インターネットに潜む罠

～スパイウェア、フィッシング～

2005年 法桜祭 学生フォーラム

山田正雄ゼミナール

はじめに

「インターネット上での厄介者は何か？」と聞かれると、まず何を思い浮かべるだろうか？
恐らく、コンピュータウイルスのことが頭に浮かぶ人が多いのではないかと思われる。
確かに、ウイルスは大事なデータを消去したり、システムを破壊したりなど多くの被害をもたらす。

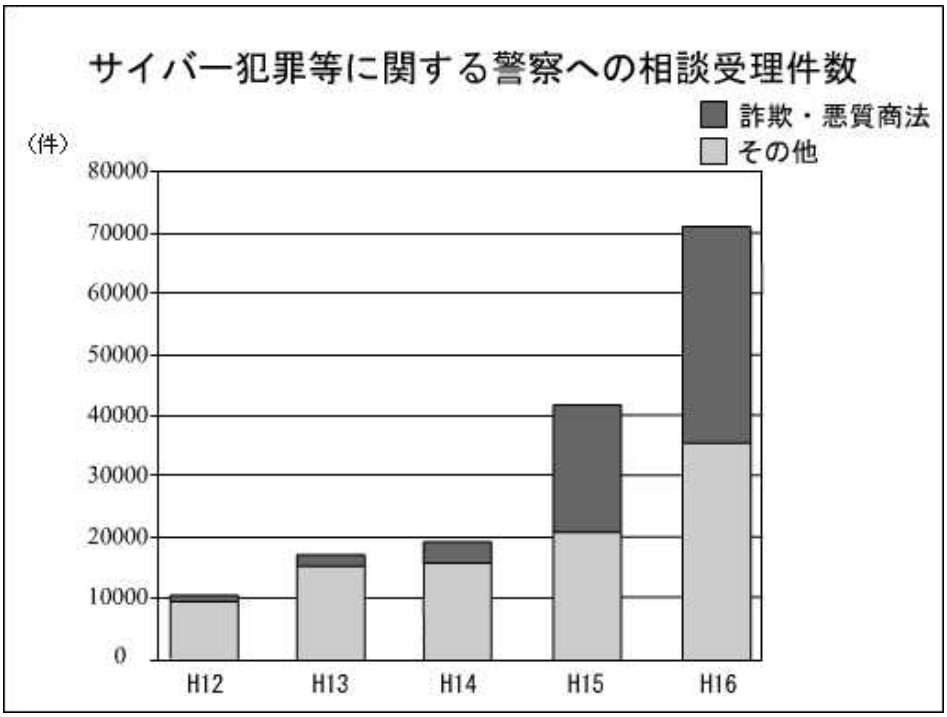
しかし、ここ最近、ウイルスの他にも極めて深刻な被害をもたらす**罠**がインターネット上に現れた。
それが、「**スパイウェア**」「**フィッシング**」と呼ばれるものである。

ウイルスと「スパイウェア」「フィッシング」の大きな違いは、その被害の質にある。
ウイルスは感染したコンピュータを攻撃すること自体が目的であることが多いのに対し、
「スパイウェア」「フィッシング」は**個人情報（※1）を盗み出すことが目的なのである。**

どちらの被害が深刻かを一概に決めることはできないが、現状では「スパイウェア」「フィッシング」は極めて重要な問題としてインターネット上を席巻している。

米 WatchGuard Technologies 社が 2005 年初頭に行った、企業の IT マネージャと管理者に対する調査では、回答者の 3 分の 2 は「この先 12 カ月で、ネットワーク・セキュリティに対して最も大きな脅威となるものはスパイウェアである」と考えているということが明らかになった。

一方、フィッシングは日本での被害はまだ少ないのだが、下図のように近年サイバー犯罪において詐欺の相談件数は急激に増えている為、新手の詐欺であるフィッシングも注意しなければならないと考えられる。



警察庁サイバー犯罪対策広報資料より

十分な知識や対策なしにインターネットを利用していれば、いずれ重要な個人情報を盗まれてしまうだろう。
これらの脅威はどのように襲い掛かってくるのか。
これらの脅威から自分の身を守るためにはどうすべきなのかを研究した。

スパイウェア (spyware)

1　スパイウェアの概要

スパイウェアとは、コンピュータに無断で侵入し、勝手に個人情報を漏洩するプログラムのことである。

パソコン 1 台に平均 30 個､多い場合では数百個ものスパイウェアが侵入しているという調査結果もあり、今までスパイウェアの存在すら知らずにいた人のコンピュータは､既に大量のスパイウェアに侵されていると予想される。では、スパイウェアは具体的にどのような被害をもたらすのか？

2　スパイウェアの実例と被害

スパイウェアには膨大な種類があり、どのスパイウェアに侵入されるかにより、被害は大きく異なる。同じスパイウェアと呼ばれるプログラムでも､ほとんど実害が無いようなものもあれば､重要な個人情報を盗むような凶悪なものもある。(※2) ここでは、スパイウェアの中でも最悪の被害をもたらす「CoolWebSearch」の説明をする。

CoolWebSearch

このスパイウェアは、個人情報漏洩以外にも様々な被害をもたらす。

- **被害１　ホームページをアダルトサイトに変更**
- **被害 2　アダルトサイトのポップアップ広告を表示**
- **被害 3　お気に入りに膨大な数のアダルトサイトを追加**
- **被害 4　セキュリティの設定を変更**
- **被害 5　コンピュータの動作不具合を誘発**

これだけでも大変な被害ではあるが、やはり CoolWebSearch の本領は情報漏洩にある。

以下の文章は、平成 17 年 8 月に掲載されたニュース記事からの引用である。

> **スパイウェア CoolWebSearch にご注意--米で大規模な個人情報盗難が発覚**
>
> セキュリティ企業 Sunbelt Software は米国時間 8 日､50 もの銀行に関係した大規模な個人情報盗難が起きていることを発見したと述べた｡同社が明らかにしたところによると､攻撃者は**キー入力ログ記録ソフトウェア**を使って「膨大な数のマシン」から個人情報を収集しているという｡現在､連邦捜査局（FBI）がこの事件について調査を進めている｡盗まれたデータには､クレジットカード番号､社会保障番号､ユーザー名､パスワード､インスタントメッセージのチャット内容､検索のために入力したキーワードなどが含まれる｡　　ZDNet Japan より引用

キー入力ログ記録ソフトウェアとは、しばしば**キーロガー**と呼ばれ、その名の通りキーボードに打ち込んだ情報を記録するプログラムのことである。インターネット通販を利用したことがある人は、クレジットカード番号をコンピュータに打ち込んだことがあるかと思われるが、そのような重要な情報を CoolWebSearch が外部に漏洩してしまったという事件である。

つまり、**・被害 6　重要な個人情報の漏洩**　ということになる。

しかも、CoolWebSearch に一度侵入されてしまうとなかなか駆除することができず、最悪の場合、ろくにバックアップも取れぬまま再インストールをする羽目になる可能性もある。

このようにスパイウェアは甚大な被害を私達にもたらす。では、このようなスパイウェアは、いつ、どのような時にコンピュータに侵入してくるのか？　また、どのようにして侵入を防げばいいのか？

3　スパイウェアの侵入方法とその予防策

スパイウェアには様々な種類があるので、それだけ侵入経路もたくさんあるわけだが (※3)、主に私達が気をつけなければならないのは、「Web ブラウザ経路で侵入してくる場合」である。このケースは、「セキュリティホール」を利用するか、「ActiveX」を利用するかで更に二つに分けることができる。

3-1　セキュリティホールを利用して侵入してくる場合

セキュリティホールとは、ソフトウェアの設計ミスなどによって生じたセキュリティ上の欠陥ことだ。これを利用されると、悪意のある Web サイトを見ただけでスパイウェアに侵入されてしまう。セキュリティホールを塞ぐためには、WindowsUpDate をしなければならない。

WindowsUpDate はインターネットに接続していれば簡単に行えるし、自動的に必要なデータをダウンロードし、インストールしてくれるように設定することもできる。

既知のセキュリティホールを攻撃してくるスパイウェアはかなりの数があるので、こまめにアップデートをするだけでもかなりの防御効果が期待できる。

3-2　ActiveX を利用して侵入してくる場合

ActiveX とは、簡単に言ってしまえば「Web ブラウザの機能を拡張するプログラム」のことである。上記の WindowsUpDate は Web ブラウザ上で行うことができるのだが、そもそも Web ブラウザというのはサイトを閲覧するためのソフトであって、セキュリティホールを防ぐような複雑な作業は本来はできない。それを可能にしているのが、この ActiveX なわけである。

ActiveX は WindowsUpDate 以外にも様々な場面で利用され、例えばブラウザ上で行うゲームをインストールする時に使われたりする。その時、下図のような警告が表示されることがある。

この警告は「何らかのデータをコンピュータにインストールしていいか？」と確認しているもので、ActiveX を利用したい場合は「インストールする」をクリックすればいいわけである。

だがこの時、何がインストールされるのかは実際にインストールしてみるまでは正確にはわからない。ゲームをインストールするつもりで了承をしたら、実際はゲームではなくスパイウェアをインストールされてしまう可能性があるわけだ。**絶対に信用できるサイト以外では、ActiveX を利用しないように心がけなければならない。**

3-3　ソフトウェアを利用する予防策

また、「SpywareBlaster」や「SpywareGuard」等といったスパイウェア対策ソフトを利用することにより Web ブラウザ経路だけでなく、**正規のソフトウェアに紛れてインストールされるスパイウェア**などからもコンピュータを守ることができる。この 2 つのソフトは海外のものでこそあるが、無料で提供されていて品質も高いのでぜひ導入すべきだろう。

WindowsXp(service pack2)で ActiveX を利用してソフトウェアをインストールしようとした際に表示される警告

4　スパイウェアに侵入されてしまった場合の対応策

セキュリティホールをしっかり塞いで無闇に ActiveX を利用せずに、SpywareBlaster などを使用しても、どうしてもスパイウェアに侵入されてしまうということはある。重要な個人情報を漏洩される前に、スパイウェアを駆除しなければならない。

4-1　アンチスパイウェアソフトを利用する対応策

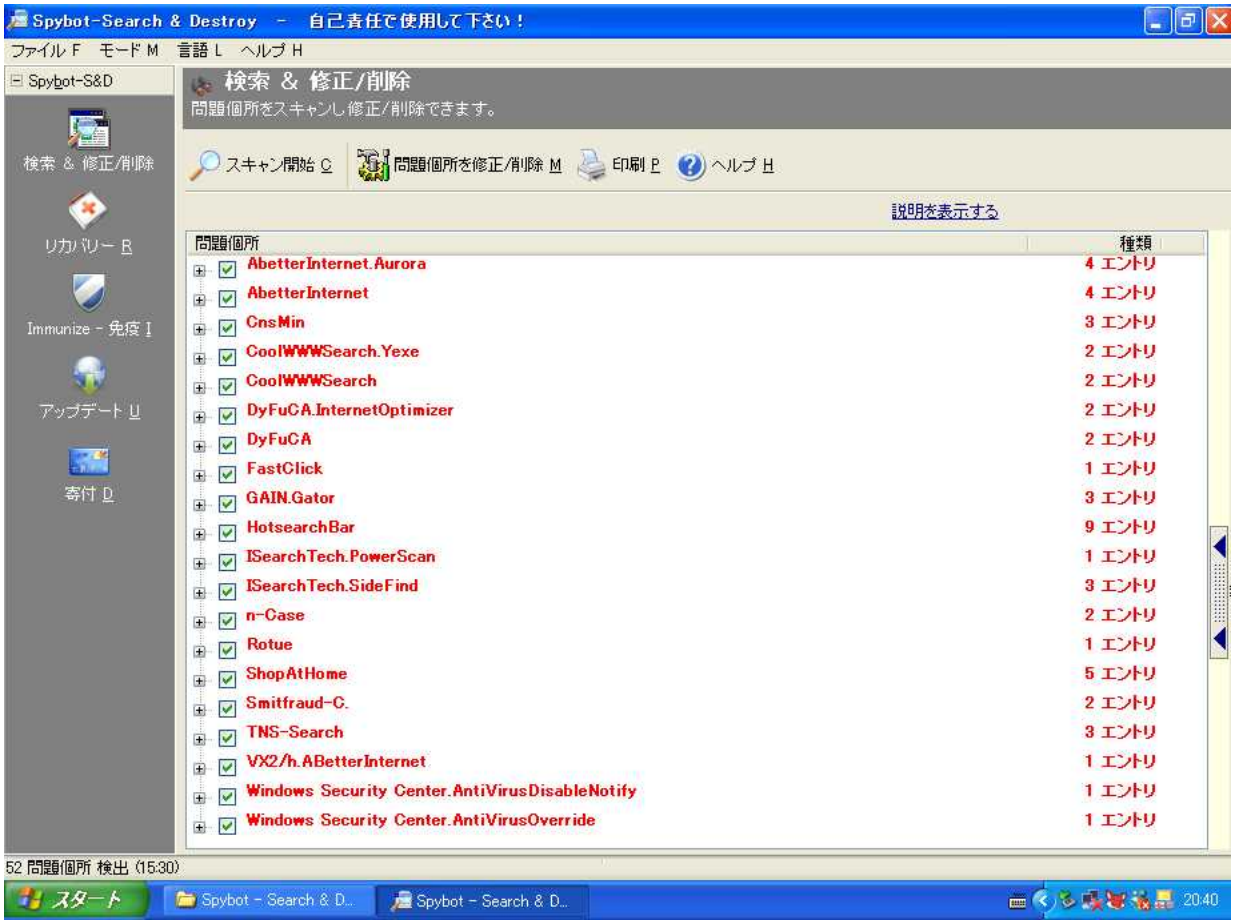
駆除する方法としては、専門の**アンチスパイウェアソフト**を利用するのがベストである。駆除用のソフトというと、「ウイルスバスター」等のアンチウイルスソフトを想像される人もいるかもしれない。だが、**数年前のアンチウイルスソフトでは、スパイウェアはほとんど駆除してくれないのである。**

例えば、大手セキュリティ会社のソフトウェアである「Norton AntiVirus」は、2003 年版まではスパイウェアには対応しておらず、2004 年版からスパイウェアも検出するようになった。最新のセキュリティパッケージソフトを利用するのも勿論対策のひとつではあるが、スパイウェアの駆除を専門としたソフトで、しかもフリーソフトとして提供されているものがいくつもある。これらを使用しない手はない。

フリーのアンチスパイウェアソフトの中でも優良なものとして「**Spybot S&D**」が挙げられる。下図は Spybot が大量のスパイウェアを検出したときの様子である。

使用にあたって気をつけるべきことは、Spybot をインストールしても、**スパイウェアを自動的に除去し続けてくれるわけではない**ということだ。加えて、スパイウェアの種類は、それこそ毎日増え続けている。**常にアンチスパイウェアソフトを最新の状態にしておかなければ、新しいスパイウェアには対応できない。** WindowsUpDate は自動更新をしてくれるが、Spybot は自分でアップデートする必要がある。

数日に一度は Spybot を起動し、最新版にアップデートをした状態で、こまめにスパイウェアを駆除することが効果的な対策となる。



Spybot S&D が 50 個以上のスパイウェアを検出した様子

4-2　ファイアウォールを利用する対応策

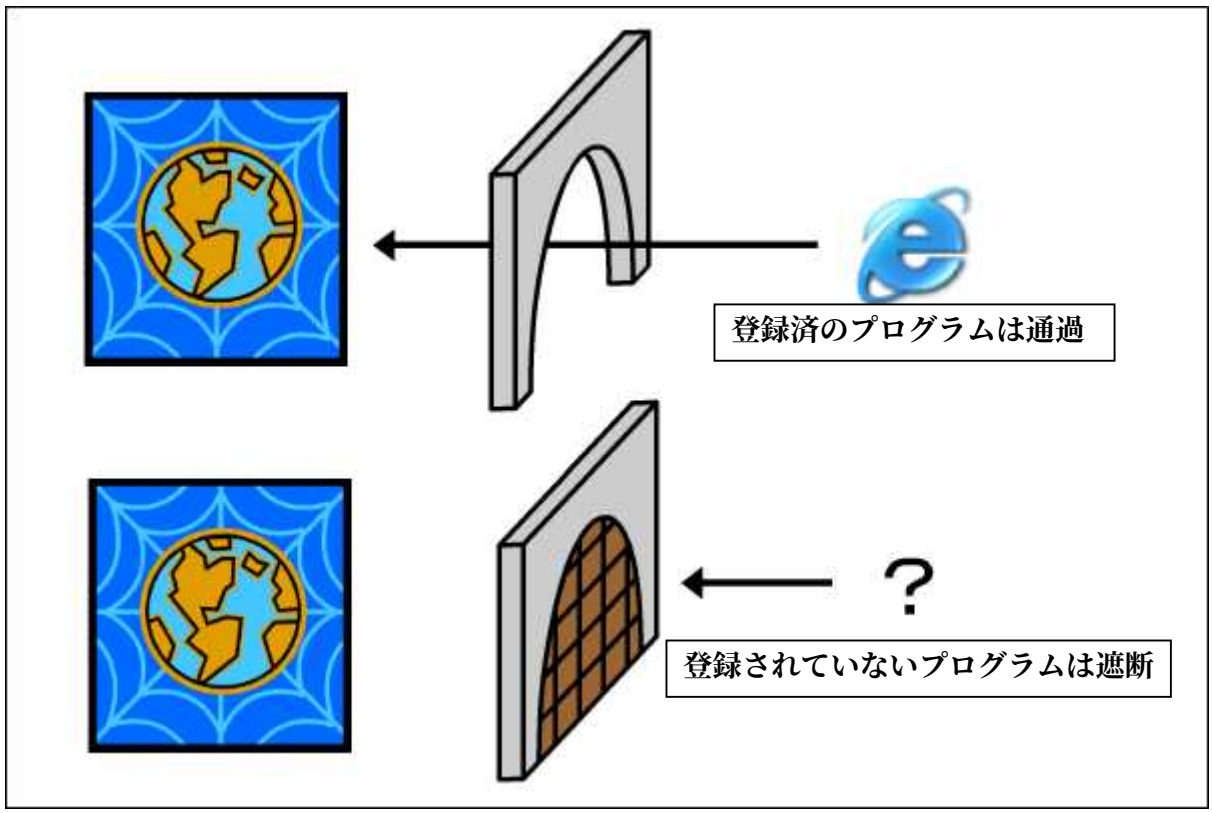
セキュリティホールの存在自体が広く公表される前にその脆弱性を悪用される「ゼロデイアタック」と呼ばれる攻撃があるように、最新のアンチスパイウェアソフトならば必ずしも全てのスパイウェアまでに対応しているというわけではない。

そこで、アンチスパイウェアソフトでは対応しきれないスパイウェアが情報漏洩するのを防ぐためには、**ファイアウォール**（※4）を導入しなければならない。最近のファイアウォールには、外部からの攻撃を防ぐだけでなく、スパイウェア等が**内部から外部へ情報漏洩するのを防ぐ機能**が搭載されている。

ファイアウォールは「プログラム単位でネット接続の可否を設定する」ことにより、不審なプログラムが外部に情報を送信するのを食い止める。コンピュータがインターネットと情報をやり取りする際には、どんな場合でもプログラムを利用している。たとえば、Web サイトを見るのであれば Internet Explorer というプログラムを利用するわけだ。この時、インターネットと情報のやり取りをしていいプログラムを事前にファイアウォールに登録しておく。そして、登録されていない不審なプログラム、つまり、スパイウェアがインターネットに接続して情報漏洩をしようとしたところを遮断してしまうわけだ。

このファイアウォール自体は、Windows のパソコンなら Windows ファイアウォールがデフォルトで使われているのだが、残念なことに、**Windows ファイアウォールには外部からの攻撃を守る機能しか搭載しておらず、内部からの情報漏洩を防止する機能は全くない。**ファイアウォールで情報漏洩を防止したいのであれば、Windows ファイアウォール以外に新たなものを別個にインストールしないといけないわけである。

ファイアウォールにも多くの種類はあるが、やはりフリーソフトでも「ZoneAlarm Free」など、優良なものはある。設定がやや難しいものもあるが、丁寧に解説をしているサイトもあるので、積極的に活用すべきだろう。



ファイアウォールがプログラム単位にインターネットへの接続を制御する様子

フィッシング (phishing)

1　フィッシングとは

1-1 フィッシングの語源

フィッシングとは、正規のメールや Web サイトを装い、それをエサにして重要な個人情報を詐取する詐欺のことである。この手法が「魚釣り」を連想させるため「fishing」が語源となった。

だが、この場合のフィッシングは英語表記にすると、「**phishing**」という綴りになる。これは、検索の時に「魚釣を意味する fishing のページ」がたくさんヒットしてしまわないようにするために、頭の部分を ph にしたという説と、偽装の手法が洗練されているという意味の「sophisticated」から一部を抜き出しこのように綴るようになったという説がある。

1-2　一般的なフィッシングの手口

一般的なフィッシングでは、下図のようなメールが届く。

UFJ銀行

UFJ銀行ご利用のお客様へ

UFJ銀行のご利用ありがとうございます。
このお知らせは、UFJ銀行をご利用のお客様に発送しております。

この度、UFJ銀行のセキュリティーの向上に伴いまして、
オンライン上でのご本人確認が必要となります。

この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします。

http://www.ufjbank.co.jp/ib/login/index.htm

また、今回のアップデートには多数のお客様からのアクセスが予想されサーバーに負荷がかかるため、下記のミラーサイトを用意しております。上記のリンクが一時期不可能になっている場合は、
下記をご利用ください。

http://www.ufjbank.co.jp/ib/login/index.htm

http://www.ufjbank.co.jp/ib/login/index.htm

お客様のご協力とご理解をお願いいたします。

UFJ銀行

金融商品勧誘方針 | 個人情報保護方針 | セキュリティについて | ご利用環境

(C) Copyright 2005, UFJ Bank Limited　UFJ銀行

UFJ 銀行を語ったフィッシングメールの実例

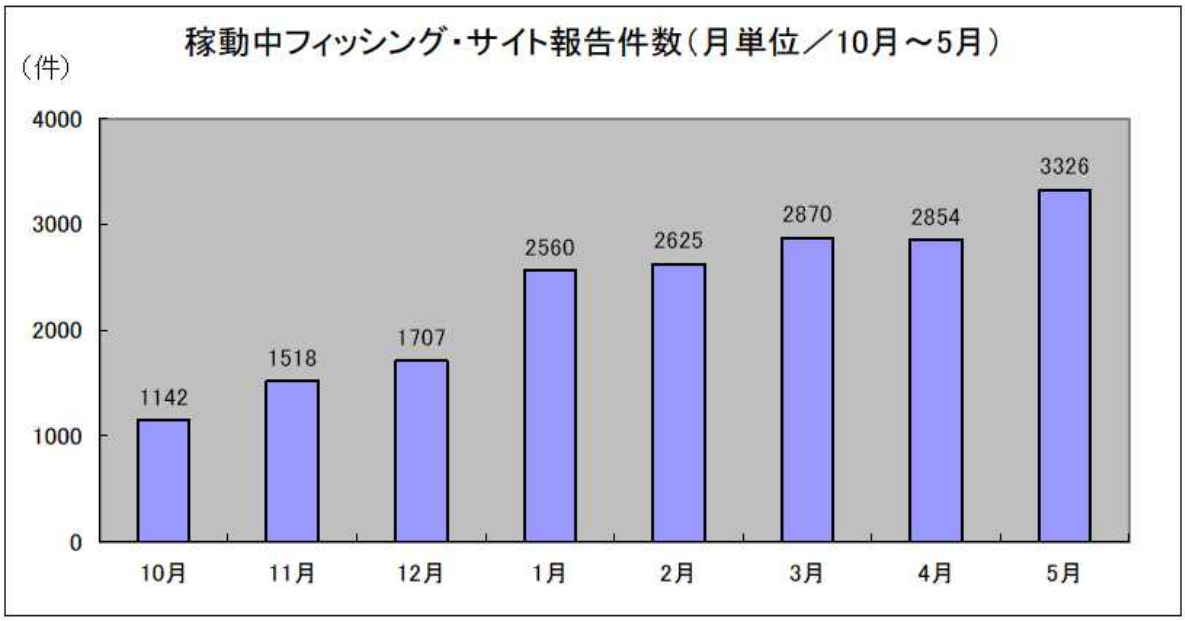
このような一般的な手口のフィッシングは「**金融機関は個人情報をメールで問い合わせたりしない**」という事実を知ることと、「**怪しいと感じたときは直接問い合わせる**」ということをすればほぼ防げる。

1-3　本論文中の定義

フィッシングの範囲には様々な説があるが、本論文中では「**e メール等の電子的な手段を使って偽物の Web サイトに誘い込み、重要な個人情報を入力させ、盗み取った情報を元に金品を奪う行為**」とする。

2　フィッシングの危険性

2-1　アメリカでのフィッシング被害



稼動中フィッシング・サイト報告件数（月単位／2004 年 10 月～2005 年 5 月）（サイト数）

図のようにアメリカでは毎月たくさんのフィッシング用の偽サイトが発見されている。このような状況で一体どのくらいの被害額になるかというと、C ネットジャパンが今年の 8 月に発表した記事で、**年間約 27 億 5000 万ドル（日本円で約 3000 億円）**という被害額が計算されている。この調査はアメリカの民間調査会社 Gartner 社が行ったものであり、調査会社によっては異なった数字が出ているところもあるが、どの調査会社も大変な金額を発表している。

2-2　日本における被害

日本における被害額は、UFJ 銀行を騙ったフィッシングが行われた際の 150 万円位のものであり(※5)、現在はほとんど被害が出ていない状況である。

しかしながら、日本の対策がゆるいと今後どんどん国内外の犯罪者に狙われてしまうということも考えられる。また、アメリカで起こった新たな種類の犯罪は必ず数年後に日本でも流行するということも言われるので、今後日本での被害や危険が増える可能性は十分あると思われる。

2-3　日本政府の動き

警察庁では、フィッシング行為自体を業務妨害罪、著作権法（複製権侵害、公衆送信権侵害等）違反等で検挙するため、**フィッシング 110 番を設置**し、フィッシング行為の取締り強化を行っている。

また経済産業省では今年の 4 月 28 日に商務情報政策局情報セキュリティ政策室に、**フィッシング対策協議会**を設立し HP による情報提供や注意喚起を開始した。

このように政府でもフィッシングの危険性を感じ、対策を講じ始めている。

3　最新のフィッシング　「ファーミング（pharming）」

3-1　ファーミングの語源

「pharming」はフィッシングと同じように「farming（農業、農場で栽培する）」の綴りの頭を ph に変えたものである。

一般的なフィッシングはユーザを偽サイトに「釣り上げる」ことからフィッシングと呼ばれているが、ファーミングでは、フィッシングとは異なりエサ（偽メール）をばら撒く必要がない。「種」さえまいておけば（仕掛けを施しておけば）、より確実かつ大量に個人情報を「収穫」できるということからこのように呼ばれている。

3-2　ファーミングの手口

ファーミングは従来のフィッシングと同じように、金融機関等を装った見た目が全く同じ偽サイトを作って個人情報を盗む。異なる部分は、従来のフィッシングがメールに偽サイトの URL を載せて送ってくるという手段で誘導してくるのに対し、ファーミングはいつも通りに**お気に入りの機能を使ったり、ブラウザに正しい URL を入力して Web サイトを開こうとするだけ**で、偽サイトへ誘導されてしまう。(※6)

つまり、ファーミングは、前述の一般的なフィッシングの対策であった「金融機関は個人情報をメールで問い合わせたりしない」という大原則を知ることだけでは防御できない、より進化した詐欺なのである。

3-3　ファーミングの対策

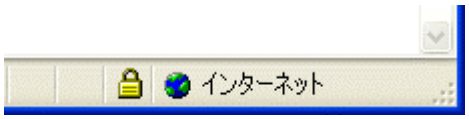
個人情報入力画面が SSL（Secure Sockets Layer）(※7) によって保護されていることを確認する。

これはフィッシング全般に有効で、偽サイトに誘導されてしまったときの予防法である。重要な個人情報を入力するページでは、通信を暗号化して情報を保護するシステム SSL が使われているので、これを確認することによりそのサイトの正当性を判断できる。

SSL が使われているか見分けるには

1.URL が「http://」から**「https://」に変わっているかどうか**確認する。

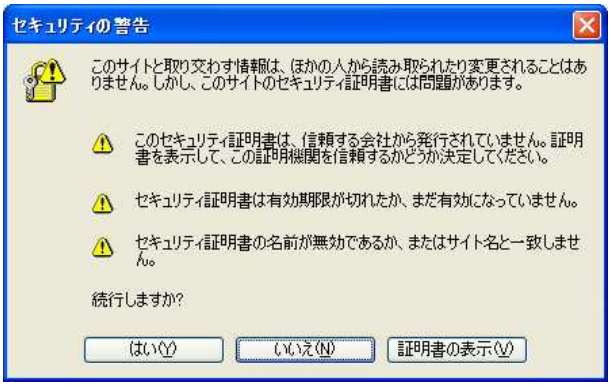
2.ブラウザの一番下や上部に**「錠前」のマークがロックされた状態で表示されているか**を確認する。



ただし、SSL を使用している画面に入る前に**「セキュリティの警告」のダイアログが出たときは偽造証明書の可能性もあるので注意が必要**である。

デジタル証明書に何らかの問題があると下図のようなダイアログが表示される。

これらの警告が出たら、偽 Web サイトである可能性があるので注意しなければならない。



Internet Explorer でデジタル証明書に問題のある SSL を利用しようとした際に表示される警告ダイアログ

4　個人情報を盗まれてしまった場合の対応策

フィッシングの一番怖いところは、被害者が気づかないまま個人情報が盗まれてしまっている点である。手口は日々進化しており、次々に新しい手口が現れるため、従来の対策では間に合わず、知らないうちに個人情報が盗まれていたということになりかねない。

最悪の事態を避けるためにも、個人情報が盗まれてしまった場合の対策も事前に講じておくべきである。

4-1　キャッシュカードの場合

銀行カードの場合、集めた個人情報を元に、ネットバンキングを用いて現金を盗むか、偽のキャッシュカードを作り、そのカードを使って現金を盗んだり、商品を購入したりしているといわれている。（Gartner 社）

ネットバンキングを行う場合は**第 2 パスワードを使用することで安全性が増す**。第 2 パスワードとは口座番号、ID、パスワードなどを入力してログインした後、さらに次の画面であらかじめユーザの持っている乱数表から指定した文字を入力させるという方法である。

指定される文字は一定時間ごとにランダムに変わるのでフィッシングにあったとしても盗まれる情報は一部分で済む。

また、偽造された銀行カードを使われないためには、最近登場した IC カード、手のひら静脈認証など最新の認証技術つきのもの（※8）を利用することが有効である。

4-2　クレジットカードの場合

クレジットカードは購買のしやすさを重視しているため先ほどの防止策をとっても依然として磁気テープの部分のみで利用できてしまう場合がある。またネットショッピングを利用する場合、カードの番号、名前、有効期限さえ分ってしまえば誰でも商品を購入できてしまう状況である。

クレジットカードの第３者の不正使用があった場合は、加盟店責任ということになっているが、決定的な防御策はないので、**カードの利用限度額、キャッシングの限度額を下げる**ということで被害を最小限にとどめることができる。

終わりに

最後に、今回伝えたい要点をまとめる。

スパイウェア対策

・Windows アップデートを行い、セキュリティホールを塞いでおく。
・信用できるサイト以外の ActiveX はインストールしない。
・ソフトウェアを利用してスパイウェアの侵入を予防する。
・アンチスパイウェアソフトでスパイウェアを駆除する。
・ファイアウォールで情報漏洩を防ぐ。

フィッシング対策

・金融機関は個人情報をメールで問い合わせたりしないということを覚えておく。
・おかしいと感じたら問い合わせてみる。
・ログイン画面など個人情報を入力する画面では SSL 認証を確認する。
・ネットバンキングは第二パスワードのあるものを使う。
・重要なカード類は偽造されにくいものを使う。
・クレジットカードの使用限度額、キャッシング限度額はなるべく低くする。

また、全般的なセキュリティ対策として情報処理推進機構が提示する基本対策を心掛ける。(※補足資料参照)
まずはこれらのことを実行して「現在潜んでいる罠」に備えなければならない。

「インターネットに潜む罠」という脅威は日々新たなものが増え続けている。私達は、更にこの「新たなインターネットに潜む罠」にもかからないようにするために、常に最新の情報に気を配る必要がある。
そして、身の回りでこれらのことを知らない人がいた時は、知っている人が教えていかなければならない。そうすることにより、罠にかかって悲しい思いをする人が１人でも減ってくれることを願う。

以上

注釈

※1

本論文中でいう個人情報とは、漏洩することによってカード偽造や直接的な金銭的被害につながるような、口座番号、ログイン ID、パスワードなどの重要な情報を指す。

※2

同じスパイウェアと呼ばれるプログラムでも、その被害の差は種類により大きく異なる。

この原因は、スパイウェアの定義の曖昧さにある。**実は、スパイウェアという用語は「コンピュータに無断で侵入し、勝手に個人情報を漏洩するプログラム」という狭義を持つ一方で、「ユーザに害を与えるプログラムは全て」という広義も併せ持っているのだ。**

この広義はいかにも範囲が広すぎるように感じられるだろうが、この広義が全世界の統一の見解というわけではない。そもそも**スパイウェアの厳密な定義はまだ出来上がってないのである。**アメリカのスパイウェア対策団体である The Anti-Spyware Coalition (ASC)が新たな定義を提唱する一方で、スパイウェアという名称そのものに反対している団体もあるのだ。

定義が確定していないため、スパイウェアという用語はしばしば混乱を招く使われ方をされる。例えば、コンピュータウイルスという用語はそれなりに認知されているが、スパイウェアとウイルスの差は実は極めて曖昧なのである。明確な差としては、「ウイルスは自分をコピーしてどんどん増殖するが、スパイウェアは他のマシンに感染することはない」ということが言える。

しかし、「ユーザの情報を漏洩し、なおかつ他のコンピュータに感染するプログラム」は、スパイウェアとウイルスの構成要件を同時に満たしていることになる。では、このプログラムはスパイウェアと呼ばれるべきか、ウイルスと呼ばれるべきなのか。現状では、呼称は完全に混乱している。

結局は何が正しいのかという話になるが、そもそも完全に正しい定義などはない。私達が理解しなければならないのは「スパイウェアには大体の意味として狭義と広義があるが、この定義は確立的なものではなく、各団体によって異なった使い方がされている」ということなのだと考えている。

日本ネットワークセキュリティ協会の各定義

ウイルス	プログラムに寄生して増殖し、感染、破壊、いたずら、盗聴などの被害を与えるプログラム
ワーム	自分自身をコピーして増殖し、感染、破壊、いたずら、盗聴などの被害を与えるプログラム
トロイの木馬	通常のソフトウェアに見せかけて、破壊、いたずら、盗聴などの被害を与えるプログラム
スパイウェア	ユーザの知らないうちに、ユーザの情報や操作履歴を外部に送信するプログラム
アドウェア	広告のウインドウをポップアップ表示させたり、ブラウザで広告を表示させるプログラム
ハイジャッカー	ブラウザ起動時に最初に表示する Web ページ（ホームページ）を変更したり、閲覧しようとするページとは異なるページへ強制的に誘導するプログラム
ボット	外部からの命令により、他人のパソコンを制御したり、攻撃の踏み台にするために、制御するパソコン側で動作するプログラム

Anti-Spyware Coalition のスパイウェア定義

下記の条件を備えるプログラム ・パソコンの操作感、ユーザのプライバシ、システムの安全性に変更を加え、ユーザによる制御を阻む。 ・ユーザがパソコンにインストールしたプログラムなどのリソースを使う。 ・ユーザの重要な情報を収集、使用、送信する。

※3

特別なプログラムを使用せずにCookie のみを使って情報を収集するスパイウェアがある。Cookie とは、Web サイトの提供者が、Web ブラウザを通じて訪問者のコンピュータに一時的にデータを書き込んで保存させる仕組みのことである。バナー広告などを表示する際に Cookie を埋め込み、ユーザが Web サイトを巡回する際に同じ会社のサーバから配信されたバナー広告を読み取ると、現在、ユーザが表示している Web サイトに関する情報を Cookie に追加していく。このため、Web サイトを巡回しているうちに、いつ、どのようなサイトを巡回したのかという情報が漏洩してしまうことになる。
正規のアプリケーションに紛れて侵入してくるタイプのスパイウェアも存在する。ダウンローダとして人気が高い「Reget Free1.7」と同時にインストールされる「TSAdBot」等が有名。

※4

このレジュメでのファイアウォールは、全て「パーソナルファイアウォール」を指している。
また、ファイアウォールの機能としては「プログラム単位にネットワークへの接続を監視する」ということ以外にも、外部からの攻撃を守る方法として「パケットのヘッダー情報チェック」や「シグネチャによるパターンマッチング」などが挙げられる。後述の参考サイトにて詳細が説明されている。

※5

UFJ カードは 2 月 7 日、同社のクレジットカード会員がフィッシング詐欺の被害に遭った可能性があることを明らかにした。同社によると、2004 年 9 月から 10 月にかけ、ルーマニアなどで偽造カードの使用が発覚。調べたところ、33 人のカードが偽造され、うち 8 人のカードでキャッシングが不正利用され、総額約 150 万円が引き出されていたという。同社は偽造されたカードの情報について、架空のメールなどで誘い、偽サイトでカード番号などの入力を促すフィッシング詐欺により不正に収集されたと見ている。

※6

ファーミングは、ウイルス、スパイウェアなどによる hosts ファイルの書き換え、DNS サーバのポイズニングという手法を用いて、ユーザを偽サイトへと誘導する。

DNS サーバのポイズニングとは、
DNS(ドメイン・ネーム・システム)サーバは、インターネット上でのコンピュータの名前にあたるドメイン名を、住所にあたる IP アドレスと呼ばれる 4 つの数字の列に変換する作業をする。URL さえわかればサイトを見ることができるのは、この DNS サーバのおかげなのである。
例えば Yahoo!のサイトをブラウザで見ようとしたときは、このようなことが行われている。

1.ブラウザのアドレスバーに Yahoo!の URL http://www.yahoo.co.jp/を入力
2.ブラウザは DNS サーバに「この URL のサーバはどこにありますか？」と尋ねる
3.DNS サーバがそのサーバのある場所 http://202.93.91.214/を指示
4.ブラウザは教えられた場所にあるサーバにアクセスして、Yahoo!のサイトを表示する

DNS ポイズニングはこの DNS サーバを攻撃して URL 情報を書き換える。つまり http://www.yahoo.co.jp/と入力しても、Yahoo!ではない偽のサイトのサーバを案内するようにしてしまうのである。

hosts ファイルの書き換えとは、

hosts ファイルはウイルスに感染したり、スパイウェアによって、書き換えられる危険がある。hosts ファイルとは、パソコンの中にあるローカルな DNS サーバのようなもので、ドメイン名とＩＰアドレスを関連付けている。hosts ファイルは、DNS サーバよりも優先して処理されるので、サーバは正常でも hosts ファイルの URL 情報が書きかえられると偽サイトへ誘導されてしまう。

※7

Web ブラウザと Web サーバ間で安全な通信を行なうために Netscape Communications が開発したセキュリティ機能。認証局の署名の入った証明書を使ったサーバの認証と Web ブラウザと Web サーバ間での通信内容の暗号化という 2 つの機能を持つ。

SSL のことを理解していれば問題はないのだが、パーソナルファイアウォールを使うとより確実な対策ができる。パーソナルファイアウォールには SSL 認証マークがないページで、指定した文字列（個人情報を登録しておく）を入力すると警告を出したり外部に送信できなくしたりする機能を持つものがある。ただし、この機能はデジタル証明書の正当性までは判断できないという欠点もある。

※8

最新の認証技術のついたカードを使う事によってカード類を偽造されにくくすることができる。

手のひら静脈認証では、

専用装置に手のひらをかざすことで、一人ひとり異なる手のひらの静脈パターンを近赤外線が読み取り、本人を確認する。これを ATM などに設置することにより安全性が向上する。

IC カードとは、

従来の偽造し易い磁気テープの代わりに偽造しにくい IC チップを使うことでカードの安全性を増したもの。

語句説明

サイバー犯罪	インターネット等の高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等、情報技術を利用する犯罪を指す。
ポップアップ	Web ページがスクリプトを使って新しいブラウザウィンドウを自動的に開き、別の内容を表示させること。
バックアップ	データの写しを取って保存すること。コンピュータに保存されたデータやプログラムを、破損やコンピュータウイルス感染などの事態に備え、別の記憶媒体に保存すること。保存されたデータのことをバックアップと呼ぶ場合もある。
インストール	プログラムをコンピュータに導入する作業のこと。
Web ブラウザ	Web ページを閲覧するためのプログラム。インターネットから HTML ファイルや画像ファイル、音楽ファイルなどをダウンロードし、レイアウトを解析して表示・再生する。
アップデート	ファイルに記録されているデータを新しい内容に変えること。更新。
デフォルト	ユーザが特に指定しない場合に設定されている標準の動作条件。
URL	Web サイトに割り振られている固有の住所のようなもの。
リソース	利用できるプログラムのこと。資源。
サーバ	インターネット上で各種のサービスを提供しているコンピュータ

参考 URL

スパイウェア対策ソフト関連

SpywareBlaster　SpywareGuard 開発サイト
　Javacool Software　　http://www.javacoolsoftware.com

Spybot S&D 開発サイト
　The home of Spybot-S&D　　http://www.safer-networking.org/

これらのソフトの使用方法は、下記のサイトでわかりやすく説明されています。
　【アダルトサイト被害対策の部屋】　http://www.higaitaisaku.com/

ファイアウォール関連

ZoneAlarm 開発サイト
　Zone Labs　http://www.zonelabs.com

このソフトの使用方法は、下記のサイトでわかりやすく説明されています。
　初心者のための Zone Alarm 導入解説　http://www5f.biglobe.ne.jp/~ayum/beginner/zonealarm.html

ファイアウォールの仕組みについては、下記のサイトでわかりやすく説明されています。
　5 分で絶対に分かるファイアウォール
　　http://www.atmarkit.co.jp/fsecurity/special/17fivemin/fivemin00.html

ニュース記事関連

ZDNet Japan スパイウェア CoolWebSearch にご注意--米で大規模な個人情報盗難が発覚
　　http://japan.zdnet.com/news/sec/story/0,2000052528,20086266,00.htm
ITmedia ニュース UFJ カード会員がフィッシング詐欺被害か
　　http://www.itmedia.co.jp/news/articles/0502/07/news048.html
IT Pro IT マネージャが考える 2005 年ネットワーク・セキュリティの脅威はスパイウエア」，米 WatchGuard
　　http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20050125/155202/

セキュリティベンダ

シマンテック・ワールド・ワイド・ホームページ　　http://www.symantec.co.jp/
Trend Micro Homepage (Japan)　http://www.trendmicro.co.jp

その他

Anti-Spyware Coalition　　http://www.antispywarecoalition.org/
NPO 日本ネットワークセキュリティ協会　　http://www.jnsa.org/
IPA 情報処理推進機構　　http://www.ipa.go.jp/
警察庁　サイバー犯罪対策　　http://www.npa.go.jp/cyber/
フィッシング詐欺サイト情報　　http://www.rbl.jp/phishing/
All About　　http://allabout.co.jp/
Anti-Phishing Working Group　　http://www.antiphishing.org/
フィッシング対策協議会　　http://www.antiphishing.jp/
IT 用語辞典 e-Words　　http://e-words.jp/

参考文献

「すっきりわかった！　セキュリティ」　ネットワークマガジン編集部編　アスキー　2005 年
「インターネット個人情報防衛マニュアル」　御池鮎樹著　工学社　2004 年
「とっておきの秘技　迷惑メール・スパイウェアの撃退法」　持丸　浩二郎著　C&R 研究所　2005 年
「日経 NETWORK　2005 年 2 月号・7 月号・9 月号」　日経 BP 社

メモ

参考資料　　情報処理推進機構が提示するパソコンユーザのための基本対策 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時は、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。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等で、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 MS Word や MS Excel のデータファイルを開く時に、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。

・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。
・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。
・タスクバーなどに妙なアイコンができる。
・いきなりインターネットに接続しようとする。
・ユーザの意図しないメール送信が行われる。
・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。