2009年9月7日
第29回JPドメイン名諮問委員会
資料6

DNSSECの導入における課題

2009年9月7日

株式会社日本レジストリサービス

1. 技術の実用度について
2. サービス導入ステップについて
3. 教育普及について
4. 利用環境の充実について
5. 責任分界について

課題1：技術の実用度について(1/2)

- 背景
  - DNSSECは、技術的には、DNSの応答偽造に対抗するにあたり、有効な解決策である
  - DNSSECの利用に当たっては、ICANN、レジストリ(JPRS)、指定事業者、DNSプロバイダ、ISP、各種機器メーカーなどが、連携する必要がある
  - しかし、これまで、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
- 課題
  - 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であろうが、その増強の必要度合いが十分にわかっていない

課題1:技術の実用度について(2/2)

- 解決の方向性(案)
  - 段階を踏んで解決する
    - 技術の検証
      - インターネット上の各種機器の動作確認
      - 処理能力増強の必要性確認
    - 運用性の検証
      - 特定プレイヤーによる連動検証
      - 各種プレイヤーが参加できるオープン参加型の検証
    - 運用の習熟
      - DNSSECを新たに利用したい者が、試用、習熟できる環境を提供

課題2：サービス導入ステップについて(1/2)

- 背景
  - DNSSECにおいては、
    ① 署名鍵および署名付き情報のDNSへの**登録フェーズ**
    ② DNSから取得される情報に付された署名の**検証フェーズ**
    という2つのフェーズがある
  - 上記の2つのフェーズは、タイミングや関わるプレイヤーが異なり、次のような多様なプレイヤーが関わって初めてDNSSECの効能が生じる
    ① ドメイン名登録者、レジストリ、指定事業者、DNSプロバイダ
    ② ISP、インターネット利用者
    ③ ①や②に機器を提供するベンダ
- 課題
  - 一挙に両フェーズの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

課題2：サービス導入ステップについて(2/2)

- 解決の方向性(案)
  - 登録フェーズは、プレイヤー数が比較的少なく、また、銀行やオンラインショップ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
  - 検証フェーズに関わるプレイヤーは、一般利用者や小規模ISPなども含み、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広い
  - セキュリティは、一般に、動機付けが難しい分野であり、最初は問題意識の高いプレイヤーが、DNSSECを理解し使うことが考えられるため、これらプレイヤーがDNSSECの署名鍵および署名付き情報を登録することが可能である状態を作ることが重要である
  - 検証は、ISPで行う方法、ユーザーのPCで行う方法などがある。他TLDのサービスモデルとの協調を考慮しつつ、広く調整・検討し、将来的に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、動機の強い人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

課題3:教育普及について(1/2)

- 背景
  - ドメイン名、DNSのセキュリティは、重要であるが、その認識はまだ低い
  - DNSSECについても、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
- 課題
  - ドメイン名登録者、一般利用者、サービス提供に関わる関係各所にDNSSECの効用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
  - しかし、現時点では、よい解説書もなく、その理解は難しい

課題3:教育普及について(2/2)

- 解決の方向性(案)
  - 煽ることなく、ドメイン名登録者や一般利用者、サービス提供に関わる関係各所に対し、適切な教育活動を行うことが重要
  - 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、JPRSが核となり、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、教育・普及を進めることを考えるべき

課題4：利用環境の充実について(1/2)

- 背景
  - DNSSECは、各プレイヤー(特に、ドメイン名登録者やユーザー)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
- 課題
  - 適切にDNSSECの恩恵を受けるに十分なレベルで、各プレイヤーが、原理と操作方法を理解し、それを実施することは難しい
  - たとえば、ドメイン名登録者もしくはDNSプロバイダは、次のようなことも考慮、実行する必要がある
    - 署名には有効期限があり、定期的に再署名を行う必要がある
    - 署名鍵を長時間使い続けるのは危険であり、定期的な変更が必要である
    - 署名鍵を漏洩しないように厳重に管理する必要がある
    - ISPを引っ越す、などのときにも再署名を行う必要がある

課題4：利用環境の充実について(2/2)

- 解決の方向性(案)
  - 段階を踏んで解決する
    - 第1フェーズ
      - DNSSECを深く理解し、自ら操作できる能力を持つプレイヤーに使ってもらう
    - 第2フェーズ
      - それぞれのプレイヤー向けの適切なツールを準備する
      - 上記環境の構築に向かうため、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道具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

課題5:責任分界について(1/2)

- 背景
  - DNSSECは、セキュリティに関連するサービスであり、セキュリティに関し、何らかの機能をユーザーに提供するものである
  - DNSSECは、JPRSが単独で提供できるサービスではなく、ICANN、指定事業者、DNSプロバイダ等との連携が必要であり、サービス提供するにあたっては多様なプレイヤーが関わる
- 課題
  - サービス利用上の問題が発生する場合も想定し、そ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
    - 各プレイヤーが何を保証するサービスなのか
    - 各プレイヤーの責任範囲はどういうものなのか
  - たとえば、次の問題が起こったとき、誰の責任でどう解決するのか
    - 署名鍵を長期間変更しなかったら、合鍵を作られてDNS応答を偽造された
    - ISPのDNSサーバがDNSSEC未対応のため、ユーザーがフィッシングに遭った

課題5:責任分界について(2/2)

- 解決の方向性(案)
  - DNSSECとは、ドメイン名登録者およびユーザーにとって何を保証してくれるものなのかの具体化
  - その中で、各プレイヤーの役割と保証範囲(責任範囲)の具体化
  - 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機能提供に関わる各種プレイヤーが連携し、その連携の中から、ドメイン名登録者およびユーザーに対し、「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