JP DNS Update

2013年11月

Internet Week 2013 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
  - DSレコードのTTL短縮
  - DNS RRL(Response Rate Limiting)の導入

JP DNSとは

JP DNSとは

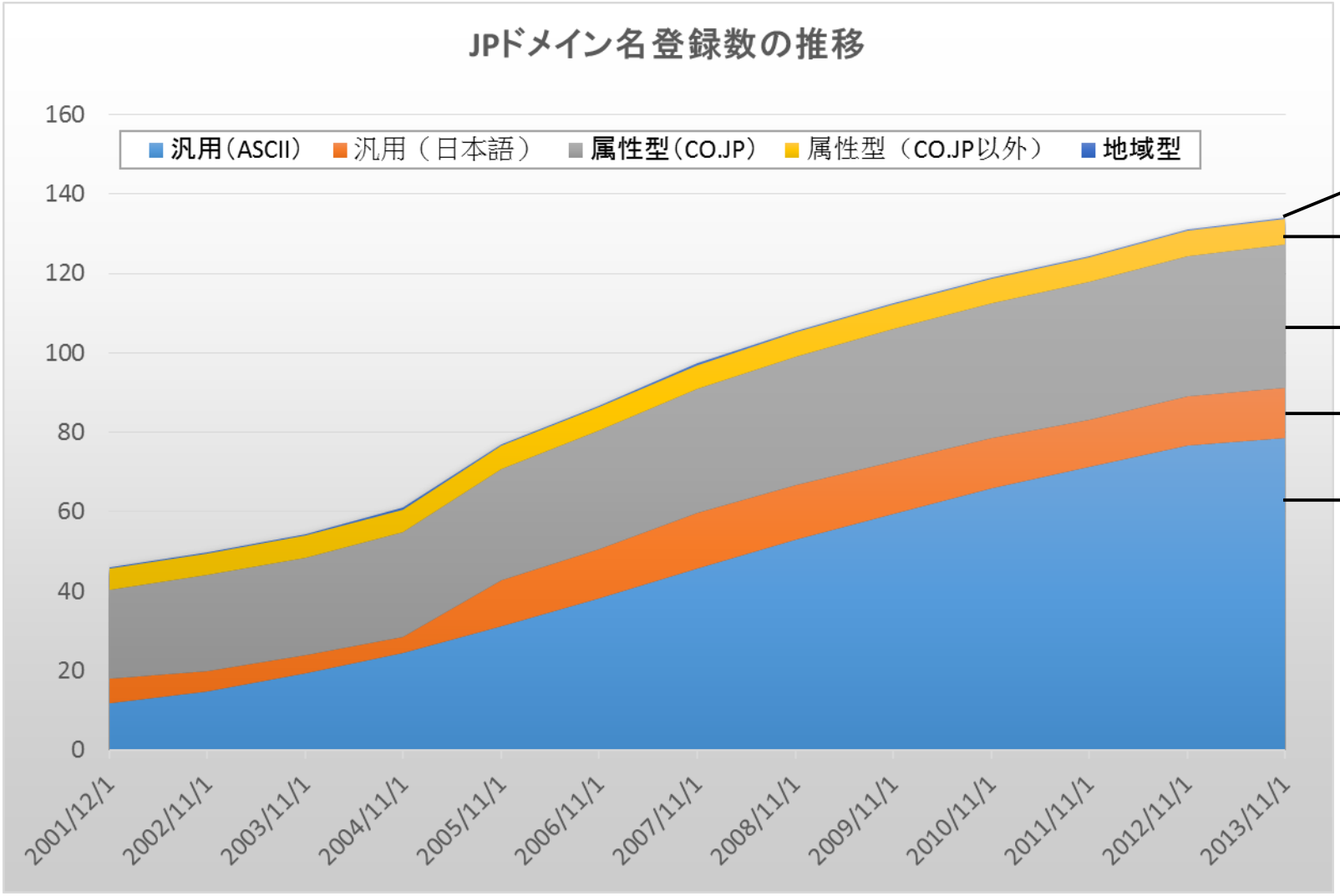
- JPゾーンを管理する権威DNSサーバー
  - JPRSが登録管理しているJPゾーンを提供
  - JPNICが割り振りを管理しているIPアドレスブロックのうち、一部の逆引きゾーンも提供（C.DNS.JPを除く）
- JP DNSサーバの構成

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
E.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

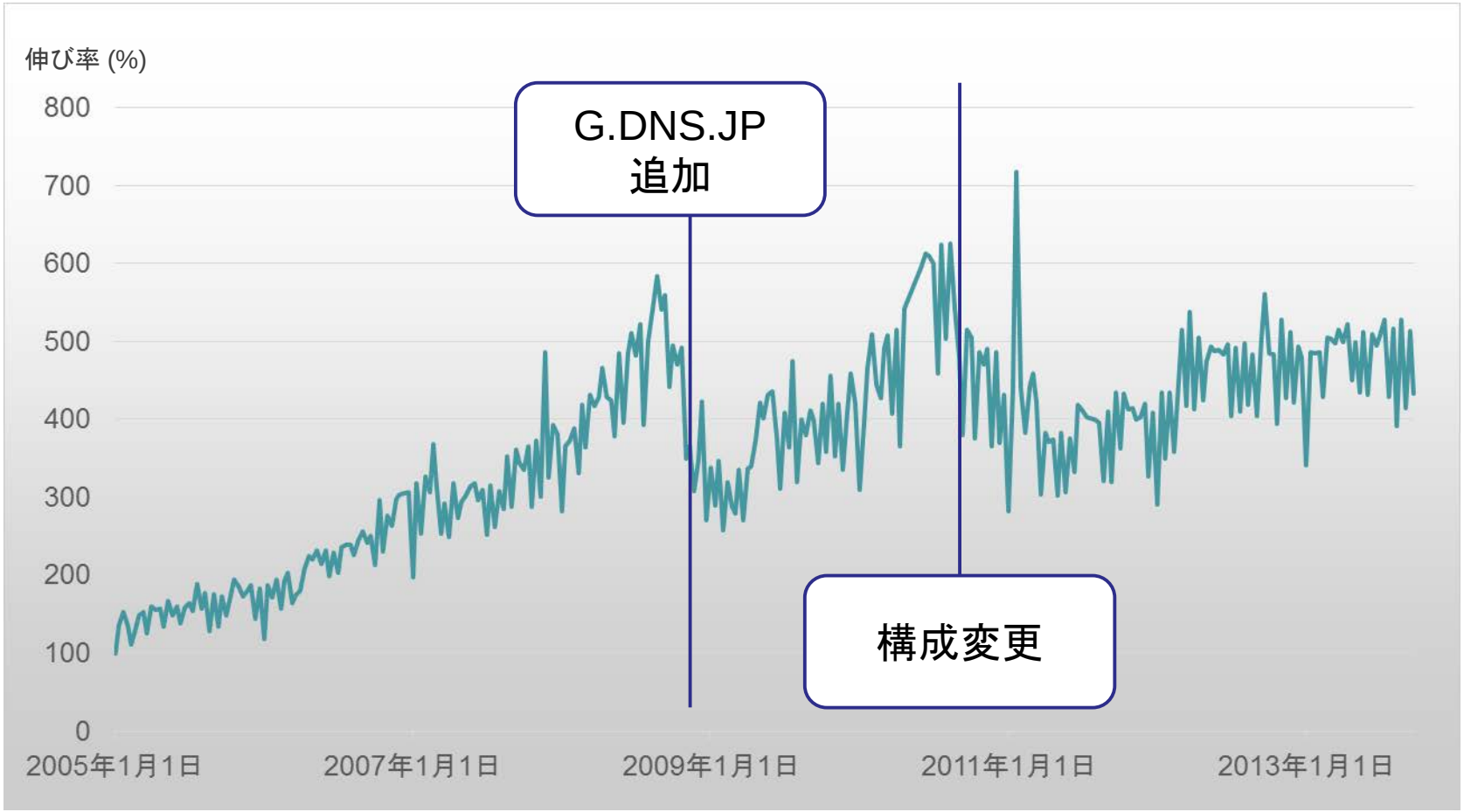
統計情報　JPドメイン名の登録数

2013年11月1日現在：約135万件

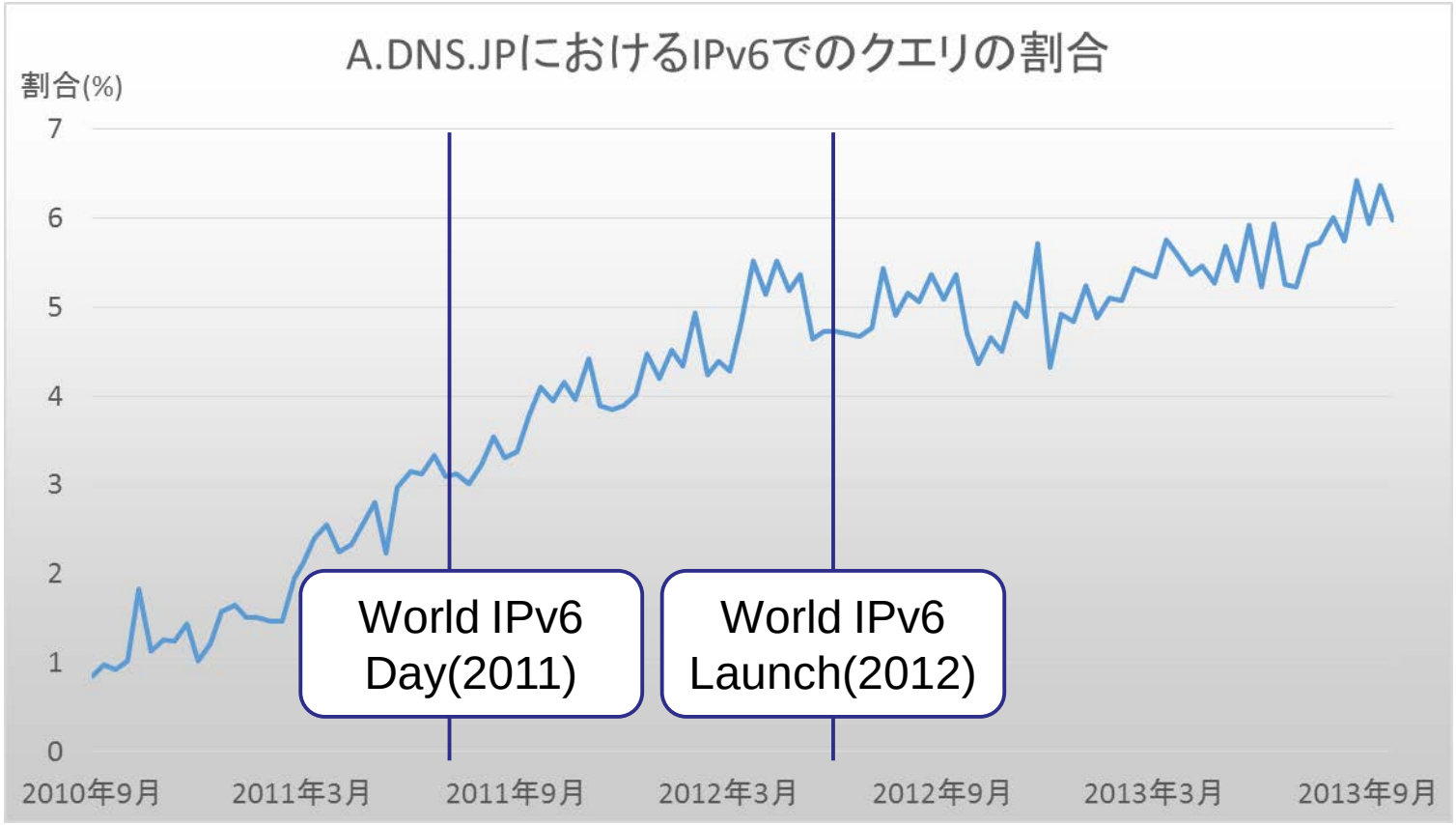


統計情報　A.DNS.JP のクエリ数

A.DNS.JPへのクエリ数の推移（2005年1月1日を100%とする）



統計情報　IPv6でのクエリの割合



- 2010年の後半から、IPv6でのクエリの割合が増加
- 2013年11月現在、IPv6でのクエリの割合は6%前後
  - 前年比1%程度増加

トピック1

DSレコードのTTL短縮

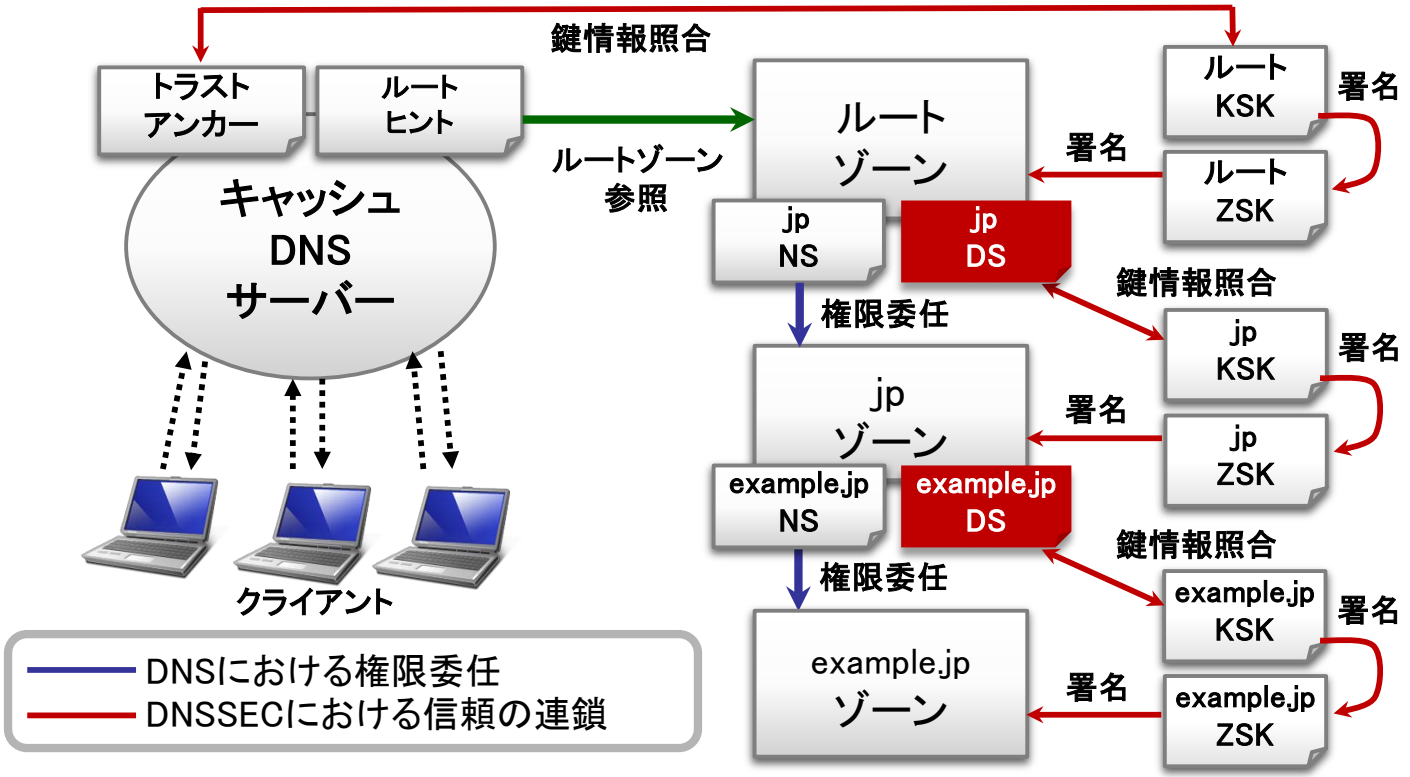
DSレコードのTTL短縮

- 11月17日 に、JP DNSに設定されるDSレコードのTTL短縮を実施

- ここからの内容
  - DSレコードの概要と設定変更の背景
  - 適切なTTL値の考察

DSレコードとは

- 子が親（レジストリ）に登録し、DNSSECの信頼の連鎖を構築
- 子ゾーンの鍵署名鍵（KSK）から生成、KSKと暗号論的に等価



設定変更の背景

- DSとDNSKEY(KSK)に不整合が生じると……

→DNSSEC検証を実施している場合、子ゾーン全体の名前解決ができなくなる

  - 事例:
    - 2010年9月　mozilla.orgが、自ゾーンのDNSSEC署名よりも先にDS登録
    - 2013年6月　bizにおける作業ミス
    - 2013年8月　govにおける作業ミス

- DSとDNSKEY(KSK)の間に不整合が発生した場合、障害復旧にはかなりの時間を要する場合がある
  - 「署名の有効期間満了」と異なる点

障害復旧に関係する時間 – DSを再設定する必要がある場合

- DS更新リクエストから実際の切り替えまでの時間
  - 利用者がレジストラにDS更新を依頼
  - レジストラがレジストリにDS更新を取り次ぎ
  - レジストリがDSレコードを切り替え
- DSレコードに設定されるTTL値
  - キャッシュされた旧DSレコードの残存時間

- 署名の有効期間満了は自らの再署名で即座に復旧
- レジストリやレジストラの対応不要

一般的に、「DSレコードに設定されるTTL値」の方が長い

DSレコードの適切なTTL値はいくつか？

DSレコードの適切なTTL値の考察(1)

- 類似性がある2つの作用
  - 不整合が発生した場合のDSレコードの作用
  - DNSデータの新規登録前にそのデータを検索してしまった場合のネガティブキャッシュの作用

- 旧DSレコード
- 名前が存在しなかったこと（ネガティブアンサー）

検索結果がキャッシュされている間、
名前解決ができない状態が継続する

ネガティブキャッシュの一般的なTTL値を
参考にし、DSレコードのTTL値を考察

DSレコードの適切なTTL値の考察(2)

- ネガティブキャッシュの一般的なTTL値の範囲からの選択
  - 3600(1時間)～10800(3時間)†
- JP DNSサーバにおける問い合わせ状況を分析
  - 障害復旧時間・待ち時間の効果的な短縮
  - 将来、DSレコードの数やバリデータの数が増加した場合にも、JP DNSの運用に大きな影響を及ぼさない

この2点を両立する値として7200(2時間)を選択

† RFC2308の5章より

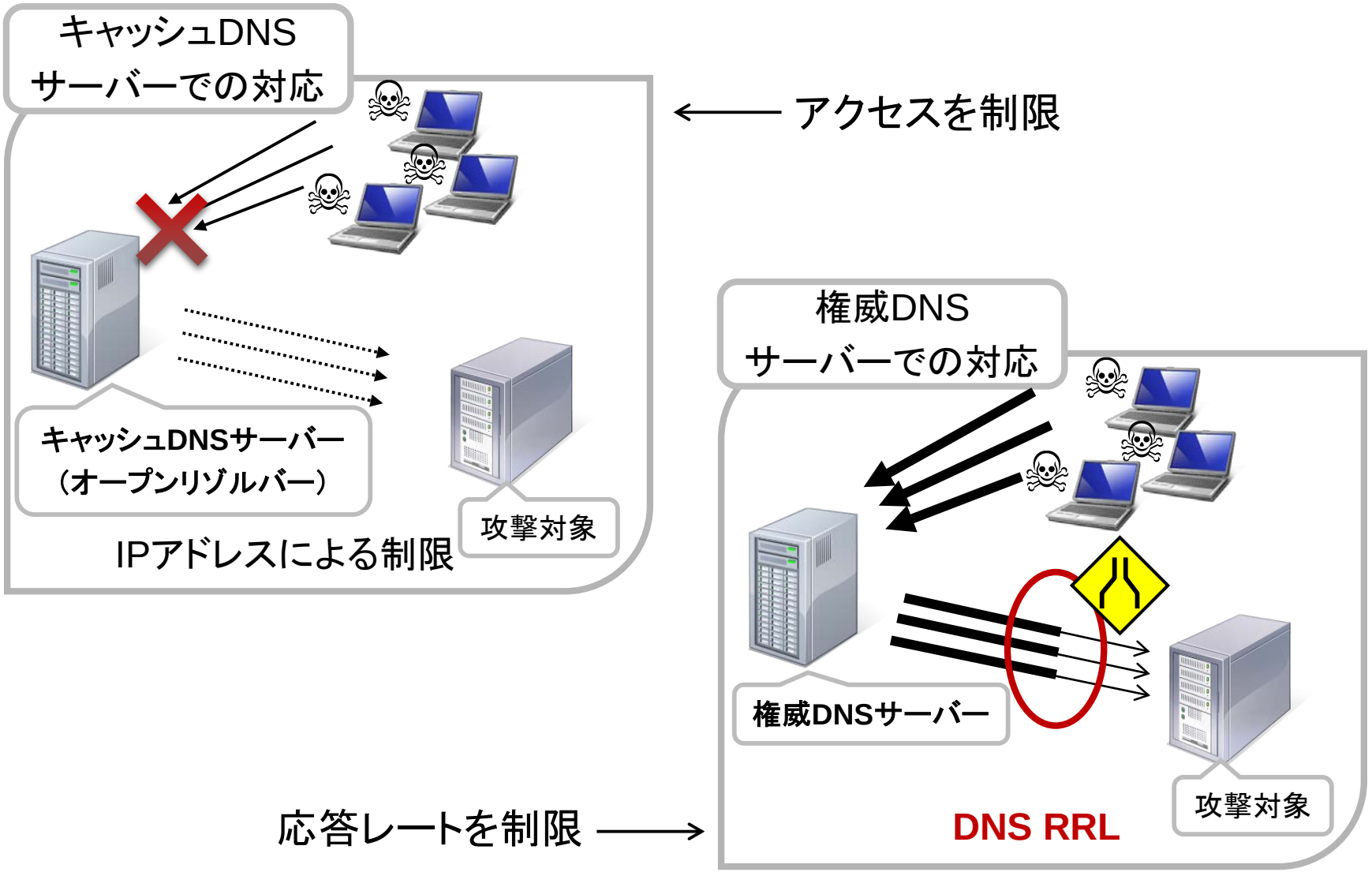
トピック2

DNS RRL(Response Rate Limiting)の導入

DNS RRL(Response Rate Limiting)

- DNS RRLとは？
  - **DNSリフレクター攻撃に対する対策**の一つ
  - 主に権威DNSサーバーへの導入を想定
  - DNSサーバへの問い合わせ……
    ではなく、DNSサーバーからの**応答**を制限する技術
  - BIND 9.9.4 で標準実装
  - NSD 3.2.15以降、Knot DNS 1.2.0-rc3以降で実装

DNS リフレクター攻撃への対応概念図



RRLの特徴（1）

- **DNSがもつ特性**に着目
  - 権威DNSサーバーのサービス提供先は、
    主にキャッシュDNSサーバーである

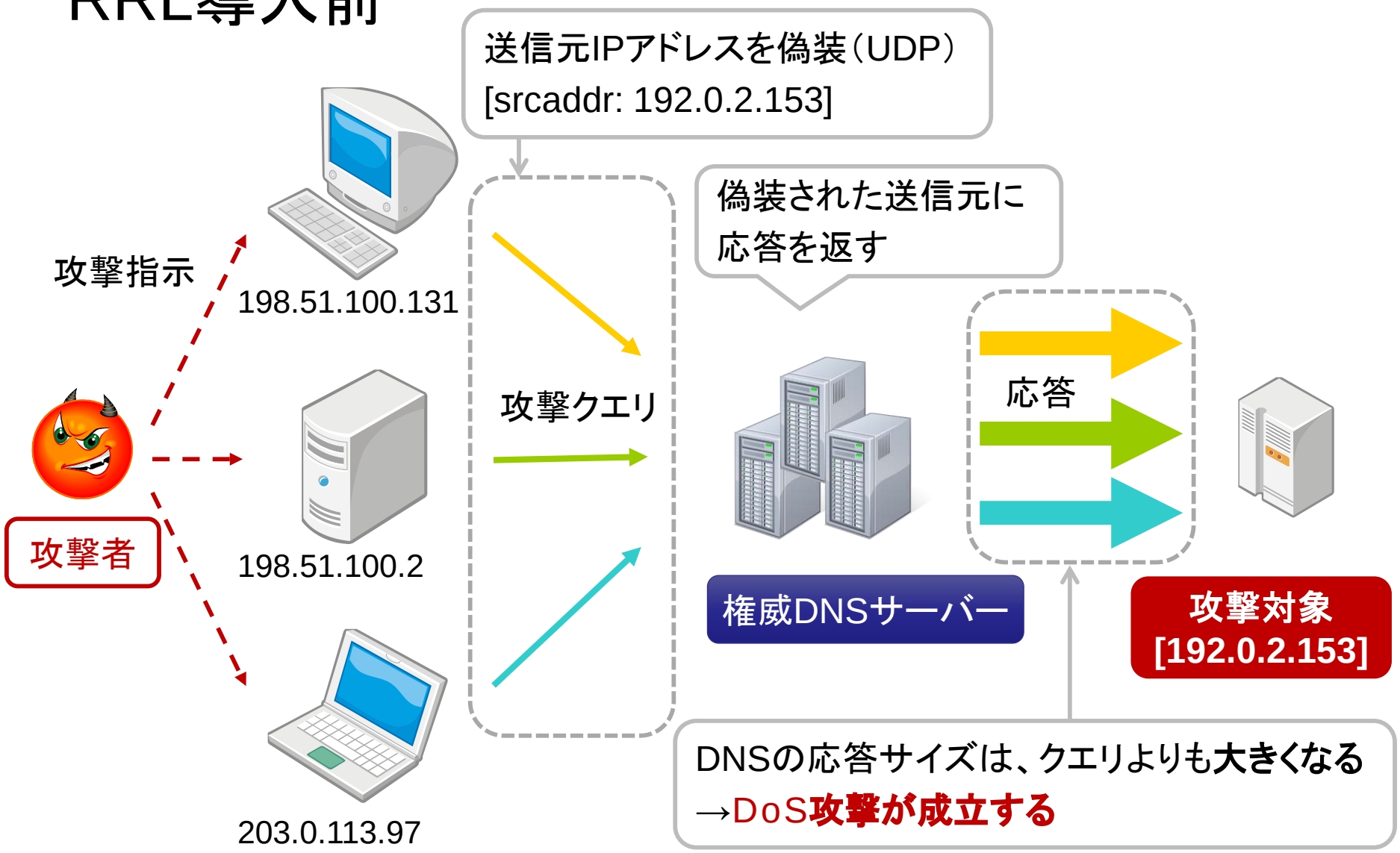
    →DNSプロトコルに従った動作を期待できる

    →キャッシュDNSサーバーはキャッシュを行うため、
    「同じ名前・タイプのクエリ」を高頻度で送ることは考えにくい

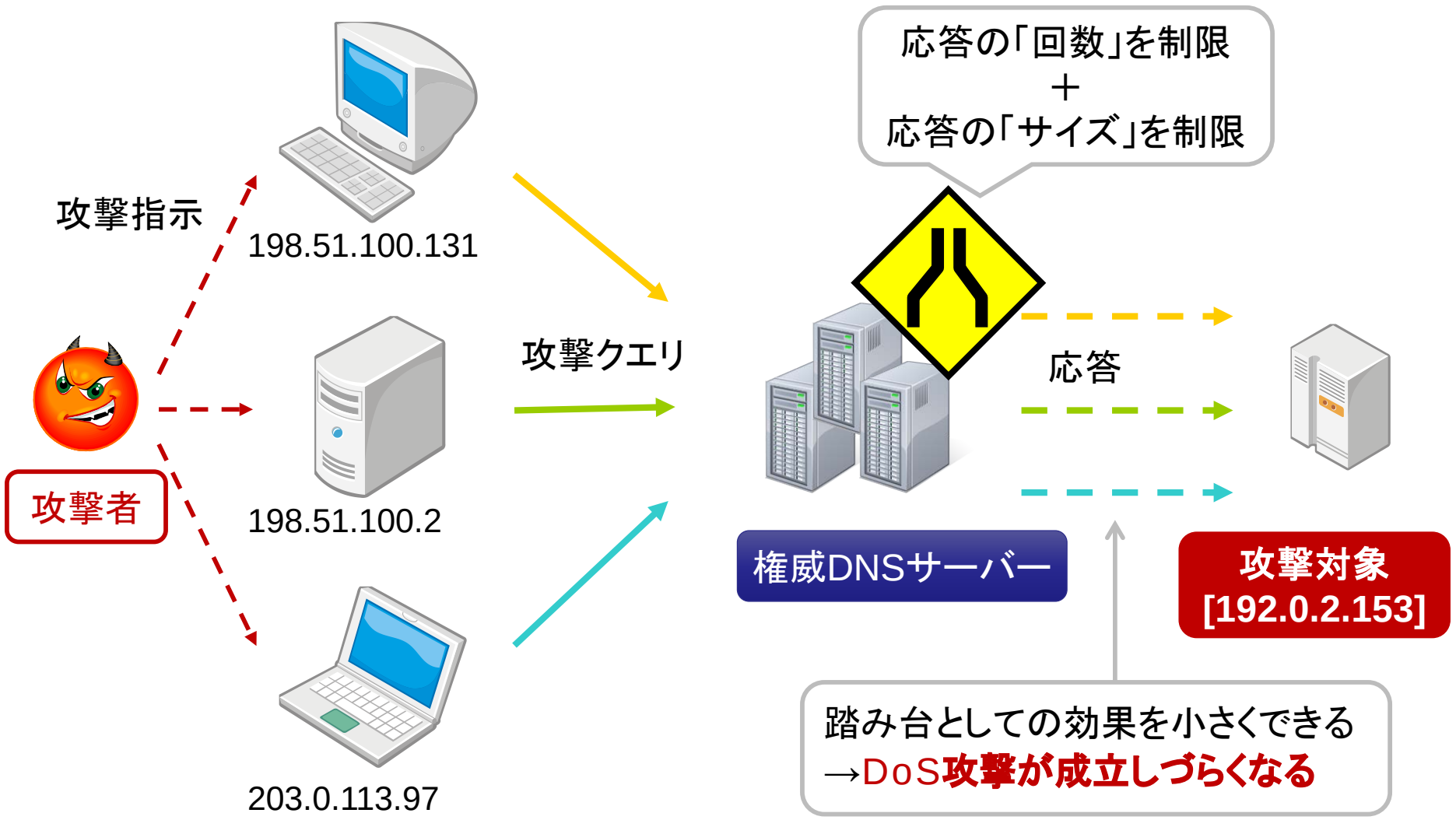
RRLの特徴(2)

- 単位時間あたりの応答の「**回数**」を制限
  - 「送信元IPアドレス(のネットワーク部)」「クエリの名前」「クエリのタイプ」「応答コード」に着目
  - 上記が同じクエリに対する応答を制限
  - 対象はUDPによるクエリのみ
- 1回の応答の「**サイズ**」を制限
  - 一部については、応答を返さない代わりにサイズを制限して応答
  - 応答のTruncated Response(TC)ビットをオンにして、クライアント側でTCPで再試行させる

RRL導入前



RRL導入後



JP DNSへの導入

- DNSリフレクター攻撃に利用できるのは、キャッシュDNSサーバーだけではない
  - 権威DNSサーバーへの対策も必要
- 2013年11月現在、導入作業中
  - 通常のキャッシュDNSサーバーからのクエリには影響が無いよう、調査を行いパラメータを決定

2014年1月に導入完了予定

Q and A