第7章　情報倫理

- ✓ 情報セキュリティ
- ✓ 不正アクセス
- ✓ コンピューターウイルス対策
- ✓ サイバーストーカーのVTR

1. インターネットは自己責任の世界

インターネット社会は、資格や事前教育があるかは問われないため、ネットワークシステムを悪用する犯罪が多発している。システムの破壊行為から自分のコンピューターやデータを守り、盗難などの攻撃による情報の流出を防ぐために、物理的・論理的にあらゆる危機管理をしておかなければならない。このように、コンピューターシステムの安全を守ること全般を**情報セキュリティ**という。

もう一度コンピューターとインターネットの使用規約(巻末付録参照)に目を通し、安全を守り他人に迷惑をかけないように注意しよう。慣れによる油断、興味本位のインターネットの操作により、自分の情報や友人の情報を安易に公開して、事故に遭わないように注意する必要がある。大学は一切の責任を負わない。<u>全ては自己責任である</u>。

2. 利用上の注意

1. **ユーザーID とパスワードを厳重に管理**する。
2. **電子メールのセキュリティを守ること**(☞**第9章1節**)。
3. **ウェブにある占いやアンケートに回答しない**→名前やメールアドレスを返事すると、知らない間に名簿に載って悪用されないとも限らない。
4. **ウェブページに自己紹介を載せないこと**→お見合い写真を電車のつり広告に出したようなものだ。大学は、個人情報を公開はしていない。
5. ウェブページから見える会議室に意見を述べるのは、ハンドルネーム(ネット上のペンネーム)を使う。意見と一緒にメールアドレスや個人名を書くと悪用されないとも限らないし、嫌がらせを受ける可能性もある。
6. ウェブページは情報の信憑性(しんぴょう)や、内容の濃さにばらつきがある。情報を鵜呑みにしない。

7. ウェブページの内容は著作権によって守られているので、**無断転載や無断で引用をしては絶対にいけない。**特にレポート等に、ウェブページの内容をそっくりコピーすることはもってのほか。
8. 学校の機器では、**オンラインショッピングをしない**。騙されても学校は責任をとらない。

3. 不正アクセスの禁止

インターネットや LAN に、権限のない人が、権限を持った人になりすまして入り、活動を行うことを**不正アクセス**といい、身に覚えのない料金を請求されるなどの被害が増大している。

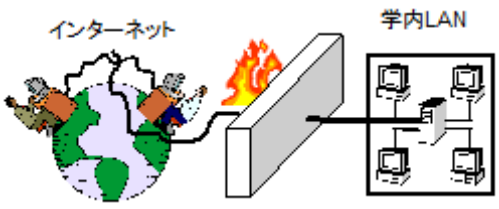
これを防ぐためには、ユーザーID とパスワードの管理が重要である。

- 他人に推測されやすいパスワードは作らない（☞**第１章７節**）。
- 定期的に変更する。
- 入力しているところを見られない。
- インターネットカフェなど共用パソコンではできるだけ避ける。
- 家族や親しい間柄でも他人のユーザーID・パスワードを使用しない。

不正にネットワークにアクセスすることは「**不正アクセス禁止法**」で禁止されている。また、他人のユーザーID・パスワードを第三者に教えることも「不正アクセスを助長する行為」として処罰の対象である。不正アクセスの被害は、情報処理推進機構（IPA）[1]で集約されている。

パソコンに入っているソフトウェアの設計ミスやセキュリティ上の弱点を探し出してそこから侵入されることがある。ソフトウェアは完成品として販売されているが、後から「**バグ**」と呼ばれる不具合が発見されることがある。バグの中には不正アクセスに使われるものがあり、**セキュリティホール**という。

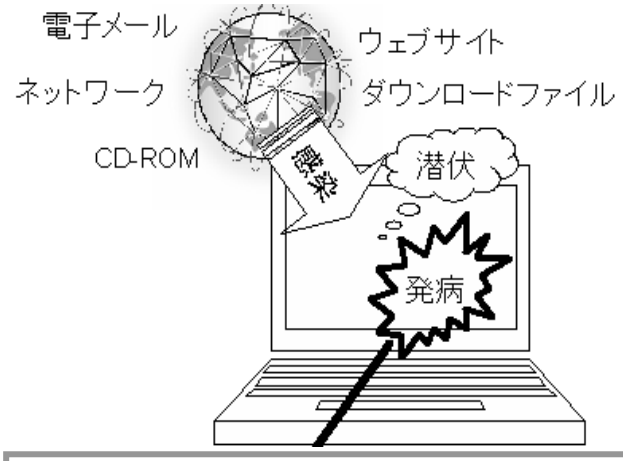
これを監視するためには**ファイアウォール**[2]が有効である。インターネット上の外敵の攻撃を防ぐ最初の砦である。インターネットと個別 LAN(例えば学内 LAN や家庭のホームネットワーク)の間で出入りする情報を監視し、決められたルールをもとに通したり破棄したりする。



1 https://www.ipa.go.jp/security/ciadr/cm01.html

2 個人所有のパソコンの場合、ワクチンソフトを購入するとファイアウォールの機能が付いている。

4. コンピューターウイルスの危険性



- 画面表示が壊れる
- 画面に覚えのないメッセージ、画像、音が出る
- 覚えのないファイルが作成される
- ハードディスク上のファイルを一部または完全に破壊
- アイコンが変更される
- メモリー不足になる
- 動作速度が遅くなる
- 電子メール大量発信
- 個人情報、ファイル内容の流出
- ダイヤル Q2や国際電話への接続
- システムエラーを起こしハングアップする

コンピューターウイルス(**ウイルス**ともいう)とは、不特定多数のコンピューターに何らかの意図的な被害をもたらすために作られたプログラムである。コンピューターウイルスに冒された状況を「感染」といい、コンピューターウイルスの被害が起きた状況を「発病」という。「潜伏期間」をおいて「発病」するものもある。「トロイの木馬」や「ワーム」「マクロウイルス」や「ボット[3]」など特徴や症状によって分けている。最近ではこれらの複合型も増えて、世界各地で非常に多くの種類のコンピューターウイルスが作られている。携帯電話のウイルスもある。

一度コンピューターウイルスに感染すると、駆除や復旧作業に膨大な手間と費用がかかり、紛失・流出したデータは戻らないばかりか、電子メールの自動送付[4]など加害者にもなる。**ワクチンソフト**[5]（アンチウイルスソフト、ウイルスチェッカーともいう）をインストールしてウイルスのパソコン侵入を水際で防ぐ必要がある。

---

3 ボットとは、コンピューターに感染し、そのコンピューターを、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いる。感染すると、外部からの指示を待ち、指示がくると、あらかじめ埋め込まれたプログラムを実行する。この動作がロボットに似ているところから、ボットと呼ばれる。

4 DoS 攻撃---ウェブサーバーに許容量以上のアクセスをしてサーバーをダウン(停止)させることを意図したウイルス。感染したパソコンを攻撃の「踏み台」にして利用し、何万台というパソコンから特定のサーバーにアクセスを仕掛ける。

5 コンピュータアソシエイツ(株):Inocu LAN、Cheyenne Anti Virus、(株)シマンテック:Norton Anti Virus、ソフォス(株):Sophos Anti-Virus、トレンドマイクロ(株):ウイルスバスター、日本エフ・セキュア(株):F-Secure アンチウイルス、マカフィー(株):Virus Scan 、Group Shield などがある。

5. アクションセンターでチェック

予防対策は、侵入を未然に防ぐしかない。被害にあった後では、ファイルは消失していたり、システムがダウンした場合は購入したときの初期状態に戻すことしかできない。また、発病したパソコンで電子メールを送るなどは非常に危険で、他のユーザーにコンピューターウイルスが感染し迷惑極まりない。

パソコンのセキュリティ状態を一覧できるところがアクションセンターである。スタート／[コントロールパネル]／[システムとセキュリティ]／[アクションセンター]をみると、[セキュリティ]と[メンテナンス]の項目があり、セキュリティが不足しているとメッセージが出る。

注意する点は

① ワクチンソフトは**常駐**させて絶えず監視する。処理速度が遅くなるが我慢する。画面右下に表示がある。

自動**スキャン**（ウイルスに感染しているかどうかのチェック）に頼らず、1 週間に 1 回位は手動ですべてのファイルをスキャンすると安全である。

新種のウイルスに対処できるように、インターネットから定期的に**ウイルス定義ファイル**をダウンロードして最新にしておくことが肝要だ。

OSの更新も定期的に行う。[コントロールパネル]／[すべてのコントロールパネル項目]／[WindowsUpdate]／[設定の変更]で更新プログラムをインストールする方法で、「更新プログラムを自動的にインストールする」が推奨される。

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など、アプリケーションのセキュリティ機能を活用する。

定期的に**バックアップ**を取ること。ファイルだけでなく、お気に入りやアドレス帳も保存しよう。

もし感染した場合は、感染したパソコンをインターネットから切り離す。その後、ワクチンソフトで、ウイルスを駆除する。できなければ、初期化し、購入したときの状態に戻す。

6. インターネットセキュリティ

ウェブサイトでは、資格や免許なしで情報を載せられるために、個人情報を取得目的のサイトもある。インターネットの被害に遭わないようにしよう[6]。

① 怪しいウェブサイトを見ない。
   1. 景品応募のサイトに見せかけて、住所や名前を集めることが目的。
   2. 旅行会社で格安のツアーがあるといって申し込ませるが、ウイルス感染を目的としている。

② ファイルのダウンロードは注意する。信頼できるサイトに限定する。
   1. コンピューターウイルスが一緒についてくる。
   2. 無料の動画や音楽関連のファイルによく仕掛けてある。

③ ネット詐欺にかからないように。
   - ✧ ネットオークション詐欺
   - ✧ フィッシング詐欺
   - ✧ 出会い系・アダルトの詐欺
   - ✧ ワンクリック・ツークリック詐欺
   - ✧ 架空請求
   - ✧ 違法販売詐欺

④ 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。

⑤ ブラウザーのセキュリティレベルを指定する。IE の場合は、[ツール]/[インターネットオプション]/[セキュリティ]/[インターネット]で指定する。

---

6 ウェブで情報倫理を勉強できるサイトに、「これだけは知っておきたいインターネット安全教室」（JNSA 日本ネットワークセキュリティ協会） http://www.jnsa.org/caravan/contents/index.html
ビデオ・冊子教材・クイズ学習・迷惑メール疑似体験・セキュリティのセルフチェックサイトがある。

⑥「SSL」(エスエスエル：Secure Socket Layer)を採用しているサイトを使う。

「SSL」とは、データを暗号化して送受信するシステムで、他人に情報を読まれる危険性が少なくなる。宿の申し込みなど、個人情報を記載しなければならないときは、プロトコルに「SSL」を使用しているサイトを使う。URLが「https://」で始まる。

ビデオを見た感想レポート

1. 「インターネットの危険性について」のビデオをみた感想
2. 自分で調べたことについて Word を使って
   1000 字程度でレポートする。

体裁：1行目：「基礎情報科学　○曜　○限」を**左寄せ**とする。
2行目：タイトル　「ビデオをみた感想」　中央揃えとする。
3行目：学籍番号と氏名を**右寄せ**とする。
4行目：空行
5行目～：本文開始
余力があれば、読みやすくするためにフォントを変えたり、太字、アンダーラインなどを活用してもよい。

コラム　スパイウェアの危険

スパイウェアとは、パソコン内の個人情報や履歴情報などの記録をインターネット経由で外部に持ち出すプログラムです。スパイウェアの多くは無償のソフトウェアや体験ソフトウェアにあらかじめ組み込まれていて、インストールのときにスパイウェアも一緒にインストールされます。対策としては、むやみにソフトウェアをインストールしないことです。Windows７には「Windows Defender」が用意されて、スパイウェアの侵入を監視します。

ウイルスとスパイウェアの違いは、ウイルスが多くのパソコンに侵入し、他人のパソコンを破壊するいたずら目的で作成されるのに対し、スパイウェアは入り込んだパソコンから個人情報を盗み出すだけで感染はしません。