DNSとDNSSEC

株式会社日本レジストリサービス
阿波連　良尚

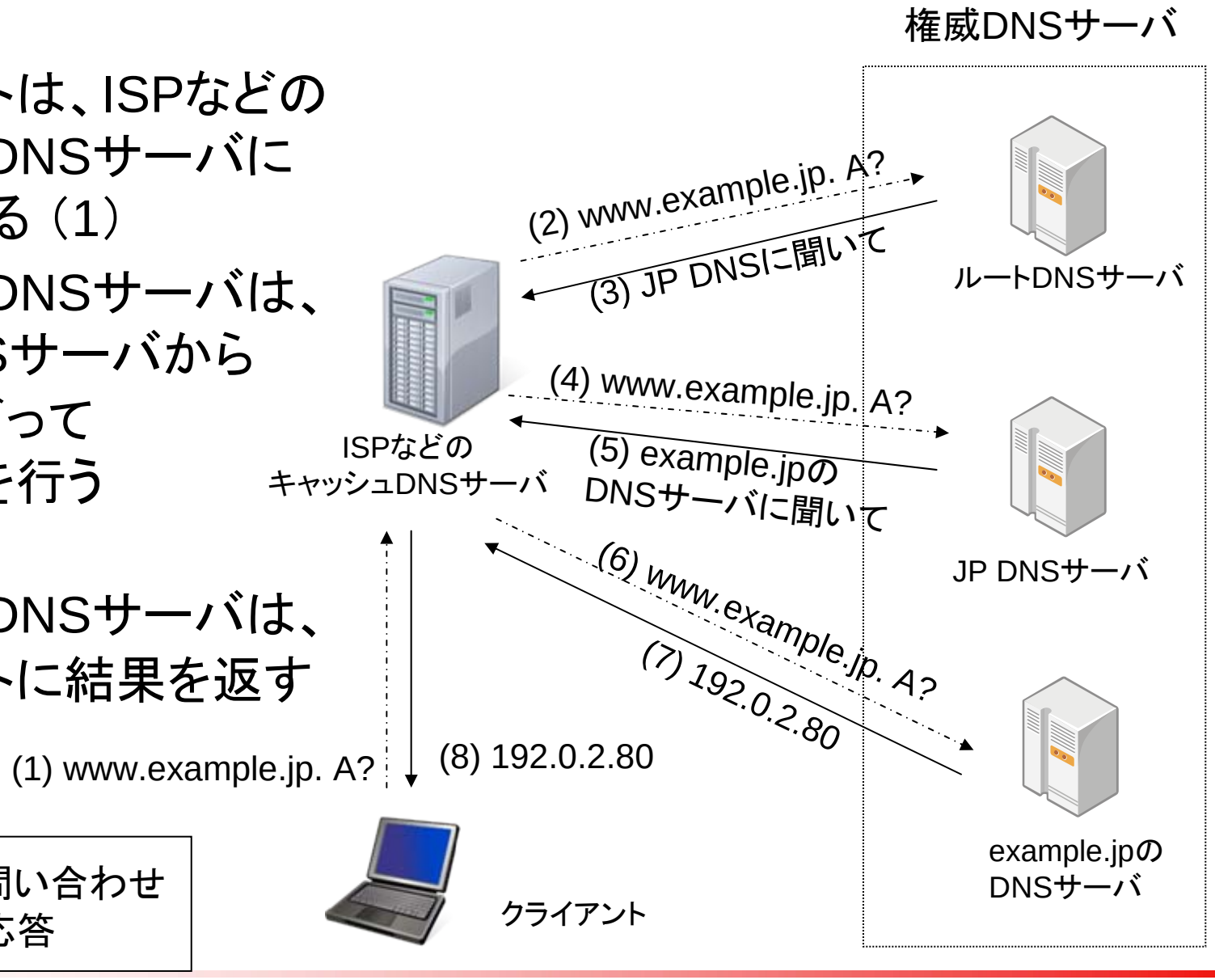
DNSSEC 2012 スプリングフォーラム
2012年4月25日

目次

- DNSの概要
- DNSSECの概要
  - DNSSECが開発された背景
  - レコードに対する署名と検証
  - 署名の検証の流れ
  - 公開鍵の入手
  - DNSSECにおける信頼の連鎖
- DNSSECでできること・できないこと
- DNSとDNSSECの運用上の変化
- DNSSECの応用例

DNSの概要 – 名前解決の流れ

- クライアントは、ISPなどのキャッシュDNSサーバにクエリを送る（1）
- キャッシュDNSサーバは、ルートDNSサーバから階層をたどって名前解決を行う（2～7）
- キャッシュDNSサーバは、クライアントに結果を返す（8）



DNSSECが開発された背景

- DNSには、受け取った応答を検証する仕組みがなかった
  - 開発された当時（1980年代）は問題になることはなかった
  - インターネットが社会で広く使われるようになり、DNSに高い信頼性が求められるようになった
- 受け取った応答を検証するための仕組みとして、DNSSECが開発された
  - 公開鍵暗号と電子署名をDNSに応用した

レコードに対する署名と検証

- 鍵ペアを作成して、公開鍵をゾーン上の情報（DNSKEYレコード）として格納する
- ゾーンの管理者は、ゾーンに対し秘密鍵で署名を行う
  - 署名はゾーン上の情報（RRSIGレコード）として格納する
- 権威DNSサーバは、応答に署名を付けて返す
  - クエリを受けたレコード（名前・タイプ）に対応する署名
- バリデータは、署名を用いて応答を検証する
  - 多くの場合、キャッシュDNSサーバがバリデータの役割を果たす

署名の検証の流れ

検証

応答のRRSet
+
署名（RRSIG）

バリデータ
（DNSSEC対応の
キャッシュDNSサーバなど）

www.example.jp. A?
+DNSSEC OK

応答のRRSet
+
署名（RRSIG）

example.jpの
DNSサーバ

署名

署名済
ゾーン情報

DNSKEY

バリデータでは、応答に
付加された署名と公開鍵を
用いて、応答のRRSetを
検証する

example.jpのゾーン管理者は、
秘密鍵を用いてゾーン情報に
署名（RRSIGレコード）し、
公開鍵（DNSKEYレコード）
とともに権威DNSサーバで公開する

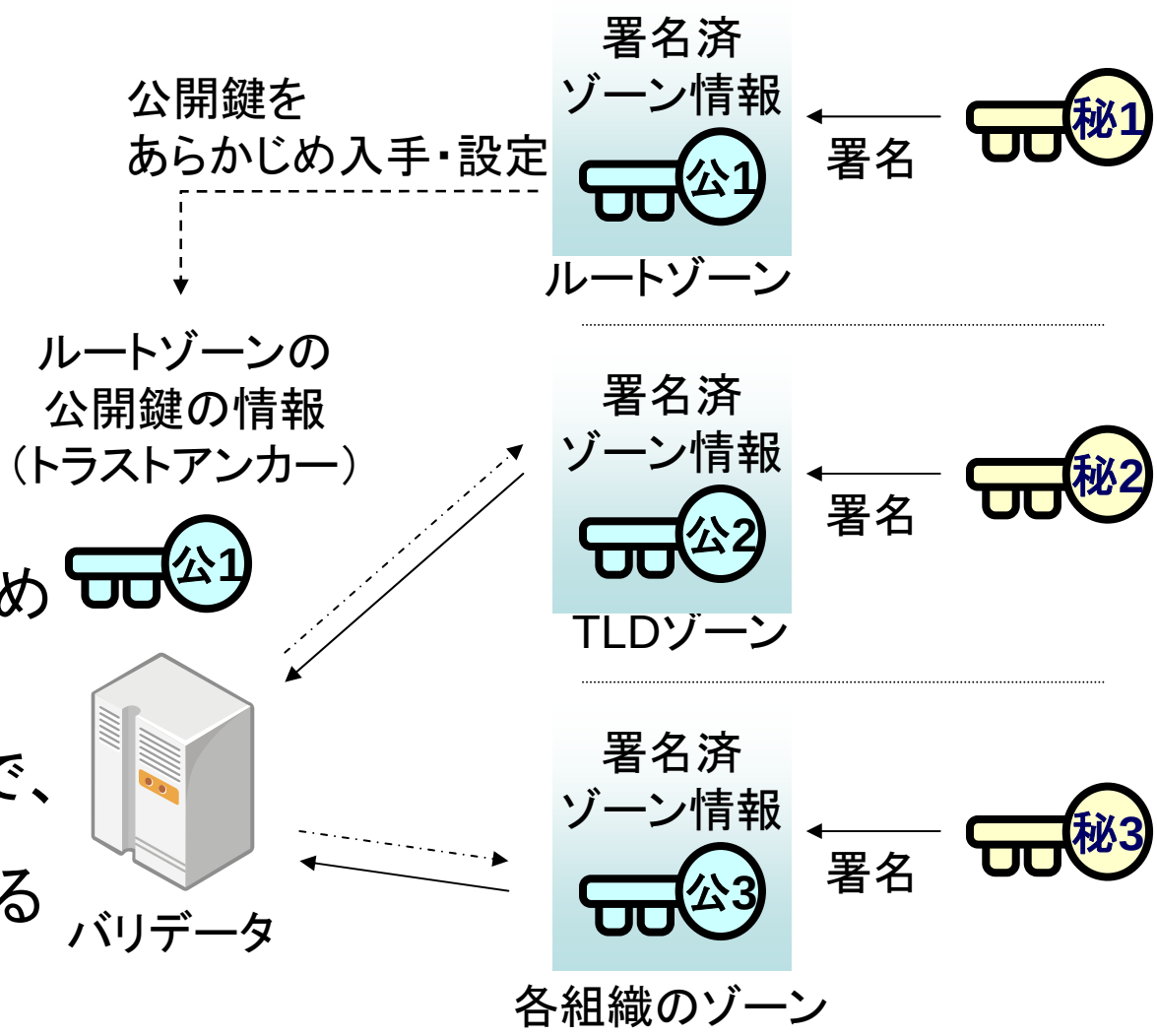
権威DNSサーバは、応答に署名を
付加して返す

公開鍵の入手

- DNSSECでは、公開鍵をDNSKEYレコードとしてゾーンに含める
  - バリデータは、上位のゾーンから公開鍵のハッシュ（DSレコード）を入手し、DNSKEYレコードと照合することで公開鍵の真正性を検証する
  - DSレコードは、上位のゾーンにて署名されている
  - DNSSEC検証の起点となる最上位のゾーン（通常はルートゾーン）の公開鍵またはそのハッシュ（トラストアンカー）は、信頼できる経路であらかじめ入手・設定しておく

DNSSECにおける信頼の連鎖

- 各ゾーンのレコードは、秘密鍵を用いて署名されている
- 各ゾーンの公開鍵は、上位ゾーンのDSレコードを参照することで、真正なものであると検証できる
- バリデータは、あらかじめルートゾーンのトラストアンカーを入手・設定しておくことで、ルートゾーンからの信頼の連鎖を確立できる



DNSSECでできること

- 出自の保証
  - 受け取ったレコードが、ドメイン名の管理者によって公開されたものであること
- 完全性の保証
  - 受け取ったレコードが、書き換えられたり一部が欠落していないこと

DNSSECでできないこと

- クエリや応答の暗号化
  - クエリや応答は平文で送信される
- 改竄検出時のリカバリ
  - 改竄を検出することはできるが、正しいレコードに訂正する機能は持たない
  - 正しいレコードを得られなかった場合、再度問い合わせを行う必要がある
- 署名の失効（revoke）
  - 署名には有効期間があるが、署名をrevokeする手段はない
  - 署名に設定する有効期間に気をつける必要がある

DNSSECの導入による運用上の変化

下記のような定期的なメンテナンスが必要となる

- 権威DNSサーバ
  - 鍵（KSKペア・ZSKペア）を適正に管理する
  - ゾーン更新時に署名する
  - 署名の有効期間が満了する前に、定期的に再署名する
  - KSK更新時には、上位ゾーンのDSレコード変更の依頼と確認を行う必要がある
- キャッシュDNSサーバ
  - ルートゾーンのトラストアンカーを設定・更新する
  - 時刻を同期する

DNSSECの応用例

- レコードの出自と完全性が保証されていることから、信頼できる分散データベースとして利用することが検討されている

（例）

- DomainKeys Identified Mail (DKIM)
  - 電子メールに電子署名を付加する仕組み
  - 公開鍵をDNSで公開する
- DNS-based Authentication of Named Entities (DANE)
  - TLSの鍵や証明書をDNSで公開する仕組み
  - IETFのワーキンググループ（DANE WG）で標準化活動が行われている