Root DNS Servers

Akira Kato

Keio Univ./WIDE Project
kato@wide.ad.jp

最近の **Root DNS** サーバ

☆ **http://www.root-servers.ORG/**

☆ **Site** 数は約 **1525**

- サーバの台数、ではない
  - 各拠点で複数のサーバというケースも
  - 小規模な local site は、1U 一枚というケースも
- クラウドとの提携も増えてきた
  - PCH、Cloudflare
  - 細かい交渉などが不要になる利点も
  - 運用責任は変わらず
  - 一地点が消滅しても大きな影響は無し

M Root: MoU with APNIC

☆ **APNIC** との **MoU : 2020** 年 **8** 月

- M-Root の展開を APNIC がサポート
  - 主に APNIC 地域
- "Small Anycast"
- 1U サーバ、1U スイッチ他、５年間で 1.5M JPY
  - 地域によって同じ機材でも大きな値段差
- 機材は APNIC が無償貸与可能
  - Root サーバが少ない地域
- 現地で準備が必要な資源
  - 物理的な場所、IX ポート、Admin Transit

M-Root DNS

☆ 現在、**21** サイト

- 東京 (3)、大阪、ソウル、サンフランシスコ (2)、
- パリ (2),
- Brisbane, Hanoi, Guam, Kuala Lumpur, Bangkok,
- シンガポール, Kaohsiung, Jakarta, Ulaanbaatar, 香港,
- Phnon Pennh, Kathmandu, サンパウロ, Dhaka, Mumbai,
- Lahore
  - 13 letter 中 9 位
- ほぼ全拠点 IPv6 ready
- 合計 94kqps 程度、おそらく全体の 1/13 程度
- IPv6 率 : 18.9%
- EDNS 率 : 88.4% (IPv4: 86.5%, IPv6: 96.3%)

M Root: MoU with APNIC

☆ **APNIC** との **MoU : 2020** 年 **8** 月

- M-Root の展開を APNIC がサポート
  - 主に APNIC 地域
- "Small Anycast"
- 1U サーバ、1U スイッチ他、５年間で 1.5M JPY
  - 地域によって同じ機材でも大きな値段差
- 機材は APNIC が無償貸与可能
  - Root サーバが少ない地域
- 現地で準備が必要な資源
  - 物理的な場所、IX ポート、Admin Transit

KSK 更新

☆ **KSK** 更新 **(RSASHA256)**

- 当初は 7 年毎を想定
  - もうすこし短い方がよい、との声
- 初代 : KSK-2010 (key tag 46211)
- 二代目 : KSK-2017 (key tag 20326)
- 2.5 代目 : KSK-2023、HSM 問題で廃棄
- 三代目 : KSK-2024 (key tag 38696)
  - 2025 年 1 月に Root Zone に出現予定
  - 2025 年 10 月に Roll over 予定

KSK 更新

☆ **RFC5011** による自動更新

・ サポートされている環境では特段の操作は必要なし

☆ 積極的な鍵更新が必要な場合

・ 長期間落ちていた計算機

・ 少し古い install media で install した場合

– ソフトウェアやアプライアンスの説明書への記述

今後の予定

☆ **KSK** アルゴリズム更新

- 楕円暗号系アルゴリズムへの移行を検討
- （同一強度なら）鍵長が短くできる
- パケットの肥満防止に貢献
  - 特に ZSK/KSK rollover 時
- KSK-2027?:
  - 2027 年 4 月に生成
  - 2029 年 10 月に導入
- ECDSAP256SHA256 (Algorithm 13) が想定