つぶらな瞳で考える、DNSSECの普及に必要な何か？は何か？

version 1.23.2

株式会社インターネットイニシアティブ
其田　学

Ongoing Innovation

IIJ
Internet Initiative Japan

自己紹介

Manabu Sonoda 其田 学

経歴

- 2008年 AS4704でL1-L8まで行うフルスタックエンジニア
  - 2010 フルリゾルバでの署名検証機能の設計、構築（日本初）
  - 2011 マネージドDNSでの鍵管理、署名機能を開発構築（日本初）

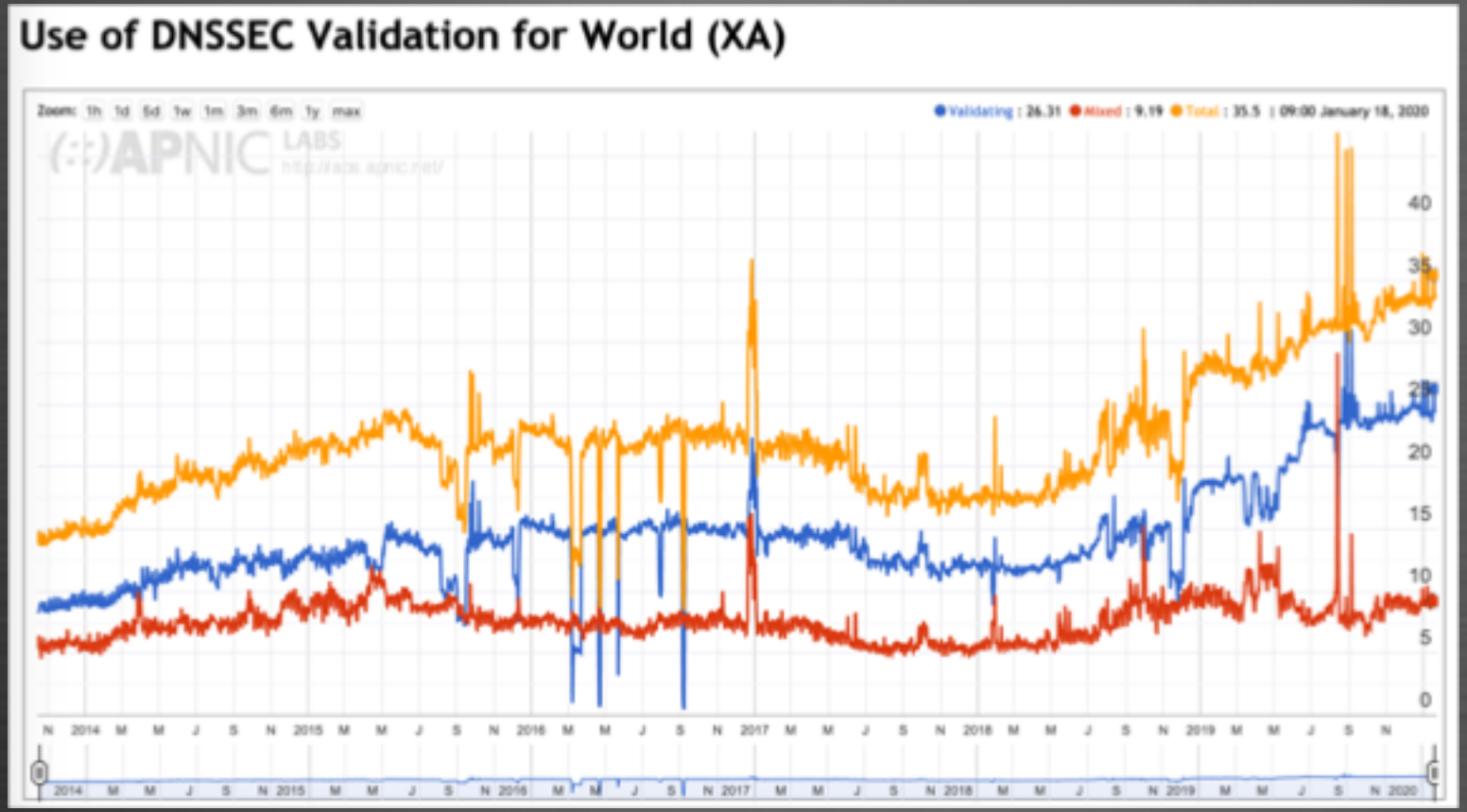
- 2014年 IIJにて現職
  - 商用環境のフルリゾルバ、権威DNSサービスの設計、構築、運用
  - D.DNS.JPの構築、運用
  - コミュニティ活動、啓蒙活動などなど（イマココ）

DNSSECの普及に必要な何？

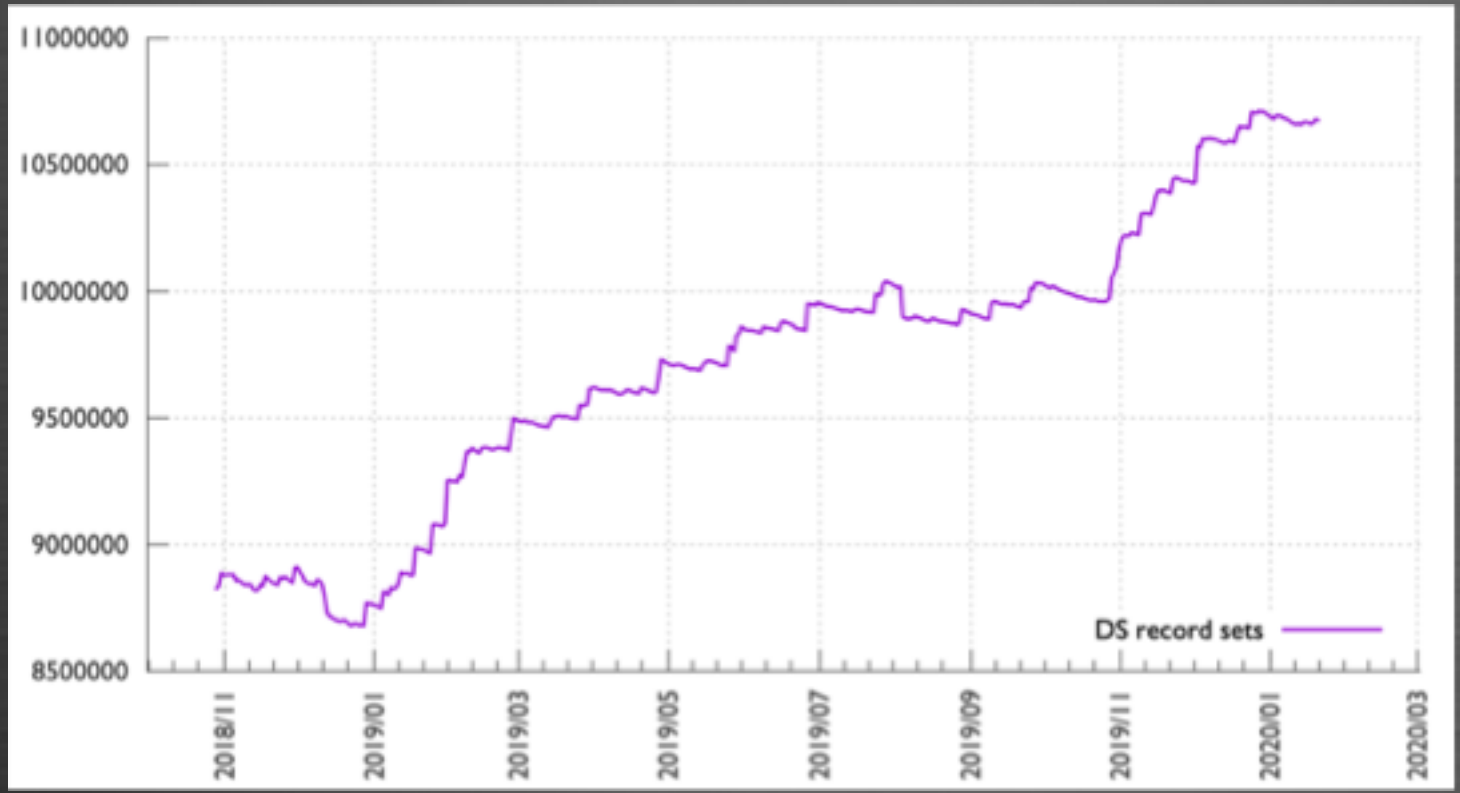
DNSSECって普及してないの？

DNSSECは順調に普及しています

すでに全世界で25%程度のクライアントが対応



署名ゾーン数も順調に増加中



海外では

DNSSECは順調に普及しています

日本でDNSSECが普及しないのは
なぜ？

アジェンダ

- 日本でDNSSECが普及しないのは？
  - 鶏卵問題
  - DNSSECがなくても、ポイズニングは防げる
  - 通信先が真正かTLSでわかるから不要

- IIJでの取り組み
  - フルサービスリゾルバ
  - マネージドDNSサービス

日本でDNSSECが普及しないのは
なぜ？

フルリゾルバ提供者

日本のサービスで署名されている
ゾーンが少ないからDNSSEC検証をしない

権威DNSサーバ提供者

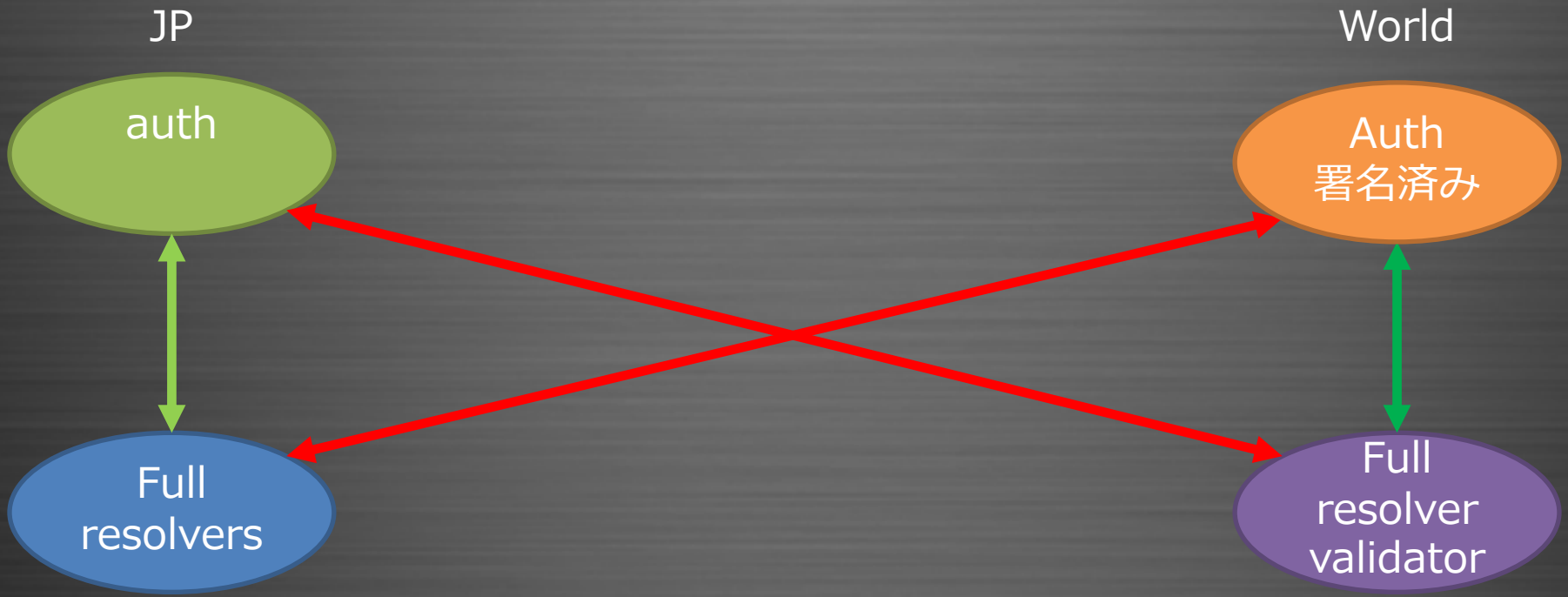
日本のサービスで検証する
フルリゾルバが少ないから署名をしない

その１鶏卵問題

日本の権威DNS、日本のフルリゾルバが
互いの普及率を導入のモチベーションにするのは
そもそも間違い

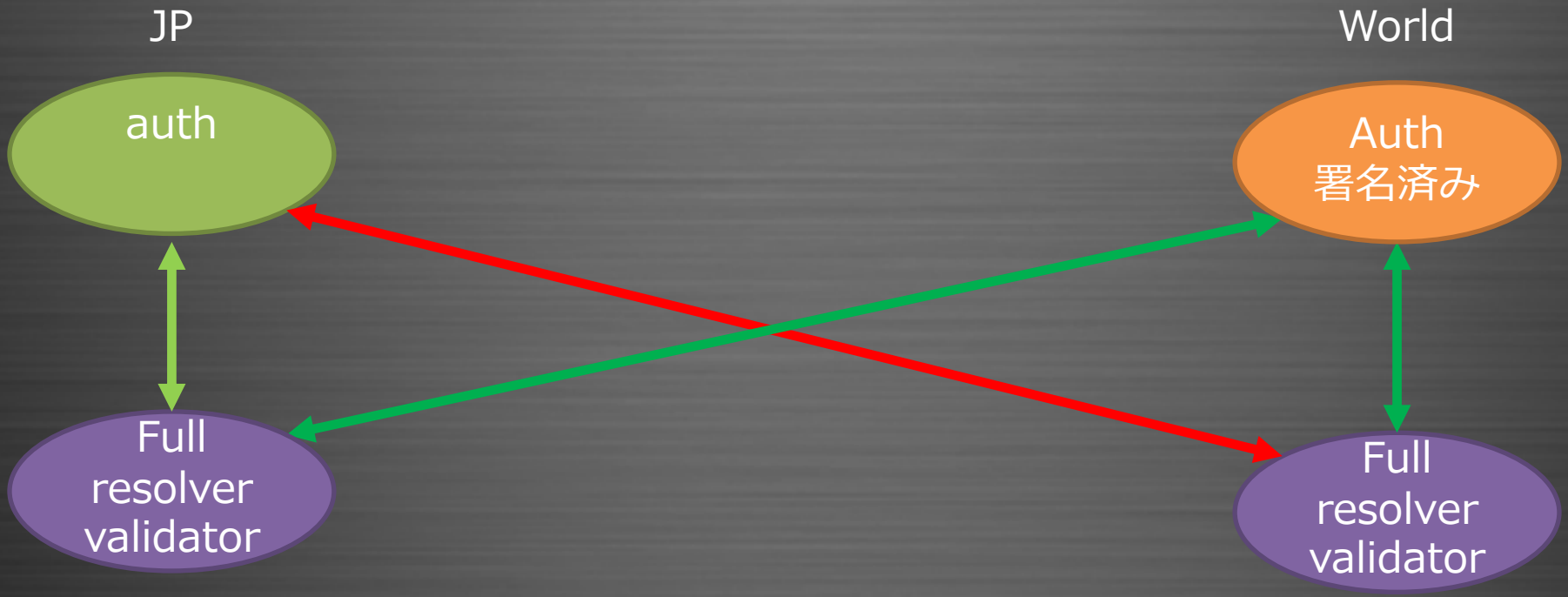
その１鶏卵問題

フルリゾルバと権威DNSサーバの間のネットワークが近ければ、
改ざんリスクは低く、遠ければリスクが高い



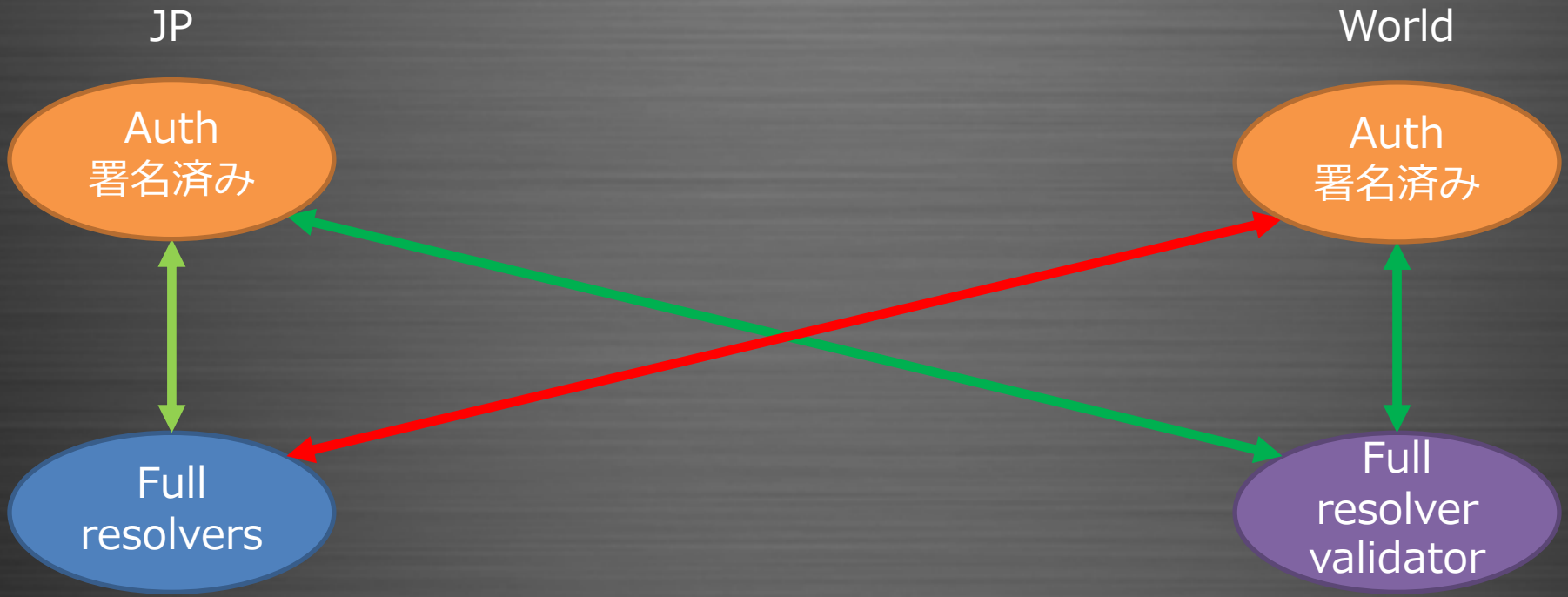
その１鶏卵問題

日本のフルリゾルバが署名検証すれば、日本以外のリスクが高いゾーンの
検証ができるようになり



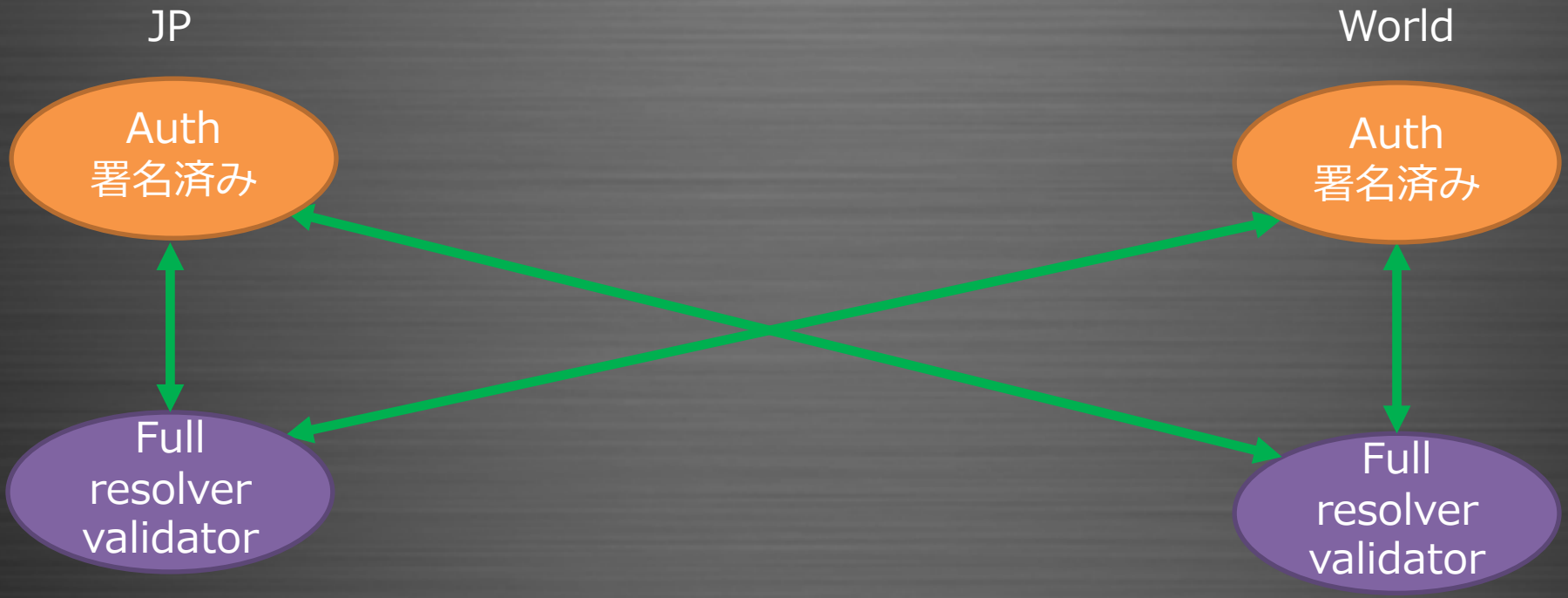
その１鶏卵問題

日本の権威DNSサーバでゾーンを署名すれば
海外のフルリゾルバはリスクの高い日本の権威DNSサーバのゾーンの
署名検証できる



その１鶏卵問題

これが多数の国で同時におこっているので、
徐々に署名検証や、署名するのがお得な状況になっていっている



その２ DNSSECなくても、キャッシュポイズニングは防げる

根本解決しなくても
　　ソースポートランダマイズ
　　IPフラグメント抑止
とかで防げるでしょ

すでに攻撃受けてますけど！

2015

スノーデン事件、広範囲の盗聴が明らかに

JANOG35(2015)

「DNSの可用性と完全性について考える。」

最大の脅威はBGPハイジャックで、RPKIとDNSSECで守るしかないと

2018

BGPハイジャックにより、Route53の一部が乗っ取られる

Myetherwallet事件

その3　通信先が真正かTLSでわかるから不要

そもそもTLSではデータの完全性は保証できない

例：
RPMなどのパッケージはhttpsで配っているが、パッケージが正しいかは
GPG署名などの電子署名で検証している。

DNSSECはこのGPG署名に相当するものである

その3　通信先が真正かTLSでわかるから不要

スノーデン事件以後、IETFのプロトコルは、広域盗聴を難しくすることが求められる様に

なんでもDNSにぶち込んどけが進んだ結果
様々なプロトコルが、DNSを信頼の起点に使い始めた
今はDNSSECがデプロイされている前提でプロトコル設計がされている。

- ドメイン認証のTLS証明書
  - ACME dns01
    - TLS証明書もDNSで登録者認証する。
    - 既にSSLでE2Eだけ守ればいいは通用しない
- MTA-STS
- ESNI
- 等

IIJのDNSSECへの取り組みを
紹介するよ

フルサービスリゾルバ

先週からDNSSEC署名検証はじめました

IIJ、接続サービスで提供するDNSのセキュリティを強化

最新のDNSプロトコル（DoT、DoH）およびDNSSECをDNSキャッシュサーバに導入し、安全性を向上

2020年1月16日

➤ このニュースのPDF版 [512KB]

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：勝 栄二郎）は、お客様のインターネット利用時の安全性を高めるため、IIJのインターネット接続サービスで提供しているDNS（Domain Name System）のキャッシュサーバにおいて、最新の標準プロトコル「DoT（DNS over TLS）」、「DoH（DNS over HTTPS）」および「DNSSEC（DNS Security Extensions）」に対応し、本日より提供開始いたします。

DNSのセキュリティ課題と業界標準の動き

DNSはドメイン名とIPアドレスを結びけるための仕組みで、お客様がWebサイトにアクセスする場合、PCやスマートフォンからDNSキャッシュサーバに問い合わせを行い、DNSの応答情報をもとにWebサーバとの通信を行います。しかし、この仕組みを悪用したサイバー攻撃によってDNSの応答情報が偽造されるリスクが指摘されており、利用者が気づかないうちに不正な偽サイトに誘導されるなど、様々な脅威にさらされる危険性があります。これまでのDNSプロトコル（通信手順）では、通信経路が暗号化されていない、DNSキャッシュサーバが正当なサーバであることを確認する方法がないなど、セキュリティの強化が課題となっていました。

こうした状況に対し、インターネット技術の標準仕様を策定する団体「IETF（Internet Engineering Task Force）」では、DNS問い合わせの暗号化やサーバの正当性確認のための仕組みを含んだ新しいDNSプロトコルの標準化が進められてきました。その最新技術の一つが、DoT/DoHによる経路暗号化であり、もう一つが電子署名を応用してサーバの正当性を検証するDNSSECです。

フルサービスリゾルバ - 署名検証を始めた理由

キャッシュポイズニングは現実の脅威
- 既にBGPハイジャックで攻撃を受けている。
- 署名検証しないとそもそもポイズニングに気づけない。

署名検証を行っていない場合のリスク
- 他社では対応して防げたのにという、
  営業的なリスクが増加

特にモバイルは、自分でDNSを変更できない為、
ISPのDNSで署名検証する必要がある。

マネージドDNSサービス

2011

- ドメイン管理サービス
  - DSの取次に対応

- DNSアウトソースサービスのオプションとして提供開始（初代システム）
  - 署名アルゴリズム RSASHA1024(ZSK)＋RSHASHA2048(KSK)
  - デフォルト署名OFF
  - IIJのドメイン管理サービスが必須

2014

- DNSアウトソースサービスのシステムの全面書き換え（２代目システム）

マネージドDNSサービス

2019

この１０年の時代の変化、使用の変化に合わせてアップデート

- ドメイン管理サービス
  - CDS Upload機能を追加し、CDSを使用した、DSの追加、更新、削除に対応
- IIJ DNSプラットフォームサービス（３代目システム）
  - 署名アルゴリズム ECDSAP256SHA256(ZSK/KSK)
  - デフォルト署名ON
    - 逆引きゾーンを含む全てのゾーンを署名
  - ゾーン転送されたゾーンへの署名機能
    - Hidden master 構成で、署名だけ、アウトソースできる
  - CDS Publish , CDS Import機能
    - CDSを使って、IIJ以外のレジストラとの連携も可能に

マネージドDNSサービス- デフォルト署名ONを始めた理由

リソース問題の解消

- CPUリソースも格段に上がり、さらに楕円暗号が使える様になり、相対的に署名のコストが非常に低くなった
- 全ゾーン署名してもリソース的には問題なくなった

署名検証率の増加

- 世界的に見ると既に25%ほどが署名検証している。

DNSSECに対する考え方のシフト

- DNSSECはモダンなDNSの標準仕様であってもはやオプションではない

まとめ

- DNSSECはDNSのオプションな機能では既になく、標準機能である
- 様々なプロトコルがDNSSECを前提に作られている
- DNSSECに対応している＝普通
  DNSSECに対応していない＝Insecure

Ongoing Innovation

IIJ Internet Initiative Japan

ご清聴ありがとうございました