JP DNS Update

2014年11月20日

Internet Week 2014 DNS DAY

株式会社日本レジストリサービス（JPRS）

水野 貴史

目次

- JP DNSとは
- 統計情報
  - JPドメイン名登録数
  - JP DNS へのクエリ数 — 最近の傾向
- トピックス
  - JPゾーンとDNS.JPゾーンのNS親子同居の分離
  - JPゾーンの empty non-terminal への TXT RR 追加

JP DNSとは

JP DNSとは

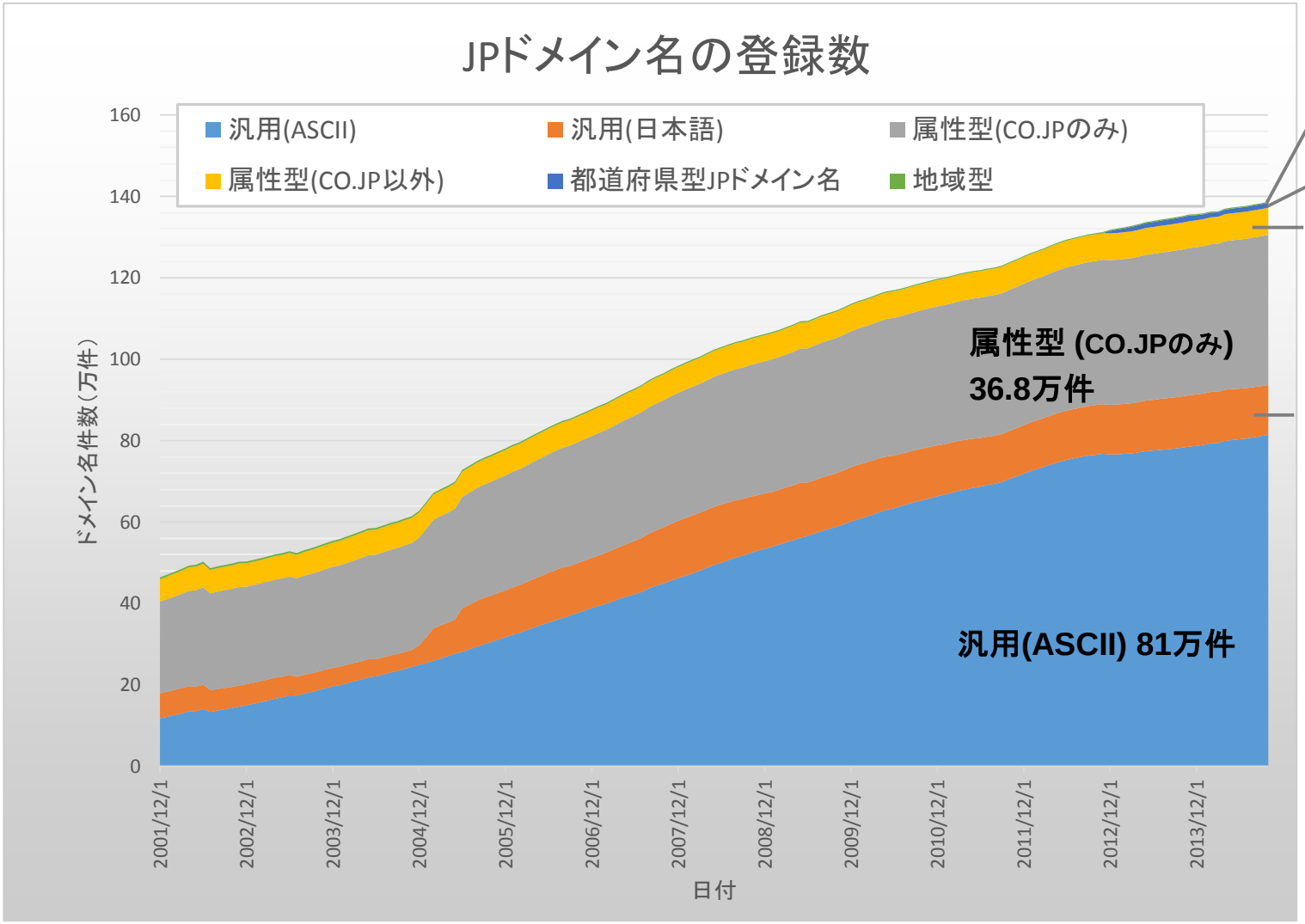
- JPゾーンを管理する権威DNSサーバー
  - JPRS が登録管理しているJPゾーンを提供
  - JPNIC が割り振りを管理しているIPアドレスブロックのうち、一部の逆引きゾーンも提供（c.dns.jp を除く）
- JP DNS サーバーの構成

サーバ	運用組織	ネットワーク	管理ゾーン
a.dns.jp	JPRS	IPv4/IPv6 + Anycast	JP, 逆引き
b.dns.jp	JPNIC	IPv4/IPv6	JP, 逆引き
c.dns.jp	JPRS	IPv4/IPv6 + Anycast	JP
d.dns.jp	IIJ	IPv4/IPv6 + Anycast	JP, 逆引き
d.dns.jp	WIDE Project	IPv4/IPv6 + Anycast	JP, 逆引き
f.dns.jp	NII	IPv4/IPv6	JP, 逆引き
g.dns.jp	JPRS	IPv4	JP, 逆引き

統計情報

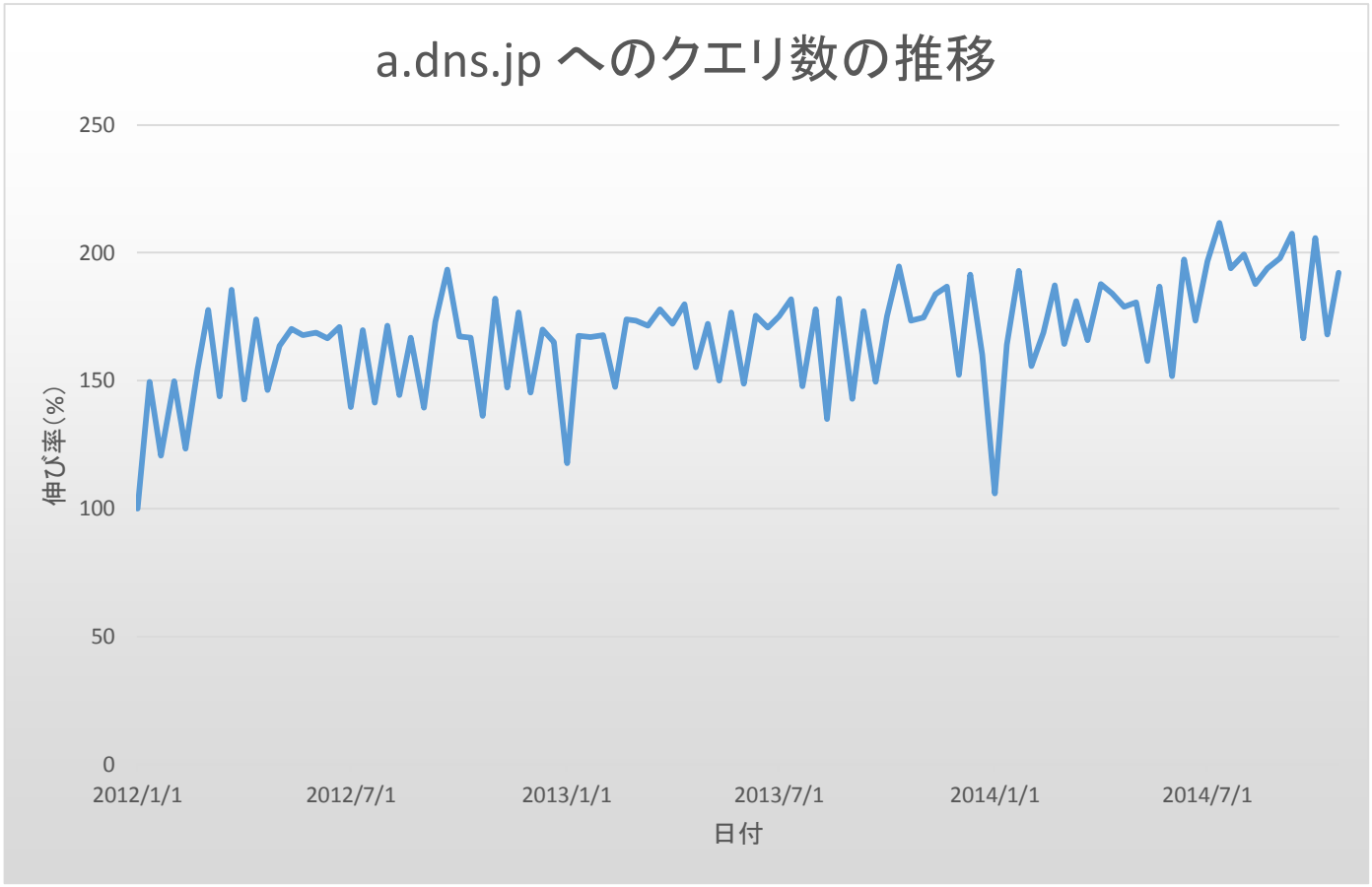
統計情報　JPドメイン名の登録数

2014年11月1日現在：約138万件

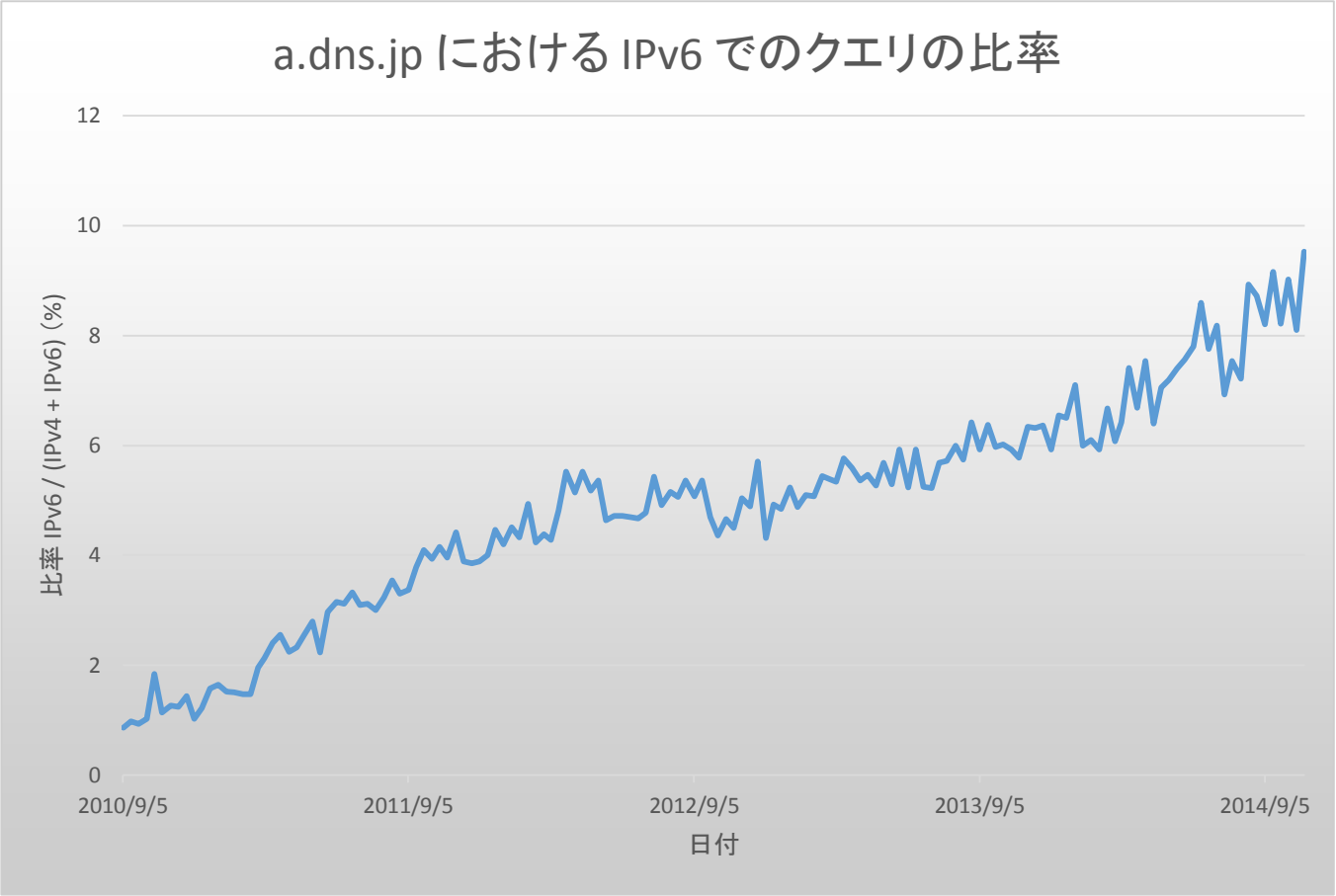


統計情報　a.dns.jp のクエリ数

a.dns.jp へのクエリ数の推移（2012年1月1日を100%とする）



統計情報　IPv6でのクエリの比率



- 2010年の後半から、IPv6 でのクエリの比率が増加
- 2014年11月現在、IPv6 でのクエリの比率は全体の9%程度
  - 前年比3%程度増加

トピック1

JPゾーンとDNS.JPゾーンのNS親子同居の分離

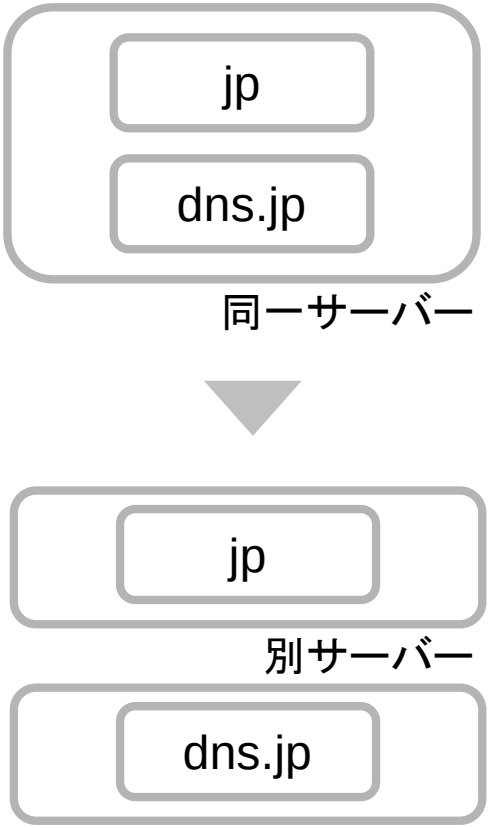
JPゾーンとDNS.JPゾーンのNS親子同居の分離

目的

キャッシュポイズニング攻撃成功時の被害を軽減するため

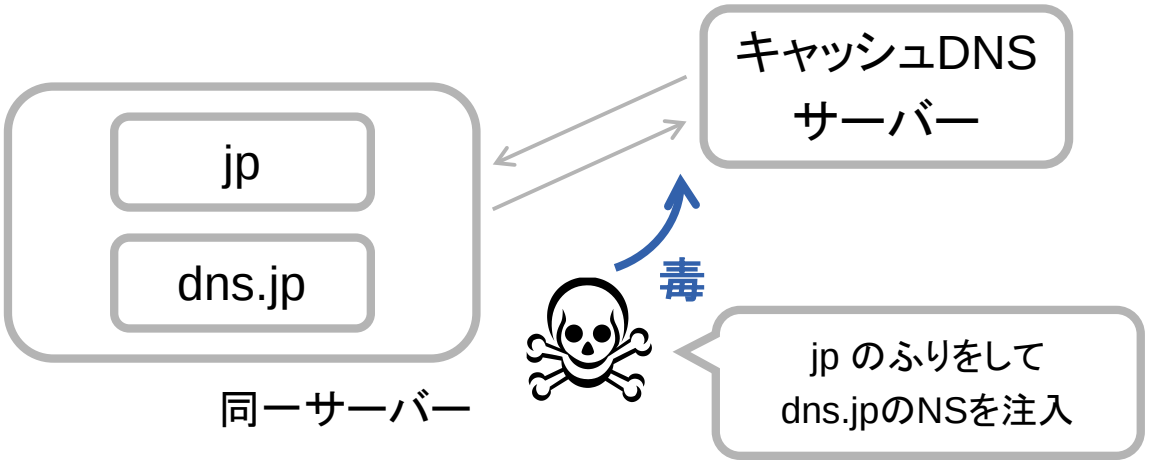
- 親子同居とは？
  - 親ゾーンと子ゾーンが、同一のサーバーに収容されている状況
  - 先祖と子孫†の場合もあり
- JRPSでの対応
  - 6月9日～6月24日にかけて、jp と dns.jp の親子同居の分離を実施

  → dns.jp ゾーンを別サーバーに分離



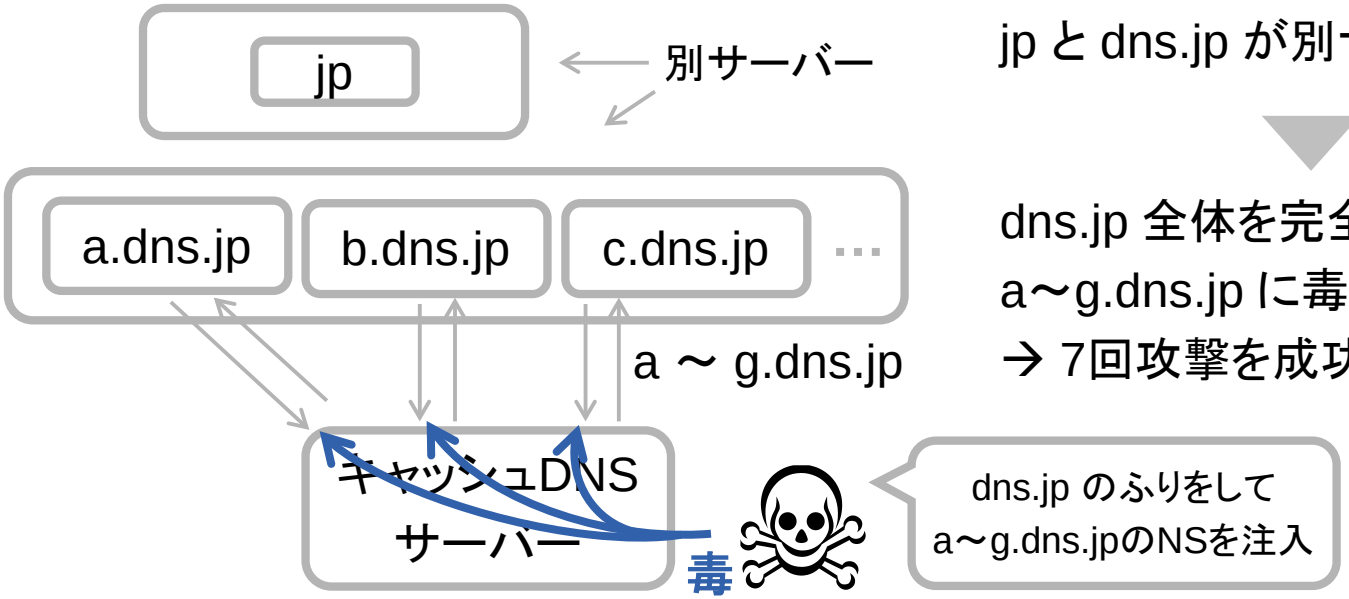
† あるゾーンからみて、子ゾーンのさらに子ゾーン以下は子孫。先祖は、あるゾーンからみて、親ゾーンの親ゾーン以上のことを指す

分離前と分離後



jp と dns.jp が同居状態

1回の攻撃成功で dns.jp を
乗っ取り可能（jp 全体）。



jp と dns.jp が別サーバーに収容

dns.jp 全体を完全に乗っ取るには、
a～g.dns.jp に毒入れする必要あり
→ 7回攻撃を成功させる必要がある

注意点

- この対策は、キャッシュポイズニング攻撃成功時の**被害を軽減**するためのもの

- **キャッシュポイズニングそのものの成功率を下げるものではない**

  →そのための対策は別途必要

  （ソースポートランダマイゼーションなど）

トピック2

JPゾーンのempty non-terminalへのTXT RR追加

empty non-terminal へのTXT RR追加

目的

DNSSEC検証において、empty non-terminal を確実に保護対象とするため

（攻撃が成功した際に気づけるようにするため）

→ DNSSEC 検証をしていない場合、変化はなし

- empty non-terminal とは？

  次のような状況のドメイン名

  – リソースレコード　：一つも設定されていない

  – サブドメイン名　　：存在する

  → co.jp や saitama.jp 、そのほか大学などのサブドメインの多いドメイン名にもみられる

TXT RR を追加する必要があるケース

- NSEC3 + Opt-Out で DNSSEC 署名を行っている場合†
  - **署名済のサブドメイン名が一つも存在しない**場合、NSEC3 + Opt-Out の仕様では empty non-terminal は必ずしも保護されない
    （キャッシュポイズニングされていても気づけない）

JP において、empty non-terminal でなくすための対策を実施（2014/3/16)

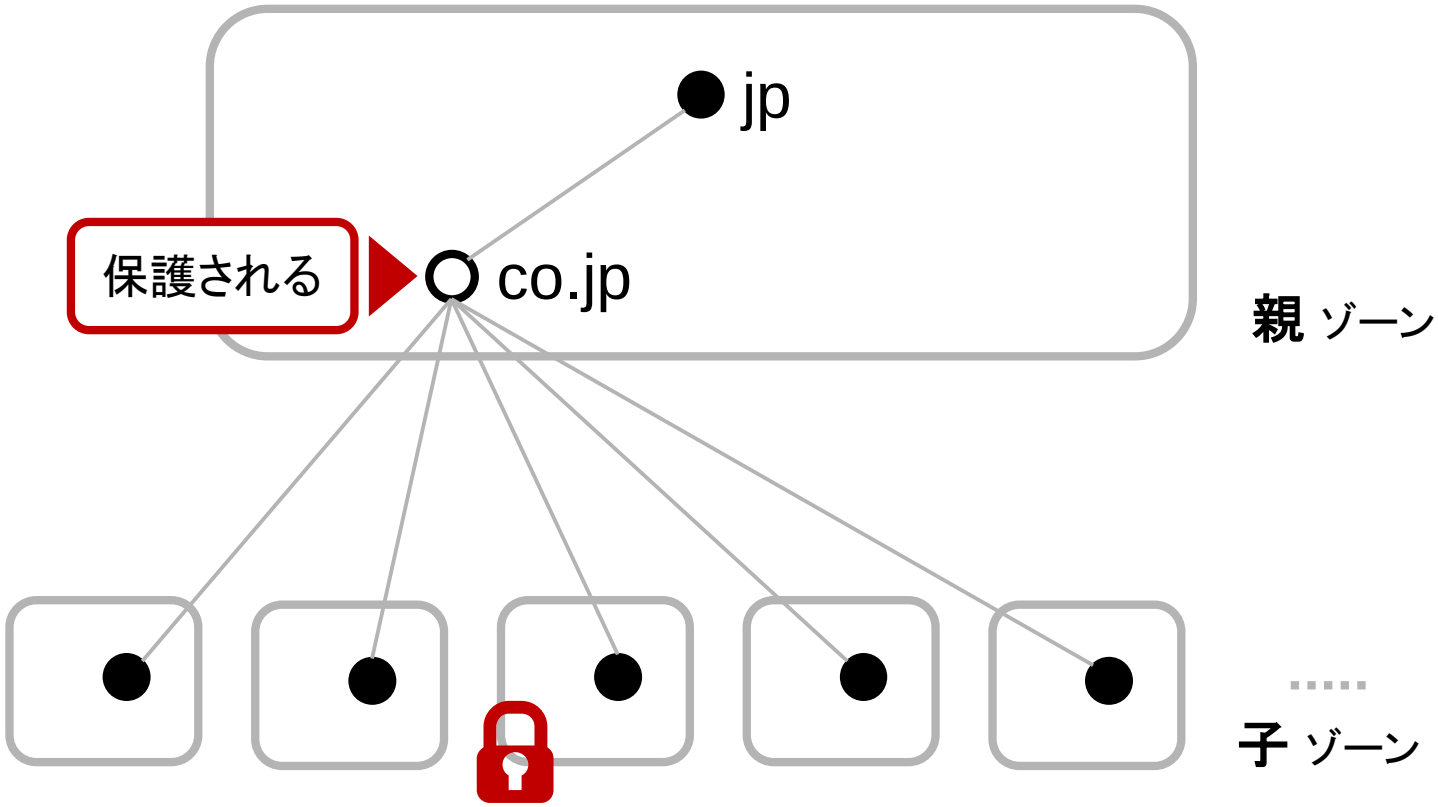
実施

TXT RR の追加

対応の必要がないものに対しても一律に追加する形で対応した

† 通常は TLD などに限定

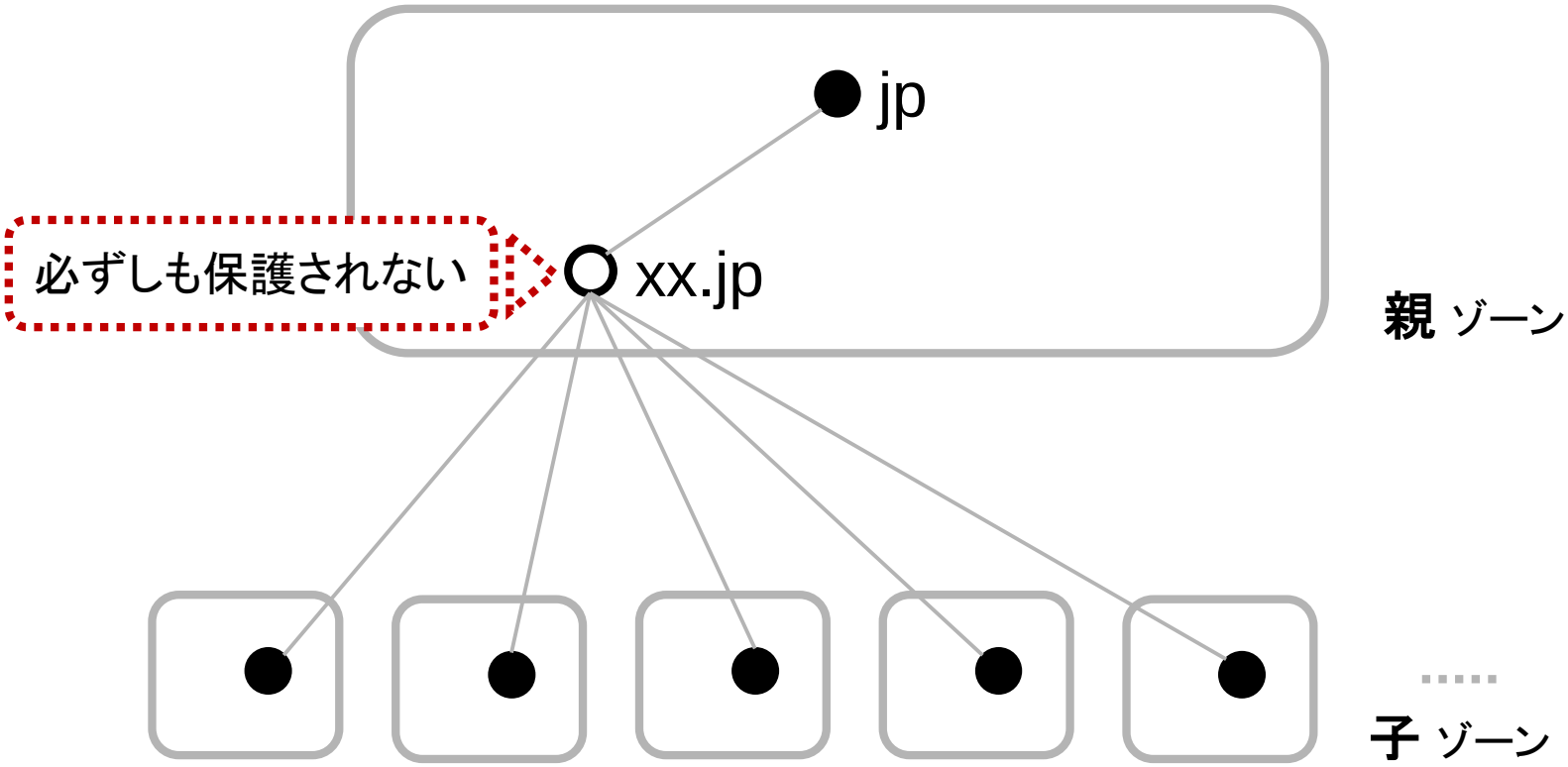
DNSSEC で保護されるケース



子ドメイン名が **1つでも** DNSSEC 署名
されていれば、その親ドメイン名も保護される†

† RFC 5155 に従った挙動

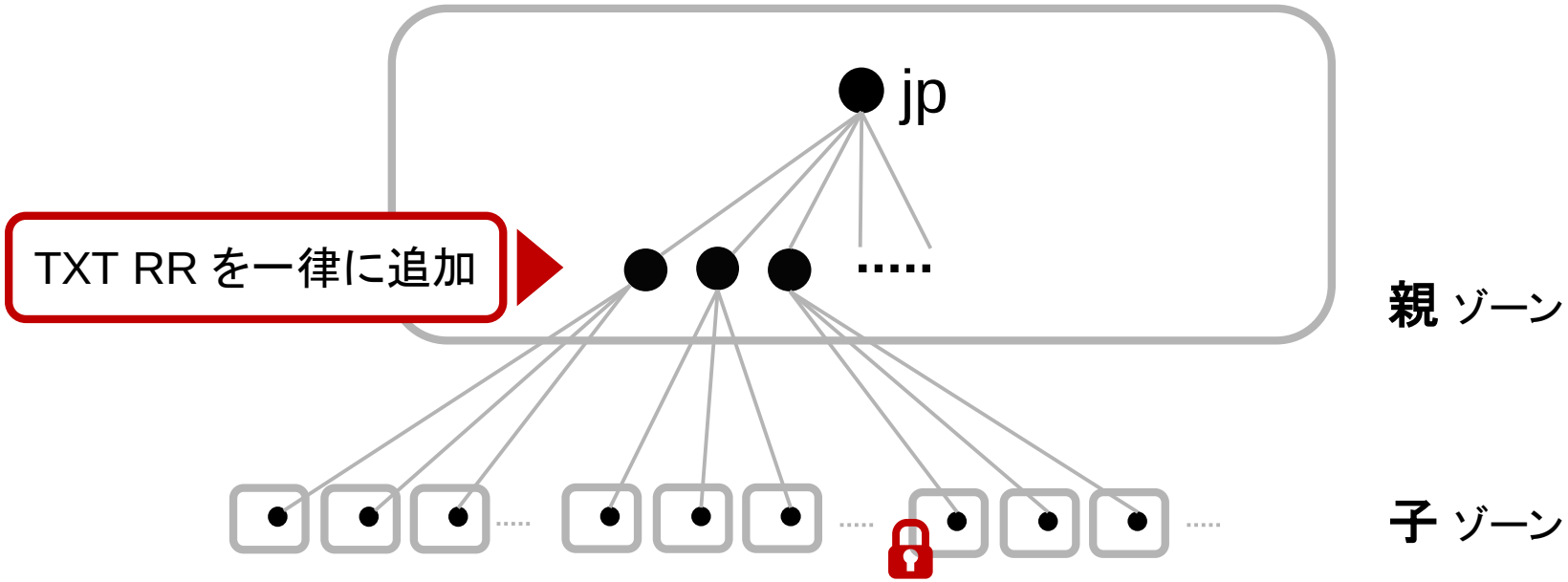
DNSSEC で保護されない場合があるケース



子が **1つも** DNSSEC 署名されていないと、
その親は保護されなくてもよい

署名
ゾーン
empty non-teminal
RR のある名前

JPRSでの対応



署名された子がいるかいないかに関わらず、
TXT RR を追加

→ empty non-terminal であったものが、
empty non-terminal ではなくなった†

署名
ゾーン
empty non-teminal
RR のある名前

† co.jp などは署名済みの子ゾーンがあったため、もともと保護された状態であった

導入**前** と 導入**後** の変化

- 導入**前**
  - JPゾーンに empty non-terminal が存在した
    - JPでは、署名された子ゾーンを持たないドメイン名が保護されていなかった
    - 署名された子ゾーンを持つドメイン名は、保護されていた
- 導入**後**
  - empty non-terminal が存在しない
    - 署名された子ゾーンを持たないドメイン名が確実に保護されるように
    - 署名された子ゾーンを持つドメイン名は、変化なし
      - ただし、一律追加を行ったため、署名をされた子ゾーンを持つゾーン（例えば co.jp）にも、TXT RR が追加された

まとめ

- JP DNS のクエリ数の変化
  - クエリ数の変化は現在も増加傾向か
  - IPv6 のリクエスト数が2010年の後半から増加
- JPゾーンとDNS.JPゾーンのNS親子同居の分離
  - 分離の結果、キャッシュポイズニング攻撃によるリスクが1/7 程度に減少
- JPゾーンの empty non-terminal へのTXT RR追加
  - DNSSEC 検証において、empty non-terminal を確実に保護対象とするため

Q and A