一般利用者のための情報セキュリティ対策－実践編

ここでは、電子メールやホームページの閲覧、ショッピングサイトなどを利用する一般利用者が、安全にインターネットを利用できるようにするために、実践すべき情報セキュリティ対策について説明します。

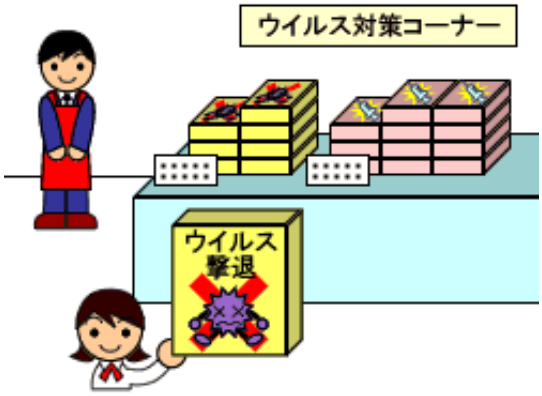
※特に重要な項目には マークがついています。

ウイルス対策の実践

重要!

ウイルスに感染しないようにすることは、コンピュータにおける情報セキュリティとしてもっとも大切な対策のひとつです。最近のウイルスは、電子メールやホームページを見たことで感染するウイルスばかりではなく、勝手にインターネットやネットワークを通じて自己増殖するワーム型というタイプのウイルスや、インターネットに接続しただけで感染するウイルスも出現してきています。

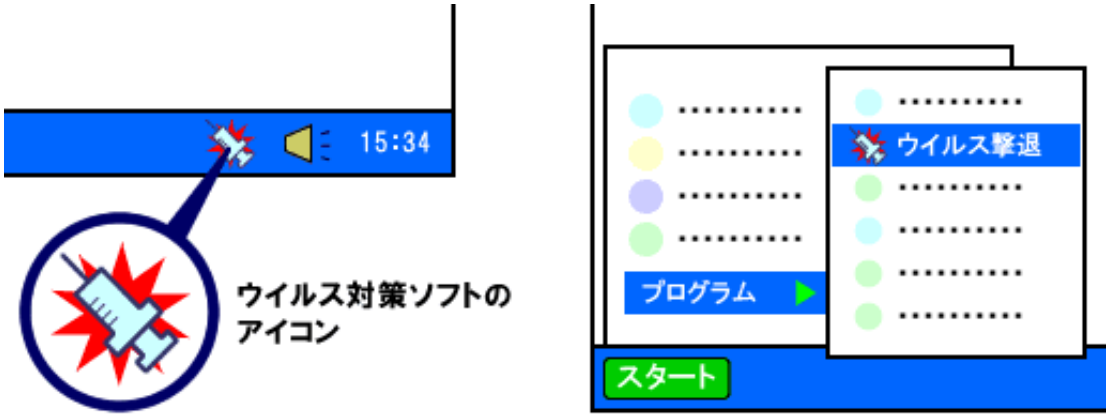
ウイルスに感染しないようにするためには、コンピュータにウイルス対策ソフトの導入が必要です。ウイルス対策ソフトは、パソコンショップや家電販売店などで販売されています。ただし、家庭向けのパソコンには、最初からウイルス対策ソフトがインストールされていることもあるので、購入前に自分のコンピュータをチェックしておく方がよいでしょう。



ウイルス対策ソフトを導入する以外にも、プロバイダが自社の接続サービスの利用者向けに提供しているウイルス対策サービスを利用する方法もあります。ウイルス対策サービスの提供の有無や提供内容などについては、プロバイダのホームページで確認するか、加入しているプロバイダに問い合わせてください。

■ウイルス対策ソフトの確認

ウイルス対策ソフトがコンピュータにインストールされている場合には、通常、コンピュータのタスクバーと呼ばれる領域にウイルス対策ソフトが動作していることを示すアイコンが表示されます。または、コンピュータのプログラムの一覧で、ウイルス対策ソフトが含まれているかどうかを確認するという方法もあります。



■ウイルス検知用データの更新

ウイルス対策ソフトが新しいウイルスに対応するためには、常にウイルス検知用データを最新のものに更新しておかなければなりません。コンピュータにウイルス対策ソフトがインストールされていても、ウイルス検知用データが古いままでは、新しいウイルスに感染してしまう危険性があります。

多くのウイルス対策ソフトでは、コンピュータの起動時にウイルス検知用データを更新する仕組みを持っています。また、常時接続環境では、起動時だけでなく、定期的な更新を行なう必要もあります。ほとんどのウイルス対策ソフトには、指定時刻や指定時間ごとの自動更新機能が装備されているため、それらの設定を行なうようにしてください。

一般的なウイルス対策ソフトでは、購入してから約１～３年ごとに、ウイルス検知用データをダウンロードするための契約を更新する場合が多いようです。ウイルス対策ソフトによっては、月ごとに契約できる「月額版」も提供されています。なお、最初からコンピュータにインストールされているウイルス対策ソフトの場合には、お試し版として３０日程度の契約しか含まれていないことがあるので注意が必要です。

自分のコンピュータのウイルス対策ソフトがどのような契約内容になっているかということを確認し、契約が切れてしまっている場合には、新たに契約を延長するか、新規にウイルス対策ソフトを購入しなければなりません。ウイルス検知用データの更新方法や契約方法については、ウイルス対策ソフトのマニュアルで確認するか、ウイルス対策ソフトのメーカーに問い合わせてください。

なお、プロバイダのウイルス対策サービスを利用する場合には、プロバイダがウイルス検知用データを自動的に更新するため、ユーザーによる更新作業は不要になります。

ヒント

ウイルス検知用データは、ウイルス対策ソフトによって、パターンファイル、ウイルス定義ファイル、シグネチャファイル、対策データなどの名前で呼ばれています。

注意

最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用 Web サイトに誘導して、ウイルスをインストールさせる方法です。

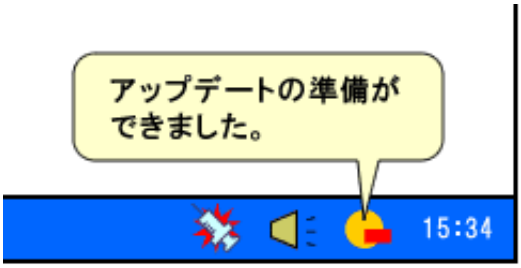
ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード / インストールしたりしないようにしてください。

ソフトウェアの更新

重要!

OS、Web ブラウザや電子メールソフト、Office アプリケーションなどでは、セキュリティホールを修正したり、情報セキュリティ上の問題を解決したり、さまざまな不具合を解消したりするための修正プログラムが、メーカーから提供されることがあります。インターネットに接続された環境でコンピュータを利用する場合には、これらの修正プログラムを定期的に適用して、できる限りソフトウェアを最新の状態に保つように心がけなければなりません。

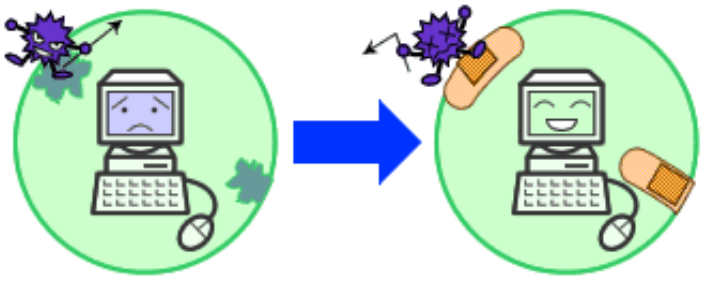
現在、家庭用のコンピュータで使用されている代表的な OS には、修正プログラムを自動的に適用するための機能が導入されています。タスクバーの右下に「アップデートの準備ができました」というメッセージが表示された場合には、自動的にアップデートする機能が準備されていることを表します。その場合には、そのメッセージをクリックして、画面上の指示に従って操作してください。



ソフトウェアのアップデートを知らせるアイコンとメッセージ

アップデートのメッセージが表示されない場合には、プログラムを選択して、手動で処理を行うことができます。そのように操作した場合にも、画面上に表示される指示に従って作業を行います。

なお、ワープロソフトや表計算ソフト、動画再生ソフト、ドキュメント表示ソフトなど、その他のソフトウェアについても、情報セキュリティ上の問題などで、修正プログラムが提供されることがあります。これらについても、コンピュータにインストールされているソフトウェアを確認して、それぞれのメーカーのホームページなどで定期的にチェックしてみてください。また、最近では、ソフトウェアのメーカーに登録をしておくと、プログラムが更新された場合に、電子メールで連絡が来ることがあります。そのため、普段使用しているソフトウェアについては、できるだけユーザー登録をしておいた方がよいでしょう。


アップデート前　　アップデート後

個人情報の保護

インターネットを使用して、ホームページを閲覧したり、ホームページを公開したりする場合には、自分や家族、知人の個人情報を保護することを心がけなければなりません。特に、次のようなことに注意してください。

●ホームページのアンケートなどには、むやみに自分の氏名、年齢、住所、電話番号、メールアドレスなどを登録しないようにしましょう。ホームページのアンケートなどの場合には、アンケートを実施している会社や組織を確認して、ホームページ上に記載されている個人情報の取り扱い規定をよく読んでから登録するようにしましょう。

●電子掲示板には、自分や知人の個人情報（名前や住所、電話番号など）を投稿しないようにしましょう。

●自分のホームページやブログでは、自分や家族、知人の個人情報や写真はできるだけ公開しないようにしましょう。

●ＳＮＳ（ソーシャルネットワーキングサービス）に参加する場合にも、自分のプロフィールは、名前などの最低限の項目だけを登録して、住所、電話番号はできるだけ記入しないようにしましょう。

●ＳＮＳ（ソーシャルネットワーキングサービス）では、日記やプロフィールの公開対象を設定することができるものもあります。個人情報を記入している場合には、公開対象を制限することを検討してください。

●インターネットで知り合った人には、むやみに氏名や住所、電話番号、メールアドレスを教えないようにしましょう。どうしても連絡先を教える必要がある場合には、メールアドレスだけにするとよいでしょう。

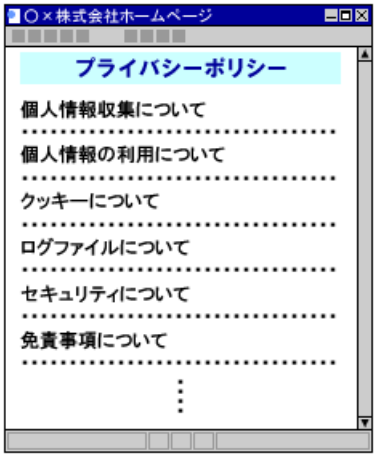
安全なオークションとショッピングサイトの利用

ネットオークションやショッピングサイトに関連するトラブルは、利用者の急増に伴い、年々増加しています。ネットオークションや悪質なショッピングサイトにおけるトラブルから身を守るためには、まず取引相手が信頼できる人や会社であることを確認することが大切です。

■取引相手を確認する

一般的なネットオークションのWebサイトでは、出品者の過去の取引実績を確認することができます。それらの取引実績を確認して、信頼できる人であるかどうかを判断しましょう。また、取引が決まった場合には、取引相手の氏名と連絡先（住所や自宅の電話番号など）を必ず確認するようにします。

ショッピングサイトの場合には、Webサイトを管理している会社が実際に存在していることや、信頼できる会社であることを確認しておくとよいでしょう。また、Webサイト内に販売者の連絡先や電話番号、商品の返品や交換の可否、代金の支払い方法などの利用規約がきちんと盛り込まれているかどうかということも、ショッピングサイトの信頼性を判断する材料になります。



■個人情報の取り扱い

最近、ショッピングサイトから顧客情報が漏洩する事件が数多く発生しています。こういった事件においては、自分で防衛することは困難ですが、事前に個々のショッピングサイトにおける個人情報の取り扱いについての方針を確認し、信頼できるショッピングサイトを選択することが重要な情報セキュリティ対策のひとつであると言えます。しっかりとしたショッピングサイトであれば、「プライバシーについて」、「個人情報について」、「プライバシーポリシー」といったページで、利用者に対して個人情報の取り扱い方法を説明しているはずです。

ネットオークションの場合には、Webサイトの中に、トラブルの事例や注意すべきことなどが記載されていることが多いので、それらをよく参考にして利用するようにしてください。なお、ネットオークション、ショッピングサイトのどちらの場合でも、他の出品者や他のショッピングサイトと比較して、あまりにも安すぎる金額が掲示されている場合には警戒した方がよいでしょう。

パーソナルファイアウォール・ブロードバンドルーターの導入

重要!

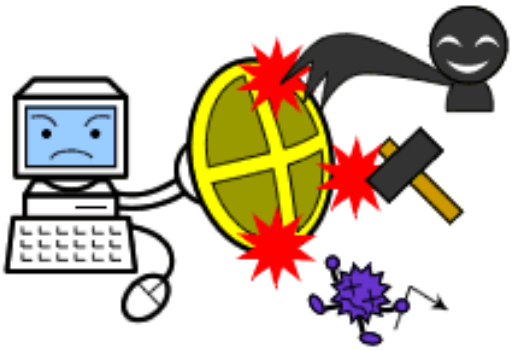
家庭においてもADSLや光回線による常時接続回線の利用が増えてきました。それに伴い、家庭内のコンピュータに対する不正アクセスの被害が発生するようになってきています。

家庭内で使用しているコンピュータを不正アクセスから防御するためには、パーソナルファイアウォールというソフトウェアを導入することをお勧めします。パーソナルファイアウォールを導入すると、ハッカーからの不正侵入を防いだり、ウイルスの侵入を防御したり、自分のコンピュータを外部から見えなくしたりすることが可能になります。また、パーソナルファイアウォールやブロードバンドルーターを使わなかったら、平均して数分で侵入されるという報告があります。ちょっとぐらいは大丈夫という感覚で、パーソナルファイアウォールやブロードバンドルーターを通さずにインターネットに接続することは避けましょう。

パーソナルファイアウォールは、ウイルス対策ソフトと同様に、パソコンショップや家電販売店などで、パッケージソフトとして販売されています。現在は、ウイルス対策ソフトとパーソナルファイアウォールを組み合わせた統合セキュリティ対策ソフトとして販売されていることが多くなっています。購入したソフトウェアをインストールして、利用環境に合わせて設定を行うことで使用できます。なお、最近はOSにも、簡単な機能を持つパーソナルファイアウォールが付属している場合があります。

また、ブロードバンドルーターにはファイアウォール機能が内蔵されているため、ブロードバンドルーターを設置することでパーソナルファイアウォールを導入した場合と同じ効果を得ることもできます。ただし、オンラインゲームをするためにセキュリティレベルを低下させたり、ゲーム向けのブロードバンドルーターの扱いを誤ったことにより不正アクセスを受けるといった事例もありますので、ブロードバンドルーターは正しく設定しましょう。

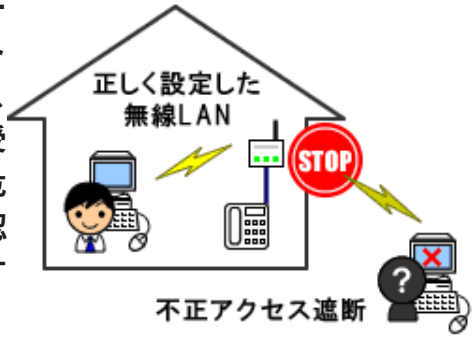
プロバイダによっては、セキュリティサービスとして、ウイルスチェックとともに、ファイアウォール機能を提供している場合もあります。必要に応じて、それらのサービスの利用も検討してください。



安全な無線LANの利用

重要!

無線LANは、LANケーブルの配線を気にせずに、コンピュータを自由に持ち運べる高い利便性から、一般家庭のネットワークにおいて広く使われるようになっています。しかし、無線LANは無線を利用するという性質上、通信内容の傍受（盗聴）や不正利用、アクセスポイントのなりすまし等の危険性が存在することから、利用の際はその危険性を十分認識し、できる限りのセキュリティ設定を行った上で利用するようにしてください。



無線LANを安全に利用するためには、暗号化の設定を行ってください。現時点では、WPA-PSK方式またはWPA2-PSK方式による暗号化を推奨します（WPA2-PSK方式の方が、より強固な暗号化技術です）。パスワードの設定に関しては、「パスワードの検討と管理」を参照してください。また、文字数は21文字以上としてください。

無線LANの暗号化方式としては、旧来からWEPという方式がありますが、近年WEP方式を短時間で解読する手法が発見されたという調査結果も発表されており、必ずしも安全ではありません。
パスワードは、無線LANのネットワーク識別子であるSSIDから類推できるようなものにしないよう注意が必要です（SSIDは一般的に公開されて使用されているため）。

なお、以下の設定を行うことで、第三者からの不正なアクセスを受けにくくなります（ただし、これらの設定は、無線LANの安全性を保証するものではありません）。

- MACアドレスによるフィルタリングを設定し、接続するクライアントを制限する。
- SSIDを隠す機能（ステルス機能）を利用する。

上記設定については機種に依存するため、無線LANのアクセスポイントに付属しているマニュアルを参照してください。

また、現在はセキュリティ機能を強化した無線LAN機器が普及していますので、新たに導入を検討しているのであれば、そのような機器を購入することをお勧めします。

パスワードの検討と管理

OS にログオンしたり、インターネットのネットオークションやショッピングサイトを利用したりする際において、なりすましを防ぐための情報セキュリティ対策には、一般的にパスワードが利用されています。そのため、コンピュータやインターネットを利用する上では、どのようなパスワードを使用するかということが、とても重要なことであると言えます。

安全なパスワードは、以下のような条件を満たしていなければなりません。

●個人情報からは推測できないこと

- ✖ yamada、tanaka、taro、hanako（名前）
- ✖ 19960628、h020315（生年月日）
- ✖ tokyo、kasumigaseki（住所）
- ✖ 3470、1297（車のナンバー）
- ✖ ruby、koro（ペットの名前）

●英単語やよくある名称などをそのまま使用しないこと

- ✖ password、baseball、soccer、monkey、dragon

●適切な長さの文字列であること

- ✖ gf、ps

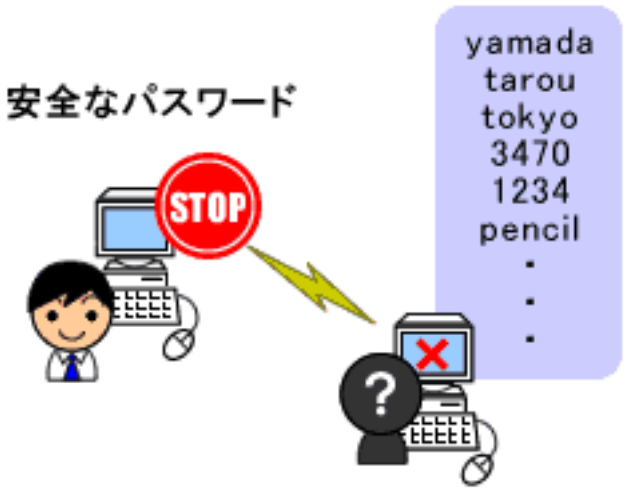
●類推しやすい並び方やその安易な組み合わせにしないこと

- ✖ aaaa、0000（同じ文字の組み合わせ）
- ✖ abcd、123456、200、abc123（安易な数字や英文字の並び）
- ✖ asdf、qwerty（キーボードの配列）

このような条件を満たすパスワードを作ることが困難な場合には、インターネットでダウンロードできるパスワード生成ソフトを利用するという方法も検討してください。パスワード生成ソフトは、指定した条件からランダムなパスワードを作り出してくれる機能を持つソフトウェアです。

また、上記のように安全なパスワードを設定しても、自分のパスワードが他人に漏れてしまえば意味がありません。登録したパスワードは、以下のような点に注意して、安全に管理しなければなりません。パスワードの管理が難しければ、パスワードが管理できる個人情報管理ソフトを使うのも良い方法のひとつです。

- パスワードは、他人には教えないこと
- ユーザー名やパスワードを電子メールでやりとりしないこと
- パスワードを記載したメモを分かりやすい場所（ディスプレイに貼ったり、コンピュータのある机の引き出しにしまったりする）に保管しないこと
- パスワードのメモが不要になった場合には、シュレッダーにかけるなどの方法で他人に読まれないように気を付けて廃棄すること
- 同じパスワードを別々の会員制のWebサイトやショッピングサイトなどで使い回さないこと
- パスワードには有効期限を設けて、できるだけ定期的に変えること



掲示板に個人情報が公開された場合の対処方法

インターネットのホームページや電子掲示板などに、個人の氏名、住所、所属（会社名や学校名など）、電話番号、写真、メールアドレスといった個人情報が公開された場合には、以下のような対応を取ってください。

1. ホームページや電子掲示板の管理者に対して、電子メールで「個人情報が公開されているため、速やかな削除を要求する」旨の連絡を行う。

2. 管理者に連絡がつかない場合には、電子掲示板を利用しているホームページのドメイン情報から所有者を調べる。ドメインが一般のプロバイダである場合には、プロバイダに連絡を取って、該当するホームページと個人情報が公開されている旨を連絡し、早急に対策を取るように依頼する。

3. ドメインの所有者が個人または企業である場合には、ドメイン情報から連絡先を調べて、同様の依頼を行う。

このように対応しても個人情報の削除が行われない場合には、以下の対応も検討してください。

- 電話番号やメールアドレス等の変更できるものは、変更することも検討しましょう。
- 個人情報が掲載されたことがきっかけで、「頻繁に嫌がらせの電子メールや電話がかかってくる」等の被害が生じた場合は、それらすべてを記録したうえで、警察に通報しましょう。