■ ルートゾーンKSKロールオーバーの概要と影響の確認方法（最終更新：2019年1月16日）

▼ルートゾーンKSKロールオーバーとは？

DNSSECでは鍵の危殆化（きたいか：守る対象が危険にさらされること）を避けるため、署名に用いる鍵（ゾーン署名鍵（ZSK）及び鍵署名鍵（KSK）の2種類）を、定期的に更新する必要があります。

ルートゾーンのKSKの運用について定めたDPS（DNSSEC Practice Statement）では、KSKの更新時期を運用開始後5年目以降と定めており、 2017年7月よりルートゾーンにおいて、DNSSEC鍵署名鍵（KSK）の更新（ルートゾーンKSKロールオーバー）のプロセスが開始されます。今回のルートゾーンKSKロールオーバーは2010年のDNSSECの運用開始後初となるもので、複数のステップにより実施されます。

▼ルートゾーンKSKロールオーバーの影響

懸念されること

ルートサーバーのDNSKEYリソースレコード（DNSKEY RR）の応答サイズが増加してIPフラグメントが発生し、フルリゾルバー（キャッシュDNSサーバー）が応答を受け取れなくなる可能性があります。なお、その可能性はDNSSEC検証の有効・無効には関係ありません。

対策・確認が必要なこと

① サイズの大きなDNS応答を正しく受け取れるかを確認

具体的な確認方法については、本資料の後半部分をご参照ください。

② DNSSEC検証を実施している場合、トラストアンカーの更新

ルートゾーンKSKロールオーバーにより、トラストアンカーの自動更新（RFC 5011）が初めて適用されます。各ソフトウェアにおける注意点と具体的な設定方法については、参考リンクに掲載した資料をご参照ください。なお、以下のバージョンのソフトウェアでは現・新双方のトラストアンカーが内蔵されており、適切な設定で使用している場合、トラストアンカーの更新による影響はありません。

BIND 9.11.0-P5/9.10.4-P8/9.9.9-P8以降、Unbound 1.6.1以降

▼重要日付と継続期間

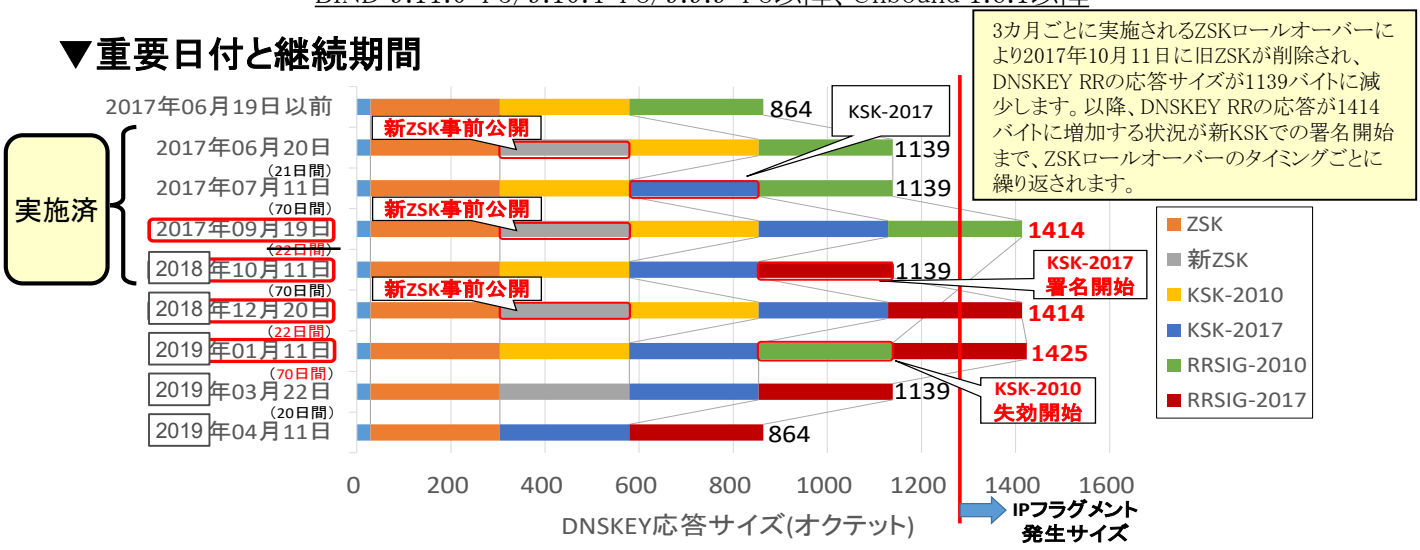

図1：2017～2019年のルートゾーンKSKロールオーバーにおけるDNSKEY応答サイズの変化

▼応答サイズ増大による影響の確認方法

自組織のネットワーク環境において、少なくとも1425バイトのDNS応答を正しく受け取れるかを事前確認することが推奨されており、以下の2種類の方法で確認できます。

＜注意＞BINDの開発元のISCが、DNS-OARCのDNS Reply Size TestはBIND 9.10以降では正しく動作しない旨を発表しています。詳細につきましては、ISC Knowledge Baseの記事をご参照ください。〈https://kb.isc.org/docs/aa-00210〉

1. DNS Reply Size Test Server（DNS-OARC）〈https://www.dns-oarc.net/oarc/services/replysizetest〉
   digコマンドにより、コマンドラインでの確認が可能です。

at leastの次に出力される数値（受け取りを確認できたDNS応答サイズ：+bufsize=4096の場合、指定した値より必ず小さくなる）が、少なくとも1425（今回におけるルートサーバーのDNSKEY応答の最大サイズ）であることを確認

```
$ dig +bufsize=4096 +short rs.dns-oarc.net txt
rst.x4050.rs.dns-oarc.net.
rst.x4058.x4050.rs.dns-oarc.net.
rst.x4064.x4058.x4050.rs.dns-oarc.net.
"192.0.2.1 sent EDNS buffer size 4096"
"192.0.2.1 DNS reply size limit is at least 4064"
"Tested at 2017-07-07 06:55:44 UTC"
```

（フルリゾルバーがIPv4で問い合わせた場合）

```
$ dig +bufsize=4096 +short rs.dns-oarc.net txt
rst.x4090.rs.dns-oarc.net.
rst.x4060.x4090.rs.dns-oarc.net.
rst.x4066.x4060.x4090.rs.dns-oarc.net.
"2001:db8::1 sent EDNS buffer size 4096"
"2001:db8::1 DNS reply size limit is at least 4090"
"Tested at 2017-07-07 09:00:00 UTC"
```

（フルリゾルバーがIPv6で問い合わせた場合）

図 2：digコマンドの出力例

＜注意＞フルリゾルバーがIPv4/IPv6のいずれで問い合わせるかは、状況により異なります。調査対象のフルリゾルバーがIPv4/IPv6双方の通信に対応している場合、digコマンドを時間を置いて複数回実行し、IPv4/IPv6双方の状況を確認しておくとよいでしょう。

2. DNSSEC Key Size Test（Verisign Labs）〈https://keysizetest.verisignlabs.com/〉
   Webアクセスにより、Webブラウザー上で確認が可能です。なお、本サイトでテストされるDNS応答サイズは1425バイトよりも大きくなっており、より大きなDNS応答を受け取れることを確認しています。

#	Description	KSKs	ZSKs	Signed DNSKEY Size	Result
1	2048 ZSK Normal	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign	949	PASS
2	2048 ZSK Rollover	2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish 2048-bit RSASHA256 publish+sign	1237	PASS
3	KSK Rollover with 2048 ZSK	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish+sign+revoke	2048-bit RSASHA256 publish+sign	1571	PASS
4	KSK Rollover with 2048 ZSK rollover	2048-bit RSASHA256 publish+sign+revoke 2048-bit RSASHA256 publish+sign	2048-bit RSASHA256 publish+sign 2048-bit RSASHA256 publish	1865	PASS
5	This should fail			0	FAIL

これら4項目が「PASS」であることを確認
（項目5は失敗表示の確認用）

図 3：DNSSEC Key Size Testの出力例

▼事前確認のポイント

ネットワーク管理者

① フルリゾルバーから組織外ネットワークまでの間に存在するネットワーク機器（スイッチ、ファイアウォール、ロードバランサー、ルーターなど）の設定確認

② 必要に応じた、ネットワーク機器のファームウェア・ハードウェアの更新

フルリゾルバーの管理者

① サイズの大きなDNS応答（少なくとも1425バイト）を正しく受け取れるかの確認

② DNSSEC検証を実施している場合、トラストアンカーの更新方法の確認

▼本件に関する詳細情報（参考リンク）

- Root Zone KSK Rollover（ICANN公式ページ）
  〈https://www.icann.org/resources/pages/ksk-rollover〉
- ルートKSKロールオーバーの実施により予想される影響について
  〈https://www.icann.org/ja/system/files/files/ksk-rollover-expect-22aug18-ja.pdf〉
- ルートゾーンのKSKロールオーバーについて
  〈https://dnsops.jp/event/20170628/20170628-RootKSKRO-02.pdf〉
  （JPRS 米谷喜朗の発表資料、2017年6月28日付）
- ルートゾーンのKSKロールオーバーについて（ISPから見た事前確認・準備のポイント）
  〈https://dnsops.jp/event/20170628/DNS_Summer_DAY_KSK_RO_suev0.1.pdf〉
  （QTnet 末松慶文氏の発表資料、2017年6月28日付）

※掲載内容は2019年1月現在のものです。