Windows ネットワーク講座Ⅲ

一般ユーザーのためのセキュリティ

2001.12.22

同朋学園本部事務局経理課
河邊憲二

Windows ネットワーク講座Ⅲ 2
1. セキュリティの考え方 2
①. セキュリティポリシー 2
②. 守るべきもの 3
③. 何からどうやって守るか 3
2. 基本のセキュリティ 4
①. BIOS のパスワード設定 5
②. Windows パスワードの設定 5
③. パスワードについて 6
④. ネットワーク接続のパスワード 8
3. ウイルスメール対策 10
①. Outlook Express のセキュリティ設定 11
②. Outlook Express のその他の設定 16
③. Outlook Express のメールのバックアップ 18
④. ウイルス対策ソフト 19
4. Web ブラウザ対策 20
①. Web ブラウザのセキュリティ設定 21
②. Cookie とプライバシー設定 22
③. SSL (Secure Sockets Layer) 対応 23
④. オートコンプリートの設定 25
⑤. ブラウザクラッシャー対策 26
5. Windows のセキュリティパッチと Update 27

Windows ネットワーク講座Ⅲ

同朋学園本部事務局経理課　河邊憲二

2002.02.18　於：名古屋高等学校

このPARTⅢでは、Windows パソコンのネットワーク上での利用に関するセキュリティについて、主に一般ユーザー向けの解説をする。個人情報保護ウイルスメール対策、Web ブラウザ対策、Windows セキュリティ対策アップデートなどを取り上げる。

1. セキュリティの考え方

Windows 環境に限らず、パーソナルコンピュータは基本的に個人ユーザーが単独で利用することを前提として発達してきた。一方 UNIX などのワークステーションは、早くからネットワーク利用を前提とした設計がなされてきた。パソコンが安価で高性能になるにつれて、LAN やインターネットに接続することが求められ、現在ではほとんどすべてのパソコンでインターネット利用ができるようになった。しかし、設計自体は相変わらずパーソナルであり、そのためセキュリティが問題となっている。とくに Windows 9X, Me の系列ではセキュリティに対して、パーソナルユースすなわちユーザーの自己責任ということで、OS 自体には対策が十分にとられていないのが実状である。

①. セキュリティポリシー

セキュリティを考える上でよくセキュリティポリシーという言葉が使われる。簡単に言えば、何を何からどう守るかということで、例えば自分の財産を泥棒から守るために自宅に鍵をかけるというように、パソコンでも同じようにセキュリティを考えていく。ネットワークに接続しないのであれば、ネットワークからパソコンを守る必要がない。また、守るべき情報が何処にあるか判らなければ守りようがない。守るのにどんな方法があるか知らなければ守ることはできない。パソコンを携帯するのか、自宅で使うのか、職場で使うのか、場合によってはインターネットカフェなどでも、セキュリティを考えた使い方が必要である。パソコンの利用形態や利用環境などによっても、セキュリティの考え方は変わってくる。ここでは、教員個人の Windows 9X ノートパソコンを職場と自宅で利用して、学校内LANやプロバイダ経由でインターネットに接続しているような場合を想定してセキュリティを考えることにする。学内 LAN には学内のセキュリティポリシーに基づいて管理者による対策がとられていることが望ましいが、ネットワーク管理者向けのセキュリティに関してはここでは取り上げない。

②. 守るべきもの

パソコンで守らなければならないものは何かを考えると、パソコン本体、システム情報、ソフトの設定情報、一般データ、個人情報などがあげられる。パソコン自体を盗難から守るには、パソコンショップのノートパソコンのようにセキュリティワイヤーでテーブルなどに取り付ける方法が一般的である。(例：ノートパソコン用（株）内田洋行セキュリティワイヤー4,300 円 http://www.uchida.co.jp/osyohin/so16.html　などがある。)またビジネス用のパソコンには、シャーシケースに鍵を取り付けているものもある。リムーバブル HD では、たいてい鍵がスイッチになっている。システム情報は、書き換えられたり削除されたりするとパソコンが正常に利用できなくなる。また、設定情報が失われるとやはり利用できなくなる。これはソフトの設定情報に関しても同じである。一般データの中にも成績データや名簿など業務で使うデータが含まれている場合がある。企業ならば内部情報や顧客情報は社外秘扱いであり、一般データといっても重要なものはやはり管理をし、情報保護を心がけるべきである。最後に個人情報であるが、これには様々なものがあり、一般ユーザーにはその情報がパソコンの何処に保存されているかもわかりにくいものである。しかし、ユーザー名やパスワード情報、メールアドレスやクレジットカード番号、電話番号など重要な情報も場合によっては自分のパソコンに保存していることがある。こうした個人情報は、他人の手に渡れば本人になりすまして利用することも可能になってしまうばかりでなく、そこから例えば学内 LAN のセキュリティを破られることにもつながる場合がある。学内 LAN の場合、最もセキュリティの甘いところが、その学内 LAN のセキュリティレベルになるからである。

他に広い意味でセキュリティに含まれるが、物理的な故障や停電による障害などについても対策を講じておく方がよい。

③. 何からどうやって守るか

一般的にネットワーク接続をするパソコンの場合、ネットワーク経由での侵入者や攻撃者、ウイルス感染からパソコンを守る必要がある。ウイルスの場合は他に FD や CD-ROM などの外部記憶装置経由による侵入や感染もある。さらに①で想定した教員個人のノートパソコンの場合、第三者により直接操作されることのないようにすべきである。Windows 9X 系列のパソコンはマルチユーザー用に設計されていない。したがって、Windows 9X が起動すれば、誰でもパソコン内にあるすべての情報にアクセスができ、ネットワークが利用できる。また Windows 9X に限らず、FD から起動できるパソコンはパスワード情報などを簡単にコピーできてしまうので、情報を抜き取ることができる。したがって第三者には直接操作させないようにすべきである。さらに言うならパスワードを入力するところを見られないことも必要になる。セキュリティを堅固にすればするほど、パソコンは使いにくくなる。外部データのやりとりがまったくできないようにして、自分だけが使うのであれば、セキュリティは守られる。しかし、常時自分のパソコンを監視することはできないし、

FD や CD-ROM も使わないわけにはいかない。インターネットも利用したい。そうすると何を何からどうやって守るのかというセキュリティ対策が必要になってくる。

Windows の場合、Microsoft は常に最新バージョンのソフトで、セキュリティパッチによるアップデートがなされたものを利用するよう推奨している。もちろん他社製のアプリケーションソフトをインストールしている場合も同様である。これは、Windows に限らず、今やすべての OS とアプリケーションソフトに共通したことである。自分のパソコンに入っている OS やすべてのアプリケーションのバージョン情報は、自分で管理しなくてはならない。そのための情報収集も自分でやらなくてはならない。自分のパソコンの管理者は自分しかいないので、職場のパソコンのように管理者がパッチをあててくれたり、委託業者が保守してくれたりするわけではない。管理がきちんとされていないパソコンが学内 LAN に接続されると、学内 LAN のセキュリティレベルが低下する。

2. 基本のセキュリティ

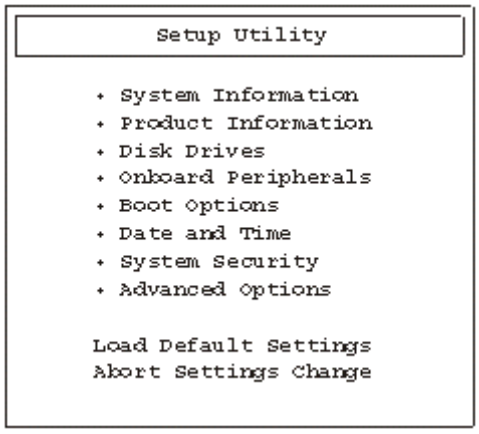
ここでは、第三者にパソコンを操作されないためのセキュリティ対策を解説する。基本的な対策としては、主にパスワードを利用した次のものがあげられる。

i. **BIOS の起動パスワードを設定する**
ii. **Windows パスワードを設定する**
iii. **スクリーンセーバーのパスワードを設定する**
iv. **セキュリティツールを使ってロックする**
v. **認証装置を導入する**

ⅰ～ⅲは通常のパソコンで設定できるものであるが、デフォルトでⅰは設定されていない。しかし、これが設定されていないとⅱやⅲは意味をなさない。Windows 9X では Windows パスワードはキャンセルしても起動するし、スクリーンセーバーは電源を切るか再起動すれば回避できる。たとえ Windows が起動できなくても FD から起動すればファイルにはアクセスができてしまうので、重要なのは起動の時の BIOS でセキュリティをかけることである。その上で初めてⅱやⅲの効果がある。BIOS（basic input/output system）は、メーカーによって設定画面が異なり、中には BIOS の起動画面を表示しないように設定して出荷しているメーカーもある。一般ユーザーの中には BIOS 設定の画面を見たことがない人もいるが、パソコンの電源を投入すると最初に BIOS が ROM から呼び出され、ハードウェアの基本設定をチェックしてから OS が起動するようになっているので、マニュアルの BIOS 設定画面呼び出し方法を確認する。たいていの場合起動時にパスワードを求めてくるように設定ができる。他に起動ドライブの設定もできるようになっているので、例えば FD や CD-ROM から起動できないように設定することもできる。こうすることで、BIOS のパスワードが破られても、FD や CD-ROM から起動することは防ぐことができる。また、FD を日常利用しないのであれば、FD ドライブ自体を無効にすることもできる。最近では、FD ドライブのないパソコンも多く販売されるようになってきた。

①. BIOS のパスワード設定

図 1.BIOS メニュー画面の例

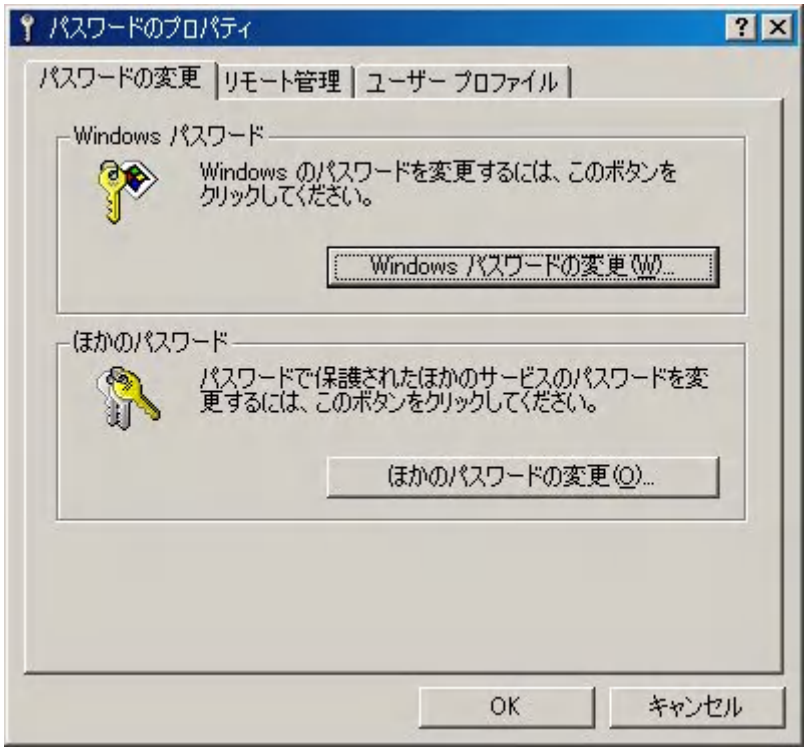


BIOS の設定画面はメーカーにより異なるが、左のようにシステムセキュリティメニューがあるので、これを選択して起動時のパスワード設定をする。設定を変更したら保存をして終了すれば、次回起動時からパスワード入力を求める画面が表示されるようになる。正しいパスワードを入力しない限りパソコンを起動することはできなくなる。たいていの場合、管理者パスワードとユーザーパスワードが設定できる。管理者パスワードを設定すると、BIOS の設定変更をする際に管理者パスワードが必要になる。

②. Windows パスワードの設定

個人が利用するパソコンの場合、Windows パスワードの設定をしていない場合が多い。起動時にパスワード入力が面倒だからというのがたいていの理由である。Windows パスワードを設定するには、コントロールパネルにあるパスワードアイコンを選択実行し、パスワードのプロパティを開く。Windows パスワードの変更をクリックする。

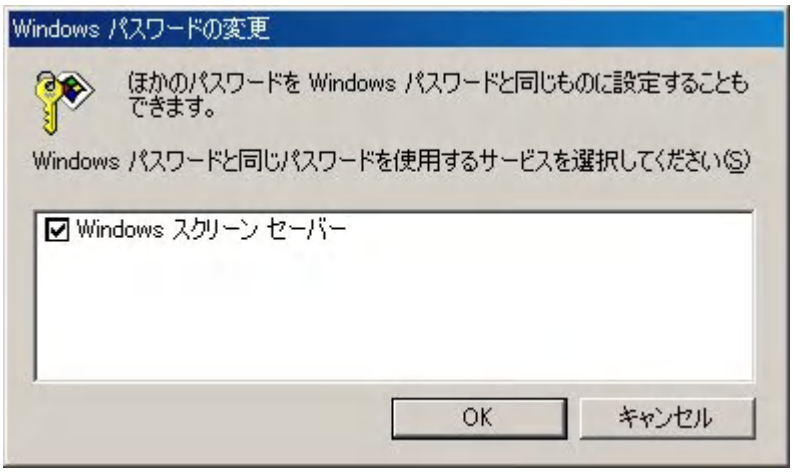
画面 1.Windows パスワードのプロパティ



他のパスワードの変更とは、スクリーンセーバーのパスワードなどの設定変更である。Windows パスワードで、同じパスワードを使用するサービスに、スクリーンセーバーがチェックされていれば、自動的に Windows パスワードがスクリーンセーバーにも適用される。

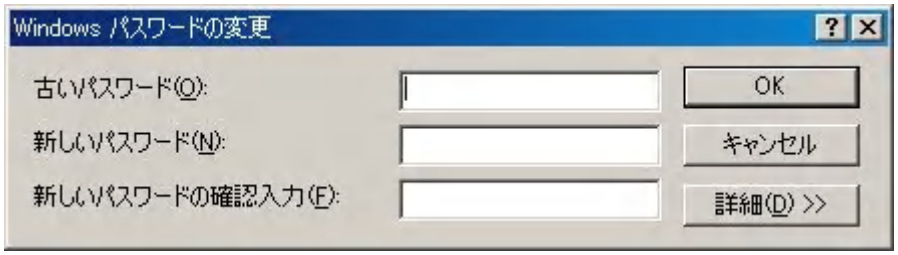
Windows パスワードの変更をクリックすると次の画面になる。

画面 2.Windows パスワードの変更



ここでOKをクリックしてパスワードを入力する。画面 3.でパスワードを入力せずに OK をすると、Windows パスワードは設定されないので、起動時にパスワード入力を求められない。

画面 3.Windows パスワードの変更入力画面



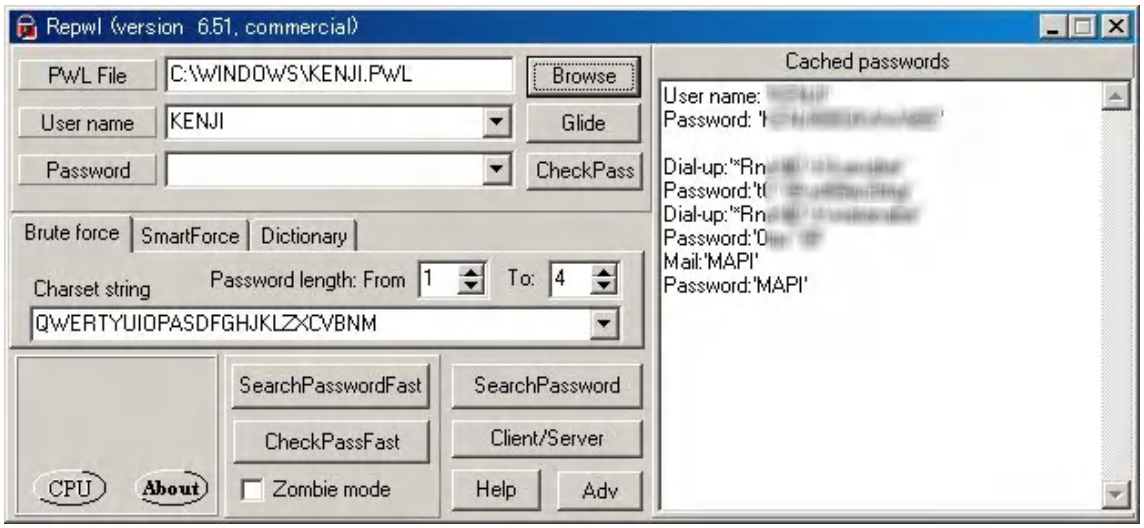
Windows パスワードは複数ユーザー登録をした場合に、ユーザーを識別するのに用いられるが、それ以上のセキュリティ上の効果はない。いったんログオンすれば基本的にはシステムも含めすべてのファイルにアクセスが可能になる。したがってセキュリティ上の効果を期待するなら、ivのセキュリティツールをインストールしてロックするか、暗号化処理などの対策をとる必要がある。あるいはvの認証装置を取り付けて、鍵や指紋などで認証しないと利用できないようにする。フリーウェアやシェアウェアなどでも役立つセキュリティツールがあるので、必要に応じてセキュリティ対策を講じておけば、パソコン内のデータを第三者に操作されないようにすることは可能である。ただし、席を離れるときにロックするなどセキュリティツールを正しく設定して利用しなければ、効果は期待できないので注意すること。Vector のダウンロードページなどでセキュリティツールを検索して（http://www.vector.co.jp/vpack/filearea/win/util/security/index.html）利用状況に応じた対策ツールを導入する。

③. パスワードについて

守るべきデータとして第一にあげられるのがパスワードファイルである。きちんとセキュリティのあるワークステーションでは、管理者以外はパスワードファイルにアクセスができないようになっている。Windows 9X の場合、すでに述べたようにこのようなアクセス権の設定などはできないので、簡単にコピーして持ち出したりすることができる。ところがほとんどのユーザーは、②で設定したパスワードが、何処に保存されているか知らない場合が多い。第一に守るべきものが何処にあるか知らなくては、セキュリティ対策のしよ

うがない。もちろんパスワードファイルは開いても内容が読みとれないようになっているが、パスワード解析ツールを使えば簡単にパスワードを知ることができる。Windows のパスワードファイルは C:¥Windows¥xxxxx.pwl にある。xxxxx はユーザー名で拡張子が.pwl となっている。ユーザー名を設定していない場合は既定.pwl となっている。このファイルを解析するには、例えば PwlTool を利用する。

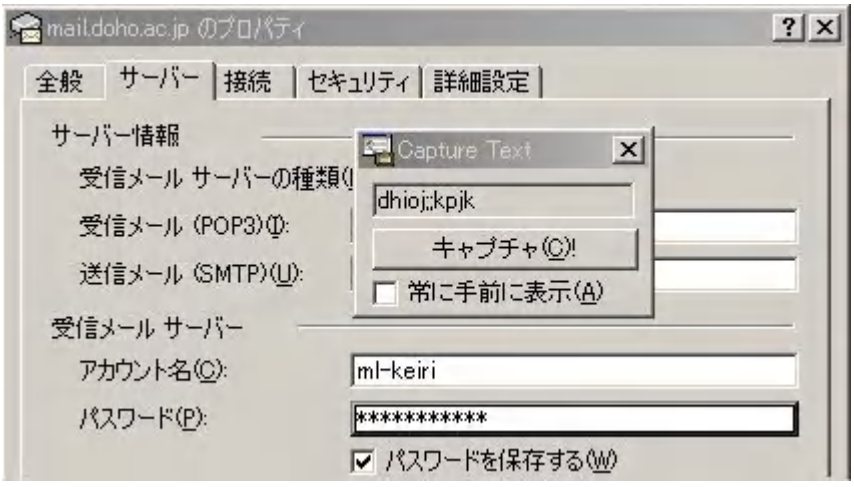
画面 4.パスワード解析ツール



最近はパソコンが高性能になり、総当たりでの解析も現実に可能である。したがって、パスワードはできるだけこうしたツールでの解析が難しくなるよう決めるのがよい。

- 英大文字と小文字、数字と記号が混在すること
- 設定できる範囲のできるだけ長い文字列
- ランダムで、推測可能な文字列などを含まない
- 定期的に変更し同じものは利用しない

パスワードファイルを守っても、パスワードを記憶させていれば表示できる場合がある。次の画面 5.は Capture Text というフリーウェアで、メールアカウントのパスワードを表示させたものである。



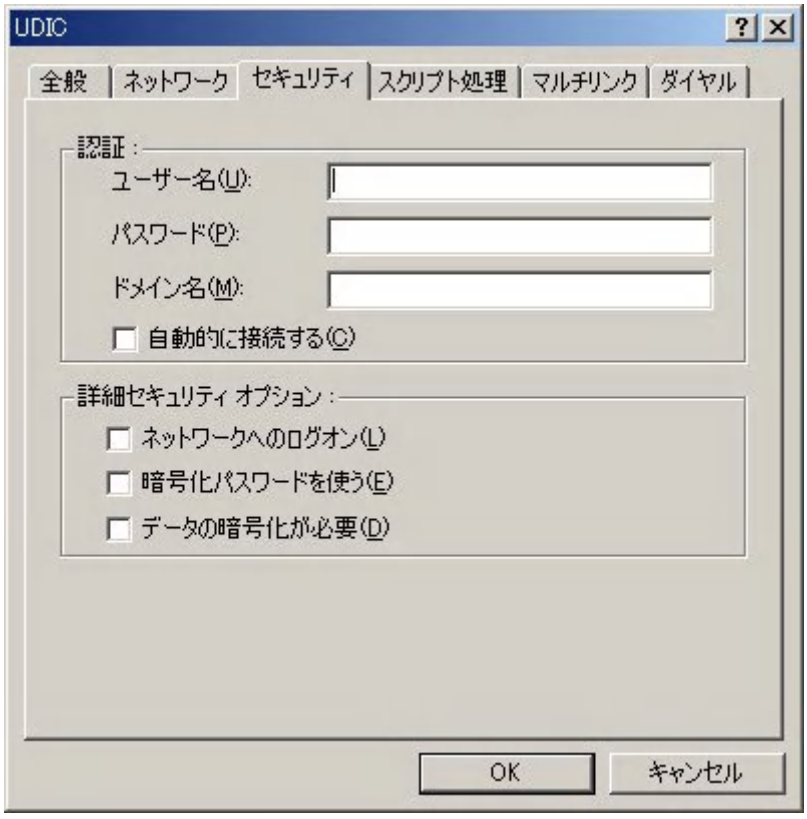
画面 5.Capture Text によるパスワード表示

このツールなら FD から起動してパスワードのある設定画面を表示すれば、パスワードを入手することができる。このようなプログラムを自分のパソコンで使われないように、自分のパソコンは、不用意に他人に貸したり使わせたりしないことである。

④. ネットワーク接続のパスワード

パソコンを TCP/IP によりダイヤルアップ接続する場合、プロバイダが指定したログイン名とパスワードを使う。この設定はコントロールパネルにあるダイヤルアップネットワークを開き、プロパティで設定する。

画面 6.ダイヤルアップネットワークの接続プロパティ



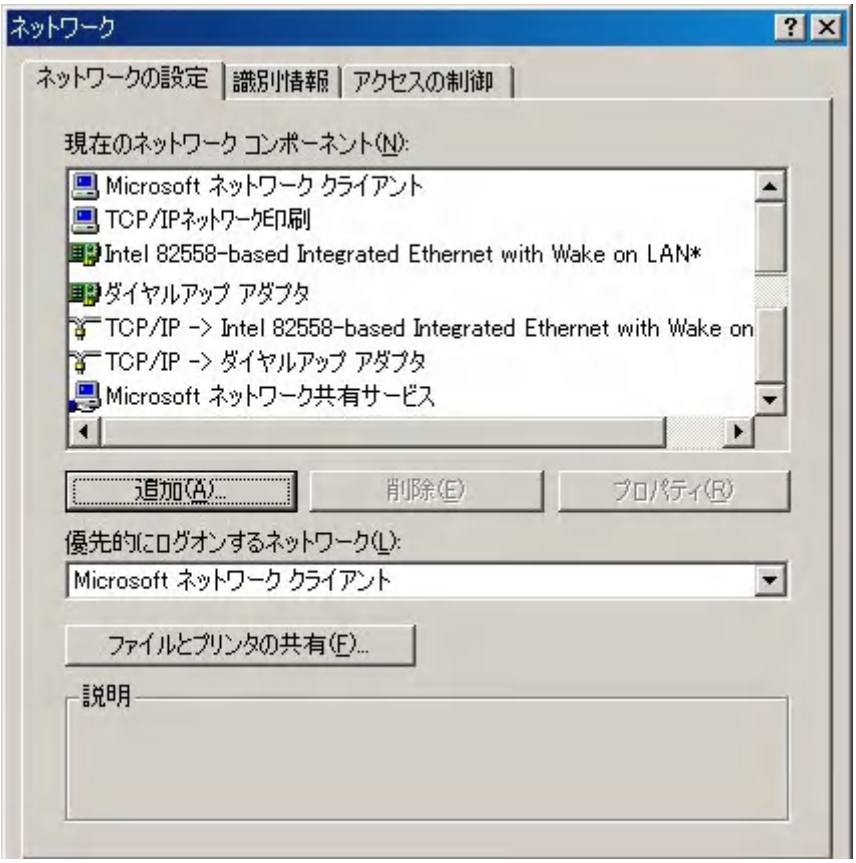
左の画面で、ログイン名とパスワードを設定するが、これもパスワードファイルである xxxxx.pwl に保存される。したがって、パスワードファイルが他人の手に渡った場合、本人に成りすましてプロバイダへダイヤルアップ接続ができるようになってしまう。こうしたケースでは、本人が気づかない限り使われていることが判明しにくいので、接続料金を定額にしている場合などは特に注意が必要である。

学内 LAN などに接続している場合に、ファイルやプリンタの共有を利用していることがある。学内 LAN の場合にはマイネットワークアイコンを右クリックしてプロパティを開くと、コンポーネントに Microsoft ネットワーククライアントがある。また、ファイルとプリンタの共有が設定されていると、Microsoft ネットワーク共有サービスがある。

Microsoft ネットワーククライアントが設定されている場合、優先的にログオンするネットワークに Microsoft ネットワークが設定されていると起動時にログオンユーザー名とパスワードを聞いてくる。さらに別に Windows ログオンのパスワードが設定されていれば、そのユーザー名とパスワードを聞いてくる。Microsoft ネットワークのログオンパスワードが間違っていると、Windows へはログオンできるがネットワーク関係のサービスは利用することができなくなる。さらに Windows 側の設定により、Microsoft ネットワークへログオ

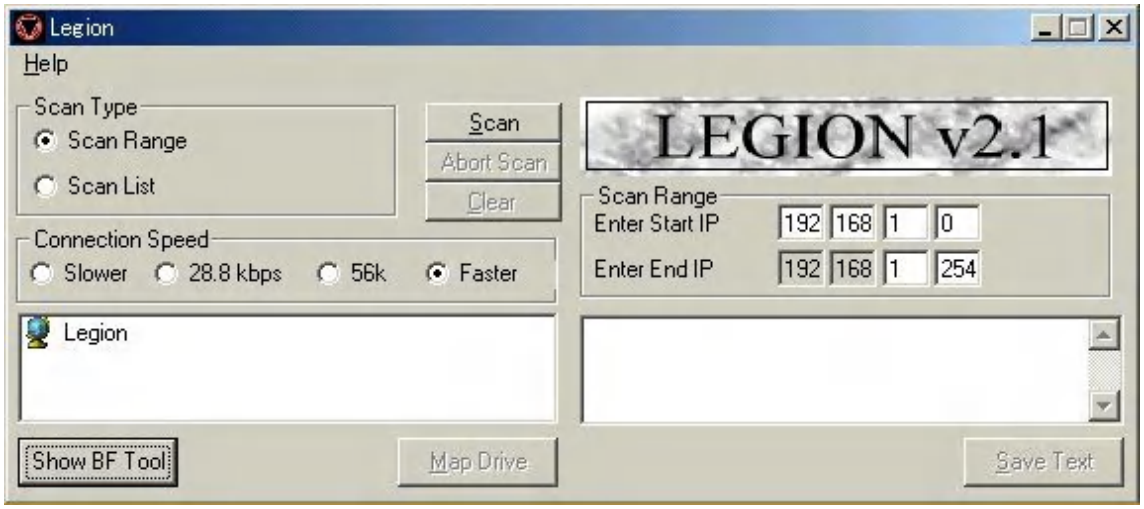
ンしないと Windows が利用できないように設定することもできる。

画面 7.ネットワークのプロパティ



ネットワークの設定に関しては、サーバー側の設定やセキュリティポリシーに依存するので管理者に確認する必要がある。また、共有サービスに関しては、共有フォルダにパスワード設定がされていたり、ファイルサーバ側でアクセス権の設定がされていたりする場合もある。Windows 9X のようにアクセス権の設定できない OS を使って共有サービスを提供するのは、セキュリティ上好ましくない。例えばネットワーク上の共有フォルダを検索してマッピングしパスワードクラックを試みるソフトがある。

画面 8.LEGION



画面 8.のソフトは指定された IP の範囲について、共有設定をしているパソコンを検索し、共有フォルダをネットワークドライブにマップして、辞書と総当たりによるパスワード解析が可能である。したがって、パスワードを設定する場合にはよいパスワードを選ぶ。

3. ウイルスメール対策

2001 年はウイルス被害が特に多かった年である。理由は Outlook Express で受信メールをプレビューしただけで感染するウイルスや、IIS などの多様な感染ルートを持つウイルスが蔓延したためである。IPA セキュリティセンターの緊急対策情報に掲載された 2001.8 月～12 月のウイルス情報をあげると次のようである。

- 「W32/Badtrans」ウイルスの亜種に関する情報（2001.12. 1 更新）
- 「W32/Aliz」ウイルスに関する情報（2001. 11. 30 更新）
- 「W32/Klez」に関する情報(2001.11. 9 掲載)
- 「W32/Nimda」ウイルスの亜種に関する情報(2001.11.26 更新)
- 「Code Red ワームに関する情報」Code Red II に注意を（2001. 8.16 更新）

また、主に Microsoft の Outlook や Outlook Express をターゲットとした、ウイルスジェネレータのようなウイルス作成ツールの登場などによって、容易にウイルスを作成できる環境になってきたことも背景となっている。さらにパソコンが情報家電化し、一般の初心者ユーザーが急激に増加したことも遠因となっている。実際、上記のウイルスは Microsoft が提供している最新のセキュリティパッチをあてて設定していれば、少なくともウイルスが実行される前に警告がされるなどで防ぐことができるものである。しかし、一般の初心者ユーザーはたいてい購入時のままで利用しているケースが多い。ユーザー登録をしてセキュリティ情報を自ら収集しているユーザーはまだ少数である。IT 講習会の講師ですらウイルスに関して全く無知な講師もいるようである。パソコンにはウイルス対策ソフトがプレインストールされていることもあるが、ウイルスデータが全く更新されていないため用をなさなかったり、せっかく警告が表示されても正しい対処の仕方を知らなかったりというケースもある。最近のウイルスは他人よりもむしろ知人からのメールで届くようになったので、この点にも注意を要するようになった。メールマガジンやメーリングリストの普及で、一通のメールが大量の感染を引き起こすことも被害が拡大した一因である。

ここで IPA がまとめたウイルス対策とメール添付ファイルの扱い心得を引用しておく。詳しくは IPA のホームページで確認のこと。(http://www.ipa.go.jp/security/isg/virus.html)

パソコンユーザのためのウイルス対策 7 箇条

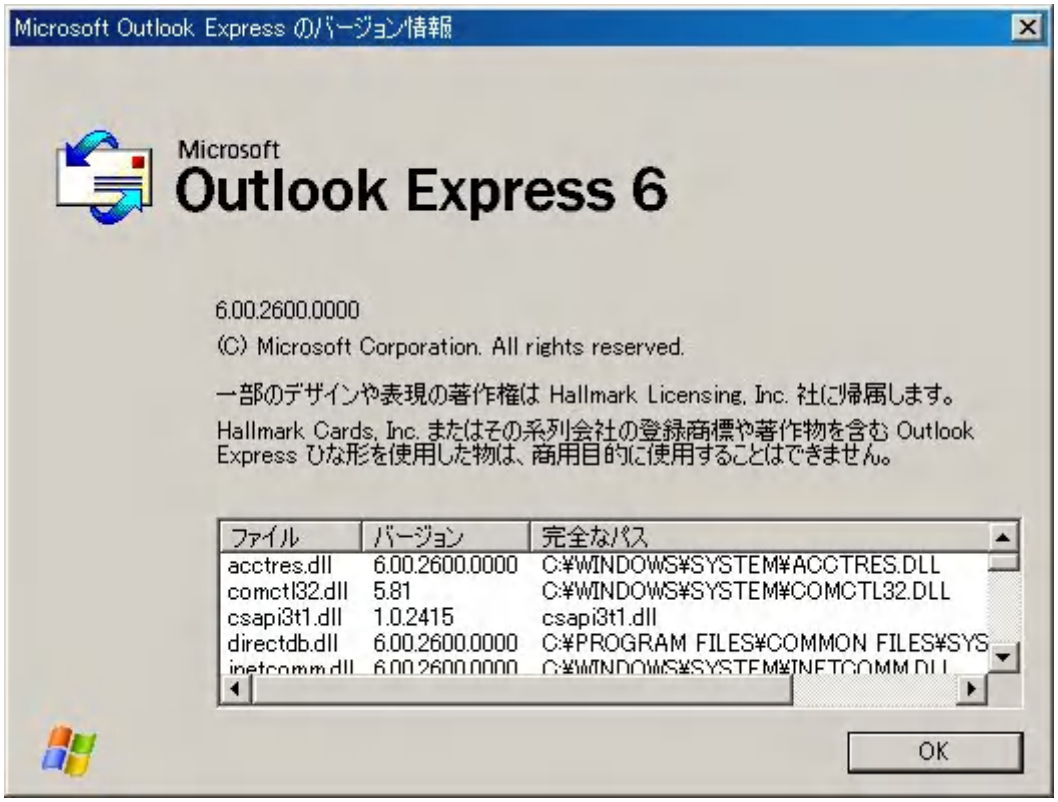
- 最新のウイルス定義ファイルに更新しワクチンソフトを活用すること
- メールの添付ファイルは、開く前にウイルス検査を行うこと
- ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
- アプリケーションのセキュリティ機能を活用すること
- セキュリティパッチをあてること
- ウイルス感染の兆候を見逃さないこと
- ウイルス感染被害からの復旧のためデータのバックアップを行うこと

メールの添付ファイルの取り扱い 5 つの心得

- 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
- 添付ファイルの見た目に惑わされない
- 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
- 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
- 各メーラー特有の添付ファイルの取り扱いに注意する

①. Outlook Express のセキュリティ設定

まずは Outlook Express のバージョンを確認し、最新のものを利用するべきである。その上で、セキュリティパッチをあて、正しいセキュリティ設定で使うことが必要である。ここで想定している Windows 9X 上で利用できる最新の Outlook Express は、12 月現在で 6.00.2600.0000 である。Outlook Express は通常 Internet Explorer の標準インストールを実行すると、自動的にインストールされる。これは、一部の機能が Internet Explorer に依存しているためである。したがって、最新の Internet Explorer のバージョンも 12 月現在で 6.00.2600.0000 ということになる。なお、すでに Service Pack 1 がリリース予定である。バージョン情報はヘルプのバージョン情報で確認できる。



画面 9.Outlook Express のバージョン情報

この最新版にあてるべきセキュリティパッチは、Internet Explorer 6.0 用のセキュリティパッチに含まれるので、実際には Internet Explorer 6.0 用のセキュリティパッチをあてることになる。12 月 14 日に「2001 年 12 月 13 日 Internet Explorer 用の累積的な修正プログラム (MS01-058)」として公開されたもの q313675.exe である。これをインストールすると、Internet Explorer のバージョン情報は次のように更新バージョンが追加される。

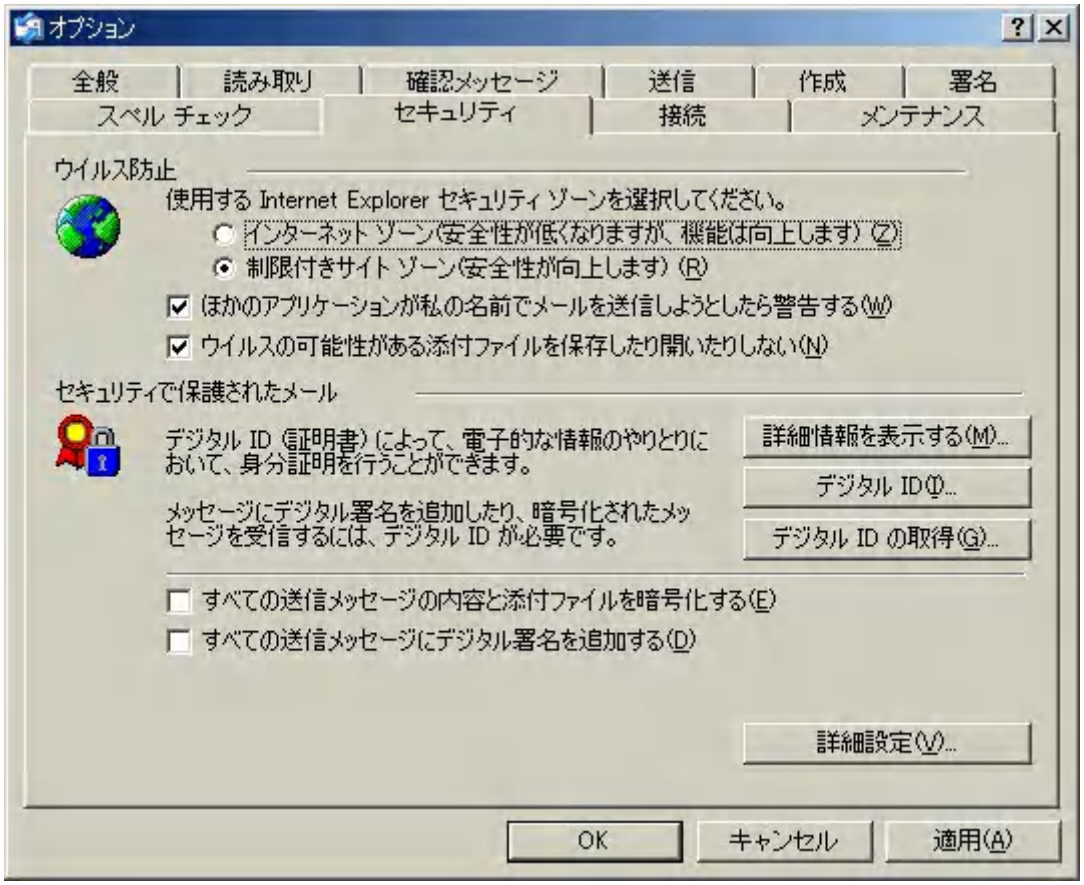
画面 10.Internet Explorer のバージョン情報

実際には、メールに対するセキュリティパッチだけあてればよいのだが、依存関係があるため、基本的には必要なすべてのセキュリティパッチをできるだけ速やかにあてた方がよい。このセキュリティ情報は Microsoft のプロダクトセキュリティ警告サービス日本語版のニュースメールを購読すれば入手できるので、購読をすすめる。この情報は、Windows Update のページには載らないものが含まれる。つまり Windows Update だけでは、セキュリティ対策にはならないということである。なお、メールソフトやブラウザを他社製に変えれば、多少はウイルスに対する耐性が向上するが、Eudora、Becky、Datula、Netscape、EdMax といったメールソフトにもセキュリティパッチは公開されており、最新のバージョンにセキュリティパッチをあてる必要があるのは同様である。

セキュリティパッチの最新版がインストールできたら、Outlook Express の設定をする。デフォルトで利用している場合がほとんどだが、よりウイルスの影響を受けにくくし、セキュリティを確保するためには設定を変更した方がよい。Outlook Express 6.0 にはウイルス対策用の設定が二つ追加されている。ひとつは「ほかのアプリケーションが私の名前でメールを送信しようとしたら警告する」、もうひとつは「ウイルスの可能性がある添付ファイルを保存したり開いたりしない」という項目で、いずれもツールオプションのセキュリティで設定できる。前者は、ウイルスが Outlook Express からメールを送信しようとすると警告がでるもので、二次感染を防ぐものである。後者は特定の拡張子を持つメール添付ファイルを開かないようにするもので、「次の添付ファイルは安全でないため、メールからのアクセスが削除されました」の警告メッセージが表示される。ただし、添付ファイルそ

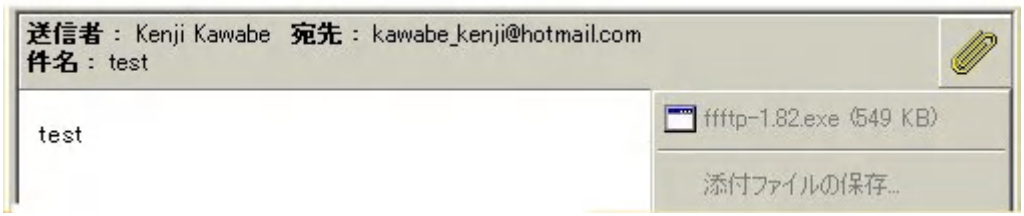
のものが削除されるわけではない。

画面 11.Outlook Express 6.0 に追加されたウイルス防止機能



ここで、まず制限付きサイトゾーンにチェックが入っていることを確認する。セキュリティゾーンの設定は、Internet Explorer で設定されているものである。画面 11 の設定で実際に添付ファイルのあるメールをプレビューすると次のように表示される。

画面 12.ウイルスの可能性がある添付ファイルの場合



添付ファイルを示すクリップマークをクリックしても画面 12 のように開けないようになっている。ここでは、実行ファイル形式 .exe の拡張子が付いたファイルを添付したものを開いている。これは、メール作成のときにも有効なので、特定の拡張子のファイルを添付したメールを作成した場合にもプレビューなどでは開けなくなる。受信トレイでこのメールを選択してクリックして開くと、新しいメッセージの画面で本文は表示されるが、添付ファイルについては次の画面 12 のように警告が表示され、添付ファイルを開くことはできな

い。ただし、ウイルス防止のセキュリティ設定を解除すれば、普通に開くことができるようになる。

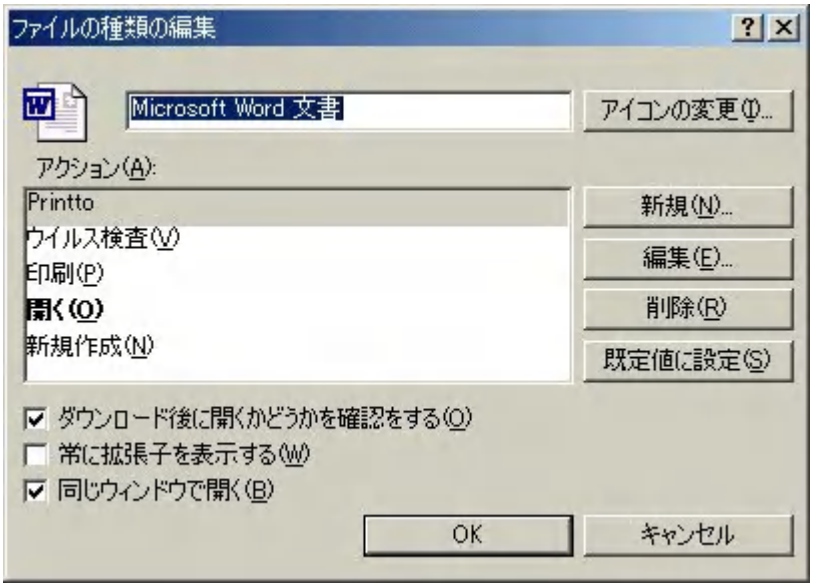
画面 13.ウイルスの可能性があるメールを開いた場合

注意が必要なのは、ウイルスの可能性のある添付ファイルを拡張子で判断しているということである。デフォルトではテキストや画像ファイルの拡張子であれば開くことができるようになっている。この設定は、コントロールパネルのフォルダオプションにあるファイルの種類で詳細設定を開いて確認変更ができるようになっている。

画面 14.登録されているファイルの種類

画面 14 のファイルの種類には、アプリケーションがインストールされたときに、自動的に登録された拡張子が登録されている。これにより、ファイルをクリックすると自動的にアプリケーションが起動するようになっている。この画面にある詳細設定をクリックすると次のような画面になる。

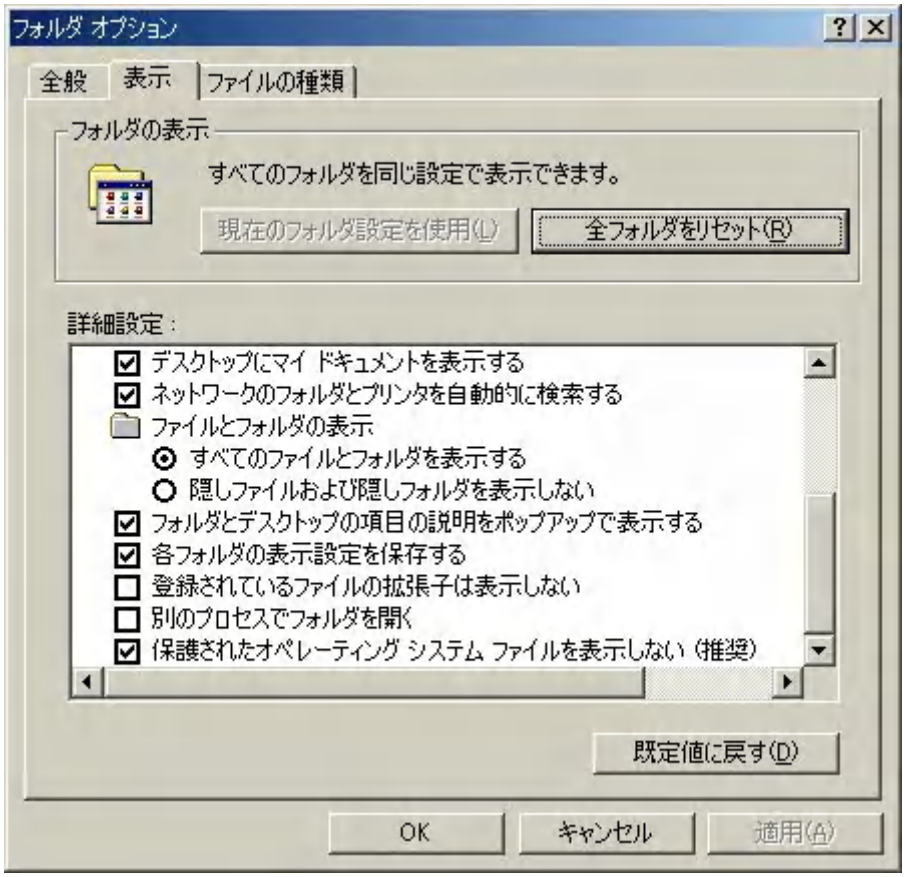
画面 15.ファイルの種類の編集



ここにアクションが登録されており、太字になっているアクションが既定値に設定されている。その下の「ダウンロード後に開くかどうかを確認する」のチェックを解除すると確認なしで開くことが可能になる。これは必要なら拡張子ごとに設定する。通常この設定を直接編集する必要はない。

フォルダオプションの全般のところでは、「登録されているファイルの拡張子は表示しない」の項目を解除しておく。これは、拡張子を TXT に見せかけた添付ファイルにだまされないためである。(例えば test.txt.doc のようなファイル名があると拡張子.doc が表示されなければ、test.txt に見える)。

画面 16.フォルダオプションの全般のファイルとフォルダの表示

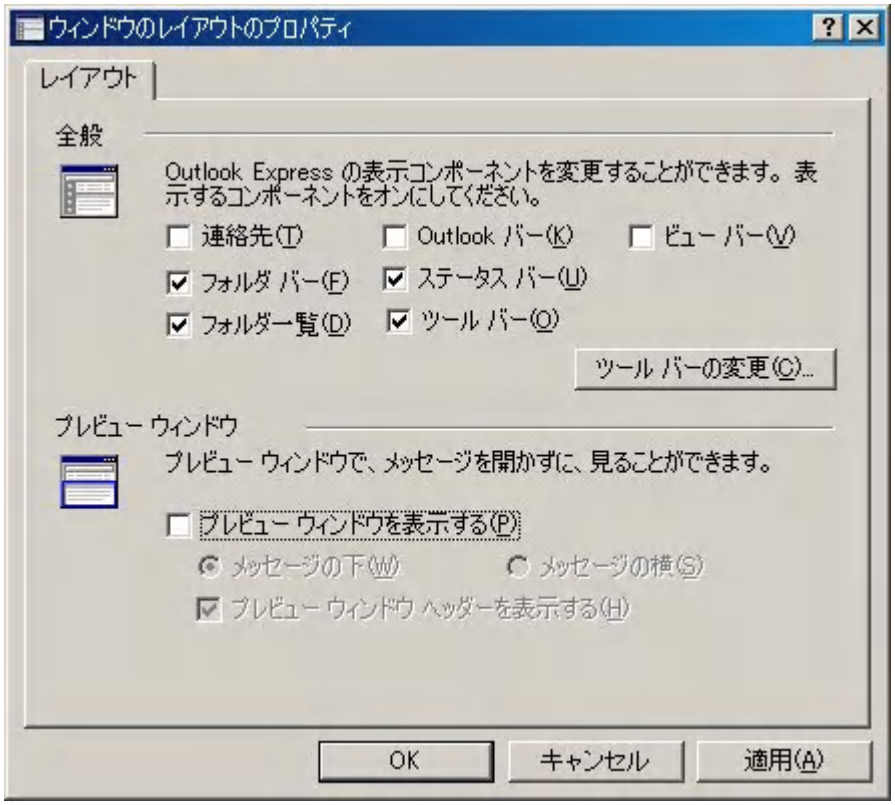


個人的には、ファイルとフォルダの表示では、その他に「すべてのファイルとフォルダを表示する」を選択しておくことを勧める。通常は、ユーザーが不用意に操作しないために、システムが利用する「隠しファイルおよび隠しフォルダを表示しない」になっている。

②. Outlook Express のその他の設定

ウイルス防止の設定以外にも、ウイルス対策に有効な設定がある。ただし、ある程度利便性を犠牲にしなければならない。まず、プレビューによるウイルス感染を防ぐためにプレビュー表示をオフにする。これは表示のレイアウトでプレビューを解除する。

画面 17.ウィンドウのレイアウトのプロパティ

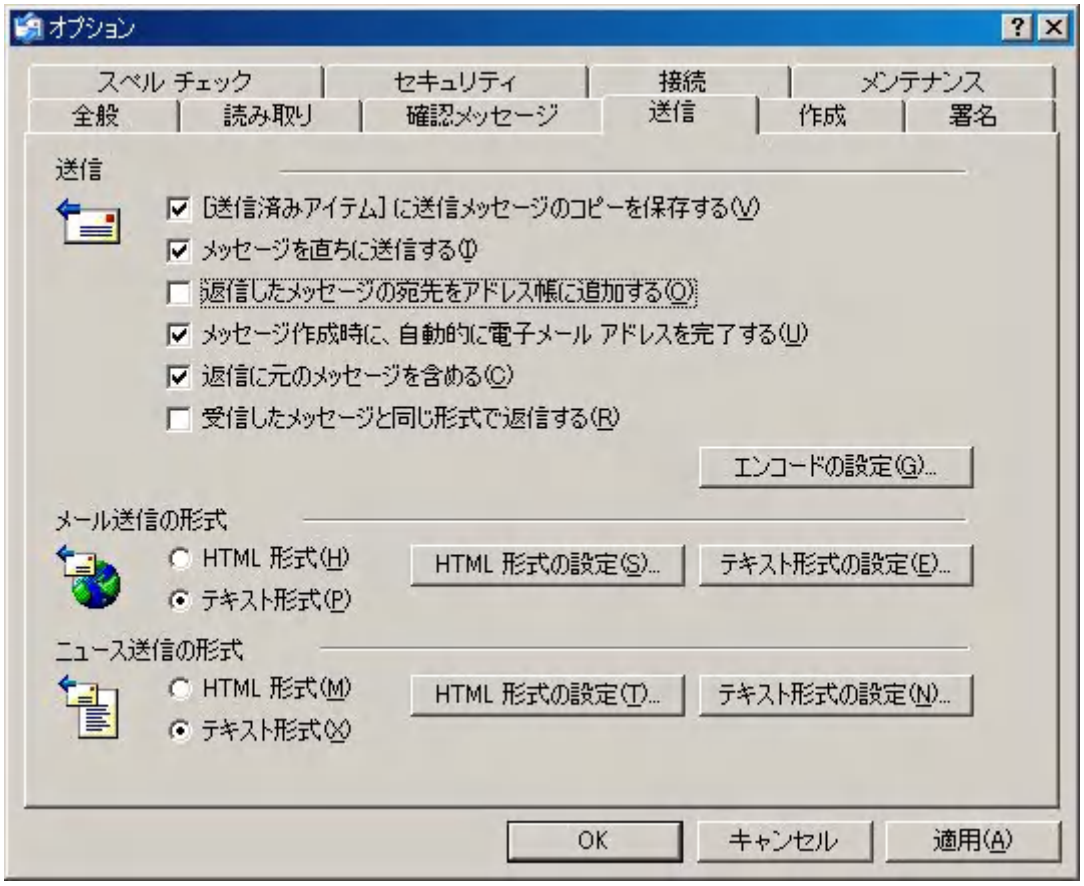


画面 17 で「プレビューウィンドウを表示する」のチェックを取る。こうすると、受信メールは一覧のみが表示されるようになる。また、ツールのオプションで送信を選択して、画面 18 のように常にテキスト形式のメールを使うように設定をする。これは、メールを出す相手に対して普段からテキストでしかメールをしないようにすることで、もしウイルスメールを送ってしまったときに、相手が気づきやすくなるよう配慮することになる。普段から添付ファイルや HTML 形式のメールをやりとりしていると、習慣で疑いなくウイルスメールを開いてしまうことにもなりかねないので、できるだけテキスト形式のメールを利用するのがよい。

「受信したメッセージと同じ形式で返信する」も解除した方がよい。また、アドレス帳を不用意に登録しないように「返信したメッセージの宛先をアドレス帳に追加する」も解除する。アドレス帳にメーリングリストの宛先が登録されていると、ウイルスに感染したときの被害が個人のミスではすまされない事件になることもある。アドレス帳はよく利用する個人アドレスだけを、登録するようにした方がよい。ウイルス対策は加害者にならないことも重要な対策である。加害者側に過失があれば、損害賠償責任を問われることもあり得るので注意すること。メールの受信に関しても、LAN に接続したままにして 30 分ごとにメールをチェックなどと設定していると、知らない間にウイルスメールに感染し、気が付いたときにはすでに加害者になって、ウイルスメールを送信していたという事態も起こりうる。メールの受信は必ず手動で行い、メールの処理が終わったらプログラムは終了

させるようにした方がよい。

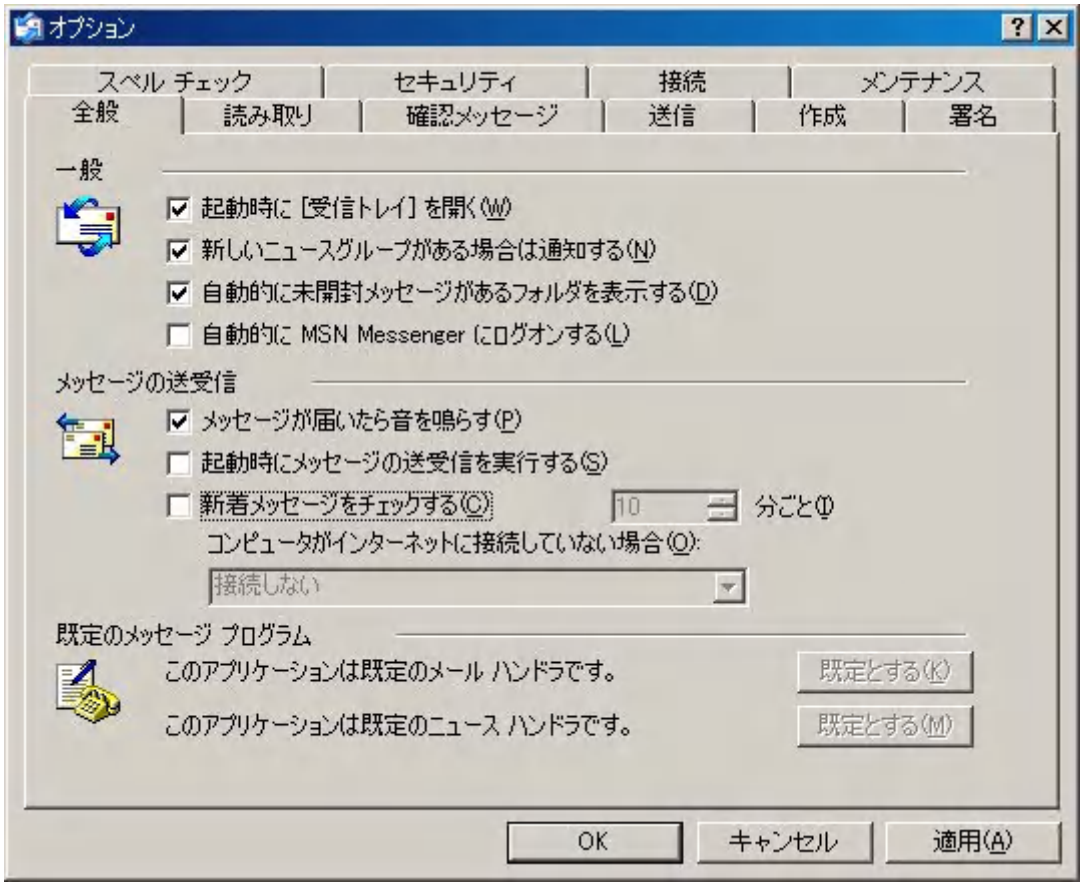
画面 18.オプションの送信設定



常駐でメールソフトを起動したままにするのは危険である。オプションの全般のところで画面 19 のように「起動時にメッセージの送受信を実行する」と「新着メッセージをチェックする」を解除しておくとよい。

他に注意する点として、例えばメッセージルールを利用してメールを仕分けしたり、特定の条件のメールを削除するようにしたりしている場合がある。これらの場合には、ダウンロードしたメールは受信トレイではなく、あらかじめ作成してある別のフォルダや削除済みアイテムに保存されることになる。したがって、そこにウイルスメールがまぎれていても、そのフォルダを開くまで気が付かないことになる。また、受信トレイで開こうとして警告が出たウイルスメールを削除しても、やはり削除済みアイテムのフォルダへ移されるだけなので、パソコン上から削除されたわけではない。削除済みアイテムのフォルダは必ず空にするように注意し、その他のフォルダ内にもウイルスメールを残さないよう確かめておくことが必要である。一部のウイルスチェック用ソフトではスキャンしても、ウイルスとして添付ファイルを検出できないものもある。

画面 19.オプションの全般設定



③. Outlook Express のメールのバックアップ

Outlook Express で受信したメールは何処に保存されているか、知っていて利用している人は少ない。また、受信メールのバックアップを取っている人はさらに少ない。メールは読んだら削除するというならそれでもよいかもしれないが、メールソフトを変えたときに設定や受信メールをインポートしたり、情報収集に使っているメールマガジンなどをデータベース代わりに利用したりするなら、バックアップも必要である。通常受信メールの保存先は、C:¥WINDOWS¥Application Data¥Identities¥の下にある特殊なフォルダの中に、¥Microsoft¥Outlook Express¥というフォルダがあり、その中にデータベース形式（フォルダ名.dbx のファイル）で保存されている。例えば、受信トレイ.dbx のようである。受信メールデータをバックアップするには、このフォルダをバックアップすればよい。Outlook Express にはインポート、エクスポートの機能があるが、専用のツールを利用した方が簡単である。例えば、Exma（http://www.vector.co.jp/soft/win95/net/se163811.html）が便利である。このソフトは Outlook Express 5.X のメール、アカウント、ルールなどの設定、アドレス帳、ダイヤルアップ接続、お気に入りをバックアップしたリストアしたりできる。Windows Me 上の Outlook Express 6.0 でも動作する。メインユーザーのバックアップモー

ドで Exma を起動すると次のようになる。

画面 20. Exma によるバックアップ

ここで適当な場所をバックアップ先に指定すれば、そこにバックアップが作成される。バックアップがあれば、リストアモードで復元が可能である。パソコンを買い替える度に、メールソフトを新規に設定し直して、旧データを捨てていた人もあるかもしれない。普通はエクスポートとインポート機能を利用して、データの引っ越しをすることになるが、例えば Exma を利用してネットワークドライブへバックアップし、そこからリストアすると簡単にデータの引っ越しができる。守るべきデータは、万が一に備えてバックアップしておくのが基本である。

④. ウイルス対策ソフト

ウイルス対策ソフトは、IPA の 7 箇条にあったように最新の定義ファイルで利用する。最近のウイルス対策ソフトは、インターネット上のサーバーから最新の定義ファイルを自動的にダウンロードできるようになっている。定義ファイルはほぼ毎週更新され、その他緊急の場合には、随時専用駆除ツールがメーカーのホームページに掲載される。

ウイルス対策ソフトは、その特徴を理解して設定をきちんとすることが必要である。一般的には手動で検査を実行するものと、常駐して監視するものとがセットになっている。ただし、受信メールに関しては、受信時に自動で添付ファイルを検査できないものもある。ウイルス対策ソフトが常駐していれば、ウイルスが活動を始めると警告が出るので、その時点でウイルスを削除するが、削除処理がどうなされるのかも知っておいた方がよい。活動しようとしたウイルスが読み込まれたメモリ上からは削除されるが、添付ファイル自体は削除されていないこともある。この場合、活動は阻止できるがその後手動でウイルス添付ファイルを削除する必要がある。また、ウイルスが活動してしまった場合、原因となったウイルスファイルを削除するだけでは復旧できない場合がある。削除は発症前のウイルスファイルを取り除くことで、感染して発症したウイルスはシステムファイルを書き換えたりレジストリを変更したりするので、正しい手順操作で駆除をする必要がある。駆除の方法についてはホームページなどで情報を収集してから行う。例えばシステムに感染した

ウイルスが、Windows Me ではシステムを復元するためのバックアップデータ内に残っていることもある。デフォルトでこの機能は自動的に動作しているので注意が必要である。

ウイルス検査については、検査設定がデフォルトでは特定の拡張子のみになっていたり、ゴミ箱のフォルダなどは検査しない設定になっていたりすることがある。検査はすべて実行するように設定したほうがよい。その他バックアップソフトで自動的に外部メディアへバックアップしている場合には、そちらも検査対象に入れるべきである。さらに最近では大手のプロバイダが、会員のメールについて有料でウイルス検査を提供しているところもある。ただし、だから自分のパソコンにはウイルス対策が必要ないというわけではない。ウイルスはメールだけでなく、FD や CD-ROM あるいはネットワークや Web からでも侵入する。参考に通商産業省告示第 429,535,952 号「コンピュータウイルス対策基準」2.用語の定義(1)を紹介しておく。

平成 7 年 7 月 7 日(通商産業省告示第 429 号制定)
平成 9 年 9 月 24 日(通商産業省告示第 535 号改定)
平成 12 年 12 月 28 日(通商産業省告示第 952 号最終改定)
コンピュータウイルス対策基準　2.用語の定義　(1)コンピュータウイルス

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能をひとつ以上有するもの。

1. 自己伝染機能
   自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより他のシステムに伝染する機能
2. 潜伏機能
   発病するための特定時刻、一定時間、処理回数等の条件を記憶させて発病するまで症状を出さない機能
3. 発病機能
   プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

4. Web ブラウザ対策

Web ブラウザを利用してインターネット上のサイトを利用する場合、注意する必要があるのは次のような場合である。

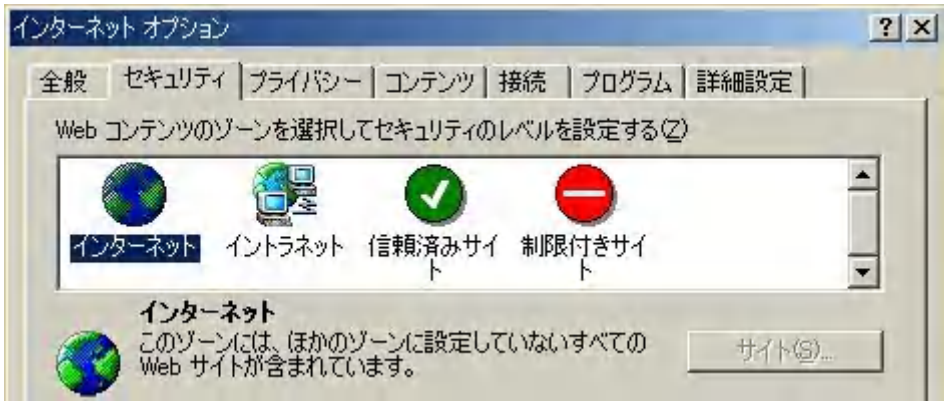
- Web 上のダウンロードサイトから不用意にファイルをダウンロードしない
- Web 上のダウンロードサイトからファイルを開いて実行しない
- 個人情報を入力する場合は SSL (Secure Sockets Layer) 対応の確認をする
- 個人情報の入力にオートコンプリートを使用しない
- ブラウザクラッシャーやウイルスの仕掛けてあるような怪しいサイトを開かない
- Web サイト側のアクセスログにユーザーの記録が残ることを知っておく

もちろん、ブラウザは最新のバージョンにセキュリティパッチをあてたものを利用する。Internet Explorer 6.0 は、すでに解説したように最新版は 12 月現在で画面 10 のバージョンになっている。セキュリティ対策としては cookie の使用条件を制限できるようになったことと、それに関連してプライバシー設定ができるようになったことである。

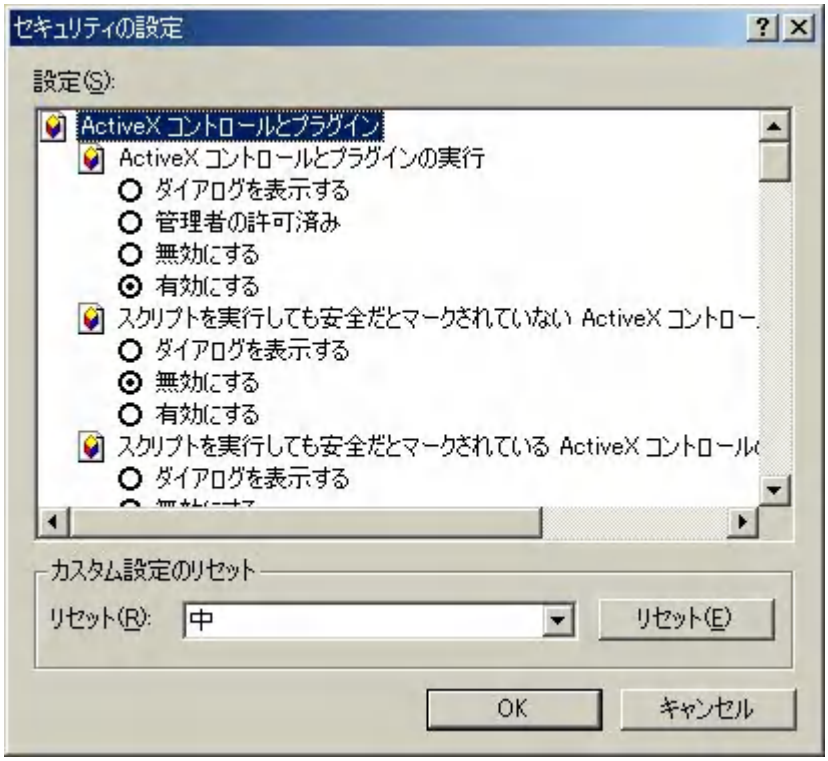
①. Web ブラウザのセキュリティ設定

Internet Explorer 6.0 のセキュリティ設定は、ツールのインターネットオプションのセキュリティで設定する。これは Outlook Express のセキュリティゾーンでも参照される。インターネットのセキュリティレベルはデフォルトで中に設定されているので、この画面でレベルのカスタマイズをクリックして設定を変更する。

画面 21.インターネットオプションのセキュリティ



画面 22.レベルのカスタマイズ　セキュリティの設定



この画面で設定を見直すポイントは、ActiveX コントロールと cookie、JAVA Script である。ActiveX は有効になっていると、Windows を外部から操作できるようになるので危険である。「ダイアログを表示する」に変更するのがよい。また、安全だとマークされていないコントロールや未署名のコントロールは、デフォルトのとおり無効にしておく。ただし、最

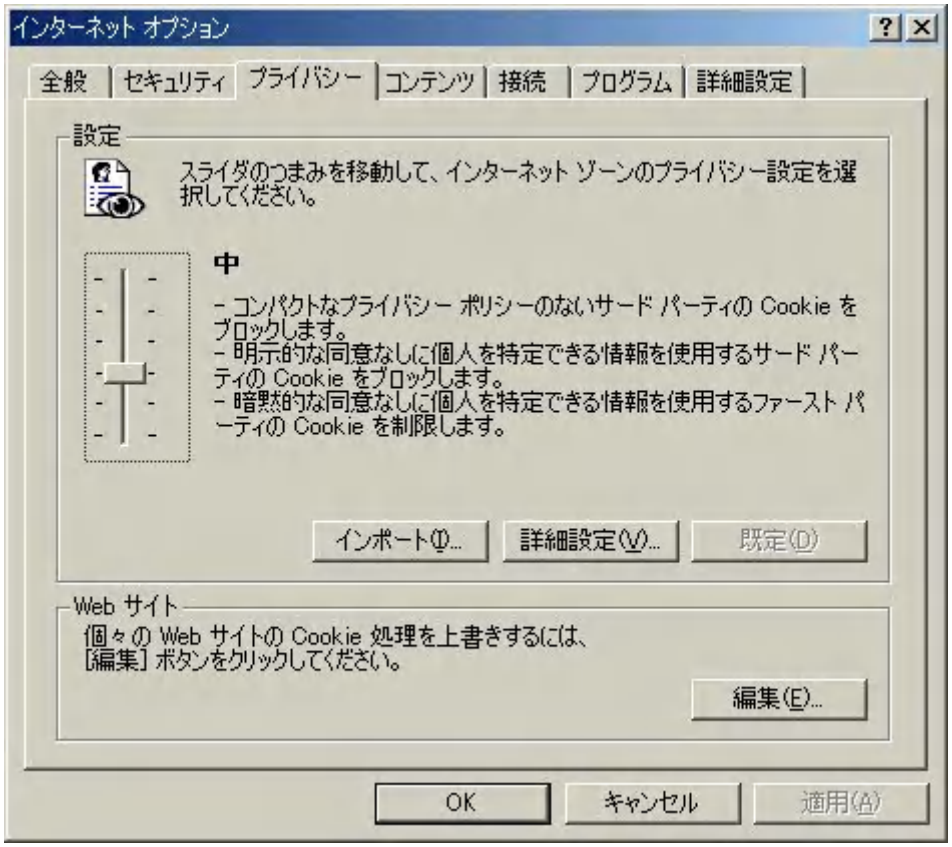
近のウイルス対策ソフトは、ActiveX を使ってウイルス定義ファイルをインターネット上からダウンロードして、インストールするものもあるので必要なときは有効にする。

スクリプトの項目の JAVA アプレットやアクティブスクリプトはデフォルトでは有効になっている。必要ならこれも「ダイアログを表示する」に設定する。そうすれば、勝手に実行されることはなくなる。セキュリティ設定の画面には、その他としてさらに詳細なセキュリティ設定ができるようになっているので、これらも必要に応じて変更する。ただし、セキュリティを高レベルに設定すると、利用できない Web サイトもあるので注意する。

②. Cookie とプライバシー設定

Cookie とは、ブラウザで参照した Web サイトが発行する識別情報や個人情報などで、ブラウザが動作しているユーザーのパソコンのハードディスク内にテキストで保存される。Internet Explorer 6.0 場合の保存場所は C:¥WINDOWS¥Cookies¥である。Internet Explorer 5.5 ではデフォルトですべてのサイトに対して cookie が利用できるようになっていたが、Internet Explorer 6.0 ではインターネットオプションのプライバシーで 6 段階に設定できるようになっている。

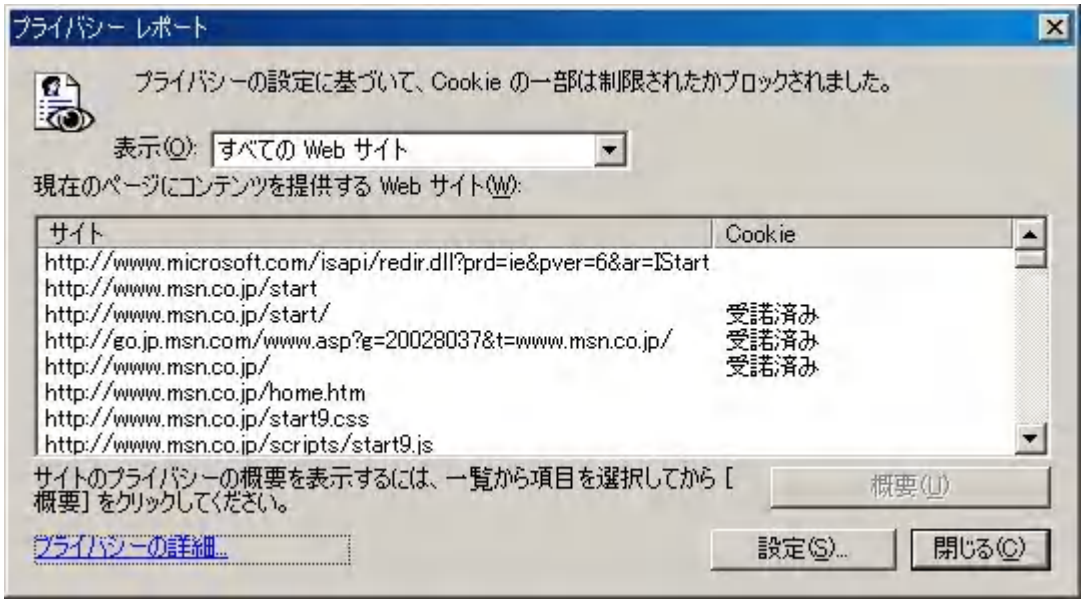
画面 23.インターネットオプションのプライバシー



プライバシーの設定は、詳細設定で変更できる。必要なら、ブロックすることもできるし、ダイアログを表示するなどにも設定できる。また、Web サイトの編集によりサイトごとに許可したりブロックしたりすることができる。cookie 利用をブラウザがブロックすると、ブラウザに下のようなサインが出る。Web サイトがプライバシー保護規格に対応していれば、

Internet Explorer 6.0 の表示のプライバシーレポートを開いて、そのサイトのプライバシーポリシーを読むことができる。

画面 24.表示のプライバシーレポート

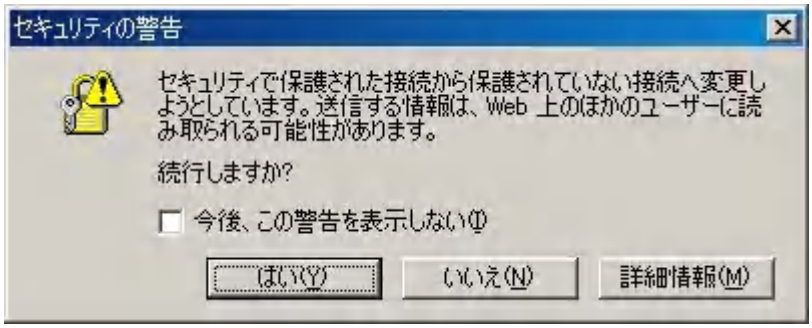


③. SSL (Secure Sockets Layer) 対応

SSL とは Web ブラウザと Web サーバーの間でデータの交換をする場合のプロトコルのひとつで、公開鍵暗号方式による相手の確認と秘密鍵暗号方式によるデータ通信を使って、暗号化されたデータ交換を実現している。Web サイト上で個人情報を入力する際には、途中の経路でデータが盗聴されることもありうるので、必ず SSL でデータ交換をする。暗号強度は Internet Explorer 5.0 SP2 から 128 ビットが使えるようになった。これは画面 10 で確認できる。SSL の Web サイトを参照するときは、プロトコルが https になる。このサイトでは

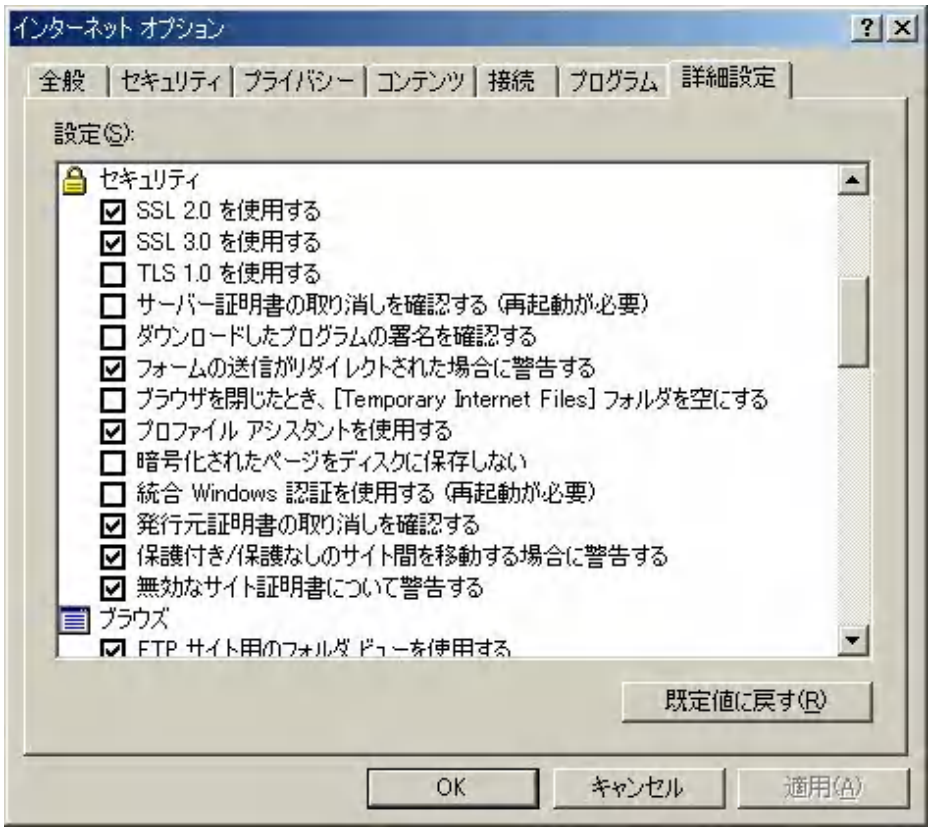
画面右下に鍵のサインが表示されており、ここから通常の Web サイトへ移動するときは警告が出るようになっている。

画面 25.セキュリティの警告



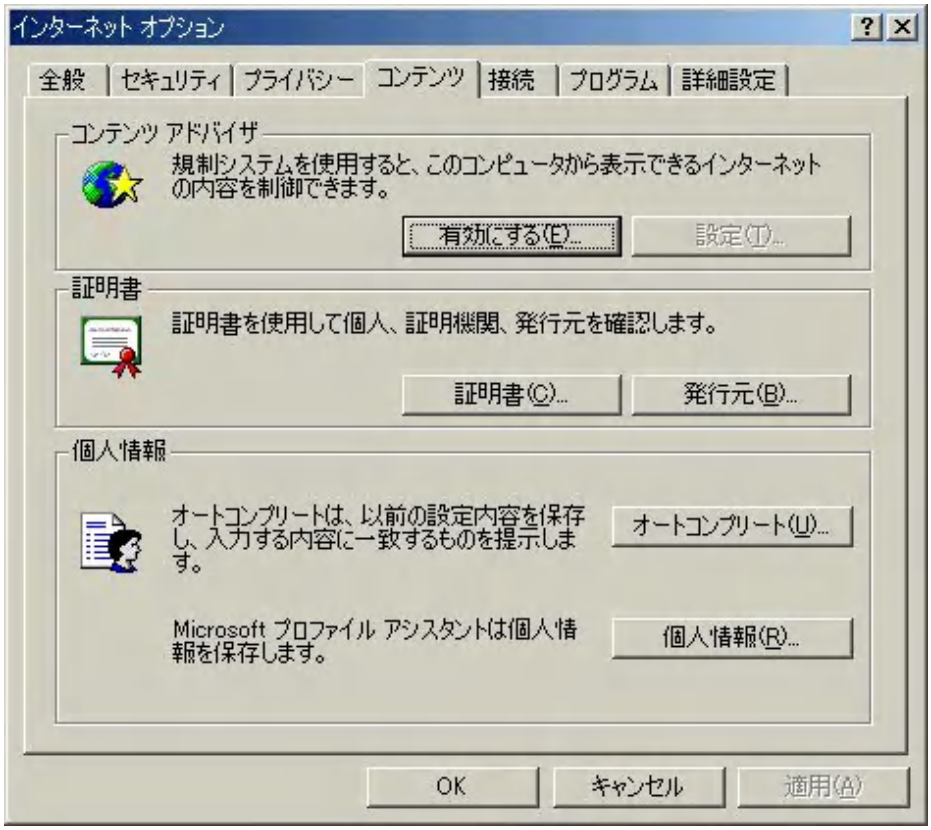
Internet Explorer 6.0 では SSL 2.0 と SSL 3.0 が使用できる。詳細設定を変更する場合には、ツールのインターネットオプションの詳細画面でセキュリティの設定をする。保護付きサイト出入りの際、警告画面を表示するかしないかもここで設定する。

画面 26.インターネットオプションの詳細設定



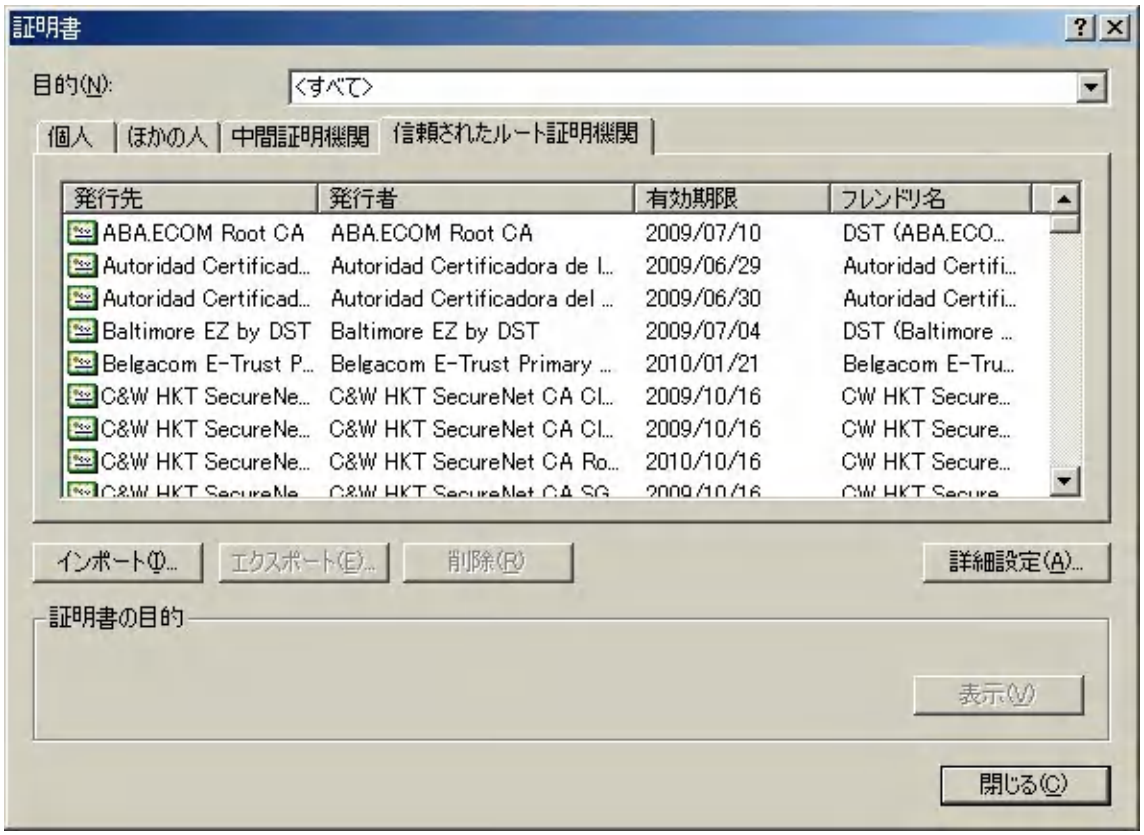
画面 26 のセキュリティ設定で TLS 1.0 は SSL 3.0 を基に標準化をしたプロトコルのことである。セキュリティに利用される証明書や有効期間について確認したければ、コンテンツの証明書を確認する。

画面 27.インターネットオプションのコンテンツ



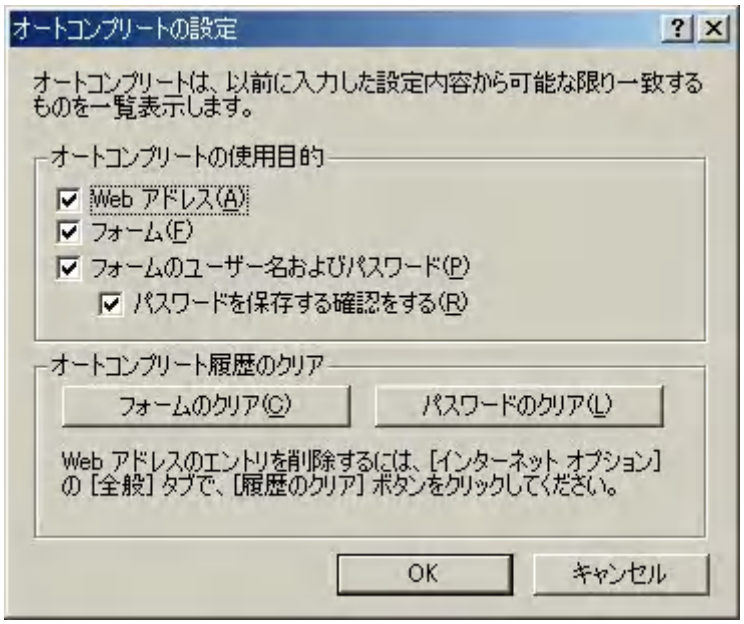
画面 27 で証明書の確認をするには証明書をクリックする。

画面 28.証明書の確認



④. **オートコンプリートの設定**

画面 29.コンテンツのオートコンプリートの設定



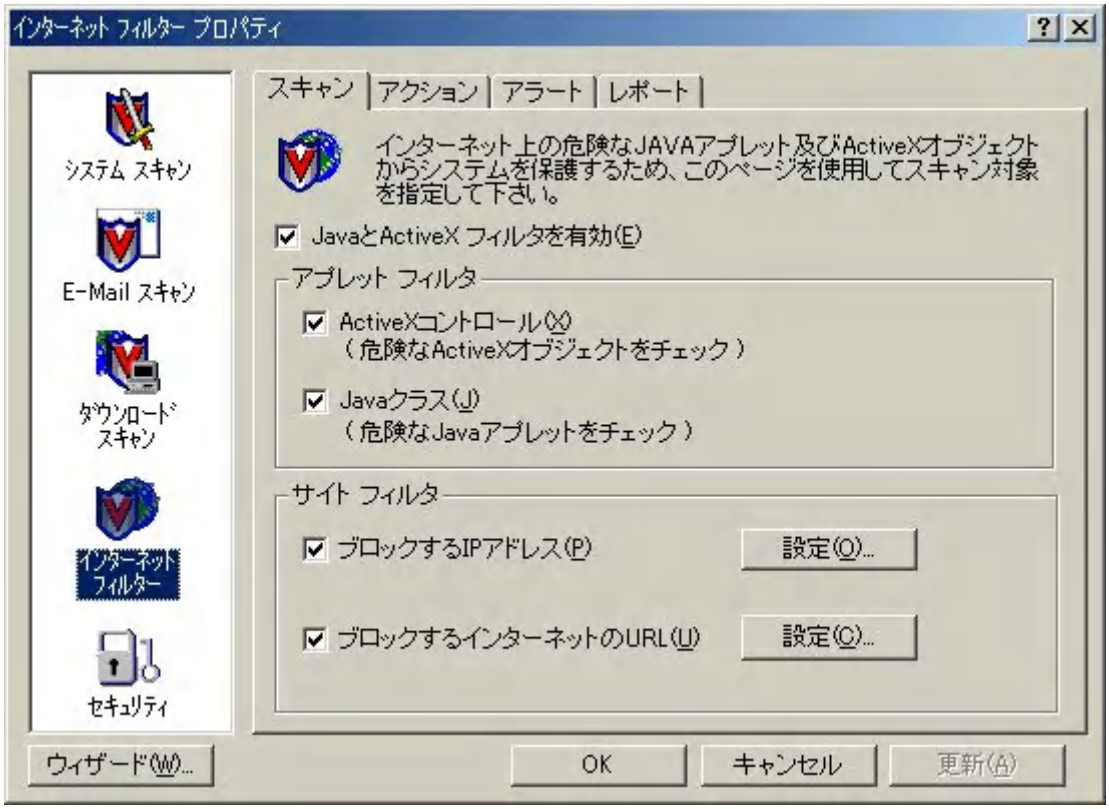
Web サイトのアドレスやフォームなどに一度入力した情報を保存して、二度目以降に一覧から選択できるようにする機能を、オートコンプリートという。この設定は画面 27 の個人情報をクリックして設定する。パスワードなどの個人情報はできるだけ保存しないほうがよい。必要ならオートコンプリートをクリアして、保存情報を削除しておく。その他の Internet Explorer 関連の情報は、履歴 C:¥WINDOWS¥History¥、お気に入り C:¥WINDOWS¥Favorites¥、インターネット一時ファイルは C:¥WINDOWS¥Temporary Internet Files¥に保存されている。

⑤. ブラウザクラッシャー対策

Web サイトを開くと、ブラウザやメールソフトなどのウィンドウがたくさん開いたり、次々と広告ページが開いたりして、やがてリソースを使い果たしてパソコンがフリーズすることがある。たいていは最新のバージョンでセキュリティパッチをあてたブラウザなら、セキュリティ設定をきちんとすれば問題はないが、防御ができないものもある。そういう仕掛けのある怪しいサイトへは、近づかないのが一番のセキュリティ対策である。インターネットを介して Web サーバーと自分のパソコンが接続しているということは、相手から自分のパソコンへもつながっていることになるので、勝手に操作されることもあるということである。

また、ウイルスを仕込んだデータやフリーソフトをダウンロードさせようとするページもある。いくつかのウイルス対策ソフトには、ActiveX や JAVA の検査をしたり、特定のサイトをブロックしたりする機能がある。これらを利用して悪意ある Web サイトに対する対策をするとよい。

画面 30.ウイルススキャンのインターネットフィルター



なお、こうした対策ソフトは正しく設定して常駐で使わないと効果がないので、自分のパソコンのソフトを、最新版にアップデートしたときには一度確認しておくとよい。

5. Windows のセキュリティパッチと Update

ここまで何度も繰り返してきたように、Windows に限らず最新版にセキュリティパッチをあてて利用することが、一番初歩的なセキュリティ対策である。

- Windows Update を実行しダウンロードサイトで更新情報を確認する
  http://windowsupdate.microsoft.com/?IE
  更新していないものがあればダウンロードして更新する
- マイクロソフトセキュリティ情報一覧でセキュリティ情報を確認する
  http://www.microsoft.com/japan/technet/security/current.asp
  必要なセキュリティパッチをダウンロードして対策をする
- 最新のサービスパックをあてる
- ハードやアプリケーションソフトに関してもメーカーの情報を確認する

とくにブラウザやメールソフトだけでなく、オフィス製品やネットワーク関係の製品も含め、対策が必要である。例えばブラウザから呼び出されて起動する Excel や Word、PDF を表示するソフトや動画や音楽を再生するメディアプレーヤーなどにも、セキュリティ対策は必要である。マイナーバージョンアップ時に対策がされることもあるし、パッチファイルで対応する場合もある。サービスパックに関しては、過去の修正プログラムをまとめてインストールできるようになっているだけでなく、新しいプログラムになっているものも含まれるので、必ずインターネットからダウンロードするか、CD-ROM を入手してインストールする。

最近では、メーカーもセキュリティ対策やプライバシー保護に関して、Web やメールなどで積極的に情報公開をするようになってきたが、これらの情報は、悪用することもできるので、広い範囲の情報収集と早めの対策が重要になっている。

- Microsoft のホームユーザー向けセキュリティ対策ガイド
  http://www.microsoft.com/Japan/enable/products/security/
- IPA 情報処理振興事業協会セキュリティセンター
  http://www.ipa.go.jp/security/

その他、セキュリティ関係の一般向け書籍もやや情報が古くなるが参考にするとよい。

- PC 自己防衛マニュアル　Michael A. Banks 著　鷺谷好輝訳　インプレス発行

セキュリティ上のトラブルが発生した場合の対応はここでは取り上げなかったが、あわてずに、専門機関などに相談するのがよい。そのような場合に、どういう環境でどんな現象が起きているか、自分のパソコンの状態を説明できるだけの基本的な知識は身につけてもらいたい。あわせて、日頃から基本的な対策を行い、必要な情報のバックアップを心がけておきたい。

kenji@kawabe.net