Internet Week 2023 - DNS DAY

CDS/CDNSKEYレコードの今とこれから

株式会社インターネットイニシアティブ
ネットワーク本部アプリケーションサービス部DNS技術課
其田　学

CDS/CDNSKEY(以降CDS)レコードの現状

DS Automation – DSレコード操作の自動化の現状

アジェンダ

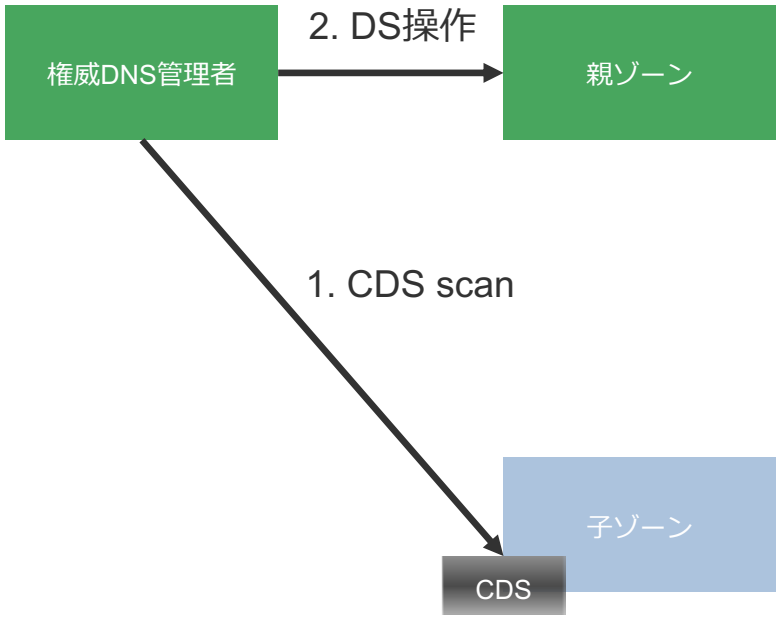
- 親ゾーン側の対応状況
    - レジストリの対応状況
    - レジストラの対応状況
    - 権威DNSの対応状況
- 子ゾーン側の対応状況
    - 権威DNSサービスの対応状況
    - 権威DNS製品の対応状況
- まとめ

親ゾーン側の対応状況

親ゾーン側の対応

親ゾーン側は、委任したサブドメインのゾーンに対応するCDSレコードをスキャンする。
スキャン結果に結果に基づいてDS RRSETの操作（追加、更新、削除）を行う。
一連の処理は、通常は親ゾーン管理者が実行する。

通常の例

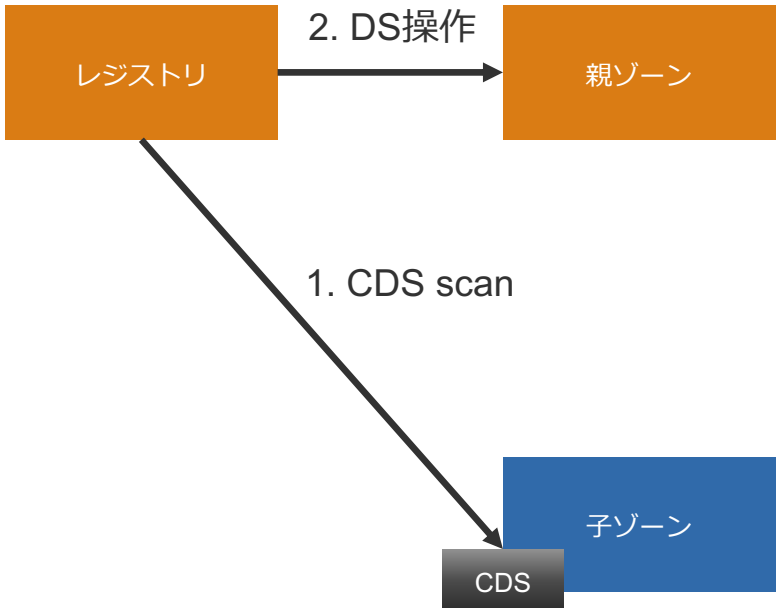


親ゾーン側の対応

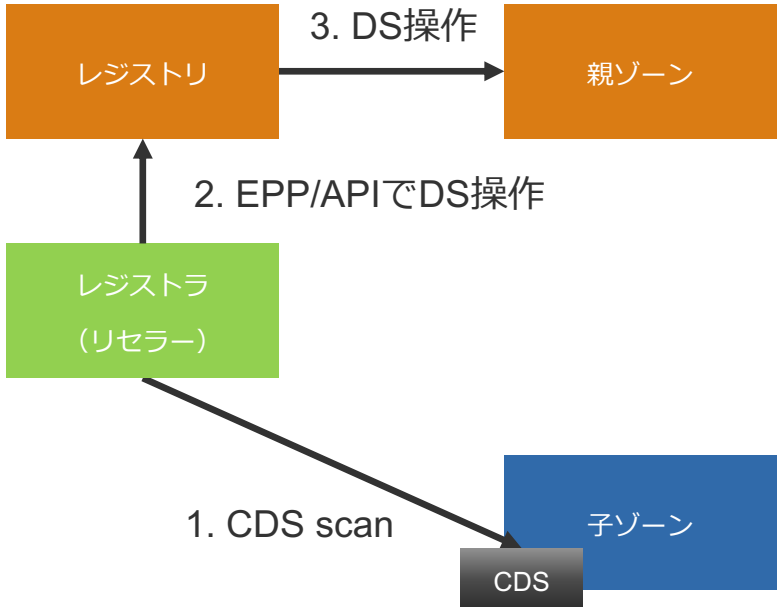
親ゾーン側がTLDの場合は２パターン

- 親ゾーンの管理者であるレジストリが実行
- レジストラが管理しているドメイン名を対象にスキャンを実行し、レジストリのAPIを利用して、DSの操作を実行

レジストリが対応する場合



レジストラが対応する場合



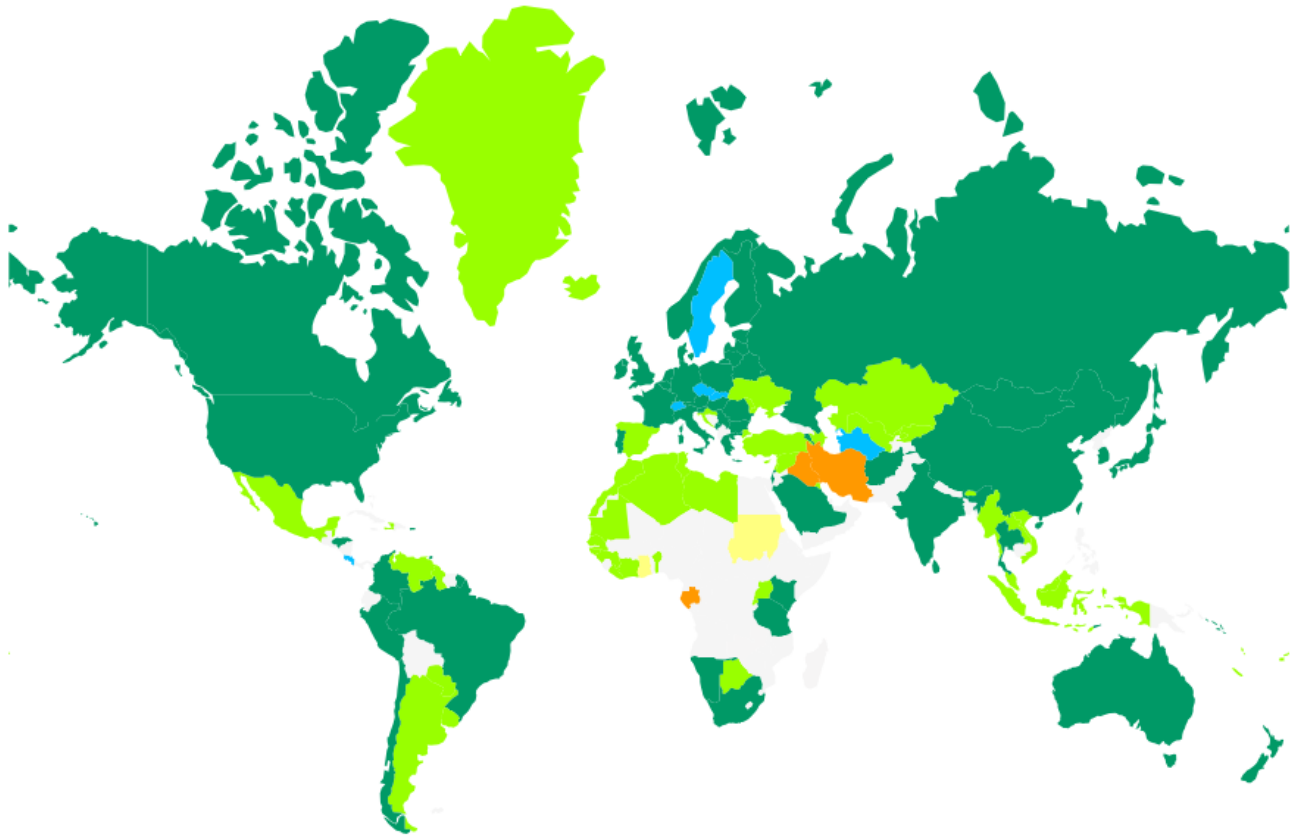
レジストリの対応状況

現在はヨーロッパを中心に8 ccTLD程度が対応

Select Region
World

Animate

2005 2023



General Statistics

Total ccTLD's

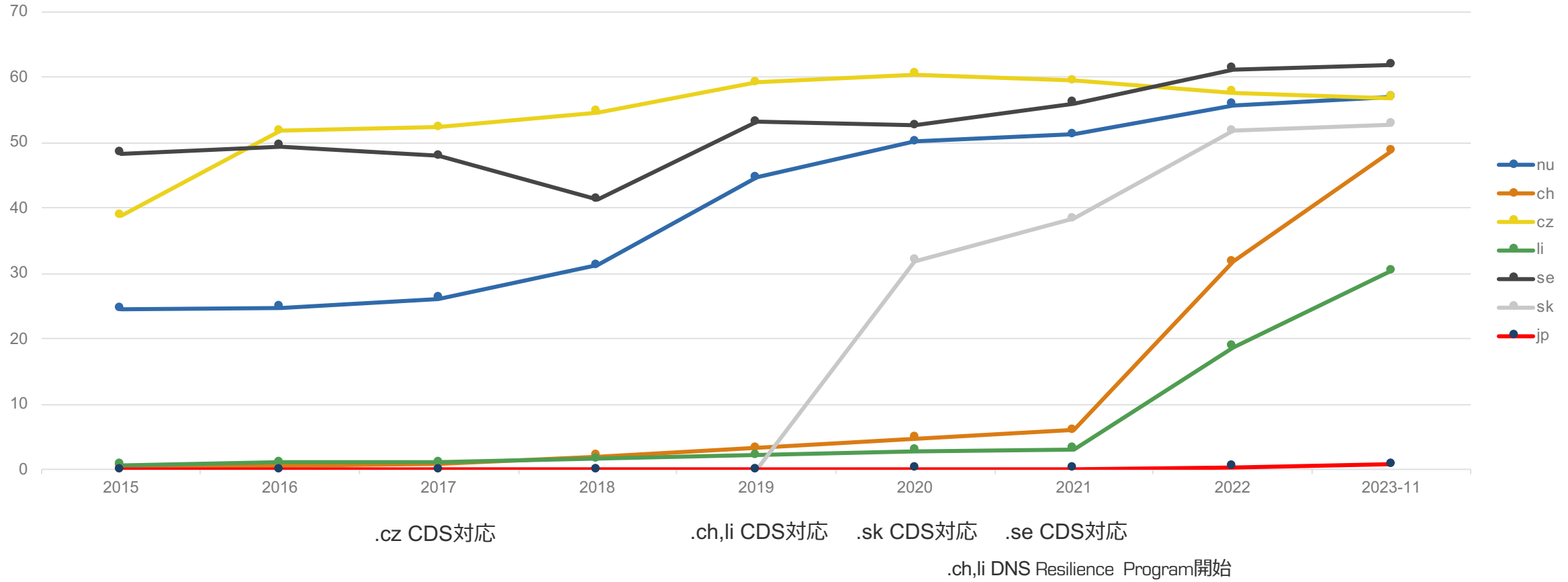
160

●	Experimental	8	5%
●	Announced	3	2%
●	Partial	0	0%
●	DS in Root	69	43%
●	Operational	70	44%
●	DS Automation	8	5%

出典元: https://maps.dnssec.gmu.edu/

対応レジストリのDNSSEC対応率

対応している8 TLDのうち、統計が取れた6TLD+JPのDNSSECの対応率



ここ5年では.sk, .ch, .liの伸びが大きい
.skに関しては、ICANN76の発表で明確にCDSの効果があった報告が上がっている

※ 年毎のデータになります。TLDによって取得できる時期が異なるため、縦軸は一致しません。ソースは末尾に掲載

レジストラの対応状況

著名なレジストラサービスでCDS対応しているサービスを調査した

Namecheep
- https://domainname.shop/faq?id=395&section=7

Cloudflare
- https://blog.cloudflare.com/one-click-dnssec-with-cloudflare-registrar/

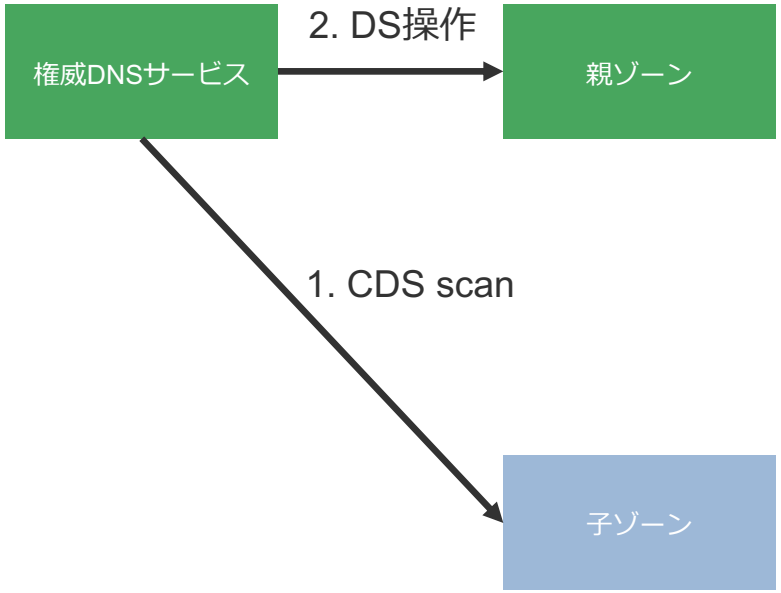
IIJ
- https://manual.iij.jp/dns/domain-help/19634186.html

他に最大手のGoDaddyが対応を表明しており、現在実装中のステータス

権威DNS

親ゾーンの機能に対応した権威DNSサービスはIIJ DNSプラットフォームサービスのみと思われる（他が見つからなかった）

また、オンプレで利用されるソフトウェア、アプライアンスなどでも対応例はない

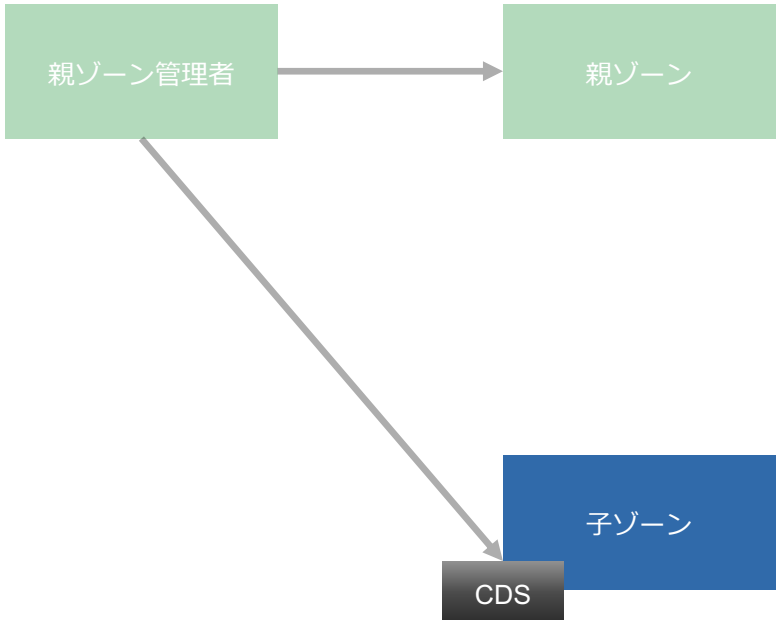


子ゾーン側の対応状況

子ゾーン側の対応内容

DS操作に基づいてCDSレコードを公開する

CDSでの対応

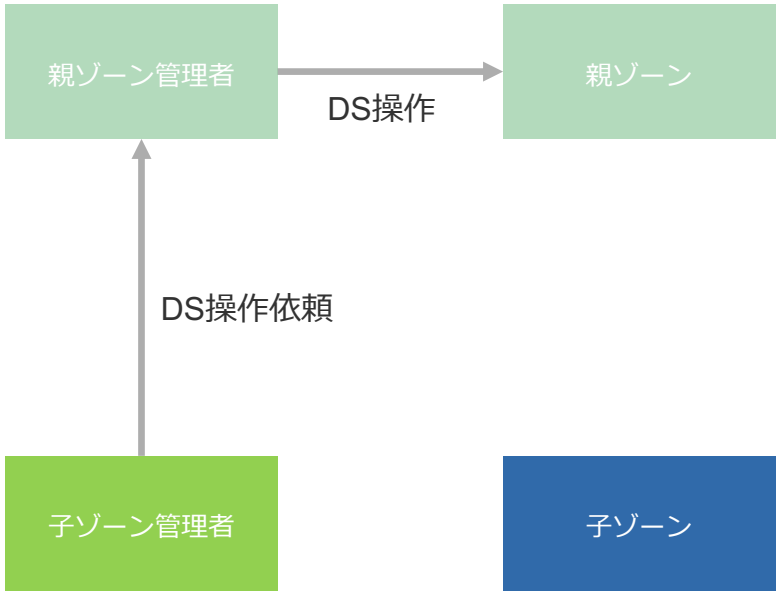


CDSレコードを公開するだけ

従来のDS操作の対応方法

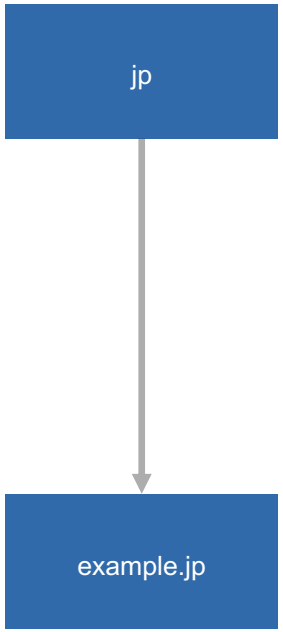
子から親ゾーンにあるDSを更新するのは、DNSSECを勉強した人なら直感的だとおもうが、それを自動化しようとすると非常に難しい

親ゾーン管理者にDS操作を依頼する



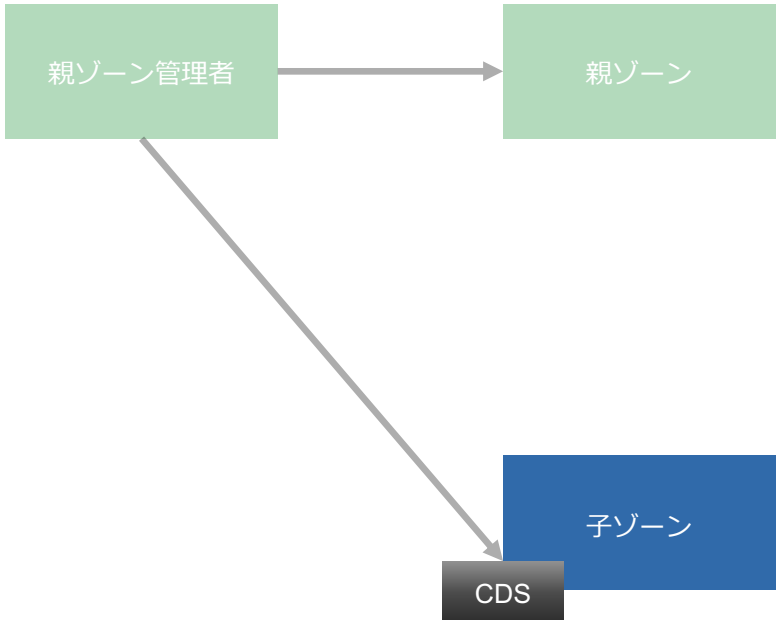
子ゾーン側が依頼方法実装する必要があった

委任されているかどうか



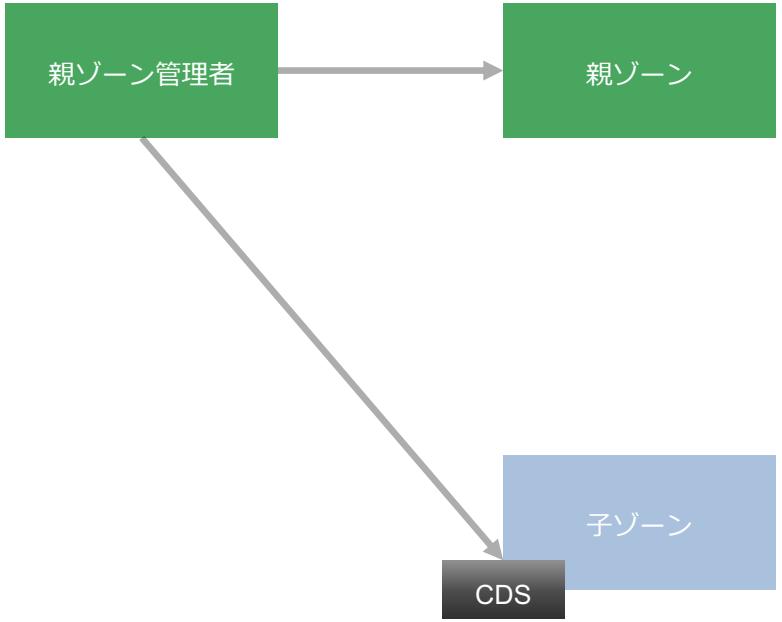
委任されていなければ、DS操作を
依頼してはいけない

CDS操作の対応方法



CDSレコードを公開するだけ

子側は親ゾーンのことを考えなくても良い



CDSレコードを名前解決=確実に委任されている

CDSレコードによる操作は、処理が一つのゾーンで完結し、かつ安全である

権威DNSサービスの対応状況

著名な権威DNSサービスでCDS対応しているサービスを調査

GoDaddy

DNSSimple

- https://support.dnsimple.com/articles/dnssec/#cdscdnskey

Cloudflare

- https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

deSEC

- https://desec.io/

IIJ DNSプラットフォームサービス

- https://manual.iij.jp/dpf/help/19630455.html

大手のDNSサービスでは対応されているところも有る。

クラウド系のDNSサービスでは対応されていない。（Azure DNSとかDNSSECも対応してない）

権威DNS製品の対応状況

機能の中にCDSを公開する機能が含まれるソフトウェアの調査結果

BIND9

- https://bind9.readthedocs.io/en/latest/dnssec-guide.html#cds-cdnskey

KnotDNS

- https://www.knot-dns.cz/docs/3.3/html/reference.html#policy-cds-cdnskey-publish

PowerDNS Authoritative Nameserver

- https://doc.powerdns.com/authoritative/guides/kskrollcdnskey.html

BIG-IP

- https://techdocs.f5.com/en-us/bigip-14-1-0/big-ip-dns-services-implementations/configuring-dnssec.html
- Defaultはdisable

他の対応状況と異なり、ほぼ対応完了している。

BIND9やknotがサポートされているため、親側(レジストリ、レジストラ)さえ対応すれば、

DNSSECの鍵管理の完全自動化は容易にできそう

まとめ

親ゾーン側

- 極少数のTLD、レジストラが対応しているにとどまる
- TLD以外の親ゾーンは、ほぼ対応していない

子ゾーン側

- 権威DNSサービス側は徐々に対応が進んでいっている状況
- オンプレで利用される権威DNSサーバ実装は対応完了している

現状はTLDと信頼の連鎖(DS)を繋ぐプロトコルとしての利用が進んでいる
子側の準備は整いつつあるため、TLD側が対応すれば、簡単に全自動でのDS操作が可能になります

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。

1. TLD毎の統計情報のソース

SE
https://internetstiftelsen.se/en/domains/domain-statistics/growth-se/
NU
https://internetstiftelsen.se/en/domains/domain-statistics/growth-nu/
CZ
https://stats.nic.cz/dashboard/en/DNSSEC.html
CH
https://www.nic.ch/statistics/dnssec/
LI
https://www.nic.li/statistics/dnssec/
JP
- InternetWeek2020 – 2023 JP DNS UPDATEより

（おまけ）IIJでの対応

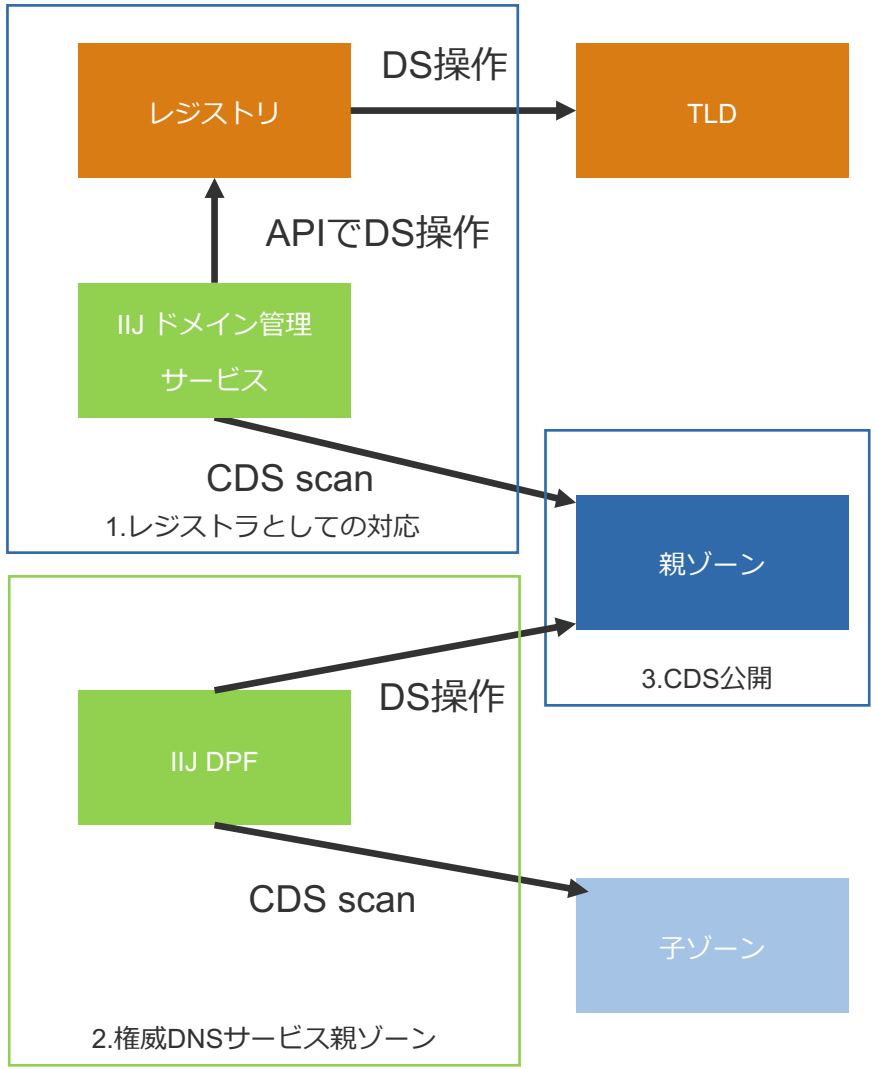
従来は権威DNSサービスとドメイン管理サービス間でシステム連携を行い、DS操作を行なっていた
2019年のIIJ DNSプラットフォームサービス(DPF)のリリースに合わせ、全面的にCDSベースに移行
(CDNSKEYは非対応)

親ゾーン側の対応

1. レジストラ（リセラー）として、顧客ドメイン名の対応
2. IIJ DNSプラットフォームサービスとして対応

子ゾーン側

3. IIJ DNSプラットフォームサービスで、CDSの公開処理を追加



CDSを採用した理由

子ゾーンがDNSSEC処理で親ゾーンにあるDS更新を直接行うのは直感的だが、実は非常に大変だったから

1. そもそも子ゾーンは委任されてるか

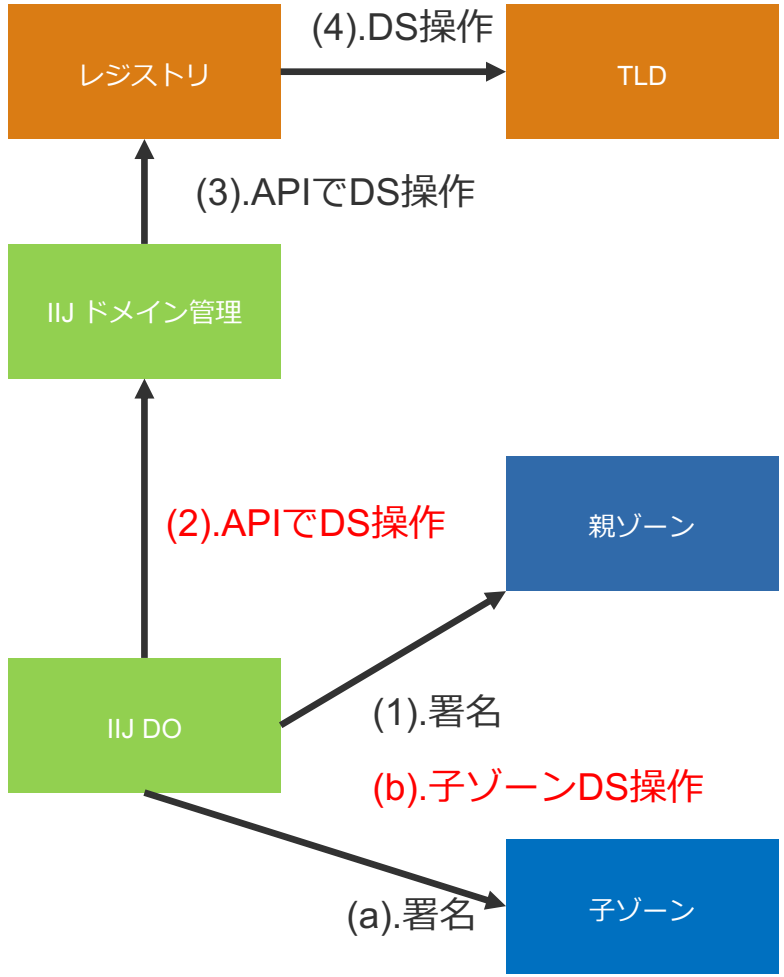
委任されてない子ゾーンの処理で、勝手に親ゾーンを書き換えを行うと事故になる。

2. 対象の親ゾーンとはどれか

親ゾーンが何かは委任によって変わるので、システム上、存在する親ゾーンが、必ずしも親じゃない場合もある。

3. 親ゾーン毎の更新処理を子ゾーン側で叩く必要がある

親がeTLDなのか、権威DNSサービスのゾーンなのかで分岐が発生する。また、種類が増える毎に処理が複雑化する。



CDSを採用した結果と課題

いまでは、CDSはIIJのDNSサービスにとって、なくてはならないものになっている

子ゾーンのDNSSEC対応が容易になった

- 子ゾーンは親が何かを意識する必要がなくなった。
- 親ゾーン側としてもCDS対応したことで、子ゾーンはCDSに対応していればDNSSEC対応可能に
  - 全く違う実装を子ゾーンに持ってきてもCDSに対応していればDS操作を自動化できるようになった
  - IIJ DNSトラフィックマネージメントサービスは、動的応答に対応した別のDNS実装を使っているが、CDS対応しているので容易にDNSSEC対応ができた

サービスの利用増に伴いスキャン対象が増加している

- 全ドメイン管理契約と、DPFのGlueNSを対象としてスキャンを実施している
- 契約者の増加に伴い処理時間が増加傾向にあるので、将来的にはスケールするスキャン処理実装が必要になりそう。

即時処理は苦手

- 一定間隔でスキャン実行している為、即時にDS操作を行うことが難しい
  - bootstrapはしょうがないが、DNSSEC有効時の処理が早くできない。
- CDSの更新を通知し受信する機能が求められる（次のRFCに期待）