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　23分

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Adobe Flash Player（Adobe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

①CD-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。
③Menu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「クイズ学習に挑戦する」をクリックします。

※「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制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」をクリックしてください。

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。
①CD-ROMのアイコンをダブルクリックします。
②「MOVIE.mpg」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 120 MHz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またはIntel Core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

冊子およびCD-ROMご利用にあたっての注意事項

はじめに

パソコンやインターネットは近年急速に普及してきており、大変便利な道具として、私たちの生活をますます豊かにする可能性を持っています。しかし、自動車のようにルールやマナーを守って利用しなければ、自分や他人に危害を加える危険性も持っており、実際にコンピュータウイルス感染や、詐欺行為、プライバシー侵害などの問題が現実の社会問題になっています。

インターネットは世界中の人々が共有する公共の場です。ひとりひとりの利用者が自分の情報や財産を守るためにも、またインターネットでつながる他の利用者に迷惑をかけないためにも、意識を高め、安全対策やモラルに関する最低限のルールやマナーを守っていなければなりませんし、そうでなければこの公共の場は成り立ちません。それは現実社会と同じことです。

このため、経済産業省と日本ネットワークセキュリティ協会（ＪＮＳＡ）では、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなどの情報セキュリティに関する基礎知識を学習できるセミナーを、「インターネット安全教室」と称して、一般利用者を対象に2003年から開催してきました。このセミナーは、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たちや、警察庁、都道府県警察の協力を得て実施していますが、今後はこの活動を全国に広げていき、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。この冊子とＣＤ－ＲＯＭを有効にご活用いただき、必要なセキュリティ対策を講じた上で、ルールを守り安全快適にインターネットを利用されることが、私たちの心からの願いです。

経済産業省
NPO 日本ネットワークセキュリティ協会

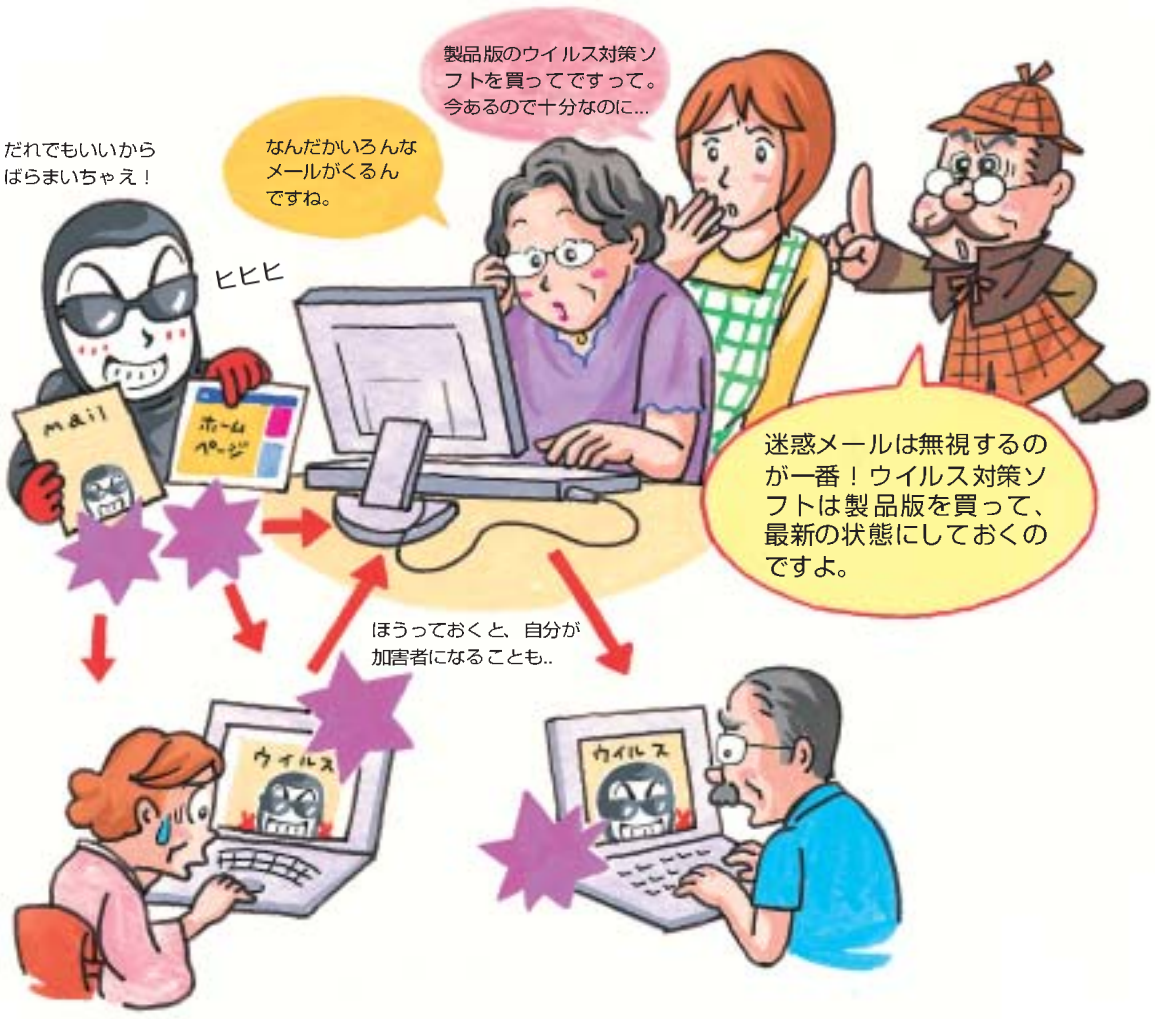
目　次

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. 迷惑メールとウイルスにご用心!

勝手に送られてくる心当たりのないメールは「迷惑メール」といいます。「迷惑メール」にはどのような危険性がひそんでいるのでしょうか？　知らぬ間にパソコンが「ウイルス（コンピュータウイルス）」に感染してしまうのも心配です。「ウイルス」感染からパソコンを守るにはどうしたらいいのでしょうか？

迷惑メールは無視！ ウイルス対策も万全に！



添付ファイルがある「迷惑メール」はとりわけご用心！

●メールは簡単に送れてたいへん便利ですが、この便利さを悪用して「**迷惑メール**」もたくさん送られてきてしまいます。
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。
●**添付ファイル**がある「**迷惑メール**」はとりわけご用心！　添付ファイルをうっかり開く（ダブルクリックする）と**ウイルスに感染**してしまう可能性が高いのです。
●心当たりのない「**迷惑メール**」は“百害あって一利なし”。**無視**をするのが一番です。
●なお、**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**がついていたら**要注意**です！
知人に添付ファイルを送ったかどうか確認しましょう。そして、添付ファイルを開くときには、必ずウイルスチェックを行ってからにしましょう。
●メールソフトは、**添付ファイル**や**HTMLメール**を自動的に**開かない設定**にしておきましょう（P.20参照）。

「ウイルス対策ソフト」とOSを最新の状態にしましょう

●パソコンを買ったときに入っていた「**ウイルス対策ソフト**」は**お試し版**であることが多いので注意しましょう。
●「**ウイルス対策ソフト**」は**製品版**を購入しましょう。そして、次々と登場する新しいウイルスからパソコンを守るために**自動更新**の設定にしておきましょう。
●新しいウイルスからパソコンを守るには、パソコンの**OSをアップデート**して**常に最新の状態にしておく**ことも大切です。
●もし**ウイルスに感染してしまったら**、すみやかに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しょう**。そして、「ウイルス対策ソフト」を使ってパソコンからウイルスを駆除します。
●不明な点があれば、もよりの**販売店など**に問い合わせましょう。

「迷惑メール」の中のリンクもご用心！

●**リンクをクリック**するように書いてある「**迷惑メール**」もご用心！　リンクをクリックすると、「**ワンクリック請求**（**ワンクリック詐欺**）」（P.18参照）や「**フィッシング詐欺**」（P.19参照）など、さまざまな**詐欺行為**に巻き込まれてしまうおそれがあります。
●「**配信停止はこちらまで**」とあっても**返信してはいけません**。配信停止にならないばかりか、メールアドレスを知られてしまい、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。

POINT 1

相手の分からない「迷惑メール」は無視しましょう。ウイルス対策ソフトは製品版を購入し、パソコンのOSもアップデートして常に最新の状態に更新しておきましょう。

2. 無線LANの落とし穴

インターネットに無線で接続することができる「無線LAN」は、とても便利です。でも、セキュリティの設定をきちんとしておかないと、とても危険です。「無線LAN」を安全に使うにはどうしたらいいのでしょうか？　そして、ファイル共有をするときには、どのようなことに注意する必要があるのでしょうか？

無線LANは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

パスワードとセキュリティの設定をしましょう

●無線LANを使うには、「**アクセスポイント**」という機器と「**無線LANカード**」を用意します（「無線LANカード」を内蔵しているパソコンもあります）。
●「**アクセスポイント**」をインターネットに接続し、「**無線LANカード**」をパソコンに差せば、無線でインターネットに接続できるようになります。
●ただし、**セキュリティの設定**をしないでいると、どのパソコン（あるいはゲーム機）でも**簡単に接続**できるようになっています。
●無線LANを使う場合は、**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。
●従来、セキュリティの設定は「**WEP**」という方式が一般的でしたが、より安全な「**WPA**」という方式を使うようにしましょう。

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、ネットワークでつながれた複数のパソコンの間でファイルのやりとりをする際に用います。それ以外のときには、ファイル共有は**OFF**にしておきましょう。
●ファイル共有は、**フォルダごとに設定**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の設定を**OFF**にしておきしょう。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

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. 個人情報の扱いは慎重に

インターネットカフェや駅などに置かれているパソコンのように、不特定多数の人が利用するパソコンでは、どのようなことに注意する必要があるのでしょうか？クレジットカード番号や暗証番号など大切な個人情報は、どのように扱ったらいいのでしょうか？　ID・パスワードはどうすればいいのでしょうか？

ID・パスワードなど大切な個人情報の扱いにご注意！

不特定多数が利用するパソコンは要注意です！

●インターネットカフェや駅などに設置されているパソコンは、不特定多数の人が利用するので、個人情報の扱いは慎重にしましょう。
●とりわけ大切な**ID・パスワード**を盗まれたり、勝手に使われてしまわないよう注意します。
●**クレジットカード番号**や**暗証番号**など**特に重要な個人情報**は**入力しない**ようにしましょう。
●ホームページを閲覧したときには、**自分が見たページの履歴を削除**（どのページを見たか、という情報）や**クッキー**（ユーザーの識別に使われる情報）、**一時ファイル**（Webページを閲覧したとき一時的に保存しておくデータ）を**削除**しておきましょう。削除しないでいると、履歴をたどるなどして、どのページを閲覧したのかが第三者にわかってしまいます。
●ファイルをごみ箱に捨てたときには、「**ごみ箱を空にする**」を選択して、ファイルを消去しておきます。
●「**オートコンプリート**」（過去の入力履歴を参照して次の入力内容を予想し、あらかじめ表示する機能）は、OFFにしておきましょう。

オートコンプリートをOFFにする

まず、［ツール］メニューから［インターネットオプション］を選択します。次に［コンテンツ］のタブをクリックします。表示された画面で「オートコンプリート」の［設定］をクリックします。左の画面で、全てのチェックをはずし、［OK］をクリックします。

ID・パスワードの扱い方

●**IDと同じパスワード**を設定するのはやめましょう。
●自分や自分に関係する人の**名前**、**住所**、**電話番号**、**誕生日など**類推されやすいパスワードを設定するのは危険です。
●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しょう。
●**長いパスワード**（できれば8文字以上）を設定しましょう。
●**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しょう。
●できるだけ**定期的にパスワードを変更**するようにしましょう（できれば3カ月に1回以上）。
●**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**をしましょう。

POINT 3

不特定多数の人が利用するインターネット環境では、IDやパスワードなど重要な個人情報の扱いは慎重に。クレジットカード番号や暗証番号など特に重要な個人情報の入力は避けましょう。

4. ファイル交換ソフトの“わな”

「ファイル交換ソフト」には、どのような“わな”がひそんでいるのでしょうか？　「ファイル交換ソフト」を使っていると、大事な書類が流出してしまうことがあるのはどうしてでしょうか？　著作物を交換するのは、なぜいけないのでしょうか？

ファイル交換ソフトには、情報漏えい、著作権侵害という2つの問題点がある

大切な情報が世界中にばらまかれてしまう危険性

●パソコンがファイル交換ソフトを悪用する**ウイルスに感染**すると、知らぬ間に**パソコンに保存されている情報**が世界中に**ばらまかれてしまう**危険性があります。
●**仕事の重要書類**が世界中にばらまかれてしてしまい、**大きな社会問題**になったケースもあります。
●**自分自身の重要な個人情報**はもちろんのこと、**家族や友人の重要な個人情報**が世界中に**ばらまかれてしまう**危険性があります。
●一度、ファイル交換ソフトを通じて世界中にばらまかれてしまった情報は、**二度と取り戻すことができません**。

著作物を交換するのは著作権侵害にあたります

●CDやDVDなどで販売されている音楽、映画、ソフトウェアなどの著作物は、著作権法によって保護されており、個人的に楽しむなどのほかは、著作権者に無断で複製することが禁じられています。このため、それらをコピーして**ファイル交換ソフト**を使って**交換**したり、**交換できる状態**にしただけでも**著作権侵害**になり、法律で罰せられることがあります。
●著作権侵害は犯罪です。刑事罰として**5年以下の懲役**または**500万円以下の罰金**が課せられることがあります（懲役刑と罰金刑の両方が課せられることもあります）。

危険性についての知識を家族みんなで共有しましょう

●家族でパソコンを共有していると、自分が**ファイル交換ソフト**を入れたつもりがなくても、**家族が入れている**ということがあります。ファイル交換ソフトの**危険性**についての**知識**を**家族みんなで共有**しましょう。

POINT 4

ファイル交換ソフトには、情報漏えいの危険性や、著作権侵害の可能性があることに注意しましょう。家族がファイル交換ソフトを使用しているかどうかの確認も忘れずに。

5. 有害サイトから子どもを守る

「出会い系サイト」というのは、不特定多数の男女が交際を求めるサイトのことをいいます。「出会い系サイト」から子どもを守るにはどうしたらいいのでしょうか？携帯電話の管理を子どもまかせにしておいて、大丈夫なのでしょうか？

フィルタリングなどで有害な情報から子どもたちを守る

フィルタリングサービス：
子どもの安全のために、有害なサイトを見せないようにするサービス

「出会い系サイト」から子どもを守りましょう

- 「**出会い系サイト**」を**18歳未満の児童**が利用することは**法律で禁止**されています。
- 「出会い系サイト」で、**18歳未満の児童**に対して**性的交渉**を求めたり、**金銭を目的とした交際**を求める書き込みをするのは**犯罪**であり、成人であれ児童であれ法律で罰せられます。

フィルタリングサービスを利用しましょう

- **有害な情報から子どもを守る**ために、有害サイトへの接続を防止する**フィルタリングサービス**を利用しましょう。
- **携帯電話**の**フィルタリングサービス**は**無料**で提供されています。詳しくは、もよりの携帯電話販売店などに問い合わせましょう。
- パソコンの場合は、**フィルタリングソフト**をインストールしておきましょう。

携帯電話の管理を子どもにまかせない

- 「**学校裏サイト**」という学校の同窓生などが非公式に開設するサイトや、「**プロフ**」という個人のプロフィールを公開して意見を書き込むサイトが、**プライバシー侵害**や**いじめ**の温床となることがあり、社会問題となっています。
- こうした**プライバシー侵害**や**いじめ**から子どもを守るためには、**携帯電話の管理を子どもにまかせない**ことが大切です。
- 子どもには、「**携帯電話のルールやマナー**」（P.18）をきちんと教えましょう。

POINT 5

18歳未満は出会い系サイトを利用してはいけません。有害な情報から子どもを守るために、フィルタリングサービスを申し込むなどの対策をしましょう。

6. SNSを上手に楽しむには

SNSというのは、友だちや同じ趣味を持つ人たちの間でお互いに日記を公開しあったり、情報交換ができるサービスです。SNSを上手に楽しむには、どうしたらいいのでしょうか？　どのようなルールやマナーを守ることが大切なのでしょうか？

SNSでは個人情報の扱いや著作権侵害に注意しましょう

プライバシーを守りましょう

●自分や家族、友人などの**個人情報**（**名前**、**住所**、**電話番号**、**年齢**、**家族構成**、**勤務先名**、**学校名など**）は**むやみに公開しない**で、プライバシーを守るようにしましょう。
●日記を書き続けているうちに、プライバシーに関わる情報が小出しにされ、個人が特定されてしまうことがあります。そして、そうした**個人情報を悪用**され、**犯罪につながる**ことがあるので注意しましょう。
●**SNS**は、自分のプロフィールや日記の**公開の範囲を自分で設定できる**ようになっています。公開の範囲の種類は、SNSによって異なりますが、「友人まで公開」「友人の友人まで公開」「SNS全体に公開」「インターネット全体に公開」などがあります。プライバシーを守るという点では、「友人まで公開」といったように公開の範囲を限定したほうがいいでしょう。
●**ブログ**もまた日記をつけられるサービスですが、ブログは基本的に「**インターネット全体に公開**」するようになっているので、より一層**注意**が必要です。

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**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使用することは著作権の侵害となります。
●文章は**出典を明らかにして引用**しましょう。
●写真、イラスト、音楽、映像は**自分に著作権のあるもの**や**著作権フリーのもの**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。
●**誹謗中傷**（ひぼうちゅうしょう）をしたり、他人の個人情報や写真などを**本人の許可なく掲載**してはいけません。**名誉毀損**（めいよきそん）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**（こうじょりょうぞく）**に反する行為**、**法律に違反する行為**をしてはいけません。

POINT 6

SNSの日記で家族や友人などの個人情報を公開するときには十分注意しましょう。
他人のプライバシーや著作権侵害にも気をつけましょう。

まとめ

インターネットを安全快適に活用するためには、きちんとルールやマナーを守ることが大切です。この「インターネット安全教室」では、そうしたルールやマナーを6つのポイントにまとめてあります。これらを参考にしてインターネットを安全快適に活用してください。

インターネットファミリー！レッツゴー！

1
相手の分からない「迷惑メール」は無視しましょう。ウイルス対策ソフトは製品版を購入し、パソコンのOSもアップデートして常に最新の状態に更新しておきましょう。

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
不特定多数の人が利用するインターネット環境では、IDやパスワードなど重要な個人情報の扱いは慎重に。クレジットカード番号や暗証番号など特に重要な個人情報の入力は避けましょう。

4
ファイル交換ソフトには、情報漏えいの危険性や、著作権侵害の可能性があることに注意しましょう。家族がファイル交換ソフトを使用しているかどうかの確認も忘れずに。

5
18歳未満は出会い系サイトを利用してはいけません。有害な情報から子どもを守るために、フィルタリングサービスを申し込むなどの対策をしましょう。

6
SNSの日記で家族や友人などの個人情報を公開するときには十分注意しましょう。
他人のプライバシーや著作権侵害にも気をつけましょう。

こんなことにも注意しましょう

ショッピングをするときの注意点

●**インターネットショッピング**はとても便利ですが、その反面、常に**詐欺**などの被害にあう**危険と隣り合わせ**である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ときには、**暗号化**などによってしっかりと**個人情報**が**保護**されているかどうかを確認しましょう。
●万が一のトラブルに備え、**注文記録**や**取引条件**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しょう。

オークションに参加するときの注意点

●**オークションサイト**は、**取り引きの仲介**をするだけです。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**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。ただし、仲間うちで“にせもの”の高い評価を作り上げ、購入者をだます**オークション詐欺**も発生しているので、うのみにするのは危険です。
●トラブルを避けるには、配送中の事故で商品が**破損**したり**紛失**したときにはどうするのか、商品が到着した後になんらかの**欠陥**が見つかったときにはどうするのか、**返品・返金**はどうするの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**をしておいたほうがいいでしょう。
●**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リスクがあるので注意しましょう。
代引を利用する方法もあります。
●落札できなかった人に「落札者が辞退したのであなたに権利が移りました」といった“にせもの”のメールを送りつけ、代金を振り込ませる「**次点詐欺**」に注意しましょう。

安全ミニ知識

子どもに教えたほうがいい「携帯電話のルールやマナー」(P.13)

「携帯電話のルールやマナー」を教えないまま子どもに携帯電話を持たせるのは、とても危険です。さまざまな犯罪にまきこまれてしまったり、“いじめ”にあったときにどう対応していいかわからず、追いつめられてしまうことがあるからです。反対に“いじめ”をしてしまったり、著作権侵害をするなど、やってはいけないことをやってしまうこともあります。子どもには次のような「携帯電話のルールやマナー」を教えるようにしましょう。

1.携帯電話で**困ったこと**や**いやなこと**があったら、どんなことでもすぐに**家の人**や**先生**に**相談**しましょう。
2.**知らない人**に、**名前**、**住所**、**電話番号**、**年齢**、**学校名**、**メールアドレス**など**個人情報**を**むやみに教えない**ようにしましょう。
3.**よくわからないサイト**に、**むやみに会員登録をしない**ようにしましょう。
4.**心当たりのない電話番号**からかかってきた**電話には出ない**ようにしましょう。
5.**知らない人**から送られてきたメールには、**返信しない**ようにしましょう。メールの中の**リンク**も**クリックしない**ようにしましょう。
6.「このメールを○人に送ってください」といった「**チェーンメール**」が届いても、**無視**をしましょう。
7.掲示板やブログ、SNSなどで**コメント**を書き込むときには、だれかを**傷つける**ようなことや、その人の大切な**個人情報**を**書き込まない**ようにしましょう。
9.音楽や歌詞、まんが、アニメ、キャラクターなどには、それを作成した人に「**著作権**」があるので、無断で勝手に友だちと**交換しない**ようにしましょう。

「ワンクリック請求」にはどう対処したらいいか？（P.5）

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（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。「ちょっとだけ覗いてみようかな」という心のスキをつき、うしろめたい気持ちを利用して料金を支払わせようとするものなので、そうした手口にのらないようにしましょう。

本当に利用していないのであれば、料金を支払う必要はありません。無視をしましょう。リンクをクリックする前であればメールを削除してもかまいませんが、もし、リンクをク

リックして「ワンクリック請求」にかかってしまった場合は、証拠としてそのメールやサイトの画面をしばらくの間保存しておいたほうがいいでしょう。

なお、恐怖心をあおる目的で、「あなたの個人情報を取得いたしました」といって、「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と脅してくる場合もあります。実際に電話をかけてくるなど悪質な脅しがあった場合は、すぐに最寄りの警察に相談しましょう。

「フィッシング詐欺」にはどう対処したらいいか？（P.5）

「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“にせもの”です。「○○○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、リンクをクリックさせて“にせ”のサイトへ誘導し、重要な個人情報を入力させようとするのです。

「フィッシング詐欺」がねらう重要な個人情報の代表例は以下のようなものです。

- **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**

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重要な個人情報を問い合せることはないので、そうしたことを尋ねるメールは「フィッシング詐欺」と思って間違いありません。

「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」にかかってしまったかもしれないというときには、次のように対処しましょう。

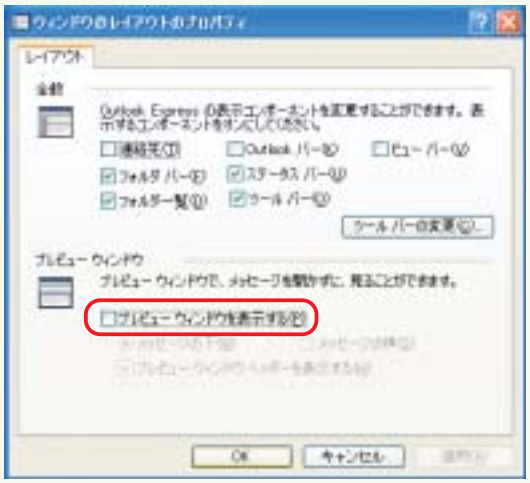
- **警察庁**や**国民生活センター**の**ホームページ**で対処法を確認します。
- **銀行**や**クレジット会社**、**ショッピングサイト**などに連絡をして相談をします。
- 契約している**プロバイダ**や**オークション**、**会員サービス**の会社に連絡をして、**ID・パスワード**の**変更手続**きをします。
- 上記でも解決できない場合には最寄りの**警察**に**相談**します。

メールソフトでプレビューやHTMLメールを自動的に開かないようにするには？（P.5）

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。

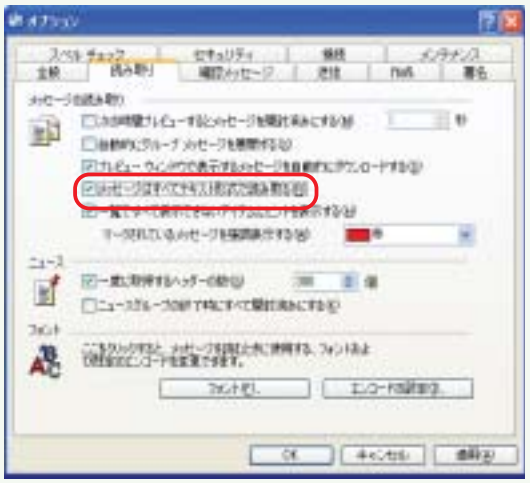
※ホームページと同じように、文字に色づけしたり、文字のサイズを変えたり、画像や表やアドレスを入れたりできるメール表示のこと

●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）

添付ファイルを自動的に開かないようにするには、プレビューウイ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［プレビューウインドウ］の項目で［プレビューウインドウを表示する］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とる］のチェックボックスをクリックしてONにします。

パソコンをより安全にするにはどうしたらいいか？

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）。

(1)ウイルス対策ソフトを最新の状態に保つ設定にする

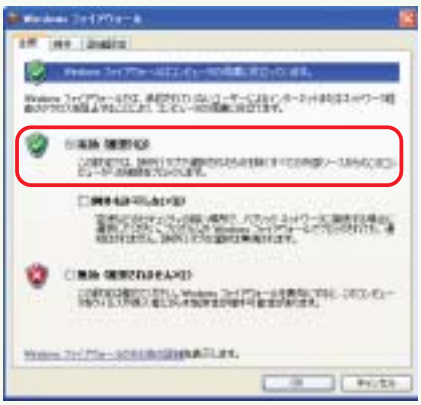
ウイルス対策ソフトをインストールし、ウイルス検出用ファイルを最新の状態に保つ設定にします。ウイルス対策ソフトについては、たとえばIPA（独立行政法人情報処理推進機構）セキュリティセンターのウイルス情報などをご覧下さい。

●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。

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/aboutus/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

サイバー犯罪対策

●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/

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/

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
●財団法人データ通信協会
http://www.dekyo.or.jp/soudan/

フィッシング詐欺

●フィッシング対策協議会
http://www.antiphishing.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
●有限責任中間法人ECネットワーク/インターネット詐欺対策集
http://www.ecnetwork.jp/sagi/
●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/

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/

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/

2007年10月1日　第5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/
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　NOF東陽町ビル
URL： http://www.jnsa.org/
E-Mail： sec@jnsa.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