コンピュータウィルスに対する正しい知識と対処方法

後藤靖宏
小幡直弘

目　次

近年，コンピュータおよびインターネット回線の普及率が著しく高くなってきており，もはや１世帯で１台以上のコンピュータを所有していることも珍しくはなくなってきた。特にインターネットに関しては，通信産業のインフラストラクチャーが整備されたことに伴い，ネットワークの常時接続が当たり前のようになってきている。

しかし，それとともに，インターネット利用に関する新しい問題や不満も噴出してきている。特にコンピュータウィルスの脅威は，個人のみならず企業や研究機関においても大きな問題となっている。このようなコンピュータウィルスによる被害を防ぐためには，コンピュータウィルスに対する正しい知識を持つとともに，被害の傾向を把握し適切な対応をとっていかなければならない。本論文では，コンピュータウィルスに関する正しい知識と適切な対処法について記述する。

１．コンピュータウィルスとは

コンピュータウィルスとは，コンピュータに侵入してデータやプログラムなどを破壊するもので，その振る舞いや性質が生物学上のウィルスと似ているところから名付けられている。一般的なアプリケーションと同様に，人間によって作成されたプログラムであり，コンピュータウィルスがコンピュータに侵入してくると，使用者に被害をもたらすような機能を持つものである。

1.1 コンピュータウィルスの定義

1995年（平成７年）に通商産業省が告示したコンピュータウィルス対策基準では，コンピュータウィルスを次のように定義している。

コンピュータウィルスとは，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１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，また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，処理回数など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

キーワード：コンピュータウィルス，ウィルス対策ソフト，情報処理教育

プログラムやデータなど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したりするなどの機能。

以上が，通商産業省が告示したコンピュータウィルス対策基準による定義である。

狭義の定義では，コンピュータウィルスは，この３つの機能をすべて含んでいるものを言い，通常は，コンピュータウィルスとよばれるものはこれに該当する。広義の定義では，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を総称して言う。たとえば，以下のものもコンピュータウィルスと言うことができる。

(１) トロイの木馬

有用なツールに見せかけて，使用者が実行すると見かけとは異なった動作をして，使用者に被害を与えるプログラムである。

(２) 論理爆弾（爆弾)

論理爆弾（あるいは単に爆弾）は，データを破壊するなどのプログラムで，感染機能は持っていない。ある設定された条件（実行された回数など）を満たしたときに発病することからこう呼ばれる。また，特に時刻や時間を発病条件に使用したものを時限爆弾と言う。

(３) ワーム

通常のウィルスは感染対象プログラムを必要とするが，感染対象となるプログラムを持たず，自分自身の複製をコピーして増殖する。ネットワークに接続されている他のマシンに出現するので，ネットワーク内をはい回るように見えることからこの名称が付けられた。

1.2 コンピュータウィルスの感染形態

コンピュータウィルスは実に多くの種類が存在しており，その感染対象も多様化している。現在ではコンピュータウィルスの感染方法や行動によっていくつかの種別，またはその複合型に大別することができる。

1.2.1. 感染する場所による分類

(１) ファイル感染型

拡張子が，「.com」，「.exe」，「.sys」などの実行型ファイルに感染する。コンピュータウィルス単体でプログラムを実行したり複製したりするのではなく，実行型ファイルに付着して制御を奪い，プログラムを書き換えて感染，増殖する。

プログラムの先頭や末尾に付着するもの，両方に付着するもの，ファイル内の使用されていない部分にウィルスコードを書き込むもの，完全に上書きしてしまうものなどがある。

(２) システム領域感染型

ハードディスクやフロッピーディスクのシステム領域（ブートセクタ，パーティションテーブルなど）に感染する。

(３) 複合感染型

システム領域感染型とファイル感染型の両方の特徴を持つ。拡張子が「.com」や「.exe」などのファイルに感染するだけでなく，ハードディスクやフロッピーディスクのシステム領域にも感染する。このタイプのコンピュータウィルスに感染したフロッピーディスクからコンピュータを起動すると，コンピュータウィルスがメモリに常駐するだけでなく，ハードディスクのシステム領域にも感染する。

(４) マクロ型

アプリケーションソフト（Word，Excelなど）のマクロ機能を利用して感染を広げる。機種やOSに依存せずに感染することから，マルチプラットホーム型ウィルスと呼ばれることもある。プラットフォームとは，機種やOSの種類のことを意味する。

(５) トロイの木馬型

基本的には他のファイルやシステムに感染活動を行わない，言い換えれば増殖を目的としない不正プログラムである。後述するワーム型やバックドア型の多くもトロイの木馬型

の一種である。他には，プログラムを実行したとたんに破壊活動を開始するものもある。

（6）携帯端末型

携帯端末（PDA など）の OS に感染する。また，携帯電話については今のところ端末上で動作するタイプのコンピュータウィルスは発見されていないが，一部の携帯電話などでは携帯電話上で動作するコンピュータウィルスが発生する可能性がある。

1.2.2. ウィルスの活動による分類

（1）ワーム型

ネットワークを通じてほかのコンピュータに拡散することを目的とした不正プログラムである。メールの添付ファイルとして自動的に自分自身のコピーを拡散させるものやネットワークを利用して次々に感染していくものは，すべてワーム型に分類される。

（2）ダイレクトアクション型

通常は添付ファイルを実行したりダウンロードしたファイルをダブルクリックしたりしなければコンピュータウィルスには感染しないが，ダイレクトアクション型と呼ばれるものは，ブラウザや OS などのセキュリティホール（コンピュータシステム上で正規の手順を踏まなくてもアクセスできてしまうような設計上の欠陥）を利用し，ウィルスファイルをクリックしなくても，自動的に実行する。

（3）ウィルスドロッパー

コンピュータに侵入したコンピュータウィルスが，感染マシン内に別のコンピュータウィルスを組み込むものを指す。またはその活動そのもののことを意味する場合もある。

（4）ネットワーク型

主にネットワーク OS を攻撃し，またそのネットワークを利用して感染増殖する。コントローラ割り込み命令を利用し，他の割り込み命令を制御する。

(5)バックドア型

トロイの木馬型の一種で，ネットワークを介して被害者のマシンを自由に操ったり，パスワードなど重要な情報を盗んだりする。被害に遭ったコンピュータはバックドア（裏口）が開いたような形になることから，こう名付けられている。

1.3. コンピュータウィルスの感染経路

コンピュータウィルスが感染する経路は，主に以下のようなものがあげられる。

（1）メール

メールに添付されているファイルをクリックする（実行する）ことで感染する。システムにセキュリティホールがある場合には，ファイルをクリックしなくても自動的にウィルスプログラムを実行してしまうこともある。

（2）Web（インターネット）

インターネットからファイルをダウンロードしたり実行したりすることによって感染する。便利なツールやゲームなど別のファイルを装っているものも存在する。また，セキュリティホールがあると自動的にダウンロードしてウィルスプログラムを実行してしまうものもある。また，コンピュータウィルスに感染しているサイトでは，そのサイトを閲覧しただけで感染してしまう場合もある。

（3）LAN（局所ネットワーク）

企業や研究機関などでコンピュータ同士をつないでネットワークが作られている場合には，他のコンピュータからコンピュータウィルスが感染することがある。ケーブルテレビのインターネットや公共の無線 LAN などでも同様に感染する場合がある。

（4）その他

これら以外にも，ICQ，MSN メッセンジャーなどのインターネットチャット，メッセンジャー，またはフロッピーディスク，CD-R などのメディアを介したファイルのやりとり，WinMX や Winny などのインターネットファイル共有システムなどによっても感染の危険がある。

1.4. コンピュータウィルスの症例

現在（2004年４月），コンピュータウィルスは全世界で20,000種類以上存在するとも言われている。ここで，最近多く見られるコンピュータウィルスの中で代表的なものとその症例を紹介する。

（１）WORM_NETSKY.Q（ネットスカイ）

流行中の NETSKY ワームの新しい亜種で，これまでのものと同様，自分自身のコピーをつくり，それをメールで不特定多数へ送信するというマスメーリング型ワーム活動を行う。また，DOS（コンピュータの基本的なオペレーティング・システム）を攻撃したり，他のワームの活動を阻害したりする。

ワームの送信する電子メールでは送信者の詐称が行われる。内容は複数の候補から選択されるため不定である。添付ファイルの拡張子は，「.pif」，「.scr」，「.zip」 のいずれかになる。

このメールは Microsoft Windows（以下，Windows）のセキュリティホールを利用してワームメールを開いたり，プレビューしたりするだけで添付ファイルが実行されるダイレクトアクション型のコードが含まれている。

（２）WORM_MSBLAST.A

(エムエスブラスト)

ワームに分類されるトロイの木馬型ウィルスの一種で，Windows のセキュリティホールを利用してネットワーク上のコンピュータに侵入する。また，Windows のアップデートサイト (windowsupdate .com) に対してネットワーク攻撃も行う。感染すると Windows が再起動を繰り返すなどの症状が見られる。

（３）WORM_KLEZ.E（クレズ）

ワームの一種で，Eメールと LAN 上の他のコンピュータへのコピーで増殖すると同時に実行可能形式ファイルへの感染を行う別プログラムも作成する。

E メールで感染する場合には，その差出人を感染コンピュータ内で取得した任意のメールアドレスに設定する場合があるが，差出人として設定されているメールアドレス使用者のコンピュータが感染しているとは限らない。ワームが送信するメールの件名(subject)，本文はランダムな文字列，もしくは「how are you」「let's be friends」などの文字列のいずれかが使用される。

コンピュータのシステム日付が奇数月の６日に，「.txt」，「.doc」，「.mp3」などの拡張子を持つファイルを「ゴミ」データ（不定な文字列・スペース等）で上書きする活動をする場合もある。

（４）JAVA_BYTEVER.A（バイト・バー）

Windows のセキュリティホールを利用したコンピュータウィルスで，実行されたファイルに不正活動を行う内容のものが含まれていると，システムを書き換えるなどの攻撃を受けることがある。

（５）BKDR_BADCODOR.A（バッドコドー）

これはバックドアに分類されるトロイの木馬型不正プログラムである。システムのプロセスに常駐し，キー入力を記録する。

この不正プログラムは使用者のキー入力を保存し，それをメールで不正な使用者に送信するため，個人情報が漏洩する危険性がある。

２．コンピュータウィルスに対する認識に関する調査

これまで，コンピュータウィルスの定義と，その種類，およびいくつかの代表的なコンピュータウィルスの症例について紹介してきた。しかし，実際にはどれぐらいの人がこれらのコンピュータウィルスに対して正しい知識と感染しないための何らかの対策を行っているのだろうか。そこで，コンピュータの初学者を対象に，コンピュータウィルスに対する認識の調査を実施した。

調査の対象は北星学園大学の共通科目「情報処理Ⅰ」を受講している学生131名だった。

大半の学生がコンピュータの初学者であった。なお，家庭にコンピュータを所有している人が131名中127名（98%）で，そのうちネットワークに接続されているものが131名中114名(90%）であった。

2.1. コンピュータウィルスの認知度

コンピュータウィルスについてどれぐらい知っているかを調査したところ，「詳しく知っている」と回答した人が１名，「だいたい知っている」と回答した人が45名，「存在だけは知っている」と回答した人は81名，「知らない」と回答した人は４名だった（図１）。

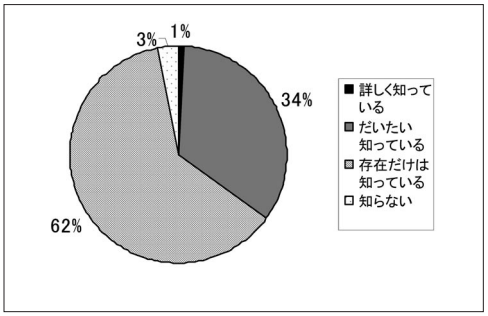

図１　コンピュータウィルスの認知度

2.2. ウィルス対策ソフトの認知度

ウィルス対策ソフトの認知度についてどれぐらい知っているかを調査した結果，「詳しく知っている」と回答した人が０名，「だいたい知っている」と回答した人が29名，「存在だけは知っている」と回答した人は51名，「知らない」と回答した人は51名だった（図２）。

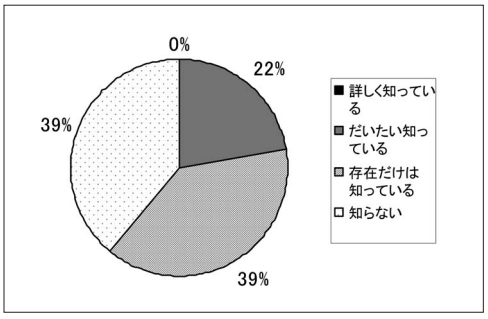

図２　ウィルス対策ソフトの認知度

2.3. ファイヤーウォールソフトの認知度

ファイヤーウォールソフトについてどれぐらい知っているかを調査したところ，「詳しく知っている」と回答した人が０名，「だいたい知っている」と回答した人が８名，「存在だけは知っている」と回答した人は11名，「知らない」と回答した人は112名であった(図３)。

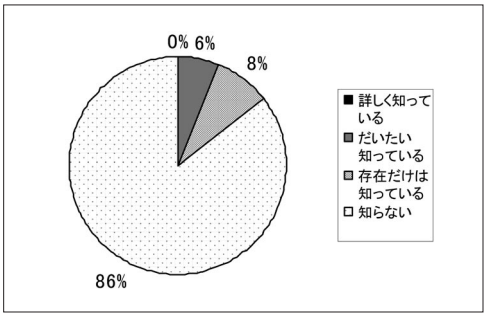

図３　ファイヤーウォールソフトの認知度

2.4. ウィルス対策ソフトの使用

家庭のコンピュータでウィルス対策ソフトを使用しているかを調査した結果，「コンピュータとは別に購入してきたものを使用している」と回答した人が17名，「コンピュータにすでに入っていたものを使用している」と回答した人が17名，「コンピュータに入っていたが別に購入してきたものを使用している」と回答した人が２名，「ウィルス対策ソフトは入っていない」と回答した人が13名，「よく分からない」と回答した人が82名だった（図４）。

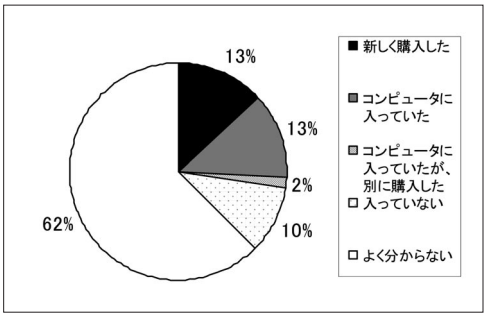

図４　ウィルス対策ソフトの使用

2.5. ウィルス対策ソフトのアップデート

ウィルス対策ソフトのアップデートを行っているかを調査した結果，「自動と手動の両方で行っている」と回答した人は３名，「自動アップデートのみ行っている」と回答した人が15名，「手動アップデートのみ行っている」と回答した人が４名，「どちらも行っていない」と回答した人が３名，「よく分からない」と回答した人が93名だった（図５）。

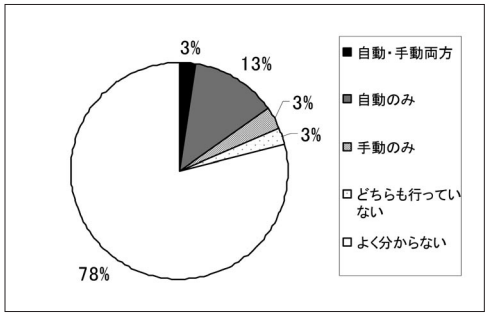

図５　ウィルス対策ソフトのアップデート

2.6. ファイヤーウォールソフトの使用

家庭のコンピュータでファイヤーウォールソフトを使用しているかを調査した結果，「ウィルス対策ソフトについているファイヤーウォールの機能を利用している」と回答した人が２名，OSについているファイヤーウォール機能を使用している」と回答した人が２名，「コンピュータとは別に購入してきたものを使用している」と回答した人が１名，「コンピュータにすでに入っていたものを使用している」と回答した人が１名，「コンピュータに入っていたが別に購入してきたものを使用している」と回答した人が１名，「ファイヤーウォールソフトは入っていない」と回答した人が３名，「よく分からない」と回答した人が120名だった（図６）。

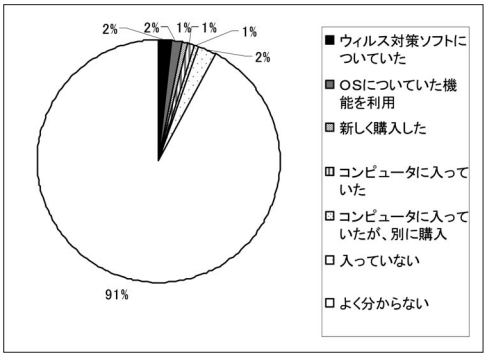

図６　ファイヤーウォールソフトの使用

2.7. コンピュータウィルスに感染した経験

コンピュータウィルスに感染したことがあるかを調査した結果，「感染したことがある」と回答した人が20名，「感染したことはないが，発見・遭遇したことはある」と回答した人が10名，「発見・遭遇したが，サーバ側で駆除された」と回答した人が６名，「感染したことも，発見・遭遇したこともない」と回答した人は48名，「よく分からない」と回答した人は47名だった（図７）。

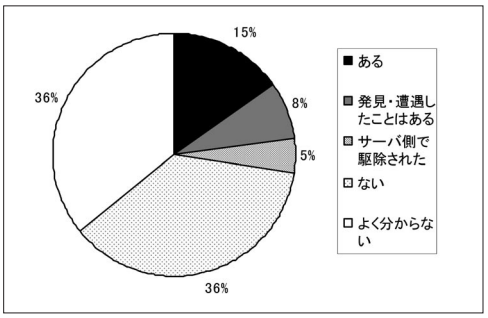

図７　コンピュータウィルスに感染した経験

2.8. コンピュータウィルスに感染した状況

コンピュータウィルスに感染，または発見・遭遇したときはどのような状況だったかを調査したところ，「メールの添付ファイルを開いたとき」と回答した人が６名，「メールを受信したとき」と回答した人が10名，「ホームページを見ていたとき」と回答した人が９名，「インターネットでダウンロードしたファイルを開いた（実行した）とき」と回答した

人が３名，「マクロを使用したとき」と回答した人が０名，「その他」が２名，「よく分からない」と回答した人が62名だった（図８）。

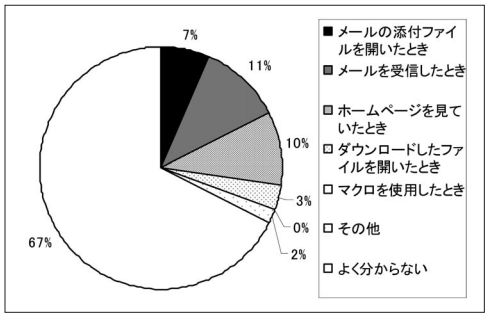

図８　コンピュータウィルスに感染した状況

2.9.　コンピュータウィルスに感染したときの対処

コンピュータウィルスに感染したときの対処法について調査した結果，「ウィルス対策ソフトで対処した」と回答した人が14名，「感染したファイルを削除，再インストールした」と回答した人が４名，「システム(OSなど)を再インストールした」と回答した人が１名，「メーカーのサポートなどに連絡した」と回答した人が５名，「よく分からない」と回答した人が64名だった（図９）。

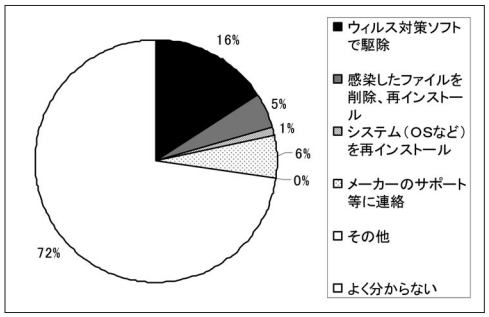

図９　コンピュータウィルスに感染したときの対処法

2.10.　コンピュータウィルスに関して知りたい情報

最後に，コンピュータウィルスに関して最も知りたいと思う情報について調査した結果，「感染しないための予防・対策」と回答した人が53名，「感染したときの復旧方法」と回答した人が47名，「コンピュータウィルスが引き起こす症状」と回答した人が14名，「コンピュータウィルス被害の状況」と回答した人が９名，「新種ウィルスの情報」と回答した人が３名，「その他」が１名だった（図10）。

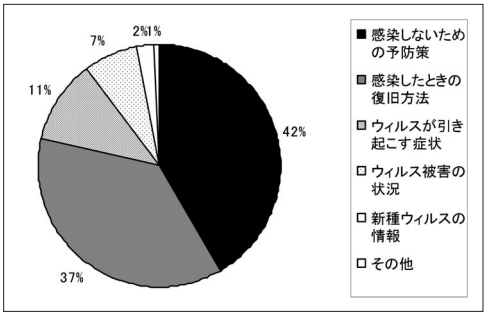

図７　コンピュータウィルスに関して知りたい情報

2.11.　調査結果のまとめ

昨今のコンピュータウィルスの蔓延によって，一般のニュース等でも情報が流れるようになってきたこともあり，コンピュータウィルスを全く知らないという人はほとんどいなかった。しかし，ウィルス対策ソフトやファイヤーウォールソフトに対する認知度は低く，コンピュータウィルスへの対策に関しても不十分であるということがうかがえる。

知りたい情報としては，感染しないための予防策と感染したときの復旧方法の２つの項目が上位に来ていた。これらの内容は，自分の所有するコンピュータやその中にあるデータを守るというだけでなく，不特定の第３者へ迷惑をかけないためにも不可欠なものであると考えられる。

３．コンピュータウィルスへの対策

コンピュータウィルスへの対策として最も有効なのは，コンピュータウィルスに感染しないようにあらかじめ予防することである。しかし，コンピュータウィルスの進化や新種の登場によっては，どれほど予防していても遭遇してしまう危険性がある。

もしコンピュータウィルスに遭遇しても，発見段階において適切な対応をとっていれば被害を最小限に食い止めることができる。さらに，特に目立った被害が出ていなくとも，実はコンピュータウィルスに感染しているというような場合には，その兆候から早期にコンピュータウィルスを発見し対処することが重要になってくる。

このようにコンピュータウィルスへの対策は，その段階において適切に対策をとっていかなければならない。そこで，それぞれの段階において，コンピュータウィルスに対する一般的な対策について紹介する。

3.1. ウィルスに感染しないための予防

3.1.1. ウィルス対策ソフト（ワクチンソフト）の導入

インターネットに接続されているコンピュータにとっては，ウィルス対策ソフトは不可欠なものである。ウィルス対策ソフトについては後の章で詳細に説明するが，感染経路として最も多いと言われるメールの送受信やWeb上からファイルをダウンロードする際にウィルス検査を行ってくれる機能を持っているので，ウィルスに感染する危険性を大幅に減らしてくれる。

3.1.2. システムの設定

ウィルス対策ソフトさえ導入しておけば，それだけで必ずコンピュータウィルスを予防，駆除できるということではない。コンピュータウィルスの多種多様化によってウィルス対策ソフトで発見・駆除ができないようなウィルスも存在している。

そのため，自身でコンピュータシステムの設定を変更することで，セキュリティを高めておく必要がある。

対策Ａ：Windows Updateを行う

使用しているコンピュータのOSがWindowsの場合，インターネット上でWindows Updateを行う必要がある。これを行わないと，Windowsのセキュリティホールを悪用したウィルスに感染する危険性がある。以下にWindows Updateの使い方を記述する。

Windows Updateの方法（付録１）

(１)Internet Explorerを開き，メニューバーの[ツール]の中にある「Windows Update」をクリック。または以下のサイトに直接アクセスする。
http://windowsupdate.microsoft.com/

(２)「更新をスキャン」をクリックすると，Windows Updateが自動的にコンピュータをチェックする。

(３)「更新の確認とインストール」をクリックする。

(４)更新したいものを選び，「今すぐインストール」をクリックする。特に重要な更新とService Packにリストされているものは，セキュリティ上において非常に重要かつ緊急であるものが多いので，必ず選択する。

なお，Windows Me，Windows 2000（SP3以降），Windows XPの場合，Windowsを自動的に最新の状態に保つ，自動更新機能があるので，更新を忘れないようにしたければ，自動更新機能を使うと良い。

対策Ｂ：Internet Explorerのセキュリティを設定する

使用しているインターネットブラウザが，Internet Explorerの場合，セキュリティレベルを設定する機能がある，初期設定では「中」に設定されている。レベル「中」では，安全でない可能性のある内容のものをダウンロードする前に警告してくれる。

しかし，ウィルスやトロイの木馬やハッカーによって，このセキュリティレベルが「低」に変更されてしまう場合がある。不正ファイルを実行してしまう危険性を減らすために，

セキュリティの設定が 「中」以上になっているかどうか，定期的に確認する必要がある。

インターネットセキュリティの設定方法（付録２）

(１)Internet Explorer を開く。
(２)メニューバーから[ツール]→[インターネット オプション]を選択し，[セキュリティ]タブをクリックする。
(３)[規定のレベル]をクリックするとセキュリティレベルは「中」に設定される。詳細に設定したい場合には，[レベルのカスタマイズ]をクリックすると，それぞれの項目を個別に設定することが可能である。

対策Ｃ：拡張子を表示する

Windows のファイルは，すべて「□□□.○○○」というように表記され，□□□の部分がファイル名を表し，○○○の部分がそのファイルの形式を表す。つまり，通常は拡張子によってそのファイルがどのような形式のものであるかを判別できる。たとえば，拡張子が「.doc」であれば Word 文書であり,「.xls」であれば Excel のワークブックであるということになる。

しかし，コンピュータウィルスの中には拡張子の名前を変えて偽装しているものが存在する。つまり見かけ上は別のファイルであるにも関わらず，クリックしたらコンピュータウィルスに感染してしまうという可能性がある。そこで，そのような危険性を減らすためにも，ファイルの拡張子は必ず表示するようにし，不確かなファイルは開かないようにするのが望ましい。

拡張子を表示する方法（付録３）

(１)[マイ コンピュータ]，または任意のフォルダを開く。
(２)メニューバーの[ツール]→[フォルダオプション]を選択する（Windows 95/98では[表示]→[フォルダ オプション]）。
(３)[表示]タブを選択し，[詳細設定]内の[登録されている拡張子は表示しない]チェックボックスのチェックをはずす。
(４)「すべてのフォルダに適用」をクリックする。

対策Ｄ：メールソフトの設定を行う

コンピュータウィルスの中には，Windows のセキュリティホールを利用して感染するものも非常に多く存在する。そのようなウィルスファイルを含むメールが送信されてきた場合，メールを開いたり添付ファイルをクリックしたりしなくても，添付ファイルをプレビュー(メッセージを開かずに表示すること）するだけで感染してしまう場合がある。そのため，添付ファイルのプレビューを表示しないように設定することが望ましい。

Outlook Express で添付ファイルをプレビューさせない設定方法（付録４）

(１)メニューバーの[表示]→[レイアウト]をクリックする。
(２)「プレビューウィンドウを表示する」の□のチェックをはずす。

3.1.3. セキュリティに対する意識を持つ

今までコンピュータの設定における予防について記述してきたが，最終的に重要なのは，ネットワークに接続しているときには，常にウィルス感染などの危険性があるということを意識しておくということである。これはウィルス対策だけでなく，個人情報などの保守においても重要になってくるものもあるので，コンピュータを使用する際には常に意識していることが望ましい。具体的には以下のような心がけが必要である。

メール送受信時

- 差出人欄が知らない人や空白になっている場合，文字化けしているなどの場合は，メールを開かずに削除する。添付ファイルは絶対に開かない。

- 知り合いからのメールでも添付ファイルを開く際には必ずウィルスチェックをする。
- メッセージに Web へのリンクが表示されているときは，リンク先が不確かなサイトの場合はそのリンクをクリックしない。

Web サイトの閲覧時

- よく分からないサイトを閲覧しない。
- 勝手に別のサイトが多数開く（ポップアップする）サイトは閲覧しない。
- 不要なファイルをダウンロードしたり実行したりしない。

3.1.4. データをバックアップする

コンピュータウィルスに感染してしまった場合に備えて，データをバックアップ（保存）しておくことは重要である。コンピュータウィルスへの対策だけではなく，コンピュータのシステムに何らかの障害が生じたときなどにも，必要なデータをバックアップ（保存）しておくことで，消失したデータを回復させることができる。つまり，万が一，コンピュータのトラブルによって重要なファイルが取り出せなくなったり，システムやプログラムを再インストールする必要ができたりしても，バックアップしたファイルを使うことで作業の復旧を迅速に行うことができる。

コンピュータのハードディスク内にバックアップをとると，コンピュータウィルスに感染したときやトラブルのときにバックアップも破壊される可能性があるため，ファイルのバックアップは CD-R などの外部のメディアに保存しておくことが望ましい。

3.2. コンピュータウィルスの発見

コンピュータウィルスは即座に被害を及ぼすタイプのものだけではなく，一定の期間潜伏して，ある程度の時間がたってから発病するタイプのものも存在する。そのようなタイプのコンピュータウィルスに遭遇・感染した場合，感染していることに気がつかない場合がある。したがって，コンピュータウィルスを発見するためには，以下のようなことを普段からおこなっておく必要がある。

3.2.1. ウィルス対策ソフトで定期的にチェックする

ウィルス対策ソフトのウィルス検索機能によって，定期的にコンピュータのハードディスクやその他のドライブをチェックする必要がある。

また，日々，新種のウィルスが発見されているので，それに対応するためにもウィルス対策ソフトのアップデートは必ず行い，最新のデータを入手する必要がある。ウィルス対策ソフトのアップデートについては後で詳しく記述する。

3.2.2. コンピュータの動作から兆候を探る

いくら予防措置を施していても，コンピュータウィルスがコンピュータシステムに侵入してしまうことがある。そのような場合にコンピュータの動作や画面表示などに不審な兆候が見られることがある。以下に，ウィルスに感染した可能性があるときの兆候を記述する。ウィルスによって深刻な症状が現れる前に，これらの兆候から早期にウィルスを発見することは，被害を最小限にとどめるためにも重要である。

動作上の変化

- 動作速度が遅くなる
- メモリが不足する
- システムが使用中に突然止まる
- システムが起動できなくなる
- キー入力ができなくなる

画面表示の変化

- アイコンが勝手に変更されている
- 覚えのないアイコンがある
- 覚えのないメッセージが画面に表示される
- 覚えのない図や絵が画面上に表示される
- 画面上の表示が崩れる（乱れる）

設定の変更

- ブラウザ起動時に表示される Web ページが変更されている
- ダイヤルアップの接続先が変更されている

その他

- ファイルがなくなる，破壊される
- 覚えのないファイルが作成されている
- ファイルのサイズや作成日付が変わっている
- 勝手にメールが送信されている，メールソフトの送信トレイに覚えのない履歴がある
- 勝手に文書ファイルを印刷する

これらの症状が必ずしもコンピュータウィルスによるものであるとは限らないが，頻繁に起こる場合にはコンピュータウィルスに感染している可能性があるため，システムをチェックしコンピュータウィルスに感染していないことを早急に確認する必要がある。

3.3. コンピュータウィルスの除去・システムの復旧

コンピュータウィルスに感染した場合には，そのコンピュータウィルスを駆除する必要がある。もし，そのコンピュータウィルスによってシステムが破壊された場合には，それを復旧しなければならない。

3.3.1. コンピュータウィルスの除去

コンピュータウィルスの除去は，ウィルス対策ソフトを導入していれば，ソフトの指示に従って駆除することができる。もし，コンピュータウィルスによってウィルス対策ソフトやシステムそのものが起動できない場合には，以下のような手順によってコンピュータウィルスを駆除する必要がある。

コンピュータウィルスに感染した場合の手順

(1)ネットワークから切断する

感染したコンピュータがネットワークに接続されている場合，他のコンピュータに感染が広がってしまう可能性がある。それを防ぐために，コンピュータの電源を切った状態で，LAN やモデムのケーブルをコンピュータからはずし，ネットワークを切断する必要がある。

(2)コンピュータウィルスを特定する

次に，感染したコンピュータウィルスがどのようなものかを特定しなければならない。しかし，ネットワーク接続を切断していたり，コンピュータウィルスによってシステムが起動できないという場合には，他の感染していないコンピュータを使用したり，ウィルスソフトメーカーのサポートに連絡したりして，コンピュータウィルスの情報を入手する。

(3)コンピュータウィルスを駆除する

コンピュータウィルスが特定されたら，感染の原因となったメールやダウンロードファイルを削除し，ゴミ箱をからにする。その後，コンピュータウィルスを駆除する。

3.3.2. システムの復旧

コンピュータウィルスを駆除したら，感染したコンピュータウィルスによって変更されてしまったシステムを復旧する必要がある。コンピュータウィルスによって Windows そのもののシステムやファイルが影響を受けた場合は，Windows を再インストールしなければならない。または，ウィルスソフトのメーカーによっては，システム修復のサービスを提供しているところもあるので，それを利用することもできる。

しかし，コンピュータの被害が大きい場合には，コンピュータ全体をフォーマットし直す必要がある場合もあり，そうなると全部のプログラムやファイルが消去されてしまうので，そのような場合に備えて重要なファイルについてはバックアップをとっておくようにすることが望ましい。

ある特定のプログラムだけに感染している

場合は，そのプログラムを再インストールするだけで十分な場合もある。

3.3.3. コンピュータウィルスの再スキャン

システムの復旧が終わったら，別種のコンピュータウィルスに感染していないことを確認するため，もう一度ウィルスチェックをしなければならない。ウィルス対策ソフトを最新版にアップグレードし，コンピュータ全体のウィルスチェックを行い，コンピュータウィルスが完全に駆除できたかを確認する必要がある。

4．ウィルス対策ソフトとファイヤーウォールソフト

4.1. ウィルス対策ソフトとは

ウィルス対策ソフトとは，コンピュータウィルスを除去するソフトウェアで，感染したファイルを修復し，コンピュータをコンピュータウィルスに感染する前の状態に回復するためのものである。その機能からワクチンソフト，アンチウィルスソフトなどとも呼ばれる。

コンピュータがインターネットに接続されているのが当たり前になってきているため，ほとんどのメーカー製のコンピュータには，ウィルス対策ソフトがあらかじめインストールされている場合が多い。

しかし，実際にはその設定や機能についてはあまり知られていないと考えられる。そこで，ウィルス対策ソフトの使用上の注意と機能について記述する。

4.1.1. ウィルス対策ソフトの機能

ウィルス対策ソフトは，多くのメーカーから販売されている。メーカーによって機能も様々だが，その中でもほとんどすべてのウィルス対策ソフトに共通している機能について以下で解説する。

（１）コンピュータウィルス検索機能

ウィルス対策ソフトは，予め用意されたウィルス検知パターンとコンピュータ上のファイルを比較してコンピュータウィルスを検出するというものである。もし該当するパターンがあれば感染ファイルであることを警告し，そのコンピュータウィルスの駆除や隔離，ファイルの復旧や回復を実行する。

（２）ネットワークの監視機能

ウィルス対策ソフトによっては，コンピュータが起動しているとき（インターネットに接続しているとき）には，常に起動してネットワーク状況を監視する機能を備えているものがある。メールの送受信，ファイルのダウンロードなどを行おうとするときに，そのファイルを自動的にスキャンし，コンピュータウィルスに感染していないかをチェックするという機能を持っている。

（３）自動アップデート機能

コンピュータウィルスを検知するためには，先述したようにコンピュータウィルスを発見したり駆除したりするのに用いられる情報ファイルが必要である。しかし，日々新しいコンピュータウィルスやその亜種が増え続けているため，コンピュータが持っているウィルス定義のファイルが古くなってしまい，ウィルス対策ソフトが最新のコンピュータウィルスに対応できなくなってしまう可能性がある。

そこで，ウィルス定義ファイルを新しいものへと更新することが必要である。ほとんどのウィルス対策ソフトでは，この定義ファイルを自動でアップデートできるような機能を持っている。

4.1.2. ウィルス対策ソフトの設定

ウィルス対策ソフトの設定は，ほとんどの場合，インストール時に設定された状態で使用することが望ましい。初回の使用時から設

定を変更していなければ特に問題はないが，設定を変更してしまった場合には，以下の点についての設定を定期的に確認するとよい。

ウィルス対策ソフトの設定

- ネットワーク（通信状態）の監視がオンになっている

  これがオンになっていないと，メールの送受信時やファイルのダウンロード時などにコンピュータウィルスの検知を行わないため，コンピュータウィルスに感染する危険性がある。
- 自動アップデートの設定がオンになっている

  これがオンになっていないと，自動アップデートが行われないため，新種のコンピュータウィルスへの対策が遅くなり，感染する危険性がある。
- システムチェックの日時を確認する

  ウィルスに感染していないかを最後に確認した日時を把握しておく。ウィルス対策ソフトによっては自動でウィルス検索を行うものもあるが，そのような機能がないものの場合には手動でウィルス検索を行う必要がある。そのため，定期的にウィルス検索を行うことが望ましい。

4.1.3. ウィルス対策ソフトの更新

先述したように，コンピュータウィルスに感染しないためには，ウィルス対策ソフトのウィルス定義ファイルを常に最新のものにアップデートしなければならない。

しかし，ほとんどのウィルス対策ソフトはライセンス契約に基づくものであり，ライセンス契約が切れていると，ウィルス定義ファイルを更新することができなくなる。

ライセンスの有効期限は１年間というウィルス対策ソフトが大半であり，ライセンスが切れたら契約を延長しなければならない。

ライセンスの更新の仕方はメーカーによって異なるが，期限切れが近くなると，メールで連絡が来たり，ウィルス対策ソフト自体が警告を発したりする場合が多い。その指示の内容によって，インターネット上で手続きできる場合や，メーカーに連絡を取らなくてはならない場合がある。ウィルス定義ファイルを更新できないと，最新のウィルス定義ファイルが入手できないため，いつコンピュータウィルスに感染してもおかしくない状況になってしまうので，ライセンスの更新は不可欠である。

4.2. ファイヤーウォールソフトについて

4.2.1. ファイヤーウォールソフトとは

ネットワーク上では，常に情報のやりとりが行われている。そのため中には不正なアクセスが行われる場合もある。そこで，そのような不正なアクセスを監視したり遮断したりする機能を持つソフトをファイヤーウォールソフトと呼ぶ。一般的には単独のソフトウェアとして販売されていることが多いが，ウィルス対策ソフトと一緒になっていたり，インターネットのモデムやターミナルアダプタなどのハードウェアにその機能がついていたりすることもある。

4.2.2. ファイヤーウォールソフトの機能

ファイヤーウォールソフトには，大きく分けると二つの種類がある。一つはアプリケーションレベルもので，もう一つはネットワークレベル（パケットフィルタなど）のものである。

アプリケーションレベルものは，通信の設定をアプリケーションごとに行うことが可能である。たとえば，あるアプリケーションを実行したときには通信を許可する，つまりこちらから情報を与えても良いという設定をし，別のアプリケーションを実行したときには，それを拒否するということができる。また，使用者が意図しないような通信の要求を受けた場合には，それを遮断することが可能である。

ネットワークレベルのファイヤーウォールは，送られてくる通信のデータサイズや内容から，それをブロックした方がよいかを判断する。

どちらの場合も，通信の要求があるたびにそれを許可するかブロックするかを使用者に判断させるように設定することができるものもあれば，ファイヤーウォールが自動で判断するものもある。前者の場合は，その通信が自分の意図したものであるか，また必要なものであるかをその都度判断しなければならない。

アプリケーションによっては，初期値ではすべての通信を許可しておらず，使用者が通信の許可を設定しないとならない場合もあるが，あまり許可しすぎると結局はファイヤーウォールの機能が発揮されていないことになるので，その判断を的確に行うことが重要である。

５．コンピュータウィルス以外のネットワークトラブルおよび迷惑行為

ネットワークに接続していると，今まで記述してきたウィルスとよく似た，様々なトラブルや迷惑行為に巻き込まれることがある。しかし，コンピュータウィルスとして認識されないものについては，ウィルス対策ソフトで防ぐことができない。

コンピュータウィルスと違い，感染したりデータを書き換えてしまったりするなどといった被害はないものの，情報の漏洩や操作の妨害をするようなものも含まれているので，これらのネットワークトラブルについても認識しておく必要がある。

5.1. デマウィルス

デマウィルスとは，騒動を起こすために人為的に流されたコンピュータウィルスのデマ情報や，そうしたデマ情報の中で言及されている実在しないコンピュータウィルスのことを総称して言う。存在しないコンピュータウィルスへの注意喚起と対策を呼びかける，使用者の混乱を狙った悪質なメールがインターネット上でよく流れている。

デマウィルスを報じる電子メールの内容は，実際には無意味な注意の喚起や対処方法の説明，知人などへの無分別なメール転送の依頼などである。情報の信憑性を高めるために，IT 関連の大手企業や政府機関の名を挙げ「〇〇社によって確認された」等の情報が掲載されている場合が多い。もちろんこれもデマである。

コンピュータウィルスに対する対処方法として OS やアプリケーションソフトが使用しているファイルの削除を指示する場合が多く，正常にコンピュータが動作しなくなるような悪質な指示が記述されている例もある。

また，デマウィルスに見せかけて実は本物のコンピュータウィルスに感染していたという例もあるため，よく分からない場合にはメッセージを開かずに削除する方が望ましい。

デマウィルス情報によりユーザはありもしないコンピュータウィルスへの対処に時間を割かれ，メーリングリスト等にこれらの情報が投稿された場合には伝播する情報量が多くなることから，ネットワークが不安定になるなどの障害が生じることもある。

セキュリティ対応機関やウィルス対策ソフトのメーカーなどでは，コンピュータウィルスに関する情報と並んでデマウィルスの情報も収集・公開しており，デマウィルスに扇動されることのないよう注意することを呼びかけている。

もし，デマウィルスに関する情報が含まれているようなメールを受信したら，その情報に確信が持てない場合には，メッセージを開かずに削除するのが望ましい。本当に深刻な状況であれば，ウィルス対策ソフトのメーカーやセキュリティ対応機関，プロバイダなどか

らの連絡や対応が必ず発表されるので，それを待ってから適切な対応をすればよい。

5.2. スパムメール

スパムメールとは，ネットワーク上で入手したEメールアドレスに向けて，営利目的のメールを無差別に大量配信することを言う。広義では，インターネットを利用したダイレクトメールの総称を意味する。単にスパムと呼んだり，ジャンクメールと呼んだりすることもある。

このようなメールは，メールソフトの受信フォルダに負荷がかかるだけでなく，同内容のメールを一度に大量に配信するため，インターネットの公共回線に負荷がかかる点も問題となっている。最近では，インターネット接続機能を持つ携帯電話（iモードなど）に対する迷惑メールが社会的な問題になっている。

このようなメールは，送信元を偽装したり，送信を拒否する方法を用意しなかったり，送信拒否の手続きに見せかけて個人情報を収集したり会員リストに登録したりするなどの悪質な手段を使っている業者も多い。そのため，このようなメールを全く受信しないようにするための有効な方法というものは存在しない。

予防策としては，できるだけ自分のアドレスをWeb上で公開しないようにしたり，必要のないメールマガジンに登録したりしないようにすることで多少は減少するかもしれないが，このようなメールの中にはアドレスを予測して一斉配信しているものも多く，完全に遮断することはできない。

最新のウィルス対策ソフトでは，このようなスパムや迷惑メールを判別する機能がついているものもあるので，それを利用すれば，通常のメールと迷惑メールを振り分けることが可能になるが，必ずしもそれだけで分類できるというわけではなく，通常のメールをスパムと誤認してしまったり，スパムを通常のメールとして受信したりすることもある。そのため，このような機能を使っている場合でも，重要なメールをスパムとして削除してしまっていないかを注意しておく必要がある。

5.3. スパイウェア

スパイウェアとは，パソコン使用者の行動や個人情報などを収集したり，システムを借用して計算を行ったりするアプリケーションソフトのことを言う。得られたデータはマーケティング会社など，スパイウェアの作成元に送られる。

スパイウェアは他のアプリケーションソフトとセットで配布され，インストール時にはそのソフトと一括して利用条件の承諾などを求められる。また，スパイウェアは使用者に気づかれないよう，ウィンドウなどを出さずに動作するため，スパイウェアがインストールされていることに気づきにくい。

スパイウェアが行なう活動の内容は，実はインストール時に表示される利用条件の中に書かれているため，インストール時にその利用条件を承諾してしまっている以上，スパイウェアの活動は直ちに違法と言えるものではない。しかし，利用条件の詳細な部分まで読む人はほとんどいないため，大半の使用者はスパイウェアに気づかず，スパイウェアごとソフトをインストールしてしまう。

こうしたスパイウェアは一つのアプリケーションソフトとして認識されてしまうために，ウィルス対策ソフトでは駆除することができない。そのため，スパイウェアを駆除するためには専用のソフトによってスパイウェアを検知し駆除しなければならない。このスパイウェアの検知・駆除ソフトは，フリーソフトとしてダウンロードできるものもあるので，コンピュータに導入して定期的にチェックすることが望ましい。

5.4. アドウェア

アドウェアとは，ソフトを使用させる代わりに，コンピュータの画面に強制的に広告を表示する機能が付随しているソフトのことを言う。

ソフトウェアの操作画面に直接広告を呼び出して表示するものや，Web ブラウザに寄生して一定の間隔で広告ウィンドウを表示させるものなどがある。また，使用者のコンピュータの環境や Web ブラウザのアクセス履歴などの情報を自社や顧客企業に通知し，その結果を元に，表示する広告内容を設定するなどの機能を持つものもある。こうしたソフトウェアはスパイウェアと同様のものであると考えられる。

通常はソフトウェアに広告表示のための機能が内蔵されているが，広告を表示する機能だけを持ったものもある。そうしたアドウェアは他のソフトウェアとセットで配布され，そのソフトウェアが無償で提供される代わりに，ソフトウェアの起動中はアドウェアも動作するようになっている。

アドウェアもスパイウェアと同様，ウィルスとしては認識されないため，駆除するには専用のソフトをインストールする必要がある。このアドウェアの検知・駆除ソフトもフリーソフトとしてダウンロードできるものもあり，導入しておくと良いが，アドウェアの中には，広告表示機能を削除してしまうと使えなくなってしまうものもあり，利用状況に応じて，削除した方がよいか削除しない方が良いかを考える必要がある。

6．まとめ

コンピュータがネットワークに接続されている状態が当たり前になってきているのにも関わらず，コンピュータウィルスに対する正しい知識や，予防・駆除のための対処法についてはまだ浸透しているとは言い切れない。

また，ウィルス対策ソフトがコンピュータに最初からインストールされていたとしても，ウィルス定義ファイルの更新や，定期的にウィルスチェックを行うなどの日々の対策を一般の使用者は十分におこなっていないと考えられる。

大学に入学してコンピュータやインターネットを利用する頻度が多くなる機会に，その利便性だけでなく，その裏に潜んでいる危険性についても十分配慮しておかなければならない。

コンピュータウィルスやウィルス対策などと聞くと，専門知識や高度な技術が必要で，一般の使用者にとっては複雑で理解できないと思う人がいるかもしれないが，今まで解説してきたように，コンピュータウィルスへの対策は基本的な操作と大きな違いはないものがほとんどである。設定方法を一度身につけてしまえば，今後，コンピュータを買ったり，または新しいシステムに入れ替えたりしたときにでも，自分でセキュリティの設定を行うことができるようになるはずである。

最後に，たとえ高性能のウィルス対策ソフトを導入しても，コンピュータウィルスに感染しないようにするためには，最終的には使用者の意識によるものところが大きいということを自覚しなければならない。そのためにも，日々の使用時にもインターネットのセキュリティに対する意識を高く持ち，膨大な情報に対する取捨選択や判断を明確に行うように心がけるべきである。

付録１．Windows Update の方法

図１．Windows Update の画面

1．Internet Explorer を開き，メニューバーの[ツール]の中から Windows Update をクリックする。または，http://windowsupdate.microsoft.com/ を直接入力してアップデートサイトにアクセスする。

2．上記の画面（画面は Windows XP のもの）が表示されるので，「更新をスキャンする」をクリックする。

図２．Windows Updateの方法（その２）

３．更新したいものを選び，「今すぐインストール」をクリックする。特に重要な更新と Service Pack にリストされているものは，セキュリティ上において非常に重要で緊急であるものが多いので，必ず選択する。

付録２．インターネットセキュリティの設定

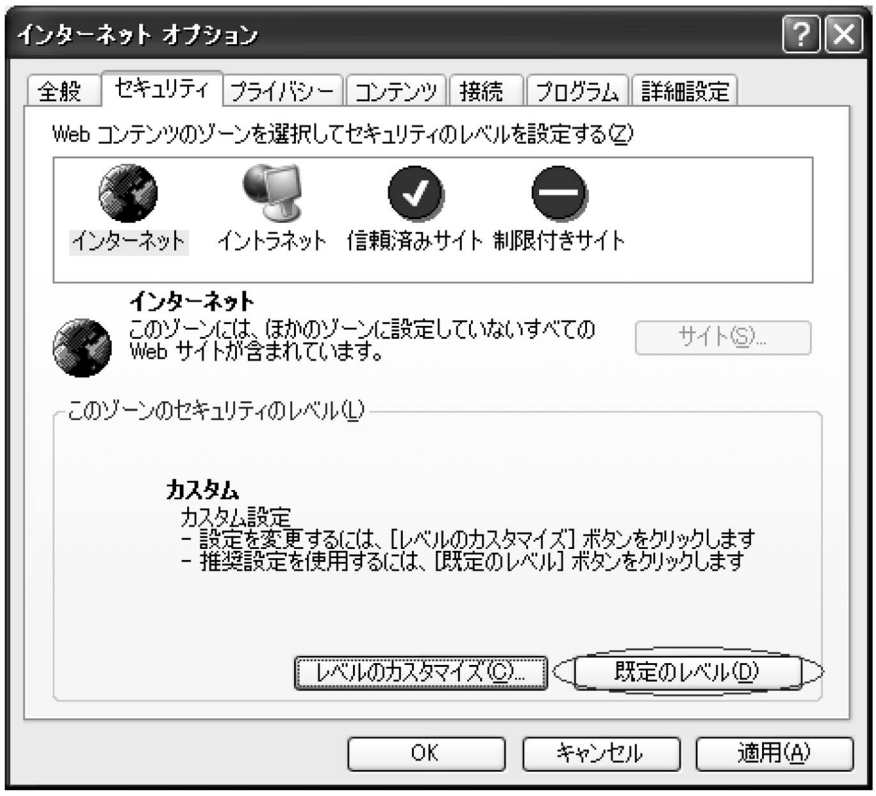

図３．インターネットオプションの画面

１．Internet Explorerを開く。

２．メニューバーから[ツール]→[インターネット オプション]を選択し，[セキュリティ]タブをクリックする。

３．[規定のレベル]をクリックするとセキュリティレベルは「中」に設定される。詳細に設定したい場合には，[レベルのカスタマイズ]をクリックすると，それぞれの項目を個別に設定することが可能である。

付録３．拡張子を表示する方法

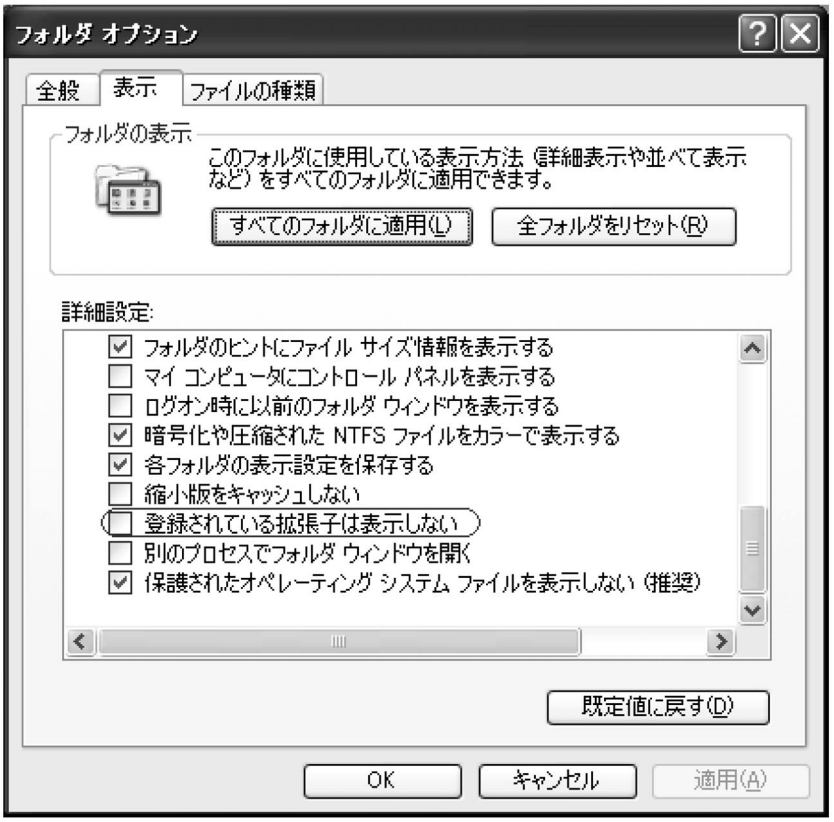

図４．フォルダオプションの設定

1．[マイ コンピュータ]を開く。

2．メニューバーの[ツール]→[フォルダオプション]を選択する（Windows 95/98 では[表示]→[フォルダ オプション]）。

3．[表示]タブを選択し，[詳細設定]内の[登録されている拡張子は表示しない]チェックボックスのチェックをはずす。

4．「すべてのフォルダに適用」をクリックする。

付録４．Outlook Express でメッセージをプレビューさせない設定方法

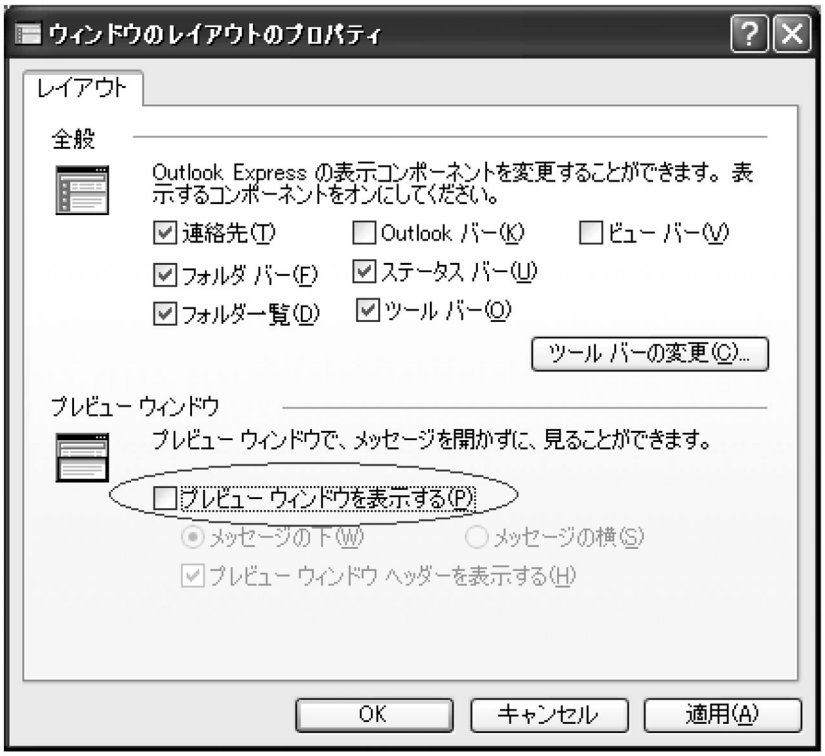

図５．Outlook Express のレイアウト設定画面

1．メニューバーの[表示]→[レイアウト]をクリックする。

2．「プレビューウィンドウを表示する」の□のチェックをはずす。

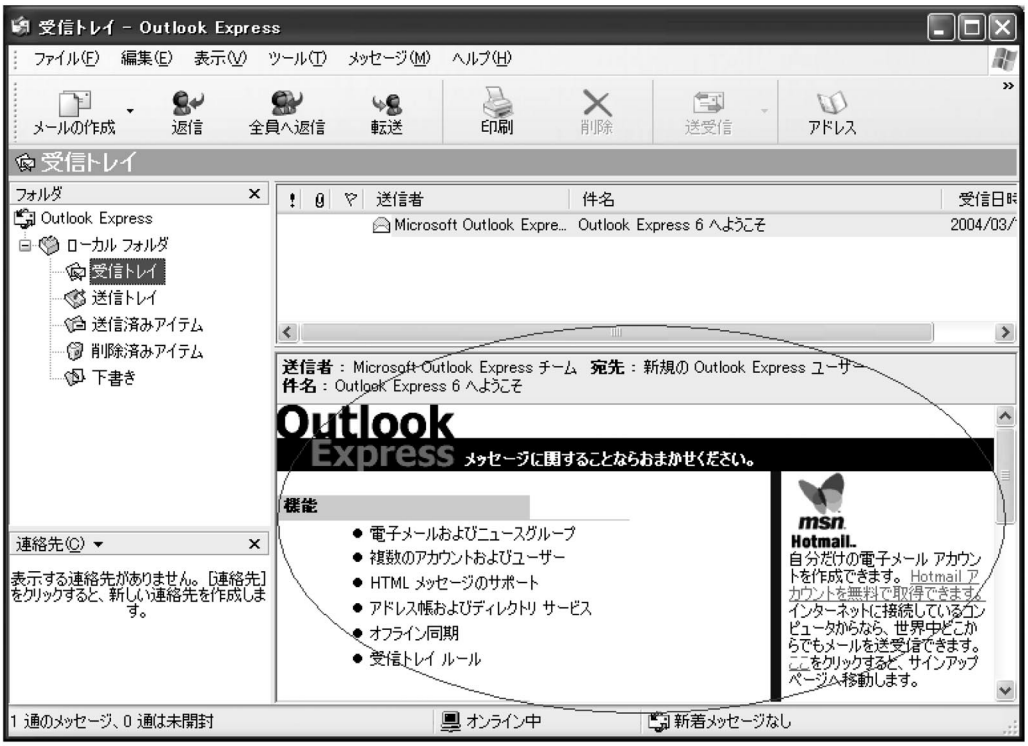

図６．Outlook Express の画面（メッセージプレビュー設定時）

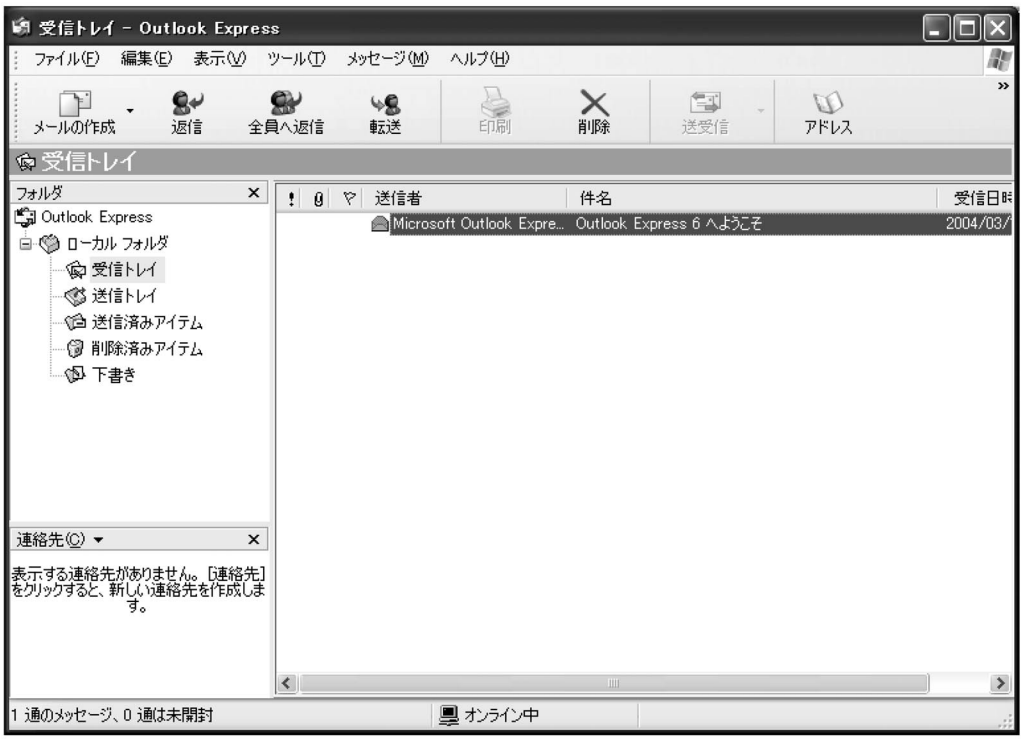

図７．Outlook Express の画面（メッセージプレビュー非設定時）