インターネットリテラシー

Internet Literacy

原　仁志*
Hitoshi HARA

要　旨

インターネットが一般家庭に普及して久しい。近年ではスマートフォンやタブレットの普及により、さらにインターネットの利用が進んでいる。これまでパソコンが苦手だった人々も簡単にインターネットを利用できるようになり、また利用者の低年齢化も進んでいる。これにより様々な問題も浮上している。そこで、一般的にインターネットを利用する場合に考えられる様々な事象や解決法について、インターネットリテラシーと定義されるインターネットを利用する際に必要な知識を考える。また教育の場面ではどのようなことを中心に指導するかということについても考察する。

キーワード：インターネット，リテラシー，IT，電子メール，SNS

１．はじめに

まず、全ての基本となるインターネットについて説明する。

次に、その上で利用できるサービスである「ウェブサイト」「電子メール」「チャット」「SNS」「電子掲示板」「オンラインゲーム」についての仕組みや脅威、対策などについて説明する。また、コンピュータウイルス対策についても考える。

最後に、各サービスにおける問題点を踏まえた上で、教育においてどのようなことについて指導すべきかを考察する。

２．インターネット

まず、インターネットとはどのようなものなのかを説明する。

おおまかな仕組みとしては企業内、学校内、家庭内など比較的小規模なネットワークを相互に接続して世界規模の巨大なネットワークにしたものである（図 1　ネットワークのイメージ）。接続の方法はどのような形態でも可能で、光ファイバ、電話回線、無線通信などが主に利用されている。

＊本学准教授、情報教育（Associate Professor, Information Education）

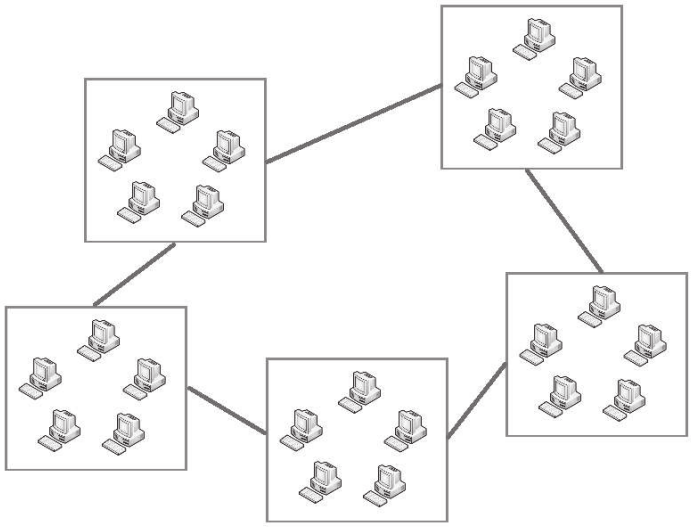

図 1　ネットワークのイメージ

(1)インターネットの歴史

1967 年にアメリカで ARPA[1] により運用開始した ARPANET[2] がインターネットの始まりであり、軍事利用が目的であった。その後、利用規約により ARPANET を利用できない組織などを接続する目的で 1981 年に CSNET が運用開始された。日本においては 1984 年に学術組織を中心とした JUNET が運用開始され、1986 年に CSNET と接続して初めて海外と接続された。1989 年に日本のドメイン名が.JP になって本格的なインターネットとしての運用が始まった。

1990 年代に入ると商用 ISP[3] が開設されて個人がインターネットに接続できるようになった。また、インターネットに接続できる機能が提供された Windows95 が発売されてインターネットの普及が進むことになった[4]。

2000 年代に入り、IT 革命においてネットワークインフラが急速に整備され、ブロードバンド化されたことによりインターネット普及に拍車がかかる。

現在では PC[5] のみならず携帯電話やスマートフォン、タブレットなど様々な機器で家庭内だけでなく屋外でもインターネットに常時接続できる環境が整った。

表 1　インターネットの歴史にインターネットの歴史における主な出来事を示す。

表 1　インターネットの歴史

年	出来事
1967 年	ARPANET 運用開始
1981 年	CSNET 運用開始
1983 年	DNS の誕生
1984 年	日本で JUNET 運用開始
1985 年	初のコンピュータウイルス誕生
1986 年	JUNET と CSNET が接続開始
1989 年	日本のドメイン名が.JP へ移行
1992 年	商用 ISP サービス開始
1995 年	Windows95 発売

(2) インターネットで利用できるサービス

インターネットでは何ができるのかを説明する。プロトコルとしてのインターネット上のサービスは WWW[6] で利用される HTTP、チャット、ファイル転送、ストリーミングなどがあるが、実際に我々が利用するサービスとしてはウェブサイト（ホームページ）、電子メール、チャット、SNS、電子掲示板（BBS[7]）、オンラインゲームなどがある。

3．ウェブサイト

ホームページという用語は本来、ウェブサイトにアクセスして最初に表示されるページのことであり、現在一般的に言われているホームページは正確にはウェブサイトと呼ぶ。既にホームページという用語はウェブサイトとして一般に認識されていると思われるが、誤用である。

(1) ウェブサイトの仕組み

まず表示したい文字・画像・動画・音声などの情報を HTML[8] によりレイアウトしサーバに置く。その後クライアント PC からサーバへアクセスしてデータを受信し、レンダリング[9] を行う（図 2　ウェブサイトの仕組み）。クライアント PC にレンダリングを任せているため、利用しているブラウザによって表示結果が異なることがある。

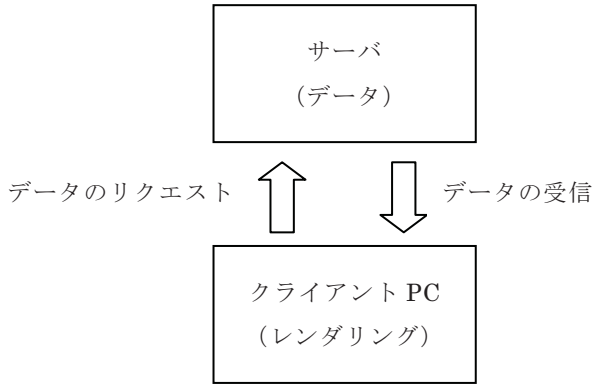

図 2　ウェブサイトの仕組み

(2) コンピュータウイルスの混入

ウェブサイト上に意図せずしてコンピュータウイルスが仕込まれていることがある。これはウェブサイトの改ざんによるものや掲示板へのスクリプト[10] 埋め込みなどがある。改ざんの方法はいくつかあるが、いずれもユーザ（利用者）側で対策できることはコンピュータウイルス対策ソフトを導入しておく他は何もなく、サーバ側（管理者）による対策が必要となる。

改ざんの手法にはどのようなものがあるか説明する。

1) ウェブサーバの脆弱性を利用したウェブサイト改ざん

ウェブサーバを提供するソフトウェアのバージョンが古いことにより、脆弱性（ぜいじゃくせい）を悪用されてウェブサイトを改ざんされることがある。また、XSS[11] と呼ばれる脆弱性を悪用されることも多い。

対策としては、ウェブサーバ全体のソフトウェアを常に最新のものに更新することが必要となる。また、設定に不備がないか確認することも重要である。特にウェブサーバとしては Apache や IIS[12] などが有名であるが、これらの設定を間違えてしまうと思わぬ抜け穴となってしまうことがあるので、十分注意しておく必要がある。

2) コンピュータウイルスによるパスワード漏えいからのウェブサイト改ざん

管理用 PC がコンピュータウイルスに感染し、そこからパスワードが漏えいすることがありうる。2009 年頃から被害が発生し始めた Gumblar（ガンブラー）ウイルスによるものが有名である。Gumblar の動作は次のようなものである。

① 攻撃者が正規のウェブサイトを改ざん
② 正規のウェブサイトへのアクセスを、用意された不正なウェブサイトへ転送
③ 不正なウェブサイトへアクセスした PC へコンピュータウイルスを送り込む

このことからわかるように、改ざんしたウェブサイト自体にコンピュータウイルスが仕込まれるわけではなく、単に不正なウェブサイトへ転送するだけである。そして送り込まれていたコンピュータウイルスは、ウェブサイトを更新するのに必要な情報（FTP[13] アカウント情報）が盗まれるというものであった。この時にはコンピュータウイルス自体が感染を広めるわけではなかったので（正確にはトロイの木馬に分類される）、不正なウェブサイトが閉鎖されたことにより事態は収束に向かっていった。

しかしこの後、亜種のコンピュータウイルスが登場する。不正なウェブサイトへ誘導するのではなく、改ざんされたウェブサイト自体にコンピュータウイルスが仕込まれていた。このコンピュータウイルスは感染するタイプのもので、二次被害、三次被害と拡大した。これからも同様のコンピュータウイルスが出現する可能性は否定できない。

対策としては、管理用 PC にもコンピュータウイルス対策ソフトを導入することはもちろんのこと、可能ならば管理する目的以外に管理用 PC を利用しないことが必要となる。通常の業務や個人的な用途に利用しないことでウイルス感染のリスクを極力減らすのである。

3) 脆弱な管理者パスワードによるウェブサイト改ざん

容易に推定できるようなパスワードを利用している場合、それを悪用されてウェブサイトを改ざんされてしまう。推定しやすいパスワードはブルートフォース攻撃[14] などにより解析される可能性が高い。対策としては、パスワードを推定しやすいものにしないことが大前提となる。推定しにくいパスワードについては後述する。

また、遠隔操作とファイル転送の仕組みに FTP ではなく SSH[15] の公開鍵認証を利用することも必要である。公開鍵認証を利用するには公開鍵と秘密鍵の鍵ペアが必要となる。これはサーバに公開鍵、管理用 PC に秘密鍵を置き、通信用の共通鍵の暗号化と復号に利用するものである。もちろんペアでない鍵を使おうとしても復号できないので、管理用 PC の秘密鍵が漏えいしない限り安全となる。

4) コンピュータウイルスの感染手法

ウェブサイトが改ざんされ、実際にクライアント PC がコンピュータウイルスに感染する方法としてはソフトウェアの既知の脆弱性を利用する。主に利用されるソフトウェアには次のようなものがある。

① Microsoft Windows
② Adobe Reader
③ Adobe Flash Player
④ Java Runtime
⑤ QuickTime

これらのソフトウェアは定期的にアップデートがなされていることからわかる通り、最新の状態にしていても未知の脆弱性が存在すると考えられる。その脆弱性を利用してコンピュータウイルスに感染するのである。

対策としては、アップデートが提供された場合にはすぐに適用することが重要となる。また、ブラウザの JavaScript を無効にして必要な時のみ有効にすること、Adobe Reader の Acrobat JavaScript を無効にすることなども必要となる。JavaScript はクライアント側で実行するスクリプトのため、コンピュータウイルスに感染させるための足がかりにされることがある。コンピュータウイルス対策ソフトを導入しておけば感染のリスクをさらに下げることができる。

大手ウェブサイトが改ざんされることもあるが、いわゆる怪しいウェブサイトにおいて改ざんや掲示板の書き込み等でコンピュータウイルスに感染する可能性のほうが高いため、こういったサイトを訪れないという対策も有効であると考えられる。

4．電子メール

電子メールは E-mail、単にメールとも呼ばれ、文字情報（メッセージ）を目的の相手へ送信する仕組みである。電話と違い、相手の都合によらず一方的にメッセージを送ることができるのが特徴である。システム的には日本における郵便の私書箱に近い。目的の相手を指定するにはメールアドレスを使用する。

電子メールは送受信に通信料金以外に料金はかからないため spam と呼ばれる迷惑メールが送られることが非常に多い。総務省の統計によると、迷惑メールの数は 2009 年 1 月から 2014 年 6 月現在までで全メール数のうち 6〜7 割を占めている。

(1) フィッシング詐欺

フィッシング[16] 詐欺とは、銀行や有名企業などを装ってパスワード変更を促すなどのメールを送り、偽のサイトへ誘導して、個人情報や ID、パスワード、クレジットカード番号などを取得することを目的とする。もちろん取得された個人情報は売買されたり、ID とパスワードで不正アクセスが行われたり、クレジットカードで不正な買い物をされたりする。

フィッシング詐欺を防ぐには、その仕組みと目的を知っておく必要がある。特にメールの偽装については知らなければ防ぐことは難しい。

(2) 架空請求詐欺

有料サイトの会費や、通信料などの名目で振り込みを請求されるものであるが、実際には利用していないものなので架空請求詐欺と呼ばれる。架空請求詐欺メールに共通していることは次のようなものである。

① 比較的少額である（2〜3 万円程度）
② 支払期日が非常に近い
③ 振り込まない場合は裁判を起こすと書いてある

比較的少額の請求であり、思い当たるようなサイトを見たことがあるという記憶と裁判という単語を見て、支払ってしまうことが多いようである。しかし実際に利用していないものに対して少額とはいえお金を払ってはならない。

架空請求詐欺で重要なのは、メールに対して返信したり、メール内のリンクをクリックしたりするような反応をしないことである。どのようなことに対しても無視することがベストな対応となる。もし反応してしまうと相手にいわゆるカモ（この場合は架空請求でお金をとれる対象）として登録され、場合によってはカモリストに載ってしまい、他の業者からも同様のメールが来ることになる。基本的に無視という対応で問題ないが、どうしても不安な場合は警察に届け出るべきであろう。

(3) コンピュータウイルス入り添付ファイル

コンピュータウイルスに感染させることを目的としたメールである。感染させた後、PC に保存されたデータを消去したり盗んだりすることが真の狙いである。メールにはファイルを添付して相手に送る機能があるが、これを悪用する。コンピュータウイルスに感染させたファイルを添付して送るのである。添付されたファイルは Word ファイルや Excel ファイル、実行ファイル、圧縮ファイル等であるが、画像ファイル（音楽ファイル、動画ファイル）に見せかけていることもある。

① Word ファイルや Excel ファイルの場合
　マクロウイルスに感染している。開かなければ問題はないが、Word や Excel の設定でデフォルトを「マクロを実行しない」にしておくべきである。
② 実行ファイル形式になっている場合

実行すると感染してしまうので、絶対に開いてはならない。

③ 圧縮ファイル

展開しただけで感染することはないが、展開後のファイルはコンピュータウイルスに感染しているので開いてはならない。

④ 画像ファイル、音楽ファイル、動画ファイル

閲覧・視聴してもコンピュータウイルスに感染することはない。例えば画像ファイルに見せかける場合、次のようなファイル名になっていることがある。

「FavoritePicture.jpg .exe」

このようになっていると表示環境によっては空白の後についた「.exe」に気づかないことがあり、結果的に画像ファイルと思い込んだ実行ファイルを開いてしまうことになり、コンピュータウイルスに感染してしまう。ファイル名をよく観察することが重要である。

(4) 対策

メールを利用する際に必要だと思われる対策・対処について考える。

① 知らない送信元からのメールは読まずに削除する

コンピュータウイルス入りのファイルが添付されたメールはほとんどが spam として送られてくる。そのため送信元に心当たりがないことが多い。そこで知らない送信元からのメールは読まずに削除するべきである。送信元が偽装されていて、知人からのメールに見せかけていることもある。

② メール内のリンクをむやみにクリックしない

たとえ知人から送られてきたメールであっても、むやみにメール内のリンクをクリックして開かないことも重要である。知人から送られてきたように見せかけた spam の可能性もある。また、HTML メールで送られてきた場合は、画面上に表示されたアドレスと、実際にジャンプするアドレスが違うことがある。正しいジャンプ先はウィンドウの下に表示されることが多いので、それをチェックしておけば間違いないが、知らなければわからないので、基本はクリックしないことが重要である。

5．チャット

チャットとは文字のみで会話を行うサービスであるが、インターネット上では主に 2 種類ある。ひとつは IRC[17] である。これはインターネットのプロトコルとして定められてい

るもので、特定のサーバへ接続してチャットを行う。もうひとつはウェブサイト上に設置されたチャットで、リアルタイムに数秒から数十秒間隔で更新される掲示板のような仕組みになっているものである。いずれも複数のユーザがリアルタイムに会話に参加し、文字のみで会話するということは変わらない。

文字のみの会話となるので、それを理解した上で利用しなければならない。実際の会話と比較すると、テンポや抑揚、表情、ジェスチャーなどで感情を伝えることができないのが最大の違いである。このため相手に意図が正しく伝わらずに、言い争いに発展することもある。後述するネチケットとも関連する部分があるが、基本的には「相手に正しく伝わっていないかもしれない」という気持ちで利用する必要があると考えられる。

６．SNS

SNS[18] は Twitter や Facebook、LINE、mixi などのサービスを指す。コミュニティとして機能する会員制のサービスとして定義される。主に登録会員間においてメッセージのやりとりを行うことを目的としたものであることが多い。特に Twitter や LINE などは短いメッセージでやりとりをする。

特徴としては会員制のサービスであることがまずあげられる。匿名かそうでないかはサービスによって異なるが、いずれにしても会員登録をした上で登録ユーザとしてメッセージを投稿する。Facebook と mixi はブログに近いが、LINE はチャットに近く、Twitter は情報拡散が非常に速いショートメッセージのミニブログに近い。

SNS を利用する場合の注意として、まずはここ数年 Twitter を中心としてたびたび不祥事が起きていることについて述べる。

- アイスクリームの販売ケースに人が寝そべった写真を投稿した
- 食洗機の中を人が通る写真を投稿した
- 冷蔵庫の中に人が入っている写真を投稿した
- 飲酒状態で運転したことを投稿した

ここにあげたのは一例で、昨年から今年にかけて急増している。ほとんどの件で次のような結果に至っている。

- ツイッターアカウントに批判殺到（炎上）
- ツイッターアカウント削除
- 退学・解雇

いずれの件も常識的にしてはいけないこととわかるはずであるが、ここで注目したいのは写真を撮ったのは友人知人だということである。つまり写っている本人はわかっていて写真を撮ってもらい、自身で Twitter に投稿している。そのような写真を投稿したらどのような事態になるか想像できていないと考えられる。

このような様々な不祥事が起きているのは次のような Twitter の誤解や自己顕示欲に原因があるのではないかと考えられる。

- 仲間内だけしか読めないのではないかという誤解
  Twitter ではデフォルトで誰でもツイート（投稿）を読めるようになっているが、これを誤解して自分のアカウントを知っている人だけが読めると思ってしまったのではないかということである。
- 自分の投稿したツイートにもっと注目して欲しい、フォロワーを増やしたい
  日本の Twitter アクティブユーザは 2000 万人以上いると言われているが、その中で平凡なツイートをしただけではもはや注目されない。そこで他人と違うツイートという意味で方向性を誤り、問題のある写真を投稿しているのではないだろうか。

また、LINE の連絡先を別の掲示板等を通じて交換して出会い系のような利用が行われ、それが発端となって事件に発展した例もある。LINE のアカウントを乗っ取り、iTunes カードなどのプリペイドカード代理購入をさせる詐欺も発生している。

こういったことから気をつけなければならないことは、現実社会の中でしてはならない行動は Twitter を含めた SNS だけでなくインターネット上でも同じで、してはならないということである。また、その投稿によってどのような反応・展開が起こるかある程度予想しておくべきである。さらに知らない人からのメッセージに注意することはもちろん、知り合いでも普段と違う発言をしているような場合はよく観察しておくことが重要である。

なお、Facebook については他の SNS と違い実名と設定したプロフィールが公開されるという特徴がある。これはプロフィールに正確な情報を登録することによる「つながり」にある。例えばプロフィールの出身高校が一致する人を検索することができ、そこから同窓生を見つけることができる。もちろんこの場合は同窓生も Facebook へ登録していなければ見つけられない。また、「つながり」でのビジネス活用も行われている。

Facebook では個人情報の公開を自分から認めることで登録しているので、それを十分理解した上で利用する必要がある。しかし全ての情報をすべてのユーザに公開する必要はなく、必要な人にだけ必要な情報を公開する設定にすることが重要になる。公開制限でプロフィールとして登録した情報などを誰に対して公開するのかを確認しておくのである。

Facebook だけでなく他の SNS や Web サービスにおいても同様の公開制限・公開設定が

ある場合は、確認して不要な情報を公開しないように設定しておく。そうすれば思わぬところからの情報漏えいを防ぐことができる。

７．電子掲示板（BBS）

かつて利用されていたパソコン通信において運用されていた電子会議室やインターネットの Netnews サービスを使いやすくしたものと考えられる。ウェブサイト上で運営され、特定のテーマに関連する話題についてのメッセージを不特定のユーザが自由に書き込み、閲覧が可能なシステムである。ウェブサイトを閲覧するのと同じ要領なので簡単に利用できるのが特徴である。Q&A サイトの運営などにもよく利用されている。

注意点は後述のネチケットに関連した部分が多い。チャットと同様、文字のみの会話となるので注意点はほぼ同じであるが、リアルタイムでない部分を考慮しておかなければならない。

ほとんどの掲示板は管理者が存在し、書き込まれたメッセージを監視して問題ないか確認し、必要があればメッセージを削除する。あるいは管理者として議論が正しい方向に進むように促すような、運営に関わる業務を行う。

Q&A サイトのような電子掲示板ではユーザ同士で質問・回答をする。そのため、正しい回答が得られるとは限らず、情報の信頼性は自分で判断する必要がある。

８．オンラインゲーム

オンラインゲームとは、インターネット（ネットワーク）を介して多人数が同時にプレイするゲームの総称である。MMORPG[19]、MORPG[20]、FPS[21]、ソーシャルゲームなど様々な形態がある。いずれも多人数がインターネットを通して同時にプレイするゲーム部分が基本であるが、コミュニケーションをとるためにゲーム内チャットやメールの機能が搭載されていることも多い。そのため前述のチャットやメールで注意すべきことが適用される。チャットだけでなく、ゲーム内での行動そのものが他人に迷惑をかけることになる可能性もあるので、画面上に表示されているキャラクタは人間が操っているという意識が必要である。それ以外では、後述のネチケットに関連する。また、個々のゲーム内でルールやマナー等も定められていることが多いので、それに沿って行動することが円滑なコミュニケーションに繋がる。

９．コンピュータウイルス対策

コンピュータウイルス対策として最初に行うことは、コンピュータウイルス対策ソフトを導入することである。コンピュータウイルス対策ソフトは有料、無料で様々な種類があるが、どれでも良いのでまずは導入することが重要となる。一般的にはアンチウイルスと

呼ばれるコンピュータウイルスを検出・ブロックするソフトと、ファイアウォールと呼ばれる通信を監視して不正なものがないか調べるソフトがセットになっており、この 2 つを導入することが必須である。

アンチウイルスではパターンファイルと呼ばれる定期更新されるファイルによりパターン照合を行い、コンピュータウイルスの検出を行う。また最近ではヒューリスティック検出と呼ばれる、パターン照合ではなくコンピュータウイルスの特徴的な動作を検出する方法も使われる。これは未知のコンピュータウイルスやゼロデイ攻撃[22)] を検出するために使われる方法である。パターン照合とヒューリスティック検出は共に利用される。

また、コンピュータウイルスの感染経路には様々なものがある。

- ウェブサイト（ダウンロード）
  いわゆる怪しいウェブサイトを閲覧すると、プラグインソフトの脆弱性を狙ってコンピュータウイルスに感染することがある。また、配布されているソフトをダウンロードし、実行することで感染することもある。先に述べたように、大手ウェブサイトでも改ざんによって感染することがあるので注意が必要である。
- 電子メール
  電子メールの添付ファイルによる感染も多い。対策は電子メールの項目で述べたとおりである。
- USB メモリ、SD カードなど
  Windows の自動実行機能により感染してしまうことがある。Windows 7 以降では CD/DVD ドライブのみ有効になっているので問題ないが、Windows Vista 以前ではこれを無効化しておかないと、USB メモリや SD カードから感染する可能性がある。
- ファイル共有ソフト
  不特定多数のユーザ同士で欲しいファイルを交換する仕組みである。ファイルの偽装などによって感染してしまう可能性がある。ファイル共有ソフトで流通するソフトやデータ自体、著作権的にグレーもしくは違法なものが多く、利用しないのが基本である。

１０．指導ポイントの考察

ここまで述べてきたインターネット上の様々な問題を元に、教育上指導すべきポイントを考察する。

(1) 情報の信頼性

インターネット上には無数の情報が散らばっている。その中から自分の欲しい情報を探

し出すには Yahoo!や Google などの検索エンジンを利用するが、検索結果に表示されたリンクからウェブサイトを表示し、その中に書いてある情報が全て正しいというわけではない。その情報が信用できるかどうかということは自分で判断するしかない。

判断材料としては、情報源が明確にされているかということがあげられる。例えば新製品が発売されるという情報を目にした時、情報源としてメーカーのサイトが参照されているかということを確かめる。あるいは情報源として大手ニュースサイトや新聞社のサイトなど、信頼できるサイトが参照されていればその情報を信用することができる。

SNS の投稿でも同じである。公式アカウントが投稿したものであれば信頼できるが、そうでなければ信頼性は低くなる。

(2) ネチケット

ネチケットとはネットワークとエチケットを組み合わせた造語であり、ネットワーク（インターネット）を利用する上で必要なエチケットという意味である。最近はネチケットという言葉自体あまり聞かなくなったが、その考え方については現在でも必要な知識なので指導する必要があると考えられる。

ネチケットには次のようなものがある。

A) 他人への気遣い

- ネットワークの先に人間がいることを認識する
  目の前にいるわけではないので錯覚してしまうこともあるが、メールやチャット、掲示板ではメッセージを書いた人がいる。決してコンピュータなどの機械ではない。それを意識して対応することが重要である。
- 機種依存文字や半角カナの問題
  最近のサーバやクライアント PC で問題になることはほとんどないと思われるが、丸囲い数字や「(株)」を 1 文字で表した文字等は機種依存文字と呼ばれ、特定の環境のみで正しく表示される文字である。インターネット上では相手がどのような環境なのかわからないので、これらの文字を使わないようにすることが求められる。
- 適度に行を開けて文章を書く
  電子メールやウェブサイト上で長文を連続して記述すると非常に読みにくくなる。適度に空行を挟むことにより読みやすくなるので、これを心がける。また、電子メールの場合は同様の理由により全角 40 文字前後で改行することもよく行われる。
- 調べればすぐわかることを質問しない
  インターネットの検索サイトを利用して調べればすぐにわかることを、掲示板や電子メール、SNS 等で聞く人を俗に「教えて君」と呼び、嫌われている。他人の時間や知

識を無駄に消費することに繋がるからである。まずは自分で調べ、それでわからなければ聞くようにすべきである。回答者や周囲もそのように促すのが良い対応と言える。

- コンピュータウイルス対策をせずにネットワークへ繋いではならない

コンピュータウイルス対策ソフトを導入せずにPCをネットワークに繋ぐと、コンピュータウイルスをネットワーク上にばら撒くことになってしまう。また、サポート期限の切れたOSやソフトウェアを利用することも危険である。例えばWindows XPやOffice 2003は2014年4月9日にサポートが終了し、これ以降に発見された脆弱性への修正は行われない。これから修正されることのない脆弱性が見つかった場合、それは必ず攻撃者に狙われる。そのため非常に危険な状態となるので、すぐに利用を中止すべきである。対応としては新しいPCへ買い換えるか、OSまたはソフトウェアを更新する必要がある。

B) 荒らしとその対応

インターネット上の掲示板やSNSなどには「荒らし」と呼ばれる他人を煽る行為がある。自分から「荒らし」をしないということはもちろんのこと、もし「荒らし」を見たり絡まれたりしたとしても適切な対処が必要となる。最も重要なのは反応しないことである。「荒らし」の目的は相手が反応することなので、反応しないことにより「荒らし」の興味を削ぐことができる。また、悪質なものに対してはその掲示板などの管理者へ報告することも重要である。

また、自分自身が気づかないうちに「荒らし」になっている可能性もある。そうならないようにメッセージを書き込む際には注意すべきである。

C) 炎上

SNSやブログ等で炎上と呼ばれるものが起きることがある。これは不適切な発言や書き込みをしたものに対して大量の批判や罵詈雑言などの反応が返ってくることである。そもそも炎上を起こすと言うことは問題となる発言や書き込みを行っているので、そのようなことがないように注意すべきである。しかし炎上してしまった場合は非を認め、素早い対応が求められる。

D) メッセージを書き込む際の注意

メールの送信、SNSやブログ、掲示板へ書き込む際には、書いたメッセージを一度読み直すと良い。読み直すことによって誤字・脱字の発見はもとより、そもそもそのメッセージを書き込むべきなのかということも考え直すことができる。不要なメッセージをわざわざ書き込むことは、ネットワーク上に余計なトラフィックを増やし、様々なトラブルの元になりかねない。

E) 他人のメールアドレスの扱い

他人のメールアドレスについては、勝手に公開しないことが基本となる。特にビジネ

スで活用する場合は個人のメールアドレスを公開してはならない。

ミスを犯しやすいケースとしては、複数の人へ同時に電子メールを送る際の TO、CC、BCC フィールドの使い方である。実際の動作としては TO も CC も BCC もほとんど同じで複数の人に同時にメールを送ることができるが、運用する際には違いがあることを理解する必要がある。TO は電子メールを送りたい宛先を書き、CC や BCC には「TO の人に送ったメールを参考程度に見ておいてください」というニュアンスの違いがある。そして CC と BCC は電子メールを送った全員にメールアドレスが公開されるのか（CC）、公開されないのか（BCC）という違いである。簡易メールマガジンのように利用する場合は BCC を利用して電子メールを送らないと、メールアドレス一覧が公開されてしまうのである。

(3) パスワードの管理

パスワードの管理は非常に難しいが重要な問題である。よくあるパスワードとしては次のようなものがある。

① password、login など
② 電話番号
③ 車のナンバー
④ 01234 などの連番
⑤ 11111 などの同じ数字の連続
⑥ 辞書に載っている英単語

これらのパスワードは容易に推定でき、パスワードとしての意味がないので、絶対に設定してはならない。場合によっては脆弱なパスワードを設定しようとするとエラーとなるシステムもある。

パスワードの運用としては全てのサイトで異なり、8 文字以上のランダムな文字列を使うことが理想的である。文字列には「アルファベット（大文字・小文字）」「数字」「記号」が含まれていることが望ましい。特に「記号」が含まれているとブルートフォース攻撃でも解析するのが難しくなる。さらにパスワードをメモに残さず、記憶しておくことが望ましい。しかしこれらを実践し、多くのサイトを対象に運用するのは厳しい。

どうしても覚えられないパスワードの場合は、自分しか見ないメモ帳に記録しておく方法や、スマートフォンのカメラでパスワードを撮影しておくという方法もある。

さらにパスワードは定期的に変更すべきという意見が多いが、これに関してはあまり意味が無いという意見もある。理由としては、攻撃者がブルートフォース攻撃を仕掛けてき

た場合は変更しても意味がないことがあげられる。これに対して定期的に変更した場合、パスワードを覚え直さなければならない、覚えられない場合はメモし直すなどの対応が必要となり手間が発生する。結果としてディスプレイ横に付箋でパスワードを貼り付け、それを定期的に交換すると言うことになりかねないリスクが存在する。ただし、不正アクセスが発覚した場合には即座にパスワードを変更すべきである。

いずれにしても、パスワードを簡単なものにすると他人から推測しやすいものになってしまい、難しいものにすると覚えられなくなる。覚えられないからといって他人から見られるような場所にパスワードを書いておくのではセキュリティの意味がない。覚えやすいものにして他人から推定されてしまってもパスワードの意味をなさないので、ここではそれなりにセキュリティが保たれるパスワードの運用を考察する。

① 覚えやすいフレーズを作り、一部を別のアルファベットや記号に置き換える
② ID とパスワードを 3 種類程度ずつ作り、組み合わせを変えて使い回す
　3 種類ずつ作れば 3×3＝9 通りの組み合わせが出来上がる

使い回すと言うことは、パスワードが漏えいした場合には他のサイトで不正アクセスされる可能性があることを認識しておかなければならないが、運用の容易さとある程度のセキュリティ確保を考えるとこのあたりに落ち着くのではないかと考えられる。

その他の対策としてはパスワード管理ソフトを使うという方法がある。これは、複数サイトの ID、パスワードを暗号化してファイルに記録しておき、閲覧・編集するマスターパスワードを設定する。そのマスターパスワードさえ覚えておけば記録したパスワードは参照できるというものである。記録したファイルがないと参照できないことと、覚えていないパスワードを入力する際に必ずパスワード管理ソフトを開かなければならないことで作業が煩雑になるが、記録しておくパスワードを 8 文字以上のランダムな文字列にしておけば安全性は飛躍的に高まる。

また、銀行等ではワンタイムパスワードを発行できるトークン（ワンタイムパスワード生成機）を配布しているところもある。ワンタイムパスワードとは、トークンと ID をあらかじめ利用登録しておくことで紐付けし、トークン利用時に一度しか使えない 6〜8 桁ほどの数字を発行（利用しなくても 60 秒毎に変更される）、それを 2 つ目のパスワードとして利用することでセキュリティを高めるものである。トークンには携帯できるサイズで専用のものや、スマートフォンなどで利用できるアプリ型のものがある。

利用できる環境であれば二段階認証を設定しておくと良い。前述のワンタイムパスワードを二段階認証に利用しているものがほとんどであるが、キャリアメール[23] や SMS[24]、電話を利用したものもある。二段階認証の手順は次のようになっている。

① ID とパスワードによる認証を行う
② ID とパスワードが正しければ二段階認証用の認証コードを入力する
③ 認証コードが正しければログインできる

認証コードによる認証が追加されているのが特徴である。この認証コードは「手元にある信頼できるデバイス」によって発行される。機器としてのトークンや携帯電話、スマートフォンなどである。これらは通常、所有者が常に持っているものと認識されるので、そこから発行される認証コードは信頼できるという考え方である。これによりパスワードによる認証だけではログインできなくなり、パスワードの変更等も認証コードがなければできないようになっているのでセキュリティは飛躍的に高まる。

(4) 個人情報漏えい対策

個人情報とは、個人を特定できる情報のことである。具体的には「氏名」「性別」「年齢」「住所」「電話番号」「メールアドレス」などの情報のうち、個人を特定できるものである。

個人情報を収集する際には、個人情報保護法により利用目的を明確にしておかなければならない。アンケートやプレゼントの応募などで個人情報を書く必要がある場合には必ずどこかに利用目的が明記されているはずである。その場合はどのような目的に利用されるのかを確認しておく。利用目的が明記されていない場合は個人情報保護法に違反していることになるので、個人情報を書くべきではない。

もちろん、自分の個人情報だけではなく他人の個人情報についても同様の配慮が必要となる。

他にも気をつけるべきこととして次のようなことがあげられる。

- 掲示板や SNS の投稿などに個人情報を書かない
- Facebook を除いた SNS やブログのプロフィール欄に個人情報を書かない
- スマートフォンなどで撮影した写真の Exif 情報を削除する

SNS の投稿やプロフィールに個人情報を書くことは絶対に避けるべきである。場合によってはストーカー被害や事件に巻き込まれる可能性もある。

特に気をつけておくべきところは写真である。写真に Exif 情報が記録されている場合には撮影状況を表すデータ「撮影機器のメーカー、モデル名」「画像の解像度」「シャッタースピード」「ISO 感度」などの他に「撮影日時」「GPS[25] 情報」（GPS がある機器の場合のみ）が付加されることがある。過去にはこの撮影日時や GPS 情報からおよその住所が特定

されたという例もあるので、もしSNSやブログ等にアップロードする写真であればこれらのExif情報は削除しておくべきである。

思わぬところから情報が漏れてしまうこともある。ゲリラ豪雨などの情報はインターネットで検索できる。日時と共にゲリラ豪雨に見舞われたことをツイートしてしまうと、その時だいたいどこに居たのかがわかるだけでなく、状況によっては住んでいるおよその場所が明らかになってしまうこともある。

(5)著作権・肖像権

著作権についても考えておかねばならない。レポートや論文を書く上で引用は認められているが盗用・剽窃は認められない。他人が創作したものを勝手に利用しはならないという意識を持つことが重要である。引用についても次にあげるルールを守らなければならない。

- 引用を行う必然性があるかどうか
- 自分のレポート・論文が「主」、引用が「従」であるか
- 引用部分を明確にし、改変せずに出典を明らかにする

また、肖像権についても知っておく必要がある。ブログ等に人物の写った写真を載せる場合、自分のみであれば本人が判断すれば良いが、他人が写っている場合は許可を得る必要がある。誰が写っているのかわからない場合（人物が小さくて顔が判別できない、後ろを向いているなど）は問題ないとされる。顔が判別できるサイズで写っている場合は、ぼかしやモザイクなどの加工を施して人物が特定できないようにした上で載せる必要がある。なお、タレントなどその人物自身が商品価値を持つ場合、パブリシティ権に関わってくる。

１１．まとめ

これから先、インターネットを利用した新しいサービスや機器が次々と出てくると思われるが、これらにいち早く注目して情報収集することが重要であると考えられる。現在注目されているものとしてはウェアラブル端末があげられる。眼鏡型や腕時計型、小型で身につけて携帯可能なサイズの情報端末である。眼鏡型であればAR[26]に応用、腕時計型であればスマートフォンより気軽に利用できる端末、歩数計や活動量計などの記録とデータ転送・管理ができる健康機器などに応用できる。一般的な機器として世間に出回った際には思わぬリスクの種となることも考えられるので、あらかじめ利用する上で問題がないか考えておく必要がある。

インターネット上で起こっている事柄を常日頃からチェックしておくことも必要である。

一般的なニュースサイトから IT 系ニュースサイトなどをこまめに閲覧しておく必要がある。特にセキュリティ関係のニュースには注目し、脆弱性やセキュリティリスクへ対応できるよう備えておくことが重要である。

インターネットが未発達だった頃と比較すると、インターネット回線もブロードバンド化されて非常に高速なものになり、PC に代表される情報端末も格段に進歩した。なにより情報量が増えて非常に便利になったと痛切に感じる。まさにインターネットなくして現在の生活は成り立たないと言っても過言ではない。しかし同時に、利用する上でのリスクも増している。個人が簡単に情報発信できるようになって、インターネット上で注目を浴びたいという気持ちは仕方のないものであるが、一度流れた情報を回収・削除することはほぼ不可能に近いことを理解した上で利用する必要がある。迂闊に情報を流すと、いつまでもインターネット上に残るのである。とはいえ、正しい対策と対処をすれば便利に使えるツールであることに間違いはない。必要とされる知識量はかなりのものとなるが、自分自身が正しい使い方を心がけるとともに、適切に指導できるように努力を続けていくつもりである。

注）

1）Advanced Research Projects Agency

2）Advanced Research Projects Agency Network

3）Internet Service Provider

4）ただし発売当初は「Microsoft Plus!」パッケージによるオプション機能であり、標準搭載されたのはバージョン OSR2 以降である

5）Personal Computer：パーソナルコンピュータ、パソコン

6）World Wide Web

7）Bulletin Board System

8）Hyper Text Markup Language

9）ブラウザが HTML とデータからウェブページを作成・表示すること

10）プログラムの一種

11）cross site scripting

12）Internet Information Service

13）File Transfer Protocol

14）Brute Force Attack：辞書ツールを利用した ID、パスワードの総当たり攻撃

15）Secure Shell

16）phishing

17）Internet Relay Chat

18）Social Networking Service

19）Massively Multiplayer Online Role-Playing Game：大規模多人数同時参加型オンライン RPG、数百～数万人の参加者が全員同時にプレイするロールプレイングゲーム

20）Multiplayer Online Role-Playing Game：複数プレイヤー参加型オンライン RPG、プレイヤーを数人～数十人程度に分割して同時にプレイするロールプレイングゲーム

21）First Person Shooter：一人称視点シューティングゲーム

22）脆弱性が発見されたとき、問題が広まる前（脆弱性が修正される前）に行われる攻撃

23）携帯電話キャリアが提供しているメールサービス

24）short message service：携帯電話や PHS 同士で短いメッセージのやりとりをする仕組み

25）Global Positioning System：地球上における位置を測定するシステム

26）Augmented Reality：拡張現実、現実世界に情報を付加することで拡張する技術

参考文献

【HP】

IPA, 情報セキュリティ 2013 年 7 月の呼びかけ,
http://www.ipa.go.jp/security/txt/2013/07outline.html

JPNIC, インターネット歴史年表,
https://www.nic.ad.jp/timeline/

警視庁, ワンクリック料金請求にご用心,
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku35.htm

総務省, ウイルスの感染経路,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/02-1.html

総務省, フィッシング詐欺に注意,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/05.html

総務省, 迷惑メール対策,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html