DNSSECがやってくる
権威DNSサーバへの導入

(株) NTTPCコミュニケーションズ
高田美紀
takata@nttpc.co.jp

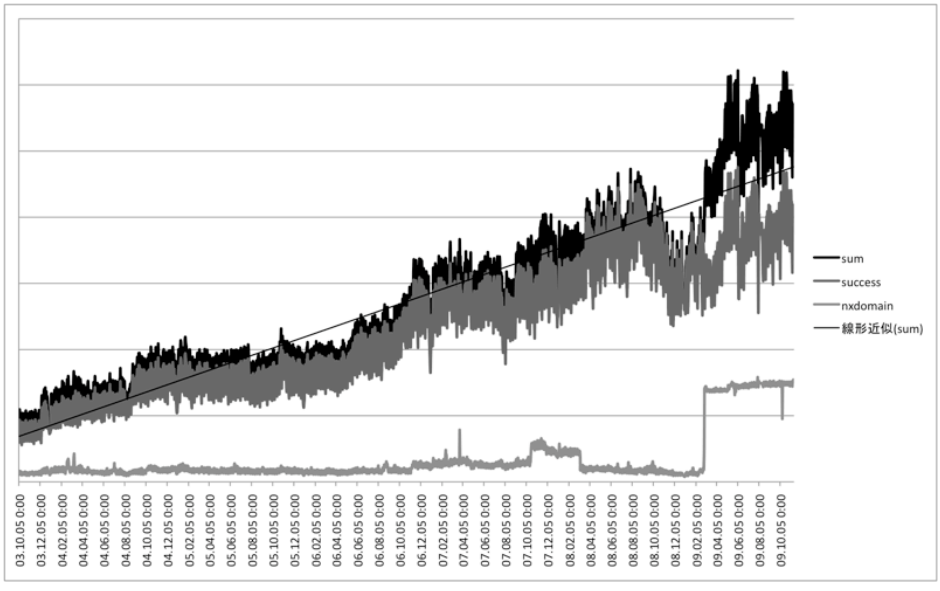
サーバ対応

- BIND
  - 9.4.3-P2, 9.5.1-P2, 9.6.1, or later
  - options { dnssec-enable yes; };
- 時刻同期
  - ntp等で適切に。

リソース

- 65,000zone, 268MB
- 全部にsignすると。。
  - 2GB
  - sign時間
  - bindの起動時間
  - その他

query数の増加



パケットサイズ

- 1queryあたりのパケットサイズ比較
  - before: 82+191=273bytes
  - after: 82+867(DNSKEY)+ 82+972(RR)=2,003bytes
  - 7.3倍。DNSKEY抜きでも3.9倍
- 段階的な導入

署名、鍵の登録フロー

- コンパネツール
  - https
  - 鍵生成ボタン、KSK表示
- レジストリへKSKを登録
- コンパネにてdlvレコード登録(DLV)

検証失敗

- 検証に失敗した場合
- SERVFAILが返る
  - RRがきちんと設定されていても
- キャッシュには古い鍵があるが、権威サーバ側には新しい鍵しかない場合等
- キャッシュ/権威サーバの切り分け
  - DNSSECによるものなのかどうか?

鍵の更新フロー(1)

- ZSK/KSK支配下のRRSIG TTL切れ前に新しい鍵ペアを作成、その鍵で署名
- 古い鍵が必要なくなった時点で削除
- ZSKはゾーン内で閉じているので他への影響はない
  - 2つ鍵を作り、片方で署名、両方を公開
  - 好きな時に新しい鍵で署名
  - 古い方のTTLを過ぎたらゾーンから削除

鍵の更新フロー(2)

- KSKの更新には親への届けが必要
  - 2つのDSなりDLVが親にある状態
- 更新時の注意点
  - セカンダリの確認
  - 鍵長と更新時期の設定
  - 更新の自動化は難しい?

そこまでやっても。。

- エンドユーザにDNSSEC検証が成功したことを知らせる術がない
  - FireFoxのAdd-Onで検証結果を見せてくれるものがある
    - http://labs.nic.cz/page/691/dnssec-add-on-for-firefox/
    - httpsの鍵マークとの違い
- ほかにはメールヘッダくらい?

NTTPC COMMUNICATIONS

まとめ

- レジストリへのDLVやDSの登録インタフェースはまちまち
- 鍵の更新、移転に混乱を生じる懸念
- DNSSEC単体では売れないだろうけど、証明書屋さんと組むといいかも(?)