

JPRS トピックス&コラム



■DNSSECの円滑導入と安定運用の実現のために ～考えなければならない「対応と現実」～

DNSSECの円滑導入と安定運用を実現するために考慮しなければならない点について、レジストラ・DNS運用者における注意事項を中心に、具体的に解説します。

■レジストリ・レジストラモデルによる管理

現在の JP ドメイン名や、.com/.net を始めとする主な gTLD では、レジストリ・レジストラモデルと呼ばれる手法でドメイン名を管理運用しています。そのため、それらの TLD を DNSSEC に対応させる場合、レジストリ・レジストラモデルに合致した形で DNSSEC に関する情報を取り扱えるようにする必要があります。

■レジストリ・レジストラモデルの登場人物

レジストリ・レジストラモデルにおける代表的な登場人物と、その役割を以下に示します。

① 登録者

そのドメイン名を登録している本人です。リセラーやレジストラにドメイン名の登録を依頼します。

② リセラー

登録者からドメイン名の管理に必要な情報を受け取りますが、自らはレジストリへの登録を行わず、レジストラへの依頼により登録を行います。

③ レジストラ¹

登録者やリセラーからドメイン名の管理に必要な情報を受け取り、レジストリに登録を依頼します。

④ レジストリ

レジストラからドメイン名の管理運用に必要な情報を受け取り、自らのシステムに登録・管理します。登録した情報は TLD の権威 DNS サーバーで公開されます。

■レジストリ・レジストラにおける情報の流れ

現在のインターネットでは登録者のドメイン名の権威 DNS サーバーは、登録者自身²、リセラー、レジストラのいずれか³により運用されることが一般的です。

¹ JPドメイン名では指定事業者がレジストラの役割を担当しています。

²登録者が依頼する第三者が運用する場合もあります。

³登録者がプライマリ DNS サーバーを、リセラーやレジストラがセカンダリ DNS サーバーをそれぞれ運用するなどの形態も見られます。

いずれの場合も権威 DNS サーバーに関する登録情報は、図1に示した形でおのこの DNS 運用者からレジストラに渡され、レジストリに登録されます。

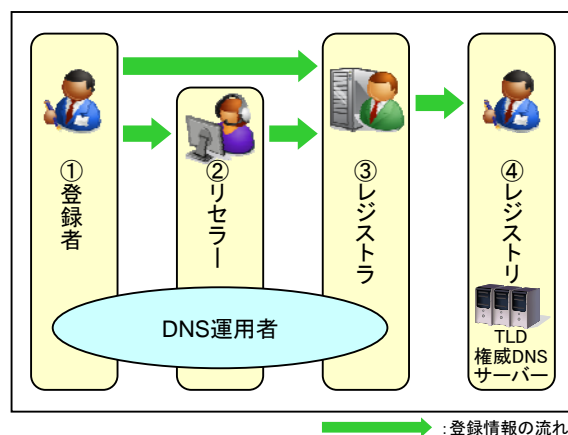


図1:レジストリ・レジストラモデルにおける情報の流れ

▼すべての情報はレジストラ経由で登録

このようにレジストリ・レジストラモデルでは、すべての情報の登録は、レジストラによる取り次ぎによって実施されることになります。

■レジストリにおける対応の次に必要なこと

現在、レジストリにおける DNSSEC への対応作業が積極的に進められています。レジストリによる DNSSEC 対応が完了することにより、その TLD における DNSSEC の導入・運用のための基礎が整うことになります。

しかし、レジストリ・レジストラモデルにおいて DNSSEC の導入を円滑に進めるためにはこれに加え、登録したドメイン名の権威 DNS サーバーにおける DNSSEC 対応、及びレジストリに権威 DNS サーバーに関する登録情報を取り次ぐレジストラにおける DNSSEC 対応が必須となります。

以降ではレジストラ及び DNS 運用者において DNSSEC 対応を実施する場合に必要な対応事項・注意事項について、具体的に解説していきます。

■レジストラにおける対応—情報の取り次ぎ

前述の通りレジストリ・レジストラモデルでは、レジストリへの情報の登録はレジストラを介して実施されます。そのためレジストラでは、DNSSEC 対応の際にレジストリへの登録が必要となる DS レコード⁴の受け付けと、レジストリへの取り次ぎに対応する必要があります。

DS レコードはドメイン名の鍵署名鍵(KSK)から生成され、レジストリの権威 DNS サーバーで公開されます。

■DNS 運用者における注意事項

ここでは、権威 DNS サーバーの運用時に鍵と署名の取り扱いにおいて特に注意が必要となる事項について、具体的に解説します。

▼DS レコードはレジストリにのみ登録

DS は従来の登録情報とは異なり自らのゾーンデータには登録されず、レジストリの権威 DNS サーバーのみに登録される情報であることに注意が必要です。

▼DNSSEC では定期的な鍵の更新が必要

DNSSEC ではセキュリティ上の理由により定期的な鍵の更新(ロールオーバー)が推奨されており、鍵(鍵署名鍵(KSK)及びゾーン署名鍵(ZSK)の双方)の定期的な更新が必要になります。

鍵の更新方法には二重署名法(Double Signature)と事前公開法(Pre-Publish)の2種類があります。

▼KSK の更新における注意

二重署名法による KSK の更新手順例を表1に示します。DNSSEC による信頼の連鎖を維持するため、単なる置き換えではなく、追加→削除という手順で更新する必要があります。

- | |
|-----------------------------|
| ①新しいKSKの生成と自分のゾーンデータへの追加 |
| ②新旧双方のKSKIによりDNSKEY(ZSK)を署名 |
| ③自分のDNSKEYのTTL設定値の時間分待つ |
| ④新しいKSKIに対応するDSレコードを親に登録依頼 |
| ⑤親のDSの登録更新を確認 |
| ⑥親のDSのTTL設定値の時間分待つ |
| ⑦古いKSKをゾーンデータから削除 |
| ⑧新しいKSKのみでDNSKEY(ZSK)を署名 |

表1:KSK の更新手順例(二重署名法)

⁴ レジストリが提供する DNSSEC サービス仕様により、DS レコードに対応する鍵署名鍵(KSK)自体の登録が必要になる場合があります。

▼ZSK の更新手順

事前公開法による ZSK の更新手順例を図2に示します。事前公開法では鍵の更新後に使用する鍵(鍵 B)を運用開始時にゾーンデータに事前登録し、あらかじめ公開しておくという方法が用いられています。

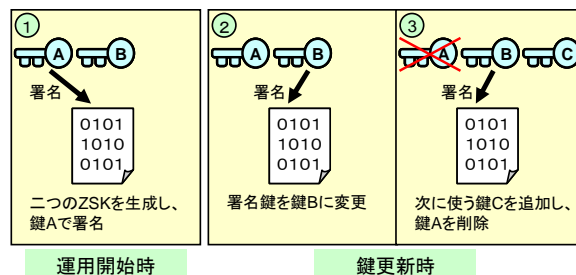


図2: ZSK の更新手順例(事前公開法)

▼ゾーンデータへの定期的な再署名が必要

DNSSEC ではセキュリティ上の理由により、署名に有効期限が設定されています⁵。そのため、ゾーンデータへの定期的な再署名が必要になります。

従来の DNS では登録情報に変化がない場合ゾーンデータの更新は必要ありませんが、DNSSEC では登録情報に変化がない場合でもゾーンデータへの定期的な再署名⁶が必要になることに注意が必要です。

■DNS 運用者間でのドメイン名移転の取り扱い

DNSSEC ではドメイン名の移転など、DNS 運用者の変更の際に従来の NS レコードと同様の手法で DS レコードを更新した場合、検証エラーが発生する可能性があります⁷。

検証エラーを避ける方法として、①いったん DNSSEC を解除してから移転する、②移転元・移転先の共同作業により、信頼の連鎖を維持したまま移転する、の二つが検討されています。

■DNSSEC の安定運用の実現に向けて

このように DNSSEC の安定運用のためには、多くの関係者における相互協力や標準的な運用管理手法の確立が必要です。JPRS では今後も各方面の関係者と協力しながら、DNSSEC の導入を推進していきます。

⁵ BIND 9 における有効期限のデフォルト設定値は 30 日となっています。

⁶ 署名の際には SOA のシリアル番号を増やす必要があります。

⁷ 技術的詳細が以下の発表資料で紹介されています。

<https://www.dns-oarc.net/files/workshop-200905/gudmundsson.pdf>