ウィルスの脅威から身を守る

☆これは、「シニアのための　ゆうゆうパソコンシリーズ」の《ウィルスの脅威から身を守る/技術評論社/14.4.25/￥880+Du》を要約し、多少の添削を加えたものです。

はじめに

ウィルスに感染すると、ウィルスを駆除するのに大変な苦労を強いられることになります。そのうえ、うっかりしていると、大切な友人にウィルスを送りつける加害者になりかねません。そのような事態から逃れるためにも、ウィルスについての最小限の知識と知恵を身に付けたいと思います。

ウィルスから身を守る最も有効な対策は、普段の予防と防御です。

予防と防御対策の記述は、第１、第２、第４、第６章にあり、感染した時の記述は第３章です。また、警告については第５です。

なお、図を沢山載せているこの本は、まだ在庫がありましたので、図を見ながら詳しく学習したい方は、この HP を訪ねて注文されたら如何でしょうか？

＜http://market.bookservice.co.jp/top/index.html＞

第１章　コンピュータウィルスとは？

目次

１、コンピューターウィルスの正体

＊コンピューターウィルス（以後ウィルスという）は、コンピュータ専門のウィルスで、１つのプログラムです。

＊ウィルスの特徴は、「密かにパソコンに感染し、増殖していく」ことです。

＊ウィルスの行動は、感染→潜伏→発病の過程をとります。

＊感染の仕組みは、インターネット、メールなどにアクセス（接触）した時、ウィル

スのプログラムが、データとして送り込まれ、それを実行した時に感染します。

＊コンピュータに入り込んだウィルスは、HD（ハードディスク）の見つかり難いところに潜み、活動のチャンスを待ちます。この状態を潜伏期といいます。

＊活動の時がくると、特定の日にコンピュータの HD に記録されていたいろいろなアプリケーションプログラム（ワード、エクセル、アウトルックなど）や苦労して作った書類などが全て消えたり、勝手に音楽が鳴り出したり、時にはパソコンがどうにも動かなくなったりします。また、勝手にメールを送りつけたりします。これが発病です。

＜ポイント＞

１、ウィルスは、利用者が意図しないにもかかわらず、他のパソコンに伝染するプログラムです。

２、コンピューターウィルスは、当然人間には伝染しませんが、仕組みの違うコンピュータ（Mac、UNIX）にも伝染しません。

２、どんなウィルスがあるのか

＊作成方法による分類

W32/Sircam（ダブリュウさんじゅうに）や VBS/Loveletter 、X92　のように、頭に付いている W32・VBS・X92 などから、作られ方が判ります。

W32 は主に、XP/2000 用として作られたもので、VBS はインターネット用の言語の「VS スクリプト」で作られたもので、X92 はワードやエクセルのマクロ（繰り返し作業を自動化する）で作られたもの（マクロウィルスともいう）等に分類されている。

＊行動による分類

ネットワークやコンピュータ上で、単純に自己増殖をするようなものを「ワーム＝いも虫」と呼んで分類している（今流行っている Klez E、Klez H がこれで、頭に WORM_が付いている）。

侵入したコンピュータの情報を持ち出すプログラムを持ったウィルスは「トロイの木馬＝トロージャン」と呼んで分けている。

エクスプローラで、インターネットにアクセスした時、勝手に、ウィンドウが次から次へと止めどなく開き、操作不能にするものを「ブラウザクラッシャー」と呼んで分類されている（ウィルスに入れないときもある）。

また、ウィルスとは呼ばないものの、迷惑なプログラムが幾つかあります。しかし、ここでは省略します。

＊最近流行した主なウィルス

＜その１、W32/Sircam（サーカム）について＞

１、ウィンドウズ 95/98/Ｍｅ/ＸＰ等に感染する。

２、メールの添付ファイルとして広まる。

３、本体は巧妙に作られた、蔓延しやすいプログラム。

４、添付ファイルの拡張子は.EXE（EXE 形式)。

（EXE 形式とは、ワープロ文書や表計算のデータと異なり、自身で動作できるファイルやプログラムのこと）

５、添付ファイルを実行する（開く）と感染する。

６、このウィルスには幾つもの亜種（枝別れした種類）がある。

７、症状は悪質で、１０月１６日にＣドライブ(普通はウィンドウズが入っているHD)の全ファイル、ディレクトリを削除する。

８、さらに問題なのは、「情報を持ち出す」ことで、次に感染させるパソコンにワードやエクセルのデータファイルをメールの添付ファイルで送信する（秘密の情報が盗み取られる)。

９、このウィルスは、本体そのものが添付ファイルになっているのではなく、添付されたワード書類やエクセル形式のデータの１部として届けられる。

▽ワードやエクセルファイルを装っていて、ウィルスと判別し難い▽

10、ファイル名は変わるが、本文は英語で、最初の行は「Hi！ How are you?」

＜その２、W32/Hybris（ハイブリス）＝WORM_KLEZ.H について＞

１、ウィンドウズ 95/98/Ｍｅ/ＸＰ等に感染する。

２、メールの添付ファイルとして広まる。

４、添付ファイルの拡張子は.EXE（EXE 形式)。

５、添付ファイルを実効する(開く)と感染する。→今ではプレビューでも感染する

６、このウィルスは自分で亜種を作ることができる。

７、いろいろな名前でウィルスを送信する。

８、日本語のウィンドウズが送信元の時は、題名（件名）差出人は空白。

（英語の時は、差出人が「hahaha」となることが多いらしい）

９、添付ファイルそのものが本体で、「不特定の８文字のアルファベット＋「.exe」の名称になっている。

10、アウトルックエクスプレスやエクスプローラにあるメールアドレスを抽出して、メールを送信する。

３、ホームページでウィルスチェック

＊手軽にできるウィルスチェック

感染しているかいないかをチェックするだけなら、インターネットでできる。

例えば、「ウィルスバスター」を発売しているトレンドマイクロ社の HP では、「ウィルスバスター、オンラインスキャン」を公開提供していますので、これにアクセスして感染のチェックができる（Mac はできない）。

１、エクスプローラを起動し、メニューから「ツール」→「インタネットオプション」を選ぶ。

２、開いたウィンドウで、「セキュリティ」のタブを選び、「レベルのカスタマイズ」をクリックして、セキュリティの設定をする。
次に、「ActiviX コントロールとプラグインの実効」と「スクリプトを実行しても安全だとマークされていない ActiviX コントロール」の両方を「有効にする」に設定する。

３、「ウィルスバスター、オンラインスキャン」のページ
＜http://www.trendmicro.co.jp/hcall/scan.html＞を表示させて、
「ウィルスバスター On-Line Scan」と書かれている部分をクリックする。

４、ウィルスチェックをしたい HD（通常はドライブ C）を選んで「検索」ボタンをクリックすると、検査が始まる。
注意）感染したウィルスに対しては駆除用のソフトが必要です。第３章参照。

第２章　ウィルス対策ソフトを活用しよう

目次

１、ウィルス対策ソフトの役割

☆ウィルス対策ソフトの機能は予防と駆除の２つです。

対ウィルスソフトは、今までのウィルスのデータを調べて、パターン化しておき、常にパソコン内を走り回ってこのパターンに似たものがあるかないかを探します。したがって、常に新しいウィルスのパターンを組み込んだものが要求されます。と同時に、ウィルス対策ソフトを常に更新することが大切です。そして、時々起動してチェック＝検索することが必要です。

ウィルス対策ソフトには、日本ネットワークアソシエイツの「Virus Scan/ウィルススキャン」、シマンテックの「Norton AntiVirus/ノートンアンチウィルス」、トレンドマイクロの「ウィルスバスター」の３種類があります。前２社は、プレインストールされていることが多いようです。

２、パソコンに入っているウィルス対策ソフトの使い方

＊ウィルススキャンの使い方

（このソフトには、スキャン操作用とデータの監視用の２つアイコンがある）

まずパターンファイルの更新をする。そのためには、タスクバーに並んでいる、ウィルススキャン関係の２つのアイコンの左側をクリックして、「Virus Scanコンソール」を開く。

次に、パターンファイルを示す「ＤＡＴの自動アップデート」をダブルクリックして、開いた画面で「今直ぐ実効」をクリックする。

パターンファイルの更新が済んだら、もう一度、「Virus Scan コンソール」を開いて、「C ドライブのスキャン」をクリックで選択し、「実効」ボタンをクリックすれば、ウィルスチェックができる。

＊ノートンアンチウィルスの使い方

まず設定をする。アンチウィルスの「初期設定」の画面が出るので、使用許諾契約に同意し、出て来た画面で購読（ウィルス定義のダウンロード）サービスの期間を確認し、「次へ」をクリックする。現れた作業の選択画面（インストール後のタスク）では、３つのボタンに全部チェックが入っているので、そのまま「次へ」をクリックする。最後に確認（概略）の画面がでるので、「完了」をクリックする。

次は定義ファイルの更新です。

現れた「定義ファイルの更新手順」の画面で、「次へ」をクリックする。更新の必要なプログラムがリストアップされる。

ここで、インターネットにアクセス（接続）する。アクセスできたら、「次へ」をクリックする。しばらくして更新作業が終了すると、「確認画面」が出る。そこで

「完了」をクリックする→完了。

ここで、更新したプログラムを有効にするために、パソコンを再起動します。

次に、パソコン全体をスキャンする。

パソコンが起動（セットアップ）したら、タスクバーの「ノートンアンチウィルスのアイコン」をダブルクリックして「ノートンアンチウィルス」を起動させる。

（起動には他の方法もあるが省略）

「システム状態；緊急注意」の画面が出る。ここで「システムの完全スキャン」をクリックして選び、右下の「今すぐスキャン」をクリックする。

また、個々に分けてスキャンする時は、「システムの完全スキャン」を選ばずに、左の「ウィルススキャン」をクリックし、タスクのリストからスキャンしたい装置をダブルクリックで選んだスキャンする。

３、市販ウィルスソフトの利用

＊ウィルスバスターのインストール

購入したウィルスバスター2002 の CD-ROM をドライブに挿入し、出て来た画面で「インストール」をクリックし、現れた「ユーザー情報」の画面で、名前とシリアル番号を入力（書き込み）し、「次へ」をクリックする。

（シリアル番号は CD-ROM のケースなどに記載されている）

次に、インストールファイル（新規に作ってくれる）を確認して「次へ」をクリックする。変わった画面で、「インストール」をクリックする。しばらくして、インストール完了画面が出たら、「完了」をクリックする→完了。

インストールが終わると、「オンライン登録」の画面が出るので、「登録する」をクリックする。

ここでインターネットに接続する。「ユーザー登録」画面が出る。この画面で手順２の枠の「オンライン登録」をクリックし、出て来た画面の「ライセンスキー」を記録しておき、次に、前の画面の手順３の枠の指示に従ってライセンスキーを入力し、「ライセンスキー」ボタンをクリックする。

登録完了確認画面で「OK」をクリックする→登録完了。

登録完了に続いて、自動的に最新のパターンファイルのアップデート（更新）作業が始まるので、出て来た画面で「はい」をクリックする。

（以後はタスクバーにあるアイコンをダブルクリックなどしてアップデート画面を開いて行う）

更新が終わると、「現在の状況」と書いてある「操作画面」がでる。ここで「全ドライブ検索」をクリックする。進行状況が出たのち、検索終了の確認画面になるの

で、「OK」を選ぶ→検索終了。

＊救済ディスクの作成

救済ディスクは、ウィルスによってパソコンが動かなくなった時に、パソコンを起動させ、潜んでいるウィルスを駆除するためのものです。

＜救済ディスクの作成手順＞

１、フォーマットを施したフロッピーディスクを６枚用意する。

２、パソコンの「スタート」（クリック）→「プログラム」（クリック）→「ウィルスバスター２００２」→「救済ディスク作成」と順にたどり、「救済ディスク作成」選んで起動する。そして確認画面で「はい」をクリックする。

３、「すべて」を選んで、「次へ」をクリックする。

４、以後は、指示に従って順次必要な作業や項目を選んで「次へ」をクリックしていく。

５、作成作業が終わったら、「完了」をクリックする→完了。

第３章　感染した！さあ、どうしますか？

目次

１、ウィルスに感染したらすべきこと

☆ウィルス対策ソフトを導入しても安心できません。なぜならば、以下のようなことが挙げられます。

１、パターンファイルの更新を忘れている。

２、自動的に駆除できないウィルスもある。

３、初めてウィルスに感染して、慌てて当てもないキーを叩いてしまう。

＊パソコンがこんな症状のときは危ない

「ウィルスの潜伏段階」

潜伏段階のウィルスは、目につかないように隠れていようと、おとなしくしています。しかし、下記のようなある程度の特徴的な症状を現わします。

１、見なれないファイルが大量にできるようになった。

２、あるファイルが正常に動作しないようになった。

（例えば、MP３という音楽データファイルで音楽を演奏できなくなった）

３、エクスプローラやワープロでの編集中に文字化けが頻発するようになった。

また、ウィルスプログラムの殆どが外国産のため、日本語を使う（MIME）ことを余り考慮していないため、感染したメール、ブラウザー、ワープロなどのソフトは、日本語の文字の処理に失敗して、文字化けを起こすこともあります。

このような異常を感じたら、前記の「オンラインウィルススキャン」やウィルス対策ソフトを使ってスキャンおよび駆除をしなくてはなりません。

「ウィルスの発症段階」

発症時にはウィルスをばらまいたり、破壊活動をするので、PC の調子が明らかに悪くなり、以下のような症状を現します。

１、動作が異常に遅くなる。

２、コンピュータが起動しなくなる。

３、全く操作できなくなる。

４、画面に変な文字や絵が現れたり、表示が乱れる。

また、HD の内容が全部消えてしまうこともある。このような異常な現象を見たら、即刻、ウィルス対策ソフトを使ってチェックおよび駆除をする。

☆感染したことに気付かずに、もしあなたの感染したパソコンからウィルスをばらまくようなことになると、自分が次の感染源になり、うつされた知人から「ウィルスをうつさないでくれ」というメールが届き、初めて自分がウィルスに感染していたことが判ることになります。

＊感染後の駆除手順

感染しても、コンピュータが動くならば、下記の対処および手順でウィルスの駆除を試みます。

１、ウィルス退治の準備

２、他のコンピュータへの感染防止

３、データの保存

４、ウィルス削除の実行

「ウィルス退治の具体的な手順」

１、まず、インターネット、イントラネット、イーサーネットなどの接続を全て切る（通信ケーブルをパソコンから抜き取るのが一番安全)。

２、コンピュータを起動する。

３、HD 内のデータを CD-R/RW、MO、FD などにドラッグなどして保存する（後で、ウィルス対策ソフトで安全を確認してから元に戻す)。

４、更新したウィルス対策ソフトを起動し、コンピュータ全体をスキャンさせて、ウィルスを駆除する。

５、次に、前３、で保存したデータをスキャンさせて、ウィルスを駆除する。

注意）システムを管理しているレジストリまでウィルスが入った場合は、通常のウィルス対策ソフトでは駆除できないので、ここでは省略します。

２、ウィルス対策ソフトでのウィルス駆除

＊一般的なウィルスの駆除（自動的駆除）

前項（４、）の通り、更新したウィルス対策ソフトをスキャンさせることで、自動的にウィルスを駆除できる。

ここで注意したいのは、感染したファイルの場所、名前を確認しておくこと。知人からのメールの添付ファイルであれば、知人に速やかに警告した方がよい。また、ソフトによっては駆除と削除を区別しているものもある。削除はファイルごと捨てることで、駆除はファイルは捨てないで、取り付いたウィルスを退治することです。

＊自動的に駆除できないウィルス（手動的駆除）

自動的に駆除できないケース

１、「ウィルスらしい」とウィルス対策ソフトが診断したファイル

２、感染したが削除できない重要なファイル

これらのファイルは、他のファイルへの感染を防ぐために、「隔離」する。

☆ただし、ファイルの重要度などが判断できない初心者の場合は、削除する方が無難です。

「手動削除の手順」（例；ウィルスバスター2002/他も基本的には同じ）

１、ウィルスバスター2002 で PC をスキャンさせる。

２、「ウィルスを駆除できません、感染ファイルを隔離しました」というコメントが出たら、慌てずに、「閉じる」ボタンをクリックする→隔離完了。

３、ウィルスバスター2002 を再起動する

４、操作画面の左上の「プロフェッショナル」タブをクリックし、出て来たリストから、「ウィルス隔離」をクリックする。

５、右下に表示された隔離ファイルをクリックし、中央部にある処理法を選び（重要でない時は削除）、確認画面で、「はい」をクリックする。

☆重要なファイルの時は、「ウィルス駆除」を選び、パターンファイルの更新をしてから再度駆除をする。

３、ウィルス対策ソフトメーカーからのアドバイス

有効度が低いので省略します。

第４章　安全のための基本対策

目次

１、ウィンドウズの安全設定

☆ウィンドウズ、エクスプローラやアウトルックのセキュリティホール（安全対策面での欠陥点）が常にウィルス（ウィルス製作者）に狙われています。したがって、メーカーは常にソフトの改良を余儀無くされています。ユーザーは、こうした改良されたソフトを逐次導入することによって、防衛効果・安全度をあげることができます。

また、上記に加えて、ワードやエクセルも、利用者自ら安全度を設定することが

できます。

＊Windows Update　を利用する

Windows の Me(ミレニアムエジション)、XP　はWindows Update機能によって、簡単に最新の改良版に更新できる。以下はその手順を示す。

１、スタートメニュウを開いて、「Windows Update」をクリックする。

２、インターネットにアクセスして開いた「Windows Update」画面で、「製品の更新」をクリックする。

３、更新できる項目が出たら、特に、「重要な更新とService Pack」の中にあるものは、必ず更新する。

４、後は指示に従ってダウンロードする。

＊ウィンドウズMeとXPの共通したセキュリティ設定

「VBスクリプトの関連付けを削除」

ウィルスの一部に「VBスクリプト」という言語で作られた普通のファイルの形をしたものがあります。したがって、ダブルクリックで開きます。そこでは、「VBスクリプト」で書かれたファイルは、ダブルクリックでは開かないように設定します。以下にその手順を示ます。

１、適当なファイルを開き、「ツール」メニュウの「フォルダオプション」をクリックする。

２、「フォルダオプション」画面で「ファイルの種類」タブをクリックする。

３、スライダーを上下して「VBS」を探し、クリックで選択し、「削除」ボタンをクリックする。

４、確認画面で、「はい」をクリックする。

「拡張子を表示する（させる)」

ウィンドウズMe と ウィンドウズXP　は、標準の設定では拡張子を表示していませんが、拡張子（ .doc や .exe）が付いていないと、どのようなファイルや文

書なのか見当がつきません。したがって、アイコンが違っていても、名前が同じだったりすると、ウィルスのファイル（.exe）を開いてしまう危険があります。

このうっかり間違いを防ぐために、拡張子を表示させます。

拡張子の表示設定は以下の手順です。

１、「ツール」メニュウの「フォルダオプション」をクリックする（前項参照)。

２、「フォルダオプション」画面で「表示」タブをクリックする。

３、スライダーを上下して「登録されているファイルの拡張子は表示しない」を探し、クリックでボタン内のチェックマークを外す。→設定完了

＊ウィンドウズ XP のセキュリティ設定

＜ファイアウォールを利用しよう＞

ファイアウォールとは、インターネットや他のパソコンなどとの接続経過状態を記録する機能です。そして、インターネットを通してパソコンのセキュリティホールを探し出して、そこに入り込もうとするウィルスを防いだり、情報を持ち出そうとするウィルスからコンピュータを守る機能です。

ここでは「ウィンドウズ XP」だけが持っている機能である、このファイアウォールを利用できるように設定する。

ファイアウォール設定は以下の手順です。

１、「スタート」→「アクセサリ」→「通信」→「ネットワーク接続」と辿り、「ネットワーク接続」を開く。

２、利用している通信ラインの種類（ADSL=LAN または高速インターネット、普通のモデム＝ダイアルアップ）をクリックで選ぶ。

３、出て来た枠内から「プロパティ」をクリックで選ぶ。

４、出て来た画面で「詳細設定」タブをクリックし、「インターネット接続ファイアウォール」の欄の「インターネットからコンピュータへのー」をクリックして、ボタン内にチェックマークを入れる。→設定完了→有効

２、ウィンドウズソフトの安全設定

＊インターネット・エクスプローラのセキュリティ設定

インターネット・エクスプローラは、最も危険の多い、インターネット関係の玄関になっているため、最も攻撃されやすいソフトです。したがって、「常に最新の状態に更新しておくこと」が大切です。

＜ゾーンとセキュリティの設定＞

ゾーンとは、「インターネット」、「信頼済みサイト」、「制限付きサイト」などと HP に接触する時の危険度によって分類した帯域を指します。

エクスプローラ 6.0 を例に手順を示します。

１、インターネット・エクスプローラを開き、「ツール」から「インターネットオプション」を開きく。

２、出た画面で「セキュリティタブ」をクリックし、枠内から「インターネッ

ト」をクリックで選び、一般的な「中」レベルを選ぶ。

注意）「中」より高くすると、[Windows Update] が利用できなくなります。

３、同様に、「信頼済みサイト」ゾーンでは、「信頼済みサイト」をクリックし、「サイト」をクリックして選ぶ。

４、登録画面で、「このゾーンのサイトにはすべての確認ー」をクリックして、安全が確認されている HP のアドレスを登録できるようにし、セキュリティレベルの最も低い「低」に設定する。

５、３、４、と同様の方法で、危険な HP は「制限付きサイト」に登録をし、最もハードルの高い「高」を設定する

＊インターネット・エクスプローラのより細かい設定

初心者向きではないので省略します。

＊アウトルック・エクスプレス のセキュリティ設定

アウトルック・エクスプレス（ＯＥ）はウィンドウズの標準付属のメール用ソフトです。

そのため、メールの内容表示などではＩＥ（インターネットイクスプローラ）の支配と手助けを受けています。したがって、ウィルスに弱いＨＴＭＬ形式のメールや添付書類（ .html,　.exe）の防御対策としては、ＩＥとセットと考えて、常に更新し、それぞれに適切な設定をすることは不可欠な作業です。

ＯＥ（アウトルック・エクスプレス）のセキュリティ設定は以下の手順です。

１、「ツール」メニュー　→　「オプション」を開く。

２、「セキュリティ」タブをクリックし、「ウィルス防止」の欄で、まず「制限付きサイトゾーンー」をクリックし、次に「ほかのアプリケーションが私の名前でメールを送信使用としたら警告」と「ウィルスの可能性がある添付ファイルを保存したり開いたりしない」をクリックしてチェックマークを入れる。

３、「表示」メニュウ　→　「レイアウト」を開く。

４、「プレビューウィンドウ」の欄の「プレビューウィンドウを表示する」をクリックでチェックマークを外す。

注意）プレビューができず不便ですが、今流行っているウィルスには不可欠

＊ワードとエクセルのセキュリティ設定

ワードでの文書の作成やエクセルでの表計算の処理などで、比較的頻繁に使われる決まった手順を決めておき、必要な時に引き出して使う機能をマクロ機能

といいますが、このマクロ機能がウィルス（マクロウィルス）に狙われやすいのです。

このマクロウィルスに対するセキュリティ設定は以下の手順です。

１、ワードを開き、「ツール」　→　「マクロ」　→　「セキュリティ」を開く。

２、「セキュリティレベル」タブで「中」をクリックで選ぶ。

（これでマクロが設定されたファイルを開く時に警告メッセージが出る。
また、「高」の設定は安全だが不便になる）

３、多くのマクロウィルスは標準テンプレートにいたずらするので、標準テンプレートに変化があった時に警告を出させるための設定をします。
「ツール」　→　「オプション」を開き、「保存」タブをクリックし、「標準設定を変更するかどうかを確認する」をクリックしてチェックを入れる。

第５章　インターネットに潜む危険

目次

１、ウィルス以外も危険が一杯

＊むやみにクリックしない

インターネットに参加している人の中には、ウィルスを送り込むものだけでなく、悪戯をしてみたいもの、個人情報を盗みだしたいもの、お金をだまし取ろうとするものなど、真面目な人にとって、甚だ迷惑な人たちも少なくありません。彼等は、ＨＰ上で隙あらばと、狙っていることを忘れてはいけません。

１、無料のＨＰや管理の行き届かないＨＰなどの掲示板にあるＵＲＬ（ＨＰのアドレス）などは危険が多いので、クリックしないこと。（先に述べたブラ

ウザクラッシャーなどを拾うことがある）
また、掲示板への記入も注意が必要です。匿名の筈が匿名ではなく、いろいろな個人情報が出てしまうこともあります。

２、アダルトもののＨＰは要注意です。「もっと見たい人はここをクリック」などをクリックすると、写真を見ている間に、いつの間にか国際電話に回され、登録されてしまいます。次からは自動的に国際電話をかけることになり、後で、吃驚するような電話料の請求書を見て気が付くようなことが起こります。

＊情報はこれだけもれている

インターネットにアクセスする時、かならずＨＰやメールサービスを提供するサーバーと呼ばれる大容量のコンピュータを通ります。したがって、利用者のかなりの情報（愛知西部の江南市、パソコン名、ウィンドウズ９８、場合によってはユーザー名まで）はサーバーに掴まれているものと知ることです。

特に通販のＨＰ関係のサーバーには、このお客さんは何時どこのＨＰのどこを訪ねたか、を追跡する裏ソフトのクッキー（Cookie）が走っています。

したがって、銀行名、講座番号などを入力して送る通販は、相当に個人情報が漏れていると考えなくてはなりませんし、慎重に行うことが大切です。

２、危険をさけるインターネットの使い方

＊知らない人からのメールに注意

ウィルス感染の大多数（約 90%）はメールからです。
ウィルスと疑うポイントは幾つかあります。

１、本文がないのに、ファイルが添付されている。
２、添付ファイルのファイル名が文字化けしている。
３、件名、本文がローマ字や英文で書かれている。
注意）この場合、知人の名前のときは特に危険です。
４、送信者名、件名が文字化けしている。

メールの添付ファイルには特に注意が必要です。ウィルスは一つのプログラムで、ある程度の大きな容量を持っているので、本文で送り難いのです。なかでも、ダブルクリックで実行する形式のもの、すなわち、拡張子に .exe、 .pif、 .bat が付いているものは最大限の警戒が必要です。

送られて来たメールにこれらの特徴があったら、読まずに捨てるのがよいでしょう。

＊忘れずに更新する

先にも記述した通り、ウィルスはOS も含めて、いろいろなソフトのセキュリティホールを突いて来ます。したがって、ソフトが改善される度に、手まめに更新することが大切です。

＊プロバイダーのセキュリティサービス

プロバイダー（インターネット接続業者）はサーバーを持っていて、ＨＰのサービスやメールのサービスをやっていますが、最近では、セキュリティサービスを提供するところが増えてきました。

現在契約しているプロバイダーが、メールのウィルスに対するセキュリティサービスを提供しているならば、個人がやるよりも速やかな更新ができ、より完全に近いセキュリティ環境が得られるので、また、料金も比較的安いようなので、セキュリティサービス契約は大変有効なウィルス対策の一つでしょう。

プロバイダーとのセキュリティ契約と、個人のＰＣでのセキュリティ対策が重なれば、より安全になることでしょう。

＊インターネットは油断大敵

これまでにほとんど全部を記述してきたので、省略します。

第６章　万が一に備えてバックアップをとろう

目次

１、バックアップの基本はコピーから

＊ファイルをコピーして安全対策

ウィルス対策だけでなく、大切な文書や苦労して作った文書、大切な記録や苦

労して集めたデータなどを、うっかり削除してしまう単純ミスから守る必要があります。

また、パソコンがどうにも動かなくなり、修理に出すはめに陥ることもあります。このときは、ＯＳ以外はすべてなくなることがあることを覚悟しなくてはなりません。このようなことを考慮するだけでも、普段からファイルのバックアップをとって、保存しておくのが賢明と言えるでしょう。

ウィルスのことを考えれば、一層その必要性が強くなります。

ファイル、フォルダをコピーする媒体としては、ＦＤ（フロッピーディスク＝3.5インチＦＤ）、ＣＤ-Ｒがあります。また、別個にドライブ装置を取り付ければ、ＭＯ（光磁気ディスク）やＨＤ（ハードディスク）もあります。

＊ウィンドウズＸＰならＣＤ-Ｒへの書き込みも簡単

写真などの容量の大きいファイルのコピーには、記録容量の大きいＣＤ-Ｒ、ＭＯ、ＨＤが有利です。ウィンドウズＸＰは標準でＣＤ-Ｒへの書き込みができるので、コピー、保存が容易です。

２、お気に入りとアドレス帳をバックアップする

＊お気に入りのバックアップ

利用価値の高いホームページのアドレスはＩＥの「お気に入り」ファイルに入っていますので、何かのときのためにコピーをとっておきます。その手順は以下の通りです。

＜エクスポート＝保存の手順＞

１、ＩＥの「ファイル」　→　「インポートおよびエクスポート」をクリックで選び、ウィザード画面を出す。

２、そこで「次へ」をクリックし、「お気に入りエクスポート」をクリック選択し、「次へ」をクリックする。

３、「Favorites」フォルダを選び、「次へ」をクリックする。

４、「ファイルまたはアドレスにエクスポートする」を選び、ファイル名（bookmark html）を入力して、「参照」をクリックし、ＦＤなどを指定し、「次へ」をクリックする。

５、ウィザードの完了画面が出るので、「完了」をクリックする。

６、「お気に入りのエクスポートに成功しました」のメッセージが出るので、「ＯＫ」を押す。→終了

＜インポート＝ＨＤへ移植の手順＞

１、ＩＥの「ファイル」　→　「インポートおよびエクスポート」をクリック

で選び、ウィザード画面を出す。

２、そこで「次へ」をクリックし、「お気に入りインポート」をクリック選択し、「次へ」をクリックする。

３、「ファイルまたはアドレスからインポートする」を選び、「参照」をクリックし、ＦＤを選び、「book mark html」を選び、「次へ」をクリックする。

４、「Favorites」フォルダを選び、「次へ」をクリックする。

５、ウィザードの完了画面が出るので、「完了」をクリックする。

６、「お気に入りのインポートに成功しました」のメッセージが出るので、「ＯＫ」を押す。→終了

＊アドレス帳とメッセージのバックアップ

アドレス帳は貴重な財産ですから、是非バックアップをとって保存しましょう。保存の手順は以下の通りです。

＜アドレス帳のエクスポート＝保存の手順＞

１、0Ｅを起動する。

２、「アドレス」をクリックする。

３、「エクスポート」　→　「アドレス帳」をクリックして開く。

４、「保存する場所」では「3.5インチFD」を選び、ファイル名を付けて「保存」をクリックする。

５、「アドレス帳が次の場所にエクスポートされました」のメッセージが出るので、「ＯＫ」を押す。→終了

＜保存したアドレス帳のインポートの手順＞

１、アドレス帳を保存した「3.5インチFD」をドライブに入れる。

２、アドレス帳の画面で、「インポート」を選び、右側の「アドレス帳」をクリックする。

３、「アドレス帳」の場所（3.5インチFD）を表示させ、保存しておいた「アドレス帳」を選び、「開く」ボタンをクリックする。

４、「インポートは完了しました」のメッセージが出るので、「ＯＫ」を押す。

＜メールの本文（メッセージ）を保存する手順＞

１、保存したいメールを開き、「ファイル」　→　「名前をつけて保存」をクリックして選ぶ。

２、開いた「名前をつけて保存」の画面で、保存先に「3.5インチFD」を選ぶ。ファイル名には自動的にメールの題名が入るが、ファイルの種類はメールの「.eml」か、テキストの「.txt」をスクロールして選ぶ。

＜保存したメールの本文（メッセージ）をインポートする手順＞

１、メールを保存したFDをドライブに入れる。
２、「マイコンピュータ」　→　「3.5インチFD」を選び、メールのファイルをダブルクリックで開く。
３、「ファイル」　→　「フォルダにコピー」をクリックで選ぶ。
４、ＯＥのフォルダが出るので、そこで戻したいフォルダを選び、「ｏｋ」をクリックする。

おわりに

ウィルスをばらまかないこと、すなわち罹らないこと、そのための対策にはいろいろありましたが、予防が最も効果的でした。

不幸にして感染したときは、慌てずに、確かな手順を一つ一つ順を追って処理すること、が求められました。

統合的な防衛と保全対策としてはバックアップがあります。

今まで述べたバックアップは、これまでに集めた情報およびデータや苦労して作った文書などのファイルやフォルダを取り上げていましたが、本当は、正常に働いている状態の時のＯＳおよびアプリケーションソフトとその設定条件を一括コピーして保存しておくのが理想的でしょう。

この正常な状態の一括コピーが保存されていれば、満一ウィルスに汚染された時やＨＤがクラッシュして動かなくなったりしたときでも、このコピーから起動し、不具合を起こしたＨＤを初期化し、逆コピーして、自分で正常に動くようにすることができるでしょう。

ただし、容量が比較的大きくなりますので、メディア（記録媒体）にはＣＤ−ＲやＭＯまたはＨＤが必要になります。

パソコンが２台ある場合は、外付けのＨＤ（ドライブ付き）を持ったと同じこと、になりますので、互いにバックアップをとりあって保存しておくのは、大変有効な方法の一つでしょう。

何はともあれ、まずウィルス対策を万全にして、メールやインターネットを存分に楽しみましょう。

青柳 房二

H14.06.09