DNSSEC
gTLD レジストラ移転実験報告

平成 23 年 4 月

DNSSEC ジャパン

DNSSEC
gTLD レジストラ移転実験報告

（目次）

1. はじめに

近年、インターネットの根幹を支える重要な仕組みである DNS に対して、DNS 応答を偽造することで引き起こされるセキュリティ上の脅威が顕在化し、リスクは急激に増大しています。

その対策として、DNS のセキュリティ拡張機能である DNSSEC の導入が急がれ、2010 年 7 月、ルートゾーンに導入されたのをきっかけに、各 gTLD,ccTLD も続々と導入に向けての施策を進めています。
DNSSEC の普及を進めるためにはルートゾーンや TLD の対応だけでなく、ドメインレジストラ、ドメイン登録者の対応・協力が必要不可欠ですが、現状ではそのノウハウが溜まっておらず、運用上の課題が山積しています。
中でもレジストラ移転・DNS プロバイダ移転は、複雑な鍵更新作業を実施しながら事業者間をまたがった作業が必要なため、信頼の連鎖を維持したままの移転が非常に難しいものとなっています。
レジストラ移転･DNS プロバイダ移転の方法としては RFC4641bis が提唱されていますが、これは実際に運用するに当たってあまり現実的ではない方法を用いているため、利用が困難な状況です。

DNSSEC ジャパン(以降、DNSSEC.jp とする)では、2010 年 11 月に発行した「DNSSEC レジストラ移転ガイドライン」に沿って、2011 年 1 月末～2 月中旬に gTLD(.ORG、 .NET)でのレジストラ移転実験を行い、以下を確認しました。

・ガイドラインに沿ってレジストラ移転が実施できること
・実際にレジストラ移転を行った際の注意事項

DNSSEC.jp は、「DNSSEC レジストラ移転ガイドライン」および本報告によって多くの人々がトラブルなく DNSSEC の運用が実施できることを願います。

1.1. 目的

本報告は、「DNSSEC レジストラ移転ガイドライン」に沿って実施したレジストラ移転の実験結果報告を目的とする。

1.2. 想定する読者

本報告は、「DNSSEC レジストラ移転ガイドライン」の読者を読者として想定している。

1.3. 用語の定義

本報告で用いる用語の定義は「DNSSEC レジストラ移転ガイドライン」に準ずる。

1.4. 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. 実験シナリオ

gTLD レジストラ移転実験(以降、本実験とする)では、現実的に起こりえると想定される 7 パターンのシナリオを作成し、そのうち既存の手順と相違ないもの、および他のパターンに包含されるものを除く 5 パターンについて、実際に gTLD に登録したドメイン名を使用してレジストラ移転実験を実施した。

2.1. 対象パターンと使用 gTLD

パターン 1：DNSSEC 利用無 → DNSSEC 利用無
RFC4641bis で紹介されているレジストラ移転手順
(非推奨方式のため省略)
―

パターン 2：DNSSEC 利用有 → DNSSEC 利用有
.NET

パターン 3：DNSSEC 利用無 → DNSSEC 利用有
.ORG

パターン 4：DNSSEC 利用有 → DNSSEC 利用無
.ORG

パターン 5：DNSSEC 利用有 → DNSSEC 利用有
レジストラ移転のみ、DNS サーバの移転は行わない
.ORG

パターン 6：DNSSEC 利用有 → DNSSEC 利用有
DS レコードを削除した後レジストラ移転
(パターン 3 と同様のため省略)
―

パターン 7：DNSSEC 利用有 → DNSSEC 利用有
移転前に移転先の NS をセカンダリとして登録する
(手順が複雑なため実験対象外とした)
―

2.2. 各パターンにおける移転フロー

以下の各パターンにおける移転フローでは、実施者を以下のように定義する。

実施者の定義：

① 登録者

② 移転元レジストラ
③ 移転元 DNS プロバイダ
④ 移転先レジストラ
⑤ 移転先 DNS プロバイダ

パターン 2 の詳細フローと状況：

項番	日付	実施者	アクション
2-1	1 日目	①	移転申請
2-2		②	移転承認
2-3		④	移転完了
2-4		④	元 DS の削除
2-5		⑤	移転先プロバイダゾーン作成完了
2-6	2 日目	④	元 DS の TTL 経過待ち(86400)
2-7		④	元 NS の削除と先 NS の登録
2-8	4 日目	④	先 NS の TTL 経過待ち(172800)
2-9		④	先 DS の登録
2-10	6 日目	④	先 NS の TTL 経過待ち(172800)
2-11		③	移転元プロバイダゾーン削除

パターン 3 の詳細フローと状況：

項番	日付	実施者	アクション
3-1	1 日目	①	移転申請
3-2		②	移転承認
3-3		④	移転完了
3-4		④	元 NS の削除と先 NS の登録
3-5		⑤	移転先プロバイダゾーン作成完了
3-6	2 日目	④	元 NS の TTL 経過待ち(86400)
3-7		④	先 DS の登録
3-8	3 日目	④	先 NS の TTL 経過待ち(86400)
3-9		③	移転元プロバイダゾーン情報削除

パターン 4 の詳細フローと状況：

項番	日付	実施者	アクション
4-1	1 日目	①	移転申請
4-2		②	移転承認
4-3		④	移転完了

4-4		④	元 DS の削除
4-5		⑤	移転先プロバイダゾーン作成完了
4-6	2 日目	④	元 DS の TTL 経過待ち(86400)
4-7		④	元 NS の削除と先 NS の登録
4-8	3 日目	④	先 NS の TTL 経過待ち(86400)
4-9		③	移転元プロバイダゾーン情報削除

パターン 5 の詳細フローと状況：

項番	日付	実施者	アクション
5-1	1 日目	①	移転申請
5-2		②	移転承認
5-3		④	移転完了

3. 実験結果

以下、各パターンで実験結果をまとめた。

3.1. パターン 2

DNSSEC 状態： 有り → 有り
使用 TLD： .NET
移転実施：想定通りの移転が実施できた
発生したトラブル等：
・DNS プロバイダの移転時に移転先ネームサーバの設定ができなかった。
⇒.NET ゾーンに移転先ネームサーバのホスト登録を行い、解決。

その他コメント：
・項番「2-10」の TTL 待ち について不要に感じた。業務フローとの兼ね合いもあるので このフロー自体に問題はないかと思われる。

3.2. パターン 3

DNSSEC 状態： 無し → 有り
使用 TLD： .ORG
移転実施：想定通りの移転が実施できた
発生したトラブル等：
・移転予定のレジストラに移転できなかった。
移転予定レジストラが.ORG に DNSSEC 適合の登録をしていなかったため。
⇒移転先を DNSSEC 適合レジストラに変更した。
・移転元レジストラ要因でレジストラ移転に時間を要した。
移転元が移転承認の時間切れまで承認・非承認を行わず、無応答であったため。

3.3. パターン 4

DNSSEC 状態： 有り → 無し
使用 TLD： .ORG
移転実施：想定通りの移転が実施できた
発生したトラブル等：
・移転元レジストラ要因でレジストラ移転に時間を要した。

3.4. パターン 5

DNSSEC 状態： 有り → 有り
使用 TLD：.ORG
移転実施：想定通りの移転が実施できた
発生したトラブル等：特に無し
その他コメント：
・レジストラ移転のみで、DNS の変更なし。
・特別な作業を行わなくても DNSSEC に影響無く移転が可能。

3.5. まとめ

ガイドラインに沿ってレジストラ移転が実施できることを確認した。
TTL 待ちの際、移転ドメインの TLD によって TTL の長さが変わるので注意したい。
(参考)

.NET	.ORG	.JP
NS：172800	NS：86400	NS：86400
DS：86400	DS：86400	DS：86400

また、レジストラ移転を行う際の注意事項としては、レジストラ移転承認に関して消極的承認(時間切れまで非承認せず無応答)のレジストラがあり、時間切れまでの時間を余計に要する場合のあることがわかった。

※.ORG の移転に関して
対象ドメイン名が DNSSEC を適用していた場合、移転先レジストラは事前にレジストリへ DNSSEC 適合レジストラとして登録しておかないと、DNSSEC を適用しているドメイン名を移管できない。
(本実験実施当時は、適合レジストラとしての登録がなくてもレジストリツールのインターフェース上に DS 登録画面が見えていたが、2011 年 4 月現在では、適合レジストラでなければ登録インターフェースが見えないようになっている。)

※ .NET 移転に関して
.NET の場合は、DNSSEC を適用しているドメイン名を移転する場合、移転先レジストラが DNSSEC 対応をしていなくても移転が可能。レジストリツールからの手動での DS 登録もできる。
当該レジストリ利用の方は注意が必要です。

4. 参考 URL

DNSSEC ジャパン（DNSSEC.jp）
http://dnssec.jp/

JPRS(DNSSEC 関連情報)
http://jprs.jp/dnssec/

JPNIC(DNSSEC)
http://www.nic.ad.jp/ja/newsletter/No43/0800.html

5. 謝辞

本実験を実施するに当たり、貴重な時間を割いてご協力いただきました以下の皆様に深く感謝いたします。

会社名(五十音順)

株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ
さくらインターネット株式会社
ソフトバンクテレコム株式会社
株式会社日本レジストリサービス
株式会社ライブドア