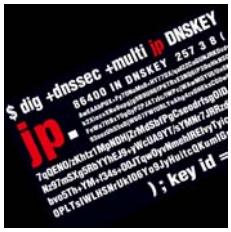
JPRS トピックス＆コラム



■本格運用が始まったDNSSEC
～運用ノウハウの蓄積と共有が今後の課題に～

ルートゾーン及び．jpゾーンにおけるDNSSEC対応が完了し、本格運用が始まりました。ルートゾーンとTLDにおけるDNSSECの導入状況と今後の課題について解説します。

■ルートゾーンへの DNSSEC 導入の実現

あるドメイン名を DNSSEC で検証するためには、検証する側が信頼の拠点（トラストアンカー）として設定したゾーンからそのドメイン名のゾーンまでのすべての階層において、DNSSEC による信頼の連鎖が構築されている必要があります。

DNS はルートゾーンを基点とする階層構造により構成されています。そのため、ルートゾーンが DNSSEC に対応することにより、DNS における権限委任の構造と DNSSEC における信頼の連鎖の構造を一致させることができ（図 1）、従来の DNS における管理運用の仕組みを DNSSEC にそのまま適用することができます。このため、ルートゾーンに対する DNSSEC の導入の実現が、長年にわたり強く望まれてきました。

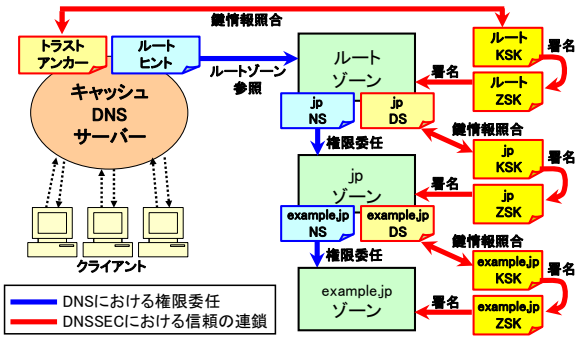


図 1：DNS の権限委任と DNSSEC の信頼の連鎖

▼ルートゾーンへの導入が遅れた理由

このような背景から、ルートゾーンにおける DNSSEC の導入は、DNSSEC が開発され始めた 1990 年代から 2000 年代を通じての、解決すべき大きな課題の一つとなりました。しかし、いくつかの理由によりルートゾーンへの DNSSEC の導入は、当初の目論見よりも大きく遅れることとなりました。

ルートゾーンへの DNSSEC の導入が遅れた理由として、DNSSEC のプロトコルそのものの開発に想定以上の時間を要したこと、インターネットにおける意思決定の構造が複雑化し、より多くの時間を要するようになったことなどが挙げられます。

中でも一番大きなものとして、インターネットそのものの重要性の向上を挙げることができます。その誕生から現在までの間に、研究者や技術者のためのネットワークであったインターネットはその役割を大きく変え、今や重要な社会基盤の一つとして、私たちの活動に不可欠ともいえる存在になりました。これは、インターネットそのものが大きく成長しその重要性が飛躍的に向上したことを示していますが、一方、その管理運用、特に DNSSEC や IPv6、あるいは国際化ドメイン名（IDN）などといったインターネットの根幹部分に対する新技術の導入に対し、より慎重な検討が求められるようになったということも意味しています。

▼慎重に進められたルートゾーンへの導入

そのため、ルートゾーンへの DNSSEC の導入は、既存のインターネットへの影響を最小限にとどめるべく、細心の注意を払った慎重かつ段階的な導入が図られることとなりました。ルートゾーンへの DNSSEC の導入を図る専門のデザインチームが ICANN に組織され、DNS-OARC[1]などの専門家の協力を得ながら、既存の DNS への影響を最小限にとどめる形で導入が進められていきました。

そして、これに並行する形でルートゾーンの管理を担当する IANA における体制の整備が進められ、TLD からの DS 情報の登録申請を受け付けるための準備が整えられました。

[1] The DNS Operations, Analysis, and Research Center
インターネットで広く利用されている DNS に関する運用、分析、調査研究に関する各種活動を通じ、DNS をより安全で高品質なものとすることを目的として、2004 年に設立された国際組織です。

※掲載内容は2011年1月現在のものです。

▼本格運用開始に向けた大きな一歩が実現

その後、ルートゾーンにおける鍵署名鍵(KSK)の作成・使用のための作業が、世界のインターネットコミュニティを代表するメンバーである TCR[2]の立会い・参加の下で進められました。

そして、DNS 応答の偽造による脅威を最初に指摘した論文[3]が執筆されてから20年目となる2010年、ルートゾーンへの DNSSEC の導入が実現し、本格運用開始に向けた大きな一歩を踏み出すこととなりました。

■TLD における DNSSEC の導入が急速に進展

ルートゾーンの DNSSEC への対応を受け、TLD における DNSSEC の導入が急速に進展しています。2011年1月3日現在、ルートゾーンに存在する295の TLD のうち65の TLD が自らのゾーンの DNSSEC 署名を実施しており(表 1)、そのうち59の TLD がルートゾーンへの DS レコードの登録・公開を完了しています。

TLD種別	主なTLD
ccTLD	be(ベルギー), bg(ブルガリア), br(ブラジル), ch(スイス), cl(チリ), cz(チェコ), dk(デンマーク), eu(欧州連合), fi(フィンランド), fr(フランス), gr(ギリシャ), in(インド), jp(日本), my(マレーシア), se(スウェーデン), th(タイ), uk(英国), us(米国)など
gTLD	asia, biz, cat, edu, gov, info, museum, net, org
その他	arpa

表 1:ゾーンの署名を実施済みの主な TLD

■本格運用が始まった DNSSEC

JPRS では 2009 年 7 月に JP ドメイン名における DNSSEC 対応を正式に表明し、具体的な準備を進めてきました。その後、2010 年 10 月に.jp ゾーンへの DNSSEC 署名を、2010 年 12 月にルートゾーンへの DS 情報の登録・公開を実施しました。

JPRS では.jp ゾーンへの署名、及びルートゾーンにおける DS 情報の登録・公開がインターネットに悪影響を及ぼさなかったことを確認した後、2011 年 1 月 16 日に指定事業者からの DS レコードの登録受け付けと JP DNS における提供を開始し、JP ドメイン名サービスにおける DNSSEC の正式運用を開始しました。

2011 年第一四半期には、.com における DNSSEC の運用も開始されます。これにより.jp 及び.com という、日本で最も多く運用されている二つの TLD において DNSSEC の本格運用が開始され、今後の普及に向けた新たな段階を迎えることになります。

■運用ノウハウの蓄積・共有が今後の課題

一方、DNSSEC への本格対応が世界的に始まった 2010 年には、DNSSEC に関連する障害が TLD を含むいくつかのドメイン名において発生しました。2010 年に発生した DNSSEC に関連する主な障害事例を表 2 に示します。

組織名・概要／ドメイン名	障害の原因・概要
RIPE NCC (欧州地域のRIR)	管理システムの障害による 署名の有効期限設定ミス
Nominet UK (.ukのccTLDレジストリ)	主システムとバックアップ システムにおける鍵の相違
Mozilla Foundation (mozilla.org)	自ゾーンの署名よりも先に DSレコードを親に登録
Internet Architecture Board (iab.org)	署名の有効期限切れ オペレーションミスと思われる

表 2:2010 年に発生した主な障害事例

今後、このような障害の早期発見と再発防止を図っていくためには、DNSSEC に関する運用経験とそこから得られるさまざまな運用ノウハウの蓄積と共有が必要になります。

JPRS では関係者と共同で進めている技術検証結果や DNSSEC 関連技術文書・関連 RFC の翻訳の公開、DNSSEC の導入・普及のために設立された DNSSEC ジャパンにおける活動などを通じ、運用経験と運用ノウハウの蓄積・共有を図っています。

DNSSEC によりインターネットの安全性を向上させるためには、インターネットで DNS を管理運用するすべての関係者の協力が欠かせません。JPRS では今後も各方面の関係者と協力しながら、DNSSEC の導入を推進していきます。

[2] Trusted Community Representatives の略で、「信頼されたコミュニティの代表者」を意味しています。TCR は DNSSEC で使用する鍵の生成・保管のための機器の稼動や、鍵の生成・更新のために実行される一連の手続き(キーセレモニー)への参加などの役割を担います。

[3]既に広まりつつあったインターネットへの影響の大きさを考慮し、著者のスティーブン・ベロビン氏はこの論文を 5 年後の 1995 年まで発表しませんでした。