押さえておきたい！基盤技術(2)
DNSの基本と最新動向

InternetWeek ショーケース in 広島

日本DNSオペレーターズグループ/株式会社インターネットイニシアティブ
其田 学

- **ドメイン名とは何かわかるようになる。**
  - ドメイン名について
  - ドメイン名登録に関わる組織

- **DNSの動きがわかるようになる。**
  - 登場人物がわかるようになる
    - 権威DNSサーバ、フルサービスリゾルバ、スタブリゾルバ
  - 分散管理の重要な仕組み、移譲がわかるようになる。

- **最新の動向を知る**
  - DNSのプライバシー問題
  - DNSSEC

主催イベントのご紹介 – DNS Summery Day

DNS Summer Day 2018

開催趣旨

インターネットの基盤技術の一つであるDNSは、重要性がますます高まっているにもかかわらず、その運用には十分な関心が払われておらず、また必要な予算や人材などもきちんと割り当てられているとは言えない状況が継続しています。

このようなDNSの状況に鑑みて、今年も引き続きDNSのイベントを開
いたしました。そして今年も協賛団体の方々にご登壇いただく予定で

終了後には、懇親会も開催いたします。

開催概要

名称	DNS Summer Day 2018
主催	日本DNSオペレーターズグループ (DNSOPS.JP)
日時	2018年6月27日 (水)
会場	〒100-0004 東京都千代田区大手町2-6-1 朝日生命大手町ビ フクラシア東京ステーション 5階 会議室H
参加費	無料
参加申込	必要ありません。直接会場にお越しください。
中継	当日の中継はありません。

https://dnsops.jp/event20180627.html

権威DNSサーバー脱自前運用のススメ

ライトニングトーク Part1

- 例の有償ソフトでDNS構築してみた
- ネット系だけど、非テック企業のDNS管理の実態
- 権威DNSサーバを作ってみよう

休憩

サービスセッション

休憩

ライトニングトーク Part2

- gTLD動向
- ID4me
- ED25519のすすめ
- 5分でわかるセキュアなローカルDNS

BIND ESVの変更 9.9から9.11へ

休憩

ドメイン名 ハイジャックされないために

休憩

DNSブロッキング

Manabu Sonoda
其田　学

株式会社インターネットイニシアティブ エンジニア
日本DNSオペレーターズグループ 幹事

経歴

- 某ISPでL1からL8までのフルスタックエンジニア
  - 本格的にDNSに取り組み始めたのは、ここで日本初のDNSSECのサービス開発から。
- 現在IIJ勤務
  - IIJの回線系フルリゾルバの設計、構築、運用
  - IIJのDNSアウトソーシング系サービスの権威DNS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（イマココ）

DNSの運用に軸足を置くネットワークエンジニアのつもりです。。

ドメイン名とは

ドメイン名＝インターネット上で使われるユニークな名前

例

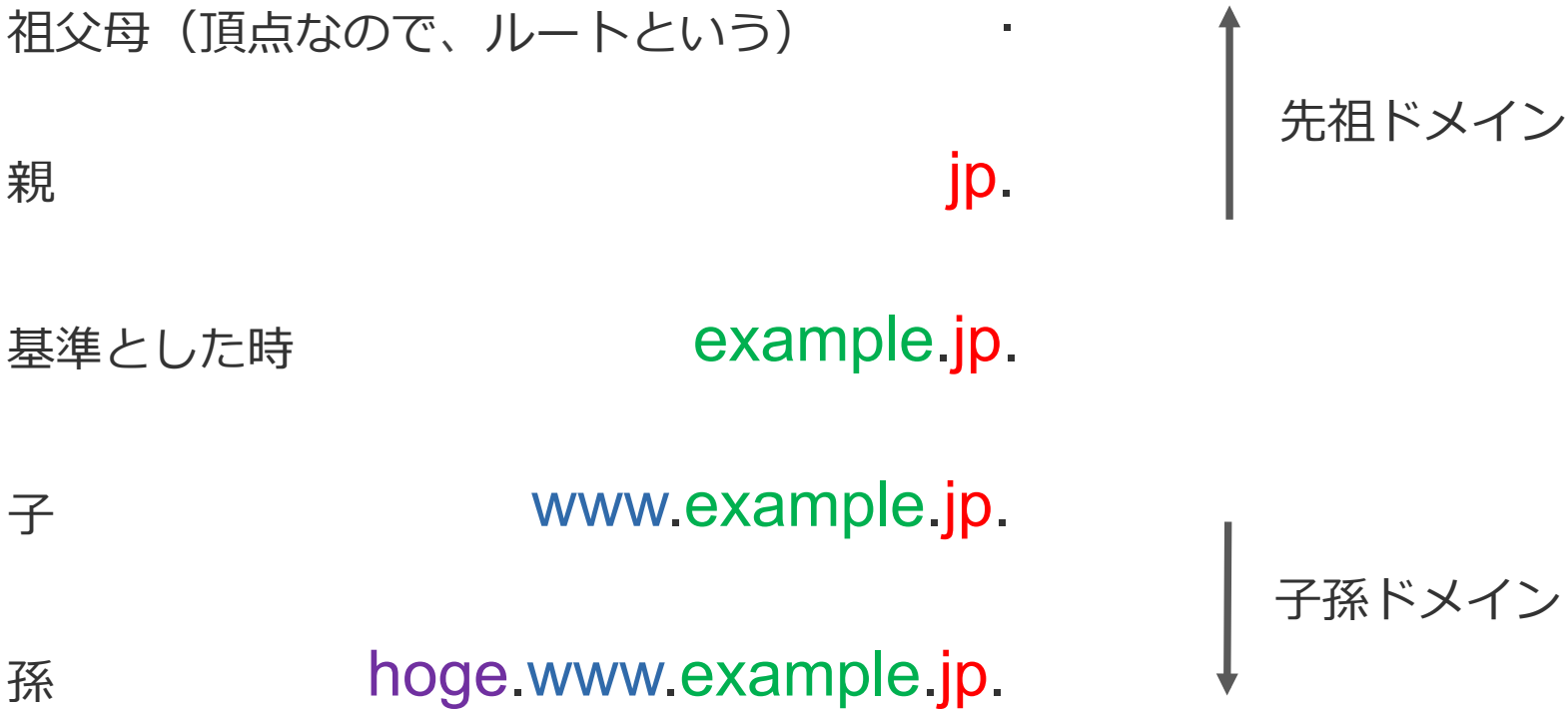
nic.ad.jp.
www.hiroshima-u.ac.jp.

※ユニークとは

例えば、田中太郎という名前は、複数人いる存在するため、ユニークではない。

一方、電話番号は、一般的に番号が重なることはないのでユニークである。

ドメイン名はドットで区切られた階層構造をしており、親子関係があります



全てのドメインの先祖ドメインをルートドメイン名と呼び通常はドットのみで表します。このドメイン名は何もないことを表します

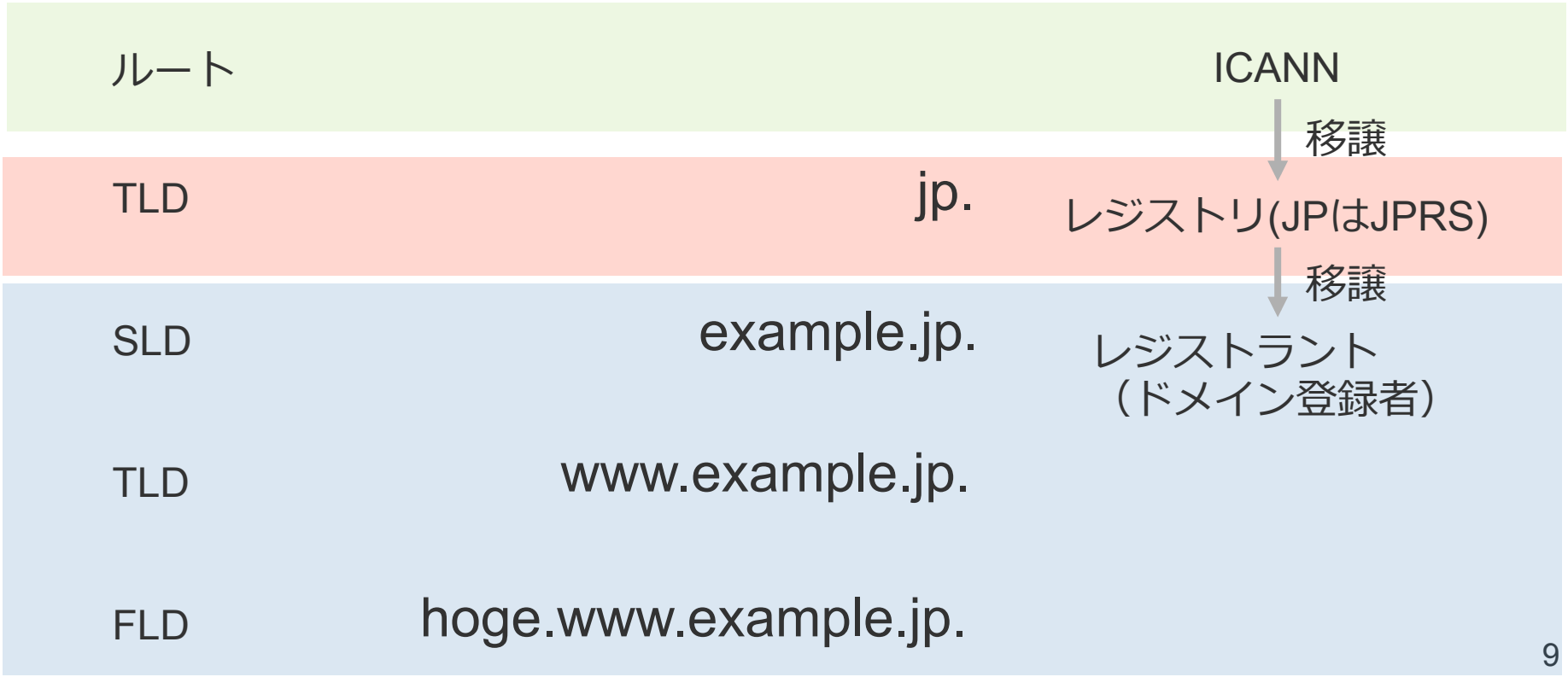
ドメイン名の管理は、管理するドメイン名と、その子孫の名前をゾーンという単位で管理し、ゾーンを一つの組織が一元管理することで、ユニークに保たれています。

しかし、これだと、ルートドメイン名の管理者が全てのドメイン名を一元管理することになります。

ルート	.
TLD	jp.
SLD	example.jp.
TLD	www.example.jp.
FLD	hoge.www.example.jp.

そこで、移譲したい子孫ドメイン名とその子孫の管理を移譲することで、分散して管理できるようにしました。

こうすることで、インターネットの爆発的な発展に伴う、ドメイン名の増加、管理コストの増加に対応しました



ドメイン名を登録したい場合、その親ドメイン名を管理している組織に対して登録を依頼します。

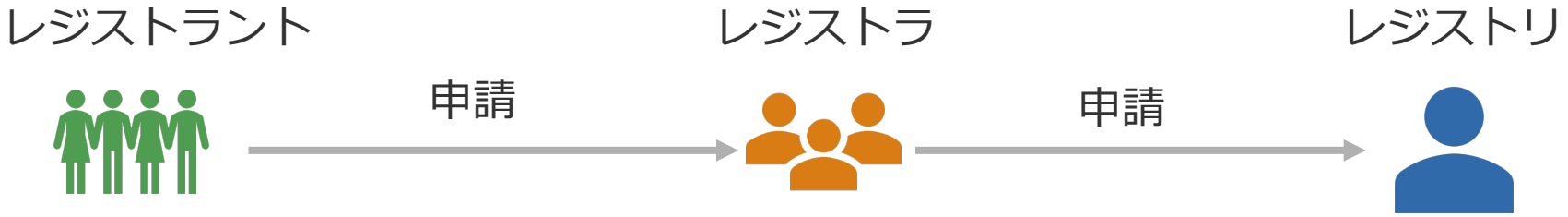
その種類は大きく３種類あります。

1. **登録したいドメイン名がTLDの場合**
   - TLD登録となり、ICANNに申請します。（ただし現在は募集停止中）
2. **ICANNから移譲されているドメイン名(TLD)のドメイン名**
   - 各ドメイン名のレジストリに対応したレジストラに依頼（詳細後述）
3. **そのほか**
   - ドメイン名を管理している組織に直接依頼
   - 企業などでサブドメインを追加したいときなどはこれ

TLDの子ドメイン名を登録したい場合、そのTLDを管理している組織に対して登録を依頼します。

しかし、レジストリと登録者だけしか存在しない場合、レジストリは１組織しかないため、レジストリの力関係が強くなってしまいます。

そのため、レジストラという取次をする組織を間に入に入ることで、取次間での競争が起き、レジストラで競争がはしる構造ができています。



ドメインを登録する
利用者

レジストラントと
レジストラを取次する組織

ドメイン名DBを
管理している組織

ドメイン名登録は、有効期限があります。

登録者は、有効期限前に更新することができます。

有効期間が過ぎると、ドメイン名は利用できなくなります。

さらに一定時間経つと、他の人の取得が可能になります。

[Domain Name] IIJ.JP

[登録者名] 株式会社 インターネットイニシアティブ

[Registrant] Internet Initiative Japan Inc.

[Name Server] dns-b.iij.ad.jp

[Name Server] dns-c.iij.ad.jp

[Signing Key] 6559 8 2 (

2DDCC6D2E218BB3B83EC03156AE676A6

0038708DC971EE4D8CEFF3BFFE7CE94F)

[登録年月日] 2001/03/26

[有効期限] 2019/03/31

現実的には、ある程度使用されているドメイン名の場合、一般に取得できるようになったタイミングで他者に取得されることが非常に多いです。

理由としては

1. ある程度WEBへのアクセスあるドメインの場合、それを利用して利益を得る目的
2. もともとの持ち主に高値で売りつけることを期待

１が様々な問題を引き起こしています。

最近の事例：

旧政府サイトのドメインを第三者が取得 - なりすましサイトを発信

過去に政府が利用したドメインが第三者に取得され、なりすましサイトが公開されていることがわかった。

問題のドメインは、2013年に観光庁が「タビカレ（日本タビカレッジ）プロジェクト」で利用したドメイン「tabicollege[.]jp」。

4月下旬に政府が、過去の事業で使用したドメインの使用状況について調査を実施したところ、同ドメインが現在も使用されていることが判明した。

国土交通省や観光庁を装い配信されている問題のサイト

引用元：http://www.security-next.com/093584

元の所有者のサイトになりすまして、オンラインカジノへ誘導していた

影響が少ない失効方法（WEBサイトドメイン名を想定）

1. A,AAAAレコードを全て削除します。
2. 検索エンジンのオプトアウトツールを使って、検索結果に出さないようにします。
3. その状態で３－５年ほど維持します。。。
4. もうそのドメイン名を欲しい人はいないはずです。

めんどくさいですよね
そもそも、そのドメイン名登録必要ありますか？

ドメイン名

- インターネット上のユニークな名前
- ルートを頂点とした階層構造をしている。
- 子孫ドメイン名とその子孫の名前の管理移譲することで、分散管理出来るようにしている。
- TLDの子ドメイン名の登録はレジストラ経由でレジストリに依頼する。
- ドメイン名登録には有効期限がある。
- 失効して一定時間経つと誰でも登録可能に
- 失効したドメインは場合によっては第３者に再取得され悪用されることも。。。

DNSの動きを知ろう

ドメイン名と、それに結びつく様々な資源情報（リソース）を提供するシステム

ほぼインターネット上で動く様々なプロトコル、サービスがDNSに依存しています

- WEB、メール
- ほぼ全てのインターネット通信をするアプリケーション
  - メッセージ系アプリ
  - オンラインゲームアプリ
  - 等

これらから、DNSはインターネット上で動くプロトコルの中で、最も重要なプロトコルの一つと言えます。

資源情報とは、DNS自身の階層構造を成立させるためのもの、また、他のプロトコル向けに提供されるものがあります。

資源の例

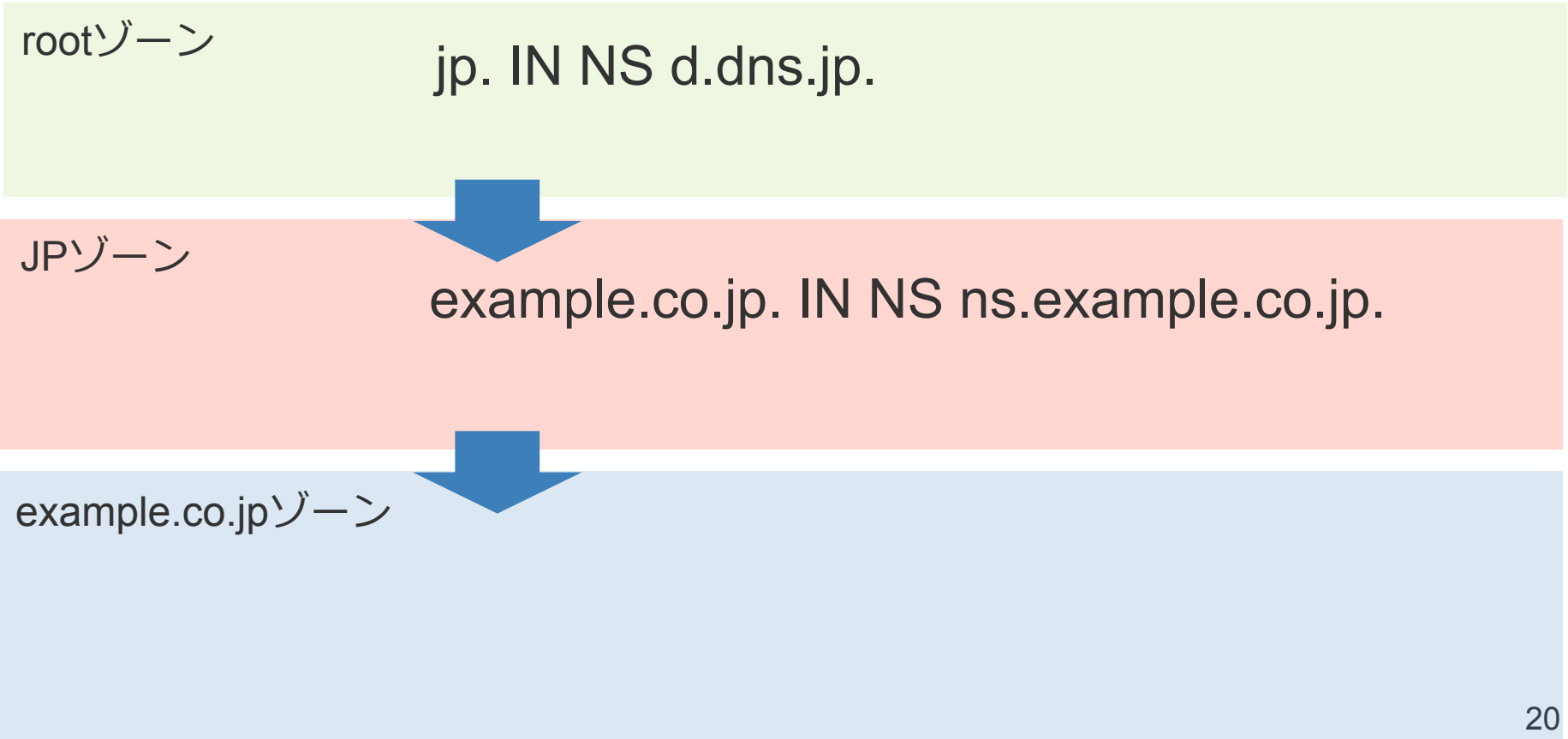
A	IPv4 アドレス
AAAA	IPv6 アドレス
NS	ネームサーバ情報
MX	メール送信先
TXT	メール送信認証系、その他いろいろ

これらを、名前と結びつけることができます。

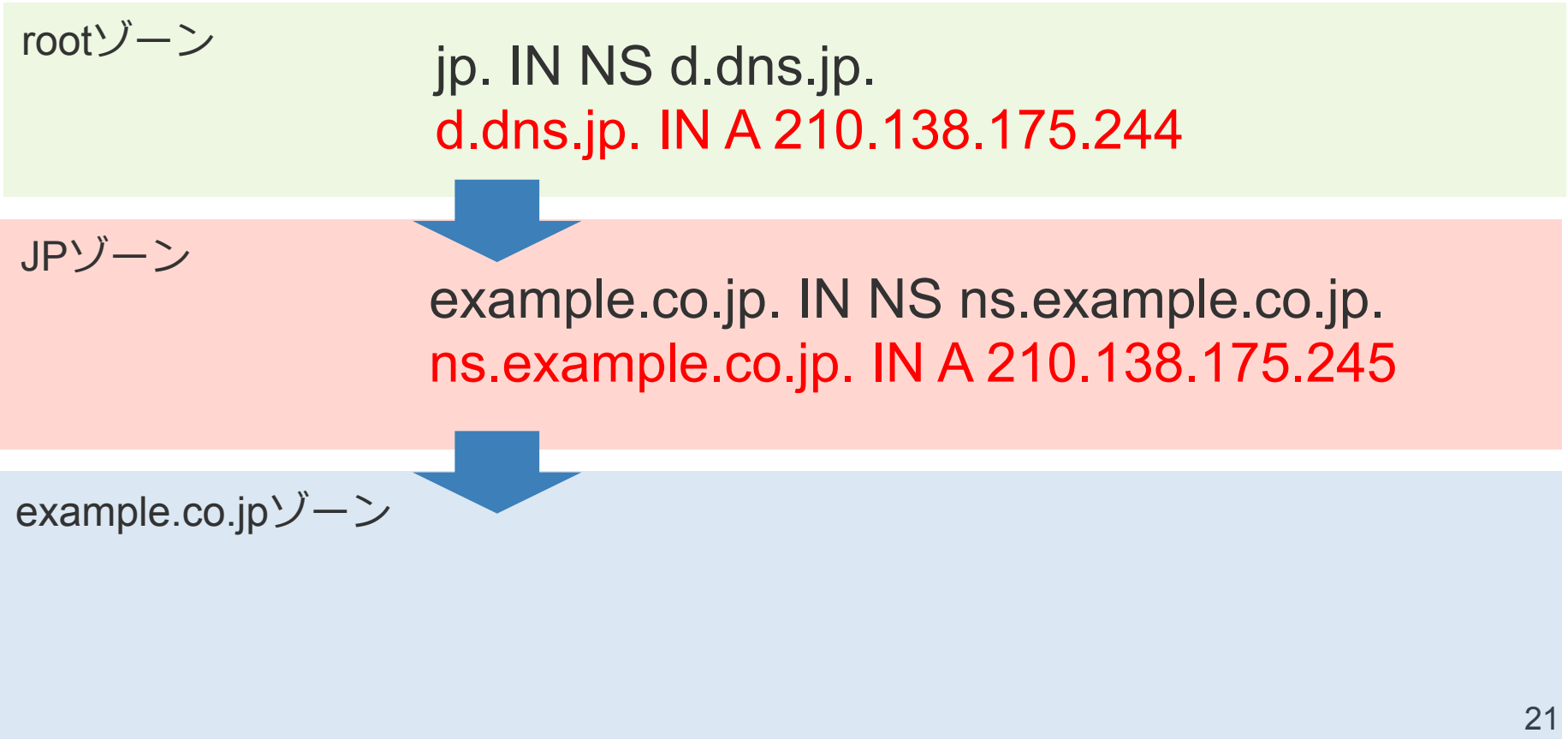
名前 name	TTL	クラス Class	資源の種類 RRTYPE	資源 RDATA
www.nic.ad.jp.	300	IN	A	192.41.192.145

この組みをリソースレコード、もしくは単にレコードと言います。

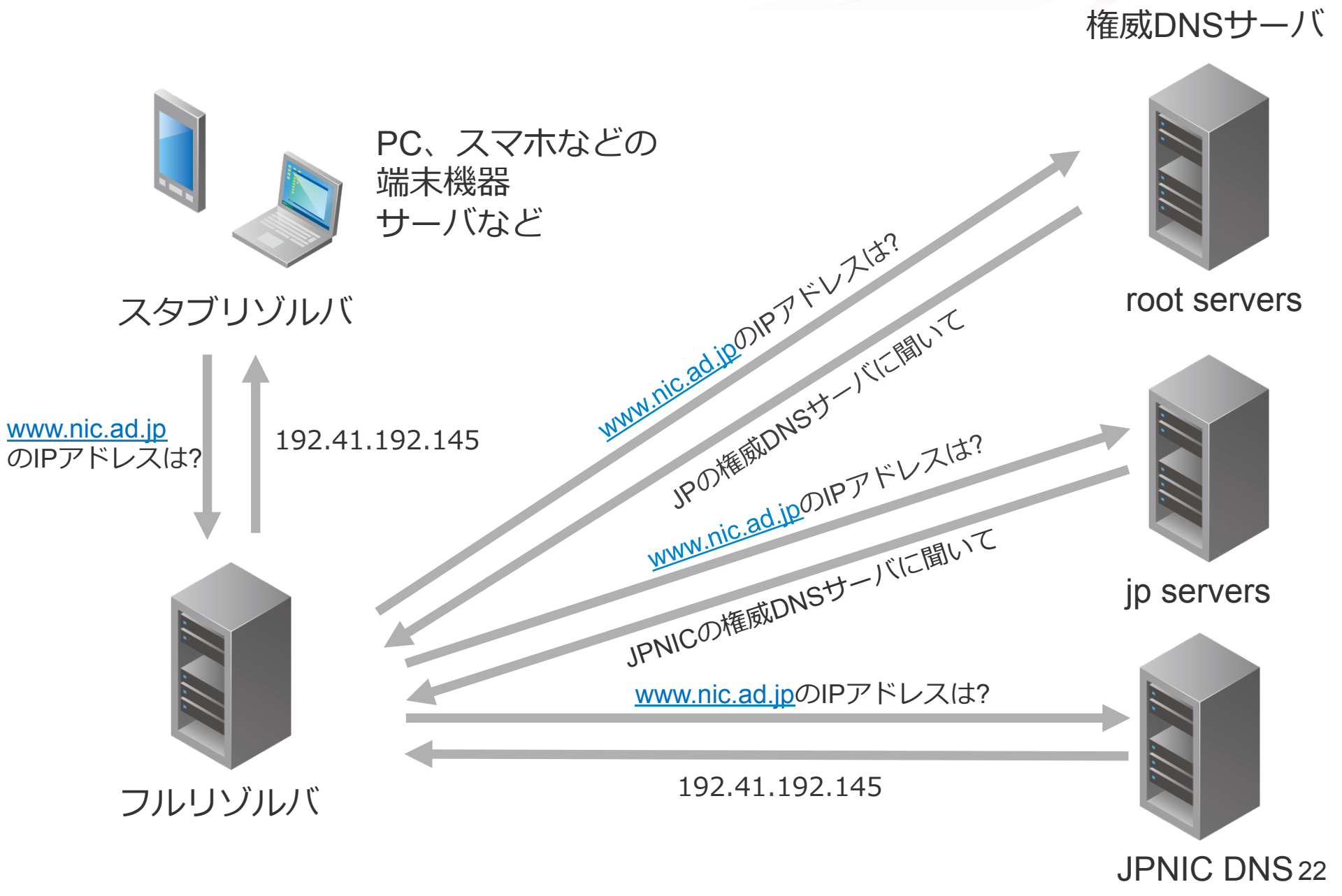
ドメイン名の移譲もゾーン単位です
ゾーンに、移譲したいドメイン名のNSレコードを
書くことで移譲します。



NSのホスト名が移譲した名前の子孫の時は
そのA、AAAAレコードを追加します。
これらをglueレコード**と呼びます。**



DNSの動き


権威DNSサーバ
PC、スマホなどの
端末機器
サーバなど
スタブリゾルバ
root servers
www.nic.ad.jp
のIPアドレスは?
192.41.192.145
www.nic.ad.jpのIPアドレスは?
JPの権威DNSサーバに聞いて
www.nic.ad.jpのIPアドレスは?
JPNICの権威DNSサーバに聞いて
jp servers
www.nic.ad.jpのIPアドレスは?
192.41.192.145
フルリゾルバ
JPNIC DNS

権威DNSサーバ

- ゾーンを保持し、ドメイン名の資源情報を提供するサーバ
- ネームサーバとも言う。

フルリゾルバ

- スタブリゾルバからの問い合わせに対して、応答を返すサーバ。
- OSなどのネットワーク設定や、DHCPで降ってくるDNSサーバと言うのはフルサービスリゾルバのこと
- 始めにに問い合わせるルートゾーンを持っているルートDNSのIPアドレスを持っている。
  - http://www.internic.net/domain/named.root
- サーバ内に応答する情報がない場合、権威DNSサーバに対して問い合わせを行う。
- 通常、権威DNSサーバからの応答をキャッシュするので、一般的にはキャッシュDNSサーバと呼ばれる。

スタブリゾルバ

- フルサービスリゾルバに対して問い合わせをする。
- PC、スマホなどインターネットに繋がっているほとんどの機器

登場人物

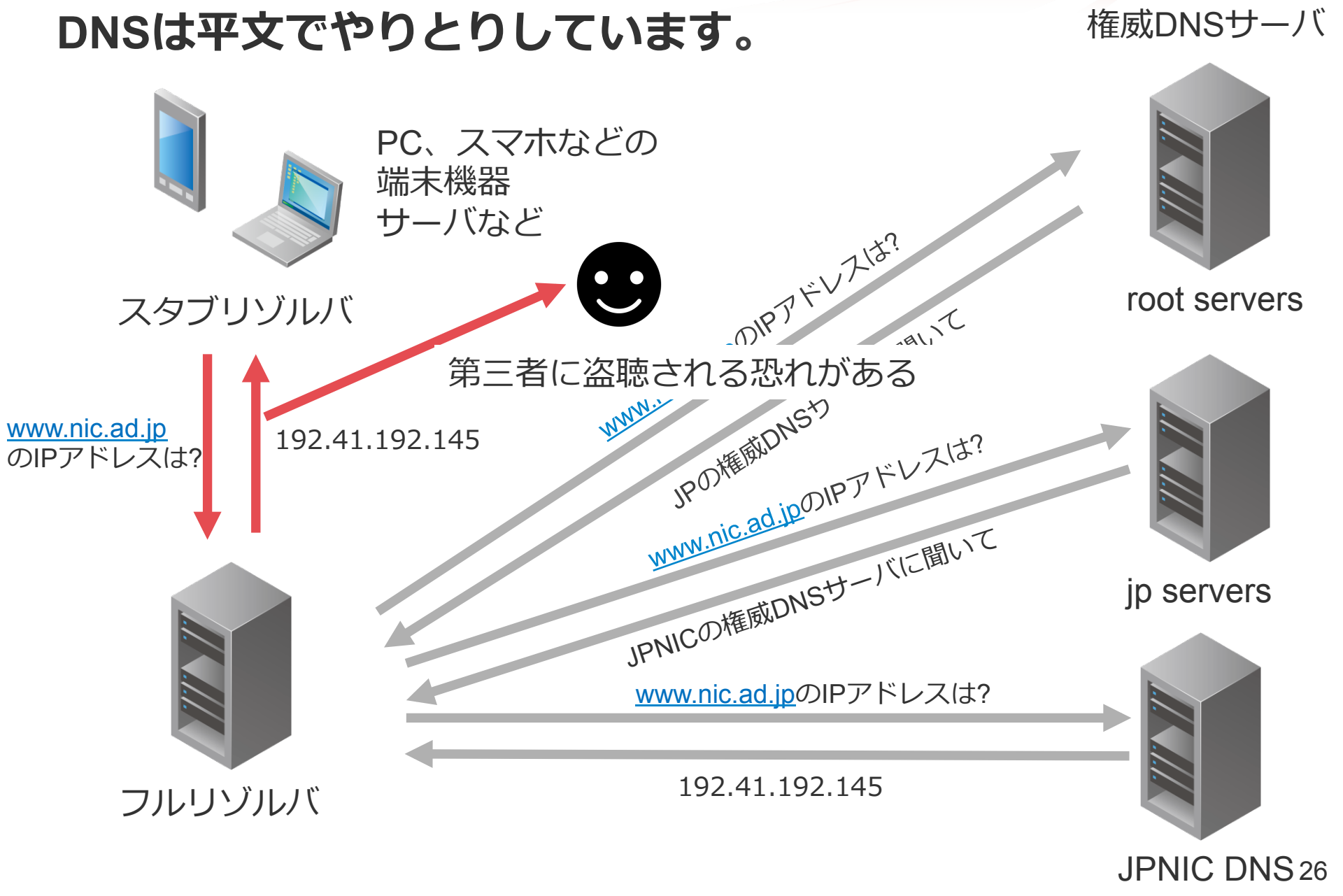
- 権威DNSサーバ
  - ゾーン情報を保持して答えてくれる。
- フルリゾルバ
  - スタブリゾルバに変わって、権威DNSサーバへ問い合わせをおこない、名前解決する。
- スタブリゾルバ
  - クライアント

移譲

- 親となるゾーンに、移譲する名前と、ホスト名をNSレコードを書くことで移譲する。
- 移譲先ホスト名が、移譲する名前の子孫の場合は親ドメイン名側にglueレコード（ホスト名のA、AAAAレコード）を追加する。

最新動向を知る１
DNSのプライバシー問題

DNSは平文でやりとりしています。



DNSの暗号化（スタブリゾルバとフルリゾルバ間の通信）

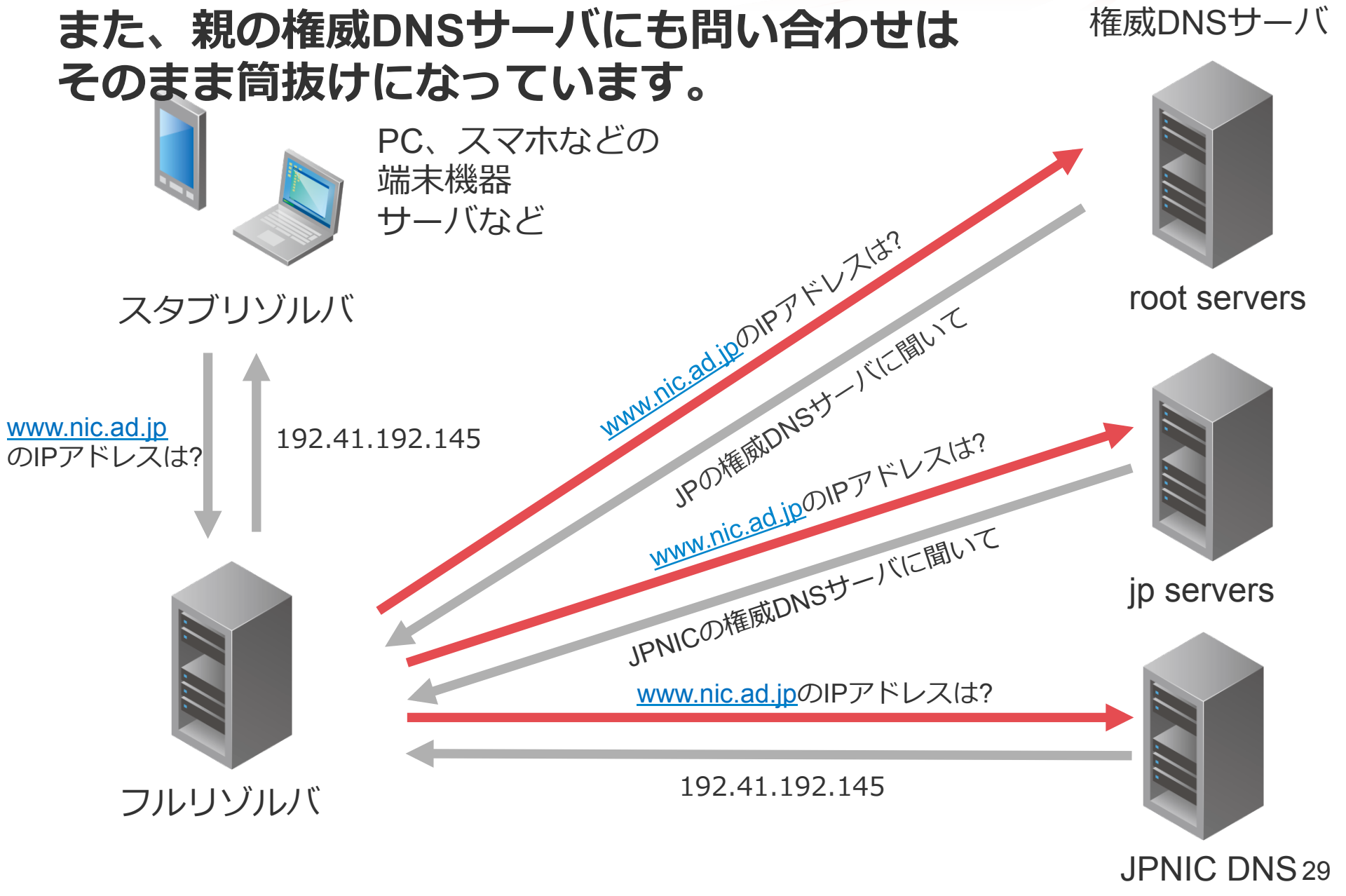
- DNS over TLS(RFC7858)
  - tcp port 853
  - httpからみたhttpsみたいなもの
  - 次期Androidから対応される模様
- DNS over DTLS(RFC8094)
  - udp port 853
  - UDP用のTLSで包んだもの

DNSの暗号化（スタブリゾルバとフルリゾルバ間の通信）

- DNS over HTTPS(draft-ietf-doh-dns-over-https-09)
  - DoHと略
  - 443番は通信が通りやすい！！
  - UDP形式のDNSのパケットをbase64urlでエンコードしたものをHTTPで包んだもの。。
  - Firefoxに試験的に実装
  - 将来的にはQUIC版も見越している感じ

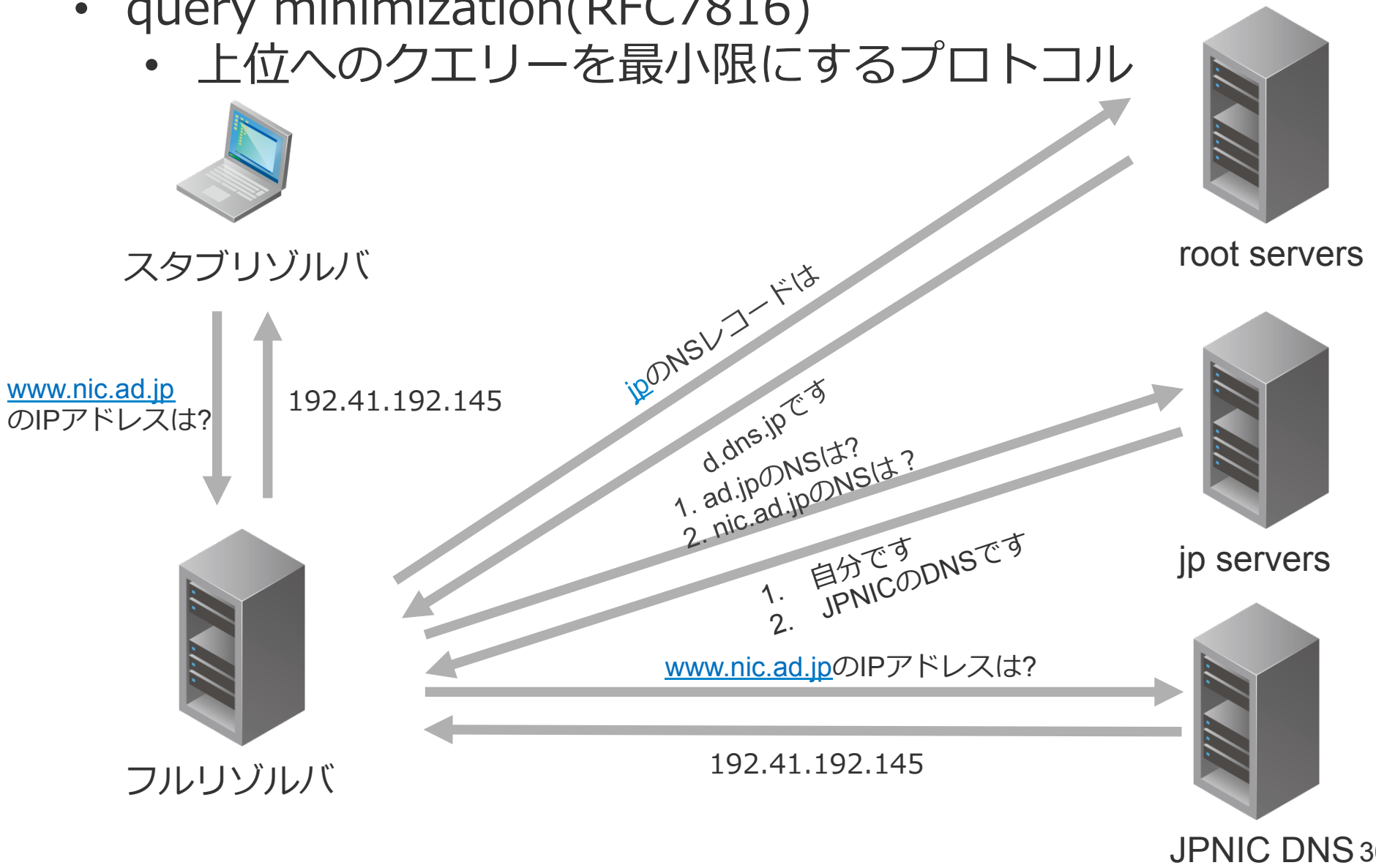
今すぐに普及するわけでは無いですが、OSベンダ、ブラウザベンダ次第で風は変わるかもしれないので注目が必要

また、親の権威DNSサーバにも問い合わせは そのまま筒抜けになっています。



上位に問い合わせが抜ける（フルリゾルバと権威DNS間）

- query minimization(RFC7816)
  - 上位へのクエリーを最小限にするプロトコル



query minimizationの実装

- Unbound
  - 実装済み
  - 次のバージョンからデフォルトON
- BIND9
  - 9.14以降に実装予定
- Knot-resolver
  - デフォルト実装

正直まだ全然枯れてないので、商用環境でONにするの勇気がいります。。

最新動向を知る２
DNSSEC

JPの署名からもうすぐ１０年
そろそろ普及が進みそうです

理由

- Googleの経路障害を受け、実際に日本の企業が経路障害によって被害を受けた。
- 経路に対しての攻撃が増え、実際に金銭的な被害が出ている。
- TLS証明書も、DNSが書き換え可能であれば発行可能な場合が多い

TLS＋DNSSEC+RPKIの複合防御で
対応していかなければならない

権威DNSのIPアドレスがルートハイジャックされ、不正なWEBサーバにリダイレクトされ、仮想通貨が盗まれた事例

AmazonのDNSトラフィック乗っ取り、仮想通貨盗まれる被害

AWSのクラウドベースのDNSサービスである「Route 53」のDNSトラフィックが何者かに乗っ取られ、「MyEtherWallet.com」のユーザーが仮想通貨を盗まれる事件が発生した。

2018年04月25日 09時00分 公開　　[鈴木聖子，ITmedia]

米Amazon Web Services（AWS）のDNSサービスで4月24日、トラフィックが一時的に不正なWebサイトにリダイレクトされ、仮想通貨Ethereumを扱うウォレットサービス「MyEtherWallet.com（MEW）」のユーザーが通貨を盗まれる被害に遭った。

MyEtherWallet.comは同日、DNS登録サーバが何者かに乗っ取られ、ユーザーがフィッシング詐欺サイトにリダイレクトされていたことを明らかにした。DNSサーバのリダイレクトには、古くからあるハッキングの手口が使われており、どんな組織であっても被害に遭う恐れがあると強調している。

引用元 http://www.itmedia.co.jp/enterprise/articles/1804/25/news063.html

RPKI+DNSSECによって守らなければならないと訴えてきた脅威がまさに現実化した

- DNSのプライバシー
  - スタブーフルリゾブバ間
    - 暗号化規格が乱立
    - OSやブラウザベンダ次第では急速に普及する可能性も。。。
  - フルリゾルバー権威DNS間
    - query minimization
    - まだ枯れてない

- DNSSEC
  - 実際の被害が発生し始めて、導入が加速中
  - 個人情報や金銭のやり取りが発生するドメイン名は対応を検討

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。

IIJ-BKLT999-0001