あなたの情報、狙われています

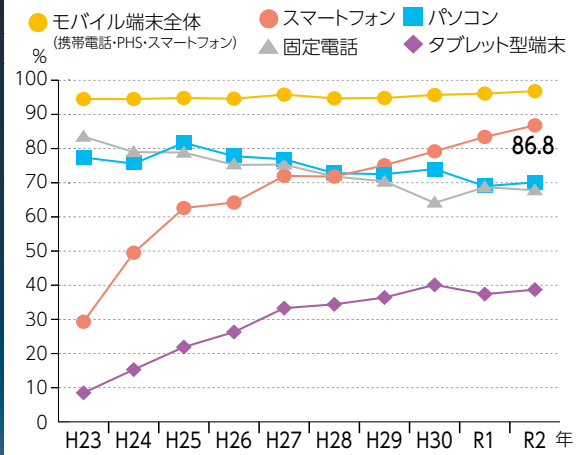
～身近に潜むサイバー犯罪※～

※サイバー犯罪…コンピューターやインターネットを悪用した犯罪のこと

社会全体でデジタル化が進み、日常のあらゆる場面で活用されるインターネット。スマートフォンの普及や新型コロナウイルス感染症の影響もあり、インターネット通販などの利用が増えるに伴い、トラブルも増加しています。人の心の隙や情報セキュリティーを悪用するサイバー犯罪に遭わないよう、日頃からしっかりと対策をして、トラブルに巻き込まれないよう注意しましょう。

情報通信機器の保有状況（世帯）

出典：「令和３年版情報通信白書（総務省）」



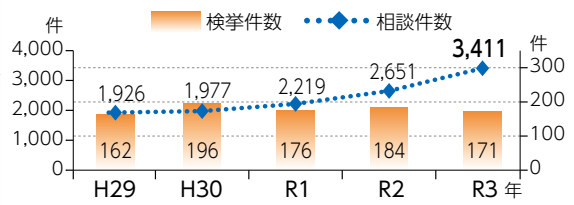
スマートフォンを保有している世帯の割合は86.8%。10年前と比べると約３倍。

全国初!! 県警察サイバーセンター始動

県内のサイバー犯罪に関する相談件数は年々増加し、犯罪の手口が巧妙化するなど、被害が深刻化しています。

県警察では、本部長直轄による迅速かつ的確な捜査や、警察官の育成などを目的に、サイバーセキュリティー部門、サイバー犯罪対策部門とサイバー攻撃対処部門を統合した**「サイバーセンター」**を全国の警察で初めて設置しました。刻々と変化するサイバー犯罪への対策を強化し、県警察一丸となって取り組んでいきます。

県のサイバー犯罪の相談・検挙状況

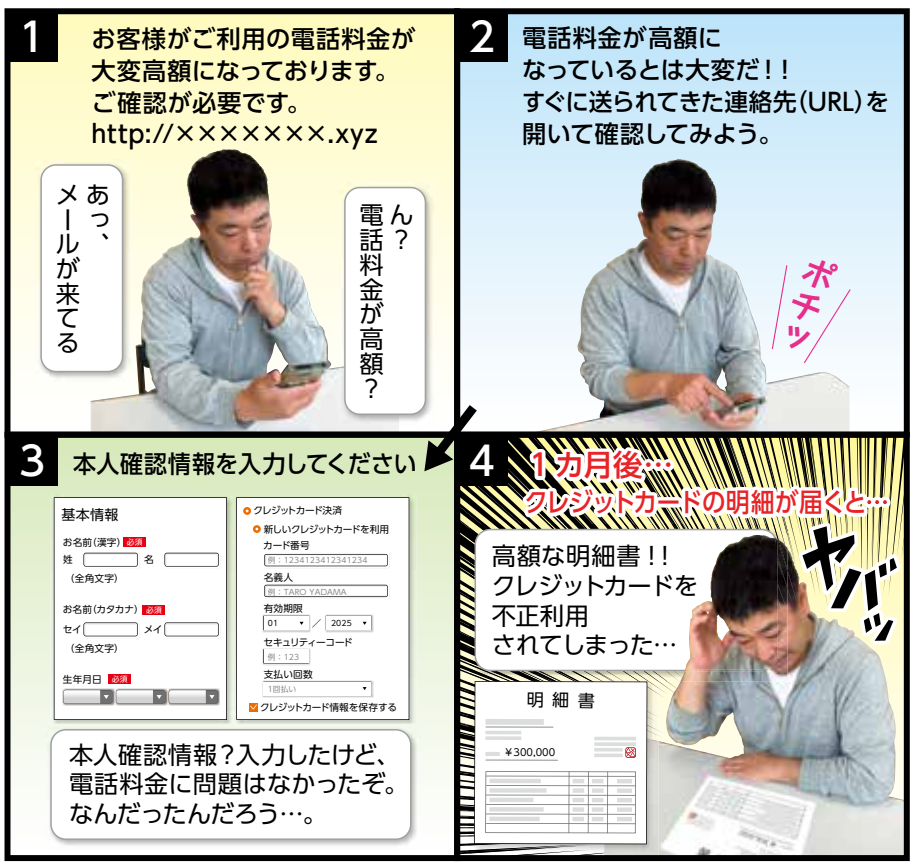


県警察への相談件数は、３年が3,411件と過去最多です。近年、スマートフォンの普及やSNSの利用が増え、インターネットを利用して犯罪に巻き込まれる被害が増加しています。

注意～トラブル事例～

事例１

メールが届いたので連絡先（URL）を開き、個人情報を入力したら不正利用された



通信事業者、宅配業者、金融機関など実在する企業を装ったメールやSMS(ショートメッセージ)を送りつけ、メールに記載された連絡先の偽サイトに誘導し、個人情報を入力させて詐取する「フィッシング詐欺」に注意。

対策は？

- 送りつけられたメールをむやみに信用しない
- メールを慌てて開かない
- 連絡先（URL）を押さない
- パスワードやクレジットカード情報などの個人情報を安易に入力しない

事例２

その安さ大丈夫？インターネットで買い物をしたら商品が届かなかった

自治体や民間企業などを装った、正規サイトと区別がつかないほど精巧な偽サイトに注意。正規サイトと同じレイアウトや記載内容のため、ほとんど見分けがつかない。中には、ウイルスに感染させるものもあります。

対策は？

- ドメインの末尾が「.jp」ではなく「.top」「.xyz」「.shop」「.buzz」のサイトは特に注意（例：http://www.●●●.●●●.xyz）
- メールやSMSに記載された連絡先を不用意に開かない
- ウイルス対策ソフトを導入し、偽サイトをブロック