

金融機関などを  
装った

偽メールに

ご注意ください!

## フィッシングメールの特徴

特徴① 》「利用停止」、「サービス利用停止」等、不安を煽る、緊急を装う

特徴② 》URL等のリンクからフィッシングサイトへ誘導

### 金融機関を装ったメールの例

【〇〇銀行】お客様の口座をセキュリティ強化のため、一時利用停止しております。再開手続きをお願い致します。

<https://●●●●●●●●>

### 通信事業を装ったメールの例

【重要】お客様がご利用の電話料金が大変高額となっております。ご確認が必要です。

<https://○○○○○○○○>

偽のリンクをひらいてしまうと…

フィッシングサイトに誘導されてID・パスワードなどの**個人情報**が盗みとられる!

盗みとられた情報が利用され…

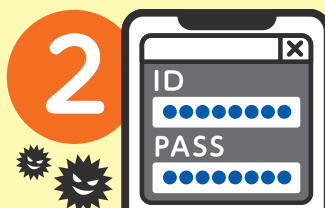
**あなたの銀行口座から金銭を盗みとられることも!**



対策



リンクを不用意に  
開かない



リンクを開いてしまっても  
ID・パスワードなどを  
絶対に入力しない



サイトへのログインは、  
公式アプリや公式サイト  
からアクセスする

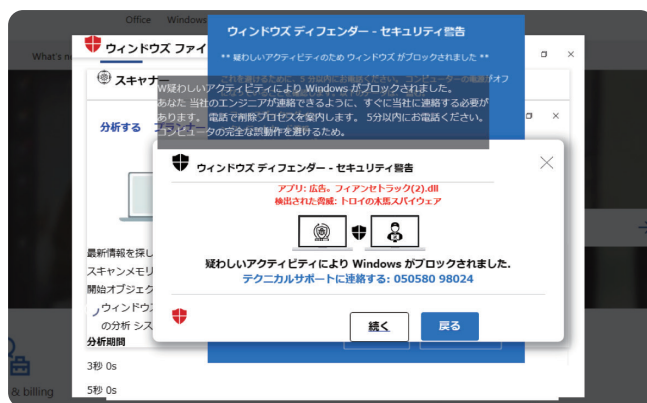


迷惑SMSブロック機能や  
セキュリティ対策ソフトを  
利用する

# 突然の警告!?! それって… サポート詐欺かも!

インターネット利用中に、突然、ウイルス感染の警告画面が表示され警告音が鳴ることがありますが、これはほとんどが偽の警告です。

## 多種・多様な種類の警告画面



## サポート詐欺の特徴

- ✓ Web 閲覧中の突然の警告や警告音
- ✓ 対応のためサポートへ連絡するように促す
- ✓ サポート対応を行う名目で詐欺を行う
- 名目1 遠隔操作するアプリのインストール
- 名目2 サポート対応のための金銭の要求

## 対策

- 1 不審な警告画面に表示された番号には電話しない
- 2 不審な警告画面は無視して閉じる
- 3 セキュリティ対策ソフトを使用する

電話をする前にまずは身近な人に相談してみましよう!