2009年12月11日
第30回JPドメイン名諮問委員会
資料２

答申骨子(案)
DNS セキュリティ拡張方式(DNSSEC)の導入に関して

〈総論〉

- DNS のセキュリティは、インターネット、ひいてはインターネット上での人間の活動にとって重要である。

- 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の１つとして、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 は、技術プロトコルは完成しているが、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こと等の観点から、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。

- DNSSEC は、特にインターネット利用者にとっては原理が難解であり、また、その利用には関わるプレイヤーが多い。このため、導入に当たっては、一挙に全プレイヤーを狙わず、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が DNSSEC の恩恵をこうむることができるように進めるべきである。それによって、DNSSEC の恩恵が世に示され、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。

- DNSSEC の恩恵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。

- さらに、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 の恩恵により広くあずかれるように、よりよい環境づくりに努めるべきである。

- 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、各プレイヤーの役割と保証範囲(責任範囲)を明確化することが重要である。

〈技術の実用度について〉

- DNSSEC は、技術的には DNS の応答偽造に対して有効な解決策であるが、運用実績が少ないという課題がある。

- そのため、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、ISP、各種機器メーカー等とも連携し、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、DNS の負荷増大により、機材・回線等の増強が必要になることも考えられることから、各プレイヤーが負担すべきコストに関しても、技術検証の中で明確化することが必要である。

〈サービス導入ステップについて〉

- DNS を利用するには、「DNS への情報登録」と「DNS からの情報取得」という 2 つの処理がある。

- DNSSEC においても同様に、「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 から取得される情報に付された署名の検証(検証フェーズ)」という 2 つの処理がある。

- この両処理は、タイミングや関わるプレイヤーが異なり、全体として、多様なプレイヤーが関わる。

- よって、一挙に全プレイヤーがそれぞれの役割を理解し、DNSSEC の効能を全面享受するのは敷居が高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 プロバイダが関わる処理となる。

- 登録フェーズに関わる者は、その数が比較的少なく、また、理解を得られやすい。

- 特に、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。

- 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、このような問題意識が高い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 プロバイダ等が 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、検証フェーズは、インターネット利用者や小規模 ISP などもが関わり、その数が多く、また、ドメイン名に関する知識や対応能力の幅も大きい。

- このため、検証フェーズについては、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から順次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。

〈情報提供について〉

- ドメイン名、DNS のセキュリティは、重要であるが、まだ各国でサービスもしくは実験が始まりつつある段階であり、その認知は低い。

- 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に DNSSEC を正しく理解してもらい、適切な期待の下、正しく使ってもらうことが大切であるが、よい解説書もなく、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、理解が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等に対し、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、判りやすく説明することが大切である。

- まずは、DNSSEC の基盤となる DNS 運用者が協力する場を作ることが重要であると考える。

- また、ISP 等から見ると、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等と協力し、適切な情報提供を行うことが望ましい。

〈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。

- 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。

- 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 の恩恵を十分に受け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、レジストリが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、)主導的役割を果たすことも考えるべきである。

〈責任分界について〉

- DNSSEC は、セキュリティに関し、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。

- DNSSEC は、JPRS が単独で提供できるサービスではなく、その提供にあたっては、ICANN、指定事業者、DNS プロバイダ等、多様な組織との連携が必要である。

- 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 に関わるプレイヤー間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。

- DNSSEC とは何を保証するものなのかについて具体化し、その中で、各プレイヤーの役割と保証範囲(責任範囲)を明確化することが重要である。

- 上記にあたっては、多様なプレイヤー間での合意が必要であるため、DNSSEC 機能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」を発信できることが望ましい。

以上