「ＤＮＳ（ドメインネームシステム）における電子署名鍵の変更について」
（経済産業省からの周知依頼・注意喚起）

この度、内閣サイバーセキュリティセンター（NISC）より、「DNS（ドメインネーム・システム)」について、経済産業省を通して、下記を会員各位等に周知・注意喚起する様、依頼が有りましたので、お知らせ致します。

記

以下、内閣サイバーセキュリティセンター（NISC）よりのお知らせ（本文のまま）

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 が、DNS（ドメインネームシステム）を安全に利用するための仕組みである DNSSEC において、電子署名の正当性を確認するために使う鍵の中で最上位となる鍵「ルートゾーン KSK」を更新することを発表しました。

この更新は信頼性維持のために行われるものであり、本年 9 月から新旧の鍵の併用が開始されます。

当該更改作業は DNSSEC の利用有無にかかわらず、全てのキャッシュ DNS サーバが影響受ける可能性があり、このキャッシュ DNS サーバの運用者においては、本年 9 月 19 日までに必要な処置が講じられない場合、ウェブアクセスやメール送信などが出来ない利用者が生じる可能性があります。

キャッシュ DNS サーバの運用者には、インターネットサービスプロバイダ、官庁、独法、学校、企業等、幅広い方々が含まれますところ、以下のとおりご対応いただきますよう、周知・注意喚起いただきたく、お願い申し上げます。

---------- 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」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。

以上