Internet Week 2006 (DNS DAY)

NTT Communications OCN
吉村　知夏 / yosimura@ocn.ad.jp
2006/12/06

1

アウトライン

- **AS112 report**
  1. **AS112とは何か**
  2. **プライベートアドレスクエリの現状**
  3. **OCN AS112トラフィック**
  4. **まとめ**

2

1. AS112とは何か

3

1-1. AS112とは

- プライベートアドレスのクエリを処理
  - 10.0.0.1の逆引きクエリ、168.192.in-addr.arpaのSOAクエリなど
  - NXDOMAINを返答する
- 世界に48箇所ほど設置されている (AS112 Project)
- 日本では、WIDE Project と OCNが設置

4

1-2. クエリの流れ

- AS112(のDNS)は…
  - プライベートアドレスの権威サーバ
  - blackhole-{1,2}.iana.org
  - prisoner.iana.org
- レコードを見ると…
  - NSレコード

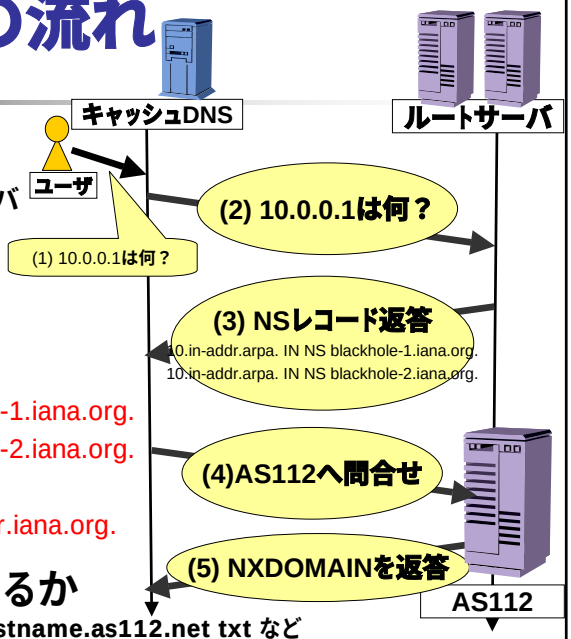
    10.in-addr.arpa. IN NS blackhole-1.iana.org.

    10.in-addr.arpa. IN NS blackhole-2.iana.org.
  - SOAレコード

    10.in-addr.arpa IN SOA prisoner.iana.org.
- どこのAS112を使っているか

  # dig @blackhole-1.iana.org hostname.as112.net txt など

  hostname.as112.net. 15 IN TXT "OCN, NTT Communications" "Tokyo, Japan"



1-3. なぜあるのか

- **プライベートアドレスのクエリは、本来閉じたネットワークで処理されるべき**
- **なぜかインターネットに流れている**
- **ルートサーバへのゴミクエリを減らしたい**
  - NANOG26 Duane Wessels(CAIDA)の発表
    - **Fルートへのクエリのうち90％超がゴミ**
    - **そのうち、プライベートアドレスのクエリは1.6％**

1-4. ゾーンファイルの中身(参考)

- **10.in-addr.arpaの中身**

```
$ORIGIN .
$TTL 604800     ; 1 week
10.in-addr.arpa         IN SOA  prisoner.iana.org.
hostmaster.root-servers.org. (
                                2002040800 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                604800     ; minimum (1 week)
                                )
                        NS      blackhole-1.iana.org.
                        NS      blackhole-2.iana.org.
```

- **Internet Draft内に詳細があります**

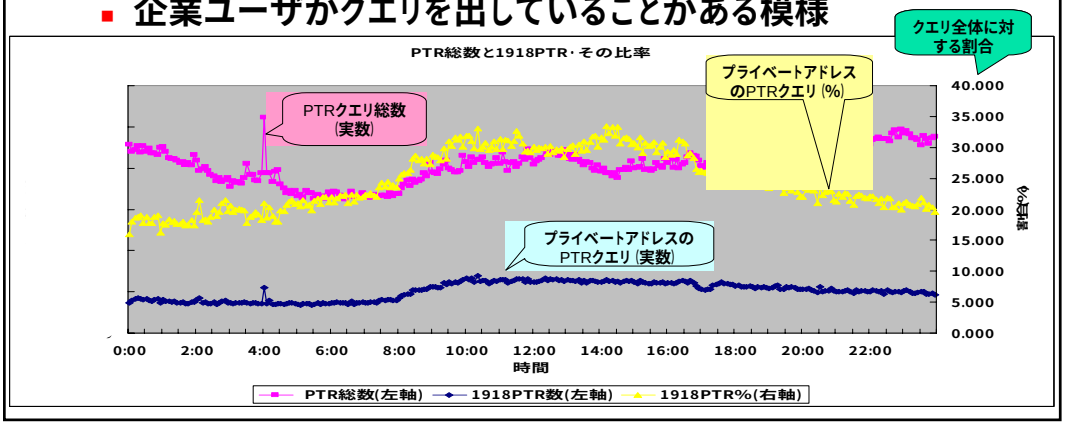
7

2. プライベートアドレスクエリの現状

8

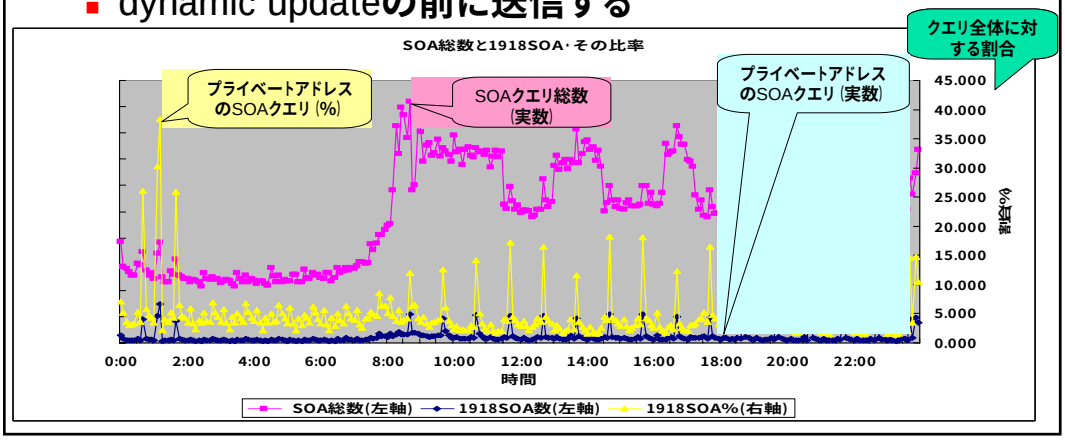
2-1. キャッシュサーバの現状 (1)

- **Private address のクエリ (逆引き)**
  - 逆引きクエリの20% (全体から見ると4%くらい)
  - 秒間数百クエリほど (キャッシュのおかげか)
  - 企業ユーザがクエリを出していることがある模様



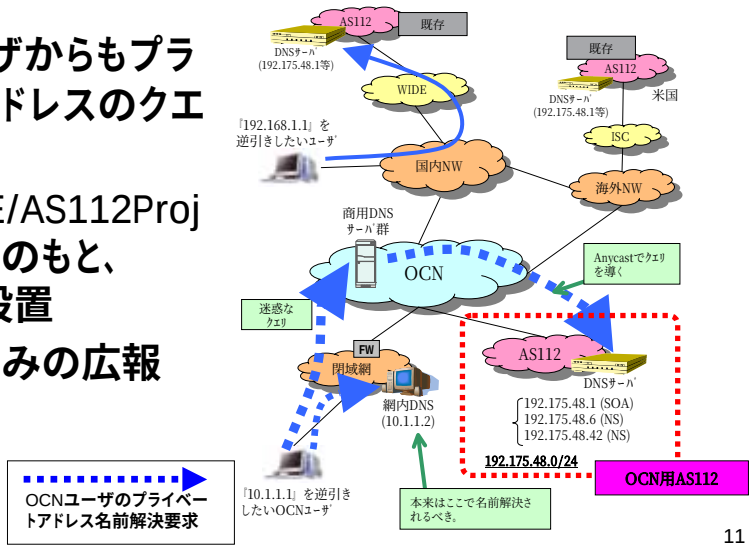
2-2. キャッシュサーバの現状 (2)

- **Private address のクエリ (SOA)**
  - SOAクエリの5〜20%
  - dynamic updateの前に送信する



2-3. OCN内AS112の設置

- OCNユーザからもプライベートアドレスのクエリを観測
- ISC/WIDE/AS112Projectの協力のもと、AS112を設置
- AS4713のみの広報



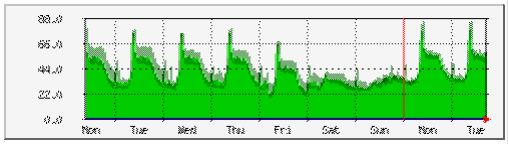
11

3. OCNのAS112トラフィック

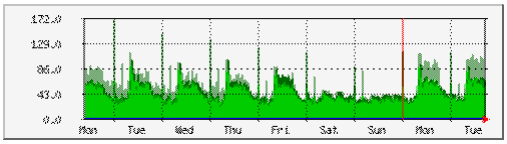
12

3-1. OCNのAS112トラフィック

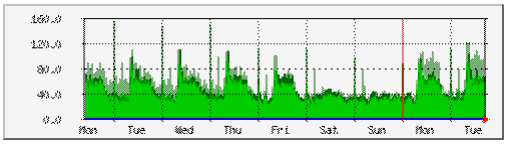
- 秒間数百クエリ
- キャッシュが効いていると思われる
- OCNのDNSサーバ、企業ユーザ、マスユーザなど
- クエリ内訳
  - Dynamic Update: 30%
  - SOA：48%
  - PTR：21%
  - その他(A,TXT,ANYなど)：1%



192.175.48.1



192.175.48.42

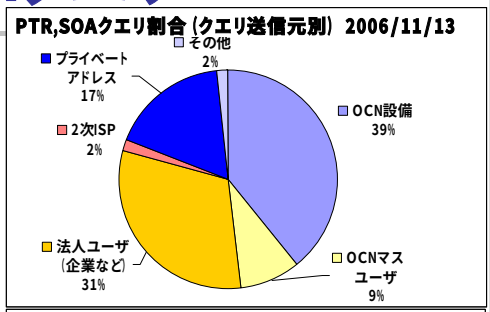


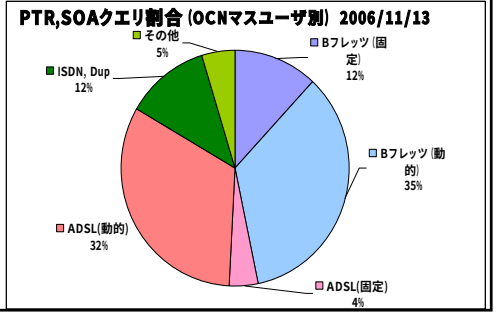
192.175.48.6

13

3-1. PTR,SOAクエリ

- OCN設備（DNSサーバ）からのクエリが多い
- ソースIPアドレスがプライベートアドレスになっているものもある
  - 処理のしようがない
- マスユーザの状況
  - Bフレッツ動的、ADSL動的からのクエリが7割
  - Update前のSOAクエリ



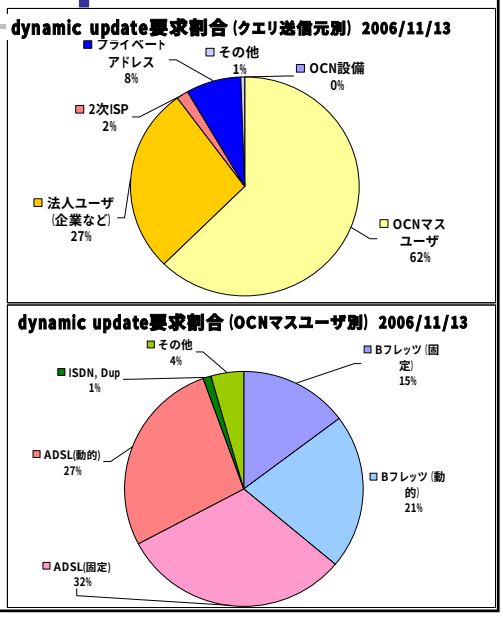


3-2. dynamic updateクエリ

- プライベートアドレスのupdateクエリ

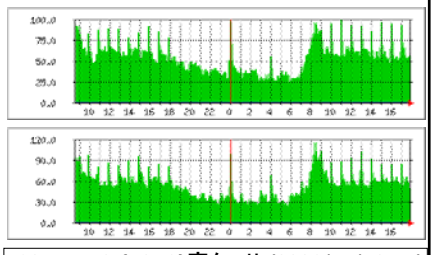
8.0.168.192.in-addr.arpa. PTR ***.local.
5.8.14.10.in-addr.arpa. PTR hostname.***co.jp

- 社内のホスト名が漏れてしまう可能性がある
- マスユーザが6割を占める (Windows端末と推測される)
- 一度確認してみてください

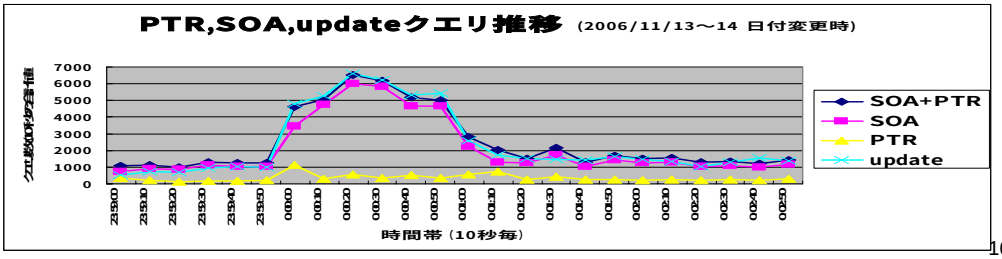


3-3. 毎時0分のスパイク

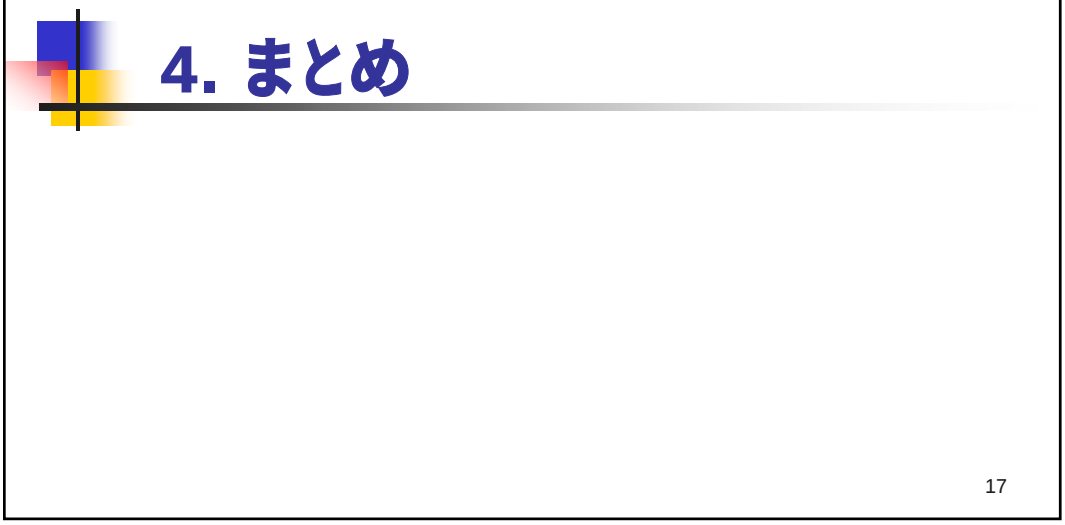
- 毎時0分にSOAクエリのスパイク
- 午前0時が最も多い
  - updateクエリも多い
- Windowsの仕様か？

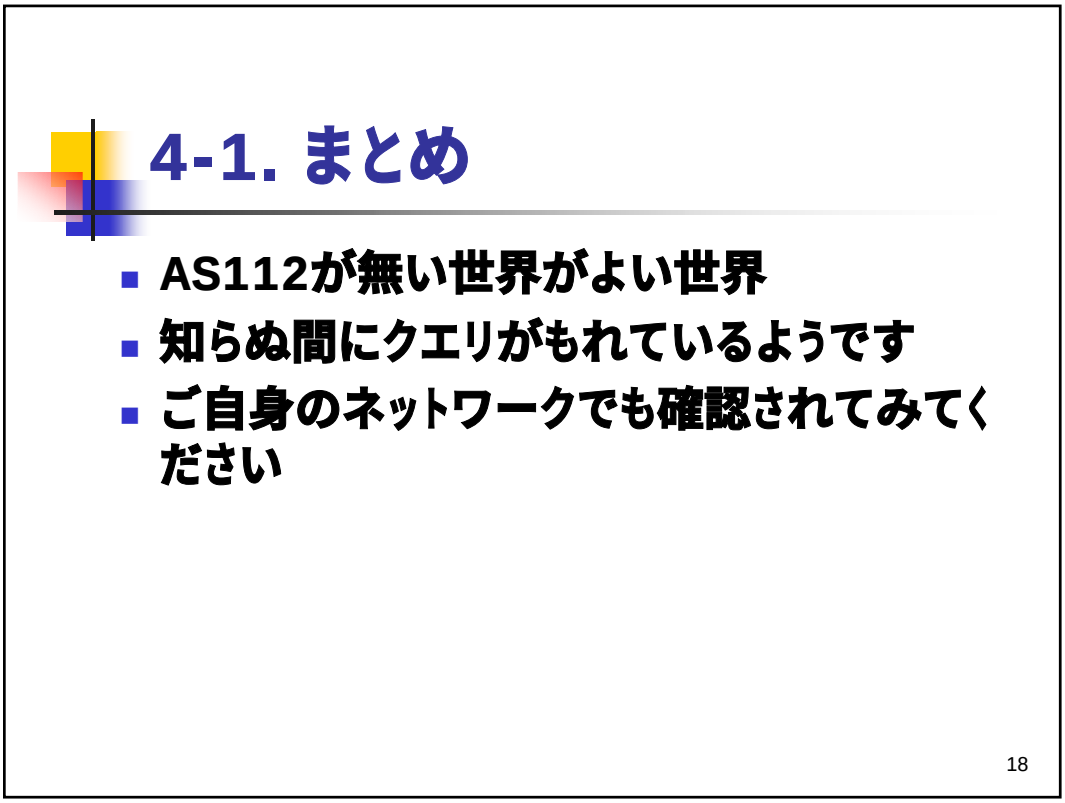


192.175.48.{42, 6}宛クエリ (2006/11/13-14)



16


4. まとめ
17


4-1. まとめ
AS112が無い世界がよい世界
知らぬ間にクエリがもれているようです
ご自身のネットワークでも確認されてみてください
18

参考情報

- **AS112 Project**
  http://public.as112.net/
- **Internet Draft**
  - **AS112 Nameserver Operations**
    http://www.ietf.org/internet-drafts/draft-jabley-as112-ops-00.txt
  - **I'm Being Attacked by PRISONER.IANA.ORG!**
    http://www.ietf.org/internet-drafts/draft-jabley-as112-being-attacked-help-help-00.txt
  - **Locally-served Zones**
    http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-00.txt

19

Special Thanks to:

- **NTTプラットフォーム研究所の皆様**

20