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

◎　**サイバーインテリジェンス**

　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生活活動に不可欠な社会基盤として定着している中において、**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のことで、**情報通信**、**金融**、**航空**、**空港**、**鉄道**、**電力**、**ガス**、**政府・行政サービス**、**医療**、**水道**、**物流**、**化学**、**クレジット**、**石油**の１４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

◎　国境を容易に超えて実行される

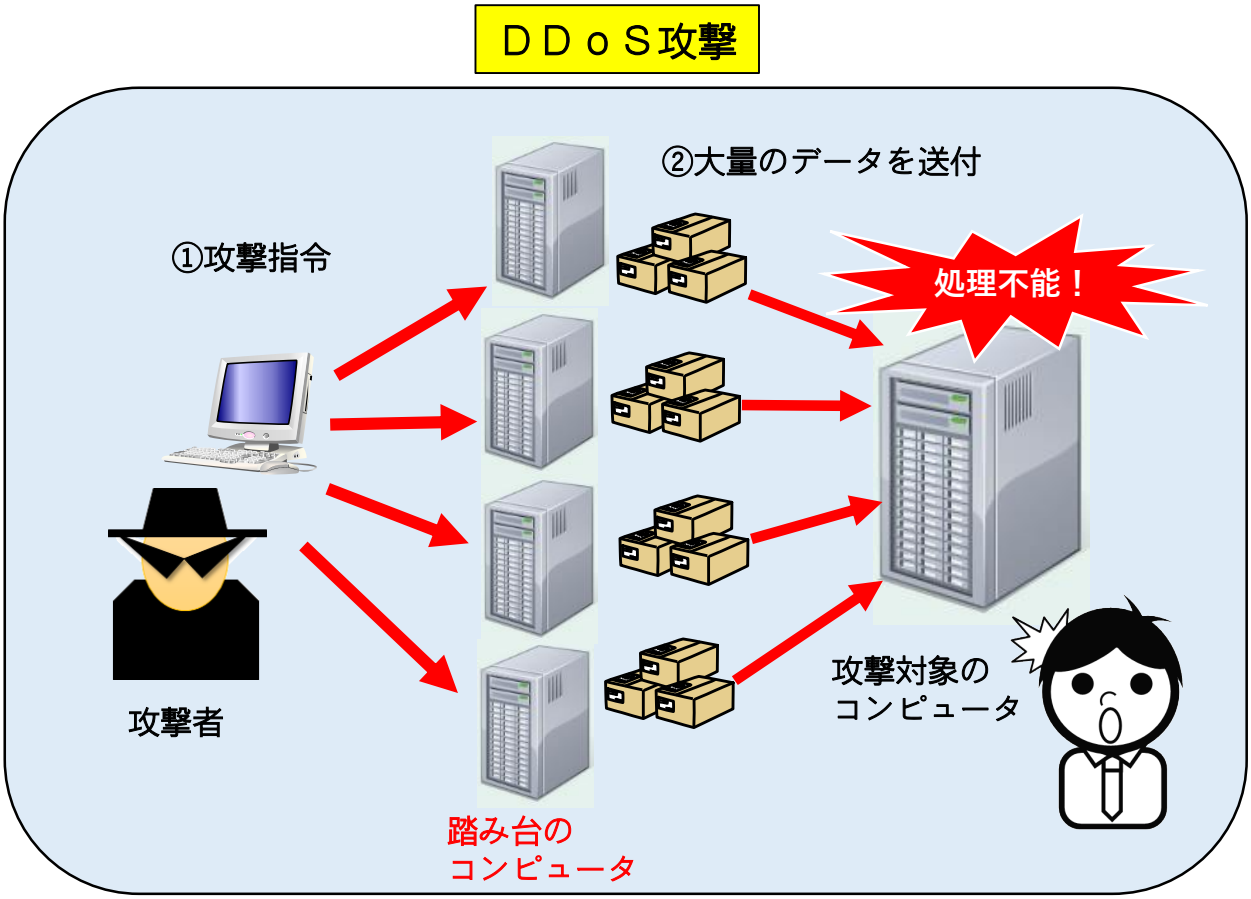
といった特徴があります。

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

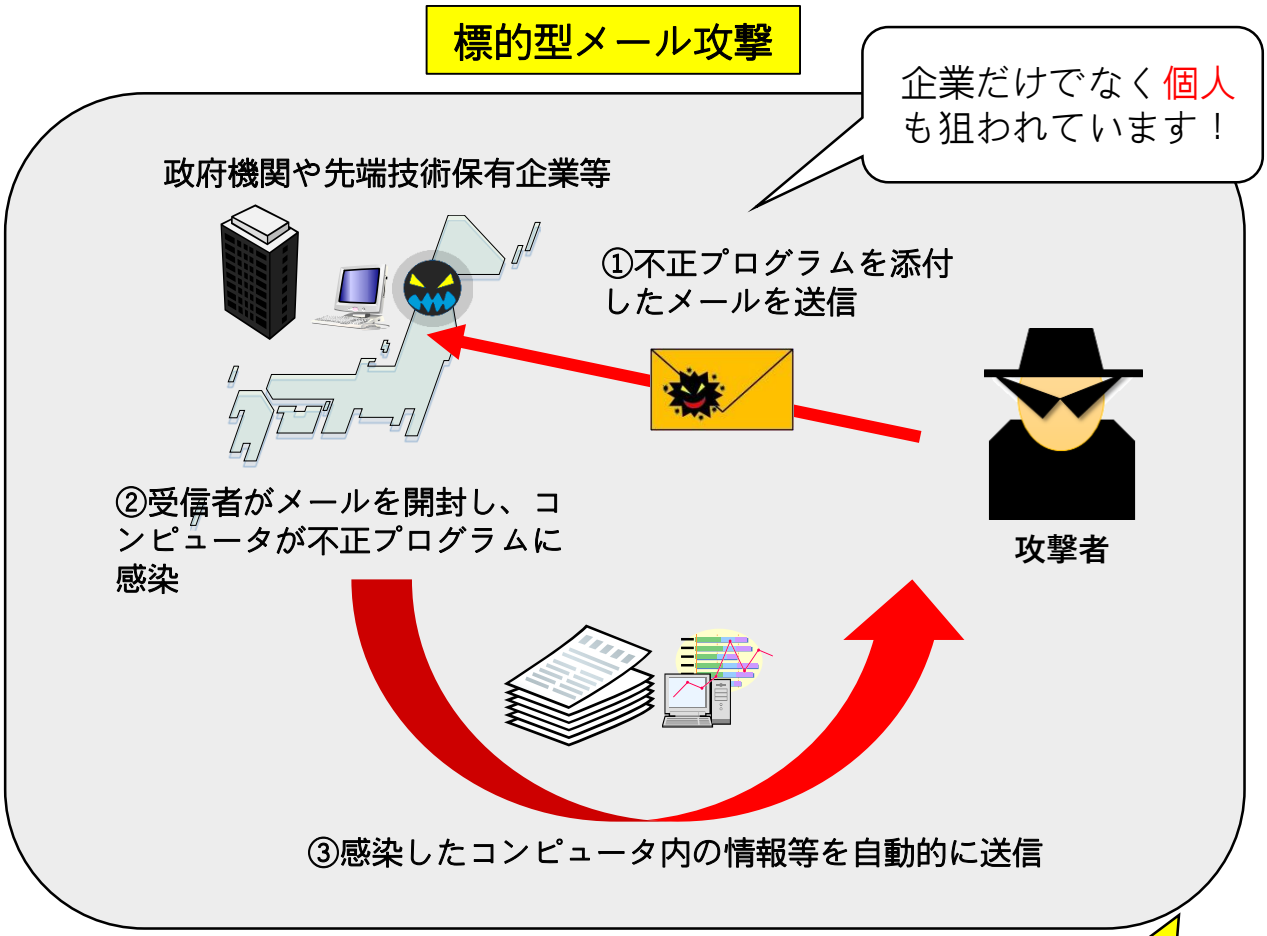
◎　交通機関が利用できなくなる
◎　金融機関のシステムが停止する
◎　病院の診療ができなくなる

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、一般の皆さんのパソコンを狙ってウイルス付きメールを送信し、ウイルス感染させて乗っ取り、「踏み台」として悪用します！

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。



攻撃のターゲットが頻繁に閲覧するウェブサイトを改ざんし、サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる「水飲み場型攻撃」も発生しています。

水飲み場攻撃の由来は、攻撃者をライオン、ターゲットを獲物、ターゲットがよく見るウェブサイトを水飲み場に例えたもので、ライオンが水飲み場に現れる獲物を待ち伏せする様子から名づけられました。