iBut
Internet Basic User Test

インターネットベーシックユーザーテスト

公式テキスト

一般社団法人 全国専門学校情報教育協会
Institute for Vocational Collage Information Technology Education

インターネットベーシックユーザーテスト 公式テキスト

Contents

第1章 インターネットの基礎

1-1 インターネットとは何か …… 4
1-2 インターネットの基本的な構造 …… 5
1-3 インターネットでできること …… 6
1-4 インターネットの影響力 …… 7

第2章 インターネットでの被害

2-1 インターネットは、具体的にどんな被害をもたらすのか …… 8
2-2 フィッシング詐欺 …… 9
2-3 ワンクリック詐欺 …… 10
2-4 詐欺、犯罪に巻き込まれないために …… 11
2-5 インターネットに関連した新たな詐欺の被害例 …… 12
2-6 迷惑メール、チェーンメール …… 13
2-7 健康面への影響 …… 14

第3章 インターネット関連の法規

3-1 著作権の重要性、保護する必要性 …… 15
3-2 著作権、肖像権、パブリシティ権 …… 16
3-3 違法ダウンロード …… 16
3-4 名誉毀損 …… 17
3-5 わいせつ物頒布 …… 17
3-6 特定商取引法 …… 17
3-7 電子契約法 …… 18
3-8 不正アクセス禁止法 …… 18
3-9 個人情報保護法 …… 18
3-10 青少年インターネット環境整備法 …… 19
3-11 特定電子メール法 …… 19
3-12 出会い系サイト規制法 …… 20
3-13 インターネット関連法規の改正 …… 20

第4章 インターネット利用者のモラル

4-1 情報発信者のモラル、心構え …… 21
4-2 ホームページを閲覧するうえで注意すること …… 22

4-3 個人情報の公開について …… 23
4-4 不正な嫌がらせや迷惑行為に遭わないために …… 23
4-5 プライバシーの保護について …… 24
4-6 インターネットにアクセスするうえでの心構え …… 24
4-7 電子メールのマナー …… 25

第5章 インターネットのしくみ

5-1 インターネットのしくみ …… 26
5-2 ホームページのしくみと利用の仕方 …… 27
5-3 電子メールのしくみ …… 28
5-4 ブログのしくみ …… 29
5-5 電子掲示板のしくみ …… 30
5-6 SNSのしくみ …… 31
5-7 ネットショッピングとは …… 32
5-8 ネットオークションとは …… 33
5-9 スマートフォンの基礎知識 …… 34
5-10 無線LANとWi-Fiの基礎知識 …… 37
5-11 クラウドサービスとは …… 39

第6章 コンピュータウイルス

6-1 マルウェアとは …… 40
6-2 コンピュータウイルスの感染経路 …… 43
6-3 コンピュータウイルス感染を防ぐには …… 44

第7章 セキュリティ

7-1 ユーザー認証の必要性 …… 45
7-2 パスワードの管理方法 …… 45
7-3 生体認証 …… 46
7-4 暗号化の必要性 …… 46
7-5 代表的な暗号化技術 …… 46
7-6 電子証明書 …… 47
7-7 フィルタリング（有害サイトアクセス制限） …… 48
7-8 ファイアウォール …… 48
7-9 ソーシャル・エンジニアリング …… 49
7-10 スキミング …… 50
7-11 スマートフォンのセキュリティ対策 …… 50

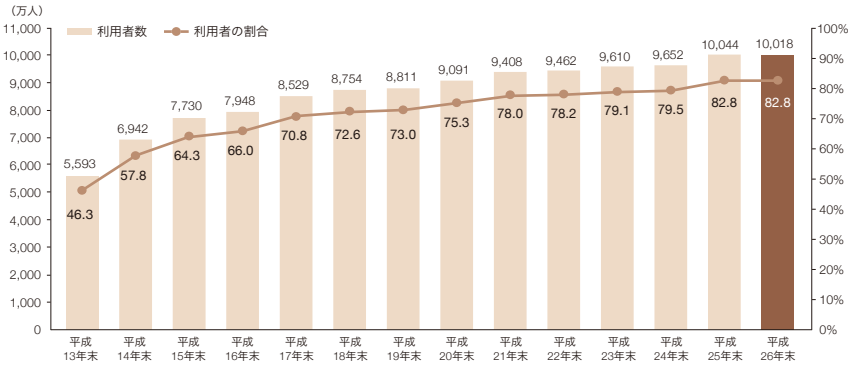
第1章
インターネットの基礎

1-1 インターネットとは何か

「**インターネット**」（Internet）は、世界中のコンピュータネットワークを相互に接続することで形成された世界規模のネットワークです。

インターネットは、1995年頃から一般家庭に急速に普及し、今では私たちの生活になくてはならない社会基盤のひとつとなりました。日本では6歳以上の人のうち、8割以上の人がインターネットを利用しているという報告もあります（**図1-1**）。

現在、インターネットは、パソコンやタブレット、スマートフォン、携帯電話などさまざまな通信機器で利用できます。今後、インターネットが利用できるデバイス（機器・装置）の変化はあっても、インターネットの使用はますます増えると予測できます。



（注）調査対象年齢は6歳以上。　　出典：総務省『平成26年通信利用動向調査』

図1-1 インターネット利用者数及び利用者の割合の推移（個人）

1-2 インターネットの基本的な構造

インターネットは、家庭や会社、学校といった小規模な単位で構成されるネットワーク（LAN）を外部のネットワークにも接続し、世界規模での通信ができるようにしたしくみのことです。

インターネットに接続されているコンピュータのうち、情報やサービスを他のコンピュータに提供する役目のコンピュータを「**サーバー**」、提供された情報やサービスを利用する役目のコンピュータを「**クライアント**」と呼びます（**図1-2**）。

例 **スマートフォンで、図書館にある雑誌について調べるとき**

- 雑誌の情報を調べるときに使うスマートフォン＝クライアント
- 雑誌の情報を提供する図書館のコンピュータ＝サーバー

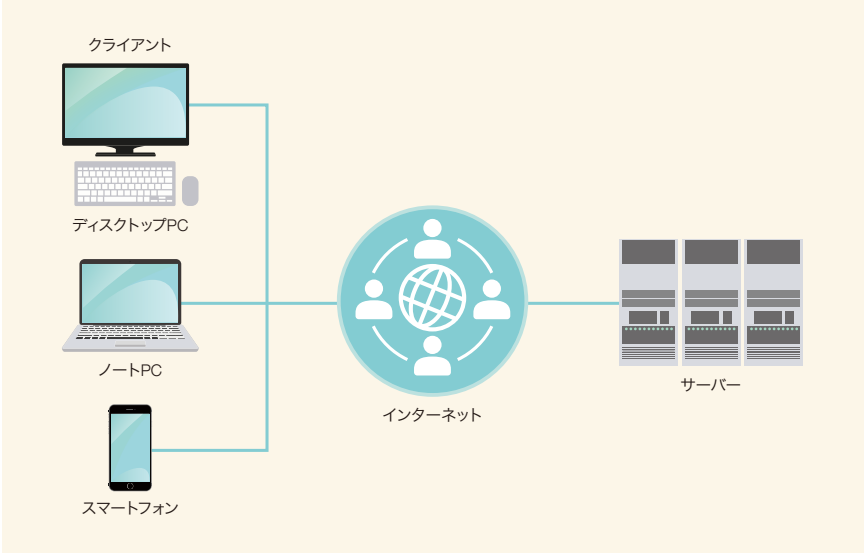


図1-2 クライアントとサーバー

1-3 インターネットでできること

インターネットを利用すると、たとえば次のようなことができます。

1 世界中の人との交流

個人のメールの送受信、複数の人によるディスカッション、掲示板やブログでの意見の発信など、さまざまな形態で、地域や国を越えて、多くの人と交流できます。

2 音楽、映像、文章などの双方向配信

情報を双方向でやりとりすることが可能です。たとえば、音楽や映像、文章などを手軽に入手したり、自分が制作した動画をWebサイトから世界の不特定多数の人に向けて配信したりできます。

3 電子商取引

インターネット上で商品やサービスを売買する「電子商取引」ができます。商品の検索から購入までを行うネットショッピングのほか、店を構えなくても物品の販売、オークションへの参加も可能です。

4 ビジネスの拡大

地域や国籍、言語の壁を越えたビジネスが可能となりました。これまではテレビや新聞などのマスメディアを活用した広報・広告活動が主でしたが、インターネットを活用すればターゲットとなる市場に直接商品の情報を届けることができます。また、電子マネー、ネットバンキングの普及により、多くの人が金融取引に参入できるようになりました。

5 その他

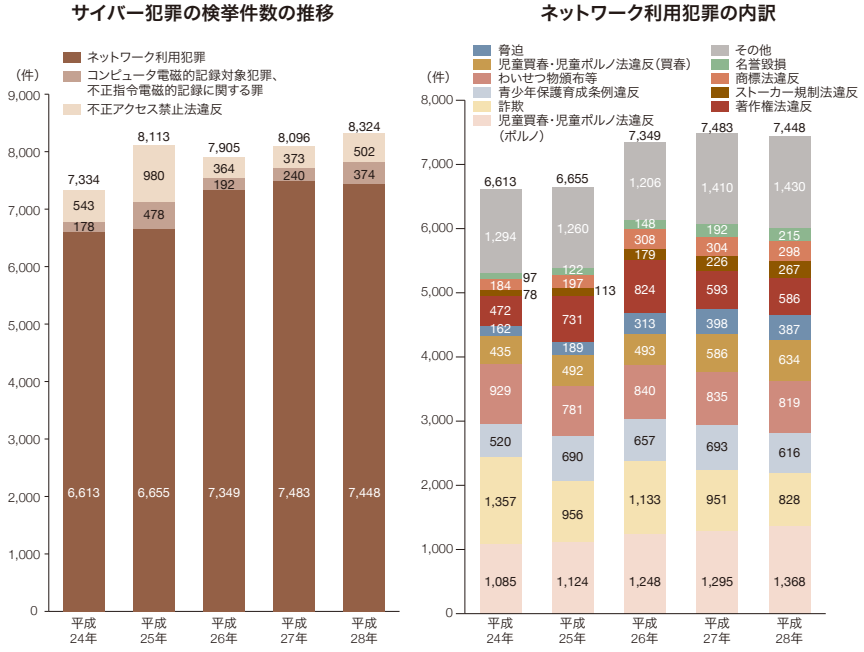
インターネットが使える環境があれば、24時間いつでも、どこからでも情報が受発信できるのがインターネットの利点のひとつです。災害時に電話回線網が寸断され、報道機関の情報発信すらままならないときに、多くの人がTwitterで連携し合い、被災状況や遭難者の位置を伝えたことが救援活動に役立ったという事例は、インターネットの利点が生かされた好例といえるでしょう。

1-4 インターネットの影響力

私たちはインターネットを利用することでさまざまな恩恵を受けています。

しかしその反面、間違った使い方や悪意をもった使い方をした場合の被害も計り知れないものがあり、インターネット上での詐欺事件や、コンピュータウイルスによるサイバー犯罪、個人情報の流出などのトラブルも年々増加しています（**図1-3**）。

このようなインターネットによるトラブルを防ぐためには、法律による規制、利用者のマナー・モラルの向上、技術的な対策、利用者の情報活用スキル（メディア・リテラシー）の習得などが必要です。



出典：警察庁『平成28年中におけるサイバー空間をめぐる脅威の情勢等について』

図1-3 サイバー犯罪の推移

第2章 インターネットでの被害

2-1 インターネットは、具体的にどんな被害をもたらすのか

情報の検索、メールの送受信、ネットショッピング、SNSなど、いろいろな場面で利用できる便利さから急速な広まりを見せるインターネットですが、その一方でインターネットによる被害も増えています。

[被害発生の例]

・金銭に関する被害
　例：オークションサイトで落札した商品が届かない
　例：フィッシング詐欺（2-2 参照）、ワンクリック詐欺（2-3 参照）
・メールに関する被害
　例：迷惑メール（2-6 参照）が大量に届く
・コンピュータやソフトウェアの不具合による事故や障害
・情報の漏(ろう)えい
　例：パスワードが盗まれ、ハードディスクの情報が流出
　例：ある企業の社員が顧客情報を保存していたUSBを紛失
・誹謗(ひぼう)中傷
　例：Web上の掲示板にいわれのないうわさが書かれて広まった
・コンピュータウイルスに感染
・政府や企業のサーバーに何者かが侵入し、システムが破壊された
・肖像権の侵害
　例：イベント参加時の写真が、許可なくWebサイトに掲載された

悪意ある行為による被害はもちろんのこと、犯罪を意図していなくてもパソコンの操作ミスにより被害が起きてしまうこともあります。また、たとえば1人の不注意な書き込みから企業が社会的な信用を失うなど、一度起きると甚大な被害が生じることもあります。

思わぬところに多くの危険が潜み、誰もが加害者にも被害者にもなる可能性があるのもインターネットによる被害の特徴です。

2-2 フィッシング詐欺

「**フィッシング詐欺**」とは、別人になりすまして電子メールを送りつけたり、有名な会社名をかたって偽のホームページに誘導したりする方法で、クレジットカード番号やアカウント情報（ログインIDやパスワード）などの個人情報を盗み出す行為です。

有名なサイトと似たURLの使用や、本物とほとんど区別がつかないような画面が偽造されるなど、年々、手口が巧妙になっており、ひと目では詐欺と見抜けないケースが増えています。

典型的な手口には次のものが挙げられます。

! 電子メールでフィッシングサイトに誘導

クレジットカード会社や銀行からの連絡メールに似せて、本物そっくりな偽サイトにユーザーを誘導し、クレジットカード番号や口座番号などを入力させて情報を盗み取ります。

! 電子掲示板からフィッシングサイトに誘導

電子掲示板やSNSの投稿サイトに、悪質なサイトのリンクを張って誘導します。

! 偽のURLでフィッシングサイトに誘導

本物のURLに見せかけて、偽サイトのURLにアクセスさせます。

2-3 ワンクリック詐欺

「**ワンクリック詐欺**」とは、Webサイトや電子メールに記載されたURLを一度クリックしただけで、一方的に不当なサービスへの入会などの契約成立を宣言され、料金の支払いを求められる詐欺の一種です（**図2-1**）。

典型的な手口は、

- 興味を引きそうな電子メールや電子掲示板などを通じて、利用者をおびき寄せる。アダルト系、出会い系のWebサイトを装った内容であることが多い。
- いかにも正当な契約手続きが完了しているかのように見せかけ、利用料を不正に請求する。
- わざとわかりにくいところに不当な利用規約などを表示し、利用者に気付きにくくする。
- 料金請求の際、携帯電話の個体識別番号やパソコンの固有識別番号、利用している通信プロバイダの情報を表示し、あたかも利用者が特定されたように見せかける。
- 期限内に支払わない場合、延滞料が加算される、法的措置を講ずる、取り立て業者を向かわせる、といった脅迫的な内容で、利用者に支払いを迫る。

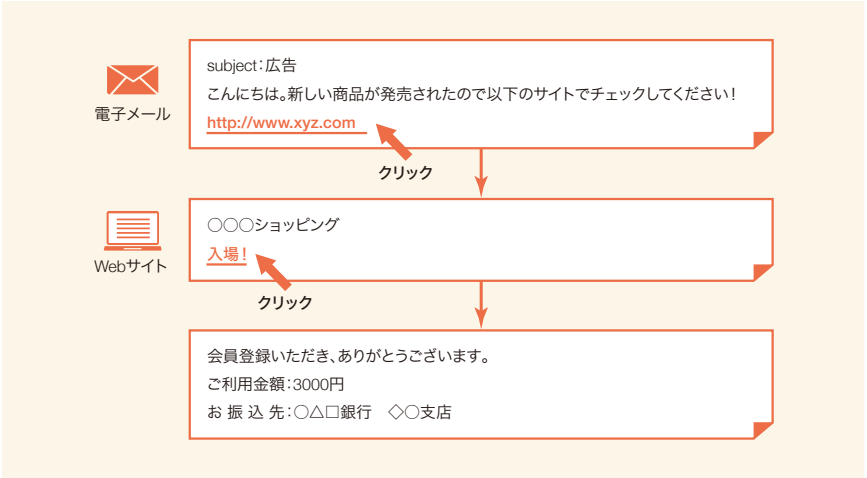


図2-1 ワンクリック詐欺の手口の例

また、クリック後に確認措置をとる画面をポップアップさせて電子消費者契約法に基づいているかのように見せかけ、キャンセルしても強制的に契約させられてしまう「ツークリック詐欺」、「スリークリック詐欺」などの手口も登場しているので注意が必要です。

2-4 詐欺、犯罪に巻き込まれないために

インターネット犯罪に巻き込まれないための対処法として、以下が挙げられます。

事前確認を十分に行う

利用規約を長文にしたり、Webブラウザで見えづらい表示に細工して、利用規約を読まずにクリックさせる手口も横行しています。Webサイトへアクセスする場合は、必ずサイトの利用規約や注意事項を確認する、電子掲示板の文面はきちんと読むなど、事前確認をする習慣をもちましょう。

不当な支払い請求は無視する

間違ってクリックしてしまい、意図せずにWebサイトを閲覧して料金を請求された場合は、相手に連絡などはせず無視しましょう。このような手口は「電子契約法」（正式名称：電子消費者契約及び電子承諾通知に関する民法の特例に関する法律）で規制されており、支払い義務は発生しません。消費者が、コンピュータの操作ミスなどで契約する意思なく申し込んだ場合も救済措置がとられます。

また、支払い拒否の意思表示や支払い理由の確認として業者に連絡を取ることは、相手に自分の個人情報を渡すことにつながるので、絶対にしてはいけません。どうしても心配なときは、支払いをする前に、総務省電気通信消費者相談センター、消費生活センター、警察などに相談しましょう。

迷惑メールを受信しない工夫をする

インターネットによる詐欺は、迷惑メールなど知らない人から送信されたメールが発端となる場合が多く見られます。このようなメールをできるだけ受信しないために、あらかじめ推測されにくいメールアドレスを使ったり、不特定多数に送信されるメールを受信しないように情報機器を設定しておいたりするとよいでしょう。

危険が潜む可能性を念頭におく

ホームページを表示した際に自動的にウイルスを埋め込む悪質なWebサイトも増えています。知らないWebサイトを訪問する場合には、危険が潜んでいる可能性を念頭におき、可能な限り事前に調べて使うことが大事です。

2-5 インターネットに関連した新たな詐欺の被害例

詐欺師は新しい手口を次々とつくり出しており、以下のような被害例も発生しています。

[事例]

インターネットバンキングを利用している金融機関から、「お知らせ」という電子メールが届きました。そこに書かれたリンクをクリックすると、その金融機関のホームページが表示されました。同時に別の画面が開かれ、ユーザー確認のためにインターネットバンキングのIDや暗証番号、秘密の質問の答えの再入力が要求されました。表示された画面には暗号化通信のSSLの鍵マークも表示されており、フィッシング詐欺ではなさそうです。

画面の指示に従い、IDや暗証番号、秘密の質問の答えの再入力を行いました。しかし、これがもととなり、インターネットバンキング口座の預金を取られてしまいました。

[解説]

従来の偽のホームページに誘導するタイプのフィッシング詐欺とは異なる、新たな詐欺の事例です。あらかじめ利用者のコンピュータにウイルスを感染させておき、不正な入力画面をポップアップして、インターネットバンキング口座にアクセスするための情報を盗み取る手口です。不正なポップアップ画面の後ろに表示されているのが、本物のインターネットバンキングのホームページなので、見分けるのが困難になっています。

[対応]

金融機関が、ポップアップ画面でユーザー情報の再入力を求めることはないので、画面が表示されても入力しないようにします。また、利用している金融機関のインターネットバンキングの機能や操作方法、注意事項などを確認し、そこに書かれていない操作はしないように気をつけましょう。

2-6 迷惑メール、チェーンメール

電子メールに関する被害には、次のようなものがあります。

迷惑メール

「迷惑メール」は、受信者の意向を無視して、無差別かつ大量に一括して送信される電子メールのことで、「スパムメール」とも呼ばれます。迷惑メールには、単なる広告活動のほか、悪意のあるWebサイトへ誘導させるものなどがあります（**図2-2**）。

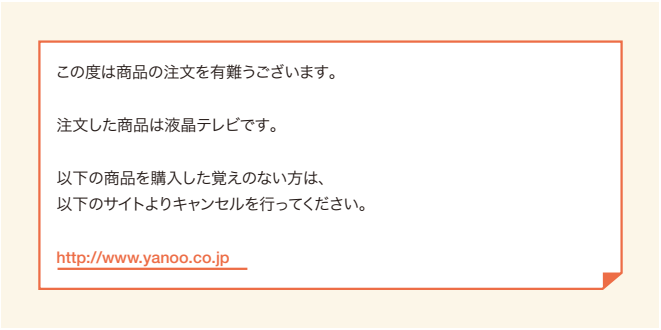


図2-2 迷惑メールの例

チェーンメール

「チェーンメール」は、連鎖的に特定多数への配布をするように求める電子メールです。「このメールを転送しないと不幸になる」など、他者への文書の転送を促すような文面がよく見られます。

迷惑メールやチェーンメールの受信が増えると、削除するのもわずらわしく、メールの使用に支障がでます。他の人に迷惑がかかるので、絶対にこれらのメールを転送しないようにしましょう。

また、電子メールアドレスは、電子掲示板などWebサイトへの書き込みや懸賞への応募などによって流出するケースもあります。迷惑メールやチェーンメールの受信を防ぐには、

・電子掲示板などに電子メールアドレスを不用意に入力しない
・第三者から推測されにくい電子メールアドレスを使用する

とよいでしょう。

もし、迷惑メールやチェーンメールがたくさん送られてくるようになったら、電子メールアドレスを変更するか、通信プロバイダが提供する迷惑メールフィルタ機能を利用してください。また、迷惑メールを利用したトラブルに巻き込まれないためにも、受信した迷惑メールは無視するようにしましょう。

2-7 健康面への影響

インターネットの普及により、一般のユーザーでもコンピュータやスマートフォンを長時間利用する人が増えてきました。これらの機器を、限度を超えて長時間利用することで生じる心身への影響は「**テクノストレス**」(techno stress)、あるいは「**VDT症候群**」(visual display terminal) と呼ばれます。

たとえば身体面では、画面を長時間見続けることによる視力低下や視力障害、キーボードや液晶画面操作による手首や首の炎症などが多く見られます。長時間の使用を避けること、休憩をとりながら使用することなどを心がけ、身体への負担の軽減に努めましょう。

また、心にも影響が生じることがあります。インターネットに依存してしまう「インターネット中毒」も、テクノストレスの一種です。特に、オンラインゲームによるインターネット中毒は、学校や会社に通えなくなるなど日常生活に支障を来すことも多く、問題となっています。

時間を決めてゲームするといった日ごろの心がけももちろん大切ですが、もし、日常生活が困難になるなどのインターネット中毒の兆候を感じたときは、家族や周囲の人に相談してカウンセリングを受けるなどの対応も必要です。

第3章
インターネット関連の法規

3-1 著作権の重要性、保護する必要性

音楽、映像、写真、イラストなど、インターネットで閲覧できるほとんどのものは、誰かが著作権を有しています。これらの著作物が製作者に無断で世間に広がった場合、本人の努力や才能が侵害されるばかりでなく、その人たちの収入源を奪うことにもつながります。

CDの不正コピーやダウンロードによる音楽業界の衰退を危惧する声があるように、お金を惜しんで利己的な行為を行う先には、よい作品が生まれない、つまらない未来が待っています。著作物に対する敬意と保護の精神をもつことが大切です。

著作物を権利者の許諾を得ないで複製することや、インターネット上に勝手に掲載して誰でもアクセスできる状態にすることは、著作権侵害にあたります。新聞や雑誌などの記事にも著作権があり、引用の範囲を超えて掲載すると著作権侵害にあたるので注意しましょう。

また、人物の写真の場合、撮った人が著作権を有するだけでなく、写っている人には肖像権があるため、ホームページに掲載するにはこれらすべての権利者の許諾が必要になる場合があります。

絵や写真などの市販の素材集や、インターネットで素材を提供しているホームページなどでは、「使用する場合に権利者に許諾を求める必要がない」旨を記載していることがあります。しかし、そのような素材であっても、商業利用については制限がかけられていることもあるため、必ず規約をよく読んでから利用するようにしましょう。

3-2 著作権、肖像権、パブリシティ権

著作権

「**著作権**」は知的財産権のひとつで、著作物に対する著作者の権利のことです。「著作権法」では、自分の制作した画像や楽曲、撮影した写真などを、他人が勝手に公開したりすることを防ぎ、著作権を保護する内容が定められています。権利者の許可を得ずに複製したり、インターネット上に掲載したりすることは著作権侵害にあたるため、情報を発信する際には十分に注意しましょう（**図3-1**）。

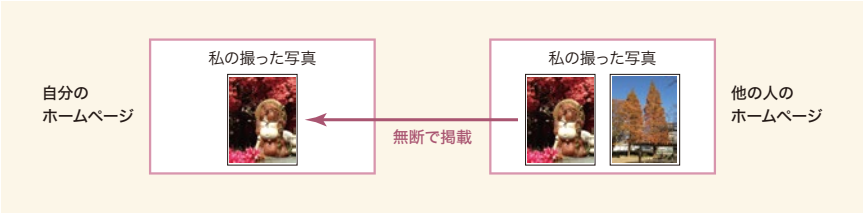


図3-1 著作権侵害の例

肖像権

「**肖像権**」は、写真や絵画など自分の肖像を、他人に勝手に撮られたり使用されたりしない権利で、個人の人格やプライバシーの保護を目的としています。他人の顔写真を無許可でWebに掲載するのは肖像権の侵害にあたります。

パブリシティ権

「**パブリシティ権**」とは、タレントなどの顔や姿などの経済的利益を保護する権利で、広くは肖像権に含まれます。肖像権と同様、タレントなどの写真を無許可でWebに掲載したりしないようにしましょう。

3-3 違法ダウンロード

有償で提供されている音楽・映像、電子書籍が無断でインターネット上に置かれていることを知り、そこから自分のパソコンや情報機器、録音／録画装置に勝手に保存することを「**違法ダウンロード**」といいます。たとえ私的使用の目的であっても著作権を侵害する行為として罰則の対象となります。

3-4 名誉毀損

「名誉毀損（めいよきそん）」とは、相手の名誉を傷つけ、損害を与える行為をいい、刑法では「公然と事実を摘示し、人の名誉を毀損した者は、その事実の有無にかかわらず、三年以下の懲役若しくは禁錮又は五十万円以下の罰金に処する。」と規定されています。

刑法の「公然と事実を摘示し」とは、公共施設や職場、インターネットの掲示板など不特定多数の人が認識できるような場所で、具体的な事実を示すことです。インターネットに「○○は前科者だ」など、相手の名誉を傷つけ、不利益を生じさせるような書き込みをすることも名誉毀損にあたります。

3-5 わいせつ物頒布

刑法に「わいせつな文書、図画その他の物を頒布し、販売し、又は公然と陳列した者は、二年以下の懲役又は二百五十万円以下の罰金もしくは科料に処する。販売の目的でこれらの物を所持した者も同様とする。」と規定されています。わいせつ物の公開はやめましょう。

3-6 特定商取引法

「**特定商取引法**」とは、消費者トラブルを防ぐために、事業者の不公正な勧誘行為を取り締まる法律です。「事業運営者の情報開示」「商品やサービスの価格と支払い時期、提供期間の適切な提示」「事実と著しく異なる情報を表示し消費者に誤認を与えることの禁止」「表示を裏付ける資料の提出」「未承認者に対するメールの禁止」「顧客の意に反する申込みをさせる広告の禁止」などが規定されています。これらのいずれかに該当するサイトでの商取引は控えましょう。

3-7 電子契約法

インターネットショッピングなどの電子商取引における契約については、「電子契約法」（正式名称：電子消費者契約及び電子承諾通知に関する民法の特例に関する法律）で規定されています。その法律によれば、電子商取引は、申込み完了前にユーザーが申込み内容を確認できる措置を講じなければならないと定められています。申込み内容の確認がないまま注文を完了してしまうサイトは、違法サイトの可能性が高いので商品購入はしないようにしましょう。

3-8 不正アクセス禁止法

「**不正アクセス**」とは、利用する権限を与えられていないコンピュータに、インターネットやLANなどのネットワーク経由で不正に接続しようとすることです。コンピュータへの侵入や、遠隔操作で使用することは「不正アクセス禁止法」違反で処罰されます。

3-9 個人情報保護法

「**個人情報**」とは、生存する個人の情報で、個人を識別できる情報のことです。単独では個人を識別できない情報でも、他の情報と組み合わせることによって特定の個人を識別できるものは、個人情報に該当します。

氏名、住所、性別、生年月日、勤務先、電話番号、電子メールアドレス、指紋認証デバイス、マイナンバー、親族情報などが個人情報にあたり、なかでも氏名・住所・性別・生年月日は基本四情報と呼ばれます。

私たち一般消費者の個人情報は、販売戦略に生かせる情報源として経済的な価値があるとされ、知らないうちに個人情報が売買されたり、企業から個人情報が盗み出されたりする事件が後を絶ちません。ほかにもUSBメモリやノートパソコンの紛失・盗難が原因で、個人情報が漏えいするケースも見られます。

日本では、1989年に「行政機関個人情報保護法」（正式名称：行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律）が施行され、2006年にすべての地方

自治体が「個人情報保護条例」を制定し、個人情報の漏えいが起きないような保護制度をつくってきました。また、企業活動を中心とする個人情報保護に関する法律として、2005年に「個人情報保護法」（正式名称：個人情報の保護に関する法律）が施行されています。

ネットショッピングやネットバンキングなどのサービスを利用する場合は、個人情報を登録する必要が生じます。安易に登録せず、セキュリティ面をしっかりと確認してから登録するようにしましょう。また、個人のホームページやブログを開設する場合には、記載する個人情報についても十分検討することが大切です。

3-10 青少年インターネット環境整備法

2009年、青少年を有害サイトから守ることを目的に「青少年インターネット環境整備法」（正式名称：青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律）が施行されました。

青少年にインターネットを適切に活用する能力を習得させることや、フィルタリングの普及促進などにより青少年の有害情報の閲覧機会を最少化することなどを基本として、インターネット関係事業者に義務などを課すとともに、保護者やインターネットの利用者みんなで青少年を有害情報から守る取り組みを求める法律です。

3-11 特定電子メール法

迷惑メール（スパムメール）は、携帯電話やスマートフォンの普及で増加傾向にあります。業務の妨げやインターネット回線を混雑させる迷惑メールの送信を取り締まるため、2002年に「特定電子メール法」（正式名称：特定電子メールの送信の適正化等に関する法律）が施行されました。

この法律により、事業者が広告メールを送信する際には送信者情報の表示が義務付けられ、偽った場合は1年以下の懲役または100万円以下の罰金が科せられます。

3-12 出会い系サイト規制法

「出会い系サイト」は、面識のない異性との交際を希望する者同士が、電子掲示板を通して、電子メールやチャットなどで互いに連絡できるようにするサービスを行うWebサイトです。

18歳未満の人が出会い系サイトを利用することは「出会い系サイト規制法」（正式名称：インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律）」で禁止されています。

警視庁の発表によると、出会い系サイトに関連した事件の被害者の多くが18歳未満です。会員登録によって高額な金額を請求されたり、出会い系サイトで知り合った人から脅されたり、自分のプロフィールを使用して誰かが偽の会員登録をしていたりするなどのトラブルが多数報告されています。

3-13 インターネット関連法規の改正

関連する法が施行された後も、法の隙間をついた事件や犯罪が発生してしまいます。それに伴い、「個人情報保護法」「青少年インターネット環境整備法」などは、より規制を強化する様な形で法改正が執り行われています。

私たちも、新聞やニュースなどでインターネット関連法規の動きに注目し、世の中の動きを捉えていく必要があります。

第4章
インターネット利用者のモラル

4-1 情報発信者のモラル、心構え

インターネットでは、ニュース記事などの文字データ、写真・動画などの画像データ、音楽データなど、さまざまな情報を入手できます。膨大な情報を簡単に入手できますが、その内容は玉石混交であり、ユーザーは信頼性や客観性を自分で判断して正しい情報を取捨選択しなければなりません。

情報の出所や情報が作成された日時、情報に書かれているのは個人的意見か公的意見かなどを確かめるとともに、新聞やテレビなどの他の情報源による情報とも比較して、信用できる情報かどうかを判断するとよいでしょう。

インターネット上の情報は電子データなので、コピーが簡単にできるのも特徴です。しかも、世界中の利用者がインターネットにアクセスできるという特性上、情報は、口コミとは比べものにならない速さで、広範囲に拡散します。つまり、一度拡散した情報をインターネット上からすべて消し去るのはきわめて困難です。また、検索技術の向上により、インターネットで公開された断片的な情報から、誰が書き込んだ情報であるかが特定されてしまう場合もあります。

ですから、インターネットで情報発信をする際は、むやみに機密情報や自身や知人、家族などの個人情報を書き込まないようにすることが大切です。「軽い気持ちで」「いたずら半分で」「すぐに消せばいいから」といった安易な気持ちで公開した情報が、あっという間にネット上に拡散し、甚大な被害と不幸を招いたケースが頻発しています。

書き込む内容や情報を公開する範囲、その結果どのような影響がありえるかを意識して、情報発信することが大切です。

インターネットが原因のトラブルは、ささいなことがきっかけで起こります。たとえば、悪気のないネットの掲示板への書き込みが他人の心を傷つけたり、心理的な圧迫を与えたり、自身の発言でサイトが炎上して大勢の人から糾弾されるケースなどがよくみられます。

また、操作や通信設定のミス、機器の紛失による情報の漏えいなど、「つい、うっかり」からも多くの被害が発生しています。発信した情報がもとで、企業や組織のブランドやイメージが大きく低下したり、他人のプライバシーを侵害したりといったトラブルも増えています。

インターネットに書かれた情報は広く不特定多数の人に公開されていること、その利便性と裏腹に情報が悪用されて思わぬ被害を受ける危険性をはらんでいることを、常に念頭において使うように心がけましょう。

4-2 ホームページを閲覧するうえで注意すること

Webブラウザは、ホームページ上でさまざまな処理ができるように、各種のプログラムを実行できるしくみになっています。これらのプログラムの脆弱性を突いて悪用するウイルスが埋め込まれたホームページを閲覧すると、それだけでコンピュータがウイルスに感染するおそれがあります。

最近では、Webブラウザへ機能を追加するアプリケーション（プラグインソフト）の脆弱性を悪用したケースが増加しています。これまでは、怪しいWebサイトを訪問しなければ大丈夫だと思われていましたが、最近では正規のWebサイトが不正侵入によって書き換えられ、ウイルスが仕込まれてしまうケースも急増しています。

また、無料のウイルス対策ソフトに見せかけて、悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」など、巧妙で悪質な手口による被害も増えています。たとえば、ホームページなどで「あなたのコンピュータはウイルスに感染しています」といったメッセージを表示し、利用者を偽のウイルス対策ソフトを配布するWebサイトに誘導し、感染させる手口です。

信頼できるサイトか確認し、少しでも怪しいと思われるサイトで配布しているプログラムはインストールしないようにしましょう。

4-3 個人情報の公開について

インターネット上で公開した情報は不特定多数の人が閲覧するので、見知らぬ人に悪用される危険性もはらんでいます。そのため、インターネット上に名前、年齢、住所、電話番号、メールアドレス、写真などの個人情報を公開することの危険性について、きちんと認識しておくことが大切です。

たとえば、写真や住所、連絡先が公開されていれば、ホームページを見た人があなたに興味をもち、自宅の周りをうろついたり、電話をかけてきたりするかもしれません。また、公開した情報が、迷惑メールや振り込め詐欺など、別の犯罪に利用されるおそれもあります。

このような被害から身を守るためにも、インターネット上にはむやみに個人情報を公開しないようにすることです。 4-1 でも述べたとおり、インターネットで公開した断片的な情報から個人が特定され、情報が広範囲に拡散するなど、思わぬ危険が潜んでいます。ですから、プライバシーの公開は慎重に行うことが大切です。さらに、自分以外の家族や他人の個人情報を、本人の許可なく掲載することは絶対に行ってはいけません。

4-4 不正な嫌がらせや迷惑行為に遭わないために

インターネットは、ホームページやブログ、SNSなどを通じて、自分の考えや日常生活の様子などを手軽に多くの人と共有できること、自分の投稿への反応をすぐに確認できることなどが魅力的です。その一方で、これらの情報発信に関連するトラブルも起きています。

自分が管理するWebサイトでは、迷惑行為への対策として、迷惑行為の禁止や「不適当と思われる発言は削除します」などを明記し、これらの行為を発見したらすみやかに書き込みの削除を行うようにします。

また、悪質な迷惑行為を受けた場合は、投稿日時、投稿者のコンピュータ名、IPアドレス、投稿内容などの情報を保存した上で、サイトの管理者などに削除を依頼しましょう。相手が接続している通信プロバイダや企業の管理者に連絡することも対策のひとつです。

自分で対応するのが不安な場合は、次の専門の相談窓口に問い合わせるのもよいでしょう。

・インターネットホットライン連絡協議会
・違法・有害情報相談センター
・法務省 インターネット人権相談受付窓口

4-5 プライバシーの保護について

プライバシーとは、「他人の干渉を許さない、各個人の私生活上の自由。」（『広辞苑 第六版』岩波書店）を意味します。インターネットにおいても実社会と同様、プライバシーが守られなければなりません。インターネットメディアは気軽に情報発信できるメディアであるために、発信のしかたを誤ってプライバシーを侵害し、トラブルに発展することも多くあります。 不特定多数の人が利用していることを常に意識して、特にプライバシーに関する情報の取り扱いには細心の注意を払いましょう。

なかでも最も重要なのは、個人情報を不用意に公開しないことです。 氏名やメールアドレスなど、たとえ自分自身の情報であっても、ホームページなどで公開するのはプライバシー保護の観点上問題はないか、十分に考えて行うようにします。また、自分以外の人の個人情報をインターネットに公開することは絶対にやめましょう。

ホームページを開設する人や企業がアンケートなどで個人情報を収集する場合には、情報管理に重大な責任があることを認識しなければなりません。プライバシーに関する情報は、万全な情報セキュリティで管理する義務があるのです。

4-6 インターネットにアクセスするうえでの心構え

インターネットでは、距離を気にせず多くの人と交流ができる反面、相手の顔が見えないため、発信した情報への反応をリアルに確認できないという弱点があります。 無遠慮なコメントを書いたり、他人のプライバシーに関わる画像を掲載したりして、知らぬ間に誰かを傷つけてしまう危険性があるので、情報の受け手がどう感じるかを常にイメージし、社会ルールを守って使うようにしましょう。

4-7 電子メールのマナー

電子メールは、ネット環境があればいつでも送れるのでとても便利ですが、受信者がいつ読むかはわからない、メールサーバーやネットワークのトラブルによって受信者にすぐに届かない場合もある、といったことがあります。そのため、返信が必要なメールは特に、時間に余裕をもって送信することが大切です。また、受信者への配慮として、メールの要件を短く表した件名を付けるとよいでしょう。

電子メールには、送信元（From）、宛先（To）のほかに、メールを他の人にも同時に送りたい場合に使用するCC（Carbon Copy）、BCC（Blind Carbon Copy）があります。CCで複数の宛先に送信した場合、受信者はCCで送信された他のユーザーの電子メールアドレスを見ることができます。

一方、BCCで複数の宛先に送信した場合、受信者は宛先（To）のユーザーと自分以外に、誰に電子メールが送られたかわかりません。面識のない複数の人に一斉にメール送信する場合は、個人情報流出の原因とならないようにBCCで送信を行うようにします（**図4-1**）。

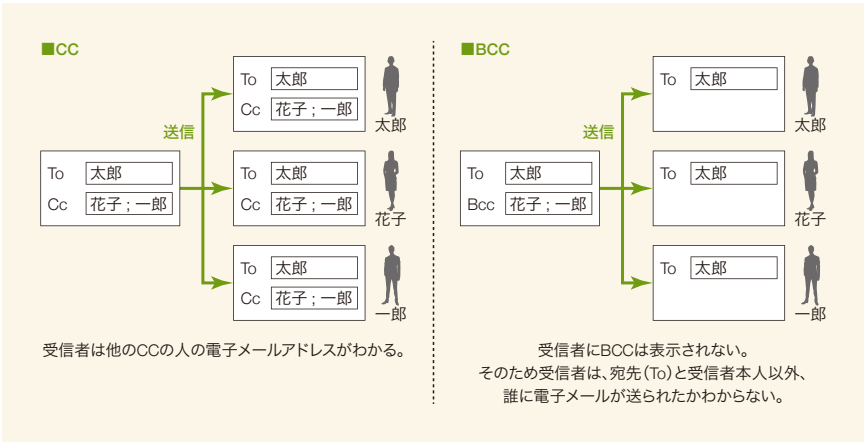


図4-1 CCとBCCの違い

第5章
インターネットのしくみ

5-1 インターネットのしくみ

インターネットに接続するコンピュータやスマートフォンは、1台1台異なる「**IP**（アイピー）**アドレス**」をもちます。インターネット上の住所にあたるIPアドレスは、「198.55.123.100」のようなデータで表され、インターネット上の情報の行き先を指定するために使用されます（**図5-1**）。

インターネットを通じてデータを送受信する際、データは「**パケット**」という単位に分割されます。パケットに分割することで、インターネット内の回線にかかる負荷を軽減しています。

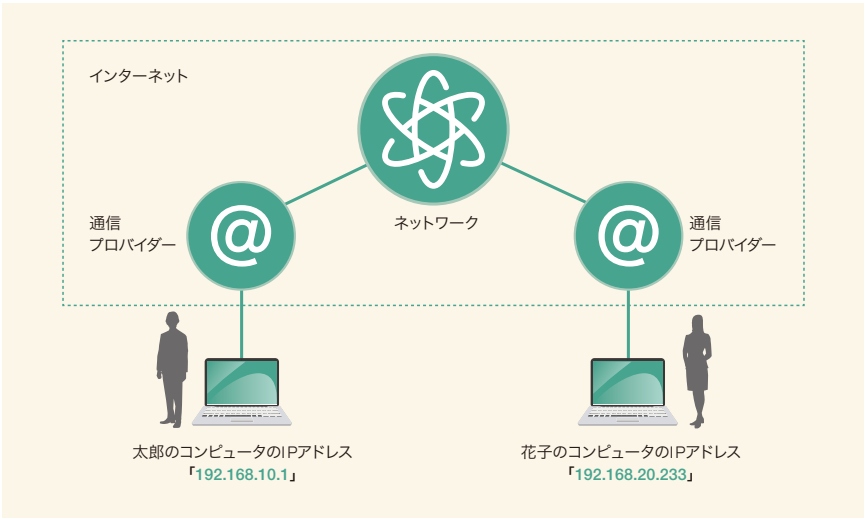


図5-1 インターネットの概念

5-2 ホームページのしくみと利用の仕方

インターネットで情報を公開するページを「**ホームページ**」、あるいは「Web(ウェブ)サイト」「Webページ」といいます。ホームページの内容は、インターネット上にある「**Webサーバー**」（ホームページ公開専用のコンピュータ）に保存されています。

ホームページは、コンピュータの「**Webブラウザ**」（ホームページを閲覧するための専用ソフトウェア）に「**URL**(ユーアールエル)」を指定することで閲覧できます（**図5-2**）。

例 **ヤフーホームページのトップページのURL**

URL：インターネット上の情報が格納されている場所を示す文字列。

http://www.yahoo.co.jp

ドメイン：Webサイトなどのインターネットサービスを提供するサーバーを表す文字列。

W W W(World Wide Web)(ダブリューダブリューダブリュー)：
世界中のサーバーで公開されている情報をインターネットのホームページとして閲覧できるしくみのこと。

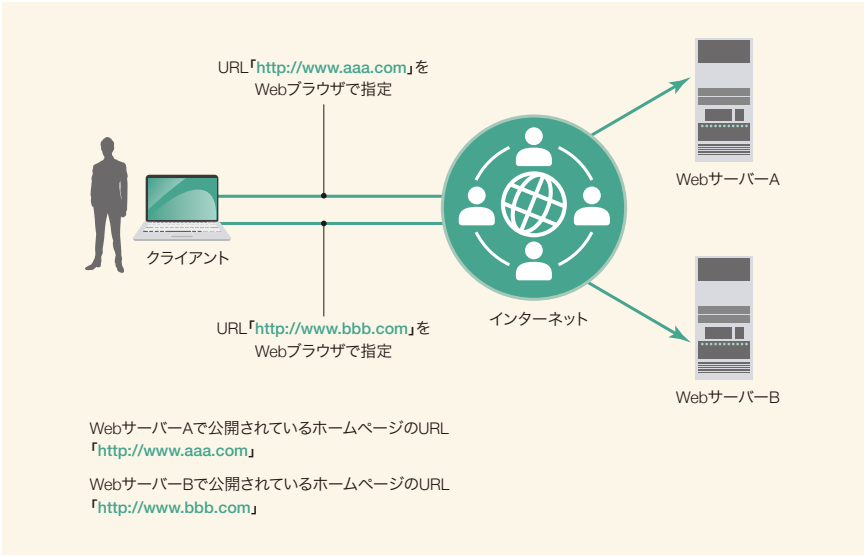


図5-2 WebブラウザでURLを指定

Webブラウザを使えば、ホームページのほか、電子掲示板、ブログ、SNS（エスエヌエス）、ショッピングサイトなどのサービスを閲覧・利用できます。

[代表的なWebブラウザ]

- Microsoft IE、Edge
- Google Chrome
- Mozilla Firefox
- Apple Safari

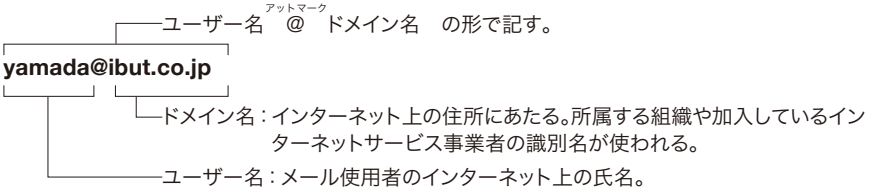
ホームページへのアクセスは、Webサーバーを公開する企業・個人や通信プロバイダーによってアクセスの記録が行われています。SNSなどに書き込んだメッセージやアクセス履歴は、常に記録されていることを意識してインターネットを使用するようにしましょう。

5-3 電子メールのしくみ

「**電子メール**」（**e-mail**）は、パソコンやスマートフォン、タブレット端末などの通信機器を使ってインターネット上で情報をやりとりする機能です。文章以外に、画像や動画、音声などを「**添付ファイル**」として受発信できます。

電子メールの利用には、個人やコンピュータを特定する「メールアドレス」が必要です。

例 **電子メールアドレス**



電子メールは、Google（グーグル）やヤフーの提供するWeb上での電子メールサービスや、メーラー（メール専用のソフトウェア）で利用可能です。

5-4 ブログのしくみ

「**ブログ**」は「ウェブログ」の略で、投稿した記事が時系列に表示されるWebサイトのことです。個人的に自分の行動を記録するためや、意見を公開するために多く利用されてきました（**図5-3**）。

ブログは、通常のWebブラウザで閲覧でき、所定のエリアに文章などを書き込むだけで自動的に更新できるしくみです。ホームページは更新するのにHTMLファイルの書き換えが必要ですが、ブログはWebの専門知識やホームページ作成ソフトを必要としません。

簡単に情報を公開できることから、以前は個人的な利用が中心でしたが、企業が自社の情報を告知するブログも増えており、利用が広まっています。

[代表的なブログ]

- アメーバブログ　http://ameblo.jp/
- Gooブログ　http://blog.goo.ne.jp/

図5-3 ブログのイメージ

ブログと類似のサービスに「**プロフ**」があります。プロフは「プロフィールサイト」の略で、生年月日や性別、趣味、写真など、自分のプロフィールを掲載するWebサイトが簡単に作成できるサービスです。当初、携帯電話で利用できたことから、主に学生の間で広まりました。

5-5 電子掲示板のしくみ

「**電子掲示板**」は、ホームページの表示エリアに多くの人が共通の話題について意見やメッセージを書き込めるようにしたWebサイトです。学校などに設置される掲示板と役割が似ていることから、「掲示板」「BBS（ビービーエス）」とも呼ばれます。その形態は、個人が運営するものから企業が運営する大規模なものまでさまざまです。

書き込まれたメッセージは、共通の話題を集めた「スレッド」（文章のまとまり）ごとに分類した形で所定のデータベースに蓄積され、閲覧者がページを参照すると最新のデータが自動的に表示されるしくみになっています（**図5-4**）。

［代表的な電子掲示板］

- 2ちゃんねる　http://www.2ch.net/
- Yahoo!知恵袋　http://chiebukuro.yahoo.co.jp/

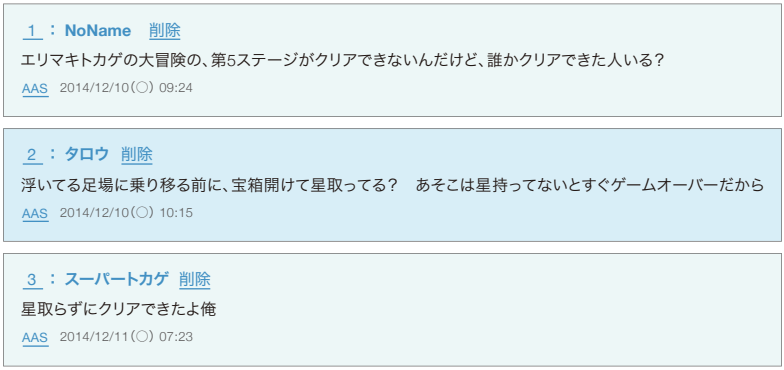


図5-4　電子掲示板のイメージ

5-6 SNSのしくみ

「SNS（エスエヌエス）」（Social Networking Service）は、ユーザー同士が交流できるWebサイトの会員制サービスです。SNSには、メッセージ機能のほか日記機能、リアルタイムで会話できるチャット機能、特定の仲間だけで情報交換するグループ機能、ホームページ作成機能など、多彩な機能があります。

SNSはパソコン、携帯電話、スマートフォンなどさまざまな通信機器で利用できる身近で便利なコミュニケーションツールとして、老若男女を問わず広まってきました。

友人同士のつながりといった小規模な利用から、地域の情報コミュニティー、同じ趣味を持つ人同士など、それぞれの会話や情報共有に使われています（**図5-5**）。ほかにも、企業や地方公共団体が広報やマーケティングツールのひとつとして利用するケースも増えています。

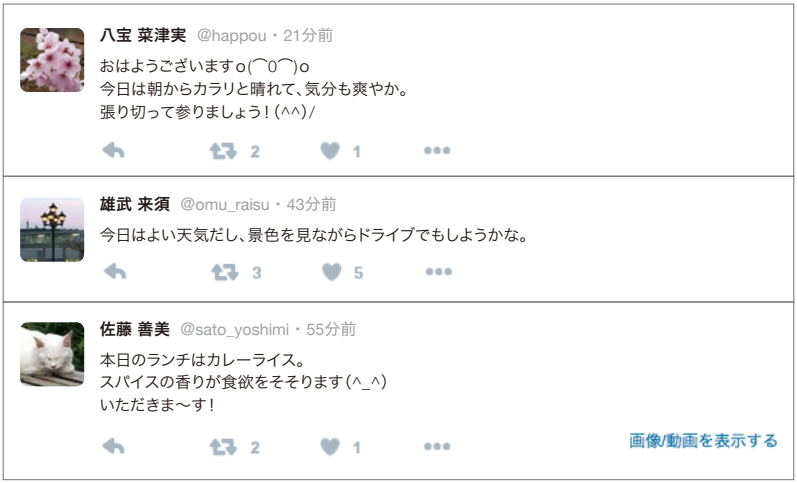


図5-5 SNSのイメージ

その手軽さで急速に広まった反面、SNSに関わるトラブルも増えています。たとえば、

- アカウントの不正利用
- 知り合い同士の空間であるという安心感を悪用した詐欺
- コンピュータウイルス配布の対象となる
- 友人間のコミュニケーションを目的にSNSを利用したが、プライバシー設定が不十分で投稿や写真が広範囲に流出して炎上する

・軽い気持ちで書き込んだメッセージが友達のプライバシーを侵害する
などの被害やトラブルが頻発しています。

SNSを利用するときは、どんなに限られた狭い範囲での会話であっても、インターネット上に情報発信していることを念頭に置き、書き込む内容に十分に注意を払うことが大切です。

[代表的なSNS]

- Twitter　https://twitter.com/?lang=ja
- Facebook　https://ja-jp.facebook.com/
- LINE　http://line.me/ja/

5-7 ネットショッピングとは

「ネットショッピング」とは、インターネット上で買い物をすることです。

ネットショッピングのWebサイトは、Webサーバーとデータベースサーバーが連携して作動しています。データベースサーバーには、顧客情報、商品情報、在庫情報、販売情報などのデータがあり、ユーザーの入力情報がリアルタイムにデータベースに書き込まれて更新されるしくみです（**図5-6**）。

図5-6　ネットショッピングサイトのイメージ

24時間、いつでもどこでも手軽に買い物を楽しめるネットショッピングは、急速に普及しています。ネットショッピングのサイトが集合して大型化した「ショッピングモール」や、企業が

提供するサービスを利用して個人で開設・運営するショッピングサイトも増えています。

[代表的なショッピングサイト]

- Amazon　http://www.amazon.co.jp/
- Yahoo!ショッピング　http://shopping.yahoo.co.jp/

5-8 ネットオークションとは

「ネットオークション」とは、インターネットを利用した電子商取引のひとつで、ネット上で競売（オークション）を行うことです。オークション専用サイトに出品された商品の中から、気に入った物を自分の指定した金額で購入できます。一般的に、オークションサイトでは開始価格が表示されており、その価格よりも高い金額で入札（購入意思を示すこと）を行い、最も高い金額を提示した人が落札（購入）できるしくみです（**図5-7**）。

個人の出品もできるようになり、ネットオークションはフリーマーケットに代わる新たな場として利用者が増えています。しかし、ネットオークションは、実店舗での購入とは異なり実際の商品の確認がしづらく、販売者の顔も見えないため、消費者トラブルに巻き込まれるケースが増えています。盗品や違法薬物の出品、偽ブランド品の販売、商品を送らずに代金をだまし取る詐欺行為のほか、利用者同士の販売上のトラブルも発生しています。

ネットオークションを安全に利用するために、以下のことに気をつけましょう。

! 出品者の過去の取引実績を確認する

過去の取引実績がないにもかかわらず、同時に大量の商品を出品している場合などは特に注意が必要です。

! 取引相手の情報を確認する

実際に入金したり、商品を送付したりする前に、取引相手の氏名、メールアドレス以外の連絡先（住所、電話番号）を確認しておきましょう。

! 取引の履歴を残しておく

万が一のトラブル発生に備えて、受発信した電子メール、銀行振込の控え、宅配便の伝票などの証拠を保存しておきましょう。

! 支払いの方法などを工夫する

購入者が商品の到着後に内容物の確認をしてから宅配業者に代金を支払う代引きサービスなどもあります。手数料はかかりますが、これらのサービスを活用するのも取引のトラブルを回避する対策のひとつです。

図5-7　オークションサイトのイメージ

5-9 スマートフォンの基礎知識

「スマートフォン」は、従来の携帯電話（フィーチャーフォン。ガラパゴス携帯〈ガラケー〉ともいう）に比べると、パソコンに近い性質をもつ通信機器です。大きな画面でパソコン向けのWebサイトや動画を閲覧でき、タッチパネルの操作で画面拡大やスクロールなどを直感的に行うことができます（**図5-8**）。

図5-8　スマートフォン

フィーチャーフォンは、電話やメールの受発信としての利用が中心だったのに対し、スマートフォンなら外出先でも豊富な情報を得ることができ、操作が簡便であることから、年々利用者数が増えています。

スマートフォンの長所と短所

長所	短所
・パソコンのファイルを閲覧できる。 ・Webサイトを閲覧できる。 ・タッチパネルによる直感的な操作が可能である。 ・アプリケーションを追加できる。	・フィーチャーフォンと比べて、バッテリーの消費が速い。 ・インターネットに常時接続するため使用料金が高くなる。 ・スマートフォン内のアドレス帳や画像ファイルを流出させる悪意のあるアプリケーションが存在する。

携帯電話やスマートフォンはいつでもどこでも利用できて便利ですが、TPO（時・場所・場面）を考慮して使用しなければ、周囲の人に迷惑をかけてしまうおそれがあります。

自宅で携帯電話やスマートフォンを使用する場合には、利用マナーやルールを意識することはあまりないかもしれません。しかし、公共の場で用いるときには、TPOに合わせてルールやマナーを守ることが大切です。

たとえば、携帯電話やスマートフォンは、使用する場所に応じたモード設定が可能です。映画館や電車内など着信音を鳴らしたくないときには「マナーモード」、飛行機に搭乗したときは、通信機能をオフにして航空安全基準に従って使用できる「機内モード」に設定します。また、場所によっては電源をオフにするなど、常に周囲への思いやりを忘れずに使うように心がけましょう。

次の場所でのルール、マナーを確認しておきましょう。

新幹線、電車、バス内で

鉄道会社やバス会社では、優先席付近では携帯電話の電源を切るようにルールが設定されています（**図5-9**）。車内では各会社のルールに従い、周りの乗客の静寂を乱さないように注意します。

図5-9　電車内の優先席に貼られているシールの例

飛行機内で

携帯電話やスマートフォンの電波は、飛行機を構成する機器に影響して誤作動を招く可能性があります。そのため、機内での使用は各航空会社のルールに従うようにします。

歩行時に

通話しながら、あるいはスマートフォンの画面を見ながら歩行する「歩きスマホ」によって、駅ホームや階段から転倒したり、他者と接触したりする事故が増えています。他者を巻き込んだ大きな事故に発展する危険性があるので、「歩きスマホ」は絶対にやめましょう。

運転時に

自転車や自動車の運転中に携帯電話やスマートフォンを保持した状態で使用することは、道路交通法の罰則対象となる違反行為です。絶対に使わないようにしましょう（ただし、傷病者の救護、または公共の安全の維持など、やむを得ない場合は対象外となります）。

レストランやホテルのロビーで

レストランやホテルのロビーなど人が集まる静粛な場所や公共の場では、マナーモードに設定する、周囲の迷惑にならないよう声のトーンを抑えて通話するなどが基本マナーです。大声で会話したり、長い時間通話したりすることは控えましょう。

位置情報を利用したゲームに関する注意喚起

位置情報を利用したゲームについて、内閣サイバーセキュリティーセンター（http://www.nisc.go.jp/）より、「個人情報を守ろう」「偽アプリ、チートツール注意」「お天気アプリは必ず入れよう」「熱中症を警戒しよう」「予備の電池を持とう」「予備の連絡手段を準備しよう」「危険な場所に入らない」「会おうという人を警戒しよう」「歩きスマホは×ですよ」と、注意喚起に関する資料が公開されています。

屋外を移動しながらプレイする必要があるこれらのゲーム、ルールやマナーを守って楽しみましょう。

5-10 無線LANとWi-Fiの基礎知識

「**Wi-Fi**（ワイファイ）」とは、無線LANの代表的な呼び名で、電波でデータの送受信を行う通信網をさします。通常、会社や家庭内でパソコンやプリンタで通信する場合、機器同士をネットワークケーブルで接続します。このケーブルの代わりに無線通信で接続するのが**無線LAN**です。

無線LANの利用には、親機（アクセスポイント）と、パソコンなどに装着する子機が必要です。最近はノートパソコンやスマートフォンに子機の機能が内蔵されており、駅や空港などの公共施設、ファストフード店などが親機を設置して公衆無線LANサービスの提供を進めており、外出先でも手軽に無線LANが利用できる環境が広がっています。

無線LANは簡単にインターネットに接続できて便利ですが、利用者が適切なセキュリティ対策を取らずにいると、気がつかないうちに情報が盗み見られたり、コンピュータウイルスの配布などに悪用されたりすることがあります。

無線LANを利用するときは以下のことに気をつけましょう。

SSL（https://～）を利用する

「SSL（エスエスエル）」は、インターネット上で通信を暗号化する技術で、パソコンとサーバーの間でやりとりする通信データを暗号化して第三者によるデータの改ざんや盗聴を防ぎます。「http」の後ろに「s」のついた、「https://～」というURLがSSL認証を受けたホームページです（**図5-10**）。

図5-10 無線LANのセキュリティ

ファイル共有機能を解除する

クラウド（5-11 参照）などによるファイル共有機能は、不正なアクセスによってデータが盗み見られたり、流出したりする危険性があります。無線LANを使うときは、共有機能を解除しておくと安心です。

親機と子機に適切な暗号を設定する

無線LANアクセスポイント（親機）と無線LAN端末（子機）に暗号を設定しておくと、親機と子機の暗号化キーが一致した場合のみ通信が可能となり、親機と子機で送受信される無線通信データは暗号化して保護されるため、盗み見られるなどのリスクを軽減できます。

5-11 クラウドサービスとは

「クラウドサービス」は、コンピュータで利用するデータやソフトウェアを、インターネット経由でユーザーに提供するサービスのことです。

従来、コンピュータのハードウェア、ソフトウェア、データなどは、会社や自宅でユーザー自身が管理する形式でした。それに対し、クラウドシステムでは、ユーザーはネットワーク上のサーバー群（クラウド。「雲」を意味する）にあるデータ類を利用します。

自分のコンピュータにデータを保存しておかなくても、クラウドで保存・管理しておけば、インターネットにつながる限り、どこからでも、どのコンピュータからでも、クラウドにあるデータが取り出せます（**図5-11**）。

データを管理するためのシステム構築やシステム管理にかかる手間がないため、業務の効率化やコストダウンを図れるのもクラウドサービスの利点といえるでしょう。

クラウドサービスを利用する際は、データが事業者側のサーバーに保管されること、インターネットを介してデータがやりとりされることを念頭に置き、十分なセキュリティ対策が施されたクラウドサービスを選択することが重要です。

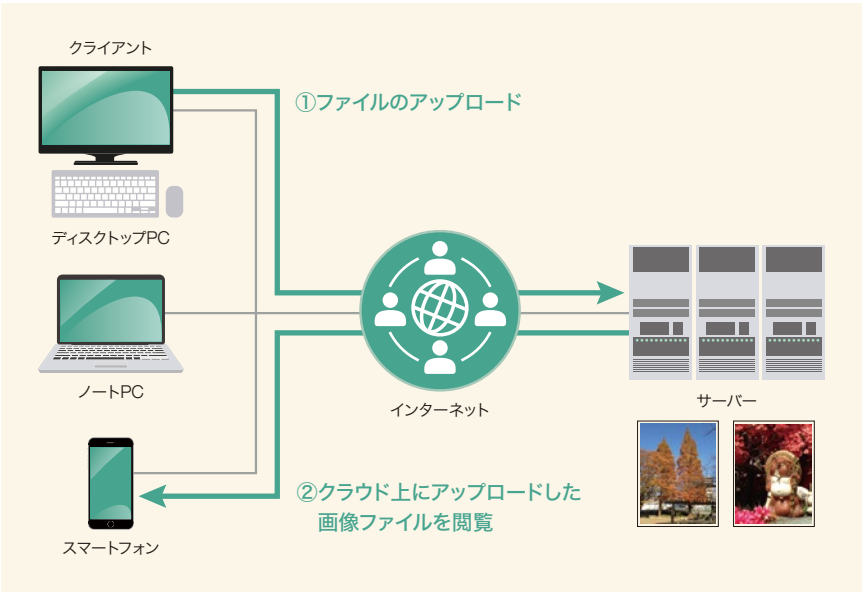


図5-11 クラウドサービスの例（ファイルの共有）

第6章
コンピュータウイルス

6-1 マルウェアとは

「**マルウェア**」(malware) は、不正あるいは有害な動作を行う意図で作成された、悪意のあるソフトウェアやプログラムの総称です。マルウェアという語は、「malicious (悪意のある)」と「software」を組み合わせてできた造語です。

[マルウェアの例]

コンピュータウイルス (computer virus)

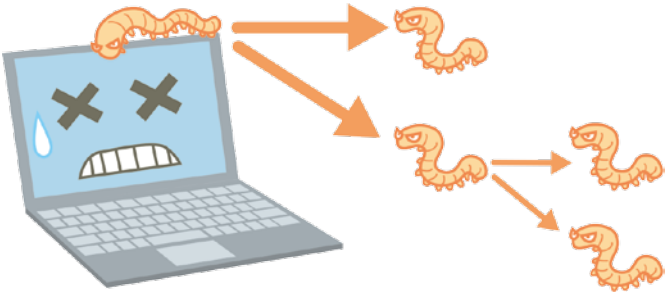
「**コンピュータウイルス**」は、他のファイルやソフトウェアに寄生して不正や有害な動作を行います。

コンピュータがコンピュータウイルスに感染すると、ハードディスクに保管されているファイルが消去されたり、コンピュータを起動できないようにされたりと、さまざまな被害を受けます。

ワーム (worm)

「**ワーム**」は、コンピュータウイルスのようにファイルやソフトウェアに寄生するのではなく、単独で実行可能で、自ら複製して感染を広げる (自己増殖)、悪意のあるプログラムです。ネットワークを介して、攻撃先のシステムの**セキュリティホール** (**脆弱性**。安全性をおびやかす弱い部分) を悪用して侵入するケースが多く見られます。

コンピュータがワームに感染すると、コンピュータ内のファイルが破壊されたり、ハードディスクがフォーマット（初期化）されたり、さまざまな被害が発生します。



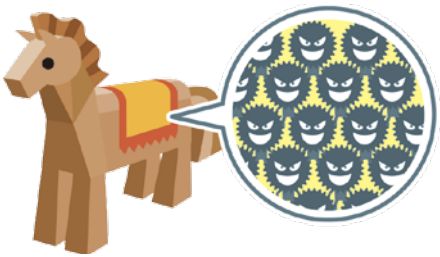
トロイの木馬（Trojan horse）

「**トロイの木馬**」は、他のプログラムに紛れ込んで侵入し、ユーザーの知らない間に不正な行為を行うプログラムです。ファイルやソフトウェアに寄生するのではなく、単独で実行可能ですが、自己増殖機能はありません。ギリシア神話に出てくる「トロイの木馬」のように、危険ではないように見せかけていることから名付けられました。

コンピュータがトロイの木馬に感染すると、ネット接続の設定や、ファイヤーウォールシステム（インターネットからの不正な侵入を防ぐシステム）の設定などを変更し、攻撃者が被害者のパソコンを乗っ取ってさまざまな被害をもたらします。たとえば、

・キーロギング（キーボードで入力した情報を盗み取ること）
・プログラムの追加／削除
・ファイルの追加／削除
・アンチウイルスソフトの無効化
・被害者のデスクトップ画面の撮影
・パスワードの奪取
・Webから悪意あるプログラムをダウンロード

などです。



スパイウェア（spyware）

「**スパイウェア**」は、ユーザーの意図に反してインストールされ、ユーザーに気付かれないように活動します。何らかのソフトウェア内に混入していることが多く、PC内のデータやWebサイトの訪問履歴などのユーザーに関する情報を、ユーザーの知らないうちに抜き取ったりします。

代表的なスパイウェアには次のものがあります。

キーロガー（key logger）

「**キーロガー**」は、ユーザーがキーボード入力した内容を記録するプログラムです。悪意をもった第三者が、キーロガーがインストールされたコンピュータで入力したパスワードなどの情報を不正に取得したりするケースがあります（**図6-1**）。

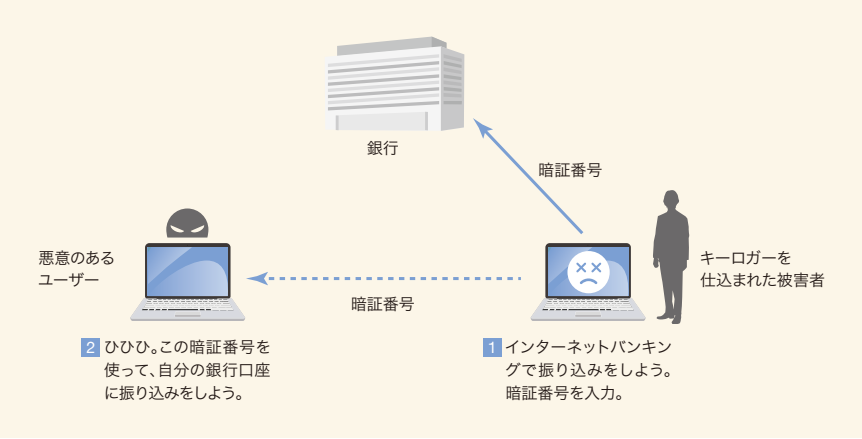


図6-1 キーロガー

バックドア（back door）

「**バックドア**」は、コンピュータに進入する目的で仕掛けられたプログラムです。バックドアが仕掛けられたコンピュータは遠隔操作されたりする場合があります。

ボット（bot）

「**ボット**」は、コンピュータを、ネットワークを通じて外部から遠隔操作する目的で作成されたプログラムです。ボットに感染すると、ユーザーは知らないうちに悪意のあるユーザーに加担する攻撃者となり、他者のコンピュータに対してスパムメール（不要な広告など、迷惑なメッセージを多数の受信者に大量に送信するメール）を送信するなど、さまざまな攻撃活動を行います（**図6-2**）。

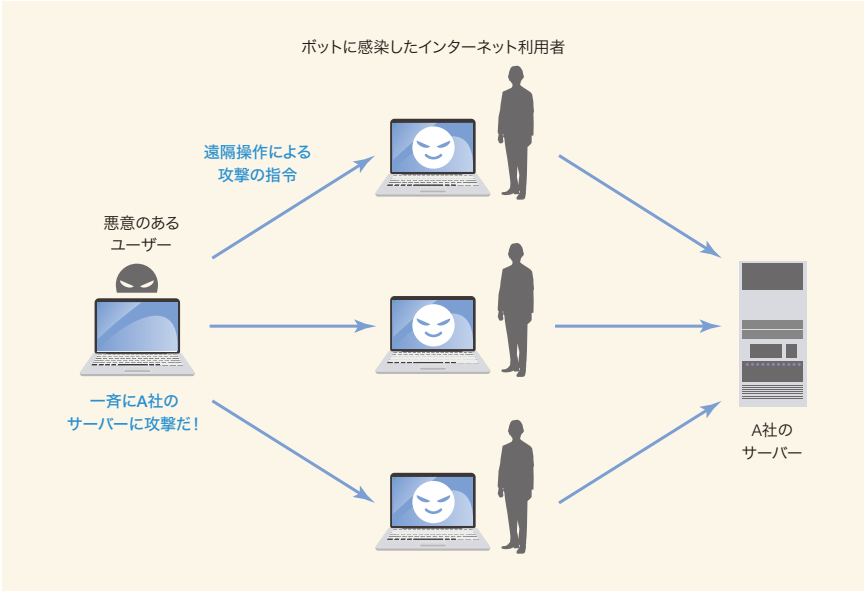


図6-2 ボット

ランサムウェア（ransomware）

「**ランサムウェア**」とは、ユーザーのコンピュータ内にある情報やデータを人質（アクセスを制限）し、この制限を解除するために身代金（ランサム）を要求するというプログラムです。アクセス制限の手段として、ハードディスクドライブの強制的な暗号化やシステムを使用不能にするなどの種類があります。

6-2 コンピュータウイルスの感染経路

コンピュータウイルスは、ユーザーの操作を利用してコンピュータに入り込み、感染します。たとえば、

・コンピュータウイルスが含まれるファイルを開いたり、実行したりする
・コンピュータウイルスが含まれる電子メール添付ファイルを開く
・悪質なホームページの閲覧
・インターネットへの接続

などの操作によって感染します。

コンピュータウイルスは、他人から借りたCD/DVDメディアやUSBメモリ内、インター

ネットからダウンロードしたファイル内、電子メールの添付ファイルに潜んでいることもあります。それらのファイルを開くことで、コンピュータがコンピュータウイルスに感染するのです。ファイルを開かせるために、ユーザーの気を引くようなファイル名になっていたり、ファイルのアイコンを偽造したりしている場合があるので、不審なファイルは開かないなど十分に気をつけるようにしましょう。

また、ネットワークに接続しているコンピュータに対し、脆弱性のあるコンピュータを探してウイルス感染したファイルを送り込む場合もあります。脆弱性を解消していないと、ホームページを閲覧するだけで感染する危険もあるので注意が必要です。

6-3 コンピュータウイルス感染を防ぐには

コンピュータウイルスに感染しないためには、基本的に次の対策が必要です。

利用しているソフトウェアを最新のものに更新する

ソフトウェアのメーカー各社は、ソフトウェアにおけるウイルス対策を強化しています。新しいバージョンにアップグレードすることで、プログラムの弱点（脆弱性）を改善したものを利用できます。

利用しているオペレーティングシステムをアップデートする

Microsoft社のWindowsに関しては、Windows Updateを行い、常に最新の状態にしておくと、Windowsの脆弱性を取り除くことができます。

ウイルス対策ソフトを導入する

使用するコンピュータには、必ずウイルス対策ソフトを導入しましょう。また、その際、常に最新のウイルスに対応できるように、ウイルス対策ソフトのウイルス検知用データも更新することが大切です。

怪しいホームページやメールに注意する

ウイルスは悪意のあるホームページで配布されていたり、メールに添付されたりなど、さまざまな経路でコンピュータに侵入してきます。悪意のあるホームページに接続する可能性のある迷惑メールや掲示板内などのリンクに注意するほか、不審なメールの添付ファイルを開かないなどの対策が必要です。SNSなどで用いられる短縮URLが、悪性ホームページなどへの誘導に使われる例も出てきているので注意しましょう。

第7章 インターネットセキュリティ

7-1 ユーザー認証の必要性

インターネットでは、「**認証**」（authentication）という方法で、通信している相手が本人かどうかを確認します。しかし、物理的な距離が離れている相手が、本当に本人であるかどうかは、実際に目で見て確認するわけではないので分かりません。そこで、「ユーザー認証」という仕組みが使われています。

ユーザー認証は、IDとパスワードなどの本人しか知らない情報を組み合わせた「アカウント情報」を用いて行われます。「ID」とは、一人ひとりのユーザーを区別するために割り振る文字列です。「パスワード」とは、そのIDを割り振られた本人だけが知り得る情報であり、それを入力することでIDを持つ本人であることが確認できます。

IDとパスワードを入力して、情報機器やインターネットサービスの利用を開始することを「ログイン」、利用を終了して機器やサービスから離れることを「ログアウト」といいます。

7-2 パスワードの管理方法

パスワードは、本人しか知り得ない重要な情報です。その為、パスワードが第三者に知られてしまうと、本人以外の人がその人になりすまして、インターネット上の様々なサービスを勝手に使用することができてしまいます。場合によっては、巨額の被害を受けてしまうかもしれません。その為、パスワードは絶対に他人に漏洩することがないよう、推測しづらい数値や文字列の羅列と利用可能な記号なども用いた複雑な文字列で作成するようにしましょう。

また、いくら複雑なパスワードを設定したとはいえ、そのパスワードそのものを自分が忘れてしまうリスクも発生します。メモ帳やPC内のテキストファイル、パスワード管理アプリなど、管理方法も様々にありますが、そうした管理方法がセキュリティ的に問題無いのかも含めてしっかり意識し、管理することが大切です。

7-3 生体認証

バイオメトリクス認証とも言われており、人間の身体的特徴を認証に用いる技術を言います。指紋や瞳の虹彩などがよく用いられています。パスワードの入力だけでなく、忘却や紛失などのリスクも解決できるというメリットがあります。しかし、身体的特徴は任意に更新することができないため、何らかの方法で生体認証情報の複製を作られてしまうと、以降、その認証方法を用いた全てに対して、利用できなくなってしまうというデメリットがあります。

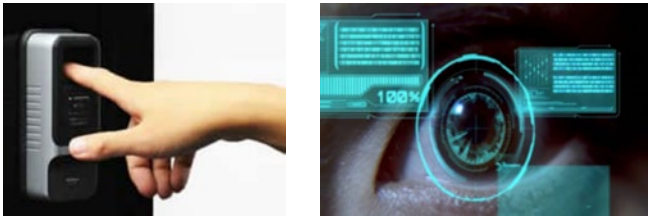


図7-1 指紋認証・虹彩認証

7-4 暗号化の必要性

「**暗号化**」(encryption)とは、データの内容を他人にはわからなくするための技術です。データを暗号データにする作業を「暗号化」、暗号データを元データに戻すことを「復号」(decryption)といい、暗号化は「鍵」(キー、key)と呼ばれる特殊なデータを使用して行われます。

もしもパスワードがそのままの文字列で保存されていたら、第三者に簡単にパスワードを抜き取られてしまう危険があります。それを防ぐために、パスワードは通常、第三者の理解できない暗号化されたデータで、コンピュータに保存する必要があります。

7-5 代表的な暗号化技術

「**SSL**」(Secure Sockets Layer) とは、インターネット上でデータを暗号化して送受信するしくみのひとつです。クレジットカード番号や個人情報を取り扱うWebサイトで、情報の改ざんや情報の盗み取りを防止するために広く利用されています。また、SSLは暗号化に加え、電子証明書により通信相手が本人であることを証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。

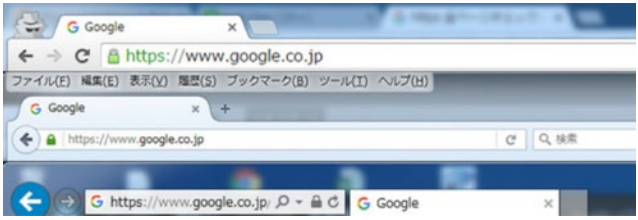


図7-2 ブラウザのアドレスバー

SSLを使ったサイトに接続するには、一般的な「http://」で始まるアドレスではなく、「https://」で始まるアドレスのサイトに接続します。また、SSLを利用したサイトに接続すると、アドレスバーの色が緑色に変わったり錠のマークが表示されたりします。

図7-3 SSLサイト鍵マーク

これらにより、SSL通信を使っているサイトかどうかを確認することができます。Webブラウザの種類やバージョンによっては、他の場所に保護を示すマークが表示されることもあるので、普段利用しているWebブラウザのどこに、どのようなマークが出るかをあらかじめ確認しておくとよいでしょう。

SSLによる暗号化の具体例として、たとえばインターネットバンキングで利用者登録する場合にもSSLを使ったホームページが使われています。入力された情報は暗号化されて金融機関のWebサーバーに送られ、通信の途中で情報が盗み見られることを防いでいるのです。

図7-4 SSLによる暗号化

7-6 電子証明書

「**電子証明書**」(Electronic certificate)とは、間違いなく本人であるということを証明す

るために、電子的に発行してもらう証明書のことです。信頼できる第三者機関（認証局）に依頼し、高度な暗号化技術に基づいて発行してもらいます。ウェブサイト向けに発行されるサーバー証明書、パソコンやスマートフォンなどのデバイス向けに発行されるデバイス証明書、個人や組織向けに発行されるクライアント証明書などの種類があります。

現実世界には、運転免許証や印鑑証明書、パスポートなどの身分証明書がありますが、インターネット世界においては、この電子証明書が身分証明書にあたります。その為、本人確認の認証や、本人以外からのアクセスを制御することなどができ、盗聴・改ざん・なりすまし・事後否認の防止に役立ちます。

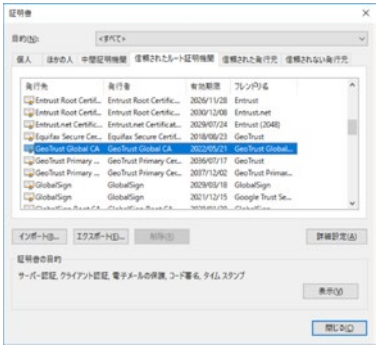


図7-5 ブラウザソフトでの電子証明書確認画面例

7-7 フィルタリング（有害サイトアクセス制限）

「**フィルタリング**」（filtering）とは、アダルトサイトや薬物・犯罪に関するサイトなどのいわゆる有害サイトをユーザーに見せないようにする仕組みのことです。専用のソフトウェアやサービスなどを用いることでWebサイトをふるいにかけ、不必要な情報を排除することができます。

青少年保護の目的が主ですが、そもそも有害サイトを閲覧することはコンピュータウイルスに感染するリスクも高いため、セキュリティ対策の１つとして位置付けられています。

7-8 ファイアウォール

「**ファイアウォール**」（firewall）は、外部のネットワークからの攻撃や不正なアクセスから、自分たちのネットワークやコンピュータを防御するためのソフトウェアやハードウェアの

ことです。

「ファイアウォール」とは本来「防火壁」という意味の言葉で、火災のときに被害を最小限に食い止める役割をすることから、ネットワークやコンピュータを守るものを示すようになりました。

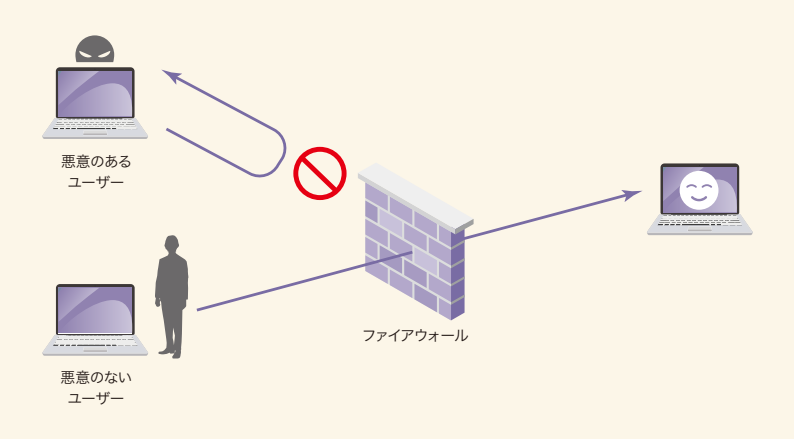


図7-6 ファイアウォール

ファイアウォールは、ネットワーク通信をする際、その通信をさせるかどうかを判断し、許可あるいは拒否するしくみです。通信をどう扱うかの判断は、通信の送信元と宛先の情報でなされ、通信の内容は判断基準にはなりません。

・外部からの不正なパケット（データ通信の際の分割された単位）を遮断する機能
・許可されたパケットだけを通過させる機能

などをもち、ファイアウォールの設置は、外部のネットワークに接続した環境にとって必須の情報セキュリティ対策のひとつです。

7-9 ソーシャル・エンジニアリング

「**ソーシャル・エンジニアリング**」（social engineering）とは、パスワードなどの情報を、コンピュータやネットワークの管理者や利用者などから、会話の最中に巧みに聞きだす、盗み聞く、盗み見るなど、通信技術によらない社会的な方法で入手することです。

技術的にセキュリティを強化しても、付箋にパスワードを書いていたり、電話などでパスワードを話したり、ログインしたままコンピュータから離れたりすれば、ソーシャル・エンジニアリングの対象となってしまいます。

7-10 スキミング

「**スキミング**」(skimming) は、カード犯罪で多く使われる手口のひとつで、磁気カードに書き込まれている情報を抜き出し、まったく同じ情報を持つカードを複製する犯罪です。

スキミングされないようにするための対策として、暗証番号の徹底管理、第三者にカードを渡さない、怪しい店ではカードを利用しない、などが挙げられます。また、仮にスキミングをされてしまったとしても、被害を最小限に抑えるために、カード利用明細の頻繁なチェックや、現金口座を複数に分散させておく、などの対策も挙げられます。

7-11 スマートフォンのセキュリティ対策

最近では、パソコン以上に重要な情報を管理している可能性があるスマートフォン。そのため、セキュリティ対策もパソコン以上に徹底する必要があります。

主なセキュリティ対策を、下記に記します。

- OSやアプリは、常に最新の状態にアップデートする。
- 信頼できる場所以外で、重要な情報の通信やアプリのインストールをしない。
- 「提供元不明のアプリはインストールしない」設定にしておく (Android端末)。
- 不審な「アクセス許可」が無いかを確認する (Android端末)。
- セキュリティ対策ソフト (アプリ) を利用する 。

図7-7 パスコードロック

また、盗難や紛失などスマートフォンそのものを失ってしまった際、被害を最小限に抑えるため、必ず端末にパスコードロックを掛けておきましょう。

平成30年9月 改訂版

一般社団法人 全国専門学校情報教育協会
Institute for Vocational Collage Information Technology Education
〒164-0003　東京都中野区東中野1-57-8　辻沢ビル3F
Tel：03-5332-5081　Fax：03-5332-5083