

第2回 インターネットお役立ち通信

フィルタリング100%キャンペーンの
校内放送の様子をホームページに
アップロードしました！

保護者の皆様へ

日頃より本校の教育活動にご支援を賜りまして、教職員一同、心より感謝申し上げます。

さて、春休みが近づいて参りました。今回は、インターネットを利用する上で脅威となるより“具体的な事象”と“一般的な対応策”について資料を作成しました。

本資料を生徒の適正なインターネット利用につなげる契機としていただければ幸いです。

1. マルウェアや詐欺行為

①. マルウェアについて

悪意のあるプログラムの総称です。犯罪を目的として開設された Web サイトのボタンをクリックしたり、メールに添付されている URL やファイルをクリックすること等で感染します。

データファイルの破壊や個人情報情報を流失させる、金銭の不正な要求等の活動を行います。

【☹厄介な点☹】

マルウェアは日々、新種が生み出されており、しくみも進化を続けています。感染した端末から別の端末にデータを送信したり、端末同士で記憶媒体を共用すると感染を拡大してしまいます。

②. インターネット上での詐欺行為について

詐欺等を目的としたメッセージを送信したり、ウェブサイトのボタンをクリックすると脅迫文を表示する等して、不正に金銭をだまし取る行為です。図1は、筆者のスマートフォンに送信されてきたメールの写真です。大手金融機関を名乗っていますが、筆者は契約をしていません。

【☹厄介な点☹】

インターネット上で商品やサービスの契約をする際に入力した個人情報などを収集したり、無作為に発生させた連絡先に連絡してきます。

インターネット上に個人情報を入力した場合は、外部に情報が洩れている可能性があると考えるべきです。

また、受信者の不安を煽るような内容や大手企業を装った内容を送信するなどして、相手の信用を得ようとする等、手口が巧妙化しています。

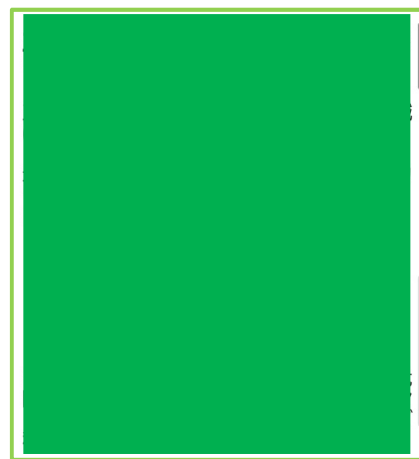


図1. 実際の不振なメール

2. 一般的な対策について

①. フィルタリングの実施

マルウェアの感染や詐欺行為に遭遇するなどのトラブルは、Web サイトへのアクセスやアプリケーション、ファイルのダウンロード等がきっかけとなる場合が多いようです。

フィルタリングを実施することで、危険性のある Web サイトの閲覧等を防止することができます。

②. マルウェア対策ソフトウェアのインストール

電気屋さん等でもソフトウェアが販売されています。マルウェアに感染していないか定期的に機器をチェックし、感染している場合には、その旨を知らせてくれる等、必要な対応をしてくれます。

③. 落ち着いて、情報を収集する

不信なメッセージの内容や添付された携帯番号などを「検索」すると有益な情報が収集できる場合があります。また、政府機関では、図2のように、国民から寄せられたトラブル情報(インターネット関連を含む)を日々、アップロードしています。

日頃から情報を収集しておくことも役立ちます。



図2. 国民生活センターWeb サイトの様子

3. 留意点について

①. 情報端末契約時の留意点

「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」では、携帯電話販売事業者や保護者に対して以下の義務を定めました。その一部を抜粋して以下にまとめます。

携帯電話事業者(義務)	保護者(責務)
携帯電話事業者は… ① フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない。(フィルタリングサービスの提供義務) ② 青少年有害情報フィルタリング有効化措置を講じなければならない。(フィルタリング有効化義務) ☆①と②は、“青少年が希望しない”場合は、この限りではない⇒ <u>家庭で、十分に検討・判断しなくてはならない！</u>	保護者は… ① インターネット上には、多くの有害情報や犯罪につながる情報があることを認識する。 ② 青少年の発達段階に応じて、利用状況を把握し、フィルタリングを設定する等、適切に管理する。 ③ 青少年のインターネットを適切に活用する能力の育成に努める。

まずは、“大人”が責任をもって、守り・育てる！

②. ソフトウェアのアップデート

マルウェア対策ソフトウェア等をインストールしても“アップデート”作業を実施していないと新たな脅威に対しては無防備な状態になります。適切に機器やソフトウェアのメンテナンスが必要です。

③. 不用意に連絡しない、開けない

怪しい連絡を受信した場合には、メッセージを開かずに“無視”をすることが大前提となります。執拗に連絡が来る場合や身の危険を感じるような内容の場合には、最寄りの警察署に相談するなどといった対応も考えられます。

④. 万が一、マルウェアに感染してしまったら…

LAN ケーブル抜いたり、スマートフォンのネットワーク接続をOFFにすることで、インターネットへの接続を物理的に遮断しましょう。接続している限り、情報が流出し続けてしまいます。

最後に

インターネット上のトラブルは、大人に見えにくいという特性があります。保護者が生徒のインターネット利用に責任をもちつつも、生徒自ら判断して適切に活用していく“ネットリテラシー”を育む必要があります。今後も、可能な限り、情報を発信していければと思いますのでご活用ください。