

# 組織・団体のサービス停止を狙うサイバー攻撃 「DDoS（ディードス）攻撃」に警戒を！

年末年始にかけ、複数の金融機関に「DDoS攻撃」が原因とみられるネットワーク障害が発生し、インターネットバンキングが利用できないなどの混乱が発生しました。

また、航空業界や通信業界にも同じくDDoSと思われる攻撃が観測されましたが、これらは決して対岸の火事ではなく、全ての組織・団体がターゲットとなっています。

本レポートでは、「DDoS攻撃」とは何かについて、説明します。



## ▶ DDoS攻撃とは？

「DDoS攻撃」はDistributed Denial of Serviceの略で分散型サービス拒否攻撃とも呼ばれます。攻撃対象のサーバーに対し、複数のコンピュータから集中的にアクセスを行うことで、サーバーに負荷をかけて、サービスの提供を妨害するものです。

ちなみに、1台のコンピュータからの攻撃は、「DoS攻撃（Denial of Service）」です。

## ▶ DDoS攻撃を受けるとどうなるか？

運営しているウェブサイトが「DDoS攻撃」を受けると、サイトが通常行うサービスが行えなくなるほか、サイトへのアクセスができなくなるため、顧客離れや信用失墜などにつながるおそれがあります。

反対に、利用しているウェブサイトが「DDoS攻撃」を受けると、そのサイトのサービスが使えなくなり、情報入手できない、買い物ができないなど、不便を強いられます。

## ▶ DDoS攻撃への対応、対策は？

### ① 海外に割り当てられたIPアドレスからの通信の遮断

→ 攻撃元IPアドレスは、約99%が海外に割り当てられたIPアドレスです。

### ② CDN、WAFの導入

→ コンテンツ配信ネットワークによる配信の高速化とアクセス負荷の軽減、サイバー攻撃の検知・遮断するサービスの利用を検討します。

### ③ IPアドレスごとにアクセス回数を制限

→ 特定のIPアドレスに制限をかけたり、1つのIPからのアクセス回数に制限をかけます。

### ④ セッションのタイムアウト時間を短く設定

→ 長時間セッションを占有する通信を切断することで、負荷を軽減します。

埼玉県警察公式YouTubeチャンネルにおいて、当課作成の「DoS攻撃」解説動画を公開中です。ぜひご覧ください！

<https://www.youtube.com/watch?v=zqpR7C6mMvo>



## バックナンバー公開中！

過去のサイバーセキュリティレポートは、埼玉県警察ホームページに掲載しています。

ぜひご覧ください。

<https://www.police.pref.saitama.lg.jp/c0070/kurashi/cyber-security-report.html>

