# ルートゾーンの
# KSKロールオーバーについて

2017年6月28日

DNSOPS.JP DNS Summer Day

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

# はじめに

- 本セッションは以下の2部構成です
  - ルートゾーンのKSKロールオーバーの概要　【JPRS米谷】
  - ISPから見た事前確認・準備のポイント　【QTNet末松】

- DNSおよびDNSSECの解説はいたしません
  - 4スライド目で紹介する元資料①の参考をご参照ください

# ルートゾーンの
# KSKロールオーバーについて
# 【概要編】

# 概要編のもくじ

1. ルートゾーンの鍵更新
2. 影響と対策
3. スケジュールと重要日付

本資料中のスライドは以下のスライドから抜粋・一部修正しています。
①IW2016 DNS DAY・DNSSEC UPDATE
https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/d3/d3-2-yoneya.pdf
②JANOG39 LT・ IPフラグメントがやってくる！準備できていますか？
https://www.janog.gr.jp/meeting/janog39/application/files/5014/8471/4979/JANOG39-LT-yoneya.pdf
抜粋したスライドには、左上に元資料の番号とページ番号を「①-15」のように示しています。修正があるものは「②-4改」のように示しています。

# 1. ルートゾーンの鍵更新

①-4

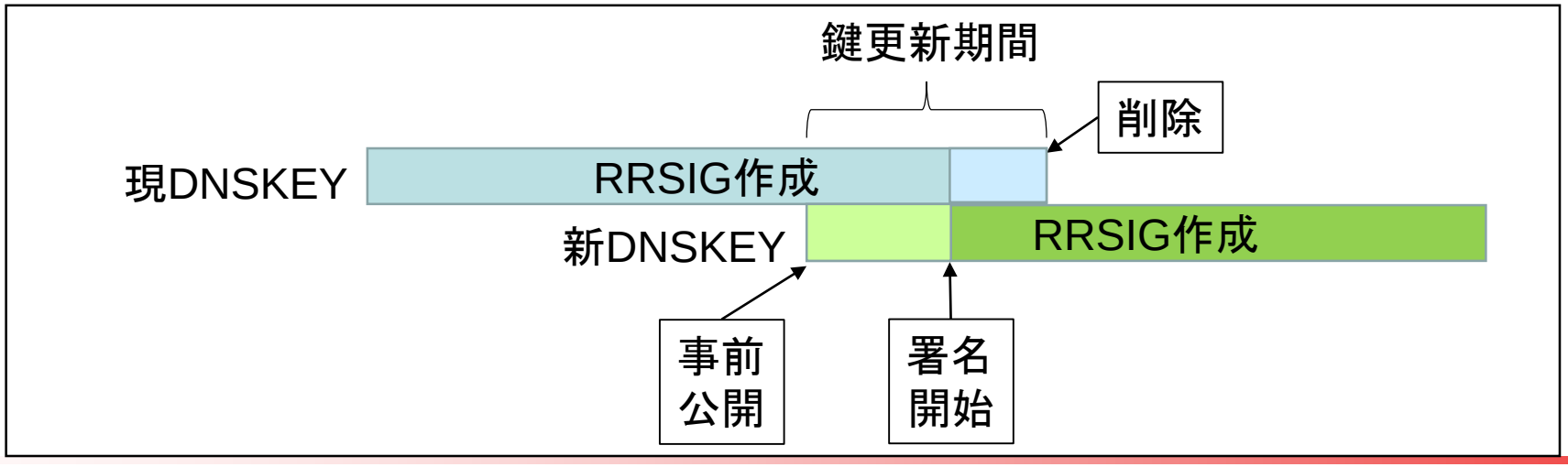
# ルートゾーンにおける鍵更新の種類

- 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



# 2. 影響と対策

①-15

# 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

# 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

②-5改

# 今すぐできる IPフラグメント確認方法

- 名前解決の失敗を発生させないため、今すぐ自分のフルリゾルバー（キャッシュDNSサーバー）がIPフラグメントで名前解決に失敗しないか確認を！
  - フルリゾルバーはDNSSEC検証の有無に関わらずDNSKEYを取得しているため
- Webでの確認方法
  - http://keysizetest.verisignlabs.com/
- コマンドラインでの確認方法（※）
  - dig +bufsize=4096 +short rs.dns-oarc.net txt

IPv4/IPv6両トランスポートをサポートしている場合は、digに-4および-6オプションをつけて両トランスポートともに確認を！

※ https://www.dns-oarc.net/oarc/services/replysizetest

# 準備しておくこと

- IPフラグメントで名前解決が失敗した場合
  - 原因の究明
    - サーバーソフトウェアか？
    - ***ネットワーク接続機器か？***
  - 対策の段取りと実施
    - フリリゾルバー（キャッシュDNSサーバー）の更新
    - ***ネットワーク接続機器の設定変更・更改***
    - ***上位ISP等への相談***
    - etc.
- IPフラグメントで名前解決が失敗しなかった場合(名前解決の失敗が解消した場合)
  - Root Zone KSK Rollover経過観察の段取り

# 3. スケジュールと重要日付

②-3

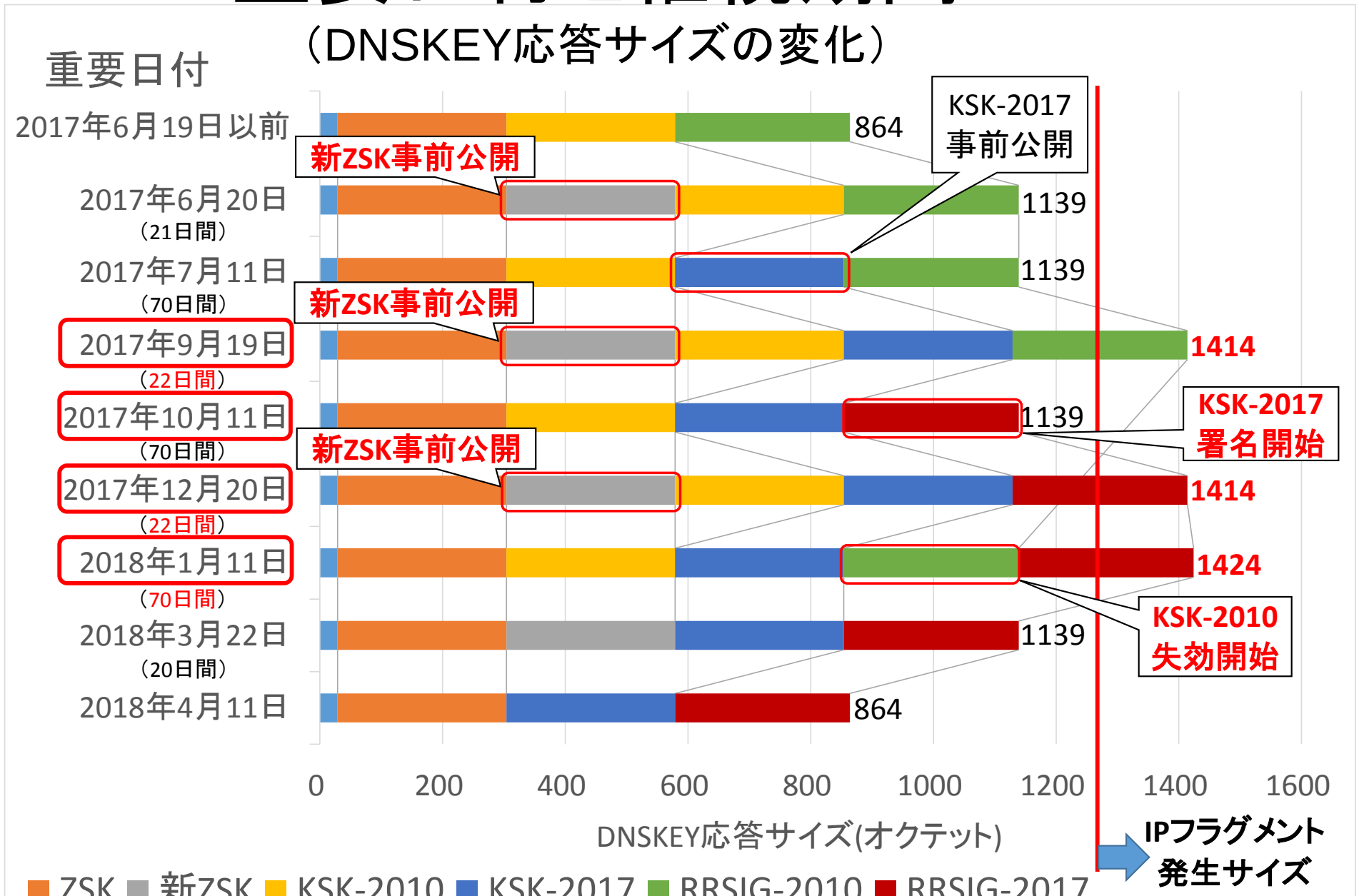
# Root Zone KSK Rolloverの概要

- 実施期間
  - 2017年7月1日～2018年3月31日
  - 2017年10月11日にKSKが更新
- 鍵更新方法
  - 事前公開方式で新KSK（KSK-2017）を公開
  - ZSKの定期更新（事前公開方式）と並行して実施
  - RFC 5011方式でトラストアンカーを自動更新（&失効）
- 影響
  - KSKとZSKの更新期間中にDNSKEYの応答サイズが1400オクテットを超える
  - KSK更新後、現KSK（KSK-2010）の失効期間中にDNSKEYの応答サイズが1400オクテットを超える

***DNS応答のIPフラグメントがやってくる！***
***Rootゾーンの名前解決に失敗するかも？***

②-4改

# 重要日付と継続期間



②-7改

# コミュニケーションチャネル・有益リンク

- 今日から始めるDNSSECバリデーション（IW2015）
  - https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/t5/
- IW2016 DNS DAY DNSSEC Update
  - https://www.nic.ad.jp/ja/materials/iw/2016/proceedings/d3/d3-2-yoneya.pdf
- JANOG39 LT・IPフラグメントがやってくる！準備できていますか？
  - https://www.janog.gr.jp/meeting/janog39/application/files/5014/8471/4979/JANOG39-LT-yoneya.pdf
- DNSSECバリデーションにおけるルートゾーンKSKロールオーバーに関する重要なお知らせ
  - https://www.nic.ad.jp/ja/topics/2017/20170531-02.html
- Root Zone KSK Rollover（ICANN公式ページ及びML)
  - https://www.icann.org/resources/pages/ksk-rollover
  - https://mm.icann.org/mailman/listinfo/ksk-rollover
  - https://mm.icann.org/mailman/listinfo/root-dnssec-announce
- ドメイン名やDNSの解説（JPRS）
  - https://jprs.jp/related-info/guide/
- DNS-OARC
  - https://www.dns-oarc.net/

Root Canary
- https://rootcanary.org/

コミュニケーションチャネルの追加をICANNと相談中デス！