# 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

ICANN CTO オフィス（OCTO）

2018 年 8 月 22 日

# 要約

現時点で、2018 年 10 月 11 日にルート KSK ロールオーバーが行われる予定です。実施後、ごく少数ながら一部のインターネットユーザーが一部のドメイン名解決で問題を抱えることが予想されます。現在のところ、少数の DNSSEC（Domain Name System Security Extensions）検証用再帰リゾルバの構成が適切でないため、これらのリゾルバを使用するする一部のユーザーで問題が発生すると予想されます。本書では、どのようなユーザーで問題が発生し、どうような場合にどのような問題が発生するかについて説明します。

- DNSSEC 検証を実行しないリゾルバを使用するユーザーは、ロールオーバーによる問題の影響を受けません。
- 新しい KSK を採用するリゾルバを使用するユーザーは、ロールオーバーによる問題の影響を受けません。
- ユーザーのリゾルバのすべてで、トラストアンカー構成に新しい KSK が含まれていない場合、ロールオーバー実施後 48 時間以内に影響が認識され始める可能性が高いと考えられます。
- 影響を受けるリゾルバのオペレータが検証の失敗に気づくタイミングを予測することは不可能です。
- データ分析では、検証リゾルバを使用しているユーザーの 99%以上は KSK ロールオーバーの影響を受けないことが示されています。

# 1. はじめに

ICANN 組織は、DNS ルートゾーン KSK のロールオーバー予定について、何年も前から情報を発信しています。[1] ロールオーバー計画の改訂[2] に関する最近のパブリックコメントでは、ロールオーバープロセスの詳細についてコミュニティの多くのメンバーから質問が出されました。ICANN 組織は、ロールオーバーの準備に役立つ資料をさらに公開することに合意しました。[3] 本書はその取り組みの一環となります。

ロールオーバー実施後に発生する（および発生しない）影響をめぐって、さまざまなコミュニティで混乱が起きています。本書では、ロールオーバーが起きる瞬間から何が予想されるかについて詳しく説明します。

本書の対象読者は多岐にわたりますが、本書は主として次の読者を念頭に置いています。

[1] http://www.icann.org/kskroll
[2] https://www.icann.org/public-comments/ksk-rollover-restart-2018-02-01-en
[3] https://www.icann.org/en/system/files/files/report-comments-ksk-rollover-restart-23apr18-en.pdf

- 検証リゾルバを使用しており、ロールオーバー実施後に何に注意する必要があるのかを知る必要のあるオペレータ
- 非技術系のメディア関係者など、ロールオーバー実施前後に関連記事を作成する予定の方々
- ロールオーバー実施後に起こるリゾルバの失敗の兆候について、DNS を監視する予定の研究者

ロールオーバーに対応しているリゾルバが少なくとも 1 つあるユーザーの場合、本書の必要性は低いと考えられます。ロールオーバー実施後に、これらのユーザーが DNS またはインターネット全般の使用で変化を認識することはありません。DNSSEC 検証をまったく実行しないリゾルバを使用しているユーザーについても、同様のことが当てはまります。現時点の推定によると、ユーザー全体の約 3 分の 2 は、現在でも DNSSEC 検証を実行していないリゾルバを使用しています。

ロールオーバーは、現在のところ 2018 年 10 月 11 日に行われる予定です。KSK ロールオーバーの日付は、ロールオーバー実施前に必要とされる ICANN 理事会の承認待ちとなっています。ロールオーバーは、当初は *2017* 年 10 月 11 日に計画されていましたが、実施直前に不明確なデータ受信があったために延期されました。[4]

本書のセクション 2 とセクション 3 では、ロールオーバーに対応している検証リゾルバと対応していない検証リゾルバのぞれぞれでロールオーバー後に予想される影響について説明します。セクション 4 では、DNS ルートサーバーシステムへのトラフィックを監視している研究者が認識する可能性のある事象について説明します。本書は全体を通して、ロールオーバーの後に起こる事象について断定的ではない表現を用いています。これは、リゾルバのオペレータでない限り、リゾルバがどのソフトウェアを実行しているかを正確に把握できず、リゾルバがロールオーバーに対応するよう適切に構成されているかどうかも判断できないためです。

***リゾルバオペレータ向けの重要事項:*** 検証リゾルバのすべてのオペレータは、ロールオーバーに対応しているかどうかを直ちに確認する必要があります。そのために、現在のトラストアンカーをチェックしてください。[5] 対応していない場合は、できるだけ早期に最新のトラストアンカーに更新する必要があります。[6] DNSSEC 検証を実行していないリゾルバのオペレータは、すでにロールオーバーに対応していることになります。

## 1.1 ルート KSK ロールオーバーの定義

2010 年に、DNS ルートゾーンに DNSSEC の署名が追加されました。DNS ルートゾーンには 2 種類の鍵があります。ゾーン署名鍵（ZSK）はルートゾーン内のメインデータに署名し、鍵署名鍵（KSK）はルートゾーン内のルート鍵セット（ZSK と KSK の両方）だけに署名します。ZSK は、3 か月ごとに新しく発行されます。新しい ZSK それぞれに、より寿命の長い KSK が署名します。

[4] https://www.icann.org/news/announcement-2017-09-27-en
[5] https://www.icann.org/dns-resolvers-checking-current-trust-anchors
[6] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

ロールオーバーは、ルート KSK が変更され、新しい KSK がそのゾーンのルート鍵セットに署名を開始するときに起こります。ロールオーバーが行われると、元の KSK が廃棄され、新しい KSK が使用されます。最初の KSK は、KSK-2010 と呼ばれます（現在も使用中）。新しい KSK は、KSK-2017 と呼ばれます。ロールオーバー後、KSK-2010 はルート鍵セットに署名しなくなり、代わりに KSK-2017 がルート鍵セットに署名します。

### 1.2 トラストアンカー

ロールオーバーがどのように行われるかを理解するには、検証リゾルバがルート KSK を信頼する仕組みを理解することも重要です。各検証リゾルバは、ルート KSK と一致する鍵または鍵識別子のコピーである一連の *トラストアンカー* で構成されます。通常、ソフトウェアベンダー、または RFC 5011 に記載されているプロセスを使用してトラストアンカーを自動的に更新するよう構成されたリゾルバ、またはリゾルバのトラストアンカーストアに新しい KSK を手動で追加するリゾルバオペレータが、トラストアンカーを自動的に構成します。[7]

KSK-2017 が作成される前は、すべての検証リゾルバでは KSK-2010 のみがトラストアンカーとして構成されていました。KSK-2017 が作成されて公開された後、ほとんどの場合にリゾルバオペレータはリゾルバのトラストアンカー構成に KSK-2017 を手動で追加したか、またはソフトウェア（RFC 5011 自動更新プロセスなど）あるいはソフトウェアベンダーによって変更が行われました。ただし、一部のリゾルバオペレータは構成を更新しませんでした。このようなオペレータは、ロールオーバーに対応しておらず、現在も KSK-2010 のみをトラストアンカーとして使用しています。ロールオーバーが行われると、これらのリゾルバオペレータは有効なトラストアンカーを持たなくなります。

## 2. ロールオーバーへの対応準備ができているリゾルバ

ロールオーバーに対応しているリゾルバには、すでに KSK-2017 がトラストアンカーとして構成されています。新しいルート KSK はすでにルート鍵セットへの署名のために信頼されているため、ロールオーバーが起こると、これらのリゾルバはロールオーバー前と同じように動作します。リゾルバソフトウェアの中には、ロールオーバーが行われたことを運用ログに記録するものもあります。しかし、そのようなログエントリ（たとえあったとしても）は、オペレータが意識的に見つけようとしない限り、認識されることはないでしょう。

ロールオーバーに対応しているリゾルバのユーザーは、ロールオーバーが起こっても変化に気づきません。通常のクエリに返される応答は、ロールオーバーの前後で同じです。APNIC が最近実施した調査によると、DNSSEC 検証を実行するリゾルバでロールオーバーに対応しているユーザーの割合は 99%以上に上ります。[8]

ほとんどのインターネットユーザーは、複数の DNS リゾルバを構成しています。ユーザーが構成したリゾルバのいずれかがロールオーバーに対応している場合、ソフトウェアはロールオー

[7] https://datatracker.ietf.org/doc/rfc5011/
[8] http://www.potaroo.net/ispcol/2018-04/ksk.html

バー後にそのリゾルバを見つけ、引き続き使用します。このとき、DNS の解決に要する時間が長くなる可能性があります。これは、対応しているリゾルバに切り替わるまで対応していないリゾルバを試していくために発生する現象です。そのような場合でも、DNS の解決は行われます。

# 3. ロールオーバーへの対応準備ができていないリゾルバ

リゾルバに構成されたトラストアンカーが KSK-2010 鍵だけの場合、ロールオーバーが起こると、リゾルバは権威サーバーから取得する応答の検証に失敗するようになります。ただし、このような失敗が起こり始める時期は予測できません。

DNS での発行は即時のアクションとなりますが、リゾルバが新しく発行されたレコードを認識するまでに時間がかかる可能性もあります。DNS 内の各レコードは「生存時間」（通常は *TTL* と呼ばれます）を持ち、この期間が続いている間は、リゾルバは新しいバージョンのレコードの取得を試みません。ロールオーバーの後も、リゾルバは KSK-2010 によって作成された署名のキャッシュされたバージョンを持っている可能性が高いため、少なくともしばらくの間は引き続き正常に検証を行います。

## 3.1 ZSK を検証できなくなると失敗が発生する

検証リゾルバは、権威ネームサーバーから応答を受け取るたびに、応答の署名をチェックします。それぞれの名前について、署名の検証ステータスがキャッシュに保存されます。たとえば、「www.example.com」という名前の署名を検証する場合、リゾルバは、ルート、「.com」、「example.com」、「www.example.com」で署名を検証する必要があります。通常、リゾルバはこれらの検証をキャッシュするので、名前ごとに検証を実行することはありません。ほとんどのリゾルバは、検証ステータスが変更された場合にのみ検証を実行します。

KSK レコードと ZSK レコードの TTL は 48 時間です。ロールオーバーが行われる*直前*にリゾルバがルート鍵セットを取得して検証した場合は、ほぼ 2 日間にわたってリゾルバはロールオーバーを認識しないことになります。これは、ルート鍵セットの TTL が期限切れになった後に最初のクエリを取得するまで、リゾルバは新しい KSK をフェッチしないためです。通常は、数名のユーザーがリゾルバを使用しています。この場合、DNSKEY レコードの TTL が期限切れになってから数分（または数秒）以内にトリガーとなるクエリが発生すると予想されます。一方、リゾルバのユーザーが 1 人だけの場合は、ルート鍵セットの TTL が期限切れになった後の最初のクエリが実行されるまでの時間が数時間あるいは数日間にも及びかねません。

ただし、実際はこれほど単純ではありません。たとえば、一部のリゾルバは TTL の最大長を強制的に適用します。これによって、より早期にリゾルバが鍵のロールオーバーを認識する可能性があります。ほかの構成要素も、リゾルバが最初にロールオーバーを認識するタイミングに影響します。

## 3.2 すべてのリゾルバが失敗したときにユーザーが受ける影響

ロールオーバーが起こってから 48 時間以内に、リゾルバがルート鍵セットを再度取得するために、一部のユーザーの DNS クエリが失敗するようになります。前述のとおり、この 48 時間のどのタイミングで失敗が始まるのかは予測できません。

この失敗が発生したとき、ユーザーが構成しているリゾルバが複数あれば（大部分のユーザーがこれに該当します）、システムソフトウェアはほかの構成済みリゾルバを試行します。このとき、DNS の解決に要する時間が長くなる可能性があります。これは、対応しているリゾルバに切り替わるまで対応していないリゾルバを試していくために発生する現象です。そのような場合でも、DNS の解決は行われ、ユーザーが遅延に気づかないこともあります。しかし、ユーザーのリゾルバのすべてがロールオーバーに対応していない場合（例：すべてのリゾルバを管理しているのが、ロールオーバーへの対応準備を整えていない 1 つの組織である場合）、ロールオーバー後 48 時間以内のいずれかの時点で失敗が発生します。

どのようなプログラムを実行しており、そのプログラムが DNS ルックアップの失敗にどのように反応するかによって、ユーザーが認識する失敗の症状は異なります。ブラウザの場合は、Web ページを利用できなくなる可能性があります（または、すでに表示されている Web ページの画像のみが表示されなくなることもあります）。電子メールプログラムの場合は、ユーザーが新しいメールを取得できなくなったり、メッセージ本文の一部にエラーが表示されたりする可能性があります。インターネットから新しい情報を表示できるプログラムがなくなるまで、失敗は連鎖して広がっていきます。

ここでの「ユーザー」は、単に人間だけを指すものではありません。自動化されたシステムも、対応していないリゾルバを DNS 解決に使用している場合には失敗し始め、場合によっては壊滅的な影響を受けます。

リゾルバのオペレータが、（トラストアンカーとして KSK-2017 を追加することによって、または検証をオフにすることによって）検証の問題を解決すると、インターネットのユーザーエクスペリエンスはほぼ直ちに正常に戻ると考えられます。

## 3.3 リゾルバオペレータが失敗を把握する方法

重大なエラーを探すためのシステム監視ソフトウェアが構成されている場合、リゾルバがルート鍵セットの新しいコピーをフェッチして検証に失敗すると、リゾルバのオペレータは直ちに警告を受けます。このような監視により、オペレータが迅速に失敗を検出して復旧する可能性が高くなります。

オペレータが重大なエラーを積極的に監視していない場合、リゾルバに依存している自動システムが失敗し始めるか、ユーザーから停止が報告され始めるまで、オペレータは検証の失敗に気づかない可能性があります。また、トラストアンカーの構成が不適切なリゾルバだけをオペレータが使用している場合も、送信された電子メールメッセージを取得できない可能性があり、問題の報告を受ける手段が電話だけになることがあります。

### 3.4 影響からの回復

リゾルバの DNSSEC 検証に失敗したことをオペレータが検出した場合は、即座にリゾルバの構成を変更して、DNSSEC 検証を一時的に無効にする必要があります。これによって、直ちに問題の発生が止まります。

その後、オペレータは、できるだけ速やかに KSK-2017 をトラストアンカーとしてインストールし、DNSSEC 検証を再度有効にする必要があります。ICANN 組織は、一般的なリゾルバソフトウェアでトラストアンカーを更新する手順を提供しています。[9]

## 4. ルートサーバーオペレータが受ける影響

ロールオーバーの後、ルートサーバーオペレータがロールオーバーに対応していないリゾルバから受け取るクエリが大幅に増加すると予想されます。クエリの多くはルートの DNSKEY（./IN/DNSKEY）に対するものになると予想され、.net ゾーンの DS レコード（.net/IN/DS）に対するものが含まれる可能性もあります。さらに、応答が正しく検証されないため、応答のキャッシュが行われず、これらの検証リゾルバからの全体的なトラフィックが増加します。同様に、ほかのリゾルバからのフォワーディングを許可しているリゾルバのオペレータでは、ロールオーバー後にこれらのリクエストが増加する可能性が高くなります。

研究者は、1 分あたりの標準的なクエリ数についてベースラインを把握するため、ルート DNSKEY 要求のルートサーバートラフィックをすでに監視しています。これらの統計情報は、12 のルートサーバー組織のうち 11 の組織によって、ニアリアルタイム（1 分に 1 回）で ICANN に報告されています。ICANN は、ロールオーバーの開始後もこれらの統計情報を引き続き監視し、ルートサーバーオペレータをはじめとする DNS 技術コミュニティ全体に結果を報告します。

## 付録 A. ロールオーバーに関する詳細情報のリソース

ロールオーバーに関する情報の主な情報源は次のとおりです。

http://www.icann.org/kskroll

このページでは、KSK ロールオーバーのクイックガイド、DNSSEC に関する多様なリソース、コミュニティがロールオーバーを選択した理由、およびロールオーバーの計画について情報を提供しています。英語、スペイン語、フランス語、ロシア語、アラビア語、中国語、ポルトガル語、韓国語、日本語で情報を入手できます。

次のメーリングリストに登録すると、ロールオーバーに関するディスカッションに参加できます。

https://mm.icann.org/listinfo/ksk-rollover

[9] https://www.icann.org/dns-resolvers-updating-latest-trust-anchor

# 付録 B. 用語

DNSSEC：DNS のセキュリティ拡張（Domain Name System Security Extensions）。レコード内のデータが変更されていないことをリゾルバが確認できるようにするため、権威サーバーが DNS レコードに暗号署名を追加します。[10]

KSK（Key Signing Key）：鍵署名鍵。ゾーン内のすべての鍵に署名するために使用される鍵です。

ロールオーバー：ゾーン内の鍵署名鍵を既存の鍵から新しい鍵へ変更すること。

TTL（Time To Live）：DNS 内の一連のレコードの「存続時間」。リゾルバが権威サーバーから一連のレコードを受け取ると、通常は TTL として示された期間中、レコードがキャッシュに保持されます。

検証：DNSSEC で保護されているゾーン内のレコードの署名を検証すること。リゾルバは、権威サーバーから受け取ったレコードが正しいことを確認するために、検証を実行します。

ZSK（Zone Signing Key）：ゾーン署名鍵。ゾーン内のすべてのレコード（ただし、鍵だけは鍵署名鍵により署名される）に署名するために使用される鍵です。

[10] https://meetings.icann.org/en/marrakech55/schedule/sun-dnssec-everybody