

サイバー攻撃の概要



サイバー攻撃とは、

◎ サイバーテロ

重要インフラの基幹システムを機能不全に陥れ、社会機能を麻痺させる電子的な攻撃

◎ サイバインテリジェンス

又は、サイバーエスピオナージ

情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取する攻撃

の総称です。

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着している中、**サイバー攻撃対策は非常に重要なものとなっています。**

★ 重要インフラとは、他に代替することが著しく困難なサービスを提供する事業者ことで、**クレジット、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、情報通信、医療、水道、物流、化学、石油、港湾の15分野**をいいます。

サイバー攻撃には

- ◎ 攻撃の実行者の特定が難しい
- ◎ 被害が潜在化する傾向がある
- ◎ 国境を超えて実行される

といった特徴があります。



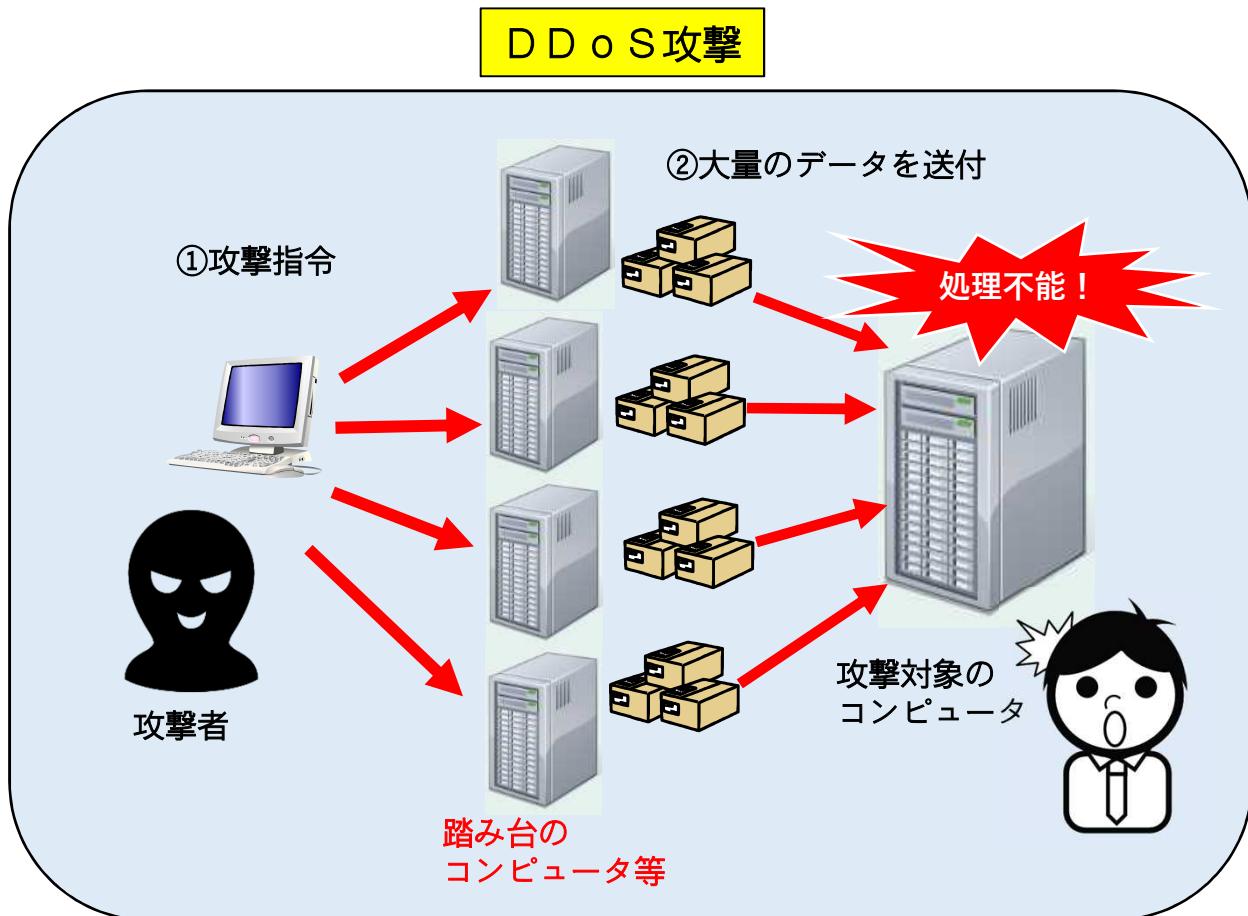
攻撃者は、一般の皆さんのパソコンなどを狙った攻撃も行い、乗っ取ったパソコンを悪用しようとします。

サイバー攻撃について正しく理解し、セキュリティに関する知識を深めましょう。



サイバーテロの主な手口

攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にする攻撃を「**DDoS攻撃**」といいます。



DDoS攻撃が重要インフラの基幹システムに対して行われると、サービスの提供が不能になります

- ◎ 交通機関が利用できなくなる
- ◎ 金融機関のシステムが停止する
- ◎ 病院の診療ができなくなる

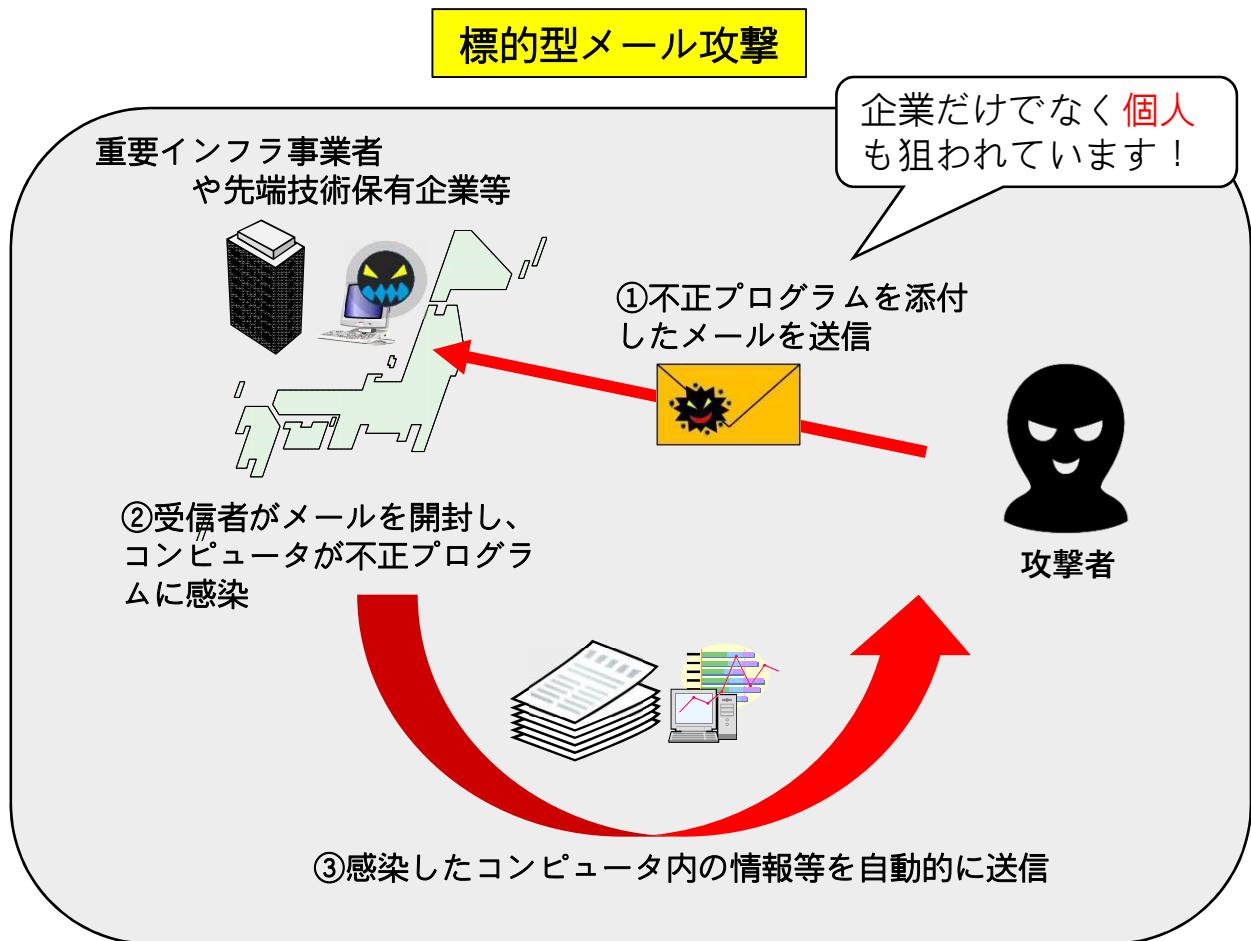
など、**私たちの生活に多大な影響を及ぼすことになります。**



攻撃者は、皆さんが自宅で使用しているパソコンや、防犯カメラ等のIoT機器を「踏み台」として悪用します！
自宅等で使用している機器の設定を確認しましょう！

サイバーインテリジェンスの主な手口

業務に関連した正当な電子メールを装い、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メールを送信し、受信者のコンピュータを不正プログラムに感染させるものを「標的型メール攻撃」といいます。



標的型メールは、電子メールだけでなく、
・SMS
・メッセージアプリ
・ゲーム等のメッセージ機能
からも送信されてきます。

ウェブブラウザに
パスワードを保存して
いて、端末が不正
プログラムに感染した
場合、パスワードを
窃取されるリスク
が上がります。

推測されにくいパス
ワードの設定や、
2段階認証等を活用
しましょう。

