関谷 勇司 (WIDE Project / 東京大学)

ROOT KSK Rollover

KSK Rollover とは

- ご存知。。。ですよね？
  - DNSSEC にて検証するための鍵です
  - KSK (Key Signing Key) と ZSK (Zone Signing Key) という鍵があります
- KSK は ZSK を署名するための鍵
  - ドメインにとっての大元となる鍵
- その鍵の更新を行うことを Rollover と呼んでいます

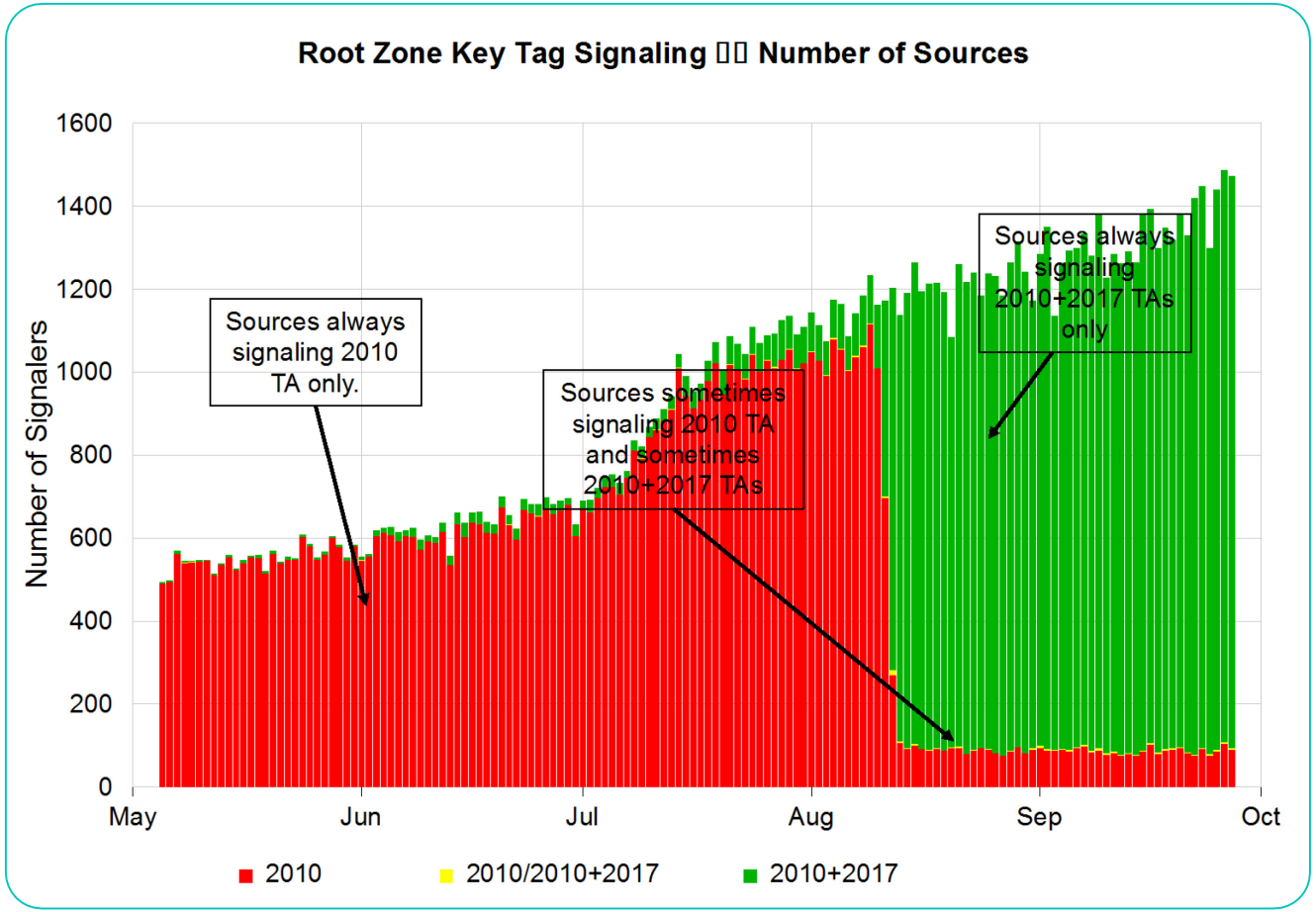
Root ZONE の KSK

- Root ZONE の KSK とは
  - 「. 」ゾーンの KSK です
  - つまり DNS 名前空間の頂点となる鍵ですね
- これを更新するというイベントが発生します
- どんな影響が？
  - 適切に設定されていないと DNSSEC の検証ができなくなります

まずその第一段階

- 新しい鍵 (KSK) での署名を開始
  - つまり Key Rollover
  - これが 2017年10月11日に行われるはずでした
- でも。。。
  - 延期されました
    (昨年報告した通り)
- なんで？
  - 新しい鍵に対応する設定がなされていない
  - パケットサイズの増大に対応できていない

IW2017 で紹介した資料



一年かけて下準備が行われました

- DNS リゾルバサーバが KSK Rollover に対応できるか
- パケットサイズの増加に対応できるか

- ICANN による積極的 (？) なリゾルバサーバ調査も行われました

こんなメールも送られてきました

From : **ksk2018prep@icann.org**

To repeat this important point: any DNS resolvers on your network with DNSSEC validation enabled that are not properly updated to use the new KSK will unable to resolve names on 11 October 2018 or shortly thereafter (the exact time of failure is uncertain due to caching).

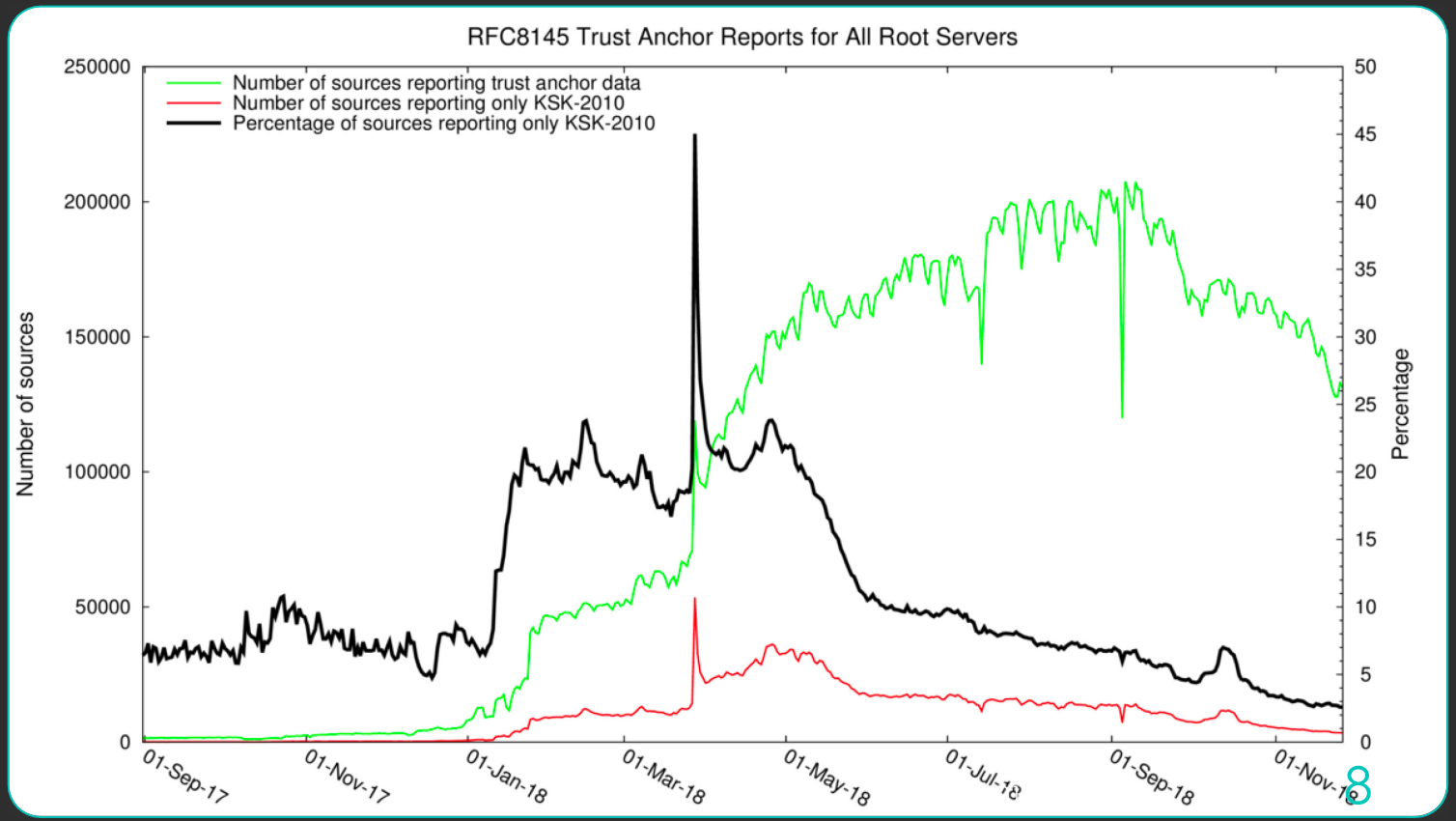
At the end of this message, please find a list of IP addresses from ASXXXX that since 1 September 2017 have sent at least one trust anchor configuration report indicating they were not configured with the new KSK.

KSK-2010 だけを持っている DNS サーバ

- リストがあります
  - http://root-trust-anchor-reports.research.icann.org/rfc8145-addresses.txt
- 皆様の AS は含まれていたりしませんでしょうか
  - 日本の AS は成績優秀みたいです
  - ほとんど含まれていない
- DNS 関連事業者の努力の結果。。。なのかな
- 本日の時点で見つけてしまったもの。。。
  - 131912　　103.79.12.129

リゾルバ DNS サーバの Trust Anchor 動向

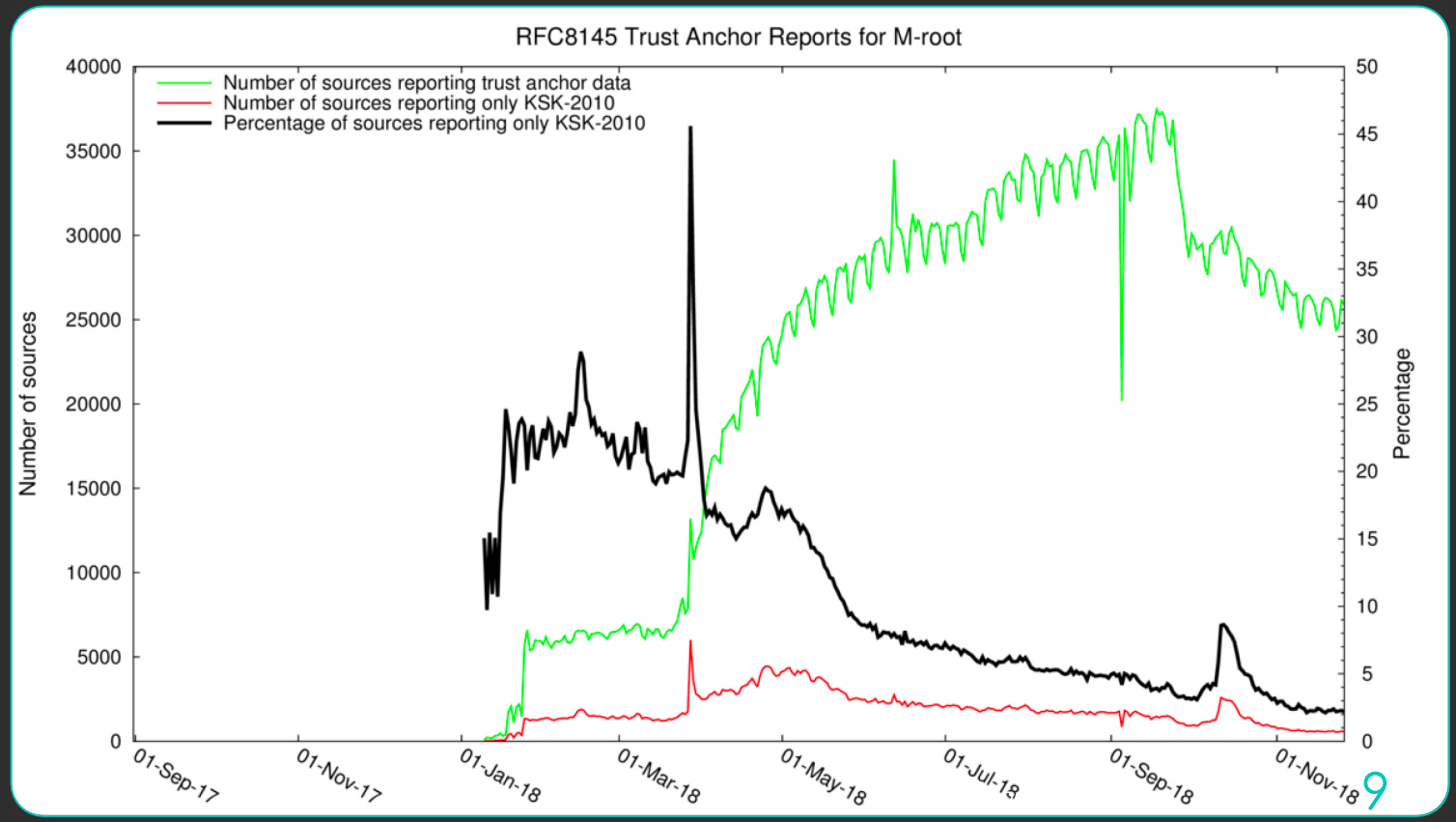
- KSK-2010 のみを持っている DNS サーバは減っています
- しかし当然ゼロにはならないですよね



http://root-trust-anchor-reports.research.icann.org/

M-ROOT だけを見てみると

- 全 ROOT DNS サーバと同じ傾向を示しています
- Rollover 時に多少の spike があるのも同傾向です



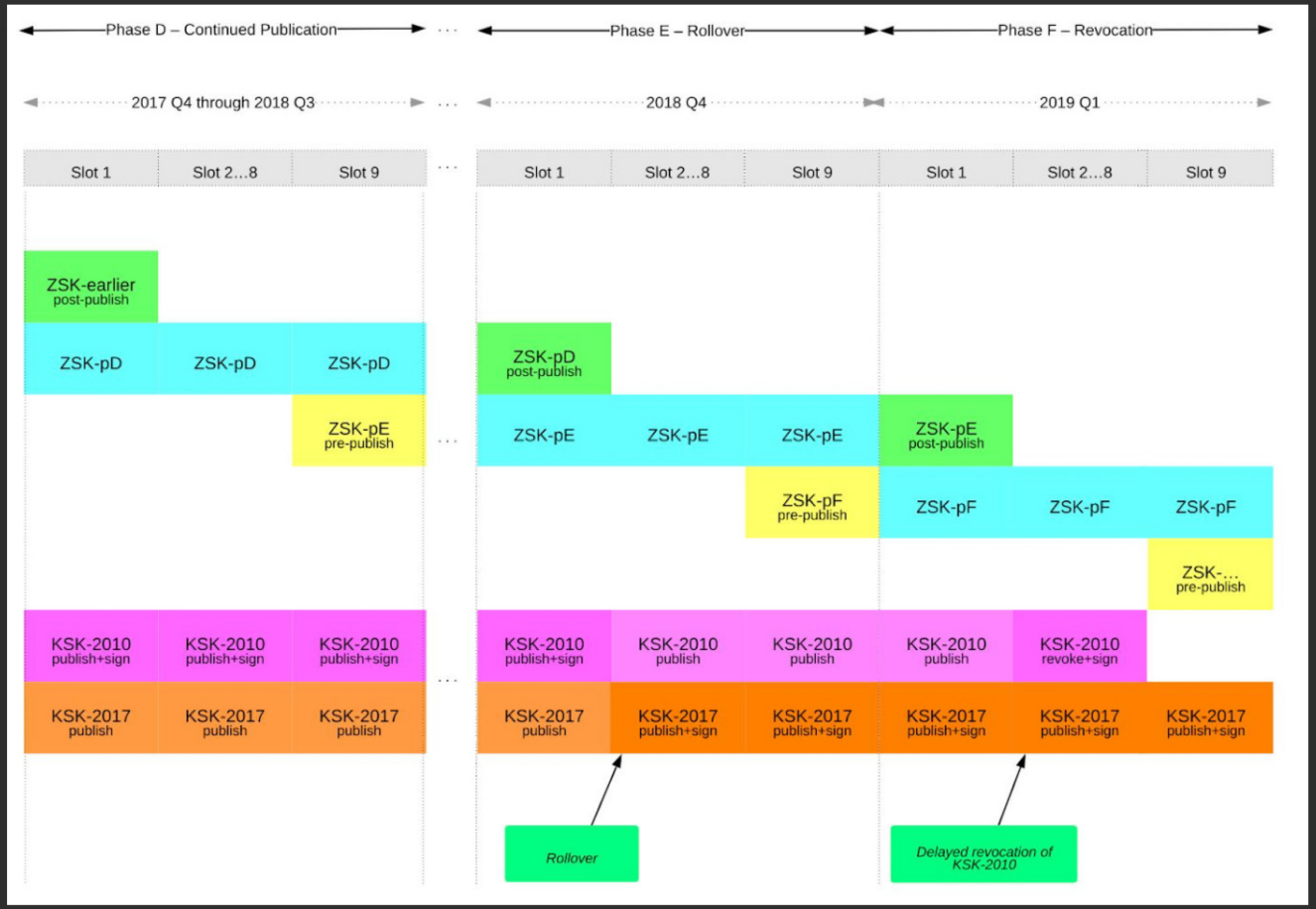
http://root-trust-anchor-reports.research.icann.org/

今更だけど確認点

- Bind の場合
  - dnssec-validation の設定
  - auto / yes / no
- auto の場合やディストリビューションのパッケージを利用している場合はほぼ問題ないでしょう
  - yes で手動更新の場合は注意
- Unbound の場合
  - auto-trust-anchor-file を指定しているか
  - してあれば問題ないでしょう
- DNSSEC を無効にしている
  - val-permissive-mode: yes
  - module-config: "iterator"
  - トラストアンカー削除

KSK Rollover の予定表

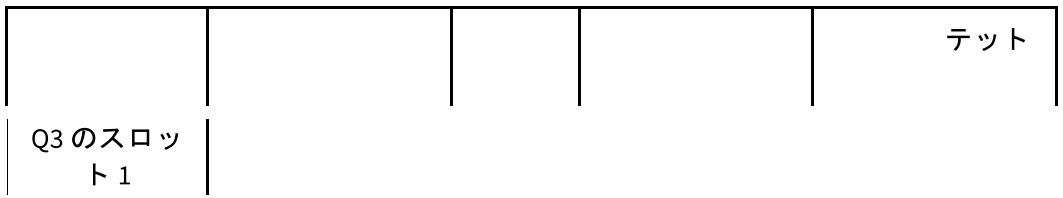
- １年遅れ
- 2017年9月19日
  - 新しい KSK と ZSK を Root zone で公開
- 2018年10月11日
  - 新しい KSK による署名開始
- 2019年1月11日
  - 古い KSK の失効開始
- 2019年3月22日
  - 古い KSK の完全失効



https://www.icann.org/en/system/files/files/2018-ksk-roll-operational-implementation-plan.pdf

パケットサイズの変化

- 要するに以下の期間は注意が必要
  - Q1 slot 2-8
  - Q1 slot 9
  - Q3 slot 2-8
- Q1 slot 2 – 8 , Q1 slot 9
  - 新しい KSK を公開してから rollover の間
  - つまりもう終わってます
- Q3 slot 2-8
  - 古い KSK の Revocation 期間



https://www.icann.org/ja/system/files/files/root-zone-ksk-rollover-plan-draft-04aug15-ja.pdf

結論として

- 平和に行われました
  - Root DNS を観測する限りでは異常事態は起こっていません
- Root DNS Server Operators からの声明

  To the extent of the knowledge of the root server operator organisations, the KSK rollover did not lead to any noticeable impact at all on the root server system. When the new version of the root zone, with signatures created by the new KSK, was published, all service points were automatically updated according to normal procedures, and no significant increase in traffic or other unusual activity occurred.

こういった KSK Rollover 関連の動向は

- スケジュール変更とかが事前に Root Operators に連絡がある。。。と思うでしょ
- 見事に全然ないんですよ
- 全く先行しての連絡は無く、ICANN の公開によって知らされることが多いです
- 文句は出ています
- いろいろ計測したりしなければなりませんから
- その準備とかね