# 情報モラルと情報セキュリティ

## 情報モラル

### 情報モラルとは

**『情報社会で適正な活動を行うための基になる考え方や態度』**

情報社会では、一人一人が情報化の進展が生活に及ぼす影響を理解し、情報に関する問題に適切に対処し、積極的に情報社会に参加しようとする創造的な態度が大切である。誰もが上の運送り手と受け手の両方の役割を持つようになるこれからの情報社会では、情報がネットワークを介して瞬時に世界中に伝達され、予想しない影響を与えてしまうことや、対面のコミュニケーションでは考えられないような誤解を生じる可能性も少なくない。このような情報社会の特性を理解し、情報化の影の部分に対応し、適正な活動ができる考え方や態度が必要となってきている。そこで、学習指導要領では、「情報社会で適正な活動を行うための基になる考え方と態度」を「情報モラル」と定め、各教科の指導の中で身につけさせることとしている。

（引用元）第5章　情報モラル教育（文部科学省）

http://www.mext.go.jp/b\_menu/shingi/chousa/shotou/056/shiryo/attach/1249674.htm

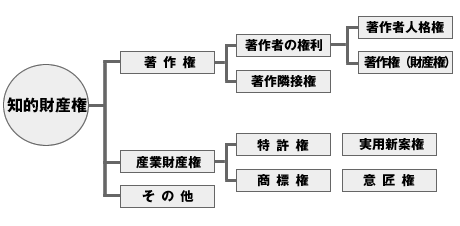
### 情報モラルの具体例

**チェックしてみよう**

|  |  |  |
| --- | --- | --- |
| No | 確認事項 | チェック |
| 1 | 自分のブログやFaceBook、twitterなどに友人の写真を公開するときには、本人の許可をもらっている。 | ( ) |
| 2 | 自分のブログやFaceBook、twitterなどに、インターネットで見つけた画像やイラストを無断で投稿していない。 | ( ) |
| 3 | サイトなどに文章を書くとき、引用は最低限にして、引用する場合は、引用元を明記している。 | ( ) |
| 4 | 購入したCDやDVDをコピーして、友人に渡したりしていない。 | ( ) |
| 5 | TV番組を録画して、その動画を動画サイトなどに投稿していない。 | ( ) |
| 6 | メールを書く場合、冒頭に差出人（自分の名）を明記し、末尾には自分のメールアドレスを明記するなど、配慮している。 | ( ) |
| 7 | お互い面識のない複数の人に一斉にメールを送信するときには、BCCを使っている。 | ( ) |
| 8 | インターネットで情報を入手し、ほかの人に伝える前に「その情報が正しいのか」を確認するようにしている。 | ( ) |
| 9 | 自分の趣味や関心のあることをまとめて、ブログやFaceBook、Twitterなどで情報発信している。 | ( ) |
| 10 | 災害時にソーシャルメディアがどう使えるのか、使い方をチェックしたことがある。 | ( ) |
| 11 | ブログやFaceBook、Twitterなどに記事を書く前に「その内容は他人を不愉快にさせる内容ではないか」を考えるようにしている。 | ( ) |
| 12 | モバイルカメラで講義の様子を録画したり板書を写したりするときには、講師に許可を得ている。 | ( ) |

### 著作権と個人情報保護

* 著作権



著作権は、知的財産権の1つで、知的財産権は他に商標・実用新案・特許権に関する産業財産権などがある。

著作権は著作物が創造された時点で発生し、申請や登録の必要がない。（**無方式主義**）

また、**著作物の保護は著作者の死後50年間**と定められている。

Webサイトにおける著作物とは、文章・イラスト・画像・音楽・プログラムなどあらゆるものが相当し、これらの著作物を使用するには、著作者から許諾を得る必要がある。引用や私的使用など、例外的に著作者から許諾を得ることなく使用できる場合があるが、出所の明治が必要などの条件があるので取扱には注意する。

例）

|  |  |
| --- | --- |
| 最終成果物であるWebデータ | 特に特殊な契約でない限り、著作権はクライアント側 |
| Webデータを制作するためのラフなどといったPhotoshopやIllustratorなどのファイル（中間生成物） | 製作者側 |

* **個人情報保護法**

何をもって個人情報であるかのポイントは、現在生きている特定の個人を、その情報によって識別可能かどうかということである。5000件を超える個人情報のデータを持ち、事業に使用している事業者などは個人情報保護法における個人情報取り扱い事業者となる。

個人情報を取り扱うには、利用目的を本人に通知し、請求によって訂正・利用停止をしなければならない。個人情報を収集する場合は、偽り・不正な手段を使用してはならず、漏洩・改ざんなどが無いよう適切な取扱い、対処を行わなければならない。第三者へ個人情報を提供する場合、あらかじめ本人の同意が必要になるが、警察の調査や国の税務調査、事故・災害など生命の危険に関わる場合はこれにあてはまらない。

（参考）

内閣府　個人情報の保護に関する法律

<http://www.kantei.go.jp/it/privacy/houseika/hourituan/>

財団法人 日本情報処理開発協会　よくわかるプライバシーマーク制度

<http://www.privacymark.jp/wakaru/index.html>

* 特定商取引法

特定商取引とは、特定商取引法における、訪問販売・通信販売・電話勧誘販売などのことで、Webにおけるネット販売はこの通信販売に相当する。

運営会社名、連絡先に加え、支払い方法、発送方法などの販売条件表示に関して決まりがあるので、注意する。

（参考）

消費者庁　消費生活安全ガイド

http://www.no-trouble.jp/

### Web制作と情報モラル

他のWebサイトの文章の引用

引用はかまわないが、引用元を明記すること。また、改変はできない。もしも、そのページの大部分が引用ばかりだとすると、それはもはや引用とは呼べない。模倣となる。このあたりは論文やレポートの作成と同様である。

ネット上の画像の利用

ネット上の画像には著作権があるので、著作権者の了解なく勝手に利用できない。ただし、無料あるいは有料で写真やイラストなどの画像を提供しているサイトもある。（写真AC、イラストAC、など）。商用利用も可能なところもあるので、そういうところを利用するとよい。

自分の撮影した写真の利用

その写真に個人が特定できる人物が写っていた場合、本人の許可なくネット上にアップロードすることはできない。また、店舗などの写真も同様である。ただ、街を写した写真の中に、一部分その建物が写っている場合はいいかも。

他のWebサイトのデザインの模倣

Webサイトのデザインにも著作権があるので、模倣はできない。

## 情報セキュリティ

### 情報セキュリティとは？

私たちがインターネットやコンピュータを安心して使い続けられるように、大切な情報が外部に漏れたり、ウイルスに感染してデータが壊されたり、普段使っているサービスが急に使えなくなったりしないように、必要な対策をすること。それが情報セキュリティ対策です。

（引用元）国民のための情報セキュリティサイト（総務省）

http://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/intro/security/index.html

# チェックしてみよう

|  |  |  |
| --- | --- | --- |
| No | 確認事項 | チェック |
| 1 | 初めて利用するネットショップやWebサービスでは、利用規約やプライバシーポリシーを確認している | ( ) |
| 2 | セキュリティーソフトをインストールしている | ( ) |
| 3 | 定期的にOSのアップデートをしている | ( ) |
| 4 | 定期的にウィルス定義ファイルを更新している | ( ) |
| 5 | ウィルスに感染した場合の対処方法を理解し、実践できる | ( ) |
| 6 | パスワードを付箋に書いてパソコンに貼るなど、人目につくところに記載していない | ( ) |
| 7 | パスワードをわかりにくいものにしている | ( ) |
| 8 | ネットショッピングやネットークションで、どんなトラブルが起こり得るか知っている | ( ) |
| 9 | 公衆無線LANの危険性を理解し、適切に利用している | ( ) |

### 情報セキュリティの知識

ユーザー名とパスワードの取扱い

ユーザー認証に使われるユーザー名とパスワードは以下のように慎重に管理する必要がある。

* 英字の大文字と小文字を組み合わせたり、英字と記号・数字を組み合わせたりする。
* 生年月日や電話番号など、推測されやすいものにしない。
* 初期のパスワードは変更する。
* 手帳などよく持ち歩くものに記録しない。
* よく見えるところに書いておいたりしてはだめ。

ファイル・アプリのダウンロード

信頼できるサイトからダウンロードする。（スマホの場合はAppStore、GooglePlay）

ダウンロードしたファイルは、Windows Defender でスキャンしてからインストールする。

解凍・インストールの知識をもつ。

IPアドレスで個人は特定されるか？

インターネットでは各パソコンはIPアドレスでお互い同士が接続している。ここでいうIPアドレスは、グローバルIPアドレスのことで、詳しくは「インターネット概論」で説明する。このIPアドレスは、ISP（インターネット・サービス・プロバイダ）によって割り振られている。このIPアドレスから個人を特定することはできない。このIPアドレスから個人を特定できるのは、ISPだけである。（警察の犯罪捜査に協力する際にIPアドレスの情報を警察に提供することはあり得る）

したがって、「あなたがこのサイトのページをクリックしたので、お金を振り込んでくれ」というのは無視しておく。「そんなことやった覚えはない」などと返事してはいけない。IPアドレスと自分とを結びつける材料を提供しているようなものである。

また、いろいろな宣伝が送られてくるかもしれないが、「配信を停止するには、ここをクリックしてくれ」というのも、クリックしてはだめ。そのメールがちゃんと届いているということを証明してやるようなものである。無視しておくに限る。

### ウィルス対策

ウィルスの種類

* ワーム

ネットワーク経由でコンピュータに感染する。単体で動作する。「這い回る虫」という意味。

* トロイの木馬

表向きは便利なアプリケーションやゲームに見せかけて、裏で悪事を働くプログラム。単体では自己増殖機能や感染機能をもっていたないため、一見有益なプログラムに偽装し、ユーザーにインストールしてもらうことでパソコン内部に侵入する。侵入に成功されると、個人情報を盗まれたり、コンピュータの設定を変えられたりする。

* スパイウェア

ネットでフリーソフトをインストールするときに、一緒にスパイウェアも入り込んでしまうというもの。

ウィルス感染経路

1. メール

受信した添付ファイルを開いた時に感染する。メール表示しただけで感染するものもある。感染源の約90%と言われている。

1. ホームページ

ホームページ上からダウンロードしたファイルで感染。ウィルス対策ソフトを装って実はウィルスをばらまいているアプリもある。 なかには「ウィルスに感染」と表示するものもあり、「GooglePlay」を装って、不正なアプリをインストールさせる。

1. メディア

USBメモリなどのメディアを介してファイルをやり取りすることで、感染する。多くの場合、USBメモリを差し込んだだけで感染する。

1. ネットワーク

WannaCryは、SMBというWindowsのネットワークを介して広がり、猛威をふるった。

ウィルス感染の症状

1. ウィルスに感染したパソコンでインターネットバンキングにログインしたり、クレジットカード情報を入力したりして、その情報を攻撃者に窃取される。
2. 攻撃者にそのパソコンを乗っ取られ、不正操作されたり、勝手にメール発信されたりする。
3. PCやスマホのファイルを暗号化され、犯人から「金銭を払えば復旧する」と脅迫される。（ランサムウェア）

ウィルス対策ソフトについて

ウィルス対策ソフトをインストールするだけでは、ウィルスは防げない。人間世界のウィルス対策と同じく、新しいパターンのウィルスが日々作られていきているので、それに対応したワクチンプログラムを更新しなくてはならない。

Windows8以降は、Windows Defender というセキュリティソフトが Windows組み込みでついているので、それで充分。

市販のウィルス対策ソフト（マカフィーやノートンなど）と同時利用はできない。もし市販のウィルス対策ソフトをインストールすると、WindowsOSから「Windows Defenderを動作停止するか、市販ウィルス対策ソフトをアンインストールするかせよ」という意味のメッセージが現れる。もしも、市販ウィルス対策ソフトを使用するならば、WindowsDefenderを停止しなくてはならない。

市販のウィルス対策ソフトのほうが優秀かもしれないが、もしそれを使うなら、Windowsの更新処理とかワクチンプログラムの更新など、さまざまなことを自分で管理する必要がある。初心者にはこれは難しいと思われる。

初心者の方には、市販ウィルス対策ソフトはアンインストールして、Windows Defender を使用することを強くおすすめする。Windows Update で自動的に更新処理がおこなわれる。これでよい。

Windows7の場合は、Microsoft Security Essencialをダウンロードし、インストールする。（無料）

WindowsOSの更新処理（Windows Update）とは何か？

Microsoftでは、以下の種類の更新処理をおこなっている。

* OSプログラムに発見された各種バグやセキュリティの脆弱性の欠陥を取り除くための更新プログラムの配布。
* Windowsの機能改善や新しい機能の追加のためのファイル群の配布。
* WindowsDefenderAntiVirus定義更新プログラムの配布。

Windowsの更新処理は**オン**にしておいたほうがよい。更新処理がおこなわれると、再起動がおこなわれることが多い。（Windows Defender AntiVirsの定義プログラムの更新では再起動はおこらない）たまに、再起動のあと不具合が起こってパソコンが動作しなくなることがあるので、更新処理のタイミングをユーザー側で指定できるようになっているはず。

### ウィルスが見つかったら

Windows Defender がウィルスを検出した場合

自動的に隔離される。あるいは隔離・削除などの処理を選ぶことができる。この場合はウィルスは駆除されている。

他のパソコンにUSBメモリを差し込んだときにウィルスが検出された場合

自分のパソコンにUSBメモリを差し込み、データをそのUSBメモリにうつして、それを他のパソコンで利用しようとしたとき、そのパソコンでUSBメモリにウィルスがあることが発見された場合のこと。

自分のパソコンにウィルス対策ソフトをインストールしていないか、もしくは、インストールしていてもワクチンプログラムの更新をおこなっていない場合、ウィルスに感染することが多い。そして、その場合は感染していても気づかないことが多い。他のパソコンにUSBメモリを差し込んで初めて気づくことになる。

とりあえず、ウィルス対策ソフトをインストールして駆除したとしても、ウィルスを完全に駆除はできないだろう。

WindowsのOSを再インストール（ハードディスクも初期化）する必要がある。（リカバリ処理）

この場合、データも全部削除されてしまうので、必要なデータは、外付けハードディスクかUSBメモリに保存しなくてはならない。（ウィルスも一緒に保存することになる）

その上でOSを再インストールする。いろいろなアプリも再インストールしなくてはならない。

そして、データを保存しておいた外付けハードディスクあるいはUSBメモリをウィルスチェックする。ウィルスを隔離もしくは、削除してからパソコン本体に戻さなくてはならない。

### インターネット利用時の注意点

* 掲示板の利用 ：不特定多数が意見する場。

テーマに沿った内容を書き込み相手を不愉快にさせる行動は避ける。

誹謗中傷するような内容を書き込んだりすると犯罪になる可能性あり。

* 不要なファイルのダウンロード：

悪意のあるホームページからフリーソフトやファイルが自動でダウンロードされる時があるので注意。

* オンラインショッピング詐欺：

代金支払いしたのに商品が届かない、掲載されていた商品と違う等の被害。

店舗住所や電話・FAX番号 メールアドレス等の連絡先の記載があるか実在するかどうかの確認が必要。

* 個人情報の入力

個人情報を入力する際はSSL（入力情報を暗号化するしくみ）に対応した信頼のあるホームページであるかどうか確認した上で。

* 迷惑メール

チェーンメール：不幸の手紙のメール版。内容の善し悪しに関わらず削除する。

* 広告宣伝メール

悪質な業者もあるので返信はしない。有効なメールアドレスだと思われ次々に迷惑メールが送られるので注意する。

* フィッシング詐欺

悪意のある第3者が有名企業を装い、ニセのWEBサイトへ誘い込んで暗証番号やクレジット情報などの個人情報を盗むこと。

### Webサイトを設置運営する上でのセキュリティ対策

今までは個人がユーザとしてインターネットを利用する上での諸注意であるが、Webサイトを制作したり、Webアプリを開発する者として知っておかなければならない事柄もある。以下はその一端である。

Webサイト・Webアプリケーションへの攻撃

* Dos攻撃（Denial of Service Attack）

サーバやネットワーク機器に大量のパケットやリクエストを送信することで過負荷をかけ、サービスが提供できない状況に追い込む攻撃。WebサーバへのDos攻撃では、ブラウザの「更新」ボタンや「F5」ボタンを連打する（通称F5アタック）単純なものから、乗っ取った複数の端末を踏み台にして集中攻撃する（DDoS攻撃）大規模なものもある。

* クロスサイトスクリプティング

電子掲示板やお問い合わせページのフォームなどにスクリプトのコードを含んだ文字列を送信し、その文字列を表示したブラウザにスクリプトを実行させることで、XSSとも表記される。ほとんどがWebアプリケーション作成時の初歩的なミスによるセキュリティホールを利用する。

* SQLインジェクション

Webサイトの入力フォームなどに不正な文字列（SQL文）を入力することで、Webサーバの裏にあるデータベースを不正に操作する攻撃。この攻撃を受けると、データベース内の情報の漏洩やファイルの改ざんなどがおこなわれる。

Webセキュリティ対策（サーバ設置）

セキュリティ対策は、それぞれに一長一短がある。大切なことは複数の対策を導入し、それぞれの対策の長所を生かして欠点をカバーすることである。

* SSL

インターネット上で送受信される情報を暗号化する仕組みの1つ。

一般的におこなわれるインターネットやLANといったネットワークでは、どのような通信が流れているかを見ることができる。この操作をパケットキャプチャという。この通信を暗号化することで、パケットキャプチャでも通信内容を確認することができなくなる。

WebブラウザのURL欄に「https://〜」となっていると、ブラウザとWebサーバ間でSSLによる暗号化通信がおこなわれている。

WebサイトをSSL対応にするには、そのWebサイトを設置しているレンタル・サーバがSSLを導入している必要がある。SSL対応は有料オプションであることが多い。

* ファイアウォール

一部のパソコンやサーバを外部から見えるようにし、その他のパソコンは外部からのアクセスを受け付けないようにすること。サーバを設置する場合、そのサーバと他のパソコンを切り離すように設定する。そのことで、ほかのパソコンを守ることができる。また、1台のパソコンの中でもソフトウェアにファイアウォールを設定し、外部との通信を制御することができる。ただ、ファイアウォールでは「許可された通信」を制御することはできないので、他の対策と併用する必要がある。

* パケットフィルタリング

設定したルールにもとづいて外部から内部の各パソコン・各ポートへの通信を許可したり、不許可にしたりして、通信を制御すること。ネットワークの出入り口にはルータが設置されているので、そのルータにパケットフィルタリングの設定をすることになる。

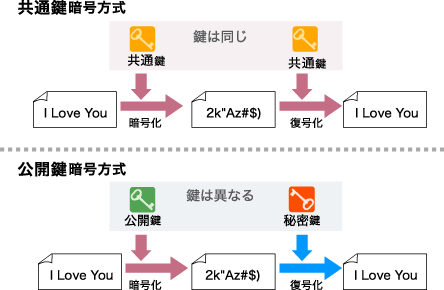
Webセキュリティ対策（暗号化技術）

* 共通鍵暗号化方式

暗号化とは、元の文書やデータ（平文）を特定の暗号化手法と鍵を使って、第3者からは意味のないデータに変えてしまうことをいう。逆に、暗号化したデータを元の読むことができるデータに変換することを復号化と呼ぶ。そして、暗号化と復号化を同じ鍵でおこなう方式を「共通鍵暗号化方式」と呼ぶ。

* 公開鍵暗号化方式

公開鍵暗号化方式は、暗号化と復号化で全く異なる２つの鍵（公開鍵と秘密鍵）を使用する。ただし、公開鍵と秘密鍵は、一対のキーペアとして生成され、片方の鍵で暗号化したデータは、キーペアとなるもう一つの鍵でしか復号化することはできない。



* メッセージ・ダイジェスト

改ざんの有無の確認として、元データのコピーと送信後の内容を比較すれば改ざんされたかどうかはすぐにわかる。この原理は、ハッシュ関数と呼ばれる計算式を使って数値を出力し、数値どうしを比較する仕組みで改ざんを証明する。この仕組みはメッセージ・ダイジェストと呼ばれている。また、ハッシュ関数で計算された数値をダイジェストと呼び、ダイジェストからは元のデータを求めることができない構造になっている。

（例）

たとえば、「山田太郎」と記述したファイルを「a.txt」として保存する。それを「コマンドプロンプト」から、以下のように入力する。

> certutil -hashfile a.txt

画面には英数字が出力されたはずである。これがダイジェストである。



今度は、a.txtの内容を少し変えてみよう。「山口太郎」とでもしてみる。その上でまた、さきほどのコマンドを実行してみよう。まったく異なったダイジェストが出力されたはずである。

今度は、もとの「山田太郎」にもどしてみよう。そして、コマンドを実行すると、最初のダイジェストとまったく同じはずである。

このダイジェストは、記述される文字数には関係しない。一文字でも、3000字でも、出力されるダイジェストの桁数は同じである。

* 電子署名（デジタル署名）

電子署名（デジタル署名）とは、公開鍵暗号化方式とメッセージ・ダイジェストによる本人確認の内容を証明するもので、ハッシュ関数の計算結果（ダイジェスト）を秘密鍵で暗号化したものになる。受信者がこの電子署名を公開鍵で復号化できるということは、それと対応するキーペアの秘密鍵で暗号化されていることを意味する。つまり、秘密鍵を持っている本人が送信したデータであるということが証明される。また、同時にハッシュ関数の計算結果（ダイジェスト）の比較が同一であれば、その署名が正しいことを証明し、改ざんされていないことまで保証することができる。

* 電子証明書

電子証明書とは、簡単にいうと送信者が確実に存在することを保証してくれるものである。その仕組みは、信頼できる第三者機関（認証局=CA:Certificate Authority）が公開鍵に対して電子署名をおこなうことにより、公開鍵の所有者の身元を保障している。認証局には、米国のベリサイン社などがある。電子証明書の中身は、認証を依頼した本人の公開鍵、暗号化手法や登録者情報などが記載されている。

* SSL

HTTP用のセキュア・プロトコルで、WebクライアントとWebサーバー間の通信における認証と暗号化を実現している。その仕組みは公開鍵暗号化方式と共通鍵暗号化方式を組み合わせである。また、その公開鍵は電子証明書によってその身元が保証されている。

公開鍵暗号化方式によって共通鍵が生成され、その共通鍵によって通信が暗号化される。互いの通信では共通鍵暗号化方式のほうが速度が速いためである。

* アップロードの暗号化

サイトの更新には通常ftpを使用するが、このポートを狙って不正アクセスされる可能性がある。したがって、ファイルのアップロードにはsshという暗号化通信の仕組みを用いたsftpというプロトコルを使用する。

不正アクセス禁止法

インターネットを使ったハイテク犯罪、コンピュータ犯罪、ネットワークをめぐる犯罪を禁止する法律で、

他人のユーザIDやパスワードを使って、本来自分が利用する権限を持っていないコンピュータを不正に使用する行為や、OSやアプリケーションソフトなどに存在するセキュリティ上の弱点を攻撃してコンピュータを不正利用したり、保存されているデータやプログラムを改ざんしたり、コンピュータを利用不能な状態に追い込んだりする行為を禁じています。

@ 2018 Seiichi Nukayama