1-1
悪質化するコンピュータウイルス

皆さんはコンピュータウイルスがどのようなものかご存じでしょうか？　テレビや新聞、雑誌などで「コンピュータウイルス」という言葉を見聞きすることがあると思いますが、具体的にどのようなものか想像できますか？

巧妙な手口で深刻な実害をもたらす

コンピュータウイルスついてあまり知識のない方は、感染するとデスクトップ上に得体の知れない画像を表示したり壁紙を変えたりするものといった割と古いイメージを持ち続けていることがあるようです。いたずら目的でユーザーを驚かせるだけなので、感染してもそれほど害はないと思っている方もいることでしょう。

10年以上前ならこうした認識でもある程度実情を反映していると言えなくもないのですが、コンピュータウイルスも時代とともに変わりつつあります。今日発見されるコンピュータウイルスは、感染してもあえて画面表示をしないようにしています。これは、感染したことをなるべくユーザーに気づかせないようにするためです。逆に、画面にはっきり何かを表示するコンピュータウイルスもあります。しかし、それも実はユーザーに感染を気づかせないための仕掛けなのです。なにやら矛盾しているようで腑に落ちないかもしれません。そこで、実際の例をご覧いただきましょう。最近のコンピュータウイルスが動作しているところを紹介します。

ところで、本書ではコンピュータウイルスのことを「マルウェア」と呼ぶことにします（理由については第2章で説明します）。この呼び名に慣れないうちは、「マルウェア」という言葉が出てきたら頭の中で「コンピュータウイルス」に置き換えてくださっても結構です。

1-2
情報が密かに盗まれる

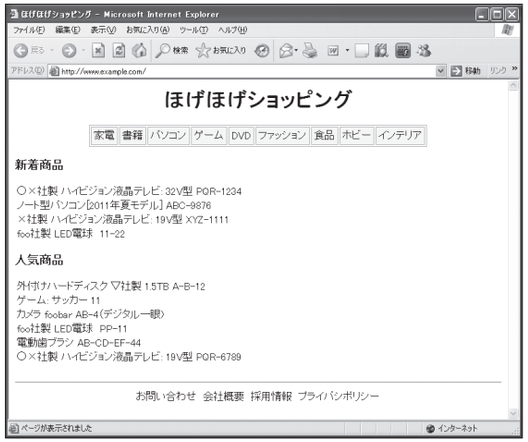
では、実際にコンピュータウイルスが動作している様子を紹介します。感染した兆候が現れないのに、裏でこっそりと情報が盗まれるというマルウェアの例です。★リードを起こしました。確認お願いします★

感染兆候はないが……

まず、1つクイズを出しましょう。コンピュータAの画面（**図1.1**）とコンピュータBの画面（**図1.2**）はいずれも実際のコンピュータの画面です。どちらもブラウザから無害そうなWebサイト（www.example.com）にアクセスしている様子を示しています。このWebサイトは筆者が架空に設置したもので、実際にありがちな状況をモデル化しています。実在のサイトではないものの、マルウェアや感染の方法は現実のものです。AとBのどちらかのコンピュータにおいて、今まさにマルウェア感染が始まっています。それはどちらでしょうか？

両方ともまったく同じ様子なので、この画面からだけではどちらで感染が起こっているのか判断することは不可能です。もうちょっと情報をお見せしましょ

図 1.1　コンピュータ A のブラウザ画面



う。**図1.3**と**図1.4**は、ブラウザの通信状況を表示するFiddlerというツールが実行されている画面で、図1.3がコンピュータAに、図1.4がコンピュータBに対応しています。Fiddlerは、ブラウザがアクセスしているURLやファイルの情報を表示します。

同じサイトにアクセスしているにも関わらず、コンピュータA（**図1.3**）とコンピュータB（**図1.4**）で通信の様子が異なることがわかります。図1-4では、得体の知れないサイト（一部マスクしています）からPDFファイルや何か別のファイルをダウンロードしています。なんだかとっても怪しいですが、これだけでは何か起こっているのかよくわかりません。このPDFファイルがどういったものか調べる必要があります。通常、PDFファイルにアクセスすると、Adobe ReaderのようなPDFビュアーが起動してPDFファイルを表示するはずですが、いくら

図 1.2 コンピュータ B のブラウザ画面

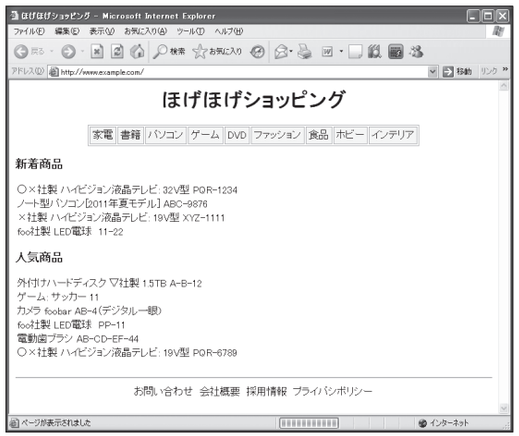
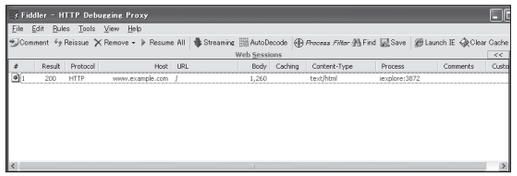


図 1.3 コンピュータ A のブラウザがアクセスしているサイト



待ってもこのPDFファイルが表示されることはありませんでした。したがって、コンピュータBの様子（**図1.5**）はなんだか疑わしいと思っていいでしょう。

こっそり不正なサイトにアクセス

突然ですが、ここでコンピュータAとBからそれぞれ自分の管理しているFTPサーバにアクセスしてみましょう。FTPサーバにアクセスするときには、ユーザーIDとパスワードを入力する必要があります。ここでは例として、FTPサーバ（192.168.0.20）にユーザー ID「nihon」、パスワード「taro」でアクセスします（**図1.6**）。

ところが、ネットワークモニタを調べてみると、FTPサーバにアクセスした直後にコンピュータBのサーバからある不審なサイトにアクセスしていることがわ

図 1-4 コンピュータ B のブラウザがアクセスしているサイト。「Application/pdf」と「application/x-msdownload」 のダウンロードがこっそりと行われている

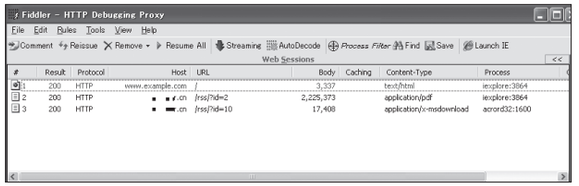
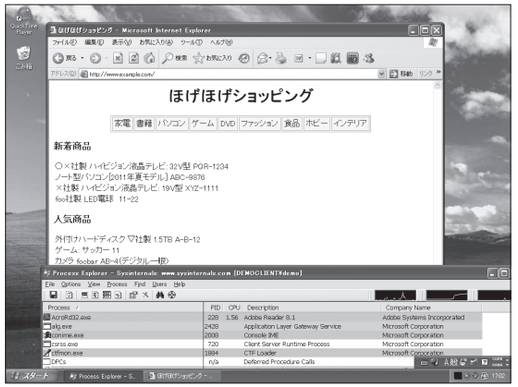


図 1.5 コンピュータ B におけるプロセスのリストの一部。Adobe Reader（AcroRd32.exe） がプロセスにあるが PDF ファイルが表示されない



かりました（**図1-7**）。

通信内容をよく見ると、FTPサーバのアドレス、入力したユーザーIDおよびパスワードが不正なサイトに送られていることがわかります。ヘッダ「SO:192.168.0.20/nohin:orat」の部分に、FTPサーバのIPアドレスと、ユーザーID（nihon）とパスワード（taro）が文字の並びを逆にして格納されています。ここまでくれば、コンピュータAとBのどちらで感染が始まっていたのかもうおわかりでしょう。答えはBです。どうやらコンピュータBでは、FTPサーバのアカウント情報を盗むマルウェアに感染していたようです。

もしこのFTPサーバに、企業や組織の機密情報などの重要な情報が保存されていたらどうでしょう？　そうした情報が攻撃者の手に渡ってしまいます。もし、FTPサーバがWebコンテンツを管理するためのものだったらどうでしょう？　攻撃者によって、Webコンテンツが不正に改ざんされてしまいます。

コンピュータA（**図1.1**）とコンピュータB（**図1.2**）のブラウザの表示ではまったく外見的な違いはありませんでしたが、Bは裏でこっそり別のサイトにアクセスしていて、結果としてFTPサーバのログインパスワードを盗むマルウェアに感染していることがわかりました。なぜコンピュータBでは、このように裏でこっそりと不正なサイトにアクセスしているのでしょうか？　感染に至る詳細は、後の章で説明します。

感染の詳細はわからなくても、マルウェアを感染させた理由は理解できるはずです。このマルウェアはFTPサーバのアカウントを盗みたいので、なるべくユーザーに気づかれないために感染兆候を出さないようにしていたのです。不気味な画面を表示していただけの以前のマルウェアとは随分変わってきていることがわかると思います。

図 1.6　コンピュータ A と B からそれぞれ FTP サーバ（192.168.0.20）にアクセスする。ユーザー ID とパスワードはそれぞれ「nihon」と「taro」

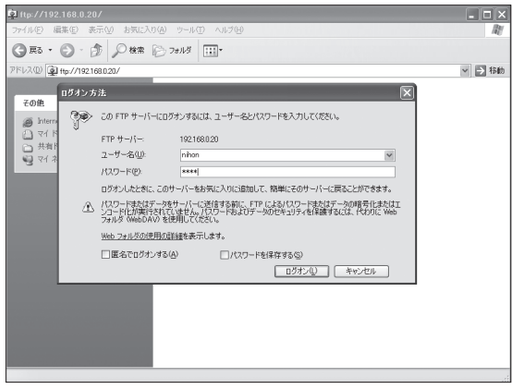


図 1.7　コンピュータ B から送信された HTTP 通信の内容

```
GET /x/?0EFokjmfoiitpolduowrmpfqjtqghyhjlqi0 HTTP/1.1
SO: 192.168.0.20/nohin:orat
SS: / HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1)
Host: ■ ■ ■
Cache-Control: no-cache
```

1-3 マルウェアによる振り込め詐欺

マルウェアの中には、偽の情報を表示してユーザーを騙し、金銭をだまし取るためのサイトに誘導するものもあります。いわゆる振り込め詐欺を目的としたマルウェアを紹介します。★リードを起こしました。確認お願いします★

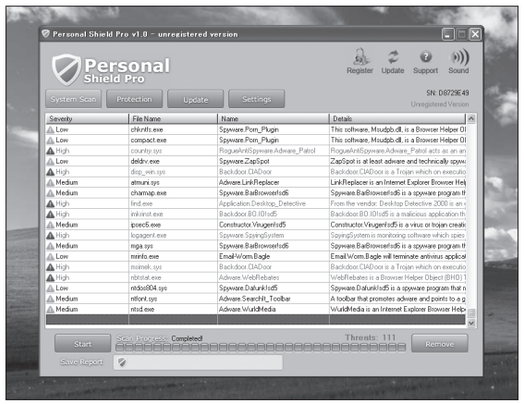
偽のセキュリティソフトで誘導

さて、次のクイズです。コンピュータCの画面（**図1.8**）とコンピュータDの画面（**図1.9**）をご覧ください。英語版のアンチウイルス製品がコンピュータをスキャンしている様子ですが、実際にマルウェアに感染しているのはコンピュータCとDのどちらでしょうか？　画面をじっくりと見比べて考えてみてください。

いかがでしょう？　コンピュータCでは大量のマルウェアが検知されているようです。一方、コンピュータDでは安全性のスコアが「33%」と示されています（かなり低いスコアのようです）。どちらがマルウェアに感染しているかわかりましたか？　難しいと思いますので、もうちょっとお見せしましょう。

しばらく経つと、コンピュータCとDそれぞれに**図1.10**と**図1.11**のようなスキャン結果が表示されました。感染数こそ違いますが、どうやらどちらもVirus

図 1.8 コンピュータ C の画面（スキャン中）

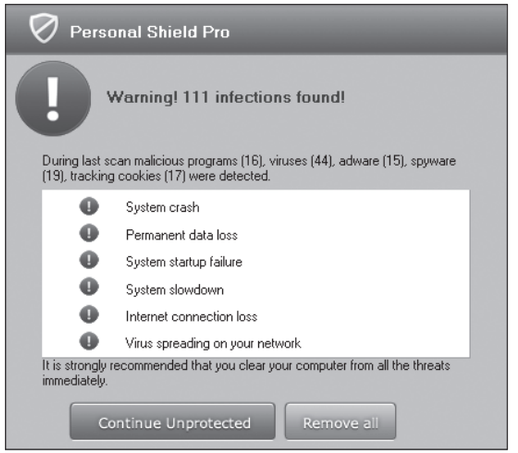


（ウイルス）に感染しているようです。検知はしているようですが、未然に感染を防ぐことはできなかったのでしょうか？

それでは答えを発表しましょう。正解は「コンピュータCとDのいずれも感染している」です。少々意地の悪い問題でしたね。ただし、感染しているといっても、検知アラートで表示されているマルウェアに実際に感染しているわけではあ

図 1.9 コンピュータ D の画面（スキャン中）

図 1.10 コンピュータ C の画面（スキャン結果）



りません。どちらも、アンチウイルス製品がシステムをスキャンしているように見えますが、これらは正式なものではなく偽物です。実は、スキャンしているアンチウイルス製品のようなもの自体がマルウェアなのです。当然、検知アラートは偽物であり、画面に表示されたマルウェアに実際に感染しているわけではありません。

これらは、偽セキュリティソフトウェアと呼ばれているもので、最近急増しているマルウェアの一種です。この偽のソフトウェアは、ユーザーを騙して購入させる、いわゆる振り込め詐欺を目的としています。

図1.10のボタンの「Remove All」（全部削除する）を押すか、図1.11のボタンで「Fix Errors」（エラーを修正する）を押してみましょう。すると、どちらも**図1.12**のような振り込みサイトが表示されます。これは偽の“正式版”購入サイトです。

つまり、勝手に偽の検知結果を表示して、駆除のために正式版を購入させて振り込ませるといった詐欺なのです。

この偽セキュリティソフトウェアは感染時に何かを表示するので、そういった意味ではマルウェアの中では今や珍しい部類に属します。しかし、昔のようにいたずら目的でないことは一目瞭然です。今日のマルウェアが何かを表示するときは詐欺目的でユーザーを騙すときであるといってもよいでしょう。

図 1.11 コンピュータ D の画面（スキャン結果）

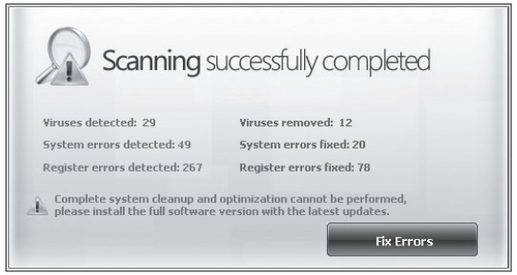
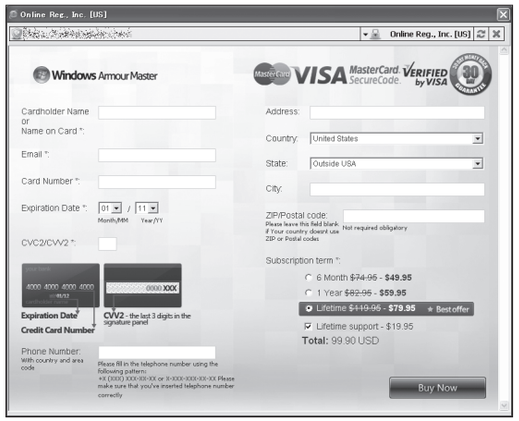


図 1.12 偽セキュリティソフトウェアが表示する振り込みサイト



1-4 口座からお金が盗まれる

最近のマルウェアは感染していることがわかりづらいという不気味さはあるものの、実際に感染しても大した被害はないのではないかと思われる方もいるかもしれません。しかし、現実に深刻な被害も多く報告されています。

金融サイトのアカウント情報を盗む

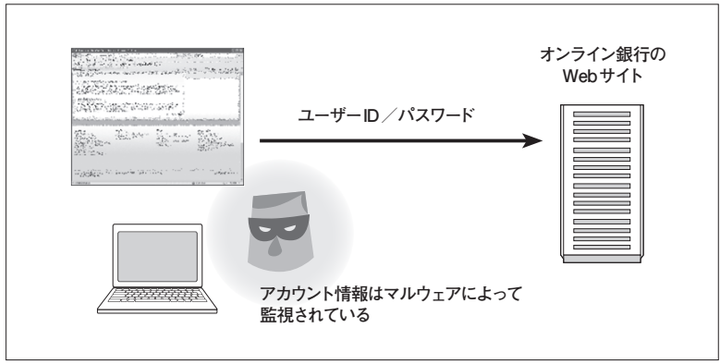
先ほど、FTPサーバのアカウントが盗まれることについて述べました。確かに、FTPサーバにアクセスしないユーザーにはあまり関係のない話かもしれません。しかし、残念ながらマルウェアにはもっと直接的に被害を及ぼすものがあります。

インターネットバンキングなどで金融機関のWebサイトを利用されている方は多いと思います。最近では多くの銀行がオンラインサービスを用意しており、パソコンやモバイル端末から振り込みが行えるなど大変便利になりました。

しかし、こうしたオンライン金融サービスのWebサイトを利用するためのユーザーIDやパスワードといった情報が盗まれたら、どのような被害が発生するでしょう？　お金が不正に他人の口座に振り込まれたり、あるいは、直接お金を引き出されたりしてしまいます。

マルウェアの中には、オンライン金融サイトのアカウント情報を盗むことを専門としたものが数多く存在しています。ひとたびこうしたマルウェアに感染してしまうと、オンライン金融サイトへのアクセスは監視されます。つまり、ユーザーIDやパスワードはすべてマルウェアによって盗み見られ、裏でこっそりと攻撃者に送信されてしまうのです。

図 1.13 オンライン金融サイトのログイン情報を盗むマルウェア



このようなマルウェアに感染する人はごく少数で、自分には関係ないだろうと思うのは危険です。被害は現実に、しかも大規模に発生しているのです。マルウェアによって口座情報やログイン情報が盗まれたことで、実際に以下のような被害が発生しています。

- **2007年、スウェーデンの銀行の顧客がHaxdoorと呼ばれるマルウェアに感染し、アカウント情報が盗まれた。被害総額は700万～800万クローナ（約1億2000万～1億4000万円）といわれている**
- **2008年、米国のある調査ではCoreFloodと呼ばれるマルウェアによって盗まれた口座情報は、トータルで50GB規模。16カ月で37万台以上のコンピュータが感染したといわれている**
- **2010年、英国のある銀行の顧客がZbotと呼ばれるマルウェアに感染。少なくとも3,000人以上の口座情報とパスワードが盗まれ、1カ月に約67万5,000ポンド（約9,000万円）が不正に送金された**

日本でも被害は発生しています。

- **2005年7月、日本の銀行の顧客が狙われ、総額940万円が別口座へ不正に振り込まれた。同年11月にも別の銀行の顧客が狙われ、不正な送金が行われた**

いたずら目的から詐欺や窃盗へ

今日のマルウェアが、10年以上前に見られたいたずら目的のものと大きくかけ離れ悪質化していることを理解していただけたでしょうか。現在ではマルウェアは、金銭をだまし取ったり情報を盗んだりする手口に使われています。不愉快な画面を出すいたずら目的のマルウェアは消え去りました。マルウェアについてのこのような過去のイメージは捨てましょう。もはや、自分のコンピュータがマルウェアに感染しているかどうかを簡単に判別できる時代は終わりました。詐欺師や窃盗犯に対して警戒するように、私たちはマルウェアを現実的な脅威と認識する必要があるのです。

身を隠してやってくる詐欺、情報の窃盗、スパイ、破壊工作といった攻撃から、コンピュータ、ネットワーク、サーバ、システムを守らなければなりません。そのために、最新のマルウェアの動作を理解して敵の戦略を知り、そして備えていきましょう。