DNS-OARC / RIPE 66 DNS WG報告 +IPv6 Pollution Traffic Analysisの紹介

Kazunori Fujiwara, JPRS
<fujiwara@jprs.co.jp>

JPOPM 24, 2013/6/18

Copyright © 2013 Japan Registry Services Co., Ltd.

報告の範囲

- RIPE 66の前日に開催された
  DNS OARC 2013 Spring Workshop
- RIPE 66のDNS WG
  + PlenaryのDNSネタ

- RIPE 66のPlenaryで報告されたIPv6 Pollution Traffic Analysis

Copyright © 2013 Japan Registry Services Co., Ltd.

全体概要

Copyright © 2013 Japan Registry Services Co., Ltd.

DNS-OARCとは

- 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
  - 日本の組織だと、NTT、WIDE、JPRSがメンバー
- 年に二度Public Workshopを開催
  - 今回はRIPE 66本会議の前に一日半
  - 日曜朝から月曜の午前中 (RIPEチュートリアルとは競合)
  - そのあとDNS-OARCメンバーミーティング (RIPE昼休み)

Copyright © 2013 Japan Registry Services Co., Ltd.

DNS OARC 2013 Spring Workshop

- 日曜と月曜の午前中の、休憩を除いて8時間
- 20件の発表と1件のパネル
- 一件あたりの持ち時間15分から25分
- 内容: DNS関係のみ
  - https://www.dns-oarc.net/ のOARC Spring 2013 Dublin Workshop リンクに資料あり
  - DNSへの攻撃とその対策について
    - オープンリゾルバ対策、DNSSECを使った攻撃
  - DNSへの負荷増大
  - 性能測定ツール
  - DNSSECの新機能 (楕円暗号)
  - DNSSEC: GPU-based NSEC3 Hash Breaking

Copyright © 2013 Japan Registry Services Co., Ltd.

RIPE 66 DNS WG

- https://ripe66.ripe.net/programme/meeting-plan/dns-wg/
- 5/15水曜の11:00-12:30, 14:00-15:30
- パラレルセッション: RIPE NCC Service, IPv6 WG
- 3時間に8件の発表
- 内容
  - DNSソフトウェア (Knot, YADIFA, OpenDNSSEC)
  - .NLへの攻撃
  - RIPEのDNSサーバの運用報告
  - ENUM WGの報告
  - SAC-057
  - .com/.netでのクエリ解析

Copyright © 2013 Japan Registry Services Co., Ltd.

RIPE 66 Plenary (DNS関連)

- https://ripe66.ripe.net/programme/meeting-plan/plenary/
- 5/14 火曜 16:00-17:30
- DNS: Attack or Defense, Paul Ebersman, Infoblox
  - DNSへの攻撃手法の解説
- DNS Amplification Attacks – Are YOU Part of the Problem?
  - Merike Kaeo, Internet Identity
  - オープンリゾルバを使った攻撃の解説と、オープンリゾルバの分布、修正方法の説明など
- Panel: Seven Years of Anti-Spoofing

Copyright © 2013 Japan Registry Services Co., Ltd.

報告のサマリ

- DNS-OARC Workshop
  - 新規性の高いネタが多い
  - 発表者や、マイクでコメントする人たちは、IETFなどと重なる
  - 藤原の出張目的はDNS-OARCにてJP DNSで観測したDNSSECの副作用について報告すること (後述)
- RIPE DNS WG
  - DNS-OARCと似た内容と、RIPE地域ローカルな内容
  - DNS WGのChairの一人はIETF dnsop WG Chair
  - DNS-OARCやIETFとそれなりに重なる参加者
- RIPE Plenary
  - オープンリゾルバ問題やDNSへの攻撃をわかりやすく解説

Copyright © 2013 Japan Registry Services Co., Ltd.

DNS-OARC Workshop

(一部)

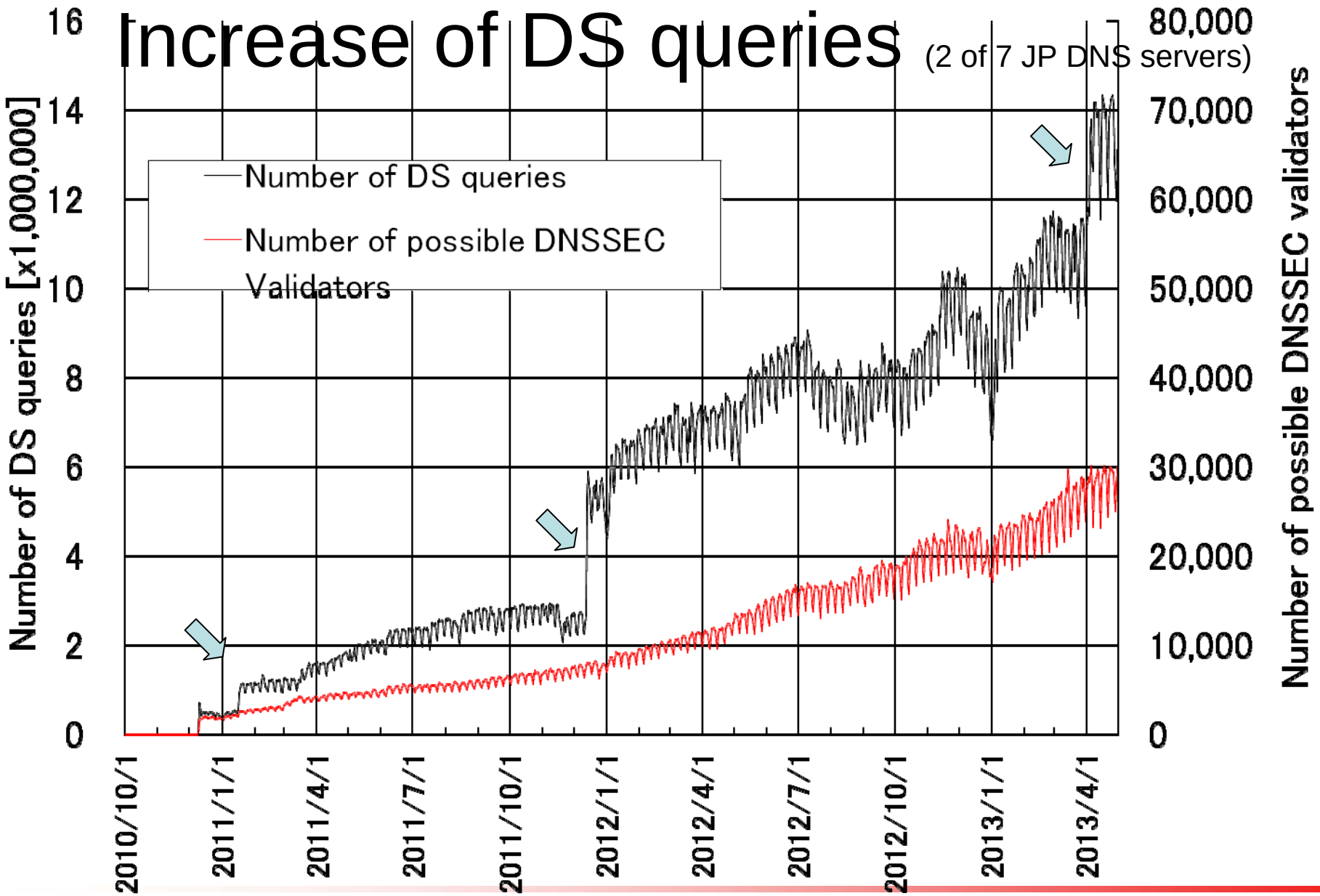
Copyright © 2013 Japan Registry Services Co., Ltd.

DNSSECの副作用 (1/2)

- JP DNSで観測したDNSSECの副作用
- DSレコードはドメイン名の鍵情報で、TLD側(.jpなど)に登録
- 現在はクエリの3.5%がDSクエリ
- TLDをDNSSEC対応させると、DNSSEC検証を行うサーバが増えるに従いDSクエリが増加していき、将来的にはTLDのDNSサーバへのクエリがDSクエリで占められるのではないかという問題
- .jpや.com, .net, .orgでは、存在しない情報をキャッシュしていい時間は900秒/15分
- DNSSEC非対応のドメイン名はDSがない
- 結果として、DNSSEC非対応の忙しいドメイン名では、DNSSEC検証サーバから15分に一度DSクエリが送られる
  - 例: www.yahoo.co.jpとかwww.google.co.jp

Copyright © 2013 Japan Registry Services Co., Ltd.

DNSSECの副作用 (2/2)



Copyright © 2013 Japan Registry Services Co., Ltd.

オープンリゾルバ対策

- オープンリゾルバプロジェクト
  - 日本ではJANOG MLで紹介
  - http://openresolverproject.org/
  - Jared Mauch氏 (NTT America)
  - だれでもどのアドレスでもチェックできるページを公開したら、最初は少数の苦情が来たが徐々に減ったとのこと
  - ISPのAbuse-teamには事前に知らせたとのこと
  - (対策が進んで?)Refusedが増えてきた
- VeriSignもチェックツールを公開
  - https://www.verisignlabs.com/orscan/

Copyright © 2013 Japan Registry Services Co., Ltd.

クライアントでのDNSSEC評価

- APNICが、IPv6のWeb広告を用いて、クライアントでのDNSSEC評価を行った
  - Flashのプログラムを仕込む: androidでは動かない

- クエリパターン
  - IPv4, IPv6
  - DNSSEC非対応/DNSSEC対応/DNSSEC対応失敗

- $100/dayの予算のため、クリックされると困る
- 一日あたり35万のデータが集まったとのこと
- 200万のテストで、3.5%がDNSSEC対応
  - Googleが対応したあとは増加傾向とのこと

Copyright © 2013 Japan Registry Services Co., Ltd.

RIPE DNS WG

Copyright © 2013 Japan Registry Services Co., Ltd.

ヨーロッパ発DNSソフトウェアの発表

- Knot DNS
  - .CZ (NIC.CZ)が開発している権威DNSサーバ
  - https://www.knot-dns.cz/
  - Zone file parserの実装の仕方についての発表
- YADIFA
  - .EU (EURid)が開発している権威DNSサーバ
  - http://yadifa.eu/
  - 動的なゾーンの追加削除機能 (ホスティング向け)
- OpenDNSSEC
  - DNSSEC管理ソフトウェア http://www.opendnssec.org/
- 他のEU産
  - NL NetLabsのNSD, Unbound, LDNS
  - PowerDNS
- アメリカ産だとISC BIND 9, BIND 10

Copyright © 2013 Japan Registry Services Co., Ltd.

.NLへの攻撃

- .NLはDNSSECで署名している
- NL ANYクエリの応答は巨大
  - 例: dig +dnssec +norec @ns1.dns.nl nl any は3571バイトの応答を返す
  - 100倍に増えるので、攻撃に使える
- 通常は10,000 q/s程度のところに25,000 q/sのNL ANYクエリがきた
- iptables u32でANYクエリをブロックしたら(攻撃の効果がでないので)攻撃が落ち着いた

Copyright © 2013 Japan Registry Services Co., Ltd.

RIPE NCCの運用するDNSサーバ

- K-root: 5 global, 12 local, 20,000 q/s ave.
- RIPE会員向けにK-rootを配る提案
  - 会員のネットワークと会員の顧客向け
  - 小規模な構成
- その他のDNSサービス
  - 5170ゾーン (逆引き, ripe.net, ENUM, ccTLD)
  - 120,000 q/s average, 180,000 q/s peak
  - 現在はBIND 9を使用しているがNSD 4とKnotを計画
- DNSMONというDNSの監視サービス (有料)
  - RIPE Atlasベースに作り直しているとのこと

Copyright © 2013 Japan Registry Services Co., Ltd.

ENUM status

- ENUM: 電話番号にドメイン名を対応付けて、URIをのせる技術、IP電話の経路制御など
  - 日本ではJPNIC ENUM研究グループやETJP (ENUM Trial Japan)という活動があった

- 活発だったヨーロッパでも活動が低調であることが報告された
  - DNS WGでENUMのステータス報告
  - Future not yet decided: 今後の活動は未定
  - Tier-0 国を登録する部分の運用は継続中

Copyright © 2013 Japan Registry Services Co., Ltd.

SAC-057 non-FQDN Certs

- www.corp, www.accounting, mail.test, www.site
- 既存のTLDで終わらないドメイン名の証明書が発行されているらしい
  - 社内、組織内向けらしい
- 新gTLDで提案されているドメイン名と競合するのでICANN, SSACが動いた
- CA/B Forum (CAブラウザフォーラム)へ連絡した
  - CA/B Forumのメンバは今後は発行しない
  - ただし、メンバじゃないCAもいるので問題が起きる可能性あり

Copyright © 2013 Japan Registry Services Co., Ltd.

.com/.net DNSサーバでのクエリ解析

- なぜVeriSignがRIPEで発表するのかは不明
- VeriSignでは.com/.netのDNSサーバのパケットを取得してクエリ解析したとのこと
- 60秒ごとに、IPアドレスごとのクエリタイプ、RD, bufsize, DO, TTL
- 2年間のデータを調べた
- 2011年6月には26,437,427 IPアドレス観測
  - 一日ごとでは270万から380万、(JPでは110~150万)
  - 16,000のAS
- クエリタイプの割合での分類
  - クラスタリングの結果、DSを多く送るグループ、ほとんどA, ほとんどMX、ほどんどAAAA、ほとんどPTRなどに分類できたとのこと
- AAAAとIPv6でのクエリの話とか
  - 2011/6から2012/6でAAAAクエリを送るIPアドレスが増えた 14.7%から18%
- 少数の忙しいIPアドレスの存在
  - 100個で全体の10%, 5000個で50%, 200,000個で90%

Copyright © 2013 Japan Registry Services Co., Ltd.

Plenaryで報告された
IPv6 Pollution Traffic Analysis

Copyright © 2013 Japan Registry Services Co., Ltd.

IPv6 Pollution Traffic Analysis (1)

- IPv6での汚染されたトラフィック？
  - 割り当てられていないアドレスへのトラフィックのこと
- 発表者はManish Karir, DHS S&T Cyber Security Division
  - DHSはアメリカ合衆国国土安全保障省
  - DHS + Merit + CAIDAの研究
- 使われていないアドレスを含む経路を出してトラフィックを吸い込んで調べたとのこと
  - 2400::/12(APNIC),2600::/12(ARIN),2800::/12(LacNIC)
  - 2A00::/12 (RIPE), 2C00::/12 (AfriNIC)
  - Merit (AS237)からアナウンス
  - RIRsとレターを交わして実施
  - 2012/11/7 ~ 現在
  - reachabilityに悪影響がないことを確認

Copyright © 2013 Japan Registry Services Co., Ltd.

IPv6 Pollution Traffic Analysis (2)

- Looking glass (bbtower) で見ると、

BGP routing table entry for 2400::/12

Paths: (3 available, best #3, table Default-IP-Routing-Table)

Not advertised to any peer

2516 6939 237

2001:370:100::12 from 2001:370:100::1 (211.14.3.252)

Origin IGP, metric 100, localpref 100, valid, internal

Community: 9607:3252

Originator: 211.14.3.252, Cluster list: 211.14.3.249

Last update: Tue May 21 16:12:58 2013

Copyright © 2013 Japan Registry Services Co., Ltd.

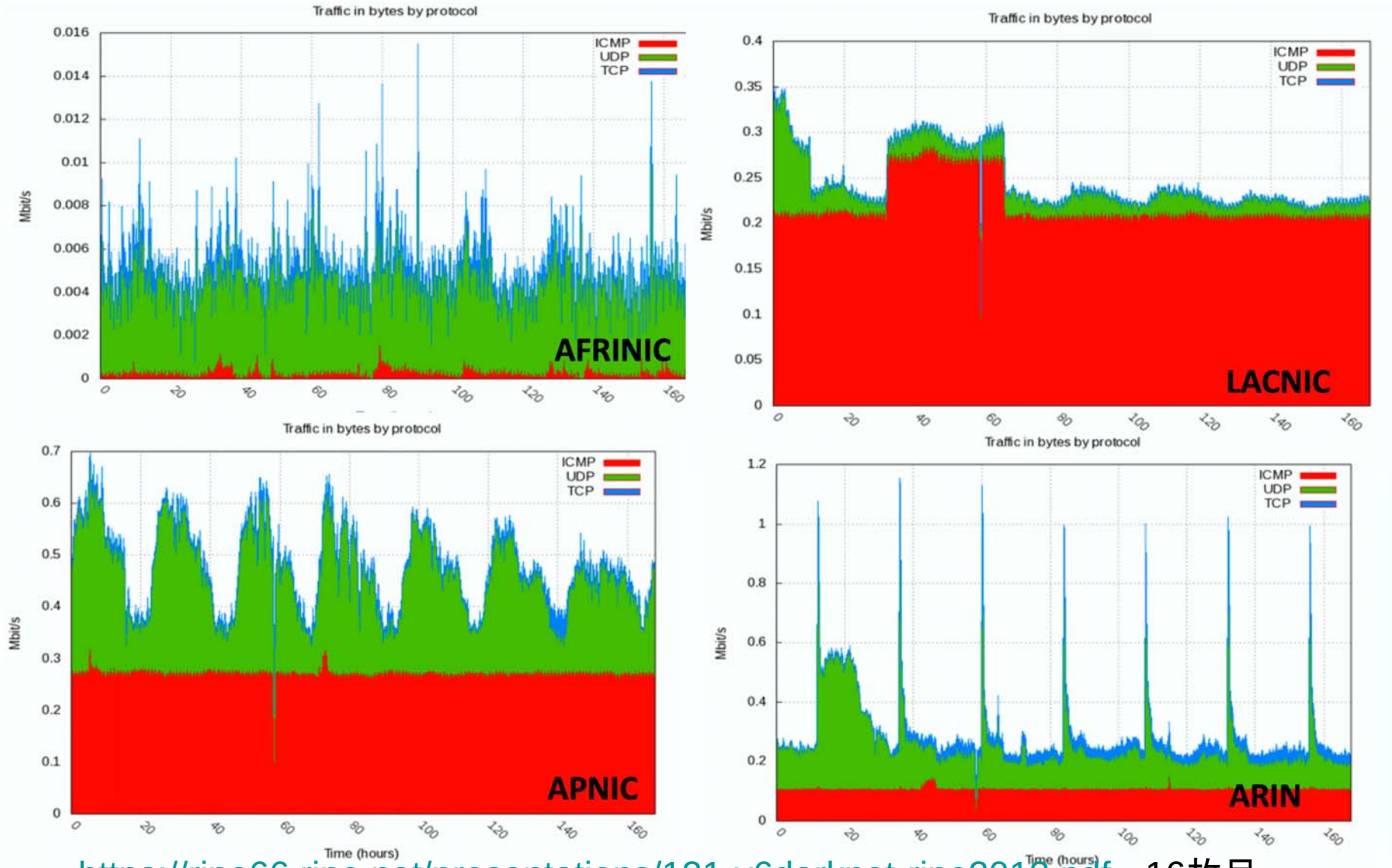
IPv6 Pollution Traffic Analysis (3)

- RIPEのデータは25%のアドレスに集中があったため、/14を除外して再調査中
- Traffic
  - APNIC: 500kbps
    - 300kbpsの定常的なICMPと、一日ごとに変化するUDP
  - ARIN: 1Mbps
    - 100kbpsの定常的なICMPと、ピークが1MbpsのUDP
  - LACNIC: 250kbps, ICMPが多い
    - 200kbpsの定常的なICMPと、若干のUDP
  - AFRINIC: 5kbps
    - ほとんどUDP

Copyright © 2013 Japan Registry Services Co., Ltd.

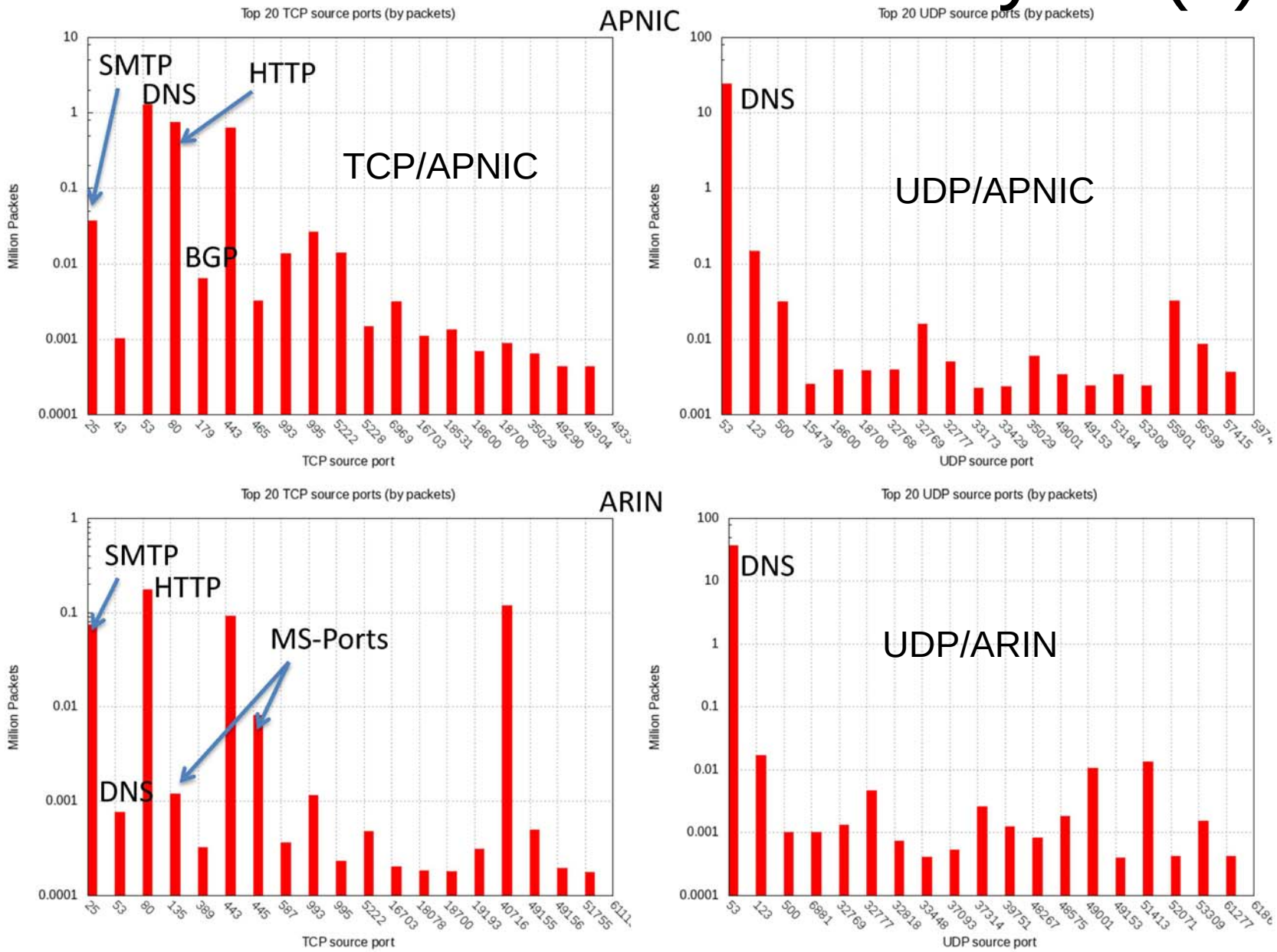
IPv6 Pollution Traffic Analysis (4)

Traffic Breakdown by Protocol



https://ripe66.ripe.net/presentations/121-v6darknet-ripe2013.pdf 16枚目

IPv6 Pollution Traffic Analysis (5)



https://ripe66.ripe.net/presentations/121-v6darknet-ripe2013.pdf　21枚目

IPv6 Pollution Traffic Analysis (6)

- ワーム？ Slammer/Conflicker portへのパケット
- スキャン？　6000以上のIPアドレスからICMPv6
- Link-localアドレスをソースとするパケット
- 以下、三ヶ月のデータから調べた結果
- NTP 4700アドレスから
- BGP 330アドレスから
- SMTP 4300アドレスから(Google, Comcastからも)
- DNS: 18万アドレスから3.3億クエリ
- DNSに間違ったアドレスが書かれている可能性あり
- 詳細は資料参照
  - https://ripe66.ripe.net/presentations/121-v6darknet-ripe2013.pdf

Copyright © 2013 Japan Registry Services Co., Ltd.

参照URI

- DNS-OARC:　https://www.dns-oarc.net/
- RIPE 66: https://ripe66.ripe.net/

Copyright © 2013 Japan Registry Services Co., Ltd.