

ここでは、ICTを利用する側からのセキュリティ上の注意点について学習します。

5-9-1 インターネットのリスク

コンピュータがインターネットにつながったことにより、インターネットを経由した様々な情報被害が発生するようになりました。ここでは、ウイルス対策と、Webサイトを利用するときの注意について説明します。

5-9-2 ウイルス対策の必要性

ここでは、ウイルスによる被害とその対策について説明します。

① ウイルスによる被害

ウイルスやワームに感染すると、主に次のような被害が発生します。コンピュータ内にサイズの大きい不要なファイルが作成されていたり、コンピュータの動作速度が遅くなったりするなどの症状があるときは、ウイルスに感染しているかもしれません。

- コンピュータのデータが破壊されたり、起動できなくなったりする。
- ウイルスに感染した電子メールがアドレス帳に登録されている電子メールアドレスに勝手に送信される。
- コンピュータをネットワークで自由に利用できるようにされ、クラッキングされる。

② ウイルスの侵入経路と対策

ウイルスがコンピュータに侵入する経路は、電子メールの添付ファイルや電子メールに埋め込まれたURL、フリーソフトやドライバ、インターネット上からダウンロードしたファイル、USBメモリなど様々です。普通にコンピュータを使用していても、危険は常に近くにあるのです。

新しいウイルスによる被害が発生すると、セキュリティソフトウェアメーカーやハードウェアメーカーのWebページなどを通じて、詳細情報や対策が公開されます。ウイルス感染を防ぐためには、すばやく情報を入手

参考

ワーム

ネットワークに接続されたコンピュータに対して、次々と自己増殖していくプログラムのこと。電子メールを大量に送信し感染を広げるものが多い。

して対策を取ることが重要ですが、日頃から対策しておけることもあります。

●OSなどの更新プログラムの適用

OSやWebブラウザのセキュリティホールが放置されていると、その弱点を突いてウイルスが侵入することがあります。最新の「パッチ」や「サービスパック」と呼ばれる対策用の更新プログラムを組み込んで、セキュリティホールをふさぐことが重要です。Windows 10では、大きな危険に対しては自動で更新プログラムが適用されます。

●ウイルス対策ソフトの導入

ウイルスからコンピュータを守る「ウイルス対策ソフト」があります。ウイルス対策ソフトは、ウイルスの「検出」「隔離」「駆除」の機能を持っています。ウイルス対策ソフトは常に稼働させておき、ウイルス定義ファイルを最新のものに更新するように心がける必要があります。

●ファイルのダウンロードと実行

インターネットからダウンロードできるソフトウェアなど、安全性が確認できていないファイルについては、むやみにダウンロードを行わないようにします。ダウンロードしたファイル以外でも、処理を実行したり、その処理で利用されたりするファイルは、ウイルスに感染している危険性があります。「.exe」や「.bat」「.pif」「.scr」などの拡張子が付いている実行ファイルやマクロが組み込めるExcelなどのファイルは、ウイルス対策ソフトなどで安全を確認してから開くようにします。

●電子メールでのウイルス対策

電子メールのメッセージをプレビューすると、ウイルスに感染することがあるため、電子メールのプレビュー機能をオフにします。また、知らない人からの添付ファイル付きの電子メールや、タイトルや差出人が不明の怪しい電子メールを受信した場合は、電子メール自体を完全に削除します。これは、フィッシング詐欺にも有効な対策になります。

参考

ウイルス定義ファイル

ウイルスを特定するためのパターン、またはコードが定義されたファイル。

参考

マクロ

Excel上の作業を記録し、自動的に操作を実行する機能。何度も同じ作業を繰り返さずに済む。