JPRS トピックス＆コラム

■DNSSECに関するよくある質問と回答（技術仕様編―2015年1月版）

DNSSECの技術仕様に関する質問と回答をQ＆A形式でまとめました。JPRSホームページ（http://jprs.jp/dnssec/）でオンライン版を公開していますので、併せてご利用ください。

■DNSSEC の技術仕様について

Q1 DNSSEC の基本仕様を定めている RFC はどれですか？

DNSSEC の基本仕様は 2005 年に発行された、RFC 4033、4034、4035 により定められています。

これに加え、キャッシュ DNS サーバーの円滑な運用に必要なトラストアンカーの自動更新の仕様を定めた RFC 5011 が 2007 年に、ゾーンの列挙（後述）を困難にするための NSEC3 と TLD における段階的な DNSSEC の導入を容易にする Opt-Out の仕様を定めた RFC 5155 が 2008 年に、それぞれ発行されました。

その後、仕様の明確化と実装のための注意点をまとめた RFC 6840 が 2013 年に発行されています。

Q2 DNSSEC では名前や RR（リソースレコード）が存在しないこと（不在証明）を、どのように検証しているのですか？

電子署名では存在する情報に対して署名を付加します。このため、そのままでは名前が**存在しないこと**は検証できません。

DNSSEC では、ゾーンの内容を大文字にした上で ASCII コード（アルファベット）順に整え[1]、対象の名前の前後の名前と RR の種別を **NSEC レコード**で提示することにより、存在しないことを検証しています（図1）。

■NSECレコードの例

```
sec1.example.jp.  IN NSEC sec3.example.jp.  NS DS RRSIG NSEC
```

■上記の意味

アルファベット順でsec1.example.jpの次に存在するのはsec3.example.jpであり、sec1.example.jpにはNS、DS、RRSIG、NSECの各RRが存在している

■使用例1：「その名前は存在しない」

sec2.example.jpのAレコードの問い合わせに対し上記のNSECレコードを提示することで、sec1.example.jpとsec3.example.jpの間には名前が存在しないことを、問い合わせ元に提示できる

■使用例2：「名前そのものは存在するが、そのRRは存在しない」

sec1.example.jpのAレコードの問い合わせに対し上記のNSECレコードを提示することで、sec1.example.jpにはAレコードが存在しないことを、問い合わせ元に提示できる

図1：NSEC レコードによる不在証明

[1] RFC 4034 の「Canonical DNS Name Order」で定義されています。

Q3 「ゾーンの列挙」とは何ですか？

前述の通り DNSSEC では、**不在証明を前後の名前と RR の存在によって検証する**という特徴があります。

そのためこの特徴を利用し、DNSSEC に対応したゾーンに存在する NSEC レコードを**外部から順にたどる**ことにより、そのゾーン内のドメイン名の一覧を外部から入手することが可能になります。この行為は「**ゾーンの列挙**（Zone enumeration）」と呼ばれます（図2）。

■ゾーン列挙の例

```
TLD.            IN NSEC 00000000.TLD. NS SOA TXT RRSIG NSEC DNSKEY
00000000.TLD.   IN NSEC 00000001.TLD. NS RRSIG NSEC
00000001.TLD.   IN NSEC 00000002.TLD. NS RRSIG NSEC
   :
example1.TLD.   IN NSEC example2.TLD. NS DS RRSIG NSEC
example2.TLD.   IN NSEC example3.TLD. NS RRSIG NSEC
example3.TLD.   IN NSEC example4.TLD. NS DS RRSIG NSEC
   :
   :
zzzzzzzz.TLD.   IN NSEC TLD.          NS DS RRSIG NSEC
```

■ゾーン列挙の手順と特徴

①そのゾーン自体（上記の例ではTLD）のNSECを検索する
②検索結果中の「次の名前」のNSECを検索する
③以下同じ手順を繰り返し、NSECを順にたどる
④次の名前としてそのゾーン自体が示されたら終了

権威DNSサーバーの問い合わせログを監視することで、ゾーンの列挙の試行を検出することはある程度可能であるが、DNSSECのプロトコルの仕様上、行為を完全に防止することはできない

図2：ゾーンの列挙（Zone enumeration）

ゾーンの列挙は**ゾーンウォーキング**（Zone walking）または **DNS ウォーキング**（DNS walking）などとも呼ばれており、特に.jp や.com/.net などといった TLD においては、セキュリティやプライバシーなどの観点から、DNSSEC 導入の障害となっていました[2]。

そのため IETF はこの問題を解決するために DNSSEC の仕様を改良し、RFC 5155 で定義される **NSEC3**（次で説明）として定めました。

[2] 例えば、入手したドメイン名の一覧を利用して spam メールを無差別に送信する、といった迷惑行為が考えられます。

※掲載内容は2015年1月現在のものです。

Q4 NSEC3 とは何ですか？

DNSSEC による不在証明を従来の NSEC から、名前情報をハッシュした結果を利用する NSEC3 に変更することで、**名前情報の列挙を困難にする**ための拡張方式をいいます（図3）。

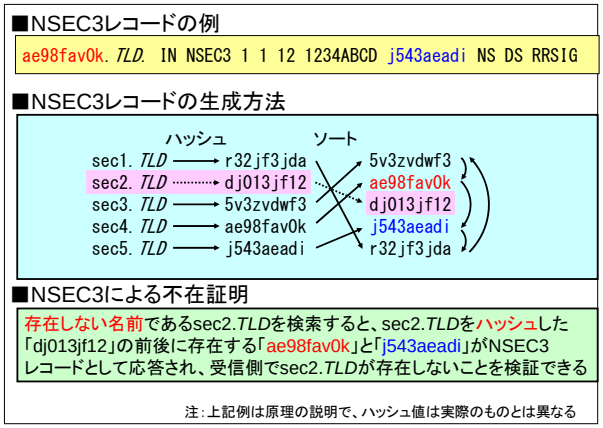

図3：NSEC3 レコードの概要

.jp や.com/.net などの主要な TLD では、NSEC3 を用いた DNSSEC の導入が図られています。

Q5 従来の NSEC はもう使われないのですか？

ゾーンの管理者は不在証明の方式として NSEC または NSEC3 のいずれかを、**それぞれのゾーン単位で自由に選択できます。**

従来の NSEC ではゾーンの列挙を抑制することはできませんが、NSEC3 と比較した場合にゾーン情報の管理運用が容易で、ゾーン情報を管理する権威 DNS サーバー、DNSSEC を検証するキャッシュ DNS サーバーの双方の負荷を低くできるという特徴があります。そのため、ゾーンの内容が既知であるルートゾーンや in-addr.arpa や ip6.arpa といった DNS 逆引き用ゾーンでは NSEC3 ではなく、従来の NSEC による DNSSEC の導入が図られています。

Q6 DNSSEC が導入されることで動作に影響の出る既存のソフトウェアはありますか？

一般的な DNSSEC の導入では DNS クライアントとキャッシュ DNS サーバー間における DNS 問い合わせ・応答のやり取りは変化しないため、各種 DNS クライアント（クライアント PC や各種サーバーソフトウェアなど）における**特別の対応は、基本的に必要ありません。**

ただし **ANY レコードに対する応答だけは例外**で、DNSSEC の導入と同時にキャッシュ DNS サーバーからの応答サイズが、無条件に大きくなります。

現時点において、メール配送ソフトウェアである qmail 1.03 がこの影響を受ける可能性があることが報告されており[3]、パッチの適用などの対応が必要になります。

Q7 DNSSEC 検証に失敗した場合どうなりますか？

DNSSEC 検証に失敗した場合、キャッシュ DNS サーバーは DNS クライアント側に、名前解決に失敗したことを示す「Server failure」エラーを返します。

このエラーは、いわゆる Lame delegation や権威 DNS サーバーの設定不備・サーバーダウンなどにより、名前解決が失敗した場合と同じものです。そのため、エラーを受け取った Web ブラウザーなどの DNS クライアントは従来の場合と同様、「指定された Web ページが表示できない」といったエラーメッセージを表示します（図4）。

図4：DNSSEC 検証に失敗した場合の動作

Q8 DNSSEC 導入後にキャッシュポイズニング攻撃による偽情報の注入が成功したらどうなりますか？

DNSSEC の導入によりキャッシュポイズニング攻撃の検知が可能になります。BIND 9 や Unbound などの現在の主なキャッシュ DNS サーバーの実装では、「Server failure」エラーを返すことで、偽サイトへの誘導を防止しています。

[3] 詳細については JPRS 公開文書「qmail/netqmail における 512 バイトを超える DNS 応答の不適切な取り扱いについて」を参照。
http://jprs.jp/tech/notice/2011-03-03-inappropriate-handling-for-long-dns-packet.html

