インターネット
利用者のための
経済産業省
JNSA
セキュリティ
対策講座

これだけは知っておきたい!

インターネット安全教室

～パソコンや携帯電話で思わぬトラブルや犯罪にまきこまれないために～

経済産業省
NPO 日本ネットワークセキュリティ協会

「インターネット安全教室」CD-ROM for Windows / Macintosh

ご注意
このCD-ROMを音楽用のCDプレーヤーで再生しないでください。
聴覚の障害や、機器の故障などの原因となる場合があります。

ご利用方法

このCD-ROMには、冊子の内容を映像で紹介する「ムービー」と、クイズ形式で楽しく学べる「クイズ学習」が収録されています。お使いになっているOSによって下記のように操作します。
※「クイズ学習」を再生するにはブラウザ(閲覧ソフト)と最新のMacromedia Flash Player(Macromedia社のホームページから無償でダウンロードできます)が必要です。

Windows

① CD-ROMドライブにこのCD-ROMをセットすると、「インターネット安全教室」のメニューが出てきます。
② 「ムービーを見る」または「クイズ学習に挑戦」をクリックします。
※もし、自動的にメニューが出てこない場合は、次のようにします。
① デスクトップ上の[マイコンピュータ]をダブルクリックします。
② CD-ROMのアイコンをダブルクリックします。
③ Menuのアイコンをダブルクリックします。
④ 「ムービーを見る」または「クイズ学習に挑戦」をクリックします。

※Windows XP SP2環境などでお使いの場合、「情報バーにお気づきですか？」という警告が表示されることがあります。このコンテンツは安全に製作されていますので、表示された場合は、警告画面の「OK」をクリックして、「情報バー」の「ブロックされているコンテンツを許可」を選択してください。

Macintosh

CD-ROMドライブにこのCD-ROMをセットすると、
「インターネット安全教室」のCD-ROMアイコンがあらわれます。
① CD-ROMのアイコンをダブルクリックします。
② 「MOVIE.mpg」のアイコンまたは「クイズ学習スタート」のアイコンをダブルクリックします。

必要なシステム構成
Windows
対応機種:Pentium 120MHz以上のプロセッサ
対応OS:Windows 98、Windows 2000、Windows XP
必要メモリ:32MB以上

Macintosh
対応機種:PowerPC搭載のMacintoshコンピュータ
対応OS:Mac OS X 10.1.3以上
必要メモリ:32MB以上

この冊子およびCD-ROMご利用にあたっての注意事項

はじめに

今日、パソコンやインターネットは社会の至る所に浸透し、もはや私たちの生活になくてはならないものとなってきました。これらは、私たちの生活をいっそう豊かにする可能性をもっていますが、同時に個人情報漏えいや、不正アクセスによる被害、コンピュータウイルス感染等の危険に直面する可能性ももっています。

最近では、個人情報の漏えい事件や、「フィッシング」と呼ばれる新たな詐欺の手口が新聞やテレビを賑わせていますが、こうした問題は決して他人事ではありません。

インターネットは大変便利な道具ですが、使い方によっては、他人に被害を与えてしまったり、様々なトラブルに巻き込まれてしまったりする可能性があることから、皆が安全・快適にインターネットを活用するには、一人一人が自覚をもって適切な情報セキュリティ対策を講じるとともに、インターネットにおけるルールやマナーを身につけることが極めて重要です。

経済産業省は、特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）と協力し、2003年度より情報セキュリティ分野での普及啓発活動の一環として、全国各地で「インターネット安全教室」を開催しております。本セミナーは、家庭や学校からインターネットにアクセスする方々を対象に、安全・快適にインターネットを利用するために必要な情報セキュリティに関する基礎知識を学習する機会を提供するものです。本セミナーは、各地でインターネットの普及や情報セキュリティ対策の啓発に携わる方々や、警察庁、都道府県警察等の御協力を頂き、これまでに全国30カ所以上で開催され、延べ6500人以上の方々が受講されました。今後はこの活動を全国に広げ、それぞれの地域の方々が主体となって自らのコミュニティを守っていく活動として根付いていくことを望んでいます。

インターネットは、使い方を間違わなければ楽しく便利なものです。皆様がこの冊子とCD-ROMを活用して頂くことで、インターネットを利用する際のルールや情報セキュリティに関する理解が深まり、ひいては一人一人が気持ちよくパソコンやインターネットを利用できる社会が作られていくことを、私たちは心から願っています。

経済産業省
NPO 日本ネットワークセキュリティ協会

目 次

ご注意
この冊子は、一般的な対策について記載しています。対策内容は状況によって異なる場合があります。巻末の「情報セキュリティ関連のホームページ」などを参考に、状況に応じた対策を確認しましょう。

1. フィッシング詐欺にご用心！

突然、金融機関やショッピングサイトを名乗るところからメールが送られてきて、あなたの重要な個人情報を聞き出そうとする内容だったらご用心。「フィッシング詐欺」にねらわれている可能性があります。本物そっくりな「ニセのメール」を送りつけ、本物そっくりな「ニセのサイト」に誘導する。そして、口座番号や暗証番号、クレジットカード番号、ID、パスワードなど重要な個人情報を入力させ、大切な財産をうばいとる、または犯罪に利用する。それが「フィッシング詐欺」なのです。相手が誰であれ、あなたの重要な個人情報を聞き出そうとする内容のメールが届いたら、まずあやしいと疑ってかかりましょう。

フィッシング詐欺の手口

本物そっくりなメールやサイトでだます「フィッシング詐欺」

「フィッシング」は、英語では「phishing」と書きますが、発音は「釣り」を意味する「fishing」と同じです。詐欺の手法が、疑似餌（ルアー）を使った「釣り」に似ていて、しかもその疑似餌（すなわちメールやサイト）が本物と見分けがつかないほど洗練（sophisticated）されていることから、「f」を「ph」に替えて「phishing」となったといわれています。

「フィッシング詐欺」は、オンラインバンキングやオンラインショッピングがすすんでいる米国を中心に2003年ごろから急速に増えはじめ、被害総額は年間数億ドル（数百億円）とも数十億ドル（数千億円）ともいわれています。日本でも「フィッシング詐欺」が発生し始めており、被害の拡大が懸念されています。

「フィッシング詐欺」対策はどうしたらいいか？

●「フィッシング詐欺」がねらう個人情報の代表的な例は以下のようなものです。
- **金融情報（口座番号、暗証番号、クレジットカード番号、有効期限など）**
- **住所、氏名、電話番号**
- **ID、パスワード（電子メール、オークション、会員サービスなど）**

重要な個人情報を聞き出そうとするメールが届いたら、まずあやしいと疑ってかかりましょう。

●「フィッシング詐欺」が送りつけてくるメールは、文面はもちろんのこと、送信者のメールアドレスですら、本物そっくりのニセモノです。とりわけ「○○○の更新手続きを下記○○○のサイトで行ってください」といったような文面とともに、アドレスをクリックさせてニセのサイトへ誘導する手口にひっかかってはいけません。心当たりのないアドレスはクリックしないようにしましょう。金融機関（銀行・保険・カード会社など）がメールで口座番号や暗証番号など個人情報を問い合わせることはありません。そうしたことを尋ねるメールは「フィッシング詐欺」です。

●メールやサイトの真偽を確かめるには、次のような方法があります。
- **キャッシュカードやクレジットカードに記された問合せ先に電話で確認をします。**
- **Webブラウザのアドレス入力欄に正しいアドレスを入力するか、検索サイトで検索するなどして本物のサイトにアクセスします。そして、そこに記されたサポート窓口に電話をかけたり、メールを送るなどして問合せをします。**

●「フィッシング詐欺」に関する情報は、フィッシング対策協議会のホームページをご覧下さい。
http://www.antiphishing.jp/

●「フィッシング詐欺」にひっかかってしまったかもしれないというときには、次のような解決策があります。
- **警察庁や国民生活センターのホームページで対処法を確認します。**
- **銀行やクレジット会社、ショッピングサイトなどに連絡をして相談をします。**
- **契約しているプロバイダやオークション、会員サービスの会社に連絡をして、ID、パスワードの変更手続きをします。**
- **上記でも解決できない場合には最寄りの警察に相談しましょう。**

POINT 1

ニセのメールを送りつけるなどして、クレジットカード番号や暗証番号などを盗みとるフィッシング詐欺にご用心。「あやしい」と思ったら、正式な連絡先に問い合わせましょう。

2. 無線LANの安全な使い方

最近、オフィスのみならず家庭でも無線LANを導入するケースが増えています。無線LANは、ネットワークケーブルを敷く必要がなく、どの部屋にパソコンを持ち込んでもすぐにワイヤレスでネットワークに接続できるので大変便利です。街中にも、誰でも自由に無線LANを使ってインターネットにアクセスできる場所が増えてきました。ところが、こうして便利なだけに、ちょっとした不注意で悪意の第三者に不正に侵入されるスキを与えてしまうことをご存じでしょうか？　無線LANを使うときには、利用者パスワードなどセキュリティの設定をきちんとして、外部からの不正な侵入を防ぎ、安全に使いましょう。

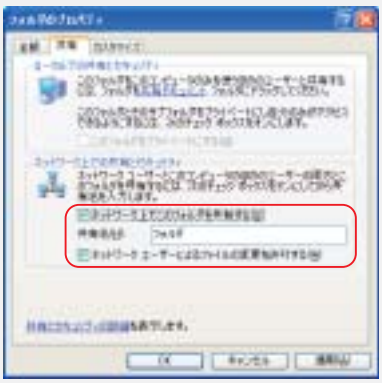
セキュリティの設定をしましょう

利用者パスワードなどセキュリティの設定をしましょう

●ネットワークに接続したパソコンは、無防備なままでいると不正に侵入される危険があるので注意しましょう（**P.18 Q&A参照**）。ネットワークケーブルを使って有線で接続している場合は、実際にネットワークケーブルをつながなければ不正に侵入されることはありません。しかし、無線LANの場合は、電波のとどく範囲にあるパソコンは、誰が使っているパソコンであっても、いつでも接続できるようになっています。このため、無線LANを使う場合は、利用者パスワードなどセキュリティの設定をして、より安全な環境で使うようにしましょう。
●節電のためにも、使用しないときはパソコンの電源を落とすようにしましょう。

ファイル共有は利用するときだけONにしましょう

●ファイル共有は、ネットワーク上の複数のパソコンでファイルをやりとりする際に使います。それ以外のときには、基本的にファイル共有をOFFにしておきます。
●ファイル共有の設定はフォルダごとに行うことができます。とりわけ重要な書類の入ったフォルダは必ずファイル共有設定をOFFにしておきます。ONにしたままネットワークに接続すると、共有設定したフォルダ内のすべてのファイルの中身を見られてしまいます。



Windows XPの場合（ファイル共有のON、OFFについて）

フォルダのファイル共有設定を確認するには、フォルダを選択して右クリックし、［共有とセキュリティ...］、［共有］を選択します。

［ネットワーク上でこのフォルダを共有する］のチェックボックスがONになっているとともに、［ネットワークユーザーによるファイルの変更を許可する］もONになっています。このままでは不正侵入した悪意の第三者に、勝手にファイルを変更されてしまう危険性があります。

このように［ネットワーク上でこのフォルダを共有する］のチェックボックスがOFFになっていれば、悪意の第三者にフォルダ内のファイルの中身を見られることはありません。

POINT 2

無線LANを使うときは、必ずセキュリティの設定をして、外部からの不正な侵入を防ぎましょう。

3. ウイルス対策は万全に

ウイルス対策は万全でしょうか？　もし、対策をおこたっていると、あなたのパソコンがウイルスに感染してしまい、ファイルを次々と消されてしまったり、パソコンを起動できなくなってしまうなど大変なことになります。そればかりではありません。ウイルスによっては、あなたがアドレス帳に登録した相手にウイルス感染メールを勝手に送りつけ、あなた自身が加害者になってしまうこともあるのです。ウイルス対策ソフトをインストールし、自動更新の設定になっていることを確認します。なお、使用期限を過ぎたウイルス対策ソフトは、すみやかに更新しましょう。

ウイルス対策はどうしたらいいか？

ウイルスの感染経路の約9割は、メールの添付ファイルといわれています。ただし、その他にもホームページからダウンロードしたファイルや、フロッピーディスクやCD-Rなどのメディアにあるファイルなど、さまざまな感染経路があるので、ウイルス対策をしないままパソコンを使うのは大変危険です。

このような準備をします

- ●パソコンにウイルス対策ソフトをインストールします（あらかじめインストールされている場合もあります）。
- ●最近のウイルス対策ソフトは、はじめからインターネットを通じて最新のウイルス情報が得られるように自動更新する設定になっていますが、そうでない場合もあるので、念のため自動更新の設定になっているかどうか確認します。
- ●ウイルス対策ソフトは、使用期限が切れる前に更新するようにしましょう。
- ●メールソフトは、プレビューやHTMLメールを自動的に表示しないような設定にしておきます**（P.19 Q&A参照）**。

日ごろの心がけ

- ●見知らぬ相手から届いたメールの添付ファイルは、ウイルスである可能性が高いので、添付ファイルを開かないままメールごと捨てます。
- ●知人から届いたメールでも、心当たりのない添付ファイルがある場合は、送信元に添付ファイルを送ったかどうか確認するとともに、添付ファイルを開く場合は、必ずウイルスチェックを行ってからにします。
- ●ホームページからダウンロードしたファイルなど、新たに自分のパソコンに取り込んだファイルは、開く前に必ずウイルスチェックを行います。
- ●OSやWebブラウザなどのセキュリティホール（弱点）を攻撃するウイルスもあります。セキュリティ更新プログラムをメーカーのホームページから入手して実行し、最新の状態に更新（アップデート）しておきます。
- ●万一ウイルスに感染しても被害を最小限にとどめられるように、普段からこまめにデータのバックアップをしておきます。また、パソコンが起動しなくなった場合に備え、起動用のディスクを用意しておきます。

もし、感染してしまったら...

- ●ネットワークケーブルを外すなどして、インターネットから切り離します。そして、ウイルス対策ソフトを使って、パソコンからすみやかにウイルスを駆除します。
- ●ウイルス定義ファイルの更新方法や、ウイルス対策ソフトでは駆除できないタイプのウイルスの駆除方法など、不明な点については、お使いのウイルス対策ソフトのベンダー（販売会社）にお問い合わせください。

POINT 3

ウイルス対策ソフトは使用期限切れに注意しましょう。新種のウイルスに対応できるように自動更新の設定も忘れずに。

4. あわてないで！脅しメール

メールは簡単に送れて大変便利ですが、それだけに犯罪や悪質ないたずらの格好の手段にもなります。実際に利用した事実がない料金請求をする「架空請求」や、メールの中のリンク（アドレス）を一度クリックしただけで「入会手続きが完了しました」などといって料金をだましとる「ワンクリック請求」。突然、そうした脅しのメールが送られてくることがあります。でも、あわてないでください。相手をパニック状態にして冷静に考えるスキを与えないのが彼らの手口。いかがわしいサイトや悪質な出会い系サイトへしつこく勧誘する「迷惑メール」も非常に危険です。そうした悪質なメールは無視しましょう。

脅しメールの手口

実際に利用していない利用料金を請求する「架空請求」

実際に利用した事実がないにもかかわらず、有料サイトを利用したかのような内容のメールを送りつけ、利用料金を請求するのが、「架空請求」メールです。

「架空請求」メールの代表例

- **「あなたのご利用のサイトで利用料金が未納となっております。至急、ご連絡ください。」**
- **「最終通告　この度、貴殿が使用されたプロバイダおよび電話回線から接続されたアダルトサイト利用料金について運営業者より未納料金に関する債権譲渡を受けました。」**

一度のクリックで利用料金を請求する「ワンクリック請求」

送られてきたメールの中のリンク（アドレス）を一度クリックしただけで、「会員登録が完了しました」などというメッセージとともに不当な利用料金を請求するのが「ワンクリック請求」（いわゆる「ワンクリック詐欺」）です。

- 「ワンクリック請求」の大半を占めるのは、アダルトサイトや悪質な出会い系サイトへの勧誘メールです。
- メールの中のアドレスは、どのアドレスをクリックしても会員登録をしたことになるように仕組まれています。どのアドレスもクリックしないようにしましょう。
- 恐怖心をあおる目的で、「あなたの携帯電話の機種名は、○○○○、個体識別番号は、××××、あなたの位置情報は、東京都○○○」「あなたの接続プロバイダは、○○○○、IPアドレスは、00.00.00.00」などの表示をするケースがよくあります。それらの情報は、実際にはあなたを特定できる情報ではありません。
- あらかじめ名簿を見ていたり、友人を装ったメールを送って返信させるなどして、メールアドレスや携帯電話の電話番号を知っているケースもあります。実際に電話をかけてくることがない限り、無視し続けるのが得策です。

悪質なメールの撃退法は？

- 返信をしたり、連絡をしないようにしましょう。「配信停止は○○○まで」というメールアドレスに返信しても、配信停止にならないばかりか、あなたのメールアドレスが有効であることを相手に知らせることになって、かえって新たなトラブルに巻き込まれる可能性があります。
- メールソフトの受信拒否者の設定を用いたり、プロバイダに連絡して受信拒否をする方法もあります。
- 詳しくは、警察や国民生活センターのホームページを確認しましょう**（P.22参照）**。
- 電話がかかってくるなど、犯罪に巻き込まれる危険性がある場合は、最寄りの警察に相談をしましょう。

POINT 4

メールを使った脅しや不当な請求には落ち着いて対処しましょう。警察や国民生活センターのホームページをチェックし、対処法を確認しましょう。

5. オークション詐欺にだまされない

インターネットショッピングを活用すれば、自宅にいながらいろいろな買い物を楽しめます。また、インターネットオークションには、掘り出し物を破格の値段で購入できたり、自分のものを予想外の高値で販売できたりといった、ショッピングとはひと味違っただいご味があります。とはいえインターネットの向こう側にいるのは、善意の人ばかりではありません。お金を振り込んだのに、品物は送られてこない、電話番号も住所も名前も架空のものだった、という詐欺にあうケースも発生しています。インターネットで取引をする際には、本当に信頼できる相手かどうか、よく確かめて対応することが大切です。

信頼できる相手かどうかよく確かめる

ショッピングやオークションをするときの注意点

ショッピングをするときには…

●インターネットショッピングは便利な反面、相手の顔が見えないだけに、常に詐欺などの被害にあう危険と隣り合わせだということを忘れないようにしましょう。
●会社名・代表者名・所在地・電話番号など会社の基本情報や、取り引き条件などの情報がきちんと書かれていないホームページは要注意です。
●クレジットカード番号など重要な個人情報を送信する場合は、暗号化や電子認証などによって個人情報がしっかり保護されているかどうかを確認します。
●万が一のトラブルに備え、注文したときの条件や、注文の確認メールなどを印刷しておくとともに、領収書など取り引きを証明する書類はしばらくの間保管しておきます。

オークションに参加するときには…

●オークションサイトは取り引きの仲介をするだけで、落札した後のやりとりは、出品者と購入者の間で、お互いの自己責任で行うことになります。
●オークションサイトの中には、出品者ごとに過去にその出品者から購入したことのある人が書いた取引評価が掲載されており、出品者が信頼できるかどうかを判断するひとつの判断材料になります。
●落札したら、実際に取引をする前に、電話をするなどして相手の連絡先と住所を確認します。所在が確かでないなど少しでも不安を感じる場合は、取り引きを控えたほうがいいでしょう。
●トラブルを避けるため、配送中の事故で商品が破損したり紛失した場合はどうするか、商品が到着した後になんらかの欠陥が見つかった場合はどうするか、返品・返金はどうするかといった点について、あらかじめよく話し合い、取り決めをしておきます。
●銀行振込、現金書留、郵便為替などで支払う方法が一般的ですが、代金を振り込んだのに商品が送られてこない、商品を送ったのに代金が振り込まれないというような危険があるので注意しましょう。代引サービスや、エスクロウ・サービス（出品者と購入者の間のやりとりを仲介し、安全確実な取り引きができるようにするサービス）を利用する方法もあるので、必要に応じて活用してください。

詐欺行為にあったときにはどうしたらいいか？

●クレジット会社から身に覚えのない利用代金の引き落とし通知が来た場合は、すぐにクレジット会社に連絡して、引き落としを止めるなど被害を最小限にとどめる手続きをします。
●証拠となるホームページを印刷するなどした上で、最寄りの警察に相談をしましょう。

POINT 5

ショッピングやオークションを利用するときには、安全確実な取引ができるサービスを利用するなどして、トラブルを避けるようにしましょう。

6. ブログやホームページの注意点

誰でも簡単にブログやホームページを公開できる時代になりました。とりわけ最近では、日記形式で簡単に思ったことを記入したり、写真や音声、映像を掲載できるブログがブームとなっています。個人のブログやホームページであっても、世界中に情報発信をすることができます。とはいえ、不特定多数の人に情報を公開する以上、勝手気ままにどのような情報を公開してもいいというわけにはいきません。著作権を侵害しない、誹謗中傷をしない、公序良俗に反しないなどといったように、社会のルールをきちんと守るとともに、自分や家族、友人のプライバシーを守ることも忘れないようにしましょう。

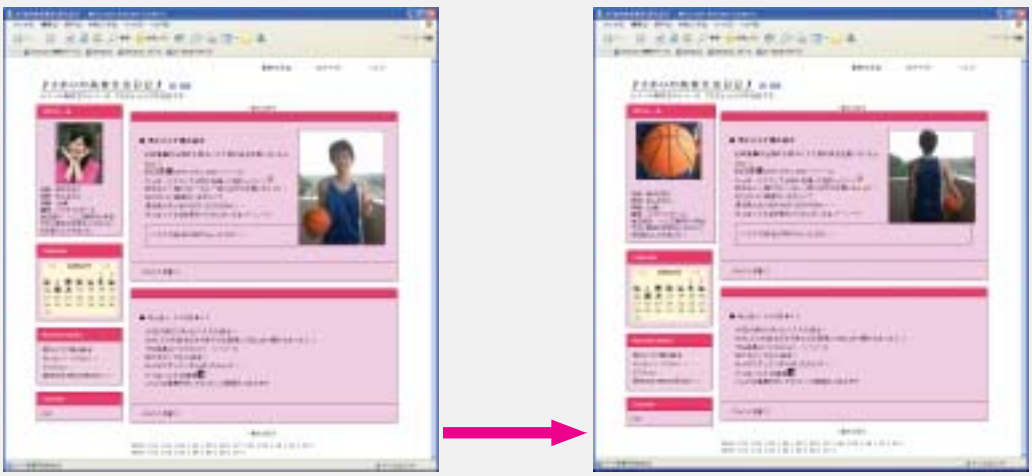
社会のルールやプライバシーを守りましょう

ルールやマナーを守りましょう

●文章や写真、イラスト、音楽、映像などには、それを制作した人に著作権があります。著作権者に無断でそのまま、あるいは一部を改変してホームページで使用することは、著作権の侵害や肖像権の侵害となります。文章は出典を明らかにした上で引用し、写真、イラスト、音楽、映像は著作権フリーの素材を用いましょう。たとえ自分で描いたイラストでも、有名なキャラクターにそっくりというような場合は、そのキャラクターの著作権者から訴えられることがあります。
●ホームページ上で誹謗中傷したり、他人の情報や写真などを本人の許可なく公開してはいけません。名誉毀損やプライバシーの侵害などで訴えられることがあります。
●わいせつな画像を掲載するなど公序良俗に反する行為、法律に違反する行為をしてはいけません。

プライバシーを守りましょう

●自分や家族、友人などの情報（特に住所や電話番号、勤務先名や通学している学校名、写真など）の掲載は、できるだけしないほうがいいでしょう。犯罪に巻き込まれる危険性があります。
●メールアドレスの掲載も、できるだけしないほうがいいでしょう。ウイルス感染メールや悪質なメールが送られてくる原因となることがあります。もし、メールアドレスを掲載する場合は、なにか問題があったときにすぐに変更できるメールアドレスを使う方法もあります。



POINT 6

ブログやホームページでは、個人情報の扱いに注意し、マナー違反や著作権侵害をしないようにしましょう。

7. まとめ

インターネットはパソコンという「モノ」と向き合っているようですが、実は世界の「人」とつながっているのです。はりめぐらされたネットを活用して、情報や物品、そして金銭を流通させることができる画期的な手段だけに、利用する際には、さまざまな注意を払い、マナーを守ることが必要です。この「インターネット安全教室」では、インターネットを安全快適に活用するにはどうしたらいいか、被害にあったときにはどうしたらいいかといった情報セキュリティに関する基礎知識を6つのポイントにまとめました。こうしたポイントに注意しながら、インターネットを毎日の暮らしに役立てて下さい。

インターネットファミリー！レッツゴー！

1
ニセのメールを送りつけるなどして、クレジットカード番号や暗証番号などを盗みとるフィッシング詐欺にご用心。「あやしい」と思ったら、正式な連絡先に問い合わせましょう。

2
無線LANを使うときは、必ずセキュリティの設定をして、外部からの不正な侵入を防ぎましょう。

3
ウイルス対策ソフトは使用期限切れに注意しましょう。新種のウイルスに対応できるように自動更新の設定も忘れずに。

4
メールを使った脅しや不当な請求には落ち着いて対処しましょう。警察や国民生活センターのホームページをチェックし、対処法を確認しましょう。

5
ショッピングやオークションを利用するときには、安全確実な取引ができるサービスを利用するなどして、トラブルを避けるようにしましょう。

6
ブログやホームページでは、個人情報の扱いに注意し、マナー違反や著作権侵害をしないようにしましょう。

ユーザーIDとパスワードの管理について

ユーザーIDとパスワードの管理は非常に重要です。もし、他人にユーザーIDとパスワードを知られてしまうと、購入履歴や住所、電話番号などの個人情報を知られてしまうばかりか、勝手に買い物をされてしまうなどさまざまな危険性があります。ユーザーIDとパスワードは、絶対に他人に知られないように注意しましょう。

- ●ユーザーIDとパスワードをメモする場合には、そのメモなどが他人に盗み見られないように注意しましょう。
- ●ユーザーIDと同じパスワードや、自分や自分に関係する人の名前、電話番号、誕生日など類推されやすいパスワードを設定しないようにします。
- ●辞書に載っている単語をそのまま使わないようにします。また、「word123」や「secure01」など、辞書単語＋数字、数字＋辞書単語の単純な組み合わせも避けます。
- ●できるだけ他で使っているパスワードをそのまま使わないようにします。
- ●長いパスワード（できれば8文字以上）を設定します。
- ●同じ文字種の単純な組み合わせ（数字のみ、英大文字のみ、英小文字のみ）ではなく、数字や記号、英大文字、英小文字を複雑に組み合わせ、類推されにくいパスワードにします。
- ●電話や電子メールでユーザーIDやパスワードを聞き出す手口にひっかからないようにしましょう。一般的に、電話や電子メールであなたにパスワードを聞くことはありません。万が一、聞かれた場合には、そのまま答えるのではなく、こちらから電話をかけ直すなどして、相手の身元を確認するといいでしょう。
- ●パスワードは、できるだけ定期的に変更するようにします。
- ●パスワードを盗まれた恐れがある場合や、不審に思うことがある場合は、パスワードをすぐに変更するとともに、運営会社に連絡をします。

未成年のための有害なサイト対策について

インターネットの世界には、子どもたちにとって有害なサイトが数多く存在しています。犯罪や暴力、わいせつ、薬物、悪質な出会い系サイトなど、数え上げればきりがありません。こうした有害なサイトから子どもたちを守るには、有害なサイトへのアクセスを自動的に禁止するフィルタリングソフトや、プロバイダのフィルタリング・サービスを活用するといいでしょう。子ども向けに作られた検索サイトを起点に利用させる方法もあります。ただし、いくらそのような形で防御しても、インターネットの危険性について子どもたちがしっかりと理解していなければ、役に立ちません。この「インターネット安全教室」で学んだことについて、親子でよく話し合ってください。

8. Q & A

Q 不正侵入を防ぐにはどうしたらいいですか？（P.7）

A Windows XPの場合、ウイルスや不正アクセスにさらされないように、次の3つを設定します（Windowsのバージョンによって設定はやや異なりますが、基本的には同じです）。

(1)ウイルス対策ソフトを最新の状態に保つ設定にする

ウイルス対策ソフトをインストールし、ウイルス検出用ファイルを最新の状態に保つ設定にします。ウイルス対策ソフトについては、たとえばIPA（独立行政法人情報処理推進機構）セキュリティセンターのウイルス情報などをご覧下さい。

●IPAセキュリティセンター
http://www.ipa.go.jp/security/

(2)Windows Update（ウィンドウズアップデート）を自動更新するように設定する

［コントロールパネル］で［システム］を選択します。［システムのプロパティ］の［自動更新］を選択して、［自動（推奨）］のチェックボックスをONにします。

(3)ファイアウォールを設定する

［コントロールパネル］で［ネットワーク接続］の種類（［ローカルエリア接続］、［ワイヤレスネットワーク接続］、［ダイヤルアップ接続］）を選択します。［右クリック］で［プロパティ］を選択し、［詳細設定］を選択します。そして、［Windows ファイアウォール］の［インターネットからこのコンピュータへのアクセスを制限したり防いだりして、コンピュータとネットワークを保護する］の［設定］をクリックします。左の画面が表示されるので、［有効（推奨）］のチェックボックスをONにします。ファイアウォールの設定は、［ネットワーク接続］の種類ごとに行います。

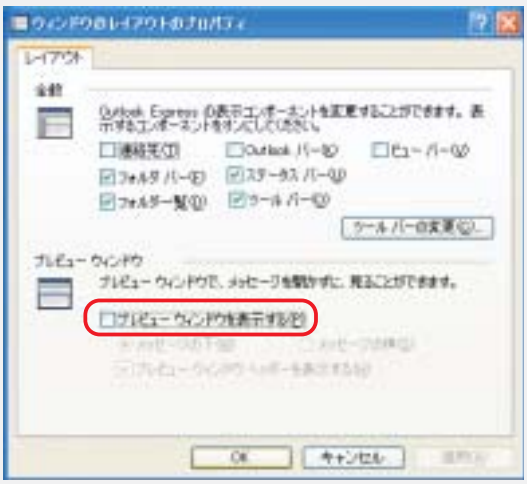
注意：ネットワーク接続のプリンタやいくつかのアプリケーションによっては、この設定をすると正しく動作しなくなる場合があります。その場合は、それぞれの製品の説明書に従ってください。

Q メールソフトでプレビューやHTMLメールを自動的に表示しないようにするにはどうしたらいいですか？（P.9）

A Outlook ExpressやOutlookなどのメールソフトでは、初期設定でプレビューウィンドウの表示やHTML表示(※)が設定されています。そのほうが便利だからなのですが、ウイルスに感染したり、迷惑メールを増やす原因になりやすいため、自動的に開かないように設定したほうがいいでしょう。

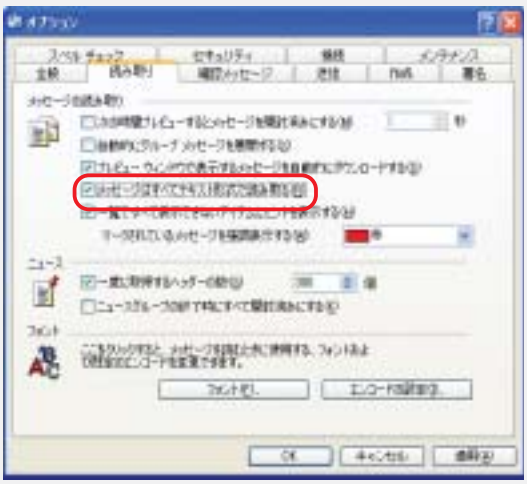
※ホームページと同じように、文字に色づけしたり、文字のサイズを変えたり、画像や表やアドレスを入れたりできるメール表示のこと

●Outlook Expressの場合



プレビューウィンドウを表示しないようにする（メールを自動で開かないようにする）

メールを自動で開かないようにするには、プレビューウィンドウを表示しないようにします。まず、[表示] メニューから [レイアウト] を選択します。次に [プレビューウィンドウ] の項目で [プレビューウィンドウを表示する] のチェックボックスをクリックしてOFFにします。



HTML表示を行わないようにする

HTMLメールを安全に表示するには、まず、[ツール] メニューから [オプション] を選択します。次に [読み取り] の項目で [メッセージはすべてテキスト形式で読み取る] のチェックボックスをクリックしてONにします。

Q スパイウェアとはどういうものですか？

A スパイウェアとは、本人が気づかないうちに勝手にパソコンに入り込み、パソコン操作の履歴や個人情報を盗み出すソフトウェアのことです。盗み出す具体的な情報には、どのサイトを訪れたか、どのようなプログラムをインストールしているか、メールアドレスはなにか、どのようなID、パスワードを入力したかなどがあります。

アダルトサイトなどには、スパイウェアが仕込まれていることが多いので注意しましょう。そうしたサイトを表示したとたん、突然ダウンロードが始まり、新たに意味不明のファイルが存在するようになったというような場合は、そのまま放置しておくと、重要な個人情報を盗まれたり、勝手に有料サイトに登録されて、利用した事実のない利用料金を請求されたりといった事件に巻き込まれる危険性があります。

インターネットカフェや駅、空港、図書館など公共施設にあるパソコンにスパイウェアが仕込まれているケースもあります。そうしたパソコンでメールの送受信をしたために、メールアドレスとパスワードを盗まれ、迷惑メールに悪用されるという事件や、オークションサイトのID、パスワードを盗まれ、オークション詐欺に悪用されたという事件が発生しています。また、オンラインバンキングやショッピングをしたために、口座番号、暗証番号、クレジットカード番号、有効期限など重要な個人情報を盗まれ、金銭的な被害を被ったという事件も発生しています。不特定多数の人が利用するパソコンでは、メールを送受信したり、重要な個人情報を入力しないほうが安全です。

スパイウェアは、ウイルスと構造が異なるため、ウイルス対策ソフトで検出して駆除できるものもありますが、対応できないものもあります。ウイルス対策ソフトを使用していてもあやしいと感じるような場合には、専用のスパイウェア対策ソフトを利用するか専門家に相談するといいでしょう。

キーボードの入力を盗むキーロガーというソフトウェアや、無料で使える代わりにポップアップの広告を表示したり、スポンサーのためにマーケティングデータを採取する目的で開発されたアドウェアというソフトウェアもスパイウェアの仲間です。これら、ウイルス、スパイウェア、アドウェア、キーロガーなど悪意のあるソフトウェア全体のことをマルウェア（Malicious Softwaerの略）といいます。

Q 掲示板やチャットで相手を傷つけないようにするにはどうしたらいいですか？

A よく「車のハンドルを握ると人格が変わる」という言い方をしますが、インターネットも時として人間の人格を変えてしまうほどの大きなパワーを備えています。このため、掲示板やチャットで人と会話をするときにも、このパワーの存在を知っておく必要があります。楽しい会話はより楽しい方向へパワーアップされるのでいいのですが、その反面、不愉快な会話はますます不愉快な方向へパワーアップされてしまうのです。面と向かって言い合うのであれば、よくある軽口にすぎない一言でも、掲示板やチャットで文字として書かれ、それが多くの人の目に触れるとなると、相手を耐えがたいほど深く傷つけてしまうことがあります。

このため掲示板やチャットに参加する場合には、いつにもましてマナーを守ること、そして、ていねいな言葉使いを心がけることが非常に大切になってきます。

車の運転の場合には、免許をとる際に、交通マナーを守ること、ていねいな運転を心がけることの大切さを教えられますが、掲示板やチャットに参加する場合には、なかなかそういう機会がありません。掲示板やチャットで相手を傷つけたり、自分が傷つかないようにするには、あらかじめ掲示板やチャットの魅力と危険性について、きちんと学習することが大切といえるでしょう。

Q 悪質なメールによる被害にはどのようなものがありますか？（P.11）

A

●架空請求メール

最近、とくに被害が増えているのは、「架空請求」メール詐欺です。実際に利用している利用していないにかかわらず、アダルトサイトなどの利用料を請求するメールを送りつけ、だまして金銭を振り込ませる詐欺の手口です。身に覚えのない（現実に利用していない）利用料金の請求については、送信してきた先に問い合わせたり、金銭を振り込むなどしないように注意して下さい。問い合わせをすると、相手側にこちらの情報を与えてしまい、その結果、恐喝されたり、その後何回も同様の架空請求を受ける場合があります。金銭を支払ってしまったなど被害を受けた場合は警察に相談して下さい。

いわゆる出会い系サイトの広告やわいせつな画像があるページへのリンク（アドレス）を掲載したメールを送りつけ、リンク先にアクセスしただけで閲覧料金などを請求する詐欺の手口もあります。こうしたいかがわしいメールに騙されないようにしましょう。

マネーゲームと称するねずみ講やマルチ商法への勧誘メールも流行しています。こうした勧誘に安易な気持ちから応じたために、多額の借金を抱えてしまう事件も発生しています。うまい話には必ず罠があるものです。甘い誘いには十分注意して下さい。

●チェーンメール

その他、「このメールを○人に転送すること」といった内容のチェーンメールを携帯電話で送ることが、とりわけ小中学生や高校生など若い世代の間で目立って蔓延しています。チェーンメールには、「このメールを転送しないと、あなたは殺されます」といった脅しをかけるものや、「このメールを転送すれば、あなたは幸福になります」といったメリットを強調するもの、「俳優の○○は、○○しているらしい」といったデマを広めようとするものなどさまざまなものがありますが、いずれにせよ送られた人が迷惑をこうむるだけでなく、その人がさらに多くの人にチェーンメールを回すことで、迷惑をまきちらす加害者になってしまうという問題があります。チェーンメールが届いたら、自分が加害者にならないように自分のところで止めるようにしましょう。なお、転送しないと直接の危害が及ぶような内容のメールが届き、どうしても不安な人のために、迷惑メール相談センターでは、チェーンメール転送先用のメールアドレス（携帯電話専用）を用意しているので、そちらに転送する方法もあります。

チェーンメール転送先（携帯電話専用）

財団法人日本データ通信協会　迷惑メール相談センター

http://www.dekyo.or.jp/soudan/top.htm

情報セキュリティ関連のホームページ

これらのページはJNSAのリンクのページ（http://www.jnsa.org/link.html）に掲載されています。

政策・緊急情報

・経済産業省／情報セキュリティに関する政策、緊急情報
http://www.meti.go.jp/policy/netsecurity/index.html

インターネットトラブルの総合相談窓口

・インターネットホットライン連絡協議会
http://www.iajapan.org/hotline/

フィッシング詐欺

・フィッシング対策協議会
http://www.antiphishing.jp/

ウイルス情報

・独立行政法人 情報処理推進機構（IPA） セキュリティセンター
http://www.ipa.go.jp/security/

インターネット犯罪

・都道府県警察本部のサイバー犯罪相談窓口
http://www.npa.go.jp/cyber/soudan.htm
・インターネット安全・安心相談
http://www.cybersafety.go.jp/
・警察庁
http://www.npa.go.jp/
・警察庁　サイバー犯罪対策
http://www.npa.go.jp/cyber/
・警察庁セキュリティポータルサイト「@police」
http://www.cyberpolice.go.jp/

ショッピングやオークションのトラブル

・経済産業省／消費者相談室
http://www.meti.go.jp/intro/consult/a_main.html#shouhisha
・次世代電子商取引推進協議会／ネットショッピング紛争相談室
http://www.ecom.jp/adr/ja/
・国民生活センター
http://www.kokusen.go.jp/
・社団法人日本通信販売協会（通販１１０番）
http://www.jadma.org/

著作
経済産業省

企画・制作
JNSA NPO 日本ネットワークセキュリティ協会

迷惑メール

・経済産業省／迷惑メール対策
http://www.meti.go.jp/policy/consumer/tokusyuu/meiwakumail-main.htm
・財団法人日本データ通信協会　迷惑メール相談センター
http://www.dekyo.or.jp/soudan/top.htm

個人情報の保護

・首相官邸／個人情報の保護に関する法律
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

著作権

・社団法人著作権情報センター
http://www.cric.or.jp/

総合知識

・総務省／国民のための情報セキュリティサイト
http://www.soumu.go.jp/joho_tsusin/security/index.htm

ネットワークセキュリティに関する情報提供

・NPO 日本ネットワークセキュリティ協会
http://www.jnsa.org/

2005年10月1日　第4版

著作
経済産業省
商務情報政策局
情報セキュリティ政策室
〒100-8901　千代田区霞が関1-3-1
URL：http://www.meti.go.jp/policy/netsecurity/index.html
E-Mail：it-security@meti.go.jp

企画・制作
特定非営利活動法人（NPO）　日本ネットワークセキュリティ協会
〒136-0075　東京都江東区新砂1-6-35　T.T.ランディック東陽町ビル
URL： http://www.jnsa.org/
E-Mail： sec@jnsa.org