

セキュリティ対策まんが クジョたいさく物語 (もう少し詳しく知りたい人のための おはなし編)

現在の私たちの生活は、IT のおかげで、とても便利になりました。インターネットで検索すると、あらゆる情報が瞬時にして手に入ります。昔は手紙という手段しかなかったのに、Eメールの登場によって、簡単に意志や情報の伝達ができるようになりました。買い物や銀行送金も、インターネット経由で自宅からできます。さらには、携帯電話や情報家電の発達によって、携帯電話でもテレビを見ることができたり、家の外にいても、お風呂を沸かしたり、DVDレコーダのスイッチを入れることができます。

しかし、このように、生活が便利になる一方で、インターネット上で起こる被害も、だんだん悪質になってきています。たとえば、ID やパスワードを盗まれて、銀行口座のお金を他人の口座へ不正に送金されたり、見ず知らずの人が、自分になりすまして Web ショッピングをしたりなど、インターネット上で被害が、現実の金銭的被害に結びつくケースが目立つようになってきています。ウイルスや不正プログラムによる被害もあとを絶たず、スパイウェアやボットの脅威も大きくなる一方です。

インターネットを使う人にとって、頭の痛いことは、これらの脅威と対策について、自ら学習して、自分の身は自分で守らなければならない、ということです。それなのに、インターネット上では、次から次へと新しい脅威が発生しています。たとえば、昔は、コンピュータウイルスについて知っていれば良かったのに、今は、スパイウェアやボット、フィッシング詐欺、ファイル交換ソフトにまつわる情報漏えいの脅威など、知らなければいけないことが多すぎるのです(しかも、知らない被害にあってしまいます)。それに、セキュリティ対策を教えてください様々なニュースや対策サイトも、ちょっと難しいセキュリティ用語を使っているの、その用語を理解するのもひと苦労です。たとえば、「ぜい弱性」という言葉の意味を知らないと、そこから先に読み進むことさえ難しくなってしまいます。だから、ぜい弱性対策をせずに、そのままほったらかし、なんてことになりかねません。そこで、この原稿では、マンガでセキュリティ対策のポイントをお知らせすることにしました。

主人公は、クジョたいさく氏。ウイルス駆除対策をはじめ、情報事件を専門にしているコンサルティング事務所の所長です。しっかり者のナイスガイのように見えますが、その実体は、ドジでマヌケなお人好しです。セキュリティ対策も穴ばかりで、被害にあってしまいます。こんなことでは、情報事件専門のコンサルティング事務所をやっているのかどうか、心配になってしまいます。そんなクジョ氏にアドバイスをしてくれるのが、クジョ氏の隣人で、セキュリティ対策の大家、Dr. セキです。フルネームは関由利貞(せき・ゆりさだ、くれぐれもせき・ゆりていと読まないように)。物語を始めるまえに、影の登場人物についてお知らせしましょう。



クジョたいさく



Dr. セキ

(この物語はフィクションであり、実在の人物や事件とは何の関係もありません。)



Mr. Jacks Modular



ウイルス



ボット



スパイウェア

ジャックス・モジュラー: 某国連邦捜査局の捜査官。未解決の情報事件を解決すべく追いかけてます。

ウイルス: 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムです。感染すると、さまざまな悪さをしかけてきます。

ボット: コンピュータウイルスの一種です。感染したコンピュータをインターネットを通じて外部から操縦することを目的として作成されたプログラムで、感染しても気づきにくいという特徴があります。

スパイウェア: 利用者や管理者の意図に反してコンピュータにインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラムです。

***** さあ、それでは、物語のはじまり、はじまり *****

この「おはなし編」は、通信協会雑誌 2006 年 9 月号、10 月号に連載された「クジョたいさく物語」に、2007 年 6 月 1 日までの状況を加味し、加筆・更新したものです。

第1話 「ウイルス対策ソフトは最新のものにすべき」の巻



ウイルス対策ソフトは・・・最新版を活用すべし



コンピュータウイルスの検出には、ウイルス対策ソフト(ワクチンソフト)が有効です。ウイルスは、次々と新種・亜種が登場しています。そこで、ウイルス対策ソフトを新しいウイルスに対応できる状態に保つようにしないと、せっかくウイルス対策ソフトを使用しているにもかかわらず、新種のウイルスの検出ができず、ウイルスに感染してしまうことがあります。ウイルス対策ソフトはいつも**最新版にすることを忘れないように**しましょう。なお、ウイルス対策ソフトには、自動更新機能が付いていますので、この機能を利用すると便利です。ウイルス対策ソフトは定期的に更新して、常に最新の状態にしておきましょう。

さて、クジヨ所長は、最近、新しいパソコンを買いました。新しいパソコンには、ウイルス対策ソフトのお試し版があらかじめインストールされていることがありますが、一定期間を過ぎると、利用できなくなったり、ウイルス定義ファイルを更新できなくなったりします。そうすると、「対策ソフトは期限切れです」などのメッセージが届くことがあります。その時は、新たにウイルス対策ソフトを購入する必要があります。クジヨ所長は、こんな基本的なことを知らなかったために、メッセージを無視して、ウイルスに感染してしまったのです。また、ウイルス対策ソフトを購入した場合でも、更新の権利には期限がありますので、期限切れの場合は、更新の権利を再度購入する必要があります。

ところで、クジヨ所長のパソコンが感染したウイルスは、どうやら何らかの症状が出るものだったらしいですね。昔のウイルスは、ある時間が来ると歌を歌ったり、クイズを出すようないたづらをしたり、パソコンの中のデータを破壊するような悪さをするものがありました。しかし、最近のウイルスは、何の症状も出さずに裏で悪事を働くものが多くなっています。たとえば、感染した PC から大量のウイルスメールを自動送信したり、外部からネットワーク経由で感染した PC が操られ、情報が漏えいしたり、特定の目標を攻撃するパケットが送信されていることもあります。

また、スパイウェアというものもあります。スパイウェアは気づかぬうちにパソコンに侵入してきます。スパイウェアに感染した PC からは、インターネットバンキングの口座の ID やパスワードが盗み出され、不正送金の被害にあった例もあります。スパイウェアの検出には、スパイウェア対策ソフトを利用します。この場合も、定義ファイルの定期的な更新が必要となります。ウイルス対策ソフトの中には、スパイウェア検出機能を持っているものがありますので、製品を購入



する際に確かめましょう。

第2話「修正プログラム（パッチ）をあてるべき」の巻



OSやソフトウェアには最新のパッチをあてるべし!

ウイルスやスパイウェアなどの不正なプログラムには、プログラムの弱点箇所(セキュリティホール=ぜい弱性)を利用して侵入するものがあります。コンピュータの中のOSやソフトウェアにぜい弱性があると、インターネットにつないただけでウイルスに感染する可能性があります。ぜい弱性は、基本ソフト(OS=オペレーティング・システム)だけでなく、各種ソフトウェアにも

存在する場合があるので、最新の修正プログラム(パッチ)をあてておくことが重要となります。

Windowsを使っている場合は、Windows Update または Microsoft Update を定期的に行います。また、自動的に更新する機能がある場合は、それを利用すると、更新のし忘れがなく、便利です。WindowsXP の自動更新は;[スタート]→[コントロールパネル]→[セキュリティセンター]→[自動更新] で設定します。

さて、クジヨ所長は、更新を促すメッセージが表示されたのに、「パッチをあてる」という基本的なことを知らなかったために、このメッセージを無視してしまいます。そこで、クジヨ所長のパソコンは、ぜい弱性を抱えたままになってしまうのです。このようなぜい弱性には、外部から自由にコンピュータを操作されてしまう、という危険なぜい弱性もあります。「おまえが我が国国防省のコンピュータに攻撃を仕掛けていることを突き止めた。」というメッセージが届いたところを見ると、どうやら、インターネット経由で不正なプログラムをインストールされて、某国のコンピュータを攻撃する踏み台として使われたようです。こんなふうに、知らないうちに、攻撃者にならないように、コンピュータのOSやプログラムには、必ずパッチをあてて、ぜい弱性を塞ぎましょう。

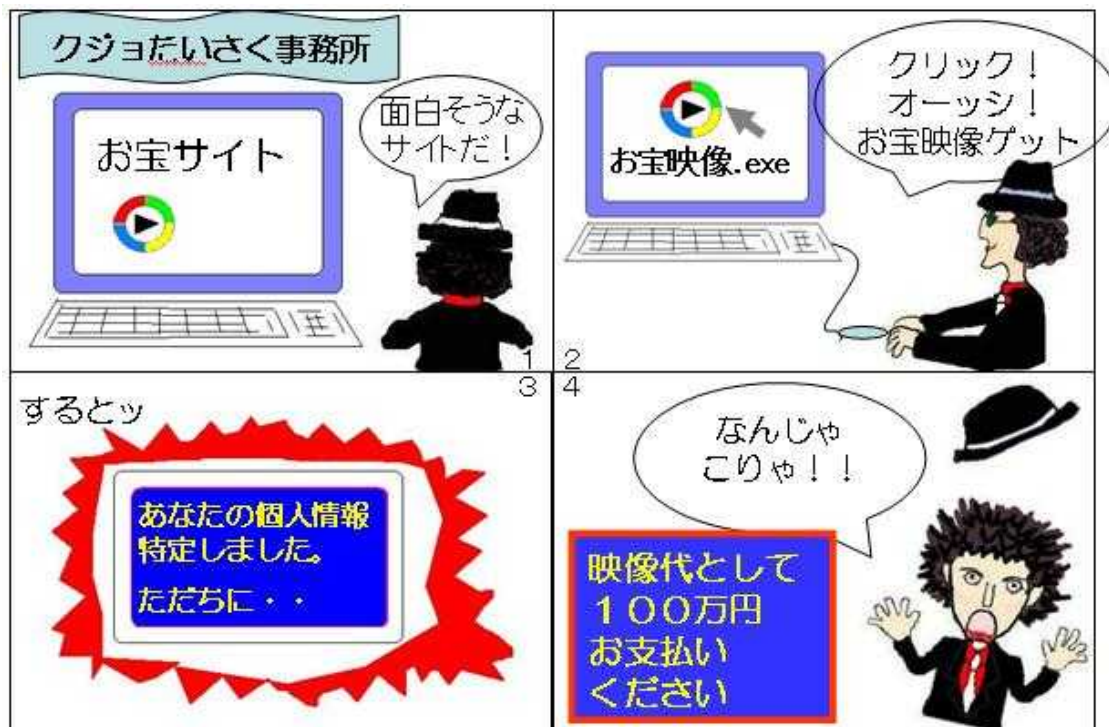


最近では、ボットというウイルスが急増しています。ボットは、メールの添付ファイルや悪意のあるWeb サイト、不正アクセス、ぜい弱性の悪用により感染します。コンピュータに侵入したボットは、ボットネット(botnet)という独自のネットワークに自動的に参加し、外部(攻撃者)からの指令により一斉に組織化された攻撃を行います。ボットは、侵入したことも、攻撃していることも、利用者に気づかれずに、何の症状もあらわれません。また、亜種も多く、多数のボットネットが形成されていると見られています。このような不正プログラムに操られて、攻撃に加担することのないよう、ウイルス対策ソフトの導入と更新、ぜい弱性の解消は、必ず行なうようにしましょう。



パソコンのOS(オペレーティングシステム)の中でも、Windows 98/Me は2006年7月に製造元のサポートが終了しています。サポートが終了した場合、セキュリティパッチが発行されませんので、ぜい弱性が解消できず、被害に遭う可能性が極めて高くなります。できることなら使用しないことが望ましいのですが、どうしてもという場合は、ネットワークに接続しない状態で利用することをお勧めします。

第3話「あやしいファイルを開くな（ホームページ編）」の巻



ソフトウェアの安易なダウンロードやインストールは避けるべし

インターネットのホームページには、不正なプログラムを、一見有用なソフトウェアや画像にみせかけて掲載しているページがあります。このようなプログラムがダウンロードされて、コンピュータの中に入りこむと、個人情報盗まれたり、ハードディスクの内容が破壊されたりする場合がありますので、注意が必要です。不審な Web サイトの閲覧を控え、ソフトウェアの安易なダウンロードは避けましょう。

さて、クジヨ所長は、インターネットのホームページで「お宝映像.exe」というファイルをクリックして開いてしまいました。そうすると「あなたの個人情報を特定しました。ただちに、映像代として 100 万円お支払いください。」というメッセージが表示されました。このような手口は、**ワンクリック詐欺**とされています。よくある手口は、アダルトサイトなどで画像をクリックしただけで、利用料金を請求され、「ご利用ありがとうございます。料金は△△円です。あなたの IP アドレスは x.x.x.x、プロバイダは ○○ です。」などと、いかにも利用者の情報を特定したようなメッセージを表示して、料金を支払うように脅します。数分おきにコンピュータに料金請求画面を表示する不正プログラムを埋め込まれる場合もあります。このようなメッセージが表示されても、料金を払う必要は一切ありません。無視しましょう。

クリックしただけで料金請求された場合の対応方法について <http://www.ipa.go.jp/security/ciadr/oneclick.html>

ワンクリック詐欺の場合、基本的には無視し続けていれば良いと思われそうですが、最近では、何回もサービス内容や使用条件を提示して、クリックさせるケースがあるようです。何回もクリックした場合、条件がわかりにくく書いてあっても、条件に同意したとみなされる可能性がありますので、注意が必要です。

料金を支払う必要があるのか心配で、法的な相談をしたい方は、お近くの消費生活センターや国民生活センター、もしくはお住まいの自治体の無料弁護士相談などへご相談したらよいでしょう。万が一、サイト側からしつこい請求などを受けるようでしたら、最寄りの警察機関にも相談されることをお勧めします。

また、画像や動画を見ようとした時に、警告画面が出ることがあります。不正プログラムを取り込まないために、警告が出たら、先に進まないような用心深さも必要です。

警告画面を無視していませんか? <http://www.ipa.go.jp/security/txt/2007/04outline.html>

拡張子に気をつけるべし！（あやしいファイルの見分け方）

怪しいファイルを見分けるためには、拡張子についての知識が必要です。「拡張子」とは、ファイル名の末尾にある3文字程度のアルファベットのことで、そのファイルの種類をあらわします。

【ファイルの種類とアイコン、拡張子の対応表】

ファイルの種類	アイコン例	ファイル名+拡張子の例
zip 圧縮ファイル		圧縮ファイル.zip
画像ファイル		画像.jpg
文書ファイル		文書.doc
動画ファイル		動画.wmv 動画.mpg
テキストファイル		テキスト.txt
実行形式ファイル		実行ファイル.exe

クジヨ氏がゲットした「お宝映像.exe」では、exe が拡張子です。この拡張子がついたファイルは、開いたとたんにコンピュータ上で動き始めるプログラムです。このようなプログラムの拡張子としては、exe, pif, scr, bat, com などがあります。

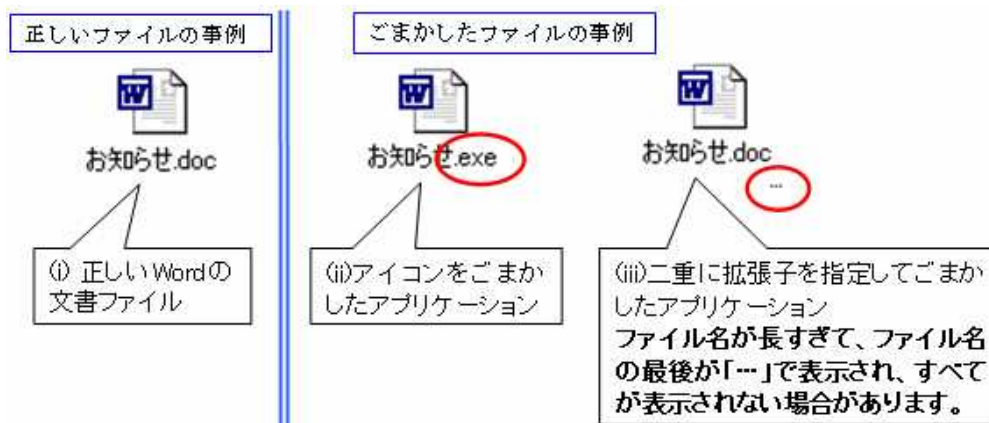


【開くと動作する拡張子の例】



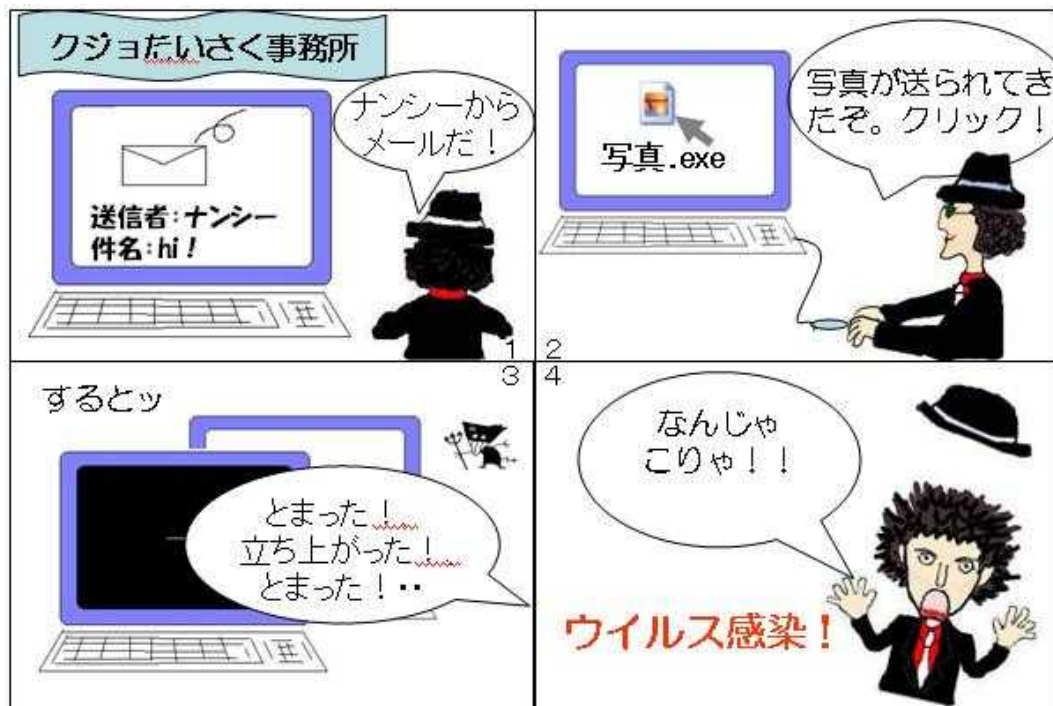
(これらの拡張子がついたファイルが、必ずしも不正プログラムというわけではありません)

拡張子が表示されない場合は、「マイコンピュータ」→ [ツール]—[フォルダオプション] を選択し、「表示」タブの中で [登録されている拡張子は表示しない] のチェックを外します。そうすると拡張子が表示されるようになります。中には、アイコンを偽装して、動画ファイルや画像ファイルなどのようにみせかけているもの、二重に拡張子をつけて拡張子をごまかす場合がありますので、注意が必要です。たとえば、「お知らせ.exe」というファイル名なのに Microsoft Word のアイコンに偽装している場合や、「お知らせ.doc (長いスペース) .exe」というように拡張子を二重に付けて、後の「.exe」を簡単に表示されないようにしている場合です。このようなファイルは次のように表示されます。



あやしいファイルの見分け方 <http://www.ipa.go.jp/security/txt/2005/12outline.html>

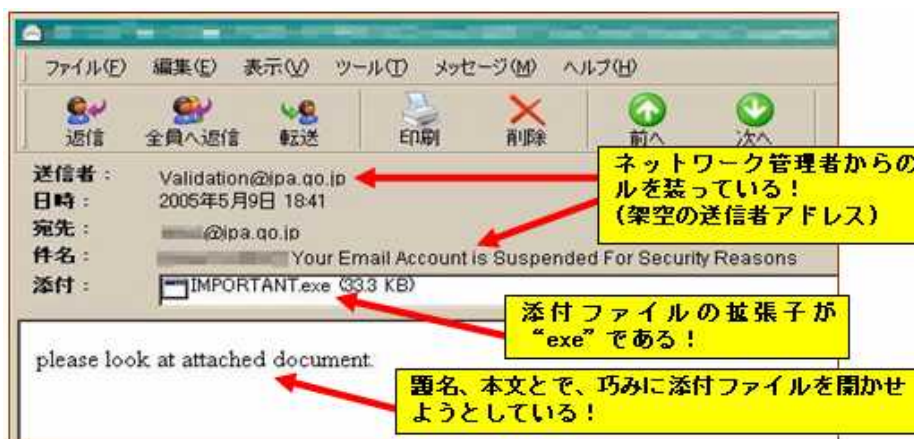
第4話 「あやしいファイルを開くな（メール編）」の巻



メールの添付ファイルは安易に開かない

ウイルスは、知人からのメールに見せかけて送りこまれることがあります。知人だけではなく、管理者や、セキュリティ会社からのお知らせのように見せかけて、添付ファイルを開かせるための、言葉巧みなメッセージがメール本文に記載されていることもあります。

たとえば、Web ショッピングサイトのオーナーに、「お宅で買った商品が壊れていたので交換してください。このメールに写真を添付したのでご確認ください!」と苦情メールにみせかけたケースがありました。オーナーは、添付ファイルをクリックしたために、キーボードから入力された情報を記録するキーロガーと呼ばれるスパイウェアがコンピュータにインストールされ、ネット銀行の口座番号や暗証番号がインターネット越しに盗み出され、不正にお金を引き出されてしまいました。これなどは、特定の個人を狙ったいわゆる「標的型攻撃」(「スパイ型攻撃」ともいいます)です。標的型攻撃を受けた場合、被害を受けても気づきにくいのが現状です。このような攻撃があることを知り、さらに十分に注意する必要があります。



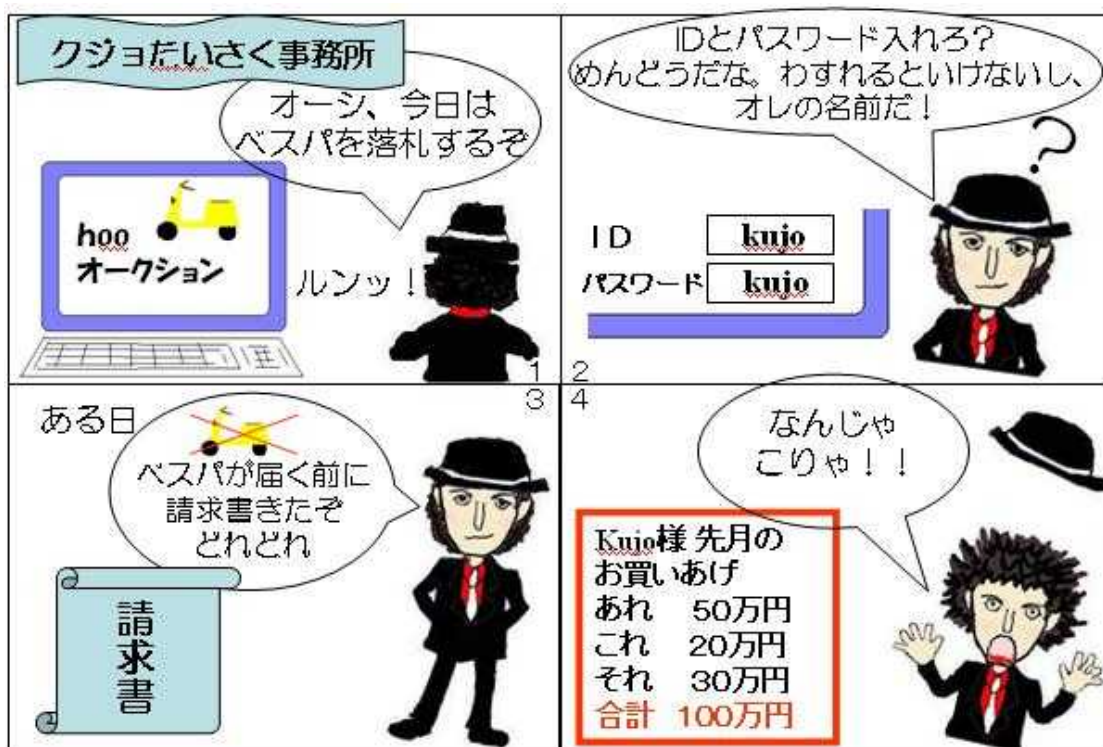
【怪しい添付ファイルの見分け方 (Outlook Express の場合)】

さて、クジヨ所長のところには、知り合いのナンシーから、写真にみせかけた実行形式ファイルが送り込まれ、「メールの添付ファイルは安易に開かない」というウイルス対策の基本を知らなかったクジヨ所長は、あっさりウイルスに感染してしまいました。添付ファイルは開く前にウイルスチェックをしましょう。また、拡張子が

「.exe」などであった場合には、ウイルスの可能性が大きいので、ナンシーにファイルを送ったかどうか確認したほうが良いでしょう。この場合、メールの送り主は、ナンシーではなく、ナンシーになりすましているウイルスかもしれないからです。

メールの添付ファイルの取扱い5つの心得 <http://www.ipa.go.jp/security/antivirus/attach5.html>

第5話 「パスワード管理に気をつけて」の巻



安全なパスワードを設定し、定期的に変更すべし

ネットワークやシステムでは、利用できるユーザを識別し、ユーザによって利用できる範囲を決めています。そのユーザを確認する方法が、ID とパスワードです。インターネット上のショッピングサイトでは、買い物をする時に、ID とパスワードの入力を求められますが、このID とパスワードが漏れた場合、なりすまして買い物をされるということも十分に考えられます。単純なパスワードは、推測されやすいので、とても危険です。また、辞書攻撃ツールというものもありますので、辞書に載っている単語をそのままつないだパスワードも、簡単に解読されてしまいます。生年月日をパスワードにするのもやめましょう。

さて、クジヨ所長は、忘れるといけないからと、ID とパスワードを同じにして、しかもそれを自分の名前にしていました。そのために、ID とパスワードが簡単に破られてしまい、自分になりすました誰かに、買い物をされてしまいます(もっとも、単純なパスワードは受けつけないショッピングサイトも多くなっています)。

生年月日のような、推測されやすいパスワードをつけていると、銀行のキャッシュカードが盗まれてお金を不正に引き出されても補償を受けられない場合がありますので注意が必要です。本人には覚えやすいが、他の人が推測できない複雑なパスワードをつけるようにしましょう。

パスフレーズによるパスワード設計の参考例

ステップ 1: パスフレーズを思い浮かべる。
(例: 人生いろいろ)

JINSEI IROIRO

ステップ 2: 母音を抜き記号や数字を挿入



パスワード **J#NS!2R\$R**

(ここで挙げたものは、公開されたことになり
ますので利用しないで下さい)

破られにくいパスワード

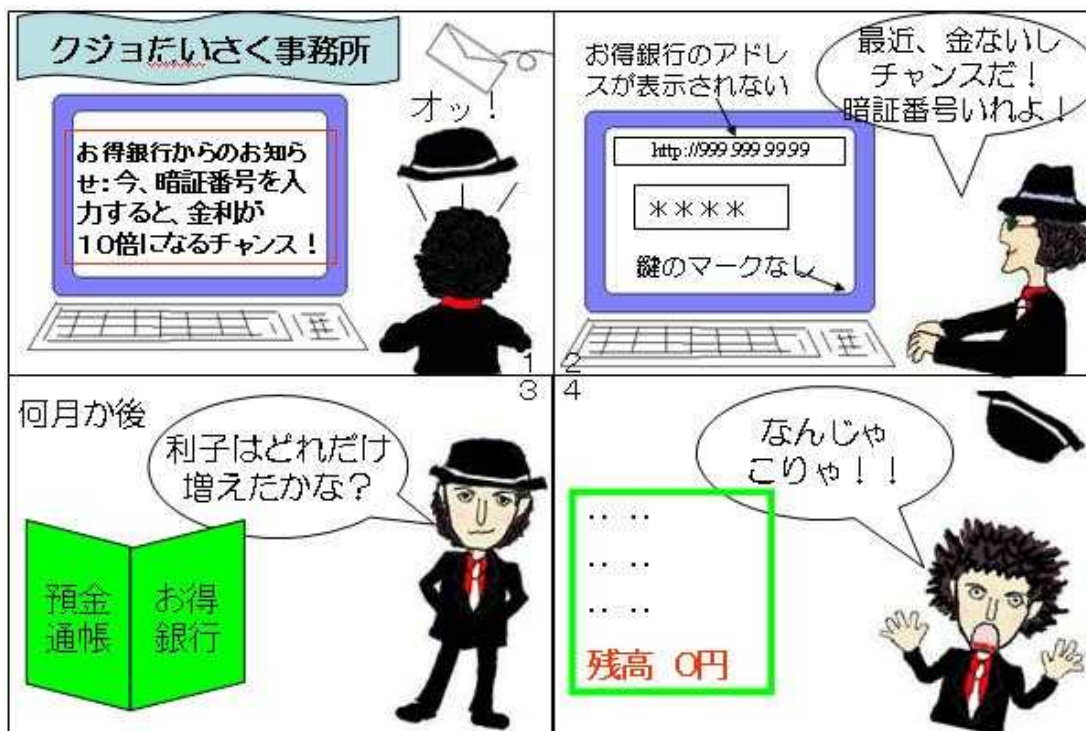
1. 大文字・小文字・数字・記号の組み合わせ:
記号(!, # 等)、数字、英字を適当に織り交ぜる。
2. 長いパスワード: 最低 8 文字以上
3. 推測しづらく自分が忘れないパスワード:
無作為で意味を持たない文字列であること。

パスワード盗難対策:

1. 定期的に変更する。
2. 紙に書き留めない。
3. 人に教えない。

たかがパスワード、されどパスワード http://www.ipa.go.jp/security/crack_report/20020606/0205.html#spe1

第6話 「うかつに個人情報を入力するな」の巻



個人情報を安易に入力しない



銀行や企業などを装った電子メールを送り、受信者を本物そっくりの偽のホームページにおびきよせて、口座番号、クレジットカード番号、ID、パスワードなどの個人情報を騙し取る行為(フィッシング詐欺)が増えています。このような情報が盗まれると、実際の金銭的被害にあらうことがあります。フィッシング詐欺に限らず、個人情報は安易に入力しないようにしましょう。

さて、クジョ所長は、「お得銀行」からの「お得なお知らせ」につられて、「お得銀行」になりすました、偽のサイトに誘導されて、暗証番号を入力してしまいます。重要な情報を入力する場合は、URLを確かめたり、暗号化通信が行なわれていることを示す鍵マークを確認する、銀行に問い合わせるというようなことが必要ですが、その基本をおろそかにして、安易に暗証番号を入力したため、お金を全部引き出されてしまいます。フィッシング詐欺は、ユーザを騙すことによって成り立っています。よって、メールの内容を安易に信用せず、まず疑ってかかることが原則です。

フィッシング詐欺の被害に遭わないためには、次の点に注意しましょう。

- (1) メールを送信元(差出人)やメールの内容を安易に信用しない
メールは送信元を簡単に偽装できます。また、金融機関がクレジットカード情報やパスワードなどを問い合わせるメールを出すことは通常ありません。あやしいと思ったら、金融機関に問い合わせましょう。
- (2) メール本文中にあるリンクを安易にクリックしない
悪意を持って設置されているWebサイトには、閲覧するだけで不正なプログラムを埋め込まれてしまうような悪質なものもあります。リンクをクリックする前に、そのメールが信頼できるものかどうか、確認しましょう。
- (3) 情報を入力する前に本物のサイトかどうか確認する。確認のポイントは次の2点です。
 1. Webブラウザのアドレスバーに表示されたアドレス(URLのドメイン名部分、「//」から一つめの「/」で区切られている範囲)が、正しく表示されていることを確認します。また、Webページの一部を右クリックし、[プロパティ]を選択するとそのページの詳細情報を表示できます。
 2. Webブラウザに鍵マークがあることを確認します。なお、鍵マークを偽装するケースや、フィッシングサイトでもサーバ証明書を取得して鍵マークを表示している場合もありますので、鍵マークをダブルクリックして、証明書を表示し、運営者を確認します。



フィッシング詐欺に騙されないために

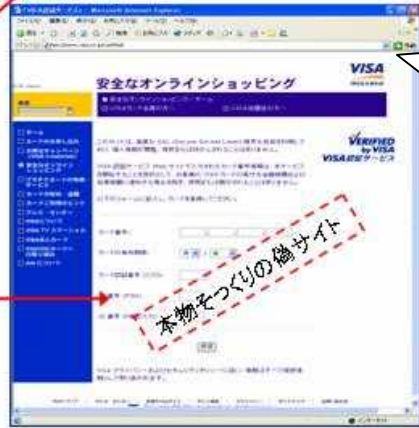
フィッシング自体は単純な原理に基づきますが、ユーザを騙すためにさまざまな工夫がこらされています。たとえば次の図のように、「ユーザを錯誤させる騙しメール」を送ってきます。あたかも本物のクレジット会社から送られてきたように見えますが、メールの送信元はなりすまされています。このメールでは、カードのセキュリティを強化するためとあって、メール本文中の URL をクリックさせます。クリックすると、「本物に見間違えるような偽サイト」に飛ばされ、そこで「個人情報の入力を求める」ページが表示されます。このような手口に騙されないようにしましょう。

ユーザを錯誤させる騙しメール

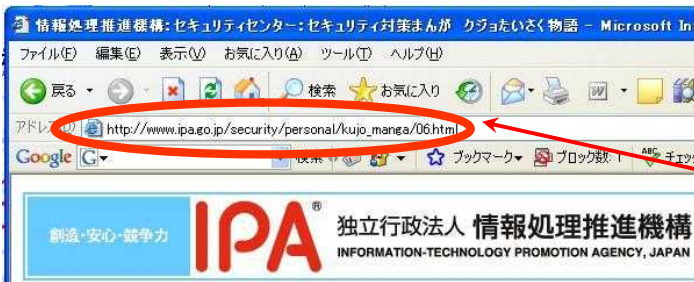


送信元が update@visa.co.jp の送信元詐称メール。文中のリンク https://www.visa.co.jp/verified/ は、VISA の正規の URL に見えるが、HTTP のソースでは http://81.196.163.74/verified/ を指していた。クリックするとフィッシングサイトへジャンプし、カード番号やID番号の入力を促す。

本物そっくりの偽サイトで、個人情報の入力を求める



【本物のサイトかどうか確認する】

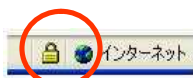


● Web サイトの URL を確認する

Web ブラウザのアドレスバーに表示されたアドレスを確認する。URL のドメイン名部分、「//」から一つめの「/」で区切られている範囲が、正しく表示されていることを確認。

● Web ページのプロパティで URL を確認する

Web ページの一部を右クリックし、[プロパティ]を選択するとそのページの詳細情報を表示できます。



- 鍵マークを確認する。
- 鍵マークをダブルクリック、証明書を表示して運営者を確認する。

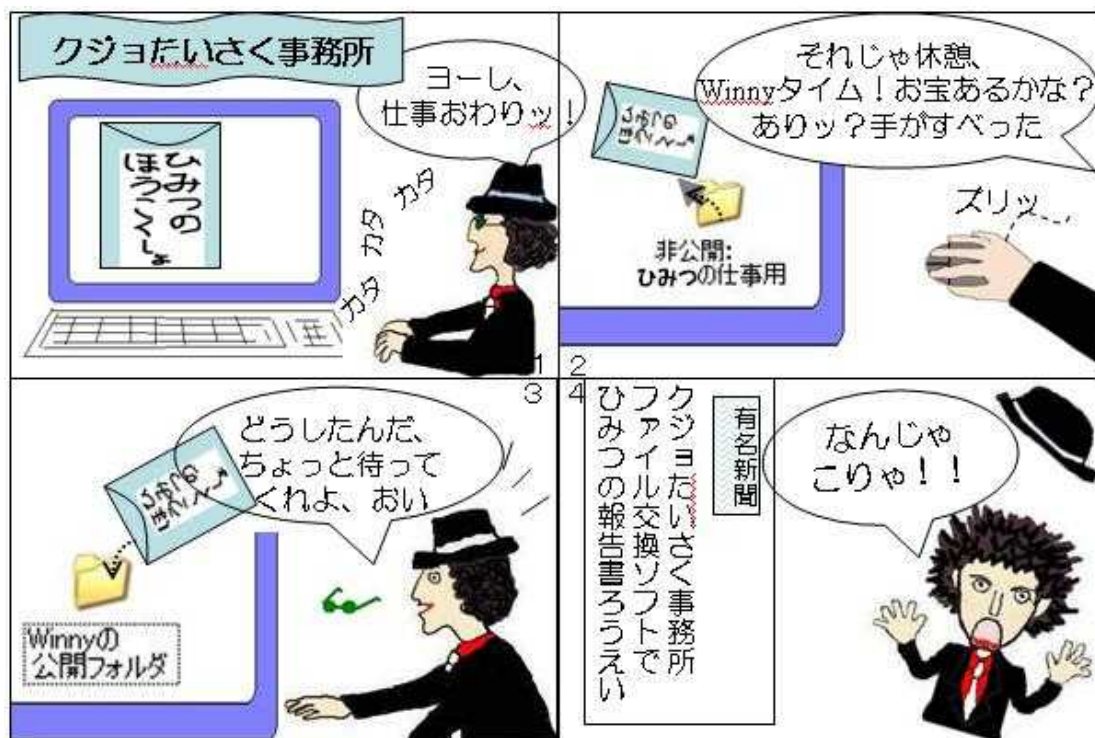
マウスの右クリックによりプロパティを表示



現在アクセスしているサイトの URL を確認



第7話 「P2P ファイル交換ソフトに注意」の巻



大事な情報を保存しているパソコンでファイル交換ソフトは使わない!

P2P(ピアツーピア)ファイル交換ソフトとは、サーバを介さずに、クライアント同士がインターネット経由で直接ファイルを交換できるようにするソフトウェアです。このところ、Winny というファイル交換ソフトを介した情報漏えい事故が多数報道されています。

これらの事件の主な原因は、コンピュータ内のファイルが、本人の意図に反し、ウイルス感染により、ファイル交換ソフトの公開用フォルダにコピーされてしまうといったものです。こうしたウイルスは、「お宝画像」、「個人情報」のような、多くの人々が興味を持つようなファイル名でファイル交換ネットワーク上に流通しています。また、本人の誤操作が原因のこともあります。公開してはならないファイルを誤って公開用フォルダに置いたり、公開したくないフォルダを誤操作により「公開」に設定してしまうケースです。

P2Pファイル交換ソフトの公開用フォルダに置かれたデータは、世界中のファイル交換ソフト利用者が入手できる状態になり、ネットワーク上に流出します。流出したデータは、不特定多数の利用者が入手するため、回収は事実上不可能です。

さて、クジヨ所長は、Winnyの愛用者で、休み時間は、Winnyタイムとばかりに、Winnyで集めてきたお宝映像をチェックしようとします。ところが手がすべってしまい、「ひみつのほうこくしょ」を公開用フォルダに誤って置いてしまいました。そこで、情報が漏えいし、新聞沙汰になってしまいます。

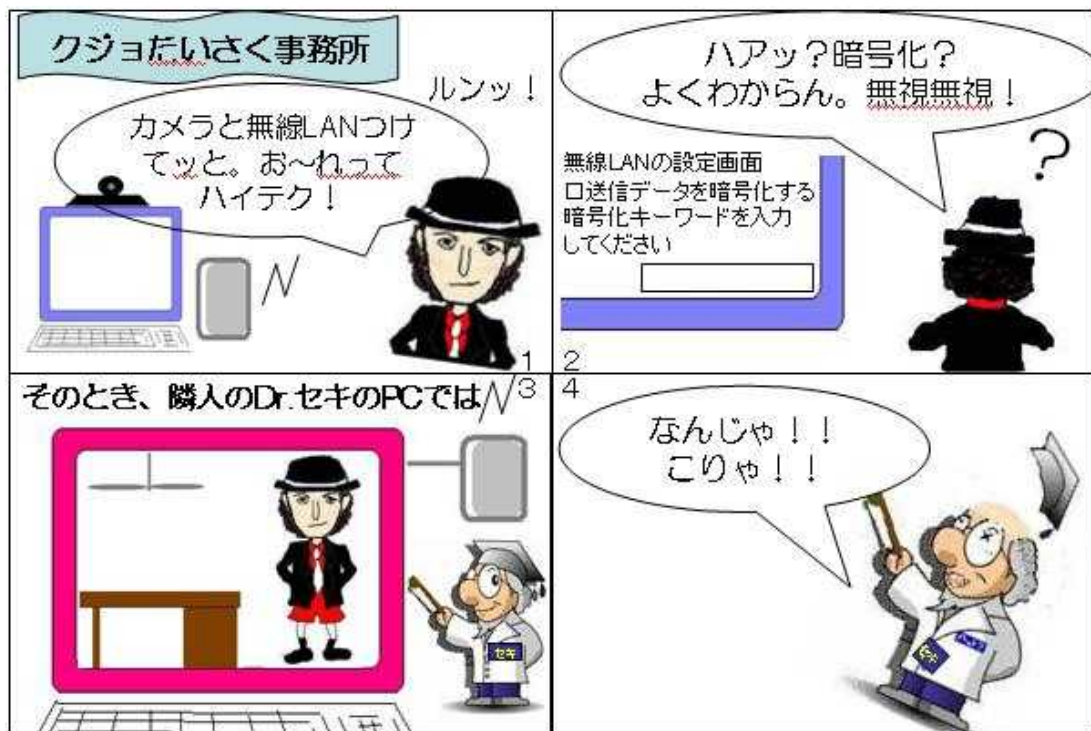
Winnyを介した情報漏えいでよくあるのは、職員が仕事を持ち帰るなどして、私物パソコンに業務用の機密情報などをコピーし、作業をしていたところ、そのパソコンにWinnyなどを導入しており、ウイルスに感染したり、誤操作により情報漏えいしてしまったというケースです。情報漏えいを起こしてしまうと、引き起こした当人も、その会社も、大きく信用を失墜させることになってしまいます。

ファイル交換ソフトを使う場合には、このような危険があることを十分に認識しましょう。また、ファイル交換ソフトを導入しているパソコンには、業務用のデータをコピーしないことです。一番確かなのは、このようなリスクのあるソフトウェアを使わないことです。そして、ウイルス対策もしっかり行ないましょう。もうひとつ大事なことは、著作権侵害を防ぐ配慮です。著作権のあるファイルは、公開用フォルダに置かないようにしましょう。



Winnyによる情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html

第8話 「無線 LAN でとなりに筒抜け」の巻



無線 LAN を使う時には暗号化すべし



無線 LAN は電波の届く範囲なら壁などの障害物を超えてどこでも通信が可能という便利さを備えています。しかし、その便利さとは裏腹に、悪意ある者から不正アクセスの対象として狙われ易い環境とも言えます。しかも、電波という、目に見えない通信経路を使うということは、侵入されていることさえも気づきにくいいため、大きな脅威となります。無線 LAN のセキュリティ設定を適切に行わないと、情報窃取、無断利用、通信データ盗聴等の被害に遭う可能性があり、とても危険です。

特に、セキュリティ設定の中でも、通信の途中で内容を見られたり改ざんされたりしないようにデータを変換処理する暗号化方式がポイントになります。この暗号化方式が強力でないと、短時間で通信内容が解読され盗聴されると同時に、認証が破られ、無断利用を許してしまいます。したがって、適切な暗号化方式を選択することが最も重要になります。

さて、クジョたいさく事務所では、最近、無線 LAN を導入しました。クジョ所長は、「俺って、ハイテク！」と粹がっていますが、暗号化の仕方がわからず、無線 LAN の暗号化機能を使っていません。そのため、隣人の Dr.セキのパソコンから、クジョ所長のパソコンのカメラがとらえた、ズボンをはいてない姿が丸見えます。無線 LAN を使う時には、次のような対策をきちんと行ないましょう。

対策その1 強力な暗号化方式を使う：

暗号化方式は、最もセキュリティ強度が高い WPA2-PSK という方式を選択します。その中から“AES 暗号を使う WPA2-PSK”という意味である「WPA2-PSK (AES)」という方式を選択することを推奨します。しかし、アクセスポイントによっては WPA2-PSK に対応していないものもあります。対応しているかどうか、自身で判断がつかない場合は取扱説明書を確認するか、メーカーへ間合わせてください。

WPA2-PSK に対応していない場合は、次善の策として WPA-PSK という方式を選択します。WPA-PSK には、AES 暗号を使う「WPA-PSK (AES)」と RC4 暗号を含んだ技術である TKIP を使う「WPA-PSK (TKIP)」と言う 2 種類の方式があり、通常はセキュリティ強度が高い「WPA-PSK (AES)」という方式を選択することを推奨します。接続できないなどの問題が生じた場合に限り、「WPA-PSK (TKIP)」を選択してください。しかし、WPA は WPA2 よりセキュリティ強度が劣りますので、あくまでも WPA2 対応機へ移行するまでの“つなぎ”としての役割であるという認識を持って使用して下さい。

WPA2-PSK と WPA-PSK に対応していない場合でも、内部ソフトウェアのアップデートにより WPA に対応できるものもあります。詳細については、メーカーのホームページなどで確認しましょう。WEP にはぜい弱性が見つかっていますので、WPA に対応できない場合は使用しないで下さい。

対策その2 推測されにくいパスワードを使用する:

WPA2-PSK や WPA-PSK では、無線 LAN の盗聴や無断利用を防ぐためのパスワードを設定します。WPS (以下、「設定の容易化について」を参照)を使用した場合は、パスワードは自動設定されます。パスワードを手動で入力する際は、容易に推測されることを防ぐため、以下の注意事項に従ってください。

- ・ 英語の辞書に載っている単語を使わない
- ・ 大文字、小文字、数字、記号の全てを含む文字列とする
- ・ 文字数は最低でも 20 文字(半角英数字+記号の場合。最大で 63 文字)

無線 LAN のセキュリティに関する注意 <http://www.ipa.go.jp/security/ciadr/20030228wirelesslan.html>

******* セキュリティ対策 まどめ *******
ここで、個人ユーザが留意すべき対策を項目別に整理してみましょう。

1. 基本的な対策

- ① OSやソフトウェアには、最新のパッチをあてる(ぜい弱性の解消)(第2話)
- ② ウイルス対策ソフトなどを導入し、定義ファイルを定期的に更新する。(第1話)
- ③ パーソナルファイアウォールを導入し、正しい設定と運用をする。
- ④ 適切なパスワードを設定し、定期的に変更する(第5話)
- ⑤ Webブラウザやメーラーの設定を適切に行なう。
- ⑥ 万が一のために必要なファイルのバックアップを取る。
(注:④⑤⑥については、あとで説明します。)

2. 基本的な心構え

- ① メール添付ファイルは安易に開かない。(第4話)
- ② 不審なWebサイトの閲覧を控える。(第3話)
- ③ ソフトウェアの安易なダウンロードやインストールを避ける(出所不明のソフトは使わない)。(第3話)
- ④ スпамメールなどの誘いのリンクはクリックしない。(第6話)
- ⑤ 個人情報を安易に入力しない。(第6話)
 - a. Webサイトなどで、ID・パスワードなどの重要な個人情報を入力する場合には、偽のWebサイトでないかどうか十分に注意してから行なう。
 - b. 自分で管理できないパソコン(インターネットカフェなど)では、重要な個人情報を入力しない。
- ⑥ 大事な情報を保存しているパソコンでファイル交換ソフトは使わない。(第7話)
- ⑦ 自宅で仕事をする場合、会社のセキュリティポリシーで禁じられている行為を慎む。(第7話)

3. 他人の権利を侵害しないための心構え

- ① 著作権について知り、著作権侵害をしないよう気をつける。
- ② 他人のプライバシーを侵害しないよう気をつける。
- ③ 他人の誹謗中傷をしない。

4. 無線LAN使用時のセキュリティ対策

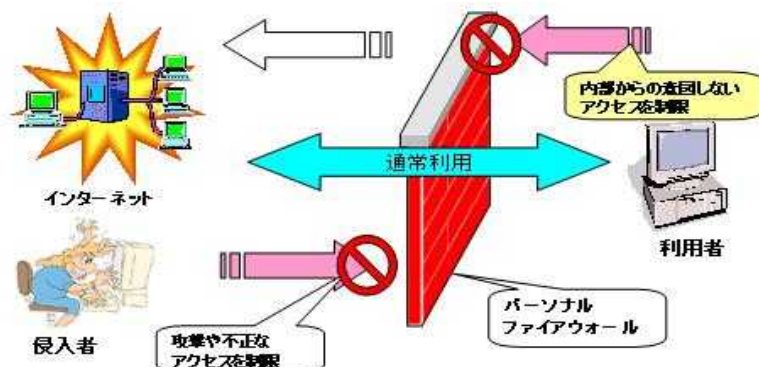
- ① 通信の途中で内容を見られたり改ざんされたりしないように、強力な暗号化方式による通信の暗号化を行なう。(第8話)
- ② パスワードを解読されて無線LANを不正に利用されないように、できるだけ推測されにくいパスワードを使用する。(第8話)

5. よりセキュリティを高めたい場合の対策

- ① インターネット上の被害や対策情報の情報収集を行い、新たな脅威にも対応できるようにする。

1.の基本的な対策を行い、2.の心構えに留意することで、ウイルス、ボット、スパイウェアなどの不正プログラム対策を行なうことができ、Web閲覧やメールの使用に伴う危険もほぼ回避できます。またインターネットを気持ちよく使うためには、お互いの権利やプライバシーを侵害しないように配慮する必要がありますので、3.の他人の権利を侵害しないための心構えも重要です。

最後に、4コマ漫画では伝えきれなかった、基本的対策の「パーソナルファイアウォールを導入し、正しい設定・運用をする。」「Webブラウザやメーラーの設定を適切に行なう。」「万が一のために必要なファイルのバックアップを取る。」がなぜ必要かについて少し説明しましょう。



ファイアウォールは正しく設定・運用すれば、ぜい弱性を悪用した不正プログラムの侵入に対して警告を表示し、侵入を防いでくれます。パソコンに侵入したスパイウェアやウイルスなどが情報を外部へ送信することを防ぐこともできます。ウイルス対策ソフトにパーソナルファイアウォールの機能があるときは、その機能をオンにします。

【Web ブラウザのセキュリティの設定】

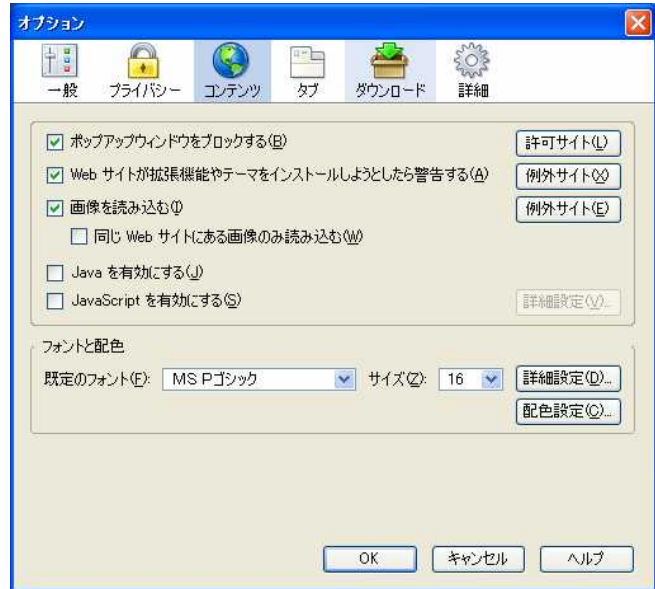
Web サイトでは、コンテンツの魅力を高めるために、JavaScript、ActiveX コントロールなどの技術が使われています。これらは Web サイトにさまざまな機能もたらし、利便性を向上させます。しかし、悪用される可能性もあります。Web ブラウザには、セキュリティレベルを設定する機能がありますので、この機能を使いセキュリティを高めます。

Internet Explorer の場合、[ツール]→[インターネットオプション]→[セキュリティ]または[詳細設定]

Firefox の場合、[ツール]→[オプション]→[コンテンツ] でこれらの設定を行います。

【Internet Explorer】

【Firefox】



【メーラーでのセキュリティの設定】

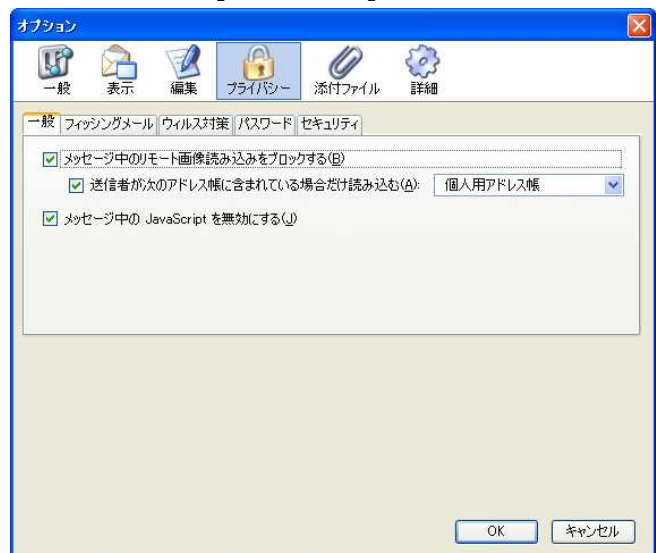
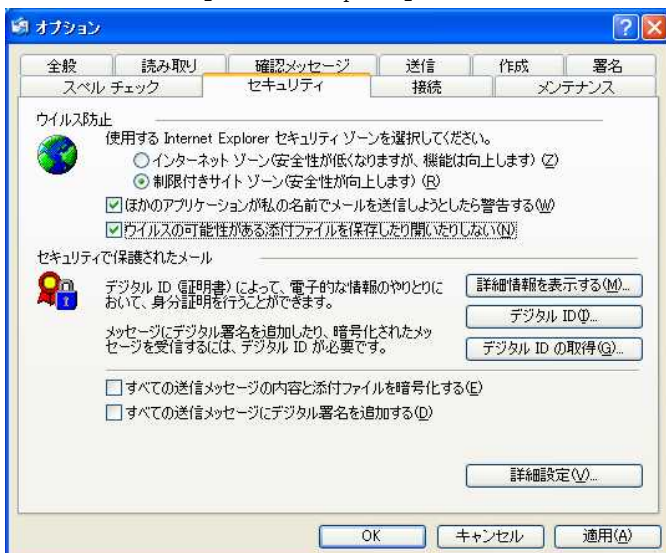
Outlook Express の場合、[ツール]→[オプション]→[セキュリティ]

Thunderbird の場合、[ツール]→[オプション]→[プライバシー] でこれらの設定を行います。

HTML メールにぜい弱性があると、そのぜい弱性を悪用して、メールをプレビューしただけで、ウイルスに感染することがあります。HTML メール機能はオフにしましょう。もちろん、ぜい弱性にパッチをあてることも必要です。

【Outlook Express】

【Thunderbird】



どんなに注意していても、ウイルス感染などにより、データを破壊されるなどの被害にあうことがあります。そこで、万が一のために、データは必ずバックアップを取っておく必要があります。

インターネット上にはどのような脅威があり、なぜこのような対策が必要かということを知って、適切な対策を行なうことで、インターネットを快適に楽しく使しましょう。

***** 終わり *****