Root Operator からみた KSK Rollover

関谷 勇司
WIDE PROJECT / 東京大学

もともとの予定

1 July 2017	New KSK published in DNS
19 September 2017	Size increase for DNSKEY response from root name servers
11 October 2017	New KSK begins to sign the root zone key set (the actual rollover event)
11 January 2018	Revocation of old KSK
22 March 2018	Last day the old KSK appears in the root zone
August 2018	Old key is deleted from equipment in both ICANN Key Management Facilities

リゾルバ DNS サーバ

みなさんが利用しているリゾルバ DNS サーバは
KSK Rollover に対応していますか？

```
sekiya[~]% dig +bufsize=4096 +short rs.dns-oarc.net txt @ns.nc.u-tokyo.ac.jp
rst.x1013.rs.dns-oarc.net.
rst.x2005.x1013.rs.dns-oarc.net.
rst.x2506.x2005.x1013.rs.dns-oarc.net.
"2001:200:180:32::120 DNS reply size limit is at least 2506"
"2001:200:180:32::120 sent EDNS buffer size 4096"
"Tested at 2017-11-28 11:20:16 UTC"
```

```
sekiya[~]%  dig +bufsize=4096 +short rs.dns-oarc.net txt
rst.x1363.rs.dns-oarc.net.
rst.x1373.x1363.rs.dns-oarc.net.
rst.x1379.x1373.x1363.rs.dns-oarc.net.
"27.86.5.20 sent EDNS buffer size 1410"
"Tested at 2017-11-28 11:25:36 UTC"
"27.86.5.20 DNS reply size limit is at least 1379"
```

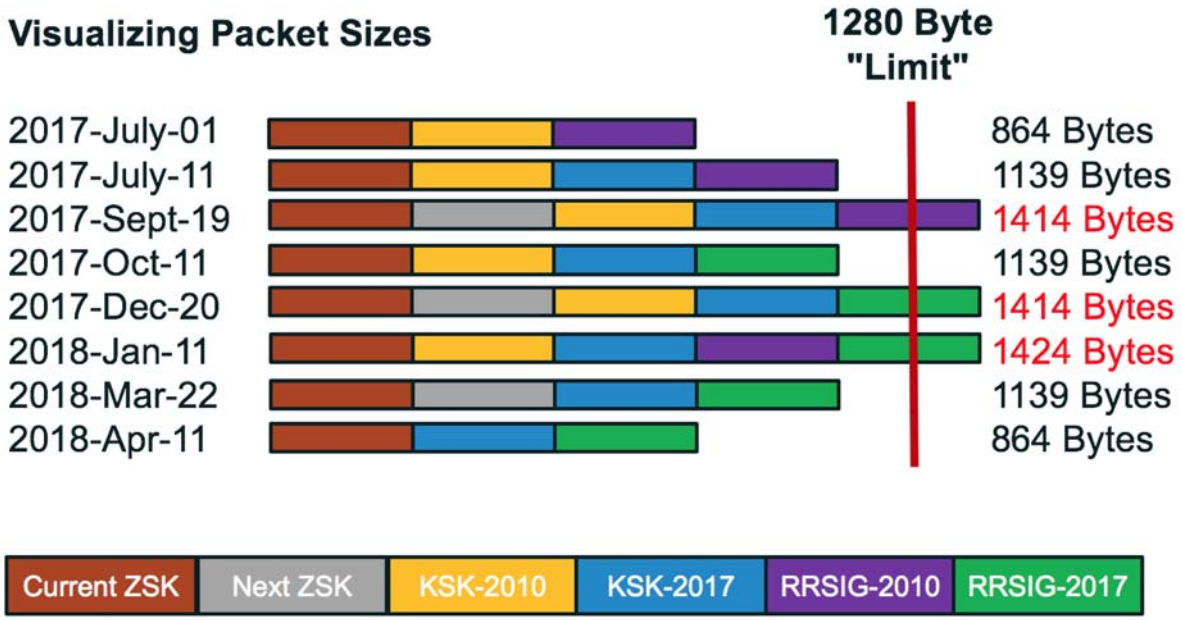
連絡が来たりもしました

「東京大学にある DNS サーバが Root ZONE の　KSK Rollover に対応しておりません」

「どれやねん」

Root ZONE KSK Rollover

Impact on the KSK Rollover Process



出典 : ICANN KSK Rollover Presentation

パケットサイズ問題 (2017/05/14 時点)

Root	IPv4			IPv6			ICMPv6 PTB	
	Truncate	Fragment	TCP MSS	Truncate	Fragment	TCP MSS	UDP	TCP
A	1,500		1,460	1,280		1,440		Y
B	1,280		1,460	1,280		1,440		N
C		1,500	1,460		1,500/1,280 *	1,440	Y	N
D	1,500		1,460	1,500		1,440	Y	Y
E		1,500	1,460		1,500/1,280 *	1,440	Y	N
F		1,500	1,460		1,280	1,440		**
G	1,280		1,460	1,280		1,440		N
H		1,500	1,460		1,500/1,280 *	1,440	N	Y
I		1,500	1,460		1,280	1,220	Y	
J	?		1,460	1,280		1,440		N
K		1,500	1,460		1,500/1,280 *	1,220	N	
L		1,500	1,460		1,500	1,440	Y	N
M		1,500	1,460		1,280	1,440		**

* 1,500/1,280 - these servers will send up to 1,500 octet responses, but will fragment at the 1,280 octet point

** These servers fragmented the TCP segments at 1,280 octets

お？

出典 : Geoff Huston (APNIC) 資料

Trust Anchor Signaling

RFC8145 として定義 (2017年4月)

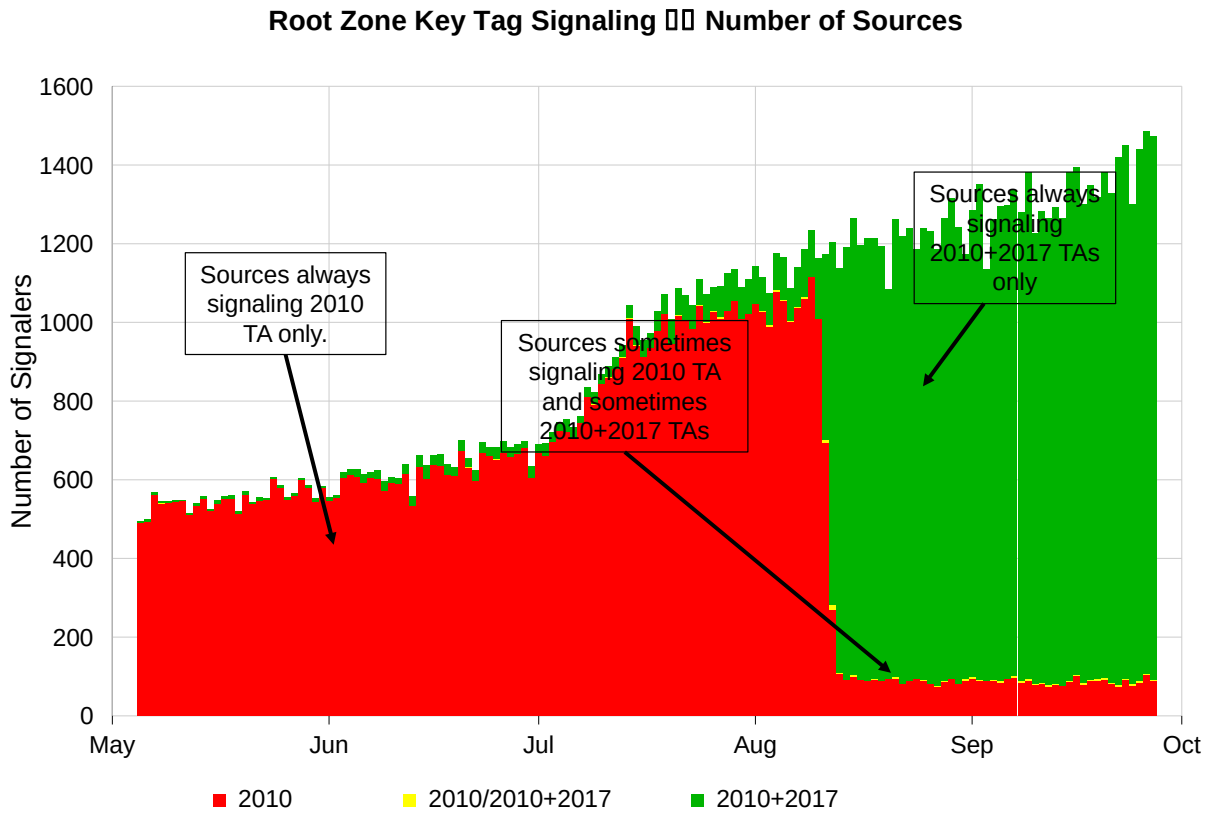
- リゾルバサーバがどのような鍵を DNSSEC 検証に用いているか通知する機構
- bind 9.10.5b1, 9.11.0b3 以降, unbound 1.6.4 以降

この機能を持っていないリゾルバ DNS サーバもまだ多く存在する

Trust Anchor Signaling の結果

DNS-OARC27

- Duane Wessels 氏の発表資料



某データでやってみよう

EDNS0 option と QNAME Key Tag があるらしい
- EDNS0 でのシグナリングはほとんどなく、大多数が QNAME でのシグナリングらしい

qtype = 10 での問い合わせ名が鍵タグ

```
1500479443  _ta-4a5c        128.x.x.x      192.58.128.30          2017 7 19
1500439539  _ta-4a5c        2a00:x:x::x    2001:503:ba3e::2:30    2017 7 19
1500476401  _ta-4a5c        2001:x:x::x    2001:503:c27::2:30     2017 7 19
1500476401  _ta-4a5c        2001:x:x::x    2001:503:c27::2:30     2017 7 19
1500495841  _ta-4a5c-4f66   188.x.x.x      198.41.0.4             2017 7 19
1500464521  _ta-4a5c        5.x.x.x        192.58.128.30          2017 7 19
1500476401  _ta-4a5c        2001:x:x::x    2001:503:c27::2:30     2017 7 19
1500476401  _ta-4a5c        194.x.x.x      198.41.0.4             2017 7 19
1500476401  _ta-4a5c        2001:x:x::x    2001:503:c27::2:30     2017 7 19
1500476401  _ta-4a5c        194.x.x.x      198.41.0.4             2017 7 19
1500495841  _ta-4a5c-4f66   188.x.x.x      198.41.0.4             2017 7 19
```

鍵タグ

19036(0x4a5c) – key tag for KSK-2010

20326(0x4f66) – key tag for KSK-2017

ふむ

2017/09/21 あたりのデータで。。。

- qtype = 10 のものを抜き出してみる

続きは発表当日