DNSOPS.jp
DNS Operators Group, Japan

DNSSEC入門
DNSSECへの対応

2013/05/29

日本インターネットエクスチェンジ株式会社
日本DNSオペレーターズグループ
石田慶樹

Agenda

- ✓DNSSEC対応
- ✓権威DNSのDNSSEC対応
- ✓キャッシュDNSのDNSSEC対応

Agenda

- ✓DNSSEC対応
- ✓権威DNSのDNSSEC対応
- ✓キャッシュDNSのDNSSEC対応

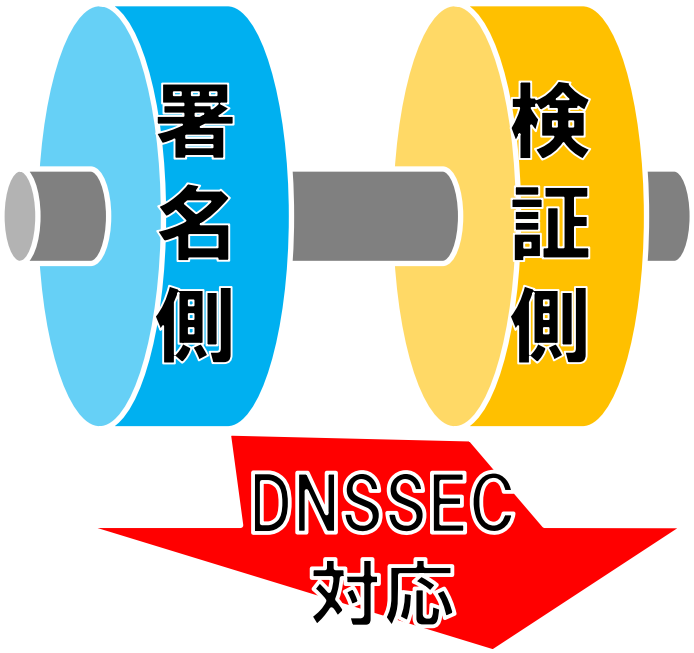
DNSSEC対応

✓DNSSEC対応には

■署名側

■検証側

の両方の対応が必要



DNSSEC対応

◆署名側の対応
- ✓レジストリ
- ✓レジストラ
- ✓DNSホスティング

◆検証側
- ✓上位アプリ
- ✓企業／組織
- ✓ISP

■権威DNSサーバでの対応

■キャッシュDNSサーバでの対応

それぞれのサーバでのDNSSEC対応について紹介

Agenda

- ✓DNSSEC対応
- ✓**権威DNSのDNSSEC対応**
- ✓キャッシュDNSのDNSSEC対応

権威DNSサーバの役割

- ✓ 2種類の署名鍵の公開
  - ■ KSK
  - ■ ZSK
- ✓ 署名 (RRSIG) の公開
  - ■ 問い合わせに対して署名を応答する
- ✓ 不在証明
  - ■「存在しない」ことを証明
- ✓ 下位ゾーンの委譲 (delegation)
  - ■ 下位ゾーンのKSK相当 (ハッシュ値) を自ら署名して公開
  - ■ 信頼の連鎖を形成

権威DNSサーバのDNSSEC対応

- ✓ 通常の権威DNSサーバの運用
- ✓ 準備作業
  - ■ DNSSECに対応した最新のソフトウェア
    - ● BIND9 (9.7系以降でISCのサポートのあるもの)
    - ● NSD (3.2系の最新のもの)
      - ロ 鍵の作成とゾーンの署名にldns等が必要
  - ■ サーバの時刻同期
    - ● 署名に有効期限が存在
  - ■ 512バイト超のDNS応答への対応
    - ● EDNS0, TCPフォールバックおよびIPフラグメントへの対応
    - ● サーバ自身のフィルタおよびミドルボックス

権威DNSサーバのDNSSEC対応

- ✓DNSSEC対応に伴って新たに発生する事項
  - ① RRへの署名／署名の更新
  - ② 署名鍵の定期的な更新（ロールオーバー）
  - ③ 下位ゾーンのDSレコードの追加と署名
- ✓自ゾーンのDSレコードを上位ゾーン（の管理者）に通知
  - ■レジストラを介してレジストリへ通知

① RRへの署名／署名の更新

- ✓ ゾーン内の各レコードに対するRRSIGの生成
- ✓ 不在証明の生成
- ✓ ゾーンを編集したら必ず署名
- ✓ ゾーンを編集しなくても定期的に署名
  - ■ 署名には有効期間（有効時限）が存在
  - ■ 放置したまま有効期間が過ぎると署名が無効になり名前が引けなくなる

② 鍵の更新（ロールオーバー）

- ✓ 同じ鍵を長期間使い続けることは危険
  - ■ DNSSECに限らずSSL/TLS/SSH等でも同様
  - ■ リスクの程度は暗号アルゴリズム、鍵長、期間に依存
- ✓ リスクを低減させるため鍵を更新
  - ■ 定期的な更新
  - ■ イベントドリブンでの更新
- ✓ DNSSECでは定期的な更新を推奨

② 鍵の更新（ロールオーバー）

- ✓DNSではキャッシュが分散して存在
  - ●鍵に関する情報、署名に関する情報も分散
  - ●TTLが過ぎていない間はどこかのキャッシュDNSサーバ上で保持されている可能性
  - ●鍵の更新時にキャッシュされている更新前の情報との整合性まで気をつけることが必要
- ✓鍵の更新は段階を踏んで実行
  - ●権威DNSサーバのDNSSEC対応で面倒かつ最もトラブルを引き起こしやすい作業

② 鍵の更新（ロールオーバー）

- ✓運用上の必要性から鍵を3つの状態で管理
  - ■Published
    - ●鍵がゾーン上で公開されているが、署名・検証には使われていない
  - ■Active
    - ●公開され、署名・検証に使われる
  - ■Inactive
    - ●署名・検証には使われないが、ゾーン上で公開されている。

② 鍵の更新（ロールオーバー）

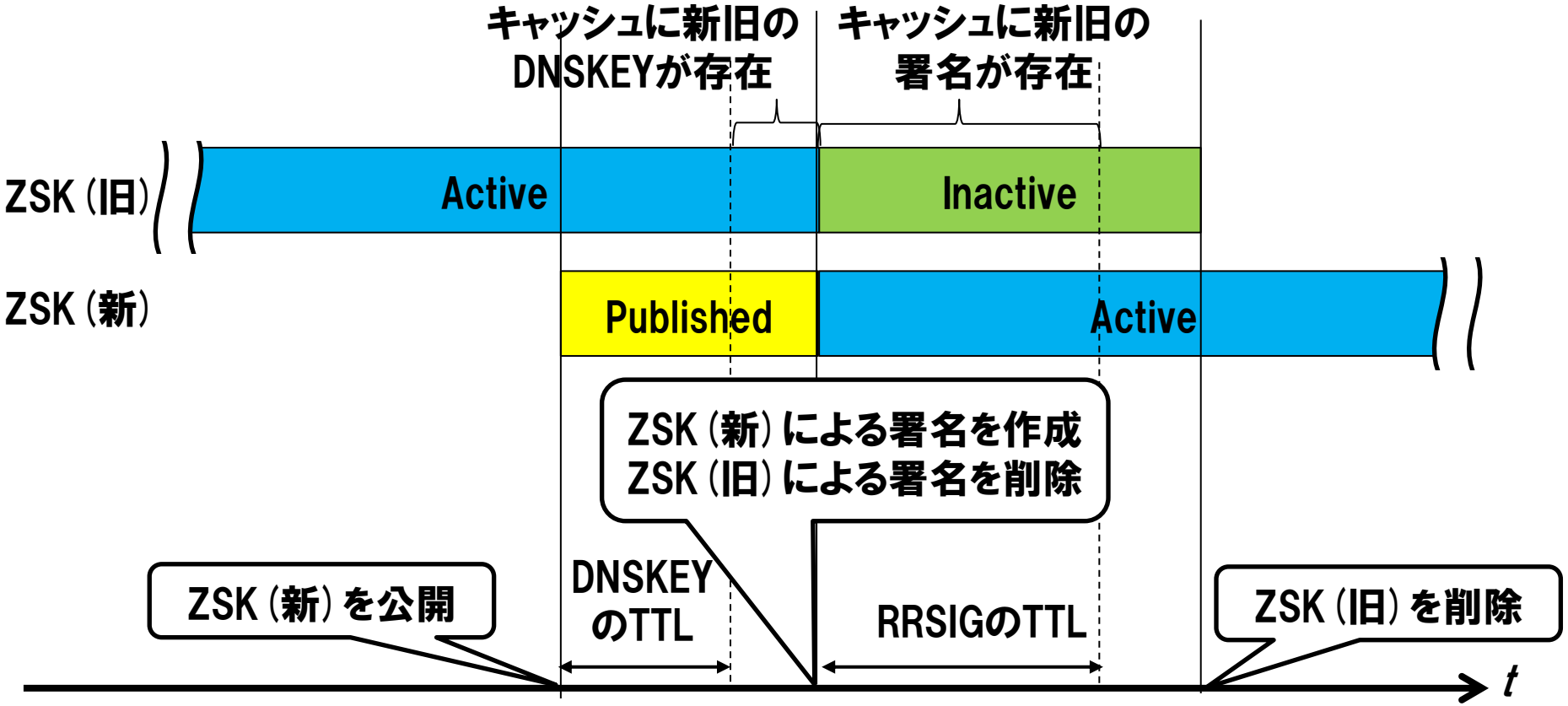
- ✓KSKとZSKの両方で更新が必要
  - ■更新頻度はKSKとZSKで別
  - ■KSKについては上位ゾーンのDSの更新も必要
- ✓ベストプラクティス的な手法が存在
  - ■ZSKについては事前公開法
  - ■KSKについては二重署名法
- ✓キャッシュされている情報でも不整合が発生しないための運用上の手法

② 鍵の更新 (ロールオーバー)

- ✓ ZSK:事前公開法
  - ■ 新しい鍵を署名に先駆けて公開する手法
  - ■ 署名は常に一つの鍵でのみ
  - ■ 鍵の公開と署名のタイミングが別
  - ■ 手順
    1. 新鍵を公開 (公開のみで署名には使わない)
    2. DNSKEYのTTL以上の時間後まで待つ (新旧の鍵がキャッシュサーバで見えるようになる)
    3. 署名に使う鍵を新鍵に切替 (旧鍵はゾーンには残す)
    4. RRSIGのTTL以上の時間後まで待つ(旧鍵による署名がキャッシュサーバから消滅)
    5. 旧鍵を削除

② 鍵の更新（ロールオーバー）

✓ZSK：事前公開法

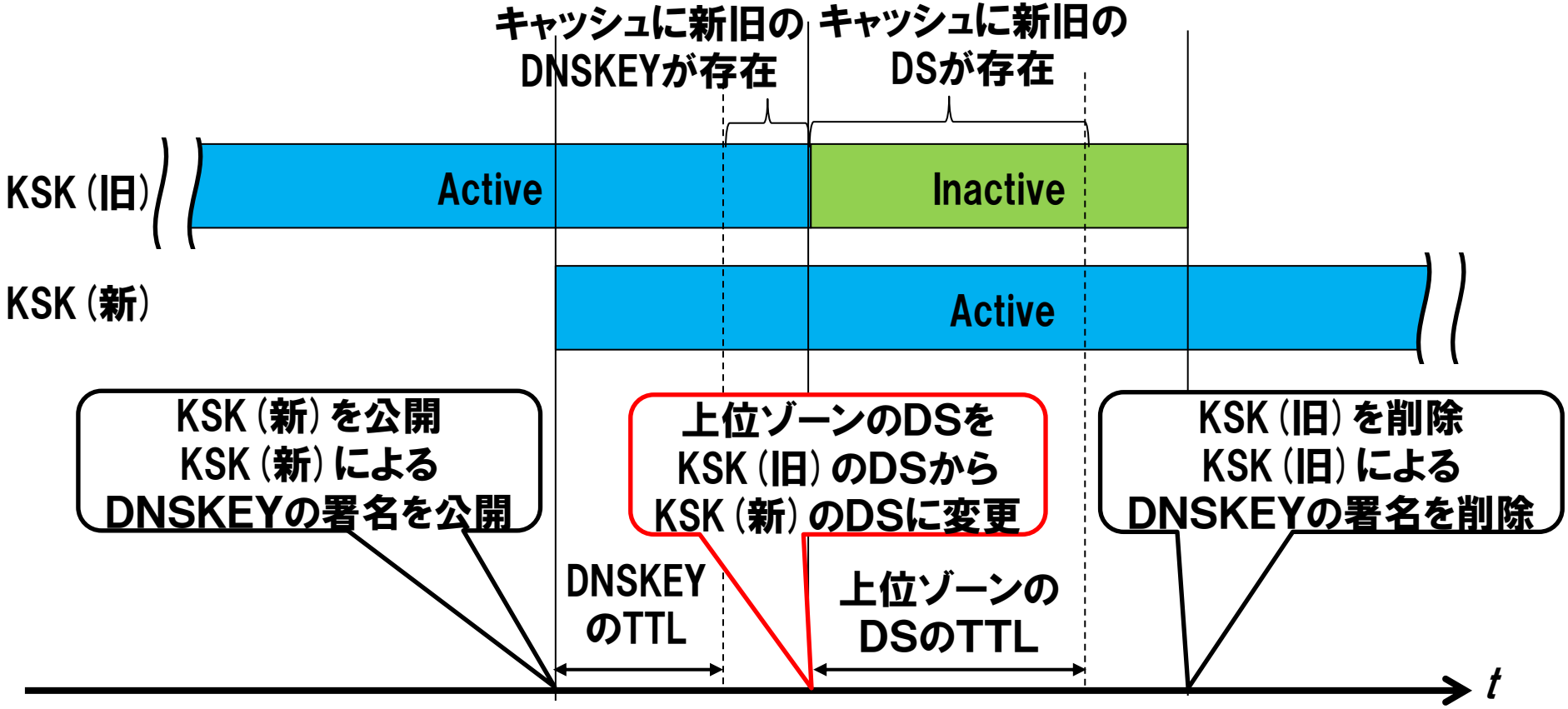


② 鍵の更新（ロールオーバー）

- ✓ KSK：二重署名法
  - ■ レコードを新旧2つの鍵で別々に署名
    - ● KSKはZSKを署名するものであるため対象は少ない
  - ■ 上位ゾーンとのDSレコードのやり取りを最小（ロールオーバー毎に1回）にするための手順
  - ■ 手順
    1. 新鍵を公開し新旧両方の鍵で署名
    2. DNSKEYのTTL以上の時間後まで待つ（新旧の鍵がキャッシュサーバで見えるようになる）
    3. 上位ゾーンに登録するDSを新鍵のものに変更
    4. 上位ゾーンのTTL以上の時間後まで待つ（旧鍵のDSがキャッシュサーバから消滅）
    5. 旧鍵と旧鍵による署名を削除

② 鍵の更新（ロールオーバー）

✓KSK：二重署名法



③ 下位ゾーンのDSレコードの登録

- ✓下位ゾーンから渡されるDSレコードの管理
- ✓作業としてDSレコードの更新（追加／削除）が発生
- ✓KSKの更新ごとに作業が発生
- ✓レジストリ・レジストラ間は何らかのI/Fを介して通知（EPPやWeb UI等）

権威DNSサーバの運用

- ✓手順とパラメータの決定
  - ■ゾーンに署名するためにはパラーメータと手順を事前に定めることが必要
  - ■手順
    - ●ゾーンの更新
    - ●ゾーンの署名
    - ●ZSKの更新
    - ●KSKの更新

パラメータの決定

- ✓ 決定するパラメータ
  - ■ 暗号アルゴリズムと鍵長
    - ● RSASHA256が一般的
    - ● KSK 2048bit, ZSK 1024bit
    - ● 楕円曲線暗号も利用可能 (ECDSA, GOST)
      - □ 署名が短くなるというメリット
      - □ 対応していないパッケージ等も存在
      - □ 様々な要因から直近の普及は見込薄
  - ■ 不在証明
    - ● 計算量が少ないがゾーンの情報をすべて辿れるNSEC
    - ● 計算量が多いがゾーン情報は辿られないNSEC3

パラメータの決定（続き）

- ✓決定するパラメータ
  - ■鍵の更新間隔
    - ●KSKは1年程度
    - ●ZSKは1，2か月程度が標準的
  - ■署名有効期間
    - ●ゾーン内レコードの最長TTLより長くする
    - ●SOA expireより長くする
    - ●2週間から2カ月程度が標準的

権威DNSサーバの運用

- ✓レジストラの対応状況の確認
  - ■すべてのレジストラが対応している状況ではない
  - ■DS取次を提供するレジストラであることが必須
- ✓DNSSEC対応による定常的な運用負荷は増加
  - ■鍵の管理（鍵の生成と更新）
  - ■署名の管理（ゾーンの署名と更新）
  - ■DSの登録（上位ゾーンとの定期的なやり取り）

権威DNSサーバの運用

- ✓権威DNSサーバの構成の見直し
  - ■サーバ負荷の上昇に伴うシステム数の見直し
  - ■ソフトウェアの変更やアプライアンスの導入
  - ■Hidden Masterの導入
  - ■HSMの導入

権威DNSサーバの運用

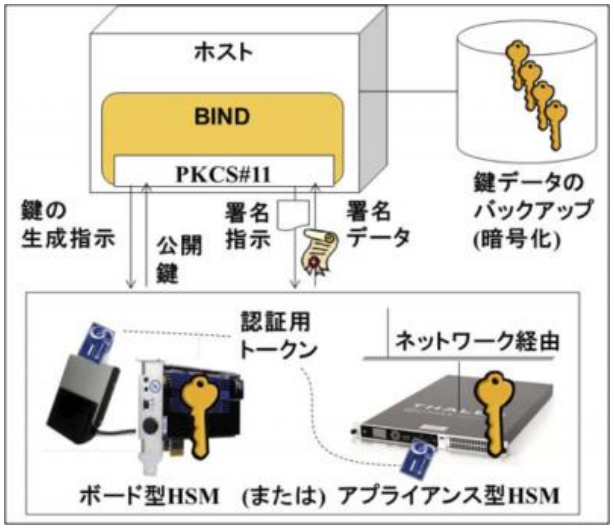
- ✓Hidden Master構成への変更
  - ■外部に非公開のサーバをマスターサーバ
  - ■マスターではゾーン管理と鍵と署名の管理のみ
  - ■スレーブにゾーン転送
  - ■問合せへの応答はスレーブのみ
  - ■マスターサーバでの変更を確認後に公開


```
example.jp.  IN NS master.example.jp.
             IN NS slave.example.jp.

example.jp.  IN NS slave1.example.jp.
             IN NS slave2.example.jp.
```

権威DNSサーバの運用

- ✓ HSM（ハードウェア・セキュリティ・モジュール）の導入
  - ■ ハードウェアによる鍵の管理
  - ■「HSM を利用した DNSSEC の運用に関する考察」
    http://dnssec.jp/?page_id=792
  - ■ コストとの見合い



http://dnssec.jp/?page_id=792 より

権威DNSサーバの運用

- ✓運用負荷を低減するために
  - ■手順書の作成
  - ■構成の変更（ハード、ソフト、アプライアンス）
  - ■ツールの導入による自動化
  - ■アウトソーシングの検討

権威DNSサーバの運用

- ✓ qmailからメイルが送信できなくなる問題
  - ■ qmailが行うANYの問い合わせに512バイト以上の応答が返ってくるドメインにメイルが送信不能
    - ● qmailの不具合
    - ● 非公式パッチで対応可能
      - □ http://www.ckdhr.com/ckd/qmail-103.patch
  - ■ DNSSECで署名すると応答パケットサイズが512バイトを超える
    - ● DNSSEC以外でも512バイト超だと同様の不具合が発生
  - ■ 1週間後のバウンスメールにより不達が判明
    - ● 送信側は設定変更なしのため受信側の問題と認識
    - ● 受信側（署名を行った側）では気づけず
  - ■ このqmailの不具合によりDNSSEC対応に二の足を踏むドメインも存在

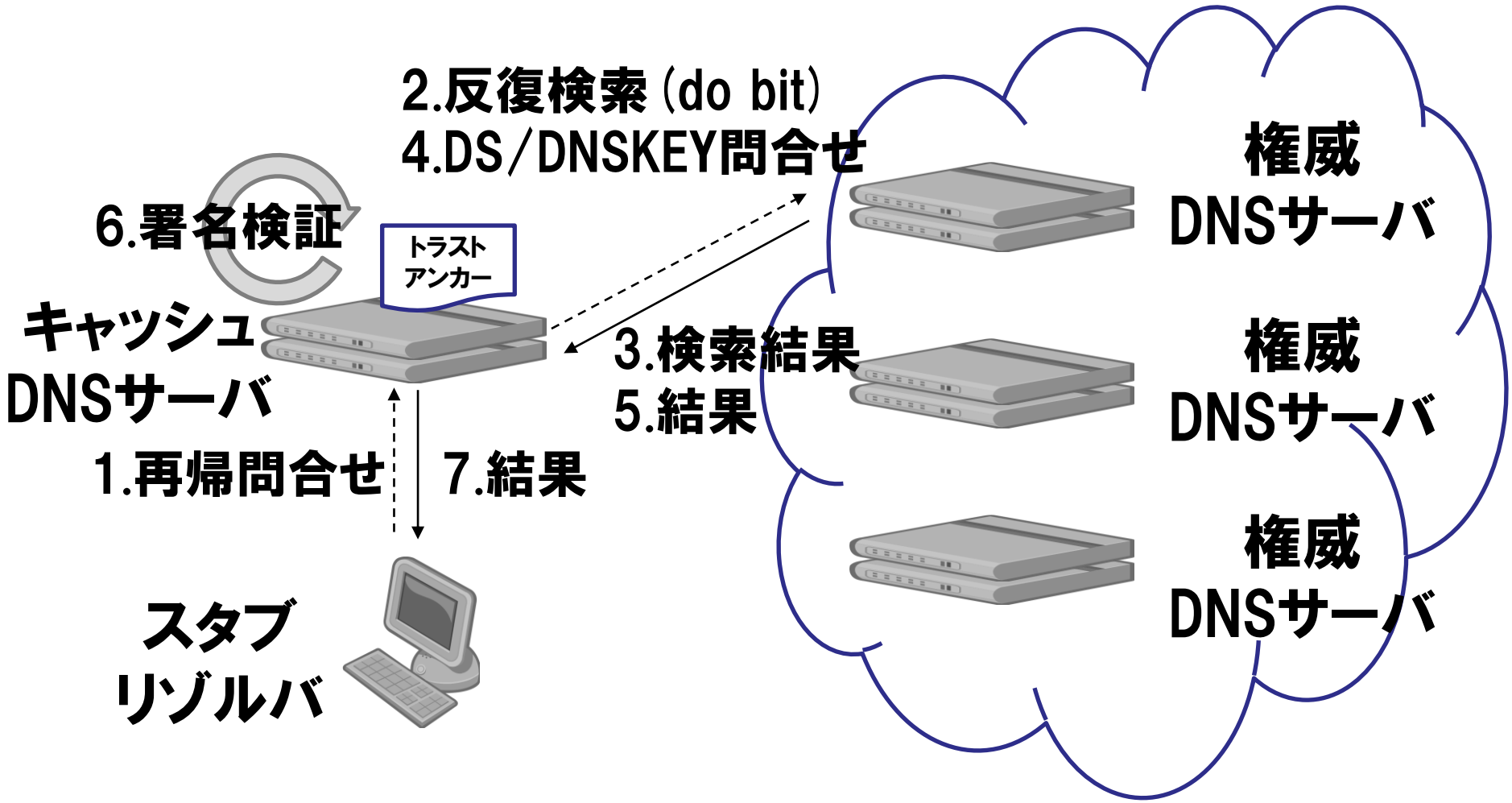
Agenda

- ✓DNSSEC対応
- ✓権威DNSのDNSSEC対応
- ✓キャッシュDNSのDNSSEC対応

キャッシュDNSサーバの役割

- ✓通常のキャッシュDNSの機能
- ✓DNSSECの署名の検証
- ✓RRsetの正当性を検証

キャッシュDNSサーバの役割



キャッシュDNSサーバの役割

- ✓検証結果による応答
  - ■DSが登録されていない
    - ●署名されていない：ad bitなしでRRsetを応答 (Indeterminate)
    - ●署名されている：ad bitなしでRRsetを応答 (Insecure)
  - ■DSが登録されている
    - ●検証に成功：ad bit付きでRRsetを応答 (Secure)
    - ●検証に失敗：SERVFAILを応答 (Bogus)

キャッシュDNSサーバのDNSSEC対応

- ✓ 通常のキャッシュDNSサーバの運用に追加
- ✓ 準備作業
  - ■ DNSSECに対応した最新のソフトウェア
    - ● BIND9 (9.7系以降でISCのサポートのあるもの)
    - ● Unboud (1.4系の最新のもの)
  - ■ サーバの時刻同期
    - ● 署名に有効期限が存在
  - ■ 512バイト超のDNS応答への対応
    - ● EDNS0, TCPフォールバックおよびIPフラグメントへの対応
    - ● サーバ自身のフィルタおよびミドルボックス

キャッシュDNSサーバのDNSSEC対応

- ✓設定の追加
  - ■BINDは設定追加とトラストアンカーの設定
  - ■Unboundはトラストアンカーの設定
  - ■Rootゾーンのトラストアンカー(TA)の追加
    - ●何らかの方法で．のDNSKEY(KSK)を取得
      - ロDNSで取得
      - ロWebから取得
    - ●取得したDNSKEYが正しいかの確認
      - ロハッシュ値の確認

キャッシュDNSサーバのDNSSEC対応

- ✓トラストアンカーの自動更新の設定
  - ■5年毎にトラストアンカーの更新が必要
  - ■RFC5011に自動更新が規定
  - ■次の更新が最初の更新（導入されて5年経っていない）

キャッシュDNSサーバのDNSSEC対応

- ✓設定の確認
  - ■検証出来ていることを確認
    - ●サーバ上でdigを利用して確認
  - ■配下のスタブリゾルバ(端末)で確認
    - ●検証用のWebサーバへの接続
- ✓日常的な運用業務
  - ■権威DNSサーバのように定期的に作業が発生するわけではない
  - ■トラブル対応による運用負荷は少なくない

キャッシュDNSサーバの運用

- ✓定期的に発生する作業は不要
- ✓監視と対応は不可欠
  - ■権威DNSサーバ側での不具合に対応
  - ■監視とトラブルシューティングの負荷が増大
  - ■トラブル解決のための方針と手順が必要

キャッシュDNSサーバの運用

- ✓監視とトラブルシューティング
  - ■ドメインの検証失敗の監視
  - ■検証失敗はポイズニングではなく権威DNS側の署名失敗がほとんど
    - ●権威DNSの署名失敗によりキャッシュDNS側で署名検証に失敗
    - ●検証失敗はSERVFAILとなるためユーザが接続不能
    - ●DNSSEC対応キャッシュDNSでのみ名前解決が失敗
  - ■影響の大きいゾーン(ルートに近いゾーン)で生じるとインパクトが巨大

キャッシュDNSサーバの運用

- ✓監視とトラブルシューティング（続き）
  - ■監視を行いトラブル時に対応
  - ■対応策
    - ① 相手が復旧するまで待つ
      - ロ ユーザへの告知
      - ロ 場合によっては何らかの方法での先方への通知
    - ② 検証を一時的に中断
      - ロ 影響が大きい場合
      - ロ ソフトウェアにより検証そのものの中断か該当するゾーンのみの中断かのいずれかにより対応

まとめ

- ✓DNSSEC対応は署名側と検証側の両輪が揃ってはじめて実現
- ✓署名側の権威DNSサーバは定常的に作業が必要
- ✓検証側のキャッシュDNSサーバは監視とトラブル時の対応手順の準備が必要

DNSOPS.jp
DNS Operators Group, Japan

DNSSECジャパン成果物 技術検証WG

タイトル	公開日
DNSSECの仕組みと現状 DNSSECの仕組みと現状について簡略にまとめました。(pdf形式, 340kB, 12p)	2010/11/24
DNSSEC導入に当たって DNSSEC導入/対応とは? 検討しておくべき項目を事業者毎にまとめました。(pdf形式, 399kB, 19p)	2010/11/24
DNSSECを利用するリゾルバーのためのトラストアンカーの設定方法について 第2版 DNSSECを利用するDNSキャッシュサーバ(またはリゾルバー)のために、現段階でよいと考えられる、トラストアンカーのデータを入手し確認する方法を説明しています。 第2版では、ルートゾーンの最新情報、KSKの更新等について「■9. 日常的な運用のために」を追加しました。 (pdf形式, 160kB, 5p)	2011/2/7
レジストリの鍵登録インターフェースに関する調査報告 技術検証WGにおいて行った、レジストリの鍵登録インターフェースの調査についてまとめました。(pdf形式, 358kB, 4p)	2010/11/24
レジストラ移転ガイドライン 技術検証WGにおいて行ったDNSSEC導入後のレジストラ移転・DNSプロバイダ移転方法の検討の報告資料です。移転時の注意事項、移転パターンの紹介、DNSSECジャパン推奨の移転方法と推奨の理由等をまとめました。(pdf形式, 433kB, 25p)	2010/11/24
キャッシュDNSサーバDNSSEC導入ガイドライン キャッシュDNSサーバへのDNSSEC導入についてのガイドラインをまとめました。(pdf形式, 180kB, 8p)	2011/3/9

DNSSECジャパン成果物 技術検証WG（続き）

タイトル	公開日
DNSサーバDNSSEC導入Load Balancer機能チェックリスト DNSサーバへのDNSSEC導入に伴い、DNSサーバ上位のNW機器においても考慮しなければならない確認事項をとりまとめました。（pdf形式，193kB，7p）	2011/3/9
DNSSECツール調査報告 DNSSEC に対応するツールやサービス、ライブラリの調査を行いました。その結果をとりまとめたものです。（pdf形式，172kB，10p）	2011/4/1
DNSSECにおける鍵管理 DNSSECにおける鍵管理の基本的なライフサイクルを説明し、ガイドラインを提供しています。（pdf形式，287kB，9p）	2011/4/18
DNSサーバDNSSEC導入鍵管理チェックリスト DNSサーバへのDNSSEC導入に伴う、鍵の作成と管理において考慮しなければならない確認事項を取りまとめました。（pdf形式，172kB，6p）	2011/4/18
DNSSEC gTLD レジストラ移転実験報告 レジストラ移転ガイドライン に沿った形で実際に行ったレジストラ移転実験の報告を取りまとめました。（pdf形式，163kB，10p）	2012/7/12

DNSOPS.jp
DNS Operators Group, Japan

DNSSECジャパン成果物
運用技術WG

タイトル	公開日
リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いるゾーンへのDNSSECの導入にあたっての注意喚起 リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いているゾーンでDNSSECを有効にしたときに観測された問題点の提示と注意喚起（印刷用pdf形式, 152kB, 5p）	2011/10/5
DNSSECゾーン検証ツール調査報告 署名後のゾーンを正しく検証できるかどうかを公開前に事前テストすることの必要性と、それを行うためのツールの紹介（印刷用pdf形式, 198kB, 6p）	2012/4/16
HSM を利用した DNSSEC の運用に関する考察 権威DNSサーバーへのDNSSEC導入において、HSMの導入意義や利用方法の情報とHSM導入要否の判断の材料を提供（印刷用pdf形式, 1.2MB, 14p）	2012/4/17
ISP等のDNSSEC対応におけるDPS作成・公開の検討 ISP等がそのDNSサービスにおいてDNSSEC対応を行う際のDPS公開についてのメリットと課題（印刷用pdf形式, 150kB, 4p）	2012/4/24
失敗事例研究まとめ DNSSEC先行導入組織における失敗事例を調査および考察することで、将来DNSSECを導入する組織に対しての知見とすべく、失敗事例情報をまとめた。（印刷用pdf形式, 720kB, 4p）	2012/7/12
DNSSEC運用失敗事例の研究 総括 DNSSEC先行導入組織における失敗事例から得られた知見の総括（印刷用pdf形式, 243kB, 5p）	2012/7/12

謝辞

✓本資料を作成するにあたり
- ■其田学氏（三洋ITソリューションズ㈱）
- ■舩戸正和氏（㈱日本レジストリサービス）
- ■山口崇徳氏（㈱インターネットイニシアティブ）

の3氏にご協力いただきました。

Agenda

- ✓DNSSEC対応
- ✓権威DNSのDNSSEC対応
- ✓キャッシュDNSのDNSSEC対応