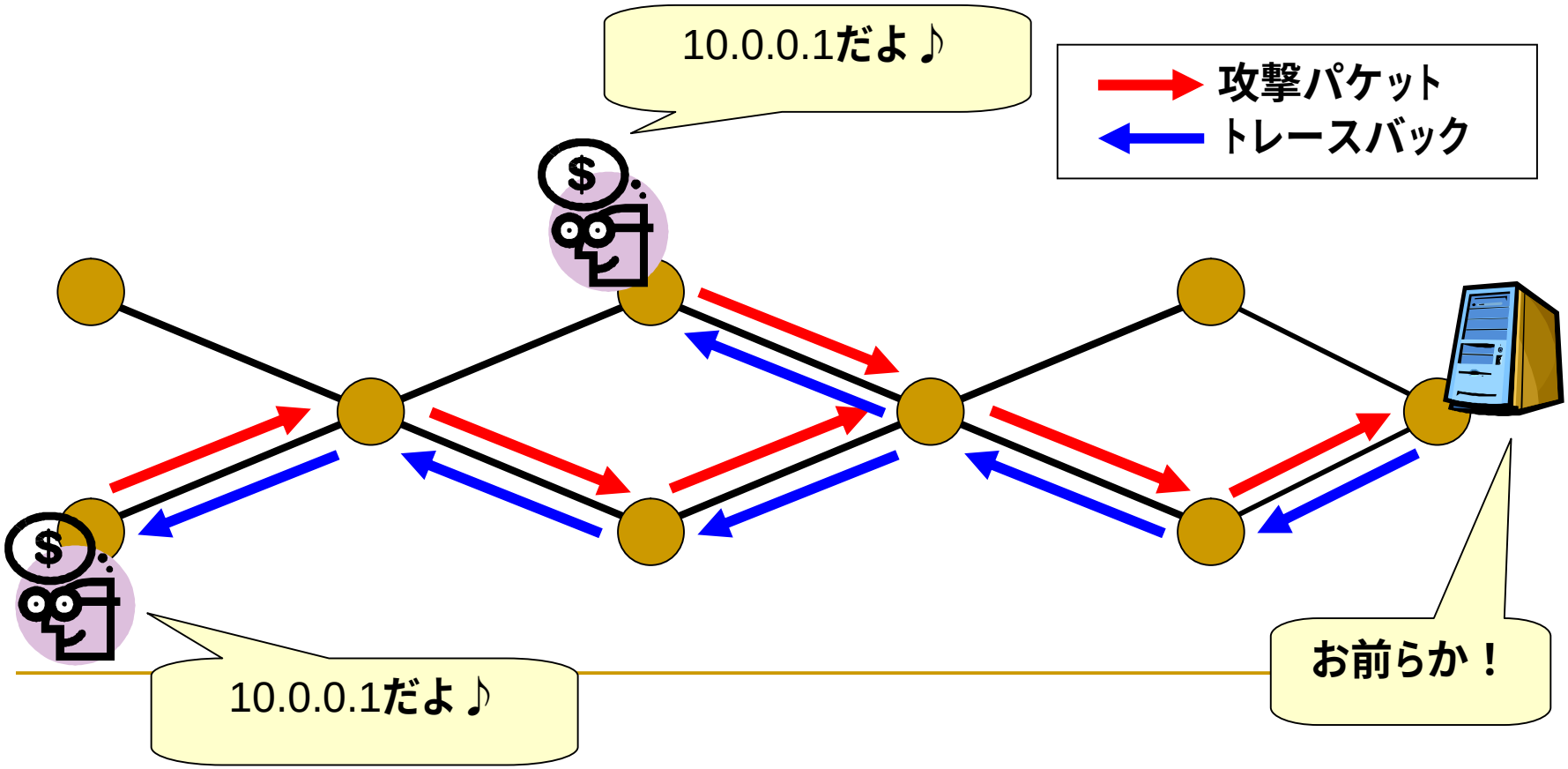
JANOG 19
「IPトレースバックとその応用」を聞く前に

門林　雄基 (奈良先端科学技術大学院大)

IPトレースバックの 5W1H を考える

IPトレースバックとは

- 始点アドレスが詐称された通信の発信源をつきとめる技術
- 「IPパケットの発信源追跡」



IPトレースバックが必要なわけ

- **始点アドレスが詐称されたDDoS**
- **始点アドレスが詐称されたUDP exploit**
- **始点アドレスが詐称されたDNSクエリ**
- …
- **発信源を突き止めて、何らかの対処をしたい**
  - **遮断する、ワームを除去する、ユーザに警告する等**
- RTBH, input debugging
  - **手作業　→　手間がかかる**

誰がIPトレースバックを使うのか

- ISPオペレータ
- JPCERT?
- SSP（セキュリティサービス事業者）？
- 法執行機関？

- 官憲の手を借りずに、できるだけ民間だけで
  インシデントを解決できるようにしたい
- 「悪いことをしたら足がつく」可能性をつくって
  DDoS攻撃などの抑止力にしたい

IPトレースバックと時間軸

- DDoSの最中や直後にIPトレースバックを実施
- 自動判定がほぼ前提

- 時間がたってからだと
  記録が残っていない可能性あり

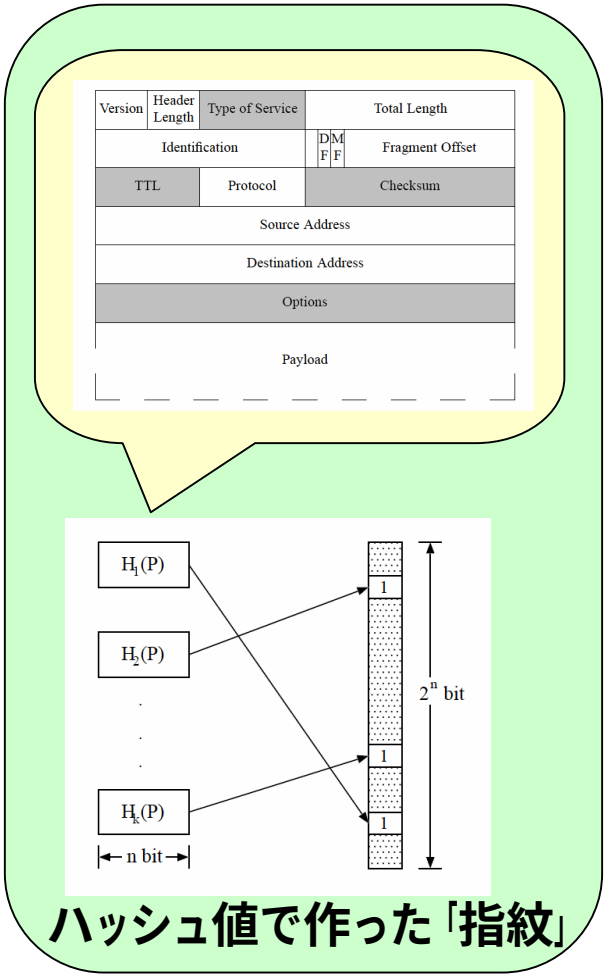
- 遡及能力はメモリオーバーヘッドに跳ね返る

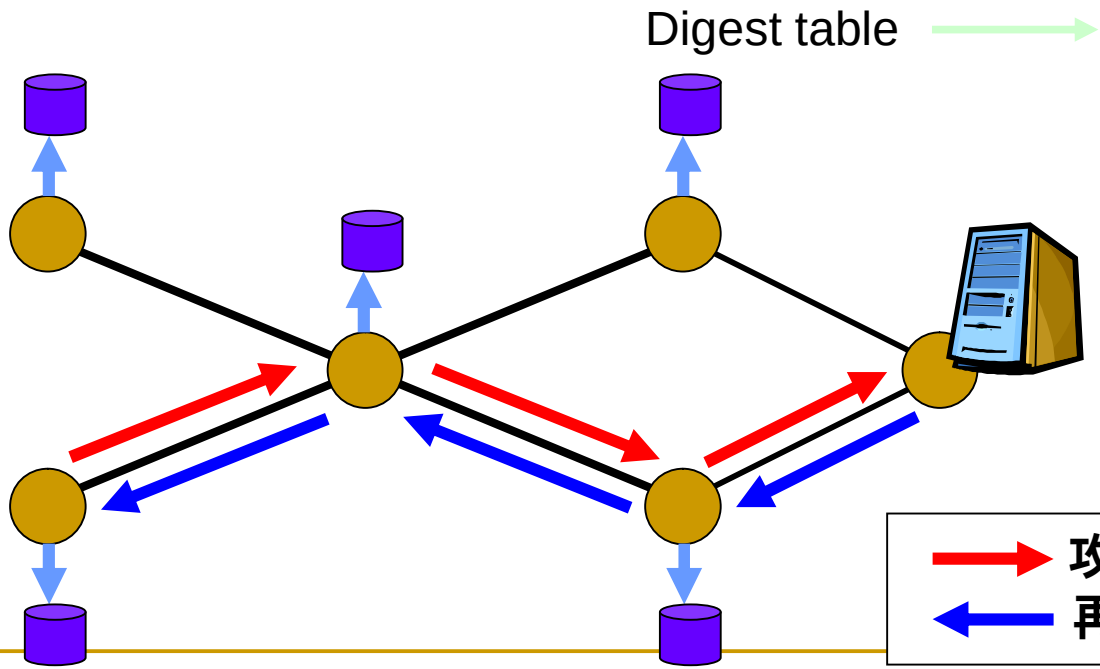
トレースバックの起点と範囲

- 起点はパケットが通過したどこか
  - ルータ、スイッチ、IDSなど
- 流入口がどこか分かれば…
- 自分のプロバイダが発信源かどうか分かれば…
- どのエッジの先か分かれば…
- 国境まで切り分けられれば…

IPトレースバックの動作原理

- パケットの一部のハッシュ値をいくつか計算し、「指紋」としてコンパクトに記録

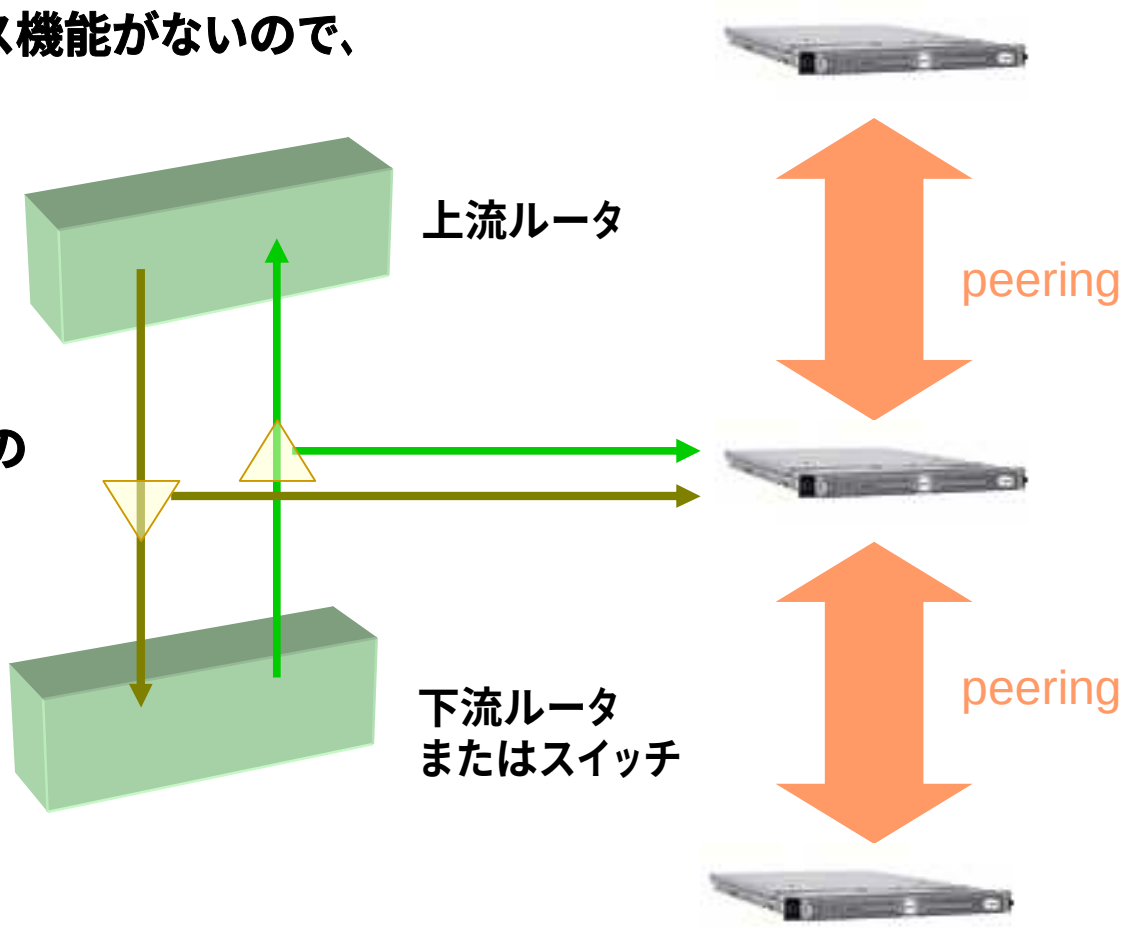




IPトレースバックの運用形態その1

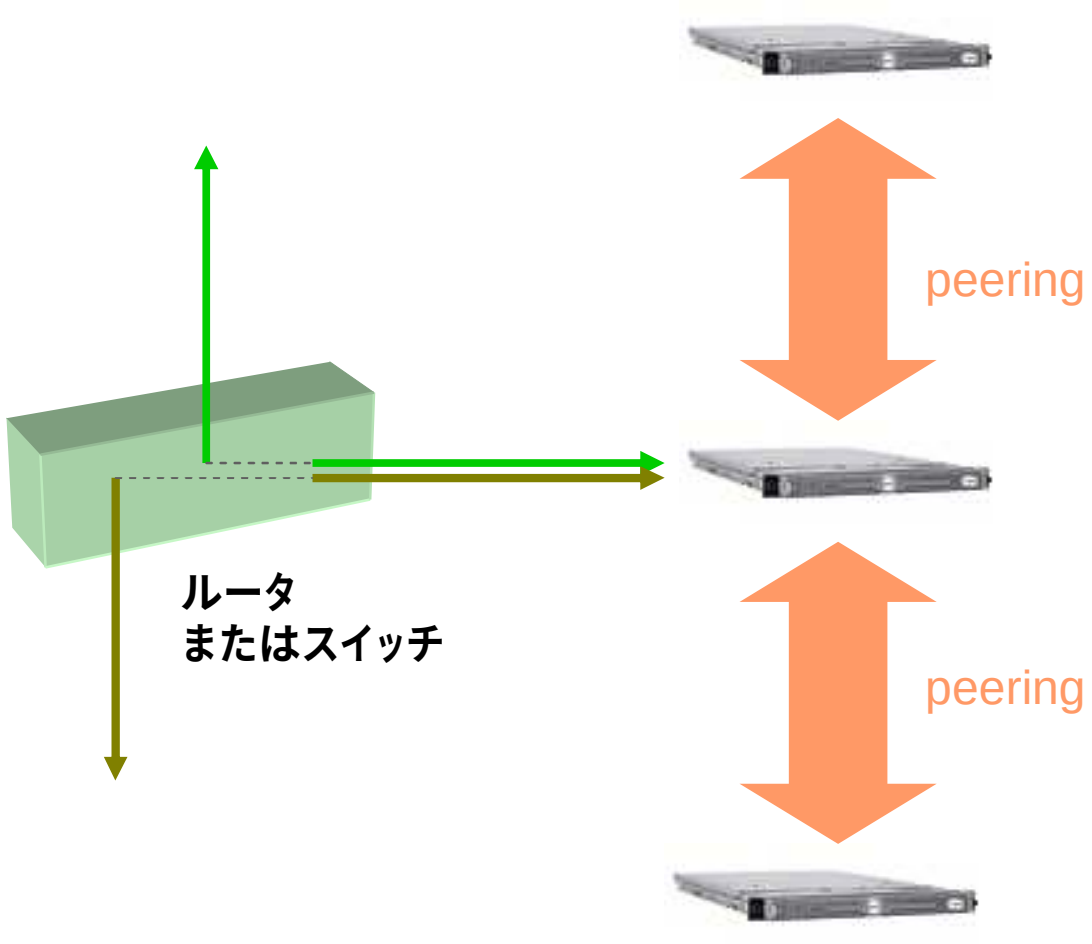
いまのところルータにトレース機能がないので、

光スプリッタ（あるいはメタルのスプリッタ）で信号を分岐してトレースバックノードへ。



IPトレースバックの運用形態その2

ポートミラーリングを設定して
トレースバックノードへ。



この続きは本会議で！

この資料とその続きをわかりやすく説明予定