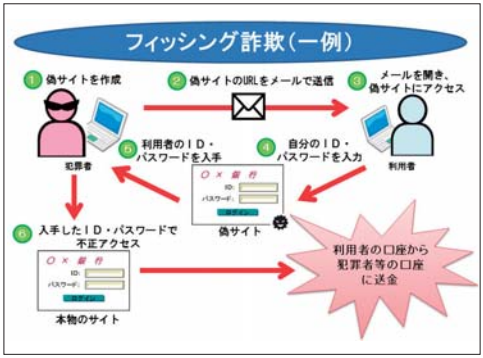
サイバー犯罪対策

サイバー犯罪とは、インターネットやコンピュータを対象とした情報技術を利用した犯罪のことです。

サイバー犯罪の具体例

●フィッシング

銀行やクレジットカード会社等を装った電子メールを送付するなどして偽のホームページに誘導し、クレジットカードやキャッシュカード番号、ID・パスワードを詐取する手口です。



情報がとられると…

本人になりすましてクレジットカード情報を勝手に使われたり、不正アクセス被害などに遭うおそれがあります。

●ランサムウェア

パソコン等に保存されているデータを使えなくして、元に戻すために金銭を要求するコンピュータウイルスの一種です。

感染すると…

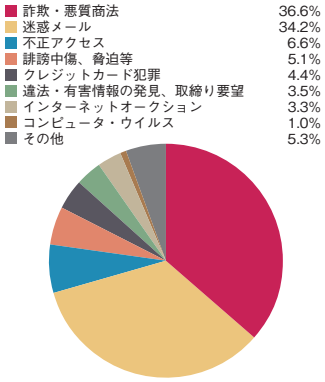
保存されたデータや機器自体が使えなくなるなどの被害が起こるほか、金銭を要求する画面が表示されます。

また、復旧が難しいことも特徴です。

サイバー犯罪に関する相談

- サイバー犯罪の相談件数は、平成30年中は7,900件となっています。
- 相談内容別では、詐欺・悪質商法の被害に関する相談や、迷惑メールに関する相談が多くなっています。

サイバー犯罪関連相談受理件数
（H30年中）



被害を防ぐためには

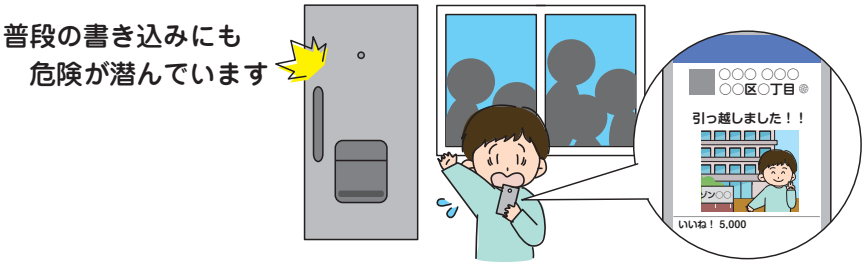
「一般的な被害防止対策」

- 個人情報を不用意に掲載するのはやめましょう。
- 簡単に推測ができるようなパスワード設定をするのはやめましょう。
- 身に覚えのないメール等に添付されたＵＲＬやファイルは開かない。また、そのようなメール等に対して返信をするのはやめましょう。
- 基本ソフト（ＯＳ）等インストールされている各種ソフトウェアを常に最新の状態に更新し、セキュリティ対策ソフトを導入しましょう。

SNS には要注意！

SNS(*)を利用して、犯罪に巻き込まれることがあります。被害に遭わないために、「個人情報が分かるような投稿をしない（画面加工等で隠す）・SNS 上で知り合った相手と二人だけで会わない」といった対策をとりましょう。友人同士のコミュニケーションを目的としていても、「インターネット上に情報が公開されている（＝不特定多数の人が閲覧できる）状態」ということを念頭において利用しましょう。

＊SNS とは「ソーシャル・ネットワーキング・サービス」の略で、メッセージや画像の投稿など、情報発信や利用者同士の交流ができる会員制 Web サービスのことです。代表的なものとして、Twitter や Instagram などが挙げられます。

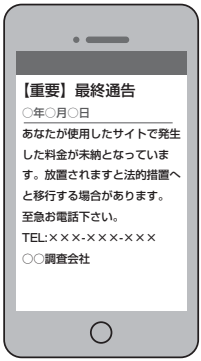


怪しいサイトやアプリを見分けるポイント

メールを受信したとき、ショッピングサイトを利用するとき、アプリをインストールするときは以下の点に注意しましょう。

怪しいサイトの利用を避けることで、架空請求や個人情報を盗まれる被害に遭う危険を減らせます。

請求メールの確認ポイント



- 「最終通告」「法的手続きに移行」「直接回収に行く」など不安を煽る文言が書かれている。
- 請求される行為を行った日にちが具体的に書かれていない。
- 連絡先が携帯電話の番号のみなど、簡素。

＊実在する企業になりすまし、メールアドレスを偽装していることもあるので注意しましょう。

詐欺サイト等の確認ポイント

- 通信が暗号化されていない(アドレスバーの鍵のマーク無い等)
- ドメイン末尾があまり見慣れないものである。
- 店舗ロゴと販売商品が矛盾している。
- 連絡先メールアドレスの末尾があまり見慣れないものである。
- 支払方法の説明と実際の決済画面とで対応可能な支払方法が違う。また、振込先口座が個人名。

＊これらに当てはまらない偽サイト等もありますので、初めて使用する通販サイトは事前によく調べてから注文しましょう。
＊改ざんされた正規サイトから知らない間に詐欺サイトに誘導されることがあります。アクセスしたサイトが怪しいＵＲＬでないか、転送されていないかを確認しましょう。

アプリの確認のポイント

- インストール時の「アクセス許可」の内容が不適切

＊「電話帳の連絡先へのアクセス」など、そのアプリにとって必要な権限なのかを注意しましょう。

- ダウンロード元が無名の配信サイト

＊配信アプリの審査をきちんと行っているところかどうかを確認しましょう。