

事例 1 1

だれもが迷わくコンピュータウイルス

指導のポイント

<ねらい>

コンピュータウイルスの被害の危険性を認識し、感染させないための心がけと対応法及び感染してしまった場合の対処法を身に付けさせます。

<学習の場面>

学級活動や授業などでコンピュータを活用する際に、取り上げて指導すると効果的です。

<指導上の留意点>

コンピュータウイルス問題は、組織のネットワークでは対応がきちんとしてきています。それにもかかわらず、ネットワーク上にメール等でばらまかれているウイルスが減らないのは、コンピュータの初心者が、家庭などでウイルス対策をしていないために、感染したコンピュータをそのまま利用していることが原因といわれています。そのことを踏まえ、コンピュータを使う場合に責任を持つことの大切さを理解させ、きちんとした対応をとれるように指導します。

ワークシートでは、まず学校のコンピュータで記入の方法などを指導し、自宅でコンピュータを利用している児童生徒には、そのコンピュータでチェックしてくるように指導します。

理論的に知っているだけでなく、技術として対応できる力をつけることが必要です。実際にコンピュータを操作させながら、具体的に指導することが大切です。

<用語>

トロイの木馬

便利なソフトウェアに見せかけて、ユーザに被害を与える不正なプログラムをいいます。

プログラム自体に感染機能はなく、感染増殖することはありません。プログラムの内部にウイルスを隠し、コンピュータに組み込んだり、コンピュータ内のファイルをインターネット上に送信してしまったり、ファイルやディスク内容を破壊するなどの機能を持たせるなどさまざまな被害を及ぼすようになります。

マクロウイルス

MS Word や MS Excel のマクロ形式のプログラムを含むファイルに感染します。

このウイルスに感染されたファイルを開くと、コンピュータがウイルスに感染します。これらの文書ファイル、表計算ファイルのやり取りだけで、ウイルスが拡散していきます。

ワーム

通常のウイルスは感染対象のプログラムを必要としますが、ワームは、感染対象となるプログラムがなく、自分自身を複製して増殖します。

ネットワークに接続されている他のマシンに出現し、ネットワーク内を這い回るように見えることから、「ワーム」という名称が付けられています。

ワクチンソフト

ウイルスを検査、駆除するソフトウェアのことです。

最新のウイルスは症状からの発見が難しいものが多いため、常にワクチンソフトでのウイルス検査が欠かせません。新しいウイルスが次々と出現していますので、漏らさず発見するには、新種のウイルスを検出するためのウイルスパターンファイル（ウイルス定義ファイル）を絶えず更新することが大切です。

添付ファイル

eメールでは、本文とは別に送付するファイルをいいます。添付するファイルのサイズには制限がありますが、ファイルの種類は問いません。

ウイルスが感染することができるファイル（プログラム、MS Word、MS Excel などの文書ファイル、表計算ファイルなど）も、添付できますので、これらの感染したファイルを受信した場合は、ファイルを開いたりプログラムを実行するとウイルスが活動を始めます。

eメールで添付ファイルがある場合には、ウイルスチェックをしてから開いたり、実行したりしましょう。また、添付ファイルを送信するときにもウイルスチェックをしてから送信するなどのマナーが求められます。

セキュリティパッチ

セキュリティパッチとは、OS やアプリケーションなどでセキュリティホール（セキュリティ上の弱いところ）に対する、修正プログラムのことをいいます。

セキュリティホールは、絶えず新しく発見されていますので、セキュリティホール発見の情報とその対応方法をインターネット等で確認し、できるだけ早くパッチを適用することが必要です。

<資 料>

今までに社会的に大きな問題になったウイルス

ウイルスの蔓延はネットワークに負荷をかけ、コンピュータにはデータの漏洩や破壊など大きな被害を与え、ネット社会の深刻な問題となっています。

2004年5月 W32/Netsky のウイルスメールが猛威

添付ファイルを開かなくても、メールをプレビューしただけで感染するものもあった。あまり症状がでないことから、自分が感染していることに気付かず、他へウイルスメールの送信を行っているケースが多い。

2003年8月 W32/MSBlaster 史上最大の被害を引き起こした

Windows のセキュリティホールを悪用し、インターネットに接続されたコンピュータであれば、メール受信をしなくてもホームページを見ていなくても感染してしまうワームであった。

会社内で感染が広まり、ワームによる不要なトラフィックでネットワークが混雑し、業務に支障をきたしたり、ワームに感染しなくても外部からのアクセスによりパソコンの動作が重くなったりした。

2002年5月 W32/Klez ウイルス蔓延

このウイルスは、データを破壊し、気付かずにいるとすべてのデータを失うという被害の大きい種類であった。

自動的にメールの添付ファイルの形でばらまかれ、しかもメールの差出人を詐称するため、どのコンピュータから送られたのか分からないという特徴があった。

2001年9月 複数の感染経路を持ち、実害も大きい W32/Nimda ウイルス

このウイルスは、ホームページを閲覧するだけで感染したり、メールをプレビューするだけで感染するなど複数の手段で感染する性質があった。Web サーバーが感染した場合には、サーバー上の Web ページが、ウイルスをダウンロードするように改ざんされるため、そのサイトを見ただけそのコンピュータはウイルスに感染した。