DNSSECの導入にむけて
～課題と検証～

白井出　　藤原和典
株式会社日本レジストリサービス

於：2009/09/04 DNSOPS.JP BoF

DNSSECの対応状況

- いくつかのTLDがDNSSEC対応済or 対応の予定を表明
  - gTLD
    - .ORG .GOV .MUSEUM
    - VeriSign (.com .net等)も対応表明
  - ccTLD(試験運用を含む)
    - .BG .BR .CZ .PR .SE .TH
  - .JPも2010年中をめどに
    - http://jprs.jp/info/notice/20090709-dnssec.html
- ROOTゾーンのDNSSEC対応も時間の問題
  - アナウンスなど
    - http://www.nist.gov/public_affairs/releases/dnssec_060309.html
    - http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
  - 年内は無理っぽいという話もちらほらと…
- いずれにしても来年か再来年くらいにはDNSSECが身近にやってきます

機能の検証

- 対応済みのTLDなどを使って試してみよう
  - IANAテストベッド
    - IANAによる技術検証用の仮想Root。基本的に本物のNSにDS設定が増えているというもの。これをroot.hintとして設定して使う。
    - https://ns.iana.org/dnssec/status.html
  - dnslab.jp
    - JPRSで検証用に使っているDNSSEC署名済みのドメイン。DLVなどにも登録されている。
  - とはいっても実際に設定するのはめんどう？

そんな人のために公開の検証サーバがあります。

公開の検証サーバ

- DNS-OARCが公開している公開の検証サーバがあります
  - DLVを参照してます
    - 149.20.64.20 (running BIND 9)
    - 149.20.64.21 (running Unbound)
    - 149.20.64.22 (IANA-testbed, running BIND 9)
  - 詳細は以下を参照
    - https://www.dns-oarc.net/oarc/services/odvr

検証をやってみよう

- 以下を検証の設定をしていない普通のサーバと比較してみよう

QNAME	TYPE	ANSWER
www.iis.se	A	-> AD=1でA RRSet
www.isc.org	A	-> AD=1でA RRSet
www.isc.org	AAAA	-> AD=1でAAAA RRSet
isc.org	MX	-> AD=1でMX RRSet
isc.org	ANY	-> AD=0でなにかが戻る
www.dotgov.gov	A	-> AD=1でA RRSet
www.dotgov.gov	AAAA	-> AD=1でNO ERROR, empty
www.nonexist.se	A	-> AD=1で不在応答
www.nonexist.se	AAAA	-> AD=1で不在応答
www.unsecure.dnslab.jp	A	-> AD=0でA RRSet
www.nsecure.dnslab.jp	A	-> SERVFAIL
eai.dnslab.jp	A	-> AD=1でA RRSet

実例

dig +dnssec @149.20.64.20 eai.dnslab.jp

```
; <<>> DiG 9.7.0a1 <<>> +dnssec @149.20.64.20 eai.dnslab.jp
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2251
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;eai.dnslab.jp.            IN     A

;; ANSWER SECTION:
eai.dnslab.jp.       2911   IN     A      203.178.129.34
eai.dnslab.jp.       2911   IN     RRSIG   A 5 3 3555 20091004010515 20090904010515 5267 dnslab.jp.
```

＜長すぎるので中略＞

```
;; Query time: 683 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Fri Sep  4 11:43:39 2009
;; MSG SIZE  rcvd: 2331
```

検証をやらないでも問題は起こる

- いままで自分が使っていたフルリゾルバ（DNSSEC検証しない）への影響は？
  - いくつかのパターンがあります
    - 普通に動く、応答に時間がかかる、引けない
  - いまどきのBINDは黙っていてもDNSSECの情報を取りにいってしまいますので影響を受けます。

- うまく動かないとしたら何が問題？
  - [DNSOPS dnsops 644]～の一連のスレッドで話されています
    - いくつか実例が報告されています
  - おおむねEDNS0かIP Fragment packetの問題なので、DNS-OARCのリプライサイズテストを使ってみる
    - https://www.dns-oarc.net/oarc/services/replysizetest
  - 53/TCPを通さない設定も影響する
    - これまではほとんど53/UDPで済んでいたのが、パケットサイズの増大によりEDNS0やFragmentの問題にひっかかるようになる。⇒TCP fallback

OARC's DNS Reply Size Test Server

◘何ができるの？

- If a resolver does not support the Extension Mechanisms for DNS (EDNS), replies are limited to 512 bytes.
- The resolver may be behind a firewall that blocks IP fragments.
- Some DNS-aware firewalls block responses larger than 512 bytes.

◘どう見える？

```
% dig +short rs.dns-oarc.net txt
rst.x4001.rs.dns-oarc.net.
rst.x3985.x4001.rs.dns-oarc.net.
rst.x4023.x3985.x4001.rs.dns-oarc.net.
"XXX.XXX.XXX.XXX DNS reply size limit is at least 4023 bytes"
"XXX.XXX.XXX.XXX sent EDNS buffer size 4096"
```

ダメっぽい例1

- [DNSOPS dnsops 645]から引用
  - さっきの例のeai.dnslab.jpくらいのサイズのパケットは通りません
  - この環境ではTCP fallbackして最終的に引けます

```
% dig +short rs.dns-oarc.net txt
rst.x1014.rs.dns-oarc.net.
rst.x1202.x1014.rs.dns-oarc.net.
rst.x1382.x1202.x1014.rs.dns-oarc.net.
"YYY.YYY.YYY.YYY sent EDNS buffer size 4096"
"YYY.YYY.YYY.YYY DNS reply size limit is at least 1382 bytes"
```

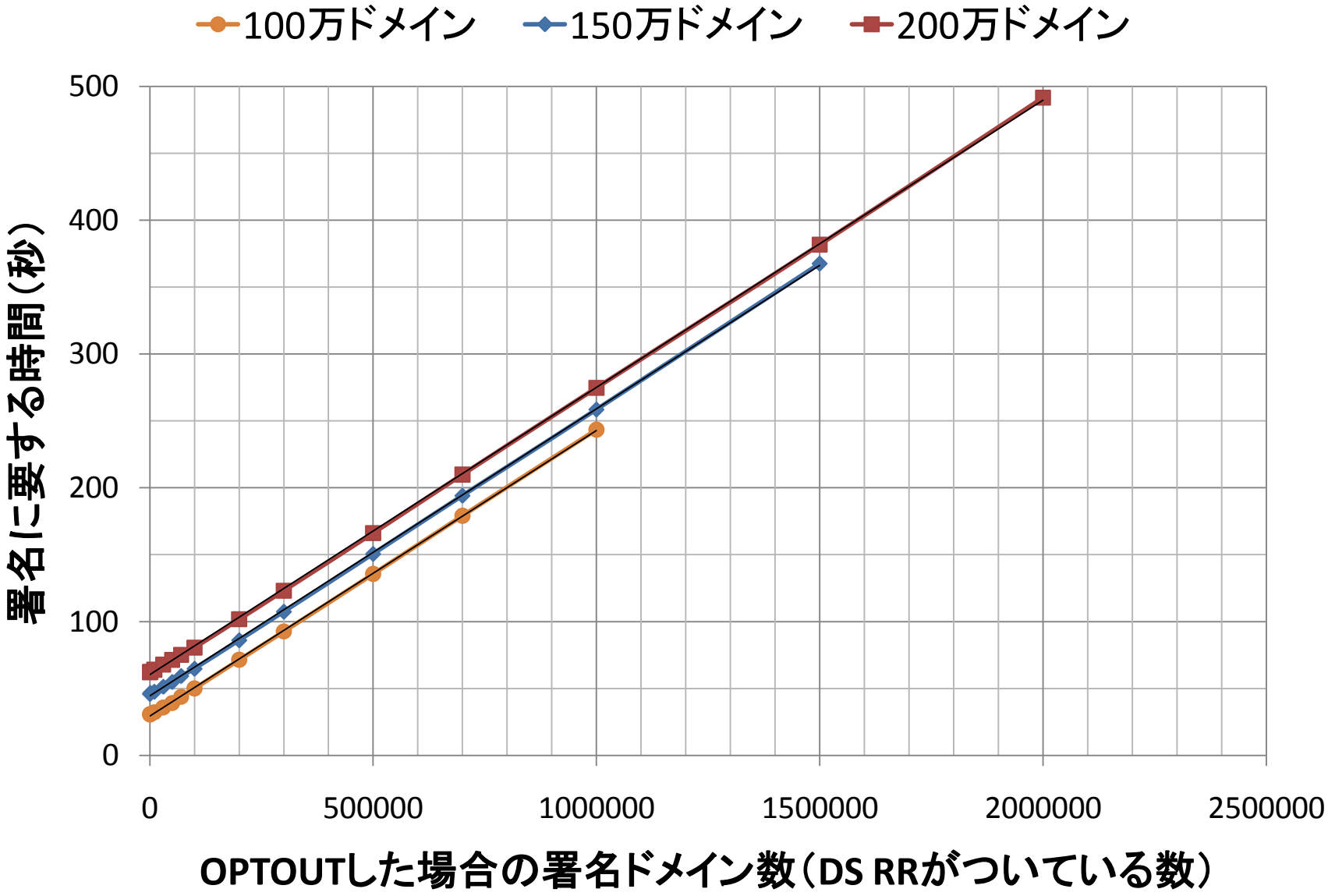
ダメっぽい例2

- [DNSOPS dnsops 646]から引用
  - このフルリゾルバはEDNS0に対応していないようです
  - ある意味影響がでないのでいいかも？

```
# dig +short rs.dns-oarc.net txt
rst.x486.rs.dns-oarc.net.
rst.x454.x486.rs.dns-oarc.net.
rst.x384.x454.x486.rs.dns-oarc.net.
"ZZZ.ZZZ.ZZZ.ZZZ DNS reply size limit is at least 486 bytes"
"ZZZ.ZZZ.ZZZ.ZZZ lacks EDNS, defaults to 512"
```

性能実験:署名速度

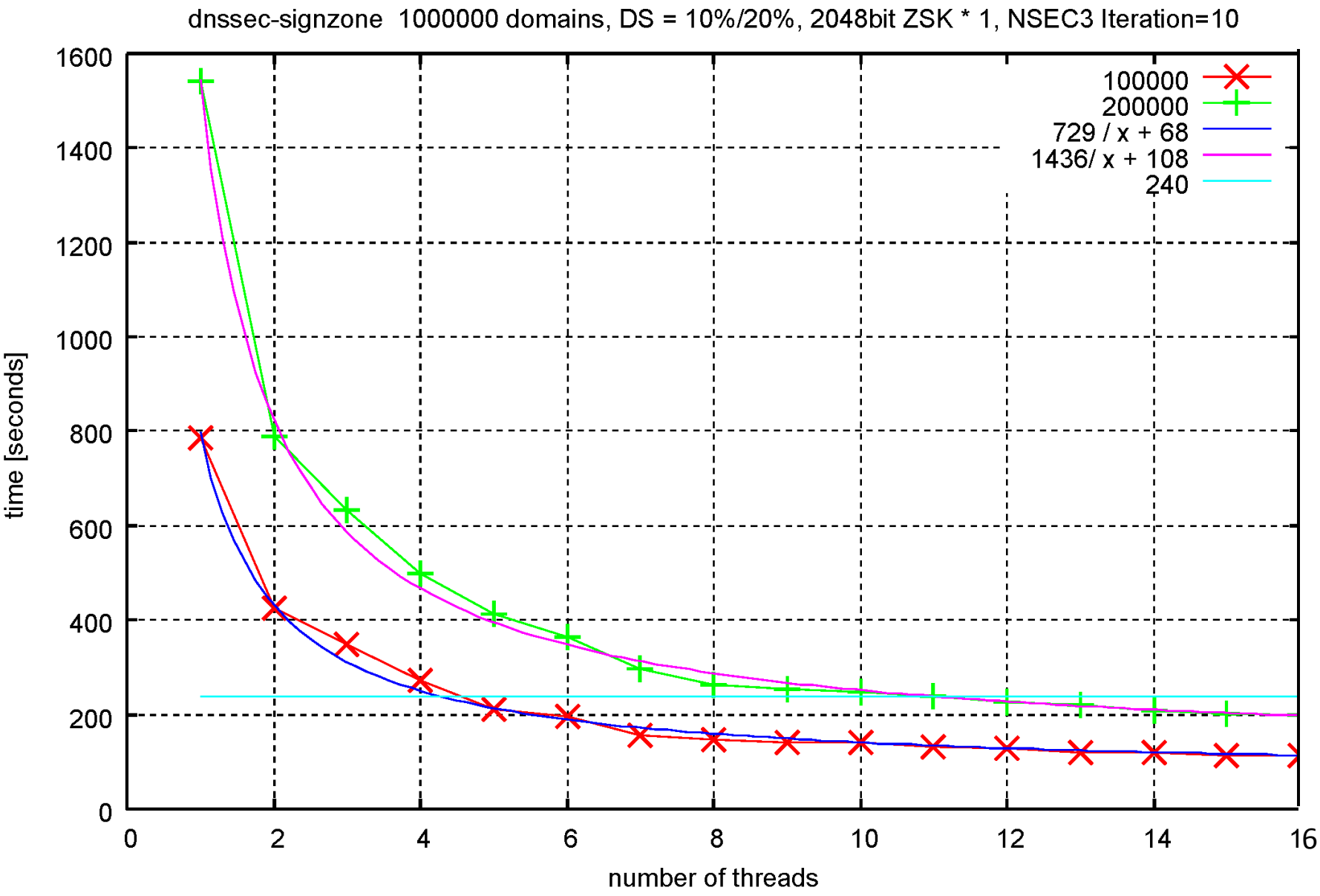
- 署名の実験
  - 大きなゾーンの署名をしたらどれくらい時間がかかるのでしょうか？気になります。
  - 適当にゾーンデータを作って測定してみました。
    - 条件
      - ゾーンのドメイン数100万、150万、200万
      - OPTOUT（DS RRが付いている分だけ署名をつける）
      - NSEC3, 1024bit, 繰り返し回数10
      - BIND9.6のdnssec-signzoneを使用
      - Xeon X5540(2.53GHz) x 2



性能実験：マルチスレッド

- 測定結果のグラフをみると線形近似に完全にのっています
  - しかもドメイン数に関係なく傾きが同じ
  - マルチスレッドが効きそう？
    - やってみよう！

調べた結果、RRSIGの計算部分がほぼ完全に並列化されていることがわかった



その他の運用課題

- 定期再署名・鍵更新
  - 権威サーバにおける問題
    - これまでかなり適当な設定がなされていても、上位が下位のサーバをポイントしてさえいればおおむね動いた。これが厳密にチェックされるようになると上位のサーバとの情報不一致が致命的な問題となる。
      - 上位のDS RRと下位のDNSKEYの間の関係がおかしいなど

DS RRは上位にしか存在しない、というこれまでにないタイプのRRだということを認識する必要がある

    - 鍵の更新時の運用方法などを検討しておく必要あり

その他の運用課題

- 定期再署名・鍵更新
  - 検証サーバにおける問題
    - Rootから後はDNSSECの検索の中で更新されるけれど、RootのTrust Anchorの更新をどうするのか？
    - BIND9.7ではRFC5011による自動更新のサポートが入った

> 2619. [func] Add support for RFC 5011, automatic trust anchor maintenance. The new "managed-keys" statement can be used in place of "trusted-keys" for zones which support this protocol. (Note: this syntax is expected to change prior to 9.7.0 final.) [RT #19248]

※BIND9.7.0a2のCHANGESより

まとめ

- DNSSEC対応が始まると
  - 対応する気がある人／ない人両方に影響がある
    - 普通にBIND9を使っていると影響をうける
  - フルリゾルバ-権威サーバ間の途中経路のMTUやFragmentなどの影響をうける
    - 途中の経路の機材などについて
      - 設定を見直す必要がないか？
      - 設定では対応できないのではないか？

インターオペラビリティの確保が必要

  - 関係者
    - 権威サーバ／フルリゾルバ／ネットワークの運用者
    - 機材／ソフトウェアベンダなどのベンダ
    - 他

補足

- などということはともかく
  - 実際に使ってみないとわからないですよね？

ということで、次の話
「DLVを使ってみよう」