2012 年 4 月 23 日
DNSSEC ジャパン
運用技術 WG

ISP 等の DNSSEC 対応における DPS 作成・公開の検討

1. はじめに

1.1. 本文書について

DNSSEC ジャパン運用技術 WG は、ISP 等(*)がその DNS サービスにおいて DNSSEC 対応を行う際、DPS を公開することに利点があると考えている。しかし一方では、ISP が現状で DPS を公開するにはいくつかの課題も存在する。本文書ではこの認識を示しつつ、今後のアクションについて提案を行う。

(*)この議論では DNS ホスティングプロバイダなどを含むものとする

1.2.注意事項

- **免責事項**

  本ドキュメントは保証されたものではない。下記 Web サイトの免責事項を確認のうえ、本ドキュメントを使用して頂きたい。

  http://dnssec.jp/?page_id=16

- **問合せ先**

  本ドキュメントに関する改善点などのコメントは下記事務局まで連絡いただきたい。

  DNSSEC ジャパン事務局 sec@dnssec.jp

2. DPS とは

DPS(DNSSEC Practice Statement)は、DNSSEC 運用者が、その運用の考え方、方式、手順などを記述する文書である。本文書執筆時点で、IETF において DPS のフレームワークに関する検討が完了しつつある状況であり、以下の Internet-Draft に仕様が纏められている。

- DNSSEC Policy & Practice Statement Framework
  (draft-ietf-dnsop-dnssec-dps-framework)
  http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework

また、DPS に関する参考情報としては、社団法人日本ネットワークインフォメーションセンター(JPNIC)主催で行われた「DNSSEC セミナー ～組織における DNSSEC の姿～」(http://www.nic.ad.jp/ja/materials/tech/)における

- ICANN 大久保氏による講演「ICANN DPS の概要」
  (http://www.nic.ad.jp/ja/materials/tech/20110712/jpnic-dnssec-seminar-okubo-01-title.pdf)
- JPRS 森氏による講演「JP ドメイン名における DNSSEC について」
  (http://www.nic.ad.jp/ja/materials/tech/20110712/jpdps-20110712-mod.pdf)

の講演資料が公開されている。DPS に関する情報源として参照されたい。

2.1. ISP が DPS を公開する利点

WG は、下記の点から、ISP が DPS を作成・公開することにメリットがあると認識している。

- セキュリティレベルの可視化／透明性の確保
  現在は、技術において先進的な事業者がパイロット的に DNSSEC 運用を開始しているフェーズであり、実質的なセキュリティの確保よりも新技術の展開に重きがおかれている。しかし、今後はその本質から、DNSSEC における実質的なセキュリティの確保が望まれることが想定される。商用サービスにおいては、DNSSEC 対応におけるセキュリティレベルを可視化し、ユーザに対して透明性を確保する必要がでてくるだろう。このために DPS を公開することが役立つ。

- 運用方針の客観的なチェック／サービス品質の一定化
  セキュリティの確保においては、客観的な検討・評価が行われるべきであり、組織ごとの事情のみを重視して判断を行うべきではない。DPS を作成する際に検討が必要となる諸項目は、このための客観性・多角性を十分に与えるものである。また、

一旦 DPS を作成しておけば、運用レベルの指標ができるため、提供するサービスの品質を一定に保つことができる。

2.2. ISP が DPS を公開するための課題

一方で WG は、現時点で ISP が DPS を作成・公開するにあたり、以下のような課題が存在すると認識している。

- 認知不足

  国内 ISP における DPS フレームワークへの認知が不足している。このため、DPS 検討必要性の意識が持たれる素地が少ない。

- コミュニティの違い

  DPS の構成は PKI における CPS(Certification Practice Statement)を雛形とするものであり、認証ビジネスを展開するコミュニティの発想・感覚に基づいている。一方、DNSSEC 対応を行う ISP は一般に DNS に関するエキスパートであるものの、必ずしも PKI 的な発想に通じているわけではない。

- 記述レベルの難しさ

  PKI コミュニティの感覚を背景にできる場合でも、DPS と CPS は異なるものである。ここで、フレームワーク自体の設計が完了しきっていないなか、実際には限定的な DPS が存在するのみである(特に ISP が書いたものはほとんどない)。このため ISP は、適切なリファレンスを持たないまま、自らが DPS の記述レベルを定めなければならない。

- コスト回収の困難さ

  単独の組織体において DPS フレームワークに習熟した要員を手配し、適切に記述レベルを設定した上で DPS を作成・公開することは、作業コスト回収の観点で困難である。

3. 今後のアクション

WG では、DNSSEC により解決できる DNS の潜在的脆弱性を真に解決するために、今後、商用サービスを提供する ISP において、DPS フレームワークに基づく DNSSEC 対応が行われることがポイントになると考えている。

上述の課題を考慮しつつ、ISP がこのような対応を行える基盤を整えていくためには、

- ISP と PKI サービスの提供者が一同に介する形で参加できる検討の場を設定する。

- その場において、これまでは主にドメインレジストリで培われてきた DPS 作成ノウハウを、これら参加者が一体となって解釈／アレンジする。

- 上記活動で得られた解釈に基づき、ISP がリファレンスとすることのできる ISP 版 DPS の雛形を作成し、コミュニティに公開する。

というアプローチが効果的と考える。

今後、関連コミュニティにおいて WG 参加者が核となり、上記アプローチに基づく形で ISP 版 DPS の雛形を作成することを提案したい。

以上