



サイバーセキュリティの置き薬

2022年
第13号

サイバー攻撃に注意！



国内外において政府機関やインフラ事業者に対するサイバー攻撃が発生しています。

重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させてしまうサイバー攻撃の脅威は、国の治安や安全保障にも影響を及ぼしかねません。

サイバー攻撃の手口としては、

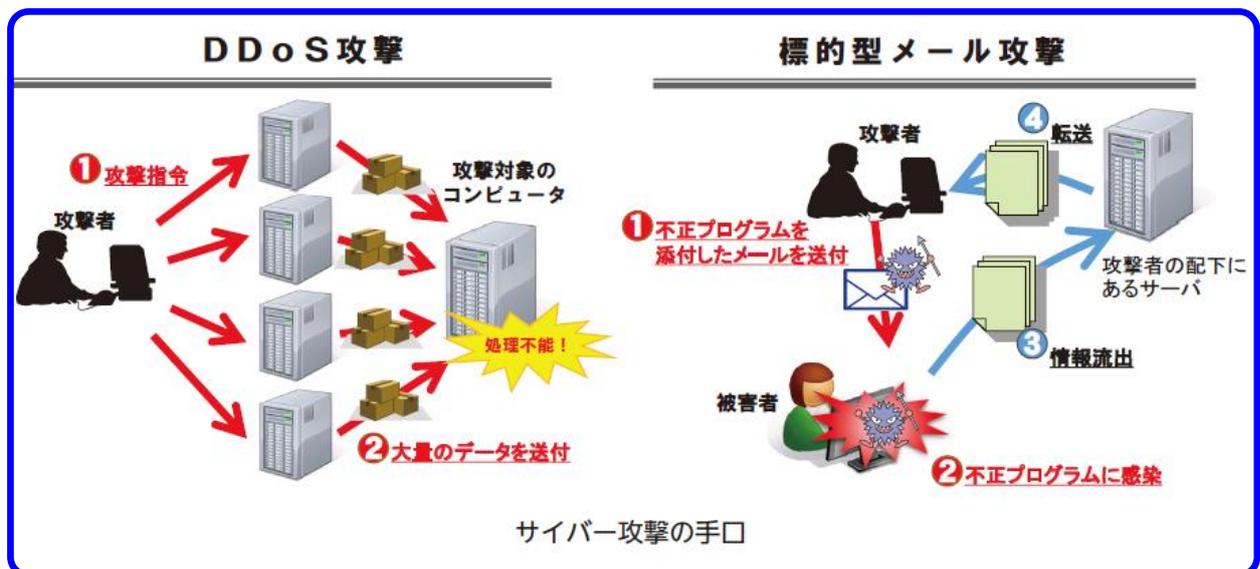
- DDoS 攻撃（攻撃対象のコンピュータに複数の端末から一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にさせる手口）
- 標的型メール攻撃（機密情報や知的財産の窃取を目的として、特定の企業や個人を「標的」にフィッシングや不正プログラムを添付したメール等を送信する手口）

などがあり、我が国においても多数発生しています。

DDoS 攻撃に対しては、「WAF」等のセキュリティ製品を導入するなどの対策が重要です。

※WAF…Web Application Firewall の略。

不正アクセスを検出して遮断したり、IPS やファイアウォールで防げない部分をカバーして防御する機能がある。



また、ランサムウェアや Emotet による被害を防止するため、

- セキュリティソフトを導入する
- OS やソフトウェアを常に最新の状態に更新する
- メールの添付ファイル、本文中の URL リンクに注意する
- 重要なデータを定期的にバックアップする

等の基本的なセキュリティ対策を徹底してください。

ウェブサイトへ接続できなくなった、ウイルスに感染したなどの場合には、警察への速やかな通報をお願いします。

