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。

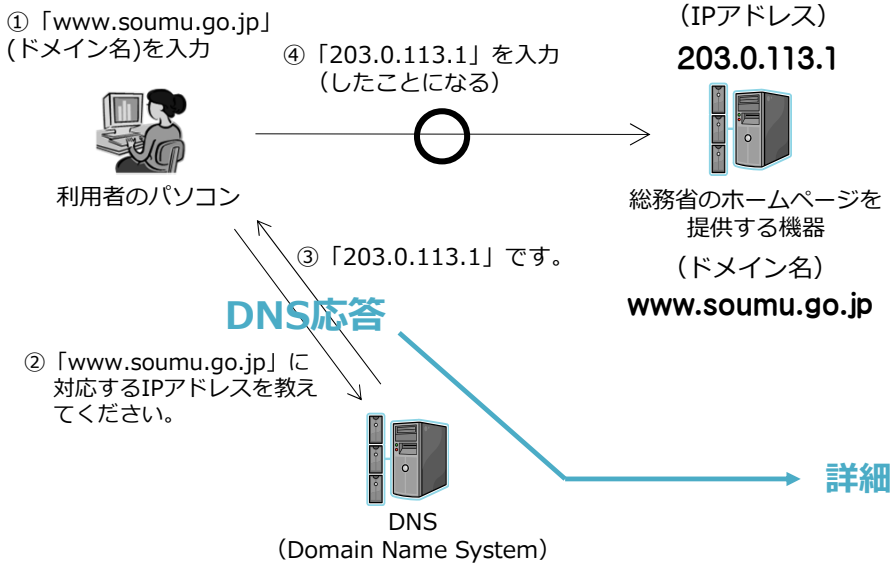
○　IPアドレスは、例えば「203.0.113.1」など人には記憶・判別しにくいため、IPアドレスに対応したドメイン名（例：総務省のホームページの場合「www.soumu.go.jp」）が利用されている。

○　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。

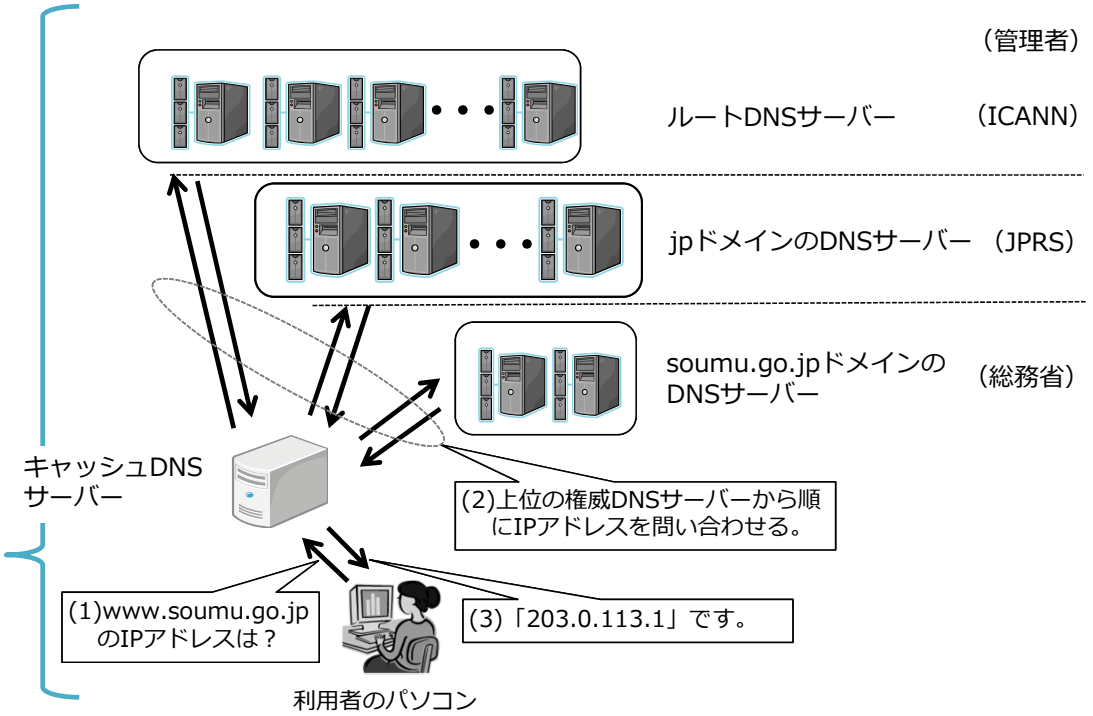
○　DNSでは、ドメイン名の各階層の管理者が管理情報（ドメイン名とIPアドレスの対応関係等）を自身の権威DNSサーバーに保持。**インターネットの利用者は、ISPやLAN内のキャッシュDNSサーバーを通じて、上位階層の権威DNSサーバーから順にIPアドレスを問い合わせる**。

＜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

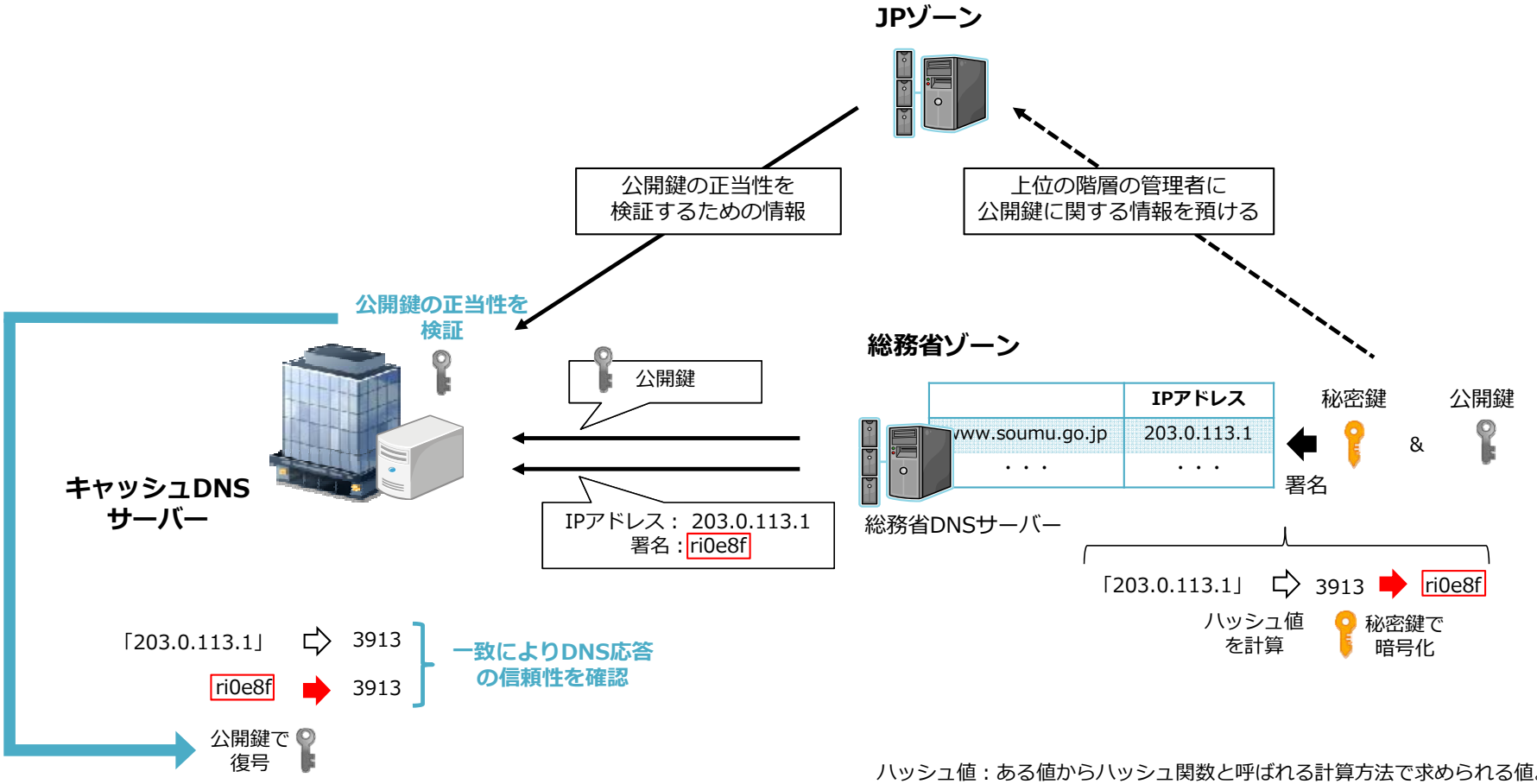


DNSの階層構造



DNSの正当性を担保する電子署名（DNSSEC）の仕組み（1/2）

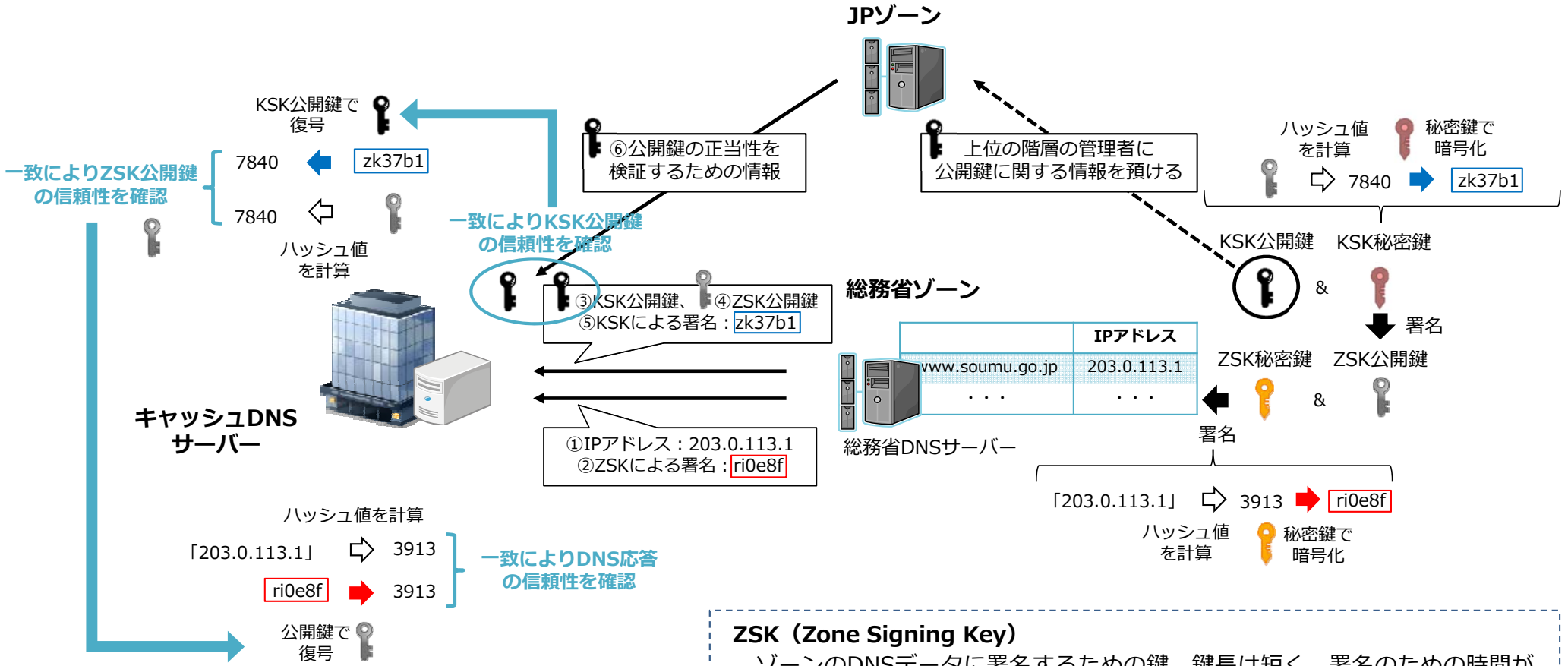
○　各階層の管理者は、自らのDNS応答の正当性を証明するために、秘密鍵と公開鍵を利用する。
○　まず、各階層の管理者は、問合せを受けたドメイン名に対応する**IPアドレスとともに、秘密鍵による署名を併せて送付**する。
○　回答を受けたキャッシュDNSサーバーの運用者は、**公開鍵により署名を復号し、IPアドレスの情報と一致することを確認**することで、回答が途中で改ざんされていないことを確認する。
○　以上に加えて、**各階層の管理者が、上位の階層の管理者に公開鍵に関する情報を預け、当該上位の階層の管理者が自らの署名を行いキャッシュDNSサーバーの運用者に提供する**ことで、公開鍵の正当性を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

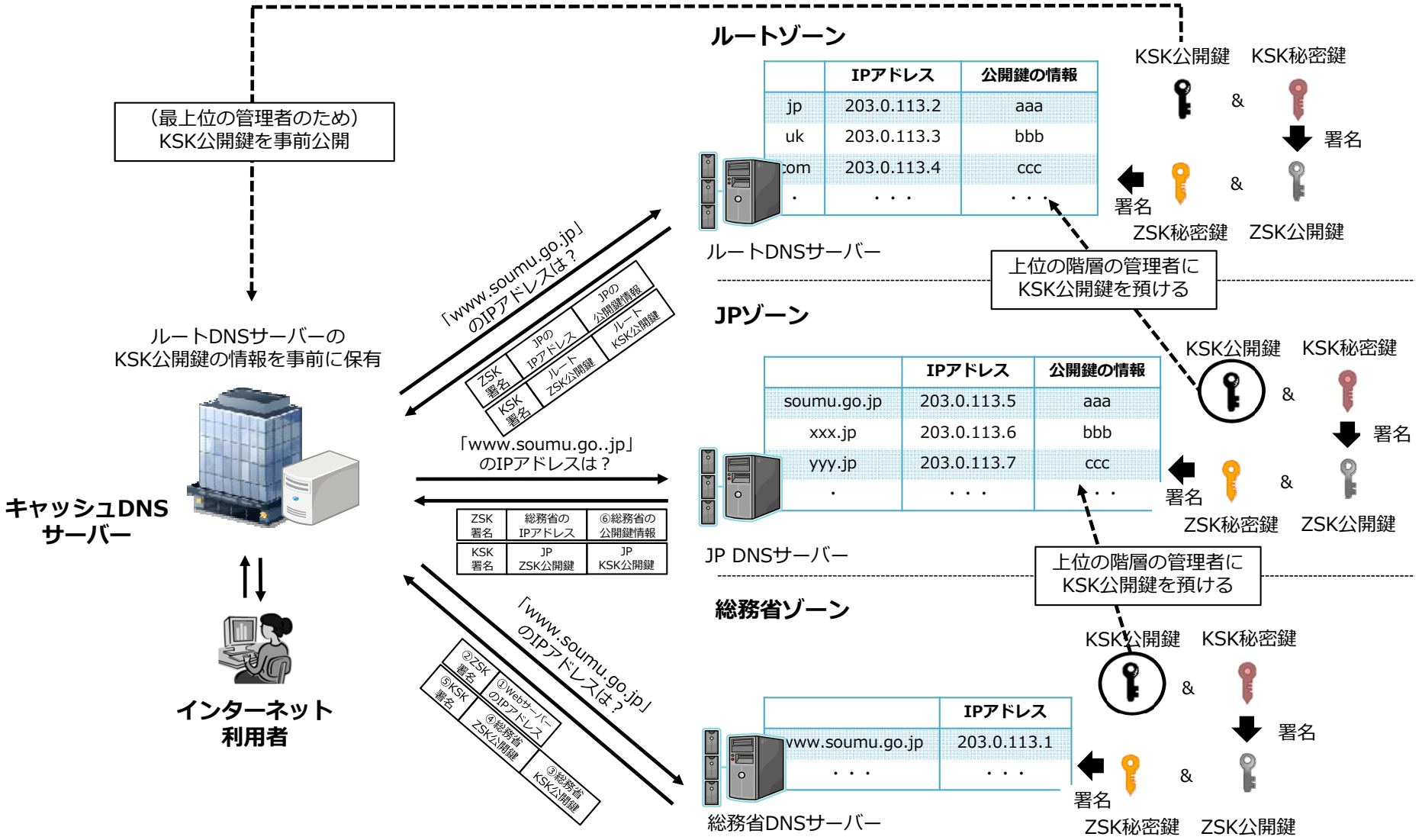
○　鍵の信頼性を確保するためには、鍵長を長くすることで解読されるリスクを小さくすること、鍵の定期的な更新を行うことが求められる。
○　しかし、前者については署名のための時間がかかる、後者については上位の階層の管理者が関与する仕組みからあまり頻繁な更新は難しいといった問題がある。
○　そこで、DNSSECにおいては、**DNSデータに署名をするZSK（Zone Signing Key）とZSKに署名をするKSK（Key Signing Key）という、性質の異なる２種類の鍵を併用**することで、問題を解決している。



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。

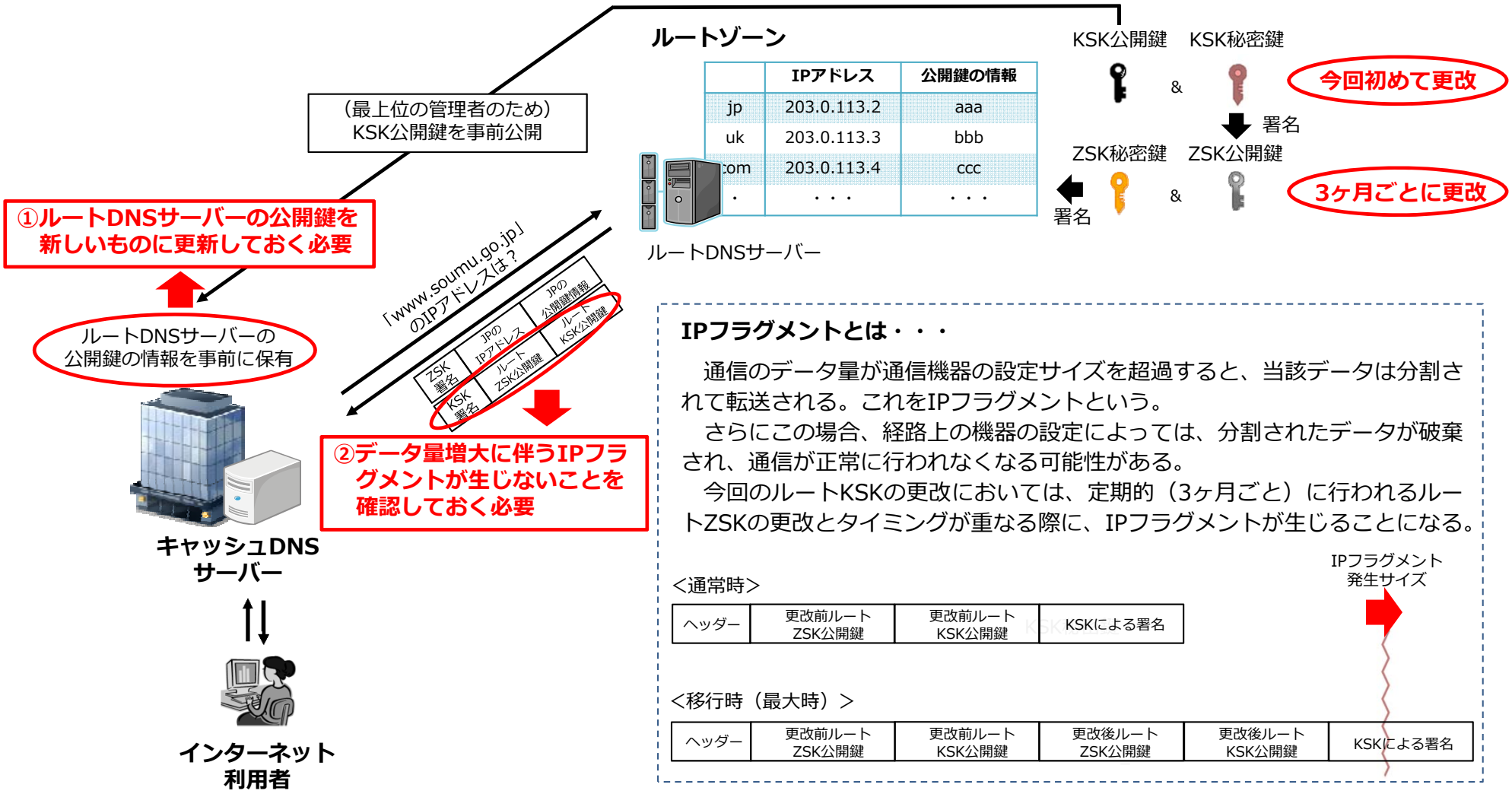
DNSSECを利用したDNS応答の流れ

○　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。