作成者によるRPKI/DNSSEC/DMARCガイドライン要点解説

DNSSECガイドライン要点解説

2024年11月21日

株式会社インターネットイニシアティブ
其田　学

自己紹介

■名前　　其田　学

■所属　　株式会社インターネットイニシアティブ

アプリケーションサービス部　DNS技術課

■職務　　IIJのお客様向けのDNSサービスの設計・運用など

■DNSとの関わり　　前職時に2010年にフルリゾルバーへの署名検証の導入

2011年に権威DNSサービスでのDNSSEC署名の導入

IIJ JOIN後はIIJのフルリゾルバーへの署名検証の導入、 IIJ DNSプラットフォームサービスの設計、運用など

DNSSECガイドラインでは、第２章フルリゾルバーのDNSSEC対応を担当

アジェンダ

- DNSSECの現状について
- DNSSECガイドラインについて
- 各章のポイントについて
- 第２章フリリゾルバのDNSSEC対応についての解説

DNSSECの現状

DNSSEC署名検証するには、署名側と検証側の２つのプレイヤーの対応が必要

署名側 （権威DNSサーバ）

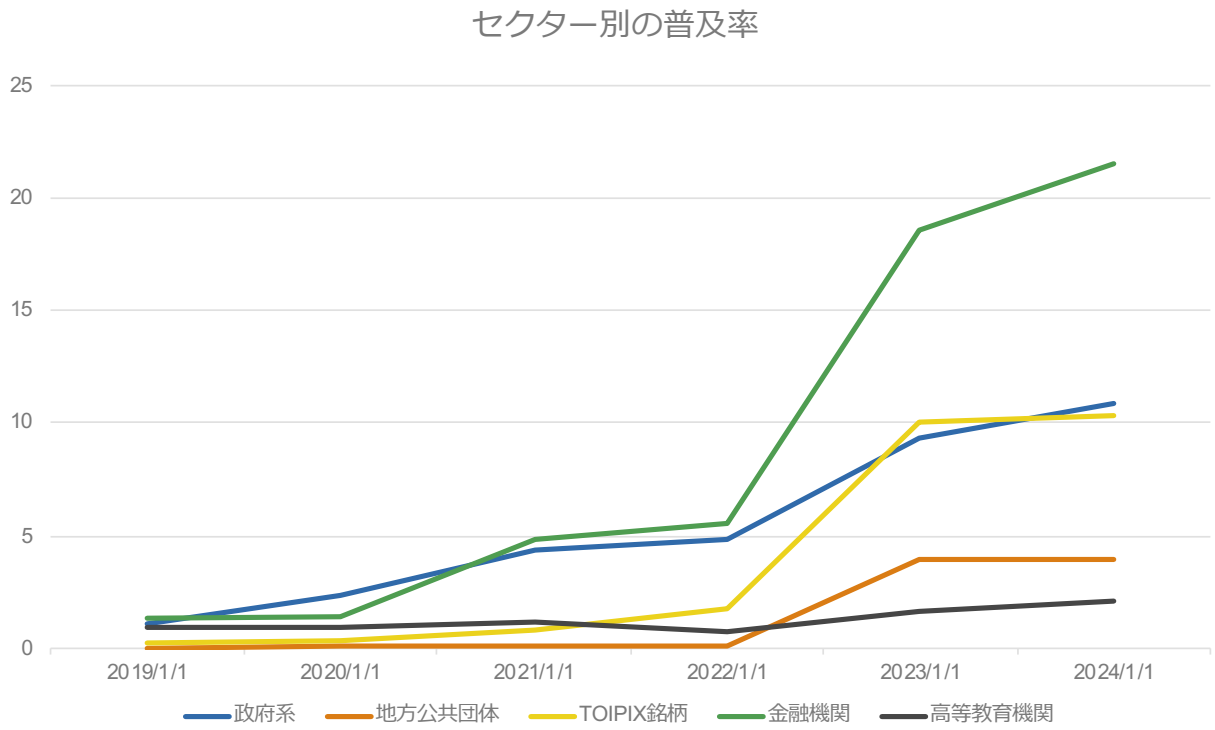
1. ゾーンデータに電子署名を行う
2. 署名検証に必要な情報（DSレコード）を上位ゾーン（レジストリ）に登録する

検証側（フルリゾルバー)

1. 最上位のルートゾーンの署名検証に必要な情報（トラストアンカー）を設定
2. 署名検証を有効化

署名側の対応率

日本のセクター別のDNSSECの署名普及率



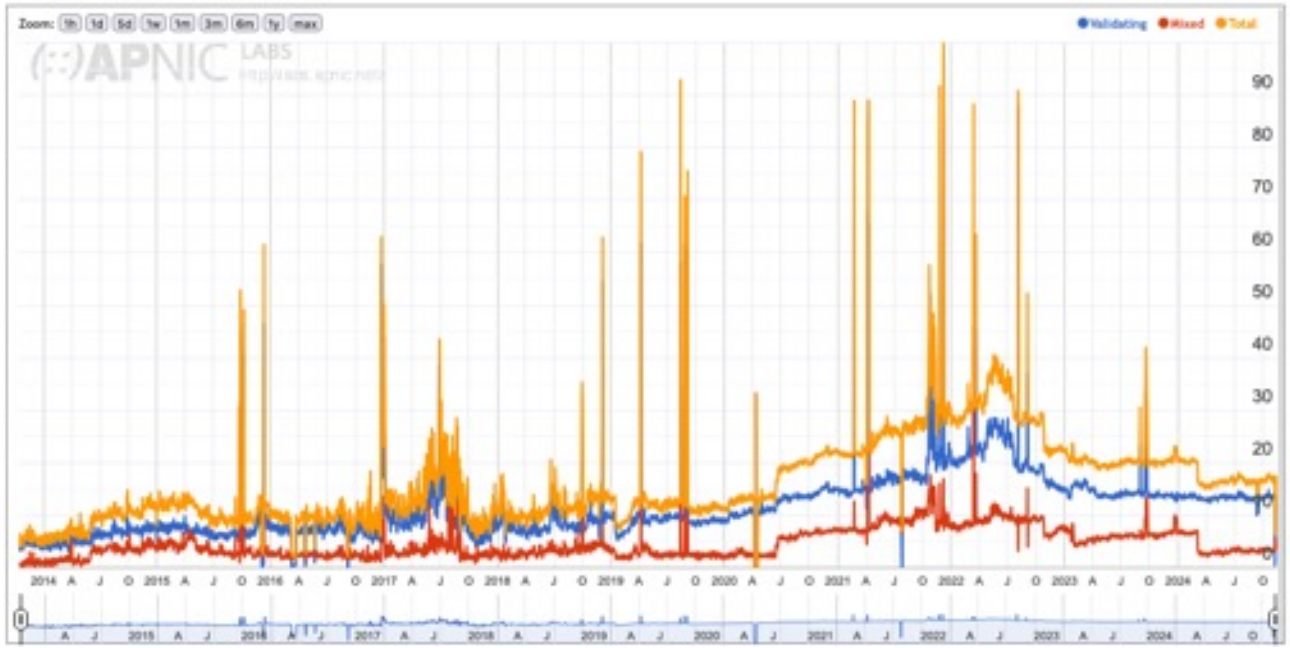
2022-2023年で大幅増、金融系は20%を超える普及率

出典: https://stats.dnsops.jp/

検証側の対応率

APNICが調査しているDNSSEC Validationしているクライアントの率

日本のDNSSEC検証率



2024年11月時点では約13%の対応率

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

DNSSECの現状まとめ

JPドメイン名全体としての署名対応率は低い状況だが、徐々に増加している

一方で金融系や、政府系などの重要なドメイン名へのDNSSEC導入は
他のセクターよりも先んじて進んでおり、多数の国民が利用しているサービスの
ドメイン名での導入も進んでいる。

しかし、多くのISPのフルリゾルバーでの署名検証がされていない状況で、多くの
国民がDNSSECに守られていない状態

次は、ISPのフルリゾルバーのDNSSEC対応のターン

DNSSECのガイドライン案について

1. ガイドラインは発行されてません

- ガイドライン案が総務省のICTサイバーセキュリティ政策分科会（第5回）の資料として配布されています
- https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00286.html

2. ガイドブックではないです

- DNSSEC対応を行うときの考え方についてまとめていますが、実際の手順については記載していません。
- 手順については、各ベンダーやサービスが公開している手順参照し、ガイドラインに照らし合わせて実施項目を確認することを想定しています。

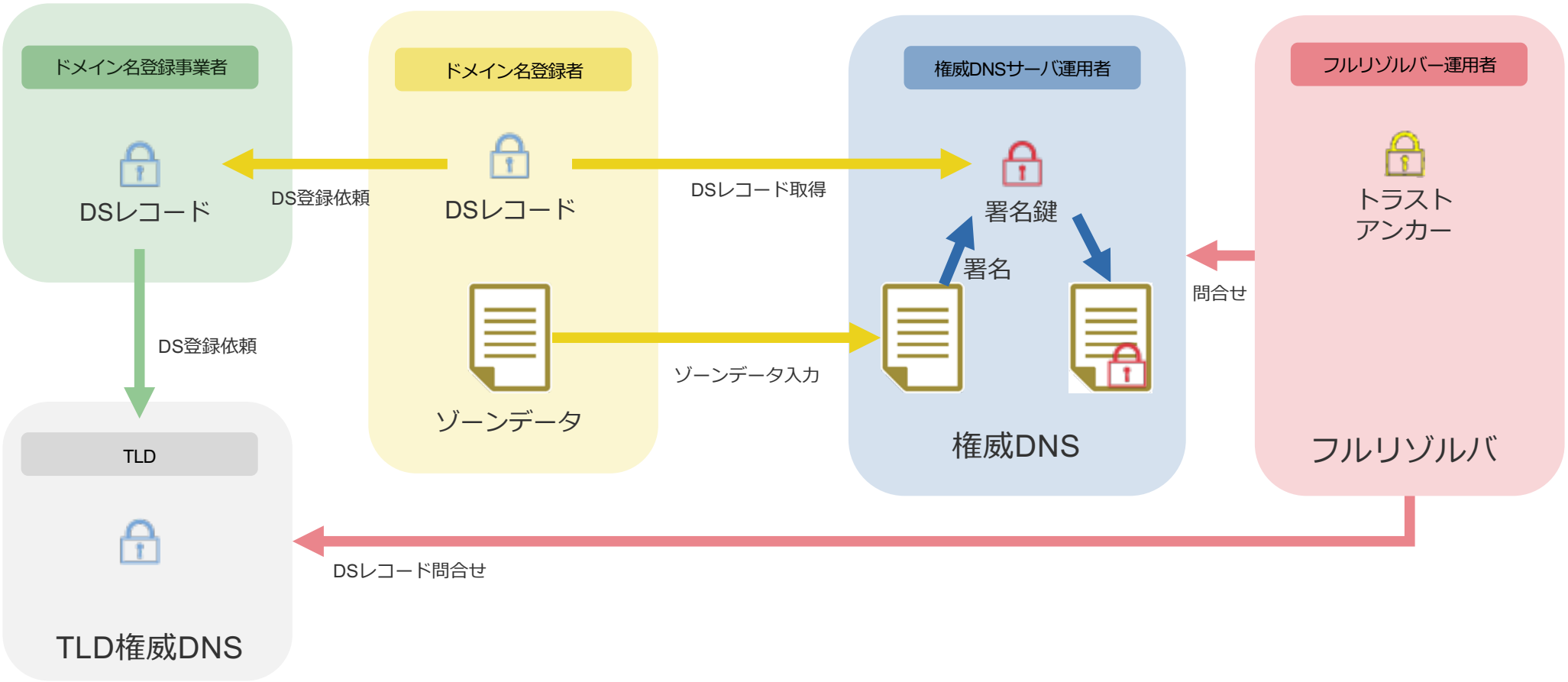
各章のPoint

序章　　想定読者と用語
第１章　ドメイン名の重要性とライフサイクルマネージメント
第２章　フルリゾルバーのDNSSEC対応
第３章　権威DNSサーバーのDNSSEC対応
第４章　ドメイン名登録・登録管理関係者

DNSSECガイドラインの想定読者

ドメイン名登録者	申請して登録されたドメイン名を維持管理するとともに、そのドメイン名を利用したサービスを提供する組織(または個人)。ゾーンデータの内容に関して責任を持つ
ドメイン名登録事業者	TLD管理組織(レジストリ)とドメイン名登録者の間に入り、ドメイン名登録に関する窓口業務を行う組織
権威DNSサーバ運用者	ドメイン名と関連情報を結びつけるデータベース機能を提供する権威DNSサーバーを運用する組織 。ドメイン名登録者が指定したゾーンデータを公開する
フルリゾルバー運用者	クライアントからのリクエストに応じて権威DNSサーバーで公開された情報を検索し、取得・分析 して結果をクライアントに返す(名前解決を行う)、フルリゾルバーを運用する組織

DNSSECガイドラインの想定読者の関係(DNSSEC対応後)



第1章 ドメイン名の重要性とライフサイクルマネージメント

ドメイン名登録者

ドメイン名登録事業者

権威DNSサーバ運用者

フルリゾルバー運用者

主な内容

- ドメイン名の重要性の説明
- ドメイン名保護の手段の一つとしてのDNSSEC

ポイント

- ドメイン名はもはや知的財産である
  - 組織の価値とドメイン名の価値がリンクしている
  - ドメイン名のインシデントは組織の価値の毀損に繋がる
- DNSSECや送信ドメイン名認証などは、ドメイン名の価値を守るための手段
- ドメイン名登録は登記に近く、リース契約に近く永続性があるものでない（ライフサイクルマネージメント）

第3章 権威DNSサーバーのDNSSEC対応

ドメイン名登録者

権威DNSサーバ運用者

主な内容

- 署名、署名鍵、信頼の連鎖の構築に関する説明
- 実装時の注意点、運用ノウハウ

ポイント

- 署名鍵のライフサイクル管理（ZSK/KSKロールオーバー）
- 権威DNSサーバをアウトソースする場合に明確化すること
  - KSKロールオーバーのタイミング
  - DSレコード更新の実施者

第4章 ドメイン名登録・登録管理関係者

ドメイン名登録者

ドメイン名登録事業者

主な内容

DSレコードに関する説明
DSレコードの登録（取次）に関する説明

ポイント

- DSレコードが存在する場合に、ゾーンデータの署名検証が行われる
- 別の権威DNSに変更する際は、DSレコードに注意しないと、署名検証エラーになる
- DSレコードはDSレコードの登録に対応したドメイン名登録事業者を通じて登録する
  - 対応していない事業者も存在する

第4章 ドメイン名登録・登録管理関係者

親ゾーンにDSがあるので署名検証が発生

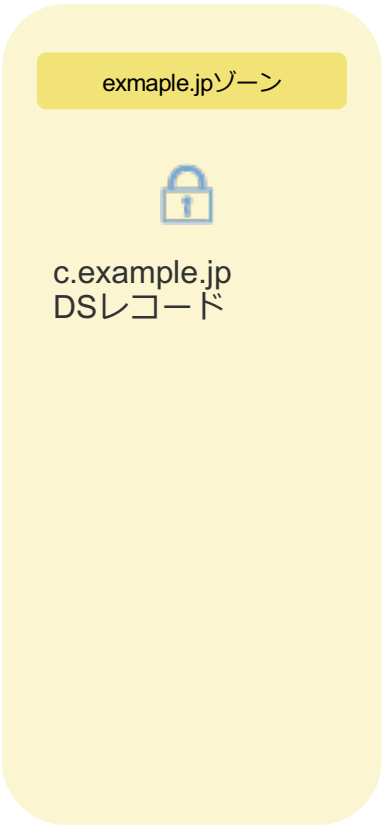
未署名なので、署名検証エラー

親ゾーンにDSがないので署名検証しない

署名しているが、認証ではない

（通常の未署名と同じ扱い)

第4章 ドメイン名登録・登録管理関係者



親ゾーンにDSがあるので署名検証が発生

署名検証できれば認証データ(ad bit)

NSレコードを変更すると

親ゾーンにDSがあるので署名検証が発生

未署名なので、署名検証エラー

フルリゾルバーのDNSSEC対応について

第2章フルリゾルバーのDNSSEC対応について

フルリゾルバー運用者

主な内容

DNSSEC署名検証に関する説明
署名検証対応に必要な確認項目、対応内容等
署名検証失敗時の対応

フルリゾルバーのDNSSEC対応レベルについて(2.7 運用ノウハウ)

フルリゾルバー運用者

レベル1
MUSTが指定された要件をすべて満たす。

レベル2
利用者に影響する署名検証失敗が発生した場合に検知でき、利用者や関係者にその 原因を説明できる。

レベル3
署名検証失敗が発生した場合に復旧に向けた適切な対応が取れる。

レベル1: MUSTが指定された要件をすべて満たす

フルリゾルバー運用者

MUST/MUST NOTな要件

項番	要約
2-1 2-2	公開しているフルリゾルバーは全てDNSSEC署名検証に対応すること
2-3	フルリゾルバーの 時刻を信頼できる時刻ソースと同期すること
2-4	EDNSのバッファーサ イズを一般的なMTU値を超えた値に設定しないこと
2-7	トラストアンカーは、常に最新のものを使用すること
2-12	監視項目に、時刻同期状況の確認、DNSSEC署名され た名前が解決できることの確認を追加すること

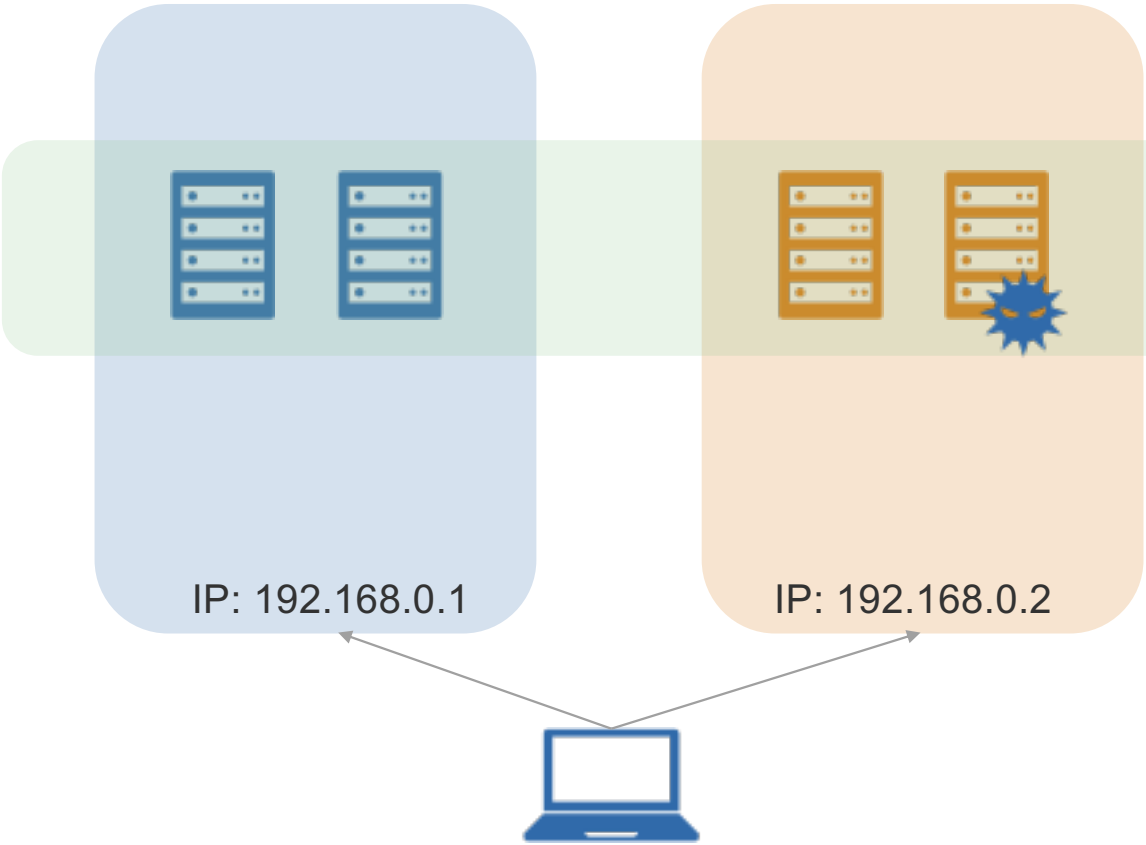
2-3,2-4,2-12(時刻同期)などは、通常のDNS運用でもやっていて当たり前の項目

2-1,2-2,2-7,2-12(検証確認)が署名検証を有効にするときに追加される項目

DNSSEC署名検証側として、正常運用できる状態になっていればレベル１

2-1. 公開しているフルリゾルバーは全てDNSSEC対応にしなければいけません
2-2. 例えば3つの異なるIPアドレスで3台のフルリゾルバーを運用している場合に、
3台中2 台をDNSSEC対応にして1台は未対応のまま残すという運用をしてはいけません (MUST NOT)

フルリゾルバー運用者

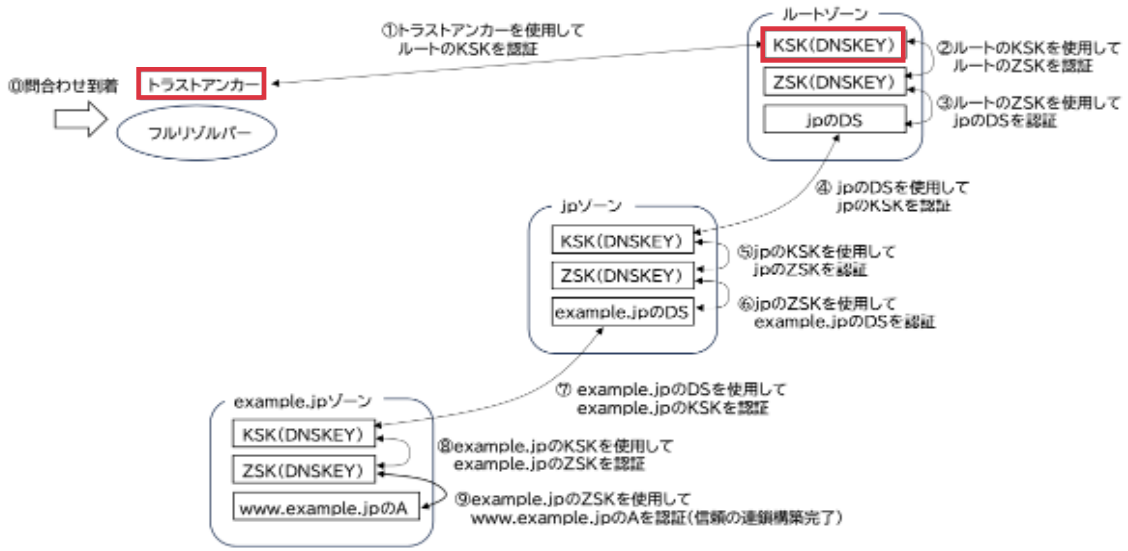


１台でもDNSSECに対応していないと、
クライアント側のリトライで、
偽の応答を受け取る

署名検証を段階的にデプロイする等で一時的に、
一部のフルリゾルバのみ署名検証することは有り得るが、最終的には全台対応する必要がある

2-7. リゾルバーに設定として与えられるトラストアンカーには、最新のものを使用しなければ いけません

署名検証はトラストアンカーを使ってルートゾーンを検証し、順番に上位のゾーンから
信頼できるデータか確認していく作業



ルートゾーンKSKロールオーバーで、KSKが変わった際に、トラストアンカーが追従できていない場合、信頼の基点は古くなったトラストアンカーのため、フルリゾルバから見ると、ルートゾーンが正しくない応答を返している状態になる。
この状態では全てのドメイン名が署名検証エラーになる

署名検証失敗時の対応について

フルリゾルバー運用者

フルリゾルバ側は正常だが、一部のドメイン名で署名検証失敗時の対応

1. そもそもDNSSECに限らず、Lameや、変な権威DNSサーバが世の中には多数存在し、それに全てリゾルバ運用者が対応するのは困難である無駄である。

2. 検証エラーの原因が設定ミスの場合、DNSSEC検証を無効にすることができるが。。

- しかし、設定ミスなのか、キャッシュポイズニングなのか、フルリゾルバ運用者側だけで判断することができない。
- 結局、設定ミスかどうかは、ドメイン名登録者や、権威DNSサーバ運用者しかわからない

署名検証失敗時の対応について

フルリゾルバー運用者

ユーザに署名検証エラーが返ることが、正しい状態である

- 署名検証エラーを返すことを目的としていることを組織内に浸透させ、回答方針を意思統一する。
- 安易にDNSSEC検証を無効にし、結果的にユーザーが偽の応答を受け取ることが、最もユーザーからの信頼を失う行為である。

署名検証失敗時のレベル別の対応内容について

フルリゾルバー運用者

レベル1

署名検証失敗時は権威DNSサーバ側の復旧をまつ

レベル2

署名検証失敗時は権威DNSサーバ側の復旧をまつ

署名検証失敗して、ユーザー影響が出ていることを、関係部署に説明できる

レベル3

署名検証失敗が発生した場合に復旧に向けた適切な対応が取れる。

- 権威DNSサーバ運用者や、ドメイン名登録者に連絡を取って早期の復旧を促しても良い
- 復旧確認後にキャッシュクリアでフルリゾルバ側での名前解決を早期に復旧させる
- ドメイン名登録者、権威DNSサーバ運用者から設定ミスの公表があれば、そのドメイン名の検証を無効化しても良い

第2章フルリゾルバーのDNSSEC対応について

フルリゾルバー運用者

ポイント

トラストアンカー

- ルートゾーンの検証を行うための情報で信頼の基点
- トラストアンカーを最新の状態に維持すること

署名検証失敗時の対応

- 権威DNSサーバ側の復旧を待てば良い
- 署名検証が失敗することは正しい挙動であると、組織全体に浸透させる事

ここで紹介できたのは全体のごく一部です、
ガイドラインはさらに深い内容になっておりますので、ご一読ください。

導入には意思決定層の理解が必要になります。
「1.1の経営者・代表者の方へ」をお読みいただき、意思決定層の方へ展開ください

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。