JPRS-ADVRPT-2009001
2010 年 3 月 29 日

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 殿

JP ドメイン名諮問委員会
委員長 後藤 滋樹

答申書

DNS セキュリティ拡張方式(DNSSEC)の導入に関しての諮問書(JPRS-ADV-2009001)に答申いたします。

主 文

DNS セキュリティ拡張方式(DNSSEC)は、ドメイン名利用におけるセキュリティの向上にとって重要であるため、JP ドメイン名に対しても適時にサービス導入すべきである。

DNSSEC の導入およびサービスの具体化を行う上では、以下の事項について考慮するのが望ましい。

1. 技術の実用度について

DNSSEC は、技術プロトコルは実用レベルに達しているとされているが、まだ運用実績がほとんどない技術である。このため、適切に DNSSEC を使用できるようにする観点から、導入コストの検討、および、十分な技術面および運用性の検証を経てからサービス導入すべきである。

2. サービス導入ステップについて

DNSSEC の利用には、ドメイン名登録者やインターネット利用者、レジストリ、指定事業者、DNS プロバイダー、ISP、各種機器メーカーなどの多様なプレイヤーが関わることになるため、全プレイヤーがそれぞれの役割を理解し、DNSSEC の効果を享受するのは難しい。このため、導入に当たって

は、まずは、セキュリティに対する意識の高いドメイン名登録者とその利用者がDNSSECを使うことができるように導入を進めるべきである。

3. 情報提供について

DNSSEC の効果を広く一般に行きわたらせるには、十分な情報提供が必要である。レジストリであるJPRSも情報提供において主導的役割の一端を担うことが望まれる。

4. 利用環境の充実について

ドメイン名登録者がDNSSECを簡単に利用できるように、また、インターネット利用者が DNSSEC の効果をより広く享受できるように、より DNSSEC を導入しやすい環境づくりに努めるべきである。

5. 責任分界について

DNSSEC のサービス提供および利用にあたっては、多様なプレイヤーが連携することになるので、DNSSECは何を保証するものなのか具体化した上で、諸外国のレジストリとも協力しつつ、各プレイヤーの役割と責任範囲を明確化することが重要である。

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の安全性が求められている。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インターネットに資するため、ひいてはインターネット上での活動をより安全なものにするために、DNSのセキュリティを向上させることが重要である。

DNSセキュリティ拡張方式(DNSSEC)は、DNS応答が偽造された場合それを検出することができる技術であり、DNSのセキュリティ向上策として、世界的に有望視されている。これは、DNS のセキュリティ向上にとって重要であるため、JP

ドメイン名に対しても適時にサービス導入すべきである。

DNSSEC の導入およびサービスの具体化を行う上では、以下の事項について考慮するのが望ましい。

1. 技術の実用度について

DNSSEC は、DNS の応答偽造に対抗するにあたり、技術的には有効な解決策である。DNSSEC は、技術プロトコルは完成しているが、その利用に当たっては、ICANN、レジストリ、指定事業者、DNS プロバイダー、ISP、各種機器メーカーなどが連携する必要があるにもかかわらず、実サービスとしての利用実績がほとんどない技術であるため、以下のような課題がある。

- インターネット上で使われる種々の機器が DNSSEC にどう対応しているかが十分にわかっていない。
- DNSSEC の利用により増加する処理量・通信量に対応して、サーバやネットワークの増強が必要となる可能性があるが、その増強の必要度合いが十分にわかっていない。

そのため、DNSSEC の導入にあたっては、十分な技術面および運用性の検証を経るべきである。

技術検証に際しては、他レジストリや指定事業者、DNS プロバイダー、ISP、各種機器メーカーなどとも連携し、検証精度を上げるとともに、協力関係を確立することが重要である。また、サーバやネットワークの増強の必要度合いや各プレイヤーが負担すべきコストなどに関しても、技術検証の中で明確化することが必要である。

2. サービス導入ステップについて

DNSSEC は、「署名鍵および署名付き情報の DNS への登録(登録フェーズ)」と「DNS から取得する情報に付された署名の検証(検証フェーズ)」という 2 つの処理を必要とするが、この両処理に関わる全プレイヤーがそれぞれの役割を適切に理解し、DNSSEC の効果を享受するのは難しいという課題がある。

このうち、登録フェーズについては、ドメイン名登録者とレジストリ、指定事業者、DNS プロバイダーなど、比較的処理に関わる者が少ない。また、銀

行やオンラインショッピング等のドメイン名登録者は、自分の Web サイトを安全にすることに対する動機が強いため、DNSSEC に関する理解を得られやすい。セキュリティは一般的に動機付けが難しい分野であるが、このような一般より強いセキュリティを必要とするドメイン名登録者が、多少障壁が高くても安全性を重視して DNSSEC を使う必要性を感じることが考えられるため、登録フェーズに関わるドメイン名登録者や指定事業者、DNS プロバイダーなどが DNSSEC の署名鍵および署名付き情報を登録することが可能となる状態を作ることが重要である。

一方、検証フェーズについては、インターネット利用者や小規模 ISP など、処理に関わる者の数が多く、また、ドメイン名に関する知識や対応能力の幅も大きい。そのため、関わる者の数や質の多彩さを考慮に入れつつ、広く調整・検討し、一般に受け入れられるように進める必要がある。

以上より、まず、登録フェーズの環境を準備し、問題意識が高いドメイン名登録者とその利用者から順次 DNSSEC を使えるような状況を、JPRS として徐々に作り出していくことが望ましい。また、検証フェーズに関わる ISP などは顧客の要望に応じて徐々に対応が進むことになると思われる。それによって、DNSSEC の効果が世に示され、ポジティブなスパイラルが描かれることを目指すのがよい。

3. 情報提供について

ドメイン名や DNS のセキュリティを向上させるために DNSSEC を導入することは重要であるが、世界的にはサービスもしくは実験が始まりつつある段階であり、DNSSEC の認知は低い状況にある。

サービス提供に関わる関係各所、ドメイン名登録者、インターネット利用者などに DNSSEC を正しく理解してもらい、DNSSEC により何がどう安全になるかを把握した上で、正しく使ってもらうことが大切であるが、現状では DNSSEC についてのよい解説書が少なく、その理解は難しい。特にインターネット利用者にとっては、DNS や DNSSEC は直接意識するサービスではないため、DNSSEC の原理などを理解することは難しいという課題がある。

そのため、DNSSEC の普及にあたっては、煽ることなく、サービス提供に関わる関係各所やドメイン名登録者、インターネット利用者などに対し、適切

な情報提供を行うことが重要である。レジストリである JPRS が DNSSEC を最もよく理解しているプレイヤーの一つであるため、関連団体等と協力して、また、世界のコミュニティと協調して、わかりやすく説明することが大切である。

そのためにも、まずは DNSSEC の基盤となる DNS 運用に携わる者が協力し、サービス環境を整えるとともに、ドメイン名登録者やインターネット利用者の DNSSEC に対する理解を促進する場を作ることが重要であると考える。

また、ISP などから見ると、DNSSEC への対応時期が IPv6 への対応時期と重なるため、両方に対応するための適切な情報も必要になると考えられる。これについても関連団体などと協力し、適切な情報提供を行うことが望ましい。

4. 利用環境の充実について

DNSSEC は、各プレイヤー(特に、ドメイン名登録者やインターネット利用者)にとって、その原理の理解が難しい技術である。また、DNSSEC の原理を理解しても、実際に自分で操作するとなると、さらに難しい技術である。そのため、ドメイン名登録者やインターネット利用者が、ISP を変更するなどの例外的な処理も含め、DNSSEC の効果を十分に享受することは難しい状況にある。

将来的には、ドメイン名登録者からインターネット利用者に渡るまで、DNSSEC を使いたい人が使いたいときに簡便に使える環境が必要である。その環境構築に向かうため、登録や検証が簡易にかつ安全に出来る環境の構築について、サービス提供に関わる関係各所と相談しつつ、DNSSEC 利用のための基本的な仕組みを各プレイヤーに提供することも含め、JPRS が主導的役割を果たすことも考えるべきである。

5. 責任分界について

DNSSEC は、セキュリティに関して一定の機能をインターネット利用者に提供するサービスである。これは JPRS が単独で提供できるサービスではなく、提供にあたっては、ICANN、指定事業者、DNS プロバイダーなど、多様な組織との連携が必要となる。さらに、DNSSEC は既存サービスに重ねて提供されるサービスであるため、運用時に発生する問題の原因切り分けも難しい。

このような点を考慮した上で、サービス利用上の問題が発生する場合も想定し、DNSSEC に関わる各プレイヤーの責任分界および責任の範囲を明確にしておく必要がある。責任範囲の明確化にあたっては、多様なプレイヤー間での合意が必要であるため、DNSSEC のサービス提供に関わる者が連携し、その連携の中から、ドメイン名登録者およびインターネット利用者に対し、「DNSSEC とは何を保証するものなのか」を発信することが望ましい。なお、その推進に当たっては、DNSSEC サービス提供に関わる連携は日本国内に限定されないため、先行事例も参考にしつつ、諸外国のレジストリとも協力すべきである。

以上