JPNIC総会講演会資料
2014年12月5日

# セキュアなDNS運用のために
# ～DNSSECの現状と課題～

株式会社日本レジストリサービス 松浦 孝康

# はじめに

## ■ 本講演の概要

- よりセキュアなDNS運用を実現するために、DNSSECの現状と課題と今後の展望について解説

## ■ 目次

1. DNSSECの導入背景
2. DNSSECの導入状況
3. DNSSECの課題と今後の展望
4. まとめ

# 1. DNSSECの導入背景

# 1. DNSSECの導入背景

- DNSSECで実現できること
  - DNS応答の出自の保証、完全性の保証
  - 応答の書き換えを検知、被害の拡大の防止

- DNSSECで守れること
  - Kaminsky型攻撃手法に加え、誕生日攻撃など検知が難しい攻撃手法に対しても効果を発揮する

DNSSECの導入がキャッシュポイズニング攻撃への有効な対策となる

# 1. DNSSECの導入背景

- Kaminsky型攻撃手法(2008年)
  - DNSSEC導入に至る大きなきっかけ
    - ✓より効率的なキャッシュポイズニング攻撃が可能になった
- DigiNotar事件(2011年)
  - 認証局(CA)の乗っ取りに加え、DNSの書き換えも実行
    - ✓不正発行したSSLサーバー証明書とDNSの書き換えの組み合わせ
- 新gTLD導入(2012年～)
  - DNSSECへの対応が必須要件の一つに
    - ✓DNSSEC対応がグローバルスタンダード化

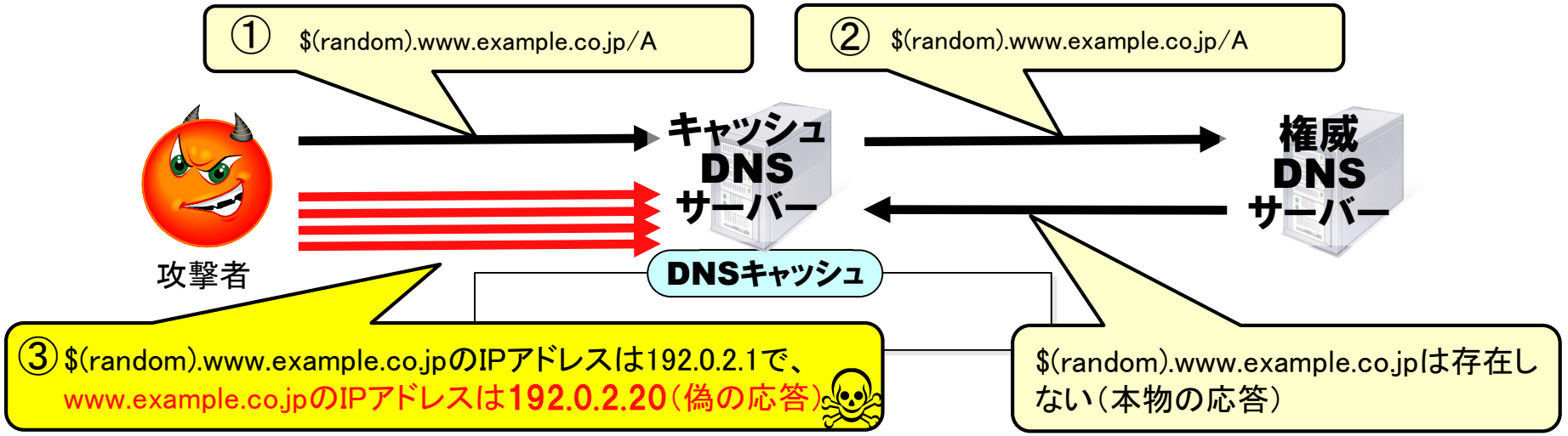
# 1. DNSSECの導入背景

## ■Kaminsky型攻撃手法

① 攻撃対象のドメイン名にランダムなサブドメインを付加した名前の問い合わせをキャッシュDNSサーバーに送る（ように仕向ける）

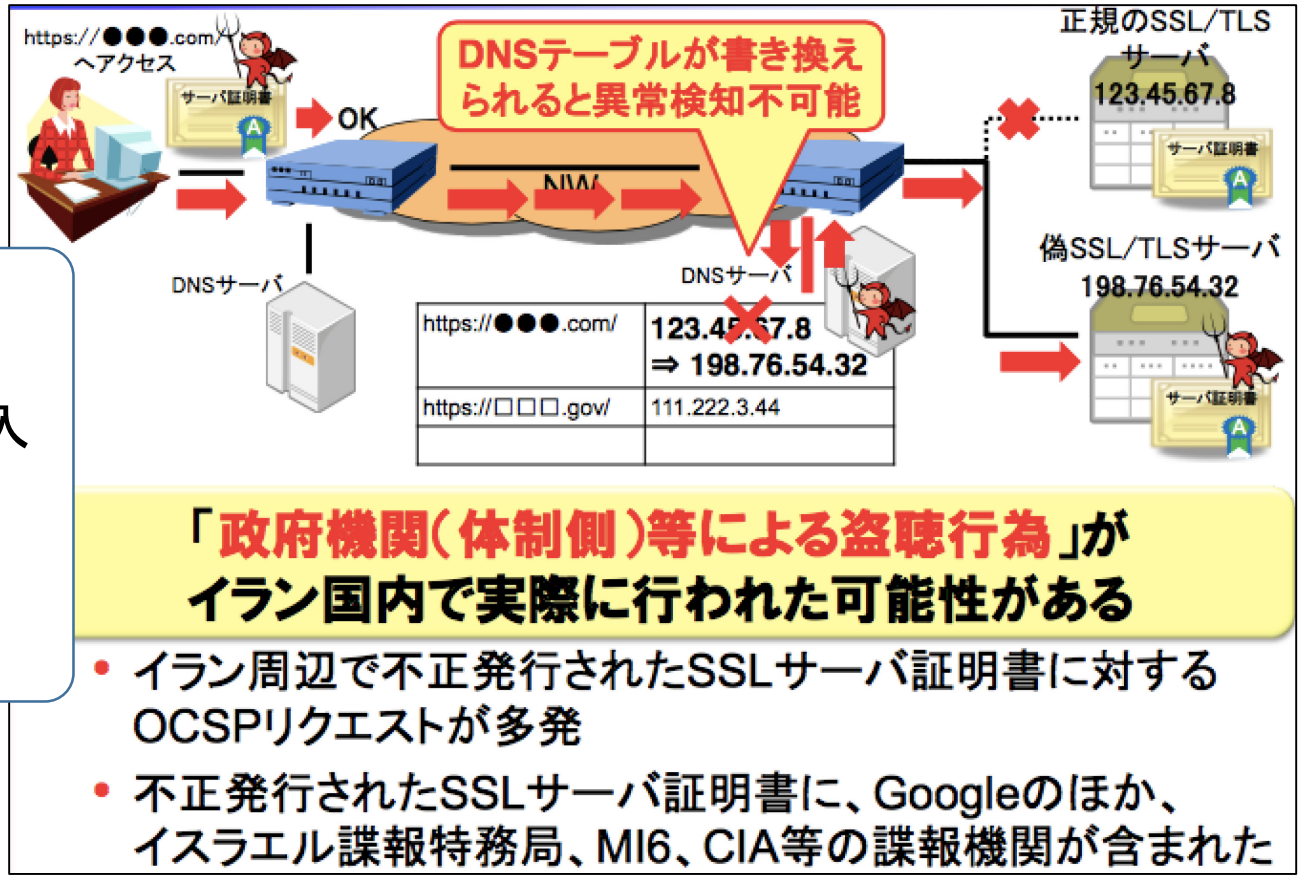
② キャッシュに存在しないため、キャッシュDNSサーバーは必ず権威DNSサーバーに同じ内容を問い合わせる

③ 問い合わせに対応する形で、攻撃対象へのアクセスに影響を与える内容を付け加えた偽の応答を問い合わせIDを変えながら連続で送りつける



# 1. DNSSECの導入背景

## ■Diginotar事件（2011年）




PKI Day 2012 IPA 神田雅透氏「サイバー攻撃ツールとしての公開鍵証明書の役割」より引用

### 攻撃手法の概要

(1) 認証局への不正侵入
(2) 証明書の不正発行
(3) DNS書き換え
(4) SSL通信の盗聴

# 1. DNSSECの導入背景

## ■新gTLDはDNSSECへの対応が必須要件

- ➢2012年より募集を開始
  - ✓DNSサーバーのDNSSEC対応はもちろん、EPP(ドメイン名の申請API)やWhois、Escrow等も対応必須
  - ✓自ドメインのDNSSEC運用の考え方をまとめたDNSSEC Practice Statement(DPS)を、ICANNへ提出することも必須
  - ✓上記に加え、新gTLDのDNSサーバーは復旧目標時間 4時間以内、レジストリシステムのディザスタリカバリ対応など厳しい要件と共にDNSSECを実装・運用する必要がある

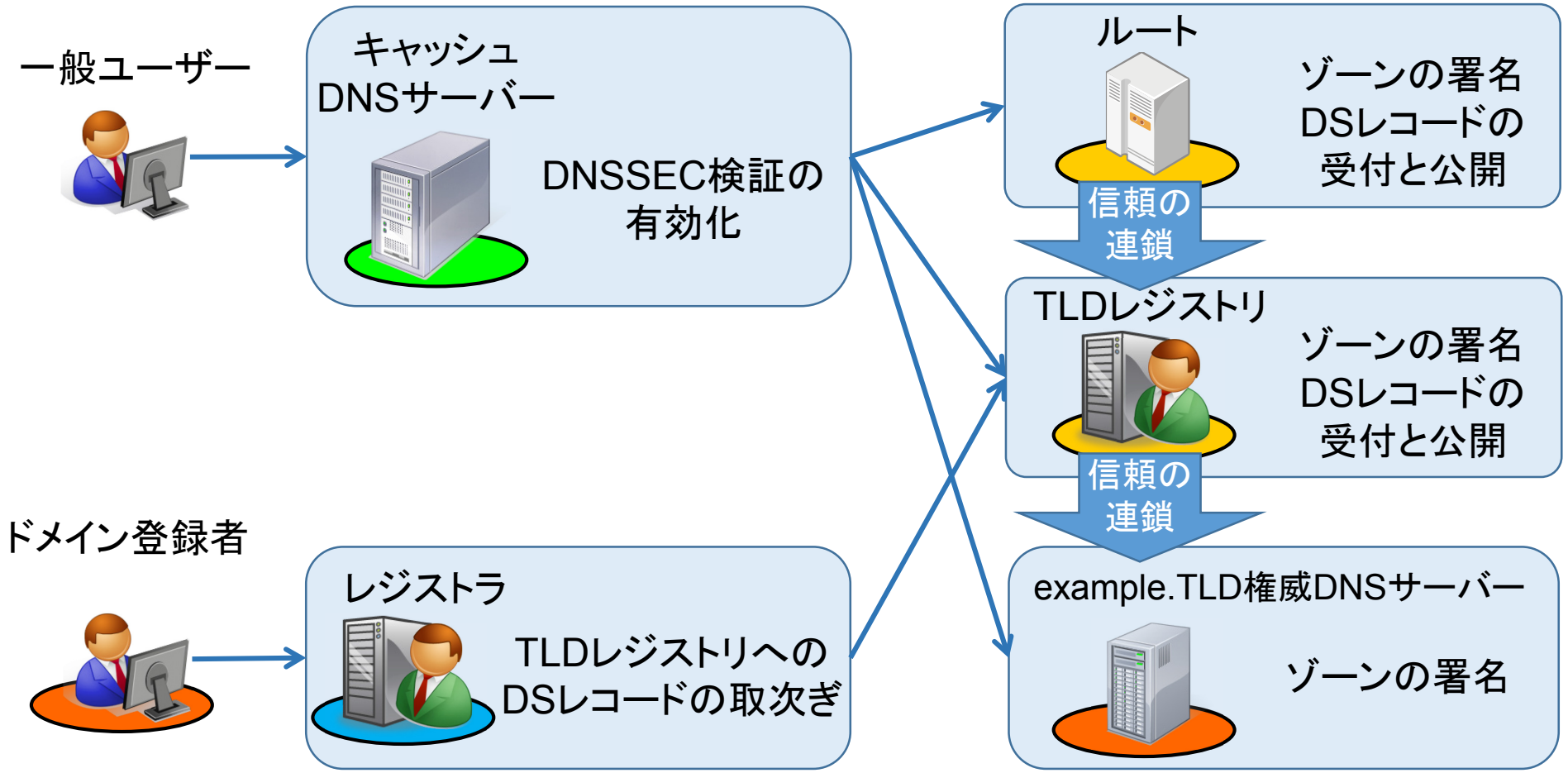
レジストリにおけるDNSSEC導入がグローバルスタンダード化

# 2. DNSSECの導入状況

# 2. DNSSECの導入状況

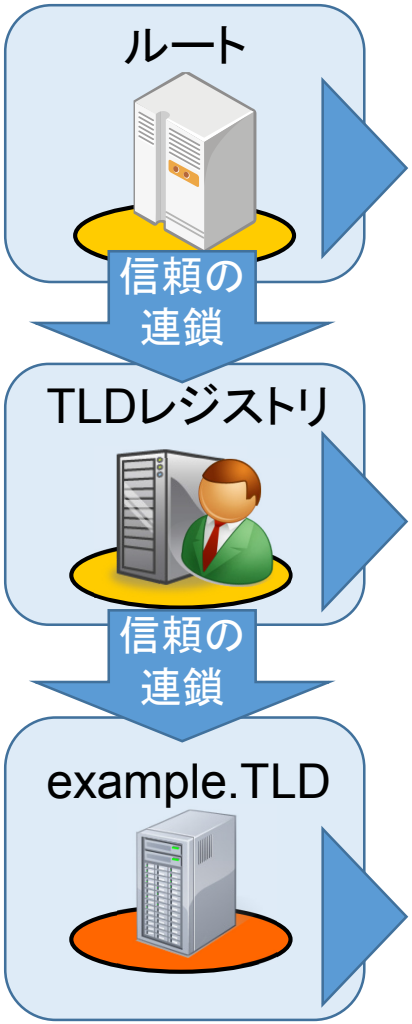
## ■一般ユーザがDNSSECを使えるようになるには

- 以下の登場人物がDNSSECに対応する必要がある



# 2. DNSSECの導入状況

## ■ 権威DNSサーバ側、レジストリ・レジストラの導入状況




2010年7月に正式サービス開始

566のTLDがDNSSEC導入済み（全体の75%、新gTLD含む）※1　JPは2011年に正式サービス開始

※1 http://stats.research.icann.org/dns/tld_report/

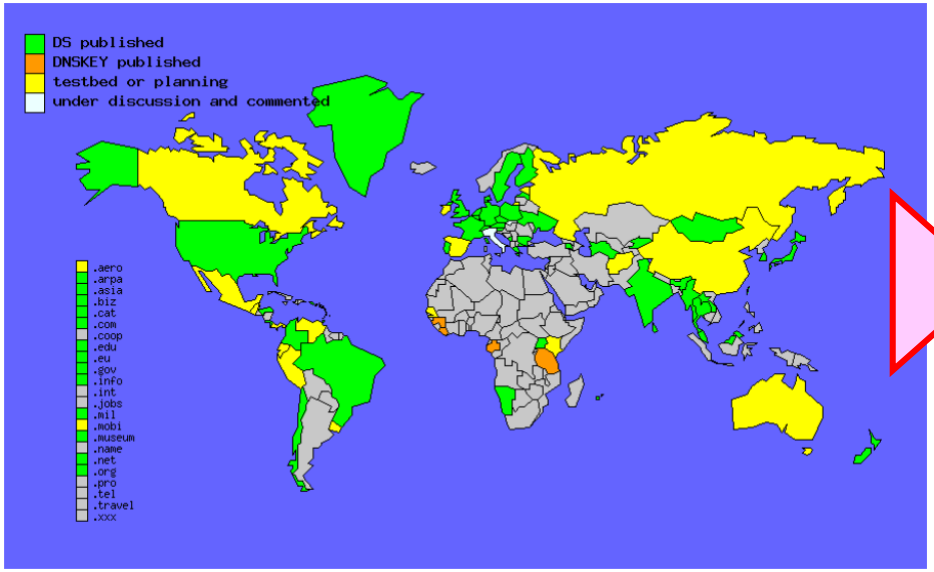
Alexa人気ランク順100万ドメイン中0.8%がDNSSECを導入 ※2

※2 Internet Week 2014 DNS DAY BBTower大本氏「DNSSEC Update」より

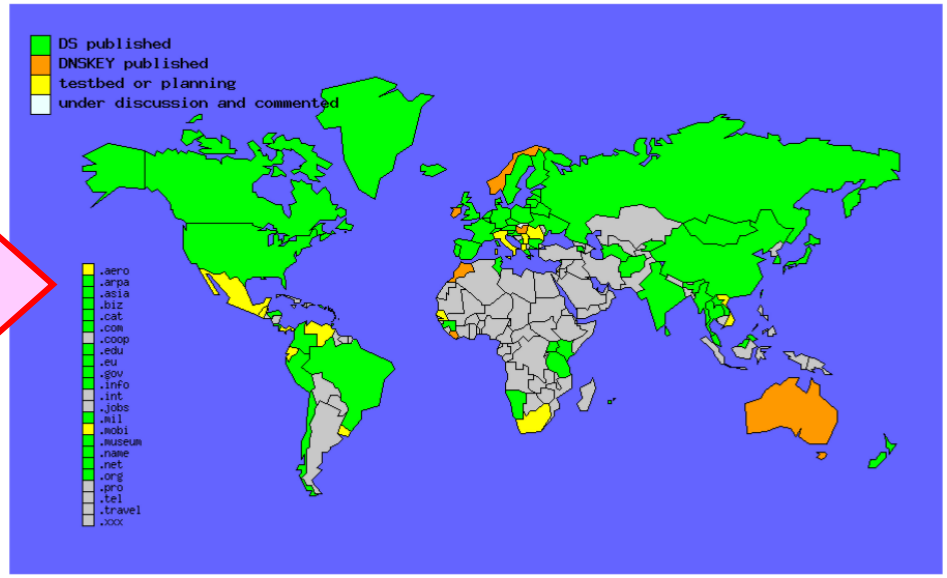
# 2. DNSSECの導入状況

## ■ccTLDレジストリにおける導入状況

2012年11月25日時点




2014年11月04日時点




http://www.ohmo.to/dnssec/maps/ より

新gTLDを除く従来のgTLDレジストリについてもマップ左端・1列に対応状況が表記されています。

# 2. DNSSECの導入状況

## ■ キャッシュDNSサーバー、レジストラ側の導入状況

キャッシュ
DNSサーバ

4.76%のキャッシュDNSサーバーがDNSSEC検証を有効にしている（Verisign Labs調べ）

Google Public DNS、米国の最大手プロバイダComcastなどがDNSSEC検証を有効に設定済み

レジストラ

レジストラが取次可能な数は1160社中、37社

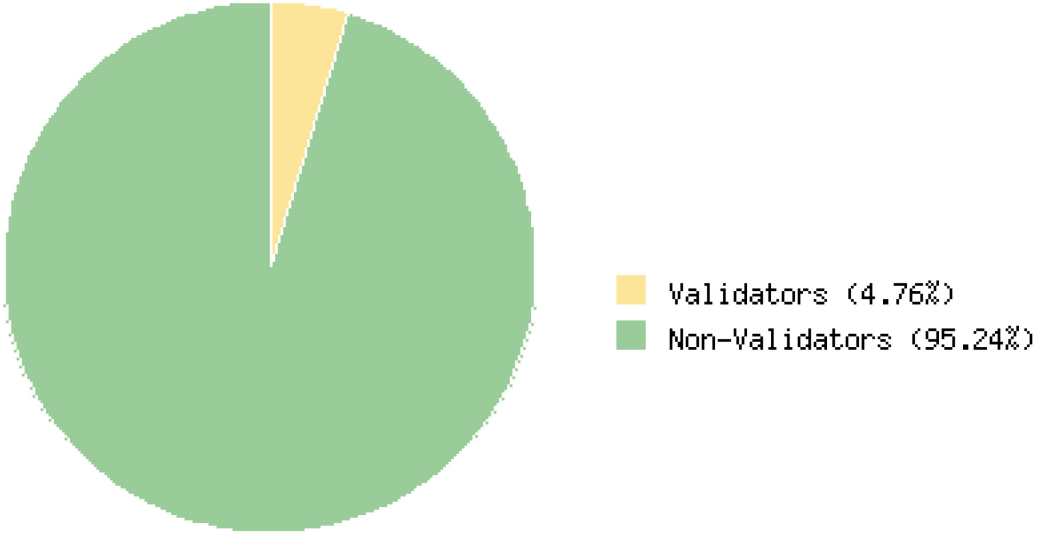
※http://www.icann.org/en/news/in-focus/dnssec/deployment（申告制）

# 2. DNSSECの導入状況

## ■キャッシュDNSサーバーの対応状況

- 4.76%が対応（Verisign Labsの調査結果）

➔ブラウザのDNSプリフェッチ機能を利用して調査




**Validators/Non-Validators: 14996/299830**

Percentage of resolvers doing DNSSEC validation

http://validator-search.verisignlabs.com/
2014年11月23日時点

# 3. DNSSECの導入状況

- JPでの運用状況
  - 関係組織と連携・実証実験をしながら、標準化技術の実装、運用設計を経て2010年よりDNSSEC署名を開始、2011年1月にサービス開始
  - DS TTL短縮などの運用改善や海外での運用ノウハウの発表・共有を実施
  - 導入から5年が経過、大きな事故なく運用中

資料D

jp DNSSECキーセレモニー 作業用チェックシート

作業日　2010 年 10 月 4 日

作業時間　12 : 56 ー 19 : 12

| | | 開始時刻 ー 終了時刻 |
|---|---|---|
| 0. | 金庫鍵搬送～作業場所への集合 | 12 : 56 ー 13 : 15 |
| 1. | 金庫の開放 | 13 : 16 ー 13 : 20 |
| 2. | データ初期化、システム運用者個別鍵の生成【初回のみ】 | 13 : 21 ー 14 : 13 |
| 3. | KSK管理用記憶媒体の初期設定【初回のみ】 | 14 : 13 ー 14 : 30 |
| 4. | KSK鍵ペアの生成 | 14 : 45 ー 15 : 00 |
| 5. | DSの生成 | 15 : 01 ー 15 : 08 |
| 6. | ZSK鍵ペアの生成 | 15 : 08 ー 17 : 22 |
| 7. | ZSK鍵ペアの署名 | 17 : 22 ー 17 : 47 |
| 8. | 署名済みZSK公開鍵の転送サーバへの格納 | 17 : 48 ー 18 : 17 |
| ~~9.~~ | ~~ZSK鍵ペアの削除【ZSK2回目以降】~~ | |
| 10. | 管理情報の複製【KSK生成時、もしくは認証情報 | |
| 11. | 金庫の施錠 | |
| 12. | メインサイト作業解散 金庫鍵搬送 | |
| ~~13.~~ | ~~KSK秘密鍵のDRサイトへの格納~~ | |

以上の作業が手順書どおり行われたことを確認しまし

立会人　松崎 吉伸　　責任者

立会人　風評 林



DNSOPS.jp DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECジャパン

- 活動内容
  - DNSSECの導入・運用に関する課題の整理・共有
  - DNSSECの導入・運用に関する技術検証の実施、ノウハウの蓄積
  - DNSSECの導入・運用に関するBCPの策定
  - 成果の対外的発信によるDNSSECの普及・啓発
- 組織
  - 部会（WG）による活動が主体
    - 技術検証WG
    - 広報WG
    - DNSSEC運用ワークショップ
      - 運用技術SWG
      - プロトコル理解SWG
- 活動状況
  - DNSSECに関する理解を深めるためにDNSSEC運動開始
  - ワークショップの内容についてはTwitterやU-Stre み

DNSSEC.JP

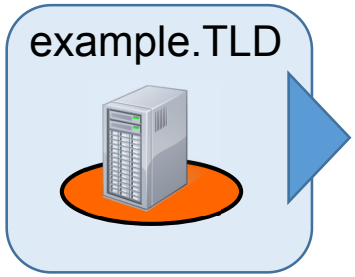


http://jprs.jp/whatsnew/notice/before2011/20101015-keyceremony.html

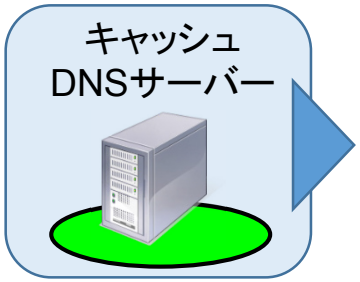
# 3. DNSSECの課題と今後の展望

# 3. DNSSECの課題と今後の展望

## ■ DNSSEC普及における課題




Alexa人気ランク順100万ドメイン中0.8%がDNSSEC署名を実施




4.76%のキャッシュDNSサーバーがDNSSEC検証を有効にしている

一般のドメイン登録者やISPのキャッシュDNSサーバーのDNSSEC対応率を向上させていくことが重要な課題。DNSSEC対応における費用対効果と対応時のリスクをどのようにして解決してくのか？

①新しい仕組みによる運用上のリスク軽減の工夫
②DNSSEC対応コストと運用サービスを組み合わせた費用と運用上の工夫
③DNSSECと連携した新しいセキュリティ技術登場によるさらなる発展(効果)

# 3. DNSSECの課題と今後の展望

## ①新しい仕組みによる運用上のリスク軽減の工夫

■ 運用者における運用上のリスク

- 運用上の失敗で最も怖い「人手」による作業、つまり鍵のロールオーバー作業が人手になっている箇所を何とかしたい

■ 新しい仕組み

- DS登録を自動化する仕組み（RFC7344 CDS, CDNSKEY）

  ➔子が生成した鍵を親ゾーンに登録する仕掛け。「レジストリへのDS登録」というステップを簡略化/自動化し、DNSサーバ間で鍵の生成・登録が連携される。人手を介していたところや、システム間連携が減り、運用上のリスクを軽減できる。

**デプロイに要する時間の問題はあるが、運用者にとって必要となるDNSSEC運用の負担を軽減する仕組みが登場しつつある**

# 3. DNSSECの課題と今後の展望

## ②DNSSEC対応コストと運用サービスを組み合わせた費用と運用上の工夫

■ ドメイン登録者における費用と運用の両立

- DNSSEC対応にかかる費用と運用の負担をうまく解決したい

■ 対策（事例紹介）

- スウェーデン(.SE)等での販売施策事例
  - ➔DNSSEC対応ドメイン名であれば登録料を安くする施策。
  - ➔.SEだけでなく、.FRや.EUでもインセンティブを導入し登録数が増加。.FRでは2013年に2ヶ月間、新規・更新ドメイン名に対し10%の割引を提供。2013年全体で登録済みDSレコード数が1.5倍に。
- ドイツ(.DE)でのDNS運用サービスの提供事例
  - ➔.DEゾーン自身に、ユーザが登録したドメイン名の「レコード」を記述。.DEはDNSSEC署名されており、ユーザはDNSサーバを用意することなくDNSSEC対応が完了する。

**ドメイン登録者において、インセンティブが導入促進に一定の効果を発揮しており、運用負担を軽減する事例も登場している**

# 3. DNSSECの課題と今後の展望

## ③DNSSECと連携した新しいセキュリティ技術登場によるさらなる発展(効果)

- 複数のセキュリティ技術
  - 複数のセキュリティ技術を組み合わせる・組み合わせられることでセキュリティレベルがより向上する。
    - ➔DNSSECが全てのセキュリティ上の問題を解決する訳ではない

- DNSSECを前提としたセキュリティ技術の登場
  - DANE (DNS-based Authentication of Named Entities)
    - ➔TLS認証においてCAの代わりにDNSSECを活用する技術。DNSSECによる保護を前提として、暗号化通信に必要な証明書をDNSに乗せて、HTTPS通信を使用する
  - DNS Resource Records for BGP Routing Data (draft-gersch-grow-revens-bgp)
    - ➔DNSSECを前提に逆引きDNSを拡張して経路情報を認証する技術(アイデア自体は古くから存在)
    - ➔このあとの吉田さんの講演ではRPKIという別の経路情報を認証する技術を紹介

DNSSECという1つのセキュリティ技術の登場が、他の新しいセキュリティ技術が登場する「場」となりつつあり、今後の発展が期待できる

# 4. まとめ

# 4. まとめ

- DNSSECで実現できること（おさらい）
  - DNS応答の出自の保証、完全性の保証を実現
  - 応答の書き換えを検知し、被害拡大の防止

- DNSSECの導入状況
  - レジストリにおけるDNSSEC対応が大きく進行中
  - 新gTLDではDNSSEC導入が必須要件
  - ドメイン登録者・キャッシュDNSサーバーでの導入率向上が今後の課題

- 課題と今後の展望
  - 新しい仕組み(CDS, CDNSKEY)登場による運用リスク軽減
  - レジストリによる販売施策とDNS運用による普及と運用負担軽減
  - DNSSECを前提とした新しいセキュリティ技術の登場

# 4. まとめ

## ■ 最後に

- DNSSECはルートやTLDレジストリにおいて導入が進んでおり、ドメイン登録者やキャッシュDNSサーバーでの普及が今後の課題

  ➔DNSSEC導入の初期段階を終えた状態

- 一般への普及段階に入り始めたところだが、レジストラやドメイン登録者がDNSSEC対応するには、リスク軽減や費用・運用の課題などを継続して解決していく必要がある

  ➔セキュリティは事故が起きたときに初めて気づくという難しさもある

JPRSは、レジストリでのDNSSEC導入・運用の知見を活かし、今後もDNSSECの普及に貢献していきます。

JPRS
JAPAN REGISTRY SERVICES