JPドメイン名サービスへのDNSSECの導入予定について

2009/07/09 公開

▼はじめに

JPRSでは、DNSのセキュリティ拡張方式であるDNSSEC[*1]を、2010年中を目処にJPドメイン名サービスへ導入する予定で準備を進めています。

この文書では、DNSSEC導入の背景と、今後JPRSが予定しているDNSSEC導入関連の活動について説明します。

*1 DNSSEC: DNS Security Extensions

▼DNSSEC導入の背景

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基盤として重要性を増す中で、その安定的な運用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現実のものとなり、このような脅威を排除し、安心して利用できるDNSであることも強く求められるようになってきました。

DNSに関するセキュリティの向上については、IETF[*2]において検討が進められ、DNSSECというDNSのセキュリティ拡張方式が策定されました。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、応答を受け取った側が正しい内容であるかどうかを検証できる仕組みです。

JPRSでは、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に対して、DNSSECの導入が現時点で最も実現性が高く、有効な解決策であると考えています。この考え方のもと、JPRSではこれまでに、大規模ゾーンに対するDNSSEC導入技法の研究開発などを行うとともに、日本国内はもとより、世界各国のDNS運用関係者とともにDNSSECの運用技術や、普及に向けたロードマップの検討なども行ってきました。今後は、JPドメイン名サービスへDNSSECを導入するための仕様検討と試験を進めていきます。

*2 IETF: Internet Engineering Task Force

▼DNSSECの導入・普及に向けた関連活動

DNSSECは、DNSを提供する側と利用する側の双方が対応することで、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、多くのDNS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。

JPRSでは、JPRS自身が提供するJPドメイン名サービスとJP DNSでのDNSSEC対応を進めることはもちろん、以下のようなさまざまな立場のDNS関係者に向けた情報提供や普及促進活動を併せて行っていく予定です。

権威DNSサーバ運用者

DNSはルートから連なる階層構造で形作られたシステムであるため、その最上位階層であるルートDNSサーバから、TLDレベルのDNSサーバ、個々のドメイン名のDNSサーバまで、全ての階層においてDNSSECを導入することが求められます。

- ルートDNS運用者

  DNSSECの円滑な運用のためには、DNSの最上位階層であるルートDNSサーバへのDNSSECの導入が必須となります。ICANN[*3]/IANA[*4]においてもDNSSECの導入に向けた検討が進められていますが、JPRSは他のTLDレジストリと協調し、早期の導入に向けた支援を継続していきます。

  *3 ICANN: Internet Corporation for Assigned Names and Numbers
  *4 IANA: Internet Assigned Numbers Authority

- 他のTLDレジストリ

  DNSの利用は、国境やTLDに閉じたものではありません。インターネット全体にDNSSECが普及しDNSの安全性が高まるよう、JPRSは他国のレジストリやコミュニティと連携、経験の共有など情報交換を積極的に行っていきます。

- 日本国内のそれぞれのドメイン名のDNSサーバ運用者

  DNSSECは、それぞれのドメイン名のDNSサーバで、DNS情報への署名や、署名に用いる鍵情報の登録手続きなどが必要になります。
  JPRSは、DNSSECの運用に関する情報提供などを、セミナーやメディアを通して積極的に展開していきます。

キャッシュDNSサーバ運用者

DNSSECにおけるDNS応答の検証は、ISPや企業・大学などが運用するキャッシュDNSサーバが担うことになります。インターネット利用者がDNSSECで安心してDNSを利用できるようになるためには、キャッシュDNSサーバでのDNSSEC対応は重要です。
JPRSは、国内のISPとの連携を深めるとともに、DNSSECの運用に関する情報提供などを、セミナーやメディアを通して積極的に展開していきます。

JPドメイン名指定事業者

JPドメイン名の登録者がJPRSが提供するDNSSECサービスを利用するためには、JPドメイン名指定事業者のサービスがDNSSECに対応する必要があります。
JPRSは、指定事業者と協力し、DNSSECのサービス利用環境の整備を促進していきます。

インターネット利用者

一般のインターネット利用者は、プロバイダなどのキャッシュDNSサーバがDNSSECの検証を行うために、特に対応を必要としません。しかし、DNSSECの必要性を理解し、自分がDNSSECを利用している環境にあるかどうかを知っていることは大切です。
その意味からも、JPRSでは一般利用者に向けたDNSSECのわかりやすい解説などを行っていきます。

▼おわりに

DNSSECは、DNSの応答の正しさを検証可能にする技術です。これはインターネットのセキュリティ向上技術の一部であり、DNSSECを使うことであらゆる脅威を排除できるというものではありません。しかし、インターネットのセキュリティ向上とは、このような要素技術をいくつも組み合わせることで達成される大きな目標です。

JPRSでは、今後もDNSSECの普及に向けた活動を進めていきます。インターネットのセキュリティ向上のために、ドメイン名・DNSに関わる多くの皆様のご協力をよろしくお願いいたします。
