6
指導ポイント

●知らないアドレスからの広告メールはネットの迷惑●

本節の目的

迷惑メールは、受け取った人が迷惑なだけでなく、インターネット全体に負荷をかける問題であるという広い視点に立った考え方を持たせる。また、迷惑メールがなぜなくならないのかを考えることで、どのような態度を取ればいいのかを自発的に発見させる。

問題解説 6-1　設問 1

1.　みんなからきらわれ、法律で規制されているにもかかわらず、迷惑メールを送る人がいなくならないのはどうしてだと思いますか？

[模範回答]

・迷惑メールにひっかかる人がたくさんいて、儲かるから

・インターネットのメールはほとんど無料†で、手間をかけずに大量に送れるから

・迷惑メールを送る専門の違法業者がいるから

問題解説 6-1　設問 2

2.　迷惑メールを受け取ったら、どのように対応すればいいでしょう？

[模範回答]

・何もしないですぐに削除する。

・書かれているリンクをクリックしたりしない。

・「迷惑メールはやめてください」などと返信しない。

迷惑メールは「無視する」ことが一番の対応であり､具体的には上記のような回答が考えられる。

迷惑メールの配信に関しては、日本では 2002 年より「特定電子メールの送信の適正化等に関する法律」（通称、迷惑メール防止法）によって規制されている。2008 年に改正され、従来のように迷惑メールに対して受信拒否を通知しなければならない「オプトアウト方式」から、事前に承諾した場合のみ広告・宣伝メールを送信できる「オプトイン方式」に変更された。また海外からの送信に関してもこの法の対象とするなど、罰則の強化などがなされた。しかし、「いたちごっこ」の状況は変わっていない。

現在、商用サイトを営む業者自身が迷惑メールを発行しているケースは少ない。多くは、迷惑メール専門の配信業者が依頼を受けて、膨大な送信先メールアドレスのデータベースを元に送信するといったように、かなりシステマティックになってきている。

また、実際の送信作業でも、ウイルスなどと同じ違法な手口で侵入した第三者のコンピュータを利用して、自動配信を行わせるという手法が増加している。配信業者の支配下に入ったコンピュータをネットワークで結ぶ「ボットネット」を形成するなど、仕組みがより高度化しているのが特徴である。

2007 年に逮捕された迷惑メール配信事業者の例では、1 日に送信した迷惑メールは約 9000 万通にものぼり、送信先リストには延べ 230 億件分のメールアドレスがあったという。

こういった業者がなくならないのは、迷惑メールの配信に元手がほとんどかからず、利益が大きいからである。ここでいう「利益」とは､出会い系などの性的なサービスをエサにした架空請求や、架空の商品代金についての振り込め詐欺など、犯罪に絡むものが大半である。

詐欺行為で「利益」が出るということは、迷惑メールに対して返信したり、リンクをクリックするなどして、迷惑メールの手口にひっかかる人がいるということである。

興味が少しあるからといってリンクをクリックしたり、返信メールを送ってしまうと、詐欺行為にひっかかりやすいユーザーとして目をつけられ、迷惑メールがさらにたくさん届いたり、もっと悪質な勧誘や脅しを受けることになる。

迷惑メールに対する最も適切な対策は、「無視する」ことである。

† 最近ではブロードバンドによる定額制のインターネット接続が増えており、パソコンからのメール利用は実質的に無料になっていると言える。一方で、子どもたちが使っているケータイでは、メールを送信するごとにパケット利用料が発生し、パケット定額制にしていないと利用料金が際限なく大きくなる恐れがある。この違いから、「パソコンでのメール利用はほとんど無料」ということが理解しづらいことがあるかもしれない。

●メールアドレスがぬすまれたのでしょうか？●

〇本節の目的

迷惑メールが増える一因には、利用者自身に隙があることを認識させ、迷惑メールの対象にならないような情報管理方法を身につけさせる。

メールマガジンの登録や、キャンペーンの応募などでは、「空メールを送信する」という手法がよく利用される。

大人であれば、そのキャンペーンの広告主が誰か、あるいはきちんとした場所に掲載されている情報か、無料キャンペーンにしては特典が良すぎないかなどを総合的に判断して、メールすべきかどうかを考えることができる。

しかし、経験の浅い子どもにその判断は難しいため、最初のうちは空メールを送信しないよう指導し、年齢と経験に応じて徐々に自分で判断できる力を身につけさせることが望ましい。。

キャンペーンそのものには問題がなくとも、キャンペーンを実施した業者が倒産するなどして、結果的にメールアドレスが大量に流出してしまうこともある。いくら商品が当たったりサービスがタダで利用できるからといって、日常的に個人の連絡用に使っているメールアドレスを、無差別に提供してしまうことは控えるべきである。

また、昨今はカメラ付きケータイの普及により、QR コードを読み取らせる広告も増えている。しかし、QR コードは誰でも生成できるため、ポスターなどの QR コード部分だけを違法業者が貼り替えしまい、大手企業の広告のはずが違うサイトに誘導されるということもありうる。きれいな印刷物かどうかでは、安全の基準にならないことを指導する必要がある。

もう一つの指導ポイントとして、ホムペや掲示板など、誰にでも見られるウェブサイトにメール

アドレスを掲載しないよう指導する必要がある。迷惑メール事業者は、ネット上に公開されているメールアドレスを自動的に収集している。

どうしても公開しなければいけない場合は、公開専用のメールアドレスを作った上で、メールアドレスを画像に変換して掲載したり、メールアドレスそのものではなく「miautan ● miau.jp　←●にはアットマークを入れてください」と表記するなど、収集に引っかかりにくい工夫をすべきである。

●メールフィルターを活用しましょう●

〇本節の目的

「迷惑メールフィルター」の基本的な知識を習得させると同時に、迷惑メール排除のための設定を自分自身で考えることの重要性を認識させる。

迷惑メールは「無視する」ことが一番の対策であるが、操作ミスでうっかりリンクをクリックしてしまう可能性もある。そのような事故を未然に防ぐには、メールフィルターを利用して、効率的に迷惑メールを排除するとよい。

迷惑メールフィルターは、携帯電話自体から設定可能である。各キャリアごとの設定メニューまでの一般的な手順を、以下に示す（契約コースや機種によって若干の違いがある）。

・NTT ドコモ

「i モード」→「お客様サポート」
→「各種設定」→「メール設定」
→（希望する設定を選択）→（暗証番号入力）

・au

「E メールメニュー」→「E メール設定」
→「その他の設定」→「メールフィルター」
→（暗証番号入力）→（希望する設定を選択）

・SoftBank

「メール」→「設定」
→「一般設定」→「迷惑メール設定」
→（暗証番号入力）→（希望する設定を選択）

問題解説 6-2

あなたが受け取るメールのうち、必要なメールは残しつつ、迷惑メールだけをうまく取り除くには、どのような条件を設定をすればよいでしょう？　条件を考えてみましょう。

[模範回答]
・特定のメールアドレスから送られてくる場合は、そのアドレスだけを迷惑メールとして登録する。
・パソコンから送信されたメールのうち、送信元アドレスをなりすましたメールだけ受信しないよう設定する。

実際にどのようなフィルターを設定すればよいかは、子どものメール利用状況や、迷惑メールの配信数およびタイプなどで異なる。

フィルターの設定を間違えると、必要なメールまで見られなくなることがある。子どもの年齢や情報リテラシーの習熟度によって、子ども本人が設定することが難しいときには、実際の設定を保護者に行ってもらうのが理想である。

そしてそれを機会に、子どもの携帯電話は保護者がきちんと管理するものだという意識を持たせるとともに、保護者にも携帯電話の機能に関心を持ってもらうきっかけとなればなお良い。参観日等に保護者を集めて設定の実習などを行うと、喜ばれるだろう。

●ワンクリック詐欺にだまされない●

○本節の目的

迷惑メールに返信したりリンクをクリックした場合のリスクを認識するとともに、個人情報は簡単には取得されないことを学ぶ。架空請求に出会った場合には、子どもに生じる過度の不安を払拭し、冷静な対応を促す。

迷惑メールでは、メール利用者の好奇心や恐怖心を煽るために、いろいろな内容の文章が送られてくる。例えば次のようなパターンが考えられる。

・個人のメールであるかのように装うもの
「私、17 歳の××です。友だちになりたいのであなたにメールしてみました。……」

・偶然の幸運を装うもの
「おめでとうございます！あなたは当社の●●キャンペーンの当選者となりました！つきましては……」

迷惑メールはこのように、いかにも受け取った個人宛ての内容であるかのように装っているが、実際には特定の個人をターゲットにしているのではなく、不特定多数にメールを送りつけて、一人でも多くの人に返信またはクリックさせることが目的である。

指導ポイント

架空請求ではないかと疑わしいメールが届いた場合には、その文面の特徴的な一部（企業名や担当者名など）を抜き出して検索すると、同様の文面による架空請求被害が報告されていることがあり、判断材料となる。

また、架空請求の手口をまとめているサイトなども参考になるだろう。一例として、東京都が提供している架空請求の情報サイトを紹介しておく。

「STOP ！架空請求！」
http://www.anzen.metro.tokyo.jp/net/

モバイル版「STOP! 架空請求サイト」
http://www.anzen.metro.tokyo.jp/net/k/

上記サイトには、架空請求の典型的なサンプルサイトもあり、体験学習にも利用できる。

「sample site ○○○ .com」
http://www.anzen.metro.tokyo.jp/net/sample_site/index.html

なお、メールだけではなく、ケータイ向け SNS サイトのメッセージでも、友だちのふりをして誘いだそうとする手口がある。ただこれは、無差別に送りつけるメールとは違い、ターゲットを絞った誘い出しの一種であるため、今回は割愛した。

● ID を共有するのはやめましょう●

○本節の目的

ID やパスワードは、一見すると個人情報には見えないが、実際には個人情報同様に各個人がそれぞれ持って管理すべき情報であることを気づかせる。

ID とは、英語の「Identification」という言葉が語源で、「識別･証明」という意味である。ID は、ネット上のサービスで本人確認を行う重要な仕組みで、その ID を利用するための鍵がパスワードである。

この ID とパスワードが漏洩すると、さまざまな問題が引き起こされる。例えば自分の名前で勝手にメールが発信されたり、自分の日記に知らないうちに更新されていたり、有料の課金サービスを使われてしまったりすることになる。

ID とパスワードがセットで盗み出されることは少ないが、誰かと共同でサイトを運営するときに、情報を漏洩させてしまうケースは多い。

問題解説 6-3

　掲示板に書きこんだのがだれなのかが本当にわからなくなってしまった場合、どのような状態になると思いますか？　またどのような問題が起こると思いますか？

　［模範回答］
・誰かが悪口を書き始め、けんかになる。
・誰かが自分を偽って嘘を書き、人間関係が壊れてしまう。
・パスワードが変えられてしまい、閉鎖もできなくなる。
・ID を登録した人の個人情報がネットに流出してしまう。

　特に、保護者と子どもで携帯電話やパソコンを共有している場合に、ID やパスワード、暗証番号まで共有するのは危険である。知らない間にクレジットカードで買い物されたり、設定を変えられて保護者が閉め出される可能性もある。
　また最近では、企業や団体が個人向けの情報発信ツールを使って広報などを行うケースも増えている。担当者が一人ならば問題ないが、今後は ID を複数人で管理することによるトラブルが社会問題化することも考えられる。個人による情報発信は、個人の責任においてなされるべきであり、そういう考え方を早いうちから身につけておくことが大切である。