TTCに寄せて

IETFでの標準化活動を振り返って
～TTC会長表彰を受賞して～

株式会社日本レジストリサービス(JPRS)
藤原　和典

1．はじめに

この度は「インターネットのドメインネームシステムの標準化にかかわる功績」に対して名誉ある情報通信技術賞 TTC 会長表彰を賜り、大変光栄に存じます。今回の受賞は、これまでの私の IETF での標準化活動を支援してくださった皆様のおかげだと思っております。この場をお借りして感謝を申し上げます。

2．IETF における標準化の流れ

Internet Engineering Task Force（IETF）は 1986 年に設立された、インターネットの標準技術を開発する標準開発組織（SDO）です。

IETF における標準化は ITU-T や 3GPP、W3C などの標準化とは異なり、個人が提案し、意見を述べ、Rough Consensus（緩やかな合意）を作り、IETF の活動と標準化プロセスを管理する Internet Engineering Steering Group（IESG）のレビューを経て、技術仕様である RFC を発行する形で進められます。

表 1　IETF と ITU-T の比較

	IETF	ITU-T
組織の形態	コミュニティに基づくボトムアップ型組織	憲章・条約に基づくトップダウン型組織
重視される項目	実装の開発	仕様の策定
標準の必要条件	相互接続性	高い品質
参加者の立場	個人のボランティア	国単位のメンバー
意思決定の仕組み	大まかな合意	メンバーによる決議
標準化文書の形式	Request for Comments（コメント求む）	Recommendations（勧告）

IETF ではアイデアを持つ者がメーリングリストで問題点や意見を表明し、自分のアイデアを Internet-Draft（I-D、草案）として提出します。IETF には個人の立場で参加しますが、I-D に所属組織名を書いたり、所属組織のメールアドレスを連絡先に使ったりすることもできます。提出された I-D はその内容を取り扱うワーキンググループ（WG）で議論されます。

IETF では年に３回、一週間のミーティングを開催しており、60 分から２時間程度、WG に分かれた会議が開かれます。発表を希望する場合、締切日の前に I-D を提出した上でメーリングリストにその旨を伝え、WG の議長（WG チェア）に発表時間を要求します。発表後は否定的な意見も含め、寄せられたコメントやメーリングリストでの議論を反映する形で、内容を更新していきます。

WG チェアが I-D の内容について関心が高いと判断した場合、WG での標準化の対象とするかをメーリングリストで問いかけます。これを WG adoption といい、対象となった I-D は WG 全体で作業が進められます。

WG での議論がまとまった時点で WG チェアが最終確認（Working Group Last Call）を実施し、Rough Consensus が成立したと判断した時点で IESG に I-D を送り、RFC の発行を申請します。

IESG は IETF の活動分野ごとに定められたエリアを担当する、エリアディレクター（AD）の集合です。IETF は７つのエリアで構成され、各エリアの AD がエリア間の調整と I-D の評価を担当しています。

発行申請された I-D は担当エリアの AD によるレビュー、IETF 全体への最終確認（IETF Last Call）、IESG メンバー全員によるレビューを経て発行が承認され、RFC Editor に送られます。その後、３～４カ月の編集作業を経て、RFC として発行されます。

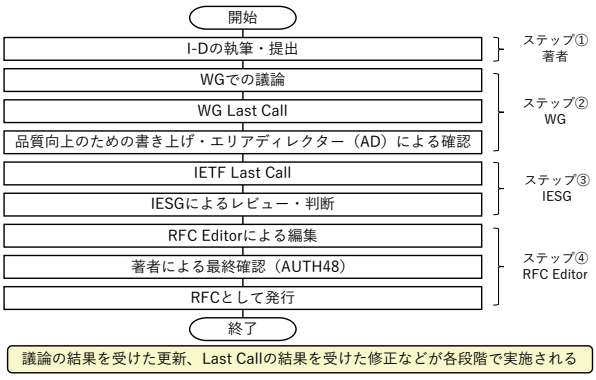

図 1　IETF における標準化の流れ

RFC にはその識別のために、通し番号が付けられます。通常、番号への配慮はありませんが、重要な RFC の改訂では以前の番号と似た番号や 1000 番後の番号などが、意図的に割り当てられる場合があります。

3．ENUM、EAI の標準化活動への参加

私は 2002 年 6 月に現在の所属先である株式会社日本レジストリサービス（JPRS）に転職しました。ENUM 技術、及び DNS 関連技術の調査・研究が、私の最初の仕事となりました。

3.1　Telephone Number Mapping（ENUM）

ENUM は電話番号をドメイン名に対応付けることで IP 電話や Web の URL など、さまざまなサービスを対応させる仕組みです。当時、JPRS は ENUM 研究グループや ENUM Trial Japan（ETJP）などと連携して、実装の試作などを行なっていました。そうした経緯から情報収集の形で IETF に参加することとなり、enum WG と DNS 関係の WG を中心に、ミーティングにも参加し始めました。

当時の enum WG では標準化作業に加え、各国における取り組みも発表されており、2004 年 3 月に開催された IETF 59 の enum WG において、日本での ENUM 実験の状況を私が報告することになりました。報告で ETJP の活動報告に加え、ENUM の仕様を定める RFC 3761 と、RFC 3761 が参照している RFC 3401、3402 などの曖昧な点を指摘したところ、WG で議論が進んでいた ENUM の実装経験の I-D に共著者として加わるように、enum WG のチェアから指示されました。

その後、WG の議論と WG チェアの指示に従う形で英国の Lawrence Conroy 氏と共に I-D を更新し、2009 年 3 月に RFC 5483 “ENUM Implementation Issues and Experiences” として発行されました。これが私が著者に名を連ねた、初の RFC となりました。

RFC 5483 は Informational（情報提供）であり Standards Track（標準化過程）ではありませんでしたが、その後、RFC 3761 を改訂する際に RFC 5483 の内容をマージすることとなり、2011 年 3 月に Standards Track である RFC 6116 “The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)” として発行されました。

ENUM は普及しませんでしたが実験は継続しており、ITU-T から委託された RIPE NCC が電話番号とドメイン名の対応付けに使われる「e164.arpa」ゾーンを管理しています。

3.2　Email Address Internationalization（EAI）

JPNIC/JPRS では .jp の ccTLD レジストリとして国際化ドメイン名（IDN）の標準化活動に参加し、漢字を使う中国・韓国・台湾の ccTLD レジストリ（CNNIC、KRNIC、TWNIC）と共に Joint Engineering Team（JET）を結成して、標準化を推進しました。JPRS では 2001 年に日本語 JP ドメイン名の提供を開始、標準化が完了した 2003 年に正式な仕様に移行し、現在に至っています。

その活動の続きとして、2005 年ごろからメールアドレスを国際化するための活動が開始されました。プロトコル国際化の専門家、メールプロトコルの専門家、ccTLD レジストリの技術者などにより Email Address Internationalization（EAI）デザインチームが作られ、そこでの検討を経て 2006 年 3 月に Email Address Internationalization ワーキンググループ（eai WG）が組織されました。

国際化メールアドレスは、メールアドレスのローカル部分（@ の左側）を国際化し、UTF-8 の文字列を許容するものと定義されます。さらに、Subject や From、Cc などのヘッダに追記する display-name にも UTF-8 文字列を許容します。

また、メールの配送に使われる SMTP でも国際化メールアドレスがそのまま使われるため、SMTP の MAIL FROM:＜日本語名@example.jp＞などのメッセージも UTF-8 で送られることになります。

SMTP はメールアドレスとして、ASCII 文字列のみを許容しています。そのため、国際化メールアドレスを使っているメールは従来のメールサーバにそのまま送ることができません。この問題を解決するため、SMTP を拡張した ESMTP ではメールサーバが国際化メールアドレスに対応している旨を示す SMTPUTF8 を返した場合にのみ、国際化メールアドレスを使ったメールを送るという仕様になっています。

デザインチームの当初の案はそれぞれの国際化メー

ルアドレスに ASCII の ALT-ADDRESS を追加しておき、従来のメールサーバに配送する際には送り先を ALT-ADDRESS に変換し、UTF-8 で書かれたヘッダを MIME 形式に変換するという複雑な仕様になっており、私は変換機構の設計を担当しました。

最初の EAI は Experimental（実験）として標準化されました。私が担当した部分は 2009 年３月に RFC 5504 “Downgrading Mechanism for Email Address Internationalization” として発行されました。また、2010 年４月に変換結果をできる限り元に戻して表示できるようにするための RFC 5825 “Displaying Downgraded Messages for Email Address Internationalization” も発行されました。

その後、IETF において実験仕様を Standards Track に置き換えるための作業が進む中で、互換性を保つ部分が削除されることとなりました。しかし、国際化メールアドレスに非対応のメールクライアントを使っている場合、POP/IMAP サーバにおけるメールの削除すらできなくなってしまうため、その部分の互換性を POP/IMAP に実装することで維持することとなり、その仕様の策定と POP への追加を担当しました。その結果、2013 年３月に RFC 6856 “Post Office Protocol Version 3 (POP3) Support for UTF-8” と RFC 6857 “Post-Delivery Message Downgrading for Internationalized Email Messages” が Standards Track として発行されました。

４．DNS の標準化活動への参加

2002 年から IETF ミーティングには継続的に参加していましたが、DNS の標準化の提案はハードルが高く、すぐにはできませんでした。

当時、IETF では DNS を扱う WG としてプロトコルを拡張する DNS Extensions（dnsext）WG と、運用技術を扱う DNS Operations（dnsop）WG の二つが活動していました。そのうち、後述する DNSSEC の標準化を進めていた dnsext WG は 2013 年に活動を終了し、プロトコルの拡張は dnsop WG に引き継がれました。

当時の DNS に関する最大のテーマは、公開鍵暗号を用いた電子署名技術で信頼性を高める、DNSSEC の標準化と普及であり、IETF の dnsext WG とその周辺で DNS ソフトウェア実装者、TLD レジストリ、サービス事業者、米国政府の関連組織などの関係者が集まり、DNSSEC の普及に関する会議やワークショップなどを頻繁に開催していました。私はそうした場に .jp レジストリの技術者として参加することで、DNS 関係の有識者と知り合うことができました。

４．１　DNS 関連で最初に投稿した提案

２年後の 2004 年に NTT コミュニケーションズが運用する OCN の DNS サーバの負荷増大への対応について相談され、NTT コミュニケーションズ、NTT 研究所の技術者と共に北米地域のネットワーク運用者が集まる NANOG ミーティングで、課題を発表することになりました。

その際、著名な有識者の一人である Bill Manning 氏（2020 年に逝去）から、運用上の問題であれば IETF の dnsop WG に I-D を提出すればよいとアドバイスされ、NTT 研究所の外山勝保氏（現：インターネットマルチフィード）、石橋圭介氏（現：国際基督教大学）と３人でホテルの部屋で I-D をまとめ、その後の IETF ミーティングで発表しました。

その問題自体は BIND ８という古い DNS ソフトウェアの実装に起因するものであったため最終的には取り下げましたが、当時の dnsop WG チェアから発表に関するさまざまな便宜を図っていただき、その後の私の活動に大いに役立ちました。

４．２　DNS 用語集（DNS Terminology）

2014 年 10 月に、DNS で使われる用語の定義が不明瞭であり、統一を図るべきだという I-D を提案しました。I-D では Full-Resolver、Referrals といった基本的な用語の定義が不明瞭であること、DNS の仕様を明確化するための RFC 2181 の記述が曖昧であることを指摘しました。

１カ月後の 2014 年 11 月に開催された IETF 91 で複数の有識者から I-D にコメントをいただき、ミーティング会場で多数の RFC を執筆している Paul Hoffman 氏と Andrew Sullivan 氏から、問題解決のため DNS 用語集を作ろうとしていることとその活動への参加を誘われ、共著者として参加しました。活動の成果として、DNS の委任における委任先ゾーンとネームサーバ名の関係を示す “in-domain”、“sibling domain”、“in-bailiwick”、“out-of-bailiwick” という用語の定義を RFC に追加できました。

DNS 用語集は 2015 年 12 月に RFC 7719 として発行された後、RFC 7719 を改訂する RFC

8499 が 2019 年 1 月、RFC 8499 を改訂する RFC 9499 が 2024 年 3 月に、Best Current Practice（BCP：現状における最良の慣行）として発行されました。BCP は重要な運用手法を記述する RFC であり、DNS 用語集には BCP 219 が割り当てられました。2回の改訂は主に dnsop WG チェアの指示によるもので、RFC の発行後に新たに定義された DNS 関連の用語を追加するためのものです。

なお、改訂の際に IETF で決めたものではないとして、一部の用語の定義が変更されています。最新版の RFC 9499 では前述した "in-bailiwick"、"out-of-bailiwick" は非推奨とされ、"unrelated" という用語が新たに定義されています。

4.3　DNSSEC の改良

私は 2010 年から 2015 年まで博士後期課程に在籍し、平日に勤務先の業務、勤務終了後と土曜に授業とゼミに参加する学生生活を送りました。勤務先である JPRS からは、論文執筆のための研究を業務時間、学会発表を業務出張とする形で、サポートを受けました。

私は研究テーマとして DNS の負荷の評価を選び、ルート DNS サーバへの無駄な問い合わせを減らすことで負荷を軽減する手法の研究を進めました。その結果、ルート DNS サーバへの無駄な問い合わせの主な原因が、BIND 9 のバグに起因する本来不必要な多数の問い合わせと、クライアントからの存在しないトップレベルドメイン（TLD）への問い合わせ要求により、ルート DNS サーバに多数の問い合わせを送っていることの2点である旨を特定し、これらを減らすことで負荷を軽減する手法を、論文としてまとめました。

クライアントからの問い合わせの原因として、ユーザの入力間違いや、組織内で閉じるべき問い合わせが組織外に洩れている場合などが挙げられます。また、Chrome ブラウザがネットワーク接続性を確認する際にランダムな TLD の DNS 問い合わせを送っていることも報告されています。

そうした問い合わせを ISP や各組織のフルサービスリゾルバに送ると、フルサービスリゾルバはルート DNS サーバにその問い合わせをそのまま送ります。フルサービスリゾルバには再問い合わせを軽減するキャッシュ機能がありますが、存在しない TLD のキャッシュが活用されるのは問い合わせのドメイン名が以前の問い合わせと完全一致する場合のみであるため、結果として多数の問い合わせがルート DNS サーバに送られることになります。

私はこの問題の解決策として、バグのある実装の使用を避けることと、DNSSEC の仕様を改良し、キャッシュ済みの不存在情報を積極的に活用することでルート DNS サーバに問い合わせることなく不存在エラーを生成する方法を提案し、ルート DNS サーバに送られる問い合わせ数を 96% 削減できることを示しました。

表2　削減可能な問い合わせ数

	ルート DNS サーバ			TLD	その他
	総数	不在	存在		
実測値	118,360	12,579	105,781	687,365	6,524,070
Unbound/L/D	12,662	11,140	1,522	1,423,789	9,112,902
理論値	11,493	10,616	877		
NSEC により削減できるクエリ数 (理論値)		9,282			
Unbound からの削減		83.3%			
NSEC による削減結果 (理論値)	3,380	1,858	1,522		
Unbound/L/D 比	26.7%	16.7%			
Unbound/L/D + NSEC による削減結果	3,997	2,652	1,345	1,418,998	9,124,388
Unbound/L/D 比	31.6%	23.8%			
Unbound からの削減	68.4%	76.2%			
実測値比	3.4%	21.1%		2.06 倍	1.40 倍
実測値からの削減	96.6%	78.9%			

本手法の普及を図るため 2015 年3月に I-D を提案し、標準化活動を進めました。

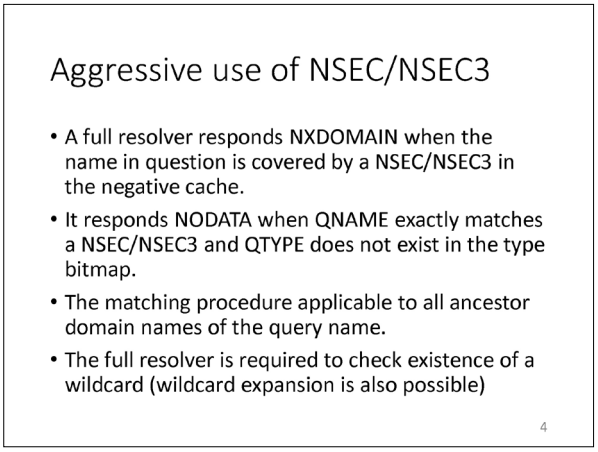

図2　IETF 92 の発表資料

本提案は 2016 年3月の IETF 95 でルートゾーンのみを特別扱いする同じ目的の対案と比較され、我々の提案が WG 案として採用されました。対案の提案者の一人であった Warren Kumari 氏に共著者になっていただき、WG で議論を進め、2017 年7

月にStandards TrackのRFC 8198 “Aggressive Use of DNSSEC-Validated Cache” として発行されました。

RFC 8198の発行後、多くのオープンソースのDNSソフトウェアやGoogle Public DNSなどのパブリックDNSサービスに本手法が実装され、ルートDNSサーバへの問い合わせ数を減少させることができました。ただし、DNSSEC検証をしていないフルサービスリゾルバはこの手法を使えないため、DNSSECへの対応が必須となります。

RFC 8198のアイデアは以前からあったらしく、識者の一人であるEdward Lewis氏から、RFC 5074 “DNSSEC Lookaside Validation（DLV）” に本手法の使用に関する言及があること、同様の内容を提案しようとしたが、DNSSECへの対応が十分でなかったため時期尚早であると判断した旨を伺いました。また、論文執筆時の実験に使用したUnboundのTODOに本機能の実装が記載されており、かつ部分的に実装するための関数が組み込まれていたことから、このアイデアは以前からあったものの、懸念があるために実装されていなかった技術であったと後で気付きました。

このように、IETFでの標準化にはその時期も重要であり、当時、ルートDNSサーバの無駄なクエリが注目されていたこととランダムなサブドメインを使ったDNSへの攻撃が流行していたことが、標準化まで進められた要因になったのではないかと考えています。

5．現在提案中のI-D

私は現在も、IETF dnsop WGにおいて標準化活動を進めています。本稿執筆時点で提案中のI-Dは2件あります。

一つは、DNS通信でUDPを使う際にIP断片化を避けるための提案で、2019年7月に最初のI-Dを提出しました。最初の発表時にDNSプロトコルの拡張とソフトウェアの実装、DNSの運用を長年続けているPaul Vixie氏からさまざまな意見をいただき、最終的に共著者になっていただきました。

この提案には多数の方から賛成意見・コメントをいただき、IESGからも重要なセキュリティ対策であるため、提案内容をより厳しいものにする旨のコメントがありました。しかし、複数のDNSソフトウェア実装者からIESGが示した内容は現在の一般的なオペレーティングシステム（OS）では実現不可能である旨が示され、標準化を進めるための調整が必要になっています。今後、共著者、dnsop WGチェア、担当ADを交えた形で、進め方を調整する予定です。

もう一つは、DNSプロトコルにおいてさまざまな上限値を設定するための提案で、2024年7月に最初のI-Dを提出しました。

DNSではドメイン名、クラス、タイプごとに複数のリソースレコードを記述できます。しかし、設定可能なリソースレコードの最大数には明確な上限がないため、例えば一つのドメイン名に数百個のIPv4/IPv6アドレスを記述することも可能です。

また、問い合わせたドメイン名が別名であることを示すCNAME/DNAMEリソースレコードには段数制限が規定されておらず、名前解決において11段のCNAMEを使用するドメイン名も運用されています。

同様に、DNSSECで使われるDNSKEY、DS、RRSIGといったリソースレコードにも、最大数の明確な上限が存在しません。2024年2月に公開されたKeyTrap脆弱性はこれを利用しており、攻撃者が準備した多数のDNSKEY、DS、RRSIGをDNSSEC検証させることで大量の計算をさせ、DNSサービスの妨害を図っています。

KeyTrap以外にもDNSプロトコルにおける上限値が明確でないことを利用した複数の脆弱性が発表されており、適切な上限値を設定することで影響を緩和し、安定性を高めることができます。この提案はまだ始めたばかりで議論は盛り上がっていませんが、DNSの悪用を減らすためには有用であり、継続して活動を進めていく予定です。

6．おわりに

IETFでの標準化活動を進めるには有識者が参加する会議や運用者コミュニティへの参加・発表を通じ、仲良くなっておくことが重要な要素の一つです。会議に積極的に参加し、有名人に顔と名前を覚えてもらうことも、活動に役立つでしょう。

その後は、I-Dを提出して議論を誘発し、IETFミーティングや関連ミーティングで発表して意見、コメントをもらい、I-Dに反映して仕上げていくという、言わば正攻法で進めることが重要になります。

私が所属するJPRSには、2002年7月のIETF 54から2024年7月のIETF 120までのすべてのIETFミーティングに業務として参加させていただき、

IETF での標準化活動を研究活動の一つとしてサポートいただきました。改めて感謝します。

本稿では、私の IETF におけるこれまでの活動を振り返りました。IETF に 22 年間参加し続けているにも関わらず、現在も有効な Standards Track と Best Current Practice の RFC が５本というのは少ないかも知れません。Obsoleted（廃止）になったものや Experimental、Informational まで範囲を広げても、10 本しか著者として関与できていません。

微力ではありますが、私は今後も IETF において、DNS プロトコル・運用技術などの改良を続けていく予定です。

表３　筆者が著者・共著者となった RFC

RFC番号	発行年月	種別	内容	備考
5483	2009年3月	Informational	これまでのENUMプロトコルの実装経験によって得られた知見	
5504	2009年3月	Experimental	国際化電子メールアドレスを使用した場合の、既存の電子メールシステムとの互換性に関する規格	
5825	2010年4月	Experimental	従来の電子メールシステムとの互換性を保つために変換されたメッセージについて、どう表示すべきかの手法	
6116	2011年3月	Standards Track	ENUMの実現のために使われる、プロトコルの標準規格を定義	
6856	2013年3月	Standards Track	電子メールアドレスの国際化におけるPOPの仕様拡張	
6857	2013年3月	Standards Track	POP及びIMAPにおいて国際化がサポートされていなかった場合に、従来との下位互換性を確保するための変換の仕様	
7719	2015年12月	Informational	DNSで使われる数多くの用語を一つの文書にまとめ、現在の定義を提示	RFC 8499により廃止
8198	2017年7月	Standards Track	DNSSECの仕様を改良してキャッシュ済み応答を不在応答やワイルドカード応答生成に利用し、パフォーマンス向上や遅延・負荷減少を図る仕組みの仕様	
8499	2019年1月	Best Current Practice	DNS用語を定義するRFC 7719を置き換え、用語追加と内容改訂したもの	RFC 9499により廃止
9499	2024年3月	Best Current Practice	DNS用語を定義するRFC 8499を置き換え、用語追加と内容改訂したもの	