情報教育コーディネーター通信

柏崎市教育情報支援システム http://kedu.netone.ne.jp/kenet/

第2号 2003/06/20 発行
情報教育コーディネーター 田村 実
柏崎市立教育センター
TEL 23-4591 FAX 23-4610
tamura@city.kashiwazaki.niigata.jp

今号のコンテンツ	
特集	セキュリティ対策をもう一度最初から
セキュリティ通信	Bugbear.B ウィルスに注意を！
教育情報支援システム通信	新規教材等の紹介

今号から各学校への回覧配布とさせていただきます。じっくりご覧になりたい方は、支援システムからアクセスしてご覧になるか、プリントして保存してください。

http://kedu.netone.ne.jp/kenet/hp/tips/index.htm

特集＜セキュリティ対策をもう一度最初から＞

1．セキュリティ対策を実施しないとどうなるの？

(1) 自分のパソコンが使えなくなる

ウィルスと一口に言っても様々な種類がありますが、多くのウィルスがもたらすものがパソコンを使えなくするという被害です。パソコンには Windows2000 や WindowsXP などの OS と呼ばれる基本ソフトや Word や Excel といったアプリケーションソフトがインストールされていますが、ウィルスはそれらのソフトが使用するデータを書き換え、正常に起動することができないようにします。また、起動はできても Word や Excel で作った文書やワークシートが意味の無いものに書き換えられている場合もあります。何年にも渡って作ってきたデータが一瞬で消えてしまったという例が多く見受けられます。

(2) 他人のパソコンに被害を与える

正しいウィルス対策を行わず、自分が被害に遭ってしまうケースはまだ序の口です。今時のコンピュータは LAN やインターネットで物理的に結ばれてネットワークを形成しているため、その内の一台でもウィルスに感染するとあっという間に被害が拡がります。ここ数年の例でも、ウィルスが活動を開始して数時間の内に世界中のネットワークが麻痺するような事態が実際に何度か起こっています。

一般的にウィルス対策を取っていない利用者は自分のパソコンがウィルスに感染していることに気づかないことがほとんどです。そのため、何日いや何ヶ月も他の人にウィルス付のメールを送り続けていたり、(知らないうちに)国際電話をかけ続け、突然数十万円の請求が届くなどのケースもあります。

(3) 機密情報が漏れる

学校現場は非常にナーバスな情報を扱う組織です。住所や電話番号といった基本的な情報でも外部に漏れると大変な問題となりますので、成績や指導記録などは細心の注意を払って機密性の確保に努めなければなりません。

昨年から猛威を振るっているウィルス Klez のように、感染するとそのパソコンに保存されているファイルを手当たり次第にばら撒くような活動をするものがあります。この場合でもやはり多くの被害者が感染に気づかずに使い続け、事態をより深刻なものにするケースが多いようです。

2．ウィルスの進入経路を知る

(1) CD-ROM やフロッピーから

過去には市販ソフトの CD-ROM や雑誌の付録 CD-ROM が感染していたケースもありますし、最近では USB 接続のメモリやハードディスク、デジタルカメラなども進入経路になり得ます。

CD-ROM や FD 内のファイルを開いたり、実行したりすることで感染します。

開く前にウィルスチェックをしましょう。

他人に渡す時にもウィルスチェックをしてから渡しましょう。

(2) メールの添付ファイルや、HTML 形式のメール本文から

以前はメールの添付ファイルを開かなければ安全と言われていましたが、最近では HTML 形式のメール本文に埋め込まれているタイプも多く、添付ファイルを開かなくてもプレビューだけで感染することがあります。

添付ファイルを開いたり、HTML 形式のメールを開いたりプレビューすることで感染します。

仕事では HTML 形式のメールを送るのは避けましょう。

メールを扱うソフトではプレビューを表示しない設定にしましょう。

英語の件名のメールは怪しい！

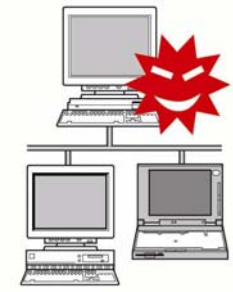
(3) ホームページから

有名メーカーや官公庁などのホームページでも、悪意のある者から攻撃を受けて内容を書き換えられることがあります。このように書き換えられたページを見ることで感染することがあります。面白半分に公序良俗に反するようなサイトにアクセスすると大きな代償を払うことになりかねません。

ウィルスが埋め込まれたホームページを見ただけで感染します。有名メーカーのホームページでも攻撃を受けて感染しているケースもあります。

怪しいサイトへはアクセスしないようにしましょう。

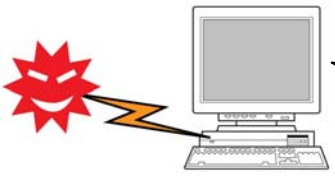
(4) LAN の共有ファイルから



ネットワーク内のパソコンが感染した場合、LAN 経由で攻撃を受けたり、共有フォルダに置かれたファイルに感染が広がります。

一人の不注意がみんなに被害を及ぼすことを忘れずに！

(5) インターネットからの不正アクセス



インターネットに接続しているときに攻撃を受け、そのパソコンを管理する権限を奪われます。

一人の不注意がみんなに被害を及ぼすことを忘れずに！

3．ウィルスなどの攻撃から守る

(1) ウィルス対策ソフトを使う

シマンテックのノートンアンチウィルス 2003 やインターネットセキュリティ 2003、トレンドマイクロのウィルスバスター 2003 などが売れ筋のウィルス対策ソフトです。これらのいずれかを購入し、インストールしてください。日々新たなウィルスが生まれている現状から、ウィルス対策ソフトを使わずにコンピュータを仕事に使うというのは何の保険にも入らずに車を運転するのと同じくらい危険です。

また、ウィルス対策ソフトには必ずウィルス検出エンジン（ウィルスを見つけるためのプログラム）やウィルス定義ファイル（ウィルスを特定するための情報）の更新機能があります。これは、新たなウィルスから守るにはそれに対応した新たな手続きが必要になるからです。いくらウィルス対策ソフトがインストールされていても、更新がタイムリーに行われていなければほとんど役に立たないということです。SARS を防ぐのに過去のワクチンが役に立たないのと同じ事です。

(2) メールソフトを正しく設定する

電子メールを媒介としたウィルスが大変多いのは疑いの無い事実です。そのため、インターネットに接続するサービスを提供するプロバイダの多くは、電子メールを（利用者に届く前に）チェックし、ウィルスが潜んでいればそれを駆除するというサービスを提供しています（有料）。このサービスを利用すれば少なくとも電子メールが感染源になることを防ぐことができます。ただし、言い換えると CD や FD、ネットワークから進入してくるウィルスを防ぐことはできません（これらはウィルス対策ソフトの役割です）。電子メール経由でウィルスが入り込むのをできるだけ防ぐ意味で、メールソフトを正しく設定するポイントを理解しておきましょう。重要なのは以下の2点です。

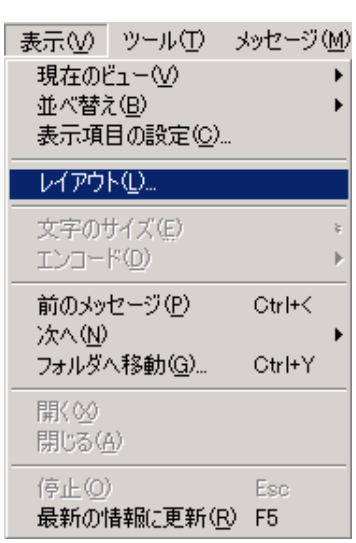
a）**プレビューを表示しないように設定する。**

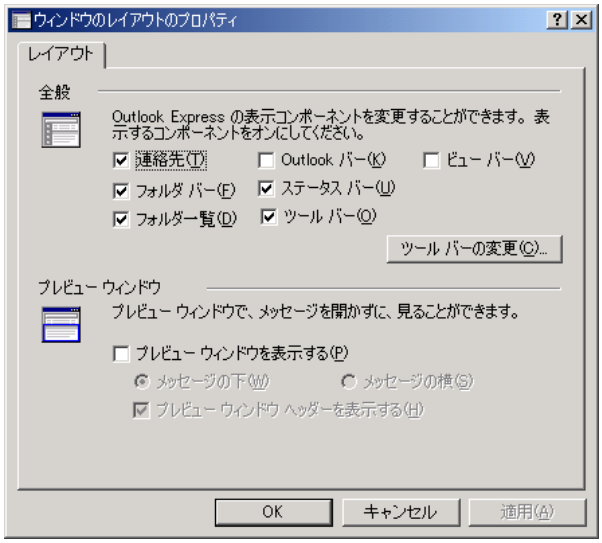
b）**送信メールの形式はテキスト形式にする。**

a）は HTML 形式で送られてくるウィルスメールがプレビューだけで感染する可能性があるからです。プレビューを OFF にしておけば、怪しいメールを開かずに削除することができます。

b）は他の人にメールを送る際に、知らないうちに HTML 形式でメールを送ってしまうことを防ぐためです。HTML 形式のメールはウィルスが潜みやすいため、受け取り手に不安を与えます。困ったことにメールソフトとして多くの人が利用している OutlookExpress は既定値で HTML メールを送るように設定されています。

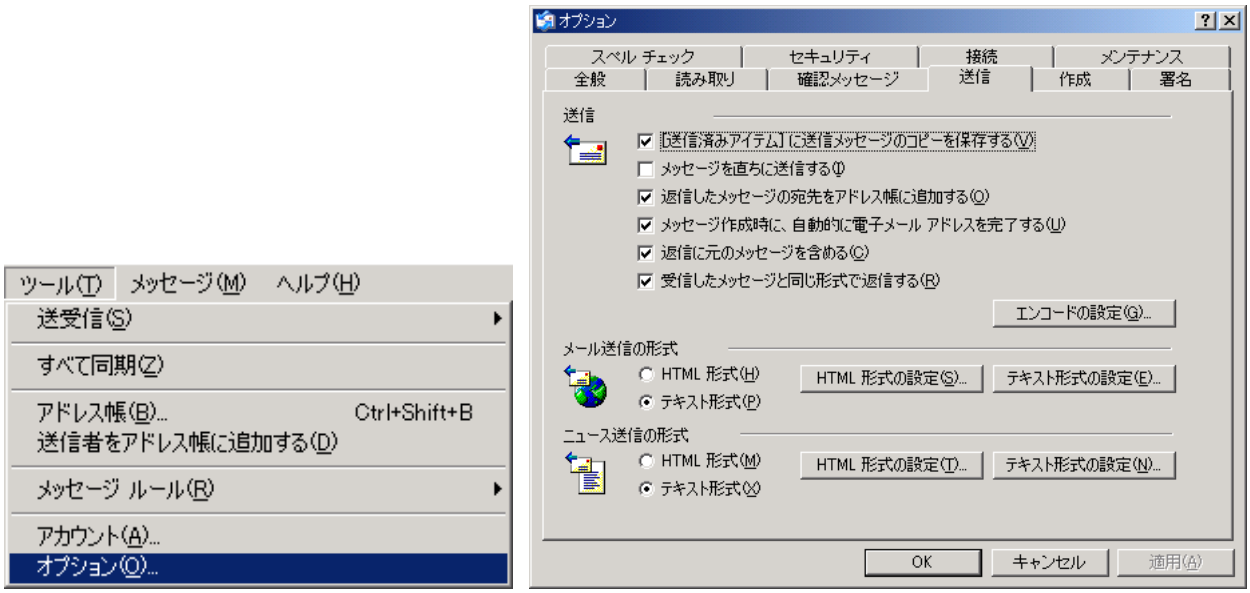
①OutlookExpress を起動して「表示」メニューから「レイアウト」を選択します。「ウィンドウのレイアウトのプロパティ」が表示されたら、「プレビューウィンドウを表示する」の欄のチェックを（マウスでクリックして）はずし、「OK」をクリックします。これでプレビュー欄がなくなりますので、受け取ったメールを選択しても表示されません。





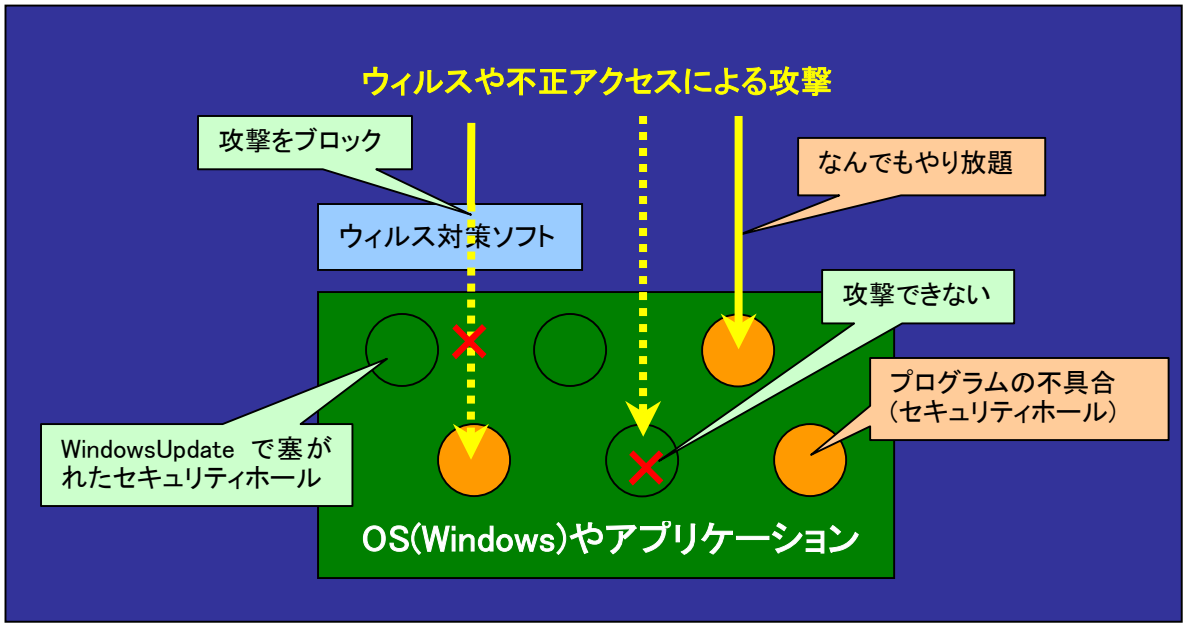
②次に「ツール」メニューから「オプション」を選択します。「オプション」が表示されたら、「送信」タブをクリックし、「メールの送信形式」欄から「テキスト形式」を選択して「OK」をクリックします。これで、他の人にメールを送る際に HTML 形式ではなく、テキスト形式で送られるようになります（送られてきたメールが HTML 形式で、そのメールに返信をす

る場合は、自動的に HTML 形式が選択されますが、送り手が HTML 形式を使っているのですから、そのまま HTML 形式で返信しても迷惑にはならないでしょう)。



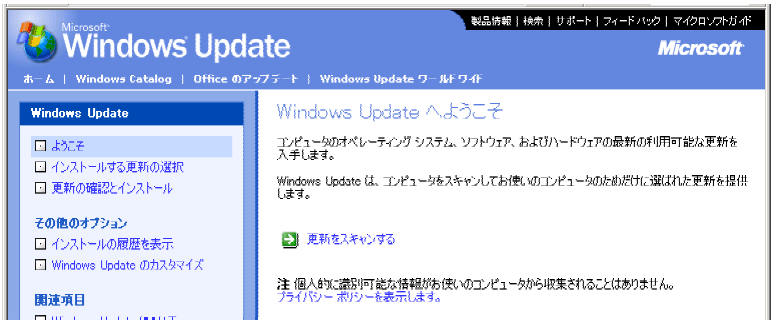
(3) 定期的に WindowsUpdate で「重要な更新と ServicePack」を適用する

WindowsUpdate の機能が利用できるのは Windows98 以降(98,Me,2000,XP)の OS です。残念ながら Windows95や WindowsNT では利用できません。そもそも WindowsUpdate は専門的な知識の無い利用者でも OS を最新の状態に保つことができるように考えられたものであり、OS を発売した後に見つかった不具合を直してくれる役割を持っています。ウィルスや不正アクセスの主な手口は、発見されたセキュリティ上の不具合(=セキュリティホール)を特別な手段で狙ってくるものです。WindowsUpdate の「重要な更新とServicePack」をタイムリーに適用していればこれらの手口による不正操作を未然に防ぐことができるわけです。逆に言えば、WindowsUpdate をしていないパソコンはウィルスや不正アクセスを「Welcome!」と歓迎しているようなものです。また、WindowsUpdate によってセキュリティホールが塞がれていない(直されていない)場合でも、ウィルス対策ソフトが正しく機能していれば、攻撃をブロックして守ってくれる場合があります。ウィルス対策ソフトを正しく利用して、さらに WindowsUpdate でセキュリティホールを塞いでおけばより安全といえるでしょう。

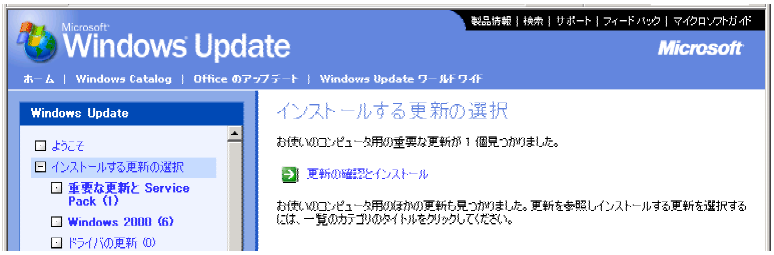


ウィルス対策ソフトや WindowsUpdate の役割

①「スタート」メニューから「Windows Update」を選択します。次の様にマイクロソフトの Web サイトが開かれますので、「更新をスキャンする」をクリックします。



②現在の（自分の）コンピュータ内の情報がチェックされ、どのような更新が必要かを表示してくれます。セキュリティ上重要な更新は自動的に選択されます。次のような画面が表示されたら、「更新の確認とインストール」をクリックします。

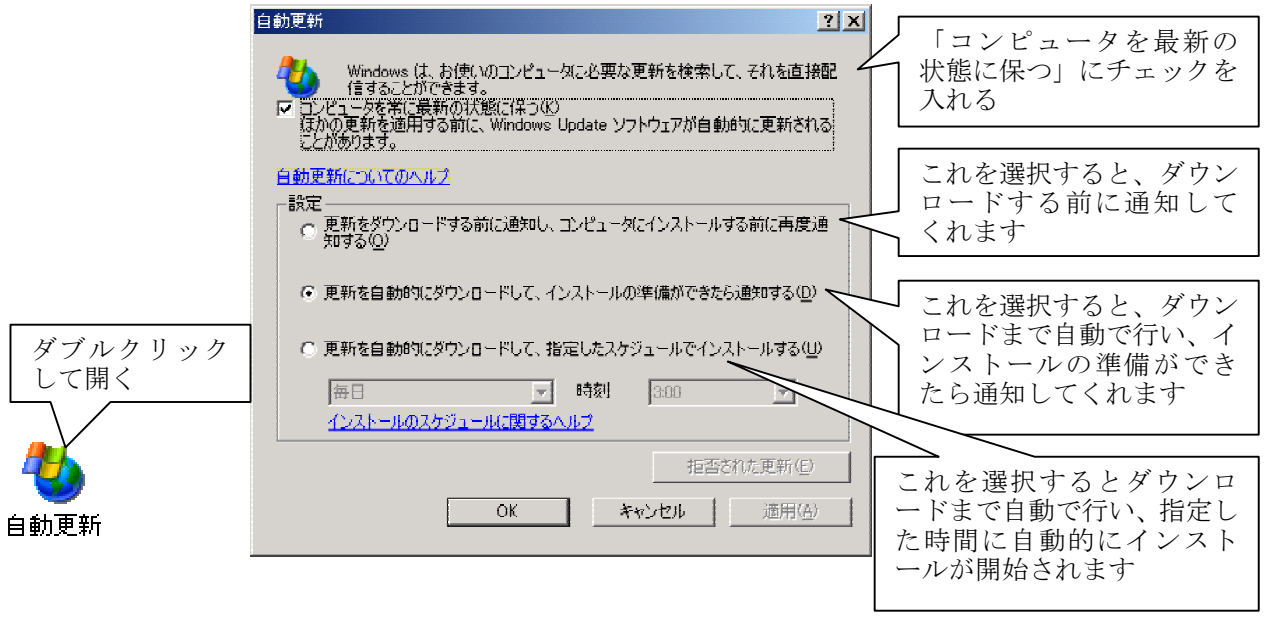


③次のような確認用のページが表示されますので、「今すぐインストールする」ボタンをクリックします。以降の手順は更新内容によって異なる場合がありますので、表示される説明に従ってください。

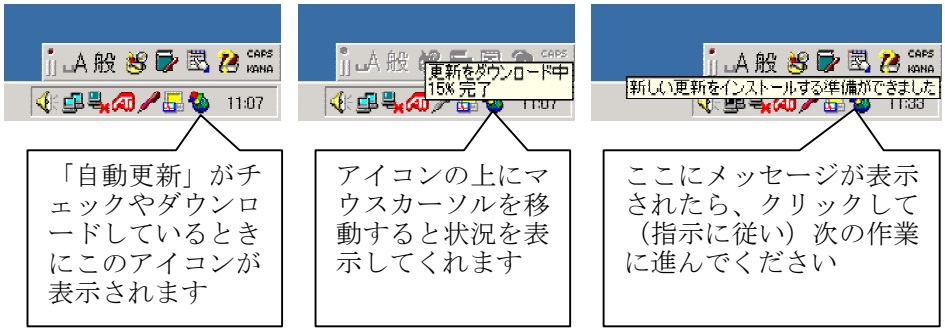
[Windows 自動更新の活用]

自分で頻繁に Windows Update を実行して、製品を常に最新の状態に維持するのは容易ではありません。しかし、「自動更新」機能を活用すれば、セキュリティ上の問題などの重要な更新が発生した場合に自動的に通知してくれるようになります（ただし、インターネットに接続されていなければ通知はされません）。

①自動更新の設定はコントロールパネルの「自動更新」アイコンをダブルクリックして開きます（WindowsXP の場合は「システム」アイコンをダブルクリックして開き、「自動更新」タブから設定します）。もし、コントロールパネルに「自動更新」のアイコンが無ければ、一度 WindowsUpdate を実行して、自動更新の機能をインストールして下さい。



②上記の設定が行われていると、パソコンがインターネットに接続できる環境にあるとき自動的に新しい更新が無いかどうかをチェックしてくれます。もし新しい更新があれば、タスクトレイで通知してくれますので、クリックして、ダウンロードまたはインストールをして下さい。



＜セキュリティ通信＞

■Bugbear ウィルスに注意を！

Bugbear.Bと呼ばれるウィルスは、大量メール送信やネットワーク共有を利用して感染を広げるタイプのウィルスです。InternetExplorer の脆弱性「MS01-020」を利用し、修正パッチをあてていない場合はプレビューしただけで感染する点が特徴です。また、このウィルスには「キーストローク・ロガー」呼ばれる機能を持ち、感染していると、ユーザーがタイピングしたキーの情報を自動的に記録し、ウィルス作成者などの特定のユーザーに送信しようとします。つまり、パスワードや個人情報などが知らないうちに盗まれているという事態を招きます。

このウィルスに関する詳しい情報はシマンテック、トレンドマイクロなどのホームページで確認してください。

シマンテックのホームページ　www.symantec.co.jp

トレンドマイクロのホームページ　www.trendmicro.com

＜教育情報支援システム通信＞

■こんな情報が新規に登録されています

・パソコンワンポイントテキストとして以下の内容を掲載しています。今後も定期的に追加していく予定ですが、「こんな内容を取り上げて欲しい」などのご要望がありましたら、ご連絡ください。

H15.5.26	パソコン操作画面のキャプチャ手順
H15.6.2	Word におけるインデントや図の微調整の仕方
H15.6.9	Word で文書にページ番号、日付、文書名などを入れる手順
H15.6.16	ファイルの拡張子を知ろう

URL はこちら http://kedu.netone.ne.jp/kenet/hp/tips/index.htm

・教材データベース

「小学校向けホームページ作成指導資料（ホームページビルダー編）」 Word 文書B4版4ページ

「算数・数学における評価のあり方」 PowerPointプレゼンテーション

・おすすめホームページ

「IT授業実践ナビ」 文部科学省による「全ての教員が IT を活用した授業を行うことができるよう、各教科におけるITを活用した効果的な指導法と具体的な授業実践例に関する Web サイト」

「教育情報ナショナルセンター」 文部科学省を中心として、経済産業省、総務省とが連携して実施しているプロジェクト。教師と学習者が求める情報を適切な形で提供することと、いろいろな形で支援することが目的のサイト。無料で利用できるソフトウェアや実践事例など豊富なコンテンツが登録されています。