DNSSEC 技術実験報告書

運用設計編

株式会社日本レジストリサービス
http://日本レジストリサービス.jp/
http://jprs.co.jp/
2010-12-17 Ver. 1.0

目次

DNSSEC 技術実験概要 3

レジストラ移転実験 4

実験実施の背景 4
実験シナリオ 5
実験結果 15
■ *事例 1 登録者 15*
■ *事例 2 登録者の ISP 16*
■ *事例 3 移転元レジストラ 18*
■ *事例 4 移転先レジストラ 19*
■ *事例 5 レジストリ 20*
■ *事例 6 一般ユーザ 21*
■ *事例 7 一般ユーザの ISP 30*
■ *事例 8 一般ユーザの ISP 31*

業務連携検討のための FAQ 35

FAQ 作成の背景 35
FAQ 共通編 36
FAQ 個別編 44

個別実験 47

個別実験 事例 1 47
個別実験 事例 2 48
個別実験 事例 3 49

DNSSEC技術実験概要

ISP やドメイン名登録の取り次ぎを行う指定事業者が DNSSEC 対応のサービスを提供する際に、従来に比べて運用や業務連携に関して新たに検討・設計しなければならない項目がある。それら項目は多岐にわたるが、特に、運用・業務フローの面で変更が大きいドメイン名指定事業者移転については、基本的なフローと想定されるトラブルへの対応策を確立する必要がある。また、DNSSEC 対応のサービスを提供した際に顧客や一般ユーザから寄せられるであろう質問や回答を想定しておくことで、運用や業務連携を検討・設計する際の確認ポイントとすることができる。

DNSSEC 対応サービスのスムーズな導入に結びつけるため、ドメイン名指定業者移転シナリオを作成して実験を行った。また、想定される質問を洗い出し、事業者によらずに共通する項目・事業者個別の項目に分類した。

この実験を通じて、ドメイン名指定事業者移転に関する知見、および DNSSEC 対応サービスを検討・設計する際の確認ポイントを FAQ という形で得ることができた。

なお、本報告書は 2010 年 7 月～11 月に実施した実験の結果を、個別の事例としてまとめたものである。

レジストラ移転実験

実験実施の背景

ドメイン名登録者は、何らかの理由によりドメイン名登録の取り次ぎを委託している指定事業者を他の指定事業者に変更することがある。一般にそれはレジストラ移転(JP ドメイン名では指定事業者移転)と呼ばれている。多くの指定事業者では、ドメイン名登録の取り次ぎだけでなく、当該ドメイン名の名前解決を行う権威 DNS サーバのホスティング（DNS プロバイダ業務）も行っているため、レジストラ移転は登録取り次ぎ業務だけでなく DNS プロバイダ移転をともなうことが多い。

DNSSEC に対応していない(DNSSEC で署名していない)ドメイン名のレジストラ移転では、DNS プロバイダ移転をともなう場合であっても、ネームサーバ登録情報の変更を同時に行うことで、対象となるドメイン名の名前解決を途切れさせることなくスムーズに移転を行うことができる。一方、DNSSEC に対応している(DNSSEC で署名している)ドメイン名のレジストラ移転では、DNS プロバイダ移転をともなう場合はネームサーバ登録情報だけでなく署名鍵情報の変更も行う必要があり、変更順序に依存性があるため手順を誤ると対象となるドメイン名の名前解決を途切れさせる恐れがある。

DNSSEC に対応しているドメイン名の名前解決を途切れさせることなくレジストラ移転を行う手順は従来のレジストラ移転には存在していないため、指定事業者ごとに新たに設計する必要がある。標準的と考えられる手順を作成し、実際に実施して名前解決を途切れさせることなくレジストラ移転が行えることを確認すること、また、途中の手順に誤りがありトラブルが生じたときの対応を確認しておくことは、指定事業者の業務設計に有益であると考えられる。

本実験では、標準的と考えられる状況および手順をシナリオとして作成し、複数の組織がレジストラ移転に係わる関係者の役割をそれぞれ分担して、レジストラ移転をシミュレーションした。

実験シナリオ

レジストラ移転実験のシナリオを作成するにあたり、最初に移転元が DNSSEC に対応している・していない、移転先が対応している・していない、DNS プロバイダ移転が発生する・しない、レジストラ移転が発生する・しないの組み合わせについて整理し、移転元・移転先ともに DNSSEC に対応しており DNS プロバイダ移転、レジストラ移転が発生する場合を対象にすれば他の組み合わせはカバーできることを確認した。組み合わせの整理結果を図 1 に示す。

No	DNSSEC対応 移転元	DNSSEC対応 移転先	DNSプロバイダ移転	レジストラ移転	検討対象	備考
1	○	○	○	○	○	
2	○	○	○	×	○	
3	○	○	×	○		DNSSECの変更はなく従来のレジストラ移転を実施すればよい
4	○	○	×	×		DNSプロバイダ、レジストラともに移転は発生しない
5	○	×	○	○		最初にDNSSECを無効化し、移転元DSのTTL経過後以降に従来のDNSプロバイダ移転・レジストラ移転を実施するよう手順を分解すればよい(※1)
6	○	×	○	×		
7	○	×	×	○		
8	○	×	×	×		DNSプロバイダ、レジストラともに移転は発生しないため対象外
9	×	○	○	○		最初に従来のDNSプロバイダ移転・レジストラ移転を実施し、その後にDNSSECを有効化するよう手順を分解すればよい(※2)
10	×	○	○	×		
11	×	○	×	○		
12	×	○	×	×		DNSプロバイダ、レジストラともに移転は発生しない
13	×	×	○	○		DNSSECに関連しない(従来のDNSプロバイダ移転＋レジストラ移転と変わりなし)
14	×	×	○	×		DNSSECに関連しない(従来のDNSプロバイダ移転と変わりなし)
15	×	×	×	○		DNSSECに関連しない(従来のレジストラ移転と変わりなし)
16	×	×	×	×		DNSプロバイダ、レジストラともに移転は発生しない

○対応 ×非対応　　○移転あり ×移転なし

(※1)TTL経過を待たなかった場合は、名前解決に失敗する期間が生じる。また、移転先レジストラがDNSSEC対応していない場合、DNSSECを無効化せずにレジストラ移転を実施すると移転元DSの削除ができなくなる。ただし、JPドメイン名の場合はNSを更新すると自動的にDSは削除されるため、TTL問題は避けられないが大きな問題にはならない。
(※2)移転先DNSプロバイダおよび移転先レジストラともにDNSSEC対応していることが必須。DNSSECの有効化は、署名されたゾーンの公開、DSの登録の順でなければならない。

図 1 組み合わせの整理結果

次にレジストラ移転に係わる関係者の洗い出しと、レジストラ移転時に関係者間で交換される情報の洗い出しを行った。洗い出した関係者を表 1 に示す。

表 1 レジストラ移転に係わる関係者一覧

関係者名	説明
登録者	ドメイン名の登録者
登録者の ISP	登録者にインターネット接続(キャッシュ DNS サーバを含む) を提供するプロバイダ
移転元 DNS プロバイダ	移転時まで登録者が保持するドメイン名の名前解決を行う権威 DNS サーバを提供していたプロバイダ
移転元リセラ	移転時まで登録者のドメイン名登録に係わる手続きの窓口となっていた事業者
移転元レジストラ	移転時まで登録者のドメイン名登録に係わる情報を管理し、レジストリとの間で必要な情報を取り次いでいた事業者
移転先 DNS プロバイダ	移転時から登録者が保持するドメイン名の名前解決を行う権威 DNS サーバを提供するプロバイダ
移転先リセラ	移転時から登録者のドメイン名登録に係わる手続きの窓口となる事業者
移転先レジストラ	移転時から登録者のドメイン名登録に係わる情報を管理し、レジストリとの間で必要な情報を取り次ぐ事業者
レジストリ	登録されたドメイン名を一元管理し、インターネットで名前解決が可能となるよう DNS への反映を行う事業者
一般ユーザ	登録者のドメイン名で提供されるサービスにアクセスする一般の利用者
一般ユーザの ISP	一般ユーザにインターネット接続(キャッシュ DNS サーバを含む) を提供するプロバイダ

洗い出した関係者間で交換される情報を表 2 に示す。

表 2 レジストラ移転に係わる関係者間で交換される情報

分類	交換される情報	情報を交換する関係者
1.契約	DNS ホスティング申込	登録者←→移転先 DNS プロバイダ or 移転先リセラ or 移転先レジストラ (*1)
	DNS ゾーン設定依頼	
	DNSSEC 利用申込	
	移転元 DNS ホスティング契約終了申込	登録者←→移転元 DNS プロバイダ
	移転元レジストラ契約終了申込	登録者←→移転元リセラ or 移転元レジストラ (*2)
2.レジストラ移転	レジストラ移転申込	登録者→移転先リセラ→移転先レジストラ→レジストリ (*2)
	レジストラ移転承認依頼・通知	レジストリ←→移転元レジストラ←→移転元リセラ左→登録者 (*2)
	レジストラ移転完了通知	レジストリ→移転元レジストラ レジストリ→移転先レジストラ→移転先リセラ→登録者 (*2)
3.DNSプロバイダ移転	移転先 DS 情報提供依頼	登録者←→移転先リセラ←→移転先レジストラ
	移転元 DS 設定有無確認	移転先レジストラ←→レジストリ
	移転先 NS 設定依頼	
	移転元 NS 削除依頼	
	移転先 DS 設定依頼	
	移転元 DS 削除依頼	
4.名前解決	ドメイン名名前解決	登録者←→登録者の ISP 一般ユーザ←→一般ユーザの ISP

(*1) 移転先リセラや移転先レジストラが DNS プロバイダを兼ねる場合があるため

(*2) 移転先リセラが存在せず移転先レジストラが登録者との窓口を持つ場合があり、その場合は、移転先リセラは省略される。移転元についても同様

これらに基づき、全ての関係者が独立している最も複雑なモデルでのレジストラ移転シナリオ（ 表 3「複雑なモデルでの移転シナリオ」）とフロー図（図 2 「複雑なモデルでの移転フロー図」）を作成した。シナリオには、想定されるトラブルも含めた。さらに、日本ではホスティング事業者が指定事業者を兼ねることが多いため、現実的なモデルとして移転元・移転先ともに指定事業者が DNS プロバイダを兼ね、リセラを置かない場合のシナリオ（ 表 4「現実的なモデルでの移転シナリオ」）を作成した。

表 3 複雑なモデルでの移転シナリオ

前提	
	移転元レジストラと移転先レジストラは鍵情報を交換しない
	レジストラ移転・DNSプロバイダ移転の期間もDNSの委任状態は連続させる(そのためDNSSECの連鎖は一時切断する)

登場人物	
	登録者
	登録者のISP(キャッシュDNS)
	移転元DNSプロバイダ
	移転元リセラ
	移転元レジストラ
	移転先DNSプロバイダ
	移転先リセラ
	移転先レジストラ
	レジストリ
	一般ユーザ
	一般ユーザのISP(キャッシュDNS)

想定するシナリオ

Ⅰ　移転先DNSプロバイダプロバイダにDNSを設定してもらう

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
1	登録者	移転先DNSプロバイダ	1. DNSホスティング申込		
2	移転先DNSプロバイダ	登録者	1. DNSホスティング申込	DNSサーバ情報(NS情報)も通知される	
3	登録者	移転先DNSプロバイダ	1. DNSゾーン設定依頼		
4	移転先DNSプロバイダ	登録者	1. DNSゾーン設定依頼		
5	登録者	移転先DNSプロバイダ	1. DNSSEC利用申込		
6	移転先DNSプロバイダ	登録者	1. DNSSEC利用申込	DNSSEC情報(DS情報)も通知される	

Ⅱ　レジストラ変更(レジストラ移転)を行う

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
7	登録者	移転先リセラ	2. レジストラ移転申込		
8	移転先リセラ	移転先レジストラ	2. レジストラ移転申込		
9	移転先レジストラ	レジストリ	2. レジストラ移転申込		
10	レジストリ	移転元レジストラ	2. レジストラ移転承認依頼・通知		
11	移転元レジストラ	移転元リセラ	2. レジストラ移転承認依頼・通知		
12	移転元リセラ	登録者	2. レジストラ移転承認依頼・通知		
13	登録者	移転元リセラ	2. レジストラ移転承認依頼・通知		
14	移転元リセラ	移転元レジストラ	2. レジストラ移転承認依頼・通知		
15	移転元レジストラ	レジストリ	2. レジストラ移転承認依頼・通知		
16	レジストリ	移転先レジストラ	2. レジストラ移転完了通知	ドメイン名設定の権限が移転先に移行する	
17	レジストリ	移転元レジストラ	2. レジストラ移転完了通知		
18	移転先レジストラ	移転先リセラ	2. レジストラ移転完了通知		
19	移転先リセラ	登録者	2. レジストラ移転完了通知		

Ⅲ　DNS設定情報の変更(DNSプロバイダ移転)を行う

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
20	登録者	移転先リセラ	3. 移転先NS設定依頼		
21	移転先リセラ	移転先レジストラ	3. 移転先NS設定依頼		
22	移転先レジストラ	レジストリ	3. 移転元DS設定有無確認	**移転先レジストラが自発的に行うアクション**	移転先レジストラがDS設定有無を確認せずにNS設定変更申請を出し、一般ユーザが登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが元DSの削除申請を出し、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
23	レジストリ	移転先レジストラ	3. 移転元DS設定有無確認		
24	移転先レジストラ	移転先リセラ	3. 移転先DS情報提供依頼	移転先レジストラは移行手順をリセラに説明する	
25	移転先リセラ	登録者	3. 移転先DS情報提供依頼	移転先リセラは移行手順を登録者に説明する	
26	登録者	移転先リセラ	3. 移転先DS設定依頼		
27	移転先リセラ	移転先レジストラ	3. 移転先DS設定依頼		
28	移転先レジストラ	レジストリ	3. 移転元DS削除依頼		
29	レジストリ	移転先レジストラ	3. 移転元DS削除依頼		
30	移転先レジストラ		元DSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
31	移転先レジストラ	レジストリ	3. 移転元NS削除・移転先NS設定依頼		移転先レジストラが元DSのTTL時間待たずにNS設定を変更し、登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが先DSの登録申請を出し、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
32	レジストリ	移転先レジストラ	3. 移転元NS削除・移転先NS設定依頼		
33	移転先レジストラ		元NSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
34	移転先レジストラ	レジストリ	3. 移転先DS設定申請		移転先レジストラが元NSのTTL時間を待たずに先DSを登録し登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
35	レジストリ	移転先レジストラ	3. 移転先DS設定申請		
36	移転先レジストラ		先NSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
37	移転先レジストラ	移転先リセラ	3. 移転先DS設定申請		登録者ドメイン名のゾーンにCNAMEがあり、CNAMEの先がDNSSEC非対応の外部ドメイン名のため、一般ユーザが登録者ドメイン名がDNSSEC対応していないと登録者に苦情を言う/ 登録者はCNAMEをやめてA/AAAAに変更する
38	移転元リセラ	登録者	3. 移転先DS設定申請		

Ⅳ　移転元リセラ・レジストラ、移転元DNSプロバイダを解約する

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
39	登録者	移転元リセラ	1. 移転元レジストラ契約終了申込		
40	移転元リセラ	登録者	1. 移転元レジストラ契約終了申込		
41	登録者	移転元DNSプロバイダ	1. 移転元DNSプロバイダ契約終了申込		
42	移転元DNSプロバイダ	登録者	1. 移転元DNSプロバイダ契約終了申込		
43	移転元DNSプロバイダ		登録者ゾーンデータ削除		

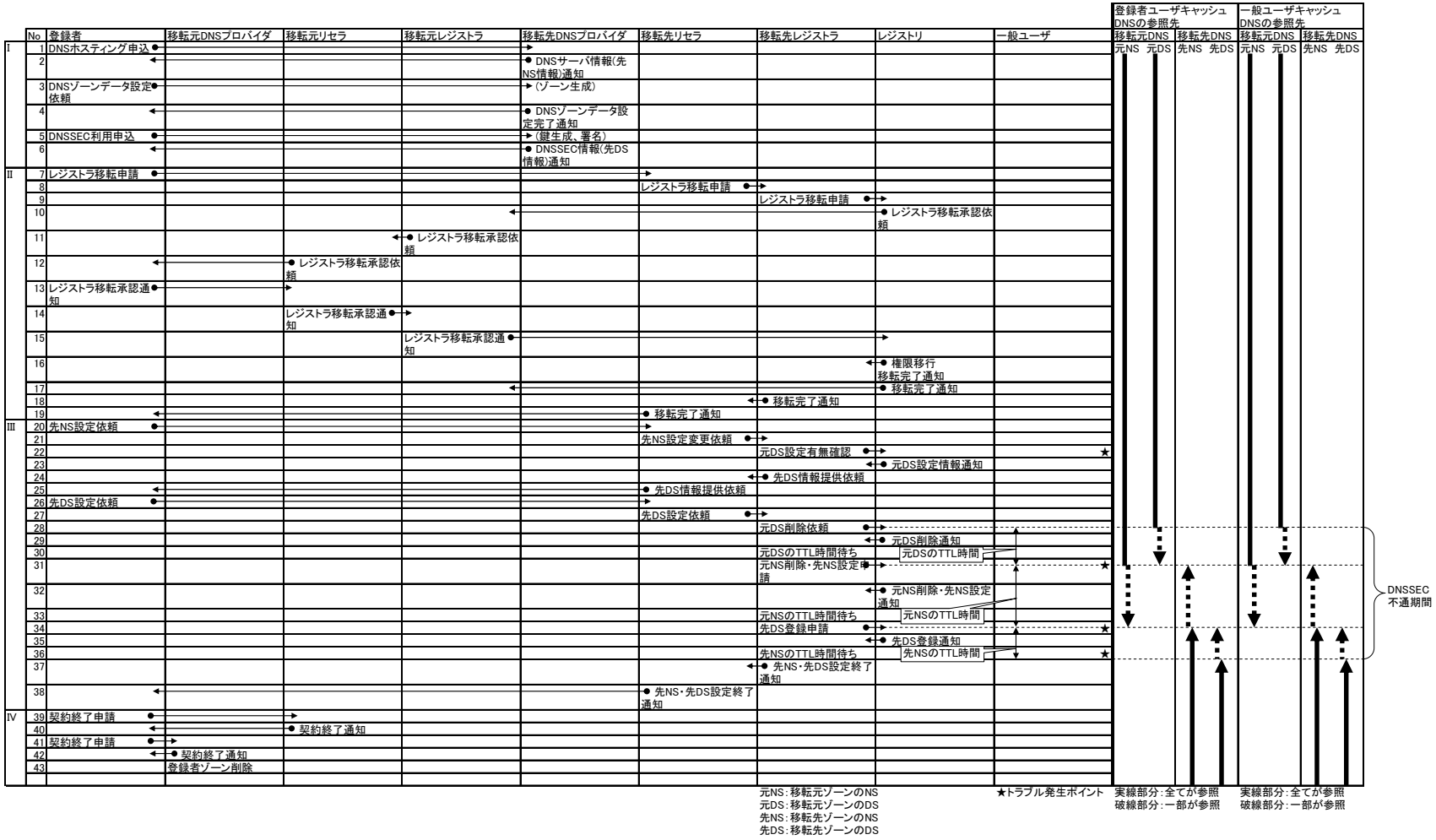


図 2 複雑なモデルでの移転フロー図

表 4 現実的なモデルでの移転シナリオ

前提	
	移転元レジストラと移転先レジストラは鍵情報を交換しない
	レジストラ移転・DNSプロバイダ移転の期間もDNSの委任状態は連続させる(そのためDNSSECの連鎖は一時切断する)
	DNSプロバイダを兼ねる移転元レジストラはレジストラ移転後もすぐには登録者ゾーンデータは削除しない

登場人物	
	登録者
	登録者のISP(キャッシュDNS)
	移転元レジストラ(移転元DNSプロバイダを兼ねている)
	移転先レジストラ(移転先DNSプロバイダを兼ねている)
	レジストリ
	一般ユーザ
	一般ユーザのISP(キャッシュDNS)

想定するシナリオ

Ⅰ　移転先DNSプロバイダプロバイダにDNSを設定してもらう

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
1	登録者	移転先レジストラ	1. DNSホスティング申込		
2	移転先レジストラ	登録者	1. DNSホスティング申込	DNSサーバ情報(NS情報)も通知される	
3	登録者	移転先レジストラ	1. DNSゾーン設定依頼		
4	移転先レジストラ	登録者	1. DNSゾーン設定依頼		
5	登録者	移転先レジストラ	1. DNSSEC利用申込		
6	移転先レジストラ	登録者	1. DNSSEC利用申込	DNSSEC情報(DS情報)も通知される	

Ⅱ　レジストラ変更(レジストラ移転)を行う

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
7	登録者	移転先レジストラ	2. レジストラ移転申込		
8					
9	移転先レジストラ	レジストリ	2. レジストラ移転申込		
10	レジストリ	移転元レジストラ	2. レジストラ移転承認依頼・通知		
11					
12	移転元レジストラ	登録者	2. レジストラ移転承認依頼・通知		
13	登録者	移転元レジストラ	2. レジストラ移転承認依頼・通知		
14					
15	移転元レジストラ	レジストリ	2. レジストラ移転承認依頼・通知		
16	レジストリ	移転先レジストラ	2. レジストラ移転完了通知	ドメイン名設定の権限が移転先に移行する	
17	レジストリ	移転元レジストラ	2. レジストラ移転完了通知		
18					
19	移転先レジストラ	登録者	2. レジストラ移転完了通知	移転先レジストラはDNSプロバイダ移行手順を登録者に説明する	

Ⅲ　DNS設定情報の変更(DNSプロバイダ移転)を行う

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
20					
21					
22	移転先レジストラ	レジストリ	3. 移転元DS設定有無確認	**移転先レジストラが自発的に行うアクション**	移転先レジストラがDS設定有無を確認せずにNS設定変更申請を出し、一般ユーザが登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが元DSの削除申請を出し、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
23	レジストリ	移転先レジストラ	3. 移転元DS設定有無確認		
24					
25					
26					
27					
28	移転先レジストラ	レジストリ	3. 移転元DS削除依頼		
29	レジストリ	移転先レジストラ	3. 移転元DS削除依頼		
30	移転先レジストラ		元DSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
31	移転先レジストラ	レジストリ	3. 移転元NS削除・移転先NS設定依頼		移転先レジストラが元DSのTTL時間待たずにNS設定を変更し、登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが先DSの登録申請を出し、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
32	レジストリ	移転先レジストラ	3. 移転元NS削除・移転先NS設定依頼		
33	移転先レジストラ		元NSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
34	移転先レジストラ	レジストリ	3. 移転先DS設定申請		移転先レジストラが元NSのTTL時間を待たずに先DSを登録し登録者ドメイン名のサーバにアクセスできなくなる/ 移転先レジストラが、一般ユーザのISPに登録者ドメイン名のキャッシュクリアを依頼する
35	レジストリ	移転先レジストラ	3. 移転先DS設定申請		
36	移転先レジストラ		先NSのTTL時間待ち	**移転先レジストラが自発的に行うアクション**	
37	移転先レジストラ	登録者	3. 移転先DS設定申請		登録者ドメイン名のゾーンにCNAMEがあり、CNAMEの先がDNSSEC非対応の外部ドメイン名のため、一般ユーザが登録者ドメイン名がDNSSEC対応していないと登録者に苦情を言う/ 登録者はCNAMEをやめてA/AAAAに変更する
38					

Ⅳ　移転元リセラ・レジストラ、移転元DNSプロバイダを解約する

No	情報発信者	情報受信者	交換される情報	補足説明	発生トラブル/対応
39	登録者	移転元レジストラ	1. 移転元レジストラ契約終了申込	DNSプロバイダ契約終了申込も兼ねる	
40	移転元レジストラ	登録者	1. 移転元レジストラ契約終了申込		
41					
42					
43	移転元レジストラ		登録者ゾーンデータ削除		

以上を踏まえて、具体的な実験の詳細シナリオとして以下の 5 シナリオを用意した。

1. 正常系
   現実的なモデルでの移転シナリオを実施する
2. 異常系 1
   移転元 DS を削除せずに、移転先 NS を設定し移転元 NS を削除する
3. 異常系 2
   移転元 DS を削除した後の TTL 経過待ちをせずに、移転先 NS を設定し移転元 NS を削除する
4. 異常系 3
   移転先 NS を設定し移転元 NS を削除した後の TTL 経過待ちをせずに、移転先 DS を設定する
5. 異常系 4
   DNSSEC 署名されているゾーンに含まれる CNAME の指す先が DNSSEC 署名されておらず、名前(アドレス)解決時に AD ビットが立たない(DNS の仕様通りの動作であるが、利用者から見ると DNSSEC 対応しているはずの名前が対応していないように見える)

実験では crisp.jp を仮想 TLD(レジストリ)とし、その配下のドメイン名である transfer.crisp.jp を移転対象ドメイン名として移転元レジストラから移転先レジストラに移転した。図 3 に実験環境構成を示す。

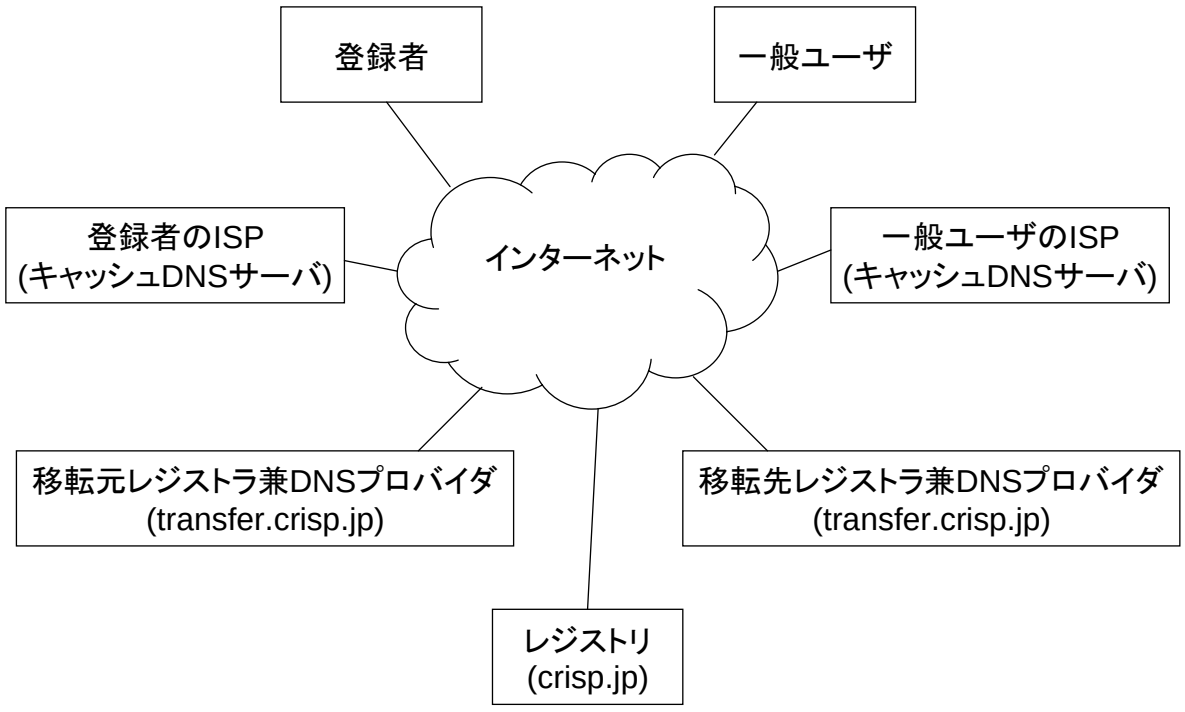


図 3 実験環境構成

また、表 5～9 に詳細シナリオ(正常系、異常系 1～5)を示す。なお、本節で示す詳細シナリオ中の時間は、実験開始からの予定経過時間を表しているが、実験結果の節で示す個別事例の時間は実験実施の際の実時間となっている。

表 5 詳細シナリオ(正常系)

I 移転先DNSプロバイダプロバイダにDNSを設定してもらう		
時間	No	作業
0:00	---	正常系の開始
0:01	1	登録者が移転先レジストラにtransfer.crisp.jpのホスティングを依頼する
0:02	2	移転先レジストラが登録者に受注した旨のAckを返す 同時に、NS情報も返す
0:03	3	登録者が移転先レジストラにtransfer.crisp.jpのゾーンデータ設定を依頼する
0:04	4	移転先レジストラが登録者に設定した旨のAckを返す
0:05	5	登録者が移転先レジストラにDNSSEC利用を申請する
0:06	6	移転先レジストラが登録者に署名した旨のAckを返す

II レジストラ変更(レジストラ移転)を行う		
時間	No	作業
0:10	7	登録者が移転先レジストラにtransfer.crisp.jpの指定事業者移転を申請する
0:11	9	移転先レジストラがレジストリにtransfer.crisp.jpの指定事業者移転を申請する
0:12	10	レジストリが移転元レジストラにtransfer.crisp.jpの指定事業者移転承認を依頼する
0:13	12	移転元レジストラが登録者にtransfer.crisp.jpの指定事業者移転承認を依頼する
0:14	13	登録者が移転元レジストラにtransfer.crisp.jpの指定事業者移転承認を通知する
0:15	15	移転元レジストラがレジストリに簡易登録システムの移転機能を使ってtransfer.crisp.jpを渡した上で、指定事業者移転承認を通知
0:20	16	レジストリが移転先レジストラに簡易登録システムの移転機能を使ってtransfer.crisp.jpを渡した上で、指定事業者移転完了を通知
0:25	---	移転先レジストラはtransfer.crisp.jpの管理権限が自分に移ったことを確認する
0:25	17	レジストリが移転元レジストラにtransfer.crisp.jpの指定事業者移転完了を通知する
0:26	19	移転先レジストラが登録者にtransfer.crisp.jpの指定事業者移転完了を通知する 同時に、移転先レジストラは登録者にDNSプロバイダ移転の手順を説明する(説明します旨のメッセージを送るのみ)

III DNS設定情報の変更(DNSプロバイダ移転)を行う		
時間	No	作業
0:30	22	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元DSを確認する あと(異常系の準備)で使うので、元DSの値をコピーしておく
0:31	28	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元DSを削除する
0:32	30	移転先レジストラは元DSのTTL時間(10分)待つ
0:42	31	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元NSを削除し、先NSを追加する あと(異常系の準備)で使うので、元NSの値をコピーしておく
0:43	33	移転先レジストラは元NSのTTL時間(5分)待つ
0:48	34	移転先レジストラは簡易登録システムでtransfer.crisp.jpの先DSを追加する
0:49	36	移転先レジストラは先NSのTTL時間(5分)待つ
0:54	37	移転先レジストラが登録者に指定事業者移転・プロバイダ移転完了を通知する

IV 移転元リセラ・レジストラ、移転元DNSプロバイダを解約する		
時間	No	作業
0:55	39	登録者が移転元レジストラにホスティングおよびレジストラ契約の終了を申し込む
0:56	40	移転元レジストラが登録者に契約終了した旨のAckを返す
0:57	---	正常系の終了

※Noの数字は表3のNoに一致する。---は一致しない項目。

表 6 詳細シナリオ(異常系 1)

III DNS設定情報の変更(DNSプロバイダ移転)を行う		
時間	No	作業
0:00	---	異常系1の開始
0:01	---	一般ユーザはwww.transfer.crisp.jpの名前解決を行う Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ
0:02	31	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元NSを削除し、先NSを追加する
0:03	---	全員、元NSのTTL時間(5分)待つ
0:08	---	一般ユーザはtransfer.crisp.jpの名前解決が失敗することを確認する(キャッシュは元DSと先NSになっている) Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR http://dnsviz.net/ ← transfer.crisp.jpのリンク状況を確認しておく
0:09	---	一般ユーザは登録者に名前が引けないことを通知する
0:10	---	登録者は移転先レジストラに名前が引けないことを通知する
0:11	28 34	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元DSを削除する 同時に、移転先レジストラは簡易登録システムでtransfer.crisp.jpの先DSを登録する
0:12	---	移転先レジストラは登録者ISPと一般ユーザISPにtransfer.crisp.jpのキャッシュクリアを依頼する
0:13	---	登録者ISPと一般ユーザISPはtransfer.crisp.jpのキャッシュをクリアする Ex. rndc flushname transfer.crisp.jp
0:14	---	一般ユーザはtransfer.crisp.jpの名前解決が成功することを確認する Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR
0:15	---	異常系1の終了

※Noの数字は表3のNoに一致する。--は一致しない項目。

表 7 詳細シナリオ(異常系 2)

III DNS設定情報の変更(DNSプロバイダ移転)を行う		
時間	No	作業
0:00	---	異常系2の開始
0:01	---	一般ユーザはwww.transfer.crisp.jpの名前解決を行う Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ
0:02	28	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元DSを削除する 同時に、移転先レジストラは簡易登録システムでtransfer.crisp.jpの元NSを削除し、先NSを追加する
0:03	---	全員、元NSのTTL時間(5分)待つ
0:08	---	一般ユーザはtransfer.crisp.jpの名前解決が失敗することを確認する(キャッシュは元DSと先NSになっている) Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR http://dnsviz.net/ ← transfer.crisp.jpのリンク状況を確認しておく
0:09	---	一般ユーザは登録者に名前が引けないことを通知する
0:10	---	登録者は移転先レジストラに名前が引けないことを通知する
0:11	34	移転先レジストラは簡易登録システムでtransfer.crisp.jpの先DSを追加する
0:12	---	移転先レジストラは登録者ISPと一般ユーザISPにtransfer.crisp.jpのキャッシュクリアを依頼する
0:13	---	登録者ISPと一般ユーザISPはtransfer.crisp.jpのキャッシュをクリアする Ex. rndc flushname transfer.crisp.jp
0:14	---	一般ユーザはtransfer.crisp.jpの名前解決が成功することを確認する Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR
0:15	---	異常系2の終了

※Noの数字は表3のNoに一致する。--は一致しない項目。

表 8 詳細シナリオ(異常系 3)

Ⅲ DNS設定情報の変更(DNSプロバイダ移転)を行う		
時間	No	作業
0:00	--	異常系3の開始
0:01	31	移転先レジストラは簡易登録システムでtransfer.crisp.jpの元NSを削除し、先NSを追加する
0:02	--	登録者ISPはwww.transfer.crisp.jpの名前解決を行う Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ
0:03	34	移転先レジストラは簡易登録システムでtransfer.crisp.jpの先DSを追加する
0:04	--	登録者ISPはtransfer.crisp.jpの名前解決が失敗することを確認する(キャッシュは先DSと元NSになっている) Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR http://dnsviz.net/ ← transfer.crisp.jpのリンク状況を確認しておく
0:05	--	登録者ISPは登録者に名前が引けないことを通知する
0:06	--	登録者は移転先レジストラに名前が引けないことを通知する
0:07	--	移転先レジストラは登録者ISPと一般ユーザISPにtransfer.crisp.jpのキャッシュクリアを依頼する
0:08	--	登録者ISPと一般ユーザISPはtransfer.crisp.jpのキャッシュをクリアする Ex. rndc flushname transfer.crisp.jp
0:09	--	登録者ISPはtransfer.crisp.jpの名前解決が成功することを確認する Ex. dig +dnssec www.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR
0:10	--	異常系3の終了

※Noの数字は表3のNoに一致する。--は一致しない項目。

表 9 詳細シナリオ(異常系 4)

Ⅲ DNS設定情報の変更(DNSプロバイダ移転)を行う		
時間	No	作業
0:00	--	異常系4の開始
0:01	--	一般ユーザはwww.transfer.crisp.jpの名前解決を行う Ex. dig +dnssec alias.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR、ADビットなし
0:02	--	一般ユーザは登録者にalias.transfer.crisp.jpはDNSSECで保護されていないことを通知する
0:03	--	登録者は移転先レジストラにalias.transfer.crisp.jpのCNAMEをやめてA/AAAAに変更することを依頼する
0:04	--	移転先レジストラはalias.transfer.crisp.jpを変更する
0:09	--	一般ユーザはalias.transfer.crisp.jpがDNSSECで保護されていることを確認する Ex. dig +dnssec alias.transfer.crisp.jp @一般ユーザISPのキャッシュDNSサーバ ← NOERROR、ADビットあり
0:10	--	異常系4の終了

※Noの数字は表3のNoに一致する。--は一致しない項目。

実験結果

本実験では、作業の効率を考慮して DS の TTL を 600 秒、NS の TTL を 300 秒（ただし、上位ゾーン内の TTL は 600 秒)とした環境を使用した。したがって、以下の結果報告は実験環境における事例である。

■ 事例 1 登録者

・ 実験環境

・ 実験結果概要

詳細シナリオ通りに進めることができた

・ 実験結果詳細

正常系

- DNS の委任が途切れなかった
- DNSSEC の委任が切れている期間は想定通り
- 名前解決は成功した

異常系

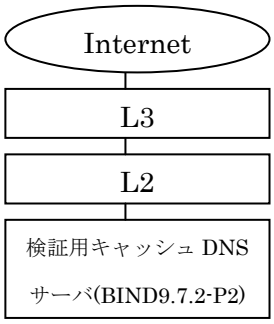
- DNSSEC の不整合(名前解決失敗)は復旧した
- alias.transfer.crisp.jp の CNAME を A/AAAA に修正して DNSSEC 検証は成功するようになった

・ 得られた知見

移転の手続きをおこなうにあたり、エンドユーザ及び各業者間での責任分界の難しさを感じた。

■ 事例 2 登録者の ISP

・ 実験環境



・ 実験結果概要

当社担当の登録者 ISP のキャッシュ DNS サーバでは、詳細シナリオ通りに進んだ。
ただし、30 秒間隔で取得したログを確認したところ、各シナリオ開始時のキャッシュクリアできていないオペミスがあった。（恐らく、実験対象外のキャッシュ DNS サーバのキャッシュをクリアしたものと思われる。）

・ 実験結果詳細

① 正常系
DNS 委任の途切れ：なし
DNSSEC 委任の切断時間：想定とおり
名前解決：成功

② 異常系 1
キャッシュクリアによる不整合からの復旧：成功

③ 異常系 2
キャッシュクリアによる不整合からの復旧：成功

④ 異常系 3
キャッシュクリアによる不整合からの復旧：成功

⑤ 異常系 4
作業なし

・ 得られた知見

登録者 ISP として想定の通り、キャッシュ DNS のキャッシュクリアすることで不整合からの復旧確認を行うことができた。
また、各シナリオ開始時のキャッシュクリアの実施はできていなかったが、SERVFAIL のステータスは TTL が切れた時点で反映されていたことを確認した。

■ 事例 3 移転元レジストラ

・ 実験環境

OS：FreeBSD 7.1 x86 / KVM 上のゲスト OS
権威 DNS サーバ：ANS 5.1 for FreeBSD

・ 実験結果概要

詳細シナリオ通りに滞りなく進めることができた。

・ 実験結果詳細

正常系 レジストラ移転：シナリオの想定通りに完了した。
正常系 プロバイダ移転：シナリオの想定通りに完了した。
異常系：移転元において対応が必要になる事象は発生しなかった。

・ 得られた知見

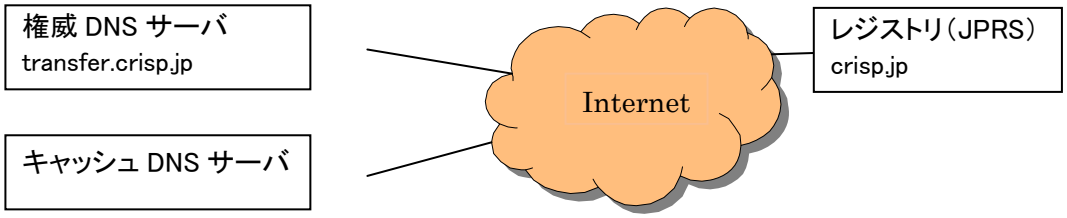
移転元レジストラとしては 変更される部分はないということが確認できたと思う。
移転先レジストラにおいては 作業そのもの、または異常が発生した際の対応が今まで以上に煩雑になる感じがした。

今回は DNS プロバイダとレジストラが同一事業者という想定で行ったものではあるが現実問題としては それぞれ別々の事業者になり一層煩雑になることが想定されるため障害対応フローとしての指針が必要ではないかと感じた。

■ 事例 4 移転先レジストラ

・ 実験環境

DNSSEC 対応の権威 DNS サーバとキャッシュ DNS サーバを設置し、権威 DNS サーバ内に移転試験用ドメイン「transfer.crisp.jp」のゾーンを登録



・ 実験結果概要

JPRS 提供のレジストラ移転実験詳細シナリオにそって、ドメイン名の移転と DNS プロバイダの移転試験を正常系・異常系ともに問題なく完了した。

・ 実験結果詳細

正常系

レジストラの移転	異常なし
DNS プロバイダ移転	異常なし

異常系

異常系 1	元 DS＋先 NS で不一致	異常なし
異常系 2	DS 無＋先 NS で不一致	異常なし
異常系 3	先 DS＋元 NS で不一致	異常なし
異常系 4	CNAME の先が DNSSEC 非対応でエラー	異常なし

・ 得られた知見

・NS 変更後、TTL 時間待機を行ってもキャッシュ DNS サーバへ十分に伝播しないことがあった。

・実際の移転時、本実験の手順をどこまでエンドユーザにやってもらうか、またどの程度詳細に案内するかの判断の難しさを感じた。

■ 事例 5 レジストリ

・ 実験環境

レジストリ作業(実験対象ドメイン名のゾーン管理権限を変更するためのシステムにアクセスする)ための端末を使用し、インターネット経由で参加した。
また、DNS の委任状態、名前解決の連続性を確認するために実験対象ドメイン名の名前解決が可能なキャッシュ DNS サーバを用意し、一定間隔でクエリを送信して状態を記録した。

・ 実験結果概要

正常系のシナリオ通りにレジストラ移転を進めれば、問題なく移転できることが確認できた。また、異常系で想定したように、キャッシュ DNS サーバにキャッシュされている NS と DS にねじれ(一方が移転元、他方が移転先)の状態が生じると DNSSEC で検証を行っている場合に名前解決が失敗(SERVFAIL)することが確認できた。

・ 実験結果詳細

正常系については、シナリオ通りに進みレジストラ移転が問題なく実施できることを確認した。
異常系については、レジストリとしては作業がなかったため問題はなかった。ただし、一定間隔でクエリを送信し名前解決の連続性を確認した記録からは、異常系シナリオ 3 で想定された名前解決の失敗(SERVFAIL)は記録されていなかった。これは、シナリオ進行が想定通りに行かず NS と DS のねじれ状態が生じなかったためと考えられる。

・ 得られた知見

異常系では NS と DS の TTL のみを対象にキャッシュの状態を検討しトラブルを想定していたが、DNSKEY や RRSIG など他の DNSSEC に関連するレコードがそれぞれ異なるタイミングでキャッシュされている可能性を考慮すべきであった。キャッシュ DNS サーバの実装によっては、それらレコードの TTL が切れた時点で NS や DS を引き直すことが考えられる(BIND や Unbound でそのような挙動が見られる)。小規模かつ TTL の短い実験用ゾーンで理屈通りにトラブルを再現するのは難しい。また、上記から、DNSSEC に関連するレコードの TTL は NS の TTL 以下にしておくのがよいと考えられる。

■ 事例 6 一般ユーザ

・ 実験環境

使用した機器：NEC 製サーバ
ネットワーク：100M/FULL でインターネットに接続
使用した DNS：BIND-9.7.2-P2
実験環境：上記サーバから 2 台の ISP キャッシュ DNS サーバに対して、30 秒毎に下記のコマンドを実施

```
dig +dnssec www.transfer.crisp.jp @キャッシュ DNS サーバ
dig +dnssec alias.transfer.crisp.jp @キャッシュ DNS サーバ
dig +dnssec +cd www.transfer.crisp.jp @キャッシュ DNS サーバ
dig +dnssec +cd alias.transfer.crisp.jp @キャッシュ DNS サーバ
```

・ 実験結果概要

正常系：
1 台のキャッシュ DNS サーバでは問題なくレジストラ移転が行われたが、もう 1 台のキャッシュ DNS サーバでは、移転元 DS が削除され移転先の NS が登録されても検証が OK であり続けたという事象が発生し、シナリオ通りの結果が得られなかった。

異常系１：
1 台のキャッシュ DNS サーバではシナリオ通りの結果が得られたが、もう 1 台のキャッシュ DNS サーバでは、SERVFAIL 後のキャッシュクリアが不完全といった事象が発生し、シナリオ通りの結果が得られなかった。

異常系２：
NS の TTL 時間によって、キャッシュ DNS サーバ毎の応答が変化した。
1 台のキャッシュ DNS サーバではシナリオ通りの結果が得られたが、もう 1 台のキャッシュ DNS サーバでは、予期しない SERVFAIL が発生するなどし、シナリオ通りの結果が得られなかった。

異常系３：
実験開始当初より異常な状態が続いており、両キャッシュ DNS サーバにおいてシナリオ通りの結果が得られなかった。

異常系４：
シナリオ通りの結果が得られた。

・ 実験結果詳細

正常系：
・キャッシュ DNS サーバ２はシナリオ通りにレジストラ移転が完了した。

・キャッシュ DNS サーバ１の+dnssec alias に異常が見受けられたが、FW の問題であることが確認されたため、考慮に含めないこととした。

・検証 OK のゾーンの場合、移転元 DNS からの+cd の応答フラグは qr rd ra cd だが、移転先では qr rd ra ad cd であったため、DNS サーバ毎に応答の違いが見て取れる。

・DS の TTL が切れた後も検証が OK となっている事象が確認された。さらに、NS が切り替わった際にも RRSIG には変化がなく、検証 OK であり続けた事象が見受けられた。その後何回か TTL が切れるものの RRSIG に変化なし。13:51 の TTL 切れにてようやく RRSIG が移転先のものに変わったが、DS のキャッシュはまだされていたのか、SERVFAIL になっている。

・SERVFAIL 後、+cd で問い合わせると A の TTL は減少するが、RRSIG の TTL は減少しないことが判明した。

・時系列の詳細図は次ページ参照

正常系シナリオ		キャッシュDNSサーバ1				キャッシュDNSサーバ2			
時間	シナリオ	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
13:00	実験スタート	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra ad 検証OK 解決OK	qa rd ra 検証NG 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
13:09	移転先DNSにDNSSEC付ゾーンの設定完了								
13:20	レジストラ移転完了								
13:22	移転先が移転元のDS削除								
13:32	DSのTTLが経過(10分)								
13:37	移転先がNSを変更								
13:39	–					NSが切り替わる qr rd ra 検証NG 解決OK	NSが切り替わる	NSが切り替わる	NSが切り替わる
13:42	移転元NSのTTLが経過(5分)								
13:45	–	NSが切り替わる	NSが切り替わる	NSが切り替わる qr rd ra ad cd 検証なし 解決OK	NSが切り替わる				
13:47	移転先のDSを登録								
13:48	–		qr rd ra SERVFAIL						
13:50	–					qr rd ra ad 検証OK 解決OK			
13:51	–	qr rd ra SERVFAIL		qr rd ra cd 検証なし 解決OK					
13:52	移転先NSのTTLが経過(5分)								
13:54	–							qr rd ra ad cd 検証なし 解決OK	
13:55	DNS移転完了	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra ad cd 検証なし 解決OK					
13:58	移転元DNSのゾーン削除 実験終了								

異常系１：

・キャッシュ DNS サーバ２ではシナリオ通りに完了した。

・キャッシュ DNS サーバ１では NS が切り替わり SERVFAIL となるところまでは想定通りであったが、その後 14:19 のキャッシュクリアの際に DS のキャッシュがクリアされていなかったのか、SERVFAIL のままとなった事象が確認された。（RRSIG の TTL は止まったまま）

・その後 14:23 のキャッシュクリア時に事象は改善し、移転先 DS 登録後であったため、検証も成功した。

・時系列の詳細図は次ページ参照

異常系1(No22)シナリオ		キャッシュDNSサーバ1				キャッシュDNSサーバ2			
時間	シナリオ	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:07	実験スタート	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra ad 検証OK 解決OK	qa rd ra 検証NG 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
14:07	レジストラ移転は完了済とし、 移転先は移転元のDSを削								
14:10	–							qr rd ra ad cd 検証なし 解決OK	
14:14	–					NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる qr rd ra cd SERVFAIL	NSが切り替わる qr rd ra cd SERVFAIL
14:15	NSのTTLが経過(5分)							qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
14:16	–	NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる	NSが切り替わる				
14:18	移転元のDSを削除する								
14:19	各キャッシュサーバが キャッシュのクリアを実施					qa rd ra 検証NG 解決OK	qa rd ra 検証NG 解決OK		
14:20	–								
14:23	移転先のDSを登録する 各キャッシュサーバが キャッシュのクリアを実施	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra ad cd 検証なし 解決OK		qr rd ra ad 検証OK 解決OK		qr rd ra ad cd 検証なし 解決OK	
14:27	実験終了								

異常系２：

・DS の TTL を 10 分、NS の TTL を 5 分と設定して実験を進めていたが、NS の TTL は上位サーバの TTL が反映されていた。この場合 crisp.jp の TTL が 10 分であったため DS と NS の TTL が同じ 10 分となっていた。そのため、タイミングよく NS の TTL が切れる前に、DS の TTL が切れた場合は、キャッシュ DNS サーバ２のように SERVFAIL にならず、シナリオ通りの結果が得られなかった。

・キャッシュ DNS サーバ１では予定通り SERVFAIL が確認された。
その際に+cd を見てみると、RRSIG だけでなく A の TTL も減少しないという事象が確認された。（NS の TTL は減少している）

・キャッシュ DNS サーバ２において、キャッシュのクリアをする直前に突然意図しない SERVFAIL が発生した。直後のキャッシュクリアにてすぐに検証可能となったが、SERVAIL になった原因は不明である。

・時系列の詳細図は以下参照

異常系2(No30)シナリオ		キャッシュDNSサーバ1				キャッシュDNSサーバ2			
時間	シナリオ	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:30	実験スタート	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra ad 検証OK 解決OK	qa rd ra 検証NG 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
14:34	レジストラ移転は完了済とし、移転元DS削除、NS変更								
14:39	NSのTTL経過(5分)								
14:40	–					NSが切り替わる qa rd ra 検証NG 解決OK	NSが切り替わる	NSが切り替わる	NSが切り替わる
14:41	–	NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる qr rd ra SERVFAIL	NSが切り替わる	NSが切り替わる				
14:44	DS登録								
14:45	–					qr rd ra SERVFAIL	qr rd ra SERVFAIL		
14:46	各キャッシュサーバがキャッシュのクリアを実施	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra ad cd 検証なし 解決OK		qr rd ra ad 検証OK 解決OK	qa rd ra 検証NG 解決OK	qr rd ra ad cd 検証なし 解決OK	
14:47	実験終了								

異常系３：

・開始当初より両キャッシュ DNS サーバが通常の状態になかったため、シナリオとは大きく異なる結果となっている。

・キャッシュ DNS サーバ１では、実験開始時にキャッシュクリアに失敗しており、異常系２から異常系３への実験の移行がスムーズに行われなかったのが原因と思われる。

・キャッシュ DNS サーバ２では、実験開始時に移転元の DS が登録されていなかったため、最初から信頼の連鎖が切れていた可能性がある。

・時系列の詳細図は以下参照

異常系3(No33)シナリオ		キャッシュDNSサーバ1				キャッシュDNSサーバ2			
時間	シナリオ	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:52	実験スタート	qr rd ra SERVFAIL	qr rd ra SERVFAIL	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra 検証NG 解決OK	qa rd ra 検証NG 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
14:53	レジストラ移転は完了済とし、NS変更を実施								
14:58	NSのTTL経過(5分)								
14:59	移転先DSを登録								
15:02	–	NSが切り替わる qr rd ra ad 検証OK 解決OK	NSが切り替わる connection timed out	NSが切り替わる qr rd ra ad cd 検証なし 解決OK	NSが切り替わる	NSが切り替わる qr rd ra ad 検証OK 解決OK	NSが切り替わる	NSが切り替わる qr rd ra ad cd 検証なし 解決OK	NSが切り替わる
15:06	実験終了								

異常系４：

・CNAME によって別のドメインを指定しているため、alias.transfer.crisp.jp に対する検証は失敗する。A/AAAA レコードに変更し、検証可能となった。

・問題なく検証は完了した。

・時系列の詳細図は以下参照

異常系4(No36)シナリオ		キャッシュDNSサーバ1				キャッシュDNSサーバ2			
時間	シナリオ	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
15:07	レジストラ移転・DNSプロバイダ移転はどちらも済として実験スタート	qr rd ra ad 検証OK 解決OK	connection timed out	qr rd ra ad cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK	qr rd ra ad 検証OK 解決OK	qa rd ra 検証NG 解決OK	qr rd ra ad cd 検証なし 解決OK	qr rd ra cd 検証なし 解決OK
15:14	aliasをCNAMEからA/AAAAに変更								
15:17	–		qr rd ra ad 検証OK 解決OK		qr rd ra ad cd 検証なし 解決OK		qr rd ra ad 検証OK 解決OK		qr rd ra ad cd 検証なし 解決OK
15:18	実験終了								

・ 得られた知見

正常系：

・想定通りに移転が行われなかった箇所が見受けられたので、この手順を使用するのであれば DNS やサーバ設定の前提条件を洗い出しおく必要があるかと思われる。

DNS サーバによってはこの手順を利用して、SERVFAIL にならないとも限らないので注意が必要である。

・SERVFAIL 発生後の RRSIG の TTL は検証できていない場合、+cd で引くと減少しないことが確認できた。

異常系１：

・キャッシュクリアが正常に行われない状態が確認された。DNSSEC 有事の際には ISP のキャッシュクリアが必要になる場面があると考えるので、キャッシュクリアの正常な動作確認は必要である。

異常系２：

・DNSSEC において TTL は非常に重要で、TTL 時間を誤ると SERVFAIL となる可能性が大幅に高まる。サーバがどの TTL を参照しているのかを正確に把握しておくのが重要である。

・意図しないところでの急な SERVFAIL なども見られることから、レジストラ移転には常に SERVFAIL の危険がある。お客様とのやりとりを行う中で、SERVFAIL は発生しないと断言するかどうかは検討の必要がある。

異常系３：

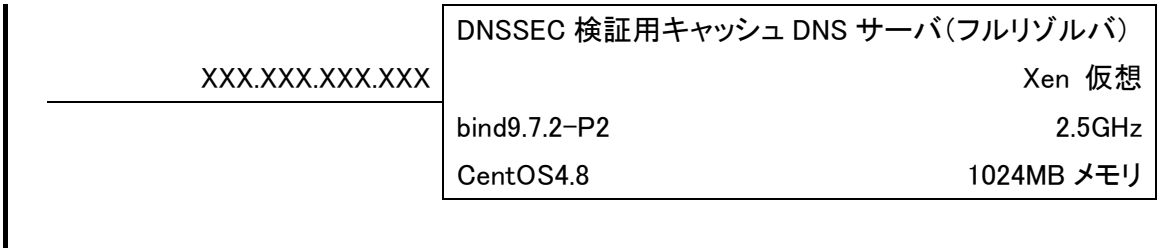
・特になし。

異常系４：

・CNAME は検証できず、A/AAAA に変更することで検証が可能になることを認識した。

■ 事例 7 一般ユーザの ISP

・ 実験環境



・ 実験結果概要

正常系の実験は、予定通りに問題なく完了した。
異常系については、一部で異常状態にならない現象も発生したが、その他は想定通り
キャッシュのクリアにて名前解決が回復した。

・ 実験結果詳細

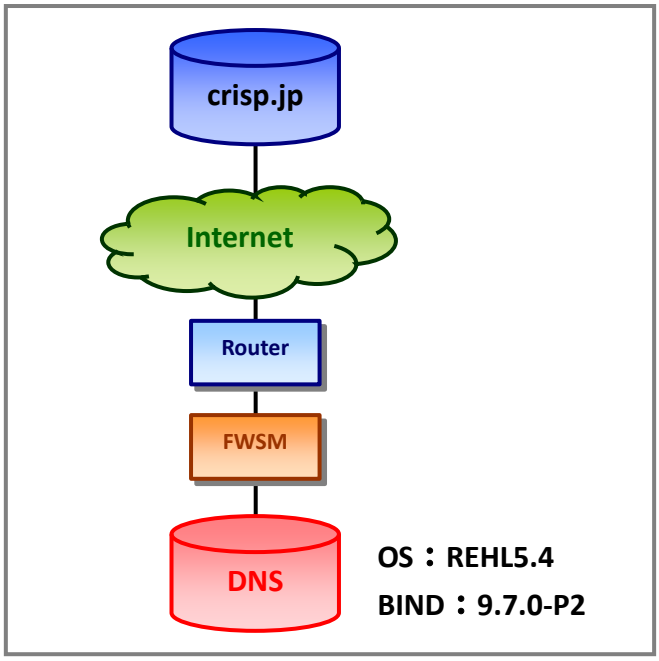
正常系：DNS の委任は正常に維持されて、DNSSEC の委任が切れている期間も想定通
りで TTL 経過後切り替えで無事に移転が完了した。
異常系：異常状態が再現できないケースが 1 件あったが、他は想定通りキャッシュクリ
アで名前解決が回復した。

・ 得られた知見

DNSSEC で追加されたレコードやキャッシュの TTL で DNS の複雑さが増している。
今回の実験はキャッシュのクリアという方法で復帰させているが、現実に展開するのは
不可能に近く、ミスをすると長期化する懸念がある。レジストラ移転は、慎重に行う必
要があることを再認識した。

■ 事例 8 一般ユーザの ISP

・ 実験環境



・ 実験結果概要

- +dnssec alias のクエリが開始当初より「connection timed out」が発生し想定する試験結果が得られなかった。これは、FW の問題であり試験前の確認漏れによるものと判明した。
  alias に対する分析報告はない。
- +dnssec www では、TTL に伴うキャッシュの動作が不安定であり、基本的には NS 側の TTL（10 分）を保持している傾向が見られた。
- キャッシュクリアしても www に関して SERVFAIL が返る等、クリア直後の状態が不安定であった。不安定事象の原因は不明である。

・ 実験結果詳細

（1）正常系確認

一般ユーザの ISP は以下の実行コマンドを 30 秒間隔で実行した結果から、分析した。NS が切り替わった際にも RRSIG には変化がなく、検証 OK であり続けた事象が見受けられた。DS,NS,RRSIG の TTL について再考慮する必要がある。

```
# dig +dnssec www.transfer.crisp.jp a @キャッシュ DNS サーバ
# dig +dnssec ns.transfer.crisp.jp a @キャッシュ DNS サーバ
# dig +dnssec transfer.crisp.jp ds @キャッシュ DNS サーバ

************************
13:32  DS の TTL（10 分）経過  ⇒  キャッシュにより名前解決 OK
************************
# dig +dnssec www.transfer.crisp.jp a @127.1
www.transfer.crisp.jp.   150     IN      A       203.178.129.44
www.transfer.crisp.jp.   150     IN      RRSIG   A 8 4 300 20101109042353

# dig +dnssec transfer.crisp.jp ds @127.1
crisp.jp.    180  IN  SOA  ns.crisp.jp. root.crisp.jp. 1288931410 3600 900 604800
crisp.jp.               180     IN      RRSIG   SOA 8 2 600 20101205033010
transfer.crisp.jp.      180     IN      RRSIG   NSEC 8 3 300 20101205033010
transfer.crisp.jp.      180     IN      NSEC    unsecure.crisp.jp. NS RRSIG NSEC

# dig +dnssec ns.transfer.crisp.jp a @127.1
ns.transfer.crisp.jp.    210     IN      A       59.106.114.121
ns.transfer.crisp.jp.    210     IN      RRSIG   A 8 4 300 20101109042353

************************
13:42  移転元 NS の TTL（5 分）経過  ⇒  状態変化なし
************************
# dig +dnssec www.transfer.crisp.jp a @127.1
www.transfer.crisp.jp.   150     IN      A       203.178.129.44
www.transfer.crisp.jp.   150     IN      RRSIG   A 8 4 300 20101109042353

# dig +dnssec transfer.crisp.jp ds @127.1
crisp.jp.   210  IN   SOA     ns.crisp.jp. root.crisp.jp. 1288932003 3600 900 604800
crisp.jp.               210     IN      RRSIG   SOA 8 2 600 20101205034003
transfer.crisp.jp.      210     IN      RRSIG   NSEC 8 3 300 20101205034003
transfer.crisp.jp.      210     IN      NSEC    unsecure.crisp.jp. NS RRSIG NSEC

# dig +dnssec ns.transfer.crisp.jp a @127.1
ns.transfer.crisp.jp.    210     IN      A       59.106.114.121
ns.transfer.crisp.jp.    210     IN      RRSIG   A 8 4 300 20101109042353
```

****
13:45　NS 変更
****

****
13:50　キャッシュが切れ、SERVFAIL 発生
****
dig +dnssec www.transfer.crisp.jp a @127.1
ANSWER SECTION なし

dig +dnssec ns.transfer.crisp.jp a @127.1
ANSWER SECTION なし

dig +dnssec transfer.crisp.jp ds @127.1
transfer.crisp.jp.　　299　　IN　　DS　　36886 8 2
transfer.crisp.jp.　　299　　IN　　DS　　36886 8 1
transfer.crisp.jp.　　299　　IN　　RRSIG　　DS 8 3 600 20101205035027

****
13:54　NS 変更後、約 10 分　⇒　名前解決 OK
****
dig +dnssec www.transfer.crisp.jp a @127.1
www.transfer.crisp.jp.　　295　　IN　　A　　203.178.129.44
www.transfer.crisp.jp.　　295　　IN　　RRSIG　　A 8 4 300 20101204033032

dig +dnssec ns.transfer.crisp.jp a @127.1
ns.transfer.crisp.jp.　　270　　IN　　A　　202.212.225.172
ns.transfer.crisp.jp.　　270　　IN　　RRSIG　　A 8 4 300 20101204033032

dig +dnssec transfer.crisp.jp ds @127.1
transfer.crisp.jp.　　29　　IN　　DS　　36886 8 1
transfer.crisp.jp.　　29　　IN　　DS　　36886 8 2
transfer.crisp.jp.　　29　　IN　　RRSIG　　DS 8 3 600 20101205035027

（2）異常系試験１（No22）

キャッシュクリア時にうまくキャッシュがクリアされていない事象を確認した。

2 回目のキャッシュクリアでユーザからの試験は OK となる。

（3）異常系試験２（No30）

NS 変更後の SERVFAIL 事象は、不明である。

（4）異常系試験３（No33）

実験開始当初の SERVFAIL は、キャッシュクリアの失敗によるものである。

NS 切替後はキャッシュがクリアされ問題なく名前解決が OK となる。

・ 得られた知見

本実験では、移行タイミングを合わせてキャッシュクリアを実施している為、名前解決が可能となるまでの時間が予測できた。しかし、実際のサービス運用時においては、手動に伴うキャッシュクリアの作業を合わせることが出来ず、DNSSEC の各レコードの TTL 値の運用を慎重に設定する必要があると感じた。

また、DNSSEC のキャッシュ情報の保持について継続して試験を行い動作を把握する必要がある。

業務連携検討のためのFAQ

FAQ作成の背景

DNSSEC 対応のサービスを開始していない事業者が、DNSSEC 対応のサービスを提供した際に顧客や一般ユーザから寄せられるであろう質問やトラブル報告を想定し、その回答を用意しておくことは、DNSSEC に関連して新たに発生する運用や業務連携を検討・設計するための重要な確認ポイントとなる。DNSSEC 技術実験に参加した組織が、実験を通じて得た知見を元に、想定される質問を洗い出し整理することは、ISP や指定事業者などサービスを提供する事業者の業務設計に有益であると考えられる。

本実験では、DNSSEC 技術実験に参加した各組織が洗い出した想定質問をまとめ、その内容にしたがって以下の 8 項目に分類した。

1. DNSSEC のメリット・デメリットに関する質問
2. 料金に関する質問
3. 業務に関する質問
4. 登録者に関する質問
5. 技術的な質問
6. 運用に関する質問
7. 世の中の動向に関する質問
8. 一般的な質問

さらに、それぞれの質問を、事業者によらず回答が共通になると考えられるもの（共通編）と、事業者毎に回答が異なると考えられるもの（個別編）に分類し、FAQ の形にまとめた。

FAQ共通編

FAQ 共通編は、事業者によらず質問(Q)への回答(A)が共通になると考えられるものをまとめたものであり、実験参加者間で作成した回答(A)を付している。

▼DNSSEC のメリット・デメリットに関する質問

Q 絶対に DNSSEC を導入しなければいけないのでしょうか。DNSSEC は本当に必要なのでしょうか。DNSSEC に対応しなかったらどうなるのでしょうか。

A 必須ではないですが、セキュリティの向上効果が得られなくなります。

Q DNSSEC 導入にあたってのメリットを教えてください。DNSSEC を導入すると何が良くなるのでしょうか。DNSSEC を導入するとどれだけインターネットのセキュリティが確保されるのでしょうか。

A 従来 DNS のデータが正しいかどうかを確認する術がありませんでした。しかしながら DNSSEC を利用することで、受け取った DNS データの正当性を確認できるようになります。これによって DNS キャッシュポイズニング攻撃から守ることが可能になります。

Q DNSSEC 導入にあたってのデメリットを教えてください。DNSSEC 導入の課題はなんでしょうか。

A 権威 DNS サーバ側では、DNSSEC 処理に必要な鍵と署名の管理コストの増大が挙げられます。またキャッシュ DNS サーバ側では、署名検証におけるコストの増大があげられます。いずれにしても運用コストの増大がデメリットといえます。

▼業務に関する質問

Q 鍵が漏洩するとどうなりますか。

A 漏洩した鍵を入手した者が、偽の DNS データを偽造できることになり、DNS データを DNSSEC で守ることができなくなります。このため鍵が漏洩した場合は、すみやかな鍵の更新が必要になります。

Q ドメインの移転時はどのようになりますか。

A JPRS の DNSSEC 技術実験報告書運用設計編や DNSSEC ジャパンのレジストラ移転ガイドラインを参照してください。

▼登録者に関する質問

Q DNSSEC が正常動作していることはどうやったら確認できますか。

A DNSSEC の設定を行ったキャッシュ DNS サーバに対し、dig コマンドを使用して、
% dig +dnssec 当該ドメイン名 A @キャッシュ DNS サーバ
などの問い合わせを行い、flags のところに、ad が表示されれば DNSSEC が正常に動作していることを判断できます。

Q 自ドメイン名の権威 DNS サーバで DNSSEC に対応していれば安全ですか。

A A いいえ。DNSSEC は権威 DNS サーバ側から署名したデータを送り、キャッシュ DNS サーバ側で署名の検証を行います。従ってキャッシュ DNS サーバが DNSSEC 対応している必要があります。

▼技術的な質問

Q DNS の動作を詳しく教えてください。

A DNS は、インターネットアドレスの一部であるドメイン名と IP アドレスの対応付けを行う「名前解決」の機構です。詳細については JPRS トピックス&コラム「DNS のしくみと動作原理～インターネットを支え続ける DNS～」<http://jpinfo.jp/topics-column/010.pdf>をご参照ください。

Q DNSSEC の動作を詳しく教えてください。

A DNSSEC は、DNS の仕様が持つ根本的な脆弱性に対応するため策定されたセキュリティ拡張仕様です。詳細については JPRS トピックス&コラム <http://jpinfo.jp/topics-column/> の DNSSEC シリーズ (No.13<http://jpinfo.jp/topics-column/013.pdf>、No.14<http://jpinfo.jp/topics-column/014.pdf>、No.15<http://jpinfo.jp/topics-column/015.pdf>、No.16<http://jpinfo.jp/topics-column/016.pdf>)をご参照ください。

Q DNSSEC はどのサービスが対象なのでしょうか。(権威、キャッシュ、セカンダリ、逆引き)

A DNS プロトコルを使用するものすべてが該当します。

Q ラストワンマイルはどのようにして安全性を確保するのでしょうか。

A 複数の案があり、エンドノードで検証する方法と、通信路の安全性を高める方法の二つがあります。
案 1: エンドノードで検証

案 2: IPsec を使って通信路の安全性を高める（Windows7 での実装）
案 3: TSIG を使って通信路の安全性を高める（事前に利用者との間で鍵交換しておく）
案 4: ISP とエンドユーザの間には第三者が存在しないので安全だと信じる

Q 事前に対応済みを確認していなくても、アクセスしたドメイン名が DNSSEC に対応しているかわかりますか。

A 1.トラストアンカーを設定したキャッシュ DNS サーバでは DNSSEC 検証できたことを判断できます。
2. 使用しているキャッシュ DNS サーバが DNSSEC 検証を行なう場合のスタブリゾルバでは、DO ビットを 1 にしてクエリを送れば、AD ビットを見て DNSSEC 検証できたかを判断できます。

Q DNSSEC が有効かどうかはクライアントでどうやって分かるのでしょうか。

A 現時点では、クライアントのアプリケーションで DNSSEC が有効かどうかを知ることができるものは多くありません。

たとえば、FireFox には DNSSEC 検証を行うアドオンがあります。これを使うと、表示中の Web サイトが DNSSEC 対応しているか、クライアントが DNSSEC 対応の DNS サーバを利用しているかの確認ができます。

DNSSEC Validator
http://www.dnssec-validator.cz/
CZ.NIC Labs

また、いくつかの Web サイトでは、使用しているキャッシュ DNS サーバで DNSSEC が有効かどうかを容易に確認する事ができる方法を提供しています。

http://test.dnssec-or-not.org/
VeriSign Labs
DNSSEC が有効かどうかによって表示する Web ページが変わる

http://www.dnssec-failed.org/
Comcast (Deliberately Broken DNSSEC Validation Test Site)
DNSSEC 検証で故意に失敗するようにしてあるため、DNSSEC 対応時はエラー表示となる

Q DNSSEC に対応していると DNS を引くのに余計に時間がかかるのでしょうか。インターネットアクセスが遅くなるのでしょうか。

A DNSSEC の検証時には、DNSSEC なしの場合と比べて、キャッシュ DNS サーバが行うクエリの数は増加します。これにより DNS を引くのにかかる時間は長くなります。しかし、DNS の応答は十分速い場合が多く、ユーザがインターネットアクセスが遅くなると感じることは少ないと考えられます。

Q クライアントで DNSSEC を使うための設定はどうすればよいのでしょうか。

A A クライアントが利用するキャッシュ DNS サーバとして、DNSSEC 検証を実施するものを指定します。ISP のキャッシュ DNS サーバを利用しているような場合、該当する ISP が DNSSEC 対応をしている必要があります。

また、DNS-OARC では、ユーザが DNSSEC 対応を試す事ができるキャッシュ DNS サーバを提供しています。

OARC's Open DNSSEC Validating Resolver
https://www.dns-oarc.net/oarc/services/odvr

Q 自宅のブロードバンドルータの DNSSEC 対応の有無はどうすればわかるのでしょうか。

A ブロードバンドルータが DNSSEC 対応かどうかは、各メーカに確認をしてください。
また、NIC.CZ では独自に確認ツールを開発し、情報を集めて公開しています。

DNSSEC Hardware Tester
http://www.nic.cz/dnssectests/
CZ.NIC Labs

Q DNSSEC を使うためにブロードバンドルータで何か設定変更する必要がありますか。必要な設定を教えてください。

A クライアント側(PC 等の端末)が DNSSEC 対応していない場合は、何もする必要はありません。
クライアント側が DNSSEC 対応している(DNSSEC の検証を行う)場合は、以下の対応が必要です。

DNSSEC 対応をするための設定が明示的に存在する場合は、指示に従いその設定を実施してください。

明示的な設定がない場合は、ブロードバンドルータが DNSSEC 対応かどうかを確認し、

必要に応じてファームウェアのアップデートなどで対応を実施してください。最新のファームウェアにより DNSSEC 対応が行われている可能性があります。

Q クライアント側(PC 等の端末)は OS やブラウザ、アプリケーションに対策が必要になるのでしょうか。

A OS に対しては、DNSSEC 検証を行うキャッシュ DNS サーバを利用するように設定を行う必要があります。

従来のブラウザ、アプリケーションのままでも、DNS キャッシュポイズニングを受けたドメイン名へのアクセスがエラーになるという形で、DNSSEC の効果が得られます。

なお、現時点では、ブラウザ、アプリケーションで DNSSEC に対応しているものは多くありません。

たとえば、FireFox には DNSSEC 検証を行うアドオンがあります。これを使うと、表示中の Web が DNSSEC 対応しているか、クライアントが DNSSEC 対応の DNS サーバを利用しているかの確認ができます。

DNSSEC Validator
http://www.dnssec-validator.cz/
CZ.NIC Labs

Q 対応している DNS アプリケーションは何ですか(Version 等)。

A キャッシュ DNS サーバとして使用する場合、ルートゾーンの署名に対応できるよう、RSASHA256 をサポートする DNS アプリケーションを使用してください。

BIND 9.6.2 以上、9.7 以上
Unbound 1.4.0 以上

Q DNSSEC を利用するには特別な機器が必要でしょうか。

A 特別な機材は必要ありません。しかし、クライアント(PC 等端末)側で DNSSEC の検証を行う場合は、一部のブロードバンドルータ等では、DNSSEC 利用時の DNS 応答サイズの増加に対応できない等、不都合が発生する場合があります。

▼運用に関する質問

Q DNSSEC を設定すると負荷がかかって送受信に影響が出ますか。

A A 導入に際しては、鍵の署名・検証によるフルリゾルバの CPU 負荷が 2 倍程度、転送データ量が 3～5 倍程度に増える事が想定されます。これに見合った機器の増強を行う必要があります。

Q レコードの大きさや負荷は具体的にどのくらい増えるのでしょうか。

A DNS の応答パケットのサイズが 3～5 倍程度になり、フルリゾルバの負荷は 2 倍程度となります。

Q トラフィックはどれくらい増えるのでしょうか。

A 主要な TLD が全て DNSSEC 対応した場合、3～5 倍程度になることが想定されます。

Q 鍵が漏洩するとどうなりますか。

A DNSSEC 対応以前と同様に、DNS ポイズニング攻撃に対する脆弱性を持つことになります。

Q 鍵更新を失敗したらどうなるのでしょうか。その影響範囲はどのくらいでしょうか。

A そのドメイン名を検索するユーザが利用しているキャッシュ DNS サーバが DNSSEC 対応をしていた場合、DNSSEC の検証失敗により名前解決が失敗します。
ISP 等のキャッシュ DNS サーバが対応している場合、その顧客は影響を受けます。

Q 鍵の有効期限が切れた場合はどうなりますか。

A 鍵には有効期限がありません。
ただし、推奨利用期間はありますので、鍵の暗号強度に合わせて適切に交換をしてください。

Q ゾーンの再署名はどのタイミングで実施すればよいですか。

A ゾーンの各種情報を更新した場合には再署名が必要です。
また、署名有効期間終了より前に運用上十分な安全期間を持って再署名をしてください。
この安全期間としては、最低限 RRSIG の TTL 時間以上確保する必要があります。

Q トラストアンカーの設定を間違えるとどういう影響がでますか。

A トラストアンカーが設定されているドメイン名の検証が全て失敗し、名前解決できなくなります。

Q トラストアンカーには何を設定すればよいですか。

A 特別な事情がない限りは、ルートゾーンのトラストアンカーを設定してください。ルートゾーンのトラストアンカーは<https://data.iana.org/root-anchors/>で公開されています。

▼世の中の動向に関する質問

Q DNSSEC の世界の対応状況を教えてください。

A ルートゾーンは 2010 年 7 月 15 日に DNSSEC の署名が開始されています。DNSSEC の署名が開始されている TLD も増加しており、最新の状況は<http://stats.research.icann.org/dns/tld_report/>で参照できるようになっています。
2010 年 7 月時点での状況は、DNSSEC ジャパンの DNSSEC 2010 サマーフォーラムで発表された「各国 ccTLD、gTLD の状況について」<http://dnssec.jp/wp-content/uploads/2010/07/20100721-tld_dnssec_deployment-koreeda.pdf>にまとめられています。

▼一般的な質問

Q DNSSEC は誰が使うのでしょうか。

A DNSSEC の利用者はインターネットの利用者です。DNSSEC は DNS の拡張であり、ドメイン名登録者や ISP が DNSSEC に対応していれば、特に利用者は DNSSEC の利用を意識することはありません。

Q なぜ今まで DNSSEC はなかったのでしょうか。最近発覚した脅威なのでしょうか。

A DNSSEC は仕様の策定が開始されてから 10 年以上経過しています。DNSSEC は DNS が持つ脆弱性に対応するための仕様拡張ですが、2008 年夏に、その脆弱性を容易に攻撃できる手法が発表されたため、注目を集めたとともに、対応が進むようになりました。
攻撃手法の詳細については JPRS トピックス&コラム「新たなる DNS キャッシュポイズニングの脅威～カミンスキー・アタックの出現～」<http://jpinfo.jp/topics-column/009.pdf>をご参照ください。

Q DNS とはなんでしょうか。

A DNS は、インターネットアドレスの一部であるドメイン名と IP アドレスの対応付けを行う「名前解決」の機構です。詳細については JPRS トピックス&コラム「DNS のしくみと動作原理～インターネットを支え続ける DNS～」<http://jpinfo.jp/topics-column/010.pdf>をご参照ください。

Q DNSSEC とはなんでしょうか。

A DNSSEC は、DNS の仕様が持つ根本的な脆弱性に対応するため策定されたセキュリティ拡張仕様です。詳細については JPRS トピックス＆コラム <http://jpinfo.jp/topics-column/> の DNSSEC シリーズ (No.13<http://jpinfo.jp/topics-column/013.pdf> 、No.14<http://jpinfo.jp/topics-column/014.pdf> 、No.15<http://jpinfo.jp/topics-column/015.pdf> 、No.16<http://jpinfo.jp/topics-column/016.pdf>)をご参照ください。

Q DNSSEC は何の略でしょうか。

A DNSSEC は DNS Security Extensions の略です。

Q DNSSEC は海外でも使えるのでしょうか。

A DNSSEC はインターネットで使えるものなので、国内でも海外でも、インターネットが利用できるところであれば使えます。

FAQ個別編

FAQ 個別編は、事業者毎に質問(Q)への回答(A)が異なると考えられるものをまとめたものであり、回答(A)は付していない。

▼料金に関する質問

Q DNSSEC を設定するにあたって費用はどれくらいかかりますか。DNSSEC の利用は課金サービスになるのでしょうか。

Q DNSSEC のサービスを提供する際に課金はできるのでしょうか。

▼業務に関する質問

Q お客様にはどうやって DNSSEC の説明をすればいいでしょうか。

Q いつから DNSSEC を導入予定ですか。

Q DNSSEC の問い合わせ先(窓口)はどこですか。

Q ユーザの鍵管理等 DNSSEC に必要は手続きを JPRS へ委託することはできますか。

Q 下位ドメインが DNSSEC 対応を希望しているが、自 DNS は DNSSEC 未対応の場合下位のみ提供させることは出来ますか。

Q DNS マスターだけ DNSSEC 対応すれば対応完了でしょうか。

Q DNS マスターを管理していますが、セカンダリ DNS でも DNSSEC 対応予定はありますか。

Q DNSSEC 対応を始めるにあたって、用意するものはありますか。

Q DNSSEC の設定が必要な部分はどこでしょうか。

Q DS 取次ぎの対象ドメインはどこまでになりますか。

Q DS 取次ぎ開始のための特別な申し込みはありますか。

Q JPRS さんへの登録だけで DNSSEC はできるのでしょうか。

Q お客様からの申請はどうやって処理するのでしょうか。インターフェースを教えてください。

Q 上位権威 DNS サーバへの DS の登録はどのように行うのでしょうか。

Q 上位 DNS への DS レコードの登録を誤るとどういう影響がでますか。

Q 設定を間違った場合、お客様にどのようなことがおきますか。

Q ゾーンファイルの内容を変更する都度、再署名と上位登録の DS の差し替えが必要になるのでしょうか。その際の連絡手段を教えてください。

Q 鍵はお客様にコロコロ変えられたりしないのでしょうか。

Q DNSSEC 導入によって指定事業者移転やドメイン移転の連携フローはどのようにかわりますか。

Q　レジストラ移転に関して、移転期間の猶予はありますか。
Q　移転元レジストラが応答ない場合の救済処置はありますか。
Q　移転手数料(費用)はかかりますか。
Q　指定事業者移転時の鍵の交換はどのような方式になりますか。
Q　DNSSEC に対応していたレジストラから DNSSEC に対応していないレジストラにレジストラ移転しますが、移転後に DS を削除してもらえますか。
Q　レジストラ移転したら、移転元レジストラが承認後すぐに DNS を消してしまいました。

▼登録者に関する質問
Q　DNSSEC 対応でお客様の作業はありますか。
Q　お客様の自社サービスに影響はないでしょうか。(金融、証券など)
Q　お客様のサービスに影響があった場合どこが責任を取るのでしょうか。

▼技術的な質問
Q　BIND 以外(PowerDNS 等)での DNSSEC 対応状況・設定方法を教えてください。
Q　DDNS サービスでも使える／使うのでしょうか。

▼運用に関する質問
Q　機器の負荷はあがるのでしょうか。
Q　DNSSEC 導入による NW・サーバ負荷増に伴い、機器を具体的にどの程度増強する必要があるのでしょうか。
Q　サーバ以外の機器（L4SW など）で考慮すべき点はありますか。
Q　鍵はどのくらいの頻度で更新するべきですか。
Q　鍵更新は誰がやるのでしょうか。
Q　鍵更新はどう管理するのでしょうか。
Q　鍵更新時に注意することはありますか。
Q　鍵更新にどのくらいの稼働がいるのでしょうか。
Q　鍵更新に失敗する要因はなにでしょうか。
Q　鍵更新失敗時の切り戻しはすぐに可能でしょうか。
Q　鍵の有効期限はどのくらいですか。
Q　署名の有効期間はどのくらいが適切ですか。
Q　署名はどこまで行うのでしょうか。内部のドメインにも署名は必要でしょうか。
Q　運用を補助するツールのようなものはありますか。
Q　鍵情報の有効期限管理を自動化することは可能でしょうか。

Q 鍵の管理・更新が煩雑かつ失敗時のリスクが大きいため手動運用は困難ではないでしょうか。
Q 導入時・導入後の技術支援はあるのでしょうか。トラブル時の対応を教えてください。
Q DNSSEC を使用するに当たって必要なことは何でしょうか。
Q 問題が起こらないように、何か監視は必要でしょうか。
Q DNS メンテナンス時に懸念点はあるでしょうか。
Q DNSSEC 対応する時の注意点はあるのでしょうか。
Q DNSSEC を利用するにはどのように設定すればいいですか？
Q なにか難しい設定はこちらで必要なのでしょうか。
Q DNSSEC 導入および運用コストはどのくらいかかるのでしょうか。
Q ゾーン転送に影響はあるのでしょうか。
Q DNSSEC 利用にあたり SOA の Expire 値等を調整する必要はありますか。
Q DNSKEY や DS の TTL 値はどのくらいが適切ですか。
Q DS を受け渡す際のセキュリティはどのように確保されるのでしょうか。

▼世の中の動向に関する質問

Q ISP や指定事業者が DNSSEC に対応するのはいつごろでしょうか。
Q JP ドメインでの普及率はどれくらいですか。
Q 逆引き(IPv4、IPv6)ドメインツリーを DNSSEC 対応する予定はあるでしょうか。

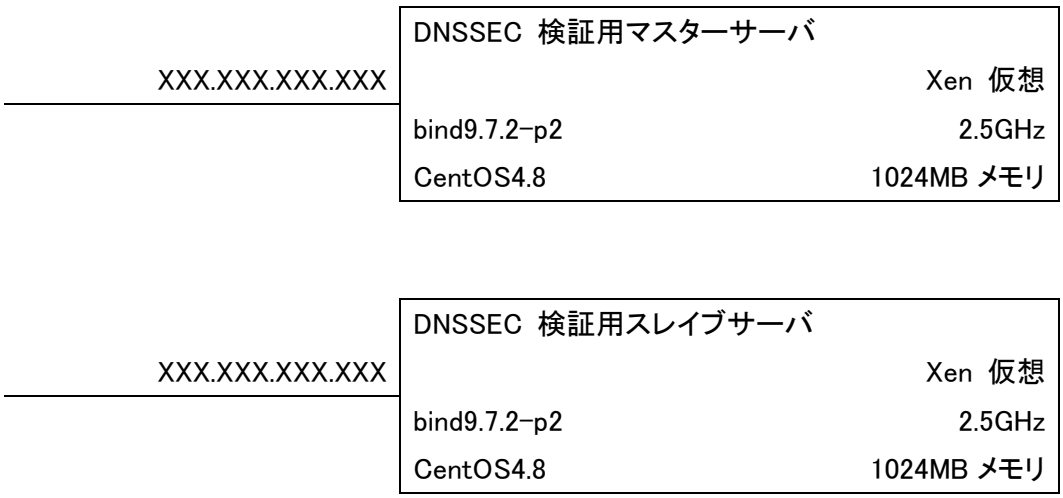
▼一般的な質問

Q DNSSEC の利用は課金サービスになるのでしょうか。
Q DNSSEC を利用するためには ISP と特別な契約が必要でしょうか。どこに申し込めば使えるのでしょうか。

個別実験

個別実験 事例 1

・ 実験環境



・ 実験結果概要

DNS のゾーン署名を実施し、実験用の指定事業者 I/F（Web）にて DS レコードを登録する手順の検証を行い問題がないことを確認した。
また、鍵管理 I/F レベルでレジストラ移管を実施した。

・ 実験結果詳細

間違ったフィールドの DS レコードを入力した際に、エラーとしか表示されないため原因特定まで時間がかかった。不慣れなことが原因だが、もう少し親切なメッセージや入力例が参照できるようになっていれば助かると感じた。
レジストラ移管は確認もなく即反映されるので不安に感じた。

・ 得られた知見

DNSSEC のバックグラウンドを知らない担当部門が評価を行ったこともあり、正常な状態がわからないで不安に感じているようだった。きちんとした運用マニュアルを作り、不測の事態に備えて動作原理を理解することが、結果としてミスを防ぐことになると思えた。

個別実験 事例 2

・ 実験環境

DNSSEC 技術実験環境を使用し、自社サーバの DNSSEC 運用試験をするにあたり、まずは自社の DNSSEC の運用方法を確立した。権威 DNS サーバ 1 台、セカンダリサーバ 1 台、キャッシュ DNS サーバ 1 台という実験環境を構築し技術実験環境にインターネット経由で接続し、前述の運用フローに乗せて、運用が可能かどうかの検証を行った。

・ 実験結果概要

DNSSEC 技術実験環境の WEB インターフェースを使用した DNSSEC の運用が問題なく実施できることが確認できた。

・ 実験結果詳細

DNSSEC 技術実験環境の WEB インターフェースを利用し、ドメインの登録等を実施。レジストリへの登録の運用が可能かどうかを検証した。
また、キャッシュ DNS サーバの検証においても正常な動作を確認できた。
これにより自社の DNSSEC 運用方法や今後の対応について、実運用に向けた方針が固まった。なお、トランザクションインターフェースについては，今後検証を進める予定である。

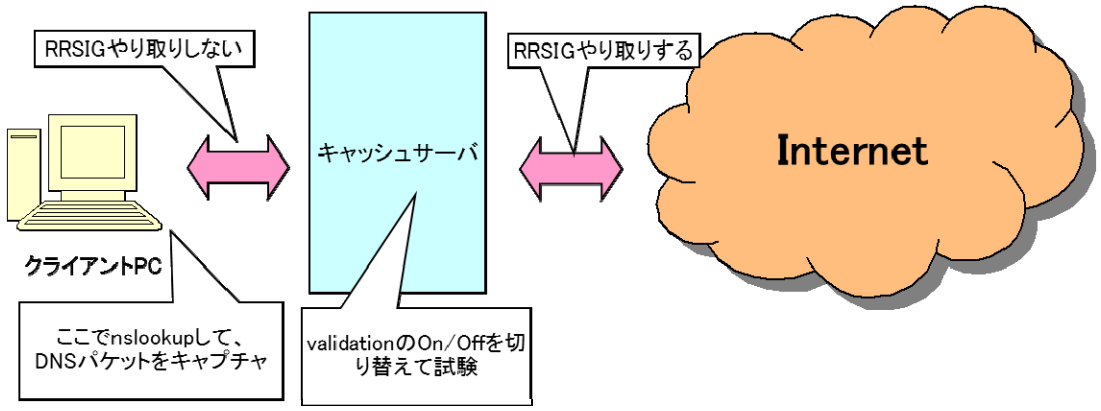
・ 得られた知見

WEB インターフェースを使用してのレジストリへの登録は問題なく実施が可能であり、現在のインターフェースと大差なく利用が出来る。

個別実験　事例 3

・ 実験環境

DNSSEC の Validation が ON の時と、OFF の時でエンドユーザが受け取るパケットサイズに大きな変化が見られるか測定を実施する。



・ 実験結果概要

エンドユーザとキャッシュ DNS サーバ間で Validation の ON／OFF でパケットサイズは大きく変化しないことがわかった。

・ 実験結果詳細

ドメイン名	validation 有り		validation 無し		備考
	応答	パケットサイズ	応答	パケットサイズ	
www.isc.org	NOERROR	318byte	NOERROR	186byte	DNSSEC 完全対応ドメイン
dnssec-deployment.org	NOERROR	97byte	NOERROR	260byte	DNSSEC 完全対応ドメイン
www.sub118.crisp.jp	SERVFAIL	79byte	NOERROR	121byte	DNSSEC 有効期限切れドメイン
yahoo.co.jp	NOERROR	151byte	NOERROR	151byte	DNSSEC 対応無しドメイン

・ 得られた知見

・キャッシュ DNS サーバを Validation を ON にしてもユーザへの影響は大きく出ないのではないかと思われた。
・ON／OFF でパケットサイズに違いが出ているのは Additional records が付いているか付いていないかのため。