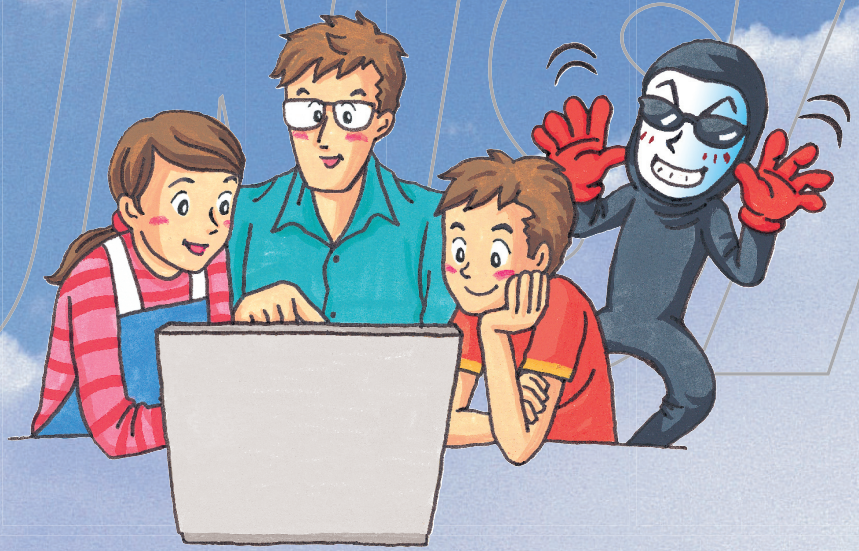
インターネット
利用者のための
経済産業省
JNSA
セキュリティ
対策講座

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「体験学習」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。
※「体験学習」を再生するにはブラウザ(閲覧ソフト)とMacromedia Flash Playerが必要となります。

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「体験学習に挑戦する」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。
②CD-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「体験学習に挑戦する」をクリックします。

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」のアイコンまたは「体験学習 スタート」のアイコンをダブルクリックします。

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。

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 95、Windows 98、Windows 2000、Windows ME、Windows XP、Windows NT Workstation 4.0(Service Pack 3以降)
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:MacOS 8.6.1、Mac OS X 10.1.3以上
必要メモリ:32MB以上

本CD-ROMご利用にあたっての注意事項

使用条件:
①情報セキュリティ啓発の目的での使用に限ること
②営利目的ではない使用に限ること
③複製・配布に際しては、この注意事項をこのままの形態で含めること
④映像・音声については、改編を行なわないこと

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といった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ましたが、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、ルールを守り、必要なセキュリティ対策が講じられていくことが、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

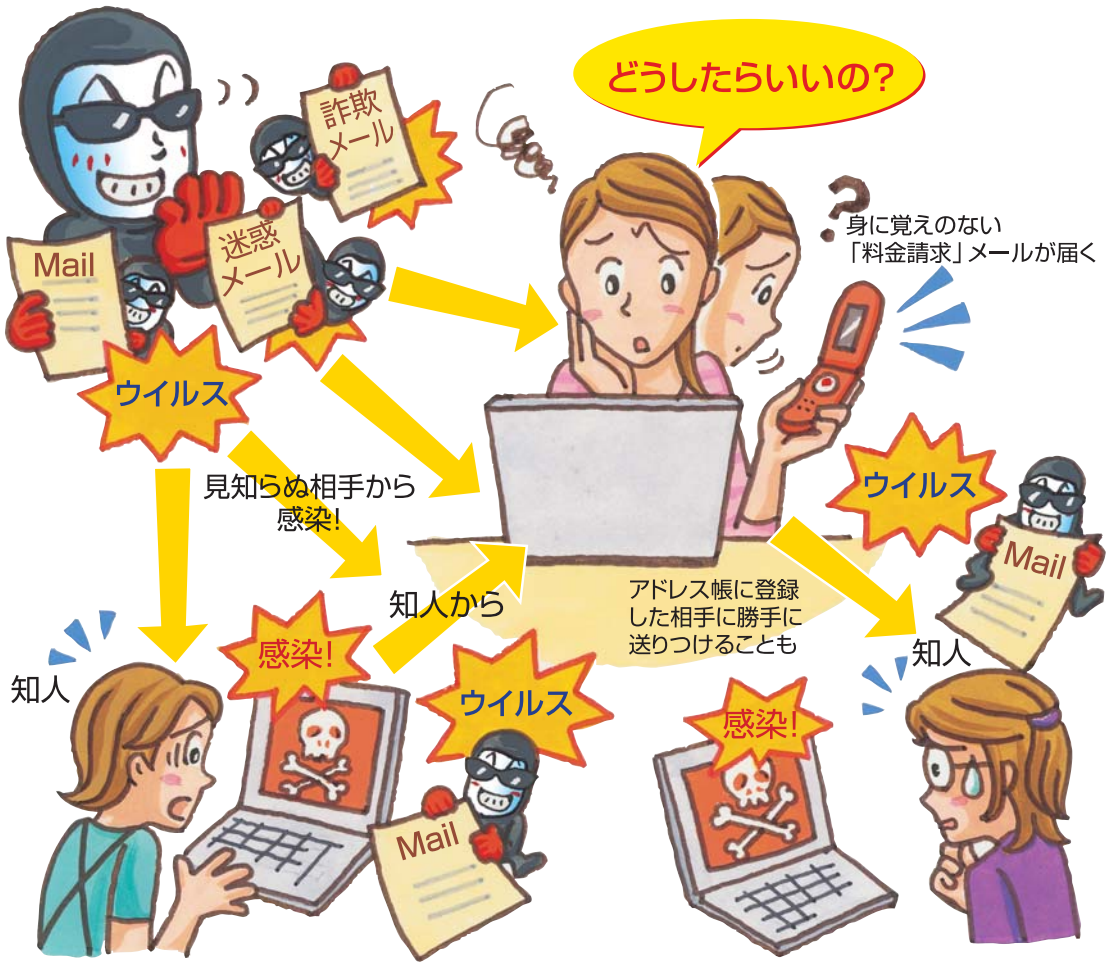
目　次

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「情報セキュリティの関連ページ」などを参考に、状況に応じた対策を確認しましょう。

1. 危険なメールやホームページ

メールは大変便利ですが、それだけに悪質ないたずらや犯罪の格好のターゲットとなります。ある日突然、ウイルス感染メールが送られてくるかもしれません。ウイルスに感染すると、ファイルを次々と消されたり、パソコンを起動できなくなってしまうことがあります。そればかりか、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だってあるのです。その他、身に覚えのない「料金請求」をする詐欺メールや、いかがわしい広告を送りつける迷惑メールなど、対応を誤ると大変なことになる危険なメールがたくさんあるので注意しましょう。

危険なメールにご注意!



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多くは、メールの添付ファイルです。ただし、それだけではありません。ホームページからダウンロードしたファイル、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

- ●パソコンにワクチンソフト（ウイルスをチェックし駆除するソフト）をインストールします。
- ●ワクチンソフトは、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しておきます。
- ●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す。（P.18 Q&A参照）
- ●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。

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、送信元にウイルス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。セキュリティ修正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、最新の状態にアップデートしておきます。

もし、感染してしまったら…

- ●パソコンから速やかにウイルスを駆除し、ネットワークを一時切断するなど、そのウイルスにあった適切な対処をほどこします。（P.19 Q&A参照）

悪質なメールにはどう対応したらいいか？

悪質なメールには、「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。」といったメールを送りつけ、料金をだましとる詐欺メールや、虚偽の内容を伝えるデマメール、「このメールを○人に転送してください。」といった内容のチェーンメール、出会い系サイトやアダルトサイトなどからしつこく送られてくる広告メールなど、さまざまな種類があります（P.19 Q&A参照）。

対応策は？

- ●悪質なメールは、無視するのが一番です。決して返信したり、連絡をしてはいけません。「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を生む可能性もあります。
- ●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。
- ●犯罪に巻き込まれる危険性がある場合は、法律の専門家や最寄りの警察に相談しましょう。

POINT 1

ウイルス感染や悪質なメールに注意しましょう

2. 個人情報の漏えい

地方の特産品から、化粧品、コンサートのチケット、デジカメ、車、海外旅行にいたるまで、プレゼントページにはたくさんのプレゼントが掲載され、人気を博しています。ハガキをポストに投函することに比べれば、インターネットでプレゼントに応募したり、アンケートに答えたりするのは、とても簡単です。でも、だからといって安易に個人情報を入力するのは要注意です。プレゼントページに限らず、どのようなホームページであっても、個人情報を入力するときは、そのホームページの個人情報の取り扱い方に納得できるかどうか、個人情報が漏えいする危険性はないかどうか、よく考えることが大切です。

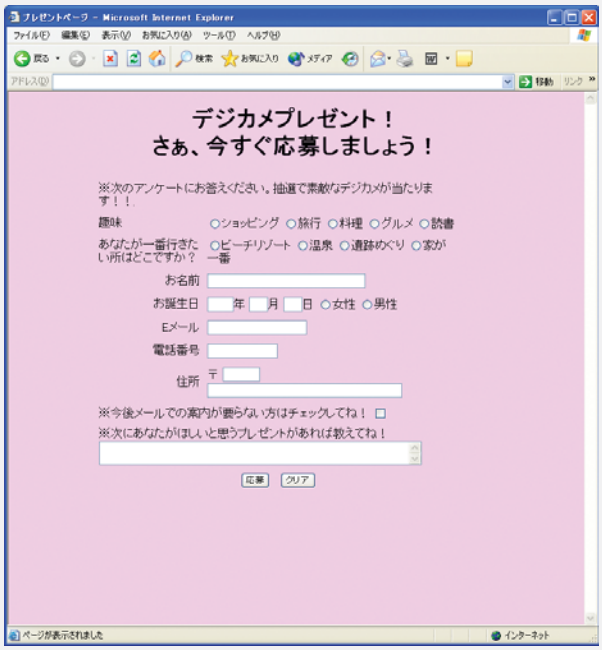
個人情報はよく考えてから入力する

個人情報を入力する前に気をつけましょう！

自分の大切な個人情報（住所、氏名、生年月日、年齢、電話番号、メールアドレス、クレジット番号など）を入力するときは、たとえホームページの運営者が意図しなくても、その個人情報が漏えいして悪用される危険性があるということを忘れてはいけません。アンケートに答えたら、身に覚えのないダイレクトメールがたくさん送られてくるようになった、しつこいセールスの電話がかかってくるようになった、いやがらせに個人情報を掲示板に掲載されてしまった、悪質な犯罪につながってしまったというような事件が実際に発生しています。こうした被害を防ぐには、個人情報を入力する前に、そのホームページの個人情報の取り扱い方はどうなっているのか、セキュリティはしっかりしているかどうかをまず確かめることが大切です。巻末の「情報セキュリティ関連のページ」などを参考に、個人情報の取り扱い方や、暗号化や電子認証などの技術対策を確認しましょう。

個人情報が漏えいし、悪用されたときにはどうしたらいいか？

- 個人情報が掲示板やホームページなどに掲載された場合は、すぐにその画面を印刷するなどして証拠を保存します。そして、掲示板の主催者やホームページを掲載しているプロバイダに連絡をして、削除を要請します。
- 場合によっては、メールアドレスや電話番号などの変更を検討します。
- しつこい勧誘やいやがらせ、脅迫などがある場合は、証拠を保存するとともに、日時や会話の内容、状況などについて、できるだけ詳しく記録します。
- 犯罪に巻き込まれる危険性がある場合は、法律の専門家や最寄りの警察に相談しましょう。



POINT 2

個人情報を入力するときは気をつけましょう

3. しのびよる詐欺行為

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セキュリティがしっかりし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プリントしておくとともに、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。
●会員制のホームページに、試しに入会したつもりが解約できず、法外な引き落としをされてしまったというような事件が発生しています。少しでもあやしいと感じるホームページでショッピングをするのは、やめておいたほうがいいでしょう。

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。
●しっかりとしたオークション・サイトには、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いることもあるので、参考にするといいでしょう。
●落札したら、実際に取引をする前に、メールを送るなどして相手の連絡先と住所を確認します。
●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リスクがあるので注意しましょう。郵便局の代引サービスや、宅配便業者やクレジット会社などが行っているエスクロウ・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。
●出品者が落札者にクレジット番号を入力させ、その口座から代金を引き落とすというような場合は、クレジットを悪用される危険性が高いので、特に要注意です。

フィッシング詐欺にご注意！（P.20 Q&A参照）

●実在のショッピング・サイトやクレジット会社を装ったメールを送りつけ、偽のサイトに呼び込んでクレジット番号など個人情報をだまし取るフィッシング詐欺に注意しましょう。

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。
●消費者センターや法律の専門家に相談し、対策を考えます。
●警察に被害届を出します。

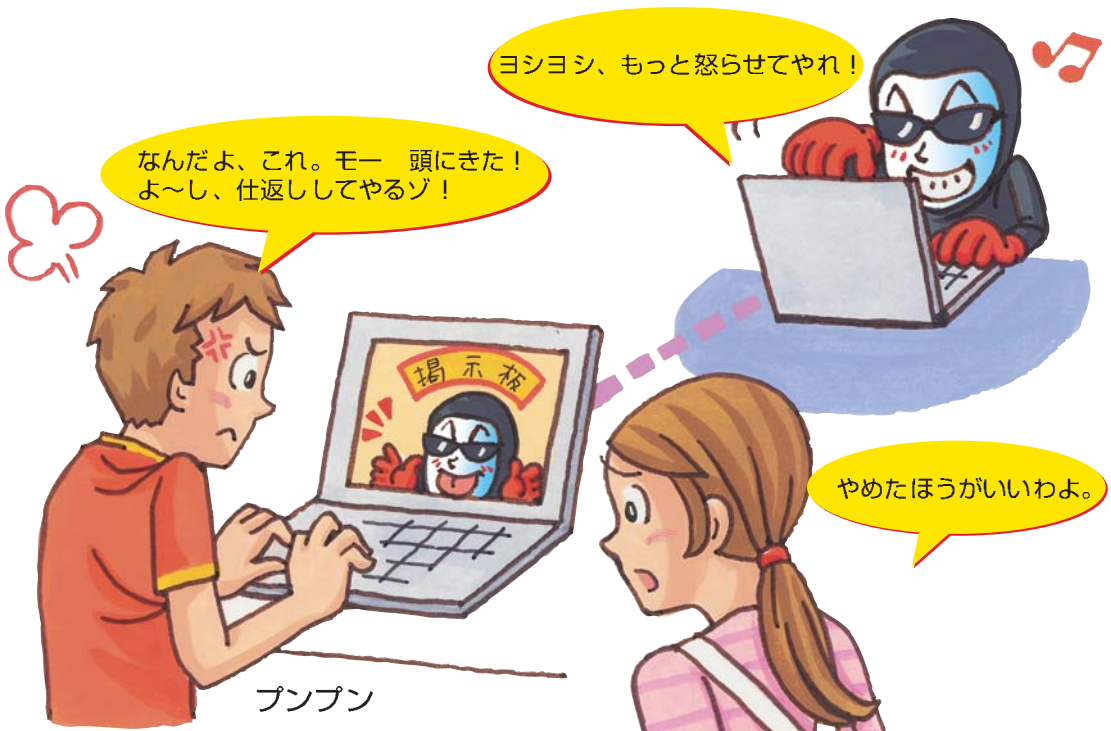
POINT 3

本当に信頼できる相手かどうか よく確かめて対応しましょう

4. 掲示板、チャットのマナー

掲示板では、自分が関心のあるテーマについてさまざまな人と意見をかわすことができます。そして、チャットなら複数の人と同時に会話ができます。誰もが気軽に書き込めて、気軽に読める。それだけに、自分勝手な振るまいをして、その場の雰囲気をだいなしにしてしまうマナー違反は絶対に禁物です。誹謗中傷はもちろんのこと、不快感を与えるような内容や言葉使い、プライバシーの侵害、法律違反はいけません。自分ではさほどひどいことを言ったつもりがなくても、言われた人にとってはとても耐えがたい場合があります、マナーを守って、インターネットで広がるコミュニケーションを楽しみましょう。

マナー違反とプライバシー侵害にご注意



掲示板、チャットのマナー

・ていねいな言葉使い・挨拶も忘れずに
・誹謗中傷はしない
・個人情報は書き込まない

マナーを大切にしましょう

掲示板やチャットの魅力は、さまざまな人と気軽にコミュニケーションできることです。とはいえ、さまざまな人が参加しているということは、どのような人が参加してくるかわからないということです。また、参加している人以外に、見ているだけの人もいます。そして、掲示板やチャットでの書き込みは、現実の世界でお互いに面と向かって話している場合と異なり、文字だけで表現されてしまうため、自分ではさほどひどいことを言ったつもりがなくても、相手を大変深く傷つけてしまうことがあります。このため、掲示板やチャットでは、マナーを守ることが非常に大切になります。そして、プライバシーを侵害したり、侵害されないように気をつける必要があるのです。(P.20 Q&A参照)

- ●不特定多数の人が参加する掲示板やチャットには、よくハンドルネーム（ニックネームのことです）で参加することがあります。本名で参加する場合には、個人情報が特定されないように注意が必要です。
- ●自己紹介をするのはマナーですが、個人情報を特定できるものは避けたほうがいいでしょう。
- ●自分や他人の個人情報は書き込まないようにします。どのような人が参加してくるかわからないところに、個人情報を書き込むのは大変危険だからです。
- ●メールアドレスの書き込みも、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ります。もし、メールアドレスを書き込む場合は、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などの対策を考えておくといいでしょう。
- ●掲示板やチャットに書き込むときの基本は、ていねいな言葉使いです。なれなれしい言葉使いや乱暴な言葉使いは、さまざまな人が参加している掲示板やチャットにはふさわしくありません。「初めまして」、「こんにちは」といった挨拶も忘れないようにしましょう。
- ●他人を誹謗中傷してはいけません。マナー違反であるばかりか、名誉毀損やプライバシーの侵害などの罪で訴えられることもあります。
- ●掲示板やチャットごとに必ず管理者がいます。そして、ルールやマナーについての記載があります。管理者が示すルールやマナーを守り、掲示板やチャットならではのコミュニケーションを楽しみましょう。

誹謗中傷、プライバシー侵害などの被害にあった場合は？

- ●掲示板で誹謗中傷やプライバシー侵害などの被害にあった場合は、すぐにその日時を記録してください。その際に、画面を印刷するなどして証拠も保存します。そして、掲示板の管理者に連絡をして削除を要請します。
- ●悪質なケースの場合は、法律の専門家や最寄りの警察に相談しましょう。

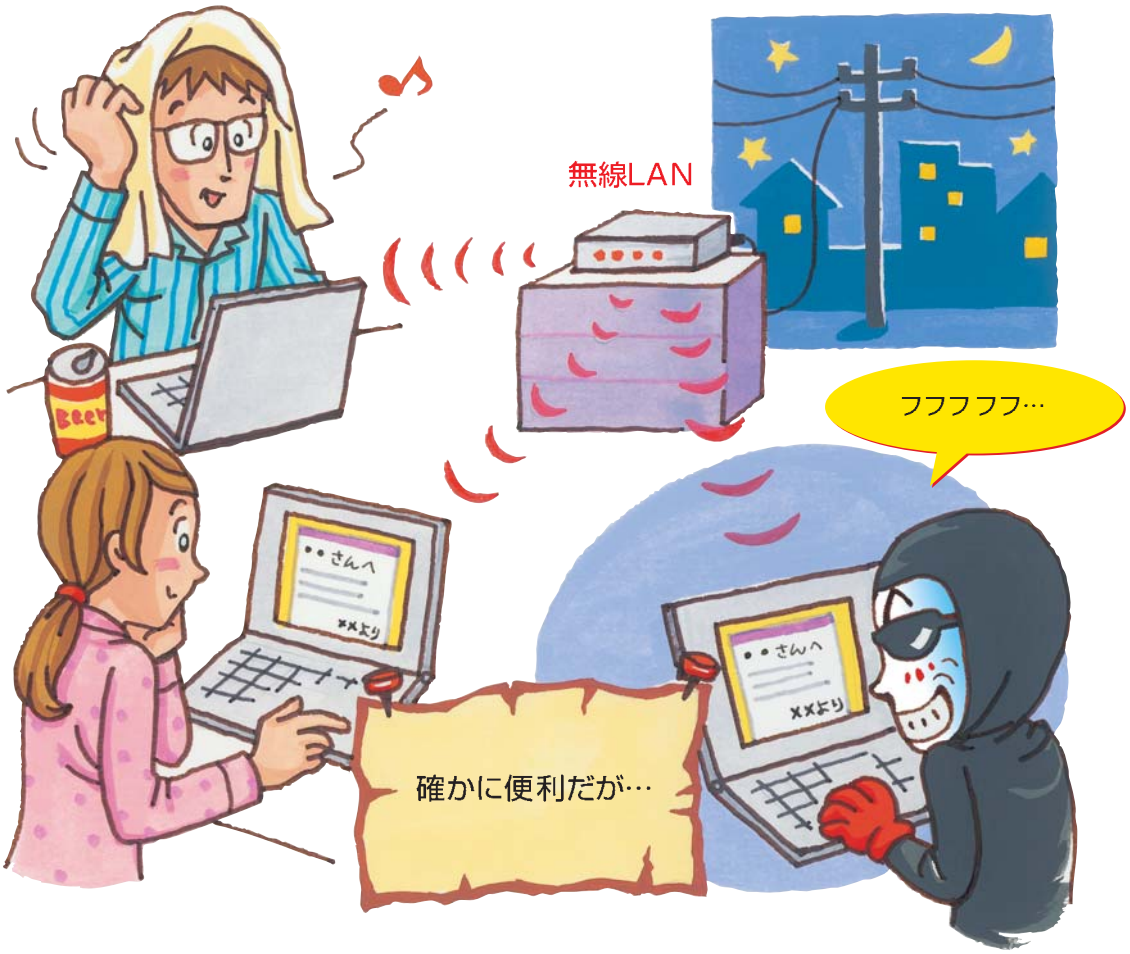
POINT 4

掲示板、チャットはマナーを大切にしましょう

5. 侵入されるパソコン

最近、オフィスのみならず自宅でも無線LANを導入するケースが増えてきました。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スペースが増えてきました。ところが、こうして便利になってくると、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すか？　利用者パスワードを設定していたり、不要なときはファイル共有をOFFにしていればいいのですが、無防備なままでいるのは危険です。

侵入にはくれぐれもご注意を！



無線LANを使う場合は、必ず利用者パスワードを設定しましょう

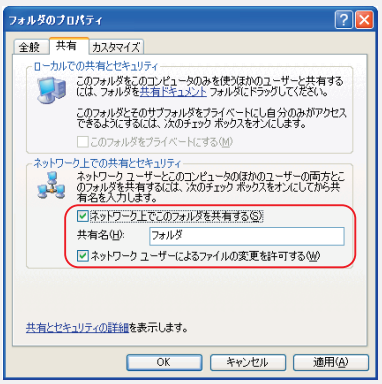
●ネットワークに接続したパソコンは、無防備なままでいると不正に侵入される危険があるので注意しましょう。（P.21 Q&A参照）ネットワークケーブルを使って有線で接続している場合は、実際にネットワークケーブルをつながなければ不正に侵入されることはありません。しかし、無線LANの場合は、電波のとどく範囲にあるパソコンは、誰が使っているパソコンであっても、いつでも接続できるようになっているわけです。このため、無線LANを使う場合は、利用者パスワードなどセキュリティの設定をして、より安全な環境で使うようにしましょう。

●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、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。

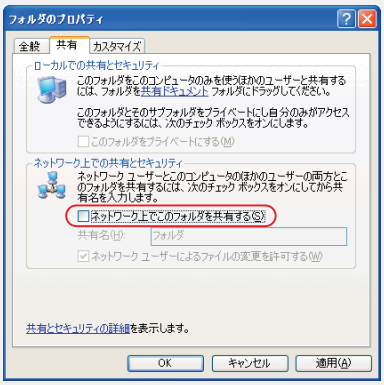
●ファイル共有の設定はフォルダごとに行うことができます。とりわけ重要な書類の入ったフォルダは必ずWindowsのファイル共有設定をOFFにしておきます。ONにしたままネットワークに接続すると、共有設定したすべてのファイルの中身を見られてしまいます。



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 5

パソコンの不正侵入には気をつけましょう

6. ホームページ作成の落とし穴

誰でも簡単にホームページを公開できる時代になりました。個人のホームページであっても、大手の新聞社や放送局のホームページと肩を並べて、世界中に向かって情報発信をすることができるのです。本人の才能と努力次第によっては、大人気のホームページを作ることも夢ではありません。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。

社会のルールとプライバシーを守らないと…

社会のルールを守りましょう

●文章や写真、イラスト、音楽、映像などには、それを著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るのでやめましょう。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。
●ホームページ上で他人の情報や写真などを本人の許可なく公開したり、誹謗中傷してはいけません。
●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。誘拐など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

ホームページを公開するときは、
社会のルールやプライバシーを守りましょう

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、情報や品物、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。こうしたポイントをしっかりと覚えて、インターネットを毎日の暮らしに役立てて下さい。

上手に利用して、インターネットを楽しもう!

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、企業や学校、公的機関からインターネットに接続するときには非常に重要ですが、家庭からの場合はこうしたユーザーIDやパスワードを入力しないで済むため、あまりその重要性を意識することがありません。しかし、ショッピングサイトで会員登録をするときなどには、このユーザーIDとパスワードの管理が非常に重要になってきます。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危険性があります。オンライン・バンキングであれは、預金を引き落とされてしまうでしょう。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。たとえば必ず思い出せるよく知っている文章や歌の中の文字をとって、任意に数字を混ぜて作ります。
  （例：「ぞうさん、ぞうさん、おはなが」→「z3z3087G@」）
- 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（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す。

有害なサイト対策について

インターネットの世界には、大人にとってはもちろんのこと、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、いわゆる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 メールソフトで添付ファイルやHTMLメールを自動的に開かないようにするにはどうしたらいいですか？（P.5）

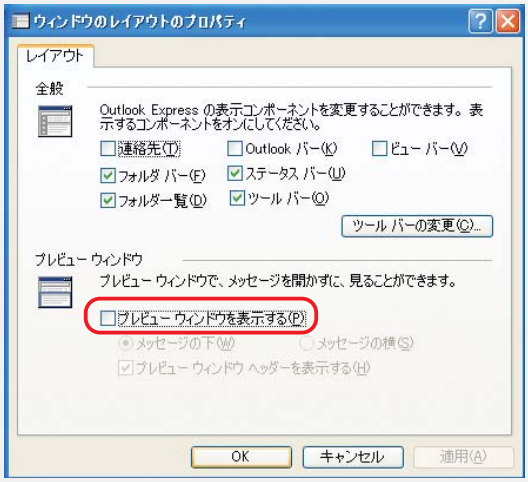
A Outlook ExpressやOutlookなどのメールソフトの場合、添付ファイルやHTMLメール（※）は、初期設定の段階では自動的に開くように設定されています。そのほうが便利だからなのですが、ウイルスに感染しやすい状態なため、自動的に開かないように設定したほうがいいでしょう。

※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、画像や表を入れたりできるメールのこと

●OutLookの場合

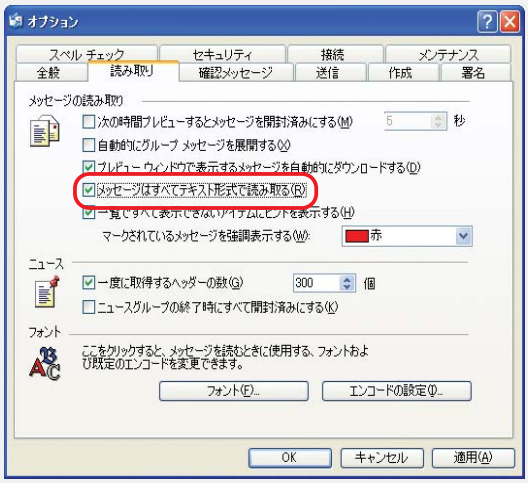
・添付ファイルを自動的に開かないようにする

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メールを自動的に開かないようにする

HTMLメールを自動的に開かないようにするには、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 もしウイルスに感染してしまったら、どうしたらいいですか？(P.5)

A

ウイルスに感染した場合、その症状はさまざまです。コンピュータの動作が不安定になる、意図しない動作をするなど異変が明確に現れる場合もあれば、知らぬまに大切な情報を消してしまうなど異変に気づきにくい場合もあります。

さらには、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、感染を拡大してゆくタイプのものもあります。そうした場合は、感染を広げないために、パソコンに接続しているネットワークケーブル（Ethernetケーブル）を抜くなどして、パソコンをいったんネットワークから切り離すようにしましょう。

コンピュータウイルスの感染を確認する一番確実な方法は、最新のワクチンソフトで検査することです。その場合、ウイルスの定義ファイルが古いと最新のウイルスを検出できないこともあるので、ウイルス定義ファイルは必ず最新のものを利用します。
ワクチンソフトは検査だけでなくウイルスの駆除も行いますが、ワクチンソフトでは駆除できないタイプのウイルスも存在します。

ウイルス定義ファイルの更新方法や、ワクチン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、お使いのワクチンソフトのベンダー（販売会社）にお問い合わせください。

ウイルスの被害にあう前に、重要なデータの定期的なバックアップやウイルス対策を行い、感染を防ぐことが大切です。

●参考：主なワクチンベンダーのWebサイト一覧
http://www.ipa.go.jp/security/antivirus/vender.html

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.5)

A

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。

また、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。

悪質なメール撃退法

身に覚えのない架空請求メールは、断固として無視をする

出会い系サイト、わいせつ画像サイトへのリンクはクリックしない！

マネーゲーム（ねずみ講、マルチ商法）への勧誘メールにひっかからない！

Q フィッシング詐欺というのはどういうものなのですか？（P.9）

A

フィッシング詐欺とは、実在のショッピング・サイトやクレジット会社、銀行を装ったメールを送りつけ、偽のサイトに呼び込んでクレジット番号やID、パスワードなど個人情報をだまし取る詐欺の手口です。

「フィッシング」は、英語では「phishing」と書きますが、発音は「fishing」と同じです。「利用者を釣る」というところからきているのですが、利用者を釣るためのえさ（メールやサイト）が洗練（sophisticated）されているところから「phishing」となったという説があります。

フィッシング詐欺は、2003年ごろから米国で大流行しはじめ、日本でも大手検索サイトからのメールをよそおって、パスワードをだまし取るなどの被害が出始めています。

メールがきっかけになっているという意味では、悪質なメールのひとつということができますが、一見しただけでは、実在のショッピング・サイトやクレジット会社、銀行から送られたメールと区別がつかないほど巧妙に偽装している点など、いわゆる悪質なメールの中でもより一層悪質なメールということができるかもしれません。

フィッシング詐欺の特徴の第一は、メールを送りつける際に、いかにも信頼できそうなメールアドレスを装って送信者（差出人、From）を詐称することです。似ているけれども、微妙に違うメールアドレスなので注意が必要です。

特徴の第二は、メールの中で「○○○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で、フィッシング詐欺を行うためのサイトへのアクセスを誘導することです。個人情報の入力をうながすようなメールが届いたら、怪しいと疑ってかかりましょう。

そして第三の特徴は、誘導したサイトが、実在のショッピング・サイトやクレジット会社、銀行のサイトとみまがうほどよくできた偽のサイトであり、そこでクレジット番号やID、パスワードなど個人情報を入力させて、まんまとだまし取ることです。

フィッシング詐欺にかからないようにするには、まず第一に、メールを信用せずに、むやみにリンクをクリックしないことが大切です。そして、そのメールの真偽を確かめたい場合は、実在のショッピング・サイトやクレジット会社、銀行に電話をかけて確認するか、Webブラウザを新規に立ち上げ、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て、サポート窓口にメールを送るなどして問合せをします。

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？（P.11）

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、免許を取る際に、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 不正侵入を防ぐにはどうしたらいいですか？（P.13）

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）。

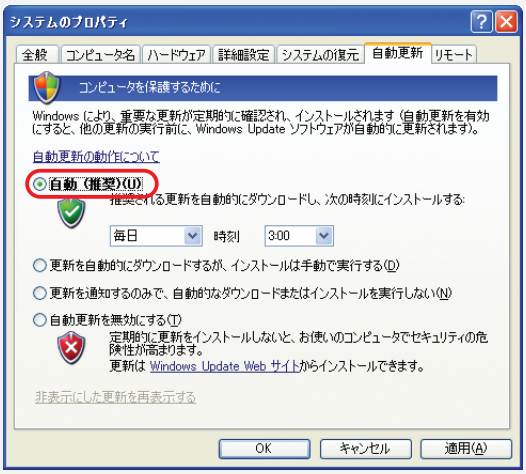
(1)ワクチンソフトを最新の状態に保つ設定にする：

ワクチン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。ワクチンソフトについては、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/

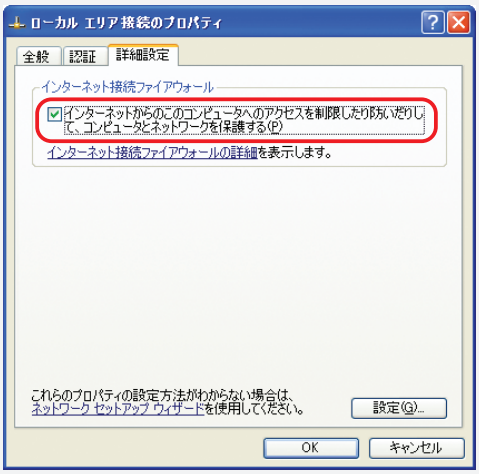
(2)Windows Update（ウィンドウズアップデート）を自動更新するように設定する：

［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、［インターネット接続ファイウォール］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/

ウイルス情報

・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等一覧
http://www.npa.go.jp/cyber/soudan/hitech-sodan.htm
・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
・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/
・国民生活センター（電話03-3446-0999、または手紙のみ受付）
http://www.kokusen.go.jp/
・NCAC:全国の消費生活センター
http://www.kokusen.go.jp/map/
・社団法人日本通信販売協会（通販１10番）
http://www.jadma.org/

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/

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/

2004年10月1日　第 2 版　第 2 刷

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