# 脆弱性対策情報の悪用に注意

（企業の情報セキュリティ担当者向け）

OS やソフトウェアに脆弱性が見つかった場合、開発した企業から修正プログラムが提供されますが、脆弱性対策情報が公開されても対策を講じないまま放置すると、攻撃者に狙われ、サイバー攻撃を受ける可能性があります。

修正プログラムが公開されていない脆弱性（**ゼロデイ脆弱性**）に比べ、公開されている脆弱性（利用者が修正プログラムを適用するまでの間を「**Nデイ脆弱性**」という。）を悪用することは、攻撃者が自ら脆弱性を見つける必要がないため、攻撃が容易となります。

近年では、脆弱性情報の公開後、攻撃コード（有害な動作を行うプログラム）が流通し、攻撃が本格化するまでの時間が短くなっているため、早急に対策を講じることが必要不可欠です。

## ○ 攻撃手口

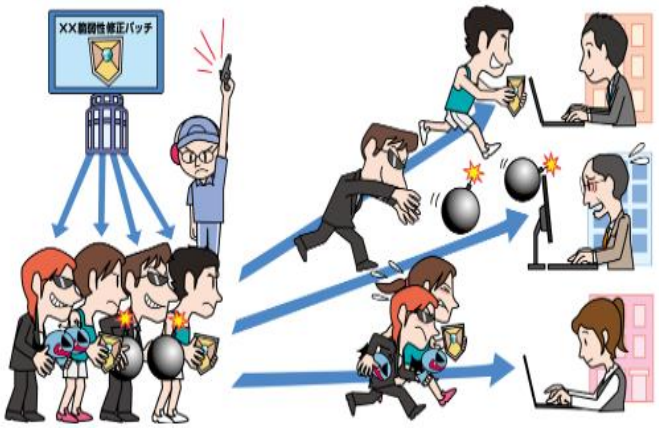
● **公開された脆弱性情報を悪用して攻撃する。**

脆弱性対策情報が公開された直後に、脆弱性を狙うことを意図して作られた攻撃ツールをインターネット上から入手し攻撃する。

オープンソースのツールに脆弱性を利用する機能が実装されている場合があり、それを悪用することもある。

● **対策が未実施又は実施までに時間を要している相手を狙う。**

脆弱性対策情報が公開されてから、利用者が修正プログラムを適用するまでの間に存在する脆弱性（**Nデイ脆弱性**）を悪用する。




（出典　IPA 独立行政法人情報処理推進機構）

## 対策

● **速やかに修正プログラムを適用しましょう。**

修正プログラムが公開されてから、できるかぎり速やかに同プログラムを適用することが重要です。

平素から OS やソフトウェアはアップデートし、常に最新の状態を保ってください。

Wi-Fiルーターのファームウェアや IoT機器も同様に、最新の状態を保ちましょう。

● **修正プログラムが公開されているかどうかを確認しましょう。**

最新の OS がサポートしていないソフトウェアの中には、サポート期間が終了したため、脆弱性が発見されても修正プログラムが公開されないものもあります。

サポート期間が終了していないソフトウェアを使用してください。

● **アカウントを適切に管理しましょう。**

IDやパスワードの使い回しはせず、利用する各サービスのアカウントごとに、長く複雑なパスワードを設定してください。

利用頻度の低いサービスや不要なサービスのアカウントは、削除してください。

【参考】 IPA 独立行政法人情報処理推進機構(情報セキュリティ 10 大脅威 2021[組織編]) https://www.ipa.go.jp/files/000089239.pdf

岩手県警察本部サイバー犯罪対策課の公式ツイッターはQRコードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

**岩手県警察本部生活安全部サイバー犯罪対策課**

**令和4年1月 26 日発行**

@Iwate_cyber