DNSSEC
レジストラ移転ガイドライン

平成 22 年 11 月
DNSSEC ジャパン

DNSSEC
レジストラ移転ガイドライン

（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。

そこで我々DNSSEC ジャパンでは、より現実的で運用可能な DNSSEC 導入後のレジストラ移転・DNS プロバイダ移転方法を検討しました。
本ガイドラインはその検討を取りまとめたもので、推奨する移転方法を紹介しています。
第一章では用語の定義や本ガイドラインにおける前提条件を記載しています。
第二章では検討の結果得られた、推奨される移転方法を解説します。
第三章ではその結果に至るまでの詳細な検討の経緯を解説しています。
なお、RFC4641bis との違いなどについては、第三章をごらんください。

DNSSEC ジャパンでは、本ガイドライン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

「DNSSEC レジストラ移転ガイドライン」（以下、「本ガイドライン」という。）は、DNSSEC を導入した DNS サーバが関係するレジストラ移転の具体的フローを明確化することで、各関係者間のトラブルを防ぎ、健全な DNSSEC 運用を確保することを目的とする。

1.2　想定する読者

本ガイドラインは、ドメイン名の DNSSEC 化を検討しているドメイン名登録者、ドメインレジストラ（JP ドメイン名の場合は指定事業者）、DNS サーバ運用者を読者として想定している。本ガイドラインの完全な理解のためには、ドメイン名登録の手順、DNSSEC を含む DNS の概念について基本的な理解があることが望ましい。

・DNSSEC ジャパンが公開している下記の文書を参考にするとよい

- ・DNSSEC について
- ・DNSSEC 導入に当たって
- ・RFC4033, RFC4034, RFC4035 など

1.3　用語の定義

本ガイドラインで用いる用語の定義は、以下のとおりとする。

1. ドメイン名登録者
   移転対象ドメインの登録者

2. 移転元レジストラ
   移転対象ドメインの登録を移転前に管理していたドメインレジストラ

3. 移転先レジストラ
   移転対象ドメインの登録を現在管理しているドメインレジストラ

4. 移転元 DNS プロバイダ
   移転対象ドメインのゾーン情報等を移転前に管理していた DNS プロバイダ

5. 移転先 DNS プロバイダ
   移転対象ドメインのゾーン情報等を現在管理している DNS プロバイダ

6. レジストリ
移転対象ドメインの登録申請を受け付ける管理組織

7. 一般ユーザ
移転対象ドメインを利用し、WEB などを閲覧しているユーザ

8. レジストラ移転
ドメイン名登録者が、レジストリへのドメイン名の登録・ 維持管理を委託するドメインレジストラを変更すること

9. DNS プロバイダ移転
ドメイン名登録者が保有するドメイン名のゾーンを運用する DNS プロバイダを変更すること

10. DNSSEC 対応リゾルバ
DNSSEC の署名検証を行うフルリゾルバ（バリデータ兼キャッシュサーバ)。

11. DNSSEC 非対応リゾルバ
DNSSEC の署名検証を行わない通常のフルリゾルバ（キャッシュサーバ)。

12. Secure (検証成功)な状態
DNSSEC 対応リゾルバのトラストアンカーから当該ゾーンまでのすべての委任点に DS レコードが存在しており、各階層のゾーンが全て DNSSEC によって署名されている。この状況において DNSSEC 対応リゾルバが全ての応答の署名検証に成功した状態。

13. Insecure (未署名状況検出)な状態
DNSSEC 対応リゾルバのトラストアンカーから当該ゾーンまでに DS レコードが存在していない委任点があるが、その階層までのゾーンは全て DNSSEC によって署名されている。この状況において DNSSEC 対応リゾルバがその階層までの応答の署名検証に成功した状態。

14. Bogus (検証失敗)な状態
DNSSEC 対応リゾルバにおいて当該ゾーンへのトラストアンカーが存在するが、何らかの理由で応答の署名検証に失敗した状態。署名検証に失敗する原因となるものは、適切な署名鍵による署名の不在、署名の期限切れなどである。

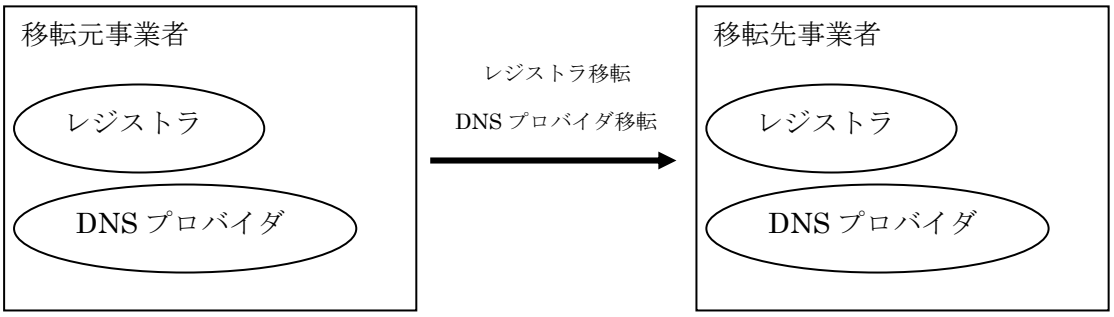
15. Indeterminate (検証対象外)な状態
DNSSEC 対応リゾルバにおいて当該ゾーンへのトラストアンカーが存在しない、もしくは DNSSEC 非対応リゾルバにおける状態。

1.4 本ガイドラインにおける前提条件

1. 一般的な商用ドメインサービスにおいてレジストラ移転が行われるとき、顧客との契約が解除されることになる移転元のレジストラおよび DNS プロバイダは追加の作業を行うモチベーションが低いと考えられる。そのため移転元レジストラには作業を課さない。
2. 既存のドメイン名登録・DNS 運用のフローを大きく変更するものは対応が困難と考えられる。そのため既存の運用フローに則った作業を想定する。
3. あるゾーンが DNSSEC 対応リゾルバにおいて検証失敗となる状況(Bogus)は、未署名状況検出または検証対象外となる状況(Insecure/Indeterminate)より問題が大きいと考える。そのため検証失敗（Bogus）な状況になることを避ける。
4. 2 章において展開するレジストラ移転方法は、移転元・移転先の事業者がともにレジストラ、DNS プロバイダの両方を兼ねている場合とする。それ以外、即ちレジストラと DNS プロバイダが異なる場合（DNS プロバイダをドメイン名登録者が行っている場合も含む）は、ドメイン名登録者自身が移行手順を実施する必要があるだろう。

本ガイドラインでは以上の条件を踏まえ、DNSKEY レコードと DS レコードの不整合(Bogus を引き起こす)がいずれの瞬間にも発生しない安全な運用フローの構築を検討した。

- 前提条件 4.の図



2. 推奨するレジストラ移転方法

この章では DNSSEC ジャパンが推奨するレジストラ移転方法を紹介する。
この結果に至った検討内容については第三章にて記載しているので、そちらを参照されたい。

2.1 移転時の基本的注意事項

DNSSEC 対応リゾルバの検証結果が Bogus となると、DNSSEC 対応リゾルバを使用するユーザの当該ドメイン名へのアクセスは全て失敗するようになる。
このため、DNSSEC 対応ドメイン名をレジストラ移転・DNS プロバイダ移転する際には Bogus の発生を防がなければならない。

具体的には、ゾーン(登録者)の署名鍵(DNSKEY レコード)と上位ゾーン(レジストリ)で登録される当該ゾーンの署名鍵相当情報(DS レコード)の対応関係を保ち、当該ゾーンにおいては適切に署名を行い続けることで Bogus を回避 する。

※親ゾーンに DS レコードが存在せず子ゾーンに DNSKEY が存在する場合は、
Bogus ではなく Insecure となるため許容範囲となる

DNSKEY レコードは DNS プロバイダごとに異なるものが使用されるため、DNS プロバイダ移転においては、レジストリに登録している DS レコードを併せて置き換える必要がある。同様に、レジストラ移転が DNS プロバイダ移転を伴う場合にも、DS レコードを置き換えなければならない。

DS レコード置き換えの際は、DNSSEC 対応リゾルバにおいても DNSKEY レコードと DS レコードの不整合が発生しないよう留意する必要がある(TTL による同期遅延がある)。

※以降、第 2 章に限り、レジストラ＝レジストラ兼ＤＮＳプロバイダとする

2.2　DNSSEC 利用あり→DNSSEC 利用ありのレジストラ移転方法

ドメイン登録者は、移転元のサービスにて既に DNSSEC サービスを利用しており、移転先においても DNSSEC サービスを利用予定。

- フロー図は別紙「パターン別移転フロー図」のパターン 2 を参照

1. ドメイン登録者は下記の申込を移転先レジストラに申請する。
   ・レジストラ移転申込
   ・DNS サービス申込
   ・DNSSEC サービス申込
2. 移転先レジストラは申込を受領後、ドメイン登録者よりゾーン情報を受け取り、ゾーン作成・鍵生成・署名を予め実施する。
   また、合わせてレジストラ移転申請をレジストリに対して実施する。
3. レジストリは移転確認を移転元レジストラに実施する。
4. 移転元レジストラは移転承認回答をレジストリに対して実施する。
5. レジストリは承認を確認後、権限移転及び移転元・移転先レジストラに結果を通知する。
6. 移転先レジストラは権限移転を確認後、早急にレジストリに登録されている移転元レジストラの DS レコードを削除する。これには下記のような理由による。
   ・移転元レジストラが権限移転後すぐに DNSKEY を削除し、ドメインが Bogus の状態になるのを避けるため。
   ・移転元レジストラが権限移転後すぐにゾーン情報を削除する可能性があるため、NS レコードを早めに移転先レジストラへ変更したいが、そのためにはまず DS レコードを削除しなければならないため。
7. 移転元レジストラの DS レコードを削除したことで DNSSEC の状態は Secure から Insecure へ移る。
8. 移転元レジストラの DS レコード TTL が経過し、全てのキャッシュが Insecure の状態へ移るのを待つ。
9. 移転元レジストラの DS レコード TTL 経過後、移転先レジストラはレジストリに登録されている移転元レジストラの NS レコードを削除。移転先レジストラの NS レコードを登録する。
10. 移転元レジストラの NS レコード TTL が経過するまで待つ。

11. 移転元レジストラの NS レコード TTL 経過後、移転先レジストラは移転先レジストラの DS レコードを登録する。これにより一部のキャッシュにて DNSSEC の状態が Insecure から Secure へ移る。また、移転元レジストラへゾーン情報削除可であることを通知する。
12. 移転先レジストラの NS レコード TTL が経過後、全てのキャッシュが NS レコードとともに DS レコードを受け取ることになるため、DNSSEC の状態は全て Secure へ移る。
13. この状態で移転先レジストラはドメイン登録者に対して、ゾーン情報の変更受付を開始する。
14. レジストラ移転は完了する。

- Insecure の期間は移転元 DS レコード TTL、移転元 NS レコード TTL、移転先 NS レコード TTL に依存する。

2.3 DNSSEC 利用なし→DNSSEC 利用ありのレジストラ移転方法

ドメイン登録者は、移転元のサービスにて DNSSEC サービスを利用しておらず、移転先において初めて DNSSEC サービスを利用する。

- フロー図は別紙「パターン別移転フロー図」のパターン 3 を参照

1. ドメイン登録者は下記の申込を移転先レジストラに申請する。
   ・レジストラ移転申込
   ・DNS サービス申込
   ・DNSSEC サービス申込
2. 移転先レジストラは申込を受領後、ドメイン登録者よりゾーン情報を受け取り、ゾーン作成・鍵生成・署名を予め実施する。
   また、合わせてレジストラ移転申請をレジストリに対して実施する。
3. レジストリは移転確認を移転元レジストラに実施する。
4. 移転元レジストラは移転承認回答をレジストリに対して実施する。
5. レジストリは承認を確認後、権限移転及び移転元・移転先レジストラに結果を通知する。
6. 移転先レジストラは移転元レジストラの DS レコードが存在しないことを確認し、移転元レジストラの NS レコードを削除。移転先の NS レコードを登録する。
7. 移転元レジストラの NS レコード TTL が経過するまで待つ。DNSSEC の状態は Indeterminate から Insecure に移る。

8. 移転元レジストラの NS レコード TTL が経過後、移転先レジストラの DS レコードを登録する。移転元レジストラにはゾーン情報が削除可であることを通知する。DNSSEC の状態は、Insecure から Secure に移る。
9. 移転先レジストラの NS レコード TTL が経過後、全てのキャッシュが NS レコードとともに DS レコードを受け取ることになるため、DNSSEC の状態は全て Secure へ移る。
10. レジストラ移転は完了する。

2.4 DNSSEC 利用あり→DNSSEC 利用なしのレジストラ移転方法

ドメイン登録者は、移転元のサービスにて DNSSEC サービスを利用しており、移転先においては、DNSSEC サービスを利用しない。

- フロー図は別紙「パターン別移転フロー図」のパターン 4 を参照

1. ドメイン登録者は下記の申込を移転先レジストラに申請する。
   ・レジストラ移転申込
   ・DNS サービス申込
2. 移転先レジストラは申し込み受領後、ドメイン登録者よりゾーン情報を受け取り、ゾーンを作成。合わせてレジストラ移転申請をレジストリに対して実施する。
3. レジストリは移転確認を移転元レジストラに実施する。
4. 移転元レジストラは移転承認回答をレジストリに対して実施する。
5. レジストリは承認を確認後、権限移転及び移転元・移転先レジストラに結果を通知する。
6. 移転先レジストラは権限移転を確認後、早急にレジストリに登録されている移転元レジストラの DS レコードを削除する。これには下記のような理由による。
   ・移転元レジストラが権限移転後すぐに DNSKEY を削除し、ドメインが Bogus の状態になるのを避けるため。
   ・移転元レジストラが権限移転後すぐにゾーン情報を削除する可能性があるため、NS レコードを早めに移転先レジストラへ変更したいが、そのためにはまず DS レコードを削除しなければならないため。
7. 移転元レジストラの DS レコードを削除したことで DNSSEC の状態は Secure から Insecure へ移る。
8. 移転元レジストラの DS レコード TTL が経過し、全てのキャッシュが Insecure の状態へ移るのを待つ。
   移転元レジストラの DS レコード TTL 経過後、移転先レジストラはレジストリに登

録されている移転元レジストラの NS レコードを削除。移転先レジストラの NS レコードを登録する。

9. 移転元レジストラの NS レコード TTL が経過し、全てのキャッシュが移転先 NS レコードを参照、DNSSEC の状態が Insecure から Indeterminate な状態へ移るのを待つ。
10. 移転元レジストラの NS レコード TTL 経過後、移転元レジストラへゾーン情報削除可であることを通知、ドメイン登録者に対してゾーン情報の変更受付を開始する。
11. レジストラ移転は完了する。

3. レジストラ移転検討詳細

この章では第二章で紹介した推奨するレジストラ移転方法がどのようにして導き出されたのか、その経緯と検討内容を記載する。

3.1 移転方式とその特徴

DNSSEC 対応ドメイン名の移転方式は、大別して以下の 2 通りとなる。

方式(1) ドメイン名の DNSSEC 対応を解除しない移転方式
移転元・移転先の関係者が緊密な連携体制を整えた上で、多数ステップからなるデータ交換・登録を行いながらドメイン名の移転を行う方式。
ICANN/IETF のメンバーを中心に手順が考案され(*)、いずれの瞬間にも DNSSEC 対応リゾルバからは DNSSEC 対応ゾーン(Secure)として扱われる。

(*) http://datatracker.ietf.org/doc/draft-ietf-dnsop-rfc4641bis/

方式(2) ドメイン名の DNSSEC 対応を一旦解除する移転方式
移転作業中の短期間、ドメイン名の DNSSEC 対応(Secure)を一旦解除する方式。
これまでの DNS 移転の手順に対し比較的少ない追加作業のみで実現できるため現実性が高いと考えられる。ただし、DNSSEC 対応解除中は DNSSEC 対応リゾルバからは DNSSEC 未対応ゾーン(Insecure)として扱われる。

3.1.1 推奨する移転方式の決定までの経緯

本ガイドラインでは方式(2)の利用を推奨している。
その理由として、RFC4641bis をベースとした方式(1)は下記のような問題を含んでいるからである。

１．移転元レジストラ・移転先レジストラ間で、鍵データの交換や署名情報の交換など多くのやり取りが必要になり、手順が複雑である。手順が複雑であれば、その過程でミスをしやすく、結果 Bogus の状態に陥ってしまう可能性が高い。
２．大手レジストラでは日々数百件のレジストラ移転作業を行っている。この膨大な作業に対して、一つ一つ移転元レジストラとのやりとりを行うのは非現実的である。
３．移転元のレジストラは顧客との契約が解除されることになるため、複雑で手間のかかる作業を追加で実施するモチベーションは低いと思われる。
４．移転元レジストラが非協力的な場合、方式(1)は成り立たない。

以上の理由から､DNSSEC ジャパンでは移転元レジストラのオペレーションを極力減らし、移転先レジストラにてほぼ全てのオペレーションが可能な方式(2)を推奨する。

3.2　詳細パターン分析

詳細パターン分析では、DNSSEC が実際に一部の事業者などで導入され始めた場合、レジストラ移転はどのようなケースが発生しうるのかを洗い出し、表にしたものである。加えてそれら一つ一つにケースに対して、どのような対応パターンが存在するのかも検討した。結果として全てのケースは 8 つのパターンで対応できることが判明した。

パターン 0：DNSSEC を利用しない通常のレジストラ移転
パターン 1：方式(1)を利用した DNSSEC あり→DNSSEC ありのレジストラ移転
パターン 2：方式(2)を利用した DNSSEC あり→DNSSEC ありのレジストラ移転
パターン 3：方式(2)を利用した DNSSEC なし→DNSSEC ありのレジストラ移転
パターン 4：方式(2)を利用した DNSSEC あり→DNSSEC なしのレジストラ移転
パターン 5：レジストラ移転のみ。DNS サーバの移転はなし
パターン 6：DS レコードを削除してのレジストラ移転
パターン 7：移転前に移転先の NS を登録する

本ガイドラインでは、方式(2)を利用した DNSSEC が関連するレジストラ移転を検討するため、下記のパターンを除外。

パターン 0,5,6 は通常のレジストラ移転と大差ないため除外。
パターン 1 は方式(1)を利用しているため除外。
パターン 7 は特殊な対応になるため、別途検討。

結果、対応パターン（2，3，4）を 2 章にて紹介した。

- 分析結果詳細については別紙「パターン洗い出しのための検討チャート」を参照

3.3 パターン別フロー図作成

パターン別フロー図作成では、詳細パターン分析で得られた 8 つのパターンを図式化し、フロー図を作成。わかりやすくパターンを紹介している。
ただし、下記のフローは除外している。

・3.1 章で紹介した方式(1)を利用しているパターン 1
・移転自体は通常のレジストラ移転と変わりないパターン 6
・別途検討予定のパターン 7

- 別紙「パターン別移転フロー図」を参照

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

本ガイドラインを作成するに当たり、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。

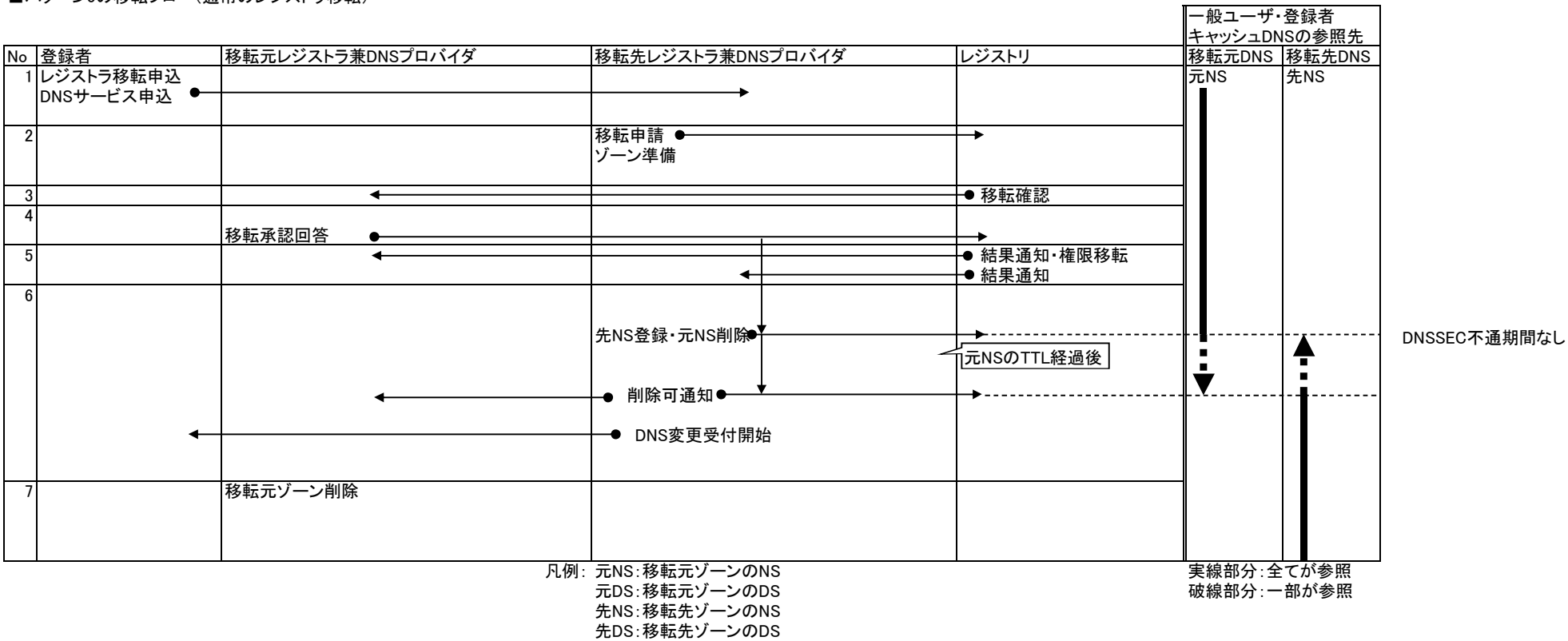
会社名（五十音順）

株式会社インターネット総合研究所
インターネットマルチフィード株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
NTT 情報流通プラットフォーム研究所
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
日本インターネットエクスチェンジ株式会社
株式会社日本レジストリサービス
株式会社ライブドア

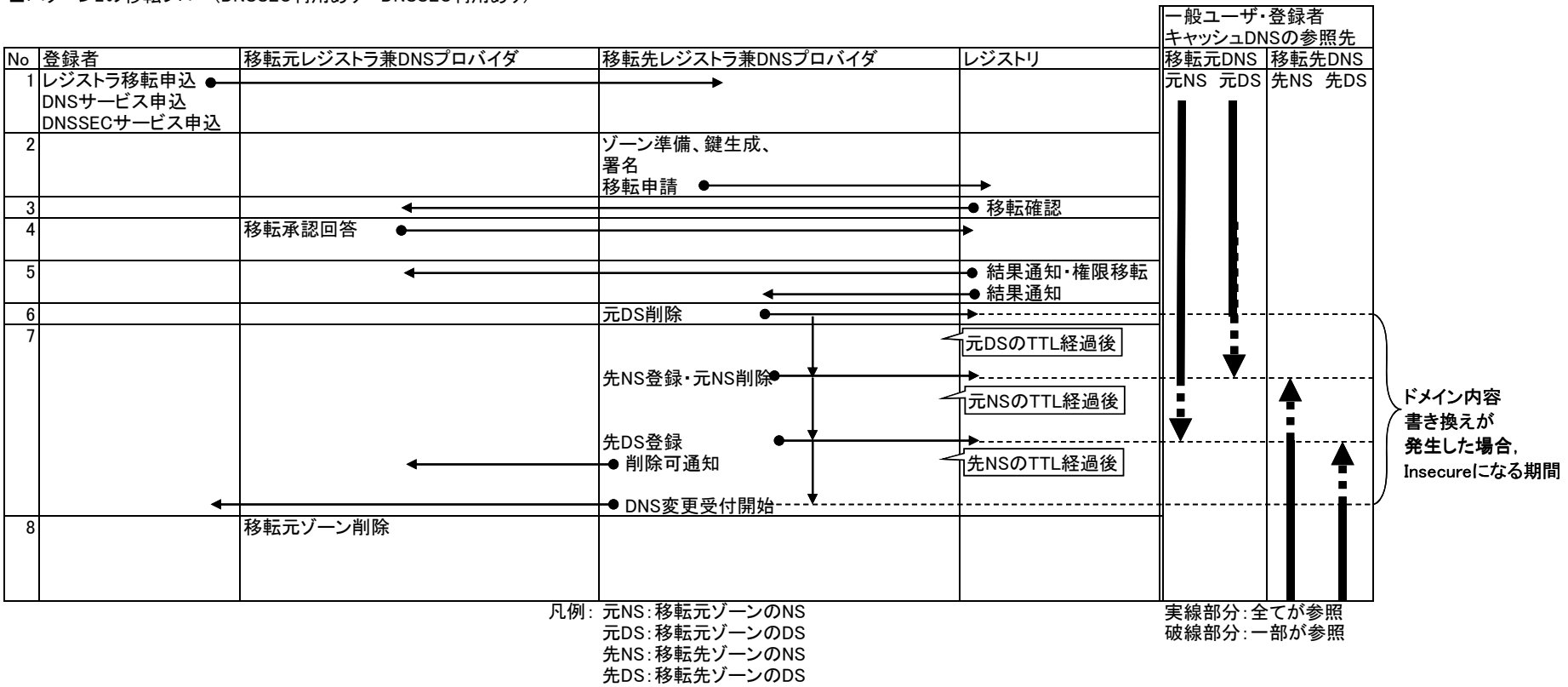
別紙　パターン別移転フロー図

平成22年11月
DNSSECジャパン

■パターン0の移転フロー（通常のレジストラ移転）



■パターン2の移転フロー（DNSSEC利用あり→DNSSEC利用あり）



■パターン3の移転フロー(DNSSEC利用なし→DNSSEC利用あり)

前提条件

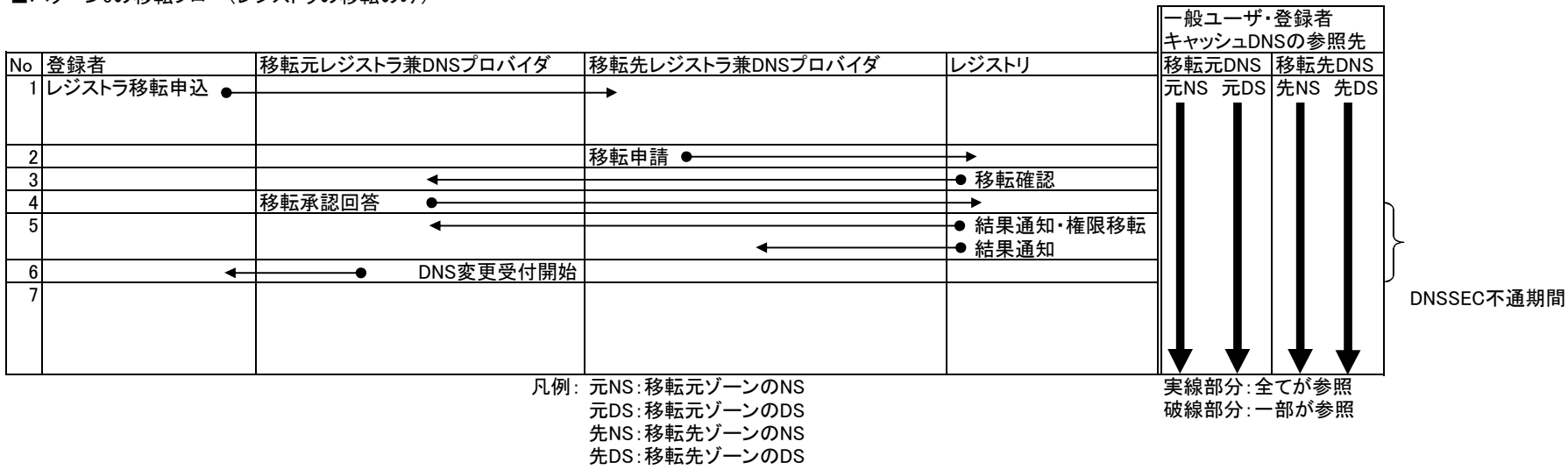
- 移転元DNSプロバイダおよび移転元レジストラは何もしない
- 移転元DNSプロバイダにより、ある程度の期間元のゾーン情報は保持される
- 各アクターはそれぞれ別エンティティとし、登録者自身がそれぞれのアクターと契約関係にあるものとする
- 移転前には登録者のドメイン名にDSは設定されていない

凡例: 元NS:移転元ゾーンのNS
元DS:移転元ゾーンのDS
先NS:移転先ゾーンのNS
先DS:移転先ゾーンのDS

実線部分:全てが参照
破線部分:一部が参照

■パターン4の移転フロー（DNSSEC利用あり→DNSSEC利用なし）

■パターン5の移転フロー（レジストラの移転のみ）



凡例：元NS：移転元ゾーンのNS
元DS：移転元ゾーンのDS
先NS：移転先ゾーンのNS
先DS：移転先ゾーンのDS

実線部分：全てが参照
破線部分：一部が参照

別紙
パターン洗い出しのための検討チャート

平成22年11月
DNSSECジャパン

レジストラ移転に伴うDNSSECの切り替え作業についての検討

前提条件

- DNSSEC対応が出来ていること(EDNSOやTCPフォールバックの問題等もクリアにしてある)
- ドメインの移転自体は問題無く行われる事。
- ここで検討する作業範囲はDNSSECの切り替えが完了するところまでとすること。
- それぞれの事業者の運用ポリシー等によるため、サービスレベルについては、検討の対象外とする。
- レジストラ移転に伴なうDNSSEC切り替えによる不通期間が生じること無く無事移転できることが、最善の方法とする。
- DNSSECにおける状態遷移「Secure/Insecure/Bogus/Indeterminate」のうちSecureを除く状態を不通期間と定義する。
  - **Insecure**:トラストチェーンのチェーンが切れている状態。木構造の一部においてDSレコードが確認できない状態。(対象アルゴリズムをサポートしていない等)
  - **Bogus**:トラストチェーンは構築されているが、検証に失敗した場合(DS情報が親に残っている、署名の消失、期限切れ等)
  - **Indeterminate**:トラストチェーン構造が無い状態。通常のDNSの状態。

■1パターン分け

DNSSEC切り替えに関係するプレイヤーを中心に考えうるパターンを洗い出す。

1 レジストラの場合
2 その他事業者の場合(NSプロバイダー)

実際には、レジストラとその他事業者のNSプロバイダとしてとして立場にあまり違いがないので、詳細についてはひとつに纏める。

移転元/移転先のパターン大別

「レジストラのNSはDNSSEC対応しないが、DSの取次だけは対応する場合」と、「NSのDNSSEC対応とDS取次ぎ対応と両方対応している場合」またはそれ以外について洗い出す。

○は有/●は無/

大別case	移転元レジストラ NS対応	移転元レジストラ DS取次ぎ	移転先レジストラ NS対応	移転先レジストラ DS取次ぎ
A	○	○	○	○
B	○	●	○	○
C	●	○	○	○
D	●	●	○	○
E	○	○	○	●
F	○	○	●	○
G	○	○	●	●
H	●	○	○	●
I	●	○	●	○
J	○	●	○	●
K	○	●	●	○
L	●	●	●	●

移転元レジストラの対応状況
- 移転元NSがDNSSEC対応も、DS取次ぎもしている
- 移転元NSはDNSSEC対応していないが、DSの取次ぎはしている
- 移転元NSはDNSSEC対応をしておらず、DSの取次ぎもしていない

移転先レジストラの対応状況
- 移転先NSはDNSSECも、DS取次ぎもしている
- 移転先NSはDNSSEC対応していないが、DSの取次ぎはしている
- 移転先NSはDNSSEC対応をしておらず、DSの取次ぎもしていない

移転元、移転先の対応状況の組み合わせで、詳細なパターンを洗い出す。
ドメインレジストラ・DNSプロバイダは同じ事業者であるという前提のため、DNSSEC対応をしていて、DS取次ぎをしないことはない。そのため、大別Case B, E, H, J, K, は詳細パターンマッチに含まれない

詳細パターンマッチ

◎移転元から移転先へそのまま移す場合　　○は有/●は無

詳細Case	移転元ネームサーバ/Zone管理者 事業者 DNSSEC	鍵交換	ユーザ DS取次ぎ	鍵交換	移転先ネームサーバ/Zone管理者 事業者 DNSSEC	鍵交換	ユーザ DS取次ぎ	鍵交換	pattern 協力的	遷移状態	パターン
1	○	○			○	○			○	Secure	1
2	○	●			○	○			−	Insecure	2
3	●				○	○			−	−	3
4	○	○			○	●			−	Insecure	2
5	○	○			●				−	Insecure/Indeterminate	4
6	○	●			○	●			−	Insecure	2
7	○	●			●				−	Insecure/Indeterminate	4
8	●				○	●			−	−	3
9	●				●				−	−	0
10			○	○	○	○			○	Secure	1
11			○	○	○	○			−	Insecure	2
12				●	○	○			−	−	3
13			○	○	○	●			−	Insecure	2
14			○	○	●				−	Insecure/Indeterminate	4
15			○	○	○	●			−	Insecure	2
16			○	○	●				−	Insecure/Indeterminate	4
17				●		○	●		−	−	3
18				●		●			−	−	0
19			○	○	○			○	−	Secure	5
20			○	○	●			○	−	Secure	5
21				●				○	−	−	3
22			○	○	○			○	−	Secure	5
23			○	○	○			●	−	Insecure/Indeterminate	4

詳細Case	移転元ネームサーバ/Zone管理者 事業者 DNSSEC	鍵交換	ユーザ DS取次ぎ	鍵交換	移転先ネームサーバ/Zone管理者 事業者 DNSSEC	鍵交換	ユーザ DS取次ぎ	鍵交換	pattern 協力的	不通期間状態	パターン
24			○	○			○	○	−	Secure	5
25			○	○				●	−	Insecure/Indeterminate	4
26				●			○	○	−	−	3
27				●				●	−	−	0
28	○	○					○	○	○	Secure	1
29	○	●					○	○	−	Insecure	2
30	●						○	○	−	−	3
31	○	○					○	○	−	Insecure	2
32	○	○						●	−	Insecure/Indeterminate	4
33	○	●					○	○	−	Insecure	2
34	○	●						●	−	Insecure/Indeterminate	4
35	●						○	○	−	−	3
36	●							●	−	−	0

◎その他の場合

詳細cas	その他	pattern 協力的	不通期間	パターン
37	移転前にDSを一度止める。移転後に再開	−	Insecure	6
38	移転前に移転先のNSを登録する。	−	Secure/Insecure	7
39	移転元のNSを利用したまま	−	Secure	5
40		−	−	
41				

※事業者のDNSSECに○がついている場合は、DSの取次ぎを行っているとみなす
※事業者のDNSSECに●がついている場合は、DSの取次ぎも行っていないとみなす
※事業者のDS取次ぎに○がついている場合は、DNSSECには対応していないとみなす
※詳細Case 19,20,22,24についてはユーザがNSを持っている状態なので、DSレコードに設定(追加・変更)があるまでは動きなし
※ここではお互いに鍵交換が可能であることを協力的と評価している

■2 パターン

1 で洗いだしたケース毎のパターンをまとめると、8つのパターンに分けられる。
それぞれのタイプを元にパターンを簡略化すると次の次の通りとなる。

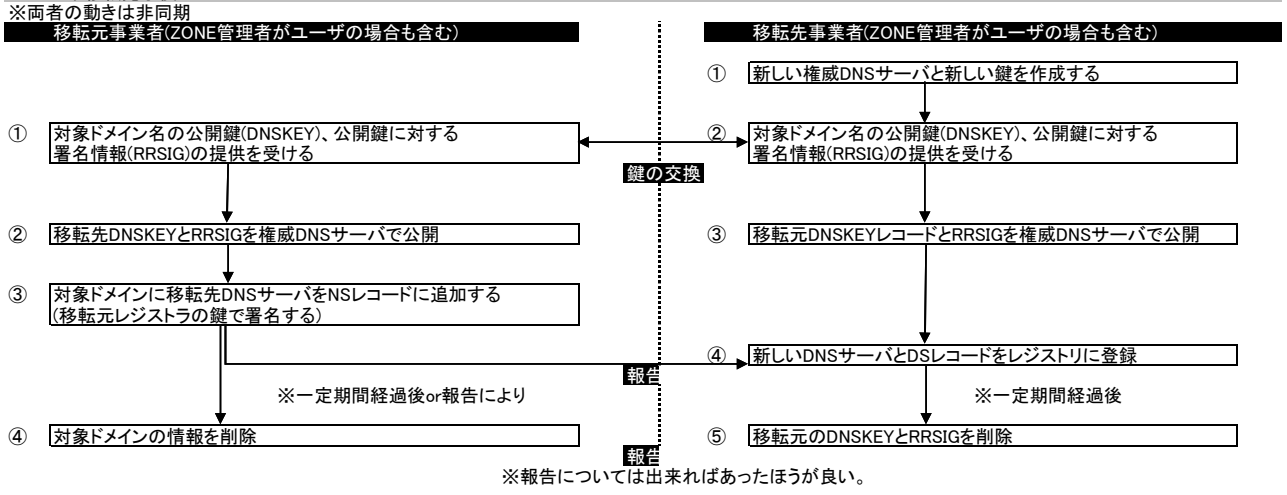
0	DNSSECを使用しない通常のレジストラ移転(Indeterminate)
1	理想的なDNSSECの切り替え。不通期間も無くDNSSECの移転が完了することができる。
2	鍵交換をしない。移転先のレジストリ情報更新に伴いInsecure。
3	新規に鍵作成をするのが、DSの登録手順に注意が必要。
4	DNSSECを終了する。移転先のレジストリ情報更新に伴いInsecure、Indeterminateとなる。
5	DS設定(追加、変更)する時まで何もしない。
6	移転前にDSを止めて、移転後に再開。DSを止めた際にDNSSECで保護されない状態となる。(Insecure)
7	移転前に移転先のNSを登録する。様々なパターンがあるので、別途検討する

※ワークフローについては4を参照

■3 RFC4641bisをベースにした場合の流れ

レジストラ移転完了後

※両者の動きは非同期



※報告については出来ればあったほうが良い。

■4 パターン別TODO(RFC4641ベース)

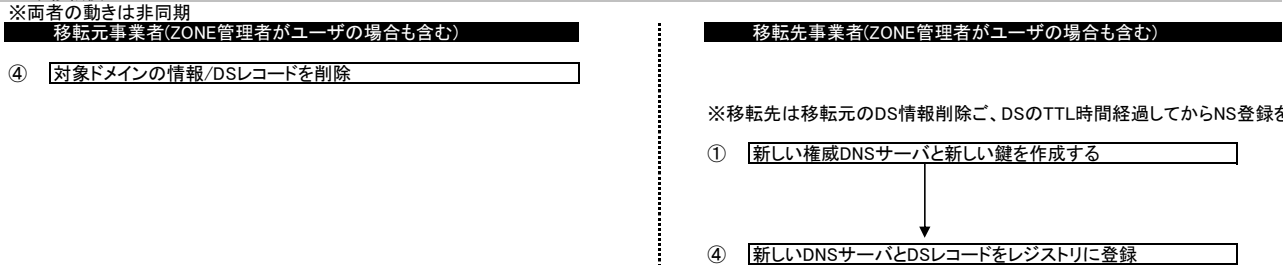
RFC4641bisをベースに考えられるパターン別アクションリスト

	移転元	移転先	
1	①,②,③,④	①,②,③,④,⑤	※パターン1はRFC4641bisベースのものと合致するため省略
2	④	①,④	
3	③	①,④*,④	
4	④	①*,④*	※「*」つきは鍵作成とDSレコード登録を除いたもの
5	–	–	※パターン5はDS情報を設定(追加・変更)するまでは何もしないため省略
6	④	①,④	
7	パターン7参照	①,④	

パターン2

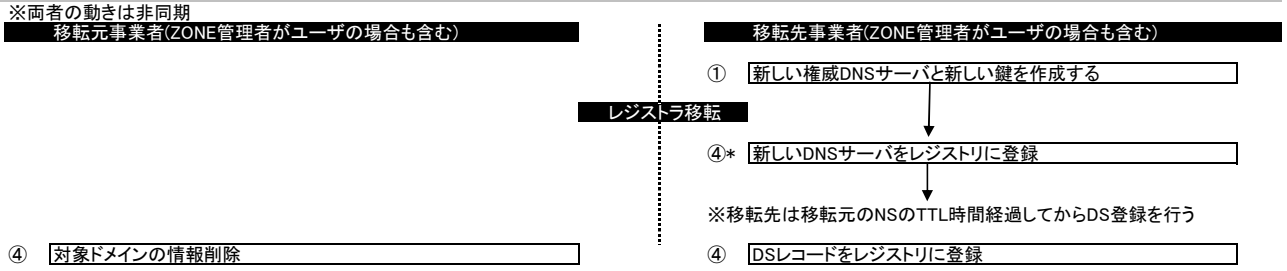
レジストラ移転後

※両者の動きは非同期



パターン3

※両者の動きは非同期



パターン4

※両者の動きは非同期

移転元事業者(ZONE管理者がユーザの場合も含む)	移転先事業者(ZONE管理者がユーザの場合も含む)
④ 対象ドメインの情報/DSレコードを削除	※移転先は移転元のDS情報削除ご、DSのTTL時間経過してからNS登録を ①* 新しい権威DNSサーバ登録 ↓ ④* 新しいDNSサーバをレジストリに登録

パターン6

移転元事業者(ZONE管理者がユーザの場合も含む)	移転先事業者(ZONE管理者がユーザの場合も含む)
④ DSレコードを削除	
レジストラ移転	※移転先は移転元のDS情報削除ご、DSのTTL時間経過してからNS登録を
	① 新しい権威DNSサーバと新しい鍵を作成する ↓ ④ 新しいDNSサーバとDSレコードをレジストリに登録

◎プロセス別詳細パターンマッチ　　○は有/●は無

case	移転	NS変更	DNSSEC		鍵交換	対応パターン	DNSSEC状態推移	備考
			移転元	移転先				
1	○	○	○	○	○	1	secure	RFC4641bis
2	○	○	○	○	●	2	一時的にinsecure	
3	○	○	○	●		4	移転以降 insecure	
4	○	○	●	○		3	移転以降 secure	
5	○	○	●	●		0	insecure (indeterminate)	従来の移転
6	○	●	○			5	secure	NS設定変更無しの場合、DNSSECのON/OFFはドメイン移転と切り離なされる。 case7,8が発生するのはレジストラがDSの取次ぎをしない場合。※下記参照
7	○	●	○⇒●			4	移転以降 insecure	
8	○	●	●⇒○			3	移転以降 secure	
9	○	●	●			0	insecure (indeterminate)	
10	●	○	○	○	○	1	secure	RFC4641bis
11	●	○	○	○	●	2	一時的にinsecure	
12	●	○	○	●		4	移転以降 insecure	
13	●	○	●	○		3	移転以降 secure	
14	●	○	●	●		0	insecure or indeterminate	従来のNS変更
15	●	●				−	−	移転もNS変更も無い。スコープ外

※鍵交換についてはどちらかが応じない場合、交換が不可能なため、移転元、移転先のどちらかは判別しない。
※DS取次ぎ不可の場合、DNSSEC対応していないと想定する。
　仮に、ユーザ独自でDNSSEC対応しているとしても、管理元のレジストラから見れば、対応していないのと同義なため。

●レジストラがDS取次ぎを行わないが、ユーザ独自でDNSSEC対応しているパターン
a) DLVにDSを登録する場合。
b) 移転元で作成したKSK、DSのセットを移転後も利用し続けている場合。

(考察)
a) NS変更ありで移転入りしてきた場合、DSはユーザが独自でDLVに登録するため、移転元でDNSSEC対応していれば、"case3"が当てはまり、
移転元でDNSSEC対応していなければ、"case5"が当てはまる。
NS変更なしで移転入りしてきた場合、既にDLVに登録されていれば、上位レジストリにDS登録されていないので、"case9"が当てはまり、
上位レジストリにDSが登録されていれば、DLV登録に変更になるため、DS削除の対応になり、"case7"が当てはまる。

b) KSK秘密鍵の受け渡しをしない前提であれば、NSの設定変更は行われないはずなので、"case7"・"case8"が当てはまる。
KSK秘密鍵の受け渡しをしてしまう場合、例外対応が必要。(上記マトリクス上は"case3"となるが、DSを削除してはいけない)