◎　それでは、おしまいに　　「簡単なパソコンセキュリティ」　　３０分

1　パソコンって壊れないの？

パソコンは通常の状態で、普通に使っていて壊れることはありません？。が、最新の電子技術、精密機器加工組立技術、ソフトウェア技術の結晶であり、大変デリケートな装置なのです。

パソコンは始めに説明したとおりハード類とソフト類の集合体で、ハード類は物理的に強い衝撃や高電圧、高温を与えないかぎり、結構丈夫で壊れにくい物なのです。

しかし、可動部がある装置(ＨＤＤ、ＤＶＤ)などは、その装置が停止中(電源断中)の衝撃では結構強いのですが、装置が動作中では、特にＨＤＤは横からの衝撃に弱く、ＤＶＤやＦＤＤなどは埃に弱い性質を持っております。

また、液晶のディスプレイでは、硬質の保護カバーが使われていないものは、鋭い物で突くとひとたまりもありませんし、強い圧力をかけても壊れます。ノートパソコンの多くはこのタイプです。

内部の電子部品は、電気的衝撃(瞬間的な高電圧でも)に弱く破損してしまうことがあります。電気的衝撃とは何でしょうか？　通常の状態では雷(落雷)がそれにあたります。近くに落雷があると、その衝撃電圧が電源線を、インターネット接続の電話線を通じてパソコンの中に入り込み、電子部品を破壊することがあります。雷が近づいて来たらパソコンを停止し、電源線と通信線をいったん外すと良いのです。また、めったにすることは無いと思いますが、パソコンの電源コンセントを瞬間的に抜き差しするのも良くありません。

温度のほうでは、半導体電子部品、特にＣＰＵなどは温度が高くなると、通常状態より電気が流れやすくなり、熱暴走という厄介な現象を起こしてしまいます。パソコンの電源を入れるとファンの回転音が聞こえますね。ファンはその防止のためにあるのです。

ソフト類も通常の使い方では壊れることは無いのですが、ソフト的破損の主原因はパソコンの使用者(あなたです)のちょっとした不注意によるものがほとんどです。ごくたまーに、コンピュータウィルスによる破壊があるかもしれませんが。

それからもう一つ、電気的衝撃もソフト的破損の原因になってしまう場合もあります。先に説明した衝撃電圧が原因であるほかに、強い電波(通常の家ではありません、不法電波です)も同じことになります。

パソコンはプログラムに従って動作していますが、電気的衝撃がＣＰＵに渡されるプログラムの一つの命令に影響し、別の動作の命令に変えてしまい、まったく別の動作をさせてしまうことが起こるからです。

いまのパソコンは大変便利にできております。同時にいくつものデータを開いたり、複数のプログラムを使うことができます。しかし、これはパソコンのメモリーが十分に搭載されていればいるほど(搭載上限有)十分に機能してくれますが、仕事量が増えていくとパソコンの動作遅くなったり、場合によってはパソコンの動作にとって重要な情報を記憶している部分を侵略破壊してしまうようなことが起こると、正しく動作しなくなってしまいます。

念のため、動作が遅くなったかなと感じたら、使わなくてもよくなったソフトはこまめに閉じ、必要なものだけを使いましょう。

また、一つのソフトであっても一日いっぱい使い続けていると、メモリー上のワークスペースを使いすぎ動作しなくなることがあります。特にワープロや画像処理ソフトで大容量のデータを使い続けているときなどは、念のため作業中のデータをいったん保存し、ソフトも終了させた後、いったん電源を切り再度起動しなおして使ってください。

だからといって、せっかくのパソコンを棚の上に上げてしまう必要はまったくありません。手荒く扱うことが無いようにし、ちょっとした操作ミスをできるだけ少なくするよう使いながら慣れてゆけばよいのです。

2　アレー！昨日作ったファイルはどこだろう！？　見つからない、どうしよう！

せっかく作ったファイル！、再度使おうとしたけれど、どこにも見つからない。このような経験は無いですか？

たいていの場合はハードディスクから完全に消してしまうことは無いのですが、一つ注意していただきたいことがあります。

前にも説明しましたが、ファイルの名前は一つの保存場所(フォルダ)の中では、同じ名前のファイルを二つ作ることができません。ところが、前に作ったファイルを参照して別物を作り、そのまま保存する場合、いつもの癖でついつい「上書き保存」を行ってしまうと元のファイルは、いま作り直したファイルに置き換わってしまい、完全に消えてしまい戻すことができなくなってしまいます。参照した元ファイルを残してお

きたい場合は、必ず別のファイル名で保存するか、別のフォルダをつくりそこに保存してください。フォルダ名もまったく同じことが言えますので注意してください。
　さらに、データ類の保存場所も、慣れるまでは必ず「マイドキュメント」フォルダの中に保存しましょう。

3　パソコンが変だ！？　どうしよう！
　パソコンを使っているうちに、なにか変だ、動かない、と感じたら
まず落ち着きましょう！　ゆっくり深呼吸をして、そしてメモの用意をしてください。
パソコンの画面や、ランプ等、音、周辺装置の状態などをゆっくり確かめてください。
・砂時計アイコンはありませんか？
　　しばらく待ってみましょう！
・小さなウインドウが出ていませんか、小さなウインドウ隠れていませんか？
　　画面やタスクバーを良く見てください。
　　出ている、隠れているウィンドウを順番に閉じてみましょう。
・なにかのランプが点滅、普段点灯していないランプが点灯していませんか？
　　何のランプなのか確認し、その原因を取り除きましょう
　　ＨＤＤのランプなら、しばらく(数分、場合によっては数時間)待ってみましょう
・なにか音が鳴りませんでしたか、鳴り続けていませんか？
・周辺装置はどうですか？

　「何をしているときに」、「どのようになってしまい」、その後「どんなことをした」のかを、可能な限り詳しくメモしてください。これらの全てのことがパソコンを復旧させる上で大切な鍵になるのです。さらに、自分でパソコンを回復させようと何かを行う場合は、落ち着いてゆっくり待ち時間をとりながら、画面状態やランプ等の状態、音などを確かめつつ、そして一々メモをとりながら作業を進めてください。

4　うっかりミス、したこと無い？
！知らず知らずに、マウスをクリックしていた、とか！
　マウスを操作するとき、緊張しすぎていつの間にかクリックしてしまうとか、ドラッグをしてしまったとか、操作しているときは夢中なので気が付かないこともあります。また、クリックするとき、つい力が入ってしまいマウスが少しずれてしまい、目的とは別の部分をクリックしてしまうことは、しょっちゅうあることです。

　イージーミスは恐れることはありません。
　もし、急に予期せぬ画面に変わったりした場合は、ミスったかな、と早く気づく事が一番大切です。
　そんなときは、前にも書きましたが、ぜひ深呼吸を、そしてメモの準備をしてください。落ち着いたら、おもむろに画面の中を見回してください。
　新しい画面が開いてしまった場合は、右上の「閉じる」ボタンをクリックしてください。
　「ＯＫ」とか「はい」ボタンが出ている小さなウィンドウも「閉じる」です。
　新しい画面ではなく、メニューなどが出た場合はキーボードの左奥にある「Ｅｓｃ」きーを押し、操作を取り消してください。
　また、ソフトによっては、今行った操作を元に戻すための「元に戻す」ボタンをクリックしてください。
　　これで今のミス操作が取り消され、前の状態に戻ります。

！キーボードのダブルタッチ（指先がふるえて）、押し続け！
　キーボード操作も同じことが言えます。チョンとキーを1回押すだけだったのに、２、３回押してしまっていた、押すつもりは無かったが、気がついたら同じ文字が幾つも並んでいたなどと。
　もし、文字が入り込んだ場合は編集キー(BackSpace、Delキー等)を使い消してください。
　新たに画面が出てきた場合は、マウスの場合と同様に！

　ミスの中で、一番恐ろしいのは、パソコンやソフトに取って大切なファイル類を、知らぬ間にどこかへ移動してしまったり、消してしまうことです。
　いろいろな操作、特に削除する操作では、確認の画面が出ますので、間違っても「ｙｅｓ」、「ＯＫ」、「はい」などは、クリック(入力)しないようにしてください。
　「閉じる」、「いいえ」、「Ｎｏ」、「キャンセル」等で操作を取り消すようにしてください。

5　パソコンから人への、メッセージ、悲鳴！　　パソコンも文句を言いますよ。

パソコンは、通常あなたの言いなりで、有能に一生懸命仕事をしてくれます。しかし、あまりにも酷使するとパソコンだって疲れ果ててしまうこともあります。
また、パソコンは利口なようですが、実は融通が利かない厄介な面も持ち合わせております。
あなたのちょっとしたうっかりミスも、素直に受け入れ実行してしまいます。その結果、変なところに入り込んでしまっても誤りに気づくこともなく突っ走って(同道巡り)しまったり、何も来ることが無い窓口でいつまででも待ち惚けしています。
これらの結果として、われわれ利用者には、パソコンが変だ、動かなくなった、などの症状としてあらわれてきます。

パソコンはその内部で作業を進めるとき、「今はこのような状態ですよ」とか、「そのとうり実行してもよいのですか」、「疲れてきました」、「仕事が多すぎます」などと、われわれ利用者にメッセージを出してくれております。それらのメッセージを見逃さぬようにしてあげてください。

メッセージが現れる場所は、
　　パソコンのあちこちにあるランプの色の変化や点灯、滅灯、点滅
　　画面上に現れる小窓と、タスクバー
　　スピーカーからの音
　　パソコンの動作スピード
これらパソコンからのメッセージを、見逃さないように少し気を配ってください。
我々はついつい一生懸命仕事を進めていくと、そのことに熱中しすぎ、パソコンからのメッセージや悲鳴を見逃し、自分の作業のつもりで行った操作が、パソコンからのメッセージの回答として扱われてしまっては大変ですので。

6　最終手段　　！最終的な方法！

もし、パソコンが動かなくなった、キーもマウスも受け付けなくなってしまった(フリーズ状態、だんまり、固まった、などといいます)場合は、

しばらく様子を見ても何の変化も無く(マウスを動かしてみても)どうしようもないときは、最終的な方法として、「Ctrl」＋「Alt」＋「Del」(「Ctrl」keyと「Alt」keyを同時に押しながら「Del」keyを押す)を実行します。状況により、いつも同じとは限りませんが、「プログラムの強制終了」ウィンドウが開くので、もう一度、「Ctrl」＋「Alt」＋「Del」を実行してください。パソコンは強制終了し再起動します。
再起動には、通常の起動より時間がかかることがありますが、あせらずに待ってください。

「Ctrl」＋「Alt」＋「Del」を実行し少し待っていても、変化が無いとき(ハードディスクランプも点滅していない)は、電源ボタンをしばらく(５秒程度)押し続けてください。パソコンの電源が切れます。
少し待って(１分近く)待ってから、電源を入れてみましょう。ハードディスクの検査、修復の画面が出てから(結構時間がかかります)ＷＩＮＤＯＷＳの起動が行われ、ディスクトップ画面が表示されます。
もしも、「セーフモード」という状態で立ち上がったならば、ＷＩＮＤＯＷＳの起動完了後、正しい終了手順でＷＩＮＤＯＷＳを終了させてください。
少し間(１分近く)を置いてから、再度、起動してみます。一見、正しく立ち起動したようなら、状態が悪くなったときに使っていたソフトや、普段使っているソフトを起動してみてください。どれも正しく起動したなら、よかったな～！　と思ってください。ただし完全にもとの状態に戻っている保証はありません。

！それでもダメなら、先輩に、買ったお店へ相談！
いろいろやってみてもやっぱりダメな場合は、パソコンの先輩に相談してみたり、パソコンを買った店、そのパソコンのメーカーへ相談してください。
この場合、特に大切なことは、
・どんなソフトを
・どうしているとき(使っていた状況をできるだけ詳しく)
・どんな状態になったか(画面、ランプ等、キーボード等周辺装置を含めて)

・その後、どんなことをしたのか
・さらに、装置の型式名、ＯＳの名前とバァージョン、メモリーの搭載容量、周辺装置名等
これらのほか気が付いたこと(音がしたとか、周辺装置が止まってしまったとか)を、メモしておき、その内容を説明しながら相談してください。ただ、「パソコンが変なのですが」だけでは、相談を受けた側で困ってしまいます。

7　大事なものは　　！大事なデータファイルは、バックアップしましょう！

もし､パソコンが壊れたらどうしますか、お金は掛かりますがパソコンは買うことができますね、しかし苦労して作ったいろいろなデータ、一生懸命打ち込んだ住所録、取り貯めた素敵な思い出の写真、お金を出しても戻ってきません。
先に説明したように、パソコンは何かの拍子でトラブルを起こすことがあります。
最近は少ないかもしれませんが、フロッピィディスクを使っていて、操作ミスや磁石の影響などで読み取れなくなってしまうことがよくありました。
このようなことから大切なデータを守るためには、バックアップを取るように心がけましょう。
パソコンにおいてバックアップとは、データ等を現在保存してあるところから、別の媒体(ＨＤＤの別ドライブを含む)に複写しておき、元のデータが破損したときそのコピー(バックアップ)から復元するための複写です。
バックアップを取ると言っても、どこにバックアップしたら良いのか、ちょっと問題が残ります。
自分のパソコンにフロッピィディスク装置はあるのか、データの大きさ(容量･サイズ)はどのくらいなのか、等々ですし、さらにコストの問題もあります。

・もし、読書きできるＤＶＤ装置が付いているのなら、ＤＶＤにバックアップするのが一番良いのかもしれません。
・ハードディスクが、論理的に２分割されているパソコン、Ｃドライブのほかにドライブもあるパソコンでは、Ｄドライブのほとんどのスペースが空き領域になっていますので、そこにバックアップするのが、手っ取り早く安く上げる方法です。
それは、ＣドライブにはＯＳや各種のアプリケーションソフト、設定情報、そして作ったデータを保存していた、マイドキュメントなどが格納されております。もし設定情報やプログラムが壊れてしまい、新にシステムやプログラムを入れなおすこと(フォーマット＆インストール)になったとしても、Ｃドライブだけの作業で済み、Ｄドライブはそのまま助かることが多いからです。
ただし、ハードディスクそのものが壊れた場合は、どうしようもありません。
・もし、バックアップすべきデータの容量が僅か(１ＭＢ程度以下)で、装置にＦＤＤがついている場合は、ＦＤＤにバックアップするのが良いでしょう。(自作した文書(画像なし)や表計算のデータ、重要なメール)
・ＵＳＢメモリーには相当量のデータが入りますので、これも良い方法でしょう。
・ＣＤ－ＲＯＭ書き込み装置があれば、これにバックアップしておくのが大変良いのでしょうが、再書き込みできないので、コスト面で幾分不利でしょう。写真などは整理した後ＣＤ－ＲＯＭに！　良いのでは！

8　パソコンを守りましょう
！インターネットを使わなければ、パソコンもつまらないですよ！

パソコンを手に入れ、一人でパソコンを使っていても、それなりの楽しみや喜びはあるでしょう。　が！
インターネットに接続することで、メールやホームページを有効に活用することができ、パソコンの先にいる多くの人とのつながりを持ち、交流の輪を広げ、そして無限の情報を活用しながら、豊かで充実したシニアライフを目指してこそ、ＯＳＳメンバーの本分でしょう。
パソコンを持ち、インターネットに繋げる、それが目的ではありません。それらは単なる手段であり、それから先が活用しだいで無限に広がっているのです。
しかし、無防備なままパソコンをインターネットに接続すると、その瞬間から世間の荒波にさらしてしまい、そのパソコンではすぐに悪意の餌食になってしまい、ウィルスに感染するだけでなく場合によっては大切な情報を盗み出されたり、知らぬ間に悪意の手先としてウィルスをばらまいたり、サイバーテロの中継基地になってしまうこともあります。

●パソコン犯罪の加害者(被害者ではないですよ！)にならないために！
　？なぜ？　自分が犯罪加害者なの、なにもしていないのに？！
　悪意な犯罪の被害者になったのならば最悪で泣き寝入りで済ますことができるでしょうが、何もしていないのに加害者になってしまうのは、合点が行かぬと言われそうですが、何もしていないからそうなってしまったのです。

　コンピュータ(ネットワーク)の悪意の種類には、コンピュータウィルス(ウィルス)やワーム、ウィルスの再配布、データの収集転送(スパイウェア)、不正アクセスやＤｏｓ攻撃(サービス不能攻撃)とその踏み台(中継者)等々とさまざまとあります。
　その手法の主なものは、まりすまし、セキュリティーホールへの攻撃等があります。
　なりすましとは、利用者(あなたです)にとって有用なメールや情報であるように装って(なりすまし)、メールを開かせその添付ファイルを開かせたり、悪意のソフトをダウンロード(ネット上から自分のパソコンに取り込む)させる方法です。
　セキュリティーホールへの攻撃とは、ソフトウエアの不完全部分を悪用してそこからパソコン内へ、悪意のソフトを送り込むことです。
　悪意のソフトの中には、メールやホームページに使う通常の出入り口(通信ポート)のほかに、バックドアと呼ばれる裏口を勝手に作り、パソコンの利用者が知らない間に、勝手にさまざまな悪意の活動を始めてしまうものまであります。

●！ならば、どうしたらいいの？
・先ず実行していただきたいことは、最新版のウィルス対策ソフト(セキュリティソフト)の導入です。
　(大手のセキュリティーソフトメーカーの製品は、バージョンアップサービス(有料)期間が決まっており、その期間より前の製品は役に立ちません。)
・常に注意し、心がけてほしいことは、ＯＳ等の最新版への更新とウィルス対策ソフトの最新版への更新
・時々実行してほしいことは、ハードディスク等のウィルスチェック
・年一度、ウィルス対策ソフトの利用契約の更新(有料)
・毎回心がけてほしいことは、パソコンを使うとき起動し、パソコンから離れるときは終了しましょう。特に、常時接続のパソコンは、パソコンを使っていないときは電源ＯＦＦにしましょう。
　常時接続のパソコンは、電源が入りパソコンとして立ち上がっていると、常に外部と接続されていることから、セキュリティソフト未対応の悪意の攻撃が入り込む可能性があるからです。
　(悪意のソフトは日々新しく作られ、ソフト自身が勝手に作ることもあります。)

●これらは大変に重要なことなので、私の独断と偏見そして私見でこのことについての説明を控え､独立行政法人「情報処理推進機構（ＩＰＡ）」セキュリティセンターのホームページで公開、注意喚起を行っていますので、そっくりそのまま引用させていただきました。

以下、全文「パソコンユーザーのセキュリティ」の引用です。

＊＊

メールの添付ファイルの取り扱い　５つの心得

１．見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する
　見知らぬ相手先から送信されたメールの添付ファイルについては、安全を確認することが難しく、また、ほとんどのケースが自分に必要ないものであるので、無条件に削除することが望ましい。

２．添付ファイルの見た目に惑わされない
　テキストファイル（拡張子.txt）や画像ファイル（拡張子.jpg）等の、ウイルスに感染することのないファイルに見せかけた添付ファイルを送りつけるウイルスが発見されており、注意が必要である。添付ファイルは、見た目に惑わされず、プロパティで拡張子を表示する等によりファイル形式を確認し、ファイルを実行するアプリケーションを把握するとともに、自分に必要なものかどうかを判断した上で使用するべきである。

３．知り合いから届いたどことなく変な添付ファイル付きのメールは疑ってかかる
　メールを送信するタイプのウイルスが激増しており、知り合いから送信された添付ファイル付きのメールは、送信者の知らない間にウイルスが送信している可能性がある。巧妙に添付ファイルを開かせるような心理をついてくるので、このような知り合いからのメールこそウイルスの疑いを持って接する必要がある。メールに付帯の情報（メール本文等）もウイルスが作成している可能性があるため、これらの情報も信用せず、例えば先方に問い合わせるなどにより安全を確認してから使用するべきである。

４．メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない
　受信者にウイルス検査の作業負担を生じさせることになり、また、検査を行ったとしても不安感を完全にぬぐいさることはできないので、添付ファイル付きのメール送信は避ける。必要にせまられ添付ファイル付きでメールを送信する場合には、当該ファイルのウイルス検査を行ってから実施するようにし、併せて、メールに付帯の情報（メール本文等）以外で、添付ファイルを付けた旨とその内容を事前に先方に伝えるような配慮が望ましい。一方、このようにして届けられたものでも、受信者はウイルス検査後使用するという用心深さが必要である。

５．各メーラー特有の添付ファイルの取り扱いに注意する
　メーラーの設定、メーラーの特殊性などの添付ファイルの取り扱いに関連する事項をよく把握して使用することが重要である。例えば、一部のメーラーでは、受信時に添付ファイルをあらかじめ指定されたフォルダに自動的に展開しファイル保存する。このようなメーラーを使用している場合は、ウイルス検出等でメール本文ごと添付ファイルを削除したときに、保存されている複製も忘れずに削除されるような設定にする必要がある。

＊＊

パソコンユーザのためのウイルス対策　７箇条

１．最新のウイルス定義ファイルに更新しワクチンソフトを活用すること
　新種ウイルスに対応するために、最新のウイルス定義ファイルに更新したワクチンソフトで検査を行うことが肝要。ウイルス定義ファイルの更新にあたっては、ワクチンベンダーのWebサイトを定期的にチェックするなどし、最新のバージョンを確認しておくことが重要である。また、プリインストールされているワクチンソフトは、機能が限定されている場合もあるので、製品版にアップグレードすること。

２．メールの添付ファイルは、開く前にウイルス検査を行うこと
　受け取った電子メールに添付ファイルが付いている場合は、開く前にウイルス検査を行う。また、電子メールにファイルを添付するときは、ウイルス検査を行ってから添付する。

３．ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
　インターネットからファイルをダウンロードした場合は、使用する前にウイルス検査を行う。また、ユーザに被害を与えるプログラム（国際電話やダイヤルＱ２に接続するプログラムなどで、ワクチンソフトで発見できない可能性が高い。）が潜んでいる場合があるので、信頼できないサイトからのファイルのダウンロードは避ける。

４．アプリケーションのセキュリティ機能を活用すること
　マイクロソフト社のWordやExcelのデータファイルを開くときに、マクロ機能の自動実行を無効にするなどのアプリケーションに搭載されているセキュリティ機能を活用する。また、メーラー、ブラウザのセキュリティレベルを適切（中レベル以上）に設定しておくことにより、被害を未然に防ぐことができる。

５．セキュリティパッチをあてること
　基本的なウイルス対策を行っていても、セキュリティホールのあるソフトウェアを使用していると、ウイルスに感染してしまうことがある。 例えば、電子メールの添付ファイルの自動実行を許してしまうメーラーのセキュリティホールは、ウイルス感染被害を著しく増大させる可能性がある。 このようなセキュリティホールは、頻繁に発見されているので、使用しているソフトウェア（特に、メーラー、ブラウザ）に関してベンダーのWebサイトなどの情報を定期的に確認し、最新のセキュリティパッチをあてておくことが重要である。

６．ウイルス感染の兆候を見逃さないこと

　下記のような兆候を見逃さず、ウイルス感染の可能性が考えられる場合、ウイルス検査を行う。
1. システムやアプリケーションが頻繁にハングアップする。システムが起動しない。
2. ファイルが無くなる。見知らぬファイルが作成されている。
3. タスクバーなどに妙なアイコンができる。
4. いきなりインターネット接続をしようとする。
5. ユーザの意図しないメール送信が行われる。
6. 直感的にいつもと何かが違うと感じる。

７．ウイルス感染被害からの復旧のためデータのバックアップを行うこと
　ウイルスにより破壊されたデータは、ワクチンソフトで修復することはできない。ウイルス感染被害からの復旧のため、日頃からデータのバックアップをとる習慣をつけておく。また、アプリケーションプログラムのオリジナルCD-ROM等は大切に保存しておく。万一、ウイルスによりハードディスクの内容が破壊された場合には、オリジナルから再インストールすることで復旧することができる。

＊＊

パソコンユーザのためのスパイウェア対策　５箇条

　スパイウェア対策も、今までのウイルス対策と同じような対策が必要です。ウイルス対策でも論じられるように、ひとつの対策をしておけば大丈夫と考えるのは危険です。不正アクセス対策で言うところの多重防御が必要なので、ここに示す ５ 箇条(および補足)を実施することをお勧めします。

１．スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
　スパイウェア対策ソフトを利用することで、スパイウェアの侵入や実行を抑止することができます。ただし、対策ソフト本体や定義ファイルを常に最新の状態にしておくことが大切です。
　また、利用者が意図的にインストールしたソフトウェアがスパイウェアとして検知される場合(スパイウェアと検知される部品プログラムを含んでいるような場合)は、該当ソフトウェア(プログラム)の検知を除外する設定が必要です。つまり、利用者の責任において使用しなければならないと言うことになります。
　一部のウイルス対策ソフトには、スパイウェアを検知できるものがあります。しかしながら、これらのウイルス対策ソフトでは、スパイウェアをすべて検知し駆除することができないことが報告されています。また、スパイウェア専用の対策ソフトでも、完全と言うことはないので、これさえあればと言う過信は禁物です。

２．コンピュータを常に最新の状態にしておく
　コンピュータにある脆弱性(セキュリティホール)を利用して侵入するスパイウェアの存在が確認されています。脆弱性を解消するために、コンピュータを常に最新の状態にしておくことが重要です。
　セキュリティホールは基本ソフト(OS)だけでなく、利用されている各種のソフトウェアにも存在する場合があります。
　Windows ユーザの場合は、Windows Update または Microsoft Update を定期的に実行することをお勧めします。それ以外の OS やソフトウェアをご利用のかたは、ベンダや各種の公開されたセキュリティ情報を参照し、脆弱性が公開された場合はすぐに対処して下さい。

３．怪しいサイトや不審なメールに注意

● Webサイトの参照

悪意のある Web サイトでは、サイトを参照しただけでスパイウェア等をインストールされる場合があります。

検索エンジンで検索された怪しげなサイト、スパムメールやポップアップメッセージに記載された怪しいと思われるサイトには近づかない方が賢明です。必要ならば、後述するブラウザのセキュリティ設定を強化してから参照して下さい。

● 便利なツールのダウンロード

シェアソフトやフリーソフトを Web サイトからダウンロードする場合は、信頼できるサイトのみから行いましょう。同様な意味で、ファイル交換(P2P)から取得したソフトウェアについても注意が必要です。これらのファイルを利用(インストール)する前に、スパイウェア対策ソフトやウイルス対策ソフトで検査することを忘れないようにして下さい。

● 不審なメール

ウイルスメールと同様に、不審なメールに添付されたファイルを開くことで、スパイウェアがインストールされたり、メール本文に記載された怪しげなサイトを訪問すると、スパイウェアをインストールされたりする場合があります。

・ 不審なメールに付いた添付ファイルは開かない
・ 不審なメールに記述されたリンクは開かない

が重要です。

● 理解できないポップアップ画面や確認メッセージ

理解できないポップアップ画面や確認メッセージ(プロンプト)は、画面上のボタンを操作することで、内蔵された不正な処理が動作する場合があります。おかしいなと思ったら、×ボタンで終了しましょう。

・ ポップアップされたメッセージは×ボタンで終了する
・ 理解できない確認メッセージ(プロンプト)は×ボタンで終了する

４．コンピュータのセキュリティを強化する

● パーソナルファイアウォールを使う

外部からのコンピュータへの不正アクセスによりスパイウェアをインストールされる可能性があります。正しく設定すれば、ファイアウォールは不正なアクセスを抑止します。また、既にインストールされてしまったスパイウェアからのデータ送信を抑止することができる場合もあります（アプリケーションファイアウォール機能等）。

● ブラウザのセキュリティ設定を行う

インターネットサーフィンを行う場合、ブラウザのセキュリティ設定を行うことをお勧めします。先にも述べた、怪しげなサイトを訪問する場合、セキュリティ設定を高い状態にしておくことが重要です。利用者の意図とは関係なしに、悪意のある ActiveX やスクリプトによって、スパイウェア等をインストールされる可能性があります。

Windows ユーザで IE(Internet Explorer)を使用している場合は、インターネットのプロパティのセキュリティ設定で必ず『中』以上の設定をしましょう。

さらに、スパイウェアを論じる場合に良く取り沙汰されるクッキー(*1)については、インターネットのプロパティのプライバシー設定で必ず『中』以上の設定をしましょう。

(*1) クッキー (Cookie)
Web サーバーと Web ブラウザの間で、ユーザに関する情報やアクセス情報などをやりとりするための仕組み。

● 必要な場合以外は管理者モードを使わない

管理者モードを使用している状態で、コンピュータで不正なプログラムが動作すると、コンピュータの制御を完全に乗っ取られる可能性があります。必要でない場合は、管理者モードで動作させないことが重要です。

５．万が一のために、必要なファイルのバックアップを取る
　どんな場合でも、コンピュータの状態を安全な状態にするには、システム自体を初期化することです。コンピュータが不正なプログラムに支配された場合で、回復不能な場合は、システムを初期化して下さい。この際、大切なファイル等はバックアップしておくことが重要です。

補足．自分で管理できないコンピュータでは、重要な個人情報の入力を行わない

　不特定多数の利用者がいるネットカフェ等、自分で管理できないコンピュータでは、スパイウェアが常駐していることを前提に、銀行の口座番号やカード情報等の重要な個人情報の入力を行わないことが重要です。犯罪の被害者にならないためにも、心得て下さい。

スパイウェアとは
　スパイウェアの定義は、いまだ明確なものはありません。それは、スパイウェアがいろいろな機能の組み合わせで構成されているからです。ある特定のソフトウェアをスパイウェアであると言い切ることができないのが実情です。つまり、悪意のない個々の機能を組み合わせることで、悪意のあるソフトウェアとなっているからです。例えば、キーロガーと呼ばれる機能(キーボードから入力されたキーストロークを記録する)は、利用者個人で利用する場合、コンピュータの動作テスト等に利用されることもあり、単体では無害なものと考えられます(*2)が、この機能に、収集したデータを送信する機能やバックドアあるいはリモートアクセス機能が組み合わされることでスパイウェアになるからです。

　実際のところ、スパイウェア対策ソフトによって検知される一部のプログラムは、企業などで使われるシステム管理用ソフトの部品であったりします。このような状況で、スパイウェアを一般的に定義することが難しくなっています。また、インターネットの利便性を向上させる目的で作成されたソフトウェアについても、提供する側と提供される側での考え方の相違により、提供される側からスパイウェアであると位置付けられる場合もあります。この問題の多くは、アドウェア(*3)と呼ばれるソフトウェアとスパイウェアの区分け部分で取り沙汰されています。

　しかしながら、コンピュータやインターネットの一般利用者にとっては、自分にとって不要なものと考えるならば、キーロガーも送信機能もスパイウェアとみなしてかまわないことになります。
　そこで、パソコンユーザにとってのスパイウェアとは、『利用者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集し、利用者以外のものに自動的に送信するソフトウェア』であると言えます。

(*2)キーロガーは無害？
　キーロガーが無害かどうかの判断は難しいところです。特に不特定多数の利用者がいるネットカフェ等のコンピュータに仕掛けられた場合は、他の利用者が記録を参照できる可能性もあるので、有害となることもあります。サイバー犯罪ということで、事件の事例も報道されています。

(*3)アドウェア(Adware)
　広告を強制的に表示する機能を持つソフトウェア。利用者の画面に広告を表示する代わりに、利用者が無料で利用できる。なかには、利用者のコンピュータの環境や Web ブラウザのアクセス履歴などの情報を外部に通知するものがあり、これがスパイウェアのはじまりと言われている。

引用終了
＊＊

以上　Ｈ１７．１１．１１　つぼみ学習会テキスト　　作成　ＯＳＳ_１３４　谷村

●ローマ字入力一覧

あ	い	う	え	お	か	き	く	け	こ	さ	し	す	せ	そ	た	ち	つ	て	と
a	i	u	e	o	ka	ki	ku	ke	ko	sa	si	su	se	so	ta	ti	tu	te	to
											shi					chi	tsu		

な	に	ぬ	ね	の	は	ひ	ふ	へ	ほ	ま	み	む	め	も	や	い	ゆ	いぇ	よ
na	ni	nu	ne	no	ha	hi	hu	he	ho	ma	mi	mu	me	mo	ya	yi	yu	ye	yo
							fu												

ら	り	る	れ	ろ	わ	うぃ	う	うぇ	を		ん
ra	ri	ru	re	ro	wa	wi	wu	we	wo		nn

が	ぎ	ぐ	げ	ご	ざ	じ	ず	ぜ	ぞ	だ	ぢ	づ	で	ど	ば	び	ぶ	べ	ぼ
ga	gi	gu	ge	go	za	zi	zu	ze	zo	da	di	du	de	do	ba	bi	bu	be	bo
						ji													

ぁ	ぃ	ぅ	ぇ	ぉ	うぁ	うぃ	う	うぇ	うぉ	ヴぁ	ヴぃ	ヴ	ヴぇ	ヴぉ	カ	ケ
xa	xi	xu	xe	xo	wha	wi	wu	we	who	va	vi	vu	ve	vo	xka	xke
la	li	lu	le	lo											lka	lke

きゃ	きぃ	きゅ	きぇ	きょ	ぎゃ	ぎぃ	ぎゅ	ぎぇ	ぎょ
kya	kyi	kyu	kye	kyo	gya	gyi	gyu	gye	gyo

くぁ	くぃ	く	くぇ	くぉ	ぐぁ	ぐぃ	ぐぅ	ぐぇ	ぐぉ	どぁ	どぃ	どぅ	どぇ	どぉ
qa	qi	qu	qe	qo	gwa	gwi	gwu	gwe	gwo	dwa	dwi	dwu	dwe	dwo

しゃ	しぃ	しゅ	しぇ	しょ	じゃ	じぃ	じゅ	じぇ	じょ	すぁ	すぃ	すぅ	すぇ	すぉ
sya	syi	syu	sye	syo	zya	zyi	zyu	zye	zyo	swa	swi	swu	swe	swo
sha		shu	she	sho	jya	jyi	jyu	jye	jyo					
					ja		ju	je	jo					

ちゃ	ちぃ	ちゅ	ちぇ	ちょ	ぢゃ	ぢぃ	ぢゅ	ぢぇ	ぢょ	つぁ	つぃ	つ	つぇ	つぉ	っ
tya	tyi	tyu	tye	tyo	dya	dyi	dyu	dye	dyo	tsa	tsi	tsu	tse	tso	xtu
cha		chu	che	cho											ltu
cya	cyi	cyu	cye	cyo											

てゃ	てぃ	てゅ	てぇ	てょ	でゃ	でぃ	でゅ	でぇ	でょ	とぁ	とぃ	とぅ	とぇ	とぉ
tha	thi	thu	the	tho	dha	dhi	dhu	dhe	dho	twa	twi	twu	twe	two

にゃ	にぃ	にゅ	にぇ	にょ
nya	nyi	nyu	nye	nyo

ぱ	ぴ	ぷ	ぺ	ぽ	ぴゃ	ぴぃ	ぴゅ	ぴぇ	ぴょ	ひゃ	ひぃ	ひゅ	ひぇ	ひょ
pa	pi	pu	pe	po	pya	pyi	pyu	pye	pyo	hya	hyi	hyu	hye	hyo

びゃ	びぃ	びゅ	びぇ	びょ
bya	byi	byu	bye	byo

ふぁ	ふぃ	ふ	ふぇ	ふぉ	ふゃ	ふぃ	ふゅ	ふぇ	ふょ
fa	fi	fu	fe	fo	fya	fyi	fyu	fye	fyo

みゃ	みぃ	みゅ	みぇ	みょ	や	ゆ	よ	りゃ	りぃ	りゅ	りぇ	りょ	わ
mya	myi	myu	mye	myo	xya	xyu	xyo	rya	ryi	ryu	rye	ryo	xwa
					lya	lyu	lyo						lwa

小さい文字

ぁ	ぃ	ぅ	ぇ	ぉ	カ	ケ	っ	ゃ	ぃ	ゅ	ぇ	ょ	わ
xa	xi	xu	xe	xo	xka	xke	xtu	xya	xyi	xyu	xye	xyo	xwa
la	li	lu	le	lo	lka	lke	ltu	lya	lyi	lyu	lye	lyo	lwa

変換を使って

wi → うぃ →「変換」→ ゐ ヰ

we → うぇ →「変換」→ ゑ ヱ