DNS-OARCワークショップ報告 (Root Zone ZSKサイズの変更)

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp

2016/4/15, JANOG 37.5

DNS-OARCワークショップでの一つの発表

- “Increasing the Zone Signing Key Size for the Root Zone”
  - Duane Wessels @ Verisign
  - 2016年4月1日のDNS-OARC Public workshop (OARC24)
    - https://indico.dns-oarc.net/event/22/timetable/#all.detailed
  - 2016年10月1日にRoot zone ZSKサイズを1024bitから2048bitに変更するという計画
- ほとんどの参加者が知らなかった様子
  - 初出がPublic workshop？　April fool ？
  - “This is not the KSK Rollover”　(4枚目)
- 推測
  - Federal Information Security Management Act的に1024bit RSAの使用を継続しにくいため、2048bit RSAに変更する？
    - https://www.dnsops.gov/FISMA-dnssec.html
    - ECDSAへの変更はいろいろ大変
  - Federal governmentの関与できるうちに変更しようと急いだ？

Root ZSKサイズ変更の影響

- RRSIGリソースレコードのサイズが大きくなる
  - RRSIGがおおよそ2048-1024bit増大　(128バイト)
  - www.janog.gr.jp A というクエリをルートに送る場合、JP DSにRRSIGが付加されるため、応答サイズは683から811程度に増大
  - 不存在応答にはRRSIGが3つ含まれるため、384バイト程度増大
- DNSSEC対応フルリゾルバはDNSSEC OKビットをセットするため、DNSSEC検証しなくてもRRSIGを受け取っている
  - BIND 9, Unbound など
- ルートサーバからの応答サイズが大きくなるが影響は少ない
  - ルートサーバでのトラフィックは3割増加と推定
  - 応答サイズは1200バイト以下であるので、MTUの影響は受けにくい
- 変更後、悪影響があれば1024bit RSAに戻すとのこと
- 今後　gov, mil, edu (com, net, org) ZSKサイズも変更？