



DNSSEC 2011 スプリングフォーラム

gTLD レジストラ移転実験報告

株式会社NTTPCコミュニケーションズ
加藤 優佐

株式会社ライブドア
門馬 優子

2011. 04. 20



レジストラ移転実験について

レジストラ移転ガイドラインで説明した各パターンの移転手順について実環境で実験を行い、以下の事項を確認した。

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



実験報告の対象者

- ・DNSSEC化を検討しているドメイン登録者
- ・ドメインレジストラ(リセラ)
- ・DNSサーバ運用者

のうち、

レジストラ移転ガイドラインを読んでいる方。



実験のシナリオ

パターン1: DNSSEC あり→DNSSEC あり
方式(1)RFC4641bisの手順
⇒非推奨方式のため省略

パターン2: DNSSEC あり→DNSSEC あり
方式(2)DNSSECを一旦解除の手順

パターン3: DNSSEC なし→DNSSEC あり

パターン4: DNSSEC あり→DNSSEC なし



実験のシナリオ

パターン5: DNSSEC あり→DNSSEC あり
レジストラ移転のみ。DNSの移転はしない

パターン6: DNSSEC あり→DNSSEC あり
DS レコードを削除してのレジストラ移転
⇒移転時はパターン3と同様のため省略

パターン7: DNSSEC あり→DNSSEC あり
移転前に移転先のNS をセカンダリ登録し、
公開鍵、署名ごとゾーン転送しておく

各パターンの移転フロー

●パターン2 使用TLD: .NET

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

各パターンの移転フロー

●パターン3 使用TLD: .ORG

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

各パターンの移転フロー

●パターン4 使用TLD: .ORG

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

各パターンの移転フロー

●パターン5 使用TLD: .ORG

項番	日付	実施者	アクション
5-1	1日目	登録者	移転申請
5-2		移転元 レジストラ	移転承認
5-3		移転先 レジストラ	移転完了

各パターンの移転フロー

●パターン7 使用TLD: .ORG

項番	日付	実施者	アクション
7-1	1日目	移転先 プロバイダ	移転先ゾーンのセカンダリ設定、ゾーン転送
7-2		移転元 レジストラ	先NSの登録
7-3		登録者	移転申請
7-4		移転元 レジストラ	移転承認
7-5		移転先 レジストラ	移転完了



実験結果

●パターン2

- ・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:
 - ー 移転先ネームサーバの設定が出来なかった。
⇒.NETゾーンにネームサーバのホスト登録を行い、解決。



実験結果

●パターン3

- ・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:
 - ー 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
⇒移転先を変更して実験を継続
 - ー 移転元レジストラの要因で移転自体に時間がかかった。
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
⇒時間切れまで待ってから実験再開



実験結果

●パターン4

- ・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:
 - － 移転元レジストラの要因で移転自体に時間がかかった。

●パターン5

- ・移転実施: 想定通りの移転が実施できた。
- ・特に特別な対応は必要無い。
 - － DNSの変更が伴わない場合の移転はDNSSECにも影響なく通常通り移転が可能。



実験結果

●パターン7

- ・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:
 - ー 移転予定のレジストラに移転できなかった。
 - ー 移転元レジストラの要因で移転自体に時間がかかった。
- ・移転はSecureな状態のまま行える。
- ・移転後、DNSSEC署名の有効期限が切れる前に鍵のロールオーバーと再署名を行う必要がある。
(署名の有効期限が切れるとBogusになってしまう)



移転時の注意事項

- ・移転を行うドメインのTLDによって、TTLが異なる。

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

- ・移転承認に関して消極的承認のレジストラがある。

(承認時間切れまで承認・非承認を行わず、無応答)



移転時の注意事項

・.ORGの移転に関して

- ーレジストラはDNSSEC適合の登録が必要
- ー移転先に上記登録が無いと、DNSSEC適用ドメインを移転入りさせることができない
- ー登録が無いとレジストリツール上のDS登録画面でもDSを登録できない
(現在は登録レジストラでないとDS登録画面も出ない模様)



移転時の注意事項

・.NETの移転に関して

- －DNSSEC適合の登録等は必要ない
- －移転先がDNSSECに対応していなくても、DNSSEC適用ドメインを移転できる
- －レジストリツール上のDS登録画面にて手動でDSを登録できる



最後に

- ・DNSSEC的にSecureな状態での移転は難しい。
- ・各TLDやレジストリ、移転前後のレジストラによって、レジストラ移転時の注意点は様々。
- ・レジストラ(リセラー含む)のレジストラ移転における作業を定型の運用に落としていくのは困難な状況。
- ・まだまだ経験の蓄積と共有が必要。