DNSへの脅威 ネットワーク編

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

権威を持つネームサーバ

- 問い合わせに応じて保持するリソースレコードを応答するだけ
- 状態もほぼ持たない

- ∴ネットワークからの攻撃も比較的単純
- 基本的にコンピュータ資源への攻撃
  - 大量の問い合わせを送ってみる
  - 何らか制限のある資源を狙い撃ちする
  - 帯域を埋める

応答性能

- 条件ざっくり
  - 今時のハードウェア＆OS
  - ちょっと多めのレコード数
- 期待値ざっくり
  - BIND9 50Kqps (数万程度の誤差あり)
  - NSD4 100Kqps(数万程度の誤差あり)
- 単サーバ当たり、これ以上の問い合わせがあると無応答などの事態が発生しうる
  - 問い合わせのIPパケットをざっくり64byteにすると50Kqpsで250Mbps前後のトラヒック

TCP接続数

- DNSではTCPのサポートもMUST [RFC7766]
- TCPの問い合わせにも答えないといけない
  - TCP接続ではサーバ側に状態ができるため、これに対してリソース消費攻撃を仕掛けられる
- UDPの方が性能は出るので、なるべくUDPで答えられるようにしておく
  - 大きな応答サイズにならないように気をつける
  - EDNS0に対応しておく

帯域

- 帯域が埋まると遅延やパケットロスが発生
  - 攻撃側が防御側以上の帯域を操作できるなら負け
  - DDoS, botnet
- 対応は一般の帯域消費型攻撃と一緒
  - 網への流入点で輻輳が発生していないか
  - 網内の輻輳箇所に至る前に何らか対策が可能か

対策

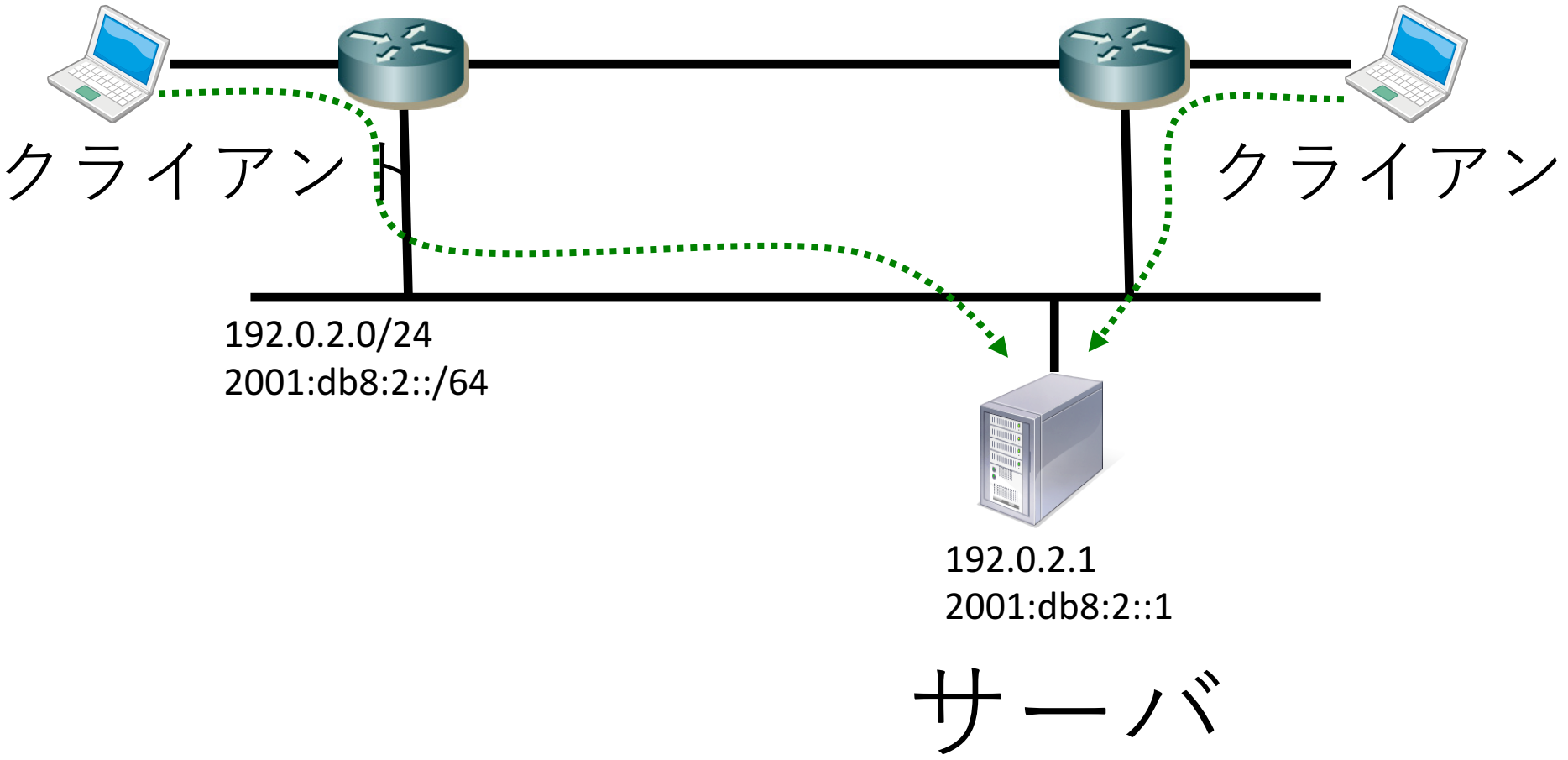
- リソース消費攻撃にはリソース追加防御！

- 応答性能を引き上げる
  - キャッシュサーバ
- サーバを並べる
  - ロードバランサ
  - IP anycast

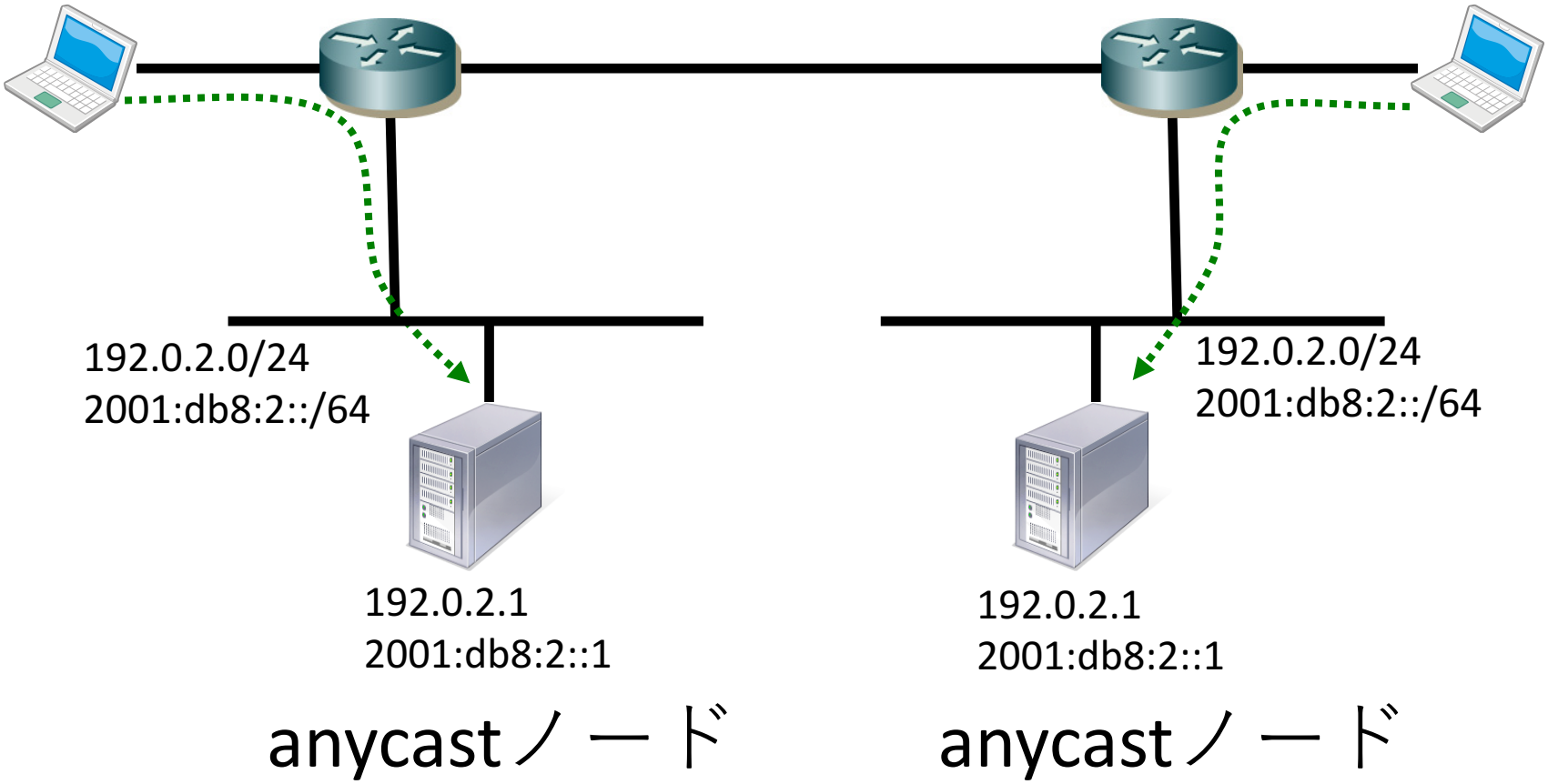
IP anycast

- 主にサーバ側で利用する技術
- 実は単なるunicast
  - 複数箇所に同じIPネットワーク
  - でも、ルータは単に宛先に投げてるだけ
  - anycastは状態だと思うのが良いかも
- ユーザからはanycastのノード数は分からない
  - 1以上のノードが稼働していればサービスは可能

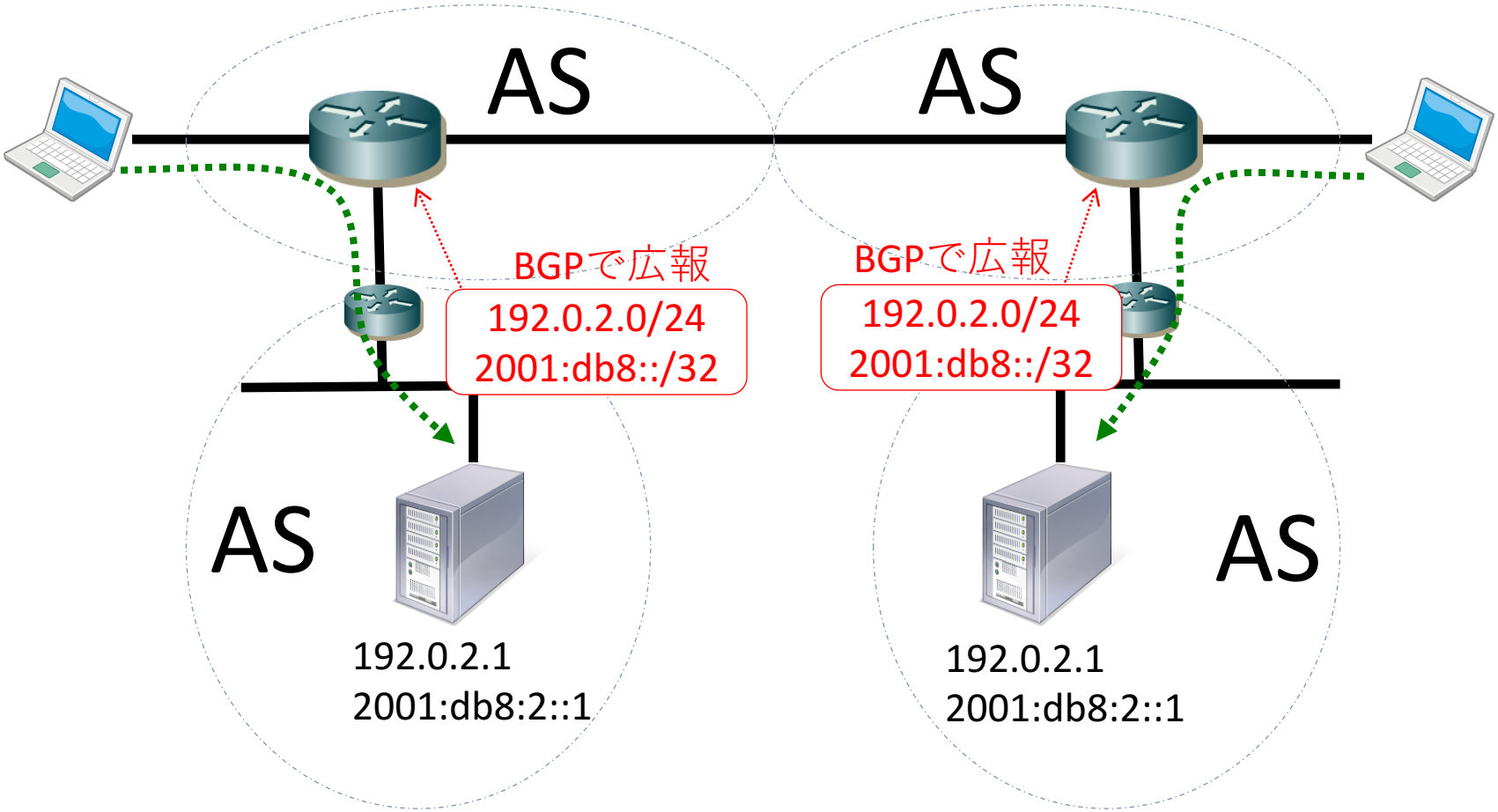
クライアントとサーバ



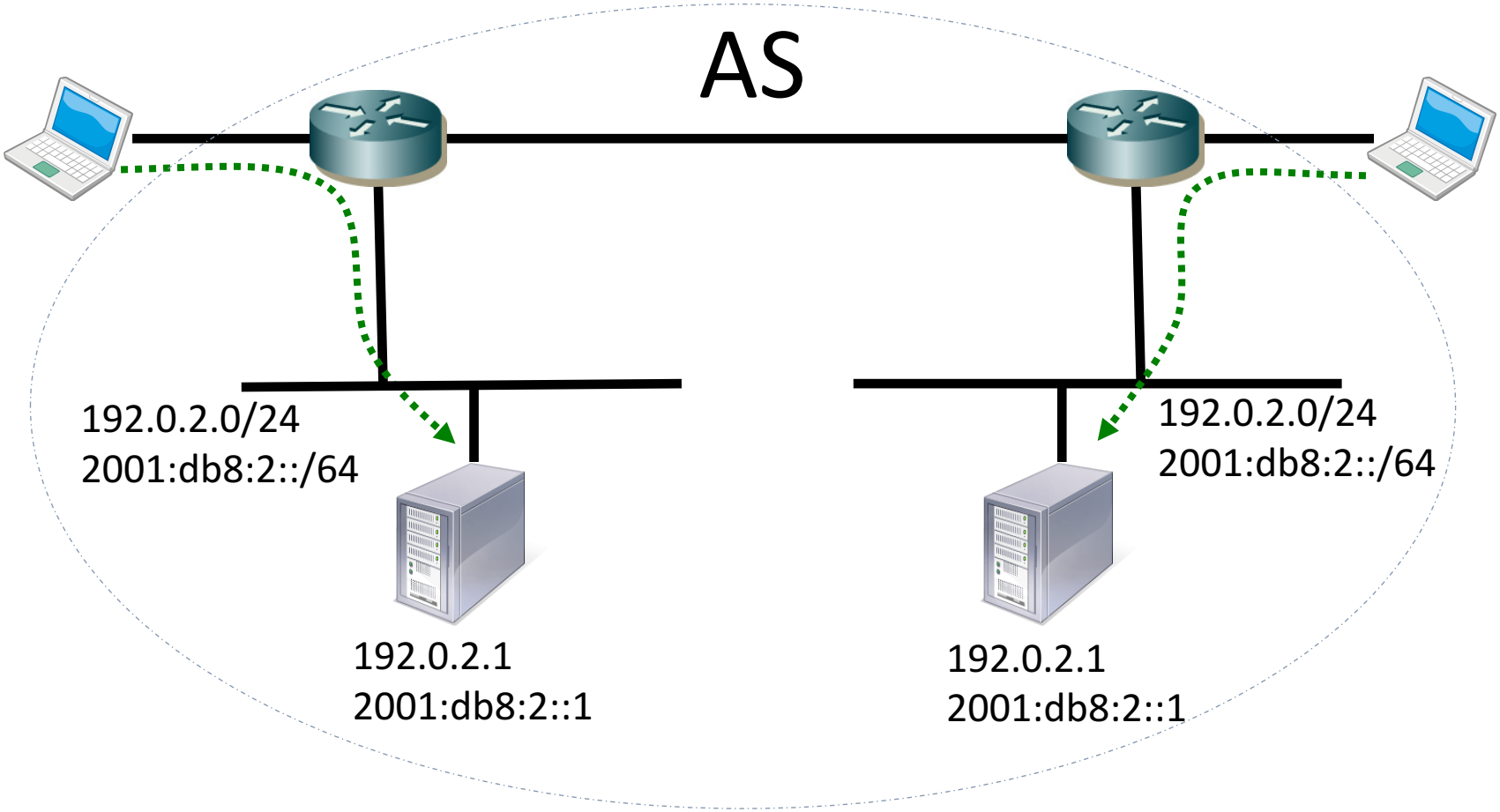
複製したら、ほらIP anycast



AS間だと、BGPで制御

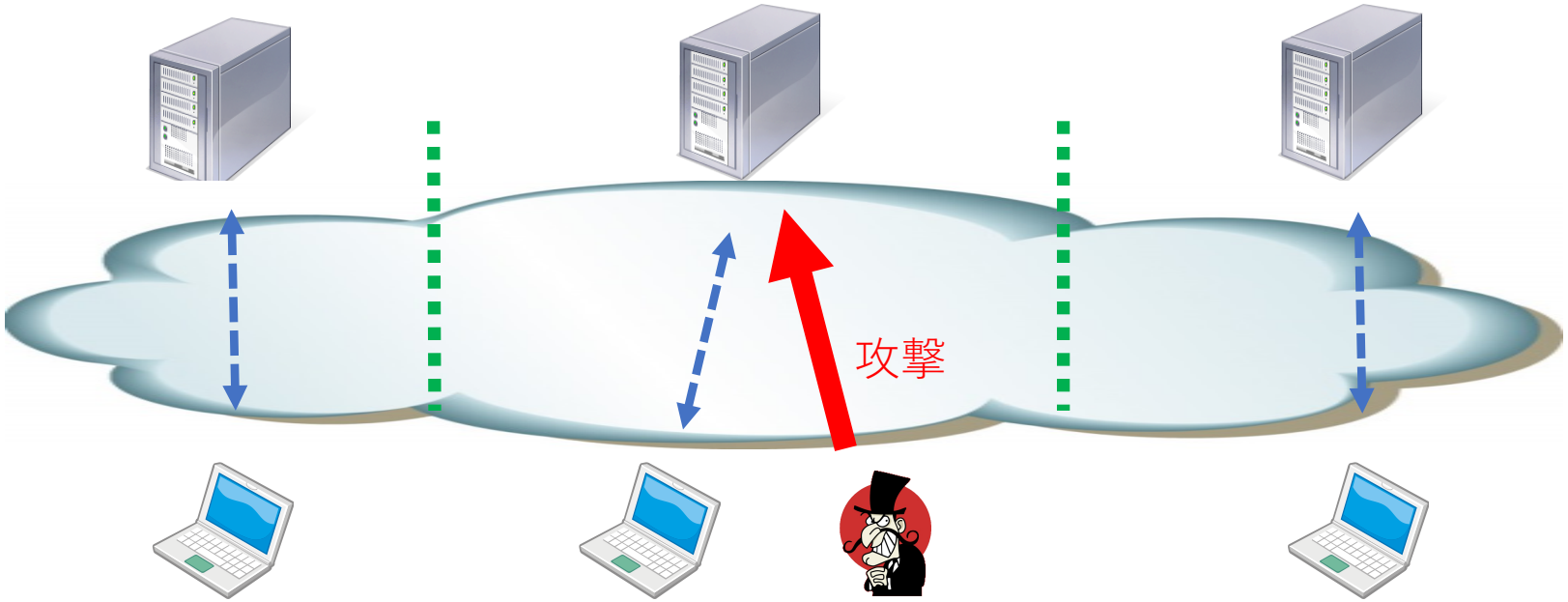


AS内だと適当に制御


AS
192.0.2.0/24
2001:db8:2::/64
192.0.2.1
2001:db8:2::1
192.0.2.0/24
2001:db8:2::/64
192.0.2.1
2001:db8:2::1

IP anycastで障害の局所化

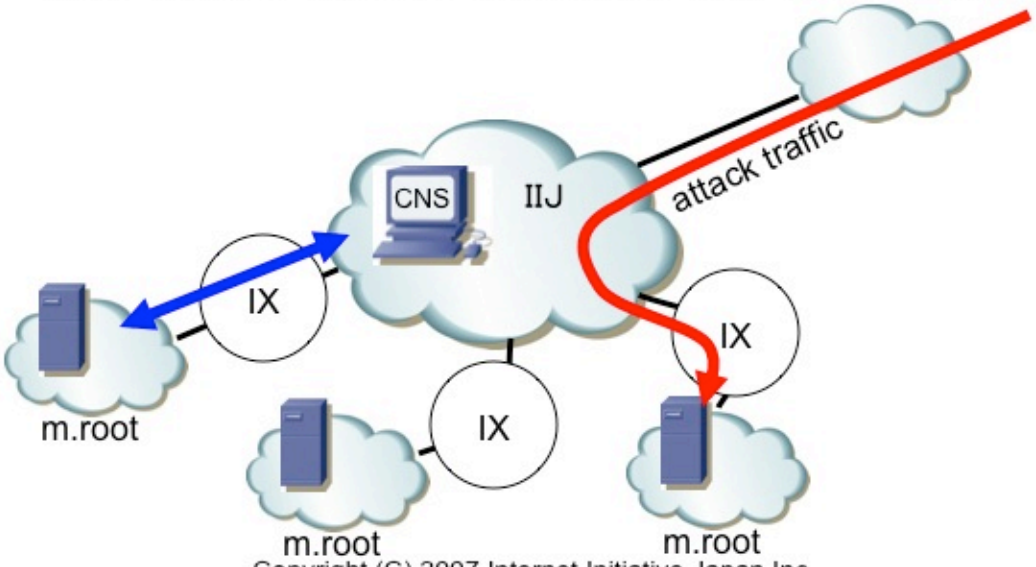
- 攻撃や障害の影響を局所化できる
  - 利用者側からはルーティングを制御できないため



2007/02/16 19:00JST~

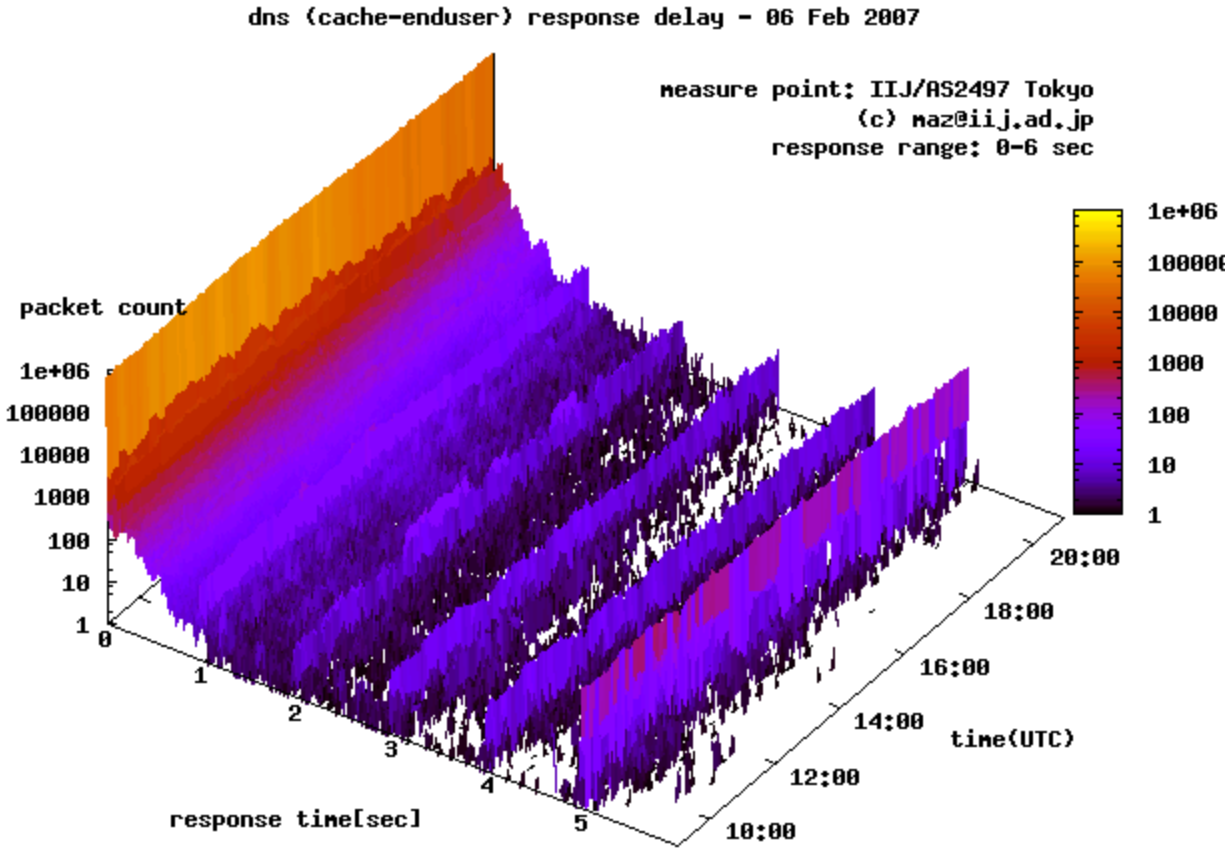
during the attack

- IIJ transited attack traffic as well...
  - IIJ's cache server selected the other site.



17

応答遅延概要


dns (cache-enduser) response delay - 06 Feb 2007
measure point: IIJ/AS2497 Tokyo
(c) maz@iij.ad.jp
response range: 0-6 sec
packet count
1e+06
100000
10000
1000
100
10
1
0
1
2
3
4
5
response time[sec]
10:00
12:00
14:00
16:00
18:00
20:00
time(UTC)

root-serversへのquery数・・・

- 1229097 total queries
  - 1223957 invalid_TLD (99.5%)
    - 1110543 AforA (90.3%)
    - 113414 other invalid_TLD (9.2%)
  - 5140 valid_TLD(0.4%)
    - 4787 .arpa (0.3%)
    - 353 other valid_TLD(0.02%)

期間 08 Feb 2007 09:00UTC-21:00UTC

防御時にあると役立つもの

- 隣接ネットワークとの良い関係
- 性能良く、しかも細かな条件を設定できるパケットフィルタ
  - ルータなどでも可
  - 性能劣化する場合があるので要検証
- 特定の問い合わせパターンをサクッと落とせる機能とスキル
  - ipfilterでもpfでも何でも