2010年5月12日
第32回JPドメイン名諮問委員会
参考資料１

JPRS-ADV-2009001
2009年9月7日

JPドメイン名諮問委員会
委員長 後藤 滋樹 殿

株式会社日本レジストリサービス
代表取締役社長 東田 幸樹

諮 問 書

下記の事項について、諮問いたします。

記

1. 諮問事項

DNSセキュリティ拡張方式(DNSSEC)の導入に関して

2. 諮問理由

DNSはインターネットの根幹を支える重要な仕組みであり、インターネットが社会活動の基盤として重要性を増す中、ますますDNSの運用の安定性が求められています。これに加えて、近年、DNS応答の偽造により引き起こされるセキュリティ上の脅威が増大していることから、安心して利用できるDNSであり、ひいては、安心して利用できるインターネットに資するために、このような脅威を排除することも強く求められるようになってきました。

DNS応答の偽造により引き起こされるセキュリティ上の脅威の例としては、偽のDNS情報によるフィッシングサイトへの誘導や電子メールの盗聴などが挙げられ、これらは一般のインターネット利用者が被害に遭う危険性が高いものとなります。

DNS応答に関するセキュリティの向上については、インターネットに関する技術標準を策定するIETFにおいて検討が進められ、DNSセキュリティ拡張方式(DNSSEC)が策定されています。DNSSECは、DNSの応答に公開鍵暗号方式による署名を付加すること

で、DNSの応答を受け取った側がその応答内容が正しいかどうかを検証できる仕組みです。現在、各TLDレジストリにてDNSSECの運用もしくは実験が始まりつつあり、JPRSにおいても、JPドメイン名登録管理サービスおよびJP DNSへDNSSECを導入する方向で検討を進めています。

DNSSECは、上記のように、DNS提供側の署名と利用側の検証という双方がDNSSECに対応することで、応答の正しさを検証する仕組みです。したがって、DNSSECの普及のためには、ドメイン名登録者、レジストリ、指定事業者、DNSサービス提供者、インターネット利用者など、DNSの提供と利用に関わる多くの関係者がそれぞれの立場でDNSSECへの対応を進めていく必要があります。また、それぞれの役割の定義、サービス導入の簡便さの追求、全体的低コストの実現など、多面的に解決せねばならない点が多く存在します。

上記のような観点から、DNSSECの導入およびサービスの具体化を行う上で考慮すべき事項に関してご答申いただきたく、お願い申し上げます。

以上