Windows システムのセキュリティ入門

安田伸一（経済学部）
yasudas@cc.saga-u.ac.jp

1. ネットワークの危険

本稿では、情報のセキュリティを守る点から Windows パソコンのネットワークの設定や使い方を説明します。具体的な設定方法などは Windows 98 と Windows 95 を中心に説明し、特に重要な事柄について Windows NT にも簡単に触れます。

1.1 ネットワーク利用の変化

今でも一部の離島では、外出中に戸締りをしないそうです。訪ねてくる人は、すべて顔見知りだからでしょう。以前のコンピュータ・ネットワークも同じでした。JUNET や BITNET を使っている人々は、計算機工学という同じコミュニティに属している仲間の意識がありました。また、NetWare や LAN manager を使ってファイルやプリンタをネットワークで共有する場合も、同じ職場のパソコンとだけつながっていましたので、業務の妨害や情報の盗難などネガティブな心配がなく、使い勝手を悪くするような制限事項には意識が働きませんでした。

しかし、現在のコンピュータ・ネットワークは、パソコンの利用者にとって二つの点で状況が変わっています。一つ目は、コンピュータが普及し、またコンピュータ・ネットワークがインターネットにつながる形で普及したことによって、さまざまな人が同時に参加するネットワークになっていることです。これは、必ずしも同じ価値観や方法論を持つ人だけでコンピュータ・ネットワークを利用しているわけではなく、スキルの差や悪意のある人の存在を意識しなくてはならなくなったことを表します。

二つ目は、Microsoft Windows 98 や Microsoft Windows 95（以下、Windows 98/95）が、インターネットの利用やファイル共有機能をユーザに意識させずに利用できるようにする設計方針を持っていることです。これは、パソコンの持ち主が自分のパソコンで今、何が起こっているのか、わかりにくくなってきたことを表し、持ち主の知らないところでデータの盗難などの被害に遭う可能性があるということです。

そこで本稿では、悪意のある第３者がコンピュータ・ネットワークの「向こう側」から行う「いたずら」と、基本的な対策について説明します。

表 1　不正利用による被害

データに対する被害	パソコンの不正利用による被害
● 不正な閲覧 ● 情報の改ざん ● 情報の削除 ● 情報の盗難	● 使用不能攻撃 ● 踏み台 ● 乗っ取り

1.2 コンピュータの被害

コンピュータ・ネットワークを経由したコンピュータへの被害は、大きく分けて二つあります（表１）。一つ目は、コンピュータが扱っているデータに対する被害で、情報の盗難や不正な閲覧、改ざん、削除などの被害があります。

二つ目は、コンピュータそれ自体を持ち主の意図に反して動作させる被害で、「使用不能攻撃」や「踏み台」、「乗っ取り」などと呼ばれる被害があります。使用不能攻撃とは、コンピュータに過大な負荷を与えることで、本来の目的のアプリケーションを動作させなくする一種の業務妨害です。

踏み台は、悪意のある第３者がコンピュータへの「いたずら」を行う際に、自分のコンピュータを使わずに他人のコンピュータに「いたずら」をさせることを言います。踏み台を使うことで、悪意のある第 3者は自分のコンピュータを被害者から隠すことができます。そして、踏み台にされたコンピュータの持ち主は、知らないうちに他人のコンピュータに迷惑をかけていることになります。

乗っ取りは、パソコンの遠隔操作プログラムを使って、パソコンを自由に操作することです。踏み台にすることが多いと聞きますが、情報の改ざんをはじめ、何でもできてしまいます。

第二章では、コンピュータが扱っているデータを不正に利用されないようにすることを中心に説明します。第三章では、パソコンそれ自体を不正利用されないようにすることを中心に説明します。

2. ファイルを不正に読まれないために

パソコンの前から離れるときに、研究室の鍵をかけていますか？

パソコンの場合、パソコンそのものに近づくことができれば、どのファイルも読むことができます。ファイルを守るのなら、まず外出のときには部屋に鍵をかけ、その次にコンピュータ・ネットワーク経由でも不正に読まれてしまわないように対策を立てましょう。

2.1 ネットワーク以前の話

Windows 98/95 を使うパソコンは電源を入れると、そのまま誰でも使えてしまいます。Windows の起動時に Windows パスワードや Microsoft ネットワークのパスワードを入力する画面が表示される設定もありますが、キャンセル・ボタンで先に進めます。いったん Windows 98/95 が起動すると、接

続されているハードディスクの内容を、すべて読むことができます。Windows NT でも、初期設定のままだと同じ危険があります。

秘密を守らなくてはならない情報や改ざんされては困る情報がパソコンに保存されているのであれば、まず他人が近づけないようにするべきでしょう。研究室に鍵をかけたり、電源操作時にパスワードを入力するように設定することができます。電源を入れたまま席をはずすことがあるのなら、スクリーン・セーバーにパスワードを登録しましょう。

- 電源操作時のパスワード

  電源を入れたときに、パスワードを入力しなければ起動しない機能です。この機能を設定しておくと、パスワードを知らない他人がパソコンを起動して操作することを防げます。

  これは Windows 98/95 の機能ではなく、パソコンのハードウェアの機能です。設定方法は、ハードウェアの説明書で BIOS（バイオス）のセキュリティ設定の項目や「パワー・オン・パスワード」といったキーワードの説明部分をご覧ください。

- スクリーン・セーバーのパスワード

  しばらく放置されているパソコンでスクリーン・セーバーを動作させて、再び使うときにパスワードを入力しなければ復帰しないようにする機能です。席をはずしている最中に、他人が操作することを防げます。

  スクリーン・セーバーを設定するには、コントロール・パネルの「画面」を開きます。「スクリーンセーバー」の項目でスクリーン・セーバーの種類を選んで、「パスワードによる保護」をチェックします。なお、「サイエンス」スクリーン・セーバーは動作中に画面が読めるので、秘密を守るためには不向きかもしれません。

2.2 ファイル共有の仕組み

Windows 98/95 ではフォルダ（ディレクトリ）ごとにパソコンのデータをネットワークに公開し、他のコンピュータとの間でファイルを共有することができるようになっています。他のコンピュータで公開されているファイルを利用するには「Microsoft ネットワーク クライアント」を使い、自分のコンピュータのフォルダを他のコンピュータから使えるようにするには「Microsoft ネットワーク共有サービス」を使います。なお、「NetWare ネットワーク共有サービス」を利用する場合もありますが、ここでは省略します。

- 共有の確認

  Windows 98/95 パソコンが、フォルダを共有する設定なのかどうかを確認してみましょう。

  コントロール・パネルの「ネットワーク」を開きます。「ネットワークの設定」の「現在のネットワークコンポーネント」（Windows 95 は「現在のネットワーク構成」）で「Microsoft ネットワーク共有サービス」の表示の有無を確認します。

「Microsoft ネットワーク共有サービス」が表示されていなければ、このパソコンは他のコンピュータにファイルを公開することはありません。一方、「Microsoft ネットワーク共有サービス」が表示されていれば、次のような手順でフォルダを公開（共有の作成）することができます。

- フォルダの共有と、共有の解除

  あらかじめコントロール・パネルのネットワークで、「ネットワークの設定」に通信のためのプロトコルを設定し、「識別情報」(Windows 95 は「ユーザー情報」)にコンピュータ名とワークグループを登録しておきます。

  共有を作成するには、共有したいフォルダを開きファイル・メニューで「共有」を選びます。はじめは「共有しない」が選ばれているので「共有する」を選び、必要に応じて「アクセスの種類」や「パスワード」を設定して、最後に OK ボタンを押します。共有を解除するには、「共有しない」を選んで、OK ボタンを押します。

他のコンピュータで共有されたフォルダのファイルを利用するには、次のようにします。

- 他のコンピュータが公開している共有フォルダの利用

  あらかじめコントロール・パネルのネットワークで、「ネットワークの設定」に「Microsoft ネットワーク クライアント」と相手側コンピュータに合わせたプロトコルを設定し、「識別情報」に相手側コンピュータと同じワークグループ名を登録しておきます。

  デスクトップの「ネットワーク コンピュータ」を開き、表示される相手側コンピュータを開きます。相手側コンピュータのウィンドウには、現在、公開されている共有フォルダのアイコンが表示されるので、目的の共有フォルダを開きます。相手側コンピュータでパスワードを設定して共有を作成すると、はじめて目的の共有フォルダを開くときにパスワードの入力ウィンドウが表示されます。パスワードを入力してください。

2.3 共有フォルダの危険さ

ファイル共有は、二台以上のパソコンを同時に利用している個人やグループにとって便利な仕組みです。しかし、第一章でも説明したようにネットワーク経由の「いたずら」は、パソコンの持ち主には見えないところで、知らないうちに被害にあってしまいます。ここでは、共有フォルダによる被害を紹介します。

1 ファイルの無断閲覧

同じネットワークに接続されていれば、どのパソコンからも共有フォルダの有無を表示できます。別の研究室のパソコンや演習室のパソコン、だれかが持ち込んで学内ネットワークに接続したノート・パソコン、こういったパソコンからでも共有フォルダの有無を表示できます。

表示される共有フォルダのアイコンをクリックするとフォルダが開きますから、パスワードのない共有フォルダは誰でも開くことができ、フォルダ内のファイルを読み出すことができます。共有フォルダを作成するときには、必ずパスワードをつけるようにしましょう。

Windows 98/95 の場合、共有フォルダごとにパスワードを設定します。この方法は個人で複数のパソコンを利用するときには安全ですが、グループで共有フォルダを利用するときには同じパスワードを複数の人が知っていることになります。時間がたったりメンバーが変わったときには、パスワードを変更するようにしましょう。また、可能なら利用者ごとに個別のパスワードを設定できる Windows NT や UNIX の samba などの利用を検討してください。

Windows 98/95 の場合には、個別のファイルの閲覧許可は設定できず、フォルダ全体に対して一括して共有するかしないかを設定します。共有フォルダ内にあるファイルは、共有フォルダを開くことができれば無条件に利用できます。また、あるフォルダを共有すると、サブ・フォルダも無条件に共有されます。例えば、C:\ を共有すれば、C ドライブ全体を共有したことになります。共有フォルダは必要最小限のフォルダだけを指定し、必要のないファイルやサブ・フォルダを作成しないようにしましょう。

また、共有フォルダ内のショートカットの挙動は、難解です。共有フォルダに C ドライブを参照するショートカット（C:\Windows など）があると、このショートカットの参照先は手元のパソコンの C ドライブを参照します。共有フォルダを作成した相手先のパソコンの C ドライブではありません。一方、共有フォルダを参照するショートカット（\\Remote\Share など）であれば、共有フォルダのファイルを参照します。わかりにくいので、Windows 98/95 の操作に慣れていない人は共有フォルダにショートカットを作成しないことをお薦めします。

2　ファイルの改ざん、無断削除

Windows 98/95 の共有フォルダは、「アクセスの種類」（Windows 95 では「アクセス権の種類」）で「読み取り専用」、「フル アクセス」、「パスワードで区別」を選ぶことができます。一つ目の「読み取り専用」は、すでにあるファイルの読み出しだけができて、変更の保存や新規作成ができないように共有フォルダを公開します。二つ目の「フル アクセス」は、変更の保存や新規作成ができるように公開します。最後の「パスワードで区別」は、読み取り専用パスワードを使うパソコンとフルアクセス用パスワードを使うパソコンで共有フォルダの挙動を区別します。

「フル アクセス」の共有フォルダでは、手元のハードディスクのファイルと同じように、ファイルの変更や削除、新規作成ができます。想定しない他人に「フル アクセス」のパスワードを知られてしまうと、ファイルの無断閲覧に加えて、内容の改ざんや必要なファイルの削除、自動実行による不正なプログラムの実行を許してしまいます。不正なプログラムの実行の危険さは、第 3 章「パソコンを乗っ取られないために」で説明します。

「フル アクセス」で共有フォルダを利用するときには、パスワードの確実な管理・更新と、必要のなくなった共有ファイルの共有解除を心がけてください。

3　パスワードや個人情報の盗難

Windows には、持ち主が作成した文書ファイルやデータベース以外にも、厳重に管理する必要のあるファイルがあります。例えば、パスワードを保存するために自動作成されたファイルなどです。

Windows 98/95 を利用していると、パスワードの入力時に「パスワードの保存」というチェック・ボックスが表示されることがあります。例えば、はじめて共有フォルダに接続するときや、ダイヤルアップ接続で電話番号やユーザ名とともにパスワードを入力する場合などに表示されます。パスワードの保存を選んだとき、これらのパスワードは、Windows の起動時に入力するユーザー名と関連づけられて C:\Windows フォルダに保存さます。

また、Netscape Messenger や Microsoft Outlook Express といった電子メール閲覧ソフトや、普

表 2　共有設定してはいけないフォルダ

パスワードが保存されるフォルダ ● C:\ ● C:\Windows ● C:\Windows\System ● C:\Program Files ● アプリケーションをインストールしたフォルダ

及している ftp クライアントにもパスワードを保存する機能があります。これらのパスワードは、それぞれのアプリケーションの方法でパスワードを保存しますが、よく使われる保存先は、C:\Windows フォルダ、C:\Windows\System フォルダ、レジストリ、インストール先フォルダなどです。レジストリとは、Windows 98/95 や Windows NT で使われる設定データベースで、Windows 98/85 の場合には C:\Windows フォルダにファイルとして保存されます。

保存されたパスワードが暗号化されている場合もありますし、そのまま保存されている場合もあります。初期の Windows 95 のパスワード・ファイルのように、暗号化されていても解読方法が広く知られている場合もあります。したがって、パスワードが保存されているフォルダを共有設定してはいけません。また、Windows98/95 や Windows NT の共有フォルダはサブ・フォルダも同時に公開するので、パスワードを保存しているフォルダをサブ・フォルダとして含むフォルダも共有してはいけません。

パスワードを保存している可能性のあるフォルダを表 2 に示します。このフォルダは、原則として公開してはいけません。やむを得ずに公開する必要のある場合には、今まで使ったことのない新しくて長いパスワードを利用し、なるべく短時間で共有解除を行うなど、無断閲覧に対する最大限の注意を払って作業するようにしましょう。

2.4 お薦めする共有フォルダの原則

以上のように共有フォルダには、さまざまな危険があります。これらの危険に対する共有フォルダの運用の目安は、次のようになります。

1. 必要な場合に限って、共有フォルダを利用する。
   公開の必要のない場合には、共有フォルダを使わない。
   「読み取り専用」での共有を基本にして、必要な場合にだけ「フル アクセス」を指定する。
2. 必要なファイルだけを共有フォルダに置く。
   共有フォルダに、目的外のファイルやサブ・フォルダを置かない。
   ショートカットを置くときには、充分に動作確認をする。
3. 共有フォルダには、パスワードをつける。
   パスワードを知らせる範囲や、更新の頻度にも気をつける。

4. パスワードなどを保存したファイルのあるフォルダを公開しない。
   表 2 のフォルダは公開しない。

3. パソコンを乗っ取られないために

コンピュータのリモート・メンテナンスをご存知でしょうか。多数のコンピュータを管理するのに、管理担当者の目の前のコンピュータから、コンピュータ・ネットワーク経由で離れたところにあるコンピュータの設定変更やソフトウェアのインストールを行う管理方式です。この方式では、管理されるコンピュータが分散配置されていても、管理担当者は出向く必要がなく、ただネットワークの接続先を変えてゆくだけで大部分の管理作業が行えます。

同じことは、あなたのパソコンと不正利用を狙っている他人のコンピュータとの間でも、条件さえ整えば成立します。他人がネットワーク経由であなたのパソコンの設定を変更したり、ソフトウェアをインストールしたり、ファイルの無断閲覧や改ざん、操作の監視などができるのです。

ここでは、上のような Windows パソコンを持ち主の意図に反して動作させる被害と、その対策を紹介します。

3.1 パソコンの不正利用

不正なパソコンの利用方法は、情報の無断閲覧に限りません。「攻撃」と称して積極的に他人のパソコンの動作を妨害したり、他人のパソコンを隠れ蓑にして他のパソコンを攻撃するようなことも知られています。さらに、あなたのパソコンで特別のプログラムを動作させれば、パソコンの動作を監視してパスワードなど機密情報を無断で報告されてしまいます。

愉快犯などはパソコンの動作を妨害して、本来の業務を行えないようにする「攻撃」を行います。使用不能攻撃と呼ばれています。また、パソコンに対する攻撃を行うときに、自分のパソコンを使わずに他人のパソコンを隠れ蓑に使うこともよくあります。これは踏み台と呼ばれています。さらに遠隔操作で他人のパソコンを自由自在に操ることは、乗っ取りと呼ばれています。

これらの不正利用は、業務の妨害にとどまりません。標的となる人物や組織の無知に付け込んで、あらかじめ使用不能攻撃や乗っ取りを行った後でパソコンの点検やアドバイスを装って訪問し、詐欺やナンパなどのきっかけにしている例もあるようです。このような場合には、単なるパソコン関連の被害にとどまらないことも考えられますので、気をつけましょう。

3.2 使用不能攻撃

使用不能攻撃とは、パソコンの動作を妨害して、本来の性能を発揮できないようにすることです。例えば、ネットワーク機能を停止させたり、ハードディスクへのデータの書きこみを妨害したり、パソコンの反応を極端に遅くして事実上何もできなくさせてしまったりします。

使用不能攻撃を行うとき、Windows 98/95 などの OS の欠陥（バグ）につけ込む場合が多いのですが、インターネット・ホームページを参照してくる Netscape Communicator や Microsoft Internet

Explorer といった Web ブラウザの欠陥を利用する場合もあります。

対策は、OS や Web ブラウザの欠陥報告に注意を払っておき、重大な欠陥の場合にはメーカの提供する修正プログラムなどを利用することです。例えば、Microsoft のホームページには、既知の欠陥を報告するページ（http://www.microsoft.com/japan/security/ ）があり、欠陥を除去する修正プログラムが用意されています。ソフトウェアの会社もハードウェアの会社も、多くのメーカが自社のホームページで欠陥と対策を公表しています。

欠陥の報告は、メーカのホームページのほかに、パソコンやインターネットなどの専門雑誌やコンピュータ・ウィルス対策ソフトの開発会社から入手することができます。また、1999 年上旬の Melissa ウィルス以来、社会的に影響の大きい欠陥はテレビや新聞で報道されるようになりました。身近なメディアに気を配るように心がけるといいでしょう。

パソコンは「現状の性能」で出荷されているので、あとから欠陥が見つかることがよくあります。自動車のリコールのような欠陥を周知させる制度がない以上、できる範囲で情報収集を行っておくと安心です。

3.3 踏み台と乗っ取り

標的となるパソコンを不正に利用するときに、自分のパソコンから不正利用を行うのではなく、別のパソコンを隠れ蓑にして不正利用を行うことがあります。踏み台とは、不正利用の隠れ蓑にされたパソコンのことをいいます。例えば、犯人 A が標的 B のパソコンに対して使用不能攻撃を行うときに、別の C のパソコンを操作して B のパソコンを停止させた場合、C のパソコンが踏み台に使われたといいます。

パソコンが踏み台にされると、その持ち主は真っ先に犯人であると疑われます。不正利用を行っていないことが証明できて疑いが晴れたとしても、管理責任を問われることになります。

乗っ取りとは、標的になるパソコンを遠隔地から自由に操作できるようにしてしまうことです。持ち主の知らないうちに、リモート・メンテナンスの管理下に入ってしまったようなものです。この場合には、標的にされたパソコンのすべての機能を自由に使われてしまいますので、ハードディスクの無断閲覧や改ざん、消去はもちろん、プログラムを起動することによって踏み台に利用したり、さらにパソコンの動作を監視することによって本来の利用者の利用状況をすべて盗み見たりすることができます。

標的となるパソコンを踏み台にする場合も、乗っ取ってしまう場合も、どちらも遠隔地のパソコンにプログラムを送りつけて、相手側パソコンでそのプログラムを実行します。したがって、踏み台にされない対策と乗っ取られない対策を、区別しないで説明します。

3.4 プログラムの送りつけと実行

パソコンで実行されるプログラムは、そのパソコンのすべての機能を利用できます。他人のパソコンを踏み台にして不正利用する場合も、乗っ取ってしまう場合も、標的となったパソコンで特定のプログラムを実行する必要があります。この方法には、標的パソコンのソフトウェアの欠陥を利用する

方法、電子メールの添付ファイルを利用する方法、ホームページを利用する方法、トロイの木馬、そして、プログラムの自動実行機能を利用する方法があります。それぞれの場合に分けて、対策を説明します。

1　ソフトウェアの欠陥

使用不能攻撃と同じように、パソコンのソフトウェアの欠陥を悪用して、プログラムを送りこみ、実行する場合があります。これは、OS やアプリケーションの欠陥を利用する方法と、モバイル・コードの欠陥を利用する方法とに分類できます。

OS やアプリケーションの欠陥のなかには、特定の操作を行うと送信したプログラムを実行してしまう欠陥もあります。非常に重大な欠陥ですが、いくつかの報告事例があります。

このような欠陥に対する対策は、利用している OS やアプリケーションの欠陥情報（バグ情報）に気を配り、ネットワーク経由で不正にプログラムを実行してしまう欠陥が発見されたとき、直ちに修正プログラムを入手することです。社会的な影響が大きいので、もし発見されればマスメディアでの報道があるでしょう。情報収集が対策の第一歩です。

一方、モバイル・コードはワールド・ワイド・ウェブ（WWW）利用の応用として開発されたもので、コンピュータ・ネットワーク経由でプログラムを転送し、実行する機能を持ったものです。Windows 98/95 の場合には Java や JavaScript、VB Script などがあり、Netscape Communicator や Microsoft Internet Explorer のような Web ブラウザで実行されます。

本来のモバイル・コードは、限られた機能だけを実行するように設計されています。例えば、モバイル・コードで書かれたプログラムは、ハードディスクの閲覧や書き込みができません。しかし、Netscape Communicator や Microsoft Internet Explorer の欠陥によって、実行されないように設計されている機能が実行できてしまう事例がいくつも報告されています。

モバイル・コードの欠陥に関する対策は、モバイル・コードを使わないようにするか、欠陥のない Web ブラウザでモバイル・コードを利用することです。モバイル・コードを使わないようにするには、Web ブラウザで設定します。例えば、Netscape Communicator では、次のように設定します。

1. 編集メニューから設定を選び、「設定」ウィンドウの「カテゴリ」から「詳細」を表示する。
2. 「Java を有効にする」と「JavaScript を有効にする」のチェック・ボックスを解除する。
3. 「OK」ボタンを押して、ウィンドウを閉じる。

欠陥のない Web ブラウザを使うには、Web ブラウザを常に最新のバージョンに更新して、発見されたモバイル・コードの欠陥のないものを利用するようにします。

2　添付ファイルによるプログラムの実行

Windows 98/95 の場合、いろいろな形態でプログラムが実行されます。Microsoft Word や Excel のマクロも一種のプログラムで、文書ファイルを開いたときなどに実行されます。拡張子に関連づけられたアプリケーション・プログラムは、データ・ファイルを開くと実行されます。このようなプログラムを起動するデータ・ファイルや、実行ファイルそのものが添付された電子メールを受け取った場合、不用意に添付ファイルを開くと、電子メールで外から送りつけられてきたプログラムを手元のパソコンで実行することになります。悪意を持って開発されたプログラムの場合なら、たった一度の実行で

パソコンを乗っ取られてしまうこともあります。

添付ファイルによる不正なプログラムの実行に対する対策は、電子メールの添付ファイルを不用意に開かないことです。実行ファイルの場合には、破棄しましょう。文書ファイルの場合には、マクロが含まれないことやマクロが悪質なものでないことをウィルス対策ソフトで検査してから開くようにします。ウィルス対策ソフトを使う場合には、定期的なウィルス情報データの更新を忘れないようにしましょう。

3　ホームページのリンクによるプログラムの実行

ホームページのリンクの中には、Windows 98/95 の実行ファイル（*.EXE）にリンクを張っているものがあります。実行ファイルを指し示すリンクを Web ブラウザで選ぶと確認のウィンドウが開き、Web ブラウザは実行ファイルをネットワーク経由で読みこんで起動しようとします。もし、読みこんだ実行ファイルを起動すれば、外部のホームページにあるプログラムを手元のパソコンで実行することになります。この場合も、上と同様に、悪意のあるプログラムであれば、パソコンを乗っ取られます。

ホームページのリンク先が実行ファイルだった場合の対策は、Web ブラウザから保存して実行する確認のウィンドウが表示されたときに拒否することです。保存したり、起動してはいけません。なお、乗っ取りなどに使われるプログラムはコンピュータ・ウィルスとは異なる種類のプログラムなので、ウィルス対策ソフトで発見できないものもあります。ウィルス検査に合格したからといって、安心して起動できるとは限りません。

4　「トロイの木馬」

トロイの木馬とは、パソコンを不正に利用するプログラムを、別の役に立つ機能を持つプログラムに抱き合わせたものです。役に立つほうの機能を利用しようとすると、同時に不正に利用するプログラムも実行してしまいます。なお、「トロイの木馬」とは、ホメロスの詩「イリアス」にあるトロイア戦争で木馬に兵士をひそませたという伝承にもとづいた言い方です。

この場合、決定的な対策はありません。消極的な目安として、実績のあるプログラムを利用することや、ソース・コードの付属するものを利用することなどでしょうか。巧妙に仕組まれた場合でも、多数のユーザが利用するプログラムであれば、秘密裏に抱き合わせられた不正な機能が発見される可能性が高いでしょう。大手ソフトウェア会社のアプリケーション・プログラムで、自動的にライセンス番号を文書ファイルに記録する機能が発見されたことがあります。また、ソース・コードが付属していれば、プログラムの動作の全体を明らかにできます。

5　プログラムの自動実行

最後は、プログラムの自動実行を利用する方法です。

Windows 98/95 には、プログラムを自動実行する仕組みが用意されています。例えば、スタート・メニューのプログラムの下に「スタートアップ」という項目があります。この項目に含まれるプログラムは、Windows 98/95 にログオンした時点で実行されます。プログラムを自動実行する仕組みは、この他に別のユーザと共有する「スタートアップ」項目を利用する方法や、レジストリで指定する方法もあります。

スタートアップ項目の実体は、「C:\Windows\スタート メニュー\プログラム\スタートアップ」フォ

ルダです。このディレクトリに不正なプログラムを書きこむことができると、次に Windows へログオンしたときに不正なプログラムを自動的に実行させることができます。レジストリの実体は C:\Windows フォルダにあるファイルなので、このファイルを書きかえることができれば同様に、不正なプログラムを自動的に実行させることができます。標的となったパソコンでは、通常とまったく同じ操作で不正なプログラムが実行されることになるので、不正の発見が困難になります。

プログラムの自動実行による不正なプログラムの実行への対策は、C:\Windows フォルダの管理を厳重にすることです。第二章でも書きましたが、不用意に共有設定を行うとパソコンの管理の甘さに乗じて、このようなわなを仕掛けられてしまう危険性があります。

3.5 パソコンを乗っ取られないための原則

以上のように、手元のパソコンでうっかり不正利用のためのプログラムを起動してしまう場合に、パソコンを乗っ取られてしまいます。そうならないための目安をまとめると、次の通りです。

1. OS やアプリケーションの欠陥情報に気を配り、重大なものに修正プログラムを適用する。
2. Web ブラウザを最新のものに更新する。
3. 電子メールの添付ファイルを、その場で開かない。必ず、ウィルス検査のあとで開く。
4. Web で実行ファイルへのリンクを選んでも、そのファイルを保存したり起動しない。
5. 実績のあるプログラムを利用する。
6. プログラムの自動実行フォルダやレジストリ・データベースの管理を厳重にする。

佐賀大学情報処理センター年報 第 9号 (2000 年 3 月)に掲載