# 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 **1530**

- 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 DNS



☆ 現在、１４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, Kaohsiung,

・ Jakarta, Ulaanbaatar

－ 13 letter 中 9 位

・ ほぼ全拠点 IPv6 ready (A/B/C/D/G/H/J/K と同位)

・ 合計 67kqps、おそらく全体の 1/13 程度

・ IPv6 率 : 16.7%

・ EDNS 率 : 84.7% (IPv4: 83.4%, IPv6: 91.0%)

# プライバシ問題



☆ **Root DNS** サーバへの問い合わせ
- Cache で処理できなかったもの
- 基本的には junk query が大部分

☆ ユーザからの **QNAME** が含まれる
- ただし、誰からの問い合わせかは分からない

☆ パケットの暗号化
- 状態管理が必要
- Anycast やロードバランスとの相性は悪い

# プライバシ問題



☆ おすすめ

- QNAME Minimization (RFC7816)
  - QNAME を最小限化、Root へは TLD のみ
  - AC.JP などの zone cut と伴わない場合との相性？
  - NCACHE による応答時間改善も期待
  - 逆引きなど '.' が多い場合の性能問題
- Aggressive Use of cache (RFC8198)
  - NSEC/NSEC3 により NXDOMAIN を直ちに返答
  - 性能改善にも

# 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: MoU with APNIC



☆ **Large (global) Sites:**

- Singapore, (Hong Kong)

☆ **Small (local) Sites:**

- Brisbane/AU, Hanoi/VN, Guam/GM, Kuala Lumpur/MY,
- Bangkok/TH, Kaohsiung/TW, Jakarta/ID, Ulaanbaatar/MN,
- (Manila/PH), (Kathmandu/NP), (Dhaka/BD), (Lahore/PK),
- (Phnon Phenn/KH), (Mumbai/IN), (Kalkata/IN),
- (Jinan/CN), (Wuhan/CN), ....

☆ **Locally funded Large (global) Site:**

- (Sao Paulo/BR by NIC.BR)

# 最近の変化



☆ **2023/09 Zone MD** の追加
- Root Zone に対して Zone MD レコード
- Zoom MD を用いたチェックは一部のみ

☆ **RoA** の追加
- 多くの Root サーバは ARIN アドレス
- RoA の署名元の Diversity が問題
- M-Root （のみ）は APNIC
  - IPv6 RoA は 2017.09 から。IPv4 はまだ。
- B-Root は LACNIC アドレスへ移転計画中
  - アドレスの変更が発生予定

# 今後の予定



☆ **KSK** 更新
- 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
- 二代目 : KSK-2017
- 新しい鍵は間もなく生成 (KSK-2023? KSK-2024?)
- ただし、同じアルゴリズム : RSASHA256

☆ **RFC5011** による自動更新
- 主要な DNSSEC 対応 DNS ソフトウェアで実装
- 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

# 今後の予定



☆ **KSK** アルゴリズム更新

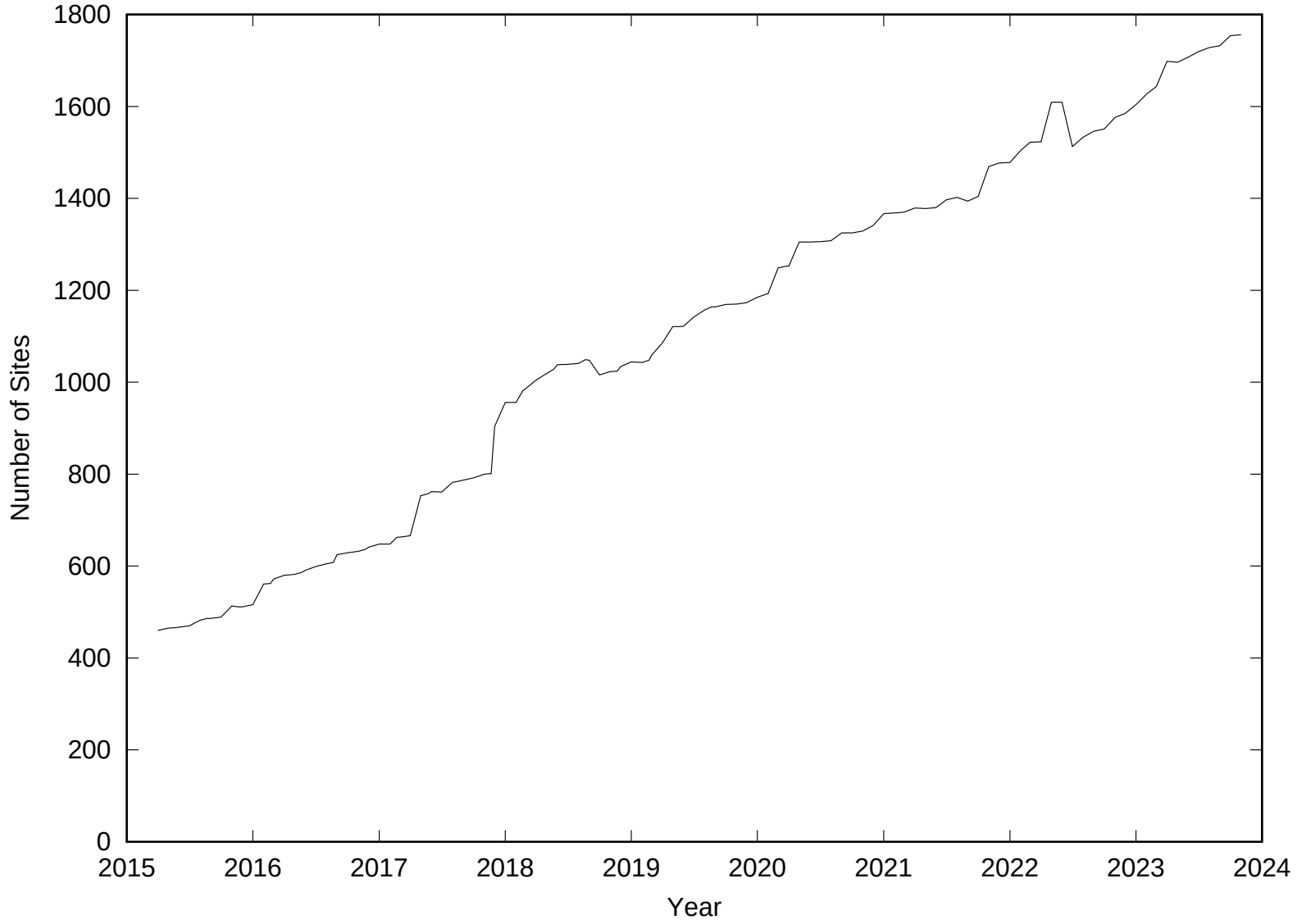
- 楕円暗号系アルゴリズムへの移行を検討
- （同一強度なら）鍵長が短くできる
- パケットの肥満防止に貢献
  - 特に ZSK/KSK rollover 時
- KSK-2023/2024 の次の更新時、に実施を検討
- ECDSAP256SHA256 (Algorithm 13) が想定

https://www.icann.org/en/public-comment/proceeding/draft-report-of-the-root-zone-dnssec-algorithm-rollover-study-19-10-2023

https://itp.cdn.icann.org/en/files/domain-name-system-security-extensions-dnssec/draft-report-root-zone-dnssec-algorithm-rollover-study-19-10-2023-en.pdf

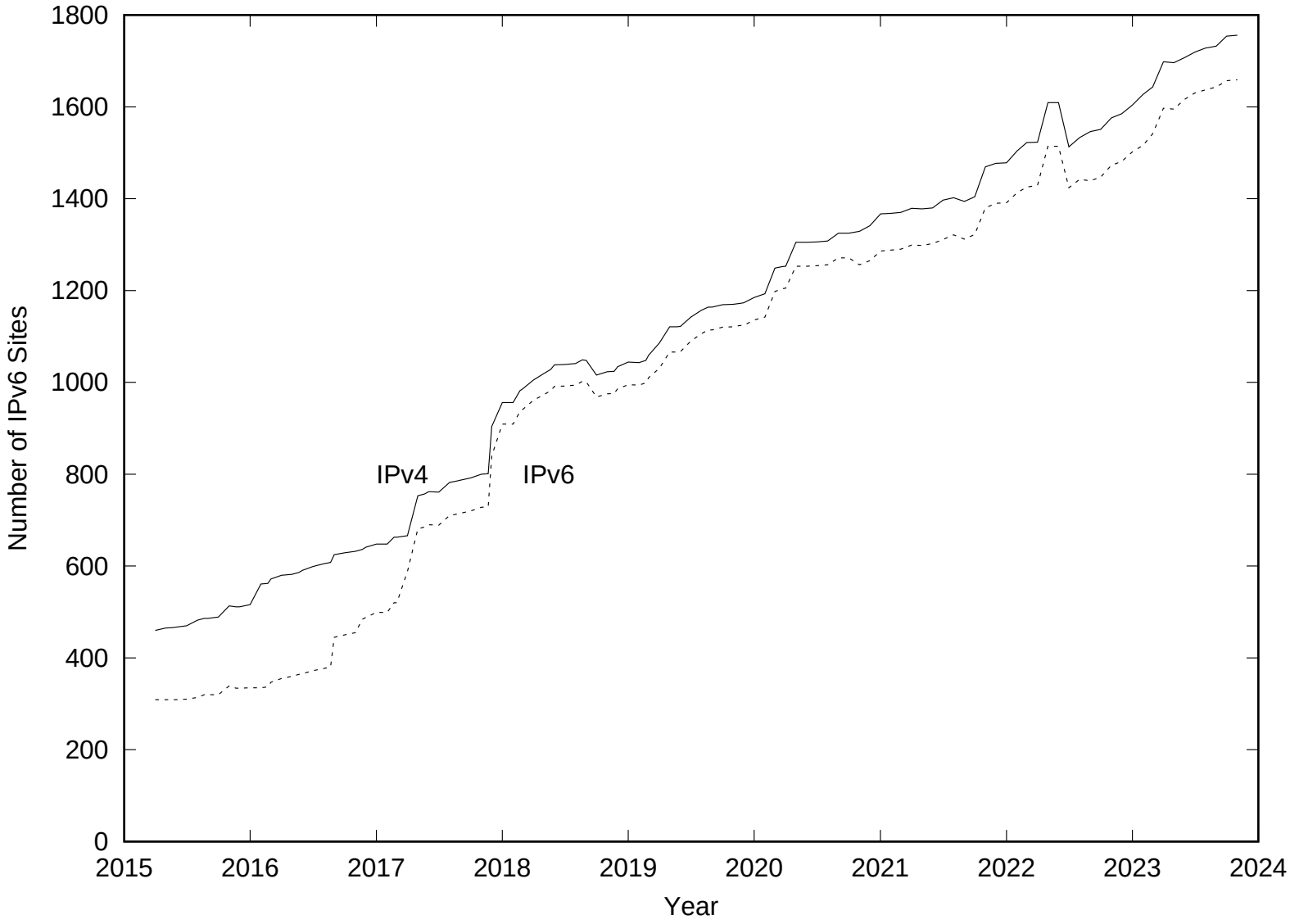
# **Root DNS** サーバ：総サイト数の推移





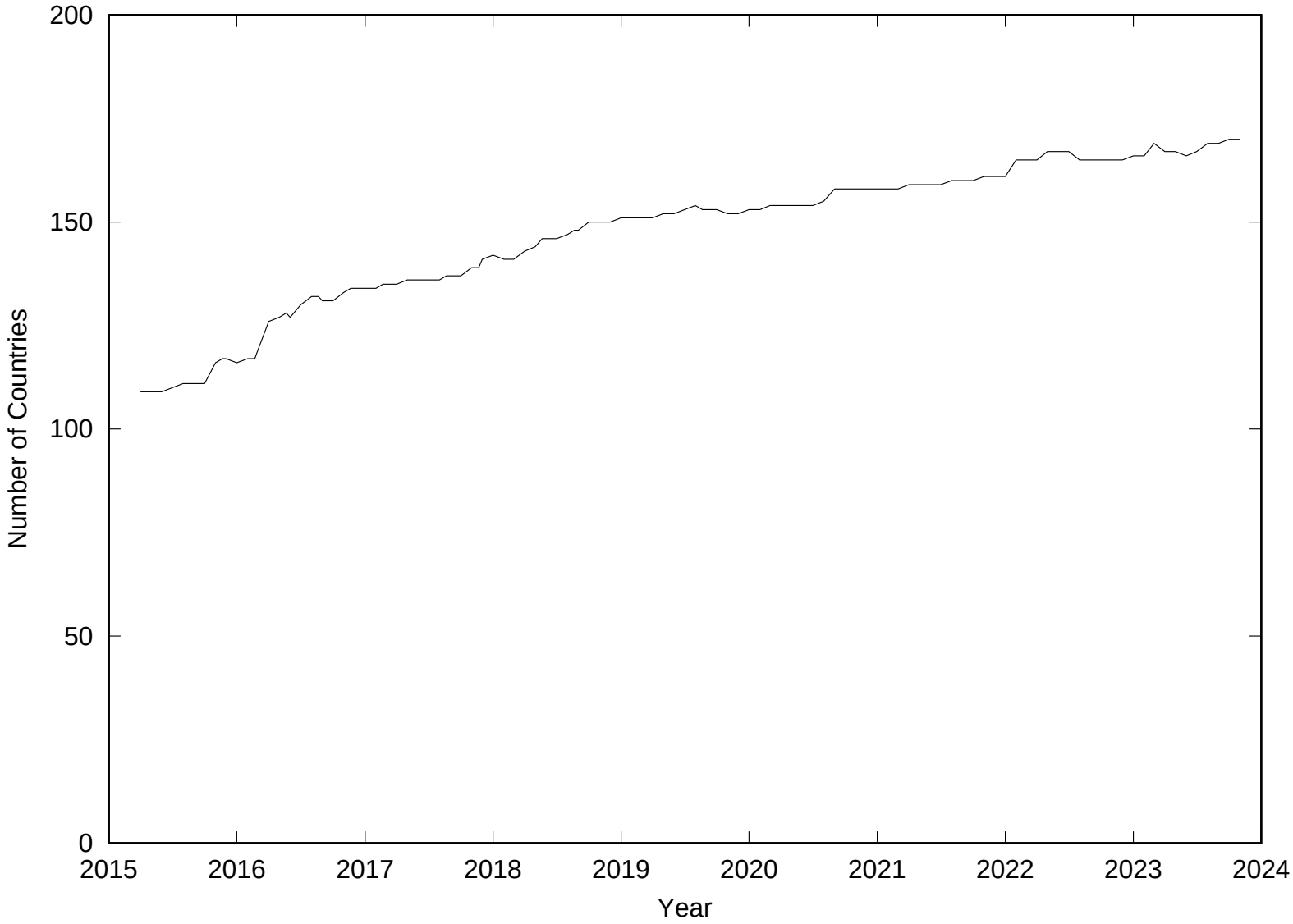
# Root DNS サーバ : IPv6 サポートの推移





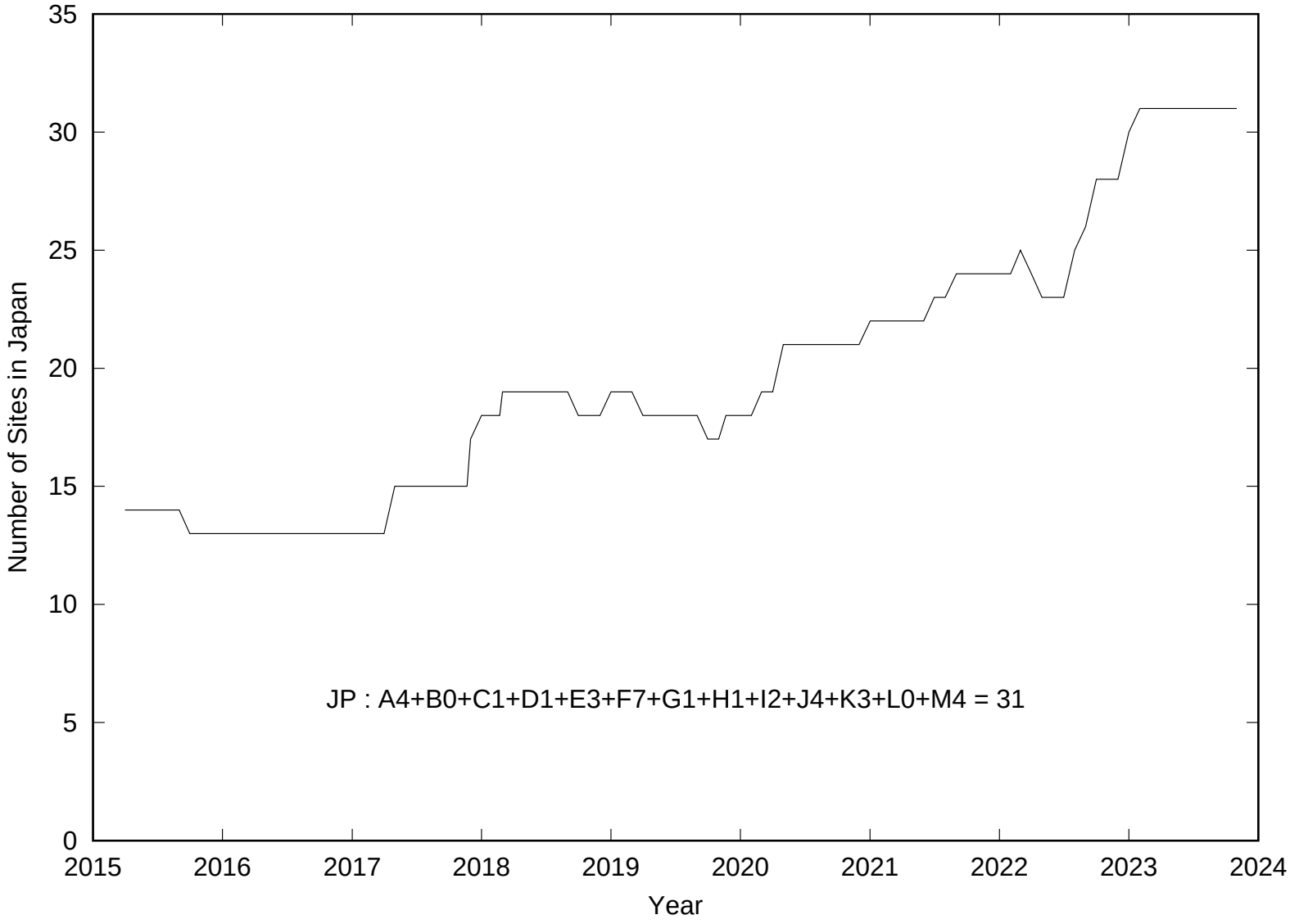
# Root DNS サーバ：国別の推移





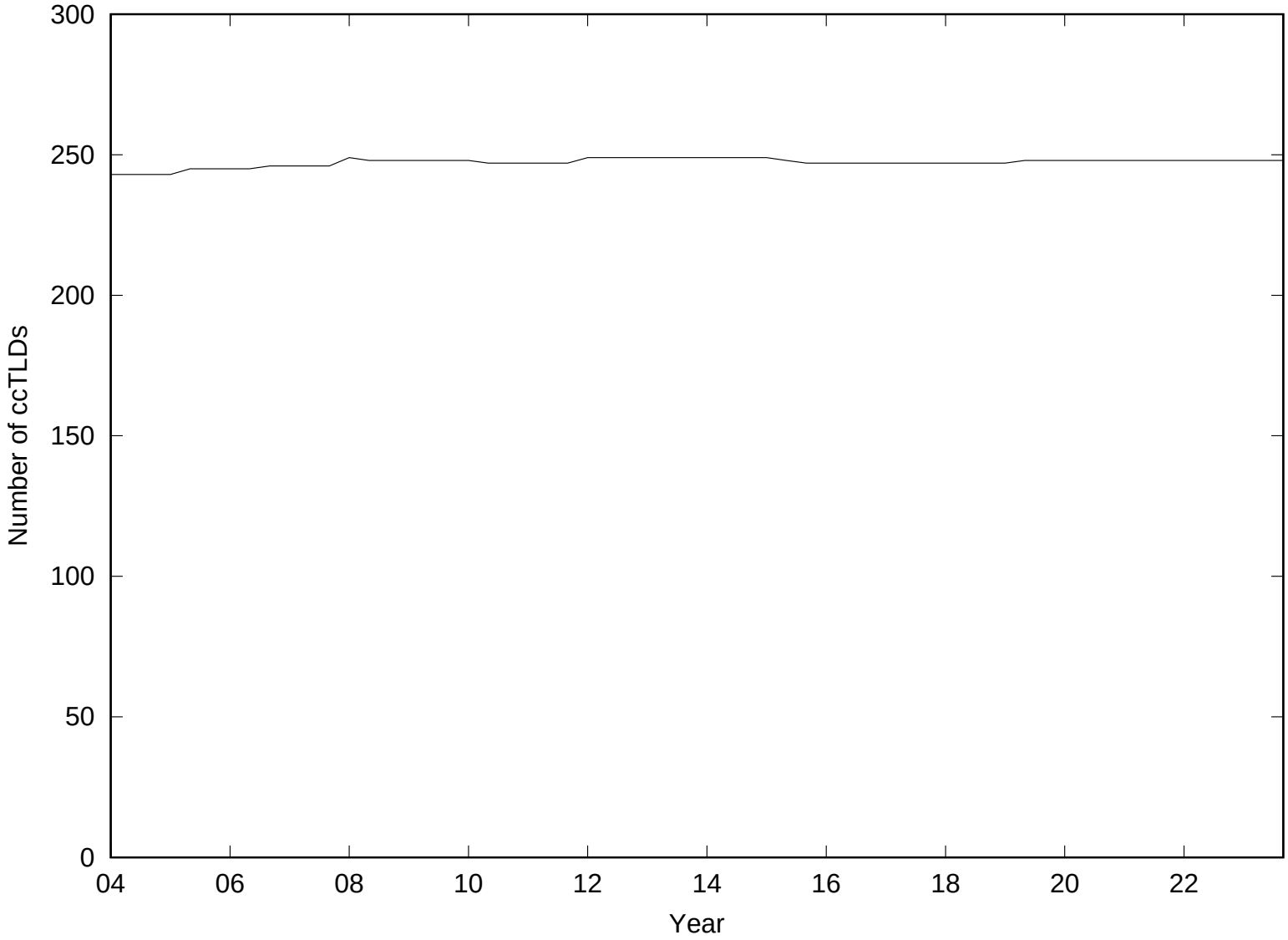
# Root DNS サーバ：わが国の推移





# Root Zone : ccTLD 数の推移

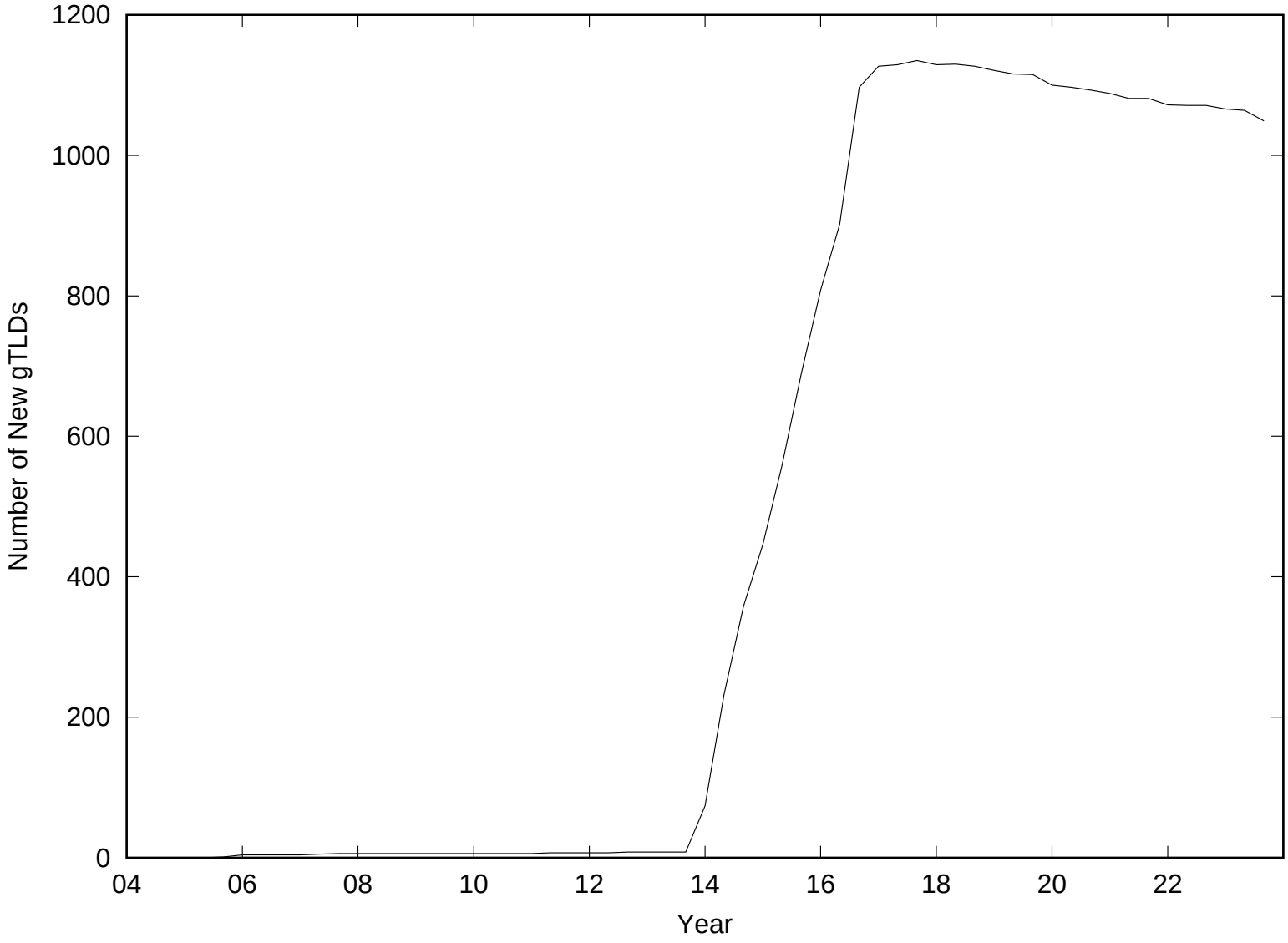





データは DNS-OARC, Yeti による

# Root Zone : 新 gTLD 数の推移

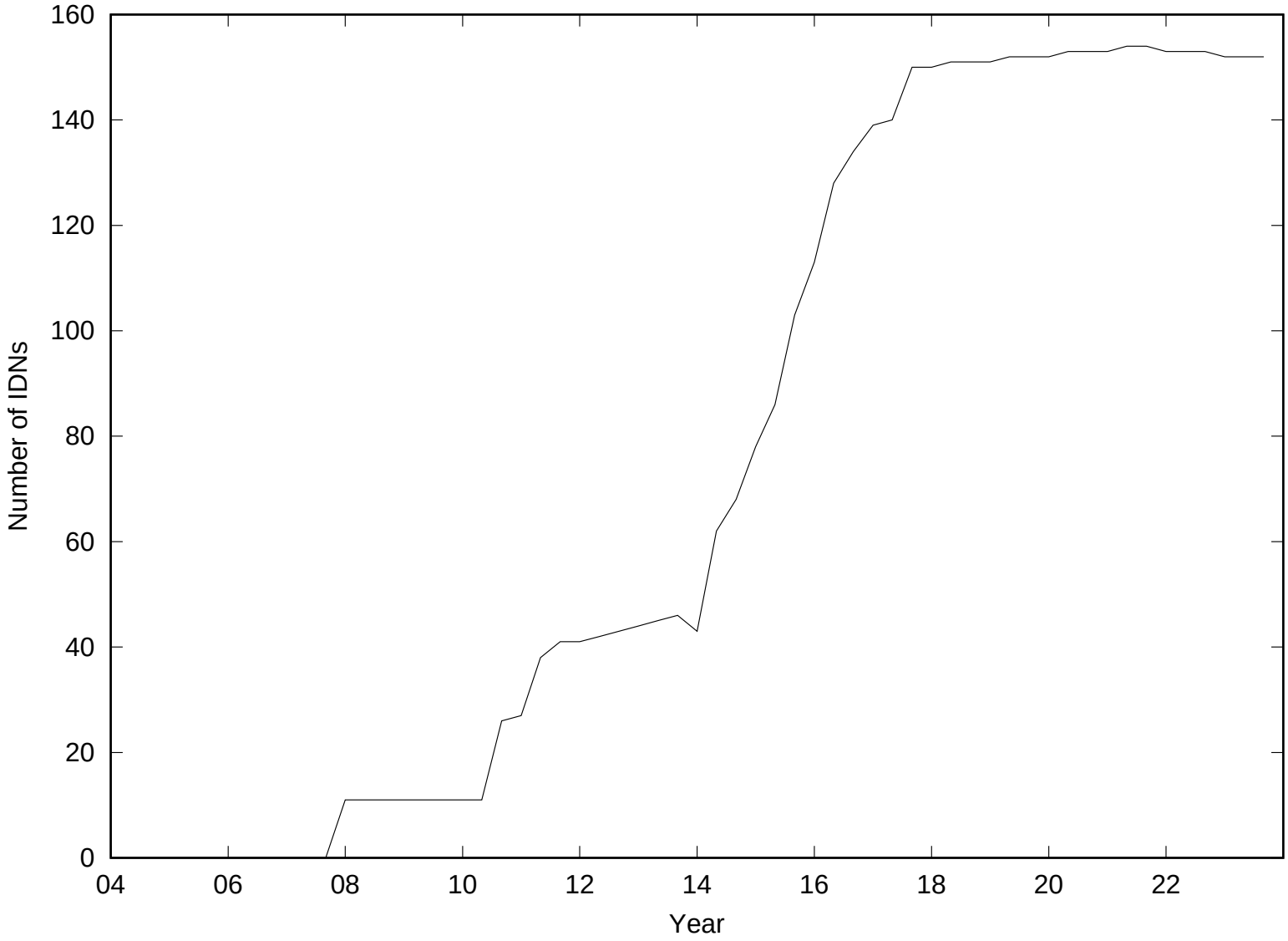





データは DNS-OARC, Yeti による

# Root Zone : IDN-TLD 数の推移






データは DNS-OARC, Yeti による