DNSSEC at the Root

加藤 朗

慶應義塾大学/WIDE Project
kato@wide.ad.jp

DNSSEC at Root 始めました

DNSSEC への長い道のり

☆ 2005 年頃

- AAAA と DNSSEC の二つが課題
- DNSSEC 可能性についての議論
  - ICANN RSSAC/SSAC
- bind8 時代
  - bind9 の性能が問題だった

☆ Root を変更することに関して

- 技術的問題
  - DNS を壊さないか
  - 問い合わせの急増はないか
- 手続き的問題
  - どう validate するか

DNSSEC への長い道のり

☆ **Kaminsky Attack : 2008/7**

- 一部には古くから知られていた手法
- 大きな社会的な警告
- 確かに検出は比較的容易
- 対応も困難ではないかも
  - 繰り返し問い合わせ
- 低確率だが成功の可能性あり
  - 再帰問い合わせの限定による回避

☆ これが **DNSSEC** への推進に大きく貢献

懸念

☆ DNSSEC の verification 過程

- Recursive Server や resolver の問題
- とりあえず Root ではない

☆ Root サーバの懸念

- 大きな応答によって起る副作用
  - ホームルータ
  - セキュリティ装置
- サーバの負荷の増大
  - Lab test : それほどではない
- 問い合わせの急増
  - やってみないと分からない

☆ Root zone

- NSEC (NSEC3 ではありません)

DURZ

☆ **DURZ**

- Deliberately-Unvalidatable Root Zone

☆ とりあえず **DNSSEC** を「模倣」

- 大きな応答を返す
  - DNSSEC したのと同じ
  - ただし、検証はできない
  - 嘘な鍵
- サーバの負荷
  - 一問い合わせの処理は DNSSEC と同じ
  - 検証による問い合わせ増は不明

DURZ

☆ **Root** に順次導入する

- 導入時にトラフィックの計測
- 大きな応答が届かない

→ 他の Root へ問い合わせ

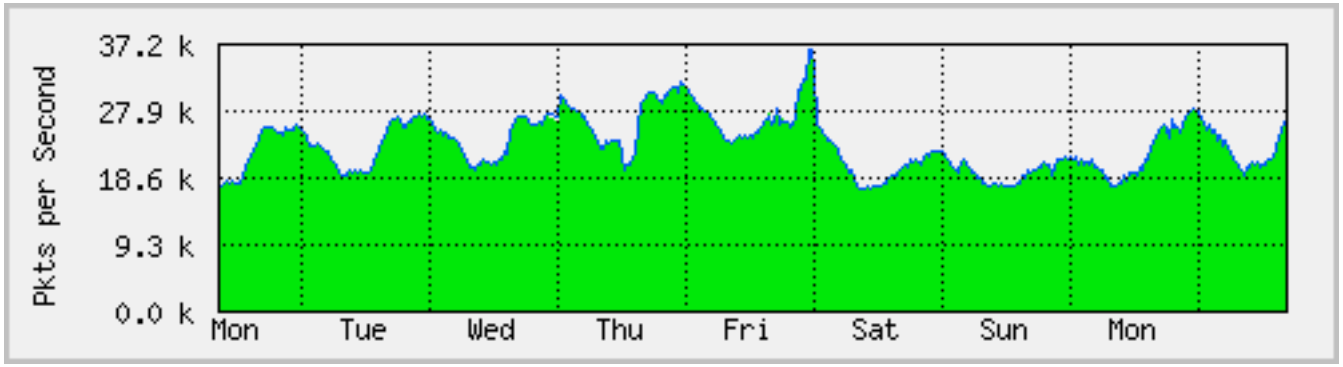
☆ 経過

- 1/27: L-Root (1)
- 2/10: A-Root (2)
- 3/03: M-/I-Root (4)
- 3/24: D-/K-/E-Root (7)
- 4/14: B-/H-/C-/G-/F-Root (12)
- 5/05: J-Root (13)

July 16th early morning

☆ アナウンス：**Jul 15, 16:51 -0400**

- つまり、Jul 15, 20:51 UTC
- つまり、Jul 16, 05:51 JST



- 鍵を交換
  - 検証可能なものに
- 以上

今後

☆ 計測

- transition に関する問い合わせデータ
- 最新版の解析はまだ

☆ **key rollover**

- bind のバグによる問い合わせの急増
  - 既に直っている
  - 古いバージョンを使っている人は...

問い合わせ

☆ ぴんぽんだっしゅ

- 約半数の TCP Query は中身なし
  - Root へ TCP セッション確立
  - 問い合わせなし
  - FIN
- インターネットの接続性確認？
  - ご存じの方は一方ください。

おあとが宜しいようで