

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



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 インターネットがもたらす
便利なサービス 6
- 1-4 インターネットの影響力 8



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 9
- 2-2 フィッシング詐欺 10
- 2-3 ワンクリック詐欺 11
- 2-4 詐欺、犯罪に巻き込まれないために 12
- 2-5 インターネットに関連した
新たな犯罪の被害例 13
- 2-6 迷惑メール、チェーンメール 14
- 2-7 健康面への影響 15



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 17
- 3-2 著作権、肖像権、パブリシティ権、
プライバシーの権利 18
- 3-3 違法ダウンロード・違法アップロード 19
- 3-4 名誉毀損 19
- 3-5 わいせつ物頒布 20
- 3-6 特定商取引法 20
- 3-7 ステマ規制(景品表示法) 20
- 3-8 電子契約法 21
- 3-9 不正アクセス禁止法 21
- 3-10 個人情報保護法 21
- 3-11 特定電子メール法 22
- 3-12 知らない人とオフラインで
会うことへの注意 22
- 3-13 インターネット関連法規の改正 23



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 24
- 4-2 Webページを閲覧するうえで
注意すること 25

4-3	個人情報の公開について	26
4-4	不正な嫌がらせや 迷惑行為に遭わないために	26
4-5	プライバシーの保護について	27
4-6	インターネットに アクセスするうえでの心構え	27
4-7	電子メール・チャットツールのマナー	28
4-8	情報の偏り	29



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	30
5-2	Webページのしくみと利用の仕方	31
5-3	電子メールのしくみ	32
5-4	SNSのしくみ	33
5-5	消費者が生み出すメディア	35
5-6	インターネットを利用した買い物	36
5-7	ネットバンキングとは	38
5-8	無線LANとWi-Fiの基礎知識	38
5-9	クラウドサービスとは	40
5-10	インターネット上で利用できる 生成AIについて	41



第6章 コンピュータウイルス

6-1	マルウェアとは	42
6-2	コンピュータウイルスの感染経路	45
6-3	コンピュータウイルス感染を防ぐには	46



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	47
7-2	パスワードの管理方法	47
7-3	パスワードを狙った攻撃	48
7-4	生体認証	48
7-5	暗号化の必要性	49
7-6	電子証明書	49
7-7	フィルタリング (有害サイトアクセス制限)	50
7-8	ソーシャル・エンジニアリング	50
7-9	スキミング	51
7-10	スマートフォンのセキュリティ対策	51
7-11	多要素認証	52



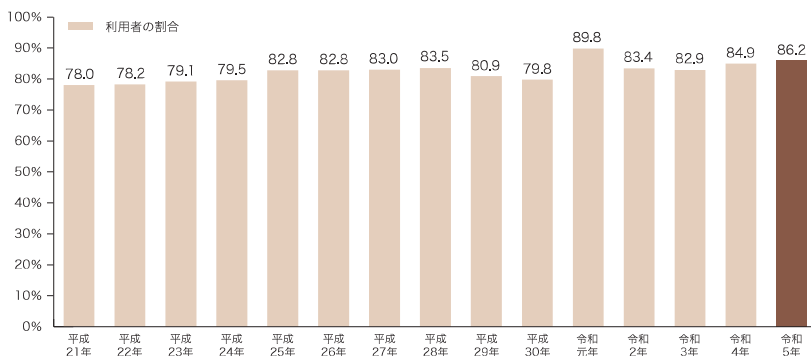
第1章 インターネットの基礎

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し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。インターネット接続状態のことをオンラインといい、それに対して、インターネットに接続していない状態のことをオフラインといいます。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やオンラインサービス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「通信利用動向調査」

図1-1 インターネット利用率(個人)の推移

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。

LANとは、「Local Area Network」の頭文字をとったもので、小規模な単位で構成されるネットワークのことを言います。一方、WANは「Wide Area Network」の頭文字で、「広域通信網」のことを言います。複数の都道府県をまたぐような地理的に離れた場所にあるLANをプロバイダーが保有している回線を利用して、広範囲のネットワークを構築する仕組みです。

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

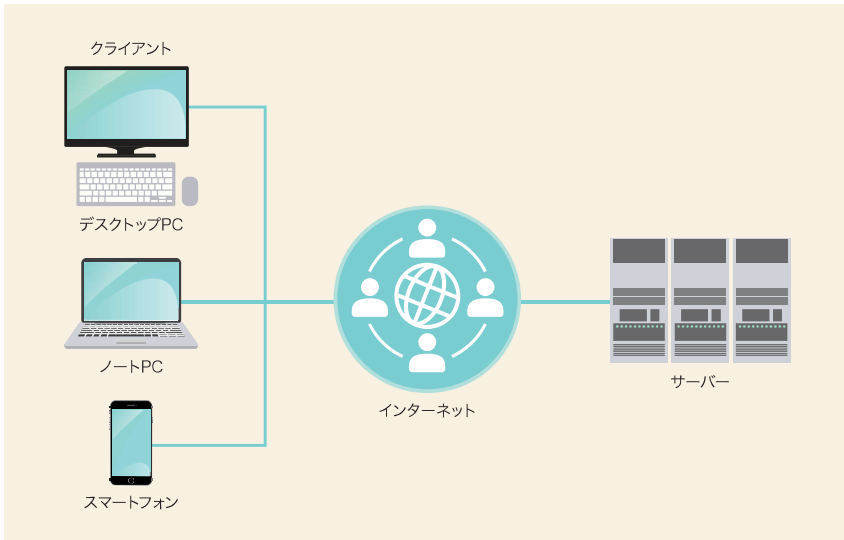


図1-2 クライアントとサーバー

1-3 インターネットがもたらす便利なサービス

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、SNSや電子掲示板、ブログ、投稿サイト、情報共有サイトなどのソーシャルメディアにおける意見の発信など、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 (EC) ・ 電子決済

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 (EC)」ができます。商品の検索から購入までをおこなうオンラインショッピングのほか、店を構えなくても物品の販売、フリーマーケットへの参加も可能です。また、現金を使わずに電子的なデータの送受信によって決済をおこなう電子決済 (キャッシュレス決済) は、コンビニなどの実店舗やインターネット上のECサイトなどで利用されています。

ECとは「electronic commerce」の頭文字から来ており、「電子商取引」のことを言います。

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 IoT (Internet of Things)

さまざまなモノ (センサー機器、駆動装置 (アクチュエーター)、住宅・建物、車、家電製品、電子機器など) が、インターネットを通じて接続され、相互に情報交換をする仕組みを指します。スマートフォンアプリや音声アシストと連携して接続された機器を操作することができます。IoTに対応した家電をスマート家電と言い、食材の在庫管理やレシピ提案をおこなう冷蔵庫や、部屋の温度を自動的に調整するエアコンなどがあります。

6 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ができないときに、多くの人がTwitter（現X）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活かされた好例といえるでしょう。

また、2019年末からの新型コロナウイルスの感染拡大にともない、自宅にいながらビデオ会議ツールを用いて仕事をするリモートワーク（テレワーク）や授業を受けるオンライン授業など、新しい形のオンラインサービス利用が、一気に拡大しました。

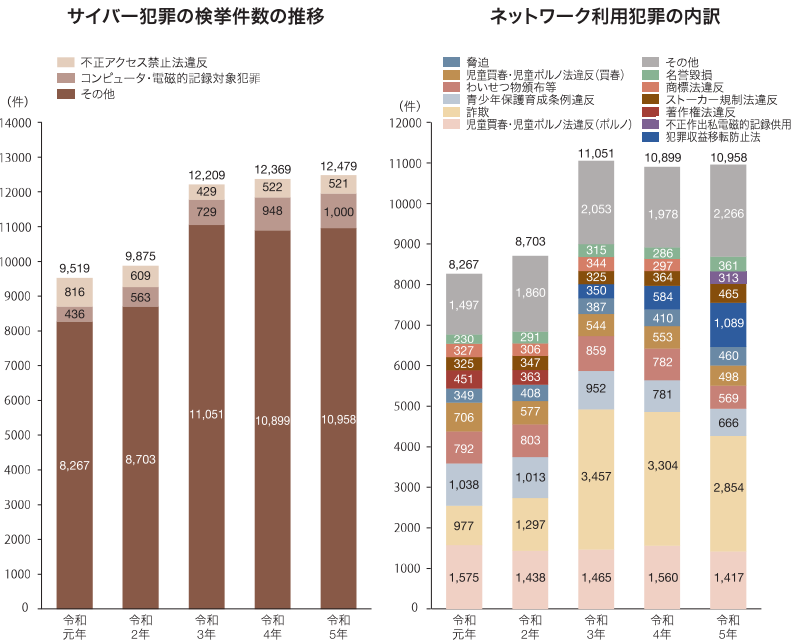
1-4 インターネットの影響力

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)。

また、誤情報が大量に拡散し、社会に混乱を招くインフォデミック現象も増加しています。特に、パンデミックや災害時においては、虚偽の情報が人々の不安を煽り、適切な対応が遅れる原因となります。ソーシャルメディアのプラットフォーム側も、誤情報の検出と削除に取り組む必要がありますが、個人としても、情報の真偽を確認し、不確かな情報を拡散しないよう心がけることが求められます。

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『令和元年～5年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犯罪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
 - 例：個人情報抜き取る目的で、宅配業者や公的機関を装ったSMSやメッセージが送られる
- ・ 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
- ・ 情報の漏えい^{ろうえい}※1
 - 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
- ・ 誹謗中傷^{ひぼう}※2
 - 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

※1 漏えい：秘密などがもれること。または、もらすこと。

※2 誹謗中傷：根拠のない悪口を言いふらして、他人を傷つけること

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^{※3}で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Web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。例えば、偽ECサイトは、実際のショッピングサイトに似せて作られた詐欺サイトで、購入手続きをおこなう際に個人情報を窃取^{せつしゆ}します。安全なショッピングのためには、URLが正式なものか確認し、不審な低価格の商品には特に注意が必要です。

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。

※3 なりすまし：氏名や生年月日などの個人情報を不正に手に入れ、その人の振りをして、金品をだまし取ったりすること

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、利用者を騙し、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。
- ・意図的に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、携帯電話の個人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、まるで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。

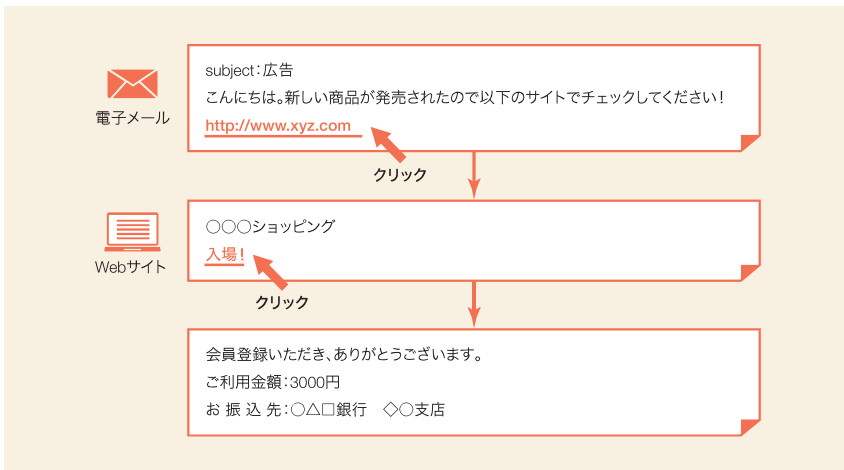


図2-1 ワンクリック詐欺の手口の例

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。

！ 事前確認を十分におこなう

利用規約を長文にしたり、Webブラウザで見えにくい表示に細工して、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しっかり読むなど、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

Web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サイトも増えていきます。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犯罪の被害例

詐欺師や犯罪者グループは、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：闇バイト】

SNSで簡単に高収入が得られると誘われ、実際には振り込め詐欺の手助けや薬物の運び屋などの犯罪行為を強要されるケースがあります。被害者は犯罪に加担してしまい、逮捕や重い罰則を受けるリスクが高まります。そもそも、実際に報酬が支払われず、逆に多額の借金を負わされる詐欺もあります。

高収入の求人飛びつかず、仕事内容や雇用条件を十分に確認し、信頼できる情報源からの求人を選ぶことが重要です。安全を最優先に考え、怪しい誘いには絶対に応じないようにしましょう。

【事例：SNS乗っ取り】

フィッシングメールや偽のログインページを使ってパスワードを盗まれ、その結果、SNSアカウントが乗っ取られて悪用されるケースがあります。乗っ取られたアカウントは、詐欺メッセージの送信や個人情報の漏えい、なりすましなどに利用され、友人や家族に被害を及ぼす可能性もあります。

これを防ぐためには、強固なパスワードを設定し、二段階認証を有効にすることが重要です。また、怪しいリンクや不審なメッセージには絶対に応じず、公式サイトからの連絡のみを信用するようにしましょう。定期的にパスワードを変更し、自分のアカウントを守る意識を持ちましょう。

【事例：ディープフェイク詐欺】

有名人や知人の顔や声を偽装して金銭を要求する動画を作成し、被害者に送信することで騙すケースがあります。これを防ぐためには、不審な要求があった場合には直接本人に確認し、動画や音声だけで判断しないことが重要です。また、ディープフェイク技術の存在を周知し、怪しい内容には慎重に対応することが求められます。

また、インターネット犯罪は、下記の事由によりビジネス化が進んでいます。

- ・匿名性と技術の進化による手法の高度化
- ・国際的な犯罪組織による詐欺や攻撃の大規模化
- ・低リスクで高リターンの経済的動機の増加

こうした状況に対抗するため、セキュリティ意識の向上や技術的な対策、法的・政策的対策や監視による違法活動の予防など、個人・企業・政府が一体となった総合的な対策が求められています。

❗ もし、被害にあったら？

インターネット犯罪に巻き込まれた際の連絡先や相談先は以下の通りです。

• サイバー犯罪全般

詐欺、脅迫、名誉毀損、不正アクセスなど、サイバー犯罪全般の被害は、最寄りの警察署や各都道府県警察本部のサイバー犯罪対策課に相談しましょう。

• 違法・有害情報

詐欺サイト、児童ポルノ、著作権侵害など、違法・有害情報に関する被害は、インターネット・ホットラインセンター (<https://www.internethotline.jp/>) に通報しましょう。

• 詐欺や購入トラブル

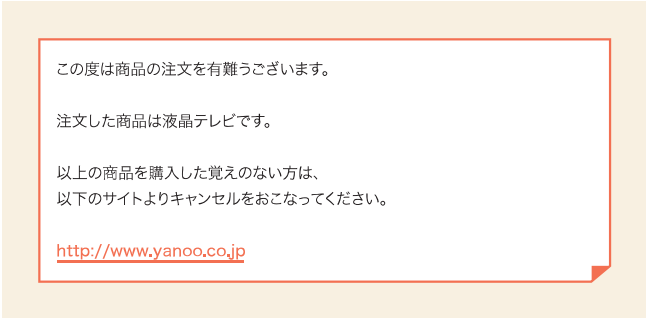
インターネットを利用した詐欺や購入トラブルに関する被害は、消費者庁 消費者相談窓口 (消費者ホットライン188番) に相談しましょう。

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)。



この度は商品の注文を有難うございます。

注文した商品は液晶テレビです。

以上の商品を購入した覚えのない方は、
以下のサイトよりキャンセルをおこなってください。

<http://www.yanoo.co.jp>

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きたすことも多く、問題となっています。

時間を決めてゲームをするといった日ごろの心がけ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おこなう先には、よい作品が生まれず、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、Web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Webページなどでは、「使用する場合に権利者に許諾を求めない必要がある」と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、プライバシーの権利

著作権

「著作権」とは知的財産権のひとつで、創作者（著作者）が自分の創作した作品（著作物）に対して持つ権利です。創作した人がその作品の使用や利用方法をコントロールするために法的保護をします。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、情報を発信するには十分に注意しましょう。

著作権で保護される著作物は、個人が創作的に表現したものであり、文芸、学術、美術、音楽などの分野に該当するものです。具体的には、小説や詩、論文などの文章、音楽や歌詞、映像や動画、写真やイラスト、コンピュータプログラムのようなものが著作物と見なされます（図3-1）。

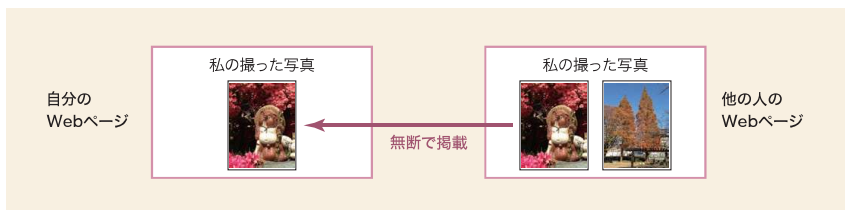


図3-1 著作権侵害の例

以前は、著作権侵害は、著作権者が訴えを起こさない限り、侵害行為は刑事訴追されないという親告罪でしたが、法改正により、特定の著作権侵害行為については、著作権者の告訴がなくても刑事訴追が可能となりました。これにより、悪質な著作権侵害行為に対して、迅速かつ厳格な対応が可能となりました。

また、インターネット配信や放送などを通じて著作物を公衆に送信する権利（公衆送信権、著作権の一部）がありますが、同時に、無許可の配信を禁止するための権利としても機能しています。

この様に、著作権者の権利が適切に保護され、不正利用に対する対策が強化されています。同様に知的財産権のひとつとして、物品の形状、模様、もしくは色彩など、商品の外観デザインを保護する権利として、「意匠権」があります。工業上利用することができる意匠を対象としており、基本的には量産品が対象となります。「意匠権」を含め、「特許権」、「実用新案権」、「商標権」の4つを産業財産権といい、創作者や企業が自らの創作物やブランドを守り、市場での競争力を高めるために重要な役割を果たしています。

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。

プライバシーの権利

個人情報に不当に公開・利用されることから保護される権利で、個人の私生活や個人データが他者によって無断で利用・公開されたりすることを防ぐための法的保護です。例えば、個人の住所、電話番号、病歴、財務情報などが含まれます。

3-3 違法ダウンロード・違法アップロード

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。

また、他人の著作物を無断でインターネットに公開することや、ファイル共有サービスにアップロードするなどの行為は、「違法アップロード」と言います。著作権侵害として法的に処罰される可能性があり、著作権者に対する経済的損害を引き起こします。

3-4 名誉毀損

「めいよ きそん名誉毀損」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、インターネットやSNSなど不特定多数の人が認識できるような場所やオンライン上で、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や、事実に基づかない誹謗中傷や侮辱的なコメント、デマの拡散なども、他人の名声を不当に傷つける行為として、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。SNSにわいせつ動画や画像をアップロードすると、「わいせつ物頒布等罪」にあたる可能性があります。合わせて、撮影対象者の同意なく、個人的な性的画像や性的動画を無断で不特定多数の人に公開する嫌がらせのことをリベンジポルノといい、「リベンジポルノ防止法(私事性的画像記録の提供等による被害の防止に関する法律)」により罰せられます。

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。

また、ECサイトにおいては、「最終確認画面ページでの注文内容に関する6条項の表示義務」、「消費者を誤認させる記載の禁止」、「申し込みの撤回、キャンセルを妨げる不実告知の禁止」、「注文に関する取消権の設定」も追加となりました。

これらを遵守していないサイトでの商取引は控えましょう。

3-7 ステマ規制(景品表示法)

ステマ(ステルスマーケティング)規制は、消費者を欺く不正なプロモーション活動を防ぐための法的枠組みを指します。ステマとは、広告であることを隠しておこなわれるマーケ

ティング活動で、消費者に対する信頼を損なうリスクがあります。例えば、有名人やインフルエンサーが広告であることを明示せずに、製品を推薦する行為が含まれます。

ステマ規制は、透明性を確保し、公正な市場環境を維持するために重要です。違反行為には罰則が設けられ、企業や広告主は法令を遵守する必要があります。

3-8 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。

3-9 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。フィッシング詐欺や、違法なアクセス行為とその準備行為等も、違反の対象となります。

3-10 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に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。

また、2020年の改正では、個人データの取り扱い、特に、データ主体の権利が拡充され、企業に対して個人データの利用目的の明示や安全管理措置の徹底が求められるようになりました。

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Web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。

3-11 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。2019年の改正では、迷惑メール対策が強化され、事前の同意なしに送信される広告メールに対する罰則が強化されました。

3-12 知らない人とオフラインで会うことへの注意

青少年インターネット環境整備法は、青少年がインターネットを安全に利用できるよう、フィルタリングの普及促進やインターネット事業者への義務付けを通じて、有害情報の閲覧機会を最小限に抑えることを目指しています。また、出会い系サイト規制法では、18歳未満の利用が禁止されており、2021年の改正により年齢確認の義務が強化されました。

こうした法整備は進んでいるものの、オンラインで知り合った人とオフラインで会う際には、まだ十分な注意が必要です。出会い系サイト関連の事件では、多くの未成年が高額請求や脅迫、個人情報の悪用などの被害に遭っています。知らない人とオフラインで会う際には、予め信頼できる友人や家族に相談し、安全な環境を確保するために会う場所や時間についても細心の注意を払って、自分自身の安全を守るために慎重に行動しましょう。

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います。それに伴い、より規制を強化する様な形で法改正が執りおこなわれています。

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^{ぎよくせきこんこう}※4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、真偽を検証（ファクトチェック）し、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、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。

※4 玉石混交：宝玉と石ころが混じり合っているところから、すぐれたものと劣ったものが区別なく入り混じっていることのため。

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。発信した情報をもとで、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 Webページを閲覧するうえで注意すること

Webブラウザは、Web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Web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、Web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ははらんでいます。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、Web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。

また、デジタルタトゥーと言われるように、インターネット上に一度出回った情報や画像、動画等は、入れ墨のように完全には消えず、将来の自分にとって不利益な情報が半永久的に残り続けてしまうこととなります。ですから、プライバシーの公開は慎重におこなうことが大切です。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おこなってはけません。

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、Web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おこなうようにします。

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お問い合わせのもよいでしょう。

- ・ インターネットホットライン連絡協議会 (<https://www.iajapan.org/hotline/>)
- ・ 違法・有害情報相談センター (<https://ihaho.jp/>)
- ・ 法務省 インターネット人権相談受付窓口 (<https://www.jinken.go.jp/>)

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、発信の方法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、Web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、十分に考えておこなうようにします。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。

Web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ります。

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・チャットツールのマナー

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齐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で送信をおこなうようにします(図4-1)。

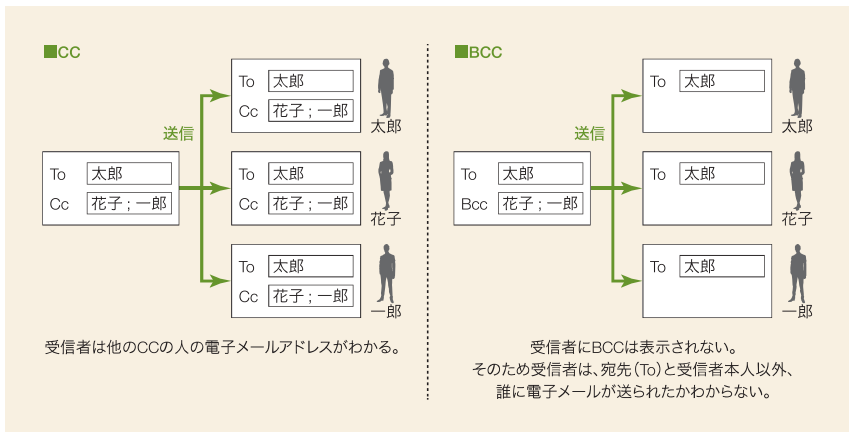


図4-1 CCとBCCの違い

チャットツールはリアルタイムなやり取りが可能であり、文章だけでは伝わりにくい感情やニュアンスを伝えるための絵文字・スタンプの活用や、重要挨拶の定型文の省略、結論を先に伝えるなど、電子メールとは異なるマナーが存在します。

電子メールをフォーマルなコミュニケーション手段とするならば、チャットツールは、よりカジュアルなコミュニケーション手段と言えます。例えば、すぐに詳細な返信が難しい場合でも、スタンプで一時的な反応を示しておき、後で詳細な返信をおこなう方法は、チャットツールの特性と言えます。

電子メールも同様ですが、カジュアルとはいえ適切な言葉遣いを心がけ、プライバシーの侵害に気を付け、感情的な議論を避けて利用しましょう。

4-8 情報の偏り

インターネット上で、ユーザーの過去の行動や興味に基づいて情報が選別される現象を、フィルターバブルと言います。“自身の考え方や価値観のバブル(泡)”の中に孤立してしまう情報環境を指します。例えば、検索エンジンによる検索結果や、動画サイトのおすすめ動画等は、ユーザーの好みや嗜好に応じた内容が表示されるため、異なる視点の情報に触れる機会が減少していることとなります。

一方、自分と同じ意見や考えを持つ人々とだけ交流することにより、異なる視点が排除される現象をエコーチェンバーと言います。例えば、自分と同じ価値観の人々が集うグループやフォーラムにおいては、自身と同じ様な考えや耳触りの良い意見が繰り返し強調されることになり、ユーザーは偏った情報のみを受け取りやすくなってしまいます。

こうした情報の偏りを避けるため、1つのニュースサイトやソーシャルメディアに頼らず、複数の異なる情報源からニュースや意見を得ることが重要です。また、自分の意見とは異なる立場の情報や意見に積極的に触れることで、視野を広げることも大切です。先述のファクトチェックと合わせて、バランスの取れた情報環境を築いていきましょう。



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アドレス**」^{アイピー}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。

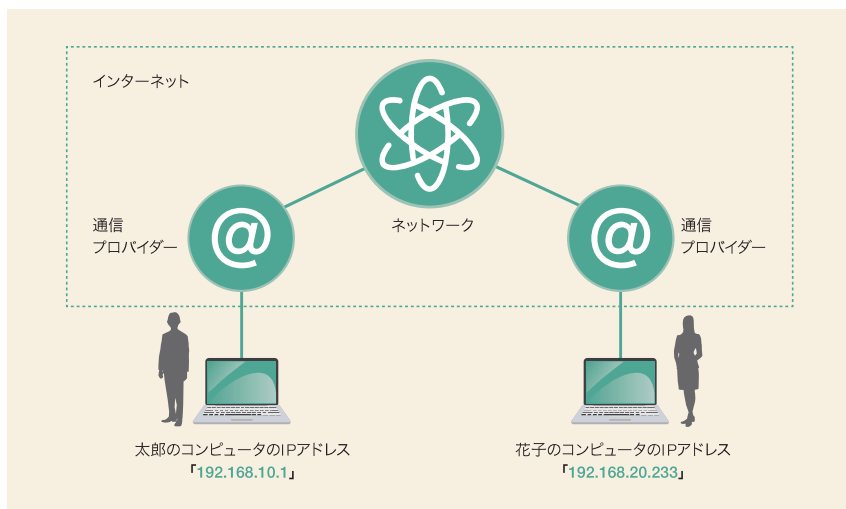


図5-1 インターネットの概念

5-2 Web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「Webページ」、あるいは「Webサイト」「Webページ」といいます。Webページの内容は、インターネット上にある「Webサーバー」(Webページ公開専用のコンピュータ)に保存されています。

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

例 ヤフーWebページのトップページのURL

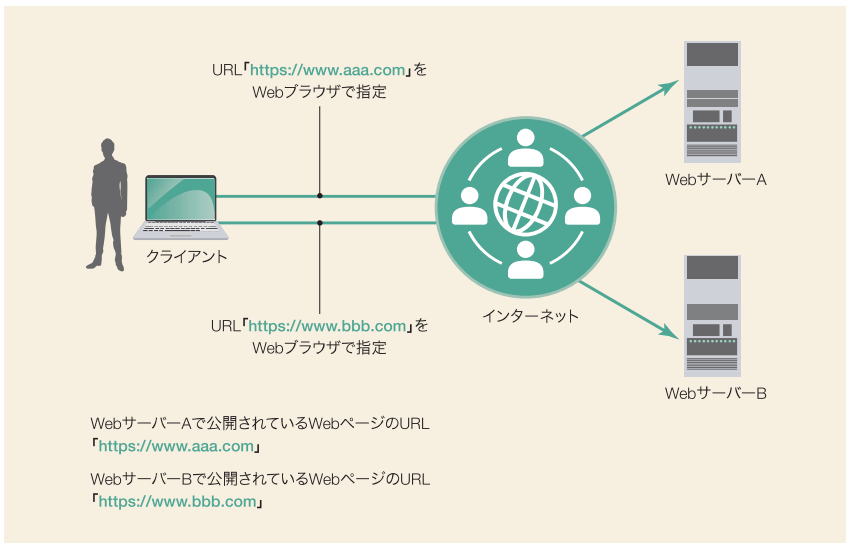
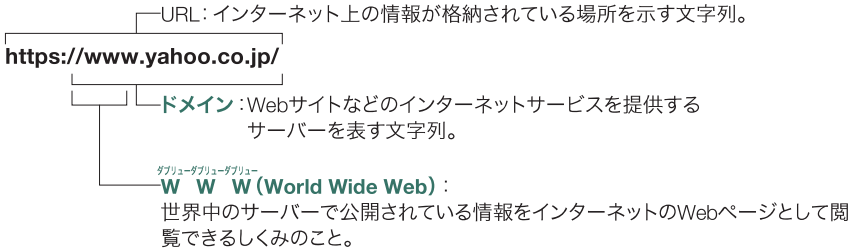


図5-2 WebブラウザでURLを指定

Webブラウザを使えば、Webページのほか、電子掲示板、ブログ、SNS、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】

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

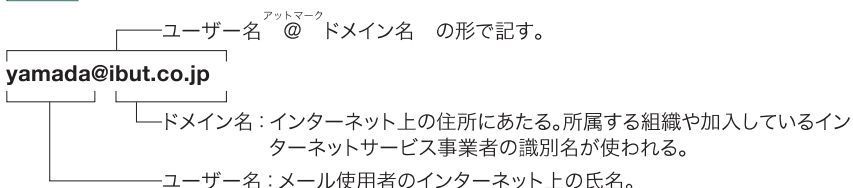
Webページへのアクセスは、Webサーバーを公開する企業・個人や通信プロバイダーによってアクセスの記録がおこなわれています。SNSなどに書き込んだメッセージやアクセス履歴（ログ）は、常に記録されていることを意識してインターネットを使用するようにしましょう。

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 SNSのしくみ

「^{エスエヌエス}SNS」(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、Web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5-3)。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。

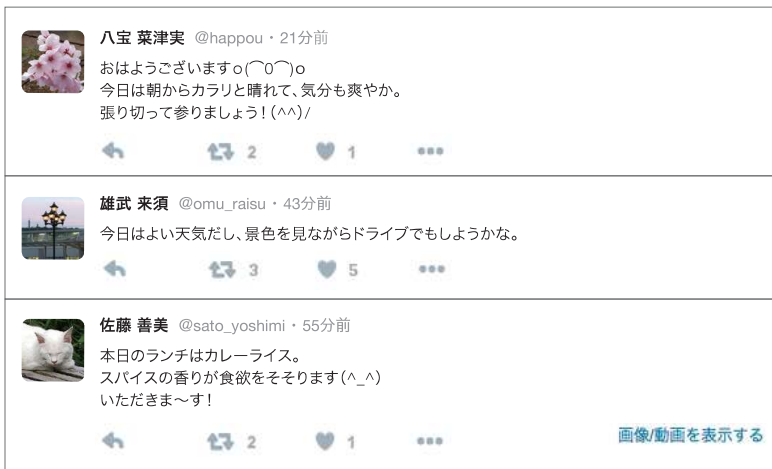


図5-3 SNSのイメージ

- 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、
- ・ハッキングにより流出したアカウントの不正利用により金融情報や住所などが悪用された
 - ・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
- ・ 誹謗中傷により深刻な精神的苦痛を受け、有名人が自殺や自殺未遂に至る事件が発生
- ・ 災害時や新型コロナウイルスの流行時にデマや偽情報（フェイクニュース）がSNSで拡散され、多くの人々が不安を抱える事態に
- ・ 無断で映画や音楽をSNSにアップロード共有したことで大規模な著作権侵害事件に発展

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】

- ▶ X (旧Twitter) <https://x.com/>
- ▶ Facebook <https://www.facebook.com/>
- ▶ LINE <https://line.me/ja/>
- ▶ Instagram <https://www.instagram.com/>

【事例：ネットいじめ／オンラインストーカー】

ある特定の生徒に対し、学校の同級生たちがグループチャットやSNSで悪口を言うことで攻撃するケースがあります。同様に、SNSで特定の人物の投稿を執拗にチェックし、リアルタイムで行動を監視したり、不快なメッセージを繰り返し送ったりするケースがあります。こうしたケースにおいて、被害者たちは加害者の想像以上に精神的に大きなダメージを受けてしまい、取り返しのつかない事態に発展してしまう恐れも考えられます。

これを防ぐためには、嫌がらせやいじめに遭った場合はすぐに信頼できる大人や学校に相談するとともに、自分自身も他人を傷つけるようなコメントや投稿をしないよう心掛けることが大切です。また、個人情報や行動履歴をSNSに公開しないよう設定を見直し、不審なアカウントからの接触はブロックすることも重要になります。

必要に応じて警察に相談することも考慮しましょう。

5-5 消費者が生み出すメディア

インターネットとデジタルデバイスの普及が進んだことで、誰もが簡単に高品質なコンテンツを作成し、発信できるようになりました。今や、ソーシャルメディアによる簡単な情報発信も当たり前となり、一般のユーザー（消費者）が企業広告よりも共感を呼ぶ情報を発信する参加型文化も広がりました。

こうしたユーザーが作り出すインターネットコンテンツは、企業やブランドにとっては貴重なマーケティング資源となり、消費者にとっては、情報交換や自己表現の場として広く利用されるようになりました。

以下に、その具体的な例を挙げます。

・写真共有プラットフォーム

写真共有サイトでは、ユーザーが日常生活や旅行先で撮影した写真をアップロードし、他のユーザーと共有します。友人たちやフォロワーから「いいね!」やコメントを寄せてもらうために、美しい風景やおしゃれなカフェの写真などが人気です。

・動画共有サイト

動画共有サイトでは、ユーザーが自分の趣味や特技を、動画にして投稿します。特に、メイクの仕方やゲーム実況動画などが人気です。視聴者からのフィードバックや質問に対してコメントで返答し、視聴者とのコミュニケーションを楽しむ配信者も多いです。

・商品レビューサイト

商品レビューサイトでは、ユーザーが購入した商品についてのレビューを書き込みます。家電製品からファッションアイテムまで、幅広い商品が対象となり、具体的な使用感や写真を添えて、他の購入を検討しているユーザーに向けた情報として提供されます。

・ブログ

例えば、個人が運営するブログでは、ユーザーが旅行記やレシピ、ライフスタイルに関する記事を投稿します。旅行の計画から現地での観光スポット、美味しいレストランの情報までを写真付きで紹介し、旅行を考えている読者にとって有益な情報が提供されます。

・オンラインコミュニティ

ディスカッションフォーラムでは、ユーザーが特定のトピックについて意見交換や情報共有をおこないます。例えば、ゲームに関するコミュニティでは、攻略方法についてスレッドを立て、他のユーザーと効率的な攻略方法や隠し要素についてディスカッションをおこないます。多くの有益な情報が集まり、コミュニティ全体が恩恵を受けます。

5-6 インターネットを利用した買い物

インターネット上で買い物をすることを、オンラインショッピングと言います。

インターネット上に開設した商品を販売するWebサイトのことをECサイトと言います。ECとは「electronic commerce」の頭文字から来ており、日本語に訳すと「電子商取引」となります。

ECサイトでは、様々な情報がリアルタイムに更新されるという仕組みとなっています。(図5-4)。



図5-4 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ため、EC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お店を個人で開設・運営する等、新しいECサイトが続々と増え続けています。

【代表的なEC サイト】

- ▶ Amazon <https://www.amazon.co.jp/>
- ▶ 楽天市場 <https://www.rakuten.co.jp/>



インターネット上のその他の買い物手段として、フリマ（フリーマーケット）サイトやオークションサイトがあります。

フリマサイトとは、インターネット上のフリーマーケットのことです。出品者は自由に価格を設定することができ、その価格に同意した人が購入できるというシステムです。取引完了時には、出品側が販売価格の数%を手数料として支払う仕組みになっています。

ネットオークションは、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）をおこなうことです。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）をおこない、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5-5）。

個人で気軽に出品できるため、フリマサイトの利用者は増えています。しかし、フリマサイトや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も数多く存在します。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。

フリマサイトや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

フリマサイトやオークションサイトには、購入者が支払ったお金を一時的に第三者が管理し、商品が無事に届いた後に売り手に支払われるエスクローサービスを利用することが

できます。他にも、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を活用することも、取引のトラブルを回避する対策のひとつです。

米〇〇社製 トランペット(中古)



入札件数	残り時間
2 入札履歴	5日 詳細

現在の価格
80,000円

入札する

出品者情報
〇〇〇〇〇〇さん

評価: 〇〇〇

[出品者の他のオークションを見る](#)

出品地域: 東京都

状態	: 中古	自動延長	: あり
個数	: 1	早期終了	: あり
開始日時	: 2014.12.16 (〇) 22:19	返品	: 返品可
終了日時	: 2014.12.23 (〇) 22:19	開始価格	: 50,000円

図5-5 オークションサイトのイメージ

5-7 ネットバンキングとは

ネットバンキングは、インターネットを介しておこなわれる銀行の取引を指します。これにより、私たちは、自宅や外出先などから24時間いつでも口座の残高確認、振込、支払、投資管理などのサービスを利用できます。

ネットバンキングは、従来の銀行窓口での手続きをデジタル化することで、利便性を大幅に向上させました。また、スマートフォンアプリを通じて、より手軽に銀行サービスを利用できるようになっています。

一方で、セキュリティ対策が重要となり、フィッシング詐欺や不正アクセスから保護するための多要素認証が普及しています。

5-8 無線LANとWi-Fiの基礎知識

「^{Wi-Fi}Wi-Fi」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おこなう通信網を指します。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。最近で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

エスエスエル
「SSL」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^{※5}や盗聴^{※6}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Webページです（図5-6）。



図5-6 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（5-9 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ことで安心です。

！ 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ことで、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 改ざん：文章などの字句を直すこと。特に、悪用するために、勝手に直すこと。

※6 盗聴：ぬすみ聞きをすること。

5-9 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5-7）。

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。

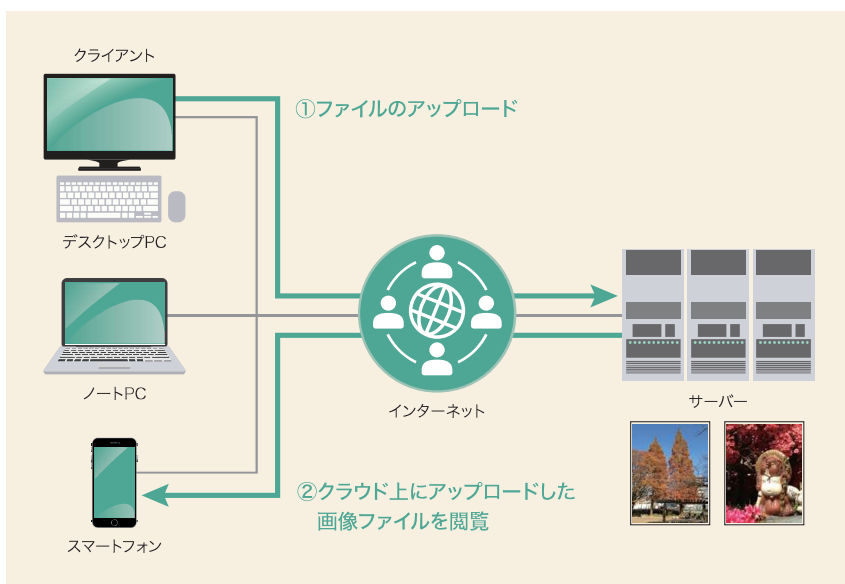


図5-7 クラウドサービスの例（ファイルの共有）

5-10 インターネット上で利用できる生成AIについて

生成AIは、コンテンツを自動で生成するAI技術の活用を指します。この技術は、自然言語処理や画像生成、音楽作曲など、さまざまなクリエイティブな分野で利用されており、インターネット上で気軽に利用できるものも多くあります。

例えば、Chat GPTのような大規模言語モデルは、人間のような文章の生成やプログラムコードの生成、翻訳や要約などをすることができます。インターネット上にある様々な情報を事前学習しているモデルが、関連性の高いレベルで結合を繰り返し、私たちに馴染み深い自然言語で提示するという仕組みです。

そのため、利用する際は、情報が正しくない、専門分野の回答精度が低い、倫理上不適切な内容、という可能性があることをしっかりと認識した上で利用するようにしましょう。

また、画像生成AIは、特定のスタイルに基づいたイラストや絵画の生成、写真の生成や修正などをおこなうことができます。しかし、オリジナルに類似した著作物の生成や、著作権侵害の発生など、個々の権利者に対して解決が困難になる可能性も秘めています。

生成AIは、クリエイティブな作業の効率化や新しいアイデアの創出に寄与する一方で、著作権や倫理的な問題も議論されています。そのため、AI技術の発展とクリエイターの権利保護、共に解決するための規制やルールが必要とされています。



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おこな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おこないます。

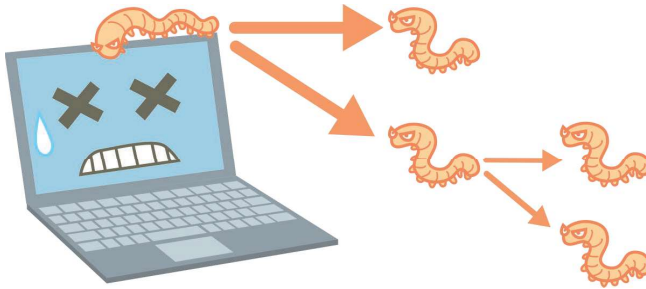
コンピュータがコンピュータウイルスに感染すると、ハードディスクに保管されているファイルが消去されたり、コンピュータを起動できないようにされたりと、さまざまな被害を受けます。



📖 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**(ぜいじゃく脆弱性。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。

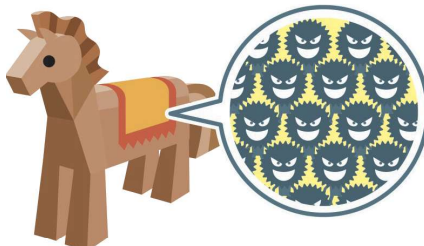


📖 トロイの木馬 (Trojan horse)

「**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おこなうプログラムです。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うちに活動します。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。悪意を持った第三者が、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)。

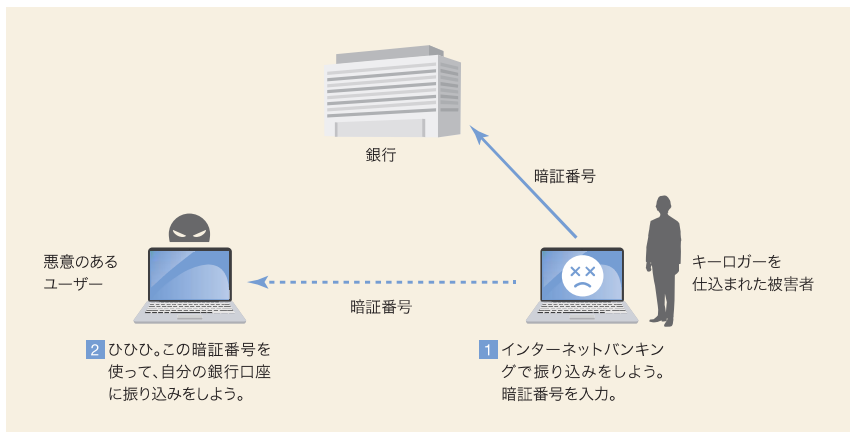


図6-1 キーロガー

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おこないます (図6-2)。

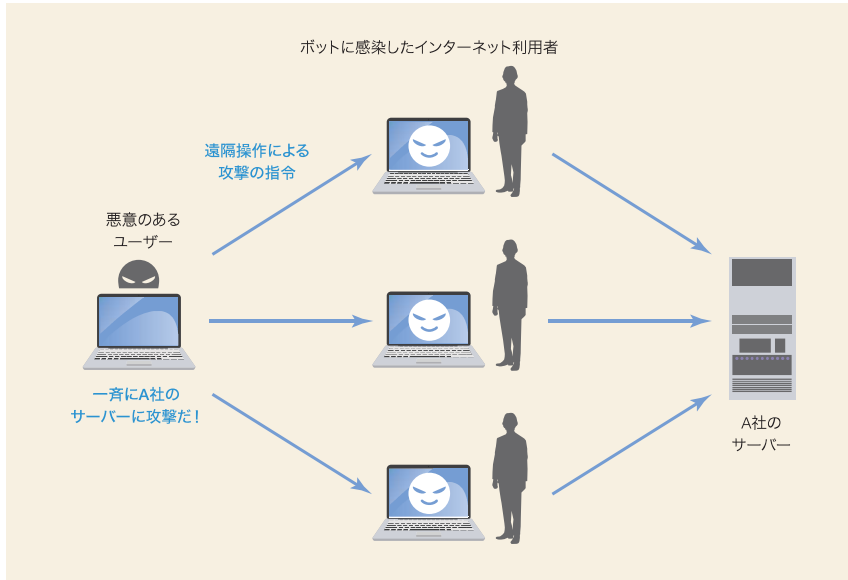


図6-2 ボット

📖 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）にし、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Web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、Web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。

❗ 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Webページやメールに注意する

ウイルスは悪意のあるWeb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Web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Web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、物理的に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」を用いておこなわれます。「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。

近年は、さまざまなシステムやサービスのセキュリティ対策として、ワンタイムパスワードが普及しています。ワンタイムパスワードとは、30秒や60秒といった短い間隔で生成される「一度しか使えない使い捨てのパスワード」で、一定時間を過ぎた後、そのパスワードは無効になるというものです。

特にネットバンキングや企業の内部システムなど、高いセキュリティが求められる場面において、こうしたワンタイムパスワードとそれ以外の要素を組み合わせた多要素認証が広く利用されています。(7-11 参照)

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さまざま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えいすることがないように、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。さらに、異なるアカウントごとに異なるパスワードを使用し、定期的に変更することが推奨されます。

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、管理方法もさまざまにありますが、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 パスワードを狙った攻撃

パスワードを狙った攻撃には、ブルートフォース攻撃、辞書攻撃、フィッシングなど、さまざまな方法があります。これらの攻撃は、パスワードの推測や、ユーザーを騙してパスワードを入力させることで、不正にアクセスを試みます。

ブルートフォース攻撃では、可能なパスワードの組み合わせを総当たりで試します。

辞書攻撃は、一般的なパスワードリストを使用して推測します。

フィッシングは、偽のWebサイトやメールを通じてユーザーからパスワードを騙し取ります。

これらの対策として、強固なパスワードの使用や多要素認証の導入が推奨されます。

7-4 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)。

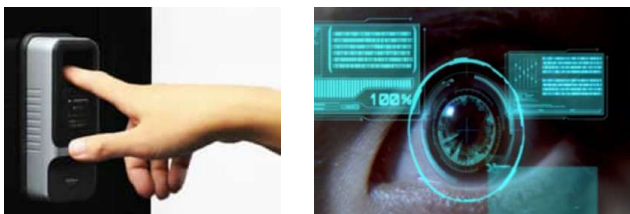


図7-1 指紋認証・虹彩認証

7-5 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おこなわれます。

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。

7-6 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。Web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(図7-2)。

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^{※7}の防止に役立ちます。

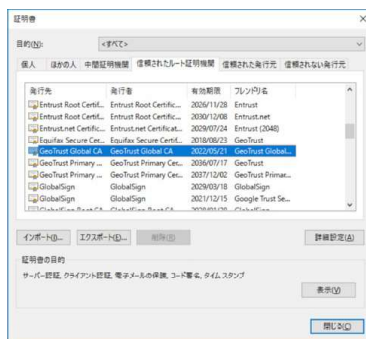


図7-2 ブラウザソフトでの電子証明書確認画面例

※7 事後否認：物事が起こったあとから、それを事実として認めず、事実の否定を主張すること

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 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、通信技術によらない社会的な方法で入手することです。主な手口と対策を、下記にまとめます。

- 電話や会話の最中に巧みに聞きだす・盗み聞く
電話は、かけ直して必ず本人確認をする
また、パスワードや機密情報を音声で話さない
- 端末の画面やキー入力を盗み見る(ショルダーハッキング)
カフェや図書館など周囲に人が多い環境では周囲に注意してパソコンなどを使う
覗き見防止フィルムやスクリーンプロテクターを貼る
- ゴミ箱を漁って機密情報を探し出す(トラッシング)
紙媒体は、シュレッダーにかける等、情報を復元できない状態にしてから捨てる
記憶媒体は、内部データを全て空に、または物理的に破壊してから捨てる
- 郵便物を盗む(メールハント)
ポストが映るように、監視カメラを設置する
セキュアなメールサービスを利用して、無人ポストに入れないようにすることも対策

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、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うため、日頃の注意と対策が大切になります。

7-9 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1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。

7-10 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7-3 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(図7-3)。

「多要素認証」とは、以下に示す認証要素を2つ以上組み合わせることでセキュリティを高める手法を指します。これにより、不正アクセスのリスクを大幅に低減でき、より安全なオンライン活動をおこなうことができます。

● 認証の3要素

- ・知識要素：パスワードやPINなど、ユーザーが知っている情報に基づく認証要素です。知識要素は、ユーザーが覚えている秘密の情報を入力することで、本人確認をおこないます。最も一般的な認証方法であり、多くのオンラインサービスで使用されています。
- ・所有要素：スマートフォンの認証アプリやSMSコード、ICカードなどのユーザーが所持しているアイテムに基づく認証要素です。所有要素は、物理的なアイテムを利用して本人確認をおこなうため、知識要素と組み合わせることでセキュリティを強化します。
- ・生体要素：指紋や虹彩などの身体的特徴に基づく認証要素です。生体要素は、ユーザーが持つユニークな身体的特徴を利用して本人確認をおこなうため、高度なセキュリティ対策として有効です。

近年、さまざまなシステムやサービスのセキュリティ対策としてワンタイムパスワードが普及しています。ワンタイムパスワードとは、30秒や60秒といった短い間隔で生成される「一度しか使えない使い捨てのパスワード」で、一定時間を過ぎた後、そのパスワードは無効になるというものです。このワンタイムパスワードと上記の3要素のいずれかを組み合わせた二要素認証は、よく使われています。

令和7年3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 College 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