

TTCに寄せて

DDoS対策プロトコル標準化の軌跡を振り返って

～TTC会長表彰を受賞して～

エヌ・ティ・ティ・コミュニケーションズ株式会社
西塚 要

はじめに

このたび、情報通信技術賞 TTC 会長表彰という栄誉ある賞をいただき、心より感謝申し上げます。限られた人生という時間の中で DDoS 対策プロトコルの標準化に携わる機会を得たことは、私にとって非常に貴重な経験でした。この成果は、多くの方々のご支援とご協力なくしては達成できませんでした。

特に、IETF という国際標準化の場に私を導き、常に支援してくださった上司の方々、そして標準化の作法を丁寧に教えてくださった業界の皆様に深く感謝いたします。

なぜ DDoS 対策プロトコルの標準化が必要だったか

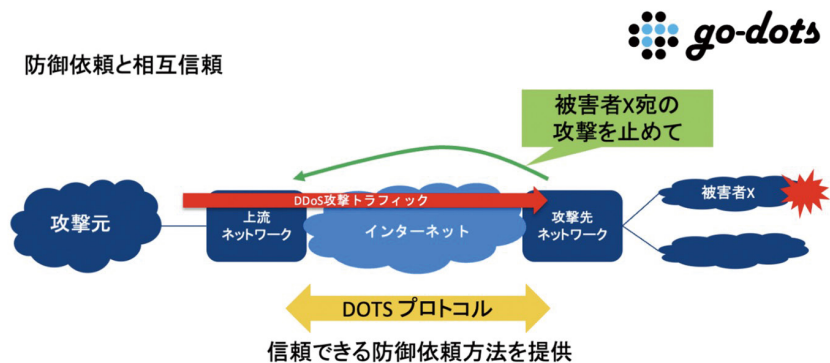
私は 2015 年から 2023 年にかけて、IETF において DOTS (DDoS Open Threat Signaling) ワーキンググループの設立から終了まで関与し、DDoS 攻撃対策のためのプロトコル策定に貢献しました。

DDoS 攻撃 (Distributed Denial of Service 攻撃) は、ボットネットなどの複数のコンピューターを利用して攻撃対象のサービスやシステムのリソース (サーバー、ネットワークなど) に過剰な通信を送り、正常なサービスを妨害するサイバー攻撃です。DDoS 攻撃自体の技術は古くから存在していましたが、インターネットの普及とともにその脅威が増大し、2000 年代初頭から急速にサイバーセキュリティの重要課題となりました。

今日では攻撃手法はますます高度化し、Tbps (テラビット毎秒) 級の強力な攻撃が可能となり、依然として大きな脅威として存在しています。DDoS 攻撃の脅威が深刻化していく中で、対策技術が国際的に整備されていないことが

大きな課題となっていました。各企業や組織が独自に DDoS 対策を施していたものの、相互に連携できず、効果が限定的でした。DDoS 攻撃の特徴は、攻撃を受けている組織単独では対策が困難な点にあります。攻撃トラフィックが上流のネットワーク帯域を埋めてしまうため、上流のネットワーク事業者に対策を依頼する必要があります。従来、この依頼は電話やメールで行われていましたが、オペレータ同士のコミュニケーションには時間がかかり、サービスへの影響が長期化する問題がありました。

そこで、DDoS 対策を国際標準として定め、世界中の事業者が統一的な手法で脅威に対応できるようにすることが求められました。この背景から、IETF において DOTS WG が立ち上げられ、DDoS 攻撃を受けているシステムと防御システムが相互に連携し、攻撃を迅速に検知・緩和できる通信プロトコルの策定が始まりました。「攻撃を検知したら、攻撃を受けているシステムが自動的に防御システムに対策を依頼できないか？」という発想が、DOTS プロトコルの重要な設計指針となりました。この標準化により、DDoS 攻撃への対応をより迅速かつ効果的に行うことが可能になると期待されています。



パケットフィルタアウトソーシングとセキュリティオートメーションを、相互信頼のもとで実現する技術として、DOTSプロトコルが注目されている

DOTS プロトコル概要

IETF ハッカソンで加速した標準化

私は、DOTS WG の立ち上げから参加しましたが、活動初期は、ごく少人数でプロトコルの目標や必要な仕様について議論を重ねていました。何もない状態から国際的な標準仕様を策定していくこのプロセスは、非常に貴重な経験となりました。その後、徐々に参加者が増え、より多様な視点が集まることで、議論はさらに深まるとともに実証が求められるようになりました。

IETF は、技術的なメリットや実装経験に基づいた合意形成のために、「動くコード」(Running Code)を重要視する実践的なアプローチで知られています。私もその方針に則り、仕様の有効性を実証するために、プロトコルのリファレンスアーキテクチャとしてオープンソースソフトウェアを実装しました。そして、そのソフトウェアを2017年に公開し、自社のネットワークを利用した実環境での試験を行いました。さらに、IETF ハッカソンに参加して他社ベンダーの実装と相互接続試験を実施し、標準化の精度を上げるためのフィードバックを提供し続けました。

IETF ハッカソンは2014年に初めて開催された比較的新しい取り組みです。その目的は、技術者が一堂に会し、策定中のプロトコルを実際のコードに落とし込み、問題点や改善点を早期に見つけることです。これにより、標準化文書(インターネットドラフト)の質が向上し、最終的なプロトコルの信頼性が増します。現在では、IETF ミーティングが年3回開催される際に、ハッカソンもその一部として定例化しています。ミーティングの直前に行われる週末2日間のハッ

カソンでは、異なる国やバックグラウンドを持つ技術者たちが一つの会場に集まり、円卓を囲んで議論しながら開発を行います。

IETF ハッカソンの黎明期、私はその場にチャレンジ精神で参加しました。前述の通り、DOTS プロトコルは当時新しいもので、ドラフトの理論検討だけではその有用性に確信を持つことができませんでした。結果的に10回近く継続してハッカソンに参加しましたが、DOTS プロトコルを実装する組織が徐々に増え、実証内容も次第に実践的な内容になっていきました。実際にDDoS対策装置ベンダーとの異実装間の相互接続試験を行い、最終的にテスト用に発生させたDDoS攻撃を止めることに成功したときの感動は、今でも忘れられません。

IETF ハッカソンには成果発表の時間が設けられており、優れたプロジェクトに対しては表彰が行われます。私たちのプロジェクトは、Best Open Source Project 賞とBest Puns 賞(ベスト・ダジャレ賞)を1回ずつ受賞しました。Best Puns 賞について少し説明すると、これは言葉遊びのうまさに対して贈られるジョークのような賞です。私たちのオープンソース実装が「go-dots」という名前だったため、発表の際に「Waiting for go-dots」とタイトルを付けました。これは、サミュエル・ベケットの戯曲『ゴドーを待ちながら』(Waiting for Godot)をもじったものです。このタイトルがなぜか好評を博し、賞を受けることになりました。DOTS プロトコルが少しでも多くの人に知られることになったので、結果的にポジティブに受け止めています。



IETF ハッカソンでの発表の様子

IETF 活動の第一歩

IETF での活動は基本的には個人単位であり、個人として認められることで国際的な技術者と交流して広い見聞を得ることができます。ですが、日本国内での IETF 活動に対する認知度やサポートはまだ十分とは言えない部分もあります。私の IETF での活動は、一緒に IETF に参加している日本人の皆様に支えられて始まりました。

IETF ミーティングに参加している日本人は毎回約 50 人程度で、全体（約 1500 人）に対して約 3～5% といったところです。IETF の活動は「ワーキンググループ（WG）」ごとに行われ、上記の日本人が様々な WG に参加しています。国際標準化の第一歩は、インターネット標準のベースとなる「インターネットドラフト」の作成者となることですが、日本人の書いたインターネットドラフトが一目置かれて WG で扱われることが多いのは、インターネット黎明期から諸先輩方が多くの貢献を残してきたことに立脚していると感じています。

また、各 WG にはチェアや副チェアがいますが、日本人もいくつかの WG でそのようなリーダーシップを担っており、標準化作業を推進しています。ハッカソンにおいても、私以外にも日本人技術者が積極的に参加しており、他国の技術者と協力してプロトコルの実装や相互接続テストを行っています。

私の初めてのインターネットドラフトは IPv4 枯渇対策技術のうちの特に NAT（Network Address Translation）技術の実装上の課題について書いたものなのですが、最初は書き方の作法、WG での発表の作法、ドラフトのメンテナンス方法などどれも知らずに提出したものでした。今思い返すと非常に未熟で恥ずかしいのですが、それでも上司や諸先輩方（特に WIDE プロジェクトの方々）にご指導をいただき、次のドラフトへと繋げることができました。この経験によりドラフトを書くことの心理的ハードルは劇的に下がり、何でも飛び込んでやってみればよいという精神に繋がりました。これらの助走が、DOTS WG での活動において積極性を発揮できた理由と感じています。

国際標準化に関わる仲間づくり

この経験を元として、日本の技術者たちに知見を伝える活動も積極的に行ってきました。ISOC-JP（インターネットソサエティ日本支部）のオフィサーある

いはインターネット標準化推進委員として、IETF での活動内容や最新の技術動向を広める「IETF 報告会」を開催してきました。

IETF 報告会では、直近の IETF における最新の議論内容や進展が紹介されます。

特に、日本人が関与しているプロジェクトやワーキンググループ（WG）での活動を中心に、国内の技術者に向けて情報が共有されます。標準化動向に関する内容が当事者から日本語でわかりやすく解説されるという点が非常に貴重です。報告会を通じて日本国内の技術者同士が情報交換を行い、新たなコラボレーションの機会を生み出す場にもなっています。これにより、日本から IETF への参加が促進されるだけでなく、日本国内の企業や大学や研究機関が国際標準化に対して積極的に貢献するための基盤が形成されていると感じます。IETF 報告会では TTC に後援をいただいております。IETF だけでなく他の国際標準化団体（ITU 等）の動向も国内で情報交換する場を設けさせていただき、デジュール標準とデファクト標準の違いなど各標準化団体の特徴（良い面も悪い面も）も勉強させていただきました。

IETF における標準化の領域は非常に広範で複数エリアに分かれているため、このようなコミュニティによる情報交換が非常に重要です。さまざまなエリアを横断して幅広い知識を得ることや、各種プロトコルの過去の経緯を理解することで、より深い議論に参加できるようになり、標準化活動において大きな強みとなります。例えば、DOTS プロトコルにおいては、トランスポートに UDP を用いる要件（DDoS 攻撃を受けている最中は双方向通信が保証されないため、暗号化のコンテキストを保持したままワンショットで情報を伝える）があったのですが、当時標準化直前であった QUIC を用いるか否かという議論があり、他エリアの WG の標準化のステータスを把握していないと議論についていけないということがありました。これらの横断的な知識の獲得によって、今でも技術の目利きができるようになっていいると感じます。

2015 年には、2009 年の IETF76（広島）以来の日本開催となる IETF94（横浜）に向けて、若手技術者を IETF に呼び込むための IETF 勉強会を開催しました。若手技術者や学生にとって、RFC の存在は知っていたとしてもインターネット標準化活動に触れる機会はあまりありません。IETF で活躍する日本人からの経験談や最新のプロトコルに関する講演は、国

際標準化活動への関心を高めるきっかけとなったのではと思います。また、IETFに初めて参加する若手技術者へのアドバイスや、ミーティング参加方法の説明など、実践的なサポートも実施しました。結果としてIETF94には普段の平均を大きく超え、364人も日本人が参加することとなりました。2023年に開催されたIETF116（横浜）も同様です。「国内で開催されたからこそ初めて参加ができた」という人が多く、その中から継続的に参加して新たにドラフトを書く人材がでてきています。IETFが個人レベルで貢献ができる形式だからこそ、国内開催をホストすることが有効だと感じます。

このように、標準化活動には多くの仲間たちの協力が不可欠です。私は、日本国内の技術者がIETF活動に興味を持ち、積極的に参加できるよう、情報の普及に努めてきました。これからも、日本の技術者たちが世界で活躍できる環境を整えることが私の使命だと考えています。

なぜ日本の技術者の活躍が大事か

IETFにおけるインターネット標準化の精神が“We reject kings, presidents and voting; we believe in rough consensus and running code”と言われるように、特定の国や組織の意見を代表せずエンジニア個人の集合がラフ・コンセンサスを形成する場所と考えられています。ですが、2017年のIETF98のplenary（全体会議）ではそれを覆す非常に示唆に富んだ基調講演がありました。この講演では標準化活動を「サッカーの競技場の設計」と考え、設計の選択に基づいて「競技場を傾ける」（tilting the playing field）ことが可能だと指摘しました。これは、特定の国や組織が標準化の場で過度な影響力を持つことによって、フィールド（標準化のプロセス）が一方に傾いてしまう状況を指摘したものです。

IETFがオープンでボランティアベースであるため、参加者のリソースや能力の差が生じ、結果として特定のプレイヤーが議論を主導する状況が生まれることがあります。

標準化のプロセスが一部の特定勢力に支配されうる状況を実際に目の当たりにしてきました。インターネット標準がいつの間にか日本市場が不利な方向に「傾け」られないように、日本の技術者たちは活躍しなければなりません。

もう一つ、技術者と国家レベルの思惑が大きく結び

つけられた出来事が2014年頃にありました。エドワード・スノーデンによるアメリカ国家安全保障局（NSA）の大規模な監視活動の暴露（スノーデン事件）は、IETFのプロトコル標準化にも深刻な変化をもたらしました。それを象徴するのが、2014年に発行されたRFC 7258「Pervasive Monitoring Is an Attack」です。この文書は、監視活動を明確に「攻撃」として扱い、標準化の際に監視対策を考慮する必要があると明記しました。

プロトコル設計において暗号化の標準を高める取り組みが加速し、インターネット上のすべての通信がデフォルトでエンドツーエンド暗号化されることが重要視されるようになりました。これらはインターネットアーキテクチャ全体について、分散型システムであることを堅持する方向性です。ですが、IETFに限らず国際標準化団体においては、Digital Sovereignty（デジタル主権）を優先する国家の中央集権型システムを志向した意見を代表する動きも出てきています。そのような国家的な意図を感じるような標準化提案に対しては、その影響を見定めて、しっかりと議論をしないといけません。

このように、技術には大きな影響力があり、標準化の結果が社会に深刻な影響を及ぼすこともあります。そのため、技術者は自らの技術がもたらす影響に対して常に責任を持つ姿勢が必要ですし、国際レベルでの議論ができる日本人技術者の育成が重要だと改めて思います。

IETFで活躍するには

改めて振り返ると、一番大変だったのは標準化のプロたちとの激しい議論であったと思います。私も含めて日本人の参加者のほとんどは本業での課題を解決する手段として、本業を抱えながらIETFに参加しています。しかし、海外には標準化活動を本業とし、RFCへの貢献自体を成果としている参加者がおり、コミット可能な時間やリソースで差があります。具体的には流量の多いメーリングリスト上の議論を追っているとそれだけで1日の仕事が終わってしまう世界です。自分の提案を通すためには、彼らに負けない論理的な思考力と、技術的な知識の深さが求められます。IETFで活躍するには彼らと上手に付き合うことが重要です。標準化のプロは読みやすいドラフトの書き方や論点の絞り方が上手く、私の場合では、著者の一人に加わってもらうことでRFC化を早期に進めること

ができました。しかし、短く簡潔なドラフトはコーナークースの議論を省略する傾向があるので、実装をしようとすると抜け漏れが見つかります。そのような細かい点を指摘するのは私が得意なことではあったのですが、仕様を複雑化して議論について来れる人を少なくしてしまうため、その匙加減の難しさについては今でも噛み締めています。

デファクト標準と言われる IETF の特徴も踏まえる必要があります。インターネット標準の場ではしばしばベンダーが有利に立ち回ることがあります。彼らの会社としての資源や影響力が強力なため、より技術的に優れた提案であっても、必ずしも通らないことがあります。例えば私見ですが、マーケットでトップの企業は、その企業の製品で実装済みの仕様を標準化すると他社の参入を招くことになるため、標準化に対して牛歩戦術に見える作戦を取っているように見えました。もしもう一度標準化活動に一から取り組むことができるなら、まずマーケットに目を向け、そこでの需要を理解した上で標準化に臨むことで、さらに良い結果が得られるだろうと思います。また、IETF の参加者は研究者や開発者に寄りがちで運用者(オペレータ)の視点が不足しています。時にはオペレータが不在のまま議論が進むこともありますが、私はそのような場面で、自身の運用経験を活かし、実際の運用に基づい

た意見を積極的に提案することができました。これにより、DOTS に関しては現実の運用環境に適合した標準化を進めることができたと感じています。

結び

国際標準化活動は、技術の普及や社会的責任を伴う重要な取り組みです。私に関わった DDoS 対策プロトコルの標準化は、その一例に過ぎませんので、広く一般化しすぎて語っているかもしれない点をご容赦ください。ですが、今後も技術者としての責任を持ちながら、世界に貢献できる活動と後進の育成を続けていきたいと思っています。

最後に、国際標準化活動を支えてくれた家族に大きな感謝をしたいと思います。この度の 2024 年度 TTC 表彰では、「標準化活動は家族の支えがあってこそで、家族にも感謝を」と祝辞をいただき、大変ありがたい言葉と感じ入りました。まだ子供が小さいのに国際会議で家を長期に離れたり、またコロナ禍になってリモート開催になった IETF ミーティングや WG の中間ミーティングでは、時差の関係で深夜での発表や議論に多く参加しておりました。これらの活動を暖かく見守ってくれる環境があってこそその受賞と感じています。