DNSの動向

森下 泰宏 ●株式会社日本レジストリサービス（JPRS） 広報宣伝室 技術広報担当・技術研修センター

運用経験に基づくDNSSEC設定の推奨値見直しと対応が進められている。また、ルートゾーンKSKロールオーバーの検討が再開され、権利侵害を理由としたDNSブロッキングの世界的な動きに注目が集まっている。

■DNSSECパラメーター設定の推奨値見直しに伴う対応

2010年にルートゾーンが署名され、DNSSECの正式運用が開始された。現在ではすべてのgTLDと.jpを含む主要なccTLDにおいてDNSSECが利用可能になっており、普及が進められている。

運用開始から10年以上に及ぶ経験に基づき、DNSSEC運用におけるパラメーター設定の推奨値の見直しが進められている。本稿ではその一つとして、2022年8月に発行されたRFC 9276[1]の概要と、RFCの発行を受けたTLDの対応について解説する。

●RFC 9276の概要

RFC 9276はDNSSECの不在証明[2]に使われるNSEC3（後述）のパラメーター設定と検証における取り扱いの指針をまとめたもので、重要な運用手法を定めた「現状における最良の慣行（Best Current Practice: BCP）」の一つとなっている（BCP 236）。

RFC 9276では、NSEC3の基本仕様（RFC 5155）[3]で定められているパラメーター設定の推奨値の一部が変更されている。NSEC3は.jpを含む多くのTLDで採用されているため（後述）、それらのTLDレジストリにおいて、変更への対応が進められている。

▼DNSSECにおける不在証明の概要と採用状況

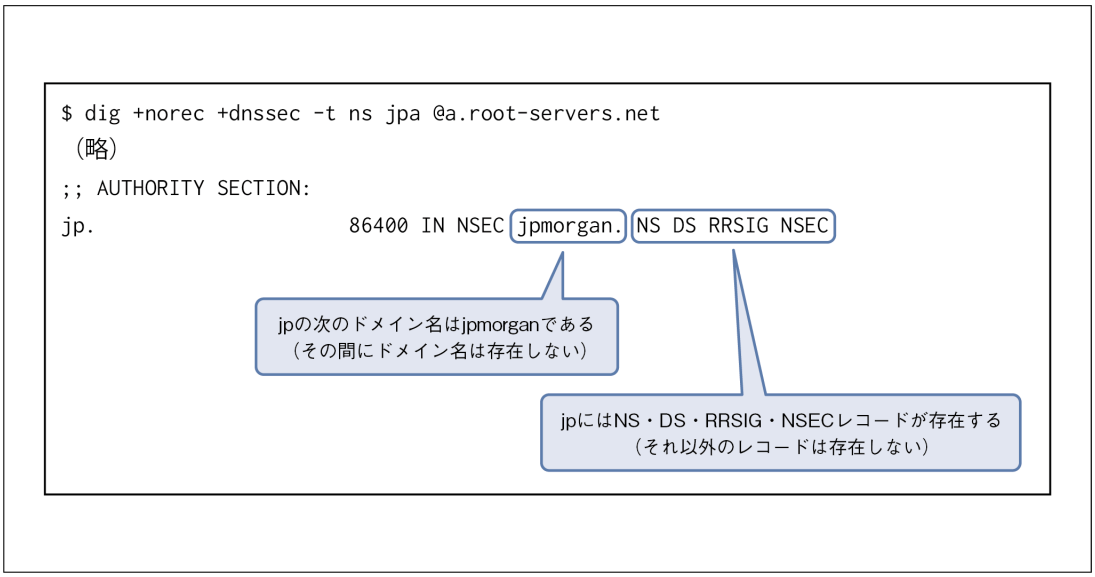
DNSSECの不在証明にはNSECとNSEC3という2つの方式がある。各ゾーンの管理者はいずれか一方の方式を選択して、自ゾーンをDNSSECに対応させる[4]。

NSECによる不在証明では、そのゾーンに存在する「前後の」ドメイン名を示すことで、問い合わされたドメイン名が存在しないことを提示する。この際の前後はそのゾーンのドメイン名ラベルの大文字を小文字と見なした上で、ASCIIコード順にソートすることで決定される。NSECレコードの例とその意味を、資料4-3-13に示す。

NSECはシンプルである半面、あるゾーンのNSECレコードをゾーン頂点から順に検索し、応答のNSECレコードに記述されたすべてのレコードタイプを検索することで、そのゾーンのすべてのデータを外部から入手可能になる。この行為はゾーン列挙（Zone enumeration）[5]と呼ばれ、DNSSECの普及の妨げになり得ることが、IETFで指摘された。

この指摘に対応するため、ドメイン名そのもの

資料4-3-13　NSECレコードの例とその意味（ルートサーバーにjpaのNSレコードを問い合わせた際の応答）



出所：筆者作成

に替えてドメイン名のハッシュ値を不在証明に用いることでゾーン列挙に要するコストを高める、NSEC3が標準化された。NSEC3による不在証明の仕組みを、資料4-3-14に示す。

なお、NSEC3にはドメイン名登録数の多いTLDにおいて段階的なDNSSECの導入をしやすくする、Opt-Out[6]の機能も追加されている。こうした状況から現在のインターネットでは、.com/.netや.jpを含む多くのTLDにおいて、NSEC3による不在証明が採用されている。

▼RFC 9276における重要な変更内容

NSEC3にはソルト[7]付きのハッシュ計算を繰り返すことで、ゾーン列挙にかかるコストを高められる機能がある。ソルトと繰り返し回数は各ゾーンの管理者が、自分の権威DNSサーバーのNSEC3PARAMレコードで設定する。

RFC 9276では、ハッシュ計算の繰り返しによるパフォーマンスの低下が名前解決に影響を及ぼすことを懸念する観点から、権威DNSサーバーで設定する繰り返し回数と受信側のDNSSEC検証における取り扱いを以下のように定め、RFC 5155の内容を更新している。

・権威DNSサーバーで設定する繰り返し回数を0、ソルトを空に設定しなければならない（MUST）
・DNSSEC検証において、応答に設定されている繰り返し回数が0より大きかった場合は検証を実施せず、検証できないため安全ではない（Insecure）、またはDNSSEC検証失敗（SERVFAIL）を返してよい（MAY）

●DNSSEC運用への影響とTLDにおける対応

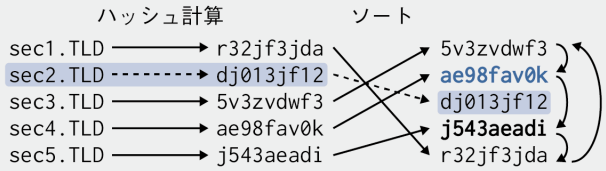
RFC 9276では、DNSSEC検証においてInsecure応答やSERVFAIL応答を返す場合の設定値について「慎重に検討されなければならない（must be considered carefully）」としている。しかし、今後本RFCの記述が厳格に適用され、0

資料4-3-14　NSEC3による不在証明の仕組み

■ NSEC3レコードの例

```
ae98fav0k.TLD. IN NSEC3 1 1 0 - j543aeadi NS DS RRSIG
```

■ NSEC3レコードの生成方法



■ NSEC3による不在証明

存在しない名前sec2.TLDを検索すると、sec2.TLDをハッシュ計算した結果「dj013jf12」の前後に存在するハッシュ計算した値「ae98fav0k」と「**j543aeadi**」がNSEC3レコードで応答され、sec2.TLDが存在しなかったことが提示される

注：上記の例は原理の説明であり、ハッシュ値は実際のものとは異なる

出所：筆者作成

より大きい繰り返し回数が設定されているゾーンの名前解決においてSERVFAIL応答が返されるように設定された場合、TLDレベルでの大規模な名前解決エラーが発生する可能性がある旨が指摘されている[8]。

このような状況の発生を防ぐため、複数のTLDにおいてNSEC3パラメーターの設定をRFC 9276の推奨値である繰り返し回数0、ソルトを空に変更する対応が進められている[9]。

なお、JPRSが管理する.jprsと.jp、およびJPRSがTLD総合支援サービスを提供している.nttと.sakuraにおいても資料4-3-15の通り、NSEC3パラメーターを繰り返し回数0、ソルトを空に変更する対応を実施済みとなっている。

■今後のルートゾーンKSKロールオーバーに向けた検討の状況

ルートゾーンKSKロールオーバーは、ルートゾーンのDNSSEC鍵署名鍵（KSK）を更新する際の、一連の作業手続きである。セキュリティ上の理由から、ルートゾーンのKSKは運用開始から5年程度で更新することが運用ポリシーに定められており、前回のKSKの更新は、2018年10月に実施されている[10]。

ICANNでは2019年11月に今後のルートゾーンKSKロールオーバーの提案に関するパブリックコメントを募集し、検討を進めていた[11]。しかし、2020年からの新型コロナウイルス感染症の急速な拡大への緊急対応と、対面でのオペレーションを必要とするルートKSKセレモニー[12]が実施不可能になったことから、検討を一時中断する旨を2020年8月に発表した[13]。

ICANNは検討の再開時期を対面でのオペレーションと米国への旅行が安全に再開できる確信が高まった時点としており、2022年9月に開催されたICANN75 Meetingにおいて、作業を再開する旨を発表した[14]。

資料4-3-15　NSEC3パラメーターの変更年月日

TLD	変更年月日
.jprs	2022年10月25日
.jp	2022年11月29日
.ntt	2022年12月20日
.sakura	2022年12月20日

出所：筆者作成

●次回のルートゾーンKSKロールオーバーの予定

2022年11月に開催されたIANA Community Dayにおいて、次回のルートゾーンKSKロールオーバーに関する検討状況が発表された[15]。

発表では、新しいKSKの事前公開期間をこれまでより長い2年間とし、ソフトウエアやデバイスが新しいKSKに対応するための十分な期間を設定すること、2023年第2四半期までに新しいKSKを作成する準備を整えることが共有された。

具体的な計画は今後、ICANNのメーリングリストおよびウェブサイトで発表される予定である。

●将来のアルゴリズムロールオーバーに向けた検討の状況

DNSSECで使われる暗号・署名のアルゴリズムを変更することを、アルゴリズムロールオーバーと呼ぶ。DNSSECによる保護を維持する形でアルゴリズムロールオーバーを実施する場合、所定の手順が必要になる。

従来、DNSSECでは署名鍵のアルゴリズムとして、RSAを用いた方式が広く使われてきた。これを楕円曲線デジタル署名（ECDSA）やエドワーズ曲線デジタル署名（EdDSA）を用いた方式に変更することで同じレベルの安全性をより短い鍵で実現でき、署名のサイズ、つまりDNS応答のサイズをより小さくできる。

そうしたメリットから、.chや.czなどのTLDではECDSAを用いた方式へのアルゴリズムロールオーバーを実施済みとなっており、ルートゾーンにおいても将来のアルゴリズムロールオーバーに向けた検討が必要になる旨が識者から指摘されていた。

ICANNではこうした指摘を受け、ルートゾーンのアルゴリズムロールオーバーの手順と計画の作成を支援するためのデザインチームの結成を決定し[16]、2022年11月に募集を開始した[17]。デザインチームは2023年1月に活動を開始し、2023年6月に最終的な推奨事項を公開する予定である旨が、ICANNから発表されている。

なお、次回のルートゾーンKSKロールオーバーではアルゴリズムロールオーバーを予定していない旨がPTI[18]から発表されている。

■権利侵害を理由としたDNSブロッキングに関する動き

2022年7月にイタリア・ミラノの裁判所がCloudflareに対し、権利侵害に利用されていた3つのドメイン名を対象に、同社のパブリックDNSサービス「1.1.1.1」における名前解決のブロッキングを命令した[19]。同社は命令を不服として上訴していたが、2022年11月に却下され、原判決が確定した[20]。

Cloudflareのウェブコンテンツ配信サービスでは顧客のウェブコンテンツについて、政府機関や裁判所などから法律に基づくブロッキング要請を受け取った場合、当該地域におけるアクセスブロッキングを実施している[21]。しかし、同社では

1.1.1.1はエンドユーザーに名前解決を提供するパブリックDNSサービスであり、名前解決されたドメイン名の使用目的やアクセス先のコンテンツの内容はサービス・責任の対象外であるとして、要請に基づく名前解決のブロッキング・結果の変更などはこれまで、実施していなかった。

裁判所の命令では、違法行為の繰り返しを防ぐための名前解決の抑制についても同社のサービスにおける注意義務であるとしており、より踏み込んだ内容になっている[22]。同様の判決は2021年7月にドイツ・ハンブルクの裁判所において、パブリックDNSサービスを提供しているQuad9に対しても出されており、係争中となっている[23]。

Quad9は本件について、DNSブロッキングの安易な適用は利用者やインターネットサービスに対する検閲・政治的動機による乱用・オーバーブロッキングなどにつながり、インターネットの根幹を脅かすものであるとし、この決定に反対する旨の意見を表明している[24]。

なお、わが国では、2011年から目的をインターネット上の児童ポルノ流通対策に限定した上で、DNSブロッキングが運用されている[25]。しかし、権利侵害を理由としたDNSブロッキングについてはWIDEプロジェクト[26]をはじめ、さまざまな団体が反対意見を表明しており[27]、問題点を明確にし、議論を深めるための緊急シンポジウムも開催されている[28]。

■DNSソフトウエアの脆弱性の状況

●BINDの脆弱性の状況

資料4-3-16に、2022年中にJPRSが注意喚起したBINDの情報を示す。2022年中に公開された11件の脆弱性のうち5件が、2022年1月にリリースされた最新の安定版ブランチである、BIND 9.18系列のものとなっている。

なお、Internet Systems Consortium（ISC）ではBINDの新しいブランチについて、大規模な本番環境への適用は、3回目のメンテナンスリリースまで待つことを推奨している[29]。

●BIND以外のDNSソフトウエアの状況

資料4-3-17に、2022年中にJPRSが注意喚起したBIND以外のDNSソフトウエアの情報を示す。

2022年4月のマイクロソフトのセキュリティ更新プログラム（月例パッチ）で、Windows DNSサーバーの脆弱性が18件報告されている。うち17件はリモートコード実行（RCE）が可能になる重大な脆弱性であり、速やかなパッチの適用が必要である。

なお、18件の脆弱性のうち15件は中国のセキュリティ企業の研究者で、著名なバグバウンティハンターでもある、Yuki Chen（陳雪斌）氏が報告したものである。

●Phoenix Domain脆弱性に関する予告

2022年10月に清華大学のXiang Li（李想）氏らの研究グループが、DNSの新たな脆弱性「Phoenix Domain」を発見したと発表した[30]。

本脆弱性は2012年に発表された幽霊ドメイン名脆弱性[31]と同様、親ゾーンの委任情報が削除された後も長期にわたってドメイン名を名前解決可能、つまり使用可能な状態にし続けるように仕向けることができるというものである。具体的な詳細は2023年2月に開催されるNDSS Symposium 2023[32]で発表される予定となっており、本稿執筆時点では公開されていない。

なお、Phoenix Domainの公式ページ[33]には、BIND、Unbound、Google Public DNS、1.1.1.1を含む7種類のDNSソフトウエアと15種類のDNSサービスが脆弱であったことを確認した旨が記載されている。

資料 4-3-16　2022 年に JPRS が注意喚起した BIND の情報

公開・更新日	タイトル
2022/3/17	（緊急）BIND 9.18.0 の脆弱性（DNS サービスの停止）について（CVE-2022-0667）
2022/3/17	（緊急）BIND 9.18.0 の脆弱性（DNS サービスの停止）について（CVE-2022-0635）
2022/3/17	BIND 9.x の脆弱性（システムリソースの過度な消費）について（CVE-2022-0396）
2022/3/17	BIND 9.x の脆弱性（キャッシュポイズニングの危険性）について（CVE-2021-25220）
2022/5/19	（緊急）BIND 9.18.x の脆弱性（DNS サービスの停止）について（CVE-2022-1183）
2022/9/22	（緊急）BIND 9.18.x の脆弱性（メモリリークの発生）について（CVE-2022-2906）
2022/9/22	BIND 9.x の脆弱性（パフォーマンスの低下）について（CVE-2022-2795）
2022/9/22	BIND 9.18.x の脆弱性（不適切なメモリの読み取りまたは DNS サービスの停止）について（CVE-2022-2881）
2022/9/22	（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（CVE-2022-3080）
2022/9/22	（緊急）BIND 9.x の脆弱性（メモリリークの発生）について（CVE-2022-38177）
2022/9/22	（緊急）BIND 9.x の脆弱性（メモリリークの発生）について（CVE-2022-38178）

出所：筆者作成

資料 4-3-17　2022 年に JPRS が注意喚起した BIND 以外の DNS ソフトウエアの情報

公開・更新日	タイトル
2022/2/10	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2022-21984）
2022/3/30	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2022-27227）
2022/3/30	PowerDNS Authoritative Server の脆弱性情報が公開されました（CVE-2022-27227）
2022/4/15	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2022-24536、他 17 件）
2022/7/15	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2022-30214）
2022/8/4	Unbound の脆弱性情報が公開されました（CVE-2022-30698、CVE-2022-30699）
2022/8/26	PowerDNS Recursor の脆弱性情報が公開されました（CVE-2022-37428）
2022/9/16	Windows DNS サーバーの脆弱性情報が公開されました（CVE-2022-34724）
2022/9/27	Knot Resolver の脆弱性情報が公開されました（CVE-2022-40188）
2022/9/27	Unbound の脆弱性情報が公開されました（CVE-2022-3204）

出所：筆者作成

1. RFC 9276: Guidance for NSEC3 Parameter Settings、https://www.rfc-editor.org/rfc/rfc9276
2. 問い合わされたドメイン名やリソースレコードが存在しないことの証明。
3. RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence、https://www.rfc-editor.org/rfc/rfc5155
4. DNSSEC の仕様により、1 つのゾーンに NSEC と NSEC3 を併用させることは不可能である。
5. DNSSEC 関連情報〜よくある質問〜/ JPRS、https://jprs.jp/dnssec/faq.html
6. DNSSEC 非対応の子ゾーンの委任情報を DNSSEC の対象から除外することで、署名済みゾーンのデータサイズを小さくする機能。
7. 元データを推測しにくくするため、ハッシュ値を計算する際に入力に付加するランダムなデータ。
8. OARC 38 (30-July 31, 2022): Are we ready for nsec3-guidance? ・DNS-OARC (Indico)、https://indico.dns-oarc.net/event/43/contributions/923/
9. RFC 9276, Afnic adopts the no-salt diet、https://www.afnic.fr/en/observatory-and-resources/expert-papers/rfc-9276-afnic-adopts-the-no-salt-diet/
10. ICANN が新 KSK への切り替え成功と、今後の予定を発表、https://jprs.jp/tech/notice/2018-10-25-rootzonekskrollover-update.html
11. Proposal for Future Root Zone KSK Rollovers、https://www.icann.org/en/public-comment/proceeding/proposal-for-future-root-zone-ksk-rollovers-01-11-2019
12. ルートゾーンの DNSSEC 鍵ペアを生成する、一連の手続き。
13. Staff Report of Public Comment Proceeding - Proposal

for Future Root Zone KSK Rollovers、https://itp.cdn.icann.org/en/files/root-zone-key-signing-key-ksk-rollover/report-comments-proposal-future-rz-ksk-rollovers-07aug20-en.pdf

14. ICANN75 | Annual General Kuala Lumpur: Meeting Details、https://75.schedule.icann.org/meetings/8jcmXcKTEoPTr3NQw
15. IDS 2022 agenda 2022-11-14、https://www.icann.org/en/system/files/files/agenda-ids-brussels-15nov22-en.pdf
16. Root Zone KSK Algorithm Rollover – ICANN、https://www.icann.org/resources/pages/ksk-algorithm-rollover-en
17. ICANN Calls for Volunteers to Plan for Changing the Root Zone DNSSEC Algorithm、https://www.icann.org/en/announcements/details/icann-calls-for-volunteers-to-plan-for-changing-the-root-zone-dnssec-algorithm-03-11-2022-en
18. ICANNの子会社で、ドメイン名、IPアドレス、プロトコルパラメーターなどのインターネット資源を管理する、IANAの役割を担っている。、https://pti.icann.org/
19. Court Orders Cloudflare's DNS Resolver 1.1.1.1 to Block Pirate Sites in Italy * TorrentFreak、https://torrentfreak.com/court-orders-cloudflares-dns-resolver-1-1-1-1-to-block-pirate-sites-in-italy-220719/
20. 海賊版サイトにパブリックDNSリゾルバ「1.1.1.1」から接続できなくするよう裁判所がCloudflareに命令– GIGAZINE、https://gigazine.net/news/20221110-public-dns-1111-blocking-order/
21. Cloudflare - Transparency Report、https://www.cloudflare.com/media/pdf/transparency-report.pdf
22. TRIBUNALE ORDINARIO DI MILANO TRIBUNALE DELLE IMPRESE SEZIONE QUATTORDICESIMA - IMPRESA A、https://torrentfreak.com/images/Ordinanza-reclamo-Cloudflare-4-novembre-2022.pdf
23. ソニーミュージックが「海賊版配信サイトのブロック命令」を無料のDNSリゾルバに対して勝ち取る– GIGAZINE、https://gigazine.net/news/20210628-sony-music-quad9-pirate-site-blocking/
24. An Update to the Quad9 and Sony Music German Court Injunction - August 2022 | Quad9、https://www.quad9.net/news/blog/an-update-to-the-quad9-and-sony-music-german-court-injunction-august-2022/
25. 児童ポルノブロッキング| 一般社団法人インターネットコンテンツセーフティ協会– ICSA、https://www.netsafety.or.jp/blocking/
26. 著作権法違反を理由とする接続遮断措置（サイトブロッキング）についての意見表明、https://www.wide.ad.jp/News/2018/20180912.html
27. 海賊版サイトの“ブロッキング”、通信業界団体などから憂慮・反対の声- INTERNET Watch、https://internet.watch.impress.co.jp/docs/news/1116597.html
28. 海賊版サイトのブロッキングはなぜ無理筋なのか？　反対派の市民団体やISP業界団体が緊急シンポジウム開催【これからのネットづくりと海賊サイトへのブロッキング要請を考える】- INTERNET Watch、https://internet.watch.impress.co.jp/docs/event/1117888.html
29. Which version of BIND do I want to download and install?、https://kb.isc.org/docs/aa-01540
30. OARC 39 & 47th CENTR Technical Workshop (22-October 23, 2022): Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation・DNS-OARC (Indico)、https://indico.dns-oarc.net/event/44/contributions/953/
31. ghost domain names（幽霊ドメイン名）」脆弱性について、https://jprs.jp/tech/notice/2012-02-17-ghost-domain-names.html
32. DSS Symposium 2023: February - 3 March 2023 in San Diego, CA、https://www.ndss-symposium.org/ndss2023/
33. Phoenix Domain
https://phoenixdomain.net/

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dおよび株式会社インプレスが1996年～2023年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&Dおよび株式会社インプレスと著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | インプレス・サステナブルラボ | ✉ iwp-info@impress.co.jp