

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

<http://www.ipa.go.jp/security/>

ウイルス対策7箇条

1

ワクチンソフトは
最新版を活用すべし

2

メールの添付ファイルは
まず、ウイルス検査すべし

3

ダウンロードしたファイルは
まず、ウイルス検査すべし

4

アプリケーションは
セキュリティ機能を活用すべし

5

セキュリティパッチを
あてるべし

6

ウイルス感染の兆候を
見逃すなかれ

7

万ーのためにデータは
必ずバックアップを行うべし



本ページの「ウイルス対策7箇条」はポスターとなっています。このポスターは、「15分でわかるウイルスの脅威」(ウイルス対策普及啓発のための動画コンテンツ)の劇中で使用したものです。入手先は以下の URL です。ご利用下さい。

<http://www.ipa.go.jp/security/y2k/virus/cdrom2/documents/7kajyou.pdf>

参考:「15分でわかるウイルスの脅威」

<http://www.ipa.go.jp/security/y2k/virus/cdrom2/>

1. ワクチンソフトは...最新版を活用すべし

ウイルス対策には、ワクチンソフト(ウイルス対策ソフト)が必須です。

ワクチンソフトを使用している方は、ウイルス対策エンジンおよびウイルス定義ファイルを最新にして、ウイルス検査を実施して下さい。

ウイルスは、常に新種が登場しています。一つの種類のウイルスも、次々に亜種が登場する状況です。そのために、ワクチンソフトを、新しいウイルスに対応できる状態に保つ必要があるわけです。

ワクチンソフトには、ウイルス定義を自動的に更新する機能が付いています。この機能を利用するか、こまめにウイルス定義の更新を行きましょう。

パソコンを購入した際に、ワクチンソフトの試用版がインストールされている場合がありますが、一定期間を過ぎると、利用できなくなったり、ウイルス定義ファイルを更新できなくなったりするものもあります。ご注意下さい。

ワクチンソフトをすぐに用意できない方で、インターネットに接続できる方は、無償のオンラインスキャン(オンラインでのウイルス検査サービス)を提供するワクチンベンダーがありますので、そちらを利用して、ウイルス検査を実施して下さい(12頁を参照下さい)。ただし、リアルタイムにチェックすることはできないので、ワクチンソフトを導入することをお勧めします。



2. メールの添付ファイルは...まずウイルス検査すべし

ウイルスは、電子メールの添付ファイルに仕掛けられている場合が多くなっています。よく知った友人からのメールでも、添付ファイルはウイルス検査を行ってから開くようにしましょう。

最近では、差出人を詐称したウイルスメールが多く見受けられます。このようなウイルスメールからパソコンを守るために、見ず知らずの人からのメールやプロバイダを装ったメールも注意が必要です。よく知った人どうしてメール交換を行う場合、ファイルを添付する必要があるのであれば、メールの本文中に、添付ファイルがある旨のコメントおよび添付ファイルの内容に関するコメントを付けると、良いかも知れません。それでも、念のために、添付ファイルを開く前にウイルス検査を実施するように、心掛けましょう。念には念を入れる...これが大切です。






また、添付ファイルの拡張子(ファイル名の末尾にある3文字程度のアルファベット)が以下のような場合は、特に注意が必要です。ただし、Windows のフォルダオプションには「登録されたファイルの拡張子を表示しない」という設定もあるので注意して下さい…チェックを外すことをお勧めします(5 頁を参照下さい)。

				
xxxxx.exe	xxxxx.pif	xxxxx.scr	xxxxx.bat	xxxxx.com

ファイルタイプの説明
 exe : アプリケーション
 pif : MS-DOS プログラムへのショートカット
 scr : スクリーン セーバー
 bat : MS-DOS バッチ ファイル
 com : MS-DOS アプリケーション

これらの拡張子のファイルは、開いたとたんにパソコン上で動き始めます。これらのファイルがウイルスである場合(必ずしも、これらの拡張子のファイルがウイルスであるとは限りませんが)、あなたのパソコンが感染することになり、個人情報盗まれたり、ハードディスクの内容が破壊されたり、最悪の場合はパソコンが乗っ取られたりする場合があります。ご注意ください。

ウイルスによっては、ファイルタイプをごまかすために、ファイルのアイコンを詐称したり、二重に拡張子を指定したりする場合があります。

		
お知らせ.doc	お知らせ.exe	お知らせ.doc ...
Word 文書 これは、正しい例です(アイコンと拡張子が一致しています)	アイコンをごまかしたアプリケーション Word 文書のアイコンで偽装しています (Word 文書ではありません)	さらに二重に拡張子を指定してごまかしたアプリケーション ファイル名が長すぎて、ファイル名が全部見えない(...で表示)場合があります

本来、Word の文書ファイルであれば のようになりますが、ファイルタイプがアプリケーションであるファイルのアイコンをごまかしたものは のようになります。さらに、二重に拡張子を指定した場合は のようになります。

例えば、 のファイルがメールに添付されて送られてくると、下図のようになります。

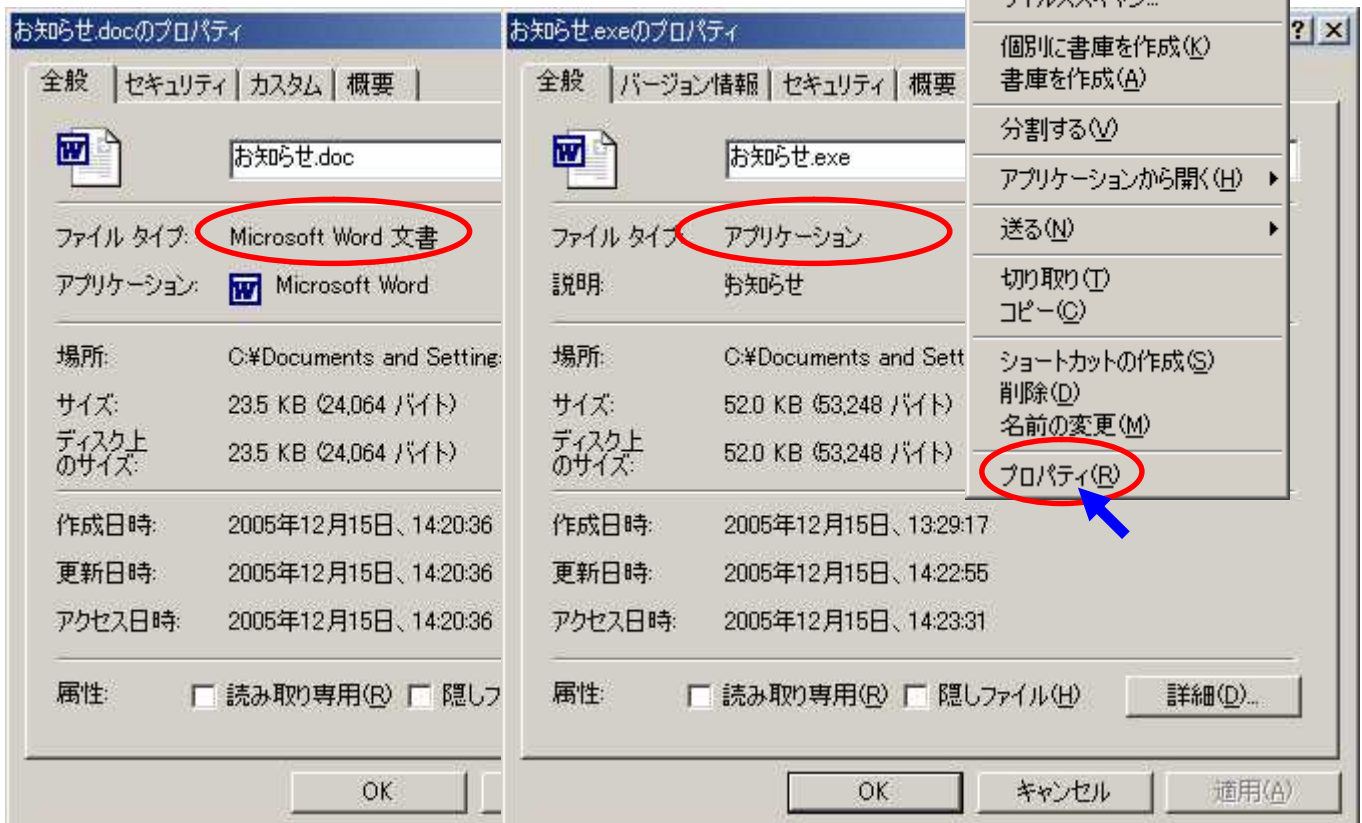


ファイルタイプを調べる手段として、以下に示す方法もあります。

例えば、 と のファイルについて調べる場合は、ファイルを選択した状態で、マウスの右クリックを行い、[プロパティ]を選択します。

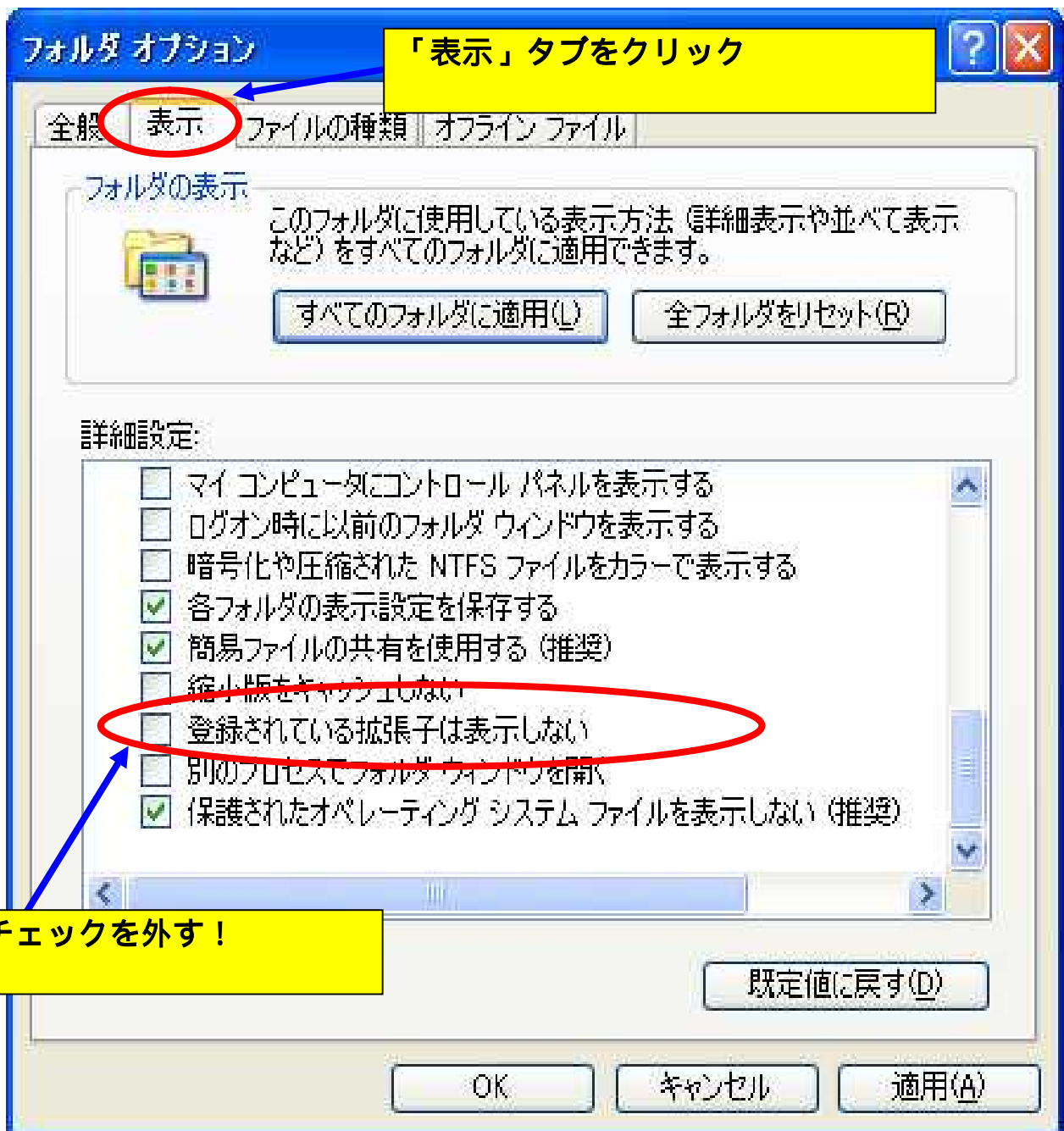
の プロパティ

の プロパティ



ファイルの拡張子を表示する設定

Windows の初期設定では拡張子が表示されないようになっていますので、マイコンピュータ もしくはエクスプローラ のメニューバーから [ツール] [フォルダオプション] を選択し、[表示]タブ内の[登録されている拡張子は表示しない] のチェックを外し、拡張子を表示させるようにします(下図を参照して下さい[Windows XP の場合])。

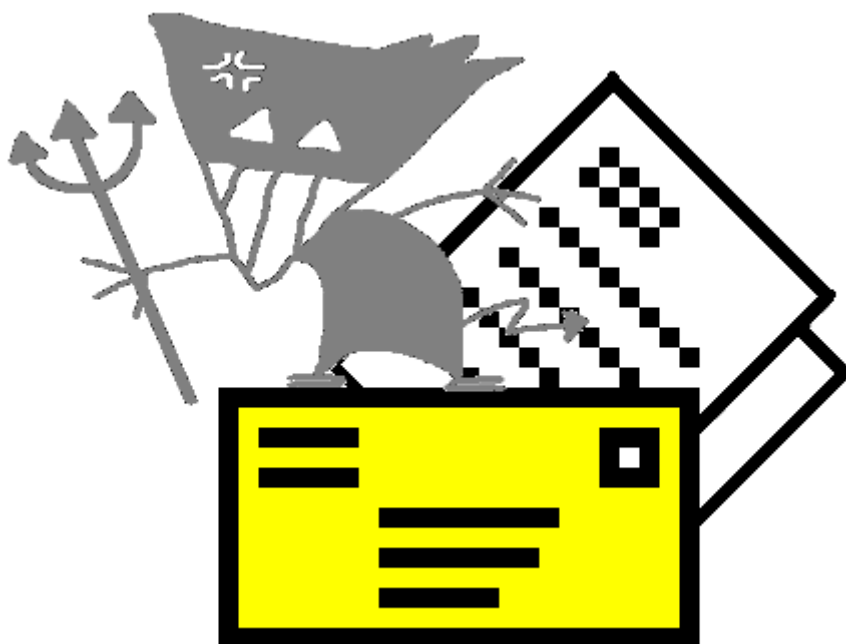


【メールの添付ファイルの取り扱い 5つの心得】

- (1)見知らぬ相手先から届いた添付ファイル付きのメールは
 厳重注意する
- (2)添付ファイルの見た目に惑わされない
- (3)知り合いから届いたどことなく変な添付ファイル付きのメ
 ールは疑ってかかる
- (4)メールの本文でまかなえるようなものをテキスト形式等の
 ファイルで添付しない
- (5)各メーラー(メールソフト)特有の添付ファイルの取り扱い
 (*)に注意する

<http://www.ipa.go.jp/security/antivirus/attach5.html>

(*)メーラー(メールソフト)が、添付ファイルを取り扱う方法をよく把握して使用することが重要です。例えば、一部のメーラーでは、メール受信時に、添付ファイルをあらかじめ指定されたフォルダに自動的に保存します。このようなメーラーを使用している場合は、ウイルス検出時等、メール本文ごと添付ファイルを削除したときに、保存されている複製も忘れずに削除されるような設定にする必要があります。



3. ダウンロードしたファイルは...まずウイルス検査すべし

インターネットから、画像ファイル、音楽ファイル、映像ファイルなど、いろいろなファイルをダウンロードできますが、これらのファイルに不正なプログラム(命令コード)が埋め込まれている場合があります。ダウンロードしたファイルは、ウイルス検査を行ってから使用するようにしましょう。



同じように、フロッピーディスクや CD 等の外部記憶媒体に格納されたファイルも、入手先や入手経路が不明な場合は、ウイルス検査を行ってから使用するようにしましょう。

素敵なプレゼント?

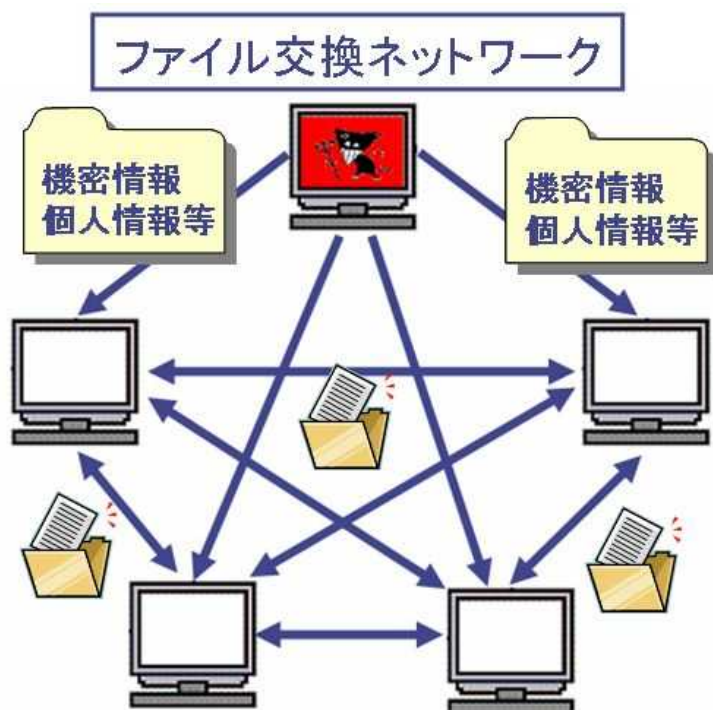


また、ファイルのダウンロードを行う場合は、できるだけ信頼のおける Web サイトから行うようにしましょう。スパムメール^(*)などに記載された Web サイトからのダウンロードや、怪しげな Web サイトからのダウンロードは、なるべく避けるべきです。

最近、Winny などのファイル交換ソフト^(*)を悪用したウイルスにより、組織からの個人情報や機密情報等の漏えいが発生しています。

一度、情報がインターネットに漏えいしてしまうと、その情報を回収することは技術的にほとんど不可能と言われており、重大なトラブルに発展することになります。

このウイルス (Antinny) は、ファイル交換ソフト (Winny) にウイルスファイルを流通させることで感染を拡大します。ファイル交換ソフトで入手したファイルについても、必ずウイルス検査を行ってから使用するようし、トラブルの発生を未然に防ぐよう対処して下さい。



4. アプリケーションは...セキュリティ機能を活用すべし

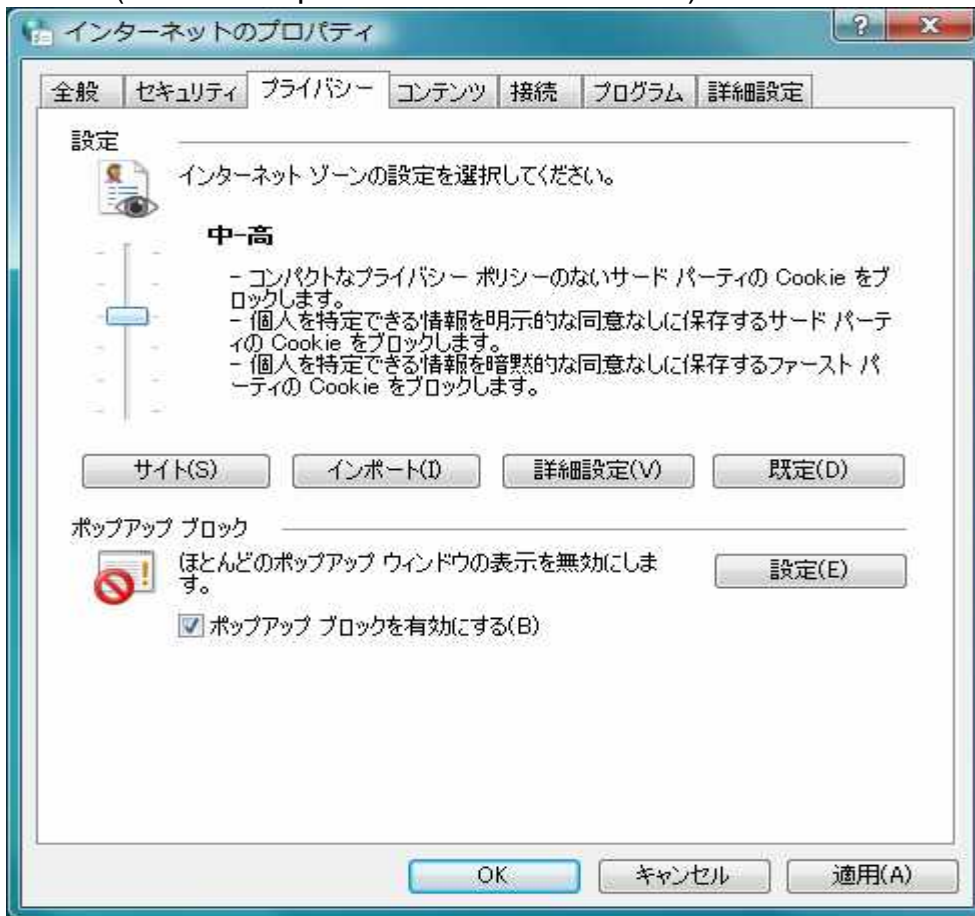
メールの送受信に使用するメーラーや、インターネット上の Web サイトを閲覧するためのブラウザなどを使用する場合は、それぞれのアプリケーションに用意されているセキュリティ機能(設定)を活用しましょう。



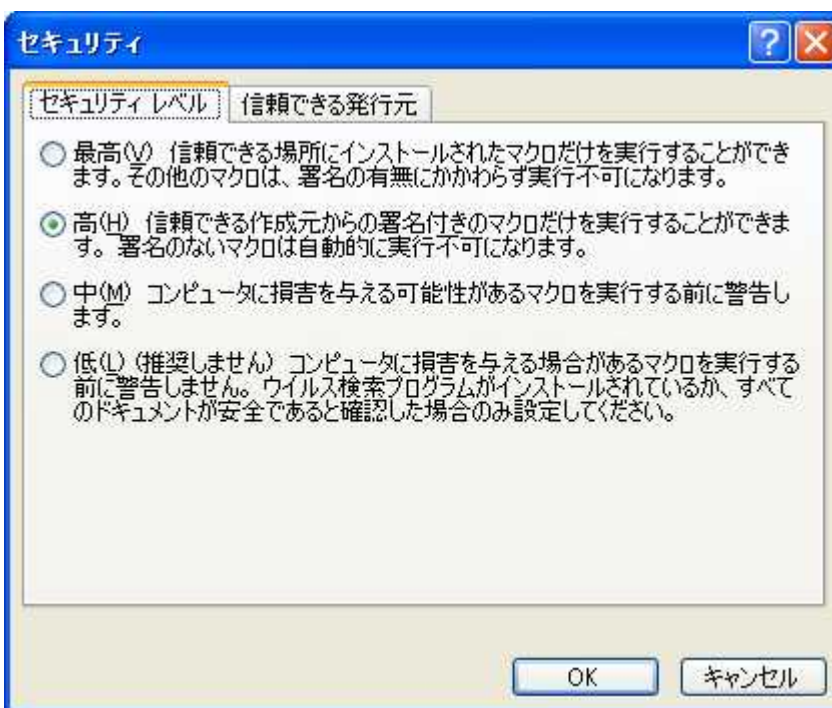
例えば、マイクロソフト社の Internet Explorer 6 をお使いの場合は、インターネットオプション([スタート] [設定] [コントロールパネル] [インターネットオプション])で、セキュリティのレベルを設定できます。この場合、セキュリティのレベルは『中』以上を設定することをお勧めします。また、Internet Explorer 7 をお使いの場合は『中高』以上を設定することをお勧めします。(下図は Internet Explorer 7 のインターネットオプション設定画面)



あわせて、スパイウェア対策として、プライバシーの設定についても『中-高』以上を設定(Internet Explorer 7 の場合の設定例)することをお勧めします。



また、最近では古いタイプのウイルスとなっていますが、**マクロ感染型ウイルス**^{(*)3}



からの感染防止対策として、マイクロソフト社の Word や Excel のデータファイルを開くときに、マクロ機能の自動実行を無効にする (Word 2003 の場合:[ツール] [オプション] [セキュリティ] [マクロのセキュリティ])などのセキュリティ機能を活用する方法もあります。

これらの設定を行うことで、ウイルスからの被害を未然に防ぐことができます。

5. セキュリティパッチを...あてるべし

最近のウイルスは、オペレーティングシステムやアプリケーションの**ぜい弱性**^(*4)(セキュリティホールとも言われる)を狙ったものが増加しています。あなたのパソコンに、これらのぜい弱性が残っていると、メールをプレビューしただけで、あるいは、インターネット(ネットワーク)につないただけで、ウイルスに感染する可能性があります。

例えば、電子メールの添付ファイルの自動実行を許してしまうメーラーのぜい弱性は、ウイルス感染被害を著しく増大させる可能性があります。このようなぜい弱性は、頻繁に発見されているので、使用しているアプリケーション(特に、メーラー、ブラウザ、PDF 閲覧ソフト、一太郎ワープロソフト)に関してベンダーの Web サイトなどの情報を定期的に確認し、**最新のセキュリティパッチをあてておくことが重要です。**



さらに、ぜい弱性によっては、インターネットにつないただけで、ウイルスに感染する場合があります。2003年8月に発生した W32/MSBlaster や W32/Welchia、さらに2004年5月に発生した W32/Sasser などが、パソコンが再起動を繰り返すことで有名になりました。

最近、話題になっている**ポット**^(*5)と呼ばれるコンピュータウイルスも、インターネットを通じて感染を広げる場合があります。

Windows 利用者は、Microsoft Update を定期的 to 実施するか、自動更新設定を行って下さい。Microsoft 社が提供している OS に用意されたパッチ、および Internet Explorer や Office 製品等に用意されたパッチが適用できます。

●Microsoft Update

<http://update.microsoft.com/microsoftupdate/>

Microsoft Update の使い方については、以下の Web サイトが参考になります。

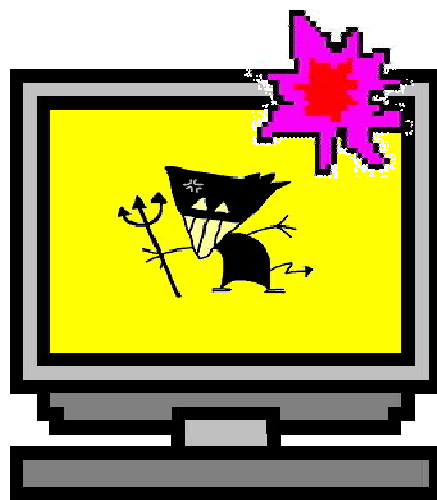
●Microsoft Update の使い方

http://www.microsoft.com/japan/athome/security/update/j_musteps.mspx

6. ウイルス感染の兆候を...見逃すなかれ

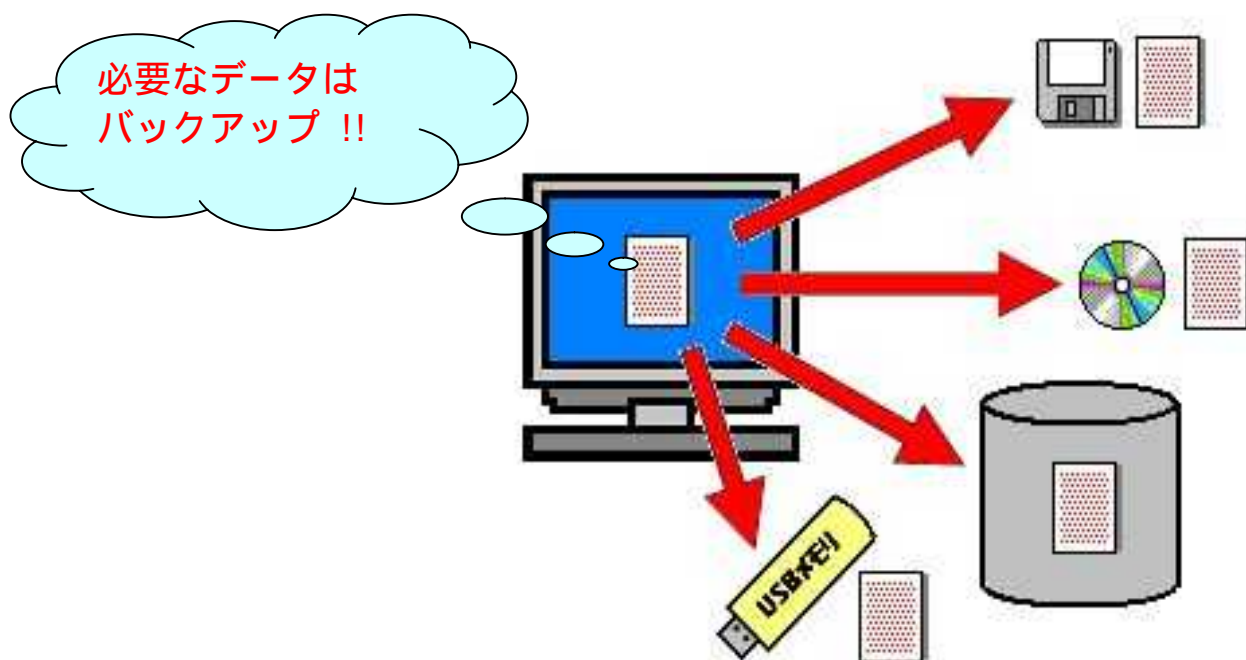
下記のような兆候がある場合、ウイルス感染の可能性が考えられるため、これらを見逃さず、ウイルス検査を行って下さい。

- (1) システムやアプリケーションが頻繁にハングアップ(途中で動かなくなる)したり、システムが起動しなくなったりする
- (2) ファイルが無くなる。見知らぬファイルが作成されている
- (3) タスクバーなどに妙なアイコンができる
- (4) いきなりインターネット接続をしようとする
- (5) ユーザの意図しないメール送信が行われる
- (6) 直感的にいつもと何かが違うと感じる



7. 万一のためにデータは...必ずバックアップを行うべし

ウイルスにより破壊されたデータは、ワクチンソフトで修復することはできません。ウイルス感染被害からの復旧のため、日頃からデータのバックアップをとる習慣をつけておきましょう。また、アプリケーションのオリジナルCD-ROM等は大切に保存しておきましょう。万一、ウイルスによりハードディスクの内容が破壊された場合には、オリジナルCD-ROM等から再インストールすることで復旧することができます。



8. 万一、ウイルスに感染したならば・・・

ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、コンピュータの検査を実施して下さい。ウイルス名は特定できたが、ウイルスの駆除や隔離ができない場合は、使用したワクチンソフトの(ワクチン)ベンダーの Web サイトで、検出されたウイルスの情報を探し、そこに記述されている対策方法についてお試し下さい。

ワクチンソフトを使用していない方で、ネットワークに接続できるのであれば、ワクチンベンダーが提供している、無償のオンラインスキャン(オンラインでのウイルス検査サービス)を利用することで、ウイルス名を特定できる可能性があります。ウイルス名が特定できたならば、オンラインスキャンと同じ Web サイトで、検出されたウイルスの情報を探し、そこに記述されている対策方法についてお試し下さい。

代表的なワクチンベンダーのオンラインスキャンを以下に紹介します。

- シマンテック Security Check
<http://www.symantec.com/region/jp/securitycheck/>
- トレンドマイクロ オンラインスキャン
http://www.trendflexsecurity.jp/security_solutions/housecall_free_scan.php
- マカフィー・フリースキャン
<http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp>

それでも、よく分からないとおっしゃる方は、コンピュータウイルスの相談窓口として、IPA コンピュータウイルス 110 番の電話を設けておりますので、こちらへお問い合わせ下さい。

IPA コンピュータウイルス 110 番

コンピュータウイルスに関連のあることは何でもご相談下さい。

03-5978-7509

受付時間 平日 10:00～12:00、13:30～17:00
また、上記相談は E-mail でも受け付けています。
E-mail : virus@ipa.go.jp

9. 参考情報

対策を含めて、以下の資料を参照下さい。

- 安易なダウンロードがもたらす大きな被害について
<http://www.ipa.go.jp/security/topics/malicious.html>
- ファイル交換ソフト使用上の注意事項
http://www.ipa.go.jp/security/topics/20050623_exchange.html
- ウイルス対策チェックシート
<http://www.ipa.go.jp/security/virus/beginner/check/check.html>
- ワクチンソフトに関する情報
<http://www.ipa.go.jp/security/antivirus/vacc-info.html>
- security at home: コンピュータを守る(マイクロソフト株式会社)
<http://www.microsoft.com/japan/athome/security/update/default.msp>
- 「ブラウジングと電子メールの安全性を強化する」(マイクロソフト株式会社)
<http://www.microsoft.com/japan/security/incident/settings.msp>

10.用語の説明

(*1) スпамメール(spam mail)

迷惑メール(UBE: Unsolicited Bulk Email)とも呼ばれ、商用目的かどうかによらず、個人的、宗教的なものも含めて宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのことです。

(*2) ファイル交換ソフト

インターネットを利用して、不特定多数のユーザ間でファイルを交換できるソフトウェア。

(*3) マクロ感染型ウイルス

MS Word、MS Excelやその文書ファイル、表計算ファイルに感染するウイルスです。感染した文書ファイルや表計算ファイルを開くと、MS WordやMS Excelなどが感染します。E-mailに添付されたこれらのファイルや、フロッピーディスク、MO(光磁気ディスク)などで受け取ったこれらのファイルが、ウイルス感染の媒体となります。

(*4) ぜい弱性 (vulnerability)

情報セキュリティ分野におけるぜい弱性とは、通常、システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことをいいます。オペレーティングシステムのぜい弱性や、アプリケーションシステムのぜい弱性があります。また、ソフトウェアのぜい弱性以外に、セキュリティ上の設定が不備である状態も、ぜい弱性があるといわれます。ぜい弱性は、一般に、セキュリティホール(security hole)と呼ばれることもあります。

(*5) ボット

ボットとは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。

感染すると、外部からの指示を待ち、与えられた指示に従って内蔵された処理を実行します。この動作が、ロボットに似ているところから、ボットと呼ばれています。

11.主なワクチンベンダー (50音順) (IPA 届出に基づき作成)

Ahnlab.Inc(アンラボ)

URL <http://ahnlab.co.jp/>

URL <http://home.ahnlab.com/> (韓国サイト)

主な製品名: ウイルスブロック

株式会社イーフロンティア

URL <http://www.e-frontier.co.jp/>

URL <http://www.rising.com.cn/> (中国サイト)

主な製品名: ウイルスキラー、スパイハンターX

株式会社Kaspersky Labs Japan

URL <http://www.kaspersky.co.jp/>

URL <http://www.kaspersky.ru/> (ロシアサイト)

主な製品名: Kaspersky Internet Security、Kaspersky Anti-Virus

株式会社シマンテック

URL <http://www.symantec.com/ja/jp/>

URL <http://www.symantec.com/> (米国サイト)

主な製品名: Norton Internet Security、NortonAntiVirus、NortonAntiVirus for Mac

ソフォス株式会社

URL <http://www.sophos.co.jp/>

URL <http://www.sophos.com/> (英国サイト)

主な製品名: Sophos Anti-Virus

ソースネクスト株式会社

URL <http://www.sourcenext.com/>

主な製品名: ウイルスセキュリティZERO

トレンドマイクロ株式会社

URL <http://jp.trendmicro.com/>

URL <http://us.trendmicro.com/us/home/> (米国サイト)

主な製品名: ウイルスバスター、Inter Scan

日本エフ・セキュア株式会社

URL <http://www.f-secure.co.jp/>

URL <http://www.f-secure.com/> (フィンランドサイト)

主な製品: F-Secure アンチウイルス

マカフィー株式会社

URL <http://www.mcafee.com/japan/>

URL <http://www.mcafee.com/us/> (米国サイト)

主な製品名: VirusScan、GroupShield



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

〒113-6591 東京都文京区本駒込2丁目28番8号
(文京グリーンコートセンターオフィス16階)

TEL 03 (5978) 7527

TEL 03 (5978) 7509 (コンピュータウイルス110番および不正アクセス相談窓口)

FAX 03 (5978) 7518

E-mail virus@ipa.go.jp (ウイルス) crack@ipa.go.jp (不正アクセス)

URL <http://www.ipa.go.jp/security/>