Internet Week
DNS Day – DNSSEC普及活動

JPCERT Coordination Center
Incident Response Group
中井尚子

JPCERT/CCとIRの紹介

JPCERT/CCとは

Japan Computer Emergency Response Team Coordination Center

インターネットを介して発生するコンピュータセキュリティインシデントの受付・調査・問題解決に向けて技術的な立場で支援を行う組織

インシデント レスポンス グループとは

- 国内・国外のセキュリティインシデントの調整
- 報告内容を理解し技術的な視点でコーディネーション

今回お話しする内容

1. DNSSECは必要なのか
2. 実際に起きたインシデント
3. DNSSECの現状
4. 今後のDNSSEC

DNSSECは必要なのか

JPCERT/CCにDNS攻撃の報告は届かない

- DNS関連の対応も実施
- DNSポイズニング攻撃などは内部観測では気付けない
- インターネットユーザは異変に気付けるだろうか

国外ではDNS攻撃を観測・回避できるようDNSSECを推奨している

- UK NCSC (英国)
- NCCIC/CISA (米国)

各国でのDNSSECに対する姿勢

UK NCSC（英国）

> UK NCSC advisory highlights further hijacking activity of Domain Name Systems, and provides mitigation advice.

- DNSハイジャックに関するコメントの中でDNSSECの必要性を言及 *1

NCCIC/CISA（米国）

- 2019年1月と7月の2度、DNSハイジャック攻撃が発生しているとコメント *2
- UK NCSCが公開したAdvisoryを支持

*1: https://www.ncsc.gov.uk/files/Advisory-DNS-hijacking.pdf (出典元：UK NCSC)
*2: https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign (出典元：US-CERT)
https://www.us-cert.gov/ncas/current-activity/2019/07/12/ncsc-releases-advisory-ongoing-dns-hijacking-campaign (出典元：US-CERT)

DNSを振り返る

役割

- 名前を解決する
- ホスト名とIPアドレスの紐づけ

重要性

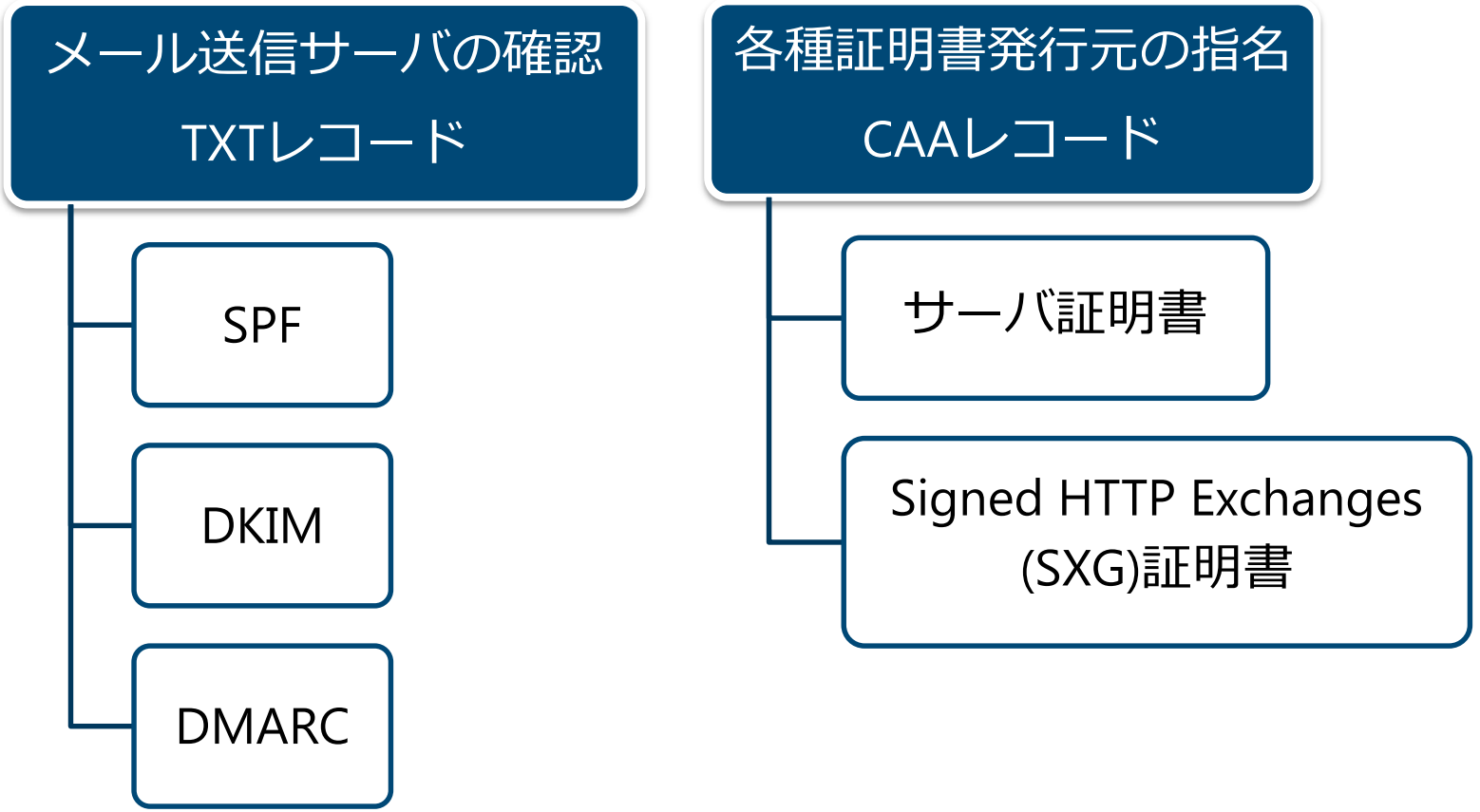
- インターネットの入り口
- インターネット上のサービスの利便性向上
- 広告塔としての用途

身近なDNS

- Public DNS
- ISPから提供されるCPE

DNSは、生活・事業を行う上で身近で大切なものである。

広範囲で使われるDNS



DNSの使い方 – インシデントレスポンス

■インシデントコーディネーション時に使うDNS

正引き

- ホスト名に紐づくIPアドレスを把握

逆引き

- 対象ホストの用途を把握
- 通信事業者のサービスを把握(法人向けか、一般ユーザ向けか)

得られた結果を基に、適切な連絡先、関連組織を把握し調整

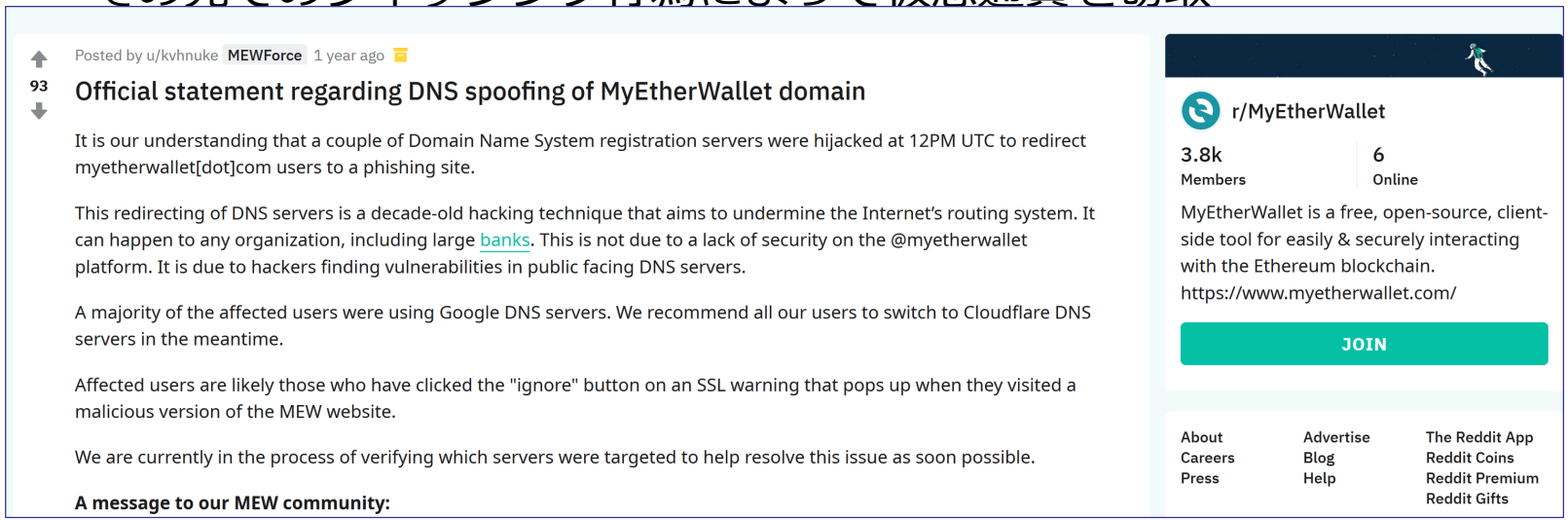
身近で大切なDNSが攻撃されたら

~実際に起きた事例を紹介~

1）仮想通貨を狙った攻撃事例
2）金融機関を狙った攻撃事例

1) 仮想通貨を狙った攻撃

- **仮想通貨を保管するサービス MyEtherWallet.com の権威DNSサーバが不正に建てられた**
  - 閲覧者を不正サイト(不正IPアドレス)に誘導
  - その先でのフィッシング行為によって仮想通貨を窃取



Posted by u/kvhnuke MEWForce 1 year ago

93

Official statement regarding DNS spoofing of MyEtherWallet domain

It is our understanding that a couple of Domain Name System registration servers were hijacked at 12PM UTC to redirect myetherwallet[dot]com users to a phishing site.

This redirecting of DNS servers is a decade-old hacking technique that aims to undermine the Internet's routing system. It can happen to any organization, including large banks. This is not due to a lack of security on the @myetherwallet platform. It is due to hackers finding vulnerabilities in public facing DNS servers.

A majority of the affected users were using Google DNS servers. We recommend all our users to switch to Cloudflare DNS servers in the meantime.

Affected users are likely those who have clicked the "ignore" button on an SSL warning that pops up when they visited a malicious version of the MEW website.

We are currently in the process of verifying which servers were targeted to help resolve this issue as soon possible.

A message to our MEW community:

r/MyEtherWallet

3.8k Members

6 Online

MyEtherWallet is a free, open-source, client-side tool for easily & securely interacting with the Ethereum blockchain.
https://www.myetherwallet.com/

JOIN

About Careers Press

Advertise Blog Help

The Reddit App Reddit Coins Reddit Premium Reddit Gifts

https://www.reddit.com/r/MyEtherWallet/comments/8eloo9/official_statement_regarding_dns_spoofing_of/ (出典元：Reddit Inc.)

インシデントの詳細

- 2018/4/24 UTC (約11:00 から13:00の2時間)
- 仮想通貨の窃取が目的のフィッシング攻撃
  1) BGP経路ハイジャックによりDNSクエリを偽権威DNSサーバに誘導
  2) 偽権威DNSサーバによってMyEtherWallet.com に対する悪意あるAレコードが返され偽サイトへ誘導

MyEtherWallet が行った対策

攻撃回避

- BGP経路ハイジャックは防げない

被害防止

- 正規な権威DNS応答であることの検証の環境

DNSSEC対応

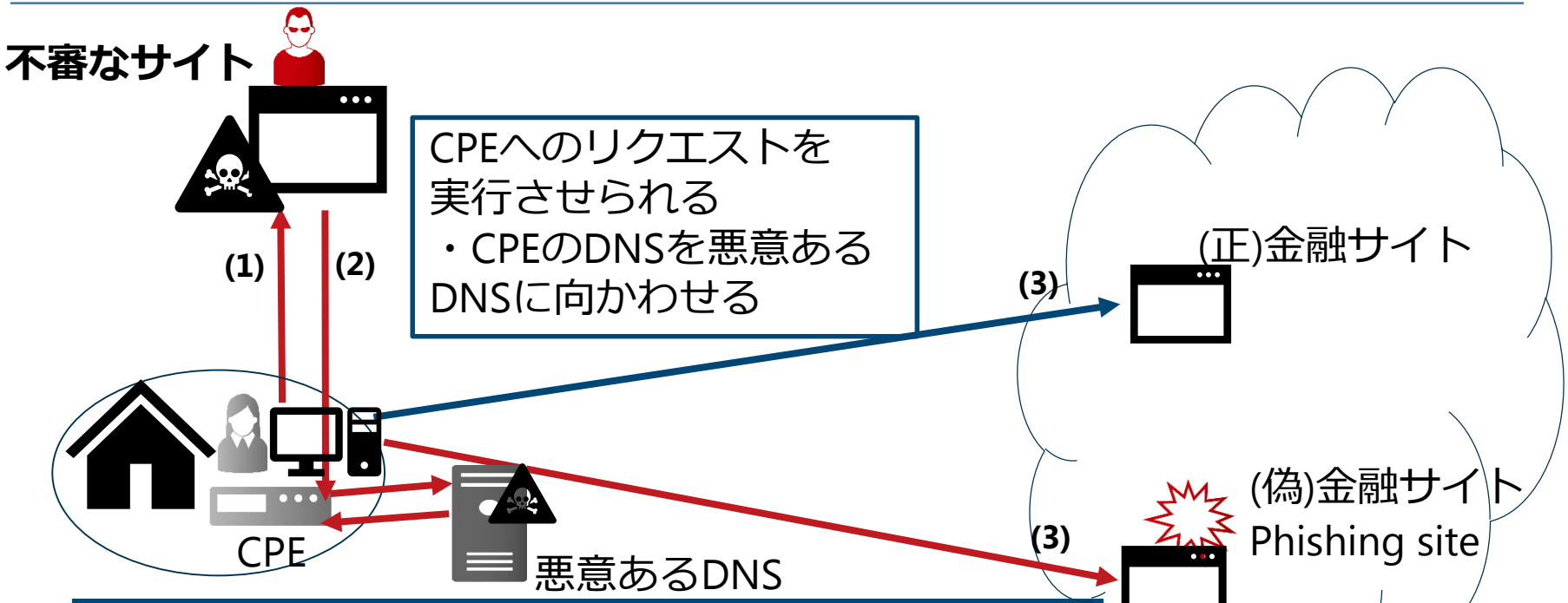
- DNSSEC対応可能なプロバイダにドメイン移管

2) 金融機関を狙った攻撃

- **ブラジル国内の金融機関を狙ったフィッシング攻撃**
  - —次に挙げた攻撃手法の組合せで行われた
  - 1）Cross-Site Request Forgery (CSRF)＋DNS ハイジャッキング
  - 2）脆弱性スキャン＋DNS ハイジャッキング
    - 攻撃対象はCPE

- **CSRFとは、ウェブサイトの脆弱性を利用した攻撃**
  - —攻撃者が用意した不審なサイトを閲覧させ、CPEに対して閲覧者が意図しないリクエストを実行させる。

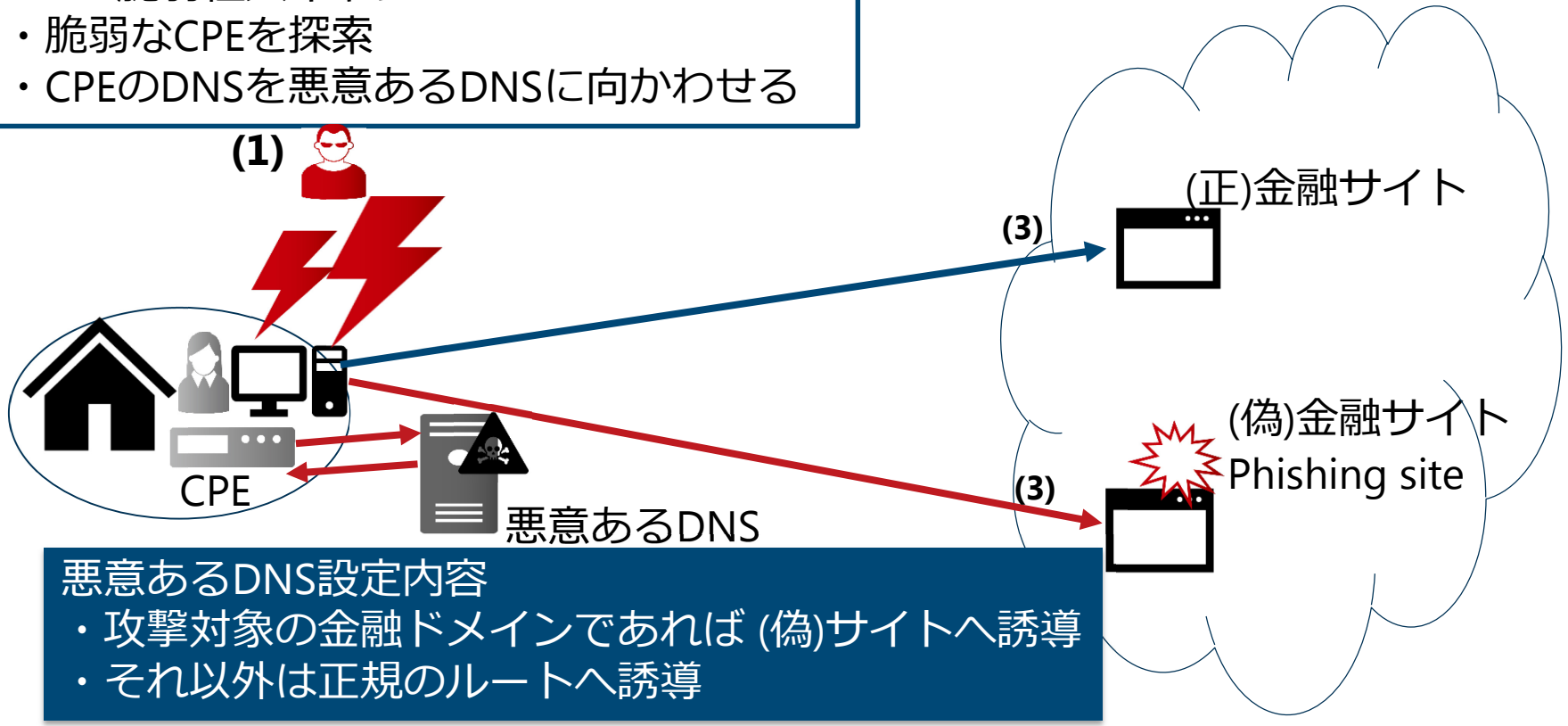
攻撃の流れ：CSRF + DNSハイジャッキング



悪意あるDNS設定内容
・攻撃対象の金融ドメインであれば (偽)サイトへ誘導
・それ以外は正規のルートへ誘導

攻撃の流れ：脆弱性スキャン＋DNSハイジャッキング

CPEの脆弱性スキャン
・脆弱なCPEを探索
・CPEのDNSを悪意あるDNSに向かわせる



悪意あるDNS設定内容
・攻撃対象の金融ドメインであれば (偽)サイトへ誘導
・それ以外は正規のルートへ誘導

金融機関で考えられる対策

DNSSECの有効化

- フルサービスリゾルバでのDNS応答パケットの正当性検証が可能

ウェブサーバにサーバ証明書の設置

- サービス利用者がサイトの正当性を確認できる状況を作る

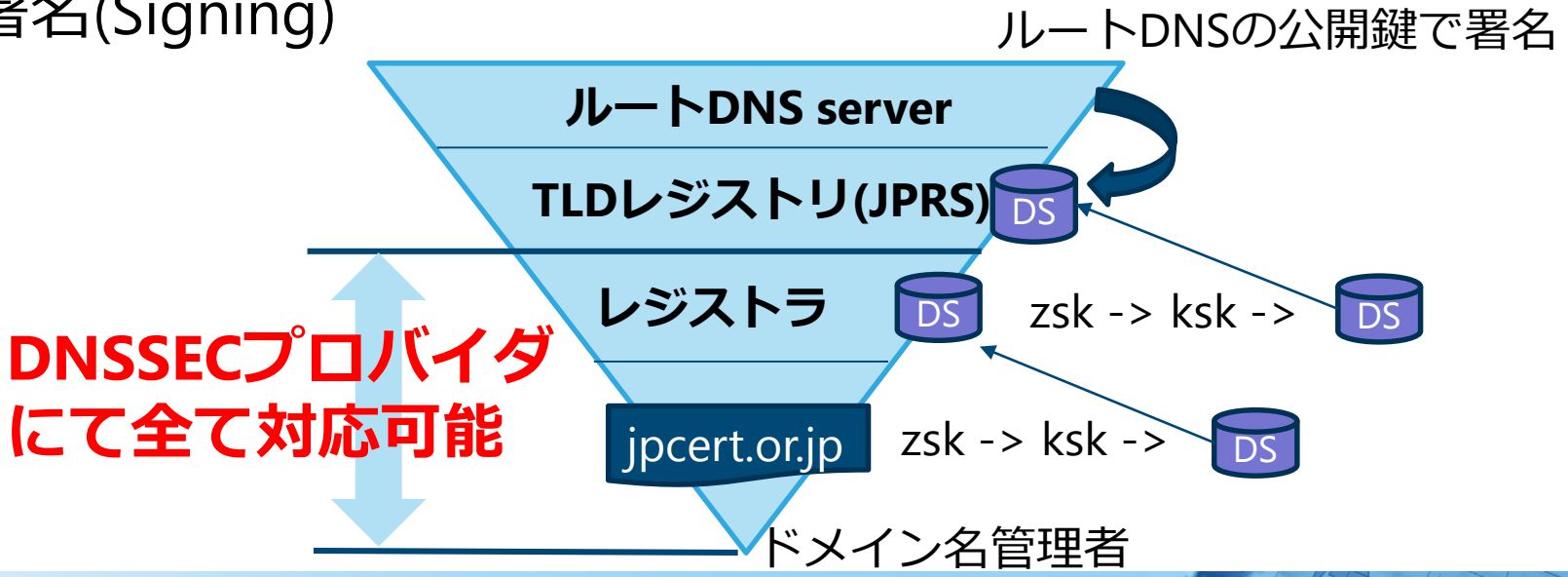
注意喚起

- サービス利用者向けの注意喚起
- フルサービスリゾルバ向けにDNSSEC検証の推奨

DNSSECの現状

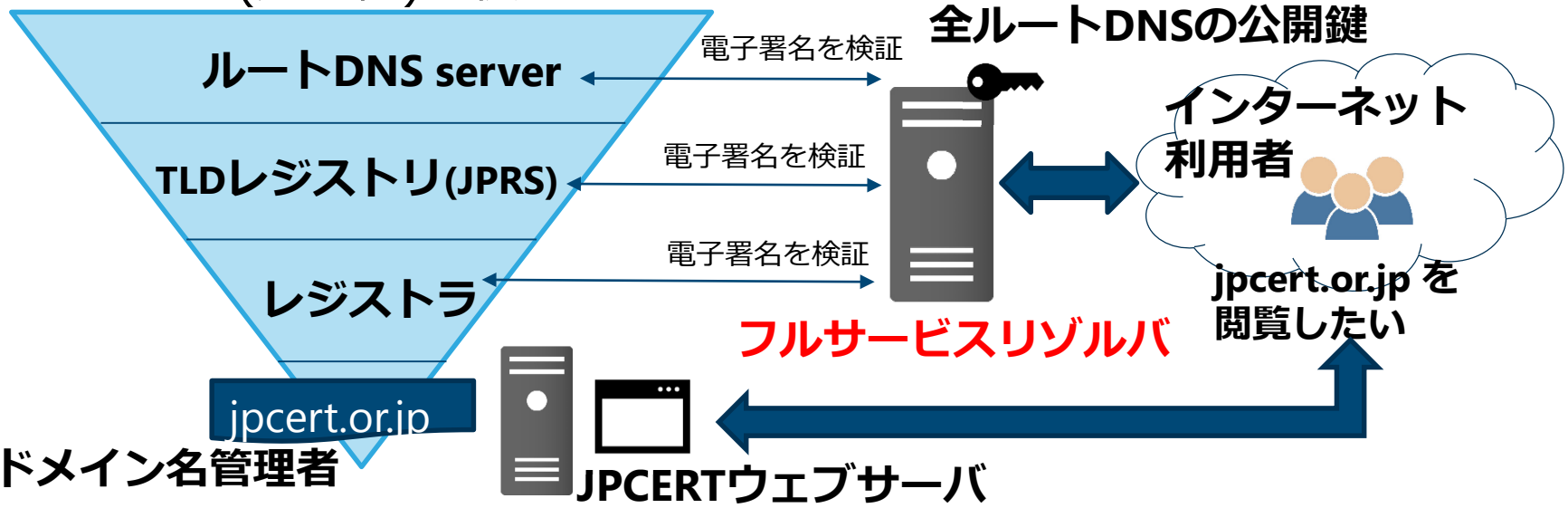
DNSSECのおさらい

- DNSSECを活かすには、次の2点が必要
  - 署名(Signing)
  - 検証(Validation)
- 署名(Signing)



検証(Validation)

- フルサービスリゾルバで実施
  - 応答パケットが正しい権威DNSからであること、改ざんされてないこと(完全性)の検証をする



- Public DNSでも検証実施

Public DNS

- Public DNSでDNSSECの検証は行われている
  - Google Public DNS
  - Cloudflare
  - IIJ Public DNS
  - Quad 101 (TWNIC)
  - など

Public DNSでDNSSECの検証結果

検証に失敗する例：　dnssec-failed.org

- **Google Public DNS**

```
dig A dnssec-failed.org @8.8.8.8

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 64614
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

- **Cloudflare**

```
dig A dnssec-failed.org @1.1.1.1

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 43563
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
```

- **Quad 101**

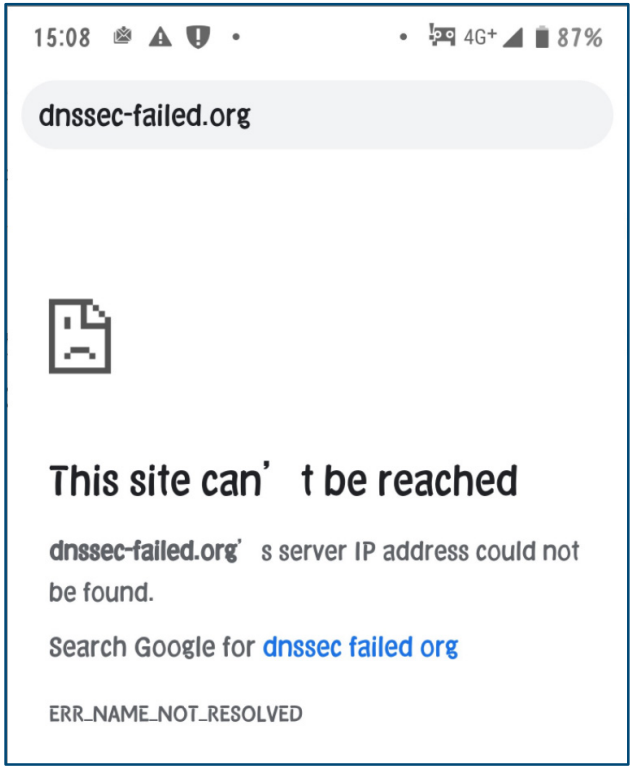
```
dig A dnssec-failed.org @101.101.101.101

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 5020
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

Public DNSでDNSSECの検証結果

検証に失敗する例：　dnssec-failed.org

- **IIJ Public DNS**

  — Android 9 で IIJ の説明
  にしたがって DNS の設定をして
  chrome で dnssec-failed.org
  にアクセスしたときのエラー画面



jpcert.or.jp のDNSSECの検証

Google Public DNS

```
dig A jpcert.or.jp @8.8.8.8

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7756
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

Cloudflare

```
dig A jpcert.or.jp @1.1.1.1

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54578
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

Quad 101

```
dig A jpcert.or.jp @101.101.101.101

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62664
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

今後のDNSの在り方

今後のDNS

- DNSSECという技術によってDNSの安全性は担保される
  - 信頼性や正当性の検証が可能となることで、DNSを認証の手段や他の機能に活かすことができる
    - CAA(Certification Authority Authorization)
    - DANE(DNS-Based Authentication of Named Entities)
    - など

まとめ

- DNSは生活・事業を行う上で重要で身近な機能
- 攻撃を気付ける環境の必要性
- DNSSEC署名検証の対応の拡大
- 安全性・正当性が担保されたDNSの重要な役割
- ユーザ保護の観点でDNSSECを検討ください