ルートゾーン KSK ロールオーバー計画

設計チームの草案 - 2015 年 8 月 4 日更新

1　概要

ICANN は、ルートゾーン DNSSEC 鍵署名鍵 (KSK) ロールオーバーの実施計画を準備しています。このロールオーバー作業は、ICANN が IANA 機能運用者の役割の一環として、他のルートゾーン管理 (RZM) パートナーと協力して計画するものです。このパートナーとは、ルートゾーンメンテナである Verisign、ルートゾーン管理者である米国商務省電気通信情報局 (NTIA: National Telecommunications and Information Administration) です。[1]

ルートゾーン KSK ロールオーバーにあたっては、ルートゾーンが DNSSEC (DNS セキュリティ拡張)[2] の定義に従って最初に署名された 2010 年以降に使用されてきた鍵の変更が参照されます。鍵の変更とはすなわち、新しい暗号シークレットコンポーネントを生成し、新しいパブリックコンポーネントを配布することを意味します。この新しいパブリックコンポーネントを適切に配布することが、鍵のロールオーバー作業において最も重要な作業です。

*本書は、パブリックコメントで使用される予定であり、DNS と DNSSEC に採用された有志の専門家、およびルートゾーン管理パートナーで構成される設計チームによる審議の草案です。本書は現段階では草案の状態であり、CANN が受け付けるパブリックコメントやその他の審議でのインターネットコミュニティからの意見に基づいて修正される予定です。*それらの意見を反映した上で、最終報告書が発行される予定です。

2　目次

1　概要 1

2　目次 1

3　要約 4

[1] 本草案は、IANA 機能契約によって現在規定されている現行のルートゾーン管理構造と、NTIA と Verisign との間で締結された共同契約に従って開発されました。設計チームと RZM パートナーは、現行の IANA 受託移行の取り組みが KSK ロールオーバー計画の内容や今後のあらゆるプロセスへの NTIA の関与に影響する可能性があることを認識しています。ただし、技術的な詳細および検討事項は、移行作業およびその最終結果に影響を与えるものではありません。

[2] RFC 4033、RFC 4034、および RFC 4035 を参照

3.1 DNS の用語 4
3.2 セキュリティ関連のその他の用語 7
3.3 ネットワーキング関連のその他の用語 7
3.4 提言の要旨 8
3.5 対象読者 9
3.6 文書のスコープ 10
4 これまでの主な経緯 10
4.1 ルートゾーンへの DNSSEC の展開 10
4.2 ルートゾーン KSK ロールオーバーのパブリックコメント 11
4.3 2013 年のルートゾーン KSK ロールオーバーに関する予備議論 11
4.4 ルートゾーンにおける DNSSEC 鍵ロールオーバーに対する SSAC の勧告 12
4.5 ICANN によるルートゾーン KSK ロールオーバー設計チームの招集 12
5 KSK ロールオーバーの概要 12
6 設計チームのアプローチ 13
6.1 運用に関する検討事項 14
6.2 プロトコルに関する検討事項 15
6.3 ルートゾーン KSK 管理に対する影響 19
6.4 暗号に関する検討事項 20
6.5 調整とコミュニケーション 22
7 認証リゾルバに対する影響 26
7.1 パケットサイズに関する検討事項 26
7.2 DNSSEC 認証の動作 30
8 テスト 32
8.1 影響のテスト 32

8.2 自己テストの設備 33
8.3 KSK/ZSK メンテナのソフトウェアとプロセスの変更互換性テスト 33
9 実施 34
9.1 次期 KSK の公開 35
9.2 次期 KSK へのロールオーバー 36
9.3 現行 KSK の無効化 36
9.4 レスポンスパケットサイズへの影響 36
9.5 ルートサーバーごとの展開 39
10 ロールバック 40
11 時期 41
12 リスク分析 42
12.1 準備不足によるリスク 42
12.2 自動トラストアンカーのメカニズムが機能しない、または不適切である 43
12.3 現行 KSK の削除による検証の失敗 44
12.4 次期 KSK の追加により DNS メッセージサイズが制限を超える 44
12.5 運用上のエラーの発生 45
13 設計チームのメンバーリスト 45
13.1 コミュニティの有志 45
13.2 ルートゾーン管理パートナー 46
14 参考資料 46
15 付録: チャネルパートナー 48
15.1 ソフトウェア作成者 48
15.2 システムインテグレータ 48
15.3 パブリックリゾルバ運用者 49

3 要約

IANA 機能運用者である ICANN は、ルートゾーンメンテナである Verisign およびルートゾーン管理者である米国商務省電気通信情報局 (NTIA) (これらをまとめて、ルートゾーン管理 (RZM) パートナーとも呼びます) と協力して、ルートゾーン鍵署名鍵 (KSK) ロールオーバー計画の策定を進めてきました。

ルートゾーン KSK は、ルートゾーン DNSKEY リソースレコードセットを DNSSEC に従って署名する際に使用されます。そのセットには、ルートゾーン内の他のすべてのレコードセット (RRset) の署名に使用されるゾーン署名鍵 (ZSK) が含まれます。ルートゾーン KSK ロールオーバーにあたっては、(ルートゾーンが DNSSEC に従って最初に署名された) 2010 年以降に使用されてきた鍵の変更が参照されます。鍵の変更とはすなわち、新しい暗号シークレットコンポーネントを生成し、新しいパブリックコンポーネントを配布することを意味します。この新しいパブリックコンポーネントを適切に配布することが、鍵のロールオーバーにおける最も重要な作業です。

2014 年 12 月、ICANN はコミュニティから有志を募り、RZM パートナーの参加を得て、本書に記載するルートゾーン KSK ロールオーバー計画を策定する設計チームを編成しました。策定にあたっては、1 回目のルートゾーン KSK ロールオーバーを実施するための詳細実装計画を作成する際に RZM パートナーがガイダンスとして使用する、技術面および運用面での推奨事項の包括的なセットを成果物として作成することとしました。本書は、それらの成果物を提供するにあたっての草案としてレビューされるべきものです。

3.1 DNS の用語

本書は、DNS および DNSSEC の技術的な詳細と関連性があります。そのため、DNSSEC 関連用語 (専門用語) および一部の関連性のある項目の定義を表 1 以下に記載します。

用語	略語	説明
Resource Record Set (リソースレコードセット)	RRSet	DNS に格納されるデータの単位で、DNSSEC 鍵によって署名される最小単位。

用語	略語	説明
Key Signing Key (鍵署名鍵)	KSK	DNS ゾーンで使用される鍵のセットの検証可能な署名を生成する役割を果たす、公開-秘密鍵のペア [3]。DNSSEC では DNS プロトコルの外部に配布する際にこの種の公開鍵が要求されるため、この役割は特殊なものです。
Zone Signing Key (ゾーン署名鍵)	ZSK	DNS ゾーンの他のすべてのデータのセットの署名を生成する役割を果たす、公開-秘密鍵のペア。この鍵は、DNS プロトコルの外部には配布されません。
DNSKEY RRset		ゾーン内で使用される鍵のセット。KSK と ZSK の役割、DNSKEY リソースレコードのセットが含まれます。
Key Rollover (鍵ロールオーバー)		ある暗号化鍵から別の暗号化鍵へと正しい規則に従って変更する行為。
(DNSSEC) Validator (バリデータ)		DNSSEC レスポンスのセキュリティチェックを実行するソフトウェア。このセキュリティチェックには、データの署名の 1 ステップでの検証が含まれます。
トラストアンカー		バリデータによって完全に信頼され、格納された公開 KSK。
Automated Updates of DNSSEC Trust Anchors (DNSSEC トラストアンカーの自動更新)	RFC 5011	バリデータでトラストアンカーを自動更新する 1 つの方法

[3] Ferguson、Niels、Bruce Schneier 著 (2003 年)、*「Practical Cryptography」*、出版元: Wiley、ISBN 0-471-22357-3

用語	略語	説明
Double-signing (二重署名)		2 つの署名。通常は、ロールオーバーの対象となる古い鍵と新しい鍵を 1 つの RRset に入れることを指します。通常は、1 つの RRset に対して 1 つの署名で十分です。
Root Server System Advisory Committee (ルートサーバーシステム諮問委員会)	RSSAC	ICANN の諮問委員会の 1 つ。ICANN コミュニティに対するルートサーバーシステムに関する助言を行います。
Extension Mechanisms for DNS (DNS の拡張メカニズム)	EDNS または EDNS(0)	現在は RFC 6891 に定義され、当初の DNS プロトコルフォーマットを拡張または拡大する手段を提供します。EDNS(0) は、最初の拡張セットを指します。
Delegation Signer Resource Record (委任署名者リソースレコード)	DS	下位の委任によって使用される KSK (ルートゾーンの場合は、トップレベルドメインの KSK) を指す DNSSEC レコード。
Negative Answer (負の答え)	NSEC または NSEC3	DNSSEC によって定義された、問いに対してデータが存在しないことを表すために使用されるリソースレコード。
DNSSEC Practices Statement	DPS	あるゾーンの DNSSEC 処理の仕様を記述する文書。
Key Ceremonies (キーセレモニー)		署名を生成するために、秘密鍵を使用して HSM で実施されるイベント。実施にあたって証人の立ち会いが妥当であると考えられる場合は、正規のプロセスが使用されます。

表 1:DNS と DNSSEC の用語

3.2 セキュリティ関連のその他の用語

用語	略語	説明
OpenPGP	OpenPGP	公開-秘密鍵の管理の方法。RFC 4880:*OpenPGP Message Format*
Cryptographic Message Syntax Standard	PKCS#7	RFC 2315:*PKCS #7:Cryptographic Message Syntax - Version 1.5*
ディレクトリ - 公開鍵と属性証明書のフレームワーク	X.509	公開-秘密鍵の管理の ITU-T 標準。提言 ITU-T X.509 | ISO/IEC 9594-8
Key Signing Request (鍵署名要求)	KSR	鍵、特に、KSK によって署名される DNSKEY セットを介した署名の要求が含まれるデータ構造。
Signed Key Response	SKR	秘密鍵によって生成された署名、特に、DNSKEY セットに対する KSK 署名が含まれるデータ構造。

表 2:セキュリティ関連のその他の用語

3.3 ネットワーキング関連のその他の用語

一般ユーザー向けと思われるいくつかの用語についても、用語とその定義を以下に記載します。

用語	略語	説明
User Datagram Protocol	UDP	インターネット経由でデータを送信するための、コンテキストフリーでベストエフォート型の伝送プロトコル。
Transmission Control Protocol	TCP	インターネット経由でデータを送信するための、接続指向でオクテットの順番が保証される伝送プロトコル。

用語	略語	説明
Maximum Transfer Unit	MTU	インターネットの一部を経由して送信されるデータに入れることができるオクテットの最大数。パス MTU は、インターネット経由のエンドツーエンドの送受信で使用されるすべての部分の最低 MTU を指します。

表 3:ネットワーキング関連のその他の用語

3.4 提言の要旨

勧告 1：ルートゾーン KSK ロールオーバーにあたっては、RFC 5011 に規定されている手順に従って、鍵署名鍵ロールオーバー時にトラストアンカーを更新すべきである。

勧告 2：ICANN は、鍵 DNS ソフトウェアベンダーを特定し、それらのベンダーと協力して、ベンダー固有のチャネルを使用してトラストアンカーが確実かつ安全に配布されるようにするためのプロセスに着手すべきである。

勧告 3：ICANN は、鍵 DNS システムインテグレータを特定し、それらのインテグレータと協力して、インテグレータ固有のチャネルを使用してトラストアンカーが確実かつ安全に配布されるようにするためのプロセスに着手すべきである。

勧告 4：ICANN は、ルートゾーントラストアンカーの正しい認証の推進を主導すべきである。具体的な内容の概要は、ICANN の IANA Web サイトに掲載されている。

勧告 5：ルートゾーン KSK ロールオーバーにあたっては、高水準の透明性を確保するため、既存の KSK の管理および使用のプロセスを大きく変更しないようにすることが要求される。

勧告 6：ルートゾーン DNSKEY RRset に対するすべての変更は、KSK 運用者の DPS に記載されている 10 日間のスロットに沿って実施しなければならない。

勧告 7：1 回目のルートゾーン KSK ロールオーバーでは、次期 KSK の既存のアルゴリズムと鍵サイズを維持すべきである。

勧告 8：アルゴリズムと鍵サイズの選定については、それ以降のルートゾーン KSK ロールオーバーで、将来的に再検討すべきである。

勧告 9：ICANN は RZM パートナーと協力し、ルートゾーン KSK ロールオーバーの認知度向上のためのコミュニケーション計画を策定し、実施すべきである。これには、しかるべき技術者向けミーティングや本書に定める「チャネルパートナー」などを活用した全世界の技術者コミュニティへの周知が含まれる。

勧告 10：ICANN は RSSAC に対し、KSK ロールオーバー期間の詳細なタイムテーブルを発表に先立って検証するよう依頼すべきであり、また、いずれかのルートサーバー運用者が運用上の理由からタイムテーブル変更を申し出た場合、妥当な要請については適切に対応すべきである。

勧告 11：ICANN は RSSAC および RZM パートナーと連携し、リアルタイムのコミュニケーションチャネルを使用して、ルートサーバーシステムのルートゾーンにおける KSK の追加または削除を伴う変更がもれなく適切に認知されるようにするべきである。

勧告 12：ICANN は RSSAC と連携し、ルートサーバー運用者に対して、後続の分析を通知し、KSK ロールオーバーの運用上の影響の特性化に役立つデータ収集を実施するよう要求すべきである。また、そのデータ収集の計画および成果物を第三者による分析に使用できるようにすべきである。

勧告 13：RZM パートナーは、ZSK サイズの将来的な拡張と KSK ロールオーバーの時期を慎重に検討して調整し、これら 2 つの作業が同時進行で実施されないようにすべきである。

勧告 14：次期 KSK に関連する作業によって発生する復旧時間を最小限にするため、現行 KSK のみで生成される SKR を、次期 KSK で生成される SKR と並行して生成すべきである。

勧告 15：RZM パートナーは、現行 KSK で生成される SKR を使用するためのプロセスを開発し、文書化すべきである。

3.5 対象読者

本書は、技術者、特に、DNS プロトコルと DNSSEC プロトコル、DNS の運用、およびルートゾーンにおける DNSSEC の使用に関するプロセスに精通している方向けのものです。

3.6 文書のスコープ

本書の目的は、RZM パートナーがルートゾーン KSK ロールオーバーの詳細実装計画を開発する際に役立つ一連の提言の概要を説明することです。

4 これまでの主な経緯

4.1 ルートゾーンへの DNSSEC の展開

2009 年、RZM パートナーが協力して [4]、DNSSEC をルートゾーンに展開しました。そして、最終的には 2010 年 7 月に認証可能な署名済みのルートゾーンが初めて公開されました。現在使用されているルートゾーン KSK は、米国バージニア州カルペパーにある、ICANN が管理する鍵管理施設 (KMF) で開催された 1 回目の KSK セレモニーで生成されたものです。ここで生成された鍵は、その後、米国カリフォルニア州エルセガンドにある 2 つ目の ICANN KMF に移送され、安全に移送されたことを確認した後に、KSK の公開部分がルートゾーンに公開され、トラストアンカーとなりました。

ルートゾーン KSK の生成およびメンテナンスの要件、およびそれぞれの RZM パートナーの役割は、NTIA によって規定されました [5]。それらの要件をルートゾーンメンテナおよび IANA 機能運用者が満足するための手順については、別途、DPS (DNSSEC Policy and Practice Statement)[6] として発表されています。

NTIA と ICANN の間で締結された IANA 機能契約は、2010 年 7 月に変更されて、ルートゾーン KSK 管理に関する役割が追加されました。そして、それらの要件は、その契約の後続の改訂に引き継がれました [7]。NTIA と Verisign の間で締結された共同契約についても、Verisign のルートゾーン ZSK 運用者の役割を反映する形で、2010 年 7 月に変更されました。[8]

IANA 機能契約により、ICANN には、ルートゾーン KSK ロールオーバーを実行することが要求されますが、その詳細のタイムラインや実装計画は明記されていません。ルートゾーン KSK 運用者の DPS にはこの件が記載されており、セクション 6.5 のロールオーバーに関する以下の要件に従うこととします。

---

[4] ルートゾーンへの DNSSEC の展開の詳細は、http://www.root-dnssec.org/に公開されています。

[5] 「Testing and Implementation Requirements for the Initial Deployment of DNSSEC in the Authoritative Root Zone (権威ルートゾーンに DNSSEC を初めて展開する際のテストおよび実装の要件)」、2009 年 10 月 29 日、http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf

[6] https://www.iana.org/dnssec、https://www.verisigninc.com/en_US/repository/index.xhtml

[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order

[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf

「それぞれの RZ KSK は、要件に定められたキーセレモニーによって、または運用の 5 年後にロールオーバーされる。」

4.2 ルートゾーン KSK ロールオーバーのパブリックコメント

2013 年 3 月 8 日、ICANN は、ルートゾーン KSK ロールオーバーの実施に関する意見を求めるため、パブリックコメント期間を開始しました [9]。6 つの団体と 15 人の個人から意見が寄せられました。それらの意見を集約し [10]、ICANN は、RZM パートナーが検討すべき 7 つの提言をまとめました。

1. RFC 5011 KSK ロールオーバーにあたっては、一連のテストと測定をテスト環境で事前に実施すべきである。テストフェーズの期間中はコミュニケーション手段を確立し、評価を成功させるためのテスト方法を用意する必要がある。
2. KSK ロールオーバーは、準備状況を十分に考慮した上で、可及的速やかに実施すべきである。
3. 測定と監視は、KSK ロールオーバーの実装による (技術者およびエンドユーザーへの) 影響を正確に判断する上で重要なモードである。
4. KSK ロールオーバーを手順に従って実施すべきである。
5. KSK ロールオーバーの実施にあたっては、複数のさまざまなステークホルダーグループに対して、十分かつ公的な方法で事前に通知すべきである。
6. 運用の安定性、繰り返しの KSK ロールオーバー、および RFC 5011 に対するコンプライアンス違反 (の可能性および影響) についてのさらなる調査が必要である。

4.3 2013 年のルートゾーン KSK ロールオーバーに関する予備議論

RZM パートナーは 2013 年 7 月下旬に、ルートゾーン KSK ロールオーバーの選択肢について議論するための会議を開催しました。この会議では、鍵ロールオーバー作業を十分な時間をかけて明確な手順に従って実施することの必要性、広範なコミュニティが参加することのメリット、および RFC 5011 ロールオーバースケジュールを修正して無効化の時期を遅らせる案が確認されました。これらの大まかな原則は、IETF 87 の IETF DNS 運用 (DNSOP) ワーキンググループのミーティングで提案されました [11]。

[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en
[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf
[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf

4.4 ルートゾーンにおける DNSSEC 鍵ロールオーバーに対する SSAC の勧告

2013 年 11 月、ICANN の安全性と安定性に関する諮問委員会 (SSAC) が、KSK ロールオーバーに関する SAC063[12]を発表しました。同報告書は、本件に伴うリスクと当時のコードベースの状態 (特に、オープンソース DNS の実装) を対象としたものであり、さらには、ルートゾーン KSK 鍵ロールオーバーの認知度向上、リゾルバの行動を収集および分析するためのテストの推奨、ルートゾーン KSK 鍵のロールオーバーにおける「被害」の受け入れ可能レベルを判断するための指標の作成、「被害」を超過した場合のロールバック対策の定義、および将来の鍵のロールオーバー作業でこれらの特性を通知するための情報収集の推奨されるコミュニケーション方法についても提案しています。

この SSAC 報告書は主として、本書で後述する 3 つのテーマを取り上げています。1 点目として、DNSSEC が有効な DNS の利用者の約 1.1%は、適切な手順に従ってルートゾーン KSK ロールオーバーを実施した場合であっても、負の影響を受ける可能性があると予想されます。2 点目として、DNSSEC トラストアンカーの自動更新 (RFC 5011) のサポートの状態については、提案されてはいるものの、予測不能であるという点です。3 点目は、DNS レスポンスのサイズについては、その基底となる UDP パケットの断片化の発生および TCP クエリへの戻りと関連性があることから、十分な検討が必要であるという点です。

4.5 ICANN によるルートゾーン KSK ロールオーバー設計チームの招集

2014 年 12 月、ICANN はコミュニティから有志を募り、RZM パートナーの参加を得て、本書に記載するルートゾーン KSK ロールオーバー計画を策定する設計チームを編成しました。

5 KSK ロールオーバーの概要

2013 年 11 月に作成された、他のすべての KSK ロールオーバー計画とほぼ同じ内容の計画では、以下の手順に従います。

1) 次期 KSK 鍵ペア (公開鍵と秘密鍵) が生成されます。

2) 次期 KSK 公開鍵がルートゾーンに置かれ、依拠当事者が使用できるようになります。

[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

3) 他のゾーンとは異なり、新しいルートゾーン KSK 公開鍵は、すべての関係者が次期 KSK として受け入れ可能な状態になります。受動的に受け入れ可能になるだけでなく、新しいルートゾーン KSK 公開鍵は、多様な電子および非電子媒体で使用可能になるため、RFC 5011 をサポートしていないサーバーを使用するリゾルバ運用者および開発者が自社のシステムや製品に新しいトラストアンカーを入れる時間的余裕が生まれます。(「その他のゾーン」の場合、この手順の代わりに、次期 KSK が存在する DS レコードの所持者に通知する手順を実行します。)

4) 署名プロセスによって、現行 KSK 秘密鍵の使用から次期 KSK 秘密鍵の使用へと切り替えられます。

5) この段階で、現行 KSK によって生成された署名が失効するか、運用ビューに表示されなくなり、次期 KSK が移行の状態になります。

6) 現行 KSK 公開鍵は、ルートゾーンから (無効化されずに) 削除されます。

7) 通常の運用とのもう 1 つの相違点として、現行ルートゾーン KSK は RFC 5011 のガイドラインに従って無効化する目的で再導入されます。この手順が別途設けられた理由は、その鍵のロールオーバーを含む ZSK 処理でルートゾーン完全鍵セットに対する DNS レスポンスのサイズ超過が発生しないようにするためです。

6 設計チームのアプローチ

設計チームは、ルートゾーン KSK ロールオーバーのいくつかの側面を考慮し、ルートゾーンパートナーによる実装計画の開発のガイダンスとなる、各研究分野からの提言をまとめました。

- 運用に関する検討事項: インターネットのエンドユーザーと DNS システムの運用者、およびそれらエンドユーザーが使用するサービスに対する影響
- プロトコルに関する検討事項: 既存の文書化されたプロトコル要素がルートゾーン KSK ロールオーバーにどの程度問題なく対応できるか
- ルートゾーン KSK 管理に対する影響: IANA 機能運用者による KSK 管理に伴うプロセスに対する影響
- 暗号に関する検討事項: システム全体として十分な暗号強度を確保すること
- 全関係者間でのコミュニケーションと調整。

これらの分野のそれぞれについて、以下のセクションで詳しく説明します。技術的なロールオーバーの詳しい解決策についても、提言にどのように従って作業を進めるかを示す図式として提示します。RZM パートナーは、実装計画の最終決定にあたり、これらの解決策を出発点として作業を進めることになります。

6.1 運用に関する検討事項

インターネットのエンドユーザーおよび DNS システムの運用者に対する影響は、上記の段階の 2 つで生じると予想されます。次期 KSK 公開鍵がルートゾーンに追加されると、ルート DNSKEY セットに対するレスポンスのサイズが大きくなります。現行 KSK 秘密鍵で署名が生成されなくなると、その公開鍵を使用した認証は期待どおりに動作しなくなります。

DNSKEY に対するレスポンスのサイズが大きくなると、IPv4 経由と IPv6 経由のどちらであるかによって、UDP パケットの断片化の発生に若干の差が生じる可能性があります。断片化が変則的になり、フィルタリングされると考えられるインターネットコンポーネントが既に存在します。DNS の場合、送信されるレスポンスに関する状態が維持されないため、クライアントが受け取るレスポンスが予測と異なるものになる可能性があります。また、UDP レスポンスがクエリで指定した DNS ペイロードバッファサイズよりも大きくなり、結果として、レスポンスが切り捨てられて、TCP を使用する後続の再クエリの割合が増える可能性があります。

現行 KSK がゾーン署名鍵を署名しなくなり、次期 KSK が署名を生成するようになると、現行 KSK だけがトラストアンカーとして構成されている DNSSEC バリデータは、署名済み DNSSEC レスポンスを認証できなくなります。バリデータは「フェイル時中断」になり、すなわち、すべての署名済み DNS レスポンスを無効であると見なします。

次期 KSK を取得できない、または、鍵ロールオーバープロセス時にサイズの大きいレスポンスを受け取ることができない認証リゾルバだけを使用するエンドクライアントは、いかなる署名済み DNS レスポンスも認証できなくなります。これは、エンドクライアントにとっては、ドメイン名が未解決の場合のインターネット障害が発生した場合と同じ状況です。同様の状況が以前に発生したことがある場合、結果として、カスタマーサポートセンターへの問い合わせ件数が増え、ISP のカスタマーサポートや運用管理の担当者の負荷が増えることになります。

ICANN は、次期 KSK の導入、および署名生成での現行 KSK から次期 KSK への切り替えのコミュニケーション方法を計画することとします (提言 8 を参照)。

6.2 プロトコルに関する検討事項

6.2.1 ルートゾーントラストアンカーの構成

次の 2 種類のトラストアンカー構成について検討します。

- オンライン認証リゾルバのトラストアンカー
- ロールオーバー時にオフラインで、その後にオンラインになったデバイス/システムのトラストアンカー

オンライン認証リゾルバは、使用する DNS ソフトウェアがこのメカニズムをサポートしていて、このメカニズムを使用してルートゾーン鍵署名鍵を更新するように構成されていれば、RFC 5011 に記載されているように、*DNSSEC (DNS セキュリティ) トラストアンカーの自動更新*を使用します。

DNS セキュリティトラストアンカーの自動更新を使用できない、あるいは使用しないオンライン認証リゾルバの場合、鍵署名鍵ロールオーバー時に手動での更新が必要になります。手動更新にあたっては、RFC 5011 メカニズムのタイミングに従うこととします。すなわち、新しいトラストアンカーをロールオーバーの公開期間内に該当する認証リゾルバの構成に追加しなければならず (詳細はセクション 11 を参照)、ルートゾーンが次期ルートゾーン KSK で署名される前に現行トラストアンカーが削除されないようにしなければなりません。さらには、以降の運用を確実に実施できるようにするため、現行ルートゾーン KSK の無効化前に現行トラストアンカーを削除しないようにします。新しいトラストアンカーを取得するメカニズムは、オフラインのデバイスの場合と同じであり、以下に記載するとおりです。

勧告 1：ルートゾーン KSK ロールオーバーにあたっては、RFC 5011 に規定されている手順に従って、鍵署名鍵ロールオーバー時にトラストアンカーを更新すべきである。

ルートゾーン KSK ロールオーバー時にオフラインであるデバイスは、ロールオーバーの終了後にオンラインになった段階で、手動で更新する必要があります。そのようなデバイスでは基本的に、新しくインストールされたデバイスと同様に、ブートストラップが必要になります。

一般的には、任意のデバイスが DNSSEC 認証を実行できるようにするプロセスでは、不適当なトラストアンカーが使用される可能性を低くするためのアプローチに従います。このようなデバイスに対する一般的なアドバイスについては、現在、「*DNSSEC Trust Anchor Publication for the Root Zone (ルートゾーンの DNSSEC トラストアンカーの*

公開)」という表題のインターネットドラフトが IETF[13]内で配布されていますが、実装者にとって役立つ同意された確定した文書とするためには、さらなる検討が必要です。

設計チームは、相互評価された確実な仕様を RFC シリーズとして公開することを目標とし、コミュニティの議論と IETF 内でのインターネットドラフトの審議を支援します。

最新のトラストアンカーの取得については、以下に概要を示す、いくつかの事例があります。

6.2.1.1 RFC 5011 の詳細議論

前述の、RFC 5011 のアプローチを「使用できない、または使用しない」リゾルバに関連し、このセクションでは、その状況のいくつかの背景を説明します。

RFC 5011 の add-hold タイマーの意味を十分に考慮することが重要です。このタイマーは、偽って提示された鍵が受け入れられてしまうのを防ぐ役割を果たします。言い換えれば、あるエンティティが偽の KSK を提示しようとした場合、その鍵の公開が成功してしまう可能性がありますが、そのような場合、信用が確定される前に、正規の機関が偽の鍵を拒否することができます。

リゾルバにおける RFC 5011 に対する拒否は、更新メカニズムの設計に関連付けられた質問に基づくものではなく、いくつかの運用上の事実に基づくものです。構成管理は、多数のサーバーを運用し、管理対象の構成ファイルの「外部への強制」を利用する場合の大きな課題の 1 つです。RFC 5011 の更新メカニズムにおいては、この課題への対応として、集中管理された構成から派生された新しいデータを多数のマシンが認識するように構成されます。

以上の点を考慮して、大規模運用者においては、手動プロセスを用意して、プロセスが多様な自動化されたメカニズムを使用するようにします。1 つの自動化されたシステムが、RFC 5011 の更新メカニズムに従うツールとなります。非公式の調査によると、大規模運用者は、人対人のやり取りによる信用の確立を含むいくつかの異なる方法で新しいルートゾーン KSK を厳格に検査することを予定しています。RFC 5011 の代替案が提案されたのは、このためです。

RFC 5011 の運用化を掘り下げる過程で、いくつかのギャップが特定されました。1 つ目のギャップは、成功した RFC 5011 プロセスの遠隔検証に関するものです。2 つ

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

目のギャップは、add-hold タイマーを考慮した場合のテスト展開の可否に関するものです。

必要となるのは、リゾルバが使用しているトラストアンカーをその信用のソースが認識するようにする手段です。過度の監視が実施される目的は、特定のリゾルバの構成や機能を知ることではなく、第一には RFC 5011 プロセスに十分に従っていると確認すること、そして、次期ルートゾーン KSK が確実に受け入れられる時期を知ることにあります。

また、機能テストを実行し、必要なセキュリティモデルを厳格に順守していない状況でも RFC 5011 の手順が実行されることを短時間で証明できるようにする必要があることもわかりました。具体的には、指定された add-hold タイマーをツールで上書きし、テスト中に設定を短くできるようにする必要があります。「安全テスト」のメカニズムを提供してテストの add-hold タイマーが本番環境で使用されないことを確認することが推奨されます。これは、ツール開発者や DNS ソフトウェアベンダーに対する推奨事項です。

6.2.1.2 その他のトラストアンカーフォーマット

ルートゾーンの最初の署名が開始して以来、ICANN は、DNS 以外のフォーマットのトラストアンカーを Web サイトに公開しています [14]。これらのトラストアンカーは、ルートゾーントラストアンカーを配布および受信する非クリティカルパスの手段、すなわち、DNS 処理の外部の手段を提供します。(ファイルにアクセスするには、Web サイトによる DNS へのアクセスが要求されます。)非クリティカルパスが考慮されているという前提で、新しいトラストアンカーを配布できます。将来のいずれかの段階で、異なる DNSSEC 暗号化アルゴリズム [15]のトラストアンカーを追加することで、必要な新しい機能を強調できます。これは、緊急ロールオーバーに備えてリゾルバを事前準備する手段にもなります。

6.2.1.3 DNS ソフトウェアベンダー

ソフトウェアベンダーが自社の DNS ソフトウェアにトラストアンカーを組み込む場合があります。ソフトウェアベンダーはその場合、ソフトウェアを最新の状態に保つために、トラストアンカーの新しいバージョンを発行します。

[14] https://www.iana.org/dnssec/files

[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

この方法で配布されるトラストアンカーが正規のものであること、すでに存在する検証メカニズムを活用してエンドシステム上のソフトウェアの整合性を保証することが重要です。ソフトウェアベンダーには、堅牢かつ有効な方法で自社が自社ソフトウェアで配布するトラストアンカーが正規のものであることを保証することが要求されます。なぜなら、特に、ベンダーのソフトウェア更新戦略の一部としてコード署名鍵で署名する場合は、非正規の鍵を配布することで多大な影響を及ぼす可能性があるためです。

勧告 2：ICANN は、鍵 DNS ソフトウェアベンダーを特定し、それらのベンダーと協力して、ベンダー固有のチャネルを使用してトラストアンカーが確実かつ安全に配布されるようにするためのプロセスに着手すべきである。

6.2.1.4　システムインテグレータ

DNSSEC トラストアンカーの 1 つの配布方法は、たとえば、パッケージメンテナやオペレーティングシステムベンダーなどのシステムインテグレータ経由で配布されることがあります。この場合、システムインテグレータは、システム内のトラストアンカーのすべてのコピーに対して、更新されたパッケージを提供します。いくつかの Linux ディストリビューションでは、パッケージと一緒にトラストアンカーの正規コピーが提供されます。

勧告 3：ICANN は、鍵 DNS システムインテグレータを特定し、それらのインテグレータと協力して、インテグレータ固有のチャネルを使用してトラストアンカーが確実かつ安全に配布されるようにするためのプロセスに着手すべきである。

6.2.1.5　システム管理者

システム管理者は、ソフトウェアをインストールまたは更新するときに、DNSSEC トラストアンカーを ICANN の IANA Web サイトから手動でダウンロードできます。最新のルートゾーントラストアンカーは、IANA 機能運用者によって、専用の Web サイト [16]上に、ルートゾーンにおける DNSSEC に関する情報として提供されます。ダウンロードしたトラストアンカーの正当性を判断することは、DNSSEC で信用を確立する上で極めて重要です。多様なタイプのデジタル署名の正当性検証をサポートするため、ルート鍵を含む、OpenPGP、PKCS#7、および X.509 の形式の証明書が同じ専用 Web サイトに公開されます。

[16] https://www.iana.org/dnssec/files に記載

オーセンティシティ (本物であること) の判断は極めて重要であるにもかかわらず、見過ごされることや、正しく規定されていないことも少なくありません。オーセンティシティの立証をサポートするプロセスがレビューのために公開された段階で、実質的な意見は多く寄せられませんでした。そのために、オーセンティシティを十分にサポートする取り組みが十分に行われませんでした。追加のレビューを (必要であれば後方互換性のある変更を使用して) 実施することが有効であると考えられます。設計チームは前述のように、相互評価された確実な仕様を RFC シリーズとして公開するという目標のもとで、コミュニティの議論と IETF 内での「*DNSSEC Trust Anchor Publication for the Root Zone （ルートゾーンでの DNSSEC トラストアンカーの公開）*」 (前述のドラフト) という表題のインターネットドラフトのレビューを支援します。

また、オーセンティシティをサポートするデジタル署名の取得を観察したところ、デジタル署名を使用していた依拠当事者は存在するとしても極わずかであることがわかりました。信用の獲得は、デジタル署名の提供だけではなく、積極的な推進によって可能になります。

勧告 4：ICANN は、ルートゾーントラストアンカーの正しい認証の推進を主導すべきである。具体的な内容の概要は、ICANN の IANA Web サイトに掲載されている。

6.3 ルートゾーン KSK 管理に対する影響

「*DNSSEC Practice Statement for the Root Zone KSK Operator (ルートゾーン KSK 運用者のための DNSSEC 実践書)*」に記載のとおり、ルートゾーン KSK オペレータは、ルートゾーン ZSK オペレータから提供される KSR を使用することで、ルートゾーンのそれぞれの apex DNSKEY RRset に署名します。これが、ルートゾーンメンテナに提供される署名済み DNSKEY RRset のセットを含む SKR となります。

これらのプロセスは、明確に文書化されており、KSK セレモニーで実行される場合は、外部監査および公開の対象となります。設計チームは、これが、KSK ロールアウトの結果としてプロセスが大幅に変更されるのを回避する極めて有効な方法であり、それによって、すでに広く認知されている現在のプロセスの中断を回避できると考えています。

勧告 5：ルートゾーン KSK ロールオーバーにあたっては、高水準の透明性を確保するため、既存のプロセスを大きく変更しないように要求すべきである。

KSR はそれぞれが 1 つの四半期 (3 か月間、または約 90 日間) のタイムサイクルに対応し、それぞれがさらに 10 日間の 9 つのスロットに分割されます。タイムサイクルが 90 日間を超える場合、その期間の最後のスロットが期間の最終日まで延長されます。したがって、ルートゾーン DNSKEY RRset に対するすべての変更、すなわち、鍵ロールオーバーで必要になる鍵の追加や削除は、この 10 日間のスロットに沿って実行し、署名済みルートゾーンの公開に使用するプロセスでの変更を最小限にしなければなりません。

勧告 6：ルートゾーン DNSKEY RRset に対するすべての変更は、KSK 運用者の DPS に記載されている 10 日間のスロットに沿って実施しなければならない。

標準期間においては、ルート DNSKEY RRset パケットのレスポンス サイズは、それぞれのタイムサイクルの最初と最後のスロットで大きくなります。最初のスロットには、前のタイムサイクルからの公開後の ZSK が含まれ、最後のスロットには、次のタイムサイクルのための公開前の ZSK が含まれます。

DNS レスポンス サイズが大きくなることで発生する問題を最小限に抑えるため、DNSKEY RRset レスポンス サイズをできるだけ小さく保つようにロールオーバーをスケジュールすることを推奨します。レスポンス サイズの問題の詳細検証とそれに関連する提言については、本書の後半に記載します。前述の検討事項を考慮して設計されたルートゾーン KSK ロールオーバーのスケジュールについても、本書の後半に記載します。

6.4 暗号に関する検討事項

設計チームは、KSK の鍵サイズまたはアルゴリズムの変更を検討すべき時期を迎えているのかどうかを議論しました。選択された鍵サイズやアルゴリズムの暗号強度に関する疑問がいくつも提起されるようになれば、変更を検討するのが十分な時期を迎えていると考えられます。

2005 年の SP 800-57, Part 1 (*Recommendation for Key Management (鍵管理に関する提言)*) の最初の発表にあたり、米国国立標準技術研究所 (NIST) は、最小暗号強度を引き上げる意向を示しました。ただし、この発表から計画されていた期日までの 5 年間、因数分解技術は、期待された速さで進歩しませんでした。ルートゾーン KSK の長い鍵長を使用する緊急性を示す動きはありません。

6.4.1　有限体暗号方式

ECRYPT II のアルゴリズムと鍵長に関する 2012 年度版報告書[17]では、2048 ビット非対称 RSA 鍵は 103 ビット非対称鍵と同等であるとされています。同報告書では、10 年までの保護を想定して、96 ビット以上のセキュリティを使用するよう推奨しています。NIST の「Recommendation for Key Management-Part 1: General (Revision 3) (鍵管理に関する提言-一般 (リビジョン 3))」[18]は、2048 ビット RSA 鍵を 112 ビットのセキュリティと同等であるとし、2014〜2030 年はこの強度の使用が容認されるだろうとしています。フランス国立情報システムセキュリティ庁 (ANSSI: Agence nationale de la sécurité des systèmes d'information) のセキュリティに関する一般基準 (*Référentiel Général de Sécurité*[19]) も、2030 年までは 2048 ビット RSA 鍵の使用で問題ないとしています。

DNSKEY 署名期間が日数 (15 日) で測定されることから、ロートゾーン内の署名済みコンテンツの存続期間は一般的に短く、設計チームは、大規模整数の因数分解の領域で飛躍的進歩を遂げない限り、今後 5 年間は 2048 ビット RSA 鍵で安全であるはずだと考えています。

6.4.2　楕円曲線暗号

DNSSEC で使用できるもう 1 つのアルゴリズムオプションとして、RFC 6605[20]で定義された楕円曲線暗号デジタル署名アルゴリズム (ECDSA) があります。ECDSA には、ルートゾーン鍵署名鍵のアルゴリズムとして使用する際に役立つ、いくつかのプロパティがあります。これらの鍵には、RSA 鍵と同等の強度を保ちつつ、サイズがはるかに小さいという特性があります。現在の概算によると、P-256 曲線の ECDSA の強度は、3072 ビット鍵 (NIST) または 3248 ビット (ECRYPT II) の RSA とほぼ同等です。ただし、このアルゴリズムの DNSSEC での使用が標準化されたのは比較的最近 (RFC 6605 は、2012 年に発表されました) であり、本書で後述する測定は、バリデータにおいては ECDSA が RSA ほどサポートされていないことを示しています (セクション 7 の運用に関する検討事項を参照)。

IETF の暗号フォーラム研究グループ (CFRG) も、新しい*「Elliptic Curves for Security (セキュリティの楕円曲線)」* RFC への新しい楕円曲線セキュリティの追加に取り組んでおり、コミュニティを代表して、ECDSA で使用されている曲線の生成と潜在的な

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
[20] https://tools.ietf.org/html/rfc6605

弱点に対する懸念を表明しています。ルートゾーンの署名の新しい楕円曲線アルゴリズムに切り替える前に、CFRG がこの文書の取りまとめを終了することが望まれます。

6.4.3　結論

上記のガイダンスに基づき、設計チームは、アルゴリズムまたは KSK のサイズの 2048 ビット RSA からの変更のいずれかを積極的に推進する必要はないものと考えます。また、DNS 認証リゾルバの実装にあたっては、構成されているトラストアンカーと一致するすべてのアルゴリズムによるルートゾーンの署名が必要となり、結果として、異なるアルゴリズムへのロールオーバーには、KSK ロールオーバーとは異なるアプローチが必要になることがわかりました。これらの事実は、現段階でのアルゴリズムの変更を回避すべきという判断を推進する現実的な動機となってきます。設計チームがベンダーに対して、この問題とベンダーの要件に関する聞き取りを実施したところ、期日未定の今後の KSK ロールオーバーへの先送りを希望していることがわかりました。

以上の理由により、最初の KSK ロールオーバーでは次期 KSK を 2048 ビット RSA 鍵とするべきではあるものの、それ以降の KSK ロールオーバーでアルゴリズムや鍵長の変更を検討する余地があると考えられます。

勧告 7：設計チームは、1 回目のルートゾーン KSK ロールオーバーで次期 KSK の既存のアルゴリズムと鍵サイズを維持することを推奨する。

勧告 8：アルゴリズムと鍵サイズの選定については、それ以降のルートゾーン KSK ロールオーバーで、将来的に再検討すべきである。

6.5　調整とコミュニケーション

6.5.1　技術者コミュニティおよびチャネルパートナーとの調整

ICANN は、ルートゾーン KSK ロールオーバーの認知度向上のためのコミュニケーション計画を立案し、実行します。DNSSEC のルートゾーンへの最初の展開が提案された場であったことから、技術者フォーラムでの認知度向上に取り組む必要があります。

これ以降で言及する「チャネルパートナー」とは、ルートゾーンの管理とは関係のない、DNSSEC の使用を調整する外部組織を指します。これらのパートナーは、RZM パートナーからのグローバルの公共インターネットへとルートゾーンの署名の価値を橋渡しする、「チャネル」の役割を果たします。

チャネルパートナーは、3 つの分野に分類されます。1 つ目はイネーブラで、主として DNSSEC 認証ソフトウェアを実装し、RFC 5011 を実装します。2 つ目は、DNSSEC 認証ソフトウェアを含むソフトウェアおよびシステムのディストリビュータで、主としてルートゾーン KSK のコピーの配布に関与します。3 つ目は、ルートゾーン KSK の使用を可能にする DNSSEC 認証システムの運用者です。

コミュニケーションを促進するため、設計チームは各チャネルパートナーに対し、可能であれば連絡先をファイルに保存し、KSK ロールオーバーに関する最新情報をそれらの連絡先に通知するよう推奨します。この連絡先リストは、非公開の資料の交換を含む他のいかなる目的にも使用しないこととし、ルートゾーン KSK ロールオーバーの手順の認知度をサンプリングする目的で使用することとします。ただし、チャネルパートナー自身がこのリストを非公開にして、選択した連絡先の認知度の情報を管理することは認められます。

勧告 9：ICANN は RZM パートナーと協力し、ルートゾーン KSK ロールオーバーの認知度向上のためのコミュニケーション計画を策定し、実施すべきである。これには、しかるべき技術者向けミーティングや本書に定める「チャネルパートナー」などを活用した全世界の技術者コミュニティへの周知が含まれる。

6.5.2　ルートサーバー運用者との調整

ルートゾーンの内容のいかなる構造的変更も、個々のルートサーバーの運用上の動作に影響を与える可能性があります。ルートゾーンにおける IPv6 アドレス (AAAA) グルーの初期プロビジョニングとその後の DNSSEC の展開は、その変更がクエリパターンの変更にもつながるという理由によって、ルートサーバー運用者に対する聞き取りと適切な調整を経て変更を実施した例です。したがって、重要なインフラストラクチャに適切に対応するには、変更に対する保守的なアプローチで、ルートサーバーシステム全体のパフォーマンス低下につながる可能性がある、予期しない事態の発生に備える必要があります。

本書の準備の一環として実施した実験から、KSK ロールオーバーに伴う大きな影響はないと予測されますが、前述の構造的変更に示した例にあるように、保守的なアプローチを採用することが推奨されます。

設計チームは各ルートサーバー運用者に対し、KSK ロールオーバー期間内のイベントを重要な計画内運用イベントとして取り扱い、重要なイベントに使用している通常のリアルタイムチャネルを利用して、現状説明を公開し、他のルートサーバーオペレータと連携して作業を進めるよう提案します。これに該当するイベントとして

は、新しい次期 KSK のルートゾーン apex DNSKEY RRSet への追加、およびその同じ RRSet からの現行 KSK の削除があります。

設計チームは、各ルートサーバー運用者と ICANN 間のリアルタイムコミュニケーションと ICANN と他の RZM パートナー間のリアルタイムコミュニケーションが、同じイベントに対して相違なく実施され、予想されるすべての影響が迅速に特定され、共有されるようにすることを提案します。

各ルートサーバー運用者が期待される運用レベルを提供するのに支障となる可能性がある、他の何らかの計画との対立が発生しないようにするために、KSK ロールオーバー期間の詳細なタイムテーブルについては、最終決定されて公開される前にルートサーバー運用者がレビューを実施することとします。運用上の対立を回避するための時期の調整についても、妥当な範囲で実施することとします。

勧告 10：ICANN は RSSAC に対し、KSK ロールオーバー期間の詳細なタイムテーブルを発表に先立って検証するよう依頼すべきであり、また、いずれかのルートサーバー運用者が運用上の理由からタイムテーブル変更を申し出た場合、妥当な要請については適切に対応すべきである。

勧告 11：ICANN は RSSAC および RZM パートナーと連携し、リアルタイムのコミュニケーションチャネルを使用して、ルートサーバーシステムのルートゾーンにおける KSK の追加または削除を伴う変更がもれなく適切に認知されるようにするべきである。

KSK ロールオーバーの過程でのルートサーバー運用者によるデータ収集を活用して、KSK ロールオーバーのバリデータおよびルートサーバーに対する運用上の影響を把握します。ルートサーバーシステムは、アーキテクチャだけでなく、インターネットにおける配置も多様であるため、各ルートサーバー運用者による長期間のデータ収集の機会にはさまざまな制約があり、システム全体を端的に特徴化するのは困難であると考えられます。また、KSK ロールオーバーの開始時に、サービスの状態のリアルタイム監視の戦術的要件を満足するための基準データ収集機能がすでに存在することも考えられます。

DNSSEC がルートゾーンに最初に展開された段階で、十分なデータ収集作業が実行され、その結果データがルートゾーンにおける構造的な変更に対する DNS の反応のオフライン分析 (DNS-OARC が推進し、サードパーティが実施する分析を含む) に利

用できるものであることが証明されています[21]。1 回目の KSK ロールオーバーでも同様の作業が実施されることが確定しています。

勧告 12：ICANN は RSSAC と連携し、ルートサーバー運用者に対して、後続の分析を通知し、KSK ロールオーバーの運用上の影響の特性化に役立つデータ収集を実施するよう要求すべきである。また、そのデータ収集の計画および成果物を第三者による分析に使用できるようにすべきである。

6.5.3 KSK 運用者と ZSK 運用者の間の調整

ルートゾーンの KSK と ZSK の管理の責任はそれぞれ、IANA 機能運用者とルートゾーンメンテナに別々に割り当てられています。この 2 つの役割は別々に管理されます。

ルートゾーン ZSK は現在、ZSK メンテナの DPS[22]に記載のとおり、1024 ビット RSA 鍵です。ルートゾーンメンテナによって将来的に ZSK 鍵サイズが拡張される可能性があります。

ZSK の通常の周期は 90 日間であり、KSK ロールオーバーは 90 日以下で終了する予定であることから、KSK ロールオーバー期間も通常通りにこの周期が継続することになり、最終計画によっては、ルートゾーン apex DNSKEY RRSet に 4 つの鍵が含まれる可能性がある期間が生じます。

鍵ロールオーバーイベントの間に ZSK サイズが大きくなると、レスポンス サイズも ZSK サイズに合わせて大きくなるため、KSK ロールオーバー期間の一部でバリデータの動作が変わる可能性があります。これにより、運用上の問題が発生した場合の問題の特定、理解、および修正が複雑になる可能性があります。

ZSK サイズに関するいかなる判断についても、本書のスコープに含まれませんが、ICANN がルートゾーンメンテナと調整し、ZSK サイズの将来的な拡張と KSK ロールオーバーの時期を十分に検討して調整し、これら 2 つの作業が同時進行で実施されないようにすることを推奨します。

勧告 13：RZM パートナーは、ZSK サイズの将来的な拡張と KSK ロールオーバーの時期を慎重に検討して調整し、これら 2 つの作業が同時進行で実施されないようにすべきである。

---

[21] https://www.dns-oarc.net

[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

7　認証リゾルバに対する影響

7.1　パケットサイズに関する検討事項

DNS は、UDP および TCP 転送プロトコル経由で処理するように定義されています。特にサーバーでの接続状態の維持という点では、UDP の方が TCP よりもオーバーヘッドが低いため、DNS プロトコルの設計においては、UDP プロトコルの設計が優先されていました。ただし、このプロトコルを選択する場合には制限があります。DNS の最初の定義である RFC 1035 では、UDP レスポンスが 512 オクテットに制限されていました。現在もまだ使用されているソフトウェアは、この 512 オクテットの制限を尊重または強制する形で順守しています。

1999 年 8 月に発表された RFC で最初に定義され、RFC 6891 で更新された、DNS の拡張メカニズムである EDNS(0) を使用することで、DNS リクエスタは DNS サーバーに対し、512 オクテットを超える UDP レスポンス サイズを処理できることを通知できます。リクエスタがこの最大 UDP ペイロードサイズ (IP パケットサイズではなく、DNS メッセージサイズ) をメモリに入れ、サーバーには、DNS ペイロードが指定されたバッファサイズを超えない範囲の UDP レスポンスを返すことが要求されます。このように処理できない場合、サーバーは、切り捨てが発生したことを表す truncate ビットをレスポンスに設定します。切り捨てられたレスポンスに有効な DNS メッセージが含まれている場合、リクエスタは、その切り捨てられたレスポンスを使用することを選択できます。または、リクエスタがサーバーに対して TCP セッションを開き、TCP 経由でそのクエリを繰り返します。

DNSSEC を使用する DNS システムは、EDNS 擬似ヘッダーの DO (DNSSEC OK) フラグを使用して、DNSSEC を使用できることを通知しなければなりません。本書で検討する運用上の影響はいずれも DNSSEC 対応のシステムに関するものであるため、それらのシステムは EDNS(0) 対応です (DNSSEC には EDNS(0) のサポートが要求されるため)。したがって、512 オクテットの制限は適用されません。

クライアントがトランザクションを TCP で開始することもできますが、一般的なリクエスタの動作では、トランザクションを UDP で開始し、truncate ビットをレスポンスで使用して、リクエスタがクエリに TCP を使用することを指示します。

UDP パケットの断片化の処理方法は、IPv4 と IPv6 で異なります。パケットが基底となる IP パケット転送媒体に対して大きすぎるときに、IP パケットは断片化します。この場合、後続の断片は同じ IP レベルヘッダー (UDP プロトコル番号フィールドを含む) を使用しますが、後続の断片では UDP 擬似ヘッダーが除外されます。IPv4 で

は、IP の *DF (Don't Fragment)* フラグが設定されていない限り、送信元または中間のいずれかのルーターが IP パケットを断片化します。IPv6 では、送信元のみが IP パケットを断片化します。中間ルーターがパケットをネクストホップインターフェイスに転送できない場合、IPv6 では、ルーターがネクストホップインターフェイスとパケットの先頭部分の MTU サイズで ICMPv6 診断パケットを生成し、この情報をパケットの送信元に返します。

UDP を使用する場合、送信元は肯定応答のないデータのバッファを維持しないため、IPv6 の送信元は、このメッセージを受け取ったときに元のデータを再送信できません。IPv6 の多くの実装でレスポンスが共通であることを示すデータから、ローカル IPv6 転送テーブルのホストエントリが生成され、このテーブルに受信 MTU を記録されて、一部のローカルで決定されるキャッシュ時間に使用されます。これはすなわち、それ以降に IPv6UDP パケットをこの宛先に送信しようとする場合は、この MTU 値が使用して、送信パケットをどのように断片化するかが判断されることを意味します。

7.1.1　測定の実施

大きいパケットサイズがリゾルバおよびユーザーにどのように影響するかを評価するため、ルートサーバーの環境を再現する実験環境が設計され、用意されました。

この実験環境では、オンラインのアドバタイズメントプラットフォームを使用して DNS リゾルバをトリガーし、異なるレスポンスサイズの 2 つのゾーンのクエリにレスポンスするよう構成された権威 DNS サーバーに対して一意のクエリを送信するようにしました。このテストで権威 DNS サーバーにクエリを送信するリゾルバの多くは、ルートゾーンにクエリを送信すると予想されるのと同じリゾルバです。

リゾルバが大きいレスポンスを受信できるかどうかをテストするため、アドバタイズメントが宛先ドメイン名のクエリを実行しました。宛先ドメイン名そのものは、通常のサイズのレスポンスを返します。ただし、宛先のレスポンスを取得するためには、リゾルバが大きい中間レスポンスを最初に受信する必要がありました。たとえ宛先ドメイン名の情報の問い合わせであっても成功すれば、このテストによって、リゾルバが大きい中間レスポンスを処理できることが証明されます。

このテストではさらに、実験環境の Web サーバーから Web オブジェクトを取得する処理も実行し、Web の取得で使用されるアドレス (エンドユーザーの IP アドレス) を DNS クエリでの送信にネームリゾルバが使用するアドレスと一致させる実験も行いました。

このテストでは、1,444 オクテットの DNS レスポンスが使用されました。

7.1.2　テスト結果

2015 年 5 月に 5 日間にわたり、約 726 万台のエンドシステムが小さい制御レコードの取得に成功し、そのうちの約 717 万台のシステムがテストレコードの取得に成功しました。この差は約 90,000 ユーザーで、1,444 オクテットの DNS テストレコードの取得が失敗したのはサンプリング対象の 1%です。

これらのエンドシステムは、約 83,000 の異なる DNS リゾルバ IP アドレスを使用しました。これらの中で、リゾルバの 94%が制御レコードとテストレコードの両方の取得に成功しました。制御レコードは取得できたもののテストレコードの取得は失敗した 4,251 のリゾルバの中で、3,396 のリゾルバは、EDNS(0) 拡張を DNSSEC OK ビットを設定して使用し、1,444 オクテットのレスポンスがトリガーされました。これらの失敗したリゾルバの中で、3,110 のリゾルバは、実験期間中の失敗回数が 1 回だけでしたが、826 のリゾルバは、失敗条件が 2 回以上発生しました。つまり、この実験に参加したリゾルバの 1%は大きいレスポンスの取得に 2 回以上失敗し、大きいレスポンスの取得が 1 回だけ失敗したリゾルバは 3%でした。この結果は、大きいレスポンスが常に失敗する何らかの確定的な条件を結論付けるのには不十分です。取得が 2 回以上失敗した、この 1%のリゾルバを使用していたのは、3,000 弱のエンドシステム、すなわち、サンプリングされたエンドシステム全体の 0.04%でした。

5,237 のリゾルバはこのテストで IPv6 アドレスを使用し (全体の 6%)、それらのリゾルバのうちの 830 のリゾルバがテストレコードの取得に失敗しました (失敗したリゾルバの 21%)。これらのデータは、一部の IPv6 リゾルバとそのリゾルバによる MTU サイズの処理に何らかの問題があった可能性があることを示しています。

レスポンスが大きくなることによるクエリロードの変化を測定するという観点から、制御名 (93 オクテットのレスポンスサイズ) のクエリが 1,640 万回実行され、TCP が使用されたクエリは 475 件でした。テスト名 (1,444 オクテットのレスポンスサイズ) のクエリは 1,860 万回実行され、これらのクエリのうちの 120 万件は TCP 経由で実行されました。これは、テスト名の合計クエリ件数の約 6.5%に相当します。制御レコードに対するクエリの合計数とテストレコードに対するクエリの合計数に差がありますが、この差は、テストレコードに対して切り捨てられたレスポンスを受け取った場合にリゾルバが TCP 経由で別のクエリを送信するためであると考えられます。これは、UDP クエリの EDNS(0) 拡張で提供される UDP バッファサイズの分布との合理的な関連性が認められる結果であると言えます。大きいレスポンスを処理する場合、権威 DNS サーバーは、高クエリロードを予測し、TCP 経由のクエリの割合が高くなると予測できます。

7.1.3 結論

DNSSEC OK フラグをクエリに設定した DNS リゾルバの約 1%は、1,444 オクテットの DNS レスポンスを受け取ることができないと考えられます (実験に伴う不確定性要素から、この数値の上限は全リゾルバの 6%であると考えられます)。これらのリゾルバの中で、IPv6 を転送プロトコルとして使用していたリゾルバに偏りがありました。この失敗の割合は、さまざまな形の DNS 中間ミドルウェアが存在するため、あるいは、IPv6 の場合は ICMP6 の「*Packet Too Big (パケットが大きすぎる)*」メッセージによるためである可能性がありますが、今回の実験方法で失敗の正確な特性を確定することはできません。

レスポンスの受信に失敗するリゾルバが処理するユーザーの割合は極少数です。このサイズの DNS レスポンスを伴う場合に DNS 名を常に解決できない DNS リゾルバを使用するユーザーの数は、全ユーザー数の 0.04%であると考えられます (実験に伴う不確定性要素から、この数値の上限は全リゾルバの 1%であると考えられます)。

これらの実験では、1,444 オクテットの DNS レスポンスをテストしました。注目すべきは、DNS の他の部分はここで検証しているサイズよりもはるかに大きいレスポンスをすでに返しているにもかかわらず、これらのレスポンスサイズが注目されたり、目立った意見が寄せられたりしたという報告がないという点です。たとえば、2015 年 6 月 6 日の.org 名に対する同等の DNSKEY クエリでは、2 つの 2048 ビット RSA 鍵署名鍵、2 つの 1024 ビット RSA ゾーン署名鍵、および 3 つの署名 (それぞれの KSK に対して 1 つ、いずれかの ZSK に対して 1 つ) を含む 1,625 オクテットのレスポンスが生成されました。このような大きい DNS レスポンスを受信できない認証リゾルバは、.org ゾーンのそれぞれの委任で DS レコードまたは NSEC3 レコード (DS レコードが存在しないことを通知するために使用されます) のいずれかの署名を認証できず、結果として、.org での委任で DNS 解決が失敗します。

設計チームは、.org のドメイン名保持者が.org 名の DNSKEY DNS レスポンスパケットのサイズに関連して発生する運用上のいかなる問題も認識していません。.org 内の署名済みゾーンが極少数であることを考慮したとしても、.org ドメイン名の解決の失敗に関するいかなる運用報告書も存在しないことは、レスポンスサイズがルートゾーン KSK ロールオーバーの運用上の重大な問題になる可能性が低いことを示しています。

テストケースと.org の場合の注意すべき相違の 1 つは、大きい DNSKEYRRset のクエリを実行するのは実際に認証を実行するリゾルバのみであるという点です。テストケースでは、DNSSEC OK を通知するすべてのリゾルバが大きいレスポンスを取得し

ようとします。セクション 8.2 に記載したように、最初のクエリで DNSSEC OK を設定したリゾルバでその後にレスポンスの認証を実行するのは 30%未満であると考えられます。認証をオンにしている、それらのリゾルバ運用者は、ネットワーク関連の問題を特定し、修正する手順に重点的に取り組んでいる可能性があります。なぜなら、ネットワーク関連の問題は発生する可能性が高く、そのために大きいレスポンスパケットを取得できなくなっている可能性があるためです。認証を実行していない、その他のリゾルバは、大きいレスポンスパケットを受け取る確率はかなり低いため、自社のネットワーク環境でそのような制限があることに気付いていない可能性があります。

テストにおいて大きいレスポンスを受信できなかったリゾルバの大半は、非認証リゾルバであり、ルートゾーンの DNSKEY リソースレコードのサイズが大きくなることの影響は受けないものと考えられます。

以上の内容を要約すると、これらのテストから、ルートゾーン KSK ロールオーバー時にレスポンスサイズが大きくなることの影響を受ける可能性があるのはユーザーの 0.04%未満であるが、これは、多くの不確定性要素を含む推定値です。また、キーセットが大きい TLD によって得られた関連する観察結果から、この数字は、レスポンスサイズが大きくなることの影響の範囲に基づく上限値であると考えられます。[23]

7.2 DNSSEC 認証の動作

DNSSEC 認証には、測定に関する 3 つの側面があります。1 つ目は DNSSEC デジタル署名 (クエリで EDNS(0) オプションの DNSSEC OK フラグを設定)、2 つ目はルートキーから認証される名前への信用の連鎖が作成される認証機能、3 つ目はユーザーの名前解決構成が DNSSEC 認証の失敗を確定的な失敗として受け取るのか、または別のリゾルバにクエリを参照するのかの相違です。

7.2.1 テスト結果

上記 (セクション 7.1.1) に記載した実験方法を使用して 2015 年 5 月に実施したテストでは、ユーザーの約 85%～90%が、クエリをリゾルバに送信しました。権威 DNS サーバーに渡された、キャッシュされていない名前に対するクエリには、EDNS(0) オプションがクエリに含まれており、DNSSEC OK フラグも設定されていました。

[23] 実験と結果の詳細は、http://www.potaroo.net/ispcol/2015-05/ksk.html に掲載されています。

同じサンプリング対象ユーザーのうちの約 24%は、後続のクエリを実行しました。すなわちこれは、リゾルバが相互署名の連鎖に従ってルートゾーン KSK の名前委任階層を逆引きし、DNSSEC を使用してレスポンスを認証したことを表します。

同じサンプリング対象ユーザーの約 11%は、「DNSSEC 認証を実行しない別のリゾルバに対してクエリを送信することで前回のクエリの送信での DNSSEC 認証の失敗に対処する」というエンドユーザーの動作に対応するものです。

以上のことから、DNSSEC 認証手順の何らかの変更がインターネットユーザー全体の約 4 分の 1 に影響を与える可能性があると予想されます。

これらのユーザー集団の半分弱は、DNSSEC 認証の失敗 (SERVFAIL のシグナル) を、DNSSEC 認証を実行しない別のリゾルバに対する同じクエリを表すシグナルとしてすでに解釈しています。インターネットのユーザーの 11%であるこの集団については、ルートゾーン KSK の変更によって未認識ルートゾーン KSK と認証の失敗が発生する可能性がありますが、これらのユーザーはすでに代替リゾルバを使用することで SERVFAIL を解釈できることが実証されています。結果として、DNSSEC で署名された名前の解決に時間がかかる可能性がありますが、名前をまったく解決できないという状況は発生しません。

残りの 13%の、SERVFAIL レスポンスの受信時に非認証リゾルバに戻さないユーザーは、ユーザーが使用するリゾルバが RFC 5011 鍵ロールオーバープロセスで提供されるシグナルに従うことができない場合に、DNSSEC で署名された名前を解決できない可能性があります。

7.2.2 結論

この測定プロセスを使用して、リゾルバが RFC 5011 プロセスに従って新しいルートゾーン KSK 値を自動取得できるかどうかをテストすることはできません。この測定プロセスで実行できるのは、DNSSEC 認証を実行するリゾルバを使用しているユーザー集団、さらには、RFC 5011 をサポートしているリゾルバ、または適切な段階で新しいルートゾーン KSK をロードする手動の介入を必要とするリゾルバを使用しているユーザー集団を数量化することです。

ユーザーの約 24%が DNSSEC 認証を実行するリゾルバを使用しており、したがって、ルートゾーン KSK ロールオーバーの影響を受ける可能性があります。認証の失敗によって SERVFAIL レスポンスが返され、全ユーザーの 11%は複数のリゾルバを使用していて、その 1 つのリゾルバからの SERVFAIL レスポンスによって、クエリが非認証リゾルバによって解決されることになります。したがって、全ユーザーの 13%

は、使用するリゾルバが RFC 5011 対応でなく、リゾルバ管理者が新しいルートゾーン KSK を適切な時期にロードしない場合に、ルートゾーン KSK ロールオーバーの影響を受ける可能性があることになります。

ただし、これらのユーザーの多くは、RFC 5011 対応のいずれかの大規模 DNSSEC 認証リゾルバサービス (Comcast の DNS リゾルバなど) を使用しているため、この 13% という数字は、この形で影響を受ける可能性があるユーザーの割合の上限です。

8 テスト

テストに関連する 2 つの要素があり、1 つは、運用停止につながる可能性がある負の影響のレベルを評価する目的で実施する、インターネットの一般的な運用に対する KSK ロールオーバーの影響を測定する作業で、もう 1 つは、自己テストのテスト環境リソースを含む、依拠当事者の運用準備に関する作業です。自己テストは、ソフトウェアを開発するチャネルパートナーや多数のサーバーを配備する運用者、または任意の希望者が実施するものです。

8.1 影響のテスト

認証の成功を測定する本報告書の他の部分のテストでは、DNSSEC 認証の失敗に対する一部のリアクションについては対象としていません。一部のクエリは DNSSEC から始めてその後に DNS に「フェイルオーバー」するという事実を前提にすると、KSK ロールオーバー時にこの方法が「被害」を評価する 1 つの手段になるとも考えられます。この「被害」とされる状況が認識されずに見過ごされる可能性もありますが、ルートゾーン KSK 鍵ロールオーバーの影響を観察するときには、重要な指標となるかもしれません。(画面を使用している) ユーザーは、この状況に気が付かず、そのために、サービスプロバイダーのヘルプデスクに問い合わせない可能性があります。

この状況を検出するテストは、現段階からルートゾーン KSK 鍵ロールオーバーが (成功または失敗のいずれかで) 終了するまでの間、定期的に (毎月) 実行するべきでしょう。鍵ロールオーバーの前にテストを実施することで、比較の基準が提供されます。

自動テストに加え、ルートゾーン KSK 鍵ロールオーバー期間中は、チャネルパートナーに連絡して、リアルタイムまたはほぼリアルタイムの詳細情報を提供する必要があります。こうすることで、影響を受ける関係者に事前に通知し、スタッフが少

ない時間帯を避け、連絡を取りやすい時間帯を優先させるという取り組みが推進されます。

8.2 自己テストの設備

依拠当事者が自己テストを実施する環境として、実速度より高速でロールオーバーの運用プラットフォームを模倣するテストプラットフォームを用意します。署名済みの偽のルートゾーンを使用し、実速度より高速のシミュレーションで RFC 5011 が動作するサーバーに加え、「別のデータ構造」のトラストアンカーを同じパス名で用意します。こうすることで、鍵の精査やバリデータでの動作 (ローカルまたはリモートの利用状況) の検出に役立つ優れたツールを生成できるようになります。

このような環境で異なるパラメータの鍵を挿入および削除できるようにすることは、新しいアルゴリズムに関する知識の習得に役立ちます。

タイミングは重要な要素であり、プロセスを十分に観察するためには、実速度より高速のシミュレーションが必要です。ただし、実速度のシミュレーションにもテストの影響を軽減するというメリットがあります。

そして最後に、ルートシステムの正確さを確保する必要があります。ルートゾーン全体がデータまたは見本の偽ゾーンとして使用されるかどうかを考慮します。

このようなテスト環境の既存の例 [24, 25]を、今後のテストでモデルとして使用できます。

8.3 KSK/ZSK メンテナのソフトウェアとプロセスの変更互換性テスト

KSK ロールオーバープロセスでは、既存のスケジュール、プロセス、および多くの場合はソフトウェアがサポートする KSK 処理の変更が必要であるため、ロールオーバーを開始する前に、これらの変更の完全テストを実行しなければなりません。この完全テストには、鍵生成、署名済み DNSKEY RRset の生成、DNSSEC 認証、KSR/SKR 交換、いずれかのフォールバックメカニズム、およびキーセレモニーのリハーサルが含まれますが、これらに限定されません。

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

9　実施

鍵ロールオーバーのプロセス案は、当初 2013 年 7 月に策定され、その後検討を重ねて練り直されました。以下に述べるプロセスは草案と見なすべきものであり、実施前に RZM パートナーによりさらに改善される可能性があります。

プロセスは以下の 3 段階に分割されます。

1) 次期ルートゾーン KSK の公開
2) 次期ルートゾーン KSK を使用する署名への移行 (「ロールオーバー」)
3) 現行ルートゾーン KSK の無効化

現行ルートゾーン KSK の無効化は、現行ルートゾーン KSK が鍵セットから削除された後に次期ルートゾーン KSK で問題が発生した場合にロールバックできるように、意図的に時期を遅らせています。プロセスは RFC 5011 に準拠することを意図し、次期 KSK の追加と現行 KSK の無効化のために十分な期間を設けています。このプロセスは、現行ルートゾーン KSK の無効化を無期限に延期するオプションを認め、ロールオーバープロセスで予期しない問題が発生し、計画された鍵ロールオーバープロセスの変更が必要となる場合に備えています。

次の図 1 は、プロセスが実施される 3 四半期の概要を示しています。四半期の番号はプロセス開始時期に対応したものであり、暦上の四半期には対応していません。たとえば、「Quarter 1」および「Q1」は、必ずしも 1〜3 月を指すわけではありません。「KSK-NEW」は次期 KSK を指し、「KSK-2010」は現行 KSK を指します。

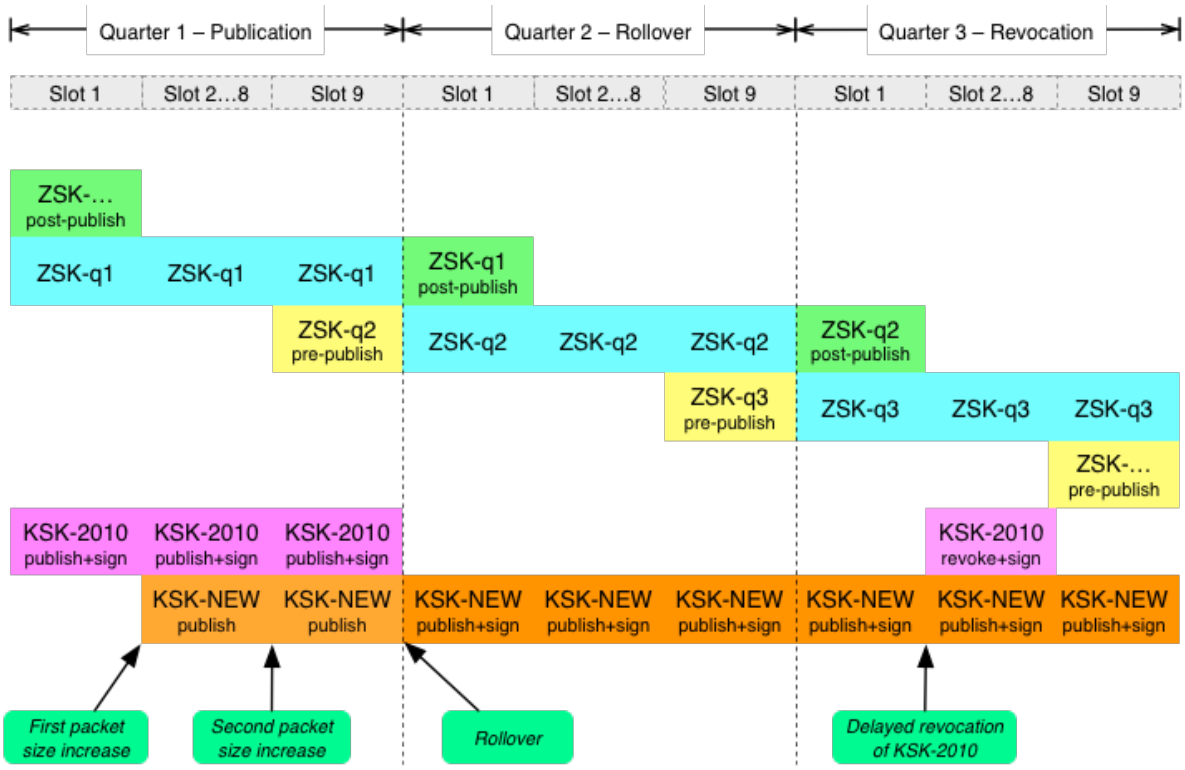

図 1: ロールオーバーのスケジュール

9.1 次期 KSK の公開

次期 KSK は、Q1 のスロット 2 で DNSKEY RRset に追加されますが、この時点では署名に使用されません。これは、RFC 5011 に準拠するバリデータが次期 KSK を選択するための暫定的な公開の段階です。次期 KSK は、署名に使用される前に合計 80 日間にわたってルートゾーンで公開 (および現行 KSK により署名) されます。手動で構成されたトラストアンカーについては、この期間前または期間内に更新して次期 KSK を含めることが期待されます。

ロールオーバーが RFC 5011 に準拠するためには、30 日以上の期間にわたって新しい鍵を公開する必要があります (「add-hold 期間」)。提案されている 80 日の公開期間が不十分であるとみなされる場合は、鍵ロールオーバーの前に公開のための四半期を 1 期またはそれ以上追加することが可能です。

次期 KSK の公開期間となる四半期中に、DNSSEC 検証リゾルバではルートゾーン DNSKEY RRset のクエリに対するレスポンスのパケットサイズ (レスポンスパケットサイズ) が 736 オクテットから 1,011 オクテットに増加することが確認されます。(この概念上の増加は、この段階で鍵ロールオーバーの期間外における DNS レスポンスのサイズと鍵ロールオーバープロセス中のサイズの比較に基づきます。)Q1 の最終

スロットの ZSK ロールオーバーでは、レスポンスパケットサイズは 833 オクテットから 1,158 オクテットに増加します。

9.2 次期 KSK へのロールオーバー

次期 KSK は、ロールオーバー後の Q2 のスロット 1 からルート DNSKEY RRset の署名に使用されます。この四半期は他の四半期と同様ですが、すべての DNSKEY RRset の署名に次期 KSK (のみ) が使用される点が異なります。DNSKEY RRset の署名に現行 KSK と次期 KSK の両方が使用されるのは、任意に実行される無効化期間中 (後述) のみです。

9.3 現行 KSK の無効化

現行 KSK が RFC 5011 に従って無効化される場合、現行 KSK は REVOKE ビットを含めて公開され、現行 KSK と次期 KSK の両方により署名されます。

現行 KSK の無効化は任意です。無効化を希望する場合、無効化した現行 KSK は Q3 のスロット 2 から Q3 のスロット 8 までの期間にわたって公開されます。

無効化期間中、レスポンスパケットサイズは 736 オクテットから 1,297 オクテットに増加します。

9.4 レスポンスパケットサイズへの影響

UDP の断片化を可能な限り回避することが期待されます。以下に、関連するレスポンスサイズの制約の一部を示します。

サイズ	閾値
512 オクテット	DNS によりサポートされる必要のある最小 DNS ペイロードサイズ。
1,232 オクテット	断片化不可能な IPv6 DNS UDP パケットの最大 DNS ペイロードサイズ
1,452 オクテット	断片化されない Ethernet IPv6 DNS UDP パケットの最大 DNS ペイロードサイズ
1,472 オクテット	断片化されない Ethernet IPv4 DNS UDP パケットの最大 DNS ペイロードサイズ

表 4: パケットサイズの閾値

前述のテスト結果には、一部の IPv6 リゾルバと大規模レスポンスの処理に潜在的な問題が示されています。このため、第一のもっとも顕著なサイズの制約は、断片化不可能な IPv6 DNS UDP パケットの閾値です。この閾値により、DNSKEY レスポンスパケットサイズは最大でも 1,232 オクテットとなります。

最初の閾値には、任意の無効化段階にならないと達しません。この段階では、現行ルートゾーン KSK を再導入して、REVOKE ビットによりフラグ付けする必要があります。RFC 5011 に完全に準拠するには、無効化段階で次期ルートゾーン KSK と現行ルートゾーン KSK の両方を使用して、DNSKEY RRset に二重署名する必要があります。RRset の二重署名により、レスポンスサイズが 1,232 オクテットを超えます。

ルートゾーンのレスポンスパケットサイズは、署名された DNSKEY RRset で最大となります。次の表は、提案されているロールオーバー期間内の DNSKEY レスポンスパケットサイズの概要と、ロールオーバー期間外のレスポンスパケットサイズとの比較を示しています。

期間	DNSKEY (ロールオーバー期間中)	RRSIG (ロールオーバー期間中)	DNSKEY レスポンスサイズ (ロールオーバー期間中)	DNSKEY レスポンスサイズ (ロールオーバー期間外)
Q1 のスロット 1	1x KSK + 2xZSK	1x KSK	883 オクテット	883 オクテット
Q1 のスロット 2〜8	2x KSK + 1xZSK	1x KSK	1,011 オクテット	736 オクテット
Q1 のスロット 9	2x KSK + 2xZSK	1x KSK	1,158 オクテット	883 オクテット
Q2 のスロット 1	1x KSK + 2xZSK	1x KSK	883 オクテット	883 オクテット
Q2 のスロット 2〜8	1x KSK + 1xZSK	1x KSK	736 オクテット	736 オクテット
Q2 のスロット 9	1x KSK + 2xZSK	1x KSK	883 オクテット	883 オクテット
Q3 のスロット 1	1x KSK + 2xZSK	1x KSK	883 オクテット	883 オクテット

Q3 のスロット 2〜8	2x KSK + 2xZSK	2x KSK	1,297 オクテット	736 オクテット
Q3 のスロット 9	1x KSK + 2xZSK	1x KSK	883 オクテット	883 オクテット

表 5:ロールオーバー期間中のパケットサイズ

(表の色付けされている部分は、次の図に対応しています。)

現行鍵の無効化を行わないことに関連するリスクについては詳細に述べませんでしたが、現時点では無効化段階は任意のものと見なされます。1 つのオプションとして、この点について RFC 5011 を更新し、現行鍵の無効化のために二重署名を必要としないように変更することが考えられます。この改訂には、失われた鍵や使用不可になった鍵を無効化できるという追加のメリットがあります。現行鍵を使用して二重署名する必要がなくなると、将来の鍵ロールオーバー、アルゴリズムの変更、および鍵長の変更がさらに推進されることにもつながります。ただし、コードを再定義、公開、開発、配布し、運用に持ち込むためには時間を要します。このため、今回の KSK ロールオーバーについて、このオプションが実行可能であるとは見なされません。

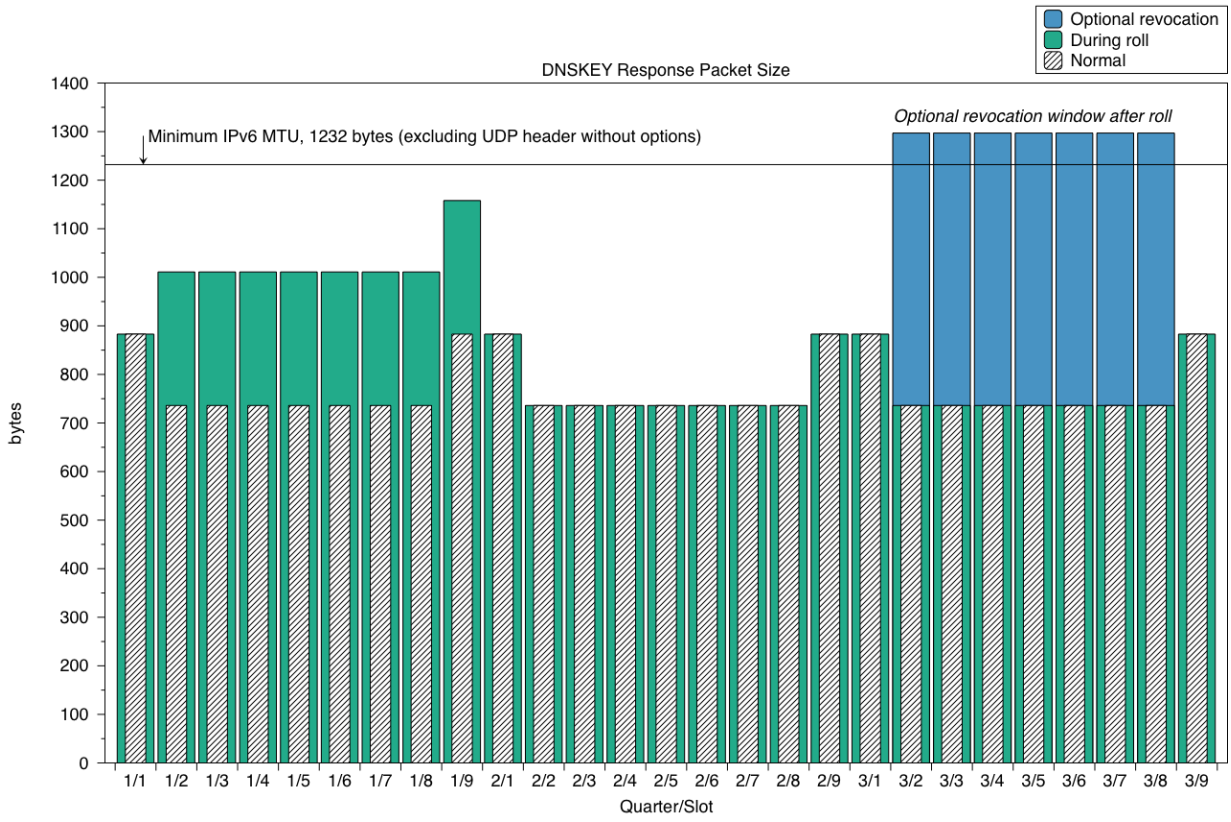

図 2: DNSKEY レスポンスパケットサイズ

9.5 ルートサーバーごとの展開

2010 年の DNSSEC の導入はルートサーバーごとに実施されました。予備バージョンの DNSSEC 署名付きゾーンが 2010 年 1 月に 1 つのサーバーに導入され、2 月には別のルートサーバーに導入され、3 月にはさらに 2 つのルートサーバーに導入されるといった形で行われました。その目的は、再帰的サーバー (または、ルートサーバーにクエリを送信するすべてのリソース) に対して、最初に DNSSEC を試行し、レスポンスが許容されない場合にフォールバックする機能を許すことでした。

この戦略は、ルートサーバーKSK ロールバックについても提案されましたが、多くの理由により却下されました。次期ルートゾーン KSK、および次期トラストアンカーの採用を評価する機能に関連する問題を回避するためには、以下の問題が現実に障害となりました。

DNSSEC の検証が失敗した場合の、検証用再帰的サーバーによる反応がツールによって異なります。再試行が非常に強引なツール、それほど強引ではないツール、積極的に試行しないツールなど、ばらつきがあります。

再帰的サーバー (または、すべてのクエリリソース) が特定のルートサーバーを優先することを明示的に決定したかどうかを検出することは、現実的ではないことが知られています。通常は、特定のルートサーバーを優先する再帰的サーバーを検出するための、ルートサーバーでのクエリソースの追跡は不十分です。　毎年、DNS-OARC により DITL の収集[26]が行われていますが、実施期間が短く、また大規模な作業であり、すべてのルートサーバーを網羅できていません。

最終的に考慮されるのは、次期トラストアンカーを徐々に導入するための期間となります。ルートゾーン ZSK 以外では、いずれの四半期も 70 日間となります。1 つの ZSK ロールオーバーの期間内で、次期 KSK を (最初のサーバーに) 追加するには 40 日間が必要であり、残りの 30 日間でタスクを完了しなければなりません。当初の逐次的展開では作業が長引き、4 か月間以上かかりました。

10 ロールバック

次期 KSK の導入後に深刻な問題が検出された場合は、現行 KSK のみを使用して署名された DNSKEY RRset を準備して、展開の準備を進める必要があります。これらの RRset は SKR (*Signed Key Response*) 形式であり、ロールバックしない RRset と同じルートゾーン KSK キーセレモニーを使用して作成できます。このようなロールバックの基準については、RZM パートナーがさらに策定する必要があります。

勧告 14：次期 KSK に関連する問題からの回復に要する時間を最小限に抑えるため、次期 KSK により生成される SKR と並行して現行 KSK により SKR が生成されるべきです。

勧告 15：RZM パートナーは、現行 KSK により生成された SKR を使用する必要のあるプロセスを開発して文書化すべきです。

プロセスのすべての四半期について、DNSKEY RRset を含むロールバック SKR を準備する必要があります。Q1 と Q2 の間、ロールバック SKR には DNSKEY RRset と共に現行 KSK、および現行 KSK により署名された現行 ZSK が含まれます。次期 KSK は除外されます。Q3 の間、ロールバック SKR には DNSKEY RRset と共に次期 KSK および次期 KSK により署名された現行 ZSK が含まれます。無効化された現行 KSK は除外されます。

閾値

[26] https://www.dns-oarc.net/ditl/2011

DNSSEC の展開のこれまでのテストでは、約 5%の誤差がこのようなテストに含まれることが示唆されています。したがって、発生する損害の大きさに関連する記述では、母集団 (測定の実施方法により人または再帰的サーバー) の 5%がパフォーマンス低下の影響を受けながら、これが検出されない可能性があることを認める必要があります。このため、特定の指標を定義することは、ロールバック実行の要因の定義に取り掛かる手段として見なされません。

さらに、損害がどのような形で顕在化するかも明らかではなく、誤った展開、誤ったコード、誤った手続き、インターネットの偶然の動作などの可能性が考えられます。このことから、チャネルパートナーとの連絡先を維持し、問題報告の手段を準備しておくことが最初のステップであり、次に報告への対応について判断します。

損害の重大度と広がりに加えて、多くのユースケースが存在するため、ロールバックせずに続行して検出された問題を修正する以上に、ロールバックにより損害が大きくなるかどうかについては明らかではありません。

11 時期

現在の運用環境を考慮すると、現行ルートゾーン KSK から次期ルートゾーン KSK に移行できる期間は 1 年に 4 日間あります。暦上の四半期の最初の日、つまり 1 月、4 月、7 月、および 10 月の 1 日がこれに該当します。変更日を具体的に選択する上では、運用上の合理性、および IANA 機能の監督権限の移管に関する現在の討議と矛盾しないことが考慮されます。[27]

運用上の合理性とは、週末、休日といった作業スケジュールに影響する日や、運用スタッフの業務に余裕のない期間を避けることを指します。全世界のユーザーに対して 3 日間を調整する必要があることから、すべてに対応できないことがあります。さらに、2016 年と 2017 年は各四半期の初日が金曜日、土曜日、または日曜日に当たり、初日が平日となる四半期は 2018 年までありません。(2015 年第 4 四半期は、10 月 1 日が木曜日ですが、この時点では計画が実施されておらず、この日に主要ロールオーバーを実施するために必要なテストも完了していません。)

非技術的な影響は、計画されている IANA 機能の監督権限の移管です。このため、特定の日付を提案することが現時点では現実的ではありません。

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

12 リスク分析

12.1 準備不足によるリスク

説明	影響	可能性	回避策
同じアルゴリズム、ハッシュ、およびサイズを使用する KSK ロールオーバーは、ステークホルダーにとって十分ではない	小	低	最初のロールオーバー完了後に次のロールオーバーを計画する。異なるパラメータが必要な場合は、変更する。
ネットワーク運用者が変更に気付かない (NOC がトラブルチケットを受け取り、対応方法を知る必要がある)	中	高	コミュニケーション計画で対応する。運用者を重視する。
ネットワーク運用者とソフトウェア開発者 (「すべてのチャネルパートナー」) が適切なテスト環境を持たない (利用できない)	中	高	加速した期間内のロールオーバーを使用して ICANN RFC 5011 のテストベッドをセットアップする。他のテストを実施する。
プロセスでの一元的なテストが実現可能でない	小	高	分散型アプローチによるテストを開発する。連絡先リストを作成する。

説明	影響	可能性	回避策
実施するかどうかの意思決定を下すための決定的な基準がない	小	高	コミュニケーションとテストを準備する必要がある。現場で使用されるメカニズムの実現可能性を調査する。更新されたトラストアンカーの受け入れの測定方法を開発するために長期的に取り組む。

12.2 自動トラストアンカーのメカニズムが機能しない、または不適切である

説明	影響	可能性	回避策
RFC 5011 が全面的に実現されていない	中	高	トラストアンカー管理の代替アプローチ
RFC 5011 の実施が不完全	中	低	ソフトウェア開発者に連絡する。RFC 5011 についての理解を確認する。
バリデータのブートストラッププロセスの実施が不完全	中	低	システムインテグレータとトラストアンカーハンドラーに連絡する
ICANN の IANA Web サイトでトラストアンカーセットを利用できない	小	低	可用性を監視する
保守の不足により、同期されていないトラストアンカーセットが機器で使用される	小	高	コミュニケーション計画

12.3 現行 KSK の削除による検証の失敗

説明	影響	可能性	回避策
自動トラストアンカープロトコルへの準拠が不十分 (プロセスのいずれかの参加者について)	小	高	テスト、コミュニケーション。運用者が問題解決を加速するためのリソースを提供する。
失敗に際しての再試行によるトラフィックの増大	小	低	「ロールオーバーと失敗[28]」による影響を審査する。ネガティブキャッシュを提案する。

12.4 次期 KSK の追加により DNS メッセージサイズが制限を超える

説明	影響	可能性	回避策
キーセットの移行によるデータグラムのサイズ肥大	中	低	メッセージサイズの審査により移行を入念に計画する
DNS ソフトウェアでの IPv6 断片化の処理に関する混乱	小	低	DNS ソフトウェアの審査とテスト

[28] http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf、http://www.potaroo.net/ispcol/2010-02/rollover.html

12.5 運用上のエラーの発生

説明	影響	可能性	回避策
KSK ロールオーバーの失敗により DNSSEC 採用の機運がくじかれる	大	低	慎重な設計/再検討
主要ロールオーバーを無期限に延期することにより、ロールオーバーが緊急に必要となった場合の影響が拡大する	大	低	ルートゾーン KSK ロールオーバーに取り組む
いったん開始すると、現在の許容された状態に戻ることができない	大	低	フォールバック計画を定義する
現行 KSK (プライベートコンポーネント) が適切に使用不可になっていない	小	低	計画の完全な実施に取り組む

13 設計チームのメンバーリスト

13.1 コミュニティの有志

- ジョー・アブリー、Dyn, Inc. (カナダ)
- ジャープ・アカフイス、NLNetLabs (オランダ)
- ジョン・ディッキンソン、Sinodun Internet Technologies (英国)
- ジェフ・ヒューストン、APNIC (オーストラリア)

- アンドレイ・スリ、CZ.NIC (チェコ)
- ポール・ボウタース、No Hats/Red Hat (オランダ)
- 米谷嘉朗、JPRS (日本)

13.2 ルートゾーン管理パートナー

- デイヴィッド・コンラッド、ICANN
- エドワード・ルイス、ICANN
- リチャード・ラム、ICANN
- アラン・デュラン、ICANN
- ヘイリー・ラフランボワーズ、ICANN
- エリーズ・ゲーリック、ICANN
- キム・デイビーズ、ICANN
- ロイ・アレンズ、ICANN
- ヤコブ・シュリーター、ICANN
- フレドリック・ユングレン、ICANN
- ブラッド・ヴァード、Verisign
- デュアン・ウェッセルズ、Verisign
- デイヴィッド・ブラッカ、Verisign
- アル・ボリヴァー、Verisign
- ティム・ポーク、US DoC NIST
- スコット・ローズ、US DoC NIST
- ダグ・モンゴメリ、US NIST
- アシュリー・ハイネマン、US DoC NTIA
- ヴェルニタ・ハリス、US DoC NTIA

14 参考資料

- 「RFC 5011:Automated Updates of DNS Security (DNSSEC) Trust Anchors」 https://tools.ietf.org/html/rfc5011
- 「SAC063:SSAC Advisory on DNSSEC Key Rollover in the Root Zone」 https://www.icann.org/en/system/files/files/sac-063-en.pdf
- 「DNSSEC Practice Statement for the Root Zone KSK Operator」 https://www.iana.org/dnssec/icann-dps.txt
- 「DNSSEC Practice Statement for the Root Zone ZSK Operator」
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

- 「DNSSEC Trust Anchor Publication for the Root Zone」
  https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- 「Establishing an Appropriate Root Zone DNSSEC Trust Anchor at Startup」
  https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 付録: チャネルパートナー

「チャネルパートナー」とは、ルートゾーン KSK の管理の価値を独立して実現または提供する外部組織です。これらの組織は RZM パートナーとの正式な関係を持ちませんが、ある程度の調整が必要です。各組織について適切な連絡先を置き、ルートゾーン KSK の変更に関連するステータスなどの情報を交換する必要があります。

チャネルパートナーの一覧に特定の順序はありません。

15.1 ソフトウェア作成者

これらのパートナーとの実質的なコミュニケーションは、ソフトウェアへの RFC 5011 トラストアンカー管理の実装 (またはその非実装) に関連します。これらは、検証用再帰的キャッシュサーバーを使用するパートナーです。これらの組織の連絡先情報は、本書には一覧されていません。

- ISC の BIND (http://www.isc.org)
- NLNetLab の Unbound (https://nlnetlabs.nl)
- Microsoft Windows Server (https://www.microsoft.com/)
- Nominum の Vantio (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/
- Secure64 DNS Cache (http://www.secure64.com/)

15.1.1 保留

以下のパートナーは、DNSSEC の検証用再帰的キャッシュサーバーについて検討しましたが、リリースしていません。コードが配布された場合はリストに含められます。(DNSSEC をサポートしない他の再帰的 DNS キャッシュサーバーは、ルートゾーン KSK に依存しません。)

- CZ.NIC の再帰的サーバー (未定) (Knot 以外)
- PowerDNS (未定)

15.2 システムインテグレータ

これらのチャネルパートナーは、構成データの一部としてルートゾーン KSK を提供します。構成データは、場合によっては前述の DNS ソフトウェアを含みます。これ

らの組織が次期ルートゾーン KSK について検討し、これをソフトウェアの更新に含めることが期待されます。

15.2.1 Linux

- Red Hat Enterprise Linux (RHEL) RPM
- Micro Focus International の SUSE (RPM)
- Fedora
- CentOS
- Debian および Canonical (Ubuntu) APT
- Montavista Linux

15.2.2 BSD

- FreeBSD ポート
- NetBSD pkgsrc
- OpenBSD ポート

15.2.3 その他

- Apple iOS、OS X
- Google Android、ChromeOS
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco/Linksys
- Wind River (RTOS)
- QNX (RTOS)
- OpenVMS
- OpenWRT

15.3 パブリックリゾルバ運用者

これらの運用者は、再帰的 DNS サーバーを実行し、場合によっては DNSSEC を検証することが報告されています。これらの運用者は、ルートゾーン KSK を構成データの一部として含むことが期待されます。このため、次期ルートゾーン KSK について情報を得るための内部審査が行われることがあります。

- Google Public DNS

- OpenDNS
- Neustar DNSAdvantage
- Symantec ConnectSafe
- Level 3
- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

パブリックリゾルバを使用する上記の運用者は、インターネット上からのトラフィックの受け入れに基づいて (把握できる限りにおいて) 選ばれていますが、その他にも依拠当事者ベースに対する制約を持つパブリックリゾルバを運用するパートナーも存在します。これらのパートナーが識別された場合には、ルートゾーン KSK イベントの通知が提供されます。