




NTTコミュニケーションズ
エバンジェリスト

西塚 要 Kaname Nishizuka

DDoS対策のための国際標準「DOTSプロトコル」

2024年末から2025年はじめにかけて、日本の公共機関、航空会社、金融会社等多くの機関に、マルウェアによりボットと化した端末から大量のトラフィックが送信され、コンピュータが停止等となるDDoS (Distributed Denial of Service) 攻撃が頻発し、それぞれのサービス提供に影響がでました。DDoS攻撃は古くからあるサイバー攻撃で、PCなどがボットとして遠隔操作されているため、攻撃者の特定が困難なこと、未然防止が困難なこと、攻撃を受けた機関単独での解決が困難なことから、対策が急務であり、国際的な課題にもなっています。こうしたDDoS攻撃への対策である新しいプロトコルDOTS (DDoS Open Threat Signaling) を開発し、IETF (Internet Engineering Task Force) において国際標準化を行った、NTTコミュニケーションズ 西塚要氏に、DOTSプロトコル、IETFにおける標準化、コンフォートゾーンにとどまらずに積極的にチャレンジする思いを伺いました。



 **DDoS対策の自動化、複数の対策事業者に対して共通のプロトコルで防御依頼、別の対策事業者を含む事業者間連携を実現するDOTSプロトコル**

現在、手掛けている業務の概要をお聞かせいただけますか。

NTTコミュニケーションズの技術開発部（現：イノベーションセンター）で「DDoS (Distributed Denial of Service) 対策のための新しいプロトコルDOTS (DDoS Open Threat Signaling)」に関する研究開発に取り組んでいました（DOTS標準化後に現所属に異動）。

インターネットにおけるサイバー攻撃やセキュリティに関する課題の1つにDDoS攻撃があります。DDoS攻撃は、攻撃者がマルウェアに感染した端末（遠隔操作を可能とする：ボットネット）を利用し、攻撃者の命令によりターゲットとなるコンピュータに過剰なトラフィックを送ることで、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、Tbit/s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。

各企業や組織が独自にDDoS対策を施しているものの、相互に連携できず、効果が限定的である現状があります。大量のトラフィックを送信しているのはボットネットと化した端末であり、それを操作する攻撃者を突き止めるのは多くの場合で困難で、さらに攻撃を受けた側もシステムやネットワーク自身がほぼ停止状態で、自ら大量の攻撃トラフィックを判別して事前に破棄することも不可能であるため、攻撃を受けている組織がその組織単独で解決することができず、DDoS攻撃は解決が難しい攻撃手法になっています。

いったんDDoS攻撃が発生すると、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、オペレーターどうし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。このような状況において、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。

こうしたDDoS攻撃に対して組織間の連携をベースとして対応するプロトコルがDOTSであり、IETF (Internet Engineering Task Force) において標準化されました。DOTSは、攻撃を受けているエンティティ（コンピュータやネットワーク）や、攻撃

元の特定等、これまでに共通的に定義されていなかった防御主体側が守るために必要な情報を伝達するためのシグナリングのプロトコルで、これによりDDoS対策の自動化、より大規模な防御システムの構築、ベンダ独自のソリューションからの開放を目的としており、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です(図1)。

DOTSプロトコルの動作は、①利用者側のDOTSがインプリメントされたクライアント(DOTSクライアント)から提供者側のDOTSがインプリメントされたサーバ(DOTSサーバ)に対して、攻撃を受けているIPアドレスなどの情報とともに防御を依頼し、②依頼を受けたDOTSサーバ側は、認証および防御依頼のバリデーションを実施したうえでフィルタリングやDPI(Deep Packet Inspection)等によるパケット弁別・破棄等のDDoS対策を実施する、という手順になります。

DOTSプロトコルにより、①人間を介さない防御受付のインタフェースが規定されることで、DDoS対策の自動化が可能になる(図2(a))、②複数の対策事業者に対して共通のプロトコルで防御依頼をすることができるようになる(図2(b))、③キャパシティオーバーの際に別の対策事業者に防御依頼をするような事業者間連携を実現できる(図2(c))といった効用が期待できます。

DOTSのIETFにおける国際標準化の経緯を教えてください。

IETFはインターネットで利用される技術・プロトコル等の標準化を行うフォーラムで、ITU-T(International Telecommunication Union Telecommunication Standardization Sector)のような法人や国などのメンバーシップにより参加してデジュール標準を策定する団体に対して、技術者等が個人として自由に参加するフォーラム標準を策定する団体です。検討課題ごとにWG(Working Group)が設置され、自由に投稿された提案(Internet Draft)をベースに、メーリングリストや年3回の全体会議で各規格の仕様の検討が行われています。検討の中では複数による仕様実装と相互接続性の確認が行われるのが特徴です。こうした検討結果はそれに引き続くいくつかの手続きの後にRFC(Request For Comments)としてドキュメント化され、国際標準となります。

さて、DDoS攻撃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ることを背景に、2015年6月に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。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。しかし、Internet Draft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ず、実証にかかわる議論を深めるために、年3回の会合と併催のIETFハッカソンに10回近く継続して参加しました。こうした中、私たちは、自社と他社のDDoS対策サービスの連携を念頭に、2017年にDOTSを世界初実装し、OSS(Open Source

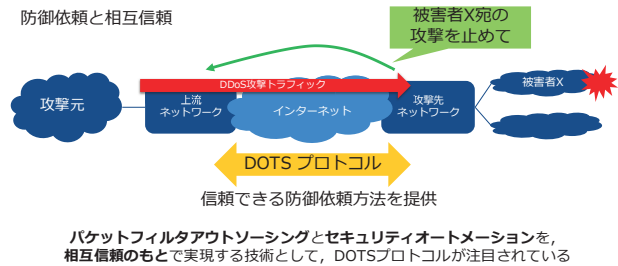


図1 DOTSプロトコルの概要

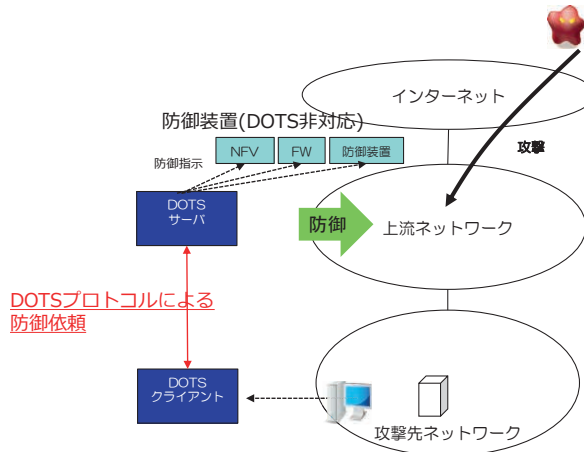
Software)化(リファレンス実装)し、NTTコミュニケーションズのネットワークを利用した実環境を構築しました。引き続き英国のDDoS対策装置ベンダがDOTSプロトコルの実装を行い、NTTコミュニケーションズの実環境との相互接続試験を行い、最終的にテスト用に発生させたDDoS攻撃を止めることに成功しました。当初は様子見状態であったRadware, Verisign, Cisco, Orangeなどの企業も、DOTS WGに人を派遣し、精力的に活動するようになり、DOTSプロトコルを実装する組織が徐々に増え、実証内容も次第に実践的な内容になりました。こうした検討、実証等を経て、DOTSプロトコルが13件のRFCとしてIETFとして国際標準となり、2023年にDOTS WGも終了しました。

これらの取り組みの中で、私は筆頭AuthorとしてのInternet Draftを3回提案し、そのうちの1つはRFC 9133(Controlling Filtering Rules Using Distributed Denial-of-Service Open Threat Signaling(DOTS) Signal Channel)としてProposed Standardになりました。その他、ユースケースを記したRFC 8903にも自身の運用経験に基づいた知見を数多く記載して貢献しています。また、IETFハッカソンにおいては成果発表が優れたプロジェクトに対する表彰、「Best Open Source Project賞」を受賞しました。さらに、IETFのDOTS WGにおけるDDoS攻撃対策のためのプロトコル策定への貢献に対して、2024年に一般社団法人情報通信技術委員会(TTC)から、情報通信技術賞TTC会長表彰をいただきました。

○ IETFへの参加がスキル向上、意識向上の貴重な経験

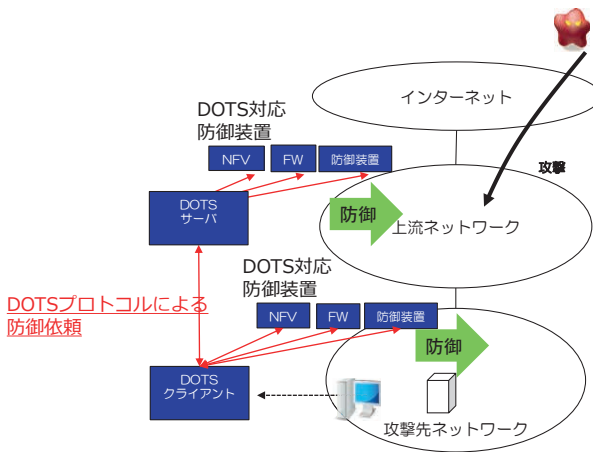
開発者としてのスキルはどのように磨いているのでしょうか。そして、IETFに参加した経験はどのような意識につながったのでしょうか。

私は2006年にNTTコミュニケーションズに入社し、OCNのアクセス系を中心としたネットワークの開発、お客さまであるISPのネットワークの開発保守に従事した後、研究開発の部署に異動しました。そして、IPv4アドレスの枯渇問題とIPv6技術の展開、トラフィックの分析・予測・異常検知とそれに基づくDDoS検知とDDoS対策等ISPが抱えている課題を解決する技術開発を行ってきました。



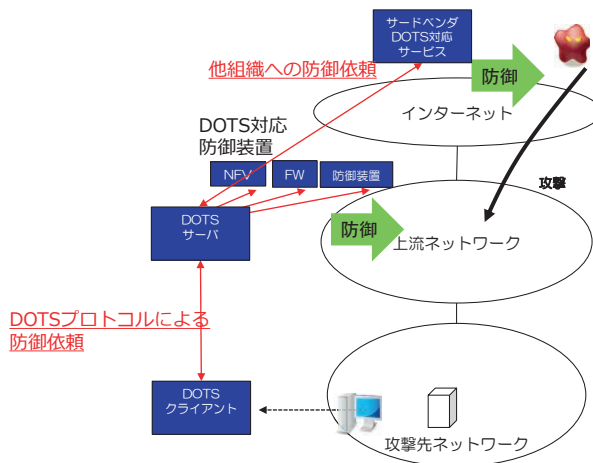
- ◆ 攻撃を受けているネットワークが、DOTSクライアントからDOTSサーバへの通信(DOTSプロトコル)により防御を依頼する
- ◆ 依頼を受けたDOTSサーバは、ネットワーク機能(NFV)・ファイアウォール(FW)・防御装置などの防御機構に対して防御を指示する
- ◆ 人間を介さない防御連携によりDDoS対策が自動化される

(a) DDoS対策の自動化



- ◆ 防御装置がDOTSプロトコルに対応していた場合、DOTSクライアントから直接防御依頼をすることができる
- ◆ 依頼を受けた上流ネットワークのDOTSサーバは、さらにDOTS対応の防御装置に防御指示を出すことができる

(b) 防御依頼の共通化



- 上流ネットワークでのDDoS防御機構のキャパシティよりも攻撃の量が大い場合には、別の対策事業者にさらに防御依頼をするような事業者間連携が実現できる

(c) 別の事業者との事業者間連携

図2 DOTSプロトコルの効用

学生時代の研究は、機械学習・データ分析系のテーマであり、入社と同時にインターネットを中心としたネットワーク系の開発を行うことになり、インターネット技術・標準・社会に関連する開発を推進することとなりました。このような環境に対応していくために、日常業務に関係するところから勉強し、経験を積むことでそれを自分のスキルとして定着させてきました。トラフィックの分析・予測・異常検知に関しては学生時代の専門知識が活かされたことはいうまでもありません。

さて、私は事業会社としては珍しくIETFで標準化に関する活動も行ってきました。IPv4アドレスの枯渇問題に取り組み出したころからIETFに参加し始めたのですが、標準化の会合に参加するためには、技術的な専門性や英語力はもちろん必要となりますが、標準化に向けた手続きや、ドキュメント作成・プレゼンテーションの作法等、独特な知識が必要となります。日本からは多くの諸先輩方がIETFの場で活躍しており、こういった方々の行動を見よう見まねで自分の中に取り込んでできました。そうした中で自然とWIDEプロジェクト系の方々と連携も出てきました。初めてのInternet Draftは、IPv4 枯渇対策技術のうちのNAT (Network Address Translation) 技術の実装上の課題に関するものなのですが、作法的なものは何も知らずに提出し、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Internet Draftへとつなげることができました。こうした経験から、何に関しても自ら飛び込んでやってみようという思いが強くなり、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。

IETFに限らず欧米から標準化の活動に参加する人のほとんどは標準化を専業として活動しています(標準をつくることそのものが成果)が、日本から参加する人は自ら研究開発を行う傍らで標準化活動を行っている(研究開発の成果の出口としての標準化)人がほとんどです。こうした環境のギャップのある中で、英語で議論を進めて標準を策定していくこととなります。英語については、こちらの伝えたいことを伝えようと話をすれば、たとえ拙い英語であっても何とか伝わるので、とにかくこちらから積極的に話しかけるようになりました。ただし、当然の話ですが、伝えたいこと(自分の考え)をしっかりと持っていることが必須です。そして、議論される技術は研究開発の成果であるため、人から伝わったものではなく、自らが検証・確認したものです。これは標準化専業の参加者の議論の戦術に勝る、説得力のある材料になります。以前上司から言われて心に残っている、日常の業務において「自ら手を動かす」「人からの伝言も自ら確認する」ことの大切さそのものだと思います。

DOTS プロトコルがIETFの標準となった後に異動されたそうですが、今後どのような業務経験をしたいのでしょうか。

DOTS プロトコルはIETF 標準となり、DOTS WGも終了し、今後製品への実装、マーケットへの展開というフェーズになります。

DOTS WGでは、各国のキャリアだけでなくDDoS対策装置のベンダが協力して標準化を進めておりましたが、多くのベンダがすでに独自のAPI (Application Programming Interface) を持っており、これとの兼ね合いでマーケットへの展開を模索している状況です。NTTコミュニケーションズとしてはすでにDOTSを実装した実績があるため、それを事業や市場の中でどのように展開していくのか検討しており、DOTSの開発という意味では一区切りついたタイミングで私は異動しました。

私は、元々DDoS対策も含めて、トラフィックの分析を自分のライフワーク的に思っているところがあり、現在の業務はDDoS対策等の対策側ではなく、トラフィック等の異常検知等、分析側の比重が高まっています。そのためデータ基盤を構築していわゆるビッグデータ解析を行う中で、機械学習をはじめとするAI (人工知能) 技術を使ってトラフィックの異常なところを探す技術開発と、それに基づいた対策に関する技術開発を行っています。しばらくはこのテーマに取り組むこととなりますが、将来的にもライフワークであるトラフィック分析にかかわりのある技術に取り組んでいきたいと思っています。

 **自分のコンフォートゾーンにとどまらず、少し無理に感じたところでも勇気をもって挑戦**

後進や読者へのメッセージをお願いします。

私は、IETFの活動で刺激を受けたところが多いのですが、自分のコンフォートゾーン、自分の知っている範囲にとどまらないで、少し無理に感じたところでも勇気をもって挑戦してみることが大事だと思います。最初の一步を踏み出してみることは、自分を成長させる一番の起爆剤であり、奮起させる材料にもなるので、どんどんチャレンジしてほしいと思います。

また、事業会社では機会が少ないとは思いますが、NTTグループに限らず、国際標準化の場に出てほしいと思います。私が参加してきたIETFは、日本人の発言力がまだまだ弱いと感じており、日本人の参加者どうしの会話の中で、これは層の薄さに起因するものではないか、という意見も出ています。標準化の場はルールをつくる場であり、そこで活躍することはまさにゲームチェンジャーになるということです。一度標準になるとそれに従うことにはなるのですが、不都合が見つかった場合、標準を上回る新しい発想、技術がある場合は、標準の変更や新しい標準の策定等、実際に行われているのです。つまり、いつでもゲームチェンジができるということです。IETFのハッカソンはまさにその典型的な例だと思います。そういった場にも積極的に参加してほしいと思います。