DNS-OARC/RIPE66 report

Kazunori Fujiwara, JPRS
fujiwara@jprs.co.jp
2014/6/27

概要

- DNS-OARCとRIPEの紹介
- 2014年5月に開催されたDNS-OARC 2014 Spring workshopとRIPE 68 meetingでのDNS関連の話題を報告

DNS-OARC

- DNS Operations Analysis and Research Center
- https://www.dns-oarc.net/
- DNSの運用、解析、研究を行う組織
  - Root DNSサーバのオペレータやTLD、大規模なユーザ組織が参加
  - 毎年50時間、Root DNSサーバのパケットキャプチャ実施
    A Day in the Life of the Internet (DITL)
  - 日本の組織だと、NTT、WIDE、JPRSがメンバー
- 年に2度Public Workshopを開催
  - 今回はRIPE 68本会議の前の土日 2014年5月10日～11日
  - 土曜の午前中にメンバー限定ミーティング実施

DNS OARC 2014 Spring Workshop

- 休憩を除いて9時間30分
- 18件の発表と4件のライトニングトーク
- https://www.dns-oarc.net/ のOARC Spring 2014 Warsaw Workshop リンクに資料あり
- 内容
  - IETFでのDNSプライバシに関する話題
  - DNSデータ収集と分析サービスの話
  - Windows Server 2012 R2でのDNSSECについて
  - Hadoopを使って.nzのクエリ情報を分析
  - .com, .net, .tvのクエリ情報からBotnetドメイン名を調査
  - ルートのクエリ情報の分析と、フルリゾルバとの比較

RIPE communityとRIPE NCC

- RIPE community = RIPE (Réseaux IP Européens) is a collaborative forum open to all parties interested in wide area IP networks in Europe and beyond.
- RIPE NCC = ヨーロッパ、ロシア、中東地域のIPアドレスレジストリ
- RIPE communityが年に2度、一週間ミーティングを開催
  - AP地域だとAPRICOTの二週目に近い

RIPE 68 meeting

- https://ripe68.ripe.net/
- 2014年5月12日～16日 ワルシャワで開催
- 主な話題
  - RIPE community 25周年の祝い
  - 25年間チェアを勤められたRob Blokzijl氏の退任
- RIPE 68でのWG BoF
  - Address Policy, Open Source, Database,
  - IPv6, DNS, Cooperation, Routing, MAT, Anti-abuse

RIPE 68 Open Source WG

- 90分
- 6件の発表
- 内容
  - Knot DNS
  - The Rise and Fall of BIND 10
  - getdns API Library
  - DANEs Don’t Lie – Email Transportencryption “Reloaded”
  - Kea Update – A Modern DHCP Engine
    - BIND 10のDHCPが独立
  - Update on the ONIE Project: pxeの後継の話

RIPE 68 DNS WG

- 3時間
- 8件の発表と1件のパネル
- 内容
  - RIPE NCC Update
  - Using DDoS to Trace the Source of a DDoS Attack
  - Measuring DNSSEC Validation Deployment
  - Measuring DNSSEC from the End User Perspective
  - Report from Ad-hoc ccTLD Group
  - Registry Infrastructure Transformation: .UKの紹介
  - Google DNS Hijacking in Turkey
  - DNSMON Developments
  - DNS Monitoring Common Practices/APIs Panel Session

“Zeroing in on Zero Days” (OARC)

- Nominumは、世界中のISPからフルリゾルバのデータを集めているとのこと
  - Chinaを含む世界中
  - 毎日数テラバイト
  - 全世界のISPの5%
- このデータを用いて攻撃に使われるドメイン名を判定しているとのこと
  - liebiao.800fy.com
  - DDoS serviceのservice menuとか
- Cache poisoning対策として、DNS responseを記録して解析することが重要である

Windows Server 2012 R2でのDNSSEC (OARC)

- Windows Server 2012 R2へのDNSSEC実装についてMicrosoftの方が紹介された
- Active Directory(AD)と統合して、Dynamic Updateやmulti master機能あり
- Wizardで簡単に設定可能
- ADにTrust Anchorの管理と配布機構
- Microsoft.comをsignするのかという質問に、yesと回答されていた

“Big Data Journey” (OARC)

- .nzで、Apache Hadoopを使ってクエリデータの解析
- 個々のマシンの設定からクラスタの構築、運用
- ハードウェア
  - 240個の2TB disk、240枚の4GB memory
  - namenodes, 20 datanodes, 1KVM
- .nzの7つのDNSサーバ名のうち4つで収集
  - 毎月約500Gbで18ヶ月分
- DNSSEC validatorの評価をされた
- Hadoop clusterをモニタ、管理するマシンが必要だった

Knot DNSの新機能 (RIPE)

- NIC.CZ製の権威DNSサーバソフトウェア
- 新機能を実装したという発表
- Synthetized Resource Records
  - IPv6アドレスの逆引きと対応する正引きを動的に自動生成する機能
  - 8.b.d.0.1.0.0.2.ip6.arpa { query_module { synth_record "reverse gen- example.org. 400 2001:db8::/32"; }}
  - で、f.e.d.c.b.a.9.8.7.6.5.4.3.2.1.0.f.e.d.c.b.a.9.8.8.b.d.0.1.0.0.2.ip6.arpa 400 IN PTR gen-2001-0db8-89ab-cdef-0123-4567-89ab-cdef. を生成

“The Decline and Fall of BIND 10” (RIPE)

- タイトルが” The Rise and Fall of BIND 10”から変更
- 発表者はShane, Kerr
  - 元BIND 10プログラムマネージャ
  - ISCからDynに転職
- BIND 10プロジェクトの運営についての暴露
- ISCの経営者の変化 (fired by boardって？)
- BIND 9からの変化を嫌うユーザ
- ISCはBIND 10を野に放ったので興味を持つ人にfork してもらったとのこと
  - Bundy DNS serverに名前を変更し、githubに移動
  - http://bundy-dns.de/

RIPE NCC DNS Update (RIPE)

- 5170ゾーン (逆引き, ripe.net, ENUM, 77 ccTLD)
  - 120,000 q/s average, 180,000 q/s peak
- 運用多様性のためBIND 9以外を評価中
  - CentOSで動いて、無停止でゾーンを追加できること
- 評価結果

	メモリ	起動	停止
BIND 9	11GB	45秒	30秒
Knot	17GB	90秒	40秒
NSD 4	25GB	3分以上	すぐ

BIND 9は「View」が便利（Knot、NSDにはない）

“Google DNS Hijacking in Turkey” (RIPE)

- 3月21日にトルコ政府がtwitter.comへのアクセスを遮断
  - ISPにフルリゾルバDNSサーバの設定を変えさせて、twitter.comの名前解決をエラーにさせた
  - Google Public DNS (8.8.8.8/8.8.4.4)を使えば到達できた
  - 3/29に、トルコのISPは8.8.8.8/32を注入してGoogle Public DNSを使えなくした
  - 4/4にフルリゾルバの嘘つきを停止
  - 4/7に経路ハイジャック停止
  - hostname.bind, Looking glass, RIPE Atlas, traceoruteなどで状況が確認された

詳細は各会議のページ参照

- プレゼンテーションとビデオが公開されている
- https://www.dns-oarc.net/
- https://ripe68.ripe.net/