インターネット10分講座

おさえておきたい基本や、最新動向を解説するコーナーです。

DOTS (DDoS Open Threat Signaling) とは

DDoS防御を自動化する仕組み

1 DDoS攻撃とは

DDoS(Distributed Denial of Service)攻撃は、相手のサービスを不能にすることを目的としたDoS(Denial of Service)攻撃の一手法です。分散された(Distributed)攻撃元から、インターネットを介して特定サイトや企業ネットワークに不正パケットを大量に送りこむことで、相手のネットワーク帯域を消費し尽くします。インターネットに接続している以上、接続回線のネットワーク帯域は有限のリソースですので、サービスの種別によらず攻撃が成立する可能性が高いという特徴を持ちます。DDoS攻撃はここ数年で複雑化してきており、被害も深刻なものになっています。攻撃帯域は年々増加しており、2016年には、Tbps(テラビット毎秒)級の攻撃が観測されたと報告されています※1。対処が必要となる現実的な脅威として、DDoS攻撃を挙げる企業も少なくありません。

DDoS攻撃が盛んになっている原因として、booterと呼ばれるDDoS攻撃代行業者の存在は無視できません。彼らは時間あたり数ドルという格安の値段で、DDoS攻撃のためのプラットフォームを提供しています。政治的な理由あるいは金銭を脅しとることを目的とした攻撃者は、特別な知識を持つ必要なく、彼らのプラットフォームを借りるだけで、DDoS攻撃によって相手のサービスを不能にすることができるのです。2017年には、そのような代行業者の一つが当局によって摘発されましたが、顧客が世界中にいたこと、売り上げが年間数千万円程度であったことも明らかになりました。DDoS 攻撃がカジュアルになっていること、そしてそのようなユーザーに支えられて、代行業者が経済的に成り立っていることがわかりました。

DDoS攻撃のためのプラットフォームの一つが、ボットネット(botnet)です。代行業者は、数千台規模のボットネットを利用して、攻撃対象に大量のパケットを送りこむことができます。その際、ボットネットから直接攻撃対象にパケットを送るよりも効率的な方法が、アンプ(Amplification：増幅)攻撃です。インターネット上のいくつかのサービス(例えば、DNSやNTPなど)は、送られてきたパケットに対して、バイト量に換算して数倍のパケットを応答として送り返すことがあります。そこで、送信元を攻撃対象のIPアドレスに偽装してこれらのサーバにパケットを送ると、何倍にも増幅された応答が、(本来の送信元ではなくIPアドレスを偽装された)攻撃対象に返ります。

そのような性質を持つサービスでは、通常は送信元のIPアドレスがフィルタリングによって絞られて運用されるべきですが、送信元制限のフィルタリングが抜けたまま運用されているサーバが、インターネット上では放置されているケースがあります。攻撃者は、数千台規模のボットネットから、さらにこれらの放置されたサーバを用いて、攻撃パケットを何倍にも増幅した上で攻撃対象にぶつけるのです。アンプ攻撃はリフレクション(Reflection: 反射)攻撃と呼ばれることもあります。

2 DDoS対策について

DDoS攻撃の元凶になっているボットネットや、アンプ攻撃で利用されているサーバをインターネットから無くすことが、本質的なDDoS対策です。しかし、脆弱性を放置してしまっている機器の管理者一人ひとりへの連絡が必要なため、撲滅には非常に時間を要すると思われます。あるいは、インターネット上からすべての脆弱な機器を無くすというのは、不可能なことかもしれません。そのため、攻撃中のDDoS攻撃による影響を抑えるための、対症療法的なDDoS対策がいくつか存在します。

大規模なDDoS攻撃を受けてしまうと、自社設備に導入しているセキュリティサービス(IPS(Intrusion Prevention System)やIDS(Intrusion DetectionSystem)など)では、検知はできるかもしれませんが対策することはできません。IPSやIDSが設置されたネットワークの入口よりも、より上流に位置する接続回線のネットワーク帯域が輻輳してしまうためです。そのため、接続回線の事業者(トランジット事業者)あるいはクラウドの場合はクラウド事業者が、DDoS対策サービスを顧客に提供している場合があります。DDoS攻撃を受けてしまったら、サービス回復のための対応ができるかどうかは、そのような上流の事業者がどのようなDDoS対策サービスを提供しているかに左右されてしまいます。

上流の事業者によるDDoS対策は、遮断型・緩和型の2種類に大別されます。

- 遮断型: 攻撃を受けているIPアドレスに対するトラフィック、すなわち攻撃トラフィックも通常トラフィックもすべて遮断してしまうもの

- 緩和型: 攻撃トラフィックと通常トラフィックを区別し、攻撃トラフィックのみフィルタリングし、通常トラフィックは救うもの

遮断型は通常トラフィックも遮断してしまうため、サービスに対する攻撃が成立しているという意味でメリットが無いように感じるかも

※1 米国で「大規模DDoS攻撃」発生：Netflix、Twitter、Spotifyがダウン https://wired.jp/2016/10/24/internet-down-dyn-october-2016/

しれませんが、回線を共用している他のサービスやテナントを救うことができるため、緊急対策として利用されることがあります。緩和型は攻撃トラフィックと通常トラフィックの区別が必要なため、DDoS対策に特化したアプライアンス製品が主に使われます。誤検知や見逃しといった問題を内在していますが、多くの場合でサービスを救うことができるため、DDoS対策として有効です。

その他にも、攻撃に耐えられるようにネットワークやサーバを一時的に増強したり、サービスを地理的に地球規模で分散させて攻撃の影響を軽減するといった、対策を採る場合があります。

3 なぜDDoS攻撃は防ぎにくいのか

少し説明が長くなりましたが、攻撃を受けている組織だけでは対策を取りにくいという、DDoS攻撃の特徴について理解いただけたと思います。その理由としては、大きく次の二つが挙げられます。

○1. 攻撃を受けている組織だけでは対策を取りにくい

DDoS対策を上流の事業者に実施してもらうためには、DDoS対策の依頼を行う必要があります※2。

○2. 組織間の連携が重要

あるサービスを運用している人が、インターネット接続回線事業者のDDoS対策サービスを契約しており、回線の輻輳などによりDDoS攻撃を受けていると判断したとします。攻撃を受けていることを回線事業者に通知するには、どのようにしたらよいでしょうか。

多くの事業者は、電話やメールによる窓口を用意しています。しかし、窓口に対して「攻撃を受けている」という情報を伝えてから実際に防御のアクションを取ってもらうまで、人手を介するために数十分もの時間がかかってしまう場合があり、DDoS対策が発動するまでの時間、攻撃が成立してしまいます。

このような問題を解決し、組織間の連携をより密接にするために、IETF（Internet Engineering Task Force）において、DOTS（DDoS Open Threat Signaling）プロトコルが提案されています。ここからは、このDOTSプロトコルについて解説します。

4 DOTSプロトコル解説

○ DOTSプロトコルの目的と概要

DOTSプロトコルは、DDoS攻撃を受けている時に、攻撃対象となっているIPアドレスなどの情報を、外部に通知する仕組みを標準化するものです。DDoS対策は一般的に、「1.検知」「2.防御依頼」「3.防御」の三つのプロセスに分けられます。DOTSプロトコルが対象としているのは、このうちの防御依頼プロセスで、DDoS攻撃を検知した組織とDDoS攻撃を防御する組織が、別の組織である場合を想定しています。

前半部分で解説しましたが、DDoS攻撃によって、インターネット接続回線が輻輳してしまっている場合には、DDoS攻撃を受けていることを検知できたとしても、オンプレミスで防御することは不可能であり、インターネット回線に到達する前に防御することができる防御主体による助けが必要です。

実は、同様の機能を持ったベンダ独自実装がいくつか存在します。同一ベンダで提供されているオンプレミス型のDDoS対策装置と、クラウド型のDDoS対策を連携させる形を取っており、一般にクラウドシグナリングと呼ばれています。オンプレミス型のDDoS対策装置では防御できない規模や種別の攻撃があった際に、クラウド型のDDoS対策と連携して、防御の一部を肩代わりさせるために使うことができます。

DOTSプロトコルがめざすのは、このベンダ実装のオープン化・標準化ですが、単にベンダロックインを避ける以上の効用があります。

○組織間の連携を自動化：セキュリティオートメーション

DDoS攻撃を受けている組織は、いち早く通常のサービス状態に戻すことが急務です。しかし、先ほど述べたように、電話やメールでの人間が介する防御依頼では、判断に時間がかかってしまいます。

そこで、DOTSプロトコルを利用して、DDoS攻撃を検知した機器が、より上流（攻撃元に近い）の事業者によるDDoS対策サービスへの防御依頼を自動的に実施することによって、DDoS対策にかかる時間を劇的に減らすことができます。より上流の事業者では、攻撃を受けている組織よりも詳細に、DDoS攻撃の状況や内容を把握している可能性が高いと考えられます。防御依頼を受けた事業者は、攻撃に使われている特徴（特定のポート番号やIPアドレスだけでなく、DPI（Deep Packet Inspection）ベースのシグネチャなど）に従って、攻撃の緩和をすることによって、効果的な防御を実施することができます。

このように、DOTSプロトコルを利用すると、DDoS対策に必要な機器同士の連携を組織を超えて自動化することができます。また、複数の上流ISPを持つような場合、両方のISPが提供するDDoS対策サービスがDOTSプロトコルに対応していれば、同一の仕組みで防御依頼の自動化をすることができます（そうでない場合には、それぞれのISPが提供する仕様に合わせてそれぞれの仕組みで防御依頼をしなくてはいけないため、開発や運用コストが増加します）。世の中のDOTS対応が進むことにより、オペレーションしやすいDDoS対策を実現することができます。

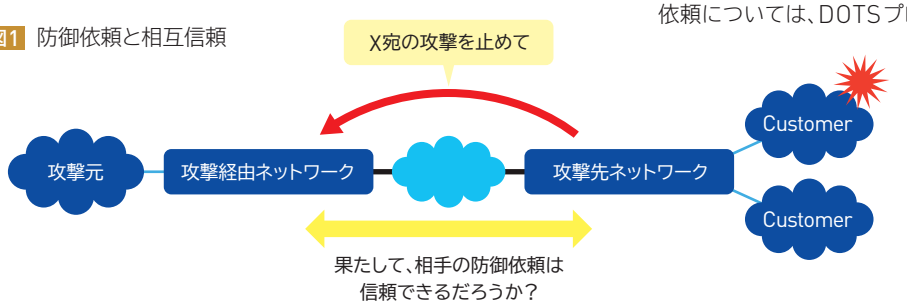
○相互認証による防御依頼の正当性担保

このような防御連携には、相互認証が必須です。なぜなら、防御依頼そのものが別の攻撃手法になり得るからです。例えば、DDoS対策の依頼を任意の第三者が勝手に実現できてしまうと、意図しない通信遮断や制限を受けてしまうことになります。

※2 上流事業者によるDDoS対策　常に通信パケットを監視し、DDoS攻撃と思われるパケットを排除するような常時型のサービスもありますが、事業者のサービス基盤の処理性能を占有するため高価になります。また、誤検知による正常パケットの廃棄といった問題が、常時発生する可能性があります。そのため、DDoS対策サービスの利用者からの申告に基づいて実施されることが一般的です。

DOTSプロトコルでは、TLS（Transport Layer Security）あるいはDTLS（Datagram Transport Layer Security）を利用して、サーバ認証とクライアント認証の両方を実施するモードがデフォルトになっています。これにより、DOTSプロトコルによる防御依頼が、正しくその組織からされていることを担保することができます。また、ある組織から防御依頼が可能なネットワークリソース（IPアドレスなどの防御対象）の範囲を前もって制限することにより、他人の所有するネットワークリソースに対して（勝手に）防御を発動してしまうことを防いでいます。それ以外にも、防御依頼のなりすましやリプレイ攻撃が実施できないように、DOTSプロトコルは設計されています。

図1 防御依頼と相互信頼

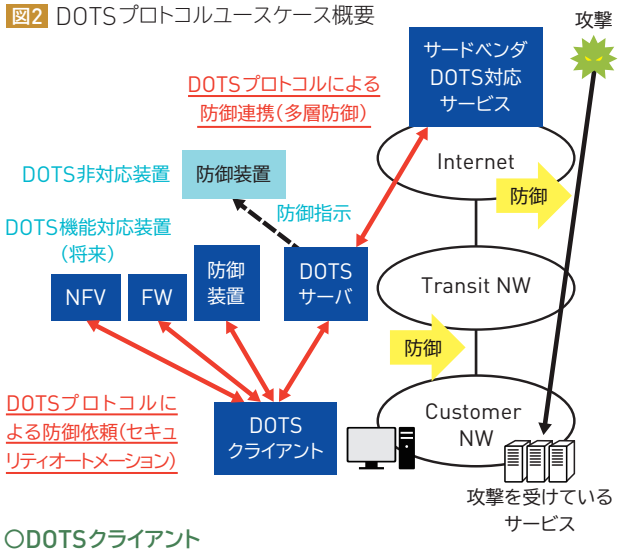


パケットフィルタアウトソーシングと**セキュリティオートメーション**を、**相互信頼のもと**で実現する技術として、DOTSプロトコルが注目されている

5 DOTS対応機器について

DOTSに対応した機器・機能をDOTSエージェントと呼びます。DOTSエージェントには、防御依頼を行うDOTSクライアントと、防御依頼を受けるDOTSサーバの2種類があります。

図2 DOTSプロトコルユースケース概要



○DOTSクライアント

DDoS攻撃が起きていることを通知する機能（DOTSクライアント）は、さまざまな機器に具備させることができます。

1. ネットワークをモニタリングしている機器（フローコレクターなど）は、トラフィック流量の異常（しきい値による判断など）をきっかけとして、DDoS攻撃を検知することができます。DOTSクライアント機能を具備することによって、フローコレクターなどから防御依頼を行うことができます。

2. Webサービスなどを提供しているサーバ自身が、トラフィック流量やCPU等の負荷状況によってDDoS攻撃を受けていると判断した時、DOTSクライアント機能を具備していれば、直接防御依頼を行うことができます。

3. IPS/IDSなどのセキュリティデバイスもDDoS攻撃を検知できるため、DOTSクライアントとなることができます。

○DOTSサーバ

DOTSサーバは防御依頼を受ける機能であり、回線事業者やクラウド事業者などDDoS防御サービスの提供者が提供します。DDoS緩和装置など、外部の装置やシステムと連携して防御を実現します。次のような仕組みとなっていることが想定されています。

1. いくつかのDDoS緩和装置が、DOTSサーバ機能への対応を始めています。その場合、防御依頼を受けたDDoS緩和装置が直接防御を行うことができます。

2. DOTSサーバ機能が、ネットワークオーケストレータなどのシステムに組み込まれている場合、防御依頼に応じてDDoS緩和装置やネットワーク機器を制御して、防御を実現することができます。

○ゲートウェイ機能

DOTSサーバは、防御依頼を受けた時に、さらに別のDOTSサーバに防御依頼を転送することができます。この機能はDOTSゲートウェイと呼ばれます。例えば、データセンター事業者がDOTSゲートウェイをデータセンターネットワークに設置し、テナントされた仮想マシンからの防御依頼を受け入れ、さらに上流のプロバイダのDOTSサーバに防御依頼を実施するようなケースが想定されます。また、より攻撃元に近い組織に防御を依頼したり、攻撃手法に応じて防御依頼をする機器や組織を変更したりといった、多層的な防御も実現します。

○BGPFlowspecにはないアクセスリストの内容評価機能

DOTSプロトコルとの比較対象として、任意の経路やアクセスリストの適応を依頼できる、BGPFlowspecというプロトコルがあります。ルータでの対応に限られますが、攻撃を遮断する内容のアクセスリストを適応することにより、DDoS攻撃の遮断あるいは緩和をすることができます。しかし、残念ながらBGPFlowspecはアクセスリストの内容を評価（Validate）する機能が不足しており、設定によっては第三者の通信を制限することができてしまいます。そのため、BGPFlowspecは組織間で使われるにはまだ問題があり、主に同一組織内での利用に限られています。組織間での防御依頼については、DOTSプロトコルの方が優れています。

6 DOTSプロトコルの仕組み

最後に、簡単にDOTSプロトコルの仕組みについて解説します。

○二つのチャンネル

DOTSプロトコルは、シグナルチャンネルとデータチャンネルの、二つのチャンネルを持ちます。両方とも、同一のDOTSクライアント・DOTSサーバ間で使われます。

図3 DOTSプロトコルスタック

	シグナルチャンネル	データチャンネル
スタック	DOTS CoAP TLS / DTLS TCP / UDP IP	DOTS RESTCONF TLS TCP IP
アプリケーション	CoAP	RESTCONF
セキュリティ	DTLS(またはTLS)	TLS
トランスポート	UDP(またはTCP)	TCP
目的	(攻撃を受けているときに) 防御を依頼するチャンネル	(攻撃を受けていないときに) 防御をセットアップするチャンネル
クライアント → サーバ	・防御依頼(開始/停止) ・攻撃を受けているIPアドレス等の情報 ・防御状況の確認	・DOTSクライアント情報の登録 ・エイリアスの登録 ・アクセスリスト(ACL)の登録 ・テレメトリ情報
サーバ → クライアント	・防御状況の報告	・テレメトリ情報

◇シグナルチャンネル

シグナルチャンネルは、防御依頼をするためのチャンネルです。UDPを利用し、認証にはDTLSを利用するのがメインのモードです。攻撃を受けているネットワークリソース(IPアドレスやポート番号)の情報を、ペイロードに載せます。防御依頼の内容はCBOR(Concise Binary Object Representation)により簡潔にエンコードされ、軽量版HTTPであるCoAP(Constrained Application Protocol)を使って操作を行います。

シグナルチャンネルは、実際にDDoS攻撃を受けている時に利用されることが想定されています。DDoS攻撃発生時には、DOTSクライアントとDOTSサーバの間の回線が攻撃トラフィックで輻輳してしまっているかもしれないので、輻輳している回線でも通信ができるようにハンドシェイクを必要としないUDPを利用し、パケットサイズをより小さくするという設計思想です。

DOTSクライアント・DOTSサーバ間では、死活監視のためのハートビート信号を定期的にやり取りします(オフにすることもできます)。DDoS攻撃によってDOTSクライアントと通信が不可能になった場合を想定し、DOTSサーバがハートビートを失った時に、防御を発動する機構(デッドマントリガーと呼ばれます)を持っています。

◇データチャンネル

データチャンネルは、DOTSクライアントの登録などに用いられる、補助的なチャンネルです。DDoS攻撃を受けていない平常時に利用されることが想定されています。そのため、TCPを利用し、認証にはTLSを利用するのがシグナルチャンネルとの違いです。また、メッセージはRESTCONFを用いてやり取りされます。

エイリアス(alias)と呼ばれる防御内容の組み合わせを、データチャンネルを利用して登録することで、シグナルチャンネルでの防御依頼の際にエイリアスを指定することにより、規定の防御を実現する機能があります。また、防御対象ではないことを明示的に指定するホワイトリストなど、アクセスリストの登録もデータチャンネルの機能です。

7 標準化・実装状況

DOTSプロトコルは2015年にIETFで提案され、DOTS WGが結成されました。そのあと3年というIETFとしては短い期間で、シグナルチャンネルやデータチャンネルのコアな仕様を決めてきました。議論には、アーバーネットワークス社やアカマイ・テクノロジーズ社(Prolexic)などの主要なDDoS対策ベンダだけでなく、キャリア・ISP事業者やルータベンダが参加しています。コアな仕様を定めたドラフトは20回以上の改版を重ねており、RFC化目前(2019年中の見込み)です。

筆者は、標準化のための議論と並行して、DOTSプロトコルのOSS実装※3を進めてきました。我々のOSS実装は、DOTSプロトコルが実際に使えるものかどうかの実証に用いられ、リファレンス実装となっています。IETFハッカソンの機会を利用して、他ベンダと5回以上の相互接続試験を実施しており、仕様上の問題点を洗い出して指摘し、提案活動をしてきました。

ベンダでの実装がさらに進み、DOTSプロトコルの利用が広がっていくことに期待しています。

○DOTSプロトコルの今後

DOTSプロトコルでまだ実現できないことも、いくつかあります。まず、シグナルチャンネルでやり取りされる情報は、攻撃を受けているネットワークリソースに関する情報に限られています。そのため、DOTSクライアント側で観測した、どのような攻撃を受けているかといった、攻撃種別情報を通知する方法は定義されていません。これらの付加的な情報はテレメトリ情報と呼ばれ、DOTSサーバ側でこれらの付加情報を利用して、より適した防御を実施できるのではないかと議論されています。

しかし、どのくらいの情報を入れるべきかという議論は、一度紛糾しています。定義をしなければいけないことがあまりにも多過ぎるため、一旦スコープを縮小し、それにより標準化を早めるという判断がされています。コアな仕様の標準化が進んだ現在、もう一度テレメトリ情報に関する議論が復活する可能性があります。

また、現在の仕様では、DOTSサーバからDOTSクライアントへは、攻撃が終了したかどうか、どのくらいの割合のパケットが防御によってドロップされているか、という情報しか通知することができないのですが、攻撃内容についての付加的な情報を追加できるようになる可能性があります。

より使えるプロトコルになるにはこのような機能を追加すべきだ、などのアイデア・助言がある方は、ぜひ筆者に声をかけてください。

(NTTコミュニケーションズ株式会社 西塚要)

※3 go-dots https://github.com/nttdots/go-dots