

# ドメインサーバーオーダーとIPv6

NTT 情報流通プラットフォーム研究所

豊野 剛

toyono@nttv6.net

# 大規模DNS Cacheサーバの運用って(ISP編)

*NTT Information Sharing Platform Laboratories*

- サービスクオリティに直結
  - 応答速度がユーザの(体感)ネットワーク品質に直接影響
- クエリ処理が大変
  - 処理クエリ数が膨大
    - RootやTLDサーバと同様, CPU負荷を気にする
  - ユーザ ⇔ Cache ⇔ Authサーバ
    - ユーザ, 権威サーバどちらが悪くても困る
    - 中間管理職状態

# Cache ⇔ Authoritative間クエリで キャッシュサーバが困ること

*NTT Information Sharing Platform Laboratories*

## クエリ増大の例

- Lame Delegation
- Referralがピンポンする, など

## 負荷増大の例

- TCP port53がフィルタされている
- ServFailでNegative Cacheされず, 高負荷になる, など

# Cache ⇔ ユーザ 間クエリで キャッシュサーバが困ること

*NTT Information Sharing Platform Laboratories*

## クエリ増大の例

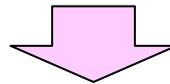
- Wormによる大量クエリ
  - Mydoom, Antinny, Netsky, 各種Botなど
- しょんぼり{ハード/ソフト}ウェアによる大量クエリ
  - イケてないBBルータ, NTPクライアントソフトなど
- 各種バックグラウンドサービス(特にWindows系に多い)
  - WPAD(Web Proxy Auto-Discovery)
  - uPnPサービス
  - DDNS自動登録機能
  - Active Directory, などなど

...を踏まえて,  
今回はユーザOSのDNSレゾルバの話

# OSのドメイン自動補完機能とは

NTT Information Sharing Platform Laboratories

- DNSでIPアドレスが得られなかった場合, 自動的にドメイン名を推測補完して再度問い合わせる
  - ユーザにとっては利便性が高い
    - (例) “host” を牽いただけで  
→ host.com → host.net → host.org ...推測して接続
  - 以下のようなドメインsuffixが指定される
    - DHCP割り当て, インターフェース, マイコンピュータ設定(Win), resolv.conf(UNIX)などで設定されたドメイン

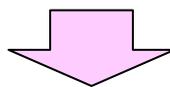


ユーザ(アプリケーション)の1つの問い合わせが  
数倍のクエリに展開される

# アプリケーションのドメイン自動補完機能とは

NTT Information Sharing Platform Laboratories

- さらに, アプリケーションによっては自動的にドメインを推測するものがある
  - (例) ブラウザなどでは入力/クリックされたURIが存在しなかった場合, 独自にドメイン自動補完する
    - Mozilla: www.  
を付与する(クエリは2倍に)
    - IE: MSNサーチ → .com → .org → .net → .edu  
を付与する(クエリは5倍に)



ユーザの1つの問い合わせが  
(更に)数倍のクエリに展開される



# 次期Windowsでは...

*NTT Information Sharing Platform Laboratories*

1. インストール初期状態でDefault IPv6 enable  
→DNSクエリは常にAAAA, Aの2倍発生
2. OSのドメイン自動補完
  - XP SP2と同等
  - 存在しなかった場合, さらにクエリ発生
3. アプリケーションのドメイン自動補完
  - XP SP2と同等 (例: Internet Explorer)
  - 存在しなかった場合, さらにさらにクエリ発生

# IPv6対応 + ドメイン自動補完で何が起こるか

NTT Information Sharing Platform Laboratories

- UNIX系(例: BSD)
  - AAAA, A共にSearchドメイン数回分繰り返す  
(4,6→4,6→4,6...)
- Windows系
  - AAAA, A共にSuffixドメイン数回分繰り返す  
(6,6,6,4,4,4→6,6,6,4,4,4...)

AAAAが全部FailするまでAを牽かない  
→2倍以上になる  
可能性大

**bsd** # telnet q.ocn.ne.jp

```
A?      q.ocn.ne.jp
AAAA? q.ocn.ne.jp
A?      q.ocn.ne.jp.co.jp
AAAA? q.ocn.ne.jp.co.jp
A?      q.ocn.ne.jp.ocn.ne.jp
AAAA? q.ocn.ne.jp.ocn.ne.jp
A?      q.ocn.ne.jp.com
AAAA? q.ocn.ne.jp.com
```

存在すると  
ここで終了

**win** # telnet q.ocn.ne.jp

```
AAAA? q.ocn.ne.jp
AAAA? q.ocn.ne.jp.co.jp
AAAA? q.ocn.ne.jp.ocn.ne.jp
AAAA? q.ocn.ne.jp.com
A?      q.ocn.ne.jp
A?      q.ocn.ne.jp.co.jp
A?      q.ocn.ne.jp.ocn.ne.jp
A?      q.ocn.ne.jp.com
```

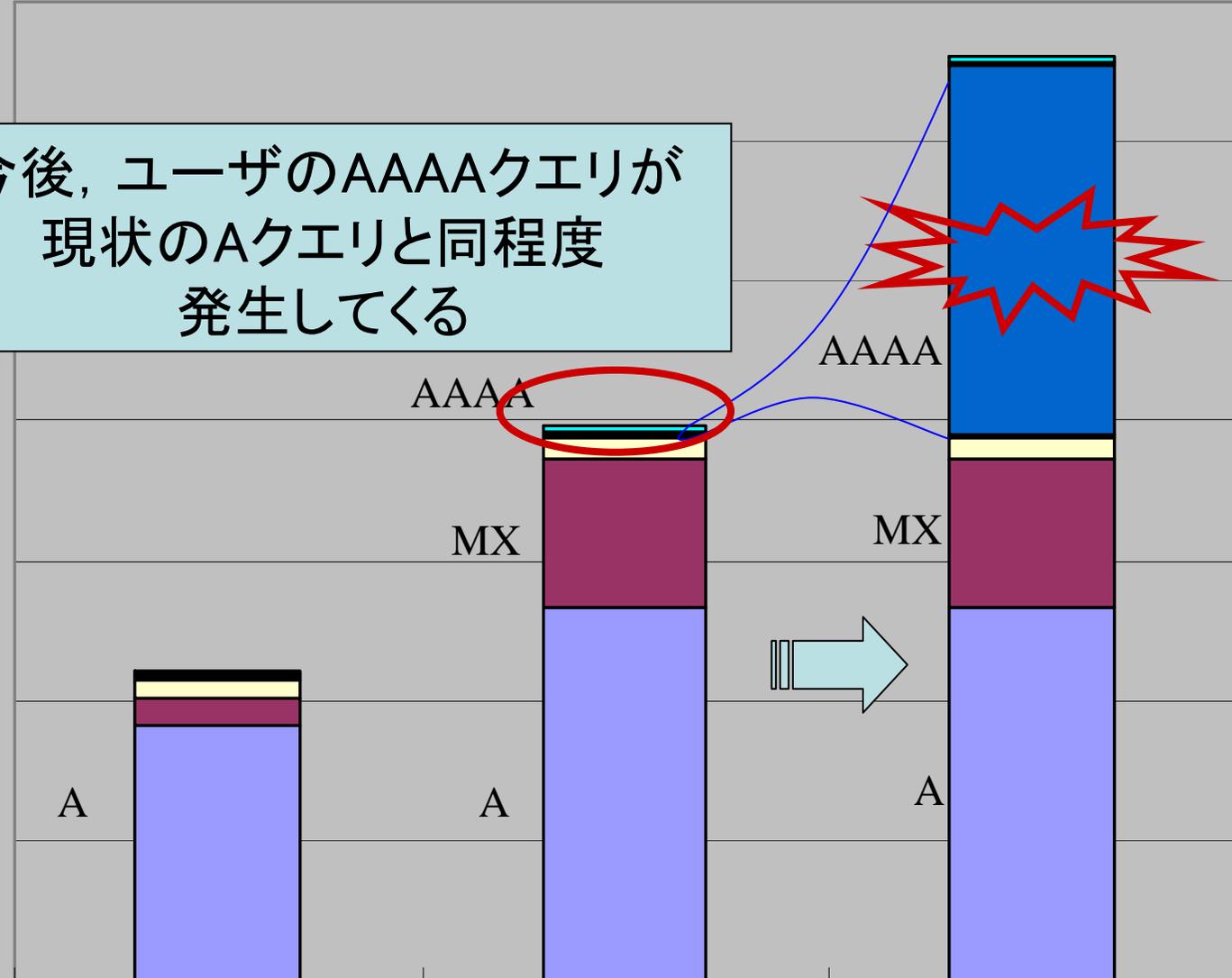
存在したとしても  
ここまでかかる!

というユーザOSの挙動を  
ネットワーク運用の立場から考えると...

# DNSキャッシュサーバへのクエリ推測

tories

今後、ユーザのAAAAクエリが  
現状のAクエリと同程度  
発生してくる



- other
- TXT
- SRV
- ANY
- A6
- AAAA
- CNAME
- SOA
- NS
- PTR
- MX
- A



Netsky以前(2004/2) 現在(2005/10/3) Vista後(2006末以降)

# 皆で考えておきたいこと

*NTT Information Sharing Platform Laboratories*

- クエリが2倍になっても大丈夫ですか？
  - 今年発売のWindowsは標準でIPv6 Enable
- 考えておきたいこと
  - Resolverの挙動はユーザ利便性とTrade Off
  - しかしユーザクエリを受けるのはISP等のDNS キャッシュサーバ
  - Authoritative Server側のAAAA応答は大丈夫？

Fin.