クイックガイド:
ルートKSKロールオーバーに向けたシステムの準備

ルートKSKロールオーバーとは?

Internet Corporation for Assigned Names and Numbers（ICANN）は、ルートゾーンKSKと呼ばれる、ドメイン名システムのセキュリティ拡張（DNSSEC）プロトコルで使用される暗号化鍵の「最上位」のペアを導入または変更することを予定しています。これは、KSKが2010年に最初に作成されてから初めての変更となります。定期的なパスワードの変更は、インターネットユーザーにとって重要なセキュリティ対策であるように、ICANNにとっても今回の措置は重要なセキュリティ対策となります。

鍵を変更するには、新しい暗号鍵ペアを生成し、新しいパブリックコンポーネントをDNSSEC検証リゾルバに配布する必要があります。DNSSECを使用するすべてのインターネットクエリがルートゾーンKSKを利用してその送信先を検証するため、これは重要な変更となります。新しい鍵が生成されると、ユーザーがWebサイトにアクセスするときに、新しいKSKでその鍵を検証できるように、ISPなどのWeb関連の事業者は、新しい鍵を使用してシステムを更新する必要があります。

準備が必要となる理由

現在、全世界のインターネットユーザーの4分の１が、DNSSEC検証リゾルバを使用しており、KSKロールオーバーの影響を受けると考えられます。新しいKSKが導入されるときに、これらの検証用のリゾルバに新しい鍵がない場合、これらのリゾルバを利用しているエンドユーザー側でエラーが発生し、インターネットにアクセスできなくなります。

DNSSECを使用していない場合、システムはロールオーバーの影響を受けません。しかし、DNSSECはドメイン名のハイジャックを防止する上で重要な役割を果たします。

ICANNは、事業者や関係者がシステムで自動更新プロセスを正しく処理できることを確認するためのテストベッドを提供しています。次のサイトにアクセスしてシステムの準備が整っていることを確認します：**https://go.icann.org/KSKtest**。

DNSSECの検証を有効にしている場合は、新しいKSKを使用してシステムを更新し、ユーザーが引き続きインターネットにアクセスできるようにする必要があります。

デザイン担当： ICANN Communications | 2018年3月

必要な操作

2017年7月11日に公開された新しいルートゾーンKSKを使用して、ロールオーバーの実施前にいつでもシステムを更新できます。また、一部のシステムではすでに自動更新が行われている場合があります。以下の状況によって、実施する必要がある操作は異なります。

DNSSECトラストアンカー（RFC 5011）の自動アップデートがソフトウェアでサポートされている場合：

KSKは適切なタイミングで自動的に更新されています。特にユーザーによる操作は必要はありません。

ロールオーバー中にオフラインになっているデバイスについては、ロールオーバーの完了後にオンラインになった場合、手動で更新する必要があります。

ICANNは、2017年3月からテストベッドの提供を開始しています。テストベッドを使用すると、事業者や関係者は、システムが自動更新プロセスを正しく処理できるかどうかを確認できます。詳細情報は、**https://icann.org/kskroll**でご確認いただけます。

お使いのソフトウェアがDNSSECトラストアンカー（RFC 5011）の自動更新をサポートしていないか、または使用するように設定されていない場合：

ソフトウェアのトラストアンカーファイルを手動で更新する必要があります。新しいルートゾーンKSKは、以下のサイトから入手できます：**https://go.icann.org/2DOB7zn**。

KSKロールオーバーの実施時期

KSKのロールオーバーは一連のプロセスであり、一度限りのイベントではありません。以下の日付は、このプロセスの重要な工程であり、エンドユーザーはインターネットサービスに一時アクセスできなくなる場合があります。

2018年10月11日

新しいKSKを最初の署名に使用することが推奨される日付。

2019年1月11日

古いKSKを失効することが推奨される日付。

今後の変更に対する準備を進める上で役立つリソースなど、ロールオーバーに関する詳細については、**https://icann.org/kskroll**を参照してください。

「KSK Rollover」という件名を付けて、**globalsupport@icann.org**に電子メールを送信いただくこともできます。#KeyRollを使用してTwitterでのコミュニケーションに参加いただくこともできます。

デザイン担当： ICANN Communications | 2018年3月