# SQAT® Security Report

2025-2026年 秋冬号

## DDoS攻撃に警戒する
## 防御策および“踏み台”にされないためには

知る・守る
続ける

BBSecは内閣サイバーセキュリティセンターの
「サイバーセキュリティ普及啓発」に賛同しています

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

# ごあいさつ

株式会社ブロードバンドセキュリティ
取締役兼 セキュリティサービス本部 本部長　齊藤 義人

サイバー攻撃のニュースを目にしない日は、もはや珍しくありません。2025年上半期も、その傾向は変わりませんでした。

国内では、損害保険会社のWebシステムが不正アクセスを受け、最大で1,700万件超の顧客情報が閲覧可能となったとされる事案が発生し、社会的な関心を集めました。また、証券口座の認証情報がダークウェブ上で売買される事例も報告され、個人情報の流出と不正利用リスクの現実性が改めて浮き彫りになっています。いずれも、長年にわたって組織を悩ませてきた脅威であり、日々の備えや基本的な対策の見直しが、今なお重要であることを再認識させられる出来事でした。

一方で、サイバー攻撃の様相はおそろしい速度で変化を遂げており、昨今では「地政学リスク」や「AI技術を活用した攻撃」が大きく注目を集めています。サイバーリスクは、単なる“技術的な問題”にとどまらず、政治的・社会的文脈と密接に結びついた複雑な現象として捉える必要があることが、改めて浮き彫りとなりました。国家間の緊張がサイバー空間にも波及している状況は、IPAが発表した「情報セキュリティ10大脅威2025」にも反映されており、現実的なリスクとして意識され始めています。また、AIを悪用した攻撃も深刻さを増しており、フィッシング攻撃を自動化するマルウェア「Darcula Suite」や、生成AIを用いて作成された精巧な偽メールが、検出をすり抜ける事例も確認されています。さらにはAIを悪用するだけでなく、AIそのものが標的となることも想定しなくてはなりません。自律的に外部サービスへアクセスするAIエージェントを狙った攻撃手法である「EchoLeak」はMicrosoft 365 Copilotの脆弱性（CVE-2025-32711）を悪用し、悪意のあるメールを受信するだけでAIが機密情報を外部へ送信してしまう危険性を示しました。
サイバー攻撃の進化に対応していくためには、最新の動向に継続的に目を向けることが欠かせません。本レポートが、皆さまの対策検討の一助となれば幸いです。

**一般社団法人　日本ハッカー協会主催**
**「Hack Fes. 2025」の様子（2025年7月開催）**

専門知識を学んだり、スキルを磨いたりするためのセキュリティエンジニア対象のイベント「Hack Fes. 2025」に弊社は協賛企業として参加しました。

※写真は弊社撮影。撮影および掲載許可を得ています。

# CONTENTS

＜巻頭企画＞
**DDoS攻撃に警戒する**
**防御策および“踏み台”にされないためには ――― 02**

＜注目テーマ＞
**セキュリティは『監視』から『理解』へ ～ヒューマンセンシングと画像処理が拓く、人に寄り添うデジタル社会～**
**秋田大学 情報データ科学部教授　景山 陽一様 寄稿記事 ――― 08**

**診断の現場から ――― 13**

＜情報セキュリティコラム＞
**2025年上半期ランサムウェアをめぐる概況 ――― 15**

＜現状分析＞
**診断結果にみる情報セキュリティの現状**
**～2025年上半期　診断結果分析～ ――― 17**

**カテゴリ別脆弱性検出状況 ――― 19**

**業界別診断結果レーダーチャート ――― 21**

**※本レポートは、弊社セキュリティサービス本部のホームページ**
**「SQAT®.jp（URL：https://www.sqat.jp/）」**
**https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。**

SQAT.jp

※ 本誌において記載されている会社名、商品名、サービス名は各社の商標又は登録商標です。なお、本文中では商標又は登録商標を表すマークを特に提示していない場合があります。

この冊子は、クリエイティブ・コモンズ表示4.0ライセンスの下に提供しております。
二次利用にあたっては、出典明示（出典：株式会社ブロードバンドセキュリティ発行『SQAT® Security Report 2025-2026年 秋冬号』）をお願いします。
また、商用利用は許諾しておりません。

SQAT®はBBSecの登録商標です。登録商標第5146108号

巻頭企画

# DDoS 攻撃に警戒する

## 防御策および“踏み台”にされないためには

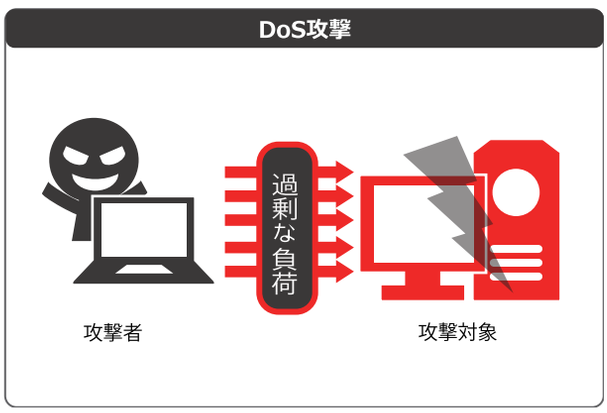
SQAT® Security Report 編集部

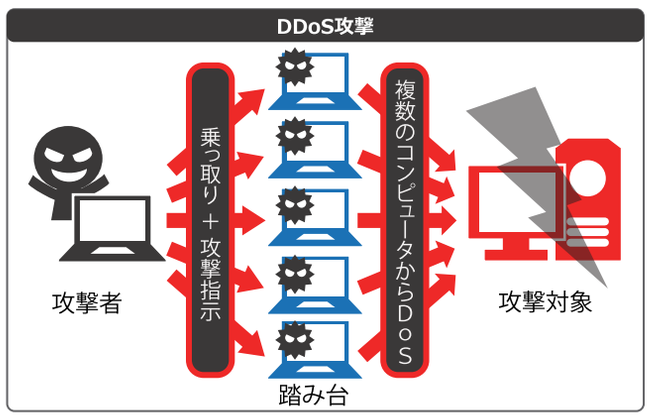
近年は社会全体のデジタル化が進んでおり、万博やオリンピック等の国際的なイベントもデジタル化による恩恵を受けている。インターネットを介してイベントの最新情報を入手したり、観戦チケット等を予約したりといった利便性が向上しているものの、攻撃者にとっては有名なイベントは格好の機会なのか、サイバー攻撃も確認されている(*1)。よって、デジタル化による利便性の向上の背景に潜む脅威についても認識しておかなければならない。そこで過去に国際的なイベントで確認された攻撃のうちの「DDoS攻撃」に注目したい。注目の理由としては、本誌執筆時点(2025年夏)に「2025年大阪・関西万博」が開催されたことや、2024年末から2025年の頭にかけて日本企業をターゲットとしたDDoS攻撃が相次いだこと(*2)、IPA(独立行政法人情報処理推進機構)の「情報セキュリティ10大脅威 2025」(組織編)で、DDoS攻撃が前回の圏外から浮上してきたこと(*3)を総合してのことである。

## ■DoS攻撃およびDDoS攻撃とは

DoS攻撃（Denial of Service attack）とは、Webサービスを提供するサーバなどに対して、単一の攻撃源から過剰なアクセスやデータ送信を行うことで負荷をかけ、対象のサーバなどをダウンさせるサイバー攻撃のことである。サーバダウンにより、そのサーバが提供しているWebサービスや機能を提供できなくすることが目的である。

DoS攻撃を複数の攻撃源から大量に行うことを、DDoS攻撃（Distributed Denial of Service attack）という。



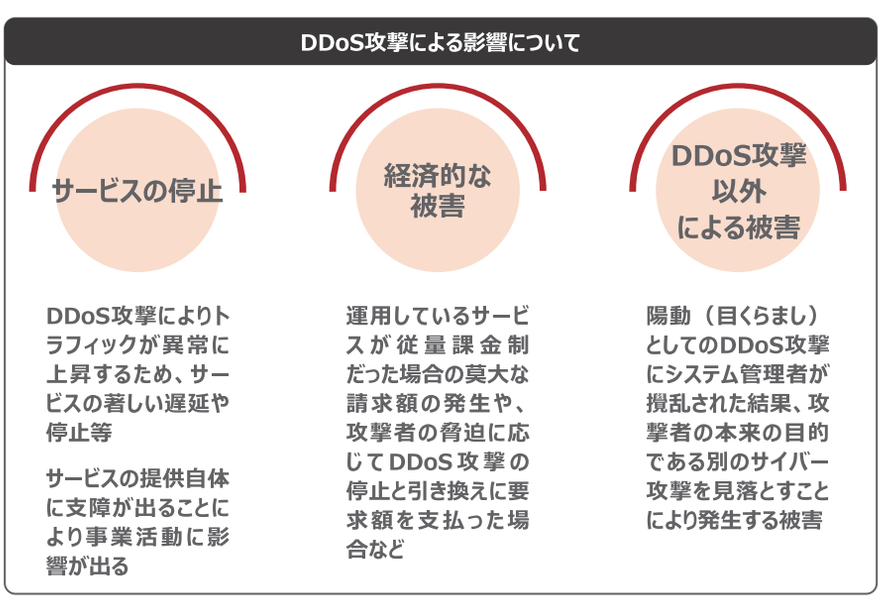




## ■DDoS攻撃の特徴

前掲の図「DDoS攻撃」のとおり、攻撃者は往々にして攻撃者所有のコンピュータではないコンピュータを乗っ取り、DDoS攻撃に利用する。攻撃者がマルウェアに感染させるなどしてDDoS攻撃に利用する他者のコンピュータのことをボット、もしくは踏み台という。また、ボット、踏み台を介した攻撃のことを踏み台攻撃という。踏み台にされていることに気付かずに加害者になってしまう危険性があるのが、DDoS攻撃の厄介なところである。なお、攻撃者が踏み台にしようと狙うのはコンピュータに限らない。ネットワークカメラなどのIoT機器を狙うこともある。過去にはMiraiとよばれるマルウェアが猛威を振るい、多数のIoT機器が踏み台となったDDoS攻撃によって、文章投稿系のSNSや世界的知名度がある動画配信サービスなどにアクセスできなくなった事例がある。

## ■DDoS攻撃の影響

サービス提供者がDoS攻撃およびDDoS攻撃を受けた場合、サービス停止によって機会損失や信用失墜の可能性がある。例えばECサイトであれば、攻撃によりサーバダウンが起こることでユーザがWebサイトを表示できなかったり、商品を購入できなかったりするようになる。結果としてユーザがそのECサイトから離脱してしまうことが考えられる。下記の「DDoS攻撃による影響について」に記載したように、ほかにも攻撃の被害は起こりうるし、さまざまな影響を及ぼしかねない。次頁からは攻撃の被害や影響をより想像しやすくするべく、攻撃事例を挙げる。



## ■2024年末から短期間に頻発した攻撃について

ここで本企画の冒頭で述べた、2024年末から2025年の頭にかけて日本企業をターゲットとしたDDoS攻撃が相次いだ件に触れたい。航空事業者・金融機関・通信事業者等に対するDDoS攻撃が相次いで発生しているとして、内閣サイバーセキュリティセンター（NISC）は、2025年2月4日付で「DDoS攻撃への対策について（注意喚起）」を公開した（*2）。NISCが注意喚起をするに至ったであろう攻撃について、該当の時期に弊社が追っていた報道や情報をもとに右記にまとめた（*4）。

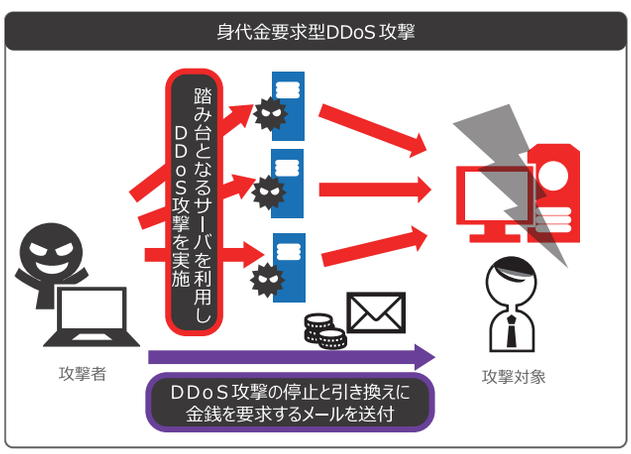
| 日付 | 被害企業・組織 | 対象システム |
|---|---|---|
| 2024年12月26日 | 航空会社 | 手荷物預かりシステム |
| 2024年12月27日 | 銀行A | ネットバンキング |
| 2024年12月28日 | 銀行B | ネットバンキング |
| 2024年12月31日 | 銀行C | ネットバンキング |
| 2025年1月2日 | 情報通信会社 | 決済サービス、ポータルサイト、インターネットサービスプロバイダ |
| 2025年1月5日 | 一般財団法人 | 気象情報Webサイト |
| 2025年1月6日 | クレジットカード会社 | 会員用インターネットサービス |
| 2025年1月6日 | 銀行D | ネットバンキング |

組織名は伏せているが、攻撃はいずれも大規模な事業者へのもので、短期間に集中している。いずれもサービスが一時的に停止したことによる信用失墜やブランド毀損は免れることができなかっただろう。なお、報道によれば直接的な金銭の要求は無かったとされている。さらに次項からは金銭の要求も確認されたDDoS攻撃の事例について述べていく。

## ■複数の金融機関への攻撃事例

海外の金融機関へ向けた、攻撃の停止と引き換えに金銭を要求するメールが送られたDDoS攻撃の事例を挙げる（*5）。以下に本稿で注目したい概要を抜粋して記す。

少し前の事例ではあるものの攻撃を想定しやすいように思うのと、同じような手口や派生した高度な手口が使われることもありえるため、事前の対策をしたり、緊急の対処をしたりするうえで知っていると有用であると考え、本件を事例として挙げている。




出典：JPCERT/CC「Web サイトへのサイバー攻撃に備えて」
「(2) 脅迫を伴った DDoS 攻撃や Anonymous による DDoS 攻撃」より引用
https://www.jpcert.or.jp/newsflash/2017080101.html

事例は海外のものだが、対岸の火事と捉えるのは得策ではない。JPCERT/CC（JPCERTコーディネーションセンター）が類似の相談を受けたという点においては、日本向けにも同様の攻撃があった可能性が高いためである。

**＜概要＞**
**●中国や韓国の証券会社や銀行など複数の金融機関を対象としたDDoS攻撃。**
**●Armada　Collectiveを名乗る攻撃グループからDDoS攻撃の停止と引き換えに金銭を要求するメールが送られた。**
**●JPCERT/CCも類似の攻撃について相談を受けていた。**

**＜攻撃グループからの脅迫メールに記された攻撃内容や要求＞**
**●期限までに支払いが無ければDDoS攻撃を実行する。**
**●要求は仮想通貨ビットコイン10BTC（当時300万円ほど）で、期限を過ぎた場合は要求額を1日ごとに10BTCずつ増やす。**
**●金銭を支払うかどうかは別として脅迫メール到着後に15分間攻撃をする（実際に攻撃があった）。**
**●攻撃は並外れた攻撃力がある（防ぐことは困難であると言いたい内容）。**

脅迫メールに記載のとおり手始めに15分間攻撃があった点と、ある程度の規模がありそうな金融機関のWebサービスを停止させる攻撃力があった点からは、金銭の支払いに確実に応じさせたいという攻撃者の意図を感じる。とはいえ、金銭を支払っても攻撃が止まる保証が無いため、金銭を支払うことは推奨されない。実際に、身代金要求型のDDoS攻撃を受けて、金銭を支払っても攻撃が止まらなかった例もある（*6）。また、仮に金銭を支払って一時的に攻撃が止まったとしても、攻撃が再開されて更なる金銭を要求されることもあり得る。