SPREAD サポーター　テキスト　β 3 版

作成日：2009-04-01-08-50-12(日本標準時)
TSS090331.indd

SPREAD サポーターへ向けて

　ウイルスやワームなどの高度化、悪質化に伴い、その出現、および蔓延の脅威が急速に拡大しています。さらに人間の誤解を誘って金銭を搾取する詐欺活動も広まってきています。これに対して、ソフトウェアの脆弱性への対処、セキュリティ技術の推進など様々な対策がとられています。 しかし、一般にセキュリティに関連する情報というものは、ユーザにとっては技術的に難解であったり、複雑であったりし、敷居が高く感じられがちです。このことは、結果としてそのような情報がユーザにはなかなか利用されないということに繋がります。

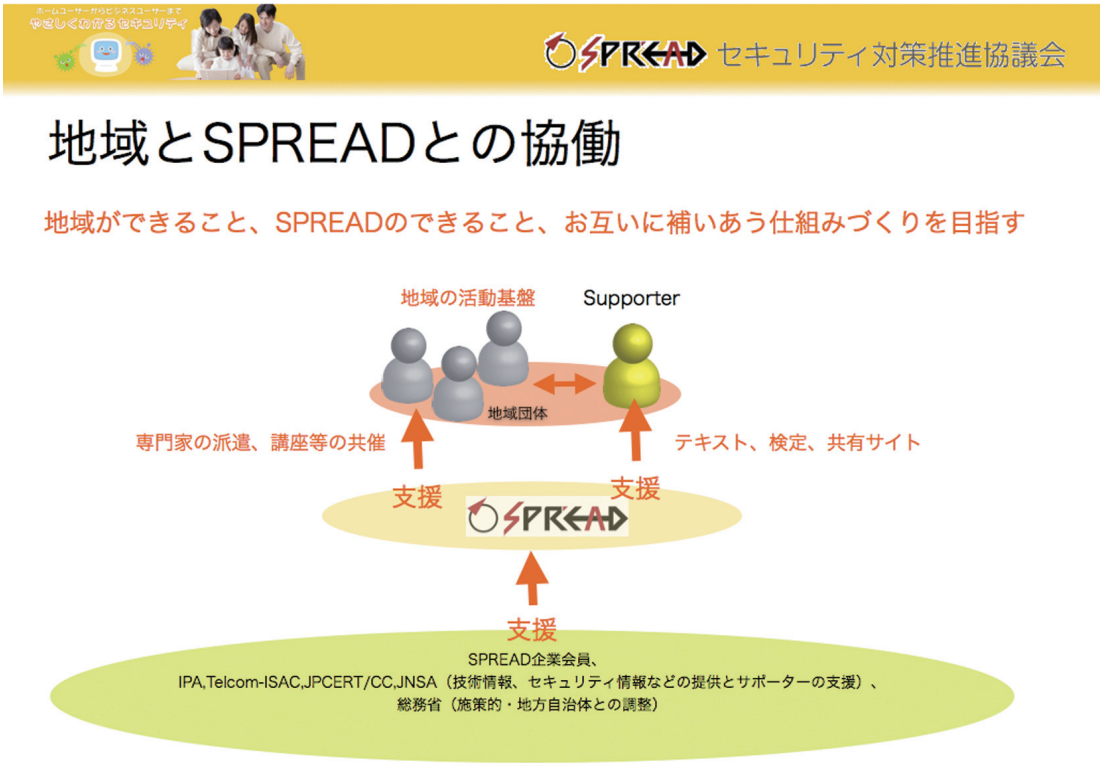
　一方、日本各地には、PC やインターネットを不得意な方々へ手厚いフォローを行っている方々がいらっしゃいます。のような方々が、情報セキュリティについての正しいノウハウを身につけられ、困っている人や初心者ユーザへ適格なサポートをされることで、インターネット社会の安全安心は格段に向上すると考えます。そこでは、私たちは、そのような方々へ適切な教材を提供し学習して頂き、その結果を一定のレベルに達した「SPREAD サポータ」として認定し世に広く知らしめたいと「SPREAD サポータ検定」を創設しました。これによって、各地で活躍されている方々のスキルが向上し、安全安心なインターネット社会が実現されればと願っております。

2009 年 3 月 31 日

セキュリティ対策推進協議会

目　次

1 SPREAD とサポーター検定について



http://www.spread-j.org/

SPREAD
セキュリティ対策推進協議会の略。
Security Promotion Realizing sEcurity meAsures Distribution の頭文字をとった。

SPREAD について

日本においては、政府の e-Japan 戦略による後押しもあり、インターネットを代表とする情報通信技術の普及は目覚しく、いまや経済活動や社会生活を営むための社会基盤のひとつとして極めて重要な地位を占めていると言っても良い状況にあります。したがって、こうした情報通信基盤は、電気、ガス、水道といったような重要社会基盤と同様に、安全かつ堅牢であることが求められています。しかしながら、コンピュータウイルス・ワーム等に関する被害の拡大、スパムメール・フィッシング等の情報セキュリティに関する事件の発生など、情報通信基盤の安全性に対する懸念が高まっており、ユーザーに対する安全対策の実施が強く望まれています。

その方策として、IT 関連団体・企業・NPO 等が相互に密接に連携を取って対策を講じていくことが重要かつ有効であるとの認識のもと、2004 年「セキュリティ対策推進協議会 (以下、SPREAD)」を設立することに致しました。

SPREAD は、公開されたセキュリティ対策情報を、ユーザーに対して「わかりやすく」、「迅速に」、「確実に」流通、浸透させ、すべての人たちにインターネットの安全安心対策を取っていただくことをその活動の目標とします。

その為に、SPREAD は次の事業を行う。

・一般ユーザが情報機器を安心して利用できる環境を創出する
・セキュリティ対策推進
・セキュリティ啓発
・一般ユーザを支援する人材の育成
・ユーザサポート活動支援

SPREAD の活動として、セキュリティ警報がある。脆弱性の発見や重大な攻撃が合った場合に発せられる。
セキュリティ警報
http://www.spread-j.org/cgi-bin/index/snew.cgi

SPREAD サポーターと検定制度について

SPREAD は個人ユーザがインターネットを安全・快適に使うための社会環境の実現を目指しております。その為、SPREAD では、ユーザの近くで相談相手になると共にインターネットを安全・快適に使うための適切なアドバイスを行える人材の必要性を鑑み、SPREAD サポータの育成を目指します。具体的には、以下の事業をおこないます。

・サポータの育成をテキスト作成、講習などの面から支援すると共に、スキルの標準化を目的にサポータ検定を実施します。

・サポータ、協働団体、SPREAD 間の双方向かつ情報共有の場を提供します。これを活用しサポータ活動に役立つ情報を分かり易く、迅速にかつ的確に伝えます。

「SPREAD サポータ検定」は 2009 年 3 月からサポータ検定トライアルをはじめました。2009 年秋にはトライアルの成果を基に本格実施を予定しています。

受験資格

SPREAD の活動に賛同し、地域活動として SPREAD、協働団体とともに継続して PC サポート活動をされる方、あるいはこれからサポート活動をされる方。

サポータ検定を受験するには、地域で活動している協働団体の推薦が必要です。

受験を希望される方は地域の協働団体に問い合わせの上、協働団体経由でお申し込みください。

検定試験

検定試験は筆記試験で、試験時間は 1 時間です。トライアルにおいては、サポータ育成講座（1 日コース）の最後に検定試験を実施します。

検定試験の出題範囲は、情報セキュリティ分野が中心ですが、パソコン一般知識も含みます。検定問題は主に「SPREAD サポーターテキスト（本書）」およびサブテキストとして使用する「情報セキュリティ読本（独立行政法人情報処理推進機構、実教出版、¥500）」を基に出題されます。「情報セキュリティ読本」については必要により各自準備ください。

情報セキュリティ読本
http://www.ipa.go.jp/security/publications/dokuhon/2006/index.html

登録と更新

検定合格後 SPREAD サポータとして登録していただきます。検定試験合格者には合格証を発行します。合格基準は PC サポート活動がおおよそできるレベルです。

検定試験の結果は協働団体経由でお知らせします。

現在実施しているトライアル版 SPREAD サポータ資格の有効期間は 2012 年 3 月末日までです。2012 年 4 月以降の扱い（資格更新）については別途お知らせします。

SPREAD 協働団体について

協働団体は SPREAD と協働してそれぞれの地域におけるサポータ活動を支援する団体・組織です。

協働団体は SPREAD と協力してサポータを育成します。また、サポータ検定受検に関しては受験希望者を推薦し、検定申込書を作成する等のとりまとめをするとともに、育成講座および検定試験の日程調整、会場手配等をしていただきます。協働団体は事前に SPREAD に登録をしていただきます。

協働団体一覧（2009 年 3 月 31 日現在）
ドリームナビゲーター横浜
ＧＩＳ総合研究所
ＮＰＯなら情報セキュリティ総合研究所
"NPO 日本コンピュータ振興協会 or
有限責任事業組合情報化支援機構
あん共育有限会社
ＮＰＯ　ナレッジふくい
ＮＰＯ　栃木県シニアセンター
NPO 法人　ＩＴアットうつのみや
鹿児島インファーメーション
山口県セキュリティーマネジメントフォーラム
くわな PC ネット

2 本書の使い方ついて

インターネット、パソコンが多様される情報社会で、ウィルス感染、詐欺、情報漏洩、著作権侵害など様々な問題がおこっています。私たちは、被害に遭わないようにまず自分のパソコンを守り、そして他の人に迷惑をかけないようにするためにいろいろと配慮することも必要になってきます。その為には、どんなことが必要でしょうか？ざっと上げただけでも次のことをしなければなりません。

・Windows など OS やアプリケーションソフトのアップデート、
・セキュリティ対策ソフトの導入と更新、そして定期的なスキャン
・パスワードの適切管理
・安全に配慮したインターネットの利用
・著作権やプライバシーの保護
・加害者にならないように法令遵守

パソコンの初心者であっても被害にあいます。パソコン内の大事な情報がとられてしますこともあります。そればかりか、コンピュータウィルスに感染し迷惑メールを発信させらる場合もあります。被害者だけではなく、加害者にもなってしまう可能性もあります。さらに、法律も知らなければ、うっかり犯罪者になってしまうこともあるかもしれません。初心者へ情報セキュリティの大切さと対策を伝えることは重要です。
では、どうしたらよいのでしょうか？　何から始めたらよいのでしょう？、
そのような時に、このテキストを活用して下さい。安全安心なパソコンの使い方とインターネットを使う上での注意点、被害に遭う前に必要なことを独自の仕方でまとめてみました。また、日頃からパソコンを使われている方々が、初心者からの質問に回答する際に参考になるように工夫しております。

○本書の構成

本書は、大きく分けて 3 部構成になっています。パソコンを安全安心に使う上で知っておかなければならない基本操作を「知っておかなければならないこと」に、インターネットは怖いと言うが実際にはどんな危険があるのかを「注意しなければならないこと」に、そして実際にどのような予防措置をとるべきかを「安全安心の為に」23 単元にまとめました。

安全安心のパソコン使用に必要な知識は？
インターネットの現状とその対策は？
被害に遭う前に必要なことは？
初心者からの質問

○各単元の構成

それぞれの単元は見開き 2 ページでからできています。左ページは概論にあたります。右ページには、それを実際に実現する具体的な方法のうち特に重要と思われるものを「安全安心への一歩」としてまとめました。

○リンクの多様

本書は、PDF ファイルからできてました。実際の操作方法や用語説明は、既にどこかで説明されていることも多きことから、信頼あるホームページにリンクしてあります。詳しく勉強する為にはインターネットに接続されているパソコンを使ってお読み下さい。

○良くある質問

各単元に、「相談内容」という項目を設けました。また、よくある相談を 1 単元にまとめ索引として使えるようにしてあります。

知識と具体的対策方法

○難易度

すぐに理解して欲しいもの、できたら理解してほしいもののメリハリを星で表示しました。初心者はすぐにすべてを理解することはできません。 ★☆☆からはじめましょう。

○認定試験

このテキストの学習度は、SPREAD サポーター認定試験で確認することができます。副読本は、情報推進機構「情報セキュリティ読本」です。

知っておかなければならにこと 「パソコン、インターネットの基礎」

注意しければならないこと 「インターネットの現状　脅威と脆弱性」

安全安心の為に、予防 「安全安心対策」

3 よくある質問

ここでは、パソコンサポータがよく受ける質問をまとめてあります。索引代わりにお使い下さい。
PDF ファイルをお使いの方は、質問をクリックすることで、解決へのアドバイスのページへ移動します。

■パソコン操作設定についての質問

■インターネットについての質問

- 無線 LAN は便利？
- ブロードバンドルーターは、セキュリティ対策になりますか？

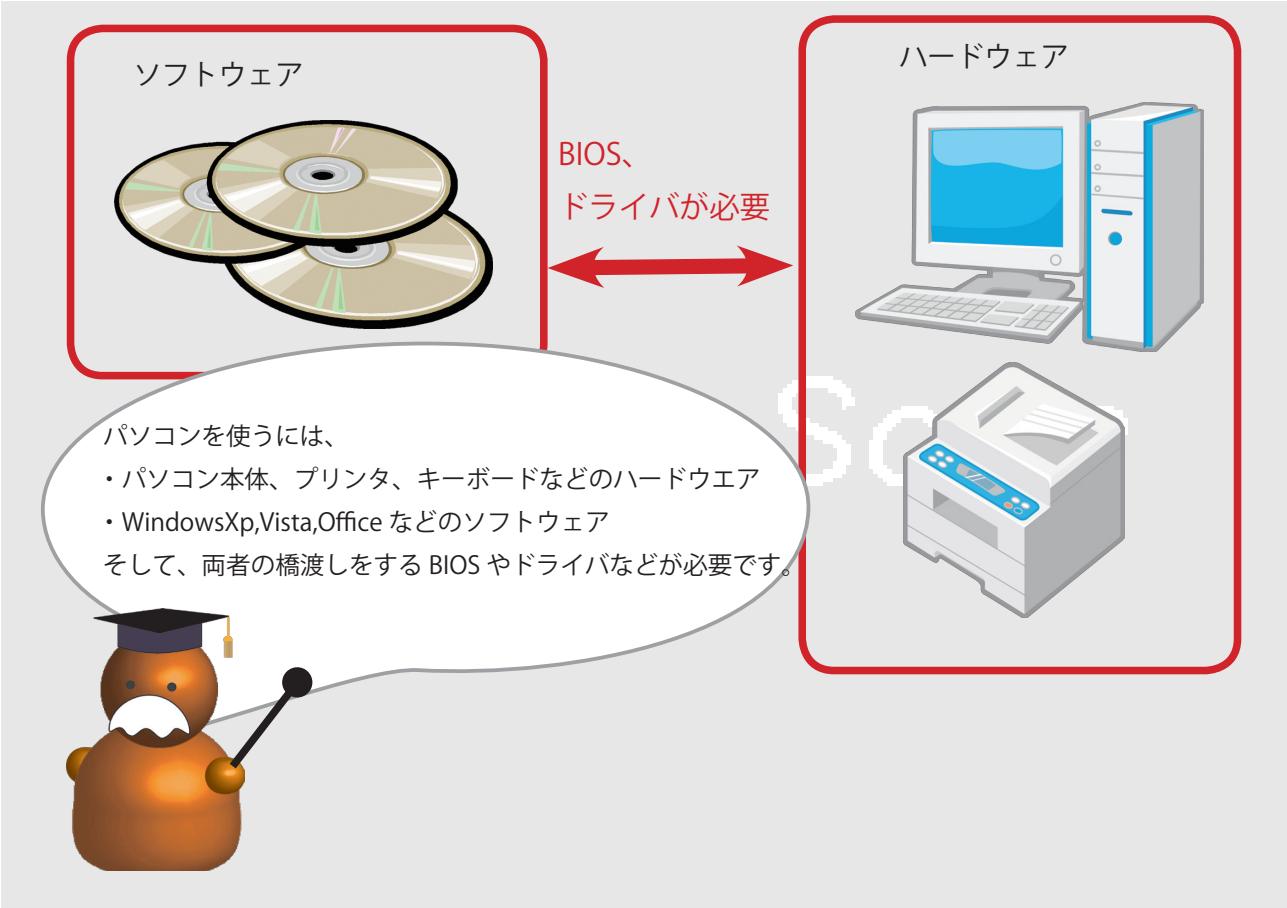
■トラブルについての質問

- インターネットはこわいのですか？
- インターネットにはどんなトラブルがあるのですか？
- インターネットを使うには、どんなことに注意すればよいでしょう？
- ホームページを見ていたら、突然「入会ありがとうございます」と表示され会費を請求された。
- クレジットカード会社からのメールにある URL をクリックしたら、クレジットカード番号を入力するホームページが現れた
- ホームページを見ていたら､突然スキャンがはじまって｢あなたのパソコンは危険です。今すぐこのセキュリティを購入してください」という表示がでた。
- 感染するとどんなことがおこりますか？
- コンピュータウィルスはどうやって感染しますか？
- インターネットに接続しないので、ウィルスには無関係です
- セキュリティ対策ソフトを入れていれば大丈夫なんですよね
- ウィルスに感染したことがありません！
- ウィルスに感染しても、特に盗られる情報はありません
- Winny で個人情報流出すると聞きました
- Winny から音楽や映画のデータを無料で入手できると聞きました
- Winny を使っていないので、安心ですよね
- 迷惑メールは、なにが「迷惑」なのですか？、迷惑メールは、ゴミメールが来るだけですよね
- 迷惑メールが多くりました。どうしたらよいでしょうか？
- 顔写真を勝手にホームページで使われました
- 地図を利用したいのですが、新聞記事をスキャンして、ホームページで公開してもよいですか？
- 私の作った画像が、勝手にホームページで使われています。
- インターネット掲示板に、誹謗中傷されました。どうしたらよいでしょう？

■安全安心対策についての質問

- ウィンドウズアップデータとを手動でやるには？、急にウィンドウズアップデートが必要になりました。
- インターネット環境にない PC に、ウィンドウズアップデートをするには？
- ウィルス対策ソフトの働きは？
- ファイアウォールとの違いは？
- 更新というのは、何を更新するの？
- 一部だけウィルススキャンしたい
- ファイアウォールって何？
- Windows ファイアウォールとの違いは？
- ファイアウォールの入手方法を教えて下さい
- ファイアウォールの設定方法、突然ネットワークにつながらなくなった、ネットワークプリンタが使用不可になった
- 暗号ってなに？
- 大切な情報はどう管理すればよいでしょう？
- バックアップのとり方 / 復元の仕方は？
- 間違えて大事なファイルを削除してしまいました
- セキュリティ対策ソフトを入れておけば十分ですよね

4 パソコンのしくみ



※パソコン
正式にはパーソナルコンピュータ(Personal Computer)。PC と略される場合もある。業務用の大型コンピュータと区別する為に、このように呼ばれます。
※ OS
オペレーションシステムの略。WindowsXp、Vista、MacOS、Linux などがこれにあたります。
※ BIOS
Basic Input/Output System の略。パソコンに接続されたディスクドライブ、キーボード、メモリなどの基本機器を制御する役割をするプログラム。パソコンに内蔵されていることがほとんどであるので、特に用意することはありません。
※アプリケーションソフト
「応用ソフト」とも呼ばれます。ワープロソフト、表計算ソフト、メールソフト、ゲームなどがこれにあたります。
※ドライバ
デバイスドライバとも呼ばれる。BIOS と同様に、OS やアプリケーションソフトがハードウェアを操作できるようにする仲介役。

私たちがメールの送受信やホームページ閲覧に通常つかったいるパソコンは、大きく分けて、機械とそれを動かすソフトウェアからできています。前者には、モニタ・キーボード・マウス、CPU と呼ばれる頭脳、情報を保存するハードディスク、メモリなどがあります。その他にも、プリンタや USB があります。これらを動かすためのプログラムをソフトウェアと呼びます。

ソフトウェアは、パソコン自体（ハードウェア）をコントロールする基本ソフト（**OS**）と、**アプリケーションソフト**からできています。アプリケーションソフトとは、文書の作成、数値計算など、ある特定の目的のために設計されたソフトウェアです。私たちがパソコンを使う場合、どちらかというと OS よりもアプリケーションに触れていることが多いです。新しいアプリケーションソフトをお店で購入し、自分でパソコンへ搭載させることができます。言い換えれば、パソコンは、その機種や OS にあうアプリケーションを入手すれば様々なことができます。そこが電卓やテレビのような決まった機能しかない機械と大きく違うところです。

また、OS とアプリケーションソフト以外に、OS やアプリケーションソフトがパソコン本体を操作可能にする「橋渡し役」として、BIOS やドライバ（またはデバイスドライバ）というプログラムがあります。これらがないと、OS やアプリケーションはハードウェアを見つけることができません。プリンタなど新しい周辺機器をパソコンに接続し印刷できるように設定するには、付属 CD-ROM が必要になります。これは、その製品のドライバが付属 CD-ROM の中に入っているからです。

相談内容

・パソコン、PC って何ですか？
・パソコンを買ったが Word が使えない
・Windows ってなんですか？
・プリンタを接続したのですが、Windows の画面には現れません。
・黒い画面になって "BIOS　Setup" とでてしまいました。

安全安心へむけての一歩

★★

ドライバの追加と変更ついて（Xp の場合）

パソコンの画面が小さい、表示色数が少ない、接続しても Windows からその装置が見えない等、その装置が正しく作動しない時は、ドライバが古いかインストールされていない可能性があります。これは、「デバイスマネージャー」で確認することができます (図 1)。図 1 の例では、「ビデオコントローラ」というドライバに問題があると？や×で表示されています。これを解消するには、そのモニタにあったデバイスドライバをインストールしてあげる必要があります。デバイスマネージャーの開き方は、http://www.microsoft.com/japan/windowsxp/pro/using/itpro/managing/devicemgr.mspx にあります。

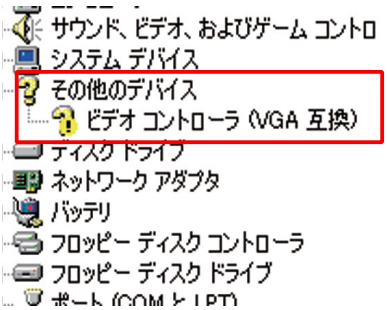


図 1 デバイスマネージャー
「ビデオコントローラ」というドライバに問題があるという表示

ドライバの入手方法

ドライバの多くは、購入したハードウェアに 付属した CD-RO 付属してます。もしそのような CD-ROM がない場合は、インターネット上で検索してから入手します。入手したら、次の方法でインストールします。

方法①セットアッププログラムから

入手したデバイスドライバに、専用のセットアッププログラム（setup.exe 等）が付属している場合には、それをダブルクリックし指示に従っていけば自動的にインストールされます。このようなセットアッププログラムがない場合には、方法②でドライバをインストールする必要があります。

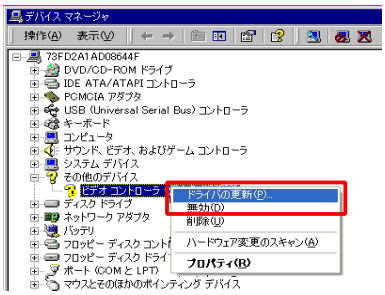


図 2 デバイスの更新

方法② Windows の「ドライバの追加と変更」

1. ハードウェアのデバイスを管理している「デバイスマネージャー」を開きます。
2. ドライバの更新

？や×が出ている装置名の上にカーソルを合わせ右クリックし「ドライバの更新」を選択すると、更新ウィザードが起動します (図 2)。

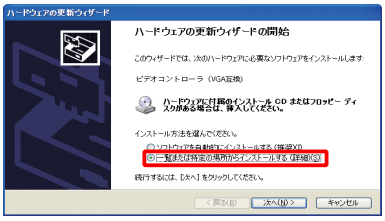


図 3 更新ウィザード

「次の場所で最適のドライバを検索する」を選択 (図 3) し、付属 CD-ROM がある場合は「リムーバブル、メディア、フロッピー、CD-ROM を検索・・・」を、インターネットなどから入手した場合は、「次をの場所を含める」にチェックを入れ (図 4)、ドライバがあるディレクトリを指定し、「次へ」。完了の表示がでれば更新は終了です。

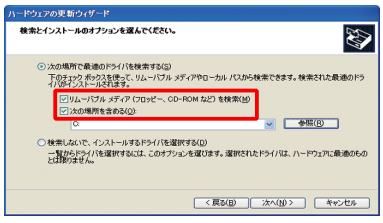


図 4 ドライバの場所を指定

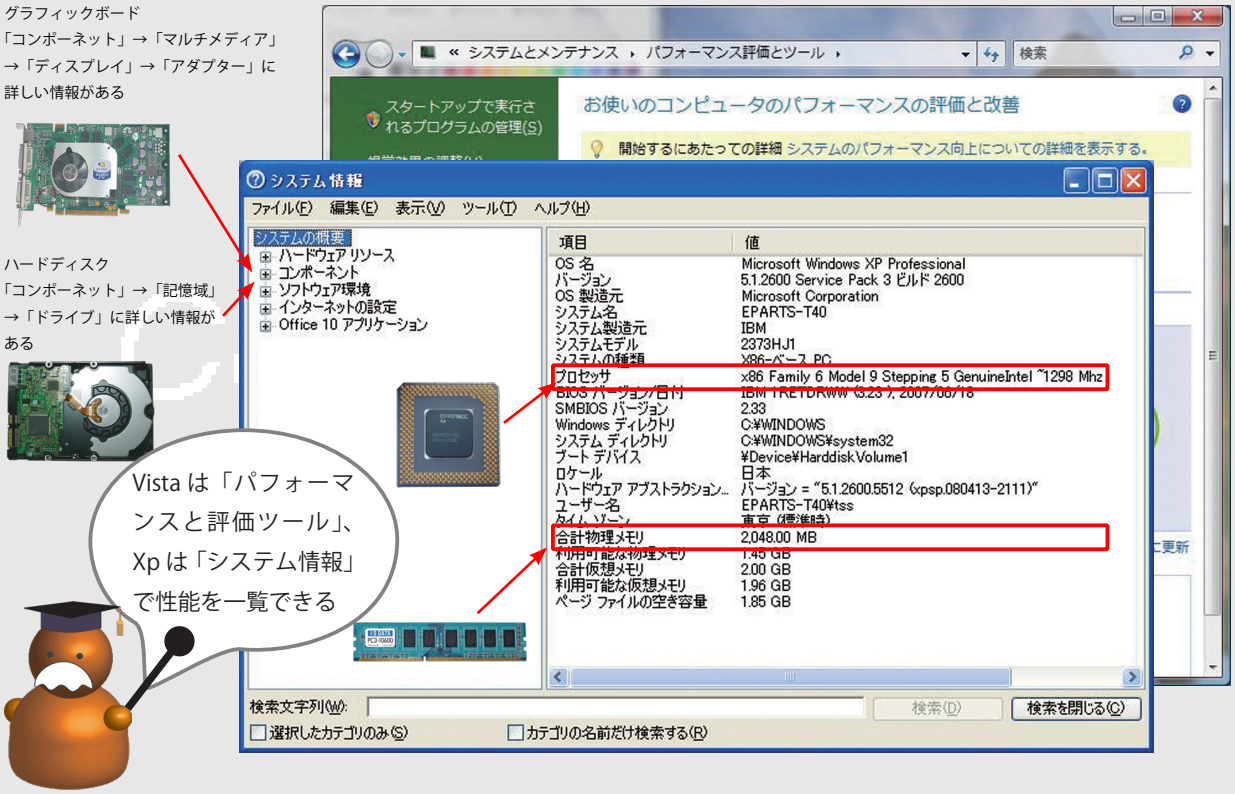
パソコンの再起動

ドライバ更新後、パソコンの再起動を指示された場合は、その通りに再起動をしてください。

Vista の　場　合　は、http://windowshelp.microsoft.com/Windows/ja-JP/help/b3c6477e-1111-4b9f-a52a-fffdc51e9c901041.mspx

5 パソコンの性能

パソコンの性能は、プロセッサ、メモリ、ハードディスク、グラフィックボードで判断しよう



※ Windows Xp 以前の「システム情報」[スタート] ボタン→ [すべてのプログラム] → [アクセサリ] → [システムツール] → [システム情報] をクリックします。

※処理速度

パソコンの処理能力が高いことを「速い」「高スペック」と呼びます。しかし、実際の処理の速さは、パソコンの性能だけではなくソフトウェアの処理能力にも関係した総合的な尺度なのです。

※ Windows Vista「パフォーマンスと評価ツール」

Vista を動かす上でこれら 4 項目がどのランクにあるか評価してくれる便利なツールです。

※ CPU

中央演算処理装置（Central Processing Unit）

※ RAM

Random Access Memory の略。半導体素子を利用した記憶装置。「メモリを増やす」というのはこの RAM を増やすことです。 PC 機種によって種類が異なりますので、増設には注意が必要です。

パソコンは、主にプロセッサ、メモリ、ハードディスク、グラフィックボードからなります。その他に CD/DVD 装置、ネットワークボード、キーボード・マウスなど多数ありますが、パソコンの処理能力つまり性能は主に前 4 つによって左右されます。特に、プロセッサ：CPU とも呼ばれます。数値計算や情報処理などを行う中枢装置です。処理の速さは「2GHz」などのクロック数で表現します。この数値が大きい程処理速度は速くなります。

メモリ：プロセッサが処理するデータを一時的に記憶する場所です。RAM という半導体が使われています。記憶できる量（記憶容量）は、GB（ギガバイト）MB（メガバイト）などの単位で表現され、その数値が大きいほど記憶する場所が広がり、データ処理は効率的となり速くなります。

ハードディスク：OS やアプリケーションソフト、作成したファイル、メールデータなどが記憶されています。電源を切ってもデータが消えない点でメモリと異なります。この容量が大きいほど、たくさんのデータが保存できるます。ハードディスク一部がメモリとしても利用されているので、容量が大きく読み書きの速度は速いほどパソコンは高速になります。容量は 200GB、回転数は 7200RPM などと表現されます。これらの数値が大きいほど高性能ということになります。くわしくは、ハードディスクメーカーのサイト（http://www.iodata.jp/promo/hdd/useful/basic/）などを参考にして下さい。

グラフィックボード：パソコンが処理した内容を表示させる為の装置です。高速に表示できた方が体感速度が向上します。ゲームなど立体画像を多用するには、それに適したグラフィックボードがあります。

相談内容

・パソコンが「はやい」ってどういうこと？
・メモリが足りませんとです。
・容量が足りません、ということはどういうこと？
・HDD の容量を増やしたい

安全安心へむけての一歩

1，性能のチェック

パソコンの性能は、Vista では「システムとメンテナンス」→「パフォーマンスとツール」でわかりやすく表示されます。Xp 以前の「システム情報」では専門的です。そこで、次の方法で、CPU、メモリ、ハードディスク容量をなどを簡単に確認することができます。

プロセッサの速度、メモリ容量の確認方法

「マイコンピューター」上にカーソルを合わせ右クリックし「プロパティ」を選択します。「全般」タブを開きます。ウィンドウの右下に「コンピュータ」という記載があり、そこにプロセッサの種類と速さ、メモリ容量が表示されています（図 1）。

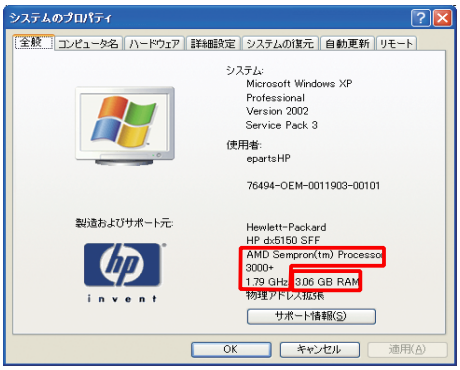


図 1 システムプロパティ
プロセッサ 1.79GHz、メモリ 3.06GB と表示されている。

ハードディスクの容量チェック

マイコンピューターを開き「ローカルディスク」を右クリックし「プロパティ」を選びます。「全般」タグにハードディスクの使用領域と空き領域が色別に表示されます（図 2）。詳しくは、http://support.microsoft.com/kb/882787/JA/。

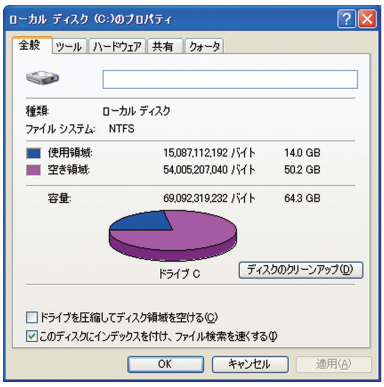


図 2 ディスクのプロパティ

2，ハードディスクの容量確保（ディスクの交換、ディスクのクリーンアップ）

ハードディスクは無限ではありません。空き容量が不足すると新しいアプリケーションソフトをインストールできない、パソコンが遅くなるという現象がおこります。そのような場合は、ハードディスクを別途購入し交換する、または増設することが必要になります。その前に、「ディスクのクリーンアップ」で不用なファイルを整理してみると意外と空き容量が増えることがあります（図 3）。
詳しくは、http://support.microsoft.com/kb/310312/ja。

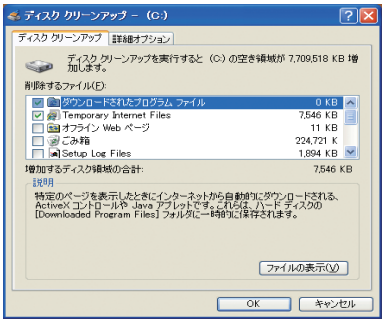


図 3 ディスクのプロパティ

3，ハードディスクの最適化

ファイルの保存・移動・削除等を繰り返していくうちに、ハードディスク内のデータがバラバラに保存されるようになり、読み書きに時間がかかるようになります。そこで同じデータはできるだけ近所に置き換えることで読み書きを速くすることができます。これを「ハードディスクの最適化」と言います。詳しくは、http://support.microsoft.com/kb/882792/ja を参照して下さい（図 4）。
Vista では、通常使用している折に自動的に最適化できるように設定可能です。手動の場合は、「コンピュータ」を右クリック→「プロパティ」→「ツール」→「最適化」を開き「最適化する」で実行できます。

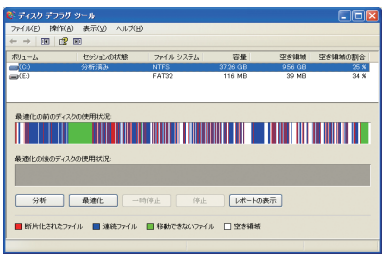
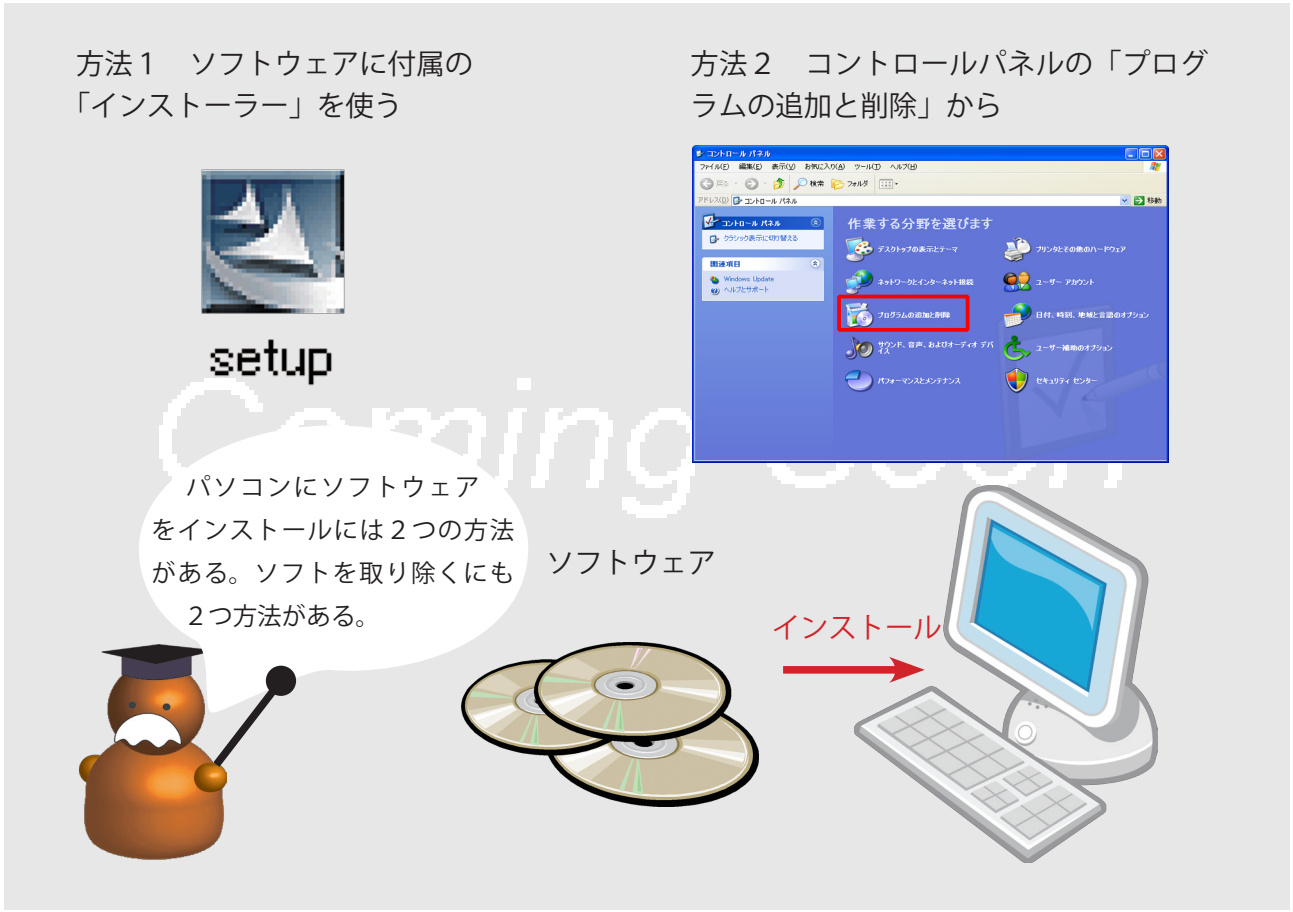


図 4 ディスクの最適化

6 ソフトウェアの追加と削除



※ダウンロード
インターネットなどのネットワーク上にあるコンピュータから、データを自分のパソコンに転送し保存すること。

米 Windws2000 以前は「プログラムの追加と削除」は「アプリケーションの追加と削除」となっています。

※「プログラムの追加と削除」が必要なものとして、Fax サービス、Outlook Express、Windows Media Player、Windows Messenger、Windows に付属しているゲームなどがあります。

ソフトウェアを購入した、ネットワークからダウンロードした、次は、それを自分のパソコンに組み込まなければなりません。この作業を「インストール」または「セットアップ」と言います。方法は大きく分けて２つあります。

A）ソフトウェアに「インストーラー」「セットアッププログラム」が付属している場合は、それらをダブルクリックするなどし実行するとインストールが始まります。後は指示に従っていけば大概完了します。

B）Windows の「コントロールパネル」の中にある「プログラムの追加と削除」を使います。

通常は A）を使うと便利ですが、中には B）でしかできない場合もあります。

インストールとは逆に、不用になったソフトウェアを削除したい時があります。この作業は「アンインストール」と言います。通常の場合、不用なソフトウェアのフォルダをゴミ箱に入れても完全にはアンインストールされません。ソフトウェアの設定がいろいろな場所でされているからです。完全にインストールするにも、２つの方法があります。

C）ソフトウェアに付属している削除ソフト「アンインストーラー」を実行します。指示に従ってクリックしていけば、ソフトウェアを削除し、パソコンの設定も元に戻してくれます。

D）Windows の「コントロールパネル」の中にある「プログラムの追加と削除」を使います。

削除の時も通常は C）を使います。

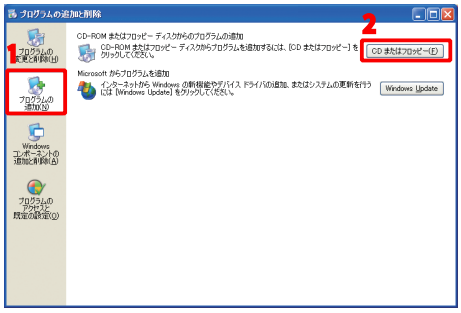
相談内容

・インストールってなんですか？
・不用になったプログラムを削除したいのですが
・フォルダを削除してもプログラムが完全に消えないのですが
・HDD の容量を増やしたい

安全安心へむけての一歩

ソフトウェアの追加と削除は、そのソフトウェアに付属している専用プログラム「インストーラー（セットアッププログラム）」「アンインストーラー」を用いるのが通常ですが、中には Windows の「プログラムの追加と削除」を使わなければならない場合もあります。ここではこれについて説明します。なお、これらの作業は「コンピュータの管理者」でないとできない場合があります。ここでは、Xp の例で説明します。

プログラムの追加

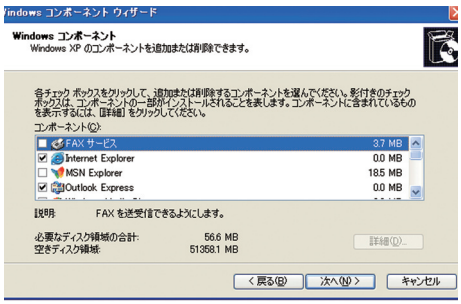


1.「コントロールパネル」→「プログラムの追加と削除」→「プログラムの追加」を選びます。
　ウィンドウ左のメニューから「プログラムの追加」を選びます。
2.「CD-ROM またはフロッピーディスクからのプログラムの追加」の「CD またはフロッピーディスク」をクリック
　指示に従って進みます。CD やフロッピーが入っていない場合は、「参照」でプログラムが保管されている場所を選ぶ必要があります。

プログラムの削除

1.「プログラムの変更と削除」を選ぶ
「コントロールパネル」の「プログラムの追加と削除」から「プログラムの変更と削除」を選びます。
2. 削除したいプログラムを選ぶ
3.「削除」をクリック
　後は指示に従って進めば削除できます。途中で「・・は他のプログラムで使われている場合があります」というメッセージが出ることがあります。もし不安でしたら「削除しない」を選んで進んで下さい。

Windows コンポーネットウィザード



Fax サ　ー　ビ　ス、Outlook Express、Windows Media Player、Windows Messenger の追加と削除は、「プログラムの追加と削除」の中の「Windws コンポーネットの追加と削除」で行います。チェックを付いているものがインストールされているものです。これは「コンピュータの管理者以外は実行できません。

Vista の場合は、「プログラムの機能」から「プログラムの追加と削除を選びます。

関連する事項

・ユーザアカウントの設定

重要用語

インストール、アンインストール、セットアップ
コントロールパネル「プログラムの追加と削除」

7 パソコンを自分流に設定する

※スタンバイ
　いちいち OS やアプリケーションソフトの終了や起動を行なう場合よりも時間や手間がかからず、消費電力も抑えることができます。

※休止状態
　休止状態になると、コンピュータはメモリ上のデータをすべて保存し電源を落とします。これを設定するには、「コンピュータの管理者」でなければなりません。「コンピュータの管理者」については、「パソコン利用者の設定」を参照して下さい。

コントロールパネルの機能を使って、パソコンを自分流に設定できます。
主に、背景の設定、文字の大きさの設定、スクリーンセーバーの設定、電源の設定ができます。
A) コントロールパネルの「デスクトップのテーマと表示」をクリックし、「デスクトップの背景を変更する」をクリックし、背景から自分の好みの壁紙を選択できます。また、自分でとった写真などを壁紙に設定したい場合は、「参照」ボタンを押し、対象となる画像を選択することができます。
B) 文字の表示を大きくしたい場合は、A) の画面上部にあるデザインタブをクリックし、フォントサイズのリストボックスを標準から、大きいフォントまたは、特大フォントに変更することによって、画面上の文字表示を大きくすることができます。
C) スクリーンセーバーの設定ができます。これは、ユーザがコンピュータを使用していない間、画面を黒くしたり、簡単なアニメーションを表示するソフトウェア。表示されている文字などや画像が CRT ディスプレイに焼きつくのを防止するためのものです。
D) 電源の設定では、スタンバイ、休止状態といった状態の設定ができます。
この手続きを行うことによって消費電力を抑えることができます。

C)D) は、ただ便利な機能だけではなく、スクリーンセイバーやスタンバイから復帰した時にパスワード入力が必要なように設定できます。これによって、第三者からパソコンを操作されるのを防ぎます。

相談内容

・文字を大きくしたい
・背景を変えたい
・スクリーンセイバー設定したい
・電源の設定をしたい
・スタンバイ、休止状態の設定がしたい。

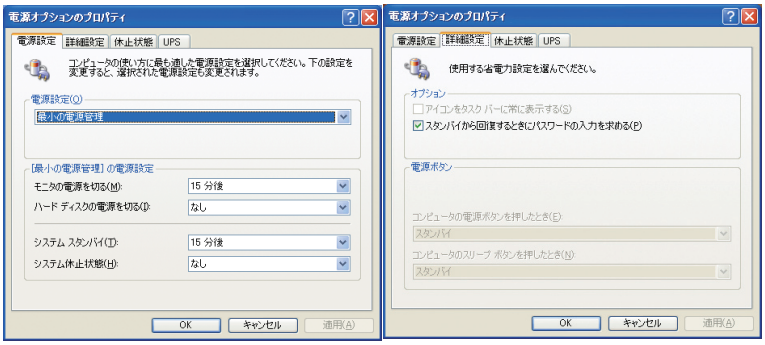
安全安心へむけての一歩

一定時間ユーザがコンピュータを使用していない場合の設定として、スクリーンセーバー、スタンバイ、休止状態の設定を行うことができます。それぞれ再開時に、パスワードの入力を求めるよう設定ができます。
以下は Xp での説明です。Vista では「コントロールパネル」から「個人設定」で以下の設定を行います。

スクリーンセーバーの設定

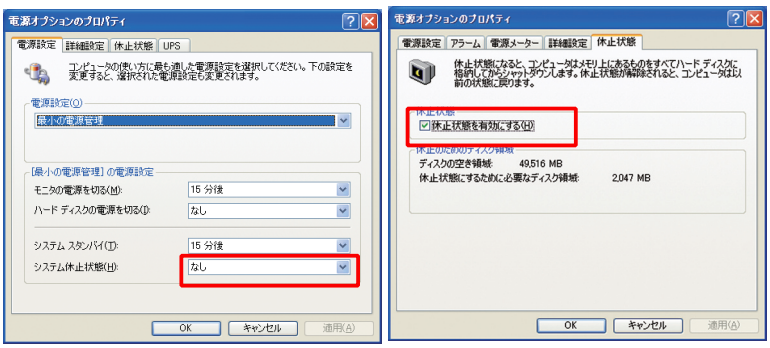
1．「コントロールパネル」→「デスクトップの表示とテーマ」→「スクリーンセーバーを選択する」を選びます。
2．スクリーンセーバーの表示時間と、表示画像の設定ができます。
3．「再開時にようこそ画面に戻る」にチェックを入れると、スクリーンセーバーを解除すると、ようこそ画面に戻り、パスワード入力が必要になります。

スタンバイの設定



1.「コントロールパネル」→「パフォーマンスとメンテナンス」→「電源オプション」→「電源設定タブ」を選びます。
システムスタンバイの時間を設定ができます。
2. スタンバイから回復時にパスワードの入力を求めるよう設定
「詳細設定タブ」を選びます。オプションの「スタンバイから回復するときにパスワードの入力を求める」のチェックボックスにチェックを入れると、回復時にパスワート入力が必要なように背一定ができます。

休止状態（ハイバネーション）の設定



1.「コントロールパネル」→「パフォーマンスとメンテナンス」→「電源オプション」を選び、「電源設定」タブを選び「システム休止状態」までの時間を設定します
2.「休止状態タブ」を選びます。「休止状態を有効にする」のチェックボックスにチェックを入れると、設定した時間で休止状態になるよう設定ができます。

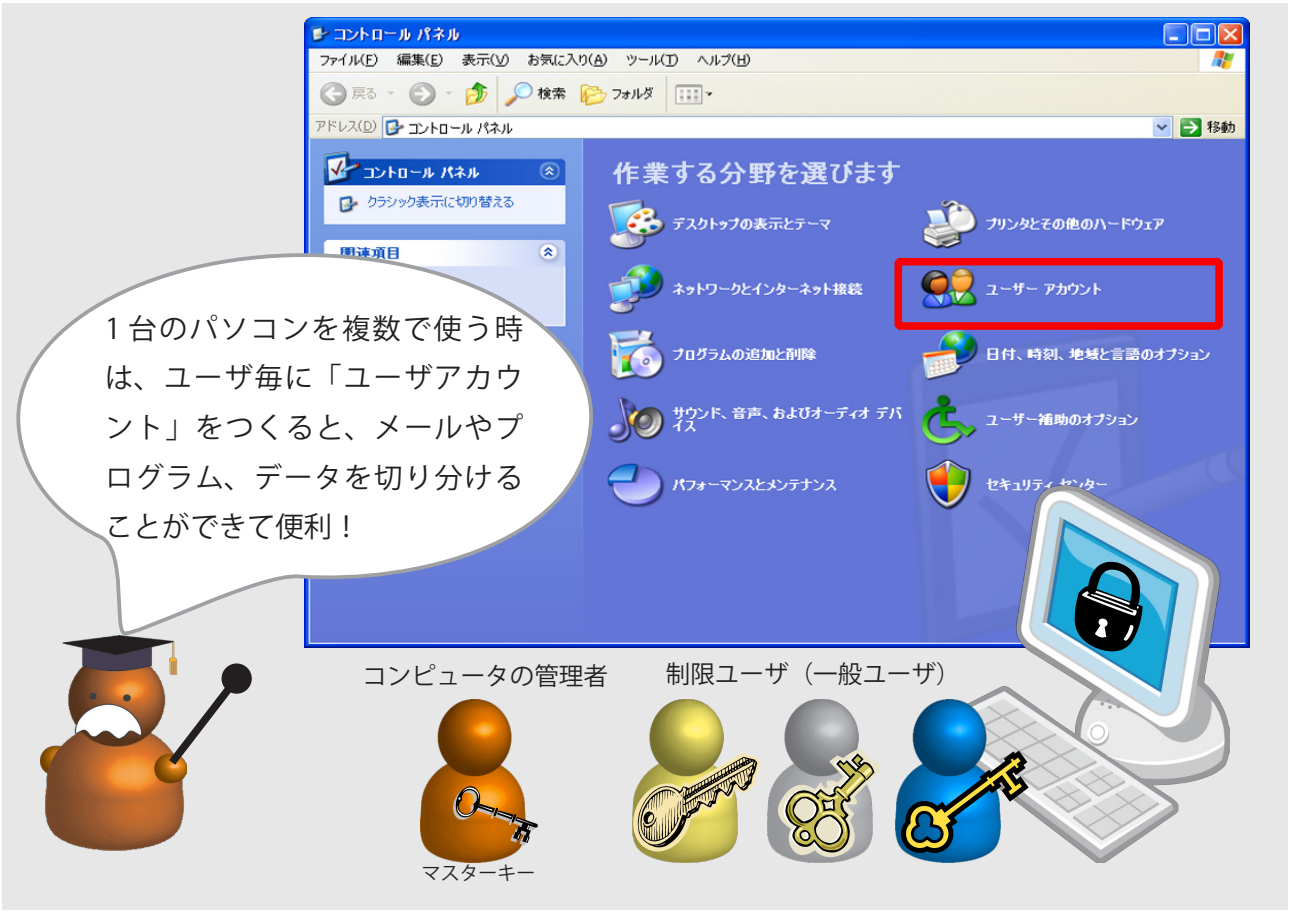
関連する事項

・パソコンの利用者の設定　コンピュータの管理者と制限ユーザ

重要用語

スクリーンセーバー、スタンバイ、休止状態、パスワードの設定

8 パソコンの利用者の設定
コンピュータの管理者と制限ユーザ



※ユーザアカウント
　ID と同意義です。

※ログイン
　ログオン、サインオン、サインインとも呼ばれます。コンピュータのシステムに対して、個人を識別させ利用できる状態にすることをいいます。

※管理者と一般ユーザ
WindowsXP では「コンピュータの管理者」と「制限ユーザ」、Vista では「コンピュータの管理者」と「標準ユーザ」と呼ばれています。

1 台のパソコンを家族みんなで使いたい、しかし、メールは見られたくない。壁紙も自分用にしたい。家族共有のパソコンを個人専用に使いたい。そんな時は、コントロールパネルの「ユーザーアカウント」で家族それぞれユーザを作成しましょう。これによって、1 台のパソコンを切り分けて使うことができます。

ユーザアカウント毎にできること
- メールの設定とメールの送受信
- 壁紙などの設定
- スクリーンセーバーの設定
- ログインパスワードの設定
- アプリケーションのインストールと設定

※セキュリティ対策ソフト、Office など PC 全体で使う場合は、ユーザ毎にインストールはできません。

ユーザの種類
パソコンのユーザには、管理者と一般ユーザとの違いがあります。管理者はパソコンの隅々まで管理できる権限を持ちます。パソコン全体でつかうようなソフトウェアのインストールや設定、ユーザの追加や削除、すべてのユーザのパスワードの変更など強い権限を持ちます。これに対して一般ユーザは、自分の使用範囲以外の設定はできません。

相談内容

・１台のパソコンを家族で使いたい
・パスワードを変更したい / 忘れてしまった
・新しいアカウントを作りたい
・コンピュータの管理者って何ですか？
・どうすれば管理者になれますか？

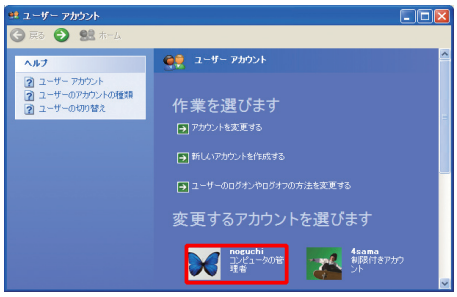
安全安心へむけての一歩

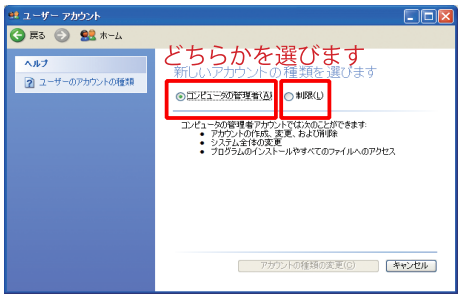
ここでは、コンピュータ管理者の権限でできる「他ユーザのパスワードの変更」「アカウントの種類の変更」「新しいアカウントの作成」について説明します。ここでは Xp に沿って説明しますが、Vista でもほぼ同じ工程となります。

他ユーザのパスワードの変更

1, コントロールパネルの「ユーザーアカウント」からパスワードを変更したいユーザを選びクリックします。
2,「パスワードを変更する」をクリックします。
3, 新しいパスワードを確認の為 2 回入力し「パスワードの変更を」クリックします。古いパスワードを知らなくても強制的に新しいパスワードを設定できます。
詳しい手順は、http://www.spread-j.org/sheet/2006/07/14windows_xp.html

アカウントの種類の変更





１．「コンピュータの管理者権限」を持つユーザで、「コントロールパネル」→「ユーザアカウント」へ進み、変更したいユーザのアカウントを選びます。
２．選択した「コンピュータの管理者」か「制限」を選ぶことができます。
選択できるユーザの内容は下記の通りです。
・コンピュータの管理者
「アカウントの作成、変更、削除」、「システム全体の変更」、「プログラムのインストールやすべてのファイルへのアクセス」が、できます。
・制限付きアカウント
「パスワードの変更、削除」、「作成したファイルの参照」、「画像、テーマ、デスクトップの設定の変更」、「共有フォルダの参照」が、できます。

新しいアカウントの作成

1.「コンピュータの管理者権限」を持つユーザで、「コントロールパネル」→「ユーザアカウント」→「新しいアカウントを作成する」を選びます。
2. 新しいアカウントに名前を付けます。
3. アカウントの種類を選びます。「コンピュータの管理者」と「制限」の２種類のアカウントを選ぶことができます。
詳しい手順は、http://support.microsoft.com/kb/880455/ja
Vista では、「別のアカウントを管理」→「新しいアカウントの作成」を選び上と同様な作業を行います。

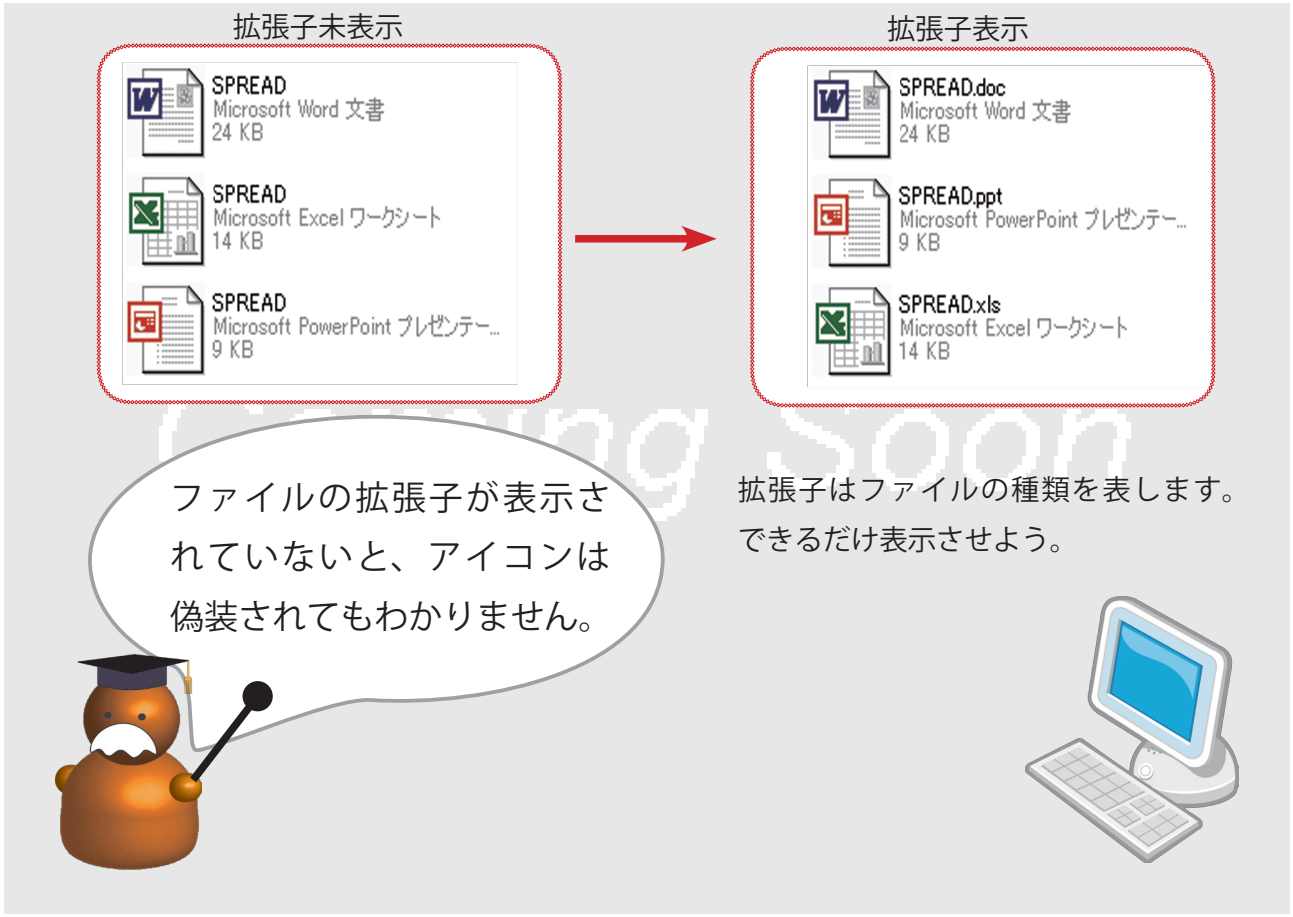
関連する事項

・パソコンを自分流に設定する

重要用語

アカウントの作成、アカウントの変更、コンピュータの管理者、制限付きアカウント

9 表示の設定　拡張子や隠しファイルの表示



※拡張子
ファイル名のピリオド「.」で区切られた一番右側の部分。
例えば、spreadText.doc ではれば「doc」の部分、spreadText.doc.pdf であれば「pdf」の部分で、そのファイルの種類を示す。

※隠しファイル
http://support.microsoft.com/kb/878601/ja
USB や CD-ROM をパソコンに入れただけで中身が表示されるのは、Autorun.inf という隠しファイルによって特定のファイルが起動されることによる。

隠しプログラムやシステムファイルの表示方法
http://www.microsoft.com/japan/windowsxp/pro/using/tips/personalize/hiddenfiles.mspx

A. 拡張子の表示

Windows では、.doc .xls などファイルの拡張子が標準では表示されません。そこで、私たちは、アイコンで、Word の文書、Excel のワークシート、メモ帳のテキストと区別しています。しかし、Windows は、ファイルについている拡張子でファイルスの種類を判別しています。主な拡張子には以下のようなものがあります。

主な拡張子

Excel ファイル	xls, xlsx	Word ファイル	doc, docx
PowerPoint ファイル	ppt, pptx	テキスト、メモ帳	txt
画像ファイル	bmp,jpg,gif,png 等	音声ファイル	wma,wav,mp3,mid
動画ファイル	wmv, mpg, mp4	ホームページファイル	html
圧縮ファイル	lhz, zip, rar	実行ファイル	exe, com

これらの拡張子と、Word や Excel などのアプリケーションが登録されているので、アイコンをダブルクリックしたいだけで自動的にアプリケーションが起動して、そのファイルが開くのです。

B. 隠しファイル

Windows ではいくつかのプログラムやシステムファイルが見えないようになっています。これは、ユーザが誤って削除しないようにという配慮からです。しかし、必要に応じて表示しなければならないことあります。日頃は隠しておいても表示の仕方は覚えておきましょう。

相談内容

・拡張子とは何ですか？
・拡張子が表示されません。
・Word 文書のはずなのですが、アイコンが変わってしまった。ダブルクリックしても開きません。
・あるはずのファイルが見あたりません。
・隠しファイルを表示させるにはどうしたよいでしょう？

安全安心へむけての一歩

ここでは、WindowsXp における「拡張子の表示非表示方法」と「アプリケーションとの関連づけ」について説明します。

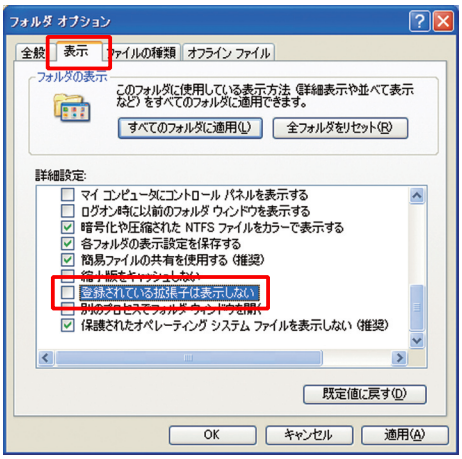


図 1　拡張子の表示・非表示の設定

拡張子の表示 / 非表示の方法

0. コンピュータの管理者でログインします。
1.「マイコンピュータ」などのフォルダをクリックしエクスプローラーで開きます。タイトルメニューの「ツール」から「フォルダオプション」を選びます。
2.「表示」タグを選び、中央「詳細設定」の「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。「適用」をクリックすることで、ファイルの拡張子が表示されます。チェックを入れることで拡張子は隠されます。

WindowsXp の場合　http://support.microsoft.com/kb/882195/ja
Windows Vista の 場 合　http://windowshelp.microsoft.com/Windows/ja-JP/help/a0b4607a-6fa8-42ab-aef6-7418183389da1041.mspx

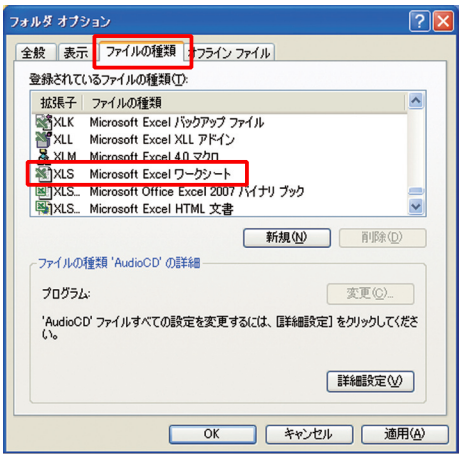


図 2　拡張子とアプリケーションとの関連づけを設定できる。「新規」をクリックし、「TXT」を Word 文書のファイルとし登録すると、アイコンも変わり、クリックすると Word で開くようになる

アプリケーションとの関連づけ
1. コンピュータの管理者でログインします。
2.「マイコンピュータ」などのフォルダをクリックしエクスプローラーで開きます。タイトルメニューの「ツール」から「フォルダオプション」を選びます。
3.「ファイルの種類」タグを選びます。、「登録されているファイルの種類」には拡張子とそれに関連づけられているアプリケーションが表示されています。例えば、「XLS」は「Microsoft Excel ワークシート」のファイルとして登録されています。ですので、拡張子 XLS のファイルをクリックすると Excel が起動するのです。「新規」で拡張子とアプリケーションの新たな関係づけをつくることも、「削除」で関係を解消することもできます。

関連する事項

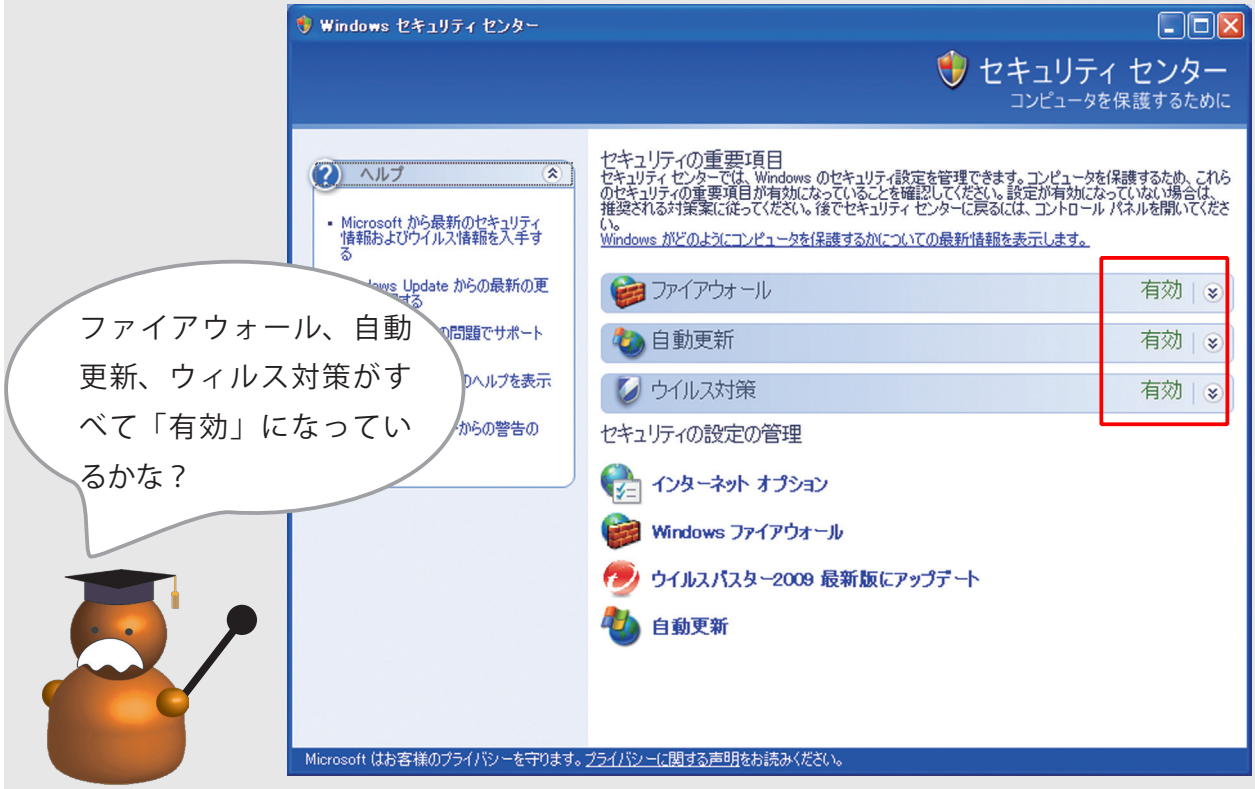
◎悪意あるソフトウェア（マルウェア）　アイコンの偽装
◎

重要用語

LAN、NAT、グローバルアドレス、プライベートアドレス

10 パソコンを守るしくみ

いろいろやるべきことはあります。まずはセキュリティセンターからはじめよう。



※セキュリティホール
国民の為の情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k01_hole.htm

※ブラウザには、一時ファイル、履歴、Cookie、保存されたパスワード、および Web フォームの情報などに個人情報が含まれる場合があります。Internet Explorer の場合、これらは「インターネットオプション」で削除できます。例えば閲覧履歴の消去方法は、http://windowshelp.microsoft.com/Windows/ja-JP/help/71a6a0e1-5f93-4bf8-aeb8-595d45dfd4a01041.mspx。

※セキュリティ対策ソフトの活用は、「21, 安全安心対策：ウイルス対策ソフト」p.41、「22, 安全安心対策：ファイアウォールの種類と働き」p.43 を参照。

※暗号については「23、安全安心対策：暗号の活用」p.45 を参照。

※バックアップについては、「24、安全安心対策：バックアップ」p.47 を参照。

インターネットで様々なトラブルが増えています。外部からネットワークを通して自分のパソコンが勝手に操作されたり、大事な情報が盗まれたり消されたりします。また、うっかりしてパソコンを壊してしまうこともあるでしょう。そのようなことがないように、パソコンとその中の情報を守る必要があります。

パソコンや情報を守るには、次のことをしなければなりません。

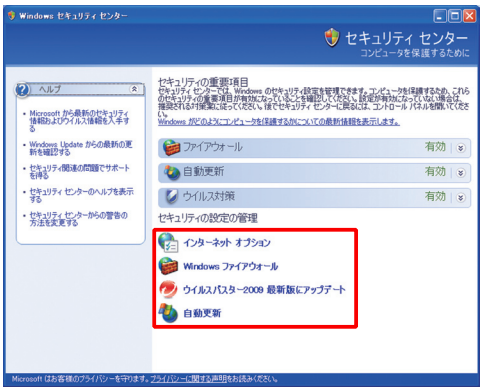
A) パソコンの基本ソフトウェア（OS）を最新のものにする。
B) Word や Excel、ブラウザなどのソフトウェアを最新のものにする。
C) OS に付属している簡易型ファイアウォールを使う。
D) セキュリティ対策ソフトを入れマルウェア対策をする。そしてその対策ソフトを最新のものにする。
E) 個人情報などが漏れたり悪用されないように、履歴から消す。
F) 大事な情報はパスワードかけたり暗号化して第三者が読めないようにしておく。
G) 大事な情報を定期的にバックアップする。
H) パソコン、ID やパスワードはしっかり管理しましょう。
I) 信頼できるホームページか、ファイルか、パソコンかチェックしましょう。

A),B) はソフトウェアのセキュリティ上弱い点（セキュリティホールと言います）を修正します。 C),D) は外部からパソコンが操作されたり、ウィルスなどの悪意あるプログラムをインストールされるのを防ぎます。

相談内容

・インターネットをすると情報がとられると聞いたのですが
・インターネットは怖いんですか？
・まず何から始めたらよいでしょう？

安全安心へむけての一歩



パソコンや情報を守る為にすべきことはたくさんあります。
それぞれの OS には、セキュリティを設定できる機能が付属しています。まずそこからはじめましょう。ここでは Windows の「セキュリティセンター」について説明します。（ここでは WindowsXp のセキュリティセンターを扱います）「セキュリティセンター」への入り口は「コントロールパネル」にあり、左ページの A) ～ D) に関係することを設定できます。

Windows の「セキュリティセンター」の活用

1.Windows のアップデートを自動的に行う「自動更新」（A 関連 ）
パソコンの基本ソフトウェア（OS) を最新のものにするには、Microsoft から提供される修正プログラムを入手しインストールする必要があります。いつ提供されるかわかりにくいので自動化する機能です。これを「有効」しておきましょう。自動更新にはいくつかパターンがあります。一番自分に合ったものを選びましょう。くわしくは、http://www.spread-j.org/sheet/2006/07/03microsoft_updatexp.html。

2.Internet Explorer の「セキュリティ」の設定 (B 関連)
Internet Explorer には AtiveX コントロール、Java アプレット、JavaScript、Cookie の受け入れを制限できる機能があります。「インターネットオプション」はそのレベルを設定できます。詳しくは、以下を参照してください。
http://www.spread-j.org/sheet/2006/07/16internet_explorer_60.html
http://www.microsoft.com/japan/windows/ie/using/howto/security/settings.mspx

3.**「Windows ファイアウォール」の設定** (C 関連)
「ファイアウォール」は、外部から PC が操作されること等を防ぐ機能です。「有効」にしておきましょう。セキュリティ対策ソフトを新たに導入した場合など安全性が確かめられた場合には「無効」にしてもかまいません。「有効」「無効」の切り替えは「Windows ファイアウォール」をクリックして行います。また「ファイアウォール」を有効した為、外部とのデータ通信やあるプログラムが起動しなくなる可能性があります。その時は、その通信やプログラムを「例外」扱いとして通信を遮断しない設定もできます。詳しくは、http://www.microsoft.com/japan/windowsxp/using/security/internet/sp2_wfexceptions.mspx。さらに詳しくはこちら

4. セキュリティ対策ソフトの確認と設定 (D 関連)
市販のセキュリティ対策ソフトがインストールされていると、「ウィルス対策」が「有効」となります。また画面下の「セキュリティの設定の管理」にそのセキュリティ対策ソフトの設定への入り口が明示されます。ここでは、「ウィルスバスター 2009 最新版にアップデート」となっています。それぞれの設定の仕方は、ソフトウェアによってことなります。

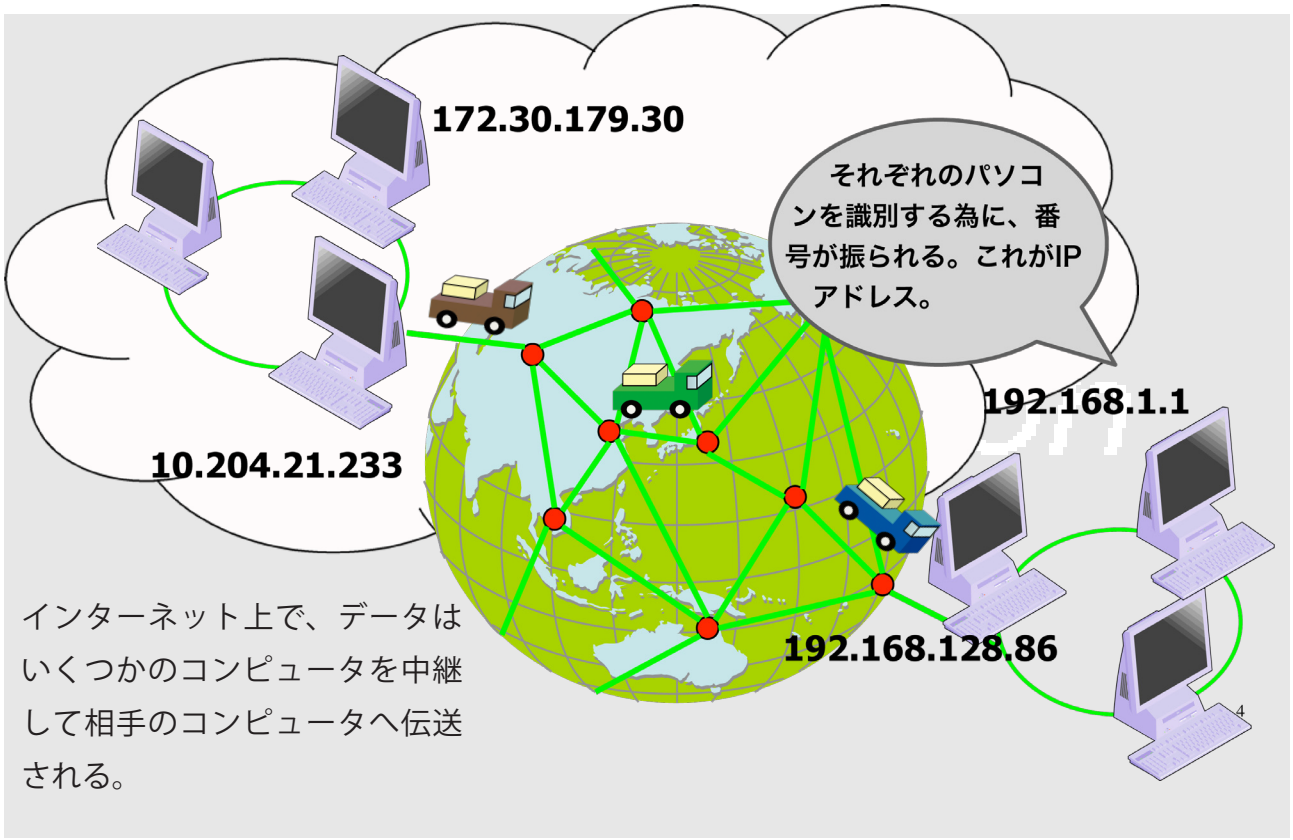
関連する事項

◎ 20、安全安心対策：ソフトウェアのアップデート、p.39
◎ 21、安全安心対策：ウイルス対策ソフト、p41
◎ 22、安全安心対策：ファイアウォールの種類と働き、p43

重要用語

セキュリティホール、Windows Update、セキュリティ対策ソフト、ファイアウォール

11 インターネット、ホームページ、メールのしくみ



※通信手順
通信プロトコルともいい、通信の為に相互に決められた約束事のこと。インターネットでは、TCP/IP というコンピュータの機種に依存しない手順が採用されている。

※プロバイダ
インターネット接続業者。電話回線、ISDN 回線、ADSL 回線、光回線、CATV 回線、無線などを通じて、企業や家庭のコンピュータをインターネットに接続する。

※ P2P
Peer To Peer（ピアツーピア）の略。特定のサーバなしに、ユーザ同士がデータを転送しあうしくみ。Winny などがこれにあたる。くわしくは、http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/yougo/eiji.htm#p

※特に、公衆無線 LAN やホテルのインターネットサービスなど公共の場所でインターネットを利用する場合は、盗聴の可能性はかなり高いと思われます。

インターネットは、共通の通信手順を用いて、世界中のコンピュータネットワークを相互につないだものです。そのネットワークを利用して、様々な情報発信や情報収集そしてコミュニケーションが行われています。個人でインターネットへ直接接続することはできません。プロバイダとよばれる業者と契約して接続してもらう必要があります。

最近では、自由に日記・写真・動画が投稿できるサービスあります。これらのサービスは有料無料のものがあり、それぞれの用途や目的に合わせて選択するとよいでしょう。インターネット上のこのようなサービスは、「サーバ」という様々なサービスを提供してくれるコンピュータと「クライアント」と呼ばれるサービスを受けるものと間でなされます。最近ではサーバとクライアントとの明確な区別がなく、対等な関係でデータのやりとりをする P2P 通信も盛んになってきました。

インターネットの仕組みや様々なサービスについてのくわしい説明は以下を参照して下さい。

総務省「国民のための情報セキュリティサイト、インターネットっ何？」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k01.htm

インターネット上では、データをパケットという形に分割しての通信しています。パケットは、手元の PC から相手のコンピュータへ直接届くわけではなく、いくつかのコンピュータを通過します。その中に、パケットの中身を「盗聴」できるコンピュータが存在する可能性も否定できません。パケットにメール内容やパスワード、クレジットカード番号などが含まれている場合は危険です。インターネットは便利ではあるが、その一方でいくつかの危険性を持っていることに注意しましょう。

相談内容

・インターネットって何ですか？
・何ができますか？
・インターネットするにはどうしたらいいのか？
・ホームページを見ることができません
・メールができません

安全安心へむけての一歩

★★☆

ホームページを閲覧できない場合

いろいろな原因がかんがえられます。
まず、ケーブルがきちんと接続されているか、ルータやハブなどのネットワーク機器の電源が入っているか、正しく接続されているかを確認しましょう。もしそれらが正しい場合はパソコン設定に問題があると考えられる。Windows では「ネットワークセットアップウィザード」（図 1）を実行してみるとよいでしょう。ネットワーク機器の接続やパソコンの設定などは、プロバイダ毎に設定の仕方が異なることが多いので、きちんとプロバイダのホームページで設定方法を確認しましょう。それでもホームページが閲覧できない場合は、ファイアウォールの設定を疑ってみるのもひとつです。

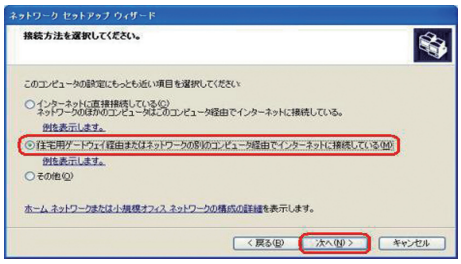


図 1 ネットワークセットアップウィザード
赤枠はブロードバンドルータなどを使った場合

メールの送受信ができない場合

まず、ID とパスワードが正しいかどうか確認しましょう。次に SMTP サーバ名と POP サーバ名に間違いがないか確認して下さい。メールを送受信するには、メールソフトに SMTP サーバと POP サーバをきちんと登録しなければならなりません。次にポート番号や暗号形式などの設定に間違いがないか確認しましょう。それぞれの設定の仕方は各プロバイダのホームページに掲載されているので、それを参考にしましょう。ここでは 2 つほど例をあげます。

KDDI の場合　http://www.auone-net.jp/support/mail/index.html
OCN の場合　http://help.ocn.ne.jp/ols/menu/mail/50001_m_mail.html

メールサーバのセキュリティ

SMTP サーバは、自分が契約しているもの以外でも使うことができました。これが迷惑メールの発信に利用されました。そこで最近では、契約者以外は使えないようにサーバに制限をかけるようになりました。その方法は、メールを受信した後数分間だけ送信可能とするもの（POP before SMTP）、送信時に ID とパスワードでの認証を必要とするものなどがあります。最近では後者が多くなった。また、メールは暗号化されずに転送されるので、第三者からその内容を読まれる可能性があります。そこでクライアントとメールサーバ間の通路を暗号化するしくみ（SMTP over SSL、POP over SSL) も普及してきました。これを利用するには、メールソフトとプロバイダがこのしくみに対応していることが前提条件になります。設定方法はプロバイダ毎に異なります。ご自身が契約しているプロバイダのホームページで確認しましょう。上以外に、メールは発信元を偽装しやすいという脆弱性もあり、なりすましの温床として懸念されている。

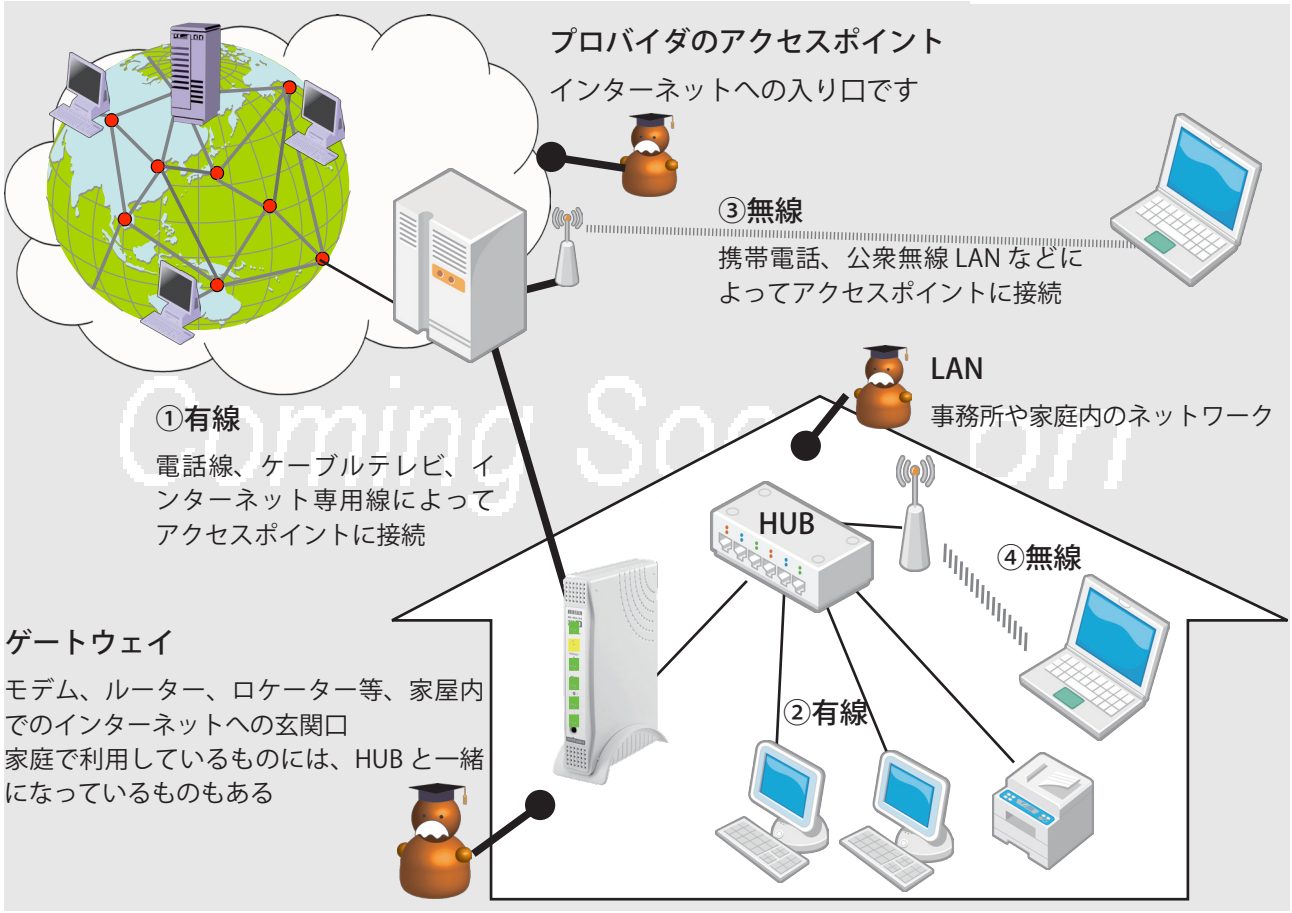
関連する事項

○ 13、インターネットが抱える問題、p.25
○ 12、様々なネットワーク、p.23
○ 23、安全安心対策：暗号の活用、p.45

重要用語

インターネット、通信プロトコル、プロバイダ、POP サーバ、SMTP サーバ、POP before SMTP、SMTP over SSL、POP over SSL

12 様々なネットワーク



インターネットを利用するには、プロバイダと契約しプロバイダのアクセスポイントに接続しなければなりません。そして、どのような機器を使ってインターネットに接続するかも決めなければなりません。一般的には、次の方法があります。

有線で接続

①電話線、ケーブルテレビ、インターネット専用線などを使ってインターネットに接続します。それぞれの線は金属や光ファイバーが主です。②パソコンのネットワークケーブルをモデム、ロケーター、ルーターなどの機器へ差し込みアクセスポイントに接続します。

無線で接続

③携帯電話や PHS などの機能をもつ端末で、電波でインターネットのアクセスポイントに接続します。④施設内でも、無線で LAN に接続し、そこから有線でプロバイダのアクセスポイントで接続する場合もあります。前者は Emobile や携帯電話など、後者は無線 LAN の 802.11 規格があります。

このような方法でインターネットに接続する装置を「ゲートウェイ」と言われます。ゲートウェイの外側はインターネットです。内側は一台のパソコンの時もあれば、事務所や家庭のように複数のパソコンがある場合もあります。インターネットに対して、このような小規模なネットワークを LAN（ラン）と呼びます。LAN は HUB（ハブ）という集線装置、パソコン、プリンタ、ケーブルなどから構成されます。無線で情報のやりとりが可能です。LAN に接続しているどのパソコンからもインターネットに接続可能です。

※プロバイダのアクセスポイント
インターネットへの入り口にあるコンピュータ。ルーターやモデムでアクセスポイントを指定し、ID とパスワードを使って接続するのが一般的。

※モデム
電話線やケーブル TV 線などのアナログ回線を利用して、インターネットに接続する為の装置。
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/yougo/#modem

※ルーター
デジタル回線を使い、複数台の PC をインターネットに接続する装置。
http://e-words.jp/w/E38396E383ADE383BCE38389E38390E383B3E38389E383ABE383BCE382BF.html

※ LAN
Local Area Network の略
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/yougo/eiji.htm#lan

相談内容

・どうやってインターネットにつないだらよいの？
・ルータの働きは？
・無線 LAN は便利？
・ブロードバンドルーターは、セキュリティ対策になりますか？

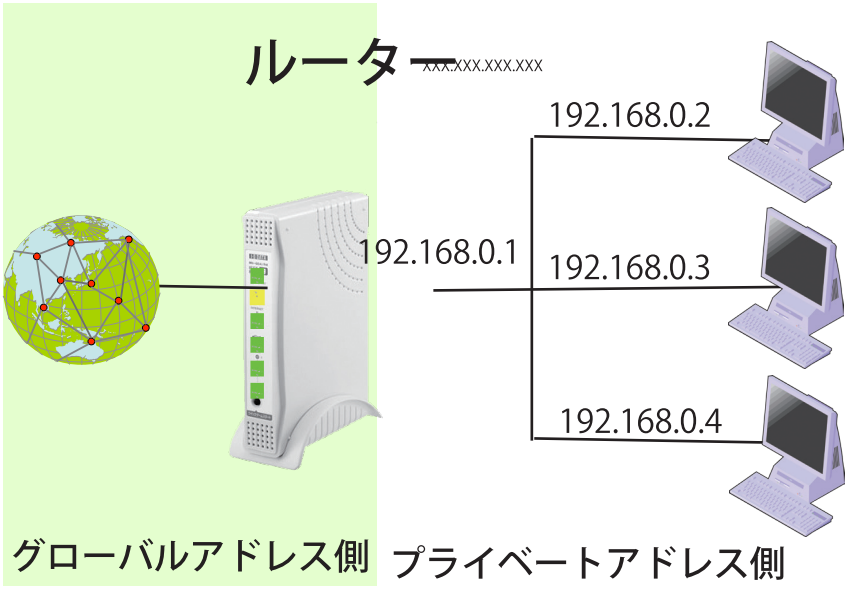
安全安心へむけての一歩

1，ブロードバンドルーターの役割

インターネットを利用する為に「ブロードバンドルーター」を使う方が増えてきました。インターネットに接続しているすべてのコンピュータには、「IP アドレス」という識別番号が割り振られています。この IP アドレスが宛先と送信元に付与されたデータを「IP パケット」と呼びます。IP アドレスを手がかりに IP パケットを最短距離で確実に宛先のパソコンへ渡すのがルーターの主な役割です。

2，2 種類の IP アドレスとブロードバンドルーターの NAT 機能

IP アドレスには、インターネット上で実際に使われてるものと、事務所や家庭内の LAN に接続しているコンピュータやプリンタに使われているものがあります。前者を「グローバルアドレス」、後者を「プライベートアドレス」と呼びます。プライベートアドレスは、インターネットには影響を与えないように、グローバルアドレスとは異なる特別な範囲の数字が使われています。



インターネット上に直接接続しているコンピュータにはグローバルアドレスが割り振られて識別されていますが、LAN などに接続されているユーザのパソコンではブロードバンドルーター（以下ルーターと略）が自動的に割り振ったプライベートアドレスが使われている場合が普通です。これは、グローバルアドレスの個数に限界がありすべてのパソコンに割り振ることがむずかしいこと、家庭や事務所なのでは自由にパソコンを増やしたりネットワーク構成を変えることができるからです。

ルーターは、そこに割り振られたグローバルアドレスをプライベートアドレスに変換し、LAN のパソコンや機器に割り振る役割をしています。この機能を「NAT（Network Address Translation）」と呼びます。

現在のルーターは、一つのグローバルアドレスを複数のプライベートアドレスに変換したり、ポートも変換する「NAPT（Network Adodress Port Translation）」が備わっているので、1 回線のインターネットを複数の PC で利用できるようになっています。

また、ブロードバンドルーターの IP アドレスはインターネット側から見え直接接続されることがありますが、LAN 内のパソコンはそうではないことから、外部から直接侵入されにくいという利点もあります。

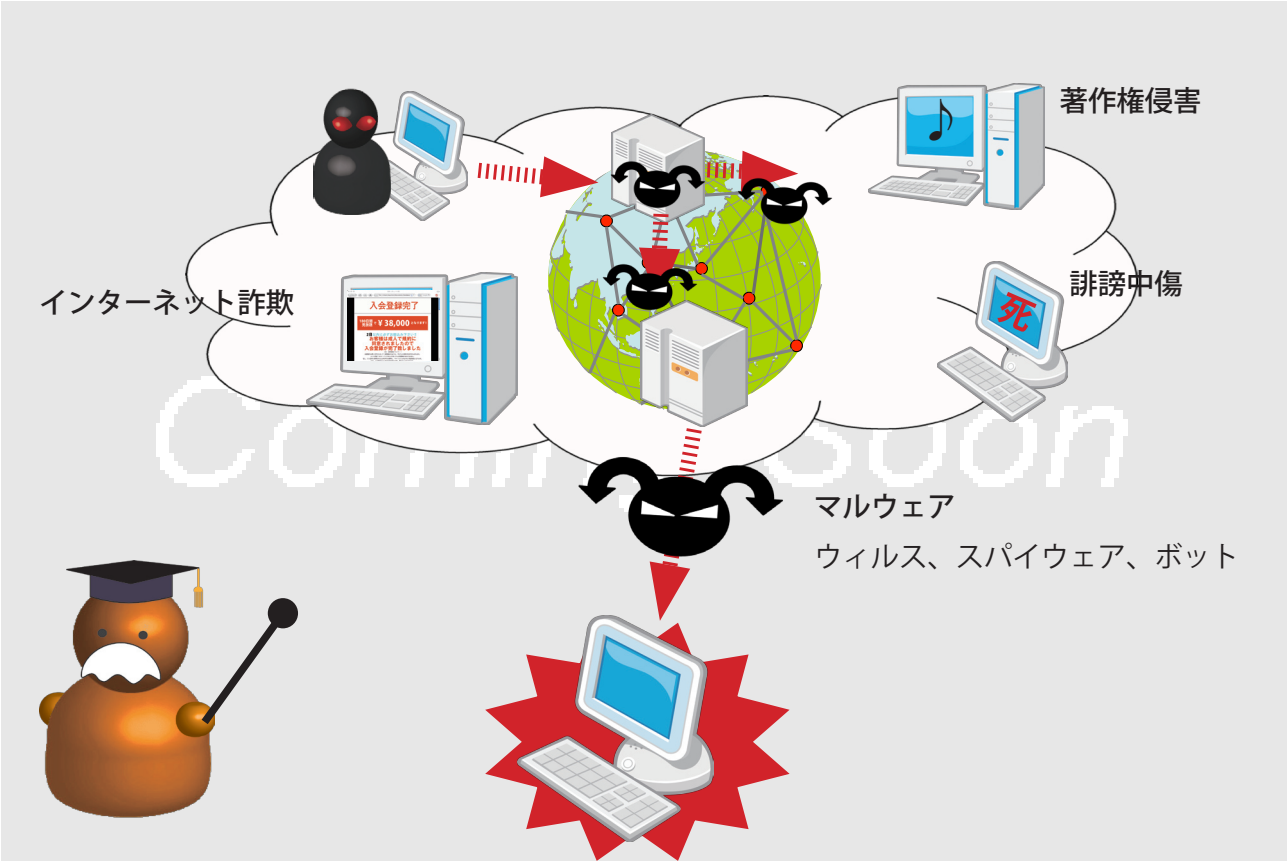
関連する事項

○

重要用語

LAN、NAT、グローバルアドレス、プライベートアドレス

13 インターネットが抱える問題



※マルウェア
「悪意をもったソフトウェア　malicious software」からきた言葉、「マル mal」は「悪」を表す。コンピュータウィルスでスパイウエアの働きをするなど攻撃が複合的になって分類することがむずかしいので、まとめて「マルウェア」と呼ぶことが多い。

※プライバシー
「私生活をみだりに公開されない権利」で、次の要件を満たすもの。
私生活上の事実又は事実らしく受け取られるおそれのある事柄、一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められる事柄、一般の人にいまだ知られていない事柄。個人情報とは近いものであるが、一致する概念ではない。

※著作権
文化芸術に関わる知的財産権の一つ。
著作権情報センター「はじめての著作権」
http://www.cric.or.jp/qa/hajime/hajime.html

インターネットは便利ですが、いろいろなトラブルが起こっています。
「マルウェア」と呼ばれる悪意あるソフトウェアが、パソコンから情報を不正に取得したり削除したり、他のコンピュータを攻撃したりするなど問題になっています。このソフトウェアは、コンピュータウィルスとしてネットワークを通じてパソコンに感染するなど被害が広がっています。また、私たちの心の隙をついてお金を払わせたり、クレジットカード番号を入力させようとする「インターネット詐欺」も増加しています。総じてその手法は巧妙になっています。
また、パソコンやインターネットの普及にともない、データを簡単にコピーしたくさんの人にコストをかけずに送ることができるようになりました。それと同時に、知られたくないプライバシーに関わる情報や許可を得ていない著作物がインターネット上で公表されたり交換されるようになる等の権利侵害が起こっています。
誰でもが自由に情報発信ができるようになりました。その反面、誹謗中傷、いじめ、炎上など、インターネット上で自由な表現が可能になった分コミュニケーションのあり方に問題が生じています。
また、毎日大量に配信されている迷惑メールも、インターネットを無駄遣いしているばかりではなく、必要なメールを見落としてしまうなど文字通り「迷惑」です。
また、自殺、薬物、出会い系など犯罪とは言えないが好ましくないサイトがお送りあり、青少年への影響が心配されています。

相談内容

・インターネットはこわいのですか？
・インターネットにはどんなトラブルがあるのですか？
・インターネットを使うには、どんなことに注意すればよいでしょう？

安全安心へむけての一歩

1, 被害者にも、加害者にも、犯罪者にならない
インターネットが抱える諸問題を解決することは簡単ではありません。まず、私たち一人一人が注意して被害に遭わないようにしなければなりません。また、パソコンにマルウェアを仕掛けられると、顧客データを流出させたり、迷惑メールを発信したり、他のコンピュータを攻撃するなど、社会に対して迷惑をかけてしまう場合があります。また、インターネット社会になって、法律も変わってきています。知らないうちに方を破っていたということがないようにしなければなりません。

2, 技術、法律、人の三要素
マルウェアによる被害、著作権侵害、誹謗中傷などインターネット上のトラブルは、価値ある情報を盗んでやろう、困らしてやろうなどと考える人がいろいろな手段で引き起こしていることが多く見られます。ウィルスを作成したり、迷惑メールを出したり、架空請求のホームページを立ち上げたり、誹謗中傷の書き込みをすることがそれらにあたります。これらは、私たちがパソコンを使って有意義な社会生活を営もうとしていることに対する「脅威」です。この脅威をできるだけ小さくするには、法律を整備し取り締まることと同時に、やってよいことといけないことを教育することも必要です。
脅威はそう簡単にゼロにはならないでしょう。被害を最小限に留める工夫も必要です。その為には、パソコンの狙われるところ、私たちがついつい欺されてしますところを修正しなければなりません。このような弱いところを「脆弱性といいます。強力なマルウェアが発生し、パソコンにそれを防ぎきれない技術的弱点があった場合など、「脅威」と「脆弱性」が同時にそろったとき大きなトラブルが起こります。セキュリティ対策ソフトの導入などの技術的対策が「脆弱性」を下げるのに有効です。
近年、様々なマルウェアが発生し脅威が多様になり、それに対する対抗策も複雑になってきました。中には「面倒だ」「対策をとるとパソコンの動きが鈍くなる」と言って、せっかくのセキュリティ対策ソフトを OFF にする人がいます。せっかくの技術も使われなければ意味がありません。また、「情報が漏洩しても困らない」と言って何も対策をしない人もいます。自分はよいのでしょうが、マルウェアをどんどん撒き散らしていることは社会にとっては脅威です。
被害にあわない、加害者にも犯罪者にもならないような社会にする為には、法律や技術を整備するだけではなく、人がそれらをどう活かすにかかっています。また、誰かがやってくれるだろう、わたし一人ぐらいはやらなくてもではなく、みんなで取り組まなければならないことなのです。

総務省「国民の為の情報セキュリティサイト　**IT 社会の繁栄と情報セキュリティ**」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k02_security.htm

関連する事柄

◎ 14、インターネット詐欺、p.27
◎ 15、悪意あるソフトウェア（マルウェア）、p.29
◎ 16、巧妙な攻撃、p.31
◎ 17、ファイル交換ソフトのトラブル、p.33
○ 18、迷惑メール、p.35

重要用語
マルウェア、著作権侵害、プライバシー、脅威、脆弱性

14 インターネット詐欺

インターネットでオンラインショッピングなどできるようになってから、クレジットカード番号を不正に取得しようとしたり、架空請求などお金に関わるトラブルが多くなってきました。

2008 年警察庁が発表した資料によれば、H16 年頃からこの傾向は顕著になっています。ひと昔前にみられたような「うで自慢」ではなく、経済的利益を得ることを第一目標にした集団が、私たちを狙っていると言えます。

彼らの手法は、クリックすると「入会完了　会費 58000 円払って下さい」というワンクリック詐欺、クレジットカード会社のホームページをまねた偽装サイトに言葉巧みにクレジットカード番号等を入力させるフィッシング詐欺、不安を募らせてセキュリティ対策ソフトを押し売りしようとする詐欺、「オークションで次点でした。今○○円払って頂ければ落札できます」という次点詐欺など、手法は様々です。このような詐欺の特徴は、「すぐに入力」「すぐに支払いを」というものです。冷静に落ち着いて、すぐには対応せず、わからない時にはそのサイトを印刷し詳しい人に相談しましょう。もしクレジットカード番号や個人情報を伝えてしまったらすぐにクレジットカード会社へ連絡し支払いをとめてもらいましょう。そして、画面をプリントアウトして最寄りの警察へ届けましょう。各地の警察窓口は以下にあります。

サイバー犯罪対策窓口　http://www.npa.go.jp/cyber/soudan.htm

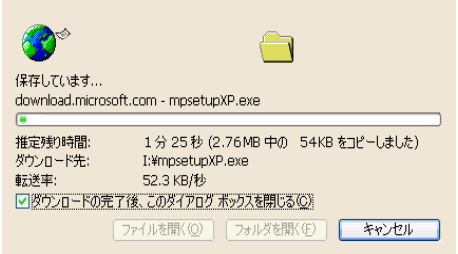
※警察庁資料
2007 年度インターネット犯罪検挙数
http://www.npa.go.jp/cyber/statics/h20/df39.pdf　より

相談内容

・ホームページを見ていたら、突然「入会ありがとうございます」と表示され会費を請求された。
・クレジットカード会社からのメールにある URL をクリックしたら、クレジットカード番号を入力するホームページが現れた
・ホームページを見ていたら、突然スキャンがはじまって「あなたのパソコンは危険です。今すぐこのセキュリティを購入してください」という表示がでた。

安全安心へむけての一歩

ワンクリック詐欺、ツークリック詐欺



クリックしてすぐに入会登録完了が「ワンクリック詐欺」、クリックすると見えにくい文字の確認ページがあり思わずクリックすると入会登録完了となるのが「ツークリック詐欺」です。ともに、登録完了ページに契約プロバイダー名や IP アドレス等が記載されることがありますが、これらは一般的に公開されている情報です。中にはアニメーションを使い情報がコピーされたかのように思わせるものもありますが、ユーザの個人情報は決して相手には渡りません。無視しても大丈夫です。

総務省　国民のための情報セキュリティサイト　「事例 19：ワンクリック詐欺って怖い…」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/jiko/jiko19.htm
国民生活センター「あわてないで !!　クリックしただけで、いきなり料金請求する手口」
http://www.kokusen.go.jp/soudan_now/click.html
情報処理推進機構「【注意喚起】ワンクリック不正請求に関する相談急増！」
http://www.ipa.go.jp/security/topics/alert20080909.html

フィッシング詐欺

クレジットカード会社や銀行を騙ったサイトへメールで誘導し、カード番号を入力させようとするものです。最新のブラウザでは、このような偽装サイトを見破ることができるようになりました。迂闊にカード番号を入力しないとともに、最新版のブラウザを利用することが一番です。

情報処理推進機構「フィッシング (Phishing) 対策」
http://www.ipa.go.jp/security/personal/protect/phishing.html

セキュリティ対策ソフトの押し売り

突然セキュリティスキャンが始まり「ウィルスが発見されました」というメッセージを表示させ、セキュリティ対策ソフトを売りつけようとします。実際には、パソコンにしかけられた不正プログラムが実行されているので、実際にスキャンを行っていません。慌ててクレジットカードで購入したりすると、クレジットカード番号が悪用されたり、購入したセキュリティソフトで逆にパソコンから情報を不正に取得されることがあります。無視しても大丈夫です。

情報処理推進機構「偽の警告を見分けよう！ ― あなたのセキュリティ対策ソフトは本物ですか？ ―」
http://www.ipa.go.jp/security/txt/2008/11outline.html#5
上記以外にも不正なセキュリティ対策ソフトを言葉巧みに売りつけようとするものもあります。

関連する事柄

重要用語

フィッシング詐欺、架空請求、ワンクリック詐欺、ツークリック詐欺、次点詐欺

15 悪意あるソフトウェア（マルウェア）

※コンピュータウィルス
国民の為の情報セキュリティサイト：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04_virus.htm
※スパイウェア
「利用者や管理者の意図に反してインストールされ、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等」、IPA「情報セキュリティ読本」2007,P.40。
国民の為の情報セキュリティサイト：
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04_virus.htm
代表的なスパイウェアとして、キーボードの動きを記録する「キーロガー」がある。
※アドウェア
広告に用いられるソフトウェア。ホームページを見ると自動的に出てくるポップアップ画面など。
※ボット
自由に操ることから、「ロボット」に由来してつけられた名前。くわしくは、http://www.ccc.go.jp/ を参照。

「マルウェア」には、コンピュータウィルス、スパイウェア、悪質なアドウェア、ボットなどが含まれます。
コンピュータウィルスの感染すると、メールアドレスやパソコン内ファイルを勝手に第三者へ送りつける情報漏洩、他のコンピュータを攻撃、迷惑メールを大量送信、セキュリティ対策ソフトを停止、パソコンの動作を不安定にする、PC 内のファイルを勝手に削除するなどの意図しない動作をします。中には、パソコンのハードディスクをインターネットを通じて全世界へ公開するものもあります。
スパイウェアは、ウィルスと同じ方法で感染することが多く、パソコンの中にそっと身を潜めてクレジットカード番号など価値がある情報を盗みます。
悪質なアドウェアには、立ち上げる度に、ポップアップ画面が勝手に開き広告を表示にしたり、正規のホームページのリンクを書き換えてしまうものもあります。
被害にあうだけではありません。犯罪の片棒を担がわせるものがボットです。ボットはウィルスの一種と分類されます。パソコンい付属しているリモート操作機能を悪用し、外から操られてしまう点です。その結果、メールの大量配信や他のコンピュータを攻撃、他にウィルスを感染できそうなパソコンを探すことなど、さまざまなことをさせられます。スパイウェアのように勝手に情報を収集し、第三者へ情報を渡します。
マルウェアはプログラムですから、やろうと思うことをパソコン上でやらせることができます。

相談内容

・コンピュータウィルスってなんですか？
・感染するとどんなことがおこりますか？
・コンピュータウィルスはどうやって感染しますか？
・インターネットに接続しないので、ウィルスには無関係です

安全安心へむけての一歩

1, マルウェアの感染経路
・マルウェアに感染したファイルを開く
・メールの開封・プレビュー
・ホームページの閲覧
・ネットワークへの接続
　メール添付、USB や CD-ROM などに保存されている、ネットワークからダウンロードした、インスタントメッセンジャーやチャットでなど様々な経緯で入手したファイルを開くことで感染することがあります。ファイル拡張子が、.exe,.pif,.scr,.bat,.com などのものを開く時は注意しましょう。また、Word、Excel などのファイルにもマルウェアが仕掛けられていることもあります。
メールソフト、OS、ブラウザが脆弱であると、メール本文を読んだだけ、ホームページを閲覧しただけでマルウェアを自動的に起動させ感染します。また、ネットワークにパソコンを接続しただけで感染する場合があります。それは、マルウェアがネットワーク上に特殊な信号を出して脆弱なコンピュータを探している場合があるからです。

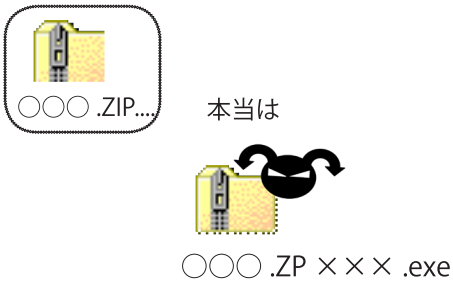


図１　アイコン・拡張子の偽装
一見すると安全にみえるファイルであるが、アイコンを偽装し拡張子を見えないようにしている。

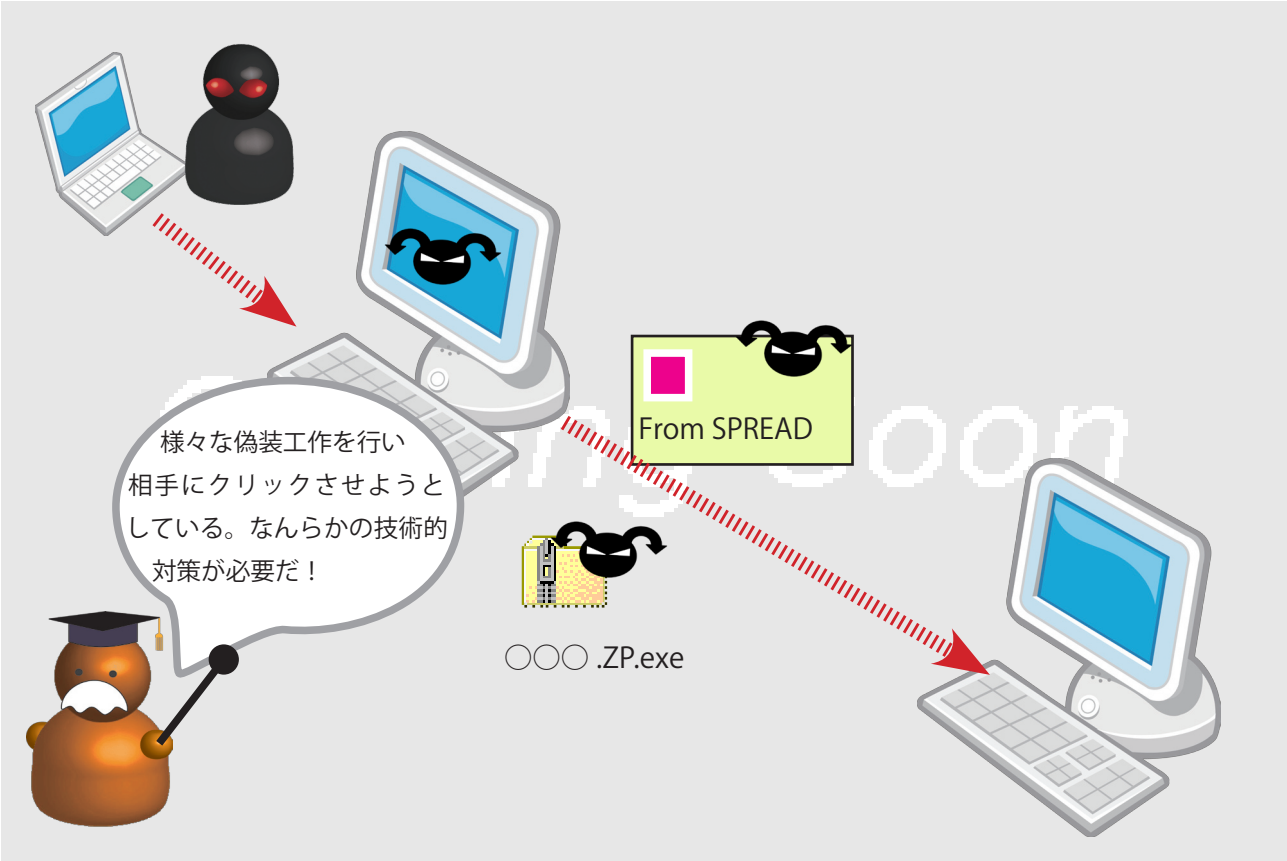
2, マルウェア対策
使用している OS やソフトウェアを最新のものにする。WindowsXp、Vista、Office のアップデート、メールソフトのアップデート、ブラウザのアップデートなどがそれにあたります。自動更新にしておくと便利です。
セキュリティ対策ソフトをいれましょう。ウィルススキャン機能はマルウエアを検知駆除してくれます。また、コンピュータへの不正侵入はファイアウォール機能が防いでくれます。Windows にも簡易型ファイアウォール（Windows ファイアウォール）があります。ただ、毎日新しいマルウエアが生まれているので、セキュリティ対策ソフトマルウェア検出用データを最新のものにしておくとともに、定期的にパソコン自体をスキャンすることが必要です（ウィルス対策ソフト）。ファイルを入手した場合は開く前に必ずマルウェア（ウィルス）スキャンをかける習慣をつけましょう。
また逆に、見知らぬパソコンで USB に保存されているファイルを開く場合には、そのパソコンがマルウエア対策がなされているかチェックして下さい。
プロバイダでマルウェアスキャンを行ってくれるサービスがありますが、これはインターネット経由でマルウエアが送られてくる場合のみですから、USB などのチェックは行いません。注意しましょう。
技術は完全でありません。見知らぬホームページにはなるべく近き安易にクリックしたり、ファイルをダウンロードしないなどの心がけることも必要です。

関連する事柄

◎ウィルス対策
◎ファイアウォール
◎巧妙な攻撃

重要用語
マルウェア、コンピュータウィルス、アップデート、スキャン

16 巧妙な攻撃



※ IPA「情報セキュリティ白書 2008」
http://www.ipa.go.jp/security/vuln/20080527_10threats.html
ますます「見えない化」が進んだと報告されている。

※ゼロディ攻撃

マルウェアに感染させる為、攻撃者は、私たちにファイルを開かせたり、ホームページをみるような仕掛けをします。

・感染してもすぐに症状がでないように「潜伏期間」を設けます。

・感染しても、表だった症状を出さないで、影で密かに動きます。もし症状が表にでるとマルウエア対策ソフトで駆除される可能性があるからです。攻撃も隠蔽されて発見しにくくなっています。

・アイコンを偽装し、拡張子を隠して安全なファイルのように思わせます。

・差出人を偽装し、マルウェアを添付したメールを送ります。受取人がよく知っている組織になりすまして安心させ添付ファイルをクリックさせます。

・迷惑メールにホームページをリンクし、それをクリックしホームページにアクセスさせマルウェアに感染させる。など、メールで誘導させる攻撃方法も良く行われています。

・正規のホームページに仕掛けをし、そこにアクセスしたユーザを他のホームページに自動的にとばしマルウェアに感染させる。

・脆弱性がみつかった時点で、それを攻撃するマルウェアを配布する。対策ソフトが間に合わない。

・自分自身ではマルウェアをばらまいたり、迷惑メールを発信させたりせずに、ボットを埋めこんだコンピュータを遠隔操作し攻撃を代行させます。

・突然にウィルススキャンを実施したようにみせ、セキュリティ対策ソフトを売りつけようとします。

相談内容

・セキュリティ対策ソフトを入れていれば大丈夫なんですよね
・ウィルスに感染したことがありません！
・ウィルスに感染しても、特に盗られる情報はありません

安全安心へむけての一歩

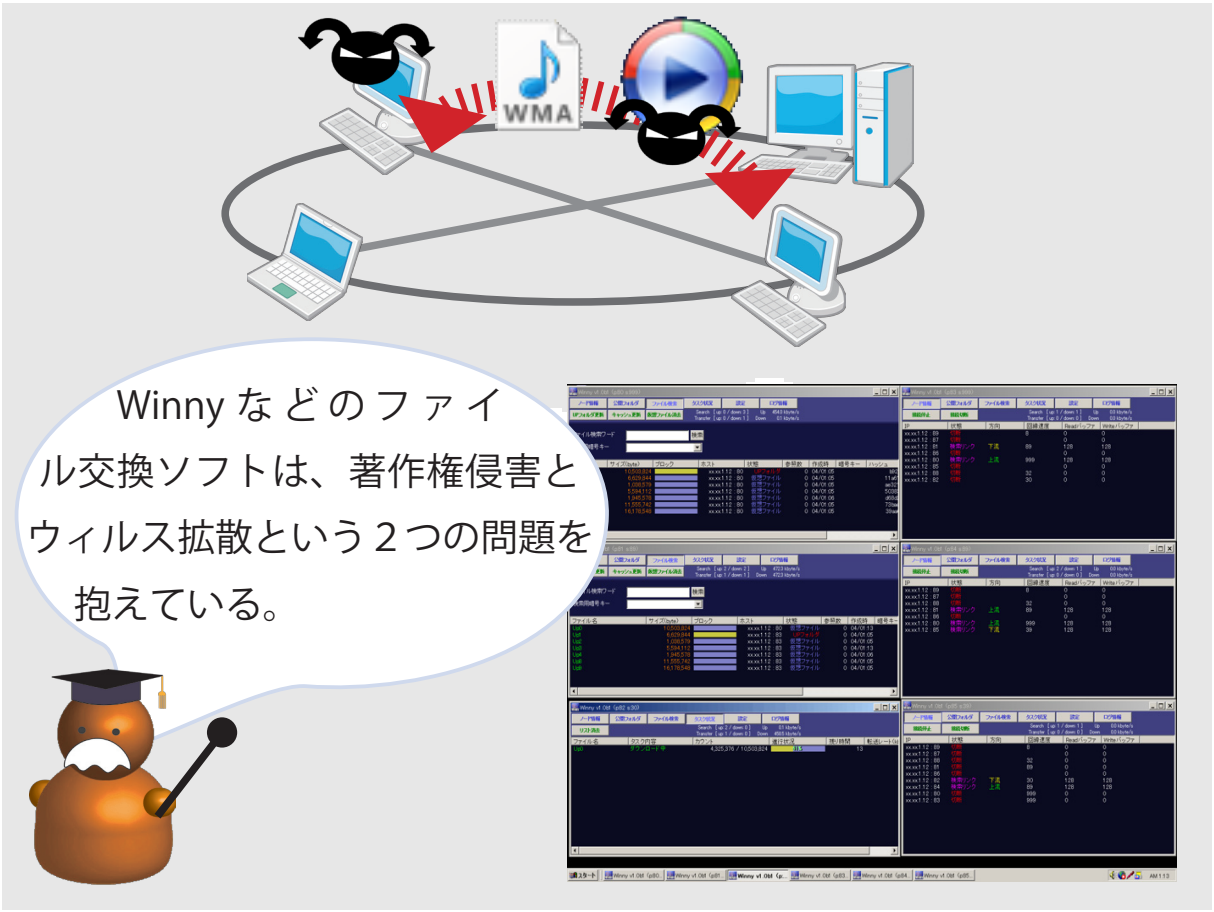
1,OS、その他ソフトウェアのアップデート、マルウェア対策ソフトを最新のものとしておきましょう。 ★☆☆
対策手段がない攻撃は防げませんが、いままでの攻撃を防ぐことはできます。
2, 定期的なマルウェアスキャンが必要です。 ★☆☆
マルウェア対策ソフトが対抗手段を見つける前に、パソコンが感染している可能性があります。一月に一回はパソコン全体をスキャンして下さい。
3, アイコンや拡張子偽装は Winny などで流れているファイルによく見られます。偽装を見破る為には、拡張子を常日頃から見えるようにしてかなければなりません。その方法は以下にあります。 ★★☆
「　表示の設定　拡張子や隠しファイルの表示　拡張子の表示 / 非表示の方法」
また、カーソルを合わせるとファイル名が表示されます。ファイルは、拡張子を確かめ、ウィルススキャンをして安全を確かめてからクリックしましょう。
4, メールの URL は安易にクリックしないようにしましょう。
5, メールの差出人が正規の人かどうかを確認することが難しくなっています。メールアドレスだけではなく、メール本文の内容も偽装されにせものとは判断できない場合があります。
IPA を語った「なりすましメール」 http://www.ipa.go.jp/security/topics/alert20080416.html
差出人を確認するには、暗号ソフトを利用したり、第三者機関が発行した証明書をメールに添付する方法があります。くわしくは、「安全安心対策：暗号の利用」を参考にして下さい。
6, インターネット詐欺は、ウィルススキャンをしたように見せたり、データがコピーされたように見せることで恐怖心を植え付けお金をとろうとします。まず、落ち着いていろいろと調べてみることが重要です。詐欺については「インターネット詐欺」を参照して下さい。

関連する事項

・

重要用語

17 ファイル交換ソフトのトラブル



※ P2P
Peer to Peer モデルのネットワーク構成は、クライアント・サーバ・モデルと対照的に、参加するコンピュータが同等または類似した役割を対等に担う。
Winny が有名になったが、正しく利用すれば、パソコンやネットワークに負担をかけずに情報共有ができる。
マイクロソフト社の Groove は、台風カトリーナ被災者の連絡に使われ、その有用性を示した。

※ Winny ウィルス
ファイル交換ソフト Winny で流通しているファイルに寄生しているコンピュータウィルス。Winny 使用者が著作権法違反幇助で逮捕された。

※総務省、Winny の危険性を告げる文書
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/ippan16.htm

ファイル交換ソフトのトラブル

現在、ファイル交換ソフトが「著作権侵害」「ウィルスの拡散」の面から問題視されています。これらは P2P 技術を利用し、ユーザ同士がフォルダを共有することでネットワークを構成し、バケツリレー的にファイルを転送し合うものです。このネットワークには、数百万台のパソコンが接続しているとも言われています。ファイル交換ソフトの代表として、もっとも有名なのが「Winny」ですが、それ以外にも Lime, Share など多く存在しほとんどが無料で利用できます。これらのソフトウェアを使い、音楽・映画・ゲームなどのデータが許諾なしにやりとりされ著作権侵害を起こしています。しかし、P2P が特定のサーバを持たずに情報をやりとりできるしくみであることから管理が難しく、なかなか取り締まることができません。

また、ファイル交換ソフトは、ウィルス感染による個人情報や機密情報の漏洩なども問題となっています。捜査書類、郵便物の誤配状況な、陸上自衛隊の内部資料、神奈川県の高校生全員の個人情報の漏洩などが報告されています。これらは、Winny がインストールされている個人用パソコンがウィルスに感染しており、そのパソコンで機密情報を扱ったことで起こっています。Winny のようなファイル交換ソフトでやりとりされているファイルの内かなりのものがウィルスに感染していると言われています。Winny のようなファイル交換ソフトを利用することはかなり危険性があると認識して下さい。

相談内容

・Winny って何ですか？
・Winny で個人情報流出すると聞きました
・Winny から音楽や映画のデータを無料で入手できると聞きました
・Winny を使っていないので、安心しています

安全安心へむけての一歩

ファイル交換ソフトでダウンロードしたファイルを実行することで感染します。ウィルスが含まれていることうぃ隠す為、アイコンが偽装されファイル名が異常に長く実行ファイルの拡張子（exe）が隠されています。例えば、「お楽しみ画像 .zip. ○○○○○○○○○ .exe」というような形になっており、一見すると「お楽しみ画像 .zip」と見え、ウィルスとは知らずにクリックしてしまうことがあります。

ファイル交換ソフトのウィルスとして、主に次のようなものがあります。

1. デスクトップ暴露型ウィルス

このウィルスは感染すると、デスクトップのスクリーンショットやデスクトップ上にあるファイルを Winny ネットワークに公開します。Antinny.G がこれにあたります。

2. ファイルばらまき型ウィルス

DSC***.jpg のような画像データや .doc,.xls のような特定のファイルを収集し、Winny ネットワークへ公開します。Antinny.Trojan などがこれにあたります。

3. サーバ公開型ウィルス

このウィルスは感染すると、つかっているパソコンのハードディスクの中身を全世界へ公開してしまいます。このウィルスは、Winny を利用していなくても感染して被害に遭ってしまう点です。友人から Winny で入手したデータをからもらいこのウィルスは感染し、インターネット上にすべてを公開してしまったという例もあります。TROJ_MELLPON.A（別名：山田オルタナティブ） などがこれにあたります。

対策と防止

対策と防止としては、Winny のようなファイル交換ソフトを利用しないことが一番です。企業などでは、業務用パソコンに Winny を入れることを禁止しています。しかし、趣味で使う個人用パソコンで使用することを強制的に禁止することはできません。その場合は、パソコンや情報をきちんと管理しましょう。

まず、仕事用と Winny 用のパソコンを明確に分けるべきです。Winny を使用するパソコンには大事な情報は入れない方がよいでしょう。しかし、ファイル交換ソフトを利用していなくても山田オルタナティブのように、Winny に由来するデータをクリックし被害に遭うこともあります。必ず、セキュリティ対策ソフトでファイルをチェックしましょう。もしウィルスに感染したと分かったら、ネットワークからそのパソコンを切り離しましょう。個人情報が流出した場合には、その本人に必ずその旨を報告し被害をできるだけ最小限に留めるよう努めなければなりません。

Winny ウィルスについての詳しい解説や対策は、以下のホームページをみて下さい。

情報処理推進機構「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

総務省　国民のための情報セキュリティサイト　「ファイル共有サイトが原因で・・・・」
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/jiko/jiko18.htm

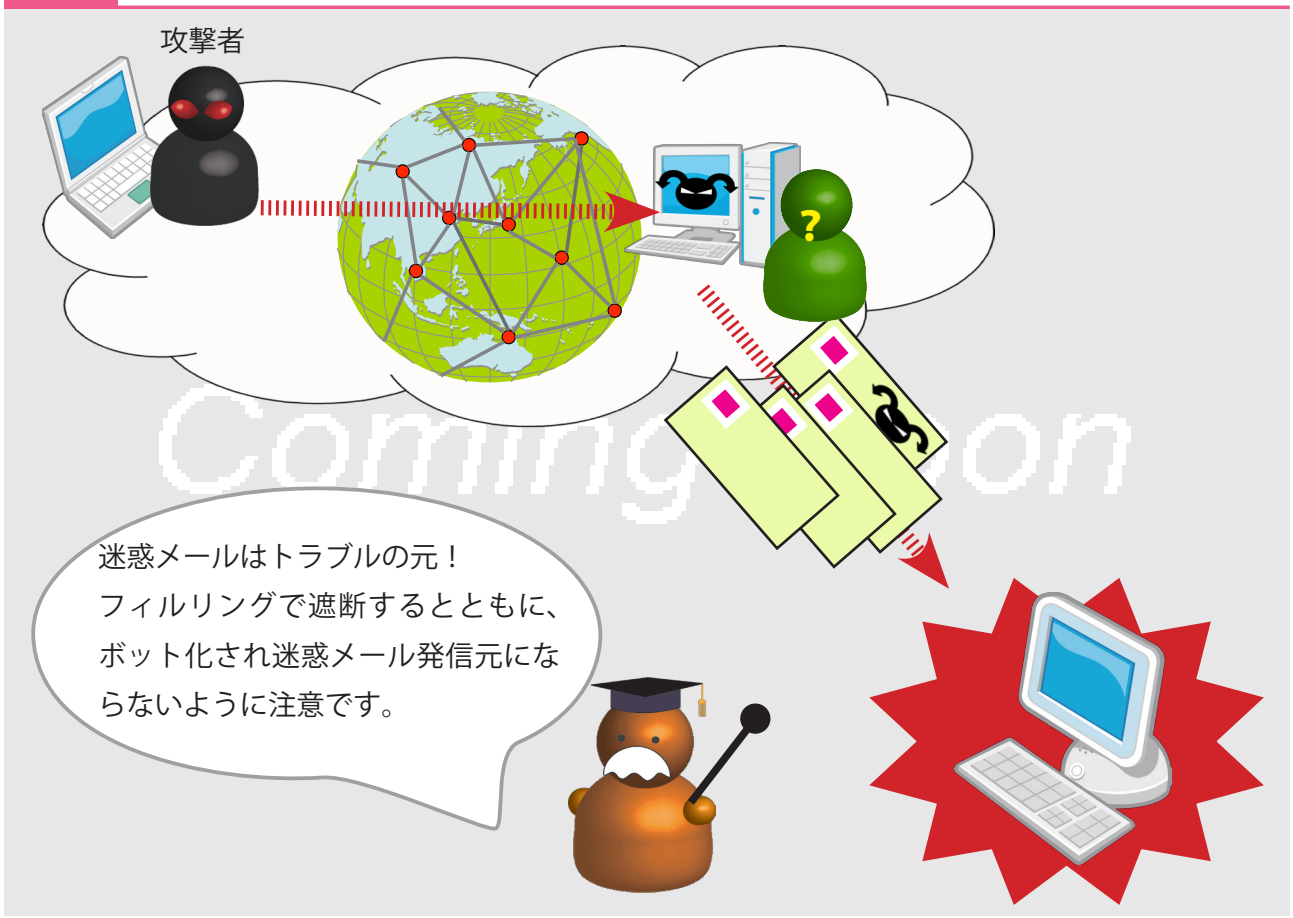
関連する事項

・ウィルス対策ソフトの活用
・インターネット関連法（著作権）

重要用語

ファイル交換ソフト、ウィルス、ウィルス対策ソフト、著作権

18 迷惑メール



※スパムメール
迷惑メールの別名。
名前の由来は、アメリカのテレビドラマ「モンティパイソン』第〇話で、主人公が意味もなく「スパム、スパム・・・」と連語したことに類して命名されたという説が有力

迷惑メールは、次の点で問題です。

・無用なメールがインターネット資源を使い、必要なメールが遅延するなどの可能性がある。
・無用なメールがパソコンに届き、必要なメールを見逃してしまう可能性がある。
・「お得情報」「すぐ H できます」など興味を引かせ、インターネット詐欺へと導かれる可能性がある
・添付ファイルでマルウエアを拡散させる場合がある。
・本文中の URL をクリックすることで、マルウエアを自動的に読み込み感染する場合がある。

迷惑メールは、攻撃者自身が発信しているというよりも、ボット化されたコンピュータが出している場合が多いと言われています。自分のパソコンがそのような発信元にならないように、OS のアップデート、マルウェア対策ソフトなどできちんとケアすることが、迷惑メール撃退につながります。

相談内容

・迷惑メールは、なにが「迷惑」なのですか？
・迷惑メールは、ゴミメールが来るだけですよね
・迷惑メールが多くりました。どうしたらよいでしょうか？

安全安心へむけての一歩

1. フィルタリング
迷惑メールを排除するには、フィルタリングが有用です。
プロバイダで自動的におこなっている「迷惑メールフィルタリングサービス」と個人のパソコンで行っている場合があります
前者は、別途契約が必要な場合もあれば、契約時にすでに盛り込まれているものなど様々です。詳しくは、契約しているプロバイダのホームページを参考にして下さい。
Outlook や Thinderbird などには前もって「迷惑メール対策機能」があります。これらを上手に設定することで、迷惑メールを取り除くことができます。また、Outlook の迷惑メール対策機能を、マルウェア対策ソフトで補強することもできます。

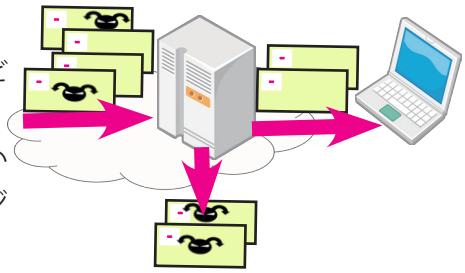


図１　プロバイダによる迷惑メールフィルタリング
迷惑メールは別フォルダへ移動。

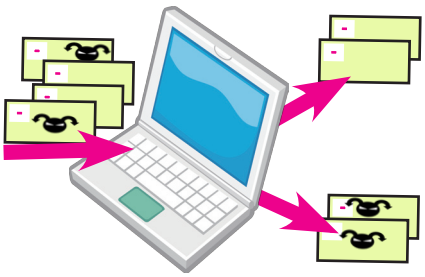


図２　メールソフトの迷惑メールフィルタリング
迷惑メールはメールの迷惑メールフォルダへ移動。

ウィルスバスターのスパムメール対策機能設定方法
Norton Internet Security の迷惑メール対策
McAfee の迷惑メール対策

自分のパソコンでフィルタリングを行う場合、最初から 100%フィルタリングできません。取り残すことも、まちがって迷惑メールと判断することもあります。メールソフトに迷惑メールの特徴を学習させてあげる時間が多少必要になります。

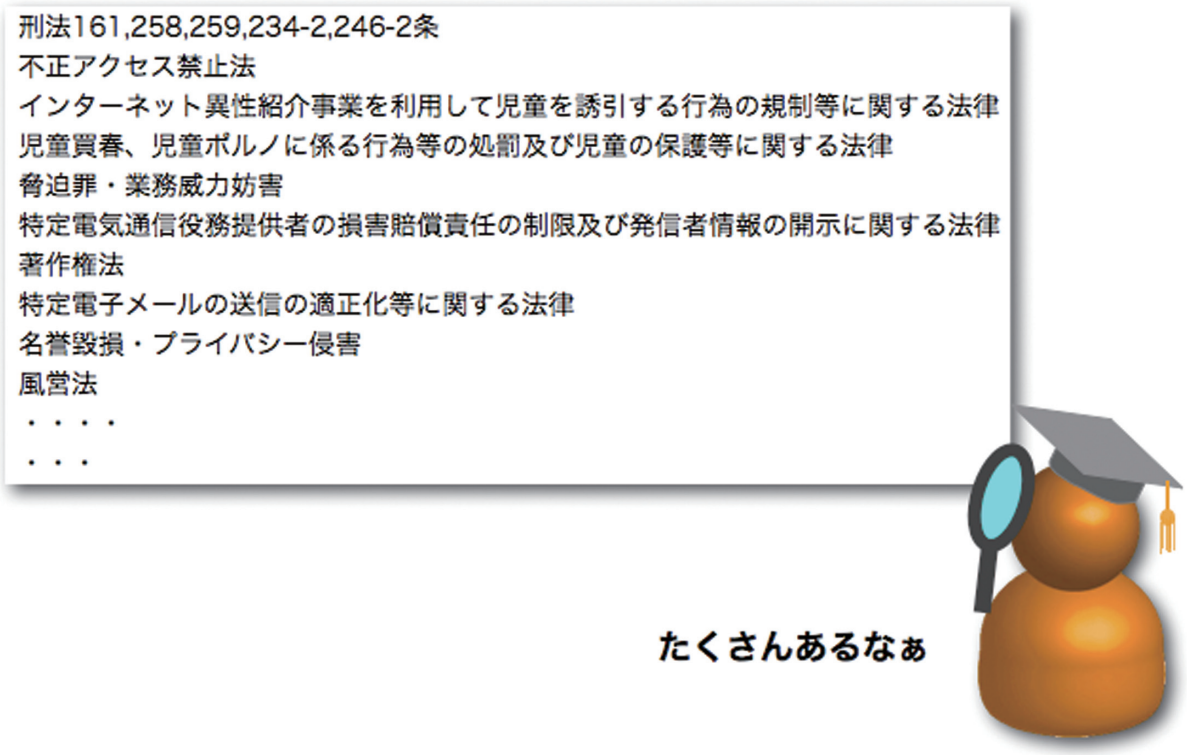
上の方法以外に、Gmail などに一端メールを転送し、そこで強力な迷惑メールフィルタリングをかけ、必要なメールだけを自分に転送するという方法もあります。

2. メールアドレスを変更する
どうしても防ぎ切れない場合は、メールアドレスを変更するのも方法です。

3. 迷惑メールを取り締まる法律
「特定電子メールの送信の適正化等に関する法律」
平成 20 年 6 月に改正され公布。了解なしに勧誘メールを送ること、海外からの発信についてなど迷惑メールに対する罰則が強化された。
http://www.soumu.go.jp/s-news/2008/pdf/080828_8_bt2.pdf

重要用語
迷惑メール
スパムメール
フィルター

19 インターネット関連法



※U市の基本台帳が勝手に売却された事件では、実行犯はインターネットを使い個人情報を勝手に売却した為罪には問われませんでした。

※不正アクセス
パスワードを不正に入手したり、パスワードを破るなどして、情報を不正に取得すること。データを改竄破壊していなくても、「盗み見」を行った場合でも処罰される。
「不正アクセス行為の禁止等に関する法律」
http://www.ipa.go.jp/security/ciadr/law199908.html

インターネットやコンピュータが普及して、社会は大きくかわりました。それと共に今までの法律では対応できない事件や事故が起こるようになりました。

ある百貨店の元課長が顧客データをフロッピーディスクに入れ名簿業者に無断で売却する事件がありました。この時、この元課長は、フロッピーディスクを盗んだ罪で罰せられました。その当時は、データ・情報は価値があるモノとして扱われなかったからです。また、情報は盗み見ても、それはモノではないので窃盗にはなりませんでした。

インターネット、コンピュータが普及する前は、印刷や情報発信はプロの仕事でした。いまでは誰もがホームページなどで情報発信することが可能となりました。それと共に、他人が作った地図・画像・音楽を勝手にインターネットで公開する、勝手に顔写真をホームページに載せる、他人を傷つける書き込みをするなど、いろいろなトラブルが発生しています。

これらに対して、法律が改正されてきました。盗んだパスワードを使いコンピュータに不正にアクセスした場合は「不正アクセス禁止法」、データベースやホームページを改ざんした場合には「器物破損」、人の作品を無許可でホームページで公開した場合は「著作権法違反」となるようになりました。それ以外にも、名誉毀損やプライバシー侵害もあります。メールで「殺すぞ」と書くことは脅迫になります。また、出会い系サイトで未成年が書き込みしすることや未成年を勧誘することも刑罰の対象となりました。悪いやつは捕まえなければなりませんが、知らず知らずに法を犯しているということがないように注意しなければなりません。

相談内容

・顔写真を勝手にホームページで使われました
・地図を利用したいのですが
・新聞記事をスキャンして、ホームページで公開してもよいですか？
・私の作った画像が、勝手にホームページで使われています。
・インターネット掲示板に、誹謗中傷されました。どうしたらよいでしょう？

安全安心へむけての一歩

インターネット上で、いろいろなトラブルが起こっています。ここでは、著作権侵害、プライバシー侵害、誹謗中傷、殺人予告、自殺予告について説明します。

1. 著作権侵害

「著作権」とは、文化芸術の分野で、はじめて創られたものを保護する制度です。絵画・楽曲・詩・映画・写真・新聞記事などを作者の無許可で公開・編集・複製することができないというものです。その作品のうまい下手にも関係なく、はじめて創られそこに独創性があるものは作家の死語 50 年（映画は 70 年）間保護され、作者や権利をもっている人の許可なしには使用できません。ただ、あまりに単純な顔文字や新聞の見出しなどよく見られるものにはありません。また、公に使用するのではなく私や家族で使う「私的利用」は無許可で行ってもよいこととなっています。インターネットの場合、それが家族やごく一部の友人しか閲覧しないものであっても、私的利用は認められません。ホームページにアップロードする（送信可能な状態にする）には、権利者の許可が必要になります。新聞記事や地図を利用する時には、許可が必要です。また、自分の作品が勝手にホームページで使われた場合には、まず管理者へ削除を求めましょう。管理者はそれにきちんと対応しなければなりません。

文化庁「著作権なるほど質問箱」 http://bushclover.nime.ac.jp/c-edu/
著作権管理センター (CRIC)　はじめての著作権講座　http://www.cric.or.jp/qa/hajime/hajime.html

2. 誹謗中傷、名誉毀損、プライバシー侵害

インターネット掲示板に悪口を書かれたり、実名や電話番号や顔写真を公開されたりした場合、その情報が広く広がることで深く傷ついたり、悪用されることがあります。このような場合は、書き込んだ人に抗議する前に、そのホームページの管理人連絡しそれらの情報を削除してもらうようにしましょう。「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」で、ホームページ運営者は、このような状況に対応しなければなりません。大概の場合は、削除要求に応じてくれると思いますが、もし応じてくれない場合は弁護士に相談しましょう。

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 (通称：プロバイダ責任制限法)
http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/denki_h.html

3. 殺人予告、自殺予告

「○月○日、スーパー××で人をころします」「・・に自殺します」という書き込みをインターネット上で見つけた場合は、すぐに最寄りの警察に通報して下さい。殺人予告は犯罪として取り締まることができます。自殺予告は、すぐに書き込み者を特定し警察が保護に向かえるようにプロバイダにガイドラインがあります。これらの書き込みをみつけたらすぐに警察へ通報しましょう。最寄りの窓口はこちら。

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.htm

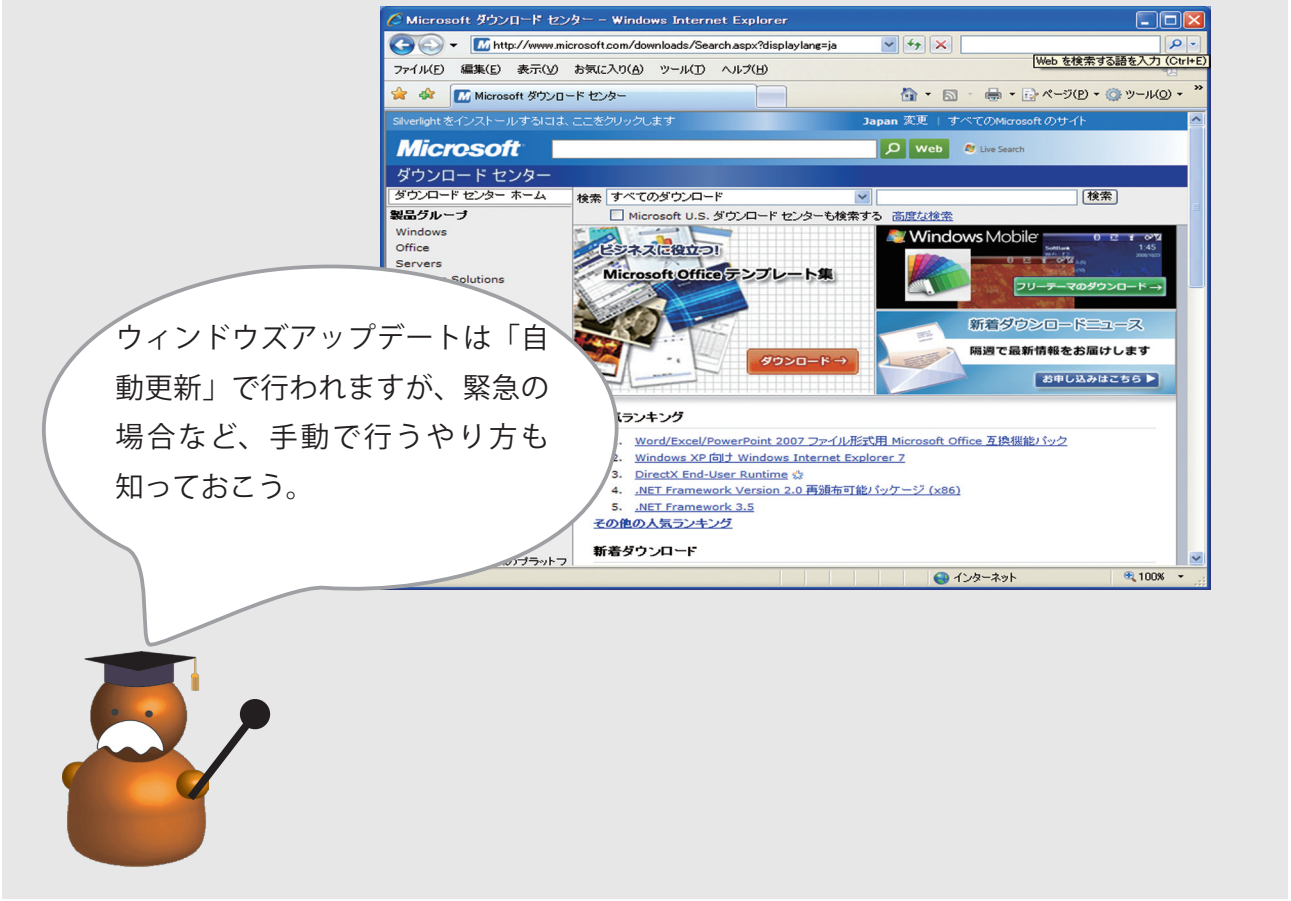
関連する事項

◎ファイル交換ソフトのトラブル
◎インターネットが抱える問題
○様々のネットワーク

重要用語

著作権
プライバシー、個人情報
プロバイダ責任制限法

20 安全安心対策：ソフトウェアのアップデート



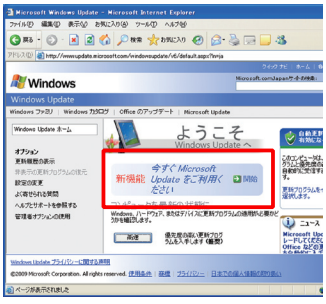
※ Windows Update … Windows Update とは、使用している Windows を自動的に更新し、システムを最新の状態に保つための機能で、製品の発売以降に見つかった問題の修正や、新しく追加された機能を自動的にダウンロードして更新します

Windows のアップデートとは、Windows に修正プログラムを適用し、最新の状態にすることです。これによって、Windows のセキュリティホールが塞がれ、ウマルウェアの侵入や悪意のある攻撃からパソコンを守ることができます。セキュリティ対策の観点から重要な役割を持ちます。

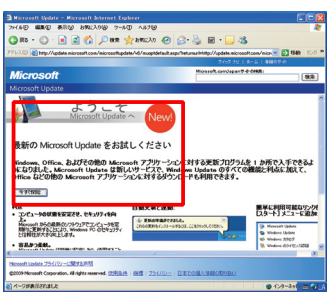
アップデートが自動化に設定されていると、インターネットに接続されていれば自動更新を確認し修正プログラムを自動的にダウンロードしインストールが行われます。自動化するの方法は以下にあります。

http://www.spread-j.org/sheet/2006/07/03microsoft_updatexp.html

ここで、更新を確認するスケジュール、ダウンロードはするがインストールはしないなどの設定が脳です。



Office 製品のアップデートは Microsoft アップデートで行います。こちらを行うと Windows Update も同時に行われます。Microsoft アップデートは Windows アップデートの画面で実行できます。Windows アップデートの代わりに Microsoft アップデートも自動化することができます。



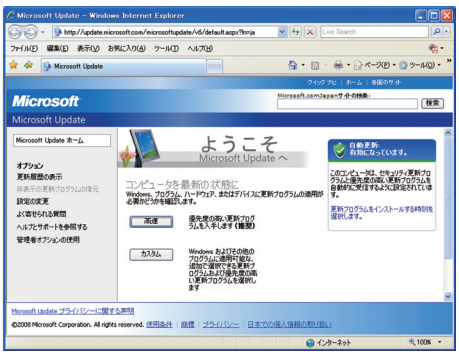
相談内容

・ウィンドウズアップデータとを手動でやるには？
・急にウィンドウズアップデートが必要になりました。
・インターネット環境にない PC に、ウィンドウズアップデートをするには？

安全安心へむけての一歩

アップデートは、通常インターネットに接続されていれば自動更新が行われますが、手動でアップデートを行う事が可能です。以下で、マニュアルでアップデートを行う方法を説明します。

インターネットを介してのマニュアルアップデートの方法



1. スタートメニュー →すべてのプログラム →「Microsoft Update」を選択することで Windows Update(http://update.microsoft.com/) のページが開きます。
2. 現在の Windows の状態が自動で確認された後、「高速」ボタンを選択し、優先度の高い更新プログラムを入手します。
3. まだ適用されていないアップデート内容が一覧で表示されるので、「更新プログラムのインストール」ボタンを選択することで、各更新プログラムが順次アップデートされていきます。

尚、アプリケーションによってはアップデートの際に Windows の再起動を行う必要がある場合があります。

Service Pack の適用

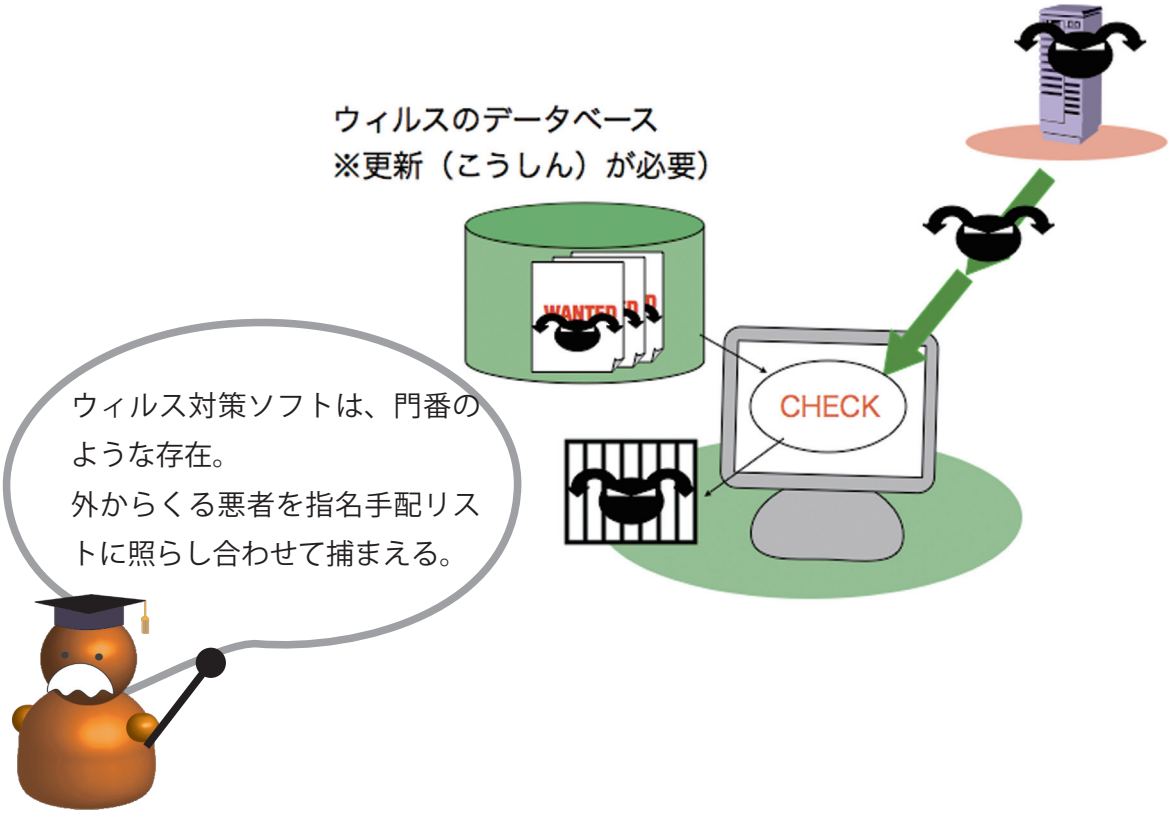
Microsoft 社が Windows の修正プログラムをまとめ、公開しているものは「Service Pack」(以下 SP) と呼ばれています。SP を適用することで、個別に公開されていた多数の修正プログラムを一括でインストールすることが出来るため、SP をインストールする事はセキュリティ上極めて重要と言えます。また、SP は段階的にリリースされることも多く Windows XP については 2008 年 11 月 24 日現在、SP3 が公開されています。

SP のインストールパッケージの入手方法

SP は Windows Update にてインターネットからインストールが行えますが、インストールパッケージをダウンロードし、CD に保存しておくことも可能です。インストールパッケージをダウンロードする場合、自身の利用している OS に合った SP を選択する必要があります。

Microsoft ダウンロードセンター (http://www.microsoft.com/downloads/search.aspx?displaylang=ja)

21 安全安心対策：ウィルス対策ソフト



ウィルス対策ソフトには、ユーザーが利用するファイルを常に監視し、ウイルスと思われるプログラムが実行された時に警告を発し、ウィルスの動きをブロックする自動保護機能を持っています。こうした機能が働くには、何がウィルスであるのかを特定しなければなりません。そこで、ウィルス対策ソフトは、パソコン内にウィルスに関するデータを持っており、それに照らし合わせてウィルスなどマルウエアを検知隔離しています。しかし、日々多くのウィルスが発生していることから、ウィルスに関するデータを常に更新（アップデート）しなければなりません。市販されているウィルス対策ソフトは、このアップデートをオンライン上で行います。

多くのウィルス対策ソフトは、インストール後一定期間（たいてい 1 年から 2 年）が過ぎるとこのアップデートができなくなります。これは、アップデートする契約がきれたからです。アップデートが行えなくなると、新たに発見されたウィルスに対応出来なくなるなど、セキュリティ上脆くなるため、契約期限が切れたら契約を更新するか、新規で購入する必要があります。契約期限が近くなると、契約更新を促すページやポップアップが表示されます。

契約更新の方法

トレンドマイクロ ウィルスバスター 2009
http://tmqa.jp/contents/contract/renewcontract.asp?ConSupWebclickID=clcs_ded08_1
マカフィーインターネットセキュリティ 2009
http://www.mcafee.com/japan/mcafee/home/msup/
Microsoft Live OneCare（無料） http://support.microsoft.com/kb/935899

※ウィルス対策ソフト
ファイアウォールなどの他のセキュリティ機能と一緒に「セキュリティ対策ソフト」として市販されています。以下、主立ったものを上げます。
トレンドマイクロ社
　ウィルスバスター 2009
McAfee 社
　インターネットセキュリティ 2009
マクロソフト社
　Microsoft Live OneCare
シマンテック社
　ノートン 360
カスペルスキー
　インターネットセキュリティ 2009

※ウィルスに関するデータ
ウィルス対策ソフトをつくっている企業によって、「パターンファイル」「ウィルス定義ファイル」などとも呼ばれます。

※ 2 つの「更新」
ウィルスに関する「データの更新」と、データを更新する「契約の更新」の意味があります。

相談内容

・ウィルス対策ソフトの働きは？
・ファイアウォールとの違いは？
・更新というのは、何を更新するの？
・一部だてウィルススキャンしたい

安全安心へむけての一歩

ウィルスに関するデータのアップデート方法

アップデートには、定期的にオンラインで自動アップデートする方法と、手動でアップデートを行う方法があります。

自動アップデート設定の仕方

ウィルスバスター http://esupport.trendmicro.co.jp/supportjp/viewxml.do?ContentID=JP-2063833
マカフィー http://www.mcafee.com/japan/mcafee/2009/documents.asp
OneCare http://www.microsoft.com/japan/protect/products/computer/onecaresteps.mspx

手動アップデートの仕方

ウィルスバスター http://esupport.trendmicro.co.jp/supportjp/viewxml.do?ContentID=JP-2063848
マカフィー http://www.mcafee.com/japan/mcafee/2009/documents.asp
OneCare http://www.microsoft.com/japan/protect/products/computer/onecaresteps.mspx

自動ウィルススキャン

ウィルス対策ソフトは、自動的にメールの送受信時、USB や CD/DVD 挿入時に自動的にウィルススキャンを行ってくれます。何を監視するかは設定できます（図 1）。

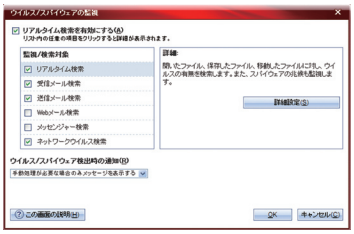


図 1　自動ウィルススキャンの設定

スケジュールスキャン

PC 内のファイルがウィルスに感染していないかを調べるためには、定期的にパソコン全体を完全スキャンをする必要があります。以前は検知できなかったウィルスが見つかることがあります。手動でも完全スキャンできますが、自動的にある時刻に定期的にスキャンするように設定しておくと便利です。自動設定の仕方は各ソフトによってことなります。以下を参考にして下さい。

ウィルスバスター http://www.eparts-jp.org/secure_method/025_vb-schedule.htm
マカフィー http://www.mcafee.com/Japan/mcafee/support/faq/answer_f_spec.asp?wk=SP-00003
OneCare http://www.microsoft.com/japan/smallbiz/startsb/029/p002.mspx

スポットウィルススキャン

USB や CD/DVD でファイルを受け取る場合、 USB などのメディア・フォルダ・ファイルを素早くウィルススキャンすることもできます。スキャンしたいファイルやフォルダを選び右クリックし、メニューからウィルススキャンを選びます（図 2）。

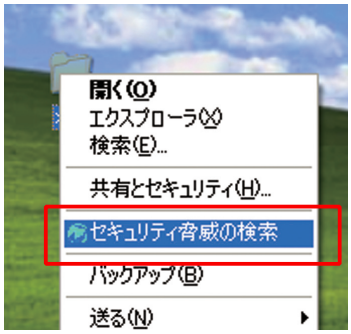


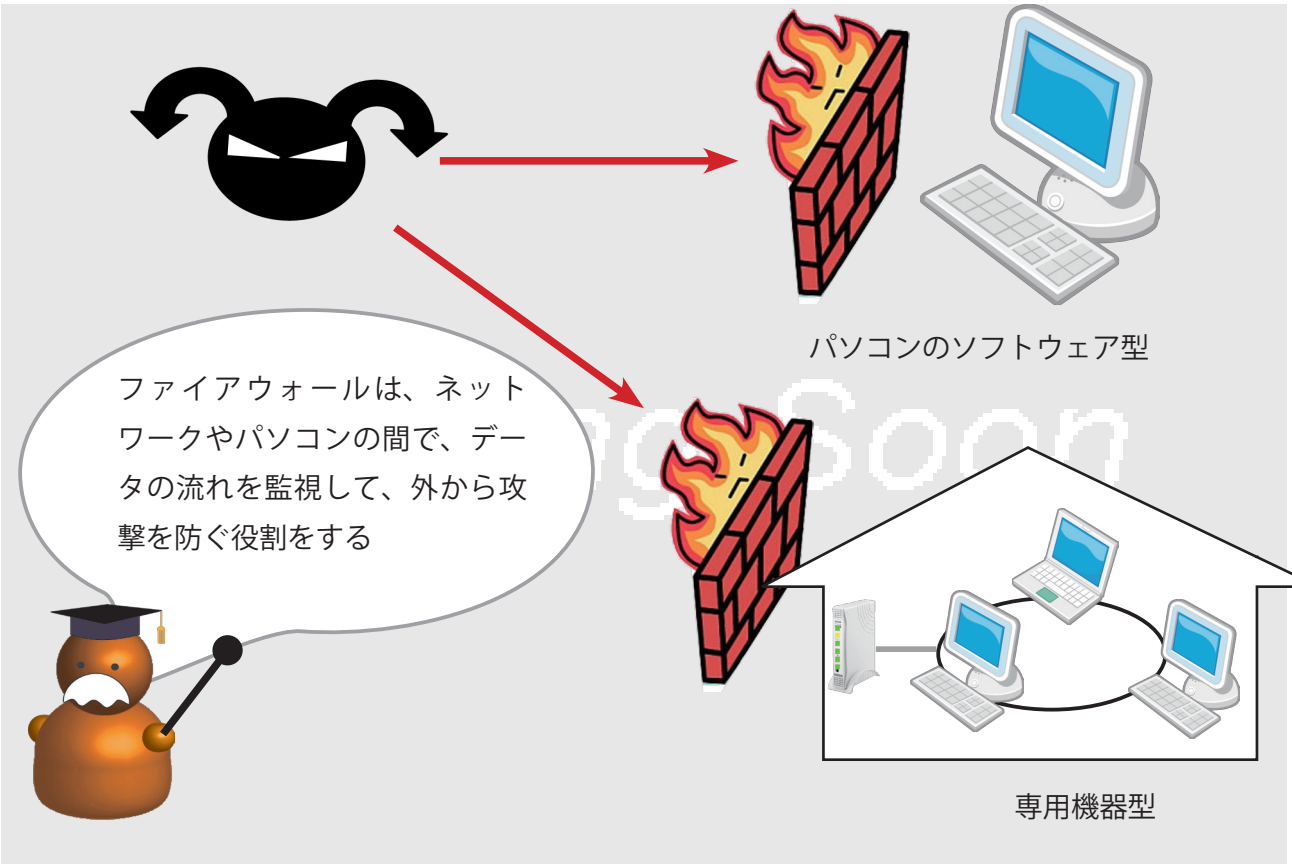
図 2　スポットウィルススキャン

ウィルスバスターでは「セキュリティ脅威の検索」、マカフィーでは「クイックスキャン」。各企業によって言葉は異なる。

関連する事項

◎ファイアウォール

22 安全安心対策：ファイアウォールの種類と働き



「ファイアウォール」とは、LAN などのネットワークまたはパソコンの外部ネットワークとの境界において、アクセスを制御するハードウェア並びにソフトウェアです。まさに、様々な脅威があるネットワークやパソコンの内側を守る防火壁の役割をします。具体的は､システムやネットワーク上のデータの流れを制御するもので、次の機能をもっています。

a) フィルタリング機能

内部から外部へ通してよいデータかどうか、逆に外部から内部へ渡してよいものかを判別します。外部から内部ネットワークやパソコンに不正に侵入しようとする動きを検知し、接続を遮断します。DOS 攻撃やセキュリティホールへの対策に有効です。

b) 内部と外部の通信を直接行わせないで、一端仲介をする

NAT によるアドレス変換がこれにあたります。ボット攻撃などで、外部からパソコンが直接操作されることへ有効とされています。

c) アクセス監視

どのような通信がされたのか等の記録をとり、外部からの攻撃に備えます。

ファイアウォールは、パソコンにインストールするタイプのものと独立した装置のものと大きく 2 つに分けることができます。前者は、市販されているセキュリティ対策ソフトに含まれています。Windows に標準装備されているファイアウォールは、前者に属するもので単体で販売されているもの　の簡易版です。

※ファイアウォール　Firewall
日本語に直訳すると火災時に類焼を防ぐ「防火壁」。インターネット上の被害が事務所や家庭そしてパソコンに及ばないように堰き止める役割をする。

※ DOS 攻撃
コンピュータに大量の信号を送りつけ、機能を停止させる攻撃。
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/yougo/eiji.htm#dos_kogeki

※ WindowsXp ファイアウォールとセキュリティ対策ソフトの同時使用
同時に使用しても、特に問題はありません。診療を受ける時のセカンドオピニオンドクターと似た関係にあると言えるでしょう。
双方を機能させると、パソコンが遅くなってしまう場合があります。その時は、WindowsXp ファイアウォールをきることをお薦めします。

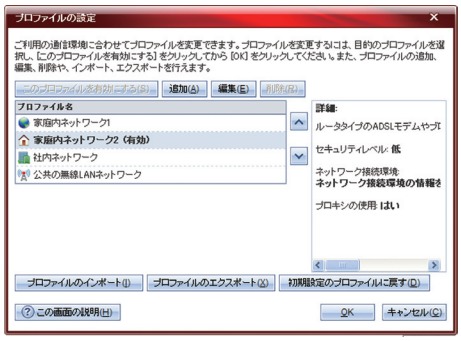
相談内容

・ファイアウォールって何？
・Windows ファイアウォールとの違いは？
・ファイアウォールの入手方法を教えて下さい
・突然、ネットワークにつながらなくなってしまいました
・突然、ネットワークプリンタが使用不可になった

安全安心へむけての一歩

市販されているセキュリティ対策ソフトに内蔵されているファイアウォールの使い方について、「ネットワーク環境に対応したファイアウォールの設定の仕方」と「" 許可 " と " 拒否 " の個別設定の仕方」を説明します。前者は既に用意されているプロファイルを使うもの、後者は個別に設定するものです。今までインターネットにつながっていたのにファイアウォールを入れた途端に接続できなくなった、ネットワークプリンタが使えなくなった場合には、以下の方法を試みて下さい。ここでは、トレンドマイクロ社ウイルスバスター 2009 を例にあげます。

ファイアウォールの設定 ★★☆

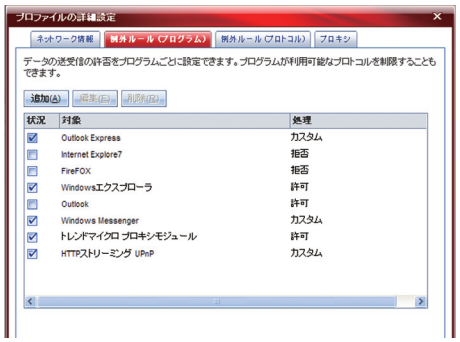


いくつかのネットワーク環境にあった設定ができるようになっています。セキュリティ対策ソフトによって多少ことなりますが、おおよそ次のようなプロファイルが用意されいます。

1. 家庭でブロードバンドルータを使わないでインターネットに接続する場合
2. 家庭でブロードバンドルータを使わないでインターネットに接続する場合
3. 事務所などのネットワーク
4. 公共の無線 LAN ネットワーク

それぞれの環境にあったファイアウォールの設定が用意されています。間違って設定すると、ネットワークを遮断されることがあります。

" 許可 " と " 拒否 " の個別設定 ★★★



用意されているプロファイルではうまく行かない場合、個別に設定したい場合にこの方法をとります。パーソナルファイアウォールは、利用するプログラム・プロトコル・ポートでインターネットとの通信を " 許可 " したり " 拒否 " を行います。例えば、Winny を拒否、telnet を許可などの個別設定が可能となります。

以上の細かな使い方は以下を参考にして下さい。

トレンドマイクロ　インターネット接続不可：ファイアウォールの設定変更
http://jp.trendmicro.com/jp/support/personal/products/netng/solution2/?ConSupWebclickID=clc_ded08_2
Macfee　ファイアウォールの設定例の紹介
http://www.mcafee.com/Japan/mcafee/support/faq/answer_f_spec.asp?wk=SP-00065
マイクロソフト　OneCare
http://support.microsoft.com/kb/923157/ja

関連する事項

◎パソコンを守る仕組み
◎悪意あるソフトウェア（マルウェア）　ボット
○ウィルス対策ソフト

重要用語

ファイアウォール

23 安全安心対策：暗号の活用

※暗号化
通信内容を第三者が読めず、取引相手と自分だけが読める表現にすること

※本人確認
インターネットショッピングなどでは、ショップと利用者が遠く離れている場合が多々あります。そこで、そのホームページがそのショップのものであるか、その利用者が本人であるかを確かめることを本人確認と言います。本人確認の手段として「電子認証」という技術があります。

※暗号の鍵は、PC や IC カードに保管されており、その使用をパスワードで管理している場合もあります。

インターネット上では、データはガラス張りのところを流れるようなものです。クレジット番号や個人情報など大切な情報は暗号化して扱った方がよいでしょう。インターネットショッピングなどでは、すでに暗号化がおこなわれています。URL が "https://・・・・" となり、ブラウザの下に鍵マークがある時は、そこで入力された情報は、暗号化され相手に伝わります。また、暗号と同時に、そのホームページが偽装されておらず本物であることも証明します。鍵マークにカーソルと当てると本物であることを証明する第三者機関（認証局）の名前が表示されます。このように、暗号は、通信内容を第三者が読めない状態にするだけではなく、本人確認にも利用されており、インターネットにも必要不可欠なものとなってきています。税務署や役所へインターネットを使った電子申告にも、暗号による本人確認がなされます。今後、暗号はますます利用されてくるでしょう。

実は、暗号は気軽に使うことができます。パソコンの中の大切なデータを簡単に暗号化することができます。ファイル、フォルダ、ハードディスクなどぞれぞれに暗号をかけ保存することができますので、必要に応じて試してみるとよいでしょう。情報漏洩や PC の盗難に備えて、PC 内の大切な情報を暗号で管理することは効果的な予防策と言えます。

暗号をかけたり外すには「鍵」が必要です。この「鍵」を忘れると解読できなくなります。また、「鍵」が盗まれると暗号は簡単に破られてしまいます。「鍵」はしっかり管理する必要があります。

相談内容

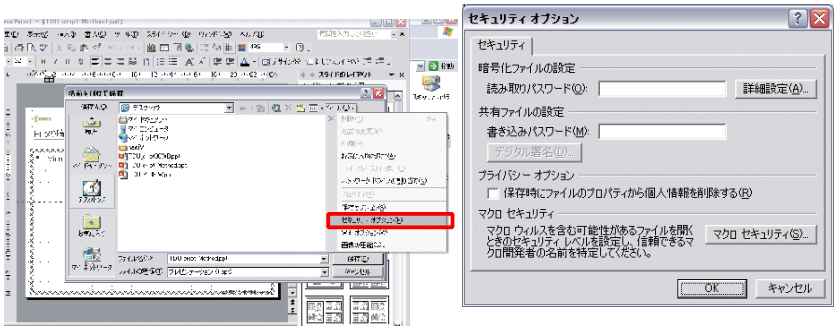
・暗号ってなに？
・大切な情報はどう管理すればよいでしょう？

安全安心へむけての一歩

★★★

ここでは、ファイル、フォルダ、ハードディスクを暗号化する方法、暗号機能をもつ USB を紹介します。

ファイルの暗号化



1.Microsoft 社 の Office 製 品、Word、Excel、Powerpoint は、保存する際にオプション」→「セキュリティオプション」で暗号化できます。
2.「セキュリティオプション」で、「読み取り」「書き込み」をパスワードで制限できるとともに、「電子署名」も可能です。この機能は、Microsoft 社の製品以外に、Adobe 社のものなどいくつかの製品に実装されています。

フォルダの暗号化

ハードディスクを外し直接 USB などで他のパソコンに接続しデータを読み取ることができます。パソコンが盗まれた場合ログイン時のパスワードは無力となってしまいます。その予防にフォルダを丸ごと暗号化することができます。
フォルダの暗号化　Windows Xp の場合
http://www.microsoft.com/japan/windowsxp/pro/business/feature/security/cryptical.mspx

ハードディスクの暗号化

ハードディスクを丸ごと暗号化するには、大きく分けて 2 つの方法があります。一つは専用のソフトを使うものです。一例として Truecrypt というものがあります。もう一つは、パソコンにもともと備わっている機能を利用するものです。その機能には BIOS で HDD パスワードでハードディスクを保護するものなどがあります。パソコンのマニュアルやホームページで調べてみましょう。
Truecrypt　http://www2.atwiki.jp/tcjpdoc/

暗号機能付き USB メモリ

USB メモリは便利ですが、紛失しやすいという欠点があります。個人情報等をどうしても入れたい時は、落としても第三者から読み取れない暗号機能付き USB メモリを使用することをお薦めします。USB メモリ差し込むとパスワードを要求されるものや決まったパソコン以外には読み取れないなどいろいろなものがあります。
I-O DATA 機器　http://www.iodata.jp/promo/security_usbmemory/
BUFFLO　　http://buffalo.jp/products/catalog/flash/security_usb/

関連する事項

○ 24、安全安心対策：バックアップ、p.47
◎ 25、安全安心対策：PC と情報の取り扱い、p.49

重要用語

LAN、NAT、グローバルアドレス、プライベートアドレス

24 安全安心対策：バックアップ

※バックアップファイル
バックアップする場合、フォルダをそのまま他のハードディスクへコピーする方法と、一つのファイルにまとめてしまう方法があります。前者は、バックアップ元と同じ状態ですので、必要なファイルなどを簡単に取り出すことができます。後者はすでにまとめられているのでそれができませんが、コンパクトであったり、復元が確実であるなどの利点があります。

※完全、完全（同期）、差分、増分
バックアップする際、どのようにデータを移行するかによって異なります。
「完全」：必要なデータ全てを一度にまとめて一括に複製する
「差分」：前回のフルバックアップ時からの変更／追加されたデータのみを複製する
「増分」：直前の増分バックアップの変更／追加分だけが複製する。
http://ja.wikipedia.org/wiki/%E3%83%90%E3%83%83%E3%82%AF%E3%82%A2%E3%83%83% 83% E3% 83% 97

最近のパソコンは丈夫になったとは言え、衝撃・水・過電圧などで大切なデータが消えてしまうこともあります。突然の故障やシステムの不具合でもデータが取り戻せなくなることがあります。バックアップは、パソコンの状態を保存しておくことです。トラブルが起こったときには以前の状態に戻すことができます。バックアップは定期的に行いましょう。ここでは、パソコンのシステムを保存する場合、データを保存する場合に分けて考えます。

システムのバックアップ

a) WindowsXp に標準装備されている「システム復元」
ある時点での WindowsXp の状態を記憶しておき、その後インストールや設定などで不具合が生じたい場合に、以前の状態に戻す。

b)PC 全体を外部の記憶装置へ保存
WindowsXp に付属しているバックアップ機能を使い、PC のハードディスク全体を保存します。専用のバックアップソフトウェアも市販されています。

データのバックアップ

c)「マイドキュメント」など必要な範囲のデータを保存
WindowsXp に標準装備されているバックアップ機能を使います。専用のバックアップソフトウェアも市販されています。
用途に応じてバックアップ方法を選択しましょう。また、バックアップしたファイルはその PC とは別途に保管し、復元に必要なソフトウェアや機器は前もって用意しておきましょう。

相談内容

・バックアップのとり方は
・復元の仕方
・間違えて大事なファイルを削除してしまいました

安全安心へむけての一歩

★★☆

ここでは、WindowsXp に標準装備されている「システムの復元」と「バックアップ」について説明します。

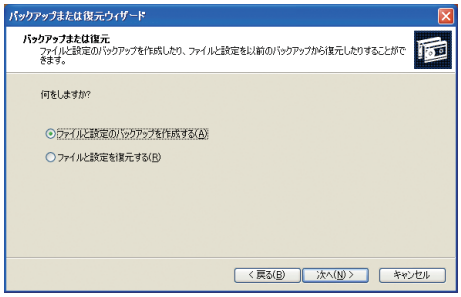
システムの復元

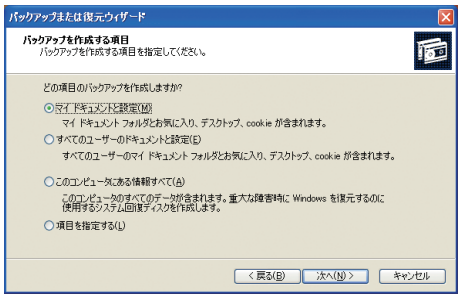
1.「スタート」→「すべてのプログラム」→「アクセサリー」→「システムツール」→「システムの復元」を選びます。
2. 現在のパソコンの状況を記憶させる為「システムの復元点を作成する」を選び、「次へ」進みます。システムの復元点に名前をつけ保存します。
3. システムを復元するには、1 から「システムの復元」を選び、2 で作成した復元点を選び「次へ」進みます。システムは自動的に終了し、システムが設定した時点に復元されます。

詳しくは、http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

バックアップ

1.「スタート」→「すべてのプログラム」→「アクセサリー」→「システムツール」→「バックアップ」を選びます。
2. バックアップウィザードが開きます。指示に従い進み「ファイルの設定とバックアップを作成する」を選び「次へ」進みます。
3.「バックアップを作成する項目」で、コンピュータ全体、マイドキュメントだけ、必要なフォルダだけとバックアップする項目を選びます。
4. バックアップは一つのファイルとして保存されます。その保存場所をしてい「次へ」進むとバックアップが完了します。
5, 復元は 2 で「ファイルと設定を復元する」で行います。コンピュータ全体の場合は、専用の起動ディスクを使います。これはバックアップ途中で作成されます。





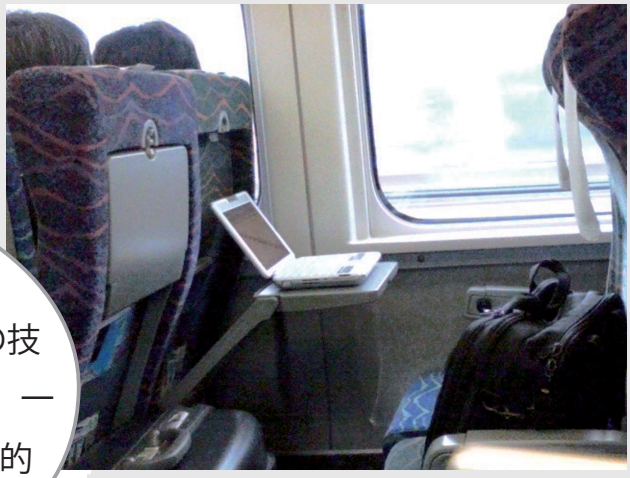
関連する事項

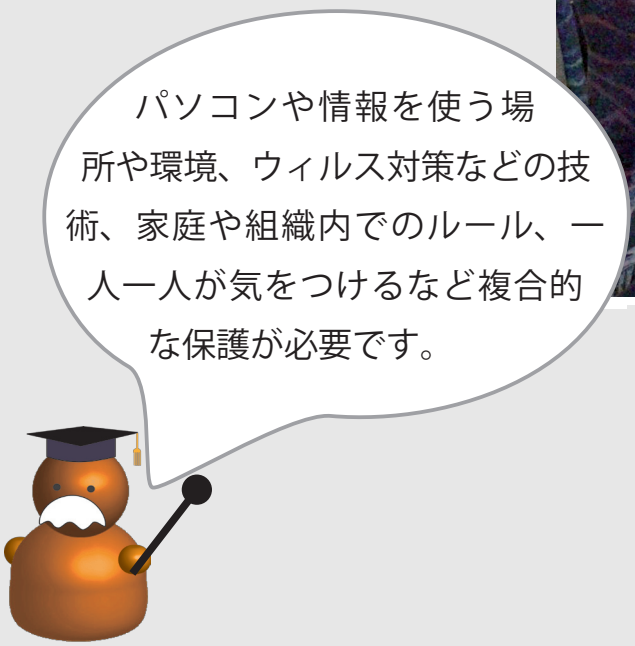
◎ PC と情報の取り扱い

重要用語

バックアップ
システムの復元
完全、差分、増分バックアップ

25 安全安心対策：PC と情報の取り扱い





情報はパソコン内だけではありません

パソコンだけに大事な情報があるわけでもありません。名簿、記名されたアンケート、連絡網など紙に記載された情報も個人情報として守らなければなりません。

また、セキュリティ対策ソフトを入れれば十分という訳ではありません。上の写真のように、新幹線内で持ち主がトイレへ行っている間置き去りにされたパソコン、誰でもその情報を見ることができます。これ以外に個人情報が入っているパソコンを酔って電車内に忘れてしまった、患者データを無断で自宅へ持ち出し泥棒に入られてしまった、いくら OS のアップデートをしてもこれでは意味がありません。大事な情報をどう守るのかという観点が必要です。

情報は完全でなければなりません

せっかく守ってもそれが誤った情報では意味がありません。そればかりか、自分たちの不利になったり、人に迷惑をかける場合があります。例えば、破産情報が誤っており、ローンを組めないということがありました。情報は正しく完全なものである必要があります。

情報は使って初めて意味があります

情報は守られる為にのみあるわけではありません。それらを使って私たちの生活が豊かになります。保護管理する一方で、パソコンや情報を必要であればいつでも使えるようにしておく必要があります。

相談内容

- セキュリティ対策ソフトを入れておけば十分ですよね
- 情報保護はどのようなやり方をすればよいのでしょうか？
- 非営利団体や家庭ではどういうルールをつくればよいの？

安全安心へむけての一歩

情報は使われることで価値が出てきます。一人で使う場合よりも何人かで使うことが多いでしょう。そこでそれぞればらばらに対策やルールを決めるのではなく、組織全体としてどう情報を扱い守るかという視点が必要になります。ここではその一例を上げます。

a) 家庭や組織内でのルールづくり
ひとりが気をつけても、家庭や職場などで情報やパソコンを共有するところでマルウェアに感染することがあります。それぞれの家庭や組織で、社会全体で情報社会の安全安心について考え、情報やパソコンの扱い方のルールを考えることが必要です。その為に、情報セキュリティ責任者のような役割をする人を決めておくことも有効です。
b) 何を守るか
すべての情報を守ることはできません。どんな情報が大切なのかを決め、必要ない情報は思い切ってすてましょう。
c) 情報やパソコンを使う場所や環境
大事な情報やそれが入っているパソコンをどう管理するかも考えなければなりません。また、それらをどこで使うのか、誰ならば使えるのかも決めておく必要があります。電車の中で個人情報を開かないなどという配慮も必要です。盗まれないようにしましょう。情報はパソコンの中だけにあるわけではありません。名簿や写真など紙媒体、ビデオテープ、CD/DVD などもきちんと管理しましょう。特に個人情報やプライバシーに関する情報は厳重に保管しましょう。また、電源やネットワークなどパソコンが快適に使えるような環境を整えることも大切です。
d) マルウェア対策などへの技術的対策
すでに多く見てきたように、パソコンにマルウエア感染させ機密情報を不正取得しようとします。それらの攻撃を防ぐ技術的な対策をとる必要があります。OS のアップデート、セキュリティ対策ソフトの導入とアップデートをいつ行うかもルール化しておくとよいでしょう。
e) 教育や心構え、モラル
ルールづくりをしても、その大切さを認識しなかったり、あえてそれを破るということでは意味がありません。それぞれの家庭や組織で、情報やパソコンを守る大切さに間する正しい知識を共有し話し合うことが必要です。
f) 見直し
情報やパソコンを守ったつもりでいても、十分ではない時もあります。定期的に現状を見直し改善点を洗い出す仕組みを前もって作っておくことが大切です。

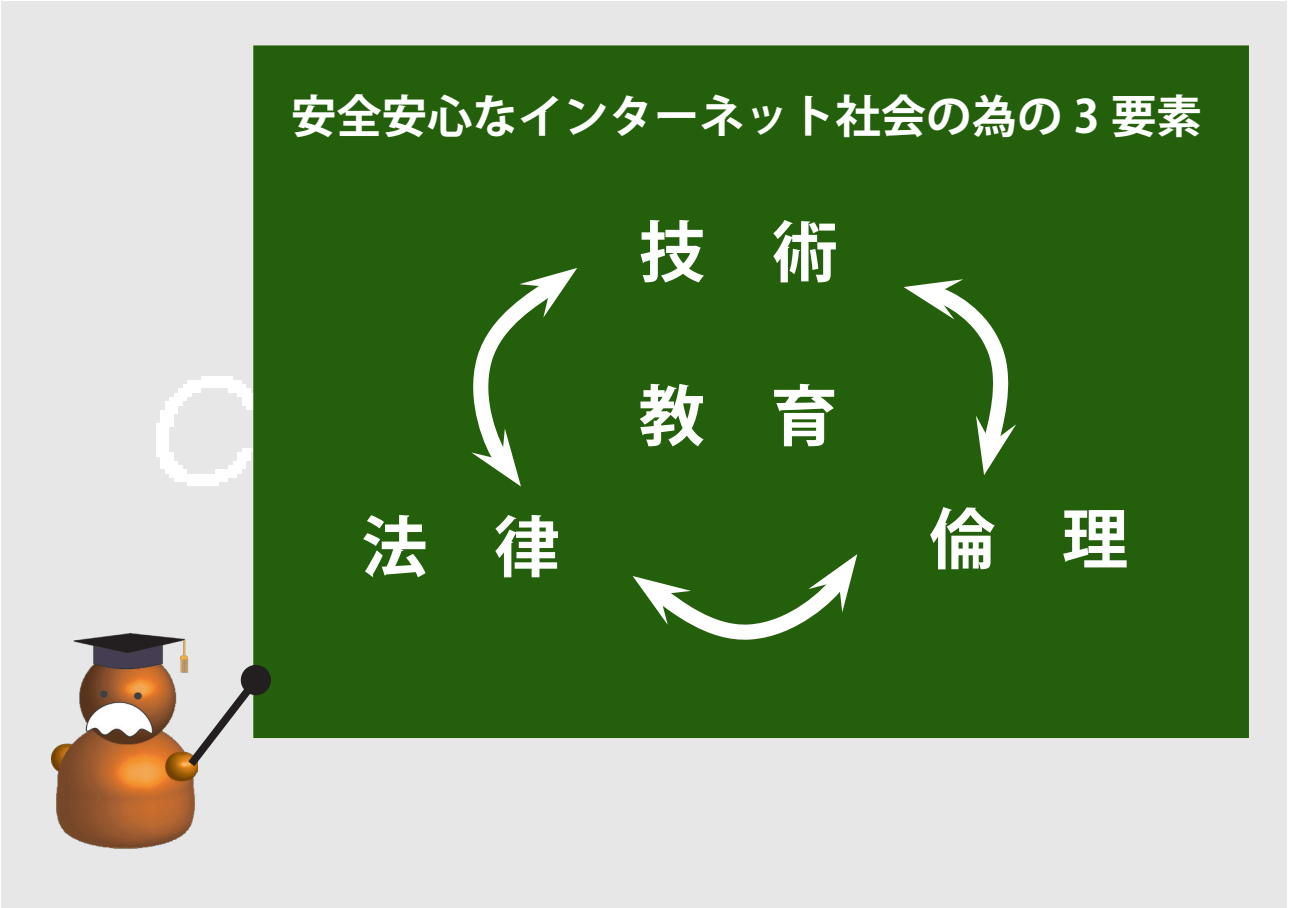
関連する事項

○ 19、インターネット関連法、p.37
◎ 26、安全安心なインターネット社会へむけて、p.51

重要用語

情報の機密性、完全性、可用性
情報セキュリティマネージメント

26 安全安心なインターネット社会へむけて



安全安心なインターネット社会の実現の為には、法的整備が必要です。社会に対して明確な規範を示さねばなりません。その実現の為に、保護技術や犯人を追い詰める技術は必要不可欠です。逆に、技術が先走り「可能なことはやってもよい」ことにならないよう規制するのは法律です。

日々進む技術そしてそれに合わせて出てくる攻撃すべてに対応することは不可能です。仮に可能であったとしても、多大な労力を私たちに強いることとなるでしょう。強すぎる法律も私たちの生活を窮屈なものとなり尊重されないこともままあります。技術的対応も法的対応も、それなりに自由度が必要ということになります。そもそも、法律も技術も、新しい問題にすぐに対応することはできません。法的規制がない、技術的に可能なら何をやってもよい、ということは正しくありません。社会全体のことを考えて、自分を律することも必要です。

また、確信犯という人がいます。「あえて法律を破る」という態度には、法は無力です。これら法律や技術がには、どうしても限界があります。
そこで、現状や問題点をひとりひとりが知って、それぞれが守らなければならないことを守ることが必要になります。それは、強制ではなく納得してもらい自主的にでなければならないでしょう。その為に、教育は大きな要素となります。

相談内容

- 私ぐらいがアップデートをしなくてもいいよね
- 大事な情報がないから、セキュリティはいいや
- どうしても、アップデートをしてくれません
-

安全安心へむけての一歩

セキュリティを学び、学んだことを実行するにあたり注意するべきこと、SPREAD サポータとして行動する上で必要なことをあげます。

- 「自分だけ」ということでは、セキュリティは守ることができません。みんなで社会をよいものにしようという意識が重要です。
- マルウェアの感染は、被害者だけではなく、加害者にもなります。
- 技術的対策には、OS のアップデート、Office などアプリケーションのアップデート、セキュリティ対策ソフトの導入と更新のすべてが必要です。
- インターネット社会の法律は、それ以前の法律と違うところがあります。知らないうちに犯罪者になることもあります。
- これで大丈夫ということはありません。常に状況は変わります。常に勉強、反省が必要です。
- ある人にとっては都合のよいことでも、他の人にとってはそうでないなど、「権利の衝突」する時があります。それには立場によって様々な意見や解決方法があります。「これが正しい」ということは難しい場合があります。
- 正しいことでも、人によっては対処することが難しい場合があります。その人の事情に配慮して計画しましょう。
- 技術的にできるからと言ってやってよいこととはかぎりません。サポータは倫理を尊重しなければなりません。
- 特定の商品やサービスを進めたり非難することには、責任が生じます。慎重に行いましょう。
- 情報社会の安全安心は、一部の組織や人の利益の為ではありません。常に社会全体の利益を考えるべきです。
- まず、自分が、どのようなポリシーをもって、自分の情報セキュリティに対して取り組むかを定め、実行しなければなりません。
- 話し方、礼儀、相手への配慮など、日頃からのコミュニケーションの仕方に注意しましょう。
- トラブルは隠蔽してはいけません。その原因を探り適切に解決し公表しなければなりません。
- 扱える時間や経費は有限です。無理無駄がないようにするコスト的視点も重要です。

情報セキュリティを進める上で、自分なりの 7 箇条を作って下さい。

1，
2，
3，
4，
5，
6，
7，

SPREAD（スプレッド）サポーター検定　公式テキスト　β版

発行日　2009 年 3 月 31 日
発　行　セキュリティ対策推進協議会
105-0003
東京都港区西新橋 1-22-12 JC ビル 3F　NPO 日本ネットワークセキュリティ協会内
Tel:：03-3581-8860　　Fax：03-3519-6441
Mail：sec@spread-j.org　　URL：http://www.spread-j.org

製作編集　特定非営利活動法人　イーパーツ　会田和弘