JP DNSが返すもの
- DNSSEC対応によるDNSトラフィックの変化 -

民田雅人<minmin@jprs.co.jp>
株式会社日本レジストリサービス
2011-01-20 JANOG27@金沢

Copyright © 2011 株式会社日本レジストリサービス

目次: JP DNSが返すもの

- JP DNS(a.dns.jp)とのDNS通信状況に注目
  - DNSSEC署名前後でのDNS応答のトラフィック分布をグラフで紹介
  - TCPでの接続状況
  - DNSSECの署名検証に不可欠な、DNSKEY RRのDNS応答サイズの状況

Copyright © 2011 株式会社日本レジストリサービス

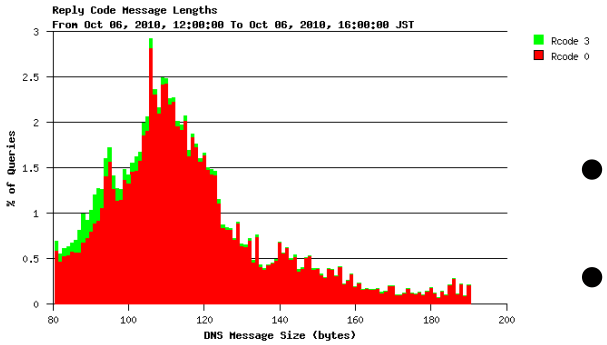
.jpゾーンのDNSSEC対応関連イベント

- 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
  (11/4に更新。その後ZSK更新2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

★が本発表のキーイベント

Copyright © 2011 株式会社日本レジストリサービス

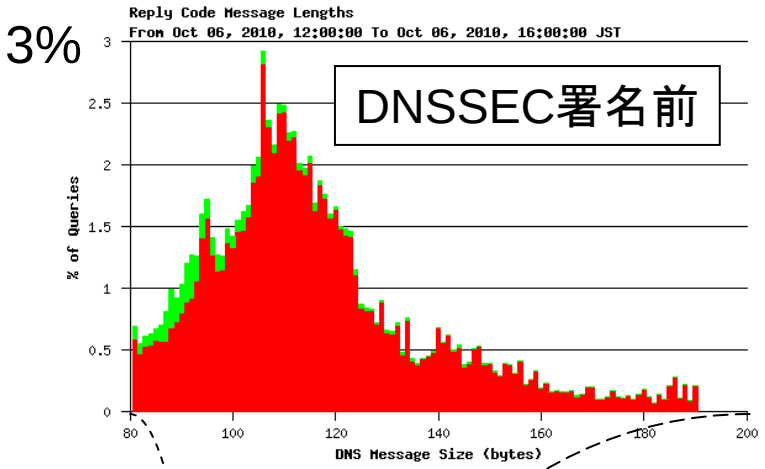
参考: DNS応答サイズの分布グラフの見方

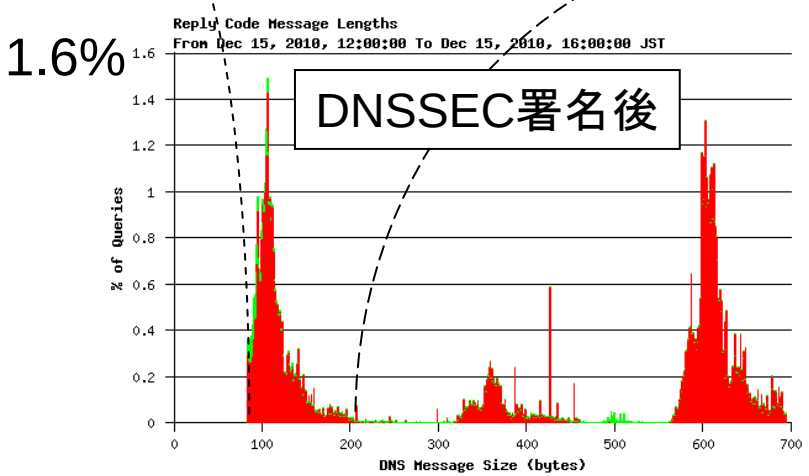


- a.dns.jpのDNS応答のパケットサイズを集計したもの
- X軸：応答パケットサイズ
- Y軸：パケットサイズの分布割合(%)
  ⇒ Y軸の値をX軸に沿って合計すると100%
- Rcode 0(赤)：正常応答
- Rcode 3(緑)：存在しないドメイン名の応答(不在応答)

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を中心とした分布のみ
- DNSSEC署名後
  - 2010-12-15 12:00-16:00
  - 110、360、610を中心とした3ヶ所にトラフィックの山が分布

Copyright © 2011 株式会社日本レジストリサービス

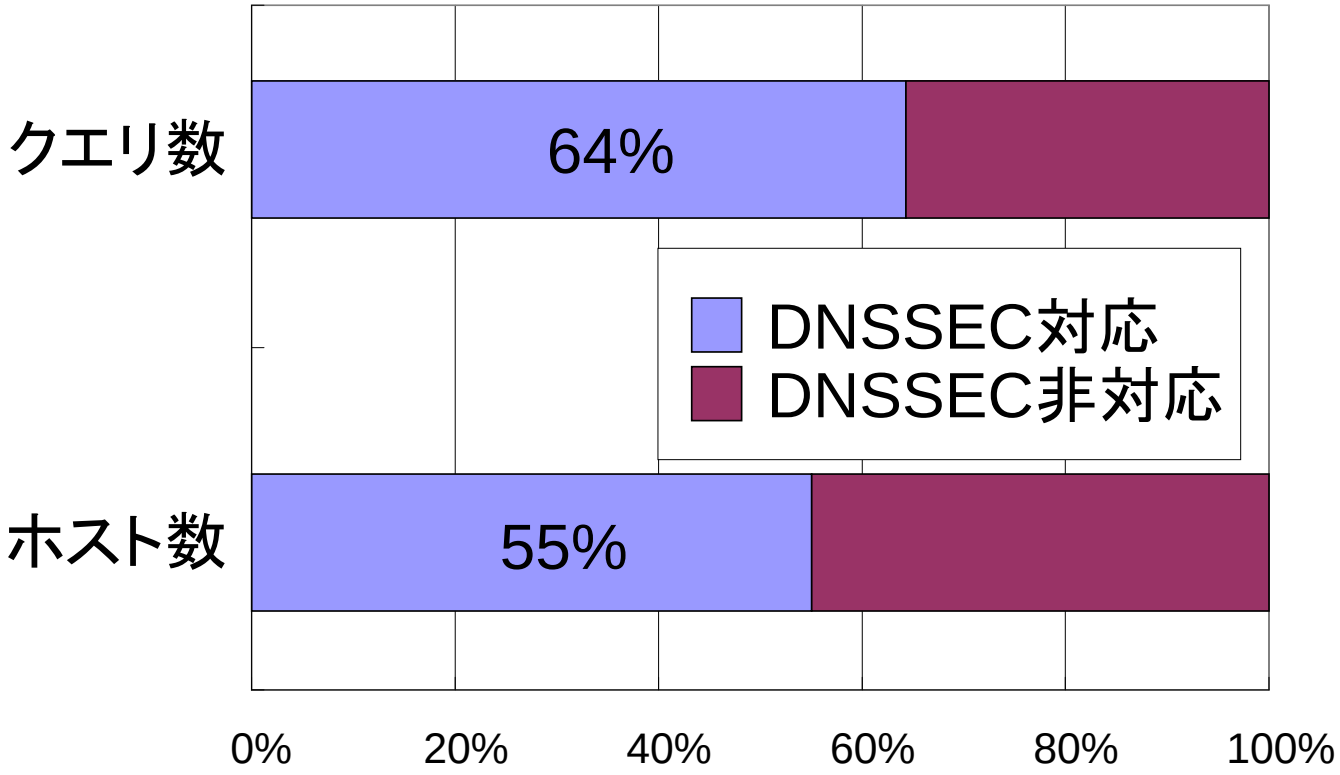
DNS応答サイズの分布 グラフの3ヶ所の山の違いは?

- 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

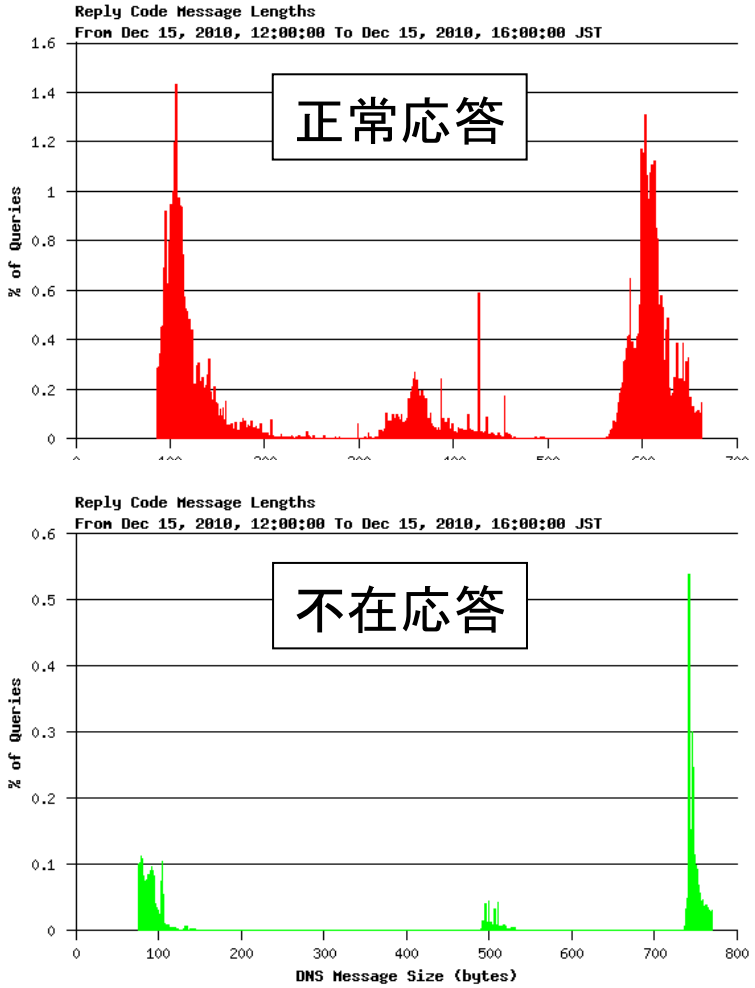
DOビットの有無から推測したDNSSEC対応実装の割合



- DNSSEC署名**検証可能な実装**を利用している割合
  - 2011-01-11 のa.dns.jpへのクエリより調査

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



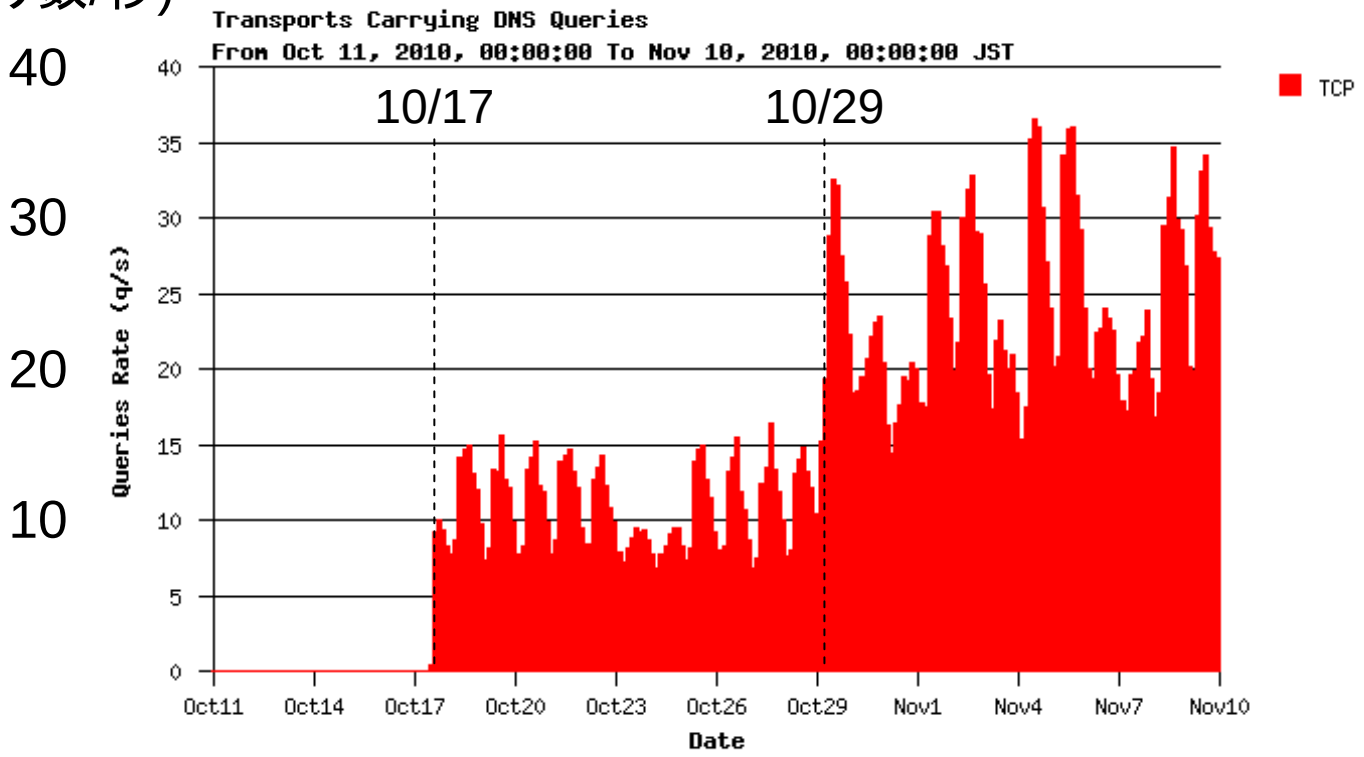
- 2010-12-15 12:00-16:00
- 正常応答
  X軸最大700　Y軸最大1.6%
- 不在応答
  X軸最大800　Y軸最大0.6%
- 不在応答は、正常応答に比べ中央と右の山が右へシフト
  ⇒大きい応答サイズの割合が正常応答より増加

参考:「あなたのDNS運用は来るべきDNSSEC時代に耐えられますか」@JANOG24

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

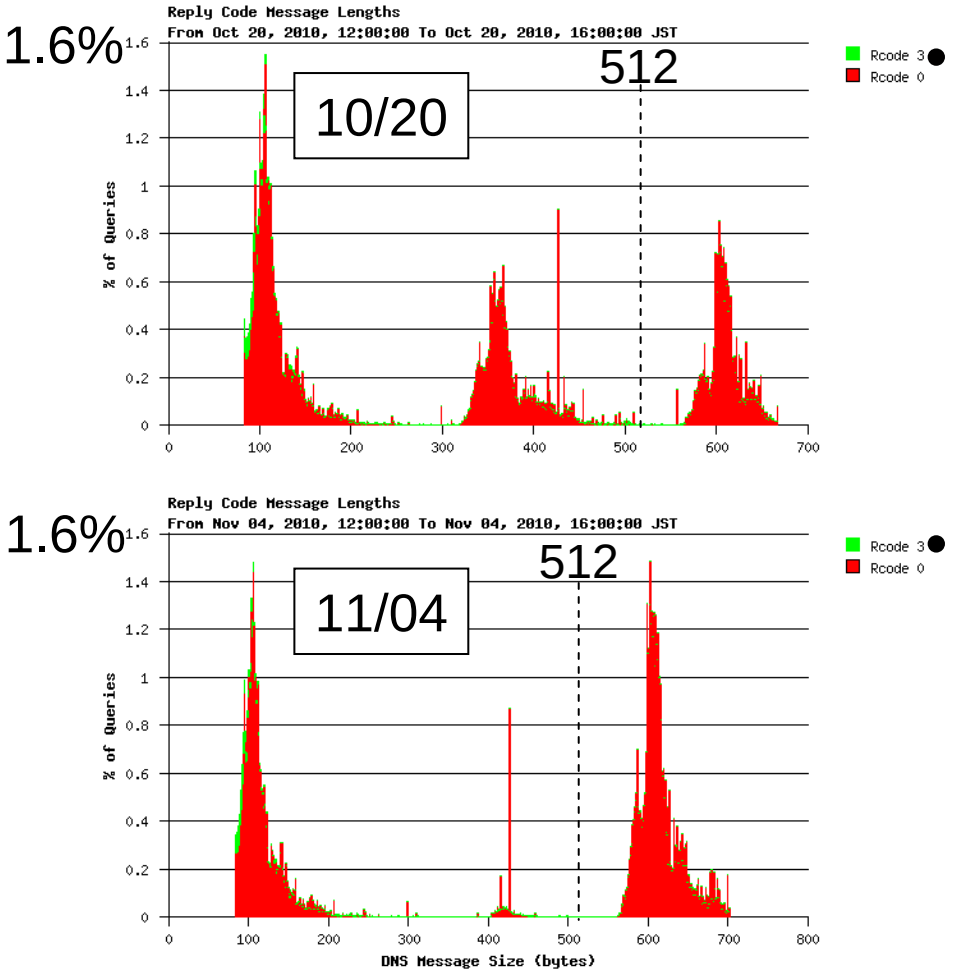
(クエリ数/秒)



- 2010-10-11 ～ 2010-11-10
- 10/17の署名開始でTCP接続数が増加し、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
10/29前後のDNS応答サイズの分布



- 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
```

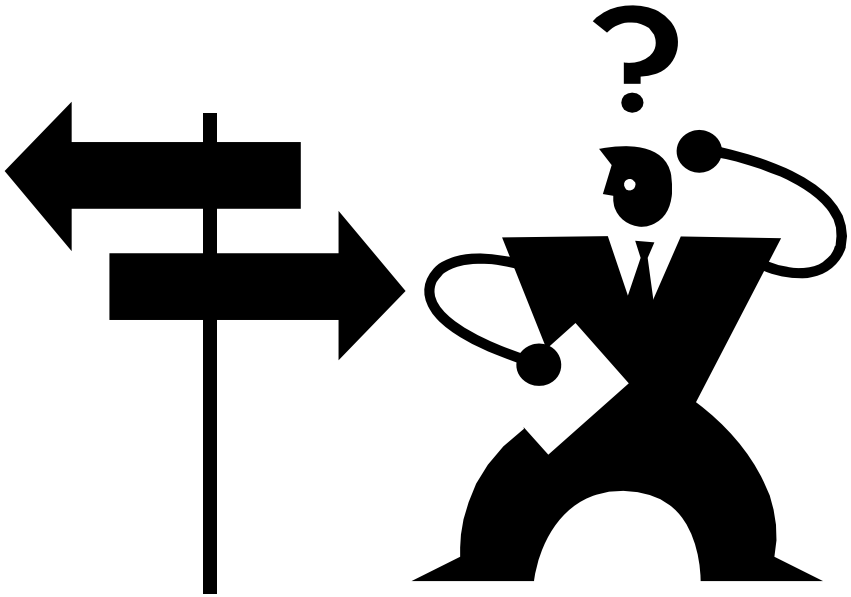
  - DNSKEYの構成は、ZSKが3個、KSKが1個、ZSKによるRRSIGが1個、KSKによるRRSIGが1個
- 現在の設定のままKSKの鍵更新を行うと、DNSパケット分だけで1769
  - 一般的なMTUである1500より大きく、UDPフラグメントの問題にあたる可能性が高い
- DNSKEYのサイズを小さくする方向で調整中

  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

御清聴ありがとうございました

JAPAN REGISTRY SERVICES



Copyright © 2011 株式会社日本レジストリサービス