---------- 今回のご依頼の詳細 ----------

【改変の目的】

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」の仕組みです。

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す。

DENSEC においては、鍵の危殆化を防ぐため、署名に用いる電子鍵を定期的に改変しています。

鍵は、ドメインの管理単位であるゾーンに署名するゾーン署名鍵"ZSK"と ZSK に署名する鍵署名鍵である"KSK"があり、それぞれ、ZSK は 3 ヶ月ごと、KSK は 5 年ごとに改変されることとなっています。

この度は、DENSEC の運用開始後初めての KSK の更新作業が行われることとなり、本年 7 月～来年 3 月にかけて実施されます。

【鍵の改変に伴い生じる可能性のあるトラブル】

(1) 検索結果の正当性が確認できなくなり、利用者のネット利用に不具合が生じる「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ります。

(2) 検索結果の受信データ量が増大することから、利用者のネット利用に不具合が生じる可能性がある

「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。

【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※DENSEC を無効にしている方も、上記(2)については影響を受ける可能性がございますので、必ずご確認ください。

【必要となる対応】

2017 年 9 月 19 日までに以下の措置をお願いいたします。

(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 WindowsServer 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。

※(2)②の確認については、以下のような確認方法がございます。

<使用している DNS サーバーが 4096 オクテットの検索結果を受信できるか確認例>

・WEB での確認例 http://keysizetest.verisignlabs.com/

・コマンドラインでの確認例 dig +bufsize=4096 +short rs.dns-oarc.net txt

なお、詳細につきましては、別添および以下の WEB サイトも併せてご確認いただきますよう、お願いいたします。

【JPRS】ルートゾーン KSK ロールオーバーによる影響とその確認方法について

・https://jprs.jp/tech/notice/2017-07-10-root-zone-ksk-rollover.html

【ICANN】Root Zone KSK Rollover

・https://www.icann.org/resources/pages/ksk-rollover