DNSSEC 2013 スプリングフォーラム

Root / .JPの状況

2013年5月29日(水)

株式会社日本レジストリサービス
坂口　智哉

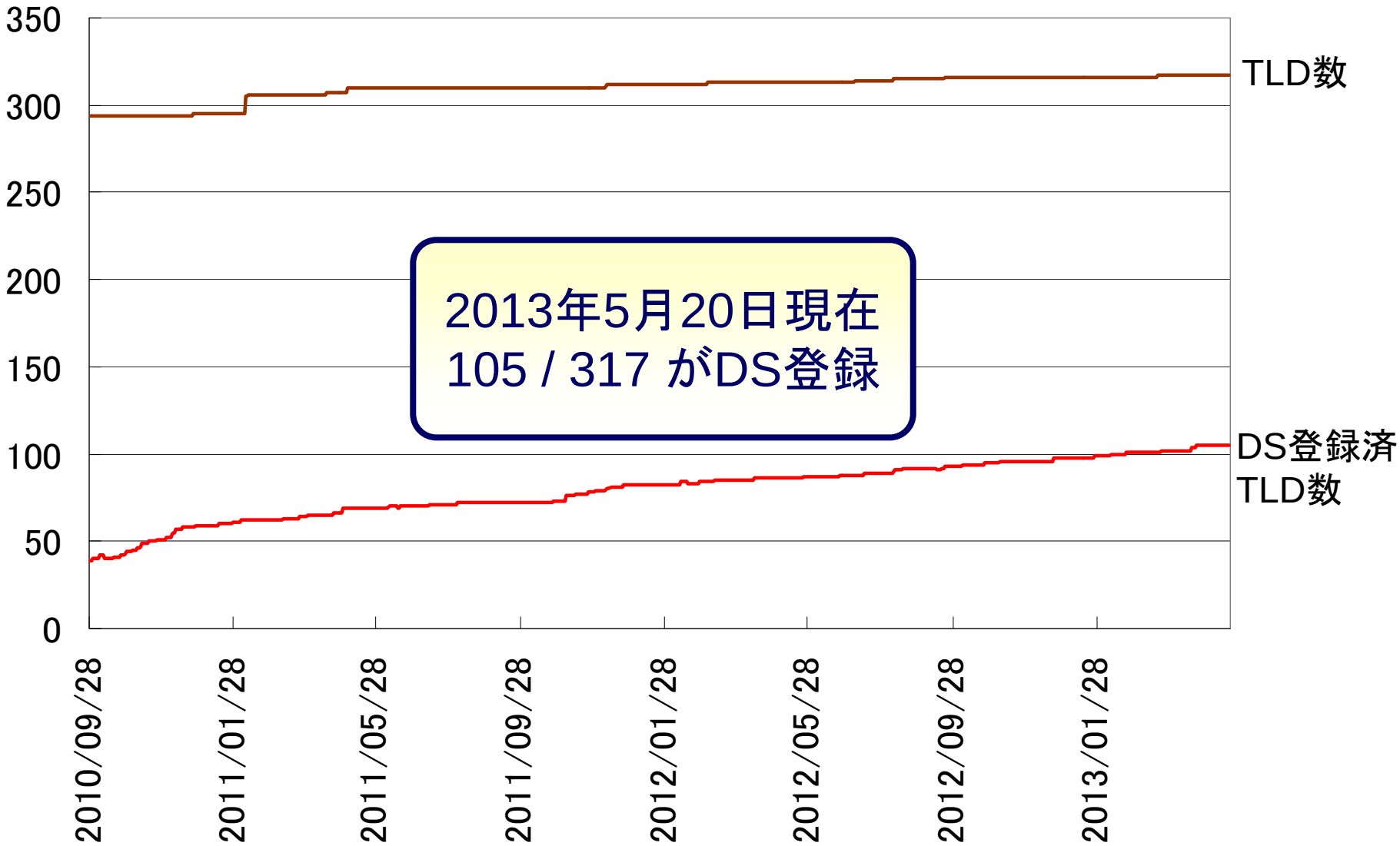
本日の流れ

I. Rootの状況
   1. DSレコードの登録状況
   2. Rootにおける主なトピックス

II..JPの状況
   1. DSレコードの登録状況
   2. DSレコードの問い合わせ数
   3. DNSSECとDNS Reflector Attacks

1. DSレコードの登録状況

Root



(http://stats.research.icann.org/dns/tld_report/ より)

2. Rootにおける主なトピックス

Root

■ ICANNがRoot KSK Rolloverについて検討開始
- 2013年3月 パブリックコメント募集中(ICANN) (※)

■ 新gTLDの登場
- 現在の予定では2013年8月から新gTLDが順次稼動開始
- 新gTLDではDNSSEC対応が必須条件の1つ
  - ➔レジストリのDNSSEC対応
  - ➔レジストリのDPS Web公開
  - ➔レジストラのDNSSEC対応

※ http://www.icann.org/en/news/public-comment/root-zone-consultation-08mar13-en.htm

2. Rootにおける主なトピックス

Root

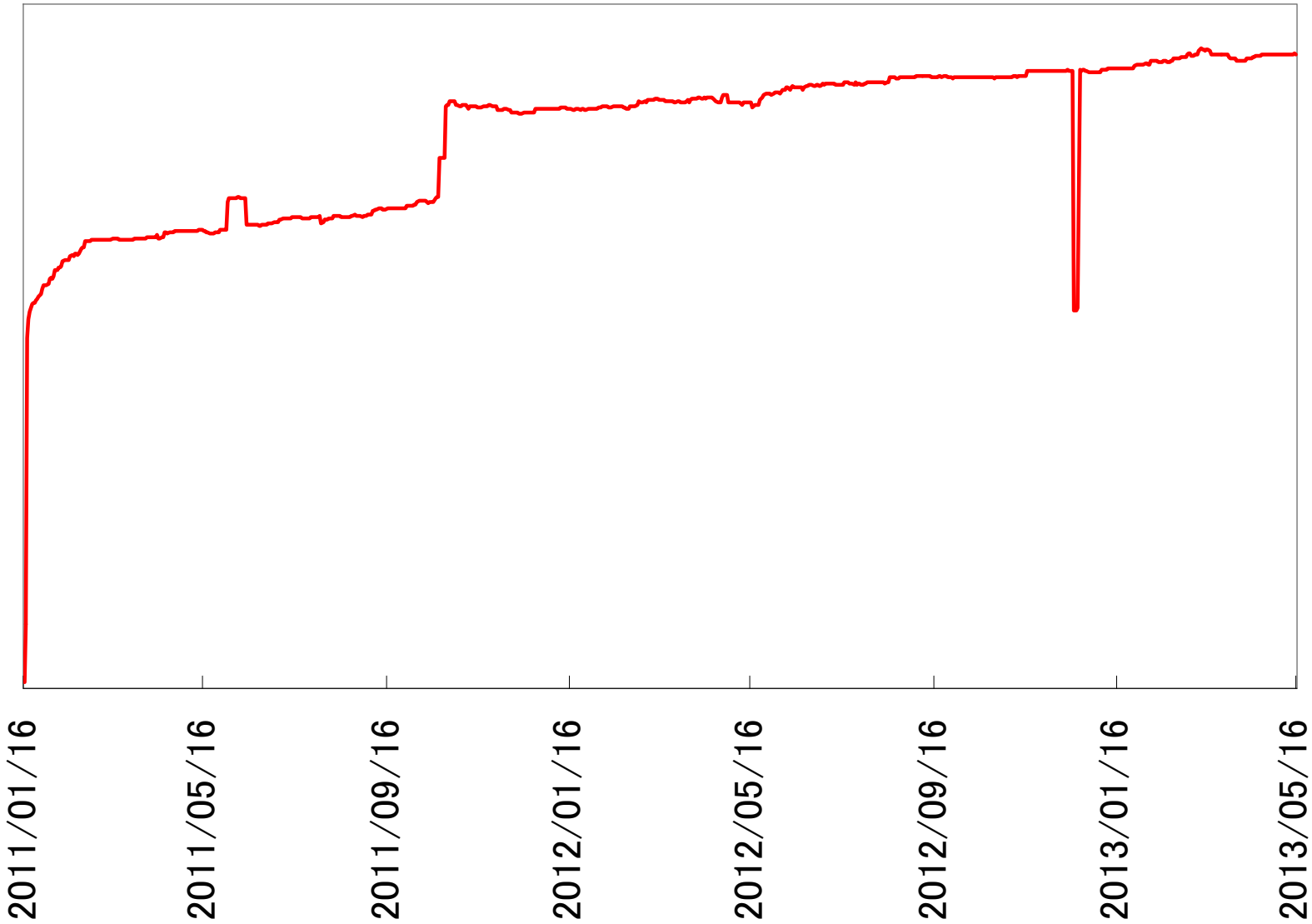
gTLD Registry Agreement (2013-04-29)

1.3. **DNSSEC**. Registry Operator shall sign its TLD zone files implementing Domain Name System Security Extensions ("DNSSEC"). During the Term, Registry Operator shall comply with RFCs 4033, 4034, 4035, 4509 and their successors, and follow the best practices described in RFC 4641 and its successors. If Registry Operator implements Hashed Authenticated Denial of Existence for DNS Security Extensions, it shall comply with RFC 5155 and its successors. Registry Operator shall accept public-key material from child domain names in a secure manner according to industry best practices. Registry shall also publish in its website the DNSSEC Practice Statements (DPS) describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material. Registry Operator shall publish its DPS following the format described in RFC 6841.

(http://newgtlds.icann.org/en/applicants/agb/base-agreement-specs-29apr13-en.pdf)

1. DSレコードの登録状況

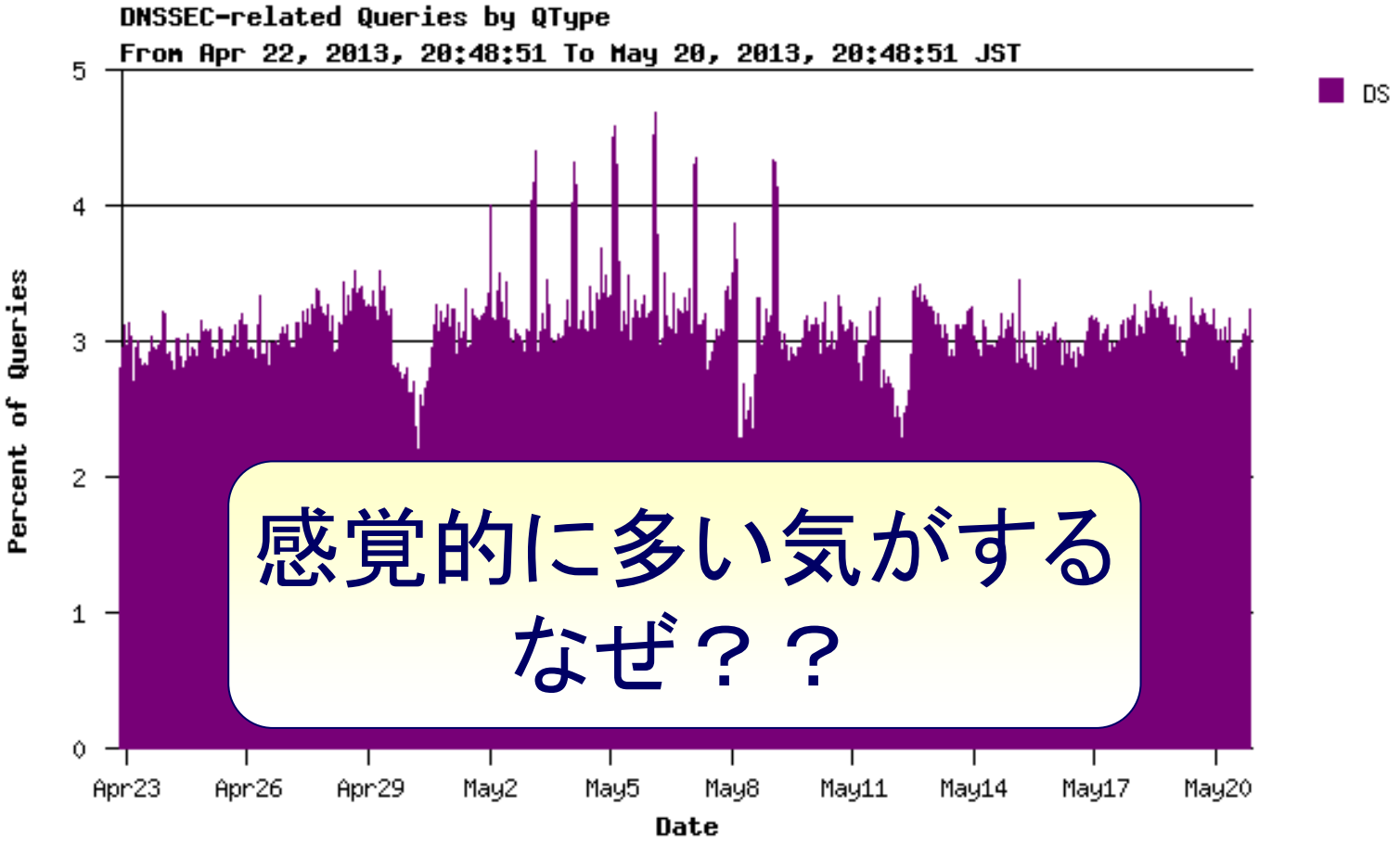
.JP



2. DSレコードの問い合わせ数(1/6)

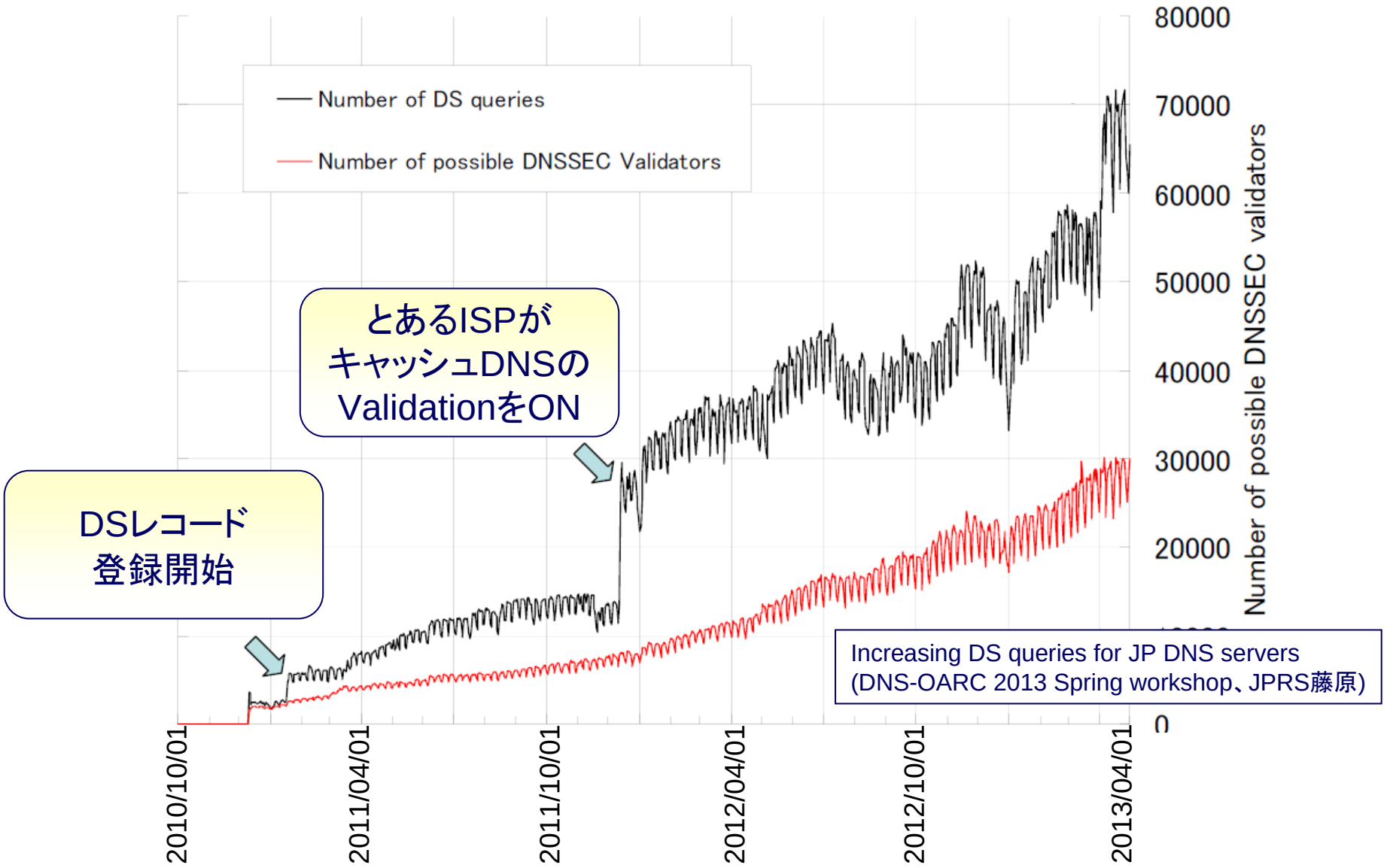
.JP

■ JP DNSへのクエリのうち3%がDSレコードの問合せ



2. DSレコードの問い合わせ数(2/6)

.JP



2. DSレコードの問い合わせ数(3/6)

.JP

■DSレコードの問い合わせ数が多い理由

– .JPのネガティブキャッシュのTTLは 900 ⇒ 15分

➔NS、DS、GlueレコードのTTLは 86400 ⇒ 1日

– JPドメイン名の多くは署名されていない

➔したがってDSレコードも登録されていない

– ValidatorはDSレコードがあるかどうか毎回確認

2. DSレコードの問い合わせ数(4/6)

.JP

■結果として・・・

– DSレコードが登録されておらず、かつ人気のある(アクセス数の多い) ドメインに対してValidation ONのキャッシュDNSサーバーから頻繁にクエリが来ることになる

– 最大で1日96回（86400÷900）のクエリが来る可能性がある

➔例えば、“google.co.jp” など

2. DSレコードの問い合わせ数(5/6)

.JP

■影響

– 権威DNSサーバー

➔Validatorの数が増えていき、かつドメイン名がDNSSEC署名(DSレコードが登録)されていかないとDSレコードのクエリが増大していく

➔ただしこれはRootやTLDなど委任の多いゾーンにおける問題

– キャッシュDNSサーバー

➔ValidationをONにしたキャッシュDNSサーバーがDSレコードを問い合わせる回数が増える

➔結果としてトラフィックが増大

2. DSレコードの問い合わせ数(6/6)

.JP

■対策案

– .JPゾーンのネガティブキャッシュTTLを長くする

➔2006年に更新間隔の短縮とともにネガティブキャッシュTTLを短くした経緯がある(※)

– すべてのJPドメイン名を署名する

➔現実的ではないか・・・

– 署名されていないJPドメイン名に対してダミーのDSを付け加える

➔プロトコルに手を加える必要あり

※JP DNSの設定変更について (http://jprs.jp/tech/dnsuis/info001.html)

3. DNSSEC と DNS Reflector Attacks

.JP

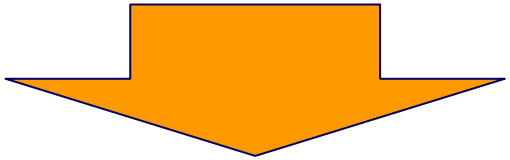
- DNSSECによって応答サイズが増大する
- 権威DNSサーバーを踏み台にして DNS Reflector Attackをしやすい状況になる
- JP DNSに対して ANY を引くと 1840 バイトの応答

  SOA, RRSIG(SOA),

  NS, RRSIG(NS),

  DNSKEY, RRSIG(DNSKEY),

  NSEC3PARAM, RRSIG(NSEC3PARAM)



Response Rate Limiting(RRL)の導入を検討中

その他

- DNSSECに対応したICANN認定レジストラの数
  - 2013年1月17日現在、25社
    (http://www.icann.org/en/news/in-focus/dnssec/deployment)
  - アメリカ(US)、スウェーデン(SE)、ドイツ(DE)、オランダ(NL)のレジストラが比較的多い
  - 申告制なので実際にはこれよりも多い可能性がある
  - 現在の契約ではDNSSECの対応は必須ではない

- DNSSECに対応したJPドメイン名指定事業者の数
  - 2013年5月1日現在、6社
    (http://jprs.jp/registration/list/)
  - 申告制なので実際にはこれよりも多い
  - 対応されている指定事業者様は是非ご連絡を！

jPRS
JAPAN REGISTRY SERVICES