ルートゾーン KSKロールオーバー の経緯

2017年11月30日

Internet Week 2017 D2 DNS DAY

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

はじめに

- 本セッションは2017年の大きなトピックスであるルートゾーンKSKロールオーバーの経緯や状況をお話しします

- DNSおよびDNSSECの解説はいたしません

(this page intentionally left blank)

経緯と状況

ルートゾーンのDNSSEC年表

年月	イベント	備考
2010/01-2010/07	検証不能な署名の追加	[A-M].root-servers.netへの段階的な展開
2010/07/15	**検証可能な署名開始・鍵公開**	
2010/10	最初のZSKロールオーバー実施	以降、3か月ごとに定期実施[1][2]
2014/12	KSKロールオーバーデザインチーム公募開始	
2015/02	デザインチーム決定・活動開始	外部識者7名＋ICANNスタッフ
2015/08	KSKロールオーバードラフトプラン公開	この時点では日程未定
2016/03	KSKロールオーバープラン確定・公開	この時点でも日程未定[3]
2016/04	**ZSK鍵長変更発表**	**1024bit→2048bitへ、6ヶ月前の発表[4]**
2016/07/26	KSKロールオーバー日程確定	1年前の発表
2016/09/20	2048bit ZSK事前公開	以降、ZSKは2048bit
2017/07/11	新KSK(KSK-2017)事前公開	
2017/09/19	**DNSKEY応答サイズが1400バイト超**	**悪影響は観測されず[5]**
2017/09/27	**KSK-2017による署名開始延期発表**	**影響調査継続中[6]**

[1][2] キーロールオーバーの計画(当初)

[1] ルートKSK

- http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt
- “6.5. Key signing key roll-over”

  Each RZ KSK will be scheduled to be rolled over through a key ceremony as required, or after 5 years of operation.

[2] ルートZSK

- http://www.root-dnssec.org/wp-content/uploads/2010/06/vrsn-dps-00.txt
- “6.4. Zone signing key roll-over”

  RZ ZSK rollover is carried out quarterly automatically by the system. ZSK key signing is conducted manually every three months. The necessary ZSKs to be used in between these gatherings are pre-generated and signed at the same occasion with the projected signature inception- and expiration time.

[3] KSKロールオーバープラン

- 想定していたこと：ロールバック
  - KSKロールオーバーが失敗したときのロールバック方法
  - ロールバックを判断する基準
    - KSKロールオーバー後72時間以内にインターネットユーザの0.5%が悪影響を受けた場合
- 想定していなかったこと：途中延期の判断基準
  - 十分に時間をかけて準備を進めたはずだったが、、、

[4] ZSK鍵長増加

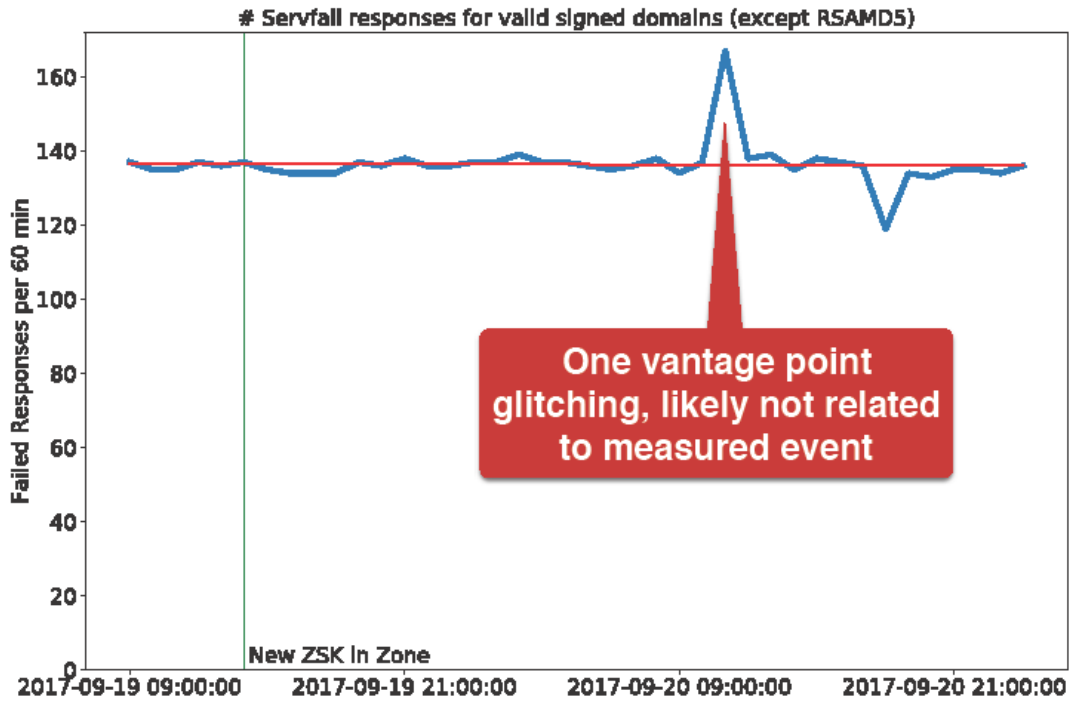
- 2016年4月のDNS-OARC Workshopで発表
  - https://indico.dns-oarc.net/event/22/session/4/contribution/14/material/slides/0.pptx
  - 2016年9月に事前公開されるZSKから2048bit化へ
  - あまりのショートノーティスに世間が驚いた
  - KSKロールオーバー時のDNSKEY応答サイズ増大が懸念されるようになった

[5] DNSKEY応答サイズ増大の影響

- 2017年9月19日にKSK-2017事前公開によりDNSKEY応答サイズが1414バイトになった
  - 国内外いずれからも、IPフラグメント発生による***名前解決失敗の事例は聞かれなかった***
  - ***みなさんの真摯な準備に感謝します！***

So what happened?

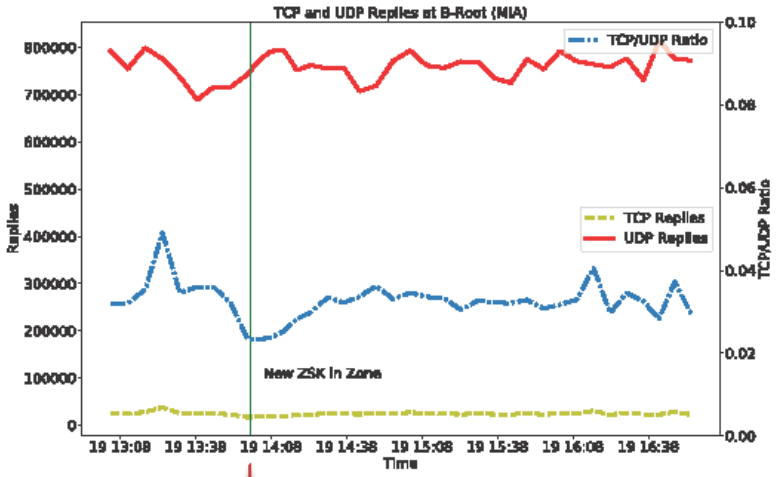
- Preliminary Findings after 2017-09-19: RIPE NCC RIPE Atlas



https://rootcanary.org/

https://datatracker.ietf.org/meeting/100/materials/slides-100-maprg-the-root-canary-measuring-the-root-ksk-rollover-and-beyond-roland-van-rijswijk/

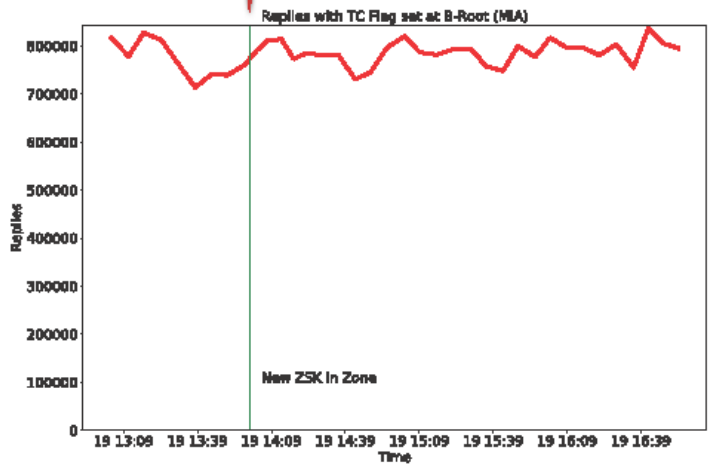
What about traffic to the root?



No noticeable increase in TCP traffic

with thanks to Wes Hardaker (USC/ISI) for preliminary access to B-root traffic

No noticeable increase in truncated responses



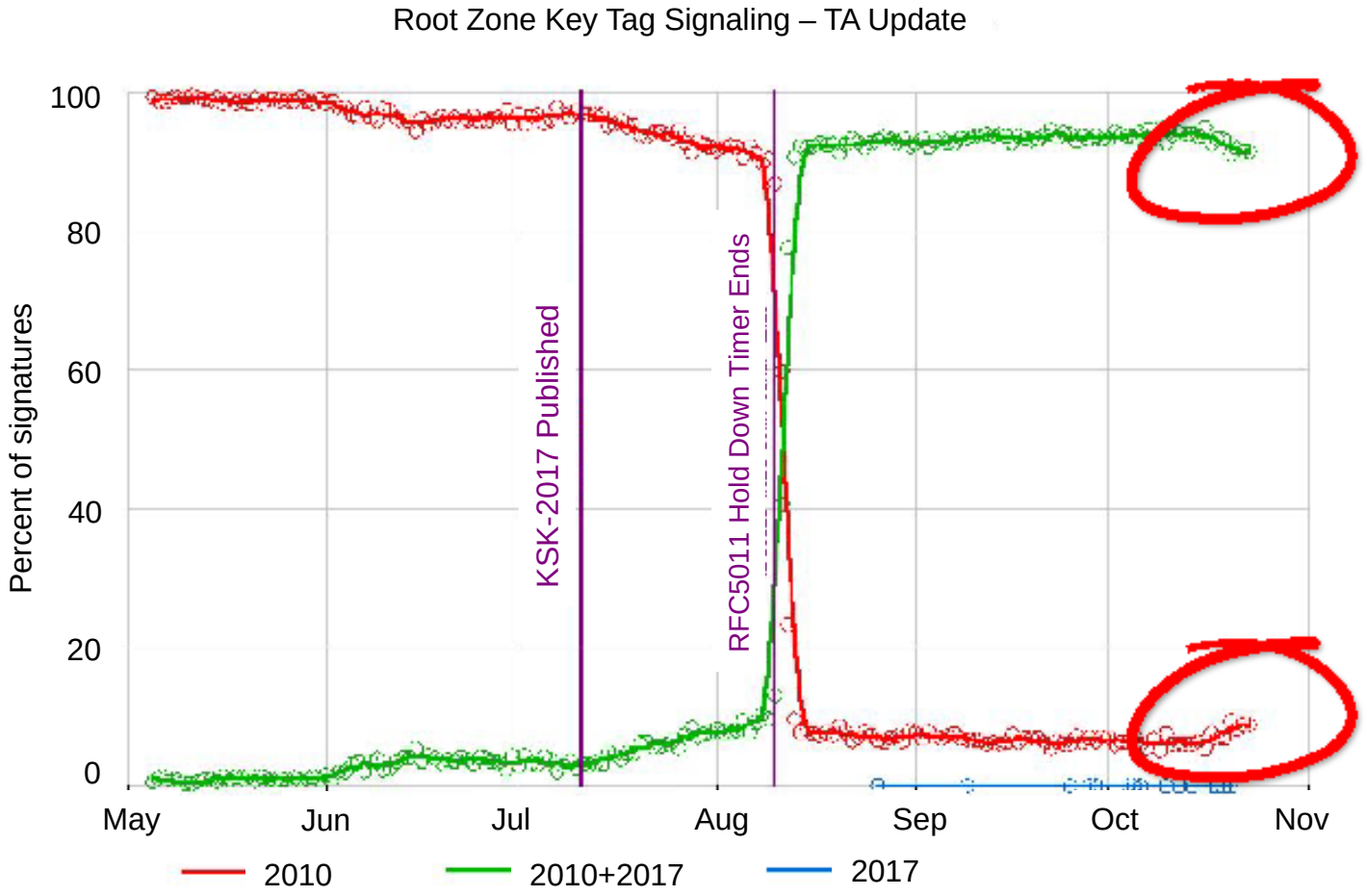
https://rootcanary.org/

https://datatracker.ietf.org/meeting/100/materials/slides-100-maprg-the-root-canary-measuring-the-root-ksk-rollover-and-beyond-roland-van-rijswijk/

[6] KSK-2017による署名開始の延期

- 2017年9月27日にICANNが発表
  - 新しいKSK(KSK-2017)を持っていないフルリゾルバの数が無視できない割り合い(5%程度)存在していることが分かった
    - ICANNは重大な影響を懸念して延期の判断を下した
    - ただしこれはルートKSKロールオーバー計画にはない判断であった
  - あまりの突然の判断に世間が驚いた
  - 次の日程は未定、早くても2018年1月ということだが、、、

Hmmmm….



http://www.iepg.org/2017-11-12-ietf100/03-dconrad-dns.pdf

覚えておいてもらいたいこと

ルートゾーンKSKロールオーバーは終わっていません

- KSK-2010からKSK-2017への変更日程、およびそれ以降の関連作業日程(KSK-2010の失効など)が延期になっただけであり、プロセスが停止されたわけではない
  - ロールオーバーが失敗してロールバックしたわけではない

フルリゾルバ運用者の対応

- ICANNから個別にKSK-2017に対応していないという連絡があったら、以下を参考に対応してください
  - https://www.icann.org/dns-resolvers-updating-latest-trust-anchor
  - BIND、Unboundともに複数のKSKを持っておくことが可能です
  - 手動でKSKを切り替える予定の人も、事前にKSK-2017も入れておくことが可能ということです
- KSK-2010+2017の観測量が多くなればICANNは日程を決定できます！

Q&A

リンク集

- Root Zone KSK Rollover (ICANN)
  - https://www.icann.org/resources/pages/ksk-rollover
- KSKロールオーバー (DNSOPS.JP)
  - http://dnsops.jp/event/20170628/20170628-RootKSKRO-02.pdf
  - http://dnsops.jp/event/20170628/DNS_Summer_DAY_KSK_RO_sue v0.1.pdf
- DNS関連技術情報 (JPRS)
  - https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.html
  - https://jprs.jp/tech/notice/2017-08-10-root-zone-ksk-rollover-qa.html
- KSKロールオーバーについて (JPNIC)
  - https://www.nic.ad.jp/ja/dns/ksk-rollover/