.JPへのDNSSEC導入その後

民田雅人<minmin@jprs.co.jp>
株式会社日本レジストリサービス
2011-04-20
DNSSEC 2011 スプリングフォーラム

Copyright © 2011 株式会社日本レジストリサービス

.jpゾーンのDNSSEC対応関連イベント

- 2010-10-04　.jp DNSSECキーセレモニーの実施
  ⇒　KSK　RSASHA256　2048bit
  　　ZSK　RSASHA256　1024bit
- 2010-10-17　DNSSECによる署名開始
  不在証明はNSEC3オプトアウト方式
- 2010-10-29　更新のためのZSK事前公開開始日
  (2010-11-04に更新。その後ZSK更新5回)
- 2010-12-10　DSがルートゾーンへ登録され、
  署名検証可能となる
- 2011-01-16　JPドメイン名サービスへのDNSSEC導入完了 ⇒ JPドメイン名登録者がJPゾーンへDSを登録しDNSSEC運用可能となる

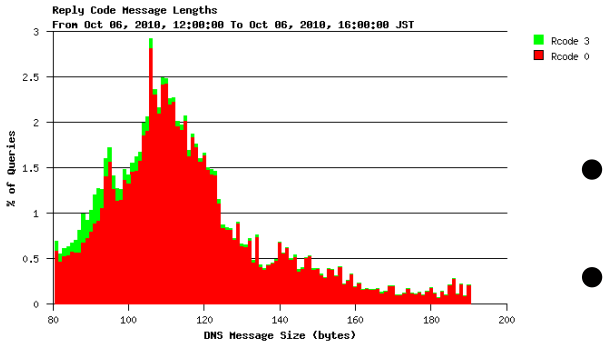
Copyright © 2011 株式会社日本レジストリサービス

DNSSEC導入後

- DNSSECに関係するトラブル等は皆無
- いくつかのドキュメントの公開
  - JPドメイン名におけるDNSSEC運用ステートメント(JP DPS)
    https://jprs.jp/doc/dnssec/jp-dps-jpn.html
    公開日は導入前、参考訳の英語版も公開
  - qmail/netqmailにおける512バイトを超えるDNS応答の不適切な取り扱いについて
    http://jprs.jp/tech/notice/2011-03-03-inappropriate-handling-for-long-dns-packet.html

Copyright © 2011 株式会社日本レジストリサービス

DNS応答サイズの分布
参考: 分布グラフの見方



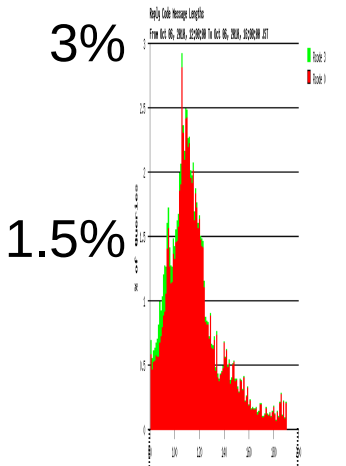
- a.dns.jpのDNS応答のパケットサイズ(バイト)を集計したもの
- X軸：応答パケットサイズ
- Y軸：パケットサイズの分布割合(%)
  ⇒ Y軸の値をX軸に沿って合計すると100%
- Rcode 0(赤)：正常応答
- Rcode 3(緑)：存在しないドメイン名の応答(不在応答)

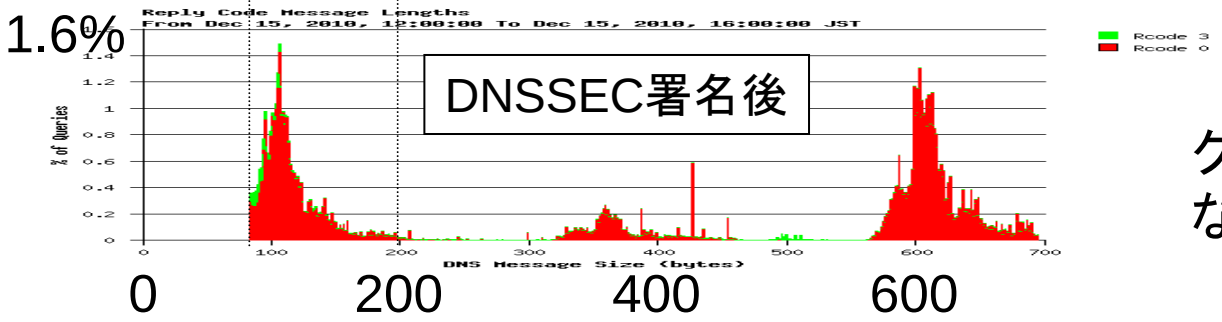
Copyright © 2011 株式会社日本レジストリサービス

DNS応答サイズの分布
DNSSEC署名前後での分布の違い

- DNSSEC署名前
  - 2010-10-06 12:00-16:00
  - トラフィックの山は110を中心とした分布
- DNSSEC署名後
  - 2010-12-15 12:00-16:00
  - 山が低くなり、110、360、610を中心とした3ヶ所にトラフィックが分布

DNSSEC署名前





グラフは、目盛りが同程度になるようリサイズ

Copyright © 2011 株式会社日本レジストリサービス

DNS応答サイズの分布
グラフの3ヶ所の山の違いは?

- 110を中心としたトラフィックの山
  - DNSSEC非対応の実装からの問合せへの応答
- 360と610を中心としたトラフィックの山
  - DNSSEC対応の実装からの問合せへの応答
  - 360の分布の山はNSEC3 RRとそのRRSIG1組、610の分布の山はそれが2組付加されたもの

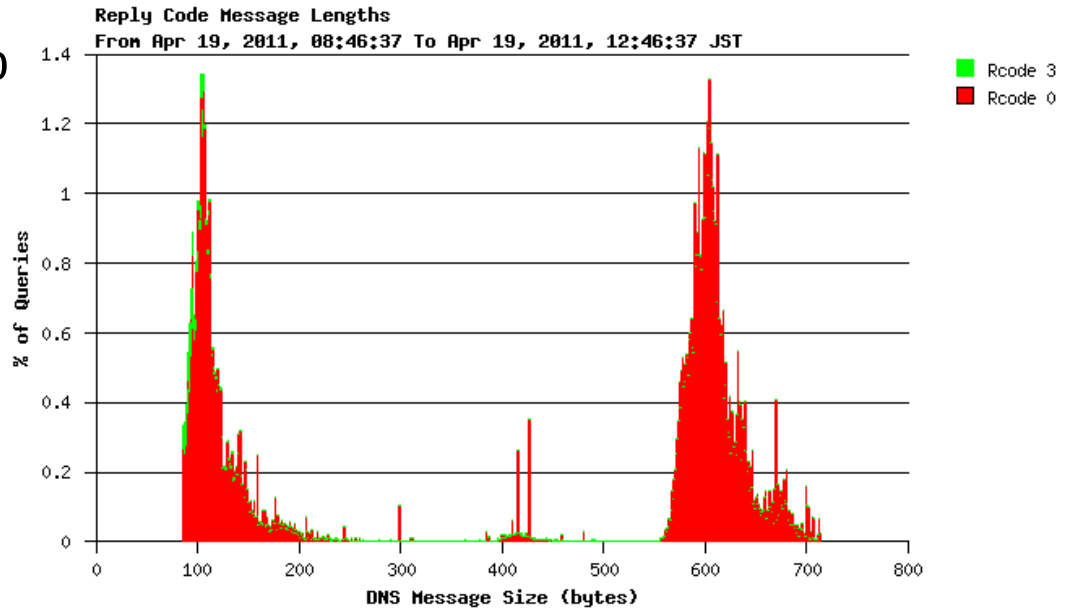
注意: 一般的にTLDのDNSSECで署名したDNSサーバの応答サイズは、末端サイトのそれより小さい

Copyright © 2011 株式会社日本レジストリサービス

DNS応答サイズの分布

現在の応答サイズの分布

1.4%



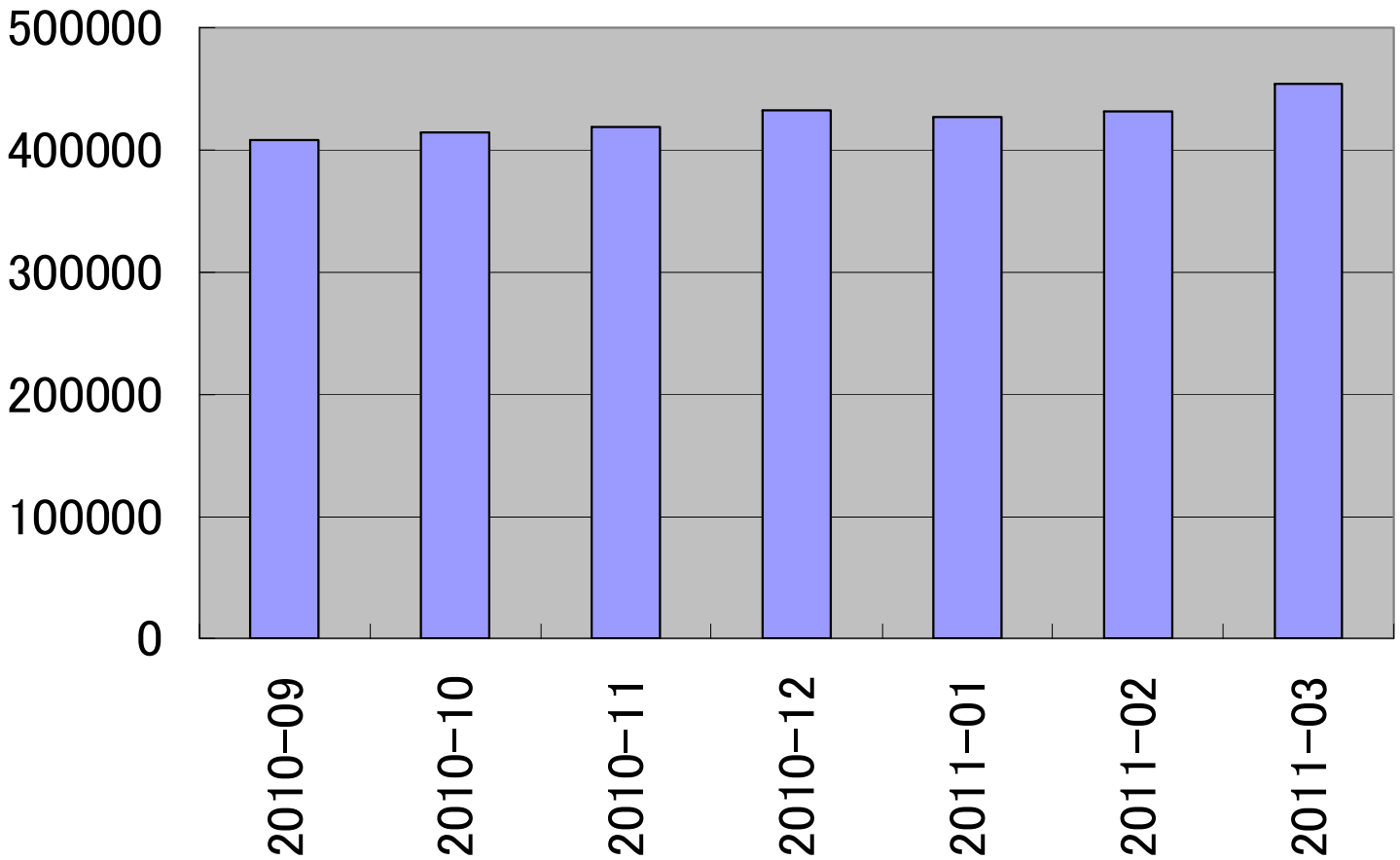
0 500

- 110の山 ⇒ DNSSEC非対応の実装への応答
- 610の山 ⇒ DNSSEC対応済み実装への応答
  - DNSSEC対応のキャッシュDNSサーバでは、JP DNSからの応答サイズは6倍程度になる

Copyright © 2011 株式会社日本レジストリサービス

DNSSEC対応実装の普及状況

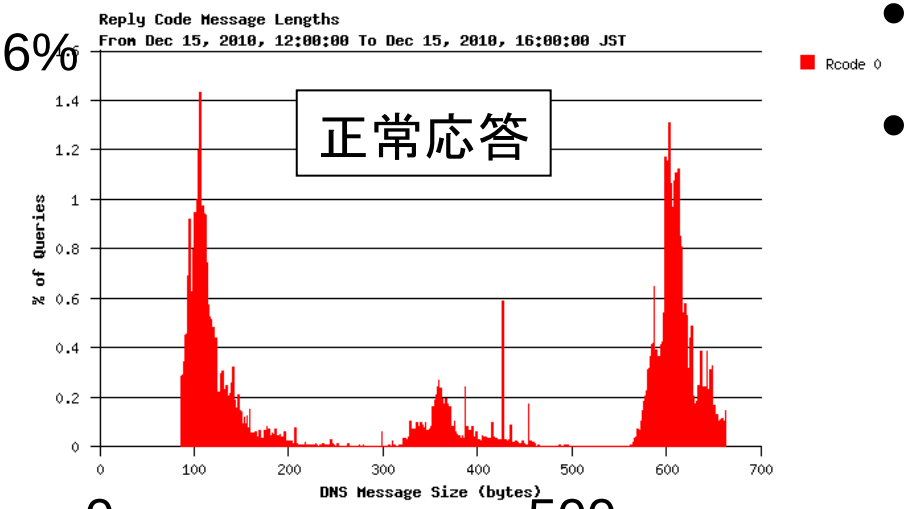
DOビット有りのユニークホスト数の変化(a.dns.jpでの調査)



Copyright © 2011 株式会社日本レジストリサービス

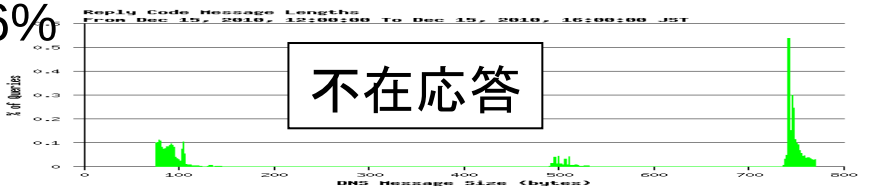
DNS応答サイズの分布
DNSSEC署名後の正常応答と不在応答

1.6%



0 500

0.6%



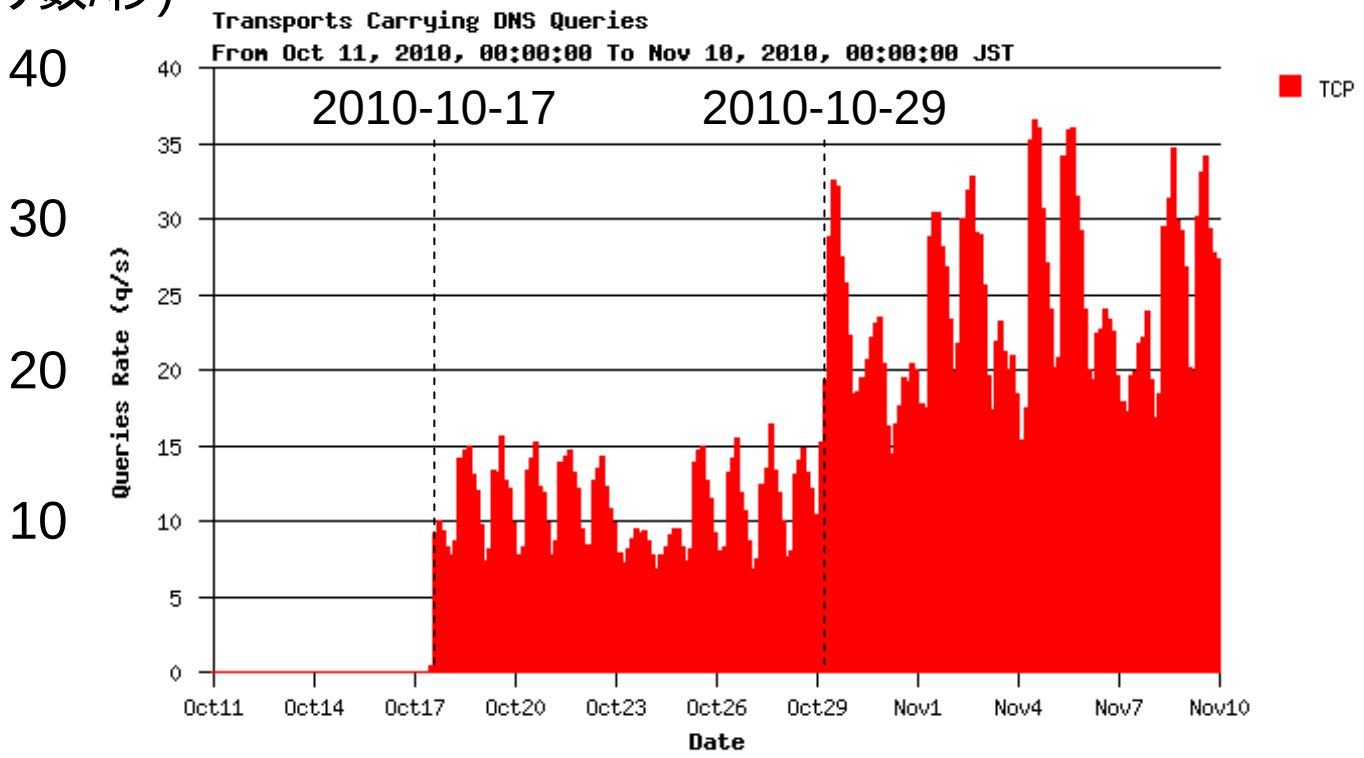
0 500

- 2010-12-15 12:00-16:00
- 不在応答は、正常応答に比べ中央と右の山が右へシフト
  ⇒ 大きい応答サイズの割合が正常応答より多い

Copyright © 2011 株式会社日本レジストリサービス

TCPでのクエリ(接続)数の変化
TCP接続数の変化のグラフ

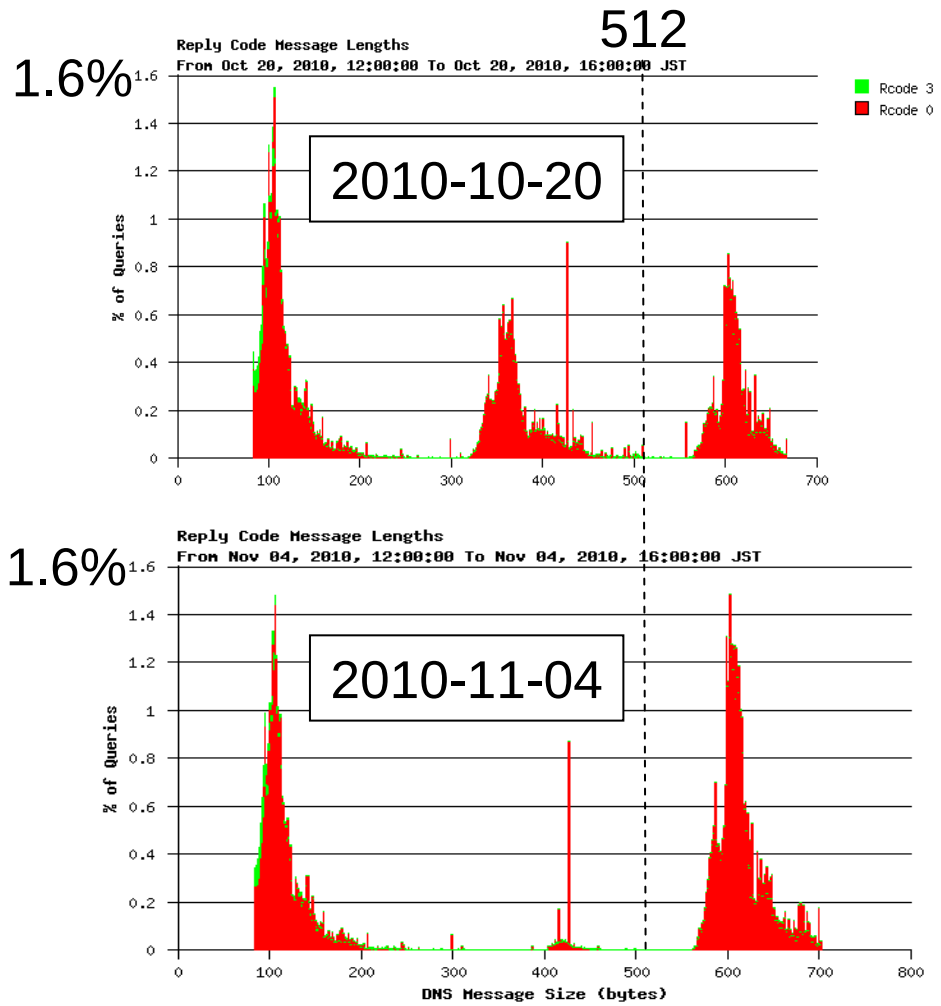
(クエリ数/秒)



- グラフの期間: 2010-10-11/11-10
- 2010-10-17の署名開始でTCP接続数が増加し、2010-10-29のZSK事前公開 (NSEC3パラメータを同時に変更)で更にTCP接続が増加

Copyright © 2011 株式会社日本レジストリサービス

TCPでのクエリ(接続)数の変化
2010-10-29前後のDNS応答サイズの分布



- 2010-10-29以降は360を中心とした分布がほとんど無い
  - NSEC3のパラメータが変わったことによる変化
  - 応答サイズがより大きいサイズに分布
- サイズの分布が大きくなるとTCPは増える傾向にある
  - DNSにUDPでの512の壁がある環境が少なからず存在すると考えられる

Copyright © 2011 株式会社日本レジストリサービス

DNSKEYの応答サイズ

- 現在のJPゾーンでのDNSKEYの応答サイズ

```
$ dig +dnssec jp dnskey | fgrep SIZE
;; MSG SIZE  rcvd: 1203
```

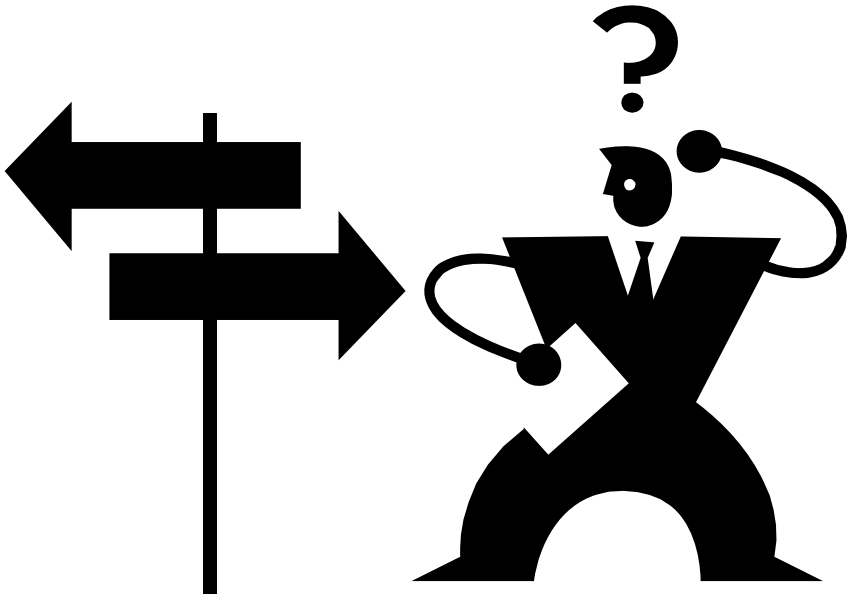
  - DNSKEYの構成は、ZSKが3個、KSKが1個、ZSKによるRRSIGが1個、KSKによるRRSIGが1個
- 現在の設定のままKSKの鍵更新を行うと、DNSパケット分だけで1769
  - 一般的なMTUである1500より大きく、UDPフラグメントの問題にあたる可能性が高い
- DNSKEYのサイズを小さくするべく準備中

  方針：DNSKEYに載せるZSKを減らし、ZSKによるDNSKEYへのRRSIGは無くす(無くしても実害は無い)

Copyright © 2011 株式会社日本レジストリサービス

Q & A

JAPAN REGISTRY SERVICES



Copyright © 2011 株式会社日本レジストリサービス