CDS/CDNSKEYレコードとは

2023年11月21日

Internet Week 2023 DNS DAY

株式会社日本レジストリサービス (JPRS)

栂 邦雄（かこい くにたか）

本発表の内容

- CDS/CDNSKEYレコードの「現状とこれから」の話に入る前に、そもそもCDS/CDNSKEYレコードとはどのような技術なのかをご紹介・解説していきたいと思います。

自己紹介

■名前

栂 邦雄 (かこい くにたか)

■所属

JPRS サービス開発部

■主な業務

ドメイン名に関連するサービスの企画、要件定義

目次

1. CDS/CDNSKEYレコードの背景と概要
2. CDS/CDNSKEYレコードの仕組み(RFC 8078)
3. まとめ

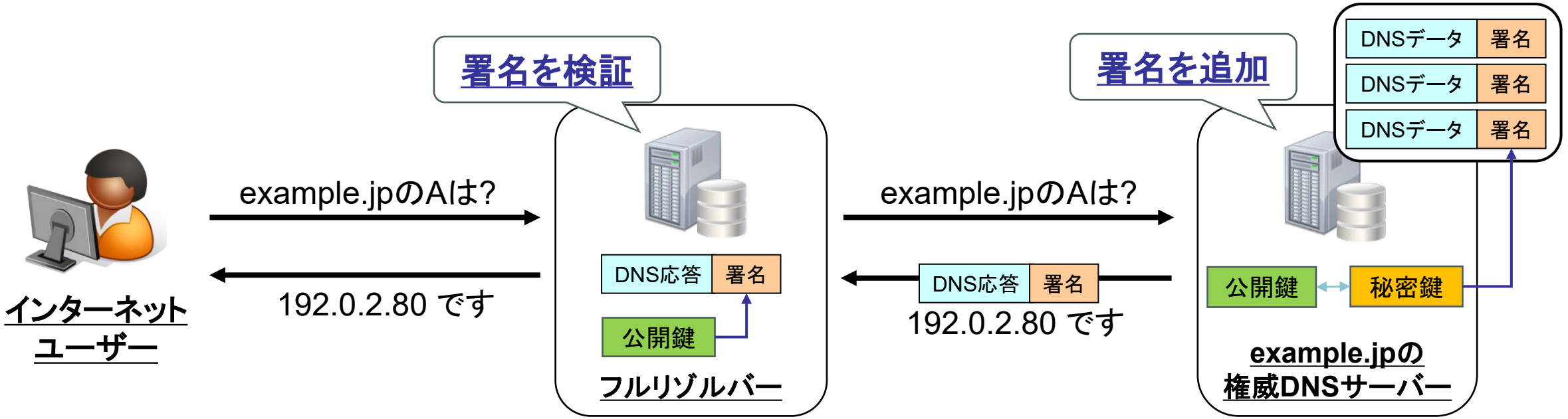
1. CDS/CDNSKEYレコードの背景と概要

CDS/CDNSKEYレコードとは

- CDS/CDNSKEYレコードは、DNSSECで必要となる「親ゾーンへのDSレコード登録」をDNSプロトコル上で行う仕組みの中で利用されるDNSレコード

DNSSECの概要

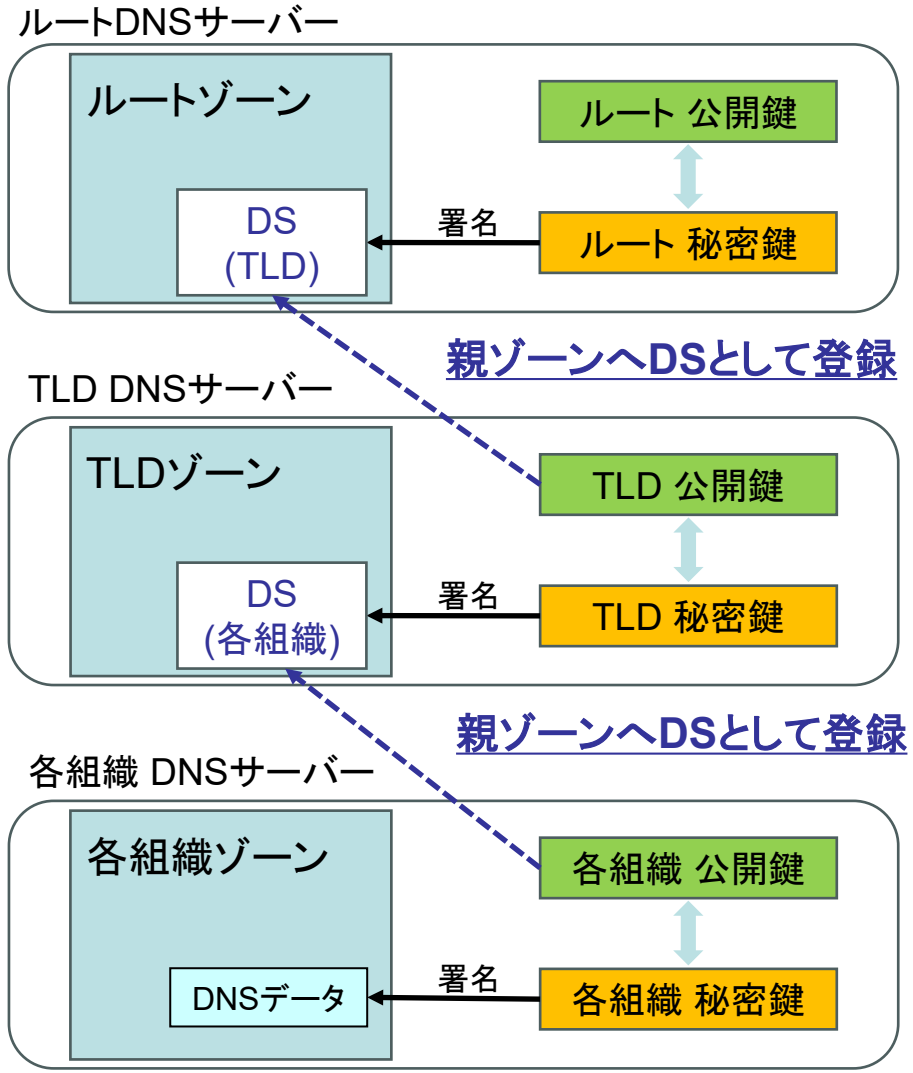
- DNSSECは公開鍵暗号の技術を使い、受け取ったDNSデータの「出自や完全性(改ざんのないこと)」を検証できる仕組み
  - 署名側(権威DNSサーバー): 秘密鍵でDNSデータに署名を追加
  - 検証側(フルリゾルバー)　　: 公開鍵でDNSデータに追加された署名を検証



DNSSECのおける信頼の連鎖

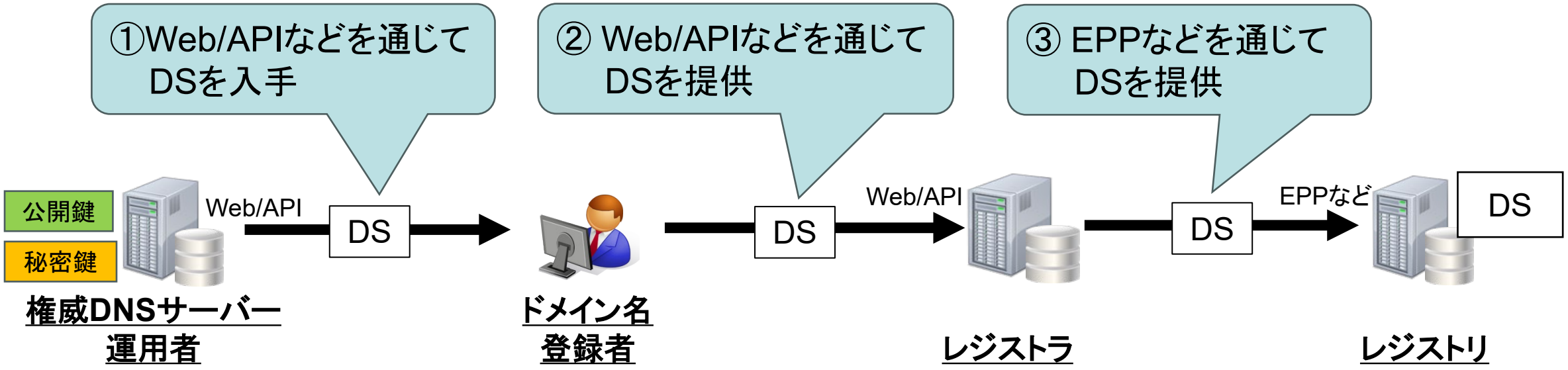
- 署名側は自身の公開鍵(DNSKEY)の信頼性担保のため、公開鍵をハッシュ化した**DSレコードを親ゾーンに登録する必要がある**
  - 親ゾーンの秘密鍵で署名されて公開される
  - 親ゾーンに公開鍵(DNSKEY)をそのまま提供し、親ゾーンでDSレコードが作成される場合もある

- 各ゾーンの管理者がDSレコードを親ゾーンに登録・公開することにより「信頼の連鎖」を構築する



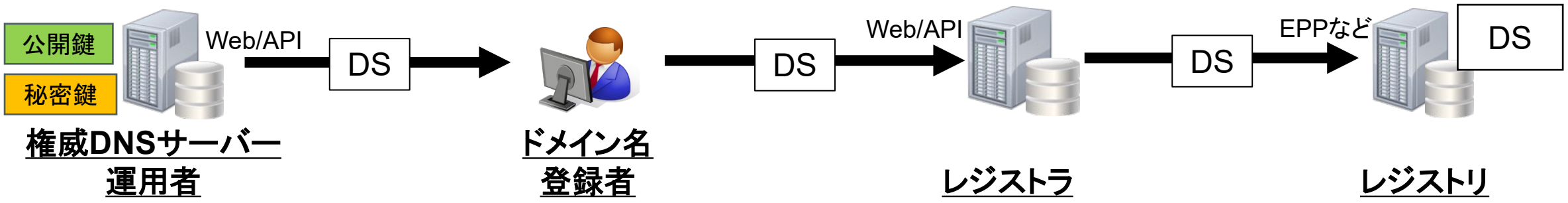
DSレコードのTLDゾーンへの登録

- DSレコードのTLDゾーンへの登録(レジストリへの登録)は、一般的に以下のような流れで行われる
  - レジストリ・レジストラモデルに沿った形で、ドメイン名登録者やレジストラなどがDS取次を行う



DSレコードのTLDゾーンへの登録に関する課題

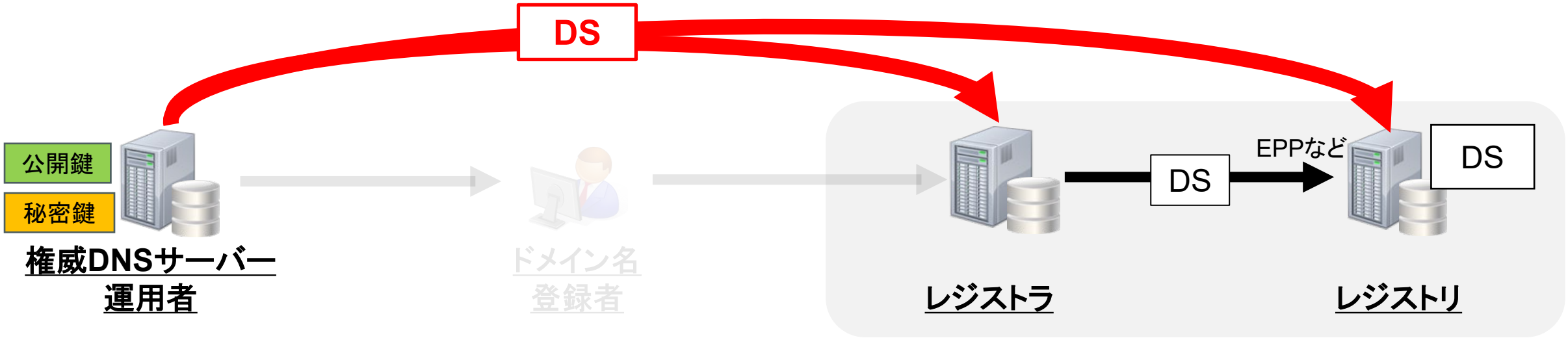
- ドメイン名登録者などは多くの場合DS取次を手作業で行なう必要がある
  - 手間やコストがかかる
  - ミスが発生するリスクがある
- 権威DNSサーバー運用者からレジストリまでの経路上の全プレーヤーがDS取次に対応する必要がある
  - 経路上のDS取次に対応していないプレーヤーがボトルネックとなりDNSSECを有効化できない



CDS/CDNSKEYレコードを用いた DSレコードのTLDゾーンへの登録

- CDS/CDNSKEYレコードを用いることで、**子ゾーン(権威DNSサーバー)が親ゾーン側(レジストリやレジストラなど)に直接DSレコードを提供できるようになる**

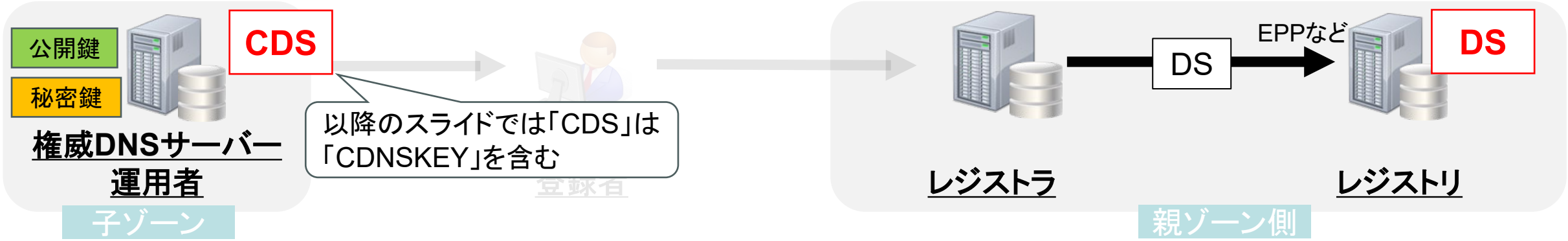
「DS登録の自動化や簡略化」が期待され、DNSSEC運用のコスト削減やリスク軽減につながる



2. CDS/CDNSKEYレコードの仕組み(RFC 8078)

CDS/CDNSKEYレコードの概要

- 2017年4月に発行された「RFC 8078 - Managing DS Records from the Parent via CDS/CDNSKEY」の中で定義されるDNSレコード
- RFC 8078は子ゾーンで設定されるCDS(Child DS)/CDNSKEY (Child DNSKEY)レコードを用いて、親ゾーンに登録されるDSレコードを操作する仕組みを標準化
  - 2014年9月に発行された「RFC 7344 - Automating DNSSEC Delegation Trust Maintenance」では「Informational (情報)」であったのが、RFC8078により「Standards Track (標準化過程)」となった



CDSレコード用いたDSレコードの登録方法 (1/2)

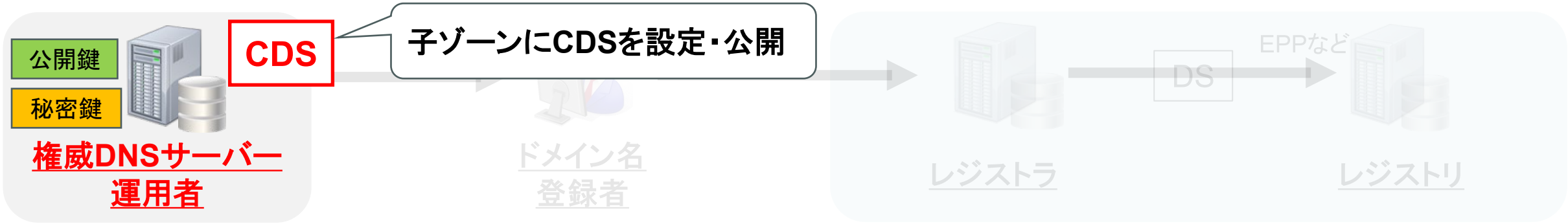
- **親ゾーン側(レジストリやレジストラなど)の対応**
  - DNS問合せにより定期的に管理ドメイン名のCDS/CDNSKEYレコードの存在をチェックし、設定されている場合、そのレコード内容に基づきDSレコードを操作する
    - ただし、全ての管理ドメイン名を定期的にチェックするのは非効率であるという課題もあるため、新しい仕組みも検討が進められている (draft-ietf-dnsop-generalized-notify)
  - CDS/CDNSKEYレコードが設定されていない場合、現在のDSレコードには何も変更を加えない

CDSレコード用いたDSレコードの登録方法 (2/2)

- **子ゾーン(権威DNSサーバー)のゾーンの記載方法**
  - 親ゾーンに登録するDSレコードの内容をCDS/CDNSKEYレコードとして設定する
    - CDSレコードのフォーマットはDSレコード(RFC 4034)と同じ

```
example.jp.  IN CDS  55648  13  2  B4…(16進数40文字)
                     ①     ②  ③      ④
```

①鍵タグ　②アルゴリズム(アルゴリズム番号)
③ダイジェスト型(ハッシュのアルゴリズム)　④ダイジェスト(ハッシュ化した公開鍵)



CDS/CDNSKEYレコードのユースケース

- CDS/CDNSKEYレコードによりDSレコードに対して以下の操作を行うことができる
  - ① DSレコードの初期登録
    - DSレコードの初期登録を行い、DNSSECを有効にする
    - ポイント: CDS/CDNSKEYレコードの正当性の担保
  - ② DSレコードの更新
    - 登録されているDSレコードを更新する
    - 親ゾーン側がCDS/CDNSKEYレコードを受け入れる際にはDNSSECが維持されることをチェックする必要がある
  - ③ DSレコードの削除
    - 登録されているDSレコードの削除を行い、DNSSECを無効にする
    - ポイント: CDS/CDNSKEYレコードのパラメーター

「① DSレコードの初期登録」における正当性の担保

- CDS/CDNSKEYレコードを用いたDSレコードの初期登録を行う際には、CDS/CDNSKEYレコードの正当性が担保される必要がある
  - CDS/CDNSKEYレコードはDNSSECにより正当性を検証するが、初期登録の際にはDNSSECによる検証ができない
  - 「② DSレコードの更新」や「③ DSレコードの削除」では、DNSSECによる検証が可能となる

- 具体的には、親ゾーン側(レジストリやレジストラなど)は「一定期間に渡って複数回CDS/CDNSKEYレコードのチェックを実施して、その間常に同じCDS/CDNSKEYレコードを確認できた場合にのみ受け入れる」といった方法などにより正当性を担保することができる
  - 初期登録の方法は親ゾーン側で定められる

「③ DSレコードの削除」における CDSレコードのパラメーター

- CDS/CDNSKEYレコードでは、アルゴリズムの値として0を指定することで登録されているDSレコードの削除を指定する
  - これまでアルゴリズム番号0は予約されており、DSレコードなどでは引き続きアルゴリズム番号0は予約される
  - アルゴリズムが「0」であれば厳密には他のパラメーターは任意の値でも構わないとなってしまうが、明確にするためにCDSレコードでは「００００」を指定しなければならない

```
example.jp.  IN CDS  0  0  0  0
```

アルゴリズム

3. まとめ

まとめ

- CDS/CDNSKEYレコードは「親ゾーンへのDSレコード登録」をDNSプロトコル上で行う仕組み（RFC 8078）に利用される
  - ドメイン名登録者などを介さずにDSレコードを入手できる
  - 「親ゾーンへのDS登録」の自動化や簡略化に繋がる

- 子ゾーン(権威DNSサーバー)でCDS/CDNSKEYレコードを設定・公開し、親ゾーン側(レジストリやレジストラなど)はスキャンしたCDS/CDNSKEYレコードに基づいてDSレコードの登録を行う
  - DSレコードの初期登録・更新・削除といった操作ができる
  - 初期登録の際は、親ゾーン側は一定期間同じCDS/CDNSKEYレコードを確認できた場合にのみ受け付けるといった方法などで、CDS/CDNSKEYレコードの正当性を担保することができる

Appendix

CDNSKEYのフォーマット

- CDNSKEYのフォーマットはDNSKEY(RFC 4034)と同じ

```
example.jp. IN CDNSEKY 256 3 5 AwEAAeNO41ymz+Iw(行末まで省略)
                       ①  ②③          ④
```

①フラグ(256:ZSK、257:KSK)　　②プロトコル番号 (3のみ)
③アルゴリズム(アルゴリズム番号)　　④公開鍵 (Base64で符号化)

- 「③ DSレコードの削除」におけるフォーマット
  - アルゴリズムの値が「0」

```
example.jp. IN CDNSKEY 0 3 0 0
```