DNSSEC Update

2016年12月1日

Internet Week 2016 DNS DAY

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

本日の概要

1. ルートゾーンの鍵更新
2. 影響と対策

(付録：DNSSECのおさらい)

1. ルートゾーンの鍵更新

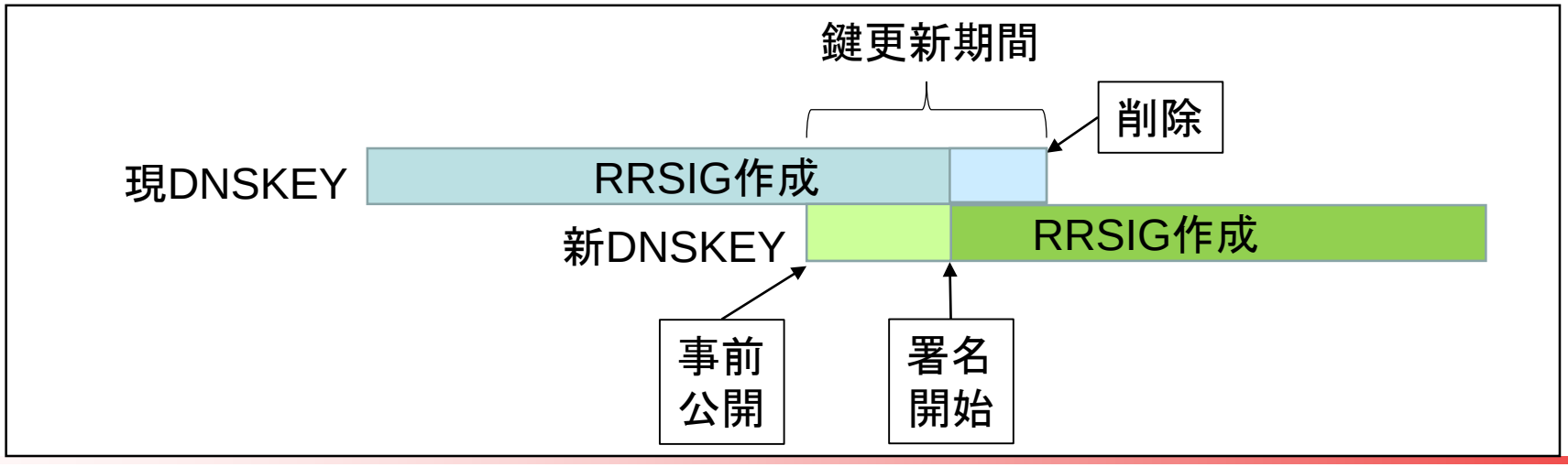
ルートゾーンにおける鍵更新の種類

- ZSK更新(実施者：Verisign)
  - 定期更新
    - 3カ月毎、鍵長・鍵アルゴリズム変更なし、実績あり
  - 鍵長更新
    - 不定期、鍵アルゴリズム変更なし、実績あり(※)
  - 鍵アルゴリズム更新
    - 不定期、鍵長変更の場合あり、実績なし
- KSK更新(実施者：IANA)
  - 定期更新
    - 5年毎、鍵長・鍵アルゴリズム変更なし、実績なし(※)
  - 鍵長更新
    - 不定期、鍵アルゴリズム変更なし、実績なし
  - 鍵アルゴリズム更新
    - 不定期、鍵長変更の場合あり、実績なし

(※)の鍵更新を本日説明

ルートゾーンの鍵更新による影響

- 鍵更新期間中
  - DNSKEY応答サイズの増加
    - 新しい鍵の事前公開のため
    - 定期更新の場合は、更新後に元のサイズに戻る
- 署名開始後
  - DNSKEY応答サイズの増加
    - 鍵長変更(ビット数増加)の場合
  - RRSIG応答サイズの増加
    - ZSK鍵長変更(ビット数増加)の場合



1.1 ZSKの鍵長更新

ZSKの鍵長更新について

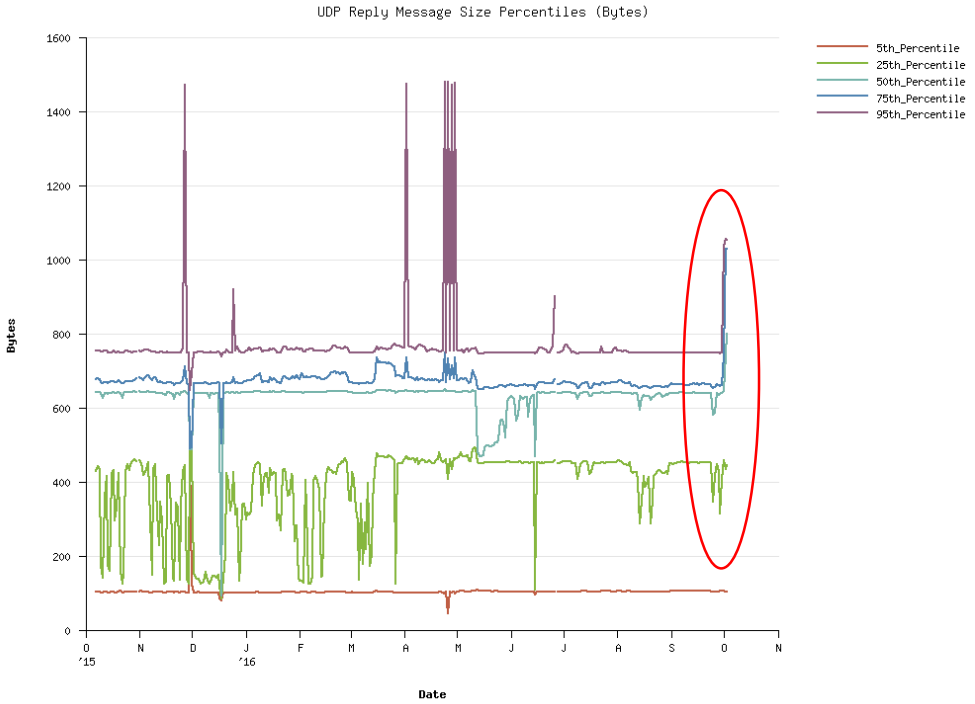
- 2016年10月1日にZSKの鍵長が1024bitから2048bitへ変更された
  - NISTの勧告に従ったもの
    - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
  - ルートゾーンのDNSSEC署名が開始されて以来初更新
- ZSKの鍵長変更によるDNSKEYおよびRRSIGサイズの増加
  - DNSKEY
    - 通常時: 736オクテット→864オクテット
    - 更新期間中: 883オクテット→1139オクテット
  - RRSIG
    - 更新後: 159オクテット→287オクテット

参考:http://schd.ws/hosted_files/icann562016/69/verisign-zsk-change.pdf

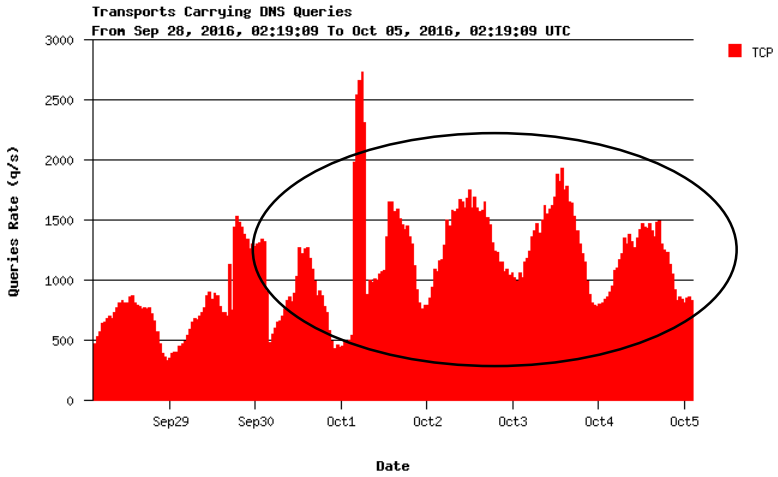
現在までに観測されている状況

- トラブルは報告されていない
  - ZSKの鍵長更新成功報告は行われている

    https://lists.dns-oarc.net/pipermail/dns-operations/2016-October/015502.html
- ルートサーバーのDNSトラフィックには大きな変化は見られない
  - UDPの応答サイズは大きくなっている
  - UDPの問い合わせ数は変わらない
  - TCPの問い合わせ数はルートサーバーによって増減がある



←Aルートサーバーでの観測
UDP応答サイズが大きくなっている
http://a.root-servers.org/static/index.html



↑Kルートサーバーでの観測
TCP問い合わせ数は増えている
https://www.ripe.net/analyse/dns/k-root/statistics/?type=ROOT&increment=weekly

←Lルートサーバーでの観測
UDP問い合わせ数は変わらないが
TCP問い合わせ数は減っている
http://stats.dns.icann.org/hedgehog/

1.2 KSKの定期更新

KSKの定期更新について(1/2)

- 2017年7月～2018年3月にかけてKSKの定期更新が実施される予定
  - ルートゾーンのDNSSEC運用方針(DPS)に従ったもの
  - ルートゾーンのDNSSEC署名が開始されて以来初更新
- KSK定期更新の重要日付
  - 2017年7月11日 :　新KSKの事前公開開始
  - 2017年10月11日 : 新KSKでのDNSKEY署名開始
  - 2018年1月11日 :　旧KSKの失効
  - 2018年3月22日 :　旧KSKの削除

KSKの定期更新について(2/2)

- KSK定期更新によるDNSKEY応答サイズの増加
  - KSK更新期間中 :
    864オクテット→1139オクテット
  - KSK+ZSK更新期間中 :
    1139オクテット→1414オクテット(※)
  - 旧KSK失効期間中 :
    864オクテット→1424オクテット(※)

※IPv6の最小Path MTU(1280オクテット)を超える
IPv4でもPath MTUは1200～1400程度が多い

2. 影響と対策

2.1 影響を受ける対象者とその影響

影響を受ける対象者とその影響

- フルリゾルバー運用者
  - 応答サイズが増加したDNSKEYがIPフラグメントにより受け取れなくなる可能性がある
    - DNSSEC検証の有効・無効に関係なし
    - DNSSEC検証を有効にしている場合、DNSKEYが受け取れないとすべてのDNSSEC検証が失敗し名前解決できなくなる
  - DNSSECのトラストアンカー(TA)が更新されない可能性がある
    - すべてのDNSSEC検証が失敗し名前解決できなくなる
- 権威DNSサーバー運用者
  - ルートゾーンのDNSSEC検証失敗により管理するゾーン(ドメイン名)の名前解決ができなくなる可能性がある
- SIer(※)
  - 顧客のフルリゾルバーや権威DNSサーバーが上記の状況になり対応が発生する可能性がある

※顧客のネットワークやサーバー(DNS等)の設計・構築・運用を請け負う事業者

2.2 フルリゾルバー運用者の対策

DNSSEC検証を行っている場合

- ソフトウェアを可能な限り最新のバージョンにしておく
  - RFC 5011(DNSSEC TAの自動更新)に対応したもの(必須)
    - 例) BIND9、Unbound
  - RFC 7646(DNSSEC Negative Trust Anchor; NTA)に対応したもの(推奨)
    - 例) BIND9.11、Unbound、PowerDNS Recursor4
- DNSSEC TAの自動更新設定を有効にしておく

DNSSEC検証を行っていない場合

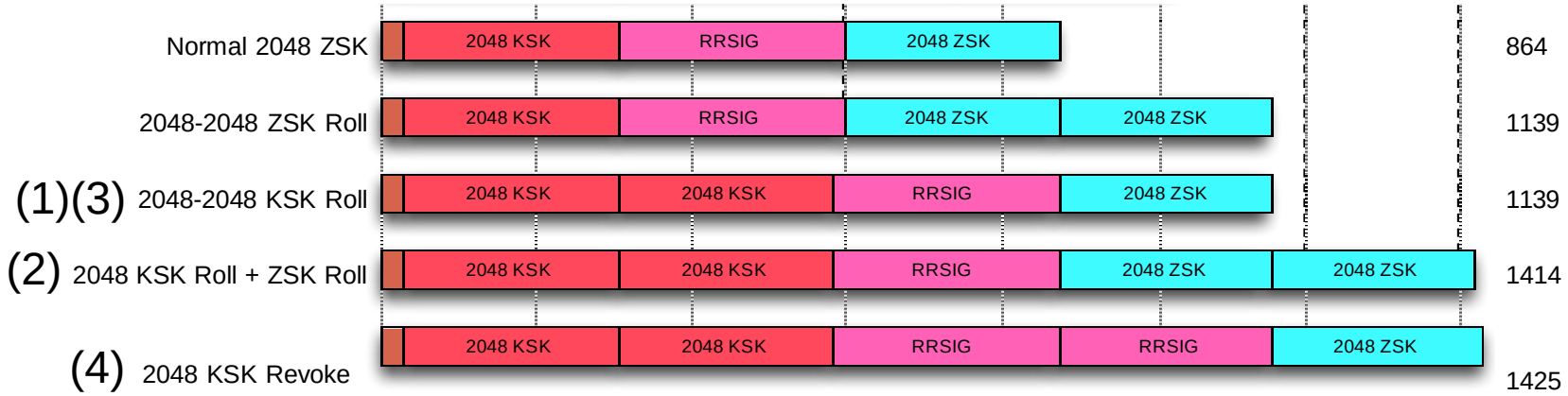
- 受信可能なDNS応答サイズを確認しておく
  - ルートゾーンのDNSKEYサイズ増加に対応できるか知っておくため
    - https://www.dns-oarc.net/oarc/services/replysizetest
- DNSSEC TA自動更新の確認用フルリゾルバーを用意しておく
  - 自分自身のDNSSEECオペレーション習熟のため
    - 貴重な機会を逃す術はない
    - 次のルートゾーンのKSK更新は未定

いずれの場合でも

- ルートゾーンのKSK更新監視手順を作成し、重要日付の前後で実施すること
- フルリゾルバーでのDNSSEC検証停止手順を作成し、ルートゾーンのKSK更新失敗に備えること

ルートゾーンのKSK更新
監視重要日付

(1) 新KSKの公開時(2017年7月11日頃)
(2) 新ZSKの公開時(2017年9月19日頃)
(3) 新KSKでの署名開始時(2017年10月11日頃)
(4) 旧KSKの失効開始時(2018年1月11日頃)



出典: http://schd.ws/hosted_files/icann562016/69/verisign-zsk-change.pdf

ルートゾーンのKSK更新 監視のポイント

- フルリゾルバーへルートゾーンのDNSKEYを問い合わせ、ADビットが返ること

```
$ dig +dnssec . dnskey

; <<>> DiG 9.10.4-P2 <<>> +dnssec . dnskey
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22791
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
```

- ADビットが返らず名前解決が失敗した場合、CDビットをつけた問い合わせは成功する(NOERRORとなる)こと

```
$ dig +dnssec  . dnskey

; <<>> DiG 9.10.4-P2 <<>> +dnssec . dnskey
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 26593
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
```

←ADビットが返らず名前解決失敗

CDビットをつけると名前解決成功→

```
$ dig +dnssec +cd . dnskey

; <<>> DiG 9.10.4-P2 <<>> +dnssec +cd . dnskey
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23311
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
```

DNSSEC検証停止のポイント(1/2)

- DNSSEC検証停止の判断は監視の結果に基づいて行うこと
  - ルートゾーンのKSK更新監視でADが返らず、CDつきは成功する場合に実施すること
  - 外部の情報に頼らないこと
    - 検証が失敗している事実を重視すること
  - 原因の切り分けはDNSSEC検証停止後に行うこと
- DNSSEC検証停止方法は、フルリゾルバーでDNSSEC検証を無効(またはNTAを有効)にすること
  - 例)
    - BINDの場合は”dnssec-validation no;”
    - Unboundの場合は”server: val-permissive-mode: yes”
  - ユーザーに通知すること
    - サポートページにDNSSEC検証無効化のお知らせを載せる、メールを送る、など

DNSSEC検証停止のポイント(2/2)

- DNSSEC検証再開の判断は外部の情報に基づいて行うこと
  - ICANN・JPRSのアナウンスを見ること
    - ルートゾーンのKSK更新そのものの失敗かどうか
  - DNSソフトウェアベンダー・パッケージメンテナのアナウンスを見ること
    - ソフトウェアのバグかどうか
  - 中継機器(ミドルボックス)ベンダーのアナウンスを見ること
    - 設定ガイドやファームウェアの更新がないか

2.3 権威DNSサーバー運用者の対策

DNSSEC署名を行っていない場合

- ルートゾーンのKSK更新に関する外部情報の入手先を整理しておく
  - ICANN・JPRSのアナウンス
  - DNSソフトウェアベンダー・パッケージメンテナのアナウンス
  - 中継機器(ミドルボックス)ベンダーのアナウンス
- ルートゾーンのKSK更新重要日付近辺に発生しうるユーザーからの問い合わせに備えて回答テンプレートを用意しておく
  - 外部情報の参照を勧めるもの

DNSSEC署名を行っている場合

- ルートゾーンのKSK更新失敗時も通常のDNSSEC運用手順を維持することを組織内で合意しておく
  - 自身の権威DNSサーバーでは何もする必要がないことの確認
  - 多重のトラブル発生の防止
- 他は、DNSSEC署名をしていない場合と同様

2.4 SIerの対策

顧客のシステム運用を行っている場合

- 前述のフルリゾールバー運用者および権威DNSサーバー運用者の準備と同様

顧客のシステム運用を行っていない場合

- システム構築時の顧客のフルリゾルバーの設定を確認しておく
  - DNSSEC検証の有無
  - DNSSEC TA自動更新設定の有無
  - ソフトウェアバージョン
- システム構築時の顧客のネットワーク接続機器(ファイウォール等)の設定を確認しておく
  - IPフラグメントを受け付けるか
  - TCPポート53を許可しているか
- ルートゾーンのKSK更新重要日付近辺に発生しうる顧客からの問い合わせに備えて回答テンプレートを用意しておく
  - 権威DNSサーバー運用者の準備と同様

補足事項

- ルートゾーンのKSK更新によるトラブルの発生は極めて低いと考えられる
  - ICANN、ルートDNSサーバーオペレータ、専門家チーム、DNSソフトウェアベンダーによる綿密な計画作成とテストが実施されているため
- なぜトラブルに備え対策するのか
  - DNSSEC検証を行っていないフルリゾルバーもDNSSEC関連レコードの問い合わせを行うため
  - インターネット全体に影響のおよぶDNSSEC TA自動更新の初めての経験であるため
  - 重要日付をわずかな準備で安心して迎えるため

参考URL

- 今日から始めるDNSSECバリデーション
  - https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/t5/
- Root Zone KSK Rollover
  - https://www.icann.org/resources/pages/ksk-rollover
- ドメイン名やDNSの解説
  - https://jprs.jp/related-info/guide/
- DNS-OARC
  - https://www.dns-oarc.net/

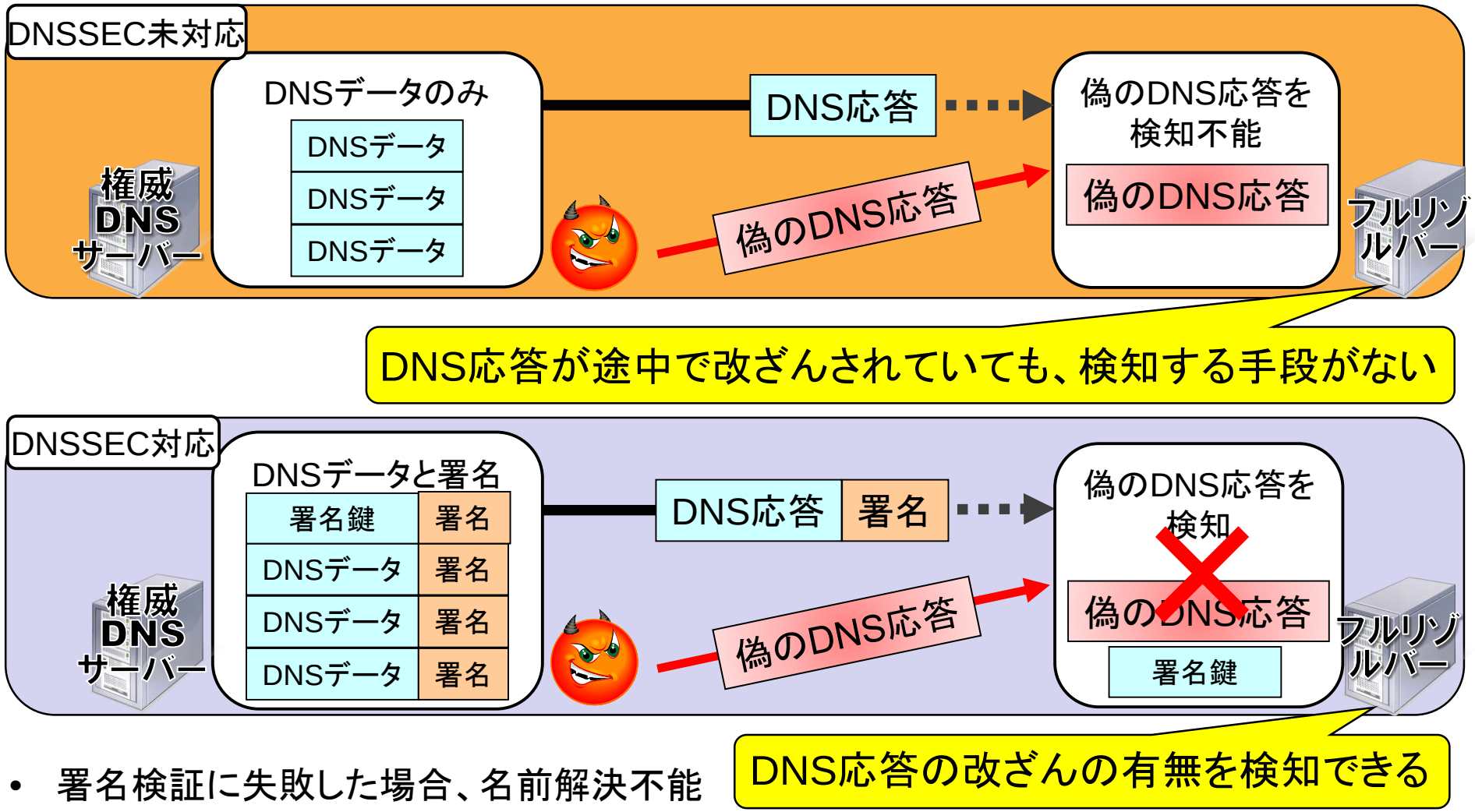
付録：DNSSECのおさらい

DNSSECの概要

- DNSセキュリティ拡張 (DNS Security Extensions)
  - 公開鍵暗号の技術を使い、検索側が受け取ったDNSレコードの出自・完全性(改ざんのないこと)を検証できる仕組み
  - 従来のDNSとの互換性を維持
- DNSSECの対象範囲
  - 対象としているもの
    - 出自の保証
      - DNS問い合わせの応答が、ドメイン名の正当な管理者からのものであることの確認
    - 完全性の保証
      - DNS問い合わせの応答における、DNSレコードの改変の検出
  - 対象としていないもの
    - DNS問い合わせ/応答内容の暗号化

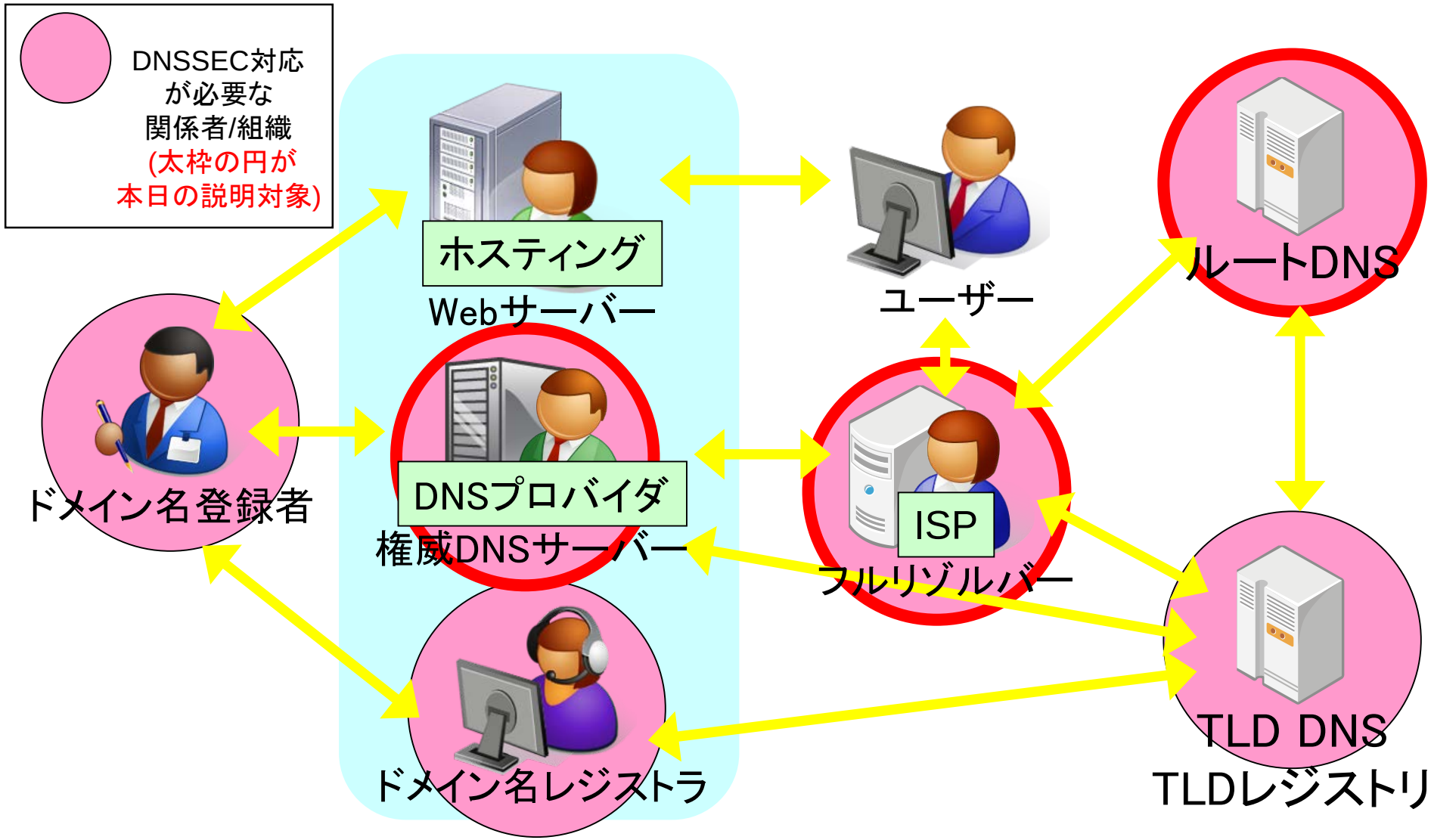
    ※ DNSレコードは公開情報という考え方から

DNSSEC未対応と対応の比較



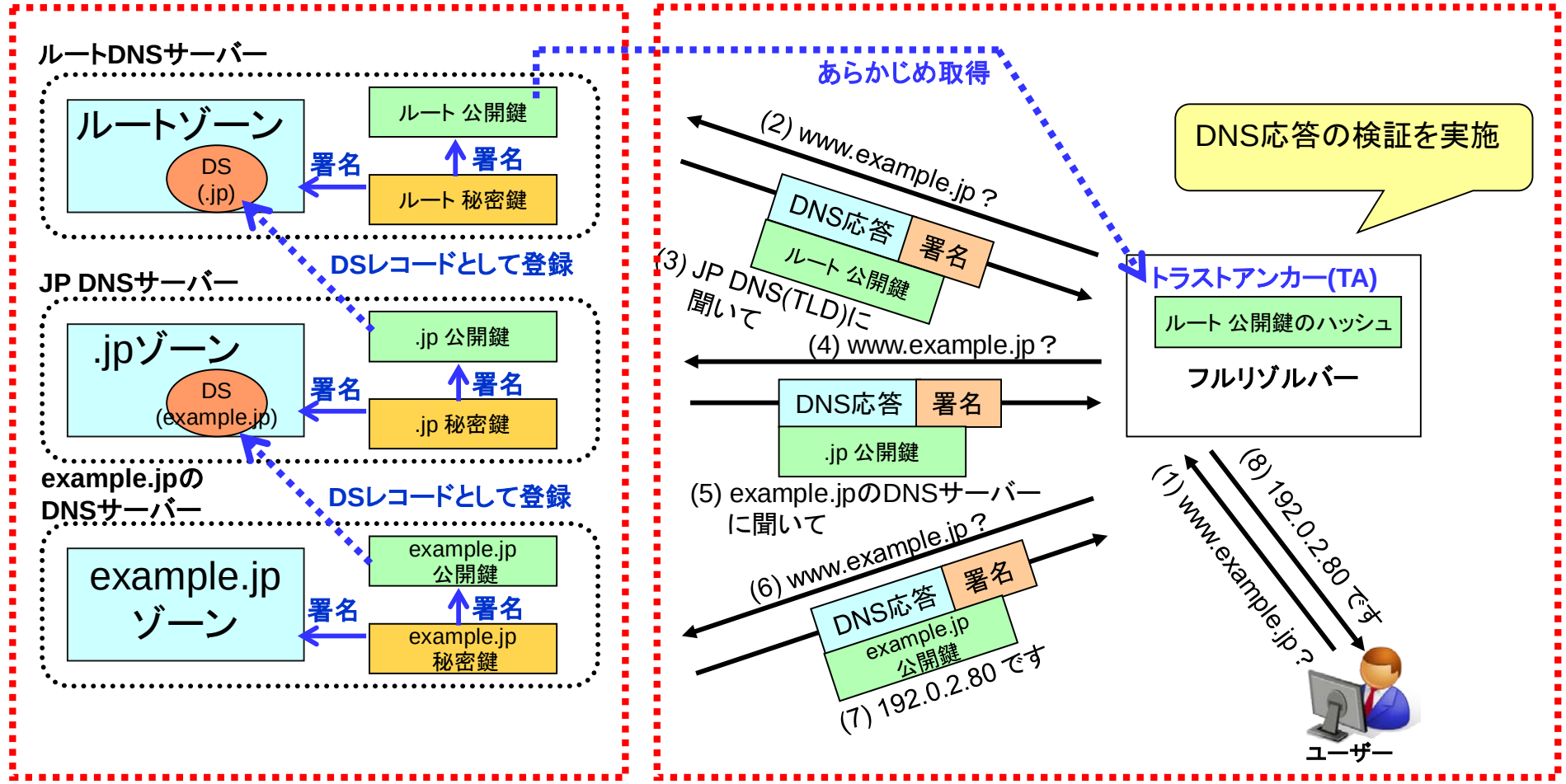
- 署名検証に失敗した場合、名前解決不能
  - DNSSECは偽の応答を検知する技術
    ⇒ 正しい応答を見つけ出す技術ではない

DNSSEC関係者/組織



DNSSEC対応時における名前解決の流れ

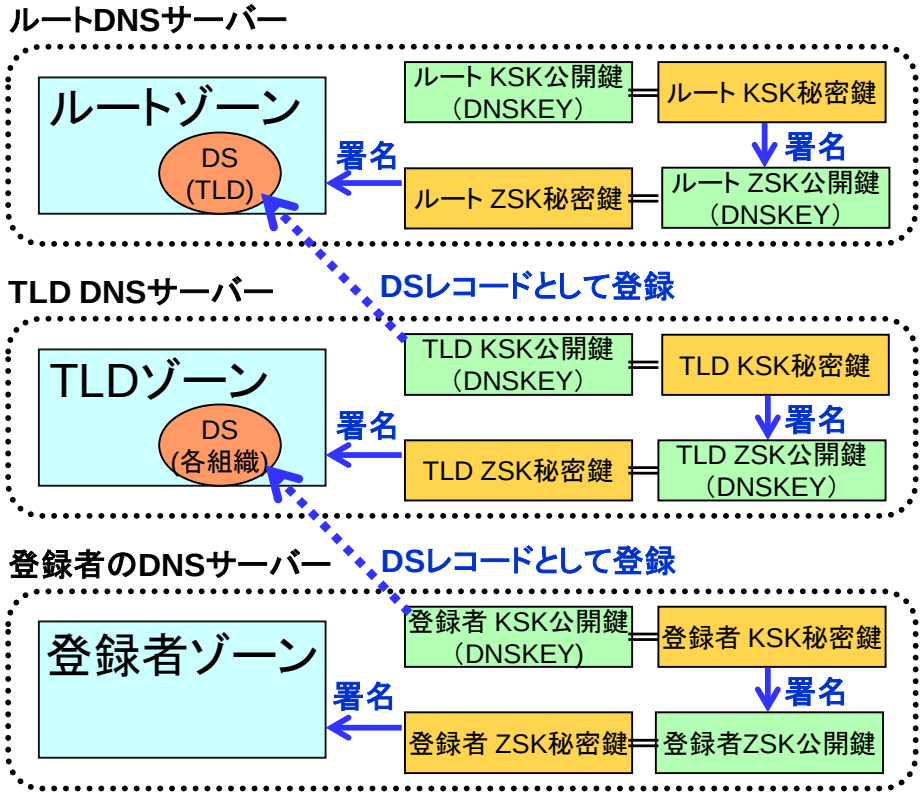
例：www.example.jp の名前解決の流れ



➢ DNSSECの鍵と信頼の連鎖　　➢ DNSSEC検証

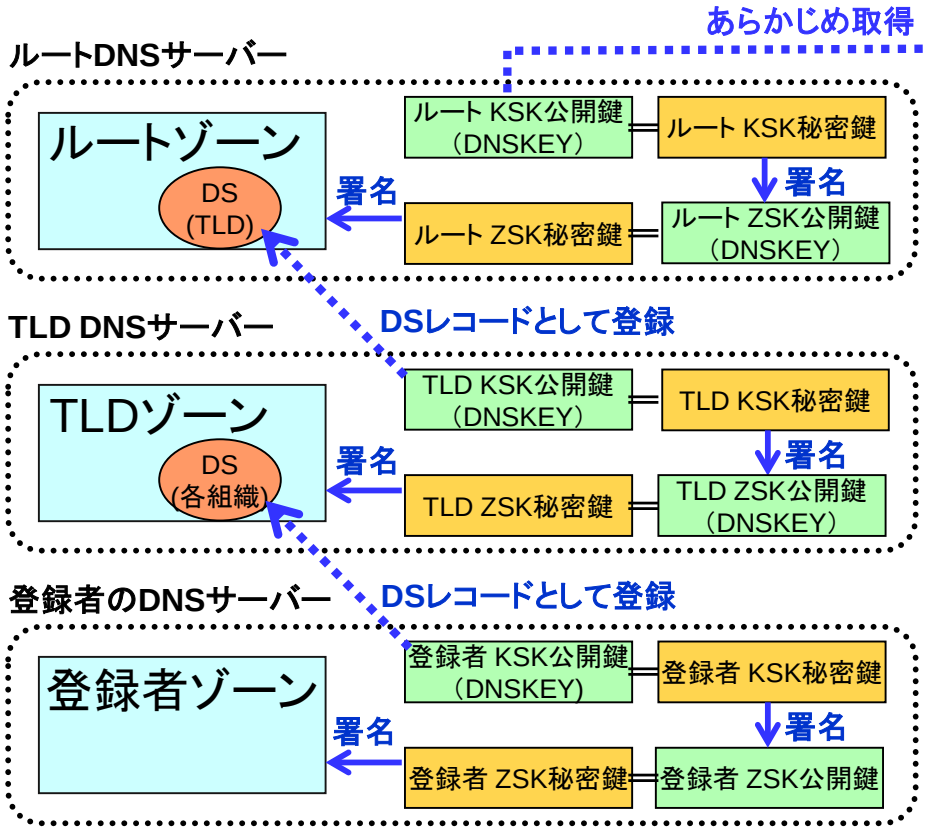
DNSSECで利用する2種類の鍵

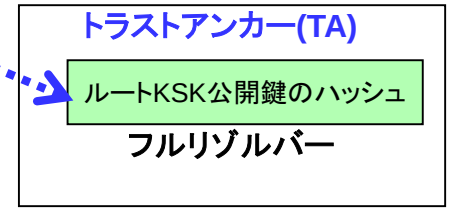
- DNSSECでは ZSK と KSK 2種類の署名鍵を使う



- ZSK (Zone Signing Key)
  - ゾーンのDNSデータに署名するための鍵
- KSK (Key Signing Key)
  - そのゾーンのDNSKEYリソースレコードに署名するための鍵
- DNSKEY (DNS Public Key)
  - ZSK/KSKの公開鍵を示すリソースレコード

DNSSECで利用するDSレコードと信頼の連鎖





- DSレコード（Delegation Signer）
  - KSK公開鍵をハッシュ関数で変換したリソースレコード

- トラストアンカー(TA)
  - 署名が正当なものであるかを検証するための最初の情報(信頼の起点)
  - DNSSECの場合はルートゾーンのKSK公開鍵のハッシュ(DSに相当)
  - フルリゾルバーへの初期設定時以外は自動更新の仕組みが標準化されている(RFC 5011)
- 信頼の連鎖
  - KSK公開鍵を親ゾーンにDSとして登録することで、親ゾーンに署名され信頼を引き継ぐ
  - 親ゾーンはさらに親ゾーンへとDS登録し、信頼を連鎖させる
  - 連鎖がTAまでつながることで、全体が信頼される

ZSKとKSKの2種類の鍵を使う理由

- 公開鍵暗号では、署名の安全性を維持するため、定期的に鍵を更新する必要がある
  - 鍵長を長くすると安全だが署名に必要なCPU時間が多くなる
  - 更新を多くすると安全だが公開鍵情報の配布(信頼の連鎖の作成)に必要な人手作業が多くなる

- DNSSECでは、署名のためのCPU時間と、鍵更新のための人手作業の低減を両立させるため、ZSKとKSKの2種類の鍵を使う

- ZSKのねらい：CPU時間の低減
  - 鍵長を短くして署名のためのCPU時間を低減する
  - 署名の安全性は鍵更新の頻度を多くすることで確保する
    - ZSKの信頼の連鎖はKSKが担う(ゾーン内で閉じる)ため、更新作業はほぼ自動化することが可能

- KSKのねらい：人手作業の低減
  - 更新の頻度を少なくしてKSKの公開鍵情報(DS)を親ゾーンに登録するための人手作業を低減する
  - 署名の安全性は鍵長を長くすることで確保する
    - 署名対象はDNSKEYのみなので署名のためのCPU時間は問題にならない