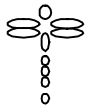


DNS amplification attacks

Matsuzaki Yoshinobu
<maz@iij.ad.jp>

DNS amplification attacksとは

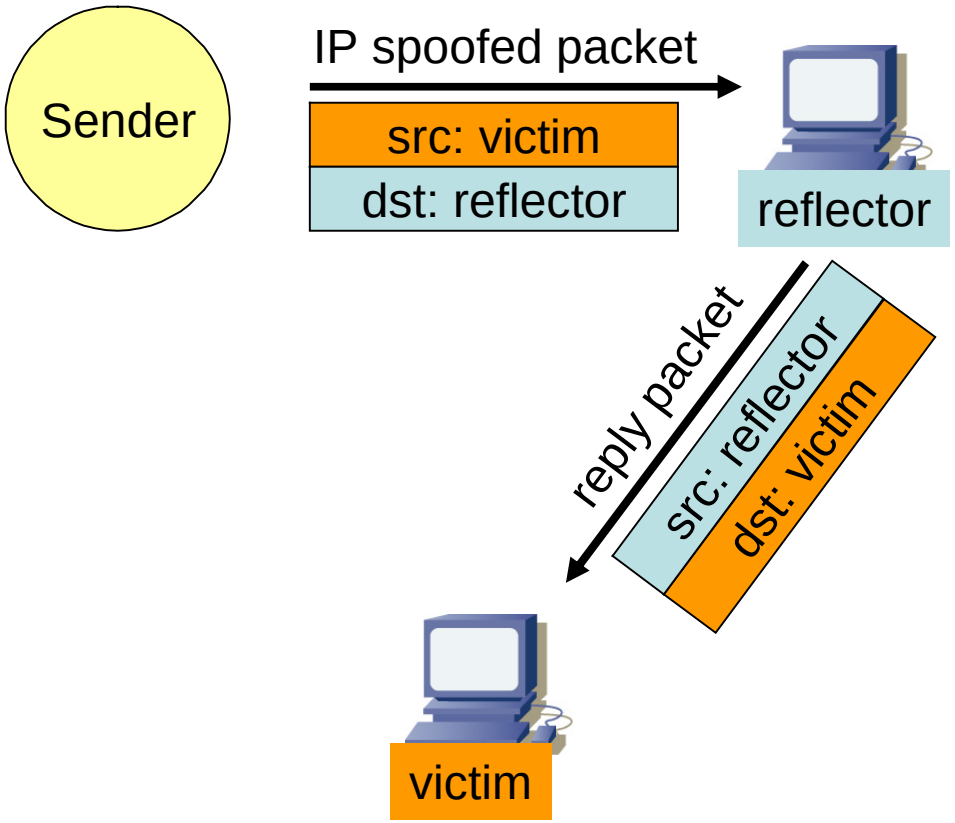
- 送信元を偽装したdns queryによる攻撃
  - 帯域を埋める
  - ‘smurf attacks’に類似

- 攻撃要素は
  - IP spoofing
  - DNS amp

IP spoofing + DNS amp

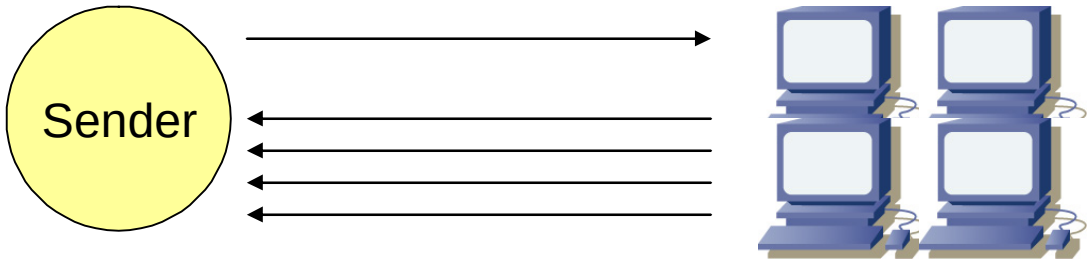
- IP spoofing
  - 送信元IPアドレスを偽装したdns query
  - 反射パケットを利用するため
- DNS amp
  - UDP (簡単に利用できる)
  - 大きな増幅率 =~ 60
  - リゾルバ (dns cache)による分散

反射(reflection)

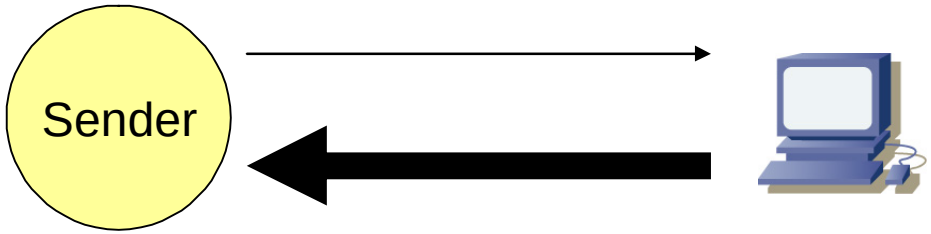


増幅(amplification)

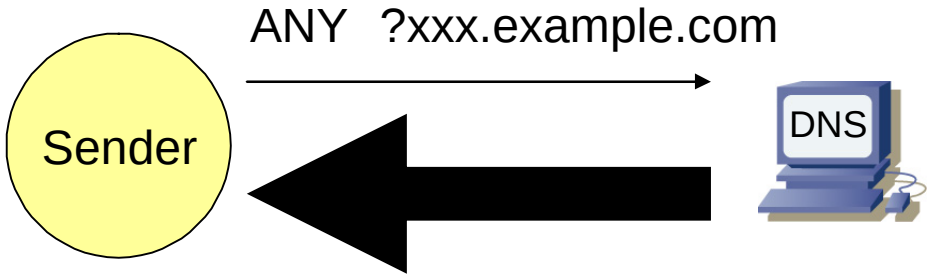
1. multiple replies



2. bigger reply

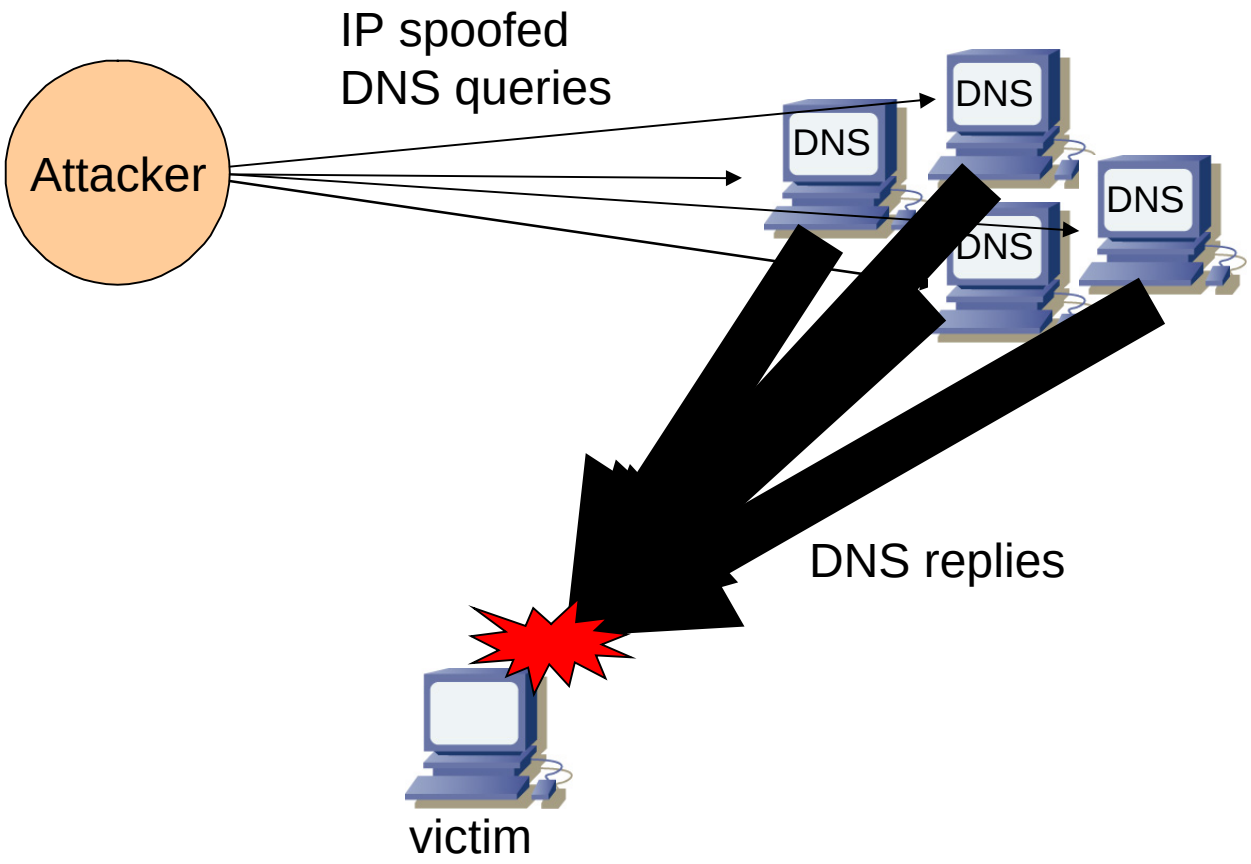


DNS amplification

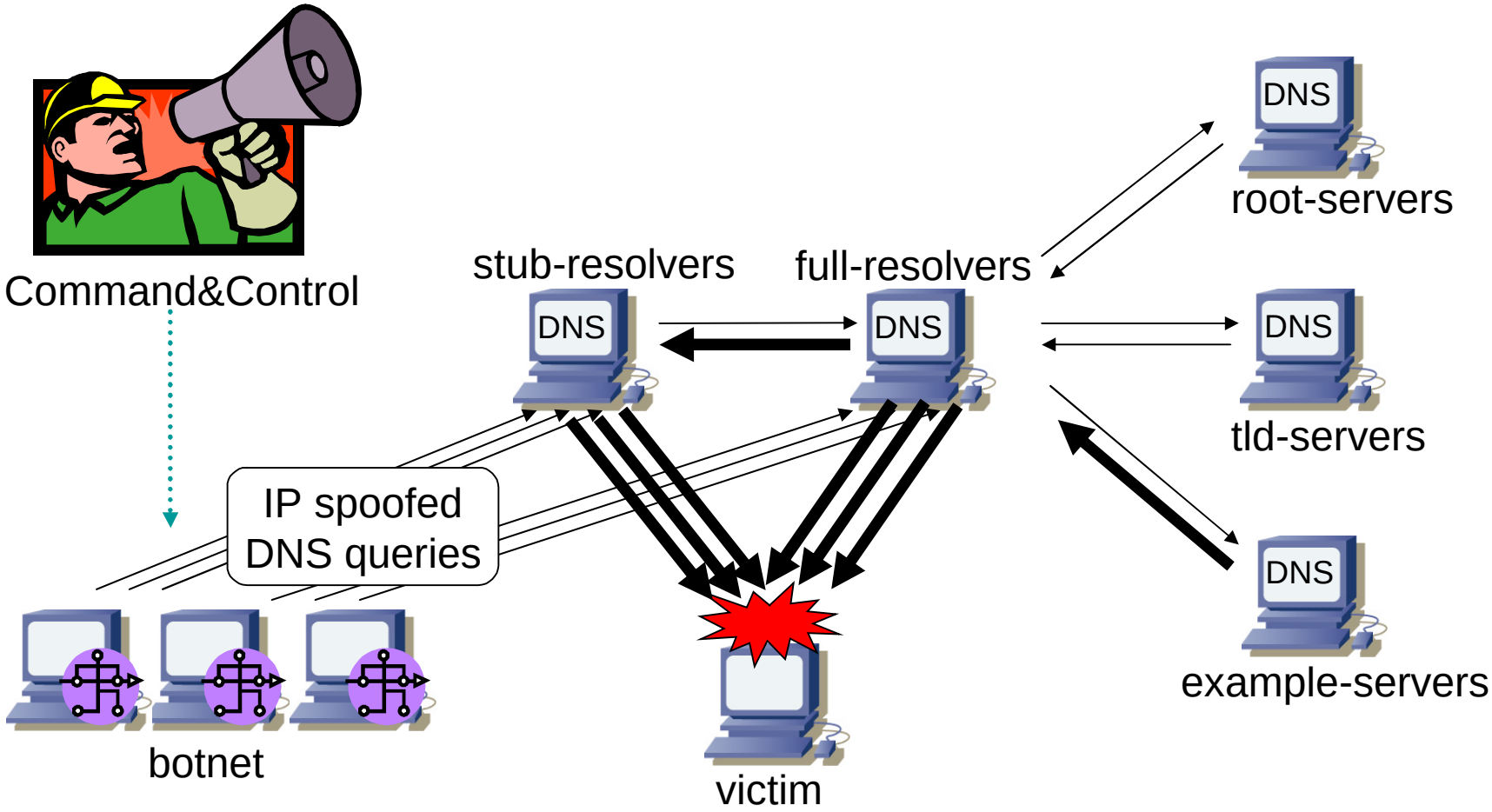


xxx.example.com IN TXT
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX

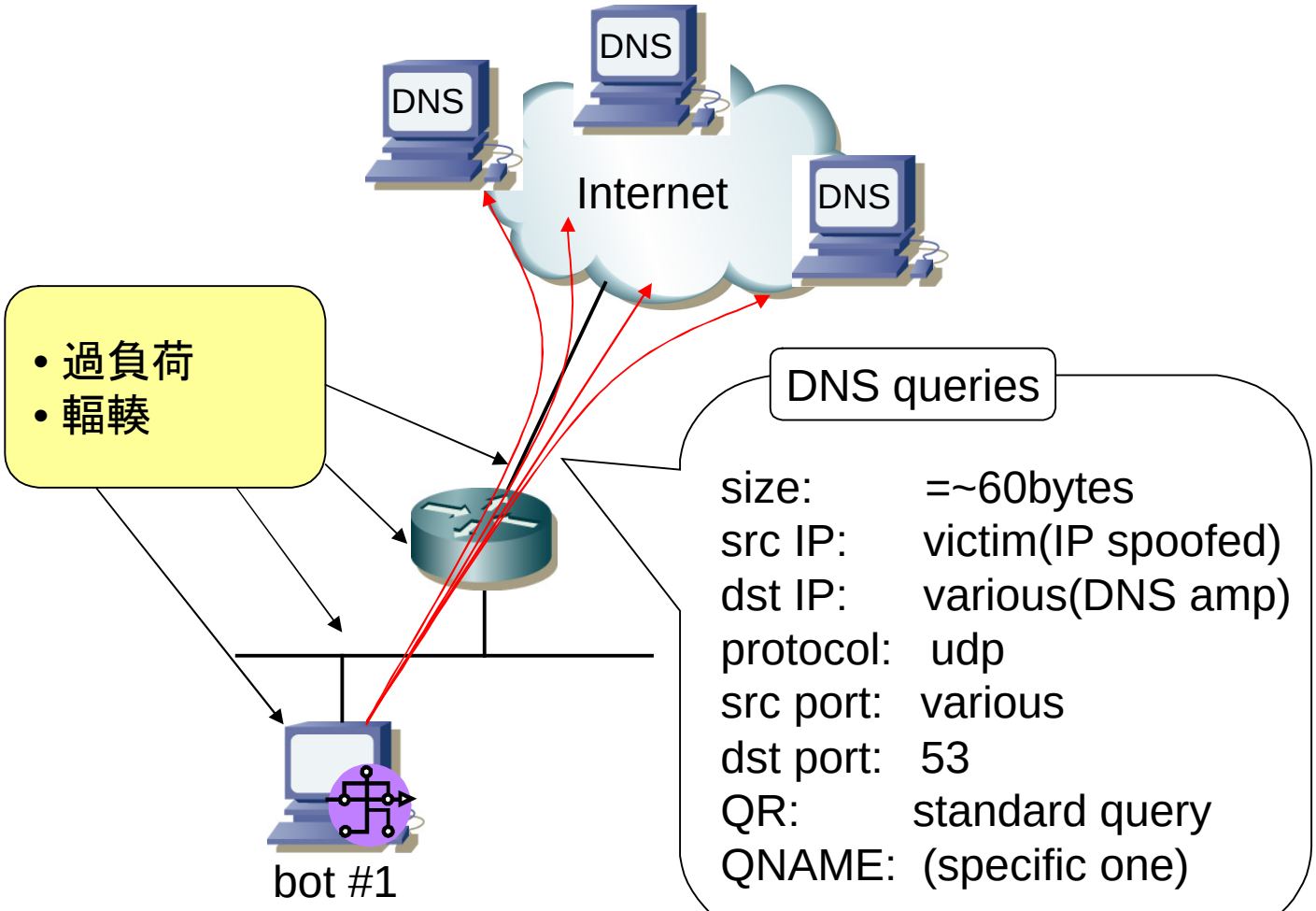
DNS amplification attack



攻撃の相関関係

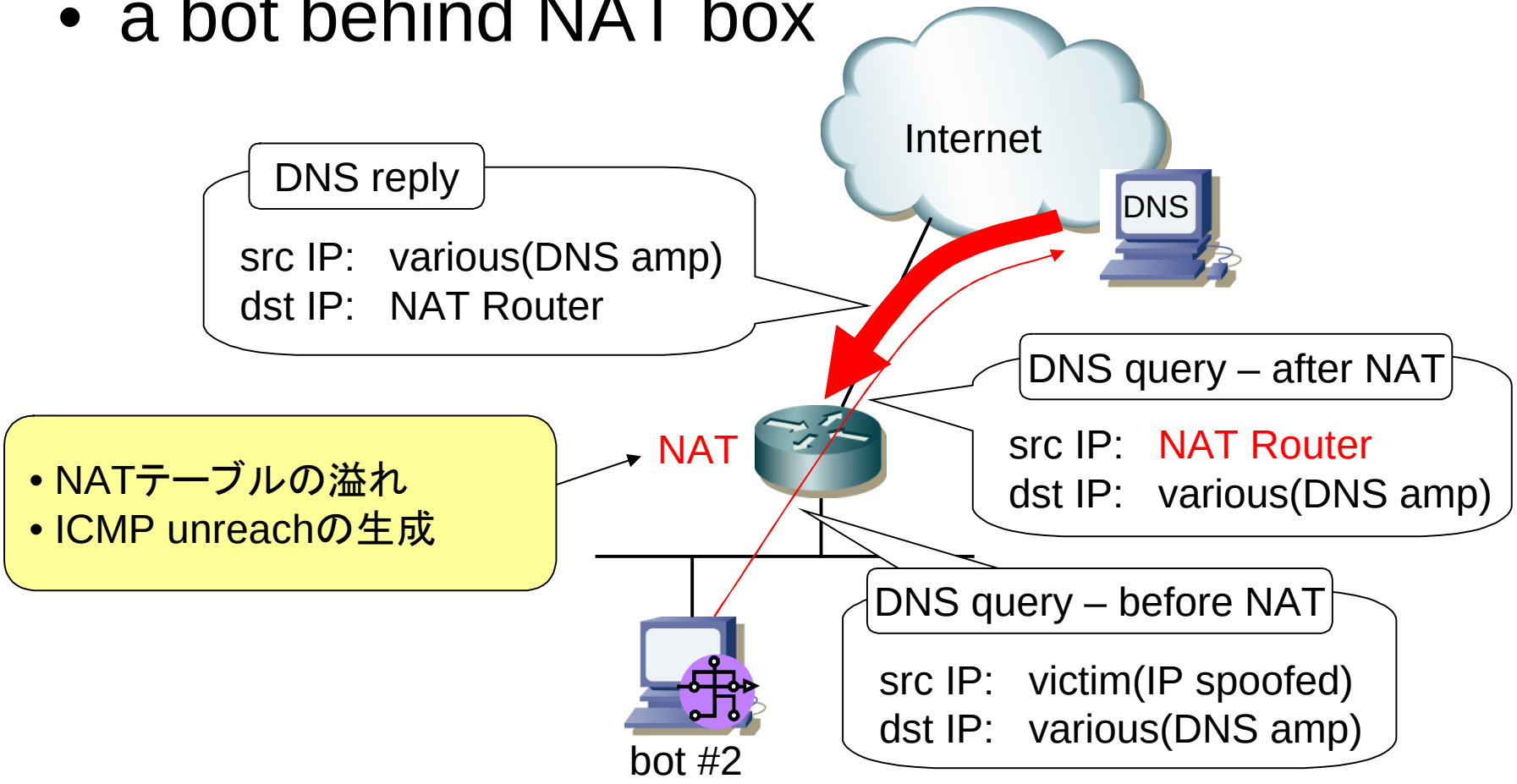


view of bot #1

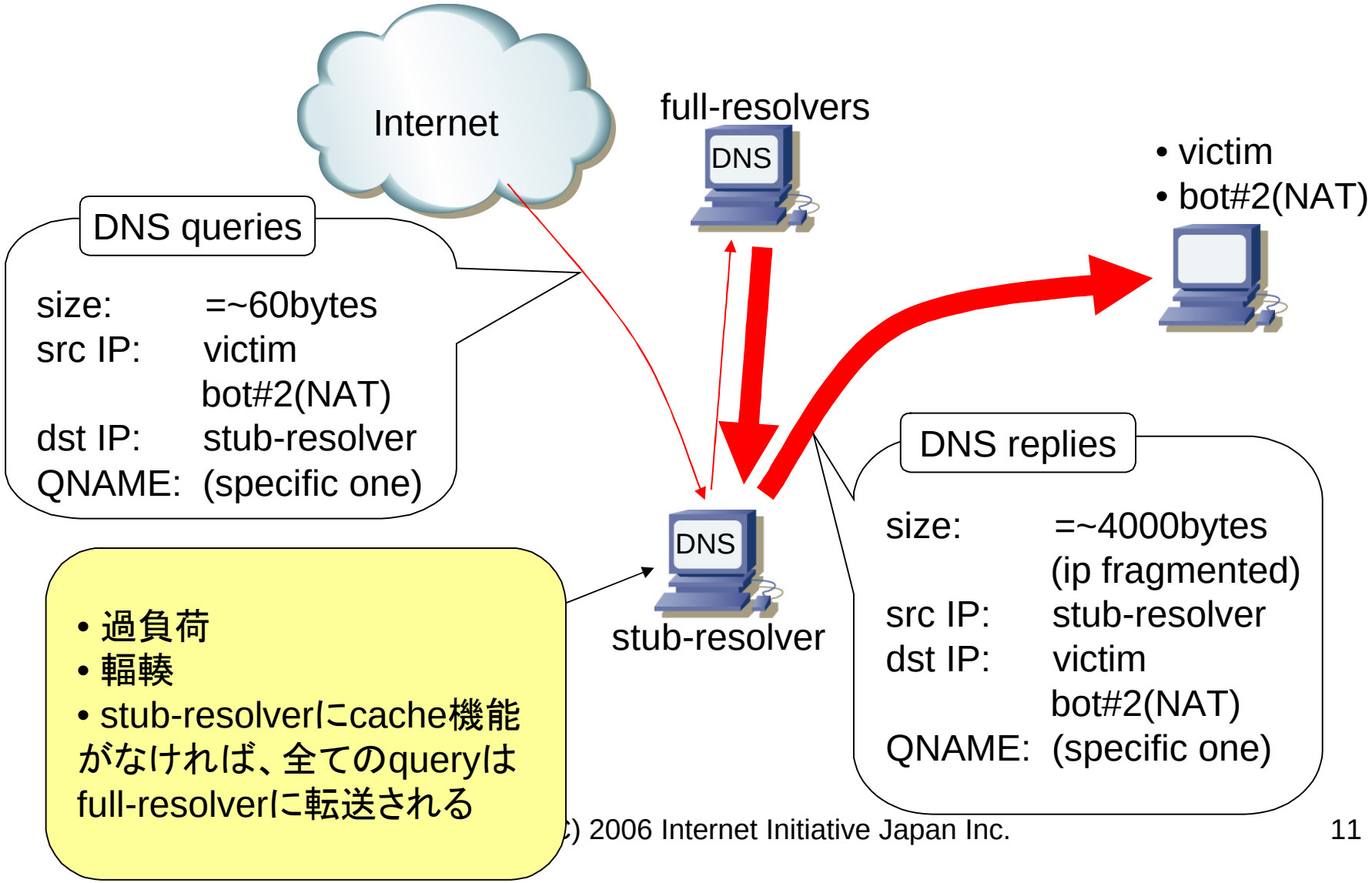


view of bot #2

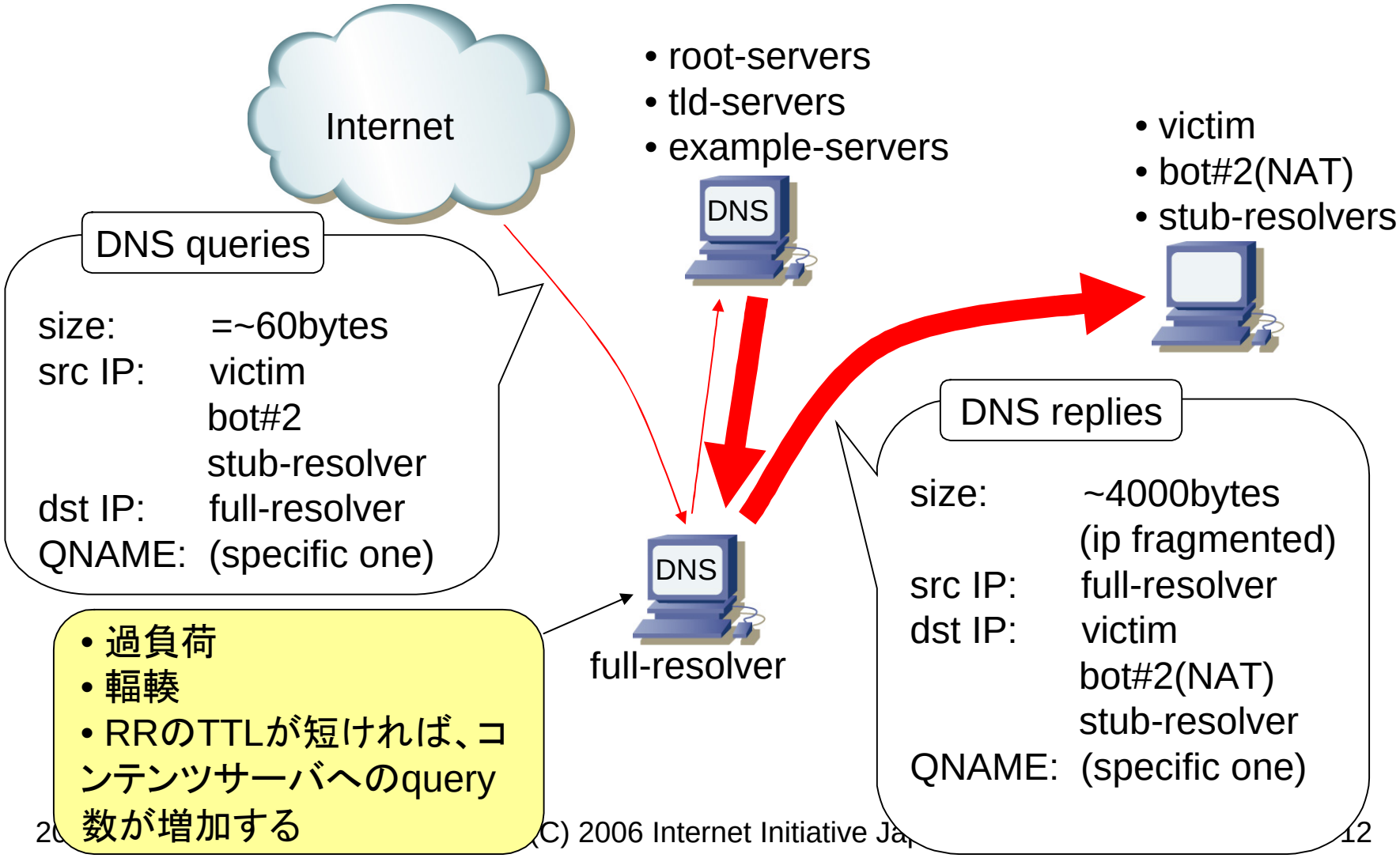
- a bot behind NAT box



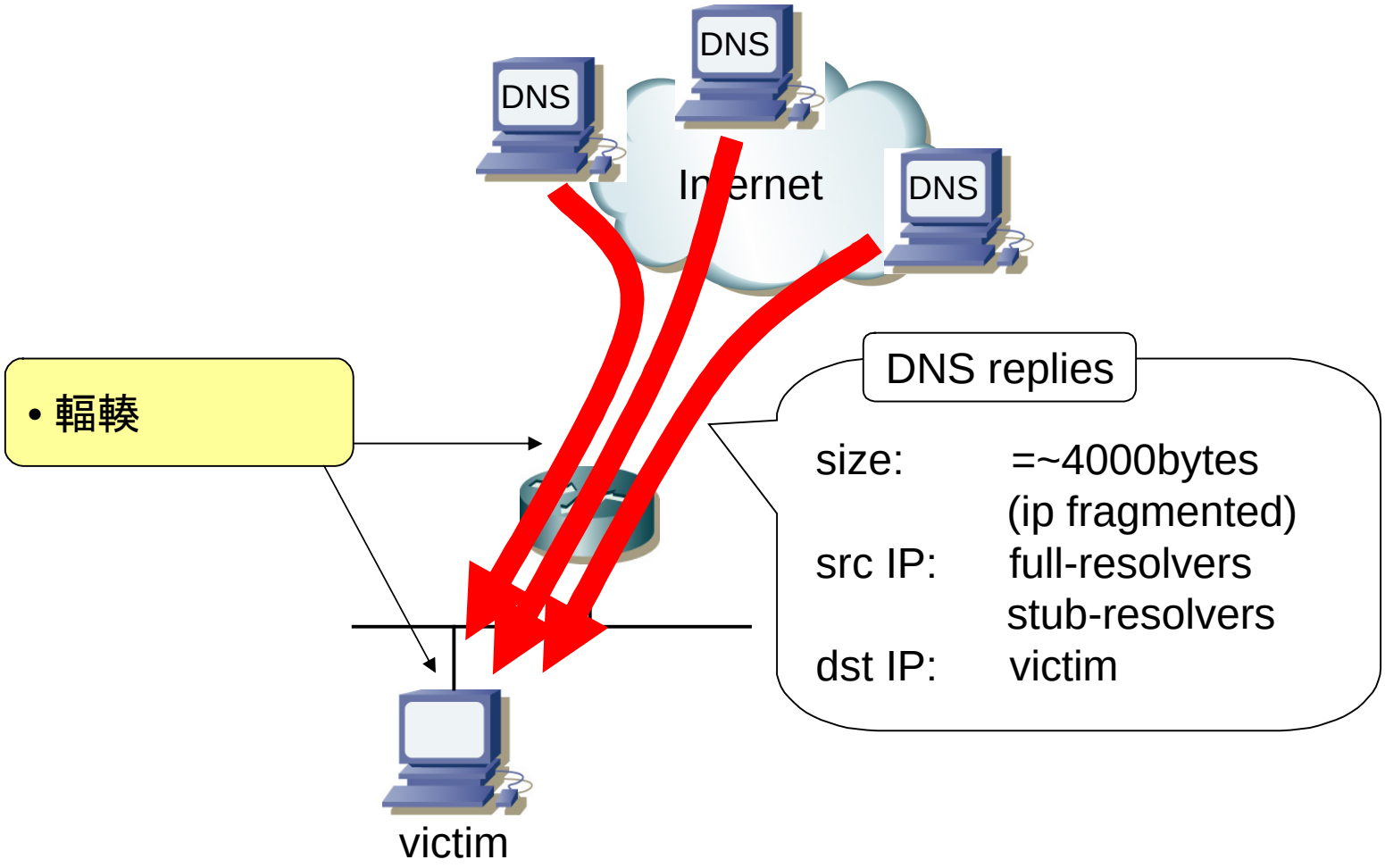
view of stub-resolver



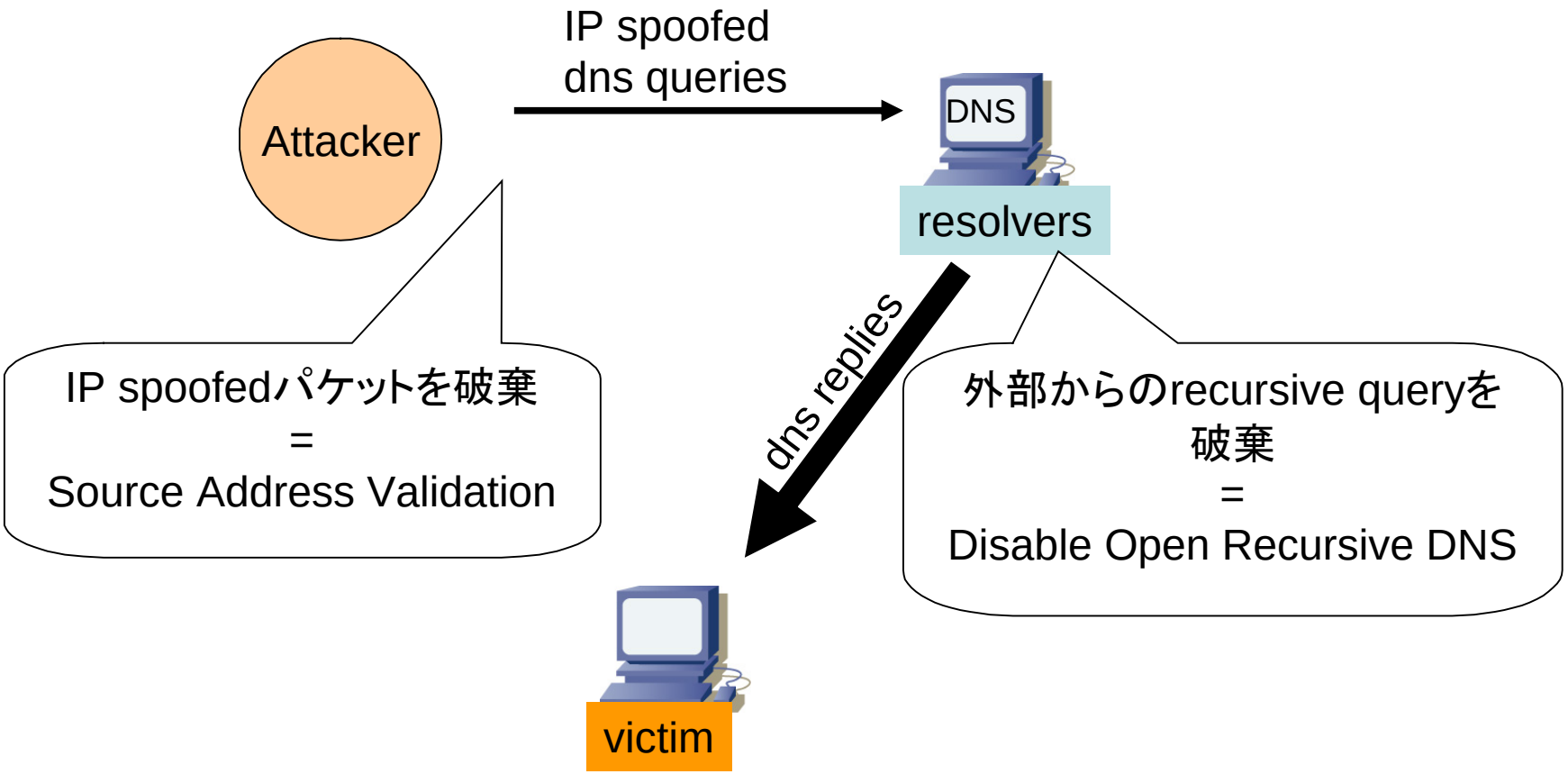
view of full-resolver



view of victim



対策は・・・



Disable Open Recursive DNS

- ‘open relay’なリゾルバがいっぱい
  - ISPのDNSサーバ
  - 各組織のDNSサーバ
  - 幾つかの、ちょっと賢い機器

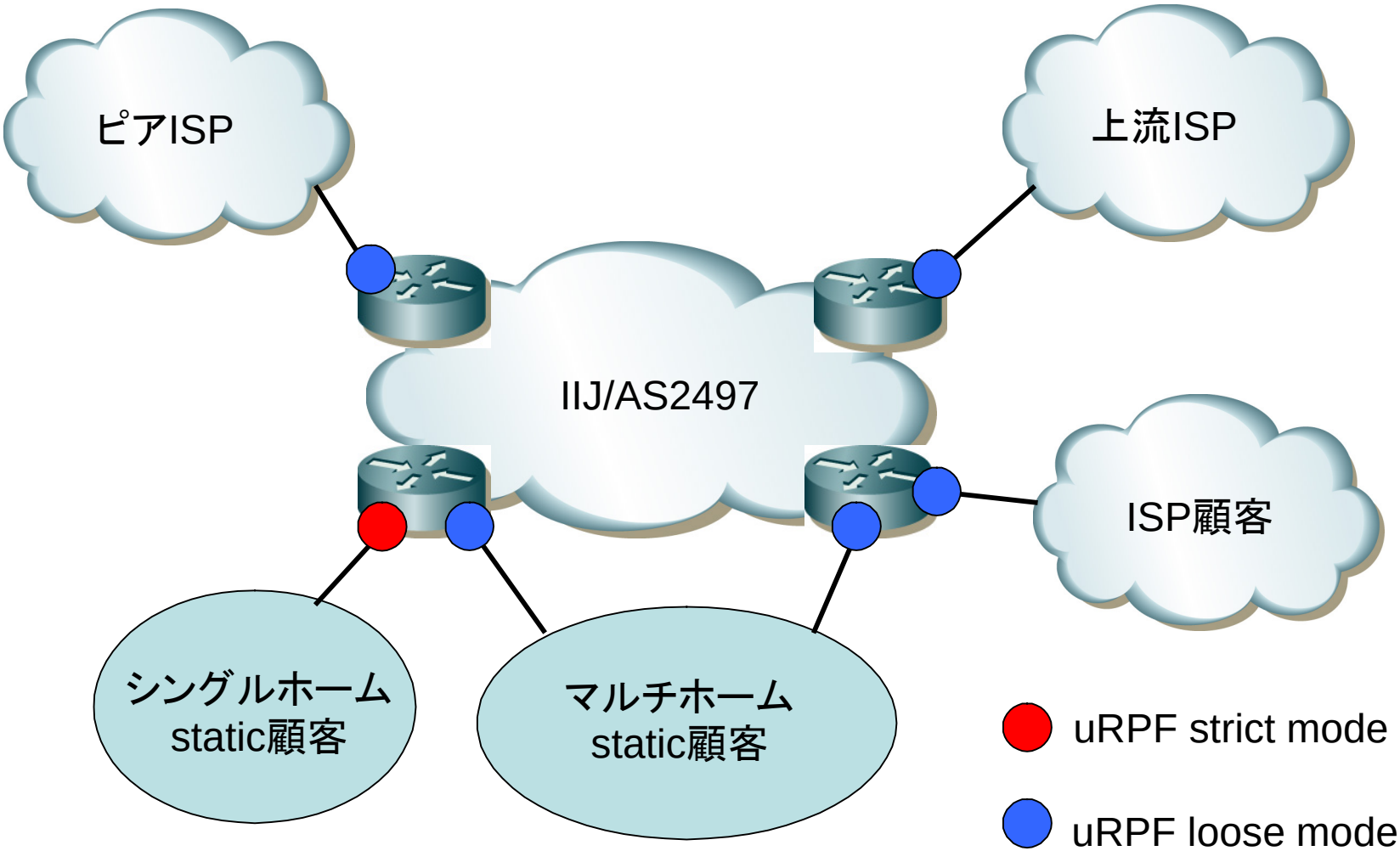
Source Address Validation

- BCP38/RFC2827
  - All providers of Internet connectivity are urged to implement filtering described in this document to prohibit attackers from using forged source addresses...

IIJ/AS2497の場合

- **IIJ、全接続サービスにおいて「Source Address Validation」を導入**
  - http://www.iij.ad.jp/pressrelease/2006/0308.html
- IIJではSource Address Validationの実装にuRPFとACLを利用しています。

IIJの基本ポリシ



CISCO uRPF configuration

uRPF strict mode

```
interface GigabitEthernet0/0
 ip verify unicast source reachable-via rx
```

uRPF loose mode

```
interface GigabitEthernet0/0
 ip verify unicast source reachable-via any
```

Juniper uRPF configuration

uRPF strict mode

```
interface { ge-0/0/0 { unit 0 { family inet {
 rpf-check;
} } } }
```

uRPF loose mode

```
interface { ge-0/0/0 { unit 0 { family inet {
 rpf-check { mode loose; }
} } } }
```

世の中の動き

- RIPE – IP Anti-Spoofing Task Force
  - EU地域での状況調査
  - documentの作成、公開
  - RIRでanti-spoofing実装を推進する手法の模索

参照先

- AL-1999.004 – DoS attacks using the DNS
  - http://www.auscert.org.au/render.html?it=80
- The Continuing DoS Threat Posed by DNS Recursion
  - http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf
- SAC008 – DNS Distributed DDoS Attacks
  - http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

END