

DNS  
応答の

IPフラグメントがやってくる！  
準備できていますか？

2017年1月20日 JANOG39 LT

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

# はじめに

- 本日の目的は以下を知ってもらうことです
  - RootゾーンのKSK更新に関する重要日付
  - IPフラグメント発生有無の確認方法
  - 影響を受ける人が準備しておくこと
- DNSSECの仕組みは解説しません

# 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

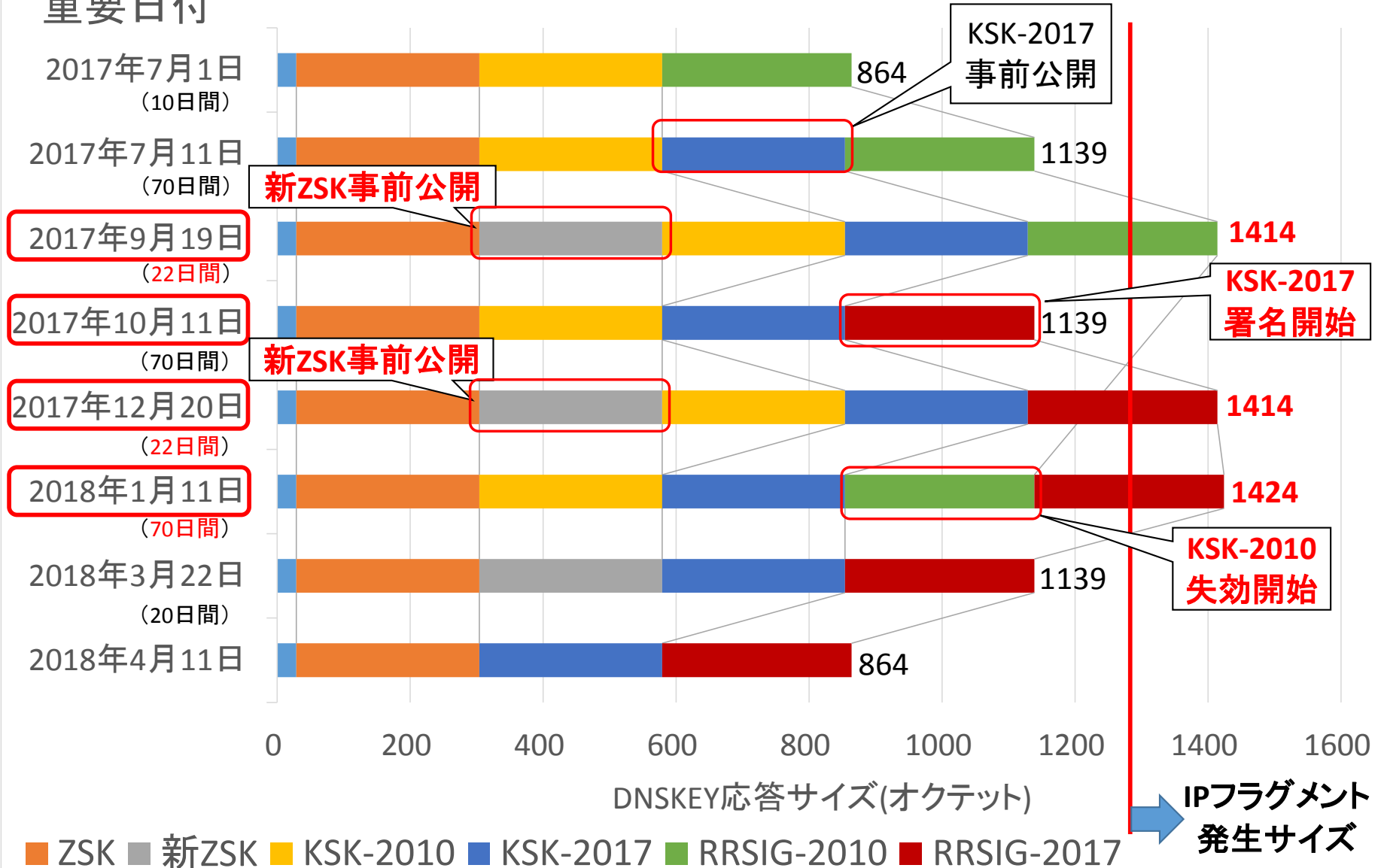


**DNS応答のIPフラグメントがやってくる！  
Rootゾーンの名前解決に失敗するかも？**

# 重要日付と継続期間

(DNSKEY応答サイズの変化)

## 重要日付



# 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`

※ <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

# 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
  - Coming soon !
- 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/>

コミュニケーションチャネルの追加をICANNと相談中デス！