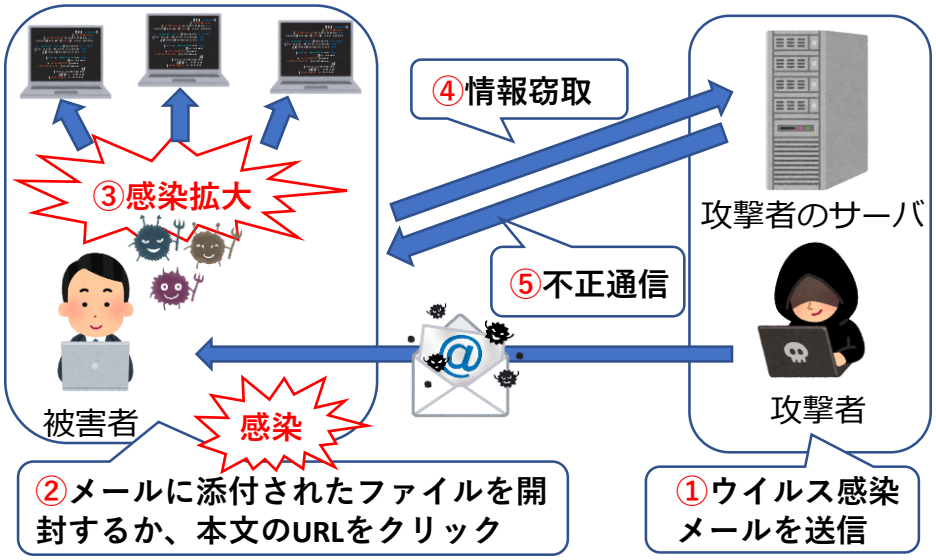
# 組織・団体の機密情報を狙うサイバー攻撃
# 「標的型攻撃メール」に要注意！

標的型攻撃メールは、企業や組織・団体を対象にした標的型攻撃の手口の一つです。
攻撃者はターゲットへ巧妙に作りこまれたメールを送信し、内部への侵入を試み、機密情報の窃取やデータの改ざん、システムの破壊を狙います。
本レポートでは、「標的型攻撃メール」によるウイルス感染の流れや対処方法等について、説明します。

## ▸標的型攻撃メールによるウイルス感染の流れ




①攻撃者がウイルス感染メールを送信
②被害者が添付ファイルを開封するか、本文のURLをクリック
③PCがウイルス感染し、組織内に感染拡大
④感染したPCが外部と不正な通信を開始し、機密情報等を窃取
⑤窃取した情報によって、データの改ざんやシステムの破壊

## ▸標的型攻撃メールの対処方法

**①ＬＡＮケーブルを抜く。**
→被害拡大を防ぐため。
**②添付ファイルを開かない、URLのリンクをクリックしない。**
→コンピュータウイルスへの感染を防ぐため。
**③端末の電源は切らない。**
→揮発性情報（電源を切ると内容が消えてしまう情報）の保全や事後調査のため。
**④速やかに自組織のセキュリティ担当に報告する。**
→被害拡大を防ぐため。

不審メールを見付けたら、担当者に連絡を！

## 標的型攻撃メール訓練をやってみませんか？

埼玉県警では、標的型攻撃メールを模したメールを送信する標的型攻撃メール訓練を実施しています。組織・団体のサイバーセキュリティ意識向上にお役立てください。詳細は、下記までお気軽にお問合せを！


埼玉県警本部生活安全部サイバー局
サイバー対策課　対策・官民連携係
☎048-832-0110


もちろん無料です