Internet Week 2005
-DNS DAY-
OCN Lameクエリの現状など

NTTコミュニケーションズ（OCN）
吉村　知夏 / yosimura@ocn.ad.jp

今日の概要

1. Lameクエリの現状
   - OCNのトラフィックデータより
   - エンドユーザから来るクエリの現状
2. “危ない”ドメインの現状(簡単に)
   - NSのwhois登録がExpireしているドメイン
   - OCNでの現状、対応方法

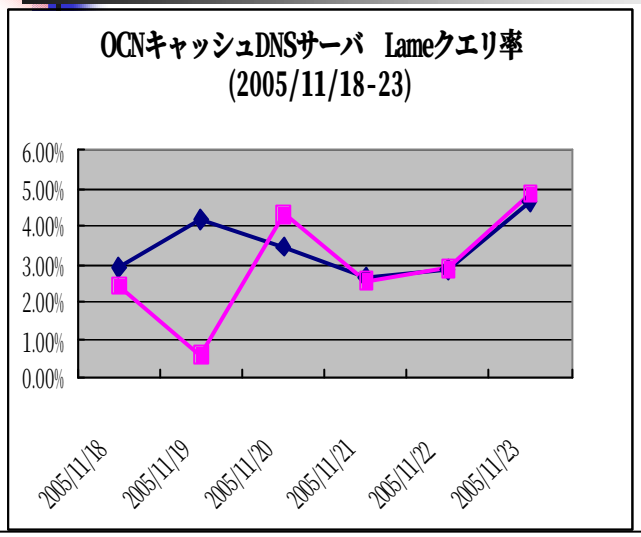
1. Lameクエリの現状

1-1. Lameとは

- **Lameとは**
  - 権限委譲されたDNSサーバが正しく動いていない状態
  - 権限委譲設定（NSレコード）は存在するが、委譲先のDNSサーバが応答しない　など
- **無駄なトラフィックを引き起こす**
- **OCNでの現状は？**
  - **“Lameになる”クエリは？**

1-2. Lameになる割合

(OCN キャッシュDNSサーバより)

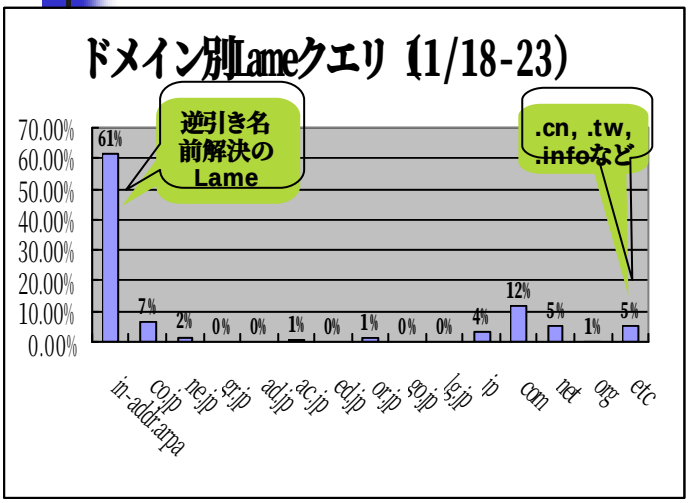


- OCNのキャッシュDNSサーバで調査
  (2005/11/18-23)
- 総クエリのうち、3～4%前後がLameになる
- なぜ？

5

1-3. Lameクエリの内訳

(OCN キャッシュDNSサーバより)

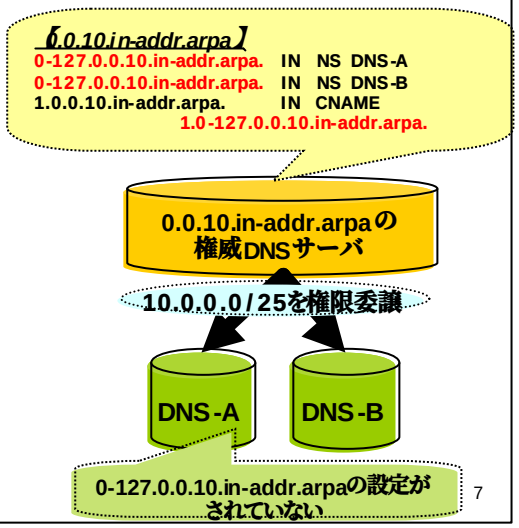


- in-addr.arpa（逆引き）の名前解決時にLameになっている（およそ60％）
- comもやや多め

6

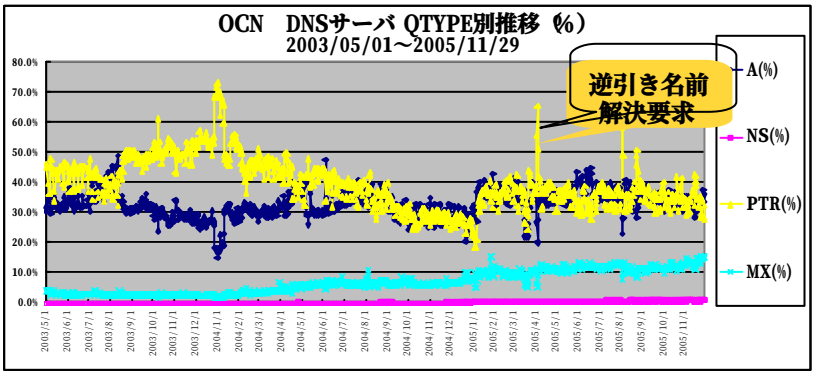
1-4. 逆引きのLame

- なぜ逆引きLameが多いのか
- Cクラス未満の権限委譲が上手くいっていない
  - /25以下の権限委譲
  - 委譲設定がわかりにくい
  - CNAMEで委譲する方法がよく紹介されるが…



1-5. 逆引きの需要

- 逆引きってそんなに重要なの？
- クエリ全体の40%を占める



1-6. Lameを減らすために

- **逆引きの委譲間違いを減らす**
  - /25以下の権限委譲方法がトリッキー
  - そもそもあまり真面目に設定してない？
    - OCNでは、委譲時に確認をしています
- **皆さんの逆引き委譲状態は大丈夫ですか？**
  - 思ったよりも、逆引きは使われている
  - OCN DNSトラフィックの4割は逆引き要求

9

2. “危ない”ドメインの現状

10

2-1. ドメイン乗っ取り問題

- **乗っ取りの仕組み**

  ocn.jp. IN NS dns1.example.com

- **ocn.jpのNSレコードである”example.com”が、誰でも取得できる状態に**
  - example.comを取得すれば、” dns1.example.com”が立てられる
  - ” dns1.example.com”が立てられれば、ocn.jpのDNSとして振舞える
- **ocn.jpを乗っ取ることができる！**

11

2-2. OCNでの現状

- **NSレコードの右側がexpireしているドメイン**
  - **OCNではどのくらいあるのか？（JPドメイン中）**
    - **【汎用ドメイン】0.03％以下　【属性ドメイン】0.01％以下**

```
+++.co.jp.      IN  NS  ns-XXX.ocn.ad.jp.
+++.co.jp.      IN  NS  ns.XXX.jp.
```

- **OCNでの対応**
  - お客様に通知の上、NSレコードの削除、修正をしている
  - お返事を頂けないお客様も多い
  - JP以外のドメインについては未調査

12