



2010年10月25日

レジストリの鍵登録インターフェースに関する調査報告

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

木村泰司

■1. 概要

DNSSEC は、DNS のサーバに公開鍵の情報を登録しユーザが参照できるようにすることで、施された電子署名の連鎖を検証できるようにする仕組みである。DNSSEC の日本国内での展開を考える場合、国内のレジストラやリセラーでは、鍵登録インターフェース（以下、鍵登録 I/F と呼ぶ）が適切に実装される必要がある。鍵登録 I/F とは、DNSSEC の署名者の公開鍵をレジストリに登録するインターフェースのことで、ユーザが操作する Web インターフェースであったり、プログラムインターフェースであったりする。基本的にドメイン名の登録の仕組みの中に追加されると考えられる。

DNSSEC ジャパン技術検証 WG では、この鍵登録 I/F について調査した。DNSSEC ジャパンのメンバーでは、2010年6月現在、DNSSEC の鍵登録 I/F を公開しているレジストラやリセラーはなかった。そこで DNSSEC 対応の準備を進めているレジストラやリセラーにヒアリングを行い、鍵登録 I/F に関する状況および要望を集約した。

■2. レジストラおよびリセラーにおける DNSSEC 対応

DNSSEC ジャパン技術検証 WG では、複数のリセラーに対して鍵登録 I/F および DNSSEC 対応に関する状況についてヒアリングを行った。その結果次のようなことがわかっている。

- レジストラおよびリセラーは、Web ページや独自の API を用いたドメイン名に関する登録 I/F で連携している。
- 「(a)レジストリ～レジストラ I/F」はデータベース登録のためのインターフェースであり、gTLD のレジストリでは EPP (Extensible Provisioning Protocol) が使われていることが多い。
- 「(b)レジストラ～リセラー I/F」は登録申請用のインターフェースで、レジストラが定める独自のプロトコルであることがある。
- 「(c)リセラー～申請者 I/F」は Web インターフェースなどのユーザ・インターフェースであることが多い。

レジストラおよびリセラーの構造と DNSSEC 対応状況を図 2 にまとめる。

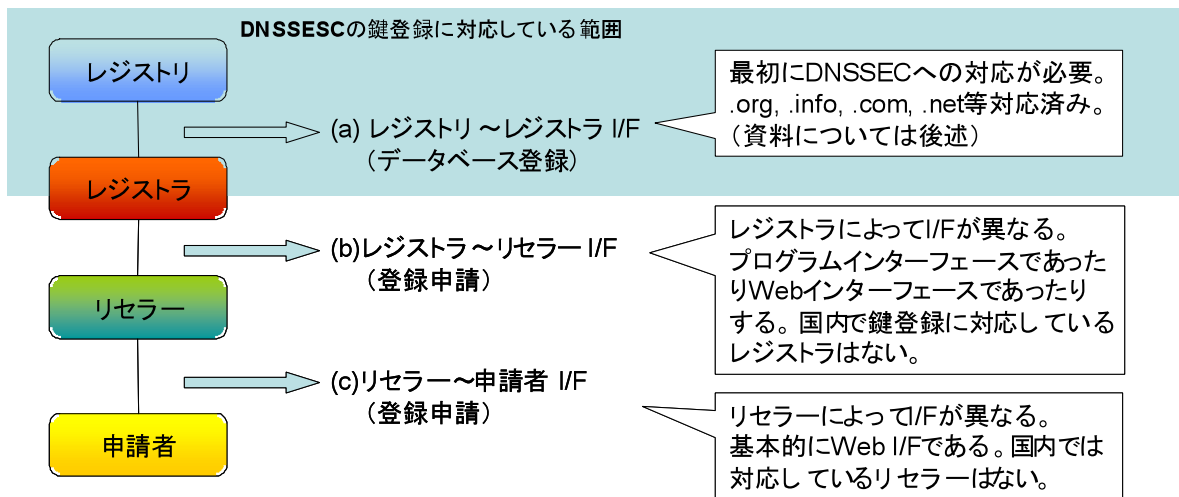


図 1 鍵登録対応が必要になるインターフェースと DNSSEC 対応状況

図 2 に示したように、日本国内では gTLD のレジストラで鍵登録 I/F を提供しているところがない。日本国内での DNSSEC の利用のためには、今後「(b)レジストラ～リセラー I/F」と「(c)リセラー～申請者 I/F」が DNSSEC の鍵登録に対応する必要がある。

■ 3. リセラーの DNSSEC 鍵登録 I/F への要望

前節で述べたヒアリングの結果、DNSSEC に関わる鍵登録 I/F に対して共通の要望があることがわかった。以下、複数のリセラーより共通にあげられた事項を挙げる。

レジストラおよび複数のリセラーに共通して挙げられた鍵登録 I/F に対する要望

- DS レコードの登録 I/F について
DNS サーバは顧客が管理していることがあるため、顧客向け Web では DS の登録を受け付けられることが望ましい。
- ドメイン名のリダイレクトサービスへの対応
ドメイン名の設置当初はリダイレクトサービス（転送サービス）が必要となる。このサービスができることが望ましい。
- ユーザ向けの鍵管理上の機能
鍵の有効期限切れを知らせてくれることが望ましい。
- ドメイン名移転への対応
ドメイン名の移転と同時に DNSSEC もできるようにすることが望ましい。
- ドメイン名移転時の DNSSEC 無効の要望
一方で、ドメイン名の移転のときは一時的に「DNSSEC なし」を前提にできると事業者としては負担が軽くなる。

■4. まとめ

本ヒアリングでは、まだ国内では DNSSEC の対応を顧客に提供している事業者がなく、国内のレジストラ・リセラー間のプロトコルの現状や DNSSEC 対応にあたって必要とされている事項を調べるにとどまった。

ヒアリングの結果、ドメイン名の移転や鍵登録 I/F において備えることが望まれる、事業者としての要望が見えてきた。この他にわかってきたことは、DNSSEC の顧客への提供については多くの事業者が国内の動向を見ている段階であるという現状である。

DNSSEC の成果物が、これらの状況を把握と、国内において DNSSEC が普及する場合に、現時点で必要な技術的な情報を提供できるような位置づけになることを願ってやまない。

以上



2010年10月25日

補足: DNSSEC に関する情報

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
木村泰司

■1. DNSSEC に関する情報

DNSSEC に対応している gTLD レジストリから、レジストラ向けに以下の情報が公開されている。

- PIR — <http://www.pir.org/dnssec>
PIR は、gTLD の.ORG のレジストリである。この Web ページでは DNSSEC の解説記事の他にブロードバンドルーターへの影響や、ISP における DNSSEC 対応のためのチェックリストなどを公開している。この他に DNSSEC の実装に関する情報や RFC へのリンクがある。レジストラ向けの鍵登録 I/F については WebEx やデータシートが提供されている。
- VeriSign
<http://www.verisign.com/domain-name-services/index.html>
VeriSign は.com、.net 等のレジストリである。レジストラに関する情報を公開している。鍵登録 I/F に関する情報はレジストラのメンバーページにて提供されている。
- Affilias — <http://www.afilias.info/dnssec>
Affilias は gTLD の.info、.org、.mobi、.asia、.aero のレジストリである。ccTLD も取り扱っている。この Web ページでは RFC 等の技術情報の他に、「DNSSEC overview」（DNSSEC の概要）や「Securing a Domain SSL vs DNSSEC」（ドメインのセキュリティに対する SSL と DNSSEC の違い）といった記事がある。鍵登録 I/F について技術したレジストラ向けのマニュアルはレジストラとして登録したメンバーのページで見られる。

以上