# サービス妨害攻撃の対策等調査

## - 報告書 -

2010 年 12 月

IPA 独立行政法人 情報処理推進機構
セキュリティセンター

# 目　次

## はじめに

本報告書は、いわゆる「サービス妨害攻撃(Denial of Service Attack、DoS 攻撃)」とはどのような脅威であり、どのように対応すべきかについて、とりまとめたものである。サービス妨害攻撃については、海外で大きな被害が発生していたり、「有効な対策がない」攻撃手段であると言われたこともあって、懸念されている方も多いと思われる。昨今ではこうした状況を悪用した恐喝[1] や詐欺[2] の存在も指摘されており、サービス妨害攻撃について十分な知識をもたないことで、詐欺にあったり、あるいは必要以上に脅威を感じることで不必要な設備投資を行ってしまったりすることも考えられる。

本報告書では、サービス妨害攻撃に対して**「まずは知ることから始まる」**との認識のもと、経営者やセキュリティ担当者が知っておくべき必要最小限の内容を中心に紹介している。是非この内容を理解し、適切な対策を講じることで、サービス妨害攻撃をむやみに恐れることなく、IT(情報技術)やインターネットの利活用を推進していただきたい。

### (1) 本報告書の想定読者

本報告書は、中小企業、小規模な公的機関、団体等、規模が比較的小さく、専任のセキュリティ管理者を置くことが難しい組織における経営者(CIO、CTO 等を含む)、情報セキュリティ担当者を主たる読者と想定して記述している。

ただし、こうした方々以外にも、サービス妨害攻撃について関心を持ったり、対策の必要性を感ずるすべての人々の利用にも資するよう、極力普遍的な内容となるように配慮している。

### (2) 本報告書の内容

本報告書はインターネットで発生しているサービス妨害攻撃に関して、以下の内容をとりまとめている。

第 1 章：サービス妨害攻撃の定義を行い、概要を説明。
第 2 章：企業や組織に対するサービス妨害攻撃を国内外の事例を交えて紹介。
第 3 章：サービス妨害攻撃の構造を、攻撃の動機、背景、手法の視点から概説。
第 4 章：サービス妨害攻撃の事前対策、被害時の相談先、法律・制度の面から説明。
第 5 章：まとめとして企業等が担うべき役割や対策等を総括。

---

[1] ここで「恐喝」とは、サービス妨害攻撃の首謀者が、被害者(企業)に対して、攻撃をやめて欲しければ金銭を支払え、と要求するなどの行為を指す。具体的な事例を 2.1.1 節等に挙げている。

[2] ここで「詐欺」とは、サービス妨害攻撃の首謀者が、被害者(企業)に対して、第三者を装って、攻撃を抑える・被害を低減させるなどとして、対価を要求するなどの行為を指す。

## 第1章 サービス妨害攻撃の概要

本章では、サービス妨害攻撃とはどのようなものかを知っていただくため、最新の動向と定義等を説明する。

### 1.1 ますます身近になるサービス妨害攻撃

インターネットで用いられる技術を用いて、コンピュータやネットワークに対してそのサービスを妨害することが可能であることは専門家の間では以前から知られていた。それが社会に対する脅威となることを人々が認識するようになったのは、2000 年 2 月に米国の大手の Web サービス(Yahoo、eBay 等)に対してサービス妨害が行われ、実質的なサービス不能に陥ったことがきっかけである。こうした大手 Web サービスは大量のユーザからの接続に対応するために非常に高い処理能力を備えており、簡単にサービス不能になることはないと考えられていたが、インターネット上の多くのコンピュータから一斉に攻撃対象に大量のデータを送る「分散型サービス妨害(Distributed Denial of Service、DDoS)」という手法が攻撃に使われるようになったことで、実際に被害が生じるに至ったのである。これ以降、第 3 章で述べるように金銭目的や組織に対する抗議・嫌がらせ、社会的・政治的意図等を動機としてさまざまなサービス妨害攻撃が発生し、今ではインターネットを用いた各種サービスの安定的な提供に対する主要な脅威の 1 つとなっている。

それでも、これまでインターネットを事業実施の主たる手段(媒体)として用いる場合を除けば、一般の企業等にとってはサービス妨害攻撃を意識する必要性は必ずしも大きくなかった。これは、攻撃者が実施するのはあくまでも妨害であり、破壊などの致命的な活動が行われるわけではないこと、攻撃を受けた場合でもインターネットとの接続を遮断することで、企業内部の業務継続が可能であったことなどが原因である。こうした状況は、一般の企業でもインターネットへの依存度が高まることで変化が生じつつある。インターネット上でひとたび大規模なサービス妨害攻撃が発生すれば、企業における事業継続に重大な影響を及ぼしかねない。

また、特に企業に対するサービス妨害攻撃では、これを材料とした恐喝や詐欺的行為が併せて行なわれることも多い。すなわちサービス妨害攻撃の実行をちらつかせて、あるいは実行して、やめて欲しければと金銭を要求する、あるいは攻撃の当事者自身が善意を装って、攻撃を止めるための支援を行うとして対価を要求するなどの行為である。

なお、近年注目されているクラウドコンピューティング(以下、「クラウド」という。)は、インターネット上のいずれかにあるコンピュータ資源(サーバ等)を用いて、これまで自前のサーバ等で行っていた処理やサービスを効率的に行おうとするものである。中小企業の立場からすると、これまではコストの点で利用できなかった大容量の回線や高速のサーバを低価格で利用出来ることになることで、サービス妨害攻撃の耐性が向上し、影響を受けにくくなる効果が期待出来る。その一方で、クラウドを使うことで多くの場合、インターネ

ットを情報が流通する機会が増える[3]。その結果、サービス妨害等の影響をはじめとするネットワーク上の障害が起きると、クラウドのようにインターネット上の外部との接続で成り立っているシステムは、その接続が切断されることで、業務やサービスに重大な影響が生じる可能性も生まれる。このように、クラウドの利用が進むことで、企業等においてサービス妨害攻撃に対して、有利な面・不利な面を含め考えておくべき事項が増えることに留意する必要がある。

### 1.2 サービス妨害攻撃の定義

本報告書の以降の各章での議論に先立ち、サービス妨害攻撃とはどのようなものかについて、その定義を明確にしておく。

#### (1) サービス妨害攻撃とは

「サービス妨害」とは、インターネット上で Web サービスやメールサービス等を提供しているサーバ等に対して過剰な負荷を与えたり、サーバ等の脆弱性を悪用することによって、サービスの運用や提供を妨げる行為をいい、このような行為を悪意を持って行い、標的としたサーバを攻撃することを「サービス妨害攻撃」という。

サービス妨害攻撃は、通常はサービス妨害の英語の略称である「DoS:Denial of Service」を使って「DoS 攻撃」と呼ばれることが多い。本書では次章以降、本文中において、サービス妨害(Denial of Service)を「DoS」、サービス妨害攻撃(Denial of Service Attack)を「DoS 攻撃」として表記する。

さらに DoS 攻撃のうち、ネットワーク上の関係のない複数のコンピュータに攻撃プログラムを仕込んでおき、それらの分散している複数のコンピュータから一斉に特定のサーバを標的とした攻撃を「分散型サービス妨害攻撃」といい、これは分散型の英語の略称を使い「DDoS 攻撃(Distributed Denial of Service Attack)」と呼ばれる攻撃がある。本書では次章以降、本文中において、分散型サービス妨害攻撃(Distributed Denial of Service Attack)を「DDoS 攻撃」として表記する。

#### (2) サービス妨害攻撃の分類

サービス妨害攻撃の手法は、主に以下の 2 種類に分類される。

##### a. 脆弱性に根ざしたサービス妨害攻撃

攻撃を受ける Web サイトのコンピュータ、又はそれをインターネットにつなぐネットワークに技術的な弱点(脆弱性)が内在し、それを悪用してサービス妨害攻撃を行うものであり、本報告書ではそれを仮に「脆弱性に根ざした DoS 攻撃」と呼ぶ。

[3] 一部のプライベートクラウドの場合は、インターネット等の外部に接続された通信回線を介さないで接続されることもあり、この記述の対象外となる。

Web サイトに「脆弱性」があることは、必ずしも Web サイトを運営する側の責任だけではないが、その脆弱性が悪用されて攻撃されるということであれば、Web サイトを運用しているシステムの脆弱性を解消する必要がある。ソフトウェア等の脆弱性はソフトウェアメーカが公表していることが多いので、脆弱性を解消していないと攻撃の対象になりやすくなる。しかし、脆弱性の存在が、いかなる意味でも、攻撃という行為を正当化することはならない。何をもって脆弱性があるかという基準は、インターネットをめぐる技術水準の変化(向上)によって変わるものでもある。ただし、こうしたサービス妨害攻撃については、攻撃を受ける側には、それを防御し、あるいは被害を低減するための方策が、その時点において現実的に存在することが多い。「脆弱性に根ざした DoS 攻撃」の対策については、第 4 章で詳しく述べる。

**b. 真正のサービス妨害攻撃**

インターネットは、ひとつの基盤の上に様々な主体が利用する環境であり、利用者全員がそのメリットを享受するために、緩やかな合意のもとで運営されている。したがってその利用者には一定の節度が求められるのであり、ましてやサービス妨害攻撃などはもちろん許されない行為であるが、その中にあっても特に悪質な攻撃がある。そうしたものの典型的な姿としては、例えばあるサイトにつながるインターネット上の経路のどこかで大量の通信を起こして、意図的に経路をふさいでしまうような攻撃である。それは現在のインターネットを支える技術標準(緩やかな合意)とそれに基づくインフラには、防御するための確実な方策のない攻撃であり、本報告書ではそれを仮に「真正の DoS 攻撃」と呼ぶ。そのように他者を攻撃し、しかもそれを確実に阻止する手立てがないとすれば、それはまさにインターネット上のテロ攻撃と言えるものであり、一人の利用者の被害ということだけでなく、インターネット利用者全員にとっても脅威となる問題である。真正の DoS 攻撃の対策についても、第 4 章で詳しく述べる。

## 1.3 サービス妨害とサービス妨害攻撃

DoS 攻撃は、インターネットで一般的に使われているプロトコルの仕組みを悪用することが多いため、悪用目的でなくてもインターネットを普通に利用していた場合でも、利用者の誤操作や設定ミスなどによりサービスの妨害が発生することがある。このような攻撃の意図がない場合は攻撃ではないため、単に「サービス妨害」と言える。サービス妨害に関しては、平常時からサービスを提供しているサーバや通信回線の状況を確認しておき、妨害が発生した場合の異常を即時に感知できるようにしておくことが望ましい。そのためには、以下の表のようなチェックシートを予め作成しておき、処理能力の上限値を超えるなどした場合に、攻撃の意図を持たない「サービス妨害」が発生していると考えられる。

さらに、一定以上の処理能力を確保していれば、大半の攻撃による影響を運用上問題ない範囲に抑えることも可能となる。

表 1.1　チェックシートの例

| 項目 | 仕様 | 条件 |
|---|---|---|
| 単位時間あたりトランザクション数 | ○○以上 | 1 秒間あたり |
| 1 トランザクションあたりの応答時間 | ○○ミリ秒以内 | 同時トランザクション数が○○以上の状態が 60 分以上持続する場合において |
| データベースのセッション数 | ○○以上 | 1 秒間あたり |
| データベースのセッションあたりの応答時間 | ○○秒以内 | 同時セッション数が○○以上の状態が 60 分以上持続する場合において、以下のコマンドを実行する場合：△△△ |
| サービスのトップページの表示時間 | ○秒以内 | http リクエスト送出からページ表示完了までの平均所要時間 |
| 通信速度(帯域保証) | ○Mbps 以上 | インターネットからサーバまでの経路を通じてこれを下回る区間がないこと |

しかしながら、サービス妨害が故意か過失かを区別することは非常に困難であるため、利用者が事象のみをもって判断した場合、結果として攻撃意図を持たない「サービス妨害」か「サービス妨害攻撃」かを判別することが難しい。

そこで、完全ではないが、サービス妨害が故意か過失か区別するには以下の図に示すような方法が有効である。上記で示したとおり、表 1.1 のチェックシートの処理能力を超過する場合、該当システムにおける「サービス妨害」が発生した可能性を考え、次の図にあるような手順・対応を取る事で被害を軽減することができる場合がある。妨害発生時にはまず、自社側の問題ではないかどうかを確認し、次に発信者の誤設定・誤操作等ではないかどうかを確認することが大切である。また、これらのことが判断できない場合や、実際に攻撃されていることが予想される場合には、独立行政法人情報処理推進機構(以下「IPA」という。)や一般社団法人 JPCERT コーディネーションセンター(以下「JPCERT/CC」という。)へ相談することが望ましいといえる。このように、必要な範囲を超えるアクセス等による被害に、攻撃意図が加わることで「サービス妨害攻撃」の可能性を考慮することが重要である。

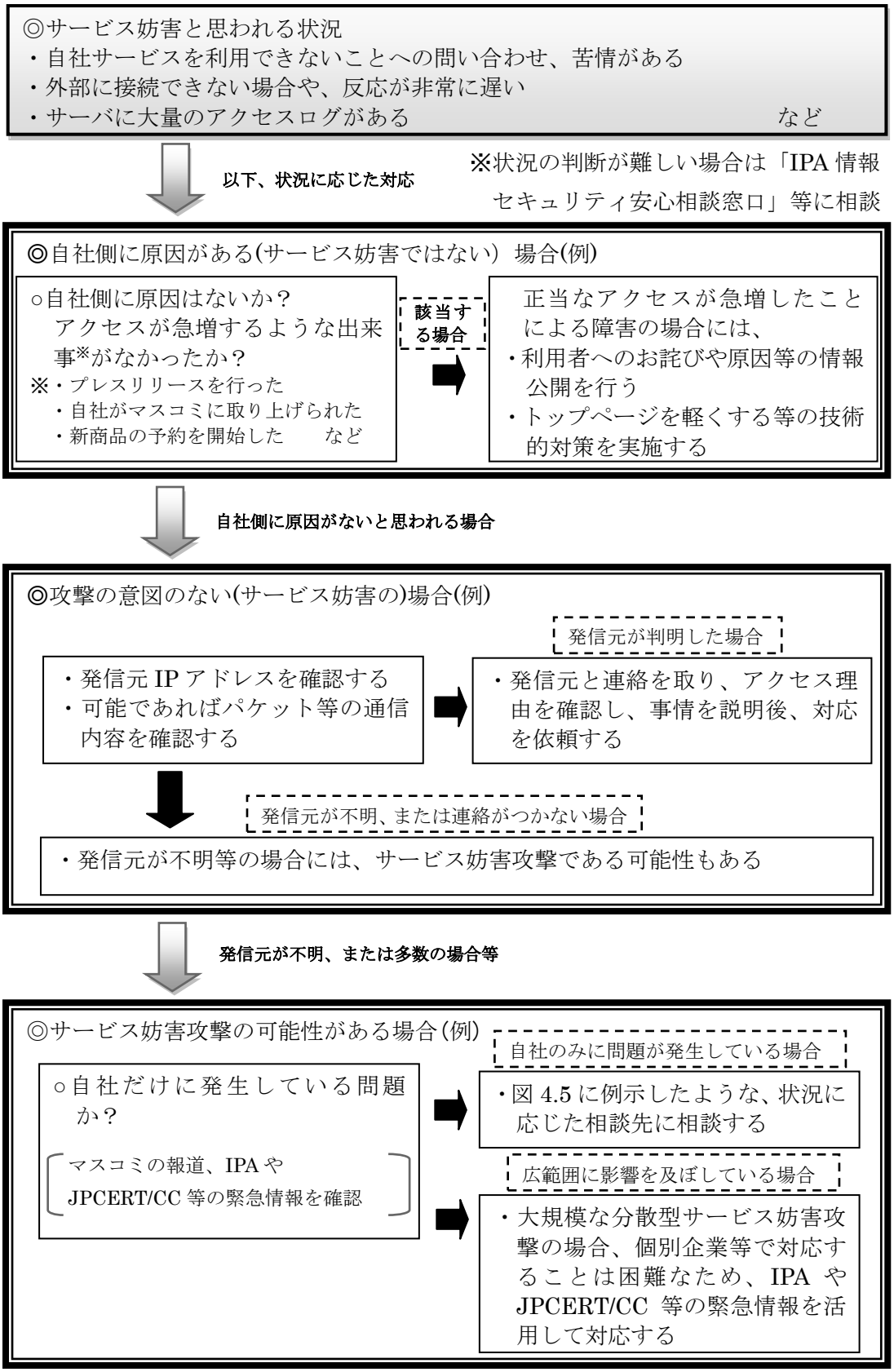


**図 1.1　サービス妨害攻撃判断チャート(例)**

# 第2章 企業や組織に対するサービス妨害攻撃

本章では、DoS 攻撃が企業や組織にどのような影響をもたらすのか、その被害に関する事項を中心に説明する。

## 2.1 企業へのサービス妨害の事例

はじめに、読者が DoS 攻撃の脅威を身近に感じることが出来るような、企業・組織等への攻撃の事例を示す。こうした被害の実態を知っておくことは、DoS 攻撃に対する対策の最初のステップとして有効である。

第 1 章では DoS 攻撃の概要について触れ、現実に存在する事象の一端を示したが、これは遠く海外の企業や政府機関、あるいは大手企業に限って直面する問題ではない。後述の「3.1 攻撃を請け負うビジネスの存在」で攻撃者のビジネスモデル及び「3.2 攻撃の背後にある動機」で攻撃の動機について分析しているが、これらの点を踏まえると、たとえ中小企業や規模の小さな公的機関であっても、攻撃の対象となり得る。

本章では、以上のことを具体的に示すため、企業や公益法人に対して行われた DoS 攻撃の事例を取り上げる。一般に、DoS 攻撃の被害を受けた企業や組織が、その事実を明らかにすることは少なく、その実情については不明な場合が多い。したがって取り上げる事例としてはそうした数少ない事例に拠らざるを得ないが、企業・組織の直面する被害をなるべく多方面から概観出来るように事例を抽出した。

2.1.1 節では、インターネットに事業基盤を 100%依存しているという意味で、攻撃があった場合の事業への影響が大きいと見られるオンラインゲームの業界に着目し、業界団体及び被害経験企業の事例を取り上げる。また、2.1.2 節では、2.1.1 節にあるような、DoS 攻撃とこれを悪用した恐喝行為・詐欺的行為がどの程度一般的な事象であるかについて、セキュリティ対策ベンダに取材した結果を示す。2.1.3 節では、やはり詳細が明らかにされている、中小規模の公益法人の直面した事例を示す。2.1.4 節では、海外に目を転じて、民間企業の Web サービスが受けた有名な DoS 攻撃や、攻撃を悪用した恐喝事件について取り上げる。2.1.5 節では、1.3 節で示した、DoS と DoS 攻撃の違いに基づくトラブルの事例について取り上げる。2.1.6 節では、DoS ではないが、DoS 攻撃と同様の影響があった典型的な事例を示す。

### 2.1.1 オンラインゲームサービス企業等への攻撃事例

オンラインゲーム[4]の事業は、その基盤を完全にインターネットに依存していることから、DoS 攻撃があった場合の影響が大きいことが推察されるため、その状況を説明する。

**＜調査事例①＞ （一般社団法人オンラインゲーム協会）**

はじめに、オンラインゲームサービスの国内における代表的な事業者団体である一般社団法人日本オンラインゲーム協会(JOGA：Japan Online Game Association)(以下、「オンラインゲーム協会」という)に対するインタビュー調査結果から、一般的なオンラインゲームサービス企業における DoS 攻撃を巡る事情を取り挙げる。

インタビューテーマ：

オンラインゲームサービス企業における DoS 攻撃の被害状況

インタビュー先概要：

オンラインゲーム協会は、国内でオンラインゲームをサービスする会員企業 21 社及び関連する事業を行う準会員企業 17 社を擁している(2010 年 09 月 06 日現在)。この会員企業は、国内のオンラインゲームの市場規模約 1,300 億円(2009 年)のうち 60～65%を占め、また、オンラインゲームユーザアカウント数では、国内総数約 8,500 万のうち 6,000～6,500 万アカウントを有する。

インタビュー結果：

オンラインゲーム協会に対するインタビューでは、主に以下の内容を聴取した。

| インタビュー内容 |
| --- |
| ・会員企業に対する DoS 攻撃による被害事例の報告は極めて少なく、本報告書執筆時点での実際的な脅威は限定的であると見られる。<br><br>・このことについては、以下の理由が大きいと見られる。<br>(1)会員企業はかねてから、海外の IP アドレスからのアクセスは遮断する方針を採っていること<br>(2)会員企業各社ともセキュリティ対策の実施レベルが極めて高いこと<br><br>・ただし、会員企業ではない同様のサービスを提供する事業者については、セキュリティの対策レベルやポリシー(海外の IP アドレスを遮断するなど)は |

[4] ここで「オンラインゲーム」とは、通信インフラを介し、PC や家庭用 TV ゲーム機等で複数のプレイヤーが同時にプレイするゲームを指す。オンラインゲームのサービスを提供する企業は、ゲーム運営サービスやクライアントソフト販売等により収益を得る。

様々である。オンラインゲーム協会としては状況については不明である。また、いわゆるコンソールゲーム[5]は、セキュリティ対策を含めてメーカがインフラを提供することが基本であり、その点でセキュリティ上の問題はある程度メーカが対応していることが推察される。

・現在、会員企業が直面する情報セキュリティ上の課題は、(DoS 攻撃ではなく)ゲーム運営サーバに対する「不正アクセス」や、不正に入手したアカウント ID による「なりすまし」とのことである。

・オンラインゲーム協会としては、DoS 攻撃は国内に設けたサーバを経由した海外からの働きかけが大部分とみており、そうした国内のサーバだけでは DDoS 攻撃を形成するだけの基盤にならないのだろうとみている。

・オンラインゲーム協会としては、実際のユーザの代わりにパソコン上でユーザの操作を模擬し、ゲーム上のポイントを稼ぐ、いわゆるボットの存在について頭を悩ませている。ボットは、一般に各社のゲームサービスの約款には抵触するが、違法行為であると判断するには疑義がある。ただし、もし多くのユーザが同時にボットを起動したら、サービス妨害に近い影響がゲーム運営サーバに出るのでは、と懸念されている。

インタビュー結果を受けての総括：

オンラインゲーム協会の会員企業に限った事情として、各社は本報告書執筆時点では DoS 攻撃についての脅威を免れている。その理由としては、協会をはじめ各社の情報セキュリティ対策への取り組みが奏功していること、また、海外からの IP アドレスを遮断していることが挙げられる。

**＜調査事例②＞ （オンラインゲームサービス企業）**

株式会社 A(以下、「A 社」という。)は、インターネット上で有料のゲームサービスを提供している。同社は 2009 年 8 月に DDoS 攻撃を受け、一時サービス停止に追い込まれた。また、この事象と並行して金銭を要求する脅迫を受けた。A 社はその事実については一定の情報開示を行なっており、それに基づいて文献から事態の経緯を取得し、同社へのインタビューから、経験を踏まえた DoS 攻撃への対応の考え方を聴取した。

[5] ここで「コンソールゲーム」とは、家庭用ゲーム専用機を指す。

インタビューテーマ：

実際の DoS 攻撃に関する状況と、この経験を踏まえた対策に関する考え方

サービス妨害攻撃の経緯：

事態の経緯については、ニュース(参考文献[1])などで比較的詳細に報じられている。これらの資料と A 社へのインタビュー調査を基に、以下に事態の経緯を整理する。

(経緯)

・2009 年 8 月 3 日、午後 3 時 38 分に脅迫メールが届く。内容は「今から DDoS 攻撃を開始する。被害を受けたくなければ、100 万円を支払え」。

・同午後 9 時 14 分、支払いを促す第 2 のメールが届く。同時に運営サポートから、サーバが高負荷状態でダウンしているという報告が入る。

・支払いを拒否する旨を回答した。

・それ以降本格的な DDoS 攻撃が始まり、サービスが提供出来ない状態となる。

・攻撃は同社の代表的なサービスであるマージャンゲームだけでなく、それをホスティングする上位のルータにまで及び、他社のサービスまで被害に巻きこまれた。

・攻撃側は一度に全力で攻撃をしかけずに、段階的にこれを強化していった。はじめに 1 台のサーバに攻撃し、これに対策を施すとその他のサーバに攻撃を移す。Apache サーバの脆弱性に対して対策を施すと、 TCP の脆弱性を突く攻撃に切り替える。攻撃元の IP アドレスに対して遮断措置を施すと、次々に別の IP アドレスから攻撃してくる、など。

・対処にあたって外部のセキュリティ対策事業者と連携を取った。

・併せて警察に届け出た(警視庁及び所轄署)。

・対策の結果、約 1 週間後、サービス再開に至った。

・その後も小規模な DDoS 攻撃が断続的に続いている。

インタビュー結果：

A 社に対するインタビューでは、主に以下の内容を聴取した。

| インタビュー内容 |
| --- |
| (脅迫に対する対応の仕方について)<br>・攻撃者からの連絡に対して「金銭の支払いの拒否」と応じたが、こちらからの不必要な意思表示は一切すべきではなかったと考えている。<br>・事態に直面したときは、突然のことで混乱し「支払いません」と回答したが、後にこの対応は失敗であり、「無視するのが正解」だったと分析している。すなわち、かえって先方に目をつけられるきっかけになったと推察している。 |

(外部の専門家の活用について)

・適切な外部の専門家にすぐ相談すること。そのために普段からそうした相談先の目処をつけておくことが大切である。また、事態の把握のために、通常時からアクセスログ、サーバ負荷のログなどを完備しておくことは当然である。

・当社の場合事業の性質からして、社内にネットワークやコンピュータシステムの専門スタッフは多いが、進行中のセキュリティ被害への対処については、やはり専門家に多くを委ねるべきである。

・なお、もとよりアクセスログ、サーバログ等を収集する設備は完備していた。

(攻撃を受けた時の対処について)

・当社の経験から学んだことは、なによりもまず、進行中の事態への対処(被害の緩和やサービスの復旧)を最優先にすべきことである。

・攻撃者の取り締まり等のためには、警察への届出を行うことも重要であり、攻撃に関する被害届を提出した。ただし、今回のケースでは届出による具体的な効果は得られなかった。

(進行中の事態についての外部への説明)

・顧客と取引先に対して、逐次、十分な情報開示と説明を行うこと。このことが最も大切なことと考えている。

・この情報開示を受けてユーザから大量の応援メールが届くなど、事態を通じてユーザとの信頼関係が深まったと感じている。また、これは望外のことであるが、ユーザ行動(どのように遊ばれているかなど)についての知見を得ることも出来た。

インタビュー及び文献による調査結果総括：

攻撃の手法面では、「Connection Flood」「TCP SYN Flood」「UDP Flood」(いずれも 3.4 節を参照)が次々と試されたり、攻撃対象のサーバを変えてくるなど、さまざまな攻撃のアプローチが取られた。トラフィック量は秒間数万 PV(ページビュー)レベルから始まり、最終的に数十万 PV まで増加したとのことである。高度な技術的対策が必要な場合、企業単独で事態に対処することは難しく、そのため同社では早い段階で信頼出来る外部のセキュリティ専門機関(4.5(2)節を参照)に協力を求めた。ただし、かねてからそうした機関と接触があったわけではなく、事態が発生してから急ぎ探し求めたとの事である。事態が起きた際、慌てることの無いよう、また、信頼出来る機関を時間をかけて選択出来るよう、普段からあらかじめそうした機関を探し、連絡を取っておくことが重要であると考えられる。また、この事例は、DoS 攻撃を脅迫に用いた恐喝行為の典型的な事例でもあるが、攻撃者からの接触に対してどのように応じるべきかについても検討材料を

与えている。すなわち、原則的には無視すること。ただし、そうしたエンジニアリング面以外の対処の仕方についても、経験のあるセキュリティ専門機関に確認してみるのもよい。また、警察への届出については、そこにすべての解決を期待しないほうが良い。警察の活動は技術的な対策実施に比べて即効性があるものではなく、ある程度の時間を要する場合があることに留意すべきである。

### 2.1.2 サービス妨害攻撃による恐喝・詐欺について

前記の調査事例②は、正に DoS 攻撃による恐喝の典型的な事例であるが、こうした事例を、どの程度一般的なものと捉えるべきかについて、セキュリティ対策ベンダ企業が公表した、DDoS 攻撃を悪用した恐喝行為に関する注意喚起(2008 年 5 月 15 日)等から明らかにする。

**＜調査事例③＞ （セキュリティ対策ベンダ企業)**

セキュリティ対策ベンダから、「【注意喚起】企業のホームページを狙った DDoS 攻撃を伴うネット恐喝行為について」(参考文献[2])が発表されている。

この中では、2008 年 4 月後半ごろから、DDoS 攻撃を通じた恐喝行為の相談が、企業から同社に相次いでいることが示されている。

恐喝行為の基本的なプロセスは、

- 突然に企業が運営する Web サーバが DDoS 攻撃を受け、Web ページの閲覧が困難になる事象が発生する。
- 次に、電子メールを通じた恐喝が行われ、攻撃を止める代わりに特定の口座への振込みが要求される。

とのことである。

また、インタビューによると、

> 「直接的に金銭を要求する恐喝行為もさることながら、攻撃者が自ら DoS 攻撃を仕掛けておきながら、セキュリティコンサルティング事業者などと名乗り、サービス妨害に対する“防御サービス”を行って、対価を要求する詐欺的な行為も頻発している。当社のセキュリティサービスに持ち込まれる事案をみると、そうしたことはまれな事象とは言えない。また、特にセキュリティにコストを掛ける企業体力が乏しく、知見も少ない企業が狙われやすい傾向にあるようだ。」

とのことである。

以上の結果から、DDoS 攻撃を悪用した恐喝行為あるいは詐欺的行為は実態として存在し、セキュリティに掛けるコストや、知見のある者が相対的に少ない中小企業や小規模な公的機関等がその対象とされる可能性が高いことが伺われる。

### 2.1.3 社団法人コンピュータソフトウェア著作権協会(ACCS)への攻撃の事例

調査事例②と同様に、DoS 攻撃の内容が公表されており、さらに対策の一部始終も明らかな事例として、社団法人コンピュータソフトウェア著作権協会(以下、「ACCS」という。)の事例を見る。

**＜調査事例④＞ (ACCS)**

インタビューテーマ：

ACCS を見舞ったウイルスに起因する DDoS 攻撃について

インタビュー先概要：

ACCS は、デジタルコンテンツ全般について著作権者の権利を保護することを目的とした団体あり、事業者が著作権に関わる法的な事務手続きの支援なども行なっている。ACCS が直面し、現在も続いているサービス妨害攻撃の事例について、その経緯はネット上のさまざまなメディアで紹介されている(参考文献[3][4]など)。ここでは、その事例のポイントを文献調査や、ACCS 及び事態への対処に中心的な役割を果たしている財団法人日本データ通信協会 テレコム・アイザック推進会議(以下、「テレコム・アイザック」という。)に対するインタビューを基に整理する。

インタビュー結果：

ACCS に対するインタビューでは、主に以下の内容を聴取した。

| インタビュー内容(回答は ACCS 及びテレコム・アイザックによる) |
|---|
| (背景として考えられるもの)<br>・ACCS は、デジタルコンテンツ全般について著作権者の権利を保護するのがミッションであり、法的な手続きを取りたいと思った事業者の事務的な手続きの支援なども行なっている。<br>・したがって、デジタルコンテンツの著作権を巡る事案について初期段階から相談を受け付け、手がけることが比較的多い。(例えば、ファイル交換ソフトの刑事事件などがある。)<br>・こうしたことから、一部の、著作権を無視してコンテンツを手に入れようとする人々からは敵視されていることが推測出来る。<br><br>(過去の攻撃の事例)<br>・2004 年の本格的な大規模攻撃の 1－2 年前に、人的な F5 攻撃(「3.4(7)リロード攻撃」を参照)があった。「2 ちゃんねる」等の掲示板サイトで、「この協会は自分たちの活動を妨害することばかりしている。攻撃しよう。」といった趣旨の呼びかけがあったようだ。そこから人的な DDoS 攻撃をやろうという呼びかけに応じた人々がいた。 |

・この攻撃があったとき、一時的に Web サーバはサービスを停止したが、1～2 日で復旧した。この間のアクセスログを解析して得られた IP アドレスを基に、告知を行った。まず、IP アドレスを押さえていること。続いて、法的な対応も視野に入れていること等を示し、実施した者は話し合おうという内容を告知した。そうしたなかで謝罪してくるものもあり、事態は収束した。
・その後 2004 年に、問題の大規模 DDoS 攻撃が発生した。

(2004 年から始まった大規模攻撃の内容)
・ファイル交換ソフト Winny が媒介し感染拡大するワーム型ウイルスである「Antinny」の亜種が、特定の日付(毎月第一月曜日や、月と日が同じ日(4 月 4 日など))に定期的に ACCS のホームページに DoS 攻撃を仕掛けるもの。Antinny に感染した多数の PC から同時に攻撃されるため結果的に DDoS 攻撃となるが、Antinny は国内を中心に広範囲に拡散しているものと見られ、また、数パターンの亜種の存在が報告されている。
・亜種によって、様々な攻撃のパターンがあるが、以下の DoS 攻撃手口の組み合わせと見られる。
  ・SYN パケットばかり送ってくるもの（SYN Flood）
  ・TCP 接続だけをしているもの（Connection Flood）
  ・データを取得しようとするもの（HTTP GET Flood）
  ・データを投げ込んでくるもの（HTTP POST Flood）
  (いずれも 3.4 節を参照)

(この事例のポイント)
・対策のひとつとして、標的にされたサーバのホストネームを変更したが、攻撃者(ウイルス作成者)は、ホストネームの変更規則を見て先回りし、今後、変更しそうなホストネームも含めて攻撃してきた。すなわち明確な攻撃意図があり、ホストネーム変更を先回りしてまで攻撃してくるという事例である。
・仮に攻撃対象のサーバをインターネット上から排除しても、攻撃日には、攻撃先を探して DNS に対して名前の解決(URL に対応した IP アドレスを得ること)を要求する大量のトラフィックが発生するため、インターネット環境での混乱は残った。
・根本的な解決には、インターネット上からウイルスを排除するしかないが、これには相当な時間が必要とみられた。また、ウイルス対策ソフトを導入していない PC も存在した。このためにマイクロソフト社は、Windows Update にこのウイルスを排除する更新内容を盛り込むなどの協力を行なってくれた(参考文献[24][25])。また、大手のセキュリティ対策ソフトベンダの製品にも同様の機能が盛り込まれた。

・最初の対処として、インターネットサービスプロバイダ(Internet Service Provider)(以下「ISP」という。)の DNS から ACCS のサーバの名前を消す処置を取ったが、それでは別の DNS に名前解決のトラフィックが集中し、他の ISP など広範に過負荷を与えてしまうと判断された。
・このため、テレコム・アイザックの協力で、集中するアクセスを捨てるためのサーバと IP アドレス(Black hole IP アドレス)を設けて対処した(参考文献[22][23])。
・さらに、大手通信キャリアが DDoS 対策サービスのテストケースとしての対策の協力を申し出、現在までこれによって定期的な攻撃を緩和させている状況である。
・ただし現時点でも Antinny は存在し、攻撃を受け続けている。これは、Antinny での攻撃特徴である第一月曜日やゾロ目の日(4 月 4 日など)に攻撃を受けていることから確認出来る。
・かつて実験的に回線容量を増やし、サーバ設備に余裕を持たせて攻撃に応答しきったところ、ピーク時には応答の通信が 700Mbps にもなった。現在はこれが数十 Mbps になっているが、一度広がったワームを根絶することは難しく、今後も攻撃を受け続けると考えられる。

インタビュー及び文献による調査結果総括：

・通常の DDoS 攻撃は、何者かのコントロールの下に攻撃が実施されるものが多いが、この事例では、攻撃の実施主体はウイルスであり、一旦拡散してしまったウイルスは誰からのコントロールも無く、指定されたタイミングで指定された先に対して攻撃を実施している。
・ACCS は、公的な事業目的を持つ団体であり、組織規模としては本報告書で想定している小規模な団体に該当する。ただし攻撃のメカニズムは上記したような極めて特殊な内容であるから、一般企業が直面する DDoS 攻撃と同列には語ることは出来ないが、インターネットコミュニティ全体が得た知見は大きい。すなわち、ウイルス起源の DDoS 攻撃は、誰も制御をしていないことからその活動を止める手立ては無く、一部の多大な負荷は、他に影響し、その結果としてインターネットコミュニティ全体に対して大きな負荷を負わせる可能性もある。一方で、技術的には DDoS 攻撃に効果的に対処する手法が確認された。ただしそのコストは大きい。
・この事例で取られている対処では、テレコム・アイザック、通信キャリア、ISP、ホスティング事業者などが事態の緩和に多くの協力を行なっている。ただし、これには各事業者とも、DDoS 攻撃対策の実験として、通常の企業の対策では考えられないほどのコストを投入しているのが実態である。

### 2.1.4 海外における民間 Web サービスへの恐喝の事例

これまで、比較的規模の小さな組織に対する攻撃の事例を見てきたが、次に調査事例⑤では、特に海外における DoS 攻撃を悪用した恐喝事例を取り上げる。海外は国内に比べてこうした先行事例もあることから、今後の国内の状況を推測する上でも有効と考えられる。

**＜調査事例⑤＞ （文献調査）**

本項では海外における民間大手Webサービスを対象に過去に行われた大規模なDoS攻撃の事例を紹介する。ここで紹介するような大規模な攻撃は世界的に知名度が高い企業であるからこそ生じるものであるが、電子商取引(EC)サイトが攻撃を受けたときの事業継続への影響と対策に関しては、規模の違いにかかわらず参考になるものと考えられる。

民間に対しての DoS 攻撃による被害が注目されるようになったきっかけは、2000 年 2 月に相次いで発生した、米国のインターネット関連企業への攻撃である。このときは、Yahoo, eBay, CNN, E*Trade, ZDNet 等が攻撃を受け、サービス不能に陥っている(参考文献[5])。

また、2004 年 7 月には英国のスポーツくじのサイトである Canbet Sports Bookmakers の事例では、実際に恐喝組織が摘発された。Canbet Sports Bookmakers では、自社サイトが攻撃されるのを防ぐための用心棒代の支払いを要求され、「用心棒代」の支払いに応じなければサイトに対して DoS 攻撃を仕掛ける組織が存在していたという。この組織に参加していたと思われる容疑者に対して、英国のコンピュータ犯罪を捜査する National Hi-Tech Crime Unit(NHTCU)は、ロシア内務省のコンピュータ犯罪専門部隊及び調査委員会と協力してこの捜査に当たった。英国の NHTCU とロシアの捜査官は従来の捜査手法とデジタルフォレンジックを駆使し、DoS 攻撃の発生源に関する情報と送金記録を使って犯人を追跡し、その身元を突き止めた。2003 年 11 月にはラトビアのリガで、恐喝組織のメンバー10 人が逮捕された。さらに、2004 年 7 月にロシア等で 3 人の男性が逮捕された(参考文献[6])。この事例のように、大規模な DoS 攻撃の攻撃者を摘発するには、国際間の協力体制が必要となることもある。

### 2.1.5 国内公共施設の事例

**＜調査事例⑥＞ （文献調査及びインタビュー調査）**

この事例は、あるソフトウェア開発者が、国内のある公共施設の Web サイトに対し、サービスを利用する目的で、自作のプログラムによって機械的に繰り返しアクセスしたところ、当該サイトで他の利用者が閲覧しにくくなる障害が発生した。このため、公共施設から DoS 攻撃と受け取られて、被害届を出されたが、取調べの結果、不起訴処分となったものである。事件の経緯は、新聞記事等で紹介されている(参考文献[7][8][9]）。

この事例は、アクセスを行なった当事者に当該公共施設の Web サイトのサービスを妨害しようという意図が存在しなかった(あるいは確認出来ない)ことから、1.2 節で示した DoS 攻撃の定義に準拠すれば、「DoS 攻撃」の事例とはいえない。また、アクセスの質的及び量的な面から考慮する[6]と、本事例を「DoS」とすることの妥当性にも疑問がある。

一方で、当該公共施設側は、「DoS 攻撃」により業務を妨害されたとの認識を持つという不整合が生じている。

この事例では、関係者(アクセスを行った当事者及びアクセスを受けた公共施設)の被った損失のほかに、インターネット技術や文化といった面からも影響が及ぶことが危惧されている。すなわち、こうした事例が今後も発生するようであれば、マッシュアップ[7]をはじめとした技術開発のモチベーションに深刻なダメージを与えるかもしれない、という観点である。

したがって、今後このような事態を避けるために、サイト運営者側(以下「サイト側」という。)としては以下ような対策を検討しておくことが重要である。

#### (1) 状況確認

サイトの管理者は、自社のサイトがどのような状態で、どのような事が発生したのか？ということを確認する必要がある。この確認によって、そのリクエストが攻撃意図のある DoS 攻撃であるか、攻撃意図のないリクエストであるかを判断出来る場合が多いと考えられる。

#### (2) 技術的対策

一般的に、同一の IP アドレスからのアクセスに対するアクセス間隔を考慮したフィルタリングや通信帯域の制限等がある。また、技術的な対策を行った結果、同一の IP アドレスからの大量のアクセス等を検知することが可能となるが、そのような大量のアクセスが、

---

[6] この事例では、サイトに対するアクセスを終えてから次のアクセスを開始するという方法で行われており、Connection Flood 攻撃(3.4 節参照)のような同時並行アクセスは行われていない。また、アクセスの頻度は毎秒 1、2 回程度であったとされている。

[7] ここで「マッシュアップ」とは、Web アプリケーション開発の分野で、Application Programming Interface(API)を通じ、複数の異なる Web アプリケーションやサービスを利用して新しいアプリケーションやサービスを形作ることを指す。

サイトの運営に障害をもたらす懸念がある場合には、サイト側は、当該アクセスを行った者に対し、アクセス方法の変更など障害の発生を回避するための措置を取るよう、適切に伝えることも重要であると考えられる。

**⑶ 外部機関等への相談**

⑴⑵を実施した上で、状況が改善されない場合は、相談窓口などへ相談することとなる。公的な相談窓口等については、4.3 節に連絡先を記している。

なお、一般的に DoS 攻撃と判断する経緯には、どの程度のアクセスリクエストを許容範囲とするかが重要になるが、サイト規模やネットワークやハードウェア構成処理能力によって一概には言えない。また、上記の⑴で状況を特定出来ない場合は、実害があることからサービス妨害ではあっても、攻撃意図を推定出来ず、DoS 攻撃とまでは言えないという状況もある。このような観点を踏まえると、どの程度のリクエストが許容範囲であるか明確でない以上、仮に法的な解決を図るにしても、刑事的な手続きより、民事で解決を図る方がより妥当な場合もある。どのように対応すべきか不明な場合には、IPA の相談窓口に相談することが推奨される。

### 2.1.6 サービス妨害攻撃と同様の影響を及ぼした事例

**＜調査事例⑦＞ （文献調査）**

ここで紹介する事例は、サービス妨害と同様の影響を生じるようなケースである。提供しているサービスに対して利用者が「同時に」かつ「大量」にアクセスし、サービスを使用することで、サービスの応答速度が低下したり、サーバが処理不能となって停止してしまうような状態を生じさせるものである。

**(1) 予約等の開始時刻を予め定めていたことによるもの**

人気の高い新製品やチケット(イベントや交通機関、宿泊施設等)の場合、その販売や予約の開始日時をあらかじめ告示し、定められた時刻から受付を開始することがよく行われる。このとき、この開始時刻に希望者のアクセスが殺到することで、サービス不能や応答速度の著しい低下を招く事例である。人気が予想される場合、サービス提供側でも処理能力を予め増強して対応するのが一般的であるが、通常のアクセスの約 100 倍以上の需要が殺到するケースも珍しくないことから、結果的に多くの利用者のアクセスへの対応が不可能となる。

**(2) テレビで紹介されたことによるもの**

オンラインのショッピングサイト等の場合、テレビ等のマスメディアで紹介されることで、需要に関する想定を著しく超えるような大量のアクセスが同時に発生すると、サービ

ス不能の状態に陥ることがある。

- 「【事例】アクセス集中でサーバが次々にダウン，サーバ増強や Akamai 導入で対処---ヘルシーネット「ケンコーコム」」(日経 BP・ITPro)
  http://itpro.nikkeibp.co.jp/members/SI/JIREI/20030729/1/

**(3) その他の事例**

ソフトウェアの脆弱性を修正するために定期的にパッチの提供を行うソフトウェアベンダのアップデートサイトにおいても、かつてはアクセスの殺到でサービス不能の状態に陥った事例がある。一般にソフトウェアベンダのアップデートサイトにおいては、大量のアクセスが生じることが前提であるため、予め需要を見越した提供体制を確保しているが、以下に示す 2004 年の事例では 1 時間あたり 300 万から 400 万件のアクセスが生じたことでベンダ側のサービス提供能力を超えた。この結果を踏まえ、ソフトウェアベンダ側ではアップデートサイトの設備を増強するとともに、アップデート用ソフトウェアにアクセス殺到時に 1 件あたりの通信負荷を下げるような機能を追加することで再発の防止を図っている。

- 「DoS 攻撃より手強い?--Windows Update サイトにアクセス殺到、一部で更新に支障」(CNET Japan)
  http://japan.cnet.com/news/sec/story/0,2000056024,20065486,00.htm

## 2.2 サービス妨害攻撃で企業等が受ける被害

以下では、2.1 節で見られたような DoS 攻撃が、具体的に企業に対してどのような被害をもたらすかを検討する。

### 2.2.1 サービス妨害攻撃による主な被害事例

DoS 攻撃による被害の内容を検討するにあたり、関連する既存の研究成果として、IPA による 2006 年度「企業における情報セキュリティ事象被害額調査」報告書(参考文献[30])の事象の分類等を参考とした。

報告書では、最終的には企業のコンピュータ環境がコンピュータウイルス(以下、単にウイルスという)に感染した場合の被害額を算出することを目的として検討しているが、その前段として、算出の可否とは別に、企業のウイルス感染がその企業にもたらす被害事象(被害の内容)について例示している。そこでは被害事象をウイルスの感染が直接的に引き起こす一次的被害と、その波及効果として間接的に発生する二次的被害に分類し、また、これらの被害事象を金額換算する場合、例えば、ウイルス感染により発生した支出と、本来得られるはずであったが感染により得られなった売上(機会損失による逸失売上)の2つに整理する方向が考えられるとしている。

今回、本報告書においてもウイルス感染の考え方を基に、企業等の DoS 攻撃による主な被害事例についてまとめてみると、以下の表のように整理することができる。

**表 2.1　企業の主な被害事象の例示(参考文献[30] より)**

| 被害額の性質 | 被害の内容 | |
|---|---|---|
| | 一次的被害(直接的) | 二次的被害(間接的) |
| 攻撃により発生する支出 | ・システム復旧に要するコスト | ・システム復旧以外の対応コスト<br>・取引先への補償等 |
| 攻撃により得られなかった収入 | ・Web サービスや Web サービスの広告等の収入 | ・風評被害 |

次項に各被害の内容について、具体的に説明する。

### 2.2.2 サービス妨害攻撃によって発生する被害の内容

被害の内容については、現実の DoS 攻撃で発生するあらゆる被害を完全に網羅しているとは言えないが、通常想定される被害の範囲は、ほぼカバーされている。

#### (1) 一次的被害

直接的な被害とは、事象が起きたことによって、金銭的に算出出来る被害と見ることができ、この中には主に以下の内容がある。

①逸失売上

提供サービスに対する攻撃影響期間に期待出来た(失われた)売上分は、そのまま損失とみなすべきである。もちろんサービスが完全に停止したか、あるいはユーザビリティが低下したのかなどによる程度の差異はある。また、企業によっては、売上の実現を完全にインターネットに依存している企業、事業紹介や商品説明など広報の媒体としての利用のみの企業など様々である。なお、一部インターネットに依存しているが、代替の売上手段を持ち、インターネット上のサービスが停止しても、計上すべき被害がないという場合もある。

②システム復旧に要するコスト

攻撃を受けた後、純粋にシステムの機能を復旧させるためのコストである。この中には復旧に当たった社員の人件費、復旧のために必要なシステムベンダ、セキュリティ対策ベンダへの外注費などがある。

#### (2) 二次的被害

二次的被害とは、事象の直後には確定しないが、時間を経た後に被害額が算定出来るもの、あるいはあくまでも被害額の算定は難しいが、実態としては確実に存在する波及的な影響を含むものとする。このなかには以下のものがあると見られる。

①対策コスト

サービス停止あるいはユーザビリティの低下に対して、顧客や取引先に事情を説明し、謝罪するための要員の人件費コスト、あるいは事態を広く告知するための広告費用などがある。

また、攻撃を経験したことにより、今後想定される被害をあらかじめ予防することや、被害を緩和するための設備の増強することなどを含める。このコストはあくまで当事者である企業の判断しだいで規模が決まるが、対策コスト自体は、攻撃を受けることで必然的に求められ、コストが発生するものでもある。

②取引先への補償等

サービス停止等によって、もし顧客や取引先に具体的な損失を与えてしまった場合、その損失を補填あるいは補償するか、あるいはそのことについての法廷費用などが発生する可能性もある。

③風評被害等

サービス停止の事実が明らかになったことによる、サービス品質に関する風評、それによる売上減、顧客減、取引先からの信用の失墜、さらには株価の低下によるブランド価値の低下などが考えられる。この内容は、被害規模の明確化は容易ではないが、直接的な被害を含むため、どの被害・影響よりも深刻な場合があり得る。

## 2.3 大規模なサービス妨害攻撃の事例と企業活動への影響

本節では、前節で示したような身近なものではないが、DoS 攻撃がどのようなものかを理解するために役立つと思われる事例として、国レベルで発生した大規模な DoS 攻撃の概要と、それが企業活動にどのような影響を及ぼしたのかについて紹介する。重要インフラとしての情報通信ネットワークが攻撃された場合、被害は広範に及ぶ可能性がある。

### 2.3.1 エストニアへの攻撃の事例

**＜調査事例⑧＞ （文献調査）**

2007 年 4 月から 5 月にかけて､エストニアで集中的に被害が生じた DoS 攻撃の事例について、以下にその概要を示す。

#### (1) 特徴

エストニアはロシアに隣接し、バルト海を挟んでフィンランドと相対する人口 134 万人の国家である。2007 年 4 月末、銅像の移設に反発したロシア系住民による暴動事件が発生し、これと同時に同国内を幅広く対象とする DoS 攻撃が発生した。この事例は、以下の各点が特徴的である。

**a. IT 先進国を対象とした攻撃**

エストニアは 1991 年の独立以降、官民で積極的に情報化に取り組んだことにより、事例の発生時点において、電子商取引の利用や行政の電子化に関しては欧州でもトップクラスの進展を示していた。例えばエストニア・インフォマティクス・センターによれば(参考文献[31][32])、国民の 75%がインターネットを利用しており、コンピュータの銀行取引の 98%、納税事務の 91%がインターネット経由で電子的に行われているほか、エストニア国内のインターネット銀行の口座数は 150 万以上に及ぶ。さらに、国レベルでは世界初の電子投票が行われた国家である。こうした状況下で DoS 攻撃が実施されたことにより、エストニアの経済・社会に幅広い影響が及ぶこととなった。

**b. 複合的な分散型サービス妨害攻撃**

現時点においてもこの事例における攻撃主体については明らかになっていないが、攻撃が開始された時期にロシア語の掲示板で攻撃の呼びかけが行われたことが明らかになっている。攻撃には多数のボットネット(3.3(1) 参照)が用いられたほか、上述の掲示板での呼びかけに呼応した人々がそれぞれ DoS 攻撃を実施したことで、エストニアから見ると短期間に大規模かつ集中的な DDoS 攻撃を受けた状態となった。

**c. 国際連携による対策の実施**

対策実施に際しては、エストニア国防省を通じて、EU 及び NATO 各国に協力の要請

が行われた。米国やドイツ等でエストニア向けの通信の遮断等の対策が実施されている。

**(2) エストニア国内の企業への影響**

攻撃はエストニアのインターネットインフラ、政府機関、民間サービス、その他のランダムなターゲットの 4 種類に対して行われた。民間サービスに関しては、エストニアの主要銀行 2 行が攻撃を受け、攻撃の期間中に 1.5 時間から 2 時間の間で 2 回の停止が生じている。これは電子化の進展しているエストニアでは大きな影響を及ぼしたが、関係機関が重要性を認識し、早期の回復に努めた結果、この時間で抑えられたという側面もある。このほか、移動通信事業者、ホスティング事業者、ディレクトリサービス事業者等も攻撃の被害を受けている。

### 2.3.2 グルジアへの攻撃の事例

**＜調査事例⑨＞ （文献調査）**

2008年8月にグルジアで被害が生じたDoS攻撃の事例について、以下のその概要を示す。

**(1) 特徴**

グルジアは黒海に面し、ロシアとトルコと国境を接する人口 426 万人の国家である。2008年8月に南オセチア州を巡ってロシアとの間に軍事衝突を含む紛争(南オセチア紛争)が発生した。ここに示す DoS 攻撃の事例はこの紛争と同時期に発生したもので、以下の特徴を有する。

**a. 武力衝突と並行して実施された攻撃**

このときの南オセチア紛争では、グルジア、ロシアを中心とする正規軍の間での戦闘が行われ、軍関係者で双方合わせ数百人、民間でもそれ以上の数の死者が出ているとされる。そうした環境下で DoS 攻撃が行われたため、「サイバー戦争」的な受け止められ方よりも、グルジアの機能を麻痺させるための手段の 1 つとしての理解がなされている。ただし、ロシアの国としての DoS 攻撃への関与は確認されていない。

**b. 情報化が未発達の状況下での攻撃**

ロシアの周辺国という位置づけは同じでも、エストニアとは対照的に、関連各国と比較してグルジアの情報化の進展は遅れている。そのため、DoS 攻撃が行われたことによる社会・経済への影響は限定的なものにとどまっている。

**(2) グルジア国内の企業への影響**

本事例における DoS 攻撃は、政府機関(大統領官邸、議会、教育科学省等)、商業銀行、各種ニュースサイト等を対象に行われた。この結果、グルジア国立銀行は電子サービスの

停止を指示し、10 日後に再開された。上述の通り、グルジアにおける情報化は先述のエストニアに比較して進展していなかったことから、こうしたサービスの停止が経済活動に及ぼした影響は限定的であったと考えられている。

### 2.3.3 日本への攻撃の事例

我が国への攻撃を意図して実施された DoS 攻撃として、大規模なものとしては以下がある。

①中国における反日デモに呼応した、我が国政府機関等への DDoS 攻撃
(2005 年 2 月～9 月)
②日銀に対しての DDoS 攻撃
(2006 年 9 月及び 12 月)
③韓国等の一般利用者からの 2 ちゃんねるサイトへの F5 攻撃(3.4(7)を参照)
(2010 年 3 月)
④衆議院の議員アドレス宛に大量の迷惑メールが送付されたことによる、受信障害
(2010 年 4 月)

ここでは、国内の関係機関へ影響の大きさから①について、また、大きな話題となったことから③について取り上げ、こうした攻撃の概要とそれぞれが我が国の社会や企業活動にどのような影響を及ぼしたのかについて紹介する。

＜中国における反日デモに呼応した、我が国政府機関等への DDoS 攻撃＞
(2005 年 2 月～9 月)
(1)どのような攻撃が行われたのか
(社会背景)
2001 年以降、首相の靖国神社参拝などで中国との関係が悪化し、中国国内でも反日感情が高まっていた。また、2005 年 3 月に韓国で竹島問題を契機として盛り上がった反日運動の機運が飛び火したように、中国各地でも 3 月下旬ころから歴史教科書問題や日本の国連安保理常任理事国入り反対の署名活動が始まった。これらの反日運動はインターネットサイト携帯メールなどで中国各地に拡大し、4 月 2 日に日系スーパーに対する暴動が発生し、4 月 9 日には北京で日本に対する大規模なデモの一部が暴動化した。4 月 16 日には上海でも日本に対するデモの一部が暴動化した。

(大規模 DDoS 攻撃)
こうした世界的な事件と同時並行に、2005 年 2 月から、首相官邸はじめ政府機関、報道機関、金融機関等に対して、大規模な DDoS 攻撃が発生した。5 月くらいから抗

議運動が沈静化するに伴って、DDoS 攻撃もその勢いを落としたが、2005 年 9 月まで攻撃自体は断続的に継続した。

⑵国内の社会や企業活動への影響

我が国では、ISP 等関係機関の努力があって、国民生活に影響が及ぶことはほとんどなく、この DDoS 事件自体が一般にはあまり知られていない。

ただし、攻撃の規模はまれに見る大規模攻撃であり、関係機関の尽力で食い止められたとのことである。

この事件を契機として、大手 ISP では、このころ検討中であった DDoS 対策サービス(4.5(1)節を参照)の開発を本格化し、2005 年末にはサービスが始まった。

＜韓国等の一般利用者からの 2 ちゃんねるサイトへの F5 攻撃＞

(2010 年 3 月)

⑴どのような攻撃が行われたのか

2010 年 2 月ころから、日本の電子掲示板サイト 2 ちゃんねるにおける、バンクーバー五輪やロシアでの韓国人留学生襲撃事件についての書き込みに反発したサイトが韓国国内で開設された。このサイトには 10 万人規模の韓国ネットユーザが終結し、3 月 1 日に主として F5 攻撃(3.4(7)を参照)による手法で、2 ちゃんねるサーバに大規模攻撃を行なった。また、ネット犯罪者グループがボットネットを用いて攻撃を行っていたとの観測もある。

⑵国内の社会や企業活動への影響

2 ちゃんねるのサーバは、米国のホスティング企業 Pacific Internet Exchange 社(PIE 社)にあり、この攻撃で、2 ちゃんねるのサーバだけでなく同社が運営する米国政府関連機関のサーバもダウンする事態となった。PIE 社は 2 ちゃんねるのサーバをすべて停止させ、攻撃の発信源となった IP アドレスからの通信を遮断する措置をとったのち、サービスを復旧した。3 月 1 日は韓国の祝日であり、これ以降は大きな攻撃は収まった。

ただし、米国政府機関など複数のサイトに被害が発生したことから、FBI 等が捜査に乗り出し、把握されている被害額は約 250 万ドルに上るとされている。日本国内における影響は、2 ちゃんねるサイトが 1 日障害に見舞われたことだけだが、著名なサイトであることから、話題となったものである。

### 2.3.4 米韓への大規模分散型サービス妨害攻撃についての事例

この事例については、詳細な事情に詳しい有識者にインタビューを行なった。インタビューにおいて特にポイントとなる点は以下のとおりである。

・韓国や米国の政府系及び主要 Web サイト等に対する、主として韓国からの大規模な DDoS 攻撃が 2009 年 7 月 7 日に発生した。この事案の発生原因など他の事象との関連等、詳細は不明である。
・観測された内容から推定された規模としては、ボットが約 20 万 IP アドレス前後、ボットからの トラフィックは、1 台あたり平均 148Kbps 程度と考えられている。
・この韓国のサイバー事案については、攻撃を受けた米韓の公的機関・政府の規模の大きさや、米韓が共同捜査を行ったことで有名である。この韓国のサイバー事案の背景としては、韓国では無償版ウイルス対策ソフトが存在するものの一般的なウイルス対策ソフトの普及が、たとえば日本に比べ極めて低いこと(市場規模は日本の 1/20)。また、Web ハードサイト[8]によって数十 GB のディスク容量が無料提供され豊富にデータのやりとりが行われている点を悪用され、悪性コード流布による侵害などが急速に広まったことが要因のひとつであると言われている。
・また、本事案では、攻撃手段が巧妙化され、10 以上のマルウェアが関連して動作し、コマンドアンドコントロール(C&C)サーバへの接続なしに特定のファイルをベースに攻撃を行うこと、攻撃時間の情報を受け取るアップデート用のマルウェアが存在していることなどによって広く拡大したと考えられている。
・韓国政府では、この事案の対策として、警報段階の変更発令、米韓共同訓練への反映、サイバー保安官 3000 人の養成、サイバー攻撃対応訓練、鉄道やガス公社等の 20 以上の公共機関の DDoS 対策状況の点検などの政策が実行され、以降の政府方針、対応策に多大な影響を与えた。また、サイバー攻撃の影響を受ける中小企業を支援するために、DDoS 対策専用の避難所の運用を予定している(本報告書公表時点では、運用開始済み)。DDoS 対策専用の避難所とは、DDoS 対応時に防御システムが完備された仮想的な避難所にシステムやネットワークなどを移し、被害を最小限に抑えるサービスである。DDoS 攻撃防御システムに対する投資余力の少ない零細な中小企業に対して、これらをサービス提供する際に、韓国政府がサポートする。

---

[8] ここで「Web ハードサイト」とは、Web 上でストレージ・サービスを提供するサイトの中で特に、データをアップロードしたサービス利用者が、データをダウンロードする利用者にダウンロードに応じて課金すること(販売すること)を意図したサイトを指す。
ファイルの違法共有を助長するとして、特に韓国において社会問題となっている。

### 2.3.5 国レベルで攻撃を受けた場合についての留意点

以上に見てきたような大規模な DoS 攻撃が行われた場合、攻撃を受けた国にある企業や団体等にも影響が及ぶことがあり得る。

このような攻撃に対し、個別の企業や団体等で対策を行うことは困難であるが、インターネットに事業を依存している事業者は、自社にとっての影響や発生し得る被害をあらかじめ想定しておく必要がある。

個別の企業や団体等に対する影響としては、主に以下が考えられる。

・銀行、クレジットカード等の決済機能の障害

・Web やメール等の顧客や取引先との通信手段の停滞

## 2.4 サービス妨害攻撃の傾向

近年の DoS 攻撃を巡る一般的な傾向について、関係事業者・機関や有識者にインタビューした結果を基に、そのポイントを以下に紹介する。

(攻撃の規模について)

◎比較的大きな攻撃としては、数百 Mbps から 1Gbps といったところである。大規模攻撃としては、2005 年前後では 1Gbps 以下でも十分に目立つものであったが、現時点(2010 年)では、大規模攻撃といえば数 Gbps といった規模である(大手 ISP)。

(攻撃の生起する頻度について)

◎ある大手 ISP が提供する DDoS 対策サービス(DDoS 対策サービスについては、「4.5(1)ISP が提供する対策サービス」に概要を紹介している)では、明らかに DDoS 攻撃と判断出来る事象の発生頻度は、平均して一日 2～3 件は観測されている。

◎したがって、国内に限っても毎日 10 件以上の DDoS 攻撃が生起している模様である。

(攻撃の内容について)

◎実際に観測される DoS 攻撃は 95%以上が DDoS である。これは、スプーフされた(成りすまされた)ソースアドレスへの返信をダークネットで観測することでわかる。ひとつの攻撃元からの DoS は非常に少ない(大手通信キャリア)。

◎DoS 攻撃で最も多いのは、最初のコネクションのところを対象とする SYN　Flood 的なものと考えられている。ボットを用いた DoS 攻撃の 90%以上がそのカテゴリに属す可能性がある(大手通信キャリア)。

◎DDoS 攻撃全体のうち、サーバリソースに対する攻撃が 9 割程度、サーバリソースと回線容量の両方に対する攻撃が残り 1 割程度である。単純に回線を埋めようとする攻撃の頻度は少なく継続時間も短い傾向にある。これは攻撃する側にとっても回線がふさ

がってしまうなど、負荷が高いからではないか。またトラフィックが目立つので、早めに発見されて対策されるということもあるだろう(大手 ISP)。

(攻撃の継続時間について)

◎攻撃の継続時間は、全体の 9 割程度が 30 分未満である。この傾向については、ひとつの見方として DDoS 攻撃をビジネスとして請け負うサービスには、攻撃の能力を顧客に示すために、無料で短時間の DDoS 攻撃を試行してみせることが多いとされ(「3.1 攻撃を請け負うビジネスの存在」)、このことが現れていると推測出来る。ただし、本格的な攻撃や国レベルの攻撃では、数日間にわたり継続するものもある(大手 ISP、有識者)。

◎マルウェアから特定の IP アドレスに DoS 的な攻撃が行われる場合は、そのマルウェアが活動している限り攻撃が続くため、短期間で終了するとは限らない(公的団体)。

## 第3章 サービス妨害攻撃の構造

本章では、DoS 攻撃を行なう側の事情について基本的な事項を概観する。これらは、対策を取る側にとっても有益な知識であると思われる。

### 3.1 攻撃を請け負うビジネスの存在(アンダーグラウンド市場)

インターネット上のブラックマーケット(あるいはアンダーグラウンド市場とも呼ばれる)の存在は、セキュリティ関連企業の各種レポート等においてかねてから指摘されていた(参考文献[18][19][20])。ブラックマーケットでは、あらゆるサーバスペース上の犯罪を実行するに必要なあらゆる商品とサービスが取引されている。そうしたなかで特に DDoS 攻撃を請け負う市場も存在する。そうしたブラックマーケットは、主に東欧圏やロシアなどに存在するといわれているが、そうしたブラックマーケット上のプレイヤーが、ビジネスとして我が国の企業や公的機関に攻撃を仕掛けることはもちろんあり得る。国内でそうした事情に精通する有識者によると、そうしたサービスを購入するにあたって必要なものは、

・取引用のコミュニケーションチャネル
・英語ないしは主要マーケットの存在する地域の言語
・インターネット決済サービスのアカウント

だけであり、手順としては、

①サイバー攻撃サービス提供サイトへアクセスする。
・大手検索エンジンで キーワードで検索 等
・(キーワード) に関するトピックの部屋で質問をする 等
・特定のスパムメールから URL を見つける 等
②取引用コミュニケーションチャネルで取引条件等を交渉する。
③インターネット決済サービスで送金する。

とのことである。たとえば日本人が、日本国内の企業や組織を攻撃することを意図した場合でも、そうしたサービスを使わないとする理由はない。参考に、インターネット上に見られた DDoS 攻撃のサービスについての価格表に以下のものがある。

表 3.1　ブラックマーケットに実際に提示された、DDoS 攻撃の価格表(2009 年前半時点)

| DDoS 攻撃サービスの請負コスト | | |
|---|---|---|
| 費用(ドル) | 期間(時間) | 帯域幅(Mbps) |
| 20 | 2 | 45 |
| 30 | 6 | 45 |
| 50 | 12 | 45 |
| 70 | 24 | 45 |
| 75 | 24 | 100 |
| 250 | 24 | 1000 |
| 100 | 24 | 1000 |
| 600 | 168 | 4750 |
| 900 | 24 | 4750 |
| 5500 | 168 | 4750 |
| 1000 | 24 | 4750 |
| 6000 | 168 | 4750 |
| 400 | 5 | 5000 |

出典：インタビュー結果による。

帯域幅 4.75Gbps の DDoS 攻撃を 24 時間行うサービスの価格が 1000 ドルとは、攻撃を受ける側の被害を考えれば極めて低価格であるといえるが、実態については不明である。いずれにしても、攻撃を行うにあたってのハードルは、今や極めて低いといえる。

最近のブラックマーケットを巡る事情について、有識者にインタビューを行なった。ポイントは以下の通りである。

・最近のブラックマーケットでは、「無料お試し」が設定されている場合が多い。これは、DoS や DDoS 攻撃などを前払い制で依頼を受け、決済後に DoS を行わず、お金を騙し取るケースがあったらしい。また、実際に攻撃能力があることを示し、確実に攻撃先に対してダメージを与えることが可能であることを示すために、まさに「無料でのお試し」が設定されている。この「無料によるお試し」があることからもわかるとおり、ブラックマーケットでも競争が激しいことが伺える。
・さらに最近では、クラウド等を用いて DoS 攻撃をアシストするサービスが低価格になっている。
・そのため、感情に任せて、攻撃を依頼するなどの発作的(刹那的)な攻撃が発生する可能性もある。実際に、韓国のサイバーテロ請負業者が同国の警察によって初めて摘発された事例(2009 年 2 月)では、ライバル企業の営業妨害を目的として依頼を受けた韓国のサイバーテロ請負業者が、60 社のホームページを麻痺させていた。摘発した同国警察は、これまで特定サイトを攻撃し脅迫していたケースはあったが、サイバーテロを行う会社を設立したケースは初めてだとコメントした。この事例のような、営業妨害等のビジネスに直結した犯罪が発生する状況になるのではないかと見ている。

### 3.2 攻撃の背後にある動機

#### (1) 個人的なトラブル

インターネットの歴史的な経緯からみると、もともと DoS 攻撃とは、インターネットに参加する者同士の「いさかい」や「ケンカ」に端を発し、意見の異なる者のネット上の活動を邪魔したい、排除したいという個人的な動機に根ざすものからはじまったという見方が有力である。それが次第にエスカレートして今や個人的な動機から、「集団の意思としての攻撃」といった様相を見せている。

#### (2) 金銭目的の攻撃

非常に厳しい競争環境にある市場では、ある会社の売上が、例えば DoS 攻撃によって失われれば、その分だけ競争している他社の売上の増加につながる。したがってその会社のビジネスが、インターネットを基盤としたものであれば、その基盤を攻撃しようとする動機は十分に成立する。3.1 節で見たように、今やインターネット上で他者(他社)の活動を妨害したいという意思があれば、それを具体的に実行する手立ては多様にあり、そのとき技術面での知識の有無はそれほど大きな問題ではない。

あるいは市場の外にいる者からでも、「この会社は自社の売上を守るために、いくらのコストを支払う用意があるか」という見方が出来る。そうした見方に基づいて、攻撃を試行して見せて、本格的な攻撃を避けたければ一定の金銭を支払えとの恐喝行為が実際に存在する(2.1.2 節を参照)。企業からすれば、こうした働きかけに経験がなく、情報セキュリティの問題に知見が乏しく、また、実際に自社のビジネスが脅かされれば、脅迫に屈することはあり得る。また、要求される金額も、比較的小額に設定されることが多い。ただしもちろん、脅迫がそれだけで終わる保証はない。こうした目的で攻撃する側からすれば、攻撃対象はどこでもよい。インターネット上に Web サーバやメールサーバを構える企業に片端からこうした試みを行い、応諾であれ拒絶であれ、反応のあった企業に反応に応じたアプローチをすればよい。(2.1.1 節の事例に示すように、あえて拒絶の姿勢を見せることはかえって良くないという見方もある。それだけ脅威を真に受けているという事実を明らかにしてしまうためである。もちろん応諾してしまうのは一番不適切な対処である。)

#### (3) 組織に対する抗議・嫌がらせ

直接的に金銭は目的にしてはいないが、特定の企業・団体に対して、その活動が「気に入らない」などという動機から、攻撃が起こることも考えられる。こうした動機は攻撃者本人にしか確実なところは不明であるが、背景にある状況から、おそらくそうであろうとみなせるものである。2.1.3 節に示した事例はその典型例である。

### 3.3 攻撃が可能となる背景

インターネットで DoS 攻撃が可能となり、かつ、頻繁に実行されている背景について整理する。

#### (1) ボットネットの存在

インターネット上で DoS 攻撃(とくに DDoS 攻撃)が脅威と考えられる最大の要因が、ボットネットの存在である。ボットネットは、ボットと呼ばれる攻撃者に乗っ取られた多数のコンピュータで構成されるネットワークであり、攻撃者が所有しているリソースではない。攻撃者が DoS 攻撃の実行を指示すると、各ボットが同時に DoS 攻撃を行ったものが、攻撃対象においては DDoS 攻撃となって威力を発揮することになる。

ボットは、システムの脆弱性への対策を実施していなかったり、コンピュータウイルス対策を実施していなかったりするコンピュータ等であり、攻撃に悪用されない間は異常な挙動を示すこともなく、通常の用途で用いられている。そのためインターネット上に存在するボットを探索することは必ずしも容易ではない。一方で、ひとたび攻撃に使用してしまうとボットであることが発覚してしまうため、攻撃者は大規模な攻撃を実行可能なように大量のボットを温存させていると言われている。

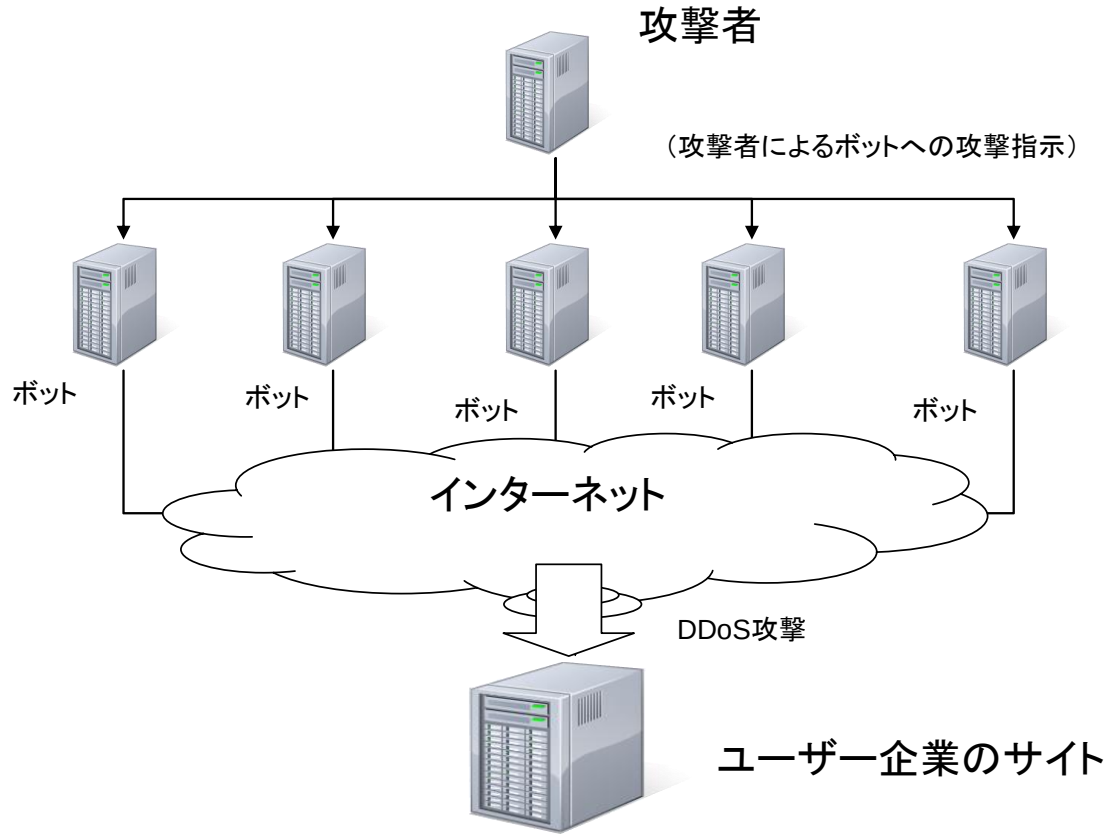


図 3.1　ボットネットによる DDoS 攻撃

**(2) 発信元の詐称が可能**

インターネットで用いられている TCP/IP プロトコルにおいて、通信される内容は「パケット」と呼ばれる情報の固まりの単位で送信される。このパケットには発信元のアドレスと送信先のアドレスを記録する領域があるが、このうち発信元については本来の発信元と異なるアドレスを記入しても、パケットとして異常とみなされることはない。パケットを中継するネットワークによっては不自然なパケットとして削除する場合もあるが、インターネットの中ではごく限定的な取り扱いである。こうした発信元を詐称したパケットを用いて DoS 攻撃が実施されることで、攻撃元の特定が難しくなっている。

**(3) 攻撃に専門的な知識が不要**

ボットとして感染させるためのコンピュータウイルスや、ボットネットを用いて DDoS 攻撃を行うツールなどはインターネット上で自由に入手することが出来る。これらを使って DoS 攻撃を行うのに情報システムやネットワークに関する専門的な知識は必要ない。

### 3.4 攻撃に用いられる手法

DoS 攻撃に用いられる手法は、(ネットワーク回線の)帯域幅･リソース消費攻撃とシステム資源消費攻撃に大別出来る。帯域幅･リソース消費攻撃(又は包括的 DoS 攻撃)とは、ネットワークの負荷を増大させて、通信を妨げる攻撃であり、また、システム資源消費攻撃とは、CPU やディスクといったリソースを枯渇化させる攻撃である。各攻撃型については、その手法及び用いるプロトコルによって個々に攻撃が分類される。DoS 攻撃の詳細な分類については下表に示す(参考文献[11])。

なお、その他に、システム欠陥悪用型 DoS 攻撃と呼ばれる、ハードウェア、OS やアプリケーション、ネットワーク、ストレージの脆弱性を狙い、システムを停止させるような攻撃を DoS 攻撃に含めることもある。

表 3.2　DoS 攻撃で用いられる手法の分類

| DoS 攻撃型 | DoS 攻撃名 | 通信<br>プロトコル | 特徴 |
|---|---|---|---|
| 帯域幅･リソースを消費させる攻撃(真正の DoS 攻撃) | UDP Flood | UDP | 攻撃者 IP アドレス詐称・特定困難<br>攻撃元の特定が困難 |
| | Smurf | ICMP | |
| | Ping Flood | | |
| システム資源を消費させる攻撃(脆弱性に根ざした DoS 攻撃) | SYN Flood | TCP Connection<br>確立前 | |
| | Connection Flood | TCP Connection<br>確立後 | 攻撃者 IP アドレスは正当<br>正常と異常の判別が困難 |
| | HTTP GET Flood | | |
| | リロード攻撃<br>(F5 攻撃) | | |

参考文献[10][11]より引用

以下に、既に知られているDoS攻撃の種類とその攻撃手法の概要を説明する。

なお、これらの攻撃手法には、1.2節で示した、DoS攻撃の分類(真正のDoS攻撃／脆弱性に根ざしたDoS攻撃)に対応関係を見出せるものがあり、それについても文末に示した。また、4.7(4)節に、これらの攻撃手法に対する対策例を示している。

#### (1) UDP Flood 攻撃

コネクションレス型の通信プロトコルである UDP の特徴を悪用する攻撃手法である。サイズの大きな UDP パケットを攻撃先アドレス宛に大量に送信する。

#### (2) Ping Flood 攻撃

通信エラーの通知や経路情報取得のための通信プロトコルである ICMP の特徴を悪用した攻撃手法である。サイズの大きなICMPパケット(ICMP echo request)を大量に送信する。

**(3) Smurf 攻撃**

(2)と同様に ICMP Echo Request を用いる。適当なブロードキャストドメインを選び、そのドメイン内のノード(パソコン、サーバ、ルータなど)に対して送信元アドレスとして攻撃先アドレスを設定して送信する。結果としてそのドメイン全体から詐称されたアドレスに向け、膨大な数の ICMP Echo Reply が送られることで、攻撃先の通信回線の帯域が占有される。

**(4) SYN Flood 攻撃**

攻撃対象のサーバに SYN パケットのみを大量に送信する。受信したサーバは、ACK パケットをタイムアウトになるまで待ち続けることになるため、メモリが消費される。今日の多くのサイト環境においては、この SYN Flood 攻撃への対策を取ることは一般的である。

以上の(1)～(4)は、一方的にパケットを送りつける攻撃であり、攻撃先の応答を受信する必要がないため、送信元の IP アドレスを詐称することが出来る。

**(5) Connection Flood 攻撃**

オープンされた状態が長時間にわたって続くような接続を繰り返し行うことにより、ソケットを占拠する攻撃である。サーバがコネクション数の制限を設けていない場合、メモリ不足になり、クラッシュする場合がある。

**(6) HTTP GET Flood 攻撃**

攻撃対象の Web サーバに対して TCP 接続を確立した後、HTTP の GET コマンドを大量に送付することで、Web サーバのメモリや処理能力を無駄に消費させる。同様に POST コマンドを使用する、HTTP POST Flood 攻撃と呼ばれるものもある。

**(7) リロード攻撃**

Web サーバに対して大量のアクセスを行う攻撃の 1 つ。送信されるデータは攻撃意図のないユーザが送るものと変わらないが、不必要に繰り返されることで攻撃となる。Web ブラウザで F5 キーを連続して押下することにより攻撃が出来ることから、「F5 攻撃」とも呼ばれる。これは Web サーバへの正当なアクセスと区別することが難しく、したがって一般的には対処が困難であるが、4.7(4)節「システム構成等の対策」である程度緩和することが可能である。

### (8) その他留意すべき攻撃

サーバ OS やサーバアプリケーションには、出荷後に脆弱性が発見され、これに対応したアップデートがベンダ等から提供される。サーバの運営者はこの情報に随時留意して、必要なアップデート等の作業を行うことが求められるが、必ずしもこのことが徹底されないという問題がある。また、脆弱性が発見されてからアップデートが提供されるまでの時間に攻撃を行うものもある。

なお、巻末の参考文献において「JVN で公表したサービス運用妨害(DoS)の脆弱性に関する情報」として公開され、ベンダによってアップデートが提供されている脆弱性についてその概要を示している。

## 3.5 攻撃の実際

実際の攻撃では、3.4 節「攻撃に用いられる手法」に例示した攻撃手法のいずれかひとつを選んで仕掛ける攻撃者はいない。複数の手法を組み合わせることが通常である。

例えば、はじめに SYN Flood 攻撃を行い、サイト側がこれに対策をすれば(あるいは対策が出来ていれば)、Connection Flood、HTTP GET Flood、UDP Flood と、プロトコルの異なるレベルや異なるプロトコルの攻撃を試みる。攻撃者自身のサーバを使った攻撃であれ、ボットネットを使った攻撃であれ、攻撃のプロトコルを切り替えることは技術的には容易である。

一方で、攻撃者側の事情として、例えば攻撃側の IP アドレスを詐称しにくい攻撃手法では、一旦その手法を取ってしまうと、IP アドレスに対して対策がなされてしまい、その IP アドレスにつながる機器が、攻撃装置としては無力化されてしまうリスクがある。また、大量のトラフィックを発生させる攻撃では、攻撃側の回線帯域も埋まってしまい、攻撃側自身の活動も制約を受ける。そうしたことから攻撃者も、なるべく少ない攻撃の資源やトラフィック量で DoS 攻撃の目的を達したいので、はじめは少なめに仕掛け、相手の反応を見ながら投入する機器やトラフィックを順次増やす、などの出方をすることが多い。

# 第4章 サービス妨害攻撃への対策

DoS 攻撃は、インターネット上のあらゆる主体(個人・企業・公的機関など)に等しく降り掛かり得る脅威であるから、その対策には、個別の企業や組織だけでなく、以下のような社会的な取組も必要である。

●社会全体の、実在する脅威についての正確な認識の醸成
●技術の変化に対応した、適切な法体系や制度の整備
　・攻撃を行なった者に対する罰則の強化
　・司法機関同士の国際連携
●DoS 攻撃の土壌となるボットネットの抑制と排除
　・技術的な対応
　・インターネット参加者全体に対する意識啓発

ただし、本報告書の読者が、短期的又は中期的な現実なリスクに対応するためには、あくまでユーザ主導で具体的に何が出来るかを整理する必要がある。

本章では、DoS 攻撃に、ユーザ企業の立場で具体的にどのように対処すればよいのか、ユーザ企業が事業活動として提供しているサービスを DoS 攻撃から保護することを想定し、その考え方と対策方法について紹介する。

## 4.1 対策の基本的な考え方

これまで事例や攻撃の状況に関して示してきたように、インターネット向けにサービスを提供している限りにおいて、いかなる対策をもってしても DoS 攻撃の影響を完全に排除することは困難である。一方で、DoS 攻撃を受ける可能性を予め認知し、必要な方針を定めておくことで、攻撃がサービスや事業・業務に及ぼす影響を緩和することが可能なことも事実である。ここでは、企業等において予め方針を定めておくべきことの例を以下に示す。

### (1) 対策に関する役割分担

対策に関する代表的な当事者としては、以下の役割が想定される。それぞれの役割に関する詳細は、後述の該当節において説明する。

- 経営者等：サービスに関する設備投資の判断、体制の整備等(4.6 節を参照)
- 情報セキュリティ担当者：異常の検知、情報収集等(4.7 節を参照)
- 契約 ISP、クラウド事業者：攻撃の証拠保全、通信のブロック等(4.8 節を参照)
- IPA：攻撃が疑われる場合の相談
- 契約 ISP、JPCERT/CC 等:攻撃の届出や被害への対処に関する調整(4.3 節を参照)
- サービス提供担当者：予め定められた手順等に従った対応(代替措置の利用等)

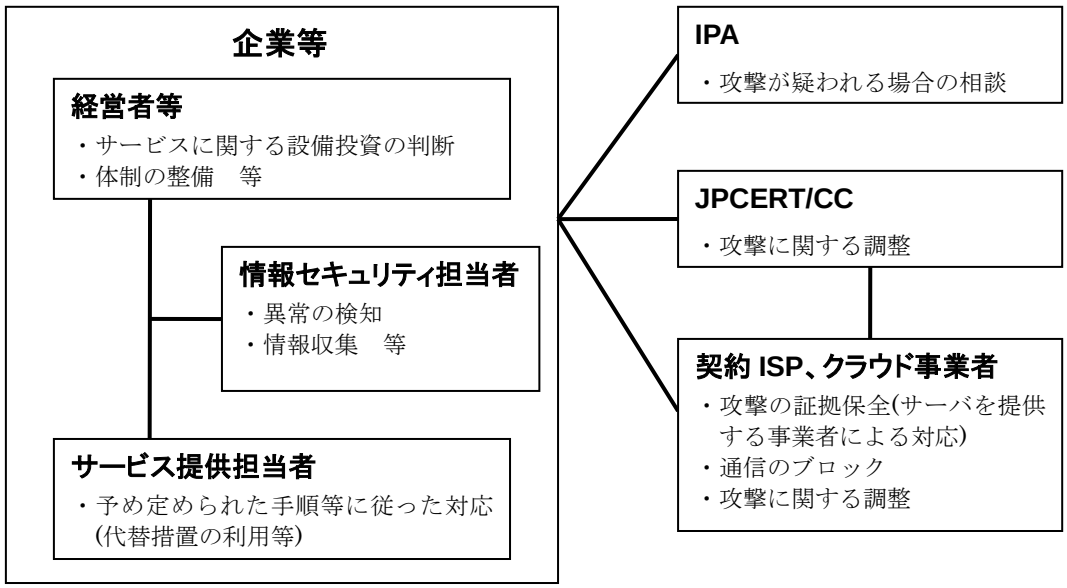


図 4.1　対策に関する役割分担

なお、DoS 攻撃においては上述の通り ISP が果たす役割が大きいが、電気通信事業法の定めにより通信の秘密を侵害することが禁止されているため、対策実施の主体となって活動することは出来ない。そこで、企業等が主体となった対策が欠かせないことを認識しておくことが重要である。この詳細については本章の 4.6 節、4.7 節にて説明する。

### (2) 事前対策の方法

DoS 攻撃の影響を緩和する対策方法としては、以下に例示するような対策案が考えられる。ただし、いずれも万能かつ導入が容易な方法とはいえず、攻撃によるリスクと対策による効果、必要なコスト等とのトレードオフの問題となる。

#### a. 高性能のサーバや高速な通信回線の利用

需要に比してオーバースペックなサーバや通信回線を利用していれば、小規模な DoS 攻撃を受けても、サービスが麻痺状態に陥ることを避けることが出来る。また、単に性能を高めるだけであれば運用管理の手間はほとんど変わらず、特殊な機器を導入する場合のような煩雑さがない。一方で、大規模な DDoS の場合は世界規模でサービスを提供しているポータルサイトやオンラインショップであっても麻痺状態にすることが可能であり、いくら投資しても「十分な安全性」を確保することは困難である。また、高性能な設備を利用することは、当然サービスの採算性を悪化させる。

**b. サービス妨害攻撃を行うおそれのある国やドメインからの通信を拒否**

現在の DoS 攻撃の主体である DDoS はボットからの攻撃によって実施される。よって、ボットに感染しているコンピュータ等が多い国やドメインからの通信を拒否することで、DoS 攻撃の影響を緩和することが可能である。この方法は、国内のみにサービスを提供している場合等には十分に有効であり、高価な初期投資も不要である。反面、現在のインターネットにおける IP アドレスの割当は、国毎に明確なブロック分けがなされておらず、新規のアドレス割当が行われるたびに、拒否するアドレスのリスト(ブラックリスト)、又は通信を許可するリスト(ホワイトリスト)の更新をしなければ対策の効果が薄れたり、本来アクセスを許可すべき利用者を拒絶したりする結果を生じかねないなど、運用管理の手間を要する方法である。

**c. クラウドの利用**

中小企業等が自社内で利用しているサーバ(オンプレミス)よりも高性能な設備が、低価格で提供されるクラウドを利用した場合、コストを抑制しつつ、a.と同様の改善効果を期待することが出来る。ただし、クラウドを利用することは、DoS 攻撃に関する別のリスクを生じる原因ともなり得る。この方法についての詳細は、本章の 4.2 節にて検討する。

**(3) サービス妨害攻撃を受けたと思われる場合の対応**

DoS 攻撃と思われる状況が発生した場合でも、それは異なる原因で発生している可能性がある。よって、本当に DoS 攻撃によるものかどうか、早い段階で判別する必要がある。さらに、DoS 攻撃によることがほぼ確実と思われる場合の対処方法についても、予め認知しておき、自組織における対処の手順について定めておくと攻撃が発生した場合の対応が円滑に進み、サービスの回復も早くなることが期待される。また、サービス妨害攻撃によるものかどうかの判別が難しい場合には、IPA の情報セキュリティ安心相談窓口(http://www.ipa.go.jp/security/anshin/)に相談することも可能である。本章の 4.8 節にこうした緊急対応(インシデントレスポンス)の考え方を示す。

### 4.2 クラウドとサービス妨害攻撃との関係

中小企業等を含む小規模組織における情報セキュリティ対策に関しては、これまで専門の担当者の不在等の結果、ソフトウェアのアップデートの不備等、基本的な部分での対策実施不足による危険性が指摘されている。クラウドへの移行はこうした危険性の削減につながることが期待される。その一方で、これまでは外部の通信回線等の影響を受けないような設備等でサービスを動作させていた状態から、クラウド上に移行することで、DoS 攻撃の影響を受ける機会は増加する。ここでは、こうしたクラウドの特徴が DoS 攻撃に対してどのような影響を及ぼすかについて、具体的に検討する。

#### (1) クラウド利用によって変化する事項

自社内に設置しているサーバでサービスを提供していたものを、クラウドに移行することで、次のような影響が生ずることが想定される。

##### a. インターネットに接続される通信回線への依存度の増大

パブリッククラウドの場合、インターネットを通じて利用することが前提にあるので、インターネットに接続される通信回線への依存度が増大する。プライベートクラウドの場合はこの限りではない。

##### b. クラウド事業者によるインフラ管理

クラウドの場合、インフラの管理はクラウド事業者が行うことが特徴である。ただし、SaaS、PaaS、IaaS の違いにより、どの範囲までクラウド事業者が管理するかが異なってくる。

##### c. 他利用者のサービスとのリソースの共有

パブリッククラウドでは、一般に他の利用者とハードウェア、通信回線等を主体とするリソースを共有することが多い。ただし、大規模なリソースを使用する場合は実質的に占有的な利用形態となる場合もある。

##### d. コスト負担方法の変更

クラウドの場合、リソースの量と使用期間に応じた費用を払うのが一般的である(従量制)。これに対し、自社でサーバを運用する場合は、買い取り、リース、レンタル等の様々な方法がある。

#### (2) クラウド利用によってもたらされる影響

前項に示したような変化から、クラウドを利用することで、企業等には以下のような影響がもたらされるものと想定される。クラウド事業者が提供する回線やサーバ等を利

用する際には、a に示すメリット、b に示すデメリット両方について確認したい。

**a. サービス妨害攻撃に関するクラウドの利用によるメリット**

クラウドを利用することで、DoS 攻撃対策について以下のような効果が期待される。

- 中小企業の場合、コスト等の観点から自社が接続に用いている回線やサーバ等の性能は相対的に低いものとならざるを得ない。この結果、小規模な DoS 攻撃であっても大きなダメージとなる可能性がある。一方、クラウド事業者が提供する回線やサーバ等は、一般には高い性能を提供するのが普通であり、小規模な DoS 攻撃の影響を受けにくくなる効果が期待出来る。
- クラウド事業者は、自ら提供するサービスを保護するために必要な範囲で DoS 攻撃対策を講じることが想定される。よって利用者はクラウドを利用することで、何らか(特にSaaSの場合はアプリケーションに近いレイヤまで)のDoS攻撃対策が講じられることを期待することが出来る。ただし、この対策が利用者における事業継続を可能とするために十分なものであるとは限らない。こうした対策の実施の有無は、クラウドの価格設定の要因の一つとなり得るが、クラウド事業者から開示がなされないと、利用者からは見えないため、クラウドサービスの選択における市場原理が働かないものとなる。
- 第 2 章 2.1.5 節で示した公共施設の事例において、公共施設側で DoS 攻撃と認識するに至ったのは、決して大量とはいえない通信量でサービス提供が困難になったサービスアプリケーションの影響が大きい。そこで、クラウド事業者がアプリケーションレベルまで提供する SaaS の場合、クラウド事業者が性能面での考慮を行うことが期待されることから、こうした事例が発生しにくくなると考えられる。一方 PaaS、IaaS においては、アプリケーションはクラウド利用者の責任で提供するものであるため、クラウドへの移行に関わらず同様の状況となる。

**b. サービス妨害攻撃に関するクラウドの利用によるデメリット**

a.の反面、クラウドを利用することで、DoS 攻撃に関して以下のようなリスクを増大させる可能性がある。

- これまで自社において DoS 攻撃への具体的な対策(パケットシェーピング等)を講じていた場合、クラウドに移行することでこうした対策を細かく実装することができなくなり、DoS 攻撃対策に関する機能低下を招く可能性がある。
- クラウドを利用することで、他社のサービスを狙った DoS 攻撃の巻き添えとなり、自社のサービスに影響を受ける可能性がある。
- 利用者が提供するサービスに DoS 攻撃を受けることで、クラウド事業者(この場合は IaaS 等)から今後のサービス提供を拒否される可能性がある。

### 4.3 サービス妨害攻撃に関する相談や届出の窓口

DoS 攻撃に関する相談や被害の届出先に関する情報を、以下に整理して示す。

#### (1) IPA

IPA は、情報セキュリティに関する総合的な相談窓口である「情報セキュリティ安心相談窓口」を設置し、広く一般からの相談に対応している。本窓口は、ウイルスや不正アクセスに関する相談のほか、DoS 攻撃が疑われるような場合の相談にも対応している。
(情報セキュリティ安心相談窓口　http://www.ipa.go.jp/security/anshin/)

#### (2) 契約している ISP・クラウドサービス等事業者

DoS 攻撃は ISP の通信回線を経由して行われることになるため、その異常に関する相談先としては ISP が最も適切である。また、クラウドサービスやレンタルサーバ等を利用している場合は、そうしたサービスを提供している事業者に相談することも考えられる。こうした ISP や事業者は、DoS 攻撃に関するログ等の情報を把握することが出来る場合がある[9]。ただし、通信の秘密を侵してはならないことが電気通信事業法によって定められていることに留意する必要がある。

#### (3) JPCERT/CC

JPCERT/CC は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントに関する日本国内のサイトを対象とした報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを技術的な立場から行う中立的組織である。DoS 攻撃はこのコンピュータセキュリティインシデントの 1 つであり、JPCERT/CC に相談することで必要なアドバイスや調整を受けることが出来る可能性がある。特に海外からの攻撃が考えられる場合、JPCERT/CC が有する海外機関とのネットワークを通じて、攻撃元 ISP との調整が可能となる利点がある。しかしながら、多くの国のボットを用いて攻撃が行われる DDoS 攻撃のような場合、対象国すべてと調整を行うことは現実的ではないため、つねに調整が有効に機能するわけではないことに留意する必要がある。

なお、ISP の場合と異なり、JPCERT/CC は相談者の攻撃に関する情報を自ら把握することは出来ないため、相談にあたっては相談者が攻撃に関する情報を収集・提供する必要がある。

---

[9] 一般に、ISP では利用者の通信記録を保存していない。クラウドにおいても、契約形態によっては利用者がログを参照出来ない場合がある。

**(4) 所属する都道府県警察**

犯罪に該当するような DoS 攻撃による被害の届出については、他のコンピュータ犯罪と同様、所属する都道府県警が窓口となる。次節で説明するように、DoS 攻撃がもたらす被害は刑法で定める電子計算機損壊等業務妨害罪等の構成要素を満たす可能性がある。警察による捜査は、被害を受けた当事者による届出がなされることで開始されるのが一般的である。届出の前段階として、被害に関する相談を行うことも出来る。

なお、障害などの人為的要因によらないものを誤って届け出ることで混乱を招く恐れもあるので、届出に先立ち、情報セキュリティや情報通信ネットワークに関する知識をもった人に相談することが望ましい。

### 4.4 サービス妨害攻撃に関する法律や制度

日本の法律において、DoS 攻撃がどのように扱われているかについて示す。

#### (1) サービス妨害攻撃に適用される法律

コンピュータウイルス等有害プログラムの法的規制に関する国際動向調査(参考文献[13])では、コンピュータウイルスを対象に刑法の適用可能性が議論されている。これを参考に、DoS 攻撃を対象として刑法における以下の適用の可能性について整理する。

##### a. 電子計算機損壊等業務妨害罪

「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者」が対象となる。DoS 攻撃が「虚偽の情報若しくは不正な指令」に該当するかどうかについては、DoS 攻撃のうち、正規の指令を大量に送付することで過剰な負荷を与える種類のものへの適用は判断が難しいところであるが、「又はその他の方法」で使用目的に沿うべき動作を妨害していることから、適用が可能と考えている専門家もいる。他方、脆弱性を悪用する種類のものについては、脆弱性を悪用するコードが「不正な指令」に相当することから、適用は問題ないものとみられる。

##### b. 偽計業務妨害罪、威力業務妨害罪

「虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者」は偽計業務妨害罪の、「威力を用いて人の業務を妨害した者」は威力業務妨害罪の対象となる。参考文献[14]によれば、「機械に対する対物的加害行為も「偽計」ないし「威力」に当たると解される」ことから、適用が可能と考えられている。

##### c. 器物損壊罪

「他人の物を損壊し、又は傷害した者」が対象となる。このとき「損壊」とは、「物質的に器物の形態を変更又は滅尽させる行為のほか、物の本来の行為を失わせる行為」であるとされる。DoS 攻撃の場合、攻撃の勢いが衰えれば自ずと本来の機能が復活するケースが多いため、これらの構成要件を満たすことは考えにくいが、上記の a.と b.がいずれも「業務」を対象とし、「単に趣味や娯楽のために情報システムを利用するようなケースは含まれない」(参考文献[15])ことから、業務目的以外の機器等を対象にした攻撃について適用される可能性がある。

### (2) 国境を越える犯罪への効力

日本国内にサーバを設置し、国内で業務を行っている状態で海外からの攻撃を植えた場合、日本の刑法が適用される。ただし、実際に法執行を行おうとすると、誰が行っているかを追跡し、何をしたかの証拠を集めて起訴する必要がある、したがって、こうした情報を集める対象が海外となった場合にはほとんど実効性が期待出来ないのが現実である。

一方、日本の企業が国内でクラウドを用いた業務を行っている場合、クラウドの拠点が海外にあり、海外から攻撃された場合については、日本の刑法の適用は難しいと考えられている。ただし、日本の刑法は属地主義であり、解釈的に日本国内で人が行っている業務が妨害されているという評価が出来るのであれば、a. 電子計算機損壊等業務妨害罪で「人の業務の妨害したものは」となっているので、電子計算機がどこにあるかは問わないという解釈が取れる限りにおいて、刑法が適用される可能性はある。

海外で事業として営まれている DoS 攻撃の請負ビジネスに日本人が攻撃を発注し、日本国内を攻撃した場合は、単純に日本の刑法により発注した日本人を正犯として適用することが可能と考えられている。

### (3) 「通信の秘密」による制限と電気通信事業者による対応

電気通信事業法において、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」(第 4 条)と定められている。このため ISP では、サービスの品質確保の立場から自ら主体的に DoS 攻撃と思われる通信を識別し、これを排除するなどの対策を講じることが十分に出来ない状況にある。

こうした状況を踏まえ、通信の秘密の保護に最大限配慮しながら電気通信サービスの円滑な提供の確保に資することを目的として、2007 年 5 月に「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」が、社団法人日本インターネットプロバイダー協会、社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本ケーブルテレビ連盟の 4 団体によって策定された。これは、「大量通信等によって電気通信事業者の設備に支障が生じる場合」や「送信元を詐称した通信が送信された場合」等の事象に即して、大量通信等への対処を行った場合の通信の秘密の保護との関係についての考え方を示すものである。ガイドラインの内容は非公開であるが、その概要が公開されており(参考文献[34])、「機械的に処理される仕組みであっても、電気通信事業者の取扱中に係る通信に関し、その通信の秘密に属する情報(通信内容、構成要素等)について機械的に検索を行い特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する行為が通信の秘密の侵害(窃用)(事業法第 4 条、第 179 条)に当たる」ことが明記されている。その上で、通信状況と通信当事者の同意の有無など、個々の状況設定に応じた考え方と通信事業者の対応例を紹介している。

## 4.5 通信事業者等が提供する対策

### (1) ISP が提供する対策サービス

複数の大手 ISP から DDoS 対策のためのサービスが提供されている。各社のサービスとも、ネットワークのうちバックボーンに近い位置に設置された DDoS 対策装置により、ユーザ回線への DDoS トラフィックを遮断する仕組みのものであり、サービス内容や DDoS 対策としての基本的な機能に大きな差異はない。DDoS 対策装置がバックボーンに近い位置に置かれる意味は、バックボーンの回線から、回線帯域がより小さいユーザ回線へと分岐していく過程で、対策装置が設置されている部分の回線の帯域が攻撃によってあふれさせられると、DDoS 対策装置が本来持っている、DDoS トラフィックと正常なトラフィックを分離する機能が十分に発揮されないことによる。したがって、効果的な DDoS 対策サービスを打ち出せるのは、高帯域なバックボーンを維持する限られた大手 ISP になる。

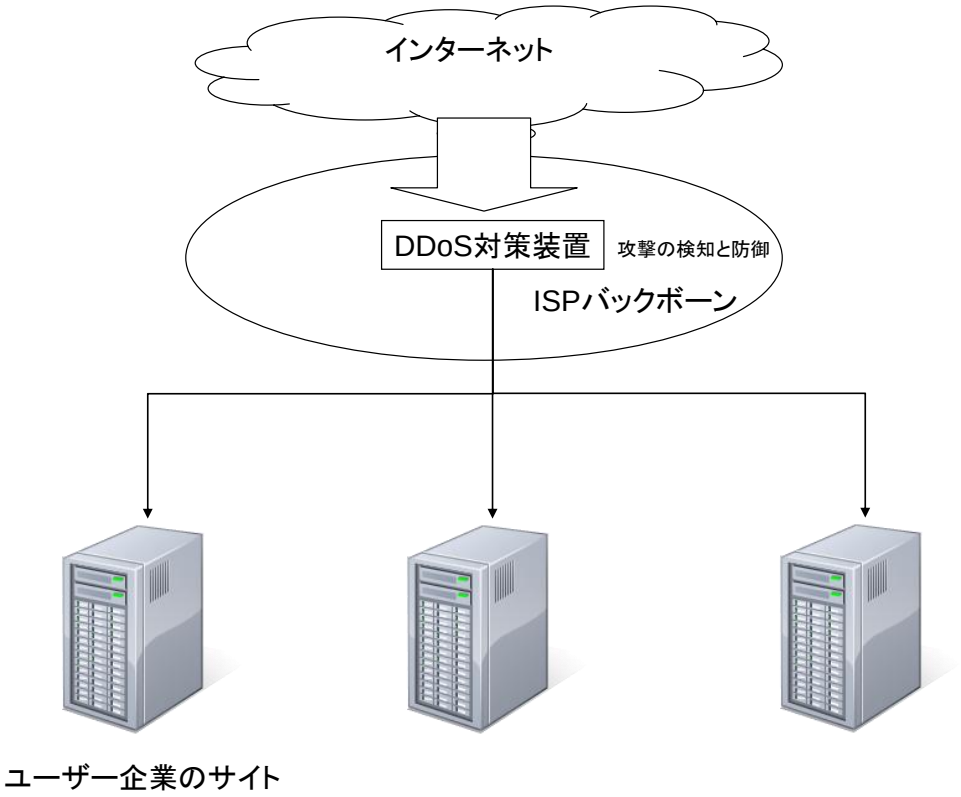


図 4.2　ISP による DDoS 対策サービスの概念図

ISP が提供する DDoS 対策サービスは、一般に以下の内容を含む。

・導入前のコンサルティング

専門の技術者が、事前にユーザに対してヒアリングとコンサルティングを実施し、ユーザ環境に合わせたアクセス制御ポリシーを設定する。

・運用

専門の技術者が、ユーザに代わって DDoS 対策装置を運用する。装置のソフトウェアの保守や機器の設置、設定管理、障害対応などを行う。

・監視

専門の技術者が、ユーザネットワークの状況を常時監視する。攻撃を検知した際に、攻撃状況と対策状況を逐次ユーザに報告する。

・復旧

異常が発生した際に、ユーザへの連絡と共に、可能な限り迅速な復旧にあたる。

・定期的なレポート

トラフィックの推移や DDoS 対策サービスの動作を、定期的あるいは常時ユーザに報告する。

参考までに、DDoS 対策サービスの相場としては、例えばユーザ回線が 100Mbps の場合、月額数十万円といったところである(初期費用は別途必要)。

こうした DDoS 対策サービスは、ISP が提供するインターネット接続サービスとは完全に別のオプショナルなサービスとされているのが普通である。すなわちこのサービス自体が高額であって、本来のインターネット接続の費用とのバランスを考えて、検討段階のユーザ企業が多い。

ただし、DDoS 対策としては現状では決定版といえるもので、SYN Flood、ICMP Flood、UDP Flood、あるいは攻撃元 IP アドレスを詐称した通信など、1.2 節に示した「真正の DoS 攻撃」に対しても、(攻撃の規模にもよるが)かなり効果的とされている。

**(2) セキュリティ専門ベンダによって提供される対策サービス**

前述の「(1)ISP が提供する対策サービス」を利用することが、現状でもっとも本格的な DDoS 対策であるとしても、それはどちらかというと攻撃を受けていない状況での平常時に導入しておくべきものであり、攻撃を受けてしまった場合については、その時点で行う対策が必要である。そうしたとき相談出来る事業者がおり、ここではセキュリティ専門ベンダと呼ぶ。そうした事業者にインタビューした結果、一般的に以下のような対策サービスが考えられるという。

セキュリティ専門ベンダの対策サービス①
(事前評価)

・企業の、DoS/DDoS に対する耐性を見極めるサービスであり、ISP との契約の内容や設備のチェックから始まり、トータルとして、そのサイトがどのような状態に置かれているかを評価する。

セキュリティ専門ベンダの対策サービス②
(予防)

・攻撃を検出する機器を導入するためのネットワークコンサル、再構築、運用を行う。
・ユーザ企業に対してインシデント発生時の対応フロー、トレーニングを行う。
・回線事業者との打合せ、回線業者への要求事項、チェック事項の取りまとめ、インシデント発生時の連絡ルートの策定などを行う。

セキュリティ専門ベンダの対策サービス③
(インシデント発生時の復旧支援)

・異常な事象が発生した場合、それが攻撃であるかどうかを見極め、攻撃であればその目的を推測し、必要ならば攻撃者との応対をとり、警察その他関連機関との連携を図り、暫定手段の提案を行う。
・また、事態が安定した後に、ユーザ企業の意向があれば、より行き届いた対応の出来る ISP への移設のコンサルティング、ISP との交渉なども考えられる。

ただし、こうしたサービスは、1.2 節に示した「脆弱性に根ざした DoS 攻撃」についてはかなり有効な対策を提示出来るが、「真正の DoS 攻撃」に対する効果は限定的である。また、一般的にセキュリティ専門ベンダとしては、必ずしも規格化したサービスとして確立しているものではない。これまでは、2.1.1 節の事例に示されるように、事象が発生してから、ユーザ企業に相談を受け、セキュリティ専門ベンダは持てる知見を総動員して対処しているという側面が大きい。したがって費用面での規模感は明確には出来ないが、数十万円台から 2～300 万円くらいではないかと推察される。

**(3) その他に外部の機関で考えられる対策サービス**

その他に選択し得る対策としては、CDN(Contents Delivery Network)の利用が考えられる。CDN とは、Web コンテンツをインターネット経由で配信するために最適化されたネットワークのことであり、コンテンツ配信網とも言う。又は、そうしたネットワークの機能を提供する事業者を指すこともある。インターネットの利用が一般に普及するにつれ、大手サイトからのリンクや動画等の配信が普通になると、それまで想定されていない大量のユーザや大量のデータ要求がサイトへ集中し、遅延あるいは応答不能になることが顕在

化してきた。これに対処するために、サーバを一ヶ所だけに置くのではなく、相互にミラーリング(データの複製をリアルタイムに複数の場所に保存)したサーバを地理的・バックボーン的に分散させ、しかも経路上最適な位置にあるサーバから各ユーザに配信するのが効果的である。このサービスは 1.2 節に示した「真正の DoS 攻撃」に対しても、(攻撃の規模にもよるが)かなり効果的とされている。

ただし、こうしたサービスは非常に大規模なコンテンツ配信を想定しているものが多く、一般に高額であり、DDoS 対策としては前述の「(1)ISP が提供する対策サービス」よりさらに敷居が高い位置づけのものである。

### 4.6 経営者等が考慮すべき事項

DoS 攻撃への対策を企業等として取り組むにあたり、企業の経営者や組織の代表者、またこれらに準ずる情報セキュリティ面の責任者が、事業遂行・組織運営の視点から検討しておくべき事項について説明する。

#### (1) サービス妨害攻撃の対策立案にあたり考慮すべき事項

##### a. 事業継続の観点からの許容停止期間

企業等が、例えばクラウドを利用している場合、クラウドが DoS 攻撃を受けることで、利用している企業等の対処しようが無いところで、その機能が麻痺してしまう可能性がある。このとき、その用途の相違により、どの程度の期間であれば止めても支障が生じないかで対策の方法も変わってくる。

すなわち、例えばお客様からの注文の処理システムであれば、遅くとも数時間以内に回答を返信する必要があるが、従業員の福利厚生用のシステムであれば数日程度の停止が許容される、といった違いが想定される。停止が許容される期間内であれば、一般的な DoS 攻撃の傾向を踏まえ、あえて特別な対策を講じないという選択もあり得る。こうした検討をもとに対策への重み付けを行うことで、停止が許容されない分野への重点投資も可能となる。

##### b. 企業等としての社会的責任

a.の内容とも関連するが、企業等が担っている社会的責任についても考慮する必要がある。DoS 攻撃により自らの事業が停止することだけでなく、自らのサービスが停止又は応答速度が著しく低下することで、他の企業や社会にどのような影響を及ぼすかを考えることは、事業継続の観点と並んで重要である。ある企業等の事業継続は、他の企業等の事業継続に一定の責任を負っている場合が多い。取引先は自社以外から調達出来るのか、利用者にとって選択肢があるかどうかなど、常に意識しておく必要がある。

また、特に Web 関連のサービスに関しては、近年のマッシュアップ的な利用のもとでアプリケーションの連動が進んでおり、電子商取引(EC)等の分野全体での影響を考慮する必要がある。

##### c. 企業価値を維持する責任

民間企業等の場合、DoS 攻撃等で事業が停止させられることは、そのほかのセキュリティ問題が発生する以上により深刻な問題であり、上場企業であれば株価に直接インパクトがあることが多い。例えば、個人情報の漏洩なども一般的には大きな不祥事ではあるが、企業に跳ね返る実質的な損害や株価への影響という意味では、DoS 攻撃により事業が停止させられてしまうことの方が、より大きなビジネスインパクトがあることが多い。そうしたことから、経営者の立場では、例えばインサイダー等によって攻撃を仕掛けられ株価イ

ンパクトを悪用されることを警戒する、などの観点は持っておくべきである。

**d. 利用可能な対策の効果とコスト**

ここで検討すべきは、DoS 攻撃に備えた事前のコストである。はじめに、インターネットに事業基盤を依存する事業者は、2.2 節で見た想定される損害額について、自社の事業内容に応じた被害の範囲・規模をなるべく精緻に見積もる必要がある。

一方で、一般的にあらかじめサービス妨害攻撃を想定した対策とコストには以下の種類がある。

①回線契約(回線容量)の見直し
②ISP による DDoS 対策
③対策の研究、セキュリティ対策要員の教育
④ネットワーク機器のグレードアップ
⑤サーバリソースの増強

①②については、ISP に対してそうした対策の実現性・効果について相談してみることができるが、現在契約している ISP から十分な示唆が得られなければ、セキュリティ専門ベンダに相談することも考えられる。また、③についても、その実施については、セキュリティ専門ベンダに相談することができる。さらに④⑤については、4.7 節に対策例とその効果について検討する材料を提示している。

以上を参考に、自社において想定される被害とバランスのとれた対策を検討する必要がある。

### (2) サービス妨害攻撃への対策のための組織

DoS 攻撃は、サイトへの不正アクセス、コンピュータウイルス感染などと同様に情報セキュリティ上のインシデントのひとつとして位置づけられる。特に情報セキュリティ上のインシデントに対しては、会社内の各部門が緊急事態に対して力を合わせる必要があり、会社内の組織を横断した対処が求められる。そのため CISO(Chief Information Security Officer：最高情報セキュリティ責任者)という役割をおくことが望まれる。ここではもちろん、CISO という名称が重要なのではなく、経営リスクに直結する情報セキュリティインシデントに対して企業として高次の状況判断ができ、それをもとに各部門に必要な指示を行なえる立場であり、経営責任者と肩を並べる程度の権限が求められる。CISO については、必ずしも技術的に高い知見を有する必要はなく、状況判断のための技術面での材料を与える者が補佐すればよい。また、実際の企業の例では、情報システム部門を統括する CIO(Chief Information Officer：最高情報責任者)あるいは事業部門を統括する CTO(Chief Technical Officer：最高技術責任者)が、実質的な CISO の役割を兼務することもある。

さらに、各部門には情報セキュリティ担当者を配置し、日頃から定期的に情報セキュリティ担当者間で情報セキュリティに関する情報を交換し、インシデント発生時にはただちに対策委員会(あるいはこれに該当する集まり)を設けて、CISO の指示のもと、インシデント情報の報告、連絡、所属する部門が担うべき役割を部門に持ち帰ることなどを行う。

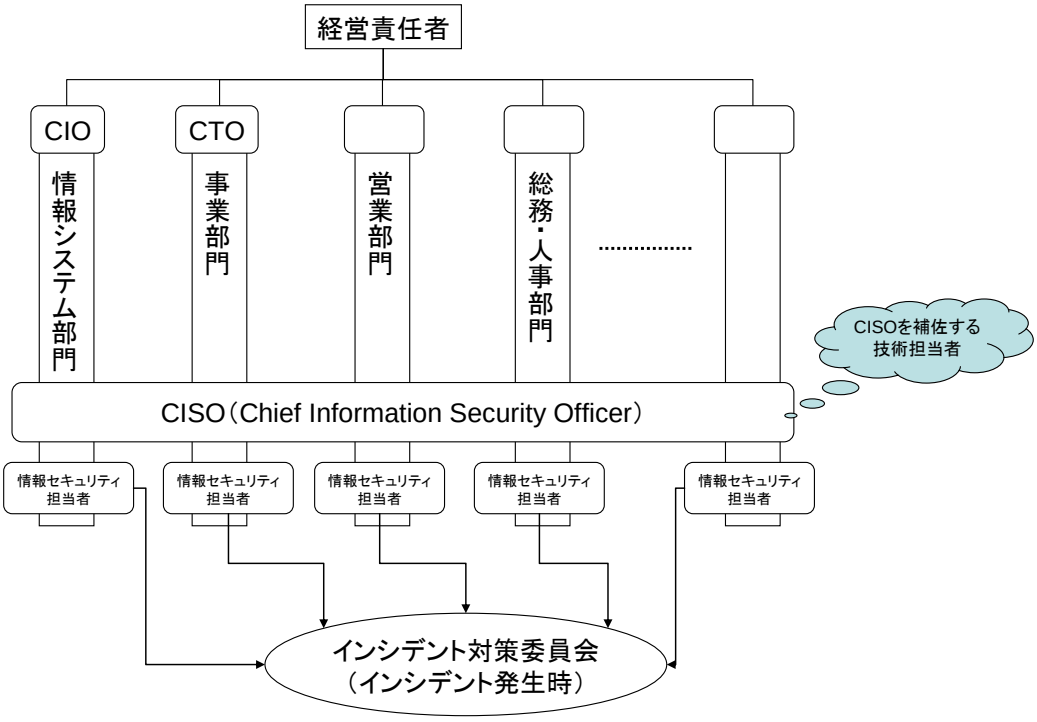


図 4.3　情報セキュリティインシデント対策のための組織

### (3) サービス妨害攻撃への対策のための計画

企業等において、DoS 攻撃に限らず広く情報セキュリティ上の事件・事故がもたらす被害に対して、事業を継続することを目的とした計画のあり方が「事業継続計画策定ガイドライン」(参考文献[35])に掲載されている。そこでは、いわゆる BCP(Business Continuity Plan：事業継続計画)として、潜在的損失によるインパクトの認識を行い、実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする計画の重要性が述べられており、その立案に対する基本的な考え方を示している。通常 BCP とは、事故・災害・感染症などを含めた、企業活動の継続を危うくする広範な事象を視野に入れるものであるが、その中で特に情報セキュリティインシデントに対応した BCP の中で、さらに DoS 攻撃に対応した計画の策定が望まれる。DoS 攻撃に対する対策は、その他の情報セキュリティ上の事件・事故、例えば、不正アクセスによる情報漏えいやシステムの改ざん、コンピュータウイルス感染によるシステム障害などに比べても、(内部・外部を含めた)より組織的な対応が要求され、企業体力そのものが問われることが多い。

同ガイドラインでは、BCP の発動から全面回復に至るまでは、①BCP 発動時、②業務再開フェーズ、③業務回復フェーズ、④全面復旧フェーズの大きく 4 つのフェーズに分けることが出来るとしている。各フェーズにおいては、BCP 発動から回復後の事後処理まで、経営層の的確な意思決定が求められる。DoS 攻撃への対策に適用した際の、各フェーズの内容及び対応のポイントは、主に以下のとおりである。

**表 4.1　BCP の観点からみた DoS 攻撃への対策フェーズ**

| フェーズ | 内容 | ポイント |
|---|---|---|
| ①BCP 発動 | DoS 攻撃事象の発生(或いは発生の可能性)を検知してから、初期対応を実施し、BCP 発動に至るまでのフェーズ。 | 発生事象の確認、対策本部の速やかな立ち上げ、確実な情報収集、BCP 基本方針を決定する。 |
| ②業務再開 | 代替手段により、DoS 攻撃によって停止・停滞させられたサービスを再開し、軌道に乗せるまでフェーズ。<br>最も緊急度の高い業務(基幹業務)の再開まで行う。 | 代替手段への確実な切り替え、復旧作業の推進、要員などの経営資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイント。 |
| ③業務回復 | 最も緊急度の高いサービスや機能が再開された後、さらに提供するサービスの範囲を拡大するフェーズ。 | 代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイント。 |
| ④完全復旧 | 代替設備・手段からサービスの平常運用へ切り替えるフェーズ。 | 全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。 |

## 4.7 情報セキュリティの担当者が対策すべき事項

各企業等において、情報セキュリティの担当者が DoS 攻撃に対してどのような対策をしておくべきかについて説明する。なお、ここでは主に日常的な運用において考慮すべき事項を中心に触れる。

なお、ここで示す事項は、可能な限り自社の情報セキュリティの担当者が掌握しておきたい事項ではあるが、例えば

4.7(3)節「サービス妨害攻撃の影響を抑制するための性能の把握」

4.7(4)節「システム構成等の対策」

などについて、技術的なハードルが高ければ、システムベンダやセキュリティ専門ベンダ(4.5(2)節を参照)に日頃から相談しておくことも有効である。実際に、DoS 攻撃を受けた場合の対応については、4.6 節で示した経営者や管理組織とあらかじめ対応方針について合意を得ておき、緊急時には定められた体制の下で危機管理対策を実施することが望ましい。

### (1) 基本的なセキュリティ対策の実践

DoS 攻撃の対策を考える以前に、インターネット上でサイトを運営しサービスを提供するシステムの管理者が当然のこととして踏まえておかなければならないことがある。

具体例としては、IPA の「小規模サイト管理者向けセキュリティ対策マニュアル」(参考文献[21])に記された内容が、適用されているか十分に検討すること等が挙げられる。

### (2) 日常的なアクセス状況や負荷についての把握

まず、通信のログをネットワーク機器等で残す設備を用意し、平常時からログを残すこと。小規模な企業では、ログが残されていない場合が意外に多い。また、単に記録を残すだけでなく、管理者が、平常時はどういうものかを把握しておくことが非常に重要である。また、そのことによって異常時との違いが認識出来ることも必要である。

また、ISP から定期的に自社のコネクションレポートの詳細をもらい、これに関心をもっておくことも有効である。

### (3) サービス妨害攻撃の影響を抑制するための性能の把握

サービスを提供しているサーバや通信回線が一定以上の性能を確保していれば、小規模な DoS 攻撃による影響を実用上差し支えない程度まで回避出来る場合も多い。こうした性能の基準については、その用途や需要に応じて異なるが、あらかじめ次表のように整理しておくことで、システムの調達の際にベンダに調達仕様として提示したり、クラウドと自組織のサーバ(オンプレミス)のいずれで実装するのが有利かを判断する際の参考にすることが出来る。

また、攻撃時に、その状態を記録するサーバ自体がダウンすることがあり、その場合、対処のための十分な情報が得られないことになる。余裕を持ったサーバを用意したい。

表 4.2　チェックシートの例(再掲)

| 項目 | 仕様 | 条件 |
|---|---|---|
| 単位時間あたりトランザクション数 | ○○以上 | 1 秒間あたり |
| 1 トランザクションあたりの応答時間 | ○○ミリ秒以内 | 同時トランザクション数が○○以上の状態が 60 分以上持続する場合において |
| データベースのセッション数 | ○○以上 | 1 秒間あたり |
| データベースのセッションあたりの応答時間 | ○○秒以内 | 同時セッション数が○○以上の状態が 60 分以上持続する場合において、以下のコマンドを実行する場合：△△△ |
| サービスのトップページの表示時間 | ○秒以内 | http リクエスト送出からページ表示完了までの平均所要時間 |
| 通信速度(帯域保証) | ○Mbps 以上 | インターネットからサーバまでの経路を通じてこれを下回る区間がないこと |

**(4) システム構成等の対策**

システム構成等を調整することで、サービス妨害攻撃への対策となり得るものもある。例えば、不要なトラフィックを排除することにより、サーバの性能を維持するなどがある。以下に、検討すべき内容(対策手段)の例を挙げる。

表 4.3　サイト側の対策の例

| 対策のカテゴリ | 対策 | 内容 |
|---|---|---|
| サイト側ネットワークにおける対策 | **FW によるフィルタリング** | インターネットからサーバに向かう経路上のファイアウォール(FW)で、不要な UDP パケット／不要な ICMP パケット／不正な IP アドレスからのパケットなどをフィルタリングする。また、明らかな攻撃元 IP アドレスからのパケットについてもフィルタリングする。 |
| | **帯域制御装置の導入** | 通信内容における IP アドレス、トラフィック・タイプ(画像、ストリーミング型データ、HTML ファイル、プッシュ型データ、FTP、NNTP、SMTP などの区別)、コネクションスピード、URL などを基にして、混雑したトラフィックを最適化し、通信量の制御を可能にする装置であり、Packet Shaper などの製品がある。 |
| | **SYN cookies の利用** | SYN cookies を利用して、TCP 接続要求が正当なものであるかどうかを確認する。 |
| サーバ周辺の設備増強 | **負荷分散** | 負荷分散装置等を導入して、サーバの台数を増やす。 |
| | **コンテンツキャッシュサーバの利用** | Web サービスについては、静的コンテンツのキャッシュサーバを設置する。 |
| | **サーバリソースの増強** | サーバのメモリ/CPU といったハードウェアリソースを増強する。 |
| サーバ OS やアプリケーションの調整 | **TCP/IP パラメータの調整** | OS で設定可能な TCP/IP のパラメータ(例えばセッションを維持する時間など)を調整する。OS のパラメータチューニングはアプリケーションやユーザへの影響を考慮する必要がある。 |
| | **HTTP サーバのパフォーマンスチューニング** | Apache 等の HTTP サーバに対するパフォーマンスチューニングを行う。 |
| サーバの負荷低減 | **静的なコンテンツの利用** | Web サービスについては、動的コンテンツをなるべく減らして、静的なコンテンツで置き換えることで、CPU 負荷を軽減する。 |
| | **コンテンツ保存のローカルディスク化** | NAS (Network Attached Storage、ネットワーク接続ストレージ)等を利用し、Web サーバ間でコンテンツを共有している場合は、ローカルディスクにコンテンツを置き、ネットワーク I/O の負荷を減らす。 |
| | **DNS 参照の抑制** | ログ書き込み等のために DNS を参照するプロセスを設けているならば、これを取りやめる。 |
| | **プログラムモジュールの精査** | 余計なプログラムモジュール等を読み込まない。 |

以上の対策は、いずれも実施に当たってガイダンスは豊富であり、比較的実施しやすい。

一部コストのかかるものがあるが、DoS 攻撃の個別の手法に対してはいずれも効果的なものばかりである。3.4 節に示す攻撃手法ごとに、対策の対応状況表 4.4 に整理する。

**表 4.4　サイト側の対策と DoS 攻撃手法の対応**

※　表中の○印は、攻撃に対して効果が期待出来る対策

| DoS 攻撃型 / DoS 攻撃名 / プロトコル / 特徴 / サイト側の対策例 | 帯域幅･リソース消費攻撃 | | | システム資源消費攻撃 | | | |
|---|---|---|---|---|---|---|---|
| | UDP Flood | Smurf | Ping Flood | SYN Flood | Connection Flood | HTTP GET Flood | リロード攻撃（F5 攻撃） |
| | UDP | ICMP | | TCP Connection 確立前 | TCP Connection 確立後 | | |
| | 攻撃者 IP アドレス詐称･特定困難 | | | 攻撃者 IP アドレスは正当<br>正常と異常の判別が困難 | | | |
| FW によるフィルタリング | ○ | ○ | ○ | | | | |
| 帯域制御装置の導入 | ○ | ○ | ○ | | | | |
| SYN cookies 利用 | | | | ○ | | | |
| 負荷分散 | | | | ○ | ○ | ○ | ○ |
| コンテンツキャッシュサーバの利用 | | | | | | | ○ |
| サーバリソースの増強 | | | | ○ | ○ | ○ | ○ |
| TCP/IP パラメータの調整 | | | | | ○ | ○ | |
| HTTP サーバのパフォーマンスチューニング | | | | | | | ○ |
| 静的なコンテンツの利用 | | | | | | | ○ |
| コンテンツ保存のローカルディスク化 | | | | | | | ○ |
| DNS 参照の抑制 | | | | | | | ○ |
| プログラムモジュールの精査 | | | | | | | ○ |

**(5) 外部情報の収集**

実際の攻撃では、企業間あるいは人と企業との関係の中に、攻撃の動機をつくる理由が明確に見出されるケースがあるので、インターネット上での自社の評判や、関係する業界の動向、コミュニティの反応など常時観察しておき、不穏な動きがないかをチェックしておくという対策も考えられる。これは負荷の多い作業であり、必ずしもどの企業にも妥当な対策とは言えないが、そうしたところに原因が見つかることもある。そうした動きを捕捉した中で攻撃があった場合、当事者に連絡を取るなどの対処で事態が収束することも考えられる。通常 DDoS 対策とは対症療法だが、これは原因に直接当たる対応と言える。

**(6) 情報交換や相談のための連絡体制の確立**

ISP との間で定期的な連絡を持ち、できれば信頼出来る担当者を決めて、自社の存在を認識させておく。また、事象の発生時にどのようなことを期待出来るのか、その範囲について見極めておく。また、4.5(2)節に示すセキュリティ専門機関をはじめとした、相談出来る外部の専門家を確保しておく。往々にしてそうした専門家は、事象が発生してから探すことになるが、日頃から自社の環境について認識を持ってもらうのも、非常時の対応に役立つ。また、そうした専門家に、どこまで期待出来るのかについても見極めておく。さらに、事象があって自社のサービス提供に支障が生じた場合、顧客・サービスの利用者及びステークフォルダにどのように告知・連絡するのかを定め、必要ならその手段をあらかじめ確保しておくことも重要である。

**(7) サービス妨害攻撃かどうかの識別**

異常な事象があった場合、それが DoS 攻撃か、単なる混雑や事故の影響かどうかの判別は、意外に難しいところもある(4.8 節を参照)。したがってそうした問題が発生した場合に相談出来る専門家を確保しておくことも重要である。

また、IPA において、DoS 攻撃が疑われる事象に対する相談も受け付けているため、もし身近に相談できる特定の専門家がいない場合には、IPA に相談することが推奨される。

**(8) サービス妨害攻撃の発生後の対応**

事象があった場合に技術的な対応以外に必要なこととして以下がある。

・被害の内容を確定しておくこと。サービスが止められてどういう被害があったか記録しておくこと。被害の記録とは、例えば、次のような事項である。

| |
|---|
| ○妨害された業務は何で、それぞれどのくらい停止したか(停滞したか) |
| ○失われたトランザクションはどのくらいか |
| ○取引量にどのような影響があったのか |
| ○能力が何%落ちたか(前月比や前年同月対比で) |
| ○消費されたコンピュータリソースはどのくらいか |
| ○調査や対応に追われた人件費はどのくらいか |
| ○再発防止のための費用はどのくらいか　など |

こうした記録は、警察に被害届を提出する場合に有用である。

・サービスの停止によって影響が考えられる顧客、サービス利用者には、基本的には十分な情報開示を行うこと。ただし、この点については企業ごとに考え方が異なるので、その方針についてあらかじめ意思決定しておくことが重要である。

・また、特に上場企業ならば、業績への影響をどう見積り、ステークフォルダに説明するのかという観点も重要である。

## 4.8 サービス妨害攻撃を受けたと思われる場合の対処

前節までは各組織等において事前に考慮しておくべき事項を示してきたが、ここでは実際に DoS 攻撃を受けたと思われる場合の緊急対応(インシデントレスポンス)の考え方を示す。

### (1) サービス妨害攻撃かどうかの判断

これまで示してきたように、DoS 攻撃が疑われる状況でも、実際には異なる原因で類似の現象が起きることがある。図 4.4 はそうした、実際には DoS 攻撃ではない現象と本物の DoS 攻撃を区別する方法の例を示したものである。

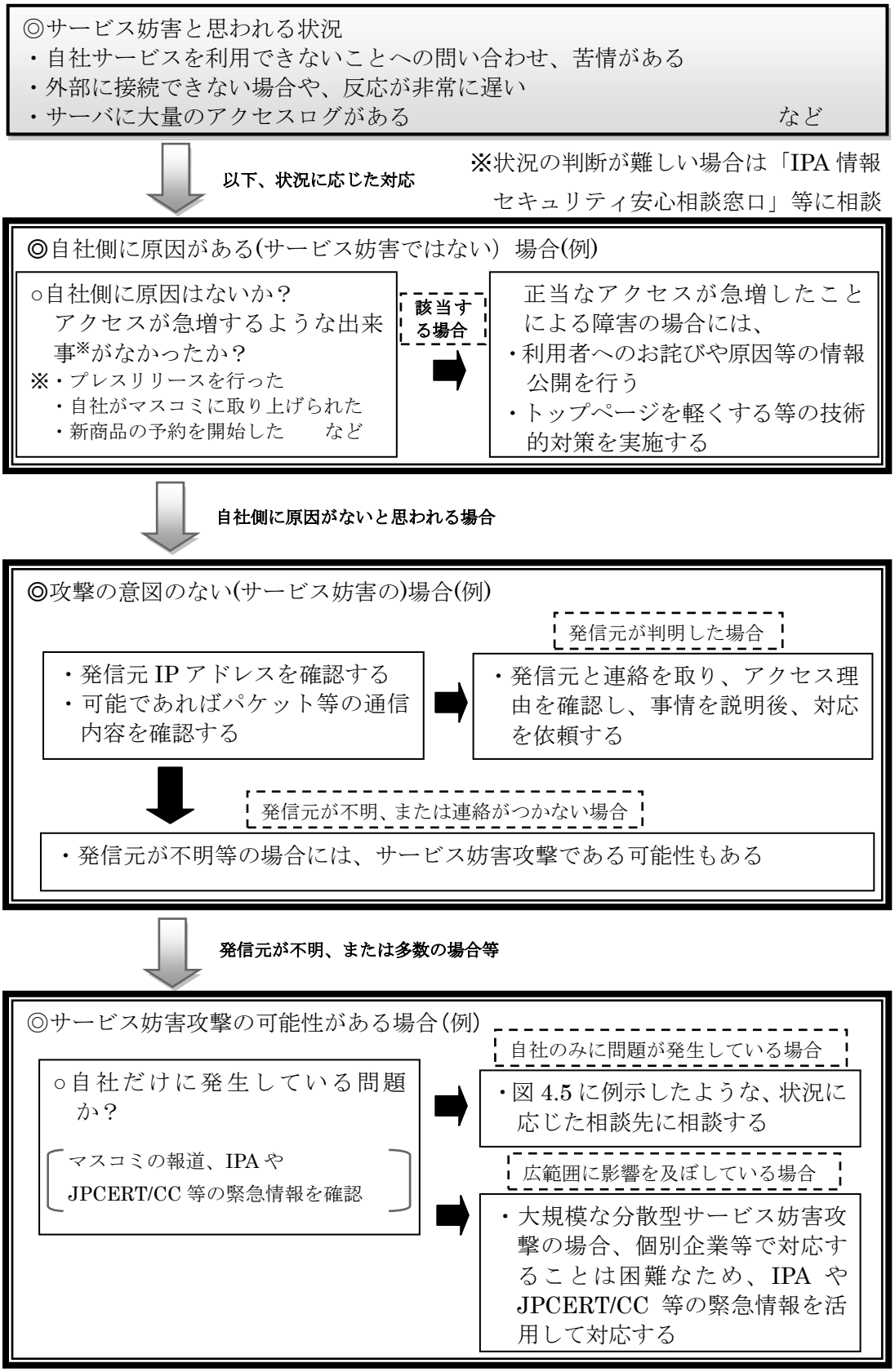


**図 4.4　サービス妨害攻撃判断チャート(例)(再掲)**

### (2) サービス妨害攻撃と考えられる場合の相談先の例

(1)における判断の結果、DoS 攻撃が疑われる場合は、サービスの提供方法に応じて以下に示すような流れに沿って相談や連絡を行うことが望ましい。なお、IPA では情報セキュリティに関して相談窓口を設置しており、広く一般からの相談を受け付けているので、これを利用することも出来る。

#### a. 自社内のサーバ(オンプレミス)でサービスを提供している場合

DoS 攻撃の発信元が特定出来る場合は、その発信側の苦情窓口(Abuse 窓口などと表記される場合がある)に相談するのが有効な場合が多い。発信元が特定出来ない場合は契約 ISP に相談することが考えられるが、一般に ISP では通信内容に応じた対応を行っていないため、有効な対応が出来ない場合も多い。ここで適切な対処が得られず、攻撃が解消されないような場合、日本国内のネットワークに関するインシデントに関する調整の役割を担う、JPCERT/CC への相談を行うことが考えられる。

なお、情報セキュリティに関する十分な知識がない場合や誰に相談するのが適切なのか分からない場合などでは、IPA の総合的な相談窓口に相談することが推奨される。

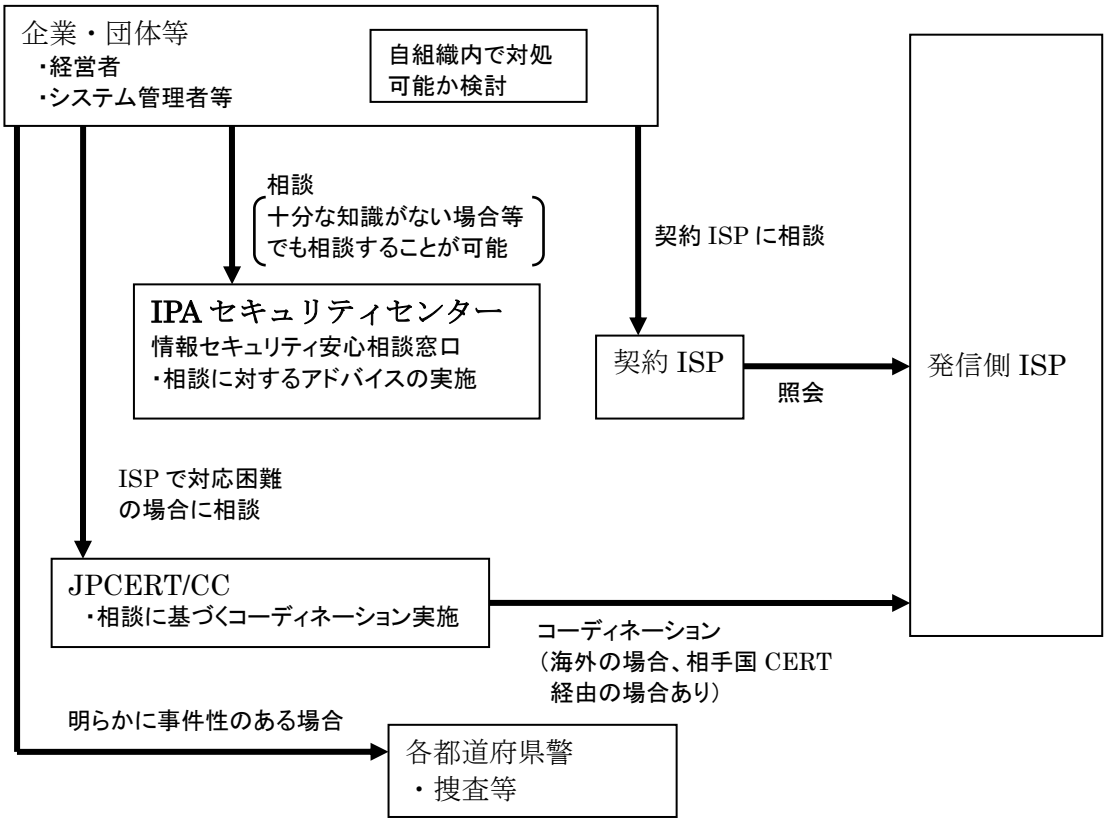


図 4.5　サービス妨害攻撃を受けた場合の相談先(例)(自社サーバの場合)

**b. クラウドやレンタルサーバでサービスを提供している場合**

SaaS、PaaS、IaaS 等のクラウドサービスやレンタルサーバを利用している場合、DoS 攻撃が疑われるときの相談先はクラウド事業者やレンタルサーバの事業者等である。ここで適切な対処が得られず、攻撃が解消されないような場合、日本国内のネットワークに関するインシデントに関する調整の役割を担う、JPCERT/CC への相談を行うことも考えられる。

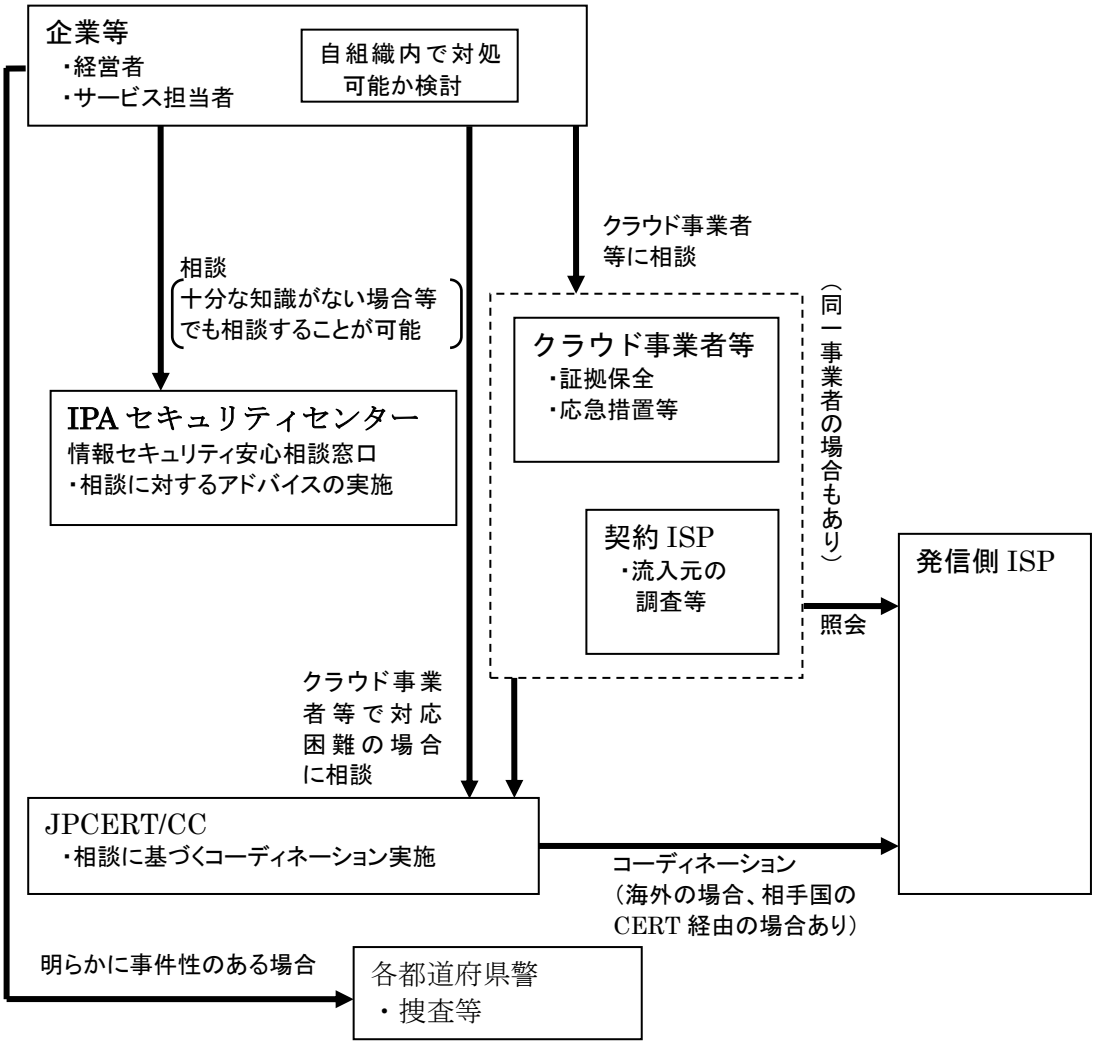


図 4.6　サービス妨害攻撃を受けた場合の相談先(例)(クラウド等の場合)

### 4.9 自らがサービス妨害を行わないための留意事項

これまで説明してきた内容は、企業等が自ら DoS 攻撃の攻撃対象となった場合の対策である。一方で、DoS 攻撃に関しては、攻撃意図を持たずに自社に通常のアクセスをしてくる利用者が DoS 攻撃と同様の結果を生じさせてしまったり、自社から他社へのアクセスが DoS 攻撃と誤解されてしまう可能性がある。こうした状況の発生を防ぐために、企業等で留意すべき事項について説明する。

なお、本節で示す内容は本来の「DoS 攻撃対策」とは異なるので、その旨留意いただきたい。

#### (1) 外部からの攻撃意図のないアクセスがサービス妨害にならないための留意事項

自らの企業等の提供するサービスに対する正当なアクセスが、サービス妨害となってしまわないように対策を行うことは、企業等の社会的責任を果たす上からも重要である。しかしながら、現実には「攻撃」の意図はなくても、サービスを過剰に利用しようとすることで、結果的に他のサービス利用者に対して迷惑を及ぼすような利用者が現れる可能性があり、サービスの公平性や採算性の観点から、このような利用者を対象としたサービス提供の制限についても考慮する必要がある。

以上の内容を踏まえ、留意すべきポイントとして以下の 3 点が挙げられる。

##### a. 需要に応じた処理能力の確保

自ら提供するサービスの需要に応じた処理能力を確保することは、DoS 攻撃への対策以前にサービスの可用性確保の観点から当然必要となる事項である。このとき検討対象となるのは、ピーク時需要に対してどこまで対応すべきかの問題となる。

社内に設置したサーバ等でオンラインショッピング等のサービスを提供するような場合、まれに起こるピーク時の需要にまで対処可能なようにサーバや通信回線を確保しようすると、過剰投資になる恐れがある。しかしながら、ピーク時にアクセス不能となることは、本来のサービス需要を逃すことにつながる。

クラウドでサービスを提供する場合、予め需要のピークがわかっているときは、その期間のみ設備を強化することが容易である場合が多く、こうした需要に応じたリソースの増減の容易性がクラウド利用によるメリットの 1 つとなっている。

##### b. 十分なテストの実施

前項の検討の結果、仕様上は十分な性能を確保したつもりであっても、実装上の問題等により、想定される需要に応えられない場合がある。可能な限り実際の需要に近い形でテストを行い、仕様上の要件を満たすことが出来るかどうかを確認することが望ましい。

**c. 上限に関するサービスレベルの提示**

極めて高頻度のアクセス等、自社で想定しているサービスの利用方法にあてはまらないような使い方(主にサービスの過剰利用)をする利用者への対処についても検討する必要がある。特に、マッシュアップなどの利用方法が進むことで、今後こうした利用者が増加する可能性がある。このような利用者の需要にも可能な範囲で対応すべきところであるが、一般的な利用者とのリソースの利用状況が極端に異なる場合で、利用状況に応じたコスト負担も期待出来ないような状況であれば、サービスの採算性の観点から制限を加えることも必要になる。この場合、対策の候補としては以下のような方法が考えられる。

- サービスの提供条件を契約書やマニュアル、利用開始時の承諾事項等の中に表記する。
- 一定の制限範囲を超えた時点で警告の画面を表示する。
- 一定の制限範囲を超えた時点でエラーとなるようにする。

**(2) 自組織からの外部へのアクセスがサービス妨害にならないための留意事項**

(1)とは逆に、自組織から外部のサービスへのアクセスについて、相手方から DoS 攻撃であるとみなされる可能性がある。こちらについても、マッシュアップ的な利用の進展により、これまでは考えられなかったサービスにおいても、サービス妨害的な影響を及ぼす機会が増えることが懸念される。

外部の企業等のサービスに連携して利用しようとする場合、まず先方のサービス提供条件を確認し、その範囲内で利用するようにすべきである。これにより、自らが DoS 攻撃の「加害者」とみなされるリスクを回避することが出来る。

## 4.10 ＜参考＞海外における分散型サービス妨害攻撃対策の事例

4.2 節から 4.5 節では、主に国内における DDoS 攻撃対策の環境について示したが、海外では大規模の DDoS 攻撃に直面して、主要な事業者あるいは政府機関はどのような対処がとられたのかについての事例には、以下のようなものがある。

・米国

2.3.4 節に示した韓国と米国に対する DoS 攻撃の事例では、大手の CDN(Contents Delivery Network ,4.5(3)を参照)事業者である Akamai 社によって、CDN のインフラを利用して、米国に対する DDoS 攻撃のトラフィックを効果的に封じ込めることに成功した。韓国からの攻撃であったため、韓国側に近いポイントで攻撃を防ぎ、政府系機関への攻撃を防ぐことが出来た。その一方で、一般の ISP は、折悪しく建国記念日に前後していたため対応に遅れた例が報告されている。

・韓国

上記の事例に対して韓国では以下の動きがあった。

韓国放送通信委員会から ISP に対する通信遮断依頼が行なわれたが、一部の ISP のみ対策を実施した。また、攻撃を受けたサイトから接続元情報をもらい、個別に abuse 対策スキームを発動して、ボットマシンを持つ個人ユーザに個別に連絡しマルウェア駆除を依頼した。大手 ISP4 社だけ数日間で 8 万台から駆除がなされたという。これにはマスコミによる情報流通も強く影響していると見られる。

・エストニア

2.3.1 節に示すエストニアにおける事例では CERT から提供された、攻撃の内容と攻撃元の IP アドレスに関する情報を持って、エストニア国内への通信の遮断を行なった。このアドレスには少数ながら日本のものもあったという。

・グルジア

2.3.2 節に示すグルジアの事例では、対策に必要な情報が提供されなかったため、ISP による対策はできなかった。

## 第5章 まとめ(企業等が担うべき役割)

DoS 攻撃の中には、2.3 節で示したように国家のレベルやネットワークの広域にわたって実施されるものがあり、このような攻撃に対しては 2007 年のエストニアの事例と同様、個別企業等の立場では対策の施しようがない場合もある。しかしながら、このような規模のものだけでなく、特定の一企業を標的とした攻撃や、攻撃を装った詐欺なども存在する。さらに、企業等が脆弱性等に関する情報セキュリティ対策を怠ることで、サーバが乗っ取られて DoS 攻撃に用いられるボットネットの一部として悪用される可能性もある。他の脅威と同様、DoS 攻撃対策においても、企業等が当事者意識をもち、主体的に対策を検討・実施していくことが重要である。

以下に、企業等における対策の検討に際して留意すべきポイントを示す。

### (1) 自組織で利用しているサーバをボットにさせない

これはいかなる組織であっても遵守すべき最低限の事項といえる。第 3 章で示したように、DoS 攻撃の攻撃効果を高めているのは、DDoS 攻撃に用いられるボットネットであり、これを構成しているボットは脆弱性が放置されている一般のサーバ群である。よって、自組織で利用しているサーバをボット化させないよう、既知の脆弱性への対策や異常の確認等を定期的に実施することは、DoS 攻撃の効果を抑制するための社会的責任の観点から必須の事項である。

### (2) サービス妨害攻撃を考慮した対策の実施

1.2 節で示したように、DoS 攻撃の中には、脆弱性を突く種類のものがある。(1)への対策と合わせて既知の脆弱性への対策を行うことで、こうした DoS 攻撃の影響を抑制することが出来る。もう 1 種類の DoS 攻撃(「真正の DoS 攻撃」)のうち、コンピュータやネットワークに過剰な負荷をかけるものについては、特に DDoS の場合には、例え大企業であっても、どんな攻撃にも万全と言える対策を取ることは難しいのが実情である。攻撃の規模で圧倒しようとする働きかけに、やはり規模で対抗しようとする試みは、どんな場合にでも万全な対策とは言えない。

ただし、自前で用意出来るサービス資源が限定される中小企業などが、自前ではなくクラウドを利用することで、ある規模以下の DoS 攻撃に対抗出来る可能性は生まれる。

特定企業を対象とする DoS 攻撃への対策については、第 4 章で示したように、サービス妨害かどうかの確認や相談方法等について、予め検討・準備しておくことが主体となる。こうして準備をしておくことで、実際に攻撃を受けたときに効率的かつ間違いを起こしにくい対策の実施が可能となる。

### (3) サービスの需要に応じた性能の提供

4.9 節で示したように、自組織で提供するサービスの需要に応じた処理能力を提供出来な

いことで、実質的に DoS 攻撃と同様の状況を招く恐れがある。DoS 攻撃対策ではないが、こうした可能性にも留意することで、サービスの品質を高め、顧客満足度の向上をもたらすことが可能になる。

**(4) 攻撃の検出**

サーバ類では記録を適切に取得、保存し、その記録の中から、異常な通信量の発生や過負荷状態を実時間で検出出来るようにすること。異常を検知した時には、保存されている記録から、その発生原因となった通信の特性(IP アドレス、ポート、量など)を可能な限り特定する。一般に DDoS 攻撃によって発生した通信は、IP アドレスの詐称や接続数の多さなどにより、膨大な量になる。多くの記録を解析し、DoS 状態の原因となる通信を分別するための手法を日頃より持つことが望ましい。

**(5) 外部組織との連携**

攻撃を受けた際に相談することができ、ともに解決策を検討、実施することの出来る外部組織と、日頃より関係を持つこと。利用している ISP やセキュリティベンダなどがこれにあたる。また、IPA の総合的な相談窓口の存在と連絡方法(情報セキュリティ安心相談窓口　http://www.ipa.go.jp/security/anshin/)、JPCERT/CC に代表される中立的な組織の存在と連絡方法なども把握しておくことが推奨される。

DDoS 攻撃に IP アドレスの詐称が行われたり、攻撃の通信量が回線容量を超えるような場合には、ISP に調査協力や対処を依頼することが必要となる。一方で、ISP では関連法規や設備上の条件などにより、調査や対策に制限が加わることがあることを理解する必要がある。特に通信の遮断に関しては、通信当事者からその依頼をする必要があるので注意が必要である。

また、外部組織に調査や対策を依頼する場合には、攻撃を受けた事実を伝えるだけではなく、自社で把握した攻撃の概要(先の IP アドレス、ポート、量など)や、対策の方針などについて、協力を要請する相手に適切に伝えないと協力してもらえない場合もある。JPCERT/CC のインシデント報告フォーム(http://www.jpcert.or.jp/form/)などを参考に、どのような情報を開示し、どのような依頼を行うかを事前に検討しておくことが望ましい。

さらに、インターネット上の攻撃では、攻撃者と被害者の間に複数の ISP が介在することが通常であり、攻撃を特定の ISP だけでは解決出来ない場合も多い。この際、被害者が接続している ISP からみてすぐ隣の ISP や、攻撃者を収容する ISP などに連絡を取ることになる。また、CSIRT に対策を依頼する場合でも同様に、他の ISP に連絡を取って対策を行う。したがって、ISP や CSIRT 組織に対策を依頼する場合には、攻撃の発生の事実やそ

の技術的特徴について、他の組織に開示する許可を与える必要がある。

## 参考文献


[1] 【OGC 2010】ある日脅迫状が届いたら・・・Maru-Jan の DDoS 攻撃への対応実例, 2010/02/19, http://www.inside-games.jp/article/2010/02/19/40525.html

[2] 【注意喚起】企業のホームページを狙った DDoS 攻撃を伴うネット恐喝行為について(プレスリリース), 株式会社ラック,2008/5/15, http://www.lac.co.jp/news/press20080515.html

[3] ACCS vs Antinny――DDoS との戦いに終わりはあるか,IT media,2004/12/03, http://www.itmedia.co.jp/enterprise/articles/0412/03/news026.html

[4] 2004 年 DDoS 攻撃対策事例(プレゼンテーション文書), 財団法人日本データ通信協会テレコム・アイザック推進会議,2004/12/13 http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/jise_ip/pdf/041213_1_s3_4.pdf

[5] DoS/DDoS 対策について, 警察庁技術対策課, 平成 15 年 6 年 3 日

[6] ITmedia エンタープライズ:「金を出さなければ DoS 攻撃」と脅迫、ロシアで 3 人逮捕, 2004/07/22 19:17 更新, http://www.itmedia.co.jp/enterprise/articles/0407/22/news071.html

[7] 朝日新聞 2010 年 8 月 21 日夕刊(東京版).

[8] 情報ネットワーク法学会:第 1 回「技術屋と法律家の座談会」岡崎市立中央図書館へのアクセスは DoS 攻撃だったか? http://in-law.jp/bn/2010/index-20100716.html

[9] 岡崎市立図書館事件に見るネットと法執行機関のズレ:賢人たちのリレーコラム セキュリティ「言いたい放題」, http://pc.nikkeibp.co.jp/article/column/20100901/1027224/

[10] 私的セキュリティポリシを利用した NGN における DoS 対策の考察, 西川 康宏, 岡田 康義, 佐藤 直, SCIS 2009.

[11] インターネットサーバーの安全性向上策に関する調査報告書, 情報処理振興事業協会, セキュリティセンター, 平成 15 年 3 月.

[12] 情報セキュリティ投資に対する企業の意志決定, 藤原正弘, KDDI R&A, 2006 年 11 月第 2 号.

[13] コンピュータウイルス等有害プログラムの法的規制に関する国際動向調査, 高橋郁夫法律事務所, 情報処理振興事業協会, 2000 年 6 月.

[14] サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」, 経済産業省, 2002 年. http://www.meti.go.jp/policy/netsecurity/downloadfiles/Cybercriminallawreport.pdf

[15] 情報セキュリティの法律, 岡村久道著, 商事法務, 2007 年.

[16] Internet Infrastructure Review, Vol.8, August, 2010. http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf

[17] Internet Infrastructure Review, vol.7, May, 2010.

http://www.iij.ad.jp/development/iir/pdf/iir_vol07.pdf
[18] マークアウレル・エスター＆ラルフ・ベンツミュラー(岸本眞輔・瀧本往人 訳) “G Data White Paper 2009　アンダーグラウンドエコノミー-”
[19] 「シマンテックアンダーグラウンドエコノミーレポート 2007 年 7 月~2008 年 6 月の傾向」、2008 年 11 月発行
[20] 「ビジネス化がさらに加速するサイバー攻撃～進化し続けるアンダーグラウンドビジネス」、LAC CSL レポート、初版 2008 年 8 月 20 日
[21] 小規模サイト管理者向けセキュリティ対策マニュアル,独立行政法人情報処理推進機構,2003/5
http://www.ipa.go.jp/security/awareness/soho/soho.html
[22] ACCS 殿の「攻撃者に対する注意喚起」に向けた取組み, Telecom-ISAC Japan News Release 2006/02/20,https://www.telecom-isac.jp/news/news20060220.html
[23] ISP との連携による ANTINNY ウイルス感染ユーザへの注意喚起の取り組み, Telecom-ISAC Japan News Release 2006/03/15,
[24] https://www.telecom-isac.jp/news/news20060315.html
[25] Telecom-ISAC Japan、Malware 対策に関してマイクロソフト社と協力, Telecom-ISAC Japan News Release 2005/10/12,
[26] https://www.telecom-isac.jp/news/news20051012.html
[27] Telecom-ISAC Japan、マイクロソフトと共同し Malware 対策で成果, Telecom-ISAC Japan News Release 2005/11/21,
[28] https://www.telecom-isac.jp/news/news20051121.html
[29] ボット対策プロジェクト「サイバークリーンセンター」からみた国内のマルウェア対策(<特集>マルウェア), 有村浩一, 情報処理, Vol.51, No.3, 275—283
[30] 企業における情報セキュリティ事象被害額調査, 独立行政法人情報処理推進機構,2006/11
http://www.ipa.go.jp/security/fy17/reports/virus-survey/index.html
[31] Facts about e-Estonia, Estonian Informatics Centre.
http://www.ria.ee/27525
[32] ユーロトレンド 2009.8, JETRO, 2009.
http://www.jetro.go.jp/jfile/report/07000120/0908R5.pdf
[33] Lessons from the cyberattacks on Estonia, Lauri Almann, Government Computer News, 13 June 2008.
http://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?Page=1
[34] 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの策定について(プレスリリース)

http://www.jaipa.or.jp/info/2007/info_070530.html
[35] 事業継続計画策定ガイドライン(企業における情報セキュリティガバナンスのあり方に関する研究会 報告書 参考資料),経済産業省,2005/6
http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

# 付録

## 略語一覧

| | |
|---|---|
| DDoS | Distributed Denial of Service |
| DoS | Denial of Service |
| ISP | Internet Service Provider |
| DNS | Domain Name System |
| CIO | Chief Information Officer 最高情報責任者 |
| CTO | Chief Technical Officer　最高技術責任者 |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| PV | Page View |
| SaaS | Software as a Service |
| PaaS | Platform as a Service |
| IaaS | Infrastructure as a Service |

DoS 攻撃に関する主な情報源

- JPCERT コーディネーションセンター(JPCERT/CC)

  http://www.jpcert.or.jp/

  大規模な DoS 攻撃に関する緊急情報の提供を行う。

**【注意】**

**本報告書中でも述べているように、大規模な DoS 攻撃が行われた場合、インターネット経由での情報収集が難しくなる可能性がある。**

- 国内に幅広く攻撃が行われている場合は、テレビ・ラジオ・新聞等のマスメディアでその旨が報道されている可能性が高い。また、この場合、最寄りの ISP までは接続出来る可能性があるので、契約している ISP の Web サイトで状況を確認することは試す価値がある。携帯電話によるインターネット接続の場合も、携帯電話事業者のサイトにはアクセス出来る可能性が高い。
- 自社のサイトへの攻撃や、自社で利用しているサーバ(クラウド等を含む)に限定した攻撃の場合は、攻撃に用いられている通信経路以外、例えば携帯電話による接続を利用するなどで情報収集を行うことが出来る。

JVN で公表したサービス妨害攻撃の脆弱性に関する情報

IPA 及び JPCERT コーディネーションセンター(JPCERT/CC)で運営している、Japan Vulnerability Notes(JVN) で公表されている、「サービス運用妨害(DoS)の脆弱性」※に関する情報(2010 年 9 月時点、17 件)を以下に示す。

これらは「情報セキュリティ早期警戒パートナーシップ」に基づき IPA が届出を受け、JPCERT/CC が調整を行い、製品開発者が修正を行った脆弱性である。

※JVN では、DoS を「サービス運用妨害」としている。

なお以下には、脆弱性に関する概要、影響を受けるシステム、想定される影響等の情報にとどめているが、参照先 URL では、対策方法、ベンダからの関連情報、IPA からの参考情報及び関連文書のリンク等が設けられている。

| | |
|---|---|
| URL | http://jvn.jp/jp/JVNDD18AD07/index.html |
| タイトル | JVN#DD18AD07<br>Tomcat におけるサービス拒否の脆弱性 |
| 公開日 | 2005/03/14 |
| 概要 | Java Servlet 又は Java Server Pages のサーバ実装である Apache Tomcat には遠隔から第三者によってサービス不能 (Denial-of-Service, DoS) 状態を引き起こされる脆弱性が確認されています。 |
| 影響を受けるシステム | Apache Jakarta Tomcat Version 3.x |
| 詳細情報 | |
| 想定される影響 | サービス不能状態 (Denial-of-Service, DoS) に陥る可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN29273468/index.html |
| タイトル | JVN#29273468<br>QRcode Perl CGI & PHP scripts におけるサービス運用妨害の脆弱性 |
| 公開日 | 2005/07/28 |
| 概要 | QR コードの画像を作成するためのツール QRcode Perl CGI & PHP scripts には、サーバ上のリソースを過剰に消費してしまう脆弱性が存在します。特定のリクエストによって、サーバリソースを使い果たし、クライアントからの要求に 応答できなくなり、当該サーバ上で動作しているほかのプロセスにも影響を及ぼす可能性があります。 |
| 影響を受けるシステム | QRcode Perl/CGI & PHP scripts ver. 0.50f 及びそれ以前( Perl 版, PHP 版ともに該当します) |
| 詳細情報 | |
| 想定される影響 | サービス運用妨害（Denial-of-Service, DoS）状態を引き起こされる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN23727054/index.html |
| タイトル | JVN#23727054<br>Pochy におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2005/08/25 |
| 概要 | Microsoft Windows 環境で動作する電子メールクライアントソフト Pochy は、特定の文字列を受信した場合に、CPU 負荷が高いまま処理が停止し、サービス運用妨害（DoS）状態になる問題があります。 |
| 影響を受けるシステム | Pochy 0.2.1a |
| 詳細情報 | |
| 想定される影響 | 遠隔から第三者がこの問題を悪用することで、Pochy 利用者に対し、特別に作成したメールを送信することでサービス運用妨害（DoS）攻撃を行える可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN18282718/index.html |
| タイトル | JVN#18282718<br>Hyper Estraier におけるディレクトリトラバーサル/サービス不能の脆弱性 |
| 公開日 | 2005/10/28 |
| 概要 | 全文検索システムの Hyper Estraier には、インデックスファイルを作成する処理に脆弱性が存在します。 |
| 影響を受けるシステム | Hyper Estraier Version 1.0.1 以前(Windows 版のみ) |
| 詳細情報 | |
| 想定される影響 | 遠隔の第三者から不正に細工されたファイルを送付され、それを検索対象ディレクトリに保存した場合、インデックス作成時に、検索対象外のファイルがインデックスに登録されたり、サービス不能状態になる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN98836916/index.html |
| タイトル | JVN#98836916<br>複数の Wiki クローン製品におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2006/07/03 |
| 概要 | ウェブブラウザを利用してウェブサーバ上の文書を編集する機能を持ついくつかの Wiki クローン製品には、特定のリクエストを処理する際に CPU 資源やメモリを多量に消費する問題があります。 |
| 影響を受けるシステム | FreeStyleWiki<br>Hiki<br>Wiki もどき |
| 詳細情報 | |
| 想定される影響 | 遠隔の第三者により、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN30994815/index.html |
| タイトル | JVN#30994815<br>MyODBC 日本語変換機能版におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2006/11/06 |
| 概要 | MyODBC は、ODBC 対応アプリケーションから MySQL データベースへの接続を中継する、オープンソースの ODBC ドライバです。MyODBC 日本語変換機能版は、ソフトエイジェンシー社が日本語文字コードの変換機能を追加した Windows 向けのバージョンです。<br><br>MyODBC 日本語変換機能版には、特定の文字列を含むレスポンスを受け取るとサービス運用妨害（DoS）状態になる脆弱性があります。 |
| 影響を受けるシステム | MyODBC 日本語変換機能版 バージョン 3.51.06, 2.50.29, 2.50.25<br><br>なお、MyODBC 日本語変換機能版はすでに開発及びメンテナンスが終了しております。MySQL 4.1 以降では文字コードの自動変換機能がありますので、MySQL 4.1 以降を利用することを推奨します。 |
| 詳細情報 | |
| 想定される影響 | 遠隔の第三者から MySQL データベースに特定の文字列を登録されることにより、利用者のマシンがサービス運用妨害（DoS）状態となる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN84798830/index.html |
| タイトル | JVN#84798830<br>Ruby の CGI ライブラリ cgi.rb におけるサービス運用妨害 (DoS) の脆弱性 |
| 公開日 | 2006/12/04 |
| 概要 | Ruby 言語の標準ライブラリである cgi.rb には、サービス運用妨害 (DoS) 状態になる脆弱性が存在します。 |
| 影響を受けるシステム | ・ 1.8 系<br>1.8.5 以前の全てのバージョン<br>・ 開発版(1.9 系)<br>2006-12-04 以前の全てのバージョン |
| 詳細情報 | |
| 想定される影響 | 遠隔の第三者から特定のリクエストを受信することにより、サーバがサービス運用妨害 (DoS) 状態となる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN77414947/index.html |
| タイトル | JVN#77414947<br>サイボウズ Office におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2007/12/11 |
| 概要 | サイボウズ Office には、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 影響を受けるシステム | サイボウズ Office 6.6 (1.3) 及びそれ以前 |
| 詳細情報 | グループウェアであるサイボウズ Office には、細工された HTTP リクエストを適切に処理出来ないために、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者によって、サーバがサービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN36635562/index.html |
| タイトル | JVN#36635562<br>nProtect：Netizen におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2008/06/25 |
| 概要 | nProtect：Netizen には、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 影響を受けるシステム | nProtect：Netizen Ver5 の npstarter.ocx が「2008, 6, 16, 1」より前のバージョン |
| 詳細情報 | ネットムーブ株式会社が提供する nProtect：Netizen は、特定のホームページで通信を行う間だけ起動させるセキュリティソフトです。<br>nProtect：Netizen には、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 想定される影響 | ユーザが細工されたウェブページを閲覧することで、nProtect：Netizen が起動できなくなる、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN66077895/index.html |
| タイトル | JVN#66077895<br>ウイルスセキュリティ及びウイルスセキュリティ ZERO におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2008/08/12 |
| 概要 | ソースネクストが提供するウイルスセキュリティ及びウイルスセキュリティ ZERO には、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 影響を受けるシステム | ウイルスセキュリティ バージョン 9.5.0173 及びそれ以前<br>ウイルスセキュリティ ZERO バージョン 9.5.0173 及びそれ以前 |
| 詳細情報 | ソースネクストが提供するウイルスセキュリティ及びウイルスセキュリティ ZERO はウイルス対策ソフトです。ウイルスセキュリティ及びウイルスセキュリティ ZERO には、ファイルのスキャン処理において細工された圧縮ファイルを適切に処理出来ないために、サービス運用妨害（DoS）状態となる脆弱性が存在します。 |
| 想定される影響 | 細工された圧縮ファイルを当該製品でスキャンした場合、当該製品が機能しなくなり、以降のファイルのスキャンなどが行われなくなる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN87272440/index.html |
| タイトル | JVN#87272440<br>Apache Tomcat におけるサービス運用妨害(DoS)の脆弱性 |
| 公開日 | 2009/06/09 |
| 概要 | The Apache Software Foundation が提供する Apache Tomcat には、サービス運用妨害(DoS)の脆弱性が存在します。 |
| 影響を受けるシステム | ・ Apache Tomcat 4.1.0 から 4.1.39 まで<br>・ Apache Tomcat 5.5.0 から 5.5.27 まで<br>・ Apache Tomcat 6.0.0 から 6.0.18 まで<br>開発者によると、現在サポート対象外となっている Apache Tomcat 3.x、4.0.x、及び 5.0.x も、本脆弱性の影響を受ける可能性があるとのことです。 |
| 詳細情報 | The Apache Software Foundation が提供する Apache Tomcat は、Java Servlet と JavaServer Pages のサーバ実装です。<br>Apache Tomcat は、Java AJP コネクタ経由で送られた不正なヘッダを含むリクエストを処理する際、エラーを返さず AJP との接続を切断します。その際、コネクタが mod_jk lb ワーカである場合はエラー状態となり、約 1 分間利用不可能となります。その結果、サービス運用妨害(DoS)攻撃などに使用される可能性があります。 |
| 想定される影響 | 遠隔の第三者により不正なリクエストを送られることで、サービス運用妨害(DoS)攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN87239696/index.html |
| タイトル | JVN#87239696<br>iPhone OS におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2009/06/18 |
| 概要 | Apple が提供する iPhone OS には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 影響を受けるシステム | iPhone OS 1.0 から 2.2.1 まで<br>iPhone OS for iPod touch 1.1 から 2.2.1 まで |
| 詳細情報 | Apple が提供する iPhone OS には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者により不正なリクエストを送られることで、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN75368899/index.html |
| タイトル | JVN#75368899<br>IPv6 を実装した複数の製品にサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2009/10/26 |
| 概要 | Internet Protocol version 6 (IPv6) を実装した複数の製品には、<br>サービス運用妨害（DoS）の脆弱性が存在します。 |
| 影響を受けるシステム | IPv6 を実装している製品が本脆弱性の影響を受ける可能性があります。 |
| 詳細情報 | IPv6 を実装した複数の製品には、Neighbor Discovery Protocol (RFC4861) に関連したパケットの処理に問題があります。細工されたパケットの処理に起因するサービス運用妨害（DoS）の脆弱性が存在します。 |
| 想定される影響 | ネットワーク内の同一リンク上に存在する悪意ある第三者によって送信された大量のパケットを受信することで、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN13011682/index.html |
| タイトル | JVN#13011682<br>SEIL/X シリーズ及び SEIL/B1 におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2009/10/28 |
| 概要 | SEIL/X シリーズ及び SEIL/B1 には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 影響を受けるシステム | SEIL/X1 firmware 2.30 から 2.51 まで<br>SEIL/X2 firmware 2.30 から 2.51 まで<br>SEIL/B1 firmware 2.30 から 2.51 まで |
| 詳細情報 | SEIL/X シリーズ及び SEIL/B1 は、ルータ製品です。SEIL/X シリーズ及び SEIL/B1 には、NAT 機能の内部処理に起因するサービス運用妨害（DoS）の脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者により細工されたパケットを送られることで、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN90872372/index.html |
| タイトル | JVN#90872372<br>WebSAM DeploymentManager におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2010/05/17 |
| 概要 | WebSAM DeploymentManager には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 影響を受けるシステム | 以下の製品から「クライアントサービス for DPM」をインストールしたサーバもしくは端末が本脆弱性の影響を受けます。<br>WebSAM DeploymentManager Ver5.13 及びそれ以前<br>また、対象の WebSAM DeploymentManager は下記製品の一部としても提供されており、同様に本脆弱性の影響を受けます。<br>SigmaSystemCenter 2.1 Update2 及びそれ以前<br>BladeSystemCenter 全バージョン<br>ExpressSystemCenter 全バージョン<br>VirtualPCCenter 2.2 及びそれ以前 |
| 詳細情報 | WebSAM DeploymentManager は、ソフトウェアの配布管理を行うための製品です。WebSAM DeploymentManager には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者により、「クライアントサービス for DPM」をインストールしているサーバもしくは端末において、OS のシャットダウン、又は再起動を行われる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN82749282/index.html |
| タイトル | JVN#82749282<br>CapsSuite Small Edition PatchMeister におけるサービス運用妨害 (DoS) の脆弱性 |
| 公開日 | 2010/05/17 |
| 概要 | CapsSuite Small Edition PatchMeister には、サービス運用妨害 (DoS) の脆弱性が存在します。 |
| 影響を受けるシステム | 以下の製品から「クライアントサービス for PTM」をインストールしたサーバもしくは端末が本脆弱性の影響を受けます。<br>CapsSuite Small Edition PatchMeister Ver2.0 Update2 及びそれ以前 |
| 詳細情報 | CapsSuite Small Edition PatchMeister は、セキュリティパッチの適用管理を行うための製品です。CapsSuite Small Edition PatchMeister には、サービス運用妨害 (DoS) の脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者により、「クライアントサービス for PTM」をインストールしているサーバもしくは端末において、OS のシャットダウン、又は再起動を行われる可能性があります。 |

| | |
|---|---|
| URL | http://jvn.jp/jp/JVN86832361/index.html |
| タイトル | JVN#86832361<br>Microsoft Windows におけるサービス運用妨害（DoS）の脆弱性 |
| 公開日 | 2010/08/13 |
| 概要 | Microsoft Windows には、サービス運用妨害（DoS）の脆弱性が存在します。 |
| 影響を受けるシステム | Windows Vista<br>Windows Vista x64 Edition<br>Windows Server 2008<br>Windows Server 2008 for x64-based Systems<br>Windows Server 2008 for Itanium-based Systems<br>Windows 7<br>Windows 7 for x64-based Systems<br>Windows Server 2008 R2 for x64-based Systems<br>Windows Server 2008 R2 for Itanium-based Systems |
| 詳細情報 | Microsoft Windows には、IPv6 拡張ヘッダの処理に起因するサービス運用妨害（DoS）の脆弱性が存在します。 |
| 想定される影響 | 遠隔の第三者により細工された IPv6 パケットを送られることで、サービス運用妨害（DoS）攻撃を受ける可能性があります。 |

お問い合わせ先


独立行政法人 情報処理推進機構セキュリティセンター

URL：http://www.ipa.go.jp/security/

〒１１３－６５９１ 東京都文京区本駒込２丁目２８番地８号

（文京グリーンコートセンターオフィス）

本報告書は以下のURLからダウンロード可能です。

URL： http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html