第 10 章　情報モラルと情報セキュリティー

近年のインターネットの普及に伴い，世界中の様々な情報をすぐに入手できる便利な世の中になった反面，インターネット・バンキング（ネットバンキング）で不正に預金を送金されたり，ＳＮＳで「なりすまし」の被害に遭ったりするなどの被害に関する報道が後を絶たない。本章では，パスワードを盗まれたり，自分のＰＣに不正にアクセスされて乗っ取られたりすることなどを防ぐにはどのようなことに注意をすればよいのかなどについて述べる。また，不用意な書き込みが「炎上」を招いたりするなどの事例も多々発生している。意図せず「加害者」の立場になってしまわないめの「情報モラル」と，自分の身を守るための「情報セキュリティー」を「車の両輪」としてしっかりと身に付けた上で，ネット（インターネット）を快適に有効に活用することがこれからの社会では求められていると言える。

10.1 コンピュータ教室の使用について

今後，コンピュータ教室（ＰＣ教室）を使う機会がある。クラス単位で使用する場合は，次の座席表のとおり座ること。数値は出席番号である。

以下，ＰＣ教室の使用上の注意事項を列挙する。

【ＰＣ教室座席表】ホワイトボード

1	8	15	22	29	35
2	9	16	23	30	36
3	10	17	24	31	37
4	11	18	25	32	38
5	12	19	26	33	39
6	13	20	27	34	40
7	14	21	28		

(1) コンピュータ教室利用時の注意事項

① 教員機＆サーバ機に無断で近寄らないこと。
② 教室内での飲食は原則禁止である。やむを得ず飲食物を持ち込む場合は，教室の左右にある棚に置くこと。
③ コンピュータに接続されているケーブルを勝手に抜いたり，差し替えたりしない。
④ 大きな音や声を出さない 。(隣の教室の中学校の授業の妨げにならないように)
⑤ イスの座り方に注意すること。座面と背もたれの間にスカートが巻き込まれることがあるので，特に女子は注意のこと。
⑥ 消しゴムのかすや，不要な紙類を放置しない。教室前方のゴミ箱へ捨てること。
⑧ 授業に関係ないものを(他の教科の教科書や課題など)持ち込まない。
教室移動等の都合で，やむを得ず持ち込む場合は，授業中は左右の棚に置くこと
⑨ 情報準備室には勝手に入らないこと。用事があるときはノックして入室のこと。
⑩ 体調がすぐれない場合は我慢せずに先生に連絡し，休むこと。ＰＣ操作は思ったよりも身体に負担がかかるので，無理をせず，早めに知らせること。

(2) コンピュータ教室におけるＰＣの利用について

① 使用するためにはＩＤとパスワードでログインする必要がある。(別途伝える)
② 個人用フォルダ(データ保存フォルダ)は，この教室からでないとアクセスできない。
課題研究では，個人用フォルダは使用しないので，データ等を保存しないこと。
③ プリンタ，デジタルカメラ，カードリーダーなどを利用する場合は必ず教員の許可を

得た後に使用すること。

④ 班別活動を行った後は，椅子や机を必ず元の状態に戻しておくこと。

(3) ＰＣ等使用時の注意事項

① パソコンの設定を勝手に変更しないこと。(壁紙の変更，インターネットでの［お気に入り］への登録等)

② 個人の外部記憶メディア（ＵＳＢフラッシュメモリーやＤＶＤなど）を持ち込まないこと，また，使用しないこと。課題研究用に用意された所定のメモリー類を，絶対に学校外に持ち出さないこと。活動終了後は，必ず所定の場所に返却すること。

③ 携帯音楽プレーヤーなどの周辺機器の持ち込みや接続をしないこと。

④ ソフトウェアや必要のないデータを許可なくダウンロードしたり，インストールしたりしないこと。

⑤ ＰＣやデジタルカメラなどの機器にトラブルが発生したときは，すぐに申し出ること。

⑥ 高校生としてふさわしくないサイトへはいかないようにする。当然であるが，学校のネットワークにはフィルタリングが設定されている。

⑦ ＳＮＳ，掲示板，Web メールなどによる不必要な情報の発信は原則禁止とする。学校内での発信者はすべて「天城高校」ということになる（外部機関から追跡可能)。

⑧ 授業中には，授業に無関係なサイトを閲覧することのないようにすること。

10.2 パスワードの作成と管理

10.2.1 パスワードの不正入手

パスワードを不正入手する人の４０％は「知り合い」である。不正入手したパスワードを使った「不正アクセス」や「なりすまし」などの悪質な行為が後を絶たない。

不正アクセス･･･通信回線を利用して，第三者のコンピュータに侵入し，権限を与えられていない行為を行うこと。 なりすまし　･･･第三者のアカウントを不正に取得し，その人のふりをすること。

パスワードを不正に入手する主な方法として，次の三つが挙げられる。

名称	方法	対策
ブルートフォースアタック	総当たり攻撃とも呼ばれ，考えられるすべての組み合わせをリストアップし，全てを検証する方法	数字だけ，英文字だけなどは避け，数字と英文字（大文字・小文字）の組み合わせなど文字の種類をできるだけ多くする。
ディクショナリアタック	辞書や人名録などのリストに載っているような既存の単語や，それらの組み合わせで検証する方法	Orange，Apple などの一般名詞や有名人の固有名詞などは避ける。
パスワードリストアタック	別のサービスやシステムから流出したアカウント情報を用いてログインを試みる方法	様々なサイトで，同一のパスワードを使い回ししない

10.2.2 認証

ユーザー名（ＩＤ）とパスワードを使って本人であることを確認することを「認証」という。従来のＩＤ，パスワードによる認証に加え，次の認証を組み合わせることでセキュリティーが向上する。この認証方法を「二要素認証」という。

【二要素認証に使われる認証】
･IC カード･･･情報を暗号化して記録できるＩＣチップを搭載したカード
･バイオメトリクス（認証）･･･指紋や虹彩，網膜，顔の輪郭など，生体の一部を読み取る認証のこと
（生体認証）
･ワンタイムパスワード･･･認証のために使用する 1 回しか使えない「使い捨てパスワード」のこと

ネットバンキングでは「ワンタイムパスワード」が使われるケースが多く，スマートフォンに専用のアプリをインストールし，表示された１回限りのパスワードを使うことになる。スマートフォンを使用しない場合は，「トークン」と呼ばれる装置が銀行から送付され，この装置に表示されたパスワードを使って取引を行う。

しかしながら，「二要素認証」といえども盤石ではなく，ネットバンキングの不正送金被害にあった口座の５割超で「ワンタイムパスワード」が突破されていたことが明らかになったとの報道がなされている（2020 年 3 月 6 日付け日本経済新聞朝刊)。どのように複雑なパスワードを設定しても，必ず破られることを認識しておいた方がよい。

大切なことは，パスワードを不正に入手しようとしている悪意を持った人に常に狙われているのだという意識を持っておくことであろう。また，パスワードは個人情報という大事な「資産」であることを意識し，「自分で守る」ことが大切である。

10.2.3 パスワードの作成と管理

(1)パスワードの作り方

①文字数は最低でも８文字以上にすること
→多すぎて困ることはほとんどない

②アルファベット(大文字・小文字)，数字，記号を混ぜること
→記号に関しては、使用できないこともあるので事前に確認すること

③推測されやすいパスワードは使用しないこと
→生年月日，電話番号，英単語，人名などは特に使用しないこと

④複数の Web サイトで同一のパスワードを使用しないこと
→1 つのパスワードが知られると，複数の Web サイトで不正アクセスされる可能性が高くなる

⇨ **自分だけが覚えやすく，他人に推測されにくいパスワード考えること**

【パスワード作成例】
(1)自分に関係のある文章を作成する
［例］私の将来乗りたい車はスカイレイン ER34 です
(2)作成した文章をローマ字表記にする
［例］Watashi no Shorai Noritai Kuruma ha Skylane ER34 desu
(3)大文字にした部分と数字だけを並べ，3 番目と 4 番目の文字は大文字にする
［例］wsNKser34 ⇒ 残すメモ:私が将来乗りたい車，34→大

この例のように，「自分にしか分からない」ことを使って作成することと，どのようなメモを残しておくかについて参考にしてほしい。

現実的には，いくつかのセキュリティーのレベルに分けてパスワードを設定し，使い分けることも考えられる。ネットバンキングやオンラインショッピングのパスワードが盗まれると経済的な被害を受けることになるが，ネット上の記事を読むためのパスワードが盗まれた場合は，決してよいことではないが，経済な被害までは受けることはない。したがって，万が一パスワードが盗まれたときに経済的な被害を受けることが想定されるような場合は，セキュリティーレベルのかなり高いものを設定する必要がある。

作成したパスワードの強度をチェックするサイトがあるので，試してみるとよい。検索ボックスに「パスワード　チェックサイト」などとキーワードを入力すると，いくつかのさいとが表示される。

では，実際にパスワードを作成してみよう。ただし，この演習で作成したパスワードを実際に使うことのないように。

【パスワード】

読み												
種類												

【記入の仕方】

①パスワードの欄に１文字ずつ**正確に，丁寧な字で**記入すること。

②「読み」と「種類」は次の例に従って入力すること。

例	パスワード	I	i	9	0	q	0
	読み	アイ	アイ	キュウ	ゼロ	キュー	オー
	種類	大	小	数	数	小	小

③パスワードは、８文字以上で欄内におさまる文字数にすること。

④記号（？　．　-　^@等）はパスワードを設定するときにサービスによっては使えないこともあるので，今回は使用しないこと。

【注意事項】

○パスワードは自分で責任を持って管理すること。

○変更後のパスワードは他人に見られない場所に貼るかメモしておくこと。

(2)パスワードの管理

①確実に管理して，紛失しないようにすること

→パスワードが不正入手される原因の多くは不注意による紛失である

②最初に配布されたパスワードは変更すること

→パスワードを発行するサーバが不正アクセスされる可能性もある

③パスワードのメモは絶対に他人に見られない場所にすること

→「メモをしてはいけない」という記述は必ずしも正しいとはいえない

④パスワード入力時に背後から見られないようにすること

→携帯電話のパスコードなども同様に注意すべきである

⑤共有のパソコンでむやみにパスワードを入力しないこと

→履歴が残るので、簡単に不正入手される可能性がある

⑥パスワードを他人に教えたり，譲渡したりしないこと

→管理者や知り合いであっても絶対に教えてはならない

10.3 マルウェア

「マルウェア」(Malicious Software が由来で，Malware）とは，コンピュータに何らかの被害を与えるよう，悪意を持ってつくられたプログラムである。「コンピュータウイルス（ウイルス)」は，マルウェアのうち，他のＰＣに感染する機能を持つものである。コンピュータウイルスは，データやプログラムに寄生し，メールやWebページを通じて広がる。パスワードもそうであるが，私たちが普段使っているＰＣも，悪意を持つマルウェアに常に狙われているという意識を持っておくことが大切である。2018年には，「WannaCry（ワナクライ)」と呼ばれる身代金を要求する「ランサムウェア」が流行した。ネットを閲覧していると突然ＰＣがフリーズし，データを回復したければ金銭を支払うよう促すメッセージが表示される。余談になるが，「Want to cry」を米国式に発音すると「ワナクライ」に近い音になる。仕事中にこのようなマルウェアに攻撃されると，文字通り「泣きたくなる」であろう。

マルウェアの種類として，ウイルスの他には，便利なアプリとしてインストールされ他のＰＣに侵入して遠隔操作を行ったりする「トロイの木馬」や，気がつかないうちに個人情報を収集して第三者に送信する「スパイウェア」などがある。

このように，日々新しいものが出現しているマルウェアによる被害に合わないためのセキュリティー対策として，最低でも次の二つは常に確認しておいた方がよい。

・ＯＳのアップデート

Windowsなどの ＯＳを常に最新のものにアップデートしておく。

・ウイルス対策ソフトウェアの定義ファイルを常に最新のものにしておく。「定義ファイル」は生物で言うウイルスの塩基配列の情報だと思ってよい。

マルウェアによる被害のほかにも，「ネット詐欺」と呼ばれる被害も多い。偽サイトに誘導してパスワードを入力するよう促してパスワードを不正に入手する「フィッシング(Phishing)」や，入会していないサービスの入会金や会費，利用料などを請求する「架空

請求」と呼ばれる詐欺もある。

フィッシングにあわないためには,閲覧しているサイトが本物かどうかを確認することが大切である。そのためには,ブラウザのアドレス欄に表示されているＵＲＬを確認するとよい。本校のトップページのＵＲＬは次のようになる。

http://www.amaki.okayama-c.ed.jp

なお,「www.amaki.okayama-c.ed.jp」　の部分を「ドメイン名」と呼ぶ。

ドメイン名の末尾の「jp」で国を識別することができる。英国は「uk」,フランスは「fr」,ドイツは「de」となる。また,「ed」は学校などの教育機関を示す「組織の種類」を表しており,次の表のような2文字が使われている。

組織の種類	記　号	意　味（英語）
大学や研究機関など	ac	academic
幼稚園，小・中・高等学校	ed	educational
民間企業，会社	co	commercial
政府関連組織	go	governmental
財団法人，社団法人など	or	organization
ネットワーク事業者など	ne	network