明日のカタチ

～なぜ、普及してしかるべき技術が普及しないのか？ ～ DNSSEC編

2021年11月24日

株式会社インターネットイニシアティブ
DNSOPS.JP
其田 学

- **DNSSECとは**
- **これまでの普及の歩み**
- **現在の状況**

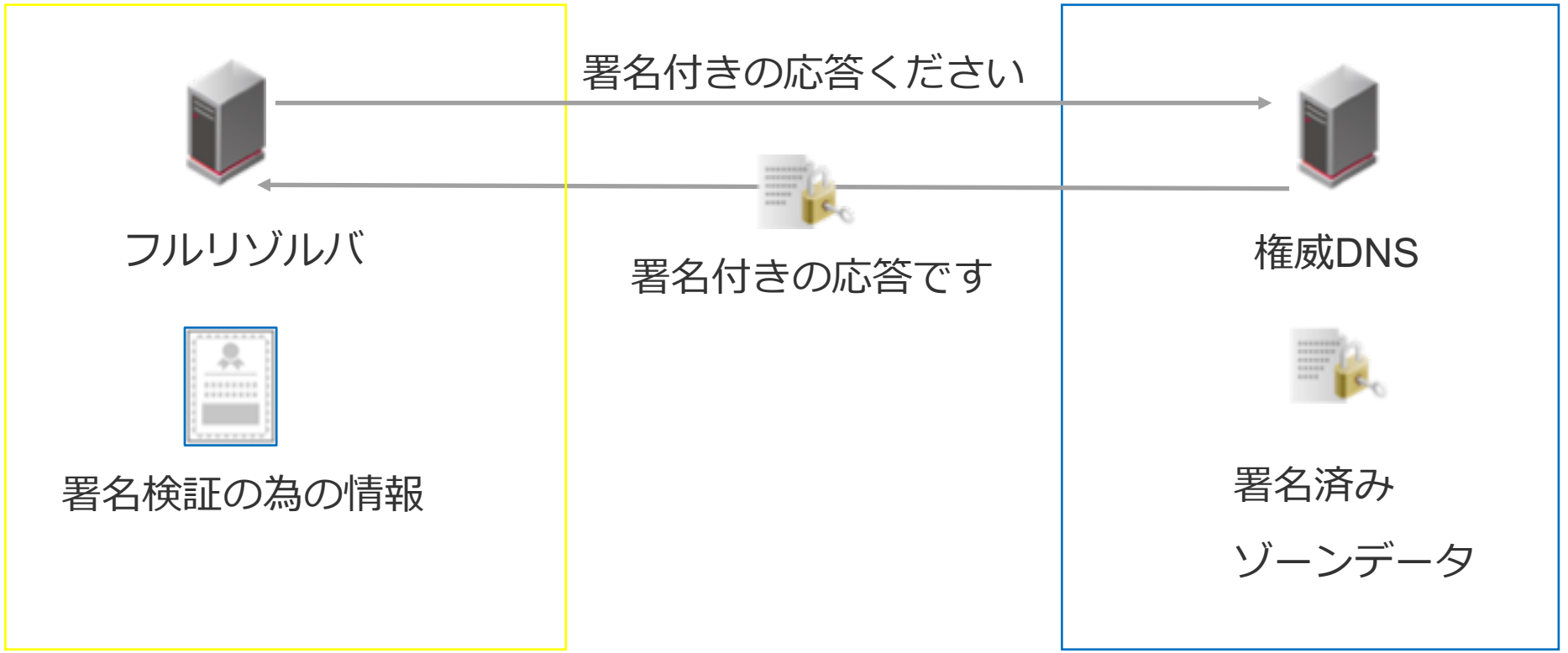
DNSSECとは

DNSメッセージが正しいデータか検証できるようにする仕組み

偽の応答をキャッシュしてしまうキャッシュポイズニング（通称：毒入れ）が成功すると、
フルリゾルバの利用者に大きな影響を与えるため開発されたプロトコル。

電子署名技術をつかって、ゾーンデータを電子署名し、DNS応答に電子署名を付与（権威DNS側）

受信側（通常はフルリゾルバ）で、電子署名を検証することで、応答が改竄されていないか検証する



DNSは平文のTCP/UDPを使うので、中間者攻撃に弱い

- 不特定のサーバー間の中間者攻撃を防ぐ機能がない
    - 特定のサーバ間ならTSIGってのがありますが。。全世界のサーバと設定するのは不可能
- 中間者攻撃日常茶飯である
    - スノーデン事件

改竄されていることに気づくことができない

- フルリゾルバの運用者はどのデータが正しいデータかわからない

DNS自体が、別のプロトコルの信頼の連鎖として使われている

- DNSSECが導入されており、レコードが改竄されてないことを前提で、
  様々なプロトコルがDNSにいろんなデータを載せ始めた。
- TLSでのdns-01認証や、メールベースでの認証などでDNSが使われている。
    - CTLog監視してますか？

これまでの普及の歩み

2009 - 2012

2009/11/24	**DNSSECジャパン発足**
2010/07/16	**ルートゾーン署名開始**
	フルリゾルバでの署名検証ができるようになった
2010/07/24	DNSSEC 2010 サマーフォーラム
	全３回のDNSSEC.JPの活動発表の初回
2010/12/xx	JPゾーンが署名検証可能になった
2011/01/16	**JPドメイン名サービスでDNSSEC導入開始**
	JPのレジストラはJPドメイン名の署名検証情報の登録ができるようになった
2011/04/20	DNSSEC 2011スプリングフォーラム
2012/04/25	DNSSEC 2012スプリングフォーラム
	DNSSECジャパン活動終了

2012 – 現在

2015/01/09　JPNICが管理している逆引きゾーンへのDNSSEC導入開始

2018 – 2019　ルートゾーンのKSKロールオーバー

初めて、ルートゾーンの署名鍵が代わり、フルリゾルバが保持していた
ルートゾーン検証の為の情報がアップデート

2019/09/19　JPドメイン名サービスで、2LD,3LD向けに新しい署名鍵のアルゴリズムに対応

CPUの負荷が低いアルゴリズムが利用可能になり、新しい権威DNSサービス
でのDNSSECが利用可能に

DNSSECジャパン

DNSSECの導入・運用に関する課題の整理・共有が目的

- さまざまな資料作成と解説
  - プロトコル解説資料
    - RFC解説資料
  - システム設計の資料
    - ツール資料、HSM利用に関する使用
  - 運用系の利用
    - 移転ガイドライン
    - 失敗事例

成果の対外的発信によるDNSSECの普及・啓発

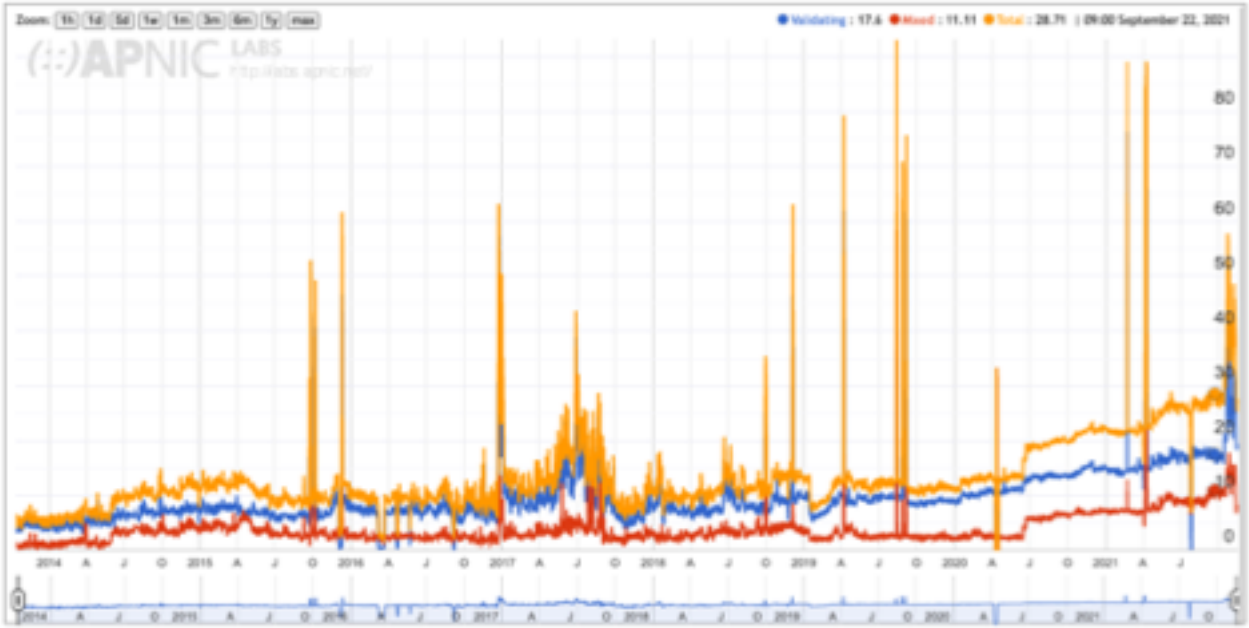
- ３回のミーティング開催
- DNSSEC Ready ロゴ

2012年4月にDNSSECの導入・運用に関する課題の整理・共有が終わった為、活動を終了

現在の状況

フルリゾルバの普及率

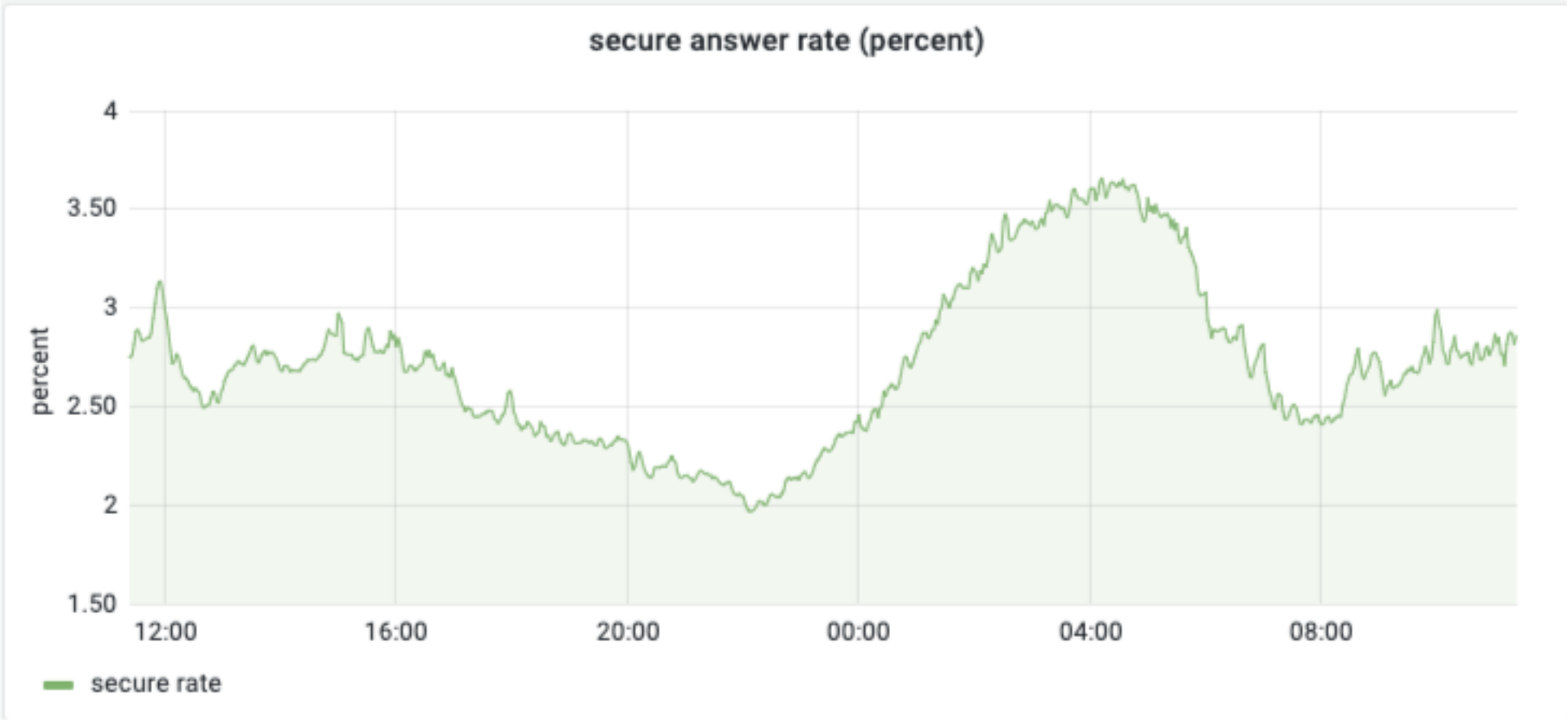
- 日本のフルリゾルバの署名検証の割合はおおよそ25%程度（ユーザ数ベース）
  - JP-DNSのデータからも24%程度なのでほぼ同じ(DNS DayのJP DNS Update資料より)
  - 2019年頃から右肩上がりで順調に増加中
- IPoE事業者の多くが署名検証に対応している。
  - IPoE化が進むにつれて有効率が高くなっていっていると思われる。



- https://stats.labs.apnic.net/dnssec/JP

フルリゾルバから見たゾーン側の普及率

- IIJのフリリゾルバが、署名検証されたレコードを顧客に返したパーセント



ドメイン登録者のDNSSEC対応のために必要なプレイヤー

ROOTゾーン

- 信頼の起点のゾーン

TLDゾーン

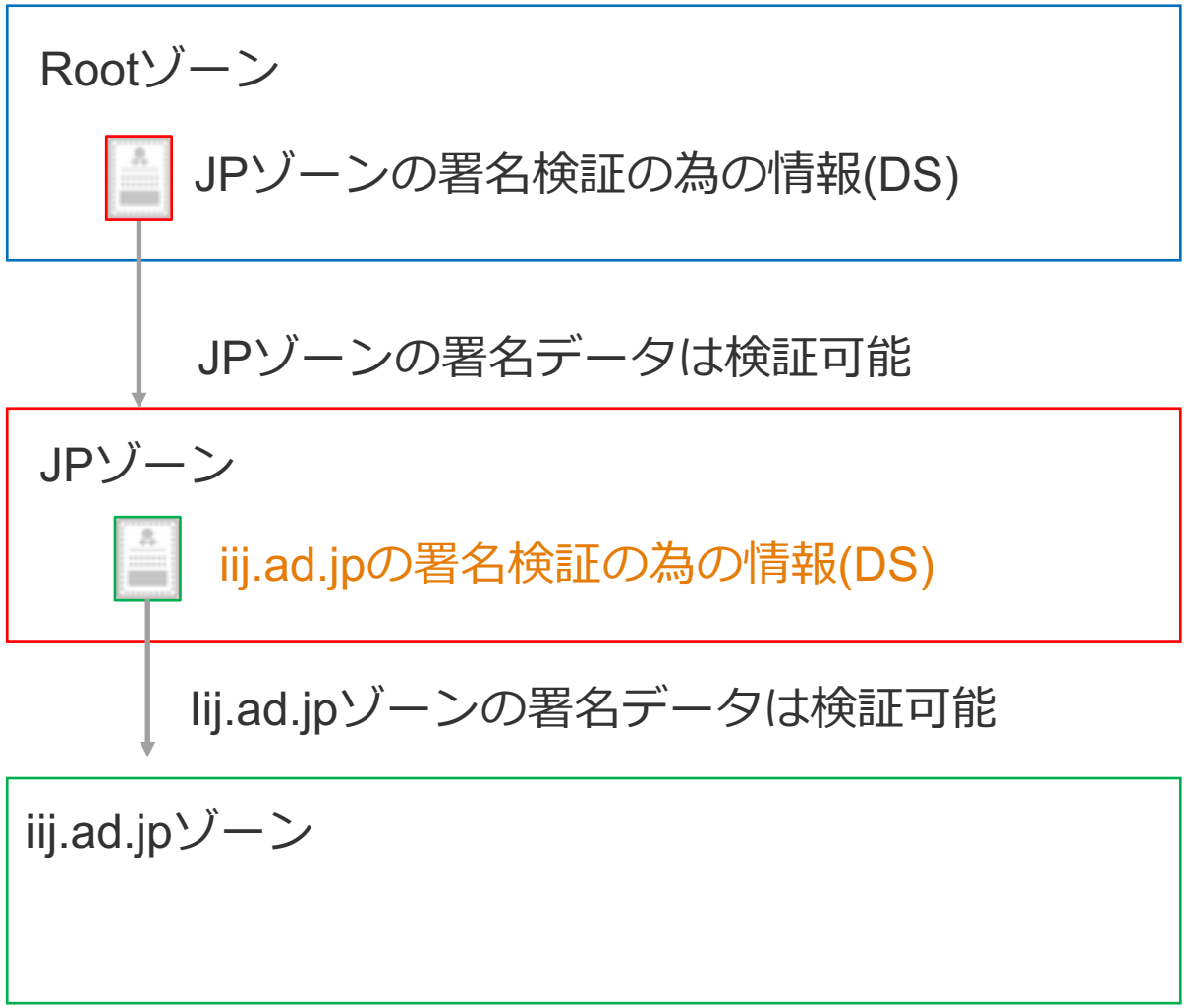
- 2LD,3LDの署名検証情報

レジストラ

- 2LD,3LDの署名検証情報(DS)を登録できる必要

権威DNS

- ゾーンデータへの署名と応答に署名を付与
- ゾーンデータ変更のたびに再署名
- 署名には有効期間がある為、定期的な再署名実行



ドメイン登録者のDNSSEC対応のために必要なプレイヤー

ROOTゾーン

- 対応済み

TLDゾーン

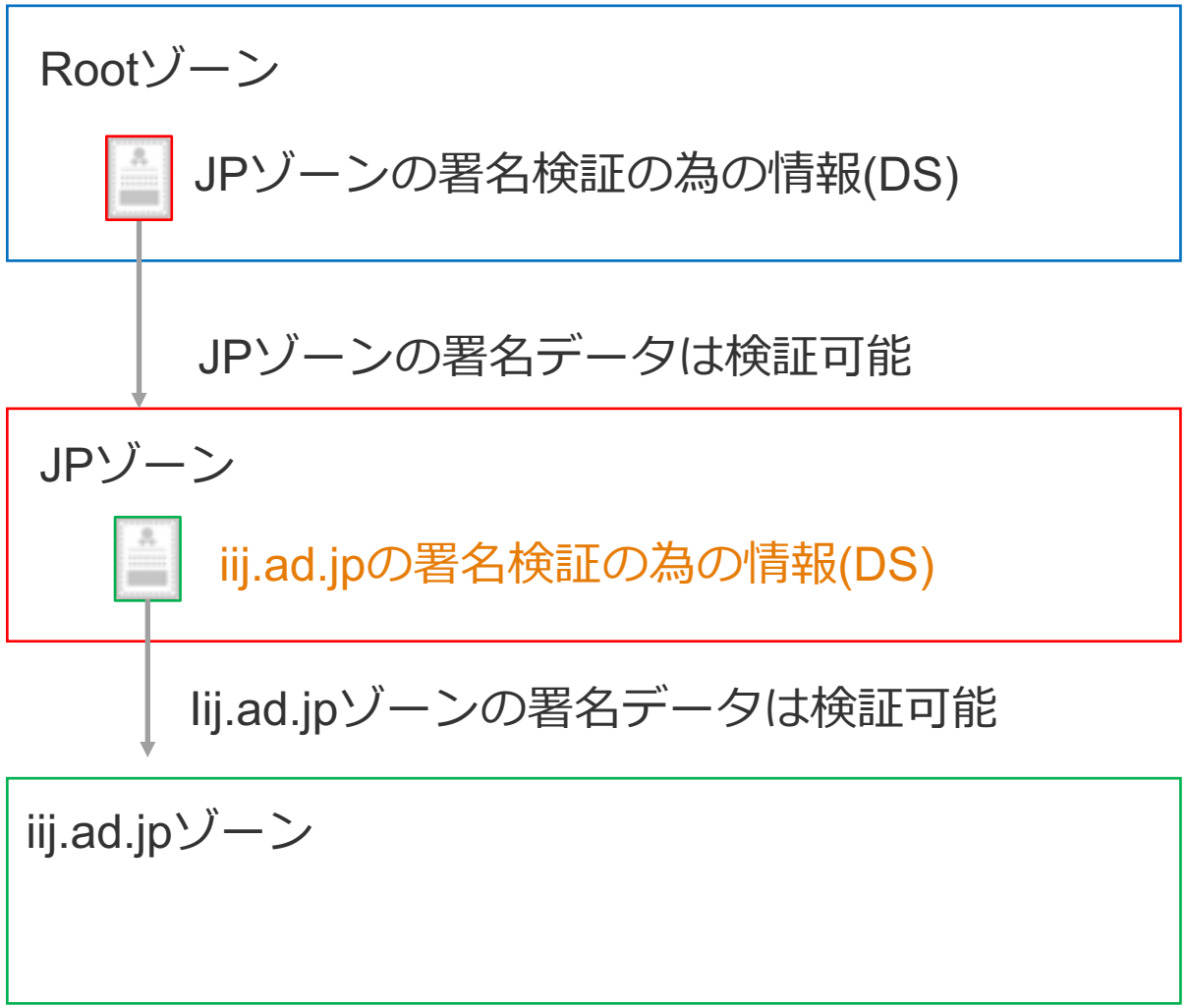
- 90%以上のTLDは対応済み

レジストラ

- 日本のレジストラで対応しているところがほとんどない
- JPドメイン名のレジストラ544サービスのうち
  対応しているのは10サービス

権威DNS

- 主要な権威DNSサーバ実装は対応済み
  - BIND9, NSD, Knot DNS, PowerDNS, CoreDNS
- 権威DNSサービス
  - かなり対応が進んでいる印象
    - Route53, cloudflare, GCP
    - お名前.com, Softbank, IIJ, etc…



※1 https://jprs.jp/registration/list/ でDS取次が有効な数

ゾーン側の普及率

- https://dnsops.jp/stats
  - 各セグメント別の普及状況を調査するために、2018年から継続実施
  - DNSSEC署名が入っていて欲しいなと思うセグメントを中心に調査
  - 個人プロジェクト

2021/11月時点の普及率

種別	ドメイン名数	DNSSEC有効数	割合(%)
高等教育機関	678	8	1.2%
銀行	144	7	4.9%
政府	824	36	4.4%
JPNIC会員	87	5	5.7%
地方公共団体	1875	2	0.1%
JPRS指定事業者	544	8	1.5%
TOPIX銘柄企業	2174	19	0.9%
仮想通貨事業者	38	2	5.3%

DNSSEC

DNSの応答を検証できるようにする技術

フルリゾルバ（検証側）の順調に普及は進んでいる

- キャズムは超えた、あとは時間の問題

ゾーン側の普及は進んでいない

- レジストラの対応に課題がある状況
- ドメイン名登録者がDNSSECを有効にするインセンティブが必要

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ

IIJはいつもはじまりであり、未来です。