サイバー戦入門　その４

－ＤＤｏＳ攻撃の仕組みとその対策－

三村　守（防大情報工学科）

１　はじめに

ＤｏＳ[1]攻撃あるいはＤＤｏＳ[2]攻撃は、サービス拒否攻撃あるいはサービス妨害攻撃とも呼ばれるサイバー攻撃の一種である。２００７年に発生したエストニアに対するサイバー攻撃では、国民の生活に深刻な影響が出たと言われている。我が国においても、官公庁のホームページに対するサイバー攻撃や、Ａｎｏｎｙｍｏｕｓと呼ばれる不特定多数の集団によるサイバー攻撃が国会や新聞で取り上げられる等、社会において注目を集めるようになってきている。ＤＤｏＳ攻撃は、専用ツール等を用いれば、攻撃先を指定するだけで手軽に実行することが可能である。ＤＤｏＳ攻撃のための専用ツールには、インターネットにおいて誰もが無料で入手することが可能なものも少なくない。したがってＤＤｏＳ攻撃は、専門知識をあまり必要としない最も敷居が低いサイバー攻撃の１つであると言える。その上近年では、安価な料金でＤＤｏＳ攻撃を代行するサービスも出現している。例えば、Anonymous Stressor や vDosStressor といった攻撃代行サービスが存在している。２０１４年には、このような代行サービスを利用し、オンラインゲーム会社のサーバを２０時間にわたってダウンさせたとして、１６歳の高校生が書類送検されるという事件が発生した。このように、ＤＤｏＳ攻撃は、誰もが容易に実施することが可能であるにもかかわらず、場合によっては社会に深刻な影響を与える可能性を秘めている。さらに、防御側はＤＤｏＳ攻撃を完全に防ぐことは難しく、攻撃コストと対策コストは非対称の関係にある。その一方で、ＤＤｏＳ攻撃の影響が過大評価され、過剰な対応をしてしまう場合も少なくない。この原因の一つとして、ＤＤｏＳ攻撃の仕組みやその影響を実務担当者が理解していたとしても、経営層[3]に正しく伝わっていない可能性が考えられる。ＤＤｏＳ攻撃の影響を適切に評価するためには、実務担当者[4]はもちろんのこと、経営層もその仕組みや対策技術の概要を理解しておくことが重要である。また、実務担当者には経営層に状況を正確に説明するコミュニケーション能力が求められる。

---

1 DoS (Denial of Service)

2 DDoS (Distributed Denial of Service)

3 防衛省においては情報保証責任者、情報システム情報保証責任者、情報システム運用者、部隊等情報保証責任者等が経営層に該当する。

4 情報システムの運用やサイバー攻撃等対処の実務を担当する者や部隊等情報保証責任者補助者が実務担当者に該当する。

「サイバー戦入門　－サイバー攻撃の技術的仕組みと対策－」では、サイバー攻撃とは何かを理解するために必要な基本的な仕組みを、技術的な観点から体系的に解説することを試み、「サイバー戦入門　その２　－サイバー戦の概念と作戦－」ではサイバー戦の概念とサイバー作戦の種類について平易に解説することを試みた。その３からは、サイバー戦に関する各トピックスをより掘り下げて平易に解説することを試みている。本稿では、ＤＤｏＳ攻撃とその対策技術をとりあげる。以下、第２節ではＤＤｏＳ攻撃の具体例を挙げて概要を説明する。第３節ではＤＤｏＳ攻撃の定義と分類を示し、第４節では各ＤＤｏＳ攻撃の仕組みについて説明する。第５節では、その対策技術について説明し、最後にまとめと課題について述べる。

２　ＤＤｏＳ攻撃の具体例

（１）初期のＤＤｏＳ攻撃

インターネットが本格的に普及し始めた１９９０年代～２０００年頃のサイバー攻撃は、何らかの政府の活動に対抗して実施されたものもあったが、その目的がはっきりしない愉快犯によるものが比較的多かったとされている。この傾向は、概ねＤＤｏＳ攻撃の場合にもあてはまる。

特に影響が大きかった例としては、２００１年７月に発見されたＣｏｄｅＲｅｄ（コードレッド）[5]が挙げられる。ＣｏｄｅＲｅｄは、ＩＩＳ[6]と呼ばれるＭｉｃｒｏｓｏｆｔのＷｅｂサーバの脆弱性を利用して自身を拡散させ、いくつかのサイトにＤＤｏＳ攻撃を実施する機能を備えていた。その攻撃対象となったサイトには、米国のホワイトハウスも含まれていた。２００１年７月１９日には、ＣｏｄｅＲｅｄに感染したコンピュータは３５万台以上に達したとされ、世界中のインターネットのトラフィックが急増し、多くのサイトにおいてつながりにくい状態が生起した。これは、現時点までででインターネットのトラフィックに最も重大な影響を及ぼした事例である。

また、２００３年１月に確認されたＳＱＬ　Ｓｌａｍｍｅｒ（エスキューエル　スラマー）[7]も、インターネットに世界規模での重大な影響を与えたと言われている。ＳＱＬ　Ｓｌａｍｍｅｒは、ＭｉｃｒｏｓｏｆｔのＳＱＬ　Ｓｅｒｖｅｒ[8]等の脆弱性を利用して自身を拡散させるだけの単純な機能を備えており、その感染動作が単純で自身のサイズも小さいことから、爆発的に感染台数を増やしたとされている。特に、韓国ではＤＮＳ[9]サーバがダウ

---

5 インターネット上でＷｅｂサーバを対象として感染を拡大するワーム
6 IIS (Internet Information Service)
7 インターネット上でデータベースサーバを対象として感染を拡大するワーム
8 データベースを提供するソフトウェア
9 DNS (Domain Name Service) ドメイン名とＩＰアドレスの関係を管理するサービス

ンしたことで、全国でインターネットが利用できなくなるなどの大きな影響が出た。

これら初期のＤＤｏＳ攻撃では、不特定多数のサーバが攻撃を受けている。そのため、愉快犯によるものである可能性もあり、攻撃者の目的ははっきりしているとは言い難い。

（２）ハクティビスト[10]によるＤＤｏＳ攻撃

２０００年代中頃に入ってくると、政治的問題への抗議や反発を目的としたサイバー攻撃が多く発生するようになってきた。これらのサイバー攻撃の主な手段は、脆弱性があるＷｅｂサイトの改ざんや、特定のＷｅｂサイトを対象としたＤＤｏＳ攻撃であった。Ｗｅｂサイトの改ざんが成功するための要件は、そのサーバに任意の命令を実行可能な脆弱性が存在することである。したがって、攻撃者は必ずしもその対象を選べるわけではない。そのため、活動の趣旨とは無関係のサイトが改ざんされることも珍しくない。これに対し、ＤＤｏＳ攻撃では必ずしも脆弱性を必要としないため、明確に対象を指定して実施することが可能である。

例えば、２００４年９月には、日本の靖国神社への参拝問題に対する中国での反発から、中国から靖国神社のＷｅｂサイトへのＤＤｏＳ攻撃が発生した。２００５年には、尖閣諸島の領有権をめぐる問題から中国での反日感情が高まり、中国から日本の官公庁のＷｅｂサイトへＤＤｏＳ攻撃が発生した。さらに、２０１０年になると、満州事変の発端となった柳条湖事件が発生した日である９月１８日に合わせ、中国紅客連盟等のハクティビストらが主体となってＤＤｏＳ攻撃を実施するようになった。これらのＤＤｏＳ攻撃は、後述するエストニアやグルジア[11]の事例と比較すると組織的とは言いがたく、ＱＱチャット、ＹＹチャット等の中国のＳＮＳ[12]を用いて攻撃参加者の情報交換が実施されていた。以後、９月１８日のような特異日には、毎年のように中国から日本へのＤＤｏＳ攻撃の実施を呼びかける情報交換が実施されるようになった。これらのＤＤｏＳ攻撃では、警察庁のＷｅｂサイトをはじめ、政府機関、民間企業等のＷｅｂサイトが標的となった。なお、２０１５年以降になると、中国での反日感情の低下に伴い、中国から日本へのＤＤｏＳ攻撃も下火となってきている。このように、中国紅客連盟等の中国を拠点とするハクティビストらの活動は、日中２国間の関係に密接に関係している。

他のよく知られたハクティビストとしては、Ａｎｏｎｙｍｏｕｓ（アノニ

---

10 何らかの政治的あるいは社会的主張を目的としてサイバー攻撃を実施する主体
11 現在のジョージア
12 SNS (Social Network Service)

マス）[13]が挙げられる。Ａｎｏｎｙｍｏｕｓは、表現の自由、インターネットの自由な利用等を信条とする不特定多数のインターネットの利用者の集まりである。Ａｎｏｎｙｍｏｕｓは、２０１０年頃からＳＮＳ等の呼びかけを利用し、特定の拠点を持たずに活動を開始するようになった。２０１１年には、プレイステーション３のハッキングに対するソニーの訴訟に抗議し、複数の関連するＷｅｂサイトに対するＤＤｏＳ攻撃が発生した（ＯｐＳｏｎｙ[14]）。２０１２年６月には、６月２０日に可決された違法なダウンロードに対する刑事罰を盛り込んだ著作権法に抗議し、関係する政府機関や団体のＷｅｂサイトに対するＤＤｏＳ攻撃が発生した（ＯｐＪａｐａｎ）。このように、Ａｎｏｎｙｍｏｕｓの活動は、その信条に反する活動を実施した主体に反発して実施される傾向がある。

以上の例に示すようなＤＤｏＳ攻撃は、政治的あるいは社会的主張を目的としていることから、その活動は大々的で目立つ傾向が認められる。そのため、攻撃者は本気で正体を隠そうとはせず、攻撃主体は比較的はっきりとしている特徴がある。ＤＤｏＳ攻撃は、政治的あるいは社会的主張を目的とするハクティビストらの主要なサイバー攻撃の手段となっている。

（３）国家の関与が疑われるＤＤｏＳ攻撃

政治的問題への抗議や反発を目的としたサイバー攻撃の中には、国家の関与が疑われるＤＤｏＳ攻撃もある。これらのＤＤｏＳ攻撃は、何らかの政治的問題への抗議や反発と関係している点はハクティビストによるＤＤｏＳ攻撃と類似しているが、その活動が実際の国家の軍事的活動と連動している点や、実施主体に国家の関与が疑われている点が異なっている。

例えば、２００７年４月に、警官隊とロシア系住民の衝突をきっかけとして発生したエストニアの政府機関、銀行、新聞、放送業者等に対するＤＤｏＳ攻撃が挙げられる。これらの一連のＤＤｏＳ攻撃は、ボットネット[15]を用いて大規模かつ組織的に実施されている点が従来とは異なっていた。エストニアは、１９９１年の独立時から国家のインフラとして積極的にインターネット技術を導入してきた。そのため、これらのＤＤｏＳ攻撃により、情報通信、銀行の決済機能等が麻痺し、国民の生活に深刻な影響が出たとされている。また、２００８年８月に発生したグルジアの政府機関や商業ネットワークに対するＤＤｏＳ攻撃は、南オセチア州を巡る紛争において、ロシアの軍事攻撃に連動して実施された。これらのＤＤｏＳ攻撃には、ロシアが関与しているとの指摘があるが、ロシア政府はこれを否定している。

---

13 匿名を意味する不特定多数のハクティビストの集まり

14 Ｏｐ～はＡｎｏｎｙｍｏｕｓが実施する一連の活動に付与される作戦名

15 攻撃者がマルウェア等を感染させて乗っ取った端末で構成されるネットワーク

他の国家の関与が疑われる事例としては、２００９年７月に米韓の政府機関、金融、情報通信事業者等のサイトに対して実施されたＤＤｏＳ攻撃が挙げられる。これらのＤＤｏＳ攻撃は、韓国国内の２３０００台の乗っ取られた端末を含むボットネットにより組織的に実施されたとされている。同様の手口によるＤＤｏＳ攻撃は２０１１年３月にも実施され、この時には最終的に踏み台とされたコンピュータのハードディスクが消去され、起動できない状態とされた[16]。韓国国家情報院はこれらのサイバー攻撃を、北朝鮮によるものとしているが、その証拠となる具体的な根拠は示されていない。

以上の例に示すようなＤＤｏＳ攻撃は、組織的で軍事的活動と連動していることもあり、実施主体に国家の関与が疑われている点が特徴である。また、ハクティビストらのサイバー攻撃とは異なり、実施主体はＤＤｏＳ攻撃への関与を明確にしていないという特徴がある。

３　ＤＤｏＳ攻撃の定義と分類

ＤｏＳ攻撃あるいはＤＤｏＳ攻撃は、対象とするサービスへの大量の通信（トラフィック）の送付や仕様の悪用等により、そのサービスの提供を妨害して使用不能とするサイバー攻撃の一種であり、サービス拒否攻撃あるいはサービス妨害攻撃とも呼ばれる。ＤｏＳ攻撃は、一般に複数の攻撃元から実施される場合がほとんどであるため、分散ＤｏＳ攻撃（ＤｉｓｔｒｉｂｕｔｅｄＤｏＳ攻撃）と同義で用いられることも多い。そのため、特に区別を必要としない場合には、単にＤＤｏＳ攻撃と呼ばれることもある。ＤＤｏＳ攻撃は、情報セキュリティの３要素である機密性、完全性、可用性のうち、情報システムの可用性を侵害するサイバー攻撃の一種である。

サイバー攻撃は、攻撃者が主体的に任意のタイミングで実施できる「能動的攻撃」と、被攻撃者による何らかの動作を必要とする「受動的攻撃」に分類できる。この分類によると、ＤＤｏＳ攻撃は「能動的攻撃」であり、その攻撃の対象は図１に示すように、主にインターネットに公開されているサーバである。Ｗｅｂサーバに対するＤＤｏＳ攻撃は、攻撃者が自分の任意のタイミングで攻撃ツールを実行する（図１①）か、あるいは踏み台となるコンピュータに指示を与えることで実施する（図１②）ことが可能である。組織の内部ネットワーク[17]でのみ公開されているサーバ（図１③）や端末（図１④）は、ほとんどの場合に能動的攻撃の対象とはならない。

---

16 韓国においては「３・２０電算大乱」と呼ばれている。

17 インターネットとは異なる体系のＩＰアドレスを付与している。

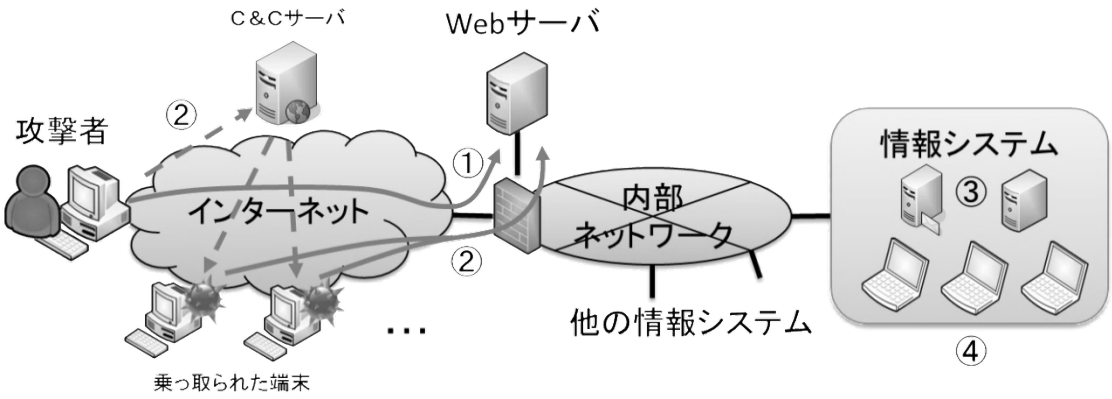

図１：Ｗｅｂサーバに対するＤＤｏＳ攻撃

ＤＤｏＳ攻撃には、大量のトラフィックを送りつける等の手法でサービスを利用不能にするフラッド攻撃や、サービスの脆弱性を利用する等の手法でサービスを利用不能にする攻撃がある。これらの攻撃において、被攻撃者側のボトルネックとなるのは、ネットワーク回線かサーバ等のリソース[18]である。この視点に基づくと、ＤＤｏＳ攻撃は、主にネットワーク回線の帯域を飽和させる帯域枯渇型の攻撃と、対象とするシステムのメモリ等のサーバのリソースを圧迫するリソース枯渇型の攻撃に分類することができる。また、やや特殊な例としては、脆弱性を用いてサーバやサービスを停止あるいは再起動させる等のＤｏＳ攻撃もある。実際のＤＤｏＳ攻撃では、これらの様々な手法やツールが組み合わせて活用されることも珍しくない。

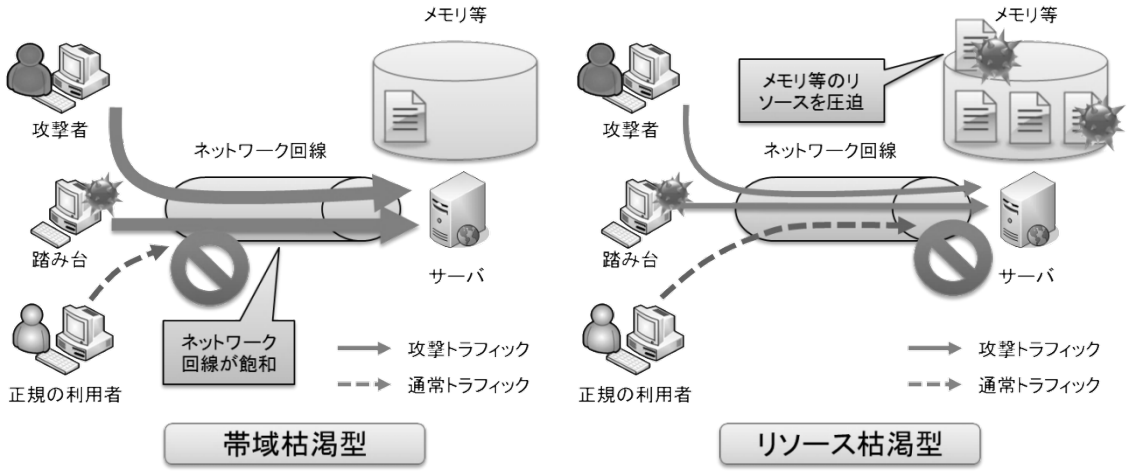

図２：帯域枯渇型とリソース枯渇型の攻撃

18 コンピュータのメモリ、同時接続数等

（１）帯域枯渇型の攻撃

帯域枯渇型の攻撃は、大量のトラフィックを送りつけてネットワークの帯域を飽和させることにより、サービスの提供を妨害する攻撃である。この攻撃では、攻撃対象となるのはネットワーク回線の帯域である。

例えば、１Ｍｂｐｓ[19]のネットワーク回線に対し、１０Ｍｂｐｓの無意味なトラフィックを送信するＵＤＰ[20]フラッド攻撃を実施すれば、理論的には９Ｍｂｐｓのトラフィックが処理できずに、途中のネットワーク機器等で破棄されることになる[21]。この時に、攻撃トラフィックと通常トラフィックを区別することができなければ、攻撃トラフィックと同様に通常トラフィックも破棄されてしまう。そのため、正規の利用者のサービスの利用に支障が生じる。これが、帯域枯渇型の攻撃により、サービスの提供が妨害される仕組みである。

帯域枯渇型の攻撃は、ネットワーク回線を埋め尽くす非常にシンプルな攻撃である。シンプルな攻撃であるがゆえに、スマートな対策は難しく、対策も力技とならざるを得ない。ネットワーク回線の帯域を増速し、余裕を持たせることができれば、サービスの利用に支障が生じる状態を解消することができる。より効果的に攻撃トラフィックのみを遮断するためには、通常トラフィックと攻撃トラフィックの区別が明確にできる必要がある。したがって、通常トラフィックを模したＤＤｏＳ攻撃では、攻撃トラフィックと通常トラフィックを区別して、攻撃トラフィックのみを遮断することは非常に困難である。また、仮に攻撃トラフィックを区別することができたとしても、遮断する位置がサービスを提供するサーバやその直前のネットワーク機器であれば、攻撃元の端末から遮断を実施するネットワーク機器等までのネットワーク回線は埋め尽くされてしまう。そのため、帯域枯渇型の攻撃に対しては、このような直前での遮断はほとんど意味をなさない。帯域枯渇型の攻撃に対して効果的な対策を実施するためには、なるべく攻撃元に近い根元のネットワーク機器において攻撃トラフィックを遮断する必要がある。

（２）リソース枯渇型の攻撃

リソース枯渇型の攻撃は、仕様や脆弱性の悪用により対象とする情報システムのリソースを圧迫し、サービスの提供を妨害する攻撃である。この攻撃では、攻撃対象となるのはサービスを提供する情報システムのリソースである。ここでいう情報システムのリソースとは、コンピュータのメモリ、同時接続数等のサービスの提供に影響を与える有限の資源のことである。

---

19 １秒間に１メガビットの情報を処理することができる速度

20 UDP (User Datagram Protocol)

21 回線速度の実測値は理論値よりも一般的に遅い。

例えば、図３に示すＳＹＮフラッド攻撃と呼ばれる手法では、攻撃者は対象とするサーバにＳＹＮパケットと呼ばれる接続を要求するためのパケットを大量に送付する（図３①）。これに対し、そのサーバは要求元の端末に対する応答のパケットを返し、接続の要求元からの応答を待つ（図３②）。この時、サーバのメモリにおいて、その応答を待つための領域が割り当てられる。ここで、通常の場合には、接続の要求元は応答のパケットを送信する（図３③）。この動作[22]により、要求元の端末とサーバの相互の接続が確立し、双方向の通信が開始される。これら動作は、ＴＣＰ[23]と呼ばれるインターネットで用いられるプロトコル[24]の仕様である。しかしながら、ここで接続の要求元の端末が応答のパケットを送信せず、接続を確立しない場合（図３④）には、そのサーバは要求元の端末からの応答をいつまでも待つことになってしまう[25]。このように接続を確立しないＳＹＮパケットが一度に大量に送付されると、そのサーバは大量のメモリを消費することになる。この時に、ネットワーク回線が飽和していなかったとしても、そのサーバのリソースが圧迫されていれば、正規の利用者のサービスの利用に支障が生じる。これが、リソース枯渇型の攻撃により、サービスの提供が妨害される仕組みである。

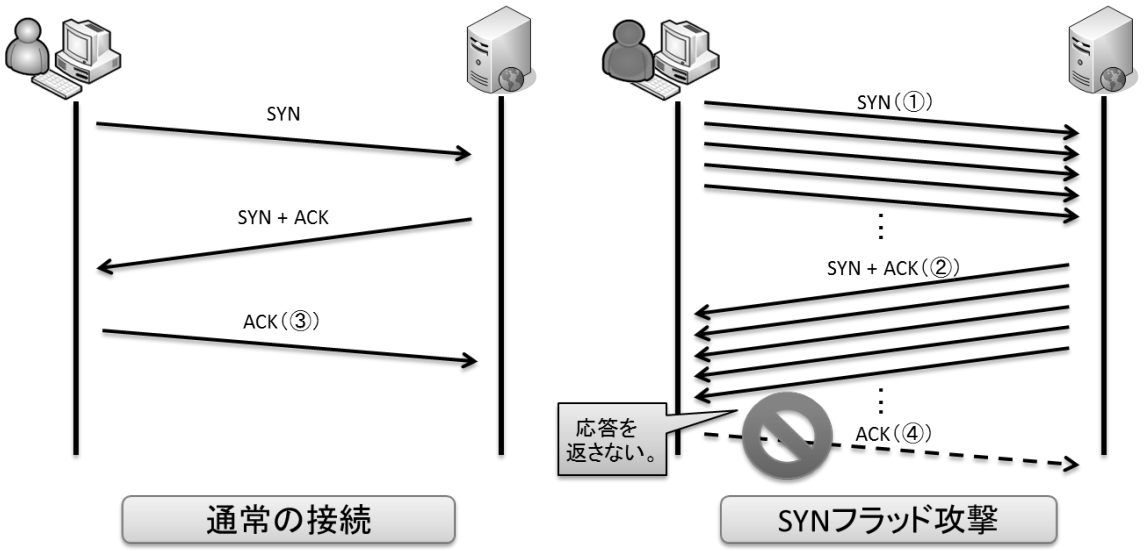

図３：通常の接続とＳＹＮフラッド攻撃

[22] ３ウェイ・ハンドシェイクと呼ばれる。
[23] TCP (Transmission Control Protocol)
[24] 通信規約
[25] 正確には設定されたタイムアウトの時間が経過するまでの間

リソース枯渇型の攻撃は、仕様や脆弱性を悪用したより洗練された攻撃である。そのため、その攻撃の仕組みを理解していなければ、効果的な対策を実施することはできない。例えば、ＴＣＰの実装の脆弱性を利用した古典的な攻撃では、正常なトラフィックには含まれない明らかに不正なパケットが用いられることが多い。このような場合には、サーバやネットワーク機器でその不正なパケットを容易に検知し、遮断することが可能である。これに対し、先に示したＳＹＮフラッド攻撃では、ＴＣＰの仕様を悪用し、通常の接続に用いられるパケットと同じパケットを用いて攻撃を実施する。そのため、単純に単一のパケットを検査しただけでは、通常トラフィックと攻撃トラフィックを見分けることは難しい。また、ＳＹＮフラッド攻撃ではサーバのリソースが圧迫されるため、ネットワーク回線が飽和するとは限らない。このような状況において、対策としてネットワーク回線の帯域を増速したとしても、サーバのリソースが圧迫されている状況が改善されなければ、サービスの提供に支障が生じている状態は改善されない。したがって、この状況では回線の増速は無意味である。他のアプローチとしては、その圧迫されているリソース（この場合はメモリ）を増強するという対策が考えられる。しかしながら、ＳＹＮフラッド攻撃では、攻撃者は送信元のＩＰアドレスを偽装し、トラフィック量を増やすことは容易であるため、増強したリソースもすぐに圧迫されてしまう可能性が高い。そこで、ＳＹＮクッキー等のいくつかの対策が考案された。ＳＹＮクッキーが実装されたサーバでは、メモリが圧迫された状態に陥ると、ＳＹＮパケットを受信したらメモリに領域を割り当てずに応答のパケットを送信する。これにより、ＳＹＮパケットを受信した時点でメモリを消費しなくなる。その後、正当な応答のパケットを受信した場合にのみ、メモリに領域を割り当てる。ＳＹＮフラッド攻撃では送信元のＩＰアドレスを偽装することが多いため、正当な応答のパケットが返されないことが多い。そのため、偽装されていない正当な接続元からの要求に対してのみ、メモリを割り当てられるようになる。このように、リソース枯渇型の攻撃に対しては、攻撃の仕組みを理解し、どのリソースが圧迫されているのかを把握して効果的な対策を講じる必要がある。

４　ＤＤｏＳ攻撃の仕組み

（１）ＤＤｏＳ攻撃

ＤＤｏＳ攻撃には、単独の攻撃、複数人による分散攻撃、あるいは乗っ取られた端末（踏み台）を経由して実施する分散協調型の攻撃がある。図４に各ＤＤｏＳ攻撃の仕組みを示す。図４の左側は単独の攻撃、右側は分散協調型の攻撃の仕組みを示している。なお、複数人による分散攻撃は、右側の分

散協調型の攻撃において、指令サーバを用いない場合に相当する。

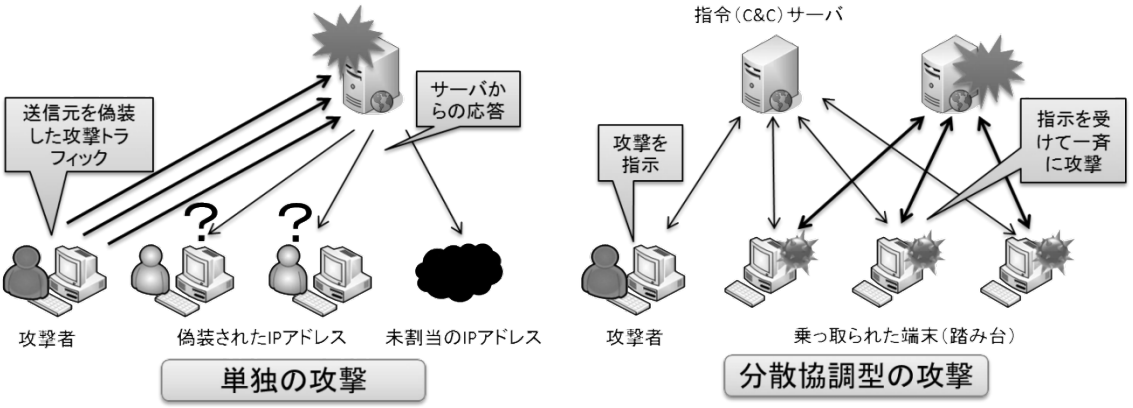

図４：各ＤＤｏＳ攻撃の仕組み

単独の攻撃においては、送信元のＩＰアドレスを偽装するために、接続を確立しない片方向の通信を用いる場合が多い。片方向の通信の場合には、分散された複数のＩＰアドレスからの攻撃のように見せかけることが容易である。片方向の通信を用いた攻撃では、実在の端末を準備する必要がない。送信元のＩＰアドレスを偽装し、あるサーバに対して接続を要求すると、そのサーバは偽装されたＩＰアドレスに対して応答を返そうとする。そのため、攻撃者はそのサーバからの応答を受信することができず、双方向の接続を確立することができない。このように接続を確立しない片方向の通信を用いた攻撃は、コネクションレス型の攻撃と呼ばれることもある。第３節で例示したＵＤＰフラッド攻撃やＳＹＮフラッド攻撃では、接続を確立しないため、コネクションレス型の攻撃に分類することができる。コネクションレス型の攻撃では、攻撃トラフィックに記録された送信元ＩＰアドレスから攻撃元をたどることは困難である。なぜならば、片方向の通信では、送信元ＩＰアドレスは攻撃者が任意に設定することが可能であるためである。

分散協調型の攻撃では、攻撃者は乗っ取られた端末（踏み台）に対し、指令サーバ[26]を経由して攻撃の指示をする。指示を受信した端末（踏み台）は、協調して一斉にサーバに対して攻撃を実施する。この攻撃では、複数の実在の端末を用いるため、接続を確立する双方向の通信による攻撃も実施することが可能である。このような双方向の通信による攻撃は、コネクションレス型の攻撃と区別して、コネクション型の攻撃と呼ばれることもある。単純なコネクション型の攻撃の例としては、Ｆ５攻撃が挙げられる。Ｆ５攻撃は、ウェブブラウザによるページの再読込を連続して頻繁に実施

[26] C&C あるいは C2 (Command and Control)

する[27]ことで、Ｗｅｂサーバに負荷をかける攻撃である。コネクション型の攻撃では、送信元のＩＰアドレスを偽装することが困難である。そのため、攻撃元を秘匿するためには、踏み台とする端末を準備する必要がある。なお、分散協調型の攻撃では、複数の端末を用いてコネクションレス型の攻撃を実施することも可能である。コネクション型の攻撃では、攻撃トラフィックに記録された送信元ＩＰアドレスから攻撃元をたどることが可能な場合がある。なぜならば、双方向の通信では、少なくともその送信元ＩＰアドレスを用いた端末は実在するためである。しかしながら、その実在する端末が、攻撃者の端末か乗っ取られた端末（踏み台）かを判断することは困難である場合が多い。

（２）ＤＲＤｏＳ攻撃

２０１０年代頃になると、ＤＲＤｏＳ[28]攻撃と呼ばれるより効果的なＤＤｏＳ攻撃が実施されるようになってきた。ＤＲＤｏＳ攻撃の仕組みを図５に示す。ＤＲＤｏＳ攻撃は、ＤｏＳリフレクション攻撃あるいは分散反射型ＤｏＳ攻撃とも呼ばれ、攻撃対象のサーバになりすました大量のリクエストを複数のリフレクタとなるサーバに送信し、反射した応答を攻撃対象のサーバに大量に送信して負荷をかける攻撃である。この時に、リフレクタとなるサーバは、その仕様や設定により、リクエストよりも増幅された応答を返す場合がある。想定していない不特定の利用者からのリクエストに対し、再帰的に応答を返してしまうＤＮＳサーバ[29]は、その典型的な例である。そのため、これらの攻撃は、増幅（アンプ）攻撃と呼ばれる場合もある。

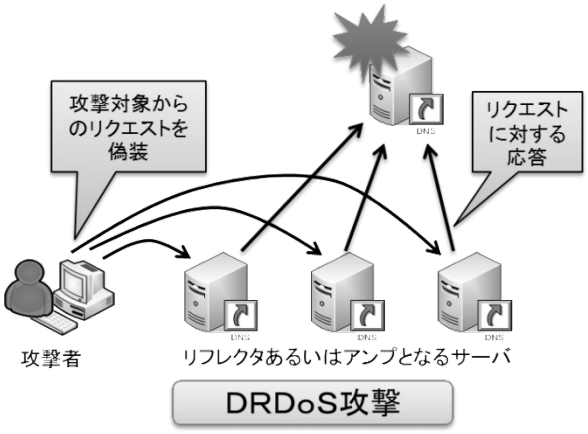

図５：ＤＲＤｏＳ攻撃の仕組み

---

[27] F5 キーを連打することで実施することも可能
[28] DRDoS (Distributed Reflective Denial of Service)
[29] オープン・リゾルバーと呼ばれる。

ＤＲＤｏＳ攻撃の例としては、ＤＮＳ[30]を利用したＤＮＳアンプ攻撃[31]やＮＴＰ[32]を利用した攻撃が挙げられる。２０１４年に高校生が代行サービスを利用してオンラインゲーム会社のサーバをダウンさせた事案では、ＮＴＰを利用したＤＲＤｏＳ攻撃が実施されたと言われている。ＤＲＤｏＳ攻撃では、攻撃トラフィックに記録された送信元ＩＰアドレスは、実在するサーバのＩＰアドレスである。しかしながら、そのサーバはリフレクタあるいはアンプとして攻撃者に悪用されたものである。さらに、攻撃者はそのサーバに対し、送信元を攻撃対象に偽装した片方向の通信を実施する。そのため、ＤＲＤｏＳ攻撃では、攻撃トラフィックに記録された送信元ＩＰアドレスから攻撃元をたどることは困難である。

（３）スローＨＴＴＰ　ＤｏＳ攻撃

これまでに示したＤｏＳ攻撃は、ネットワーク回線やリソースを枯渇させるために、大量のトラフィックを用いる攻撃であった。スローＨＴＴＰ　ＤｏＳ攻撃は、少量のトラフィックで接続時間を可能な限り引き伸ばし、長期間Ｗｅｂサーバのセッションを占有するリソース枯渇型の攻撃である。例えば、スローＨＴＴＰヘッダ攻撃[33]やスローＨＴＴＰ　ＰＯＳＴ攻撃[34]では、攻撃者の端末からサーバに対し、故意に大量のトラフィックを分割して十分な間隔をあけて送信する。スローリードＤｏＳ攻撃では、逆にサーバからの応答を故意に少量ずつ受信する。これらの手法により、攻撃者の端末からサーバのセッションが長期間占有されてしまうと、正規の利用者の端末とのセッションを確立することができず、サービスを提供することが困難となってしまう。スローＨＴＴＰ　ＤｏＳ攻撃はコネクション型の攻撃であり、送信元のＩＰアドレスを偽装することが困難である。そのため、攻撃元を秘匿するためには、踏み台とする端末を準備する必要がある。しかしながら、スローＨＴＴＰ　ＤｏＳ攻撃では少量の通常のトラフィックを用いるため、発見が困難であるという特徴がある。

（４）ＩＤＤｏＳ攻撃

ＩＤＤｏＳ[35]攻撃は、インターネットに接続された脆弱なＩｏＴ[36]機器を

---

30 DNS (Domain Name Service) ドメイン名等とIPアドレスの対応を管理するためのサービス
31 DNS リフレクタ攻撃あるいは DNS リフレクション攻撃とも呼ばれる。
32 NTP (Network Time Protocol) 正確な時刻を提供するためのサービス
33 攻撃ツールの名称から Slowloris 攻撃とも呼ばれる。
34 攻撃ツールの名称から R.U.D.Y 攻撃とも呼ばれる。
35 IDDoS (IoT Distributed Denial of Service)
36 IoT (Internet of Things) モノのインターネット

踏み台として用いるＤＤｏＳ攻撃のことである。２０１６年９月には、Ｍｉｒａｉと呼ばれる監視カメラ等のＩｏＴ機器に感染する機能を持つマルウェアによって構成されたボットネットによるものとされるＤＤｏＳ攻撃が発生した。さらに、そのマルウェアのソースコードが公開されたため、新たな亜種の発生やさらなる被害の拡大が懸念されている。

ＩＤＤｏＳ攻撃は、ＩｏＴ機器を踏み台とする点を除くと、その攻撃の手法自体に目新しい特徴があるわけではない。したがって、攻撃を受ける側の対策としては、これまでの攻撃に対する対策と同様となる。それにもかかわらずＩＤＤｏＳ攻撃が注目されたのは、その踏み台が一般的なコンピュータではなく、ＩｏＴ機器である点が極めて重要視されたためである。Ｍｉｒａｉは、ランダムにインターネットに接続されているＩｏＴ機器を探索し、パスワードの辞書攻撃[37]によって認証を突破し、感染を拡大する機能を持っていた。Ｍｉｒａｉが感染に使用していた辞書は、監視カメラ等のＩｏＴ機器に工場出荷時に初期値として設定されていたパスワードや、「admin」「12345」等の容易に推測可能な単語によって構成されていた。工場出荷時の初期のパスワードは、容易に推測可能な単語の場合や、インターネットに公開されている製品のマニュアルに記載されている場合すらある。そのため、このような機器をそのまま安易にインターネットに接続した場合には、攻撃者は容易に認証を突破し、その制御を奪うことが可能となる。このような脆弱性は、一般のコンピュータのＯＳやアプリケーションが対象の場合には、そのソフトウェアをアップデートして修正すればよい。しかしながら、ＩｏＴ機器は組込機器といういわゆるハードウェアの一種であるため、容易にオンラインでアップデートできない場合が多く、ウイルス対策ソフトのような対策もほとんど存在しない。事実、Ｍｉｒａｉの攻撃対象となったデバイスの中には、リコールの対象となって回収されたものもある。その上このようにアップデートが難しいスマートデバイス、スマード家電、スマートカー、制御システム等は、２４時間稼働していることも多く、今後も爆発的に増えていくことが予想されている。

このような現状においてとり得る対策は、極めて基本的な事項ではあるが、工場出荷時の初期のパスワードを容易に推測できないものに変更することである。また、不要なＩｏＴ機器を安易にインターネットに接続せず、やむを得ず接続する場合には、必要最低限度のアクセスに制限するように、適切にアクセス制御を実施することが重要である。ただし、これらの対策は、ＤＤｏＳ攻撃を受ける側だけが実施すればよい対策ではなく、インターネットやスマートデバイスを利用する誰もが常日頃から実施する必要がある対策

[37] 辞書に示された単語を順にパスワードとして試行し、認証の突破を試みる攻撃

である。そのため、すべてのＩｏＴ機器にこのような対策を徹底するのは困難である。スマートデバイスの利用者の中には、脆弱なデバイスがサイバー攻撃の踏み台として利用されるリスクを認識していない者も多い。また、自らが利用している機器が、一般的なコンピュータと同様の仕組みで動作するＩｏＴ機器であることを自覚していない場合も珍しくない。このように、急速に増えているスマートデバイスは、サイバーセキュリティ上のリスクを急増させており、根本的な対策と教育カリキュラムの立案が急務である。

（５）Ｎｏｄｅ．ｊｓに対する攻撃

Ｎｏｄｅ．ｊｓ[38]と呼ばれる環境を用いたサーバの増加に伴い、その処理の脆弱性を用いた新たな攻撃も出現している。例えば、ＲｅＤｏＳ[39]攻撃では、サーバに長い正規表現を含む文字列を送信し、その解釈に時間をかけさせることによりサービスの提供を妨害する攻撃である。また、ハッシュ関数等の暗号に関係する処理に負荷をかけることにより、サービスの提供を妨害する攻撃も報告されている。これらの攻撃は、長期間Ｗｅｂサーバの計算資源を占有するリソース枯渇型の攻撃である。これらの攻撃はコネクション型の攻撃であり、送信元のＩＰアドレスを偽装することが困難である。これらの攻撃の対象となるのはＮｏｄｅ．ｊｓ環境を用いたサーバのみであるが、今後その普及に伴い脅威が拡大する可能性も考えられる。

５　ＤＤｏＳ攻撃の対策技術

ＤＤｏＳ攻撃の対象となるのは、主にインターネットに公開されているサーバである。したがって、ＤＤｏＳ攻撃の対策は、これらのサーバを管理あるいは監視する主体が実施することになる。ＤＤｏＳ攻撃の対策においてポイントとなる事項は、攻撃トラフィックと通常トラフィックをどのように区別し、どの位置で遮断するかの２点である。これまでに示したとおり、通常トラフィックを模した攻撃トラフィックは、技術的に検知することが困難である。ネットワーク回線を飽和させる帯域枯渇型の攻撃に対しては、遮断する位置がサービスを提供するサーバやその直前のネットワーク機器であれば、ほとんど効果は期待できない。ＤＤｏＳ攻撃の対策技術は、その対策を実施する位置に基づくと、ネットワークの末端に位置する各サイトにおける対策と、ネットワークの途中に位置するＩＳＰ[40]における対策に分類することができる。各サイトにおける対策はさらに、ネットワークにおける対策と各サーバにおける対策に分類される。

---

38 サーバで JavaScript が動作する環境
39 Regular Expression Denial of Service Attack
40 ISP (Internet Service Provider) 通信事業者

（１）各サイトのネットワークにおける対策

各サイトのネットワークにおける最も基本的な対策としては、ファイアウォール、ＷＡＦ[41]、不正侵入防止装置（ＩＰＳ[42]）等による攻撃トラフィックの遮断（フィルタリング）が挙げられる。伝統的なファイアウォールでは、主としてＩＰアドレスに基づいたアクセス制御や、比較的単純な攻撃トラフィックを検知して遮断することが可能である。したがって、攻撃元のＩＰアドレスが判明すれば、伝統的なファイアウォールによって攻撃トラフィックを遮断することが可能である。しかしながら、通常トラフィックを模した攻撃トラフィックやより洗練された攻撃トラフィックを検知するためには、ＷＡＦ、ＩＤＳ[43]／ＩＰＳ、あるいは高額なＤＤｏＳ攻撃対策の専用機器が必要となる。これらの機器では、伝統的なファイアウォールと比較し、より高度な検知あるいは遮断のための複雑なルールあるいはシグネチャ[44]を設定することが可能である。例えば、ＤＲＤｏＳ攻撃やスローＨＴＴＰ　ＤｏＳ攻撃では、通常トラフィックを模した攻撃トラフィックが用いられる。このような通常トラフィックに紛れ込んだ攻撃トラフィックを検知するためには、一定時間ごとの通信回数、１つのＩＰアドレスからのセッション数等、何らかの値を監視し、上限や下限等の適切な閾値を設定する必要がある。なお、このような複雑なルールの設定の可否については、各機器の仕様を確認する必要がある。

他のネットワークにおける対策としては、帯域制御装置の導入が挙げられる。帯域制御装置は、ＩＰアドレス、プロトコル、通信速度等を基に、混雑したトラフィックを最適化した通信量を制御する装置である。帯域制御装置では、通信量を監視することができるため、適切な閾値を設定しておけば、ネットワーク回線を飽和させる帯域枯渇型の攻撃を検知することが可能である。さらに帯域制御装置が、攻撃トラフィックと通常トラフィックを区別することができれば、攻撃トラフィックの通信量を制御することで、攻撃の影響を緩和することも可能となる。例えば、ＮＴＰを用いたＤＲＤｏＳ攻撃の場合には、帯域制御装置によってＮＴＰの通信量を制御しておけば、他のプロトコルを用いるＷｅｂサービスへの影響を緩和することができる可能性がある。しかしながら、各サイトにおいて帯域制御を実施したとしても、攻撃元（この場合はリフレクタとなるサーバ）からその帯域制御装置までの間のトラフィックは占有されてしまう。そのため、各サイトにおける帯域制御の効果については限定的であると考えられる。

---

41 WAF (Web Application Firewall)
42 IPS (Intrusion Prevention System)
43 IDS (Intrusion Detection System)
44 ＩＤＳ／ＩＰＳにおいて不正な通信を検知するためのパターンファイル

（２）各サーバにおける対策

各サーバにおける最も基本的な対策としては、ボトルネックとなり得るリソースの増強が挙げられる。例えば、負荷分散装置[45]やキャッシュサーバ[46]の導入、サーバのＣＰＵやメモリを増強すれば、ボトルネックとなる各リソースを増強することができる。また、サーバのＯＳ[47]やアプリケーションのパラメータの調整についても重要である。特に、スローＨＴＴＰ　ＤｏＳ攻撃では少量のトラフィックが用いられるため、各サーバにおけるパラメータの調整が鍵となる。例えば、スローＨＴＴＰヘッダ攻撃やスローＨＴＴＰＰＯＳＴ攻撃に対しては、アプリケーションで適切な通信サイズ、受信速度、タイムアウトの時間等を設定しておけば、その影響を緩和することが可能である。サーバのＯＳやアプリケーションのパラメータを調整するに当たっては、正規の利用者のパフォーマンスへの影響を最小限にすることも考慮する必要がある。

スローＨＴＴＰ　ＤｏＳ攻撃は、少量かつ正常なトラフィックを用いるため、ネットワーク回線の帯域の監視やＩＤＳ／ＩＰＳのシグネチャでは検知することが困難である。このような攻撃に関しては、Ｗｅｂサーバからの応答が正常に得られるかを定期的に監視する製品を用いることで、異状を検知することは可能である。ただし、その製品が検知した異状が、一般の利用者による過負荷によるものか、ＤＤｏＳ攻撃によるものかを判断するためには、より詳細な調査が必要となる。

（３）ＩＳＰにおける対策

ネットワーク回線を飽和させる帯域枯渇型の攻撃に対しては、各サイトや各サーバよりも、上流のＩＳＰにおける対策が効果的である場合が多い。

ＩＳＰにおける基本的な対策としては、Ｉｎｇｒｅｓｓフィルタ及びＥｇｒｅｓｓフィルタが挙げられる。Ｉｎｇｒｅｓｓフィルタ及びＥｇｒｅｓｓフィルタは、ＩＳＰの出入口にて送信元が詐称されているパケットを遮断する技術である。Ｉｎｇｒｅｓｓフィルタは、そのあらかじめ設定した正当なＩＰアドレス以外の送信元ＩＰアドレスが付与された外部から内部へ流入するパケットを遮断する。Ｅｇｒｅｓｓフィルタはその反対に、そのＩＳＰが管理する正当なＩＰアドレス以外の送信元ＩＰアドレスが付与された内部から外部へ流出するパケットを遮断する。インターネットは一元的に管理されている単一のネットワークではなく、管理する組織が異なる複数のＩＳ

---

45 ロードバランサとも呼ばれ、外部からの接続要求を同等の機能を有する複数の装置に割り当て、一台あたりの負荷を軽減するための装置

46 サーバのコンテンツの複製を蓄積し、本来のサーバの代わりに応答することで負荷を軽減するためのサーバ

47 OS (Operating System) コンピュータを制御するための基本ソフトウェア

Ｐの集合体である。インターネットを世界、ＩＳＰを国家、パケットを国民に例えると、Ｉｎｇｒｅｓｓフィルタは入国審査、Ｅｇｒｅｓｓフィルタは出国審査のようなものである。仮にすべてのＩＳＰがこれらのフィルタを厳密に運用すれば、インターネットにおける詐称パケットは理論的には存在しなくなるはずである。しかしながら、現実の世界での出入国審査は各国で異なるように、すべてのＩＳＰがこれらのフィルタを厳密に運用するのは難しいのが現実である。

ＩＳＰにおけるより実践的な対策としては、ＤＤｏＳ攻撃遮断サービスが挙げられる。これらのサービスは、各ＩＳＰが独自に提供するものであり、ＩＳＰによってその内容には若干の差異がある。その内容は概ね、そのＩＳＰが管理するネットワークにてＤＤｏＳ攻撃を検知して遮断するという内容である。これらのサービスを検討するにあたって重要なのは、攻撃を検知する手法と攻撃を遮断する位置である。これまでに示したとおり、通常トラフィックを模した攻撃トラフィックをどのように検知するかについては、対策の効果に大きな影響を及ぼす事項であるため、その内容を十分に確認すべきである。また、攻撃を遮断する位置についても、通常トラフィックが流入してくる位置よりも、攻撃者に近い位置で攻撃トラフィックを遮断することができなければ、通常トラフィックも攻撃の影響を受けてしまう可能性が高い。そのため、このようなＤＤｏＳ攻撃遮断サービスを効果的に運用できるのは、大規模なバックボーンネットワークを保有しているＩＳＰに限られてくるものと考えられる。このように、ＩＳＰにおけるＤＤｏＳ攻撃遮断サービスは、完全に攻撃を遮断できるものではなく、あくまでも攻撃の影響をある程度緩和するものと認識すべきである。

（４）ＣＤＮの活用

ＩＳＰよりも上流でのアプローチとしては、ＣＤＮ[48]が挙げられる。

ＣＤＮは、もともとＡｋａｍａｉ社が提唱したコンテンツを配信するためのネットワークであるが、ＤＤｏＳ攻撃対策としても注目されるようになった。ＣＤＮでは、世界各地に分散したサーバに、対象とするオリジナルのサーバのコンテンツの複製を分散配置する。これにより、論理的には、オリジナルのサーバと同じコンテンツを提供するサーバが、世界各地に分散して配置されることになる。利用者は、そのコンテンツを取得するために、オリジナルのサーバではなく、論理的に一番近い位置にあるサーバに自動的にアクセスする。そのため、オリジナルのサーバに対する負荷を分散できるだけでなく、高速に利用者にコンテンツを配信することも可能となる。ＣＤＮの方式としては、オリジナルのサーバのコンテンツを各サーバに手動でアップロ

48 CDN (Contents Delivery Network)

ードするプッシュ方式と、各サーバがオリジナルのサーバのコンテンツをダウンロードしてキャッシュ[49]するプル方式がある。プッシュ方式では、あらかじめ各サーバにコンテンツをアップロードする手間がかかるが、仕組みが単純であり、パラメータのチューニングの必要がない。プル方式では、オリジナルのサーバに変更を加えずに簡単に負荷分散を実施することができるが、キャッシュの有効期間や対象のファイルを選択する等のチューニングを実施する必要がある。

ＣＤＮは、もともと大規模配信のための仕組みであり、アクセスが増大した場合にも、多くの利用者に大容量のコンテンツを提供することを可能とする。このアクセスが増大した状況は、ＤＤｏＳ攻撃を受けた状況と基本的には同じである。そのため、ＣＤＮはそのままＤＤｏＳ攻撃の対策としても活用することが可能である。ＣＤＮが実施しているのは、ＤＤｏＳ攻撃を受けた場合にボトルネックとなり得るリソースの増強である。ＣＤＮでは、サーバのリソースやネットワーク回線だけでなく、ネットワークの経路も含めたサービス全体のリソースの増強が可能である。オリジナルのサーバのコンテンツを、より多くかつ広範囲のサーバに分散することで、ＤＤｏＳ攻撃の影響を根本的に緩和することが可能となる。しかしながら、ＣＤＮはその分散の規模にもよるが、一般にその費用も高額となる傾向が認められる。したがって、ＣＤＮの採用の適否や規模については、その必要性については十分に検討すべきである。

（５）ＩＰトレースバック技術

これまでに示した対策技術は、主にＤＤｏＳ攻撃を検知して遮断あるいは緩和する防勢的な技術であった。より攻勢的な対策技術としては、ＤＤｏＳ攻撃の攻撃元を追跡するためのＩＰトレースバックという技術が挙げられる。

ＩＰトレースバック技術は、対象とするパケット（ここではＤＤｏＳ攻撃に用いられたパケット）を中継した直近のルータをたどり、この手順を再帰的に繰り返すことでその送信元を追跡する。対象とするパケットがどのルータから物理的に中継されたのかを判断する手法については、パケットに何らかの情報を埋め込む方式、ルータにパケットの情報を記録する方式等が挙げられる。例えば、あるルータを経由したパケットに、ユニークに識別できる情報を埋め込むという手法が考えられる。このようにすれば、パケットの送信元が偽装されていた場合でも、そのパケットから一意に識別できる情報を抽出できれば、物理的にそのルータを経由したことを確認することができる。

---

49 アクセスしたデータを蓄積し、２回目以降は実際にアクセスせずに蓄積したデータを使用すること

ＩＰトレースバック技術には様々な方式が考案されているが、いずれの方式においても共通する課題を抱えている。それは、効果的に運用するためには、すべてのＩＳＰに共通の機能を備えたルータやトレースバック装置を導入する必要がある点である。すでに示したとおり、インターネットは一元的に管理されている単一のネットワークではなく、管理する組織が異なる複数のＩＳＰの集合体である。よって、すべてのＩＳＰが共通のトレースバック機能を備えた機器を導入するのは現実的ではない。このように、ＩＰトレースバック技術はＩｎｇｒｅｓｓフィルタ及びＥｇｒｅｓｓフィルタの場合と同様に、実現可能性における課題を抱えている。したがって、ＩＰトレースバック技術は、攻撃者を追跡するための根本的な解決策とはなりえていないのが現状である。

６　おわりに

本稿では、ＤＤｏＳ攻撃とその対策技術についてやや専門的な内容に踏み込みつつも、なるべく平易に解説することを試みた。第２節ではＤＤｏＳ攻撃の具体例を、初期のＤＤｏＳ攻撃、ハクティビストによるＤＤｏＳ攻撃及び国家の関与が疑われるＤＤｏＳ攻撃に分類して説明した。第３節ではＤＤｏＳ攻撃を帯域枯渇型とリソース枯渇型に分類して各々の特徴について説明し、第４節では各ＤＤｏＳ攻撃の仕組みについて説明した。第５節では、各サイト、各サーバ、ＩＳＰ等における対策技術について説明した。

本稿で説明したＤＤｏＳ攻撃は、誰もが容易に実施することが可能である。ＤＤｏＳ攻撃は、情報システムに致命的な影響を与える場合もあれば、単にホームページの閲覧が困難となるような微々たる影響の場合も少なくない。ＤＤｏＳ攻撃の仕組みやその影響が、実務担当者だけでなく、経営層にもある程度は正しく理解されていれば、ＤＤｏＳ攻撃の影響を適切に評価し、適切な対応をとることが可能となるものと考える。サイバー攻撃に関する分野は、技術の進歩が著しい分野であり、その脅威は刻々と変化している。このような変化する脅威に適切に対応していくためには、その仕組みや対策技術の基本となる仕組みを理解した上で、日ごろの情報収集を継続し、保有している知識を継続的にアップデートしていくことが不可欠である。

本稿に示したように一口にＤＤｏＳ攻撃と言っても、様々な分類や手法があり、様々な特徴がある。ある攻撃に対して有効な対策が、他の攻撃に対しても有効であるとは限らない。したがって、ＤＤｏＳ攻撃の対策を検討するにあたっては、攻撃の特徴を見極め、効果的な対策を選択することが重要である。また、対策を導入するにあたっては、攻撃コストと対策コストの非対称性についても留意すべきである。攻撃側はＤＤｏＳ攻撃を容易に低コストで実施できる

が、防御側はこれを完全に防ぐことは技術的に難しい。あらゆる対策をとろうとすると、対策コストも高額となってしまう傾向がある。また、すでに導入されている対策と競合する類似の対策を、高額の費用を投じて導入してしまう場合も少なくない。そのため、本当にそこまでの対策を実施する必要があるのかについては、現状実施している対策を把握した上で、よくよく検討する必要があるものと考える。