# JPRS トピックス＆コラム

## ■運用者から見たDNSSECと従来のDNSの違い ～運用上特に注意が必要なポイント～

**DNSSECの運用には、従来のDNSにはなかった手順や注意点が存在しています。**
**従来のDNSと比較して特に注意が必要なポイントについて、具体的に解説します。**

### ■相対時間と絶対時刻

従来の DNS プロトコルでは、ある事象が発生した時点からの**相対時間**（タイムインターバル）で時間を管理しており、「○年○月○日○時○分○秒」といった、絶対的な時刻情報は使用していません[1]。各リソースレコードの TTL や SOA レコード内の各設定値などは相対時間による秒数であり、例えば TTL の場合、キャッシュ DNS サーバーが受け取った TTL の値が初期値となり、1 秒ごとに減算されていきます（図 1）。

このように、従来の DNS プロトコルでは絶対時刻を使用していないため、DNS サーバーにおける正確な時刻の維持は、必須ではありません。

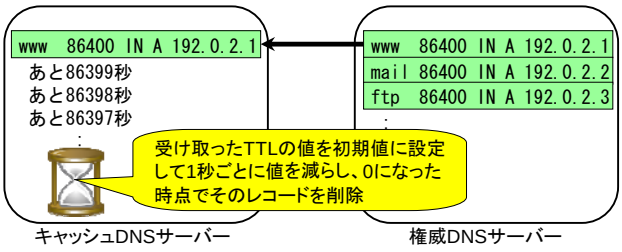


図 1: キャッシュ DNS サーバーにおける TTL の扱い

### ▼DNSSEC では正確な時刻の維持が必要

これに対し、DNSSEC で導入された署名（RRSIG レコード）には、有効期間の開始（inception）と終了（expiration）の双方が、1970 年 1 月 1 日からの**絶対時刻**で記述されています。

そして、送信されてきた署名を受信側で検証する際には、その署名が有効期間内であるかを**自身が管理する時計を参照して確認する**ため、DNSSEC を構成するすべての DNS サーバーでは、正確な時刻の維持が必要になります（図 2）。

[1] SOA のシリアルに時刻を使用することがありますが、これはバージョン番号であり、DNS プロトコルでは時刻として管理されません。

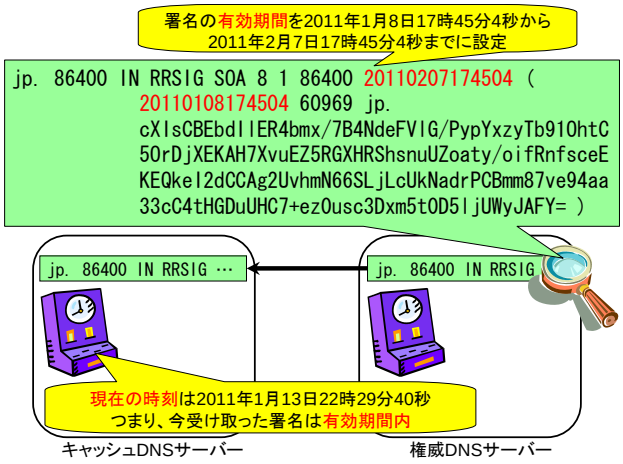


図 2: 正確な時刻の維持が必要な理由

### ■データの有効期間に注意

このように DNSSEC では、従来の DNS では発生しなかった「**データは存在しているが、そのデータはもう（まだ）有効ではない**」という状況が発生します。そのため、DNS サーバーに対するヘルスチェックを外部から実施する場合、単にデータの存在のみのチェックだけでは不十分で、データの内容の**有効性のチェックについても併せて実施する**必要があります（図 3）。

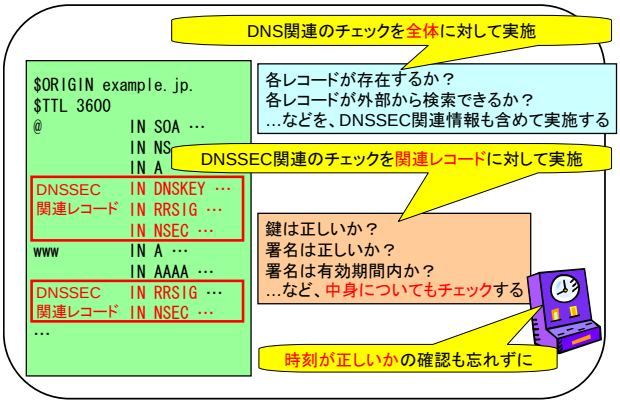


図 3: ヘルスチェックの際のポイント

なお、ヘルスチェックを実施するシステムにおいても正確な時刻の維持が必要になります。


※掲載内容は2011年1月現在のものです。

## ■NS レコードと DS レコードは「似て非なるもの」

DNSSEC では親子間の信頼の連鎖を構築するために **DS レコード**の親への登録・公開が必要になります。DS レコードは従来の NS レコードに**似た**形で取り扱うことが可能ですが、その取り扱いには NS レコードとは異なる点が存在しています。

### ▼NS は親子双方が持ち、子が権威を持つ

NS レコードは**親子双方に同じ内容が登録・公開**され、子の NS レコードが権威を持ちます。親の NS レコードは権威を持たない委任情報として扱われます（図 4）。

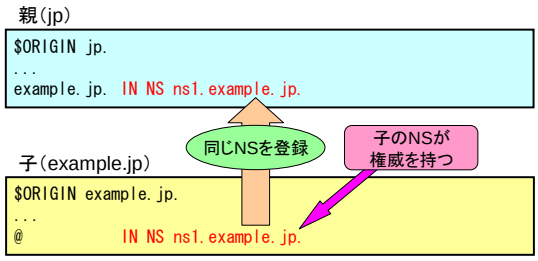


図 4: NS レコード

### ▼DS は親のみが持ち、親が権威を持つ

これに対し DS レコードは子の鍵署名鍵（DNSKEY（KSK））から生成され、**親にのみ登録・公開**されます。そのため、DS レコードは NS レコードとは異なり、親のものが権威を持つことになります（図 5）。

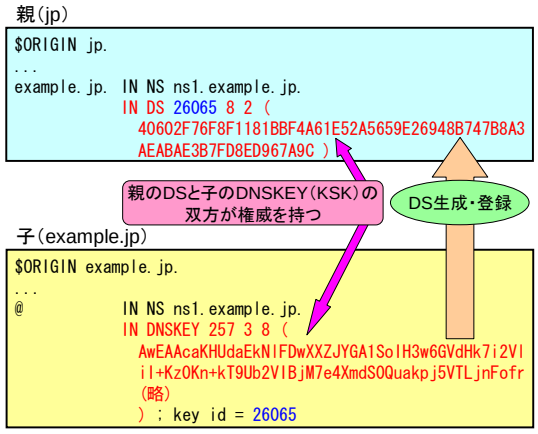


図 5: DS レコード

そして、DNSSEC では親子間の信頼の連鎖を、親の DS レコードと子の KSK を**照合**することにより検証します。もし親の DS レコードに対応する KSK を子が一つも保持していなかった場合、即座に **DNSSEC 検証エラーとなり名前解決に失敗する**ため、特に注意が必要です。

## ■データの登録・更新・削除のタイミングと順番

DNS では従来から、子の DNS サーバーでの準備完了後に親のデータを登録・更新することが必要でした。DNSSEC の導入後はこれに加え、**更新前の古いキャッシュデータが完全にクリアされた後に次の手順を実行するという手順を、これまで以上に遵守する**必要があります。

例として、二重署名法による KSK のロールオーバー手順を表 1 に示します。

| |
|---|
| 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KSKによりDNSKEY（ZSK）を署名 |
| ③自分のDNSKEYのTTL設定値の時間分待つ |
| - DNSKEY（KSK）の古いキャッシュデータがクリアされる |
| ④新しいKSK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 |
| - DSの古いキャッシュデータがクリアされる |
| 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 のロールオーバー手順

## ■NSEC3 を用いる場合の注意点

ゾーンの列挙（詳細はトピックス&コラム No.16 を参照）を防止するために NSEC3 を使用する場合、そのゾーンのすべての権威 DNS サーバーが NSEC3 に対応している必要があります。

NSEC3 では存在しない名前を問い合わされた際に権威 DNS サーバーが必要なハッシュ値を動的に計算するため、**権威 DNS サーバーに NSEC3 に非対応のものが含まれていた場合、正しく動作しません**（図 6）。

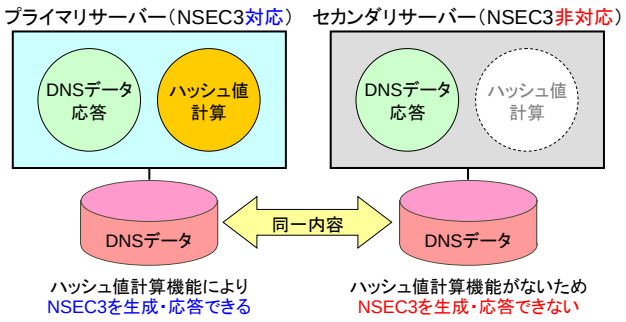


図 6: NSEC3 を用いる場合の注意点

セカンダリサーバーを DNS サービス事業者に委託する場合などに、特に注意が必要です。