DNSの統計調査結果の紹介(仮)、DNS-OARC2014,ICANN51,IETF91の話題

藤原 和典
<fujiwara@jprs.co.jp>
株式会社日本レジストリサービス (JPRS)
dnsops.jp BoF, Nov.,2014

DNSの統計調査結果の紹介(仮)

- “2014 Root DITL Data analysis and TLD popularity analysis” としてDNS-OARC Workshopで発表
- 2014年のDITLデータの分析と、TLDの人気度の分析

- DNS-OARC DITLデータセットを評価した発表などは事前にチェックを受ける必要があるため、DNS-OARC Workshopの資料を使用
  - https://indico.dns-oarc.net//getFile.py/access?contribId=2&sessionId=2&resId=4&materialId=slides&confId=20

DNS-OARC2014,ICANN51,IETF91の話題

- DNS-OARC + ICANN 51
  - 2014/10/12: DNS-OARC 2014 Fall Workshop
  - 2014/10/13: ICANN 51 + DNS-OARC joint Tech day
    - https://www.dns-oarc.net/
    - http://la51.icann.org/en/schedule/mon-tech
- IETF 91, 2014/11/9~14
  - http://www.ietf.org/meetings/91/
- Workshop on DNS Future Root Service Architecture, 2014/12/8

DNS-OARC 2014 Fall Workshop
+
DNS-OARC / ICANN joint Tech Day

The GIft that Keeps on Giving: Open DNS Proxies, nominum

- Random subdomain attacks
- Open DNS proxiesからの大量のクエリ
  - wxctkzubkb.liebiao.800fy.com
  - 一日あたり1800万のunique query names
- 香港の熱血時報が13時間オフライン (2014/9/28)
- 対策は、random drop など
- ISCはBIND 9.11に対策機能を導入予定

.FR (.WF)への攻撃

- Google Public DNSを使ってRandom Subdomain attacksをやると、TLDもつらいという話
- WFはフランス領ウォリス・フツナ
- Random qnames - dafa888 DoS attack
- ********.www.dafa888.wf
- Google Public DNSのIPアドレスから秒10万クエリが14時間
- .FR,.WFのDNSサーバは、AFNIC直営とNetnod、PCH、ISC、SIDNへの委託
  - それぞれの所在地も地図に示されている
- Netnodからアラーム
- Google Public DNSへ大量のランダムクエリ名クエリが送られたようだ
- dafa888.wfを削除してもトラフィックは減らず (当然)
- 最終的には、Googleにフィルタしてもらったとのこと

DNSソフトウェア実装者のパネル

- Nominum: Vantioの宣伝、DoS対策
- ISC
  - BIND 9.11の話題
  - Subscription契約の話
- .CZ: Knot DNS
  - 自組織が使うための権威サーバ
  - 2.0でOpenSSLからGnuTLSに変更
  - online signing実装
- .EU: YADIFA
  - 自組織が使うための権威サーバ
- Microsoft DNS サーバ
  - パネル以外での発表
  - 高度なデータ収集機能を追加した
  - クエリ、ゾーン転送、パフォーマンス
- NLNet Labs: Unbound, NSD, LDNS, OpenDNSSEC
  - 資金調達についての困難さ紹介 (引用)

http://la51.icann.org/en/schedule/mon-tech/presentation-nlnet-labs-13oct14-en.pdf
13 ページ

Open Source Dilemma
- Free as in Free Beer
- Beer Barrels are not infinite
- Standards evolve
- Tracking standards does have it's costs
- Requires long term commitment (and funding)

IETF 91

dprive WG

- DNS PRIVate Exchange (dprive) WG設立
  - スタブリゾルバとフルリゾルバの間の通信を TLS(Transport Layer Security ~ SSL)で暗号化する
- 提案
  - DNS/TCPをそのままTLS (16ビットのデータ長 + binary のDNSデータ)
    - ポート53+STARTTLS (SMTP/POP3のようにコマンドで格上げ)
    - ポート443
    - 443、53以外
  - DNS (JSON format) over HTTPS
  - DNS (BinaryをASCII encode) over HTTPS
- 懸念事項
  - Middle box (CPEやFirewall) が通すかどうか

dnsop WG

- DNS Cookies復活
  - Cache poisoning対策の一つ
  - draft-eastlake-dnsext-cookies-05
  - 2008年にexpireしていたものを復活、WG docへ
  - BIND 9.10のSIT(Source Identity Token)と連携
    - ただし、フォーマットは違う (SITにはerror codeがない)
- TCPトランスポートについて熱い提案と議論
  - Server side close
  - TCP fast open
  - Query pipelining
- ISPでのIPv6の逆引きドキュメント → 否定的ではない
- Negative Trust Anchor: DNSSEC検証オフ設定 → 肯定的

.home TLD

- 新gTLDプログラムで10組織が提案するも、Name collisionで”high risk”と評価され保留中
- IETF 91 にて、Stuart Cheshire氏がhomenet向けに使いたいと提案
  - homenet WGではdnssd WGの仕事と指摘
  - dnssd WGでは質問程度
  - Mailing listでは、arpaの下ならIETFから提案しやすいといったコメント
  - ICANNの領域にはかかわりたくないという雰囲気
- .local
  - Stuart Cheshire氏がRFC 6762で.localを予約

その他

Workshop on DNS Future Root Service Architecture

Location: Hong Kong, HK
Venue: The Mira Hotel (Kowloon district)
Date: December 8-9, 2014
Hosted by: ISOC-HK
Sponsors: ZDNS/BII and CNNIC
Co-chairs: Warren Kumari and Paul Vixie

1. draft-wkumari-dnsop-root-loopback-01.txt
   - Decreasing Access Time to Root Servers by Running One on Loopback
   - ローカルにルートのデータを持つ権威DNSサーバを動かし、フルリゾルバからルート向けはそこに向けるという提案、設定例あり
   - W. Kumari, Ed.; P. Hoffman
2. draft-lee-dnsop-scalingroot-00
   - How to scale the DNS root system?
   - ルートDNSサーバの増やしかたの提案 (現在の仕組みを変更)
   - Xiaodong Lee; Paul Vixie; Zhiwei Yan