

第3章 ウイルス・スパイウェア対策

PC を使用するうえで、最も注意しなければならないことのひとつがウイルス・スパイウェアへの対策です。感染ルートはインターネットやメールに加え、最近では USB メモリーを介して混入するケースも発生しています。感染することにより、PC の動作の不具合・不利益だけではなく、新たな感染源となって他の利用者にも悪影響を及ぼす可能性があります。

この章ではウイルス感染のリスクを減らす、主な手段を説明します。

3.1 Windows Update (Microsoft Update) の実施

更新プログラムは、コンピューターのセキュリティ向上およびパフォーマンス強化を図ることができます。使用する Windows OS、ソフトウェアを最新の状態に保つことで、脆弱性をついたコンピューターウイルスの感染を防ぐことができます。常時ネットワークに接続している場合は自動更新機能でアップデートされますが、手動でなければインストールされないものもあります。最低でも 1 ヶ月に 1 度は実施しましょう。

- (1) 「スタートボタン」→「すべてのプログラム」→「Windows Update」の順でクリックしてください。



- (2) 自動更新が有効で、かつネットワークに接続されている場合は、利用可能なプログラムが表示されます。「更新プログラムのインストール(I)」をクリックして更新を実行します。

(電源投入直後や自動更新を無効にしている場合など、「更新を確認してください」と表示されることがあります。「更新プログラムの確認」をクリックし、表示された更新プログラムをインストールしてください。)



- (3) 完了後、PC の再起動を求められる場合はその指示に従ってください。再起動後、他にダウンロードすべき更新が残っていないかを確認するため、再度 Windows Update を実施してください。

3.2 ウイルス対策ソフトについて

前述の Windows Update も重要な対策の一つですが、コンピューターウイルスの感染をより防止するには対策ソフトの導入が必要不可欠です。一般に販売されている PC は、ウイルス対策ソフトがインストールされていても、試用版として期間を限定したものや、全くインストールされていない製品があるので注意が必要です。

- (1) PC の状態を確認するには、コントロールパネルを開き、「システムとセキュリティ」→「アクションセンター」の順にクリックします。

アクションセンター画面ではセキュリティ情報のほかに、バックアップなどのメンテナンスに関する情報も表示されます。ここでの説明は割愛しますが、必要に応じて活用してください。



- (2) 各項目が有効な状態に保たれているか、確認してください。ウイルス対策ソフトがインストールされていない、あるいは最新の状態でない場合は対策が必要です。



ウイルス対策ソフトはインストールただけで安全とは言えません。新たなウイルスやスパイウェアに対応するには、定期的に定義ファイルの更新を行う必要があります。対策ソフトを導入する際は、利用開始手続きを忘れずに行うとともに、期限切れにならないよう十分注意してください。

代表的なソフトウェアとして、トレンドマイクロ社のウイルスバスター、シマンテック社のノートンセキュリティ、マカフィー社のインターネットセキュリティ等があります。