総 基 デ 第 ４ ９ 号
平成２９年７月１４日

内閣官房内閣サイバーセキュリティセンター
　副センター長　殿
内閣官房情報通信技術（ＩＴ）総合戦略室
　副政府ＣＩＯ　殿

総務省　総合通信基盤局長

ＤＮＳの世界的な運用変更に伴うキャッシュＤＮＳサーバーの
設定更新の必要性について

この度、インターネットの重要資源の世界的な管理・調整業務を行う団体ＩＣＡＮＮ（Internet Corporation for Assigned Names and Numbers）が、ＤＮＳ（ドメインネームシステム）において電子署名の正当性を検証するために使う暗号鍵の中で最上位となる鍵（ルートゾーンＫＳＫ）の更改を実施します。

これに伴い、キャッシュＤＮＳサーバーを運用する者（契約者向けにサービス提供するインターネットサービスプロバイダ、ＬＡＮ利用者向けにサービス提供する官庁、独法、学校、企業等。以下「運用者」という。）においては、別紙のとおり、速やかに事前公開されているルートゾーンＫＳＫの公開鍵の情報を更新する等の措置を講じる必要があります。

なお、本年９月１９日までに必要な措置が講じられない場合、web サイトへのアクセスやメールの送信ができない利用者が生じる可能性があります。

つきましては、貴センターから、各府省等担当部局を通じ、運用者に対して別紙の事項を周知いただきたく、ご協力をお願いします。

なお、本文書は、ＩＣＡＮＮから総務省に対する周知依頼文書（総基デ受 50）に基づき、発出するものです。

DNS における電子署名鍵の更改について

平成２９年7月１４日

総務省総合通信基盤局データ通信課

１．目的

DNS（ドメインネーム・システム）は、「www.soumu.go.jp」などのホスト名（人が理解しやすいようにつけたサーバーの名前）を、インターネット上の住所である IP アドレスに変換するために利用される「検索」の仕組み。

この検索結果が第三者の成りすましにより改ざんされないよう、電子署名を付加した「DNSSEC」という仕組みで運用されるのが一般的である。

本年 7 月～来年 3 月にかけて、当該電子署名の正当性を検証するために使う鍵の中で、最も中核をなす「ルートゾーン KSK」について、その信頼性維持のため、史上初めて更改することが発表された。

２．対応が必要となる者

DNS を用いた検索を実際に行う「キャッシュ DNS サーバー」の運用者全て

（例：契約者向けに提供するインターネットサービスプロバイダ、LAN 利用者向けに提供する官庁・独法・学校・企業など）

３．鍵の更改に伴い生じる可能性のあるトラブル

(1) 「鍵の更改」に追従できず、検索結果の正当性が確認できない（結果として、検索結果が「信用できない」ものとして取り扱われる）ため、web サイトへのアクセスやメールの送信ができない利用者が生じる可能性がある。

(2) 「鍵の移行期間」において、「鍵の正当性を確認する情報」や「電子署名」について、旧来の鍵用と新しい鍵用の双方を送受信する必要があるため、当該期間において検索結果として送受信されるデータ量が増大することから、検索結果をインターネット経由で正常に送受信できなくなり、web サイトへのアクセスやメールの送信ができない利用者が生じる可能性がある。

４．トラブルを生じさせないために必要となる措置

本年９月１９日までに、以下の措置が必要。

(1) 「鍵の更改」に追従するために、

①「キャッシュ DNS サーバー」のソフトウェア（一般に「BIND」又は Windows Server を利用）を最新版に更新する（今回の対策だけでなく、脆弱性への対応のためにも、最新版への更新は必須。）。

②「キャッシュ DNS サーバー」において、「DNSSEC のトラストアンカーの自動更新」の設定を行う。

③念のため、「キャッシュ DNS サーバー」において、「DNSSEC」が有効になっており、また「DNSSEC の検証」が有効になっていることを確認する。

(2) 「鍵の移行期間」のデータ量増大に対応するために、

①「キャッシュ DNS サーバー」において、UDP 受信サイズを 4096 バイトの検索結果が受信できる設定（RFC6891 による推奨設定）を行う。

②「キャッシュ DNS サーバー」において、「dig コマンド」などを使い、4096 オクテットの検索結果が受信できるか確認する。

③不明点がある場合には、運用委託先や上位 ISP に問い合わせを行う。

詳細は、https://go.icann.org/KSKtest を参照。

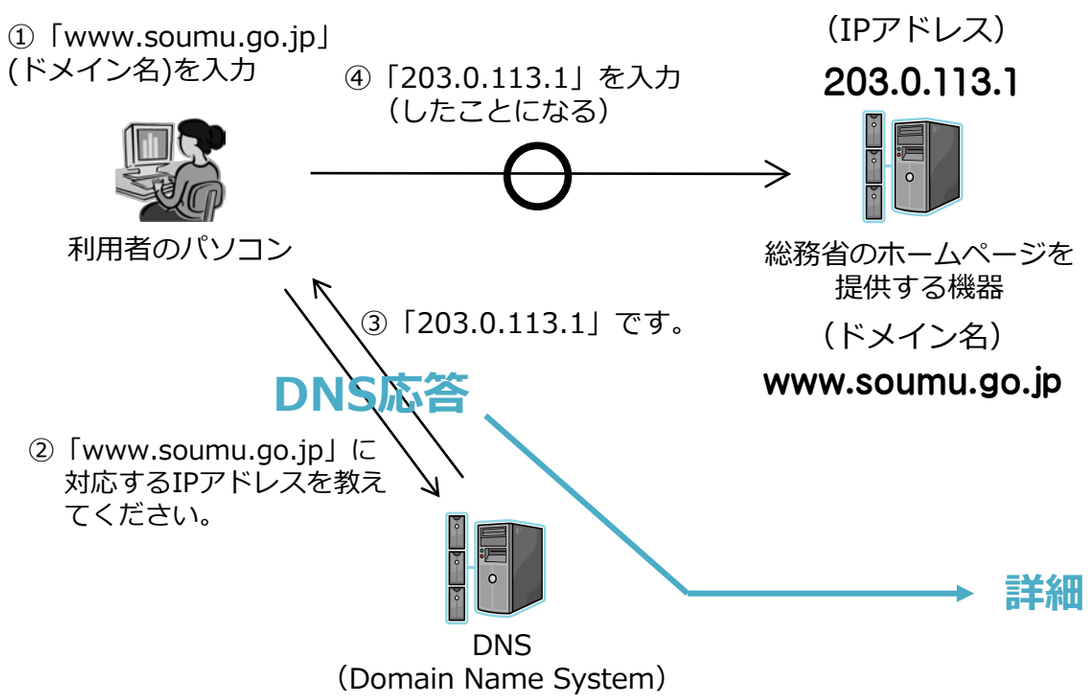
【連絡先】
総務省総合通信基盤局データ通信課
０３－５２５３－５８５３

DNS応答の仕組み

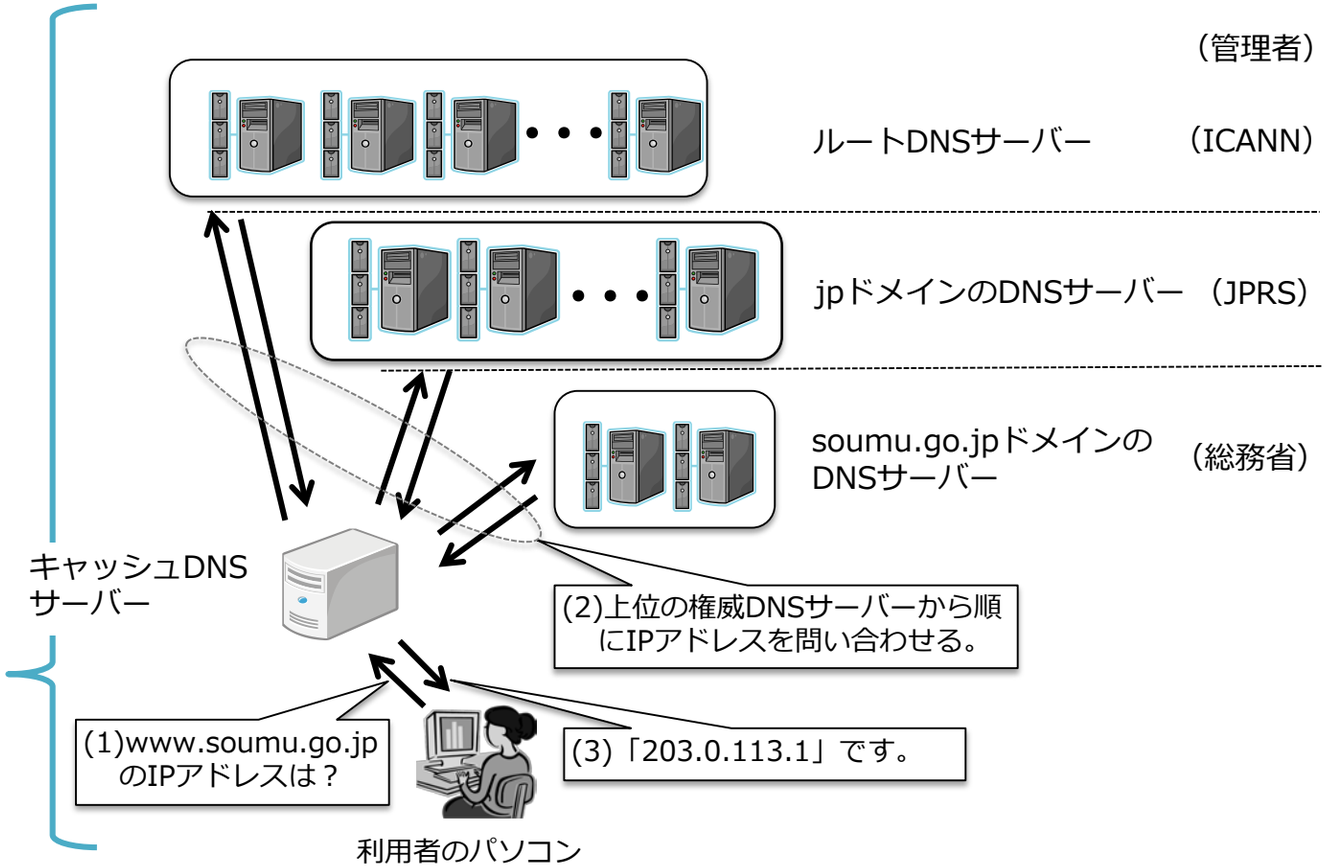
○　インターネット上の機器は、IPアドレスと呼ばれる番号で管理され、インターネット上の通信は、IPアドレスを宛先として行われる。 ホームページの閲覧やメールの送信をするためには、相手方の機器（サーバー）のIPアドレスを知っていることが必要。
○　IPアドレスは、例えば「203.0.113.1」など人には記憶・判別しにくいため、IPアドレスに対応したドメイン名（例：総務省のホームページの場合「www.soumu.go.jp」）が利用されている。
○　ドメイン名をインターネット上の宛先とするためには、対応する**IPアドレスに変換する仕組み（DNS: Domain Name System）**を利用。
○　DNSでは、ドメイン名の各階層の管理者が管理情報（ドメイン名とIPアドレスの対応関係等）を自身の権威DNSサーバーに保持。**インターネットの利用者は、ISPやLAN内のキャッシュDNSサーバーを通じて、上位階層の権威DNSサーバーから順にIPアドレスを問い合わせる**。

＜総務省のホームページを見る場合＞

IPアドレスとドメイン名の変換

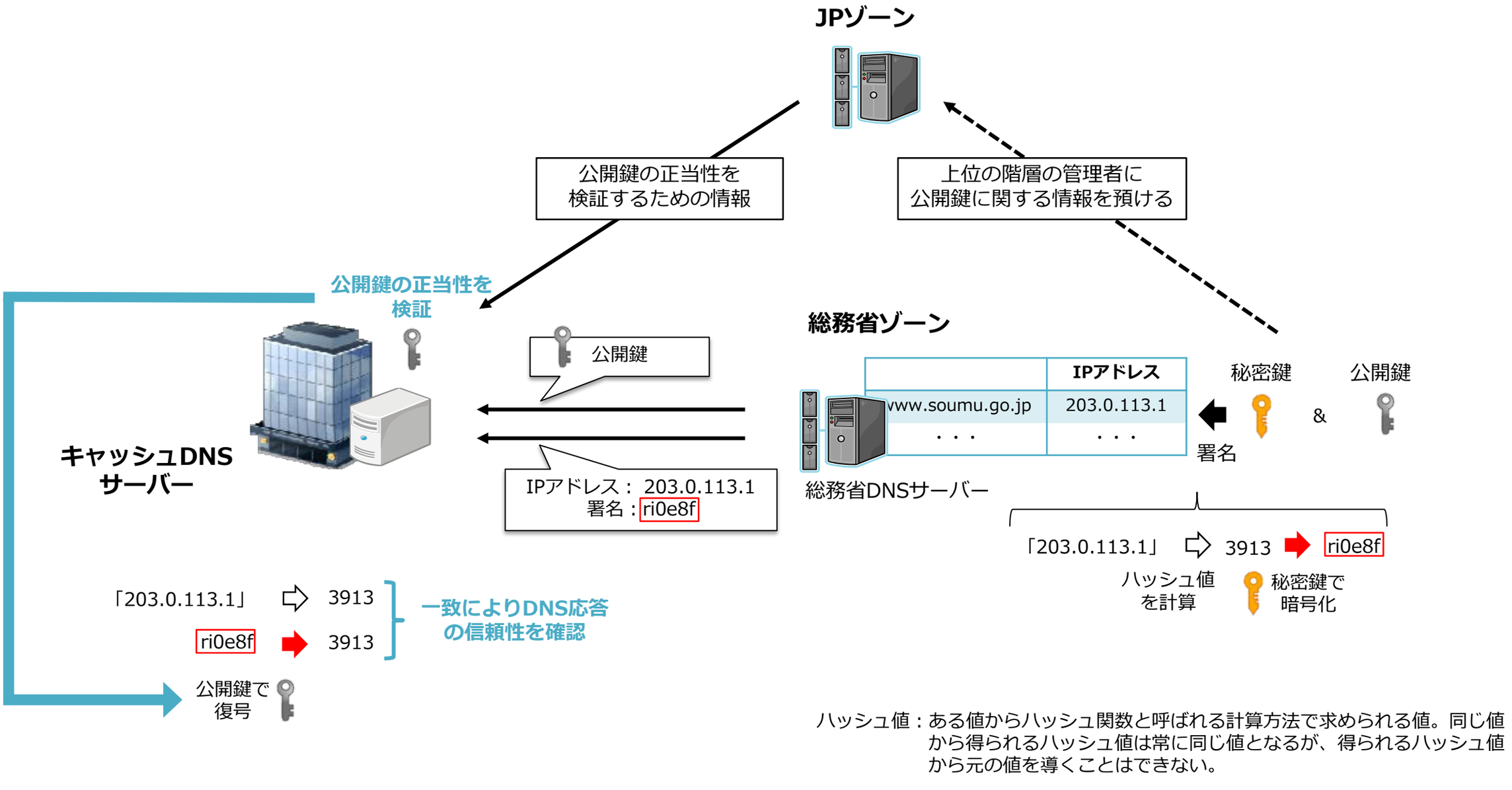


DNSの階層構造



DNSの正当性を担保する電子署名（DNSSEC）の仕組み（1/2）

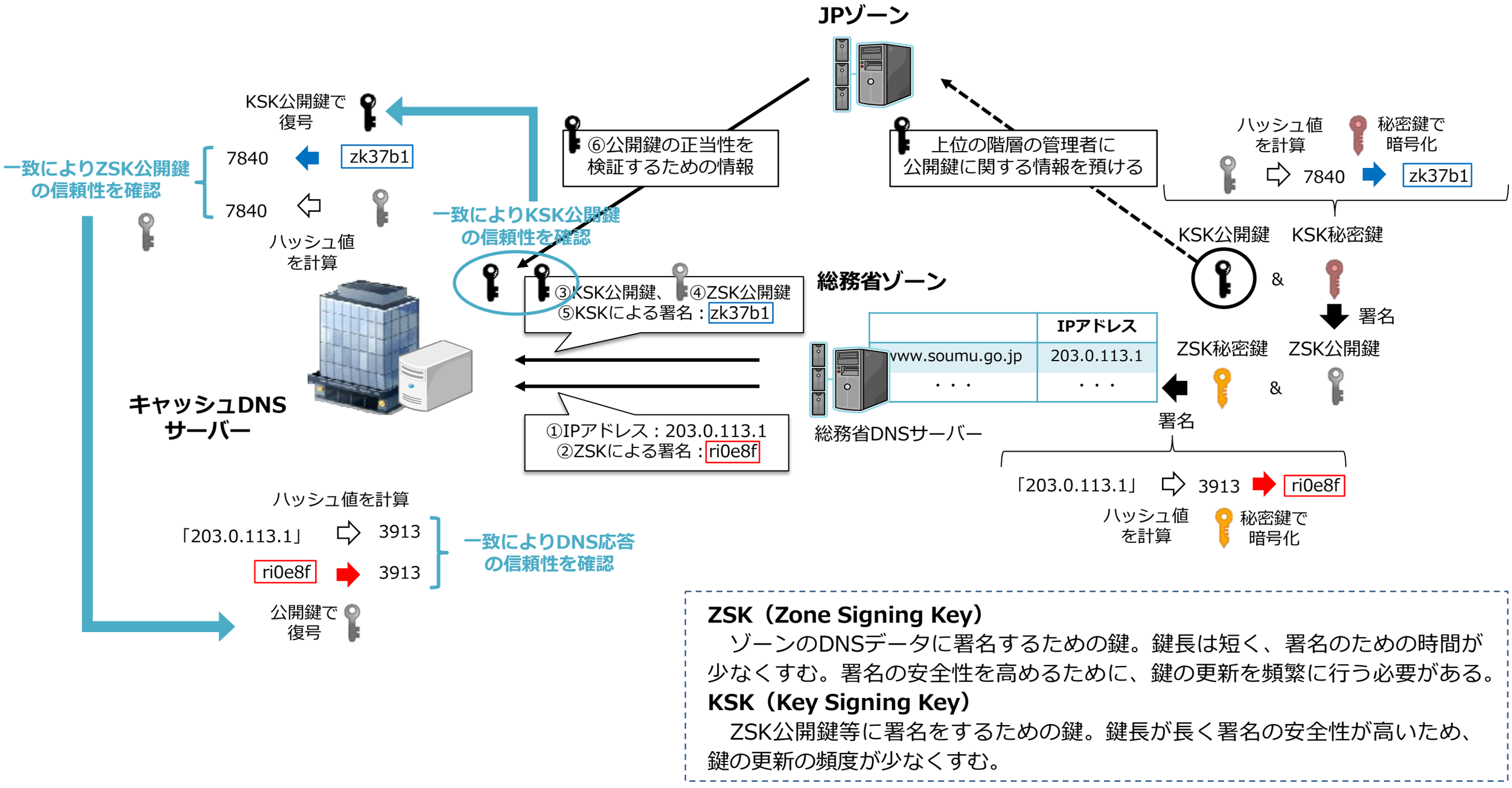
○　各階層の管理者は、自らのDNS応答の正当性を証明するために、秘密鍵と公開鍵を利用する。
○　まず、各階層の管理者は、問合せを受けたドメイン名に対応する**IPアドレスとともに、秘密鍵による署名を併せて送付**する。
○　回答を受けたキャッシュDNSサーバーの運用者は、**公開鍵により署名を復号し、IPアドレスの情報と一致することを確認**することで、回答が途中で改ざんされていないことを確認する。
○　以上に加えて、**各階層の管理者が、上位の階層の管理者に公開鍵に関する情報を預け、当該上位の階層の管理者が自らの署名を行いキャッシュDNSサーバーの運用者に提供する**ことで、公開鍵の正当性を検証することを可能としている。



ハッシュ値：ある値からハッシュ関数と呼ばれる計算方法で求められる値。同じ値から得られるハッシュ値は常に同じ値となるが、得られるハッシュ値から元の値を導くことはできない。

DNSの正当性を担保する電子署名（DNSSEC）の仕組み（2/2）

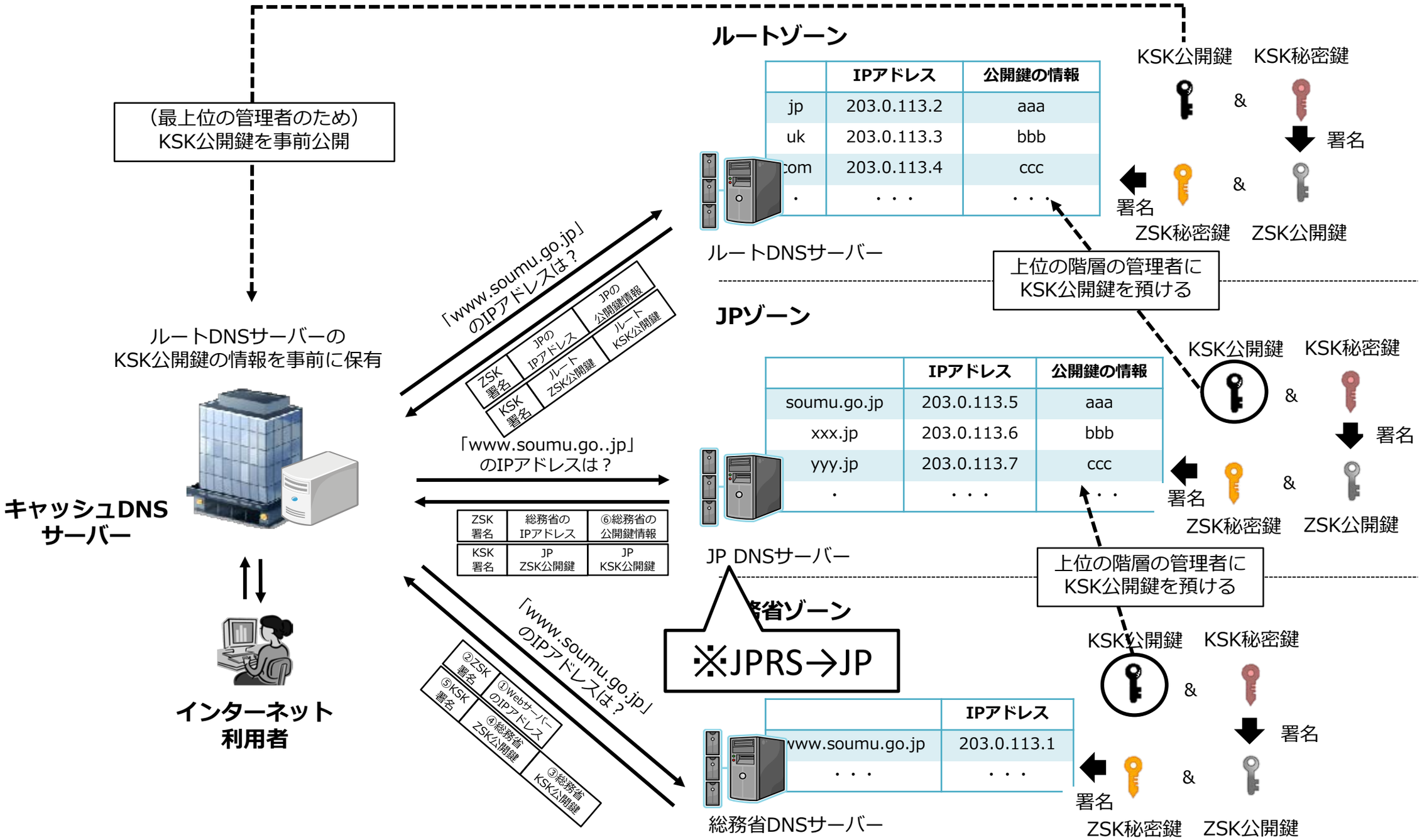
○　鍵の信頼性を確保するためには、鍵長を長くすることで解読されるリスクを小さくすること、鍵の定期的な更新を行うことが求められる。
○　しかし、前者については署名のための時間がかかる、後者については上位の階層の管理者が関与する仕組みからあまり頻繁な更新は難しいといった問題がある。
○　そこで、DNSSECにおいては、**DNSデータに署名をするZSK（Zone Signing Key）とZSKに署名をするKSK（Key Signing Key）という、性質の異なる２種類の鍵を併用**することで、問題を解決している。



ZSK（Zone Signing Key）
　ゾーンのDNSデータに署名するための鍵。鍵長は短く、署名のための時間が少なくすむ。署名の安全性を高めるために、鍵の更新を頻繁に行う必要がある。
KSK（Key Signing Key）
　ZSK公開鍵等に署名をするための鍵。鍵長が長く署名の安全性が高いため、鍵の更新の頻度が少なくすむ。

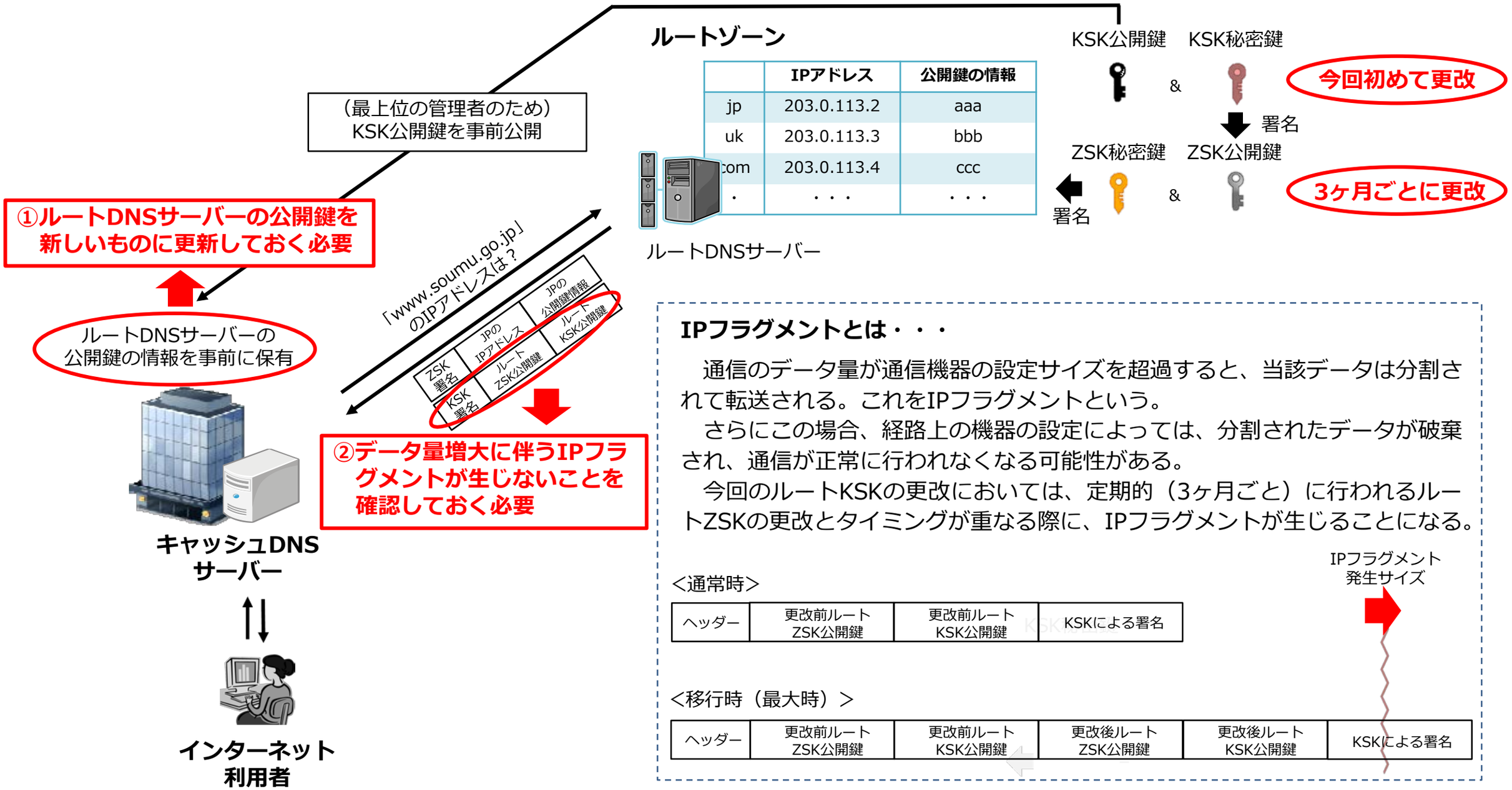
DNSSECを利用したDNS応答の流れ

○　各階層の管理者は、**あらかじめ自らのKSK公開鍵を上位の階層の管理者に預ける**。
○　各階層の管理者は、キャッシュDNSサーバーからの問合せに対し、自らの**ZSK秘密鍵による署名**及び下位階層の管理者の**IPアドレス及び当該下位階層の管理者のKSK公開鍵の情報**を応答する。
○　加えて、各階層の管理者は、自らの**KSK秘密鍵による署名**及び**ZSK公開鍵及びKSK公開鍵**を送付する。
○　応答を受け取ったISP等は、**あらかじめ上位階層の管理者から受け取っていたKSK公開鍵の情報により、問合せ先からの応答の正当性を確認**したうえで、次の問合せを行う。



ルートKSKの更改（ルートKSKロールオーバー）について

○　2010年のルートKSKの導入以来、初めての鍵の更改が本年7月～来年3月にかけて予定されている。
○　これに伴い、キャッシュDNSサーバーを保有するISP等は、**事前公開されているルートKSKの公開鍵の情報を更新する必要**がある。
○　また、ルートKSKの円滑な更改のために、**一時的に新旧両方のKSK公開鍵を送信する期間**がある。当該期間は、**送信されるデータ量が増大し、IPフラグメントが生じる**ことがある※。ISP等の事業者は、自らのDNSの応答に係る経路上の機器の設定が**IPフラグメントに対応可能か否かを事前に確認しておく必要**がある。
※　なお、ルートDNSサーバーは、応答相手のDNSSEC対応・非対応に関わらず公開鍵情報を送信してしまうため、**DNSSEC非対応の機器についてもIPフラグメントによる問題が生じる可能性がある。**



IPフラグメントとは・・・

通信のデータ量が通信機器の設定サイズを超過すると、当該データは分割されて転送される。これをIPフラグメントという。

さらにこの場合、経路上の機器の設定によっては、分割されたデータが破棄され、通信が正常に行われなくなる可能性がある。

今回のルートKSKの更改においては、定期的（3ヶ月ごと）に行われるルートZSKの更改とタイミングが重なる際に、IPフラグメントが生じることになる。

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。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25%（7億5,000万人）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。

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。DNSSECの導入についての詳細は、**こちら**をご覧ください。

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。**go.icann.org/KSKtest**.

必要な操作

新しいルートゾーンKSKは2017年2月に公開されており、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17日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。詳細については、**icann.org/kskroll**をご覧ください。

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、2017年3月以降、**ここから**入手できます。

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。

2017年 9月19日

ルートネームサーバーからのDNSKEY応答のサイズが増大。

2017年 10月11日

新しいKSKを初めて署名に使用。

2018年 1月11日

古いKSKを失効。

2018年 3月22日

古いKSKがルートゾーンに表示される最終日。

2018年 8月

古い鍵を、両方のICANNの鍵管理システムの機器から削除。

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、**icann.org/kskroll**をご覧ください。

「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。

Designed by ICANN Communications | 2017年3月

ICANN

Los Angeles Headquarters

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

+1 310 301 5800
+1 310 823 8649

16 June 2017

Suzuki Shigeki
Vice Minister for Policy Coordination
Ministry of Internal Affairs and Communications

Re: Upcoming changes to root zone DNS Security Extensions

Dear Mr. Shigeki,

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to help ensure a stable, secure and unified global Internet. ICANN helps coordinate and manage the highest level of the domain name system (DNS), called the root zone. The root zone plays a critical role in how the DNS converts domain names to Internet addresses worldwide. Without this seamless DNS resolution process, the Internet could not operate the way it does today.

I am writing regarding an upcoming change to an important security configuration parameter related to the root zone, which is scheduled to take place on 11 October 2017.

The root zone is digitally signed using a security protocol called DNS Security Extensions (DNSSEC), which adds a layer of trust on top of the DNS by providing a way to authenticate DNS data. DNSSEC enables network operators to protect their users from a form of malicious attack known as "cache poisoning," that could redirect their users' traffic to an incorrect website to, for example, steal passwords or financial information. DNSSEC deployment is optional and not all network operators have enabled it, but operators who have deployed it could be affected by the upcoming change.

The DNS is organized in a hierarchy and ICANN manages changes to the top-most level of the DNS. ICANN also manages the top-most cryptographic key in the DNSSEC protocol, known as the root zone key signing key, or KSK. On 11 October 2017, ICANN will change this key, in a process called a key rollover. This is the first time the key will be changed since DNSSEC was enabled in 2010.

This change must be widely and carefully coordinated with network operators that have enabled DNSSEC to ensure that the rollover does not interfere with normal operations. ICANN is informing you about the change now so you can notify Internet operators and user communities in your country before this change occurs.

It is important that every Internet service provider or network operator that has enabled DNSSEC validation in your country updates their systems with the new KSK. To help ensure a smooth transition, ICANN would appreciate if you could contact operators in your country and inquire if they are ready for the KSK rollover. If an operator fails to update systems with the new KSK, end users in your country could encounter errors when looking up any domain name and thus, be unable to access the Internet on 11 October 2017.

According to the data available to us and our partners in the Regional Internet Registries, we believe that recursive resolvers within the following networks may be performing DNSSEC validation in your country and could be affected by the KSK rollover.

Please note that the recursive resolvers performing validation may be owned by the network operator, by customers of the network operator, or both. The data just shows which recursive resolvers within the network are validating, but not who operates those recursive resolvers.

Autonomous System Number (ASN)	Network Operator

We encourage you to share ICANN's testing platform as an easy way for your operators to confirm their infrastructure supports the ability to handle the rollover without manual intervention. The testing platform can be found at https://go.icann.org/KSKtest.

An estimated 750 million people could be affected by the KSK rollover worldwide. It is critical that we coordinate our efforts to keep the Internet users in your country from experiencing difficulties with domain name lookups.

If you or your operators have any questions, you can contact my team by emailing globalsupport@icann.org with the subject line "KSK Rollover."

Thank you in advance for your support.

Göran Marby
President & CEO, ICANN

cc: ICANN Governmental Advisory Committee (GAC) Representatives from Japan
Kazuhiro Mita, Director, Computer Communications Division, Telecommunications Business Department, Telecommunication Bureau, Ministry of Internal Affairs and Communications
Shin Takamura, Director for Global ICT Strategy, Computer Communications Division, Telecommunications Business Department, Telecommunication Bureau, Ministry of Internal Affairs and Communications