脅威

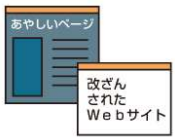
新井康平

- 脅威にはそれを引き起こす者がいます。悪意を持って攻撃をする者は、お金を稼いだり、請求を逃れたりといった金銭目的や恨みや不満を晴らす目的を持っています。そのために、インターネットを通じて、ウイルスを送りつけたり、政府機関や企業のサーバやシステムに不正アクセスを行ったりします。その他、政治目的やいたずらなどで同じような行為をする者もいます。これにより、サーバやシステムが停止したり、ホームページが改ざんされたり、重要情報が盗みとられたりするのです。

- ウイルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムです。最近では、マルウェア（“Malicious Software”「悪意のあるソフトウェア」の略称）という呼び方もされています。
- 数年前までは記憶媒体を介して感染するタイプのウイルスがほとんどでしたが、最近はインターネットの普及に伴い、電子メールをプレビューしただけで感染するものや、ホームページを閲覧しただけで感染するものが増えてきています。また、利用者の増加や常時接続回線が普及したことで、ウイルスの増殖する速度が速くなっています。

- 多くのウイルスは増殖するための仕組みを持っています。たとえば、コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖します。最近はコンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して、自動的にウイルス付きの電子メールを送信するものや、ホームページを見ただけで感染するものも多く、世界中にウイルスが蔓延する大きな原因となっています。
- ウイルスに感染しないようにするためには、ウイルス対策ソフトを導入する必要があります。また、常に最新のウイルスに対応できるように、インターネットなどでウイルス検知用データを更新しておかなければなりません。

- ウイルスは、USBメモリなどの記憶媒体や電子メール、ホームページの閲覧など、そのウイルスのタイプによってさまざまな方法で感染します。また、ウイルスに感染すると、コンピュータシステムを破壊したり、他のコンピュータに感染したり、そのままコンピュータに残ってバックドアと呼ばれる不正な侵入口を用意したりするなど、さまざまな活動を行います。



- 現在のWebブラウザは、ホームページ上でさまざまな処理を実現できるように、各種のプログラムを実行できるようになっています。これらのプログラムの脆弱性を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してしまう危険があります。最近では、Webブラウザへ機能を追加するプラグインソフトの脆弱性（ぜいじゃくせい）を利用した感染方法が増加しています。
- かつては怪しいWebサイトを訪問しなければ大丈夫と思われていましたが、最近では正規のWebサイトが不正侵入を受けて書き換えられ、ウイルスが仕込まれてしまうケースも急増しています。この場合は、正規のWebサイトを閲覧しても、ウイルスに感染してしまうことになります。

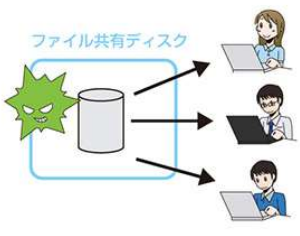
- あたかも無料のウイルス対策ソフトのように見せかけて、悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、利用者を偽のウイルス対策ソフトを配布するWebサイトに誘導する方法です。

- 電子メールの添付ファイルもウイルスの感染経路として一般的です。電子メールに添付されてきたファイルをよく確認せずに開くと、それが悪意のあるプログラムであった場合はウイルスに感染してしまいます。
- かつては、電子メールで実行形式のファイル(ファイルの拡張子が.exe　のファイル)が送られてきたときには特に注意するように言われていましたが、最近はファイル名を巧妙に偽装し、文書形式のファイルに見せかけて悪意のあるプログラムを実行させ、ウイルスに感染させる事例もあります。
- また、文書形式のファイルであっても、文書を閲覧するソフトウェアの脆弱性を狙った攻撃も増加していることから、メールに添付されてきたファイルを安易に開くのは危険な行為です。

- 多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。このようなウイルスの中には、感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で、被害を拡大させるものもあります。

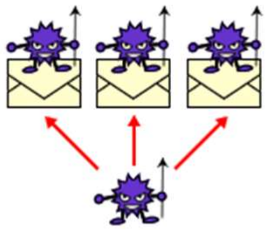
- ファイル共有ソフトとは、インターネットを利用して他人とファイルをやり取りするソフトウェアのことです。自分が持っているファイルの情報と、相手が持っているファイルの情報を交換し、お互いに欲しいファイルを送り合ったりすることから、ファイル交換ソフトとも呼ばれています。
- ファイル共有ソフトでは、不特定多数の利用者が自由にファイルを公開することができるため、別のファイルに偽装するなどの方法で、いつの間にかウイルスを実行させられてしまうことがあります。
- 添付ファイルが付いていなくても、HTML形式で書かれているメールの場合、ウイルスに感染することがあります。HTMLメールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTMLメールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

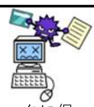
- ウイルスによっては、感染したコンピュータに接続されているファイル共有ディスクを見つけ出し、特定のファイル形式など、ある条件で探し出したファイルに感染していくタイプのものがあります。このようなウイルスは組織内のネットワークを通じて、他のコンピュータやサーバにも侵入して感染を拡げる可能性があります。とても危険度が高く、完全に駆除することが難しいのが特徴です。



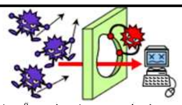
- マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Accessなど）には、特定の操作手順をプログラムとして登録できるマクロという機能があります。このマクロ機能を利用して感染するタイプのウイルスが知られており、マクロウイルスと呼ばれています。
- Officeアプリケーションでは、マクロを作成する際に、高度なプログラム開発言語であるVBA（Visual Basic for Applications）を使用できるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能です。そのため、マクロウイルスに感染した文書ファイルを開いただけで、VBAで記述されたウイルスが実行されて、自己増殖などの活動が開始されることになります。

- ウイルスの中には、インターネットやLANを使用して、他の多くのコンピュータに感染することを目的としているものがあります。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルとして送信したりネットワークドライブに保存されているファイルに感染したりするなど、利用者の操作を介さずに自動的に増殖していきます。



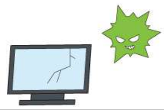


- ウイルスによる情報漏洩は、大きく分類すると、コンピュータに保存されている情報が外部の特定のサイトに送信されて起こる場合と、インターネット上に情報が広く公開されて起こる場合があります。ウイルスによって漏洩する情報は、ユーザIDやパスワード、コンピュータ内のファイル、メール、デスクトップの画像など、さまざまです。情報漏洩を引き起こすタイプのウイルスには、利用者がキーボードで入力した情報を記録するキーロガーや、コンピュータ内に記録されている情報を外部に送信するスパイウェアと呼ばれるものなどがあります。コンピュータがこのようなウイルスに感染していたとしても、コンピュータの画面上には何の変化も起こらないことが多いため、利用者はウイルスに感染していることに全く気が付きません。
- なお、漏洩した情報がインターネットに掲載され、公開されてしまった場合は、その情報をネットワーク上から完全に消去することは非常に困難です。



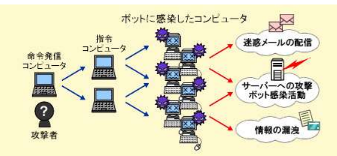
- 感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でも、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウイルスは極めて悪質なものです。この種のウイルスに感染すると、コンピュータを外部から自由に操作されてしまうこともあります。
- 外部からコンピュータを操作するタイプのウイルスは、RAT (Remote Administration Tool)とも呼ばれ、利用者に気が付かれることもなくコンピュータを遠隔操作します。多くの場合、コンピュータの画面上に何も表示されることなく、プログラムやデータファイルの実行・停止・削除、ファイルやプログラムのアップロード・ダウンロードなど、不正な活動を行います。

- ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。
- いたずらを目的としたウイルスは、一定期間コンピュータ内に潜伏して、ある日時に特定のメッセージや画像を表示することがあります。ただし、最近はこのようないたずらを目的としたウイルスは減ってきています。

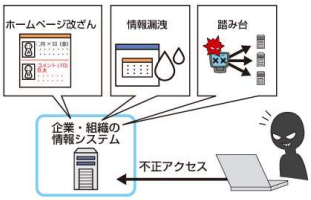


- ボット（BOT）とは、コンピュータを外部から踏み台にして遠隔操作するためのウイルスです。ボットに感染したコンピュータは、同様にボットに感染した他の多数のコンピュータとともに一員として悪意のあるネットワークを形成し、ネットワークを通じて感染します。外部から攻撃者が、ボットを遠隔操作し、コンピュータを自由に操るという動作から、遠隔操作ソフトウェアのことを、ロボット（Robot）をもじってボット（BOT）と呼んでいます。
- 攻撃者は、ボットに感染したコンピュータを遠隔操作することで、インターネットに対して、「迷惑メールの配信」、「インターネット上のサーバへの攻撃」、「さらにボットを増やすための感染活動」などの迷惑行為や犯罪行為を行います。また、感染したコンピュータに含まれる情報やコンピュータの利用者が入力した情報を盗み出す「スパイ活動」も行います。ボットは旧来のウイルスのように愉快犯的な迷惑行為ではなく、個人情報を不正に取引するといった犯罪者の利用を目的とするようになり、手口が巧妙化しています。旧来のウイルスと比べると、感染していることに利用者が気付きにくいように作られているというのも特徴のひとつです。

- もし、あなたのコンピュータがボットに感染した場合、あなたはもちろん被害者なのですが、あなたのコンピュータが迷惑メールを送信したり、別のサイトを攻撃したりするため、攻撃の標的となったコンピュータから見ると、あなたのコンピュータは加害者になってしまいます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことなのです。



- 不正アクセスとは、本来アクセス権限を持たない者が、サーバや情報システムの内部へ侵入を行う行為です。その結果、サーバや情報システムが停止してしまったり、重要情報が漏洩（ろうえい）してしまったりと、企業や組織の業務やブランド・イメージなどに大きな影響を及ぼします。
- インターネットは世界中とつながっているため、不正アクセスは世界中のどこからでも行われる可能性があります。



- 攻撃者は、インターネットを通じて企業や組織のサーバや情報システムに侵入を試みます。手口としては、ツールを用いてアカウント情報を窃取するための総当たり攻撃を行ったり、OSやソフトウェアの脆弱性（ぜいじゃくせい）、設定の不備などを調べて攻撃することが知られています。
- 攻撃者は侵入に成功すると、その中にあるホームページの内容を書き換えたり、保存されている顧客情報や機密情報を窃取したり、重要なファイルを消去したりすることもあります。

- ホームページの書き換えは、攻撃者が全く関係のない画像を貼り付けるようなものもありますが、最近はホームページにあるリンクやファイルの参照先を不正に書き換え、接続してきた利用者をウイルスに感染させたり、パソコンから情報を盗み取ったりするものが増えています。ホームページが書き換えの被害を受けるということは、その企業や組織のセキュリティ対策が不十分であることを示すことになり、社会に対するイメージ低下は避けられません。
- また、顧客情報などが漏洩してしまった場合は、その企業や組織の信用が大きく傷つけられてしまうのは言うまでもないことですが、過去には損害賠償にまで発展した事例もあります。このように、不正アクセスは甚大な被害をもたらすこともあるのです。

- 不正アクセスによって侵入されたシステムは、攻撃者がその後いつでもアクセスできるように、バックドアと呼ばれる裏口を作られてしまうことが知られています。攻撃者は、そのシステムを踏み台として、さらに組織の内部に侵入しようとしたり、そのシステムからインターネットを通じて外部の他の組織を攻撃したりすることもあります。
- この場合に多く見られる例は、攻撃者によってボット ウイルスを送り込まれ、自分がボットネットの一員となってしまうというものです。ボットネットとは、攻撃者によって制御を奪われたコンピュータの集まりで、数千～数十万というネットワークから構成されていることもあります。攻撃者はボットに一斉に指令を送り、外部の他の組織に対して大規模なDDoS攻撃を行ったり、スパムメールを送信したりすることもあります。
- このように、不正アクセスの被害に遭うと、知らない間に攻撃者の一員として利用されてしまうこともあるのです。

- インターネットでは、詐欺や犯罪行為などが増加しています。それらの詐欺や犯罪の中には
  - 偽物のホームページに誘導し個人情報などを窃取するフィッシング詐欺
  - 電子メールなどで誘導してクリックしたことで架空請求などをするワンクリック詐欺
  - 商品購入などで架空出品をしてお金をだましとるオークション詐欺
  - 違法薬物など、法令で禁止されている物を販売する犯罪
  - 公序良俗に反する出会い系サイトなどに関わる犯罪

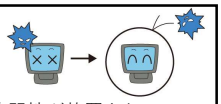
  など多様な手口があります。

- インターネットでの犯罪は、主に金銭目的で行われることも増えてきました。そのために、デマなどのウソの情報を流す、他人になりすます、ユーザIDやパスワード、プロフィールなどの個人情報を盗んで悪用するなど、さまざまな手法で行われます。金銭目的以外では、相手への恨みや不満、興味本位などの動機から、攻撃や嫌がらせなどを目的として行われることもあります。
- インターネットが広く普及したことにより、これまで現実世界でも存在した詐欺やの犯罪行為などでもこの便利な技術が使われるようになってきたのです。インターネットが便利なのは、犯罪者にとっても同じです。これからも、ますます犯罪行為にインターネットが使われ、多様な手口が出現してくることは間違いありません。利用者はよりいっそうの注意が必要になります。

- インターネットの脅威は、外部の攻撃者などにより意図的に行われるものばかりではありません。人による意図的ではない行為や、組織などの内部犯行、システムの障害などの事故も大きな情報セキュリティ上の脅威です。
- 人は意図的ではなく、脅威を引き起こすこともあります。操作ミスや設定ミス、紛失など、いわゆる「つい、うっかり」の過失（ヒューマンエラー）です。電子メールの送り先を間違えたり、書類や記憶媒体の廃棄の方法を誤ったり、携帯電話やスマートフォンを紛失したり、といった過失が多く発生しています。実は、企業や組織における情報漏洩（ろうえい）の原因のほとんどが、このような人の「つい、うっかり」やITの使いこなし能力（リテラシー）の不足によるものとされています。

- 組織などの内部犯行も想定される脅威の一つとして、セキュリティ対策を講じておく必要があります。例えば、アカウント管理やデータのアクセス権限を適切に設定したり、アクセス記録を取ることで、人による脅威を未然に防ぐことになり得ます。
- その他の脅威としては、機器やシステムの障害や自然災害などがあります。機器やシステムの障害は、コンピュータやネットワークを使っている限りは常に起こり得る問題です。システムの障害によって、データが失われてしまったり、業務が継続できなくなったりするなどの大きな影響が発生することもあります。自然災害は、頻繁に起こる問題ではありませんが、ひとたび発生すれば企業や組織に甚大な被害や影響を与えます。
- 以上の脅威を起こり得ることとして想定し、あらかじめ事故や障害・災害が発生した場合の情報セキュリティ対策を講じておく必要があります。

- 脆弱性とは、コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います。脆弱性は、セキュリティホールとも呼ばれます。脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性があります。
- このような脆弱性が発見されると、多くの場合、ソフトウェアを開発したメーカーが更新プログラムを作成して提供します。しかし、脆弱性は完全に対策を施すことが困難であり、次々と新たな脆弱性が発見されているのが現状です。



- 脆弱性には、いくつかの種類があります。脆弱性が放置されていると、外部から攻撃を受けたり、ウイルス（ワーム）の感染に利用されたりする危険性があるため、インターネットに接続しているコンピュータにおける情報セキュリティ上の大きな問題のひとつになっています。
- 脆弱性はクライアントとサーバ、どちらのコンピュータにおいても重要な問題ですが、特にインターネットに公開しているサーバの場合には、脆弱性を利用した不正アクセスによって、ホームページが改ざんされたり、他のコンピュータを攻撃するための踏み台に利用されたり、ウイルスの発信源になってしまったりするなど、攻撃者に悪用されてしまう可能性があるため、脆弱性は必ず塞いでおかなければなりません。

- 脆弱性を塞ぐには、OSやソフトウェアのアップデートが必要となります。たとえば、Windowsの場合には、サービスパックやWindows Updateによって、それまでに発見された脆弱性を塞ぐことができます。ただし、一度脆弱性を塞いでも、また新たな脆弱性が発見される可能性があるため、常にOSやソフトウェアの更新情報を収集して、できる限り迅速にアップデートを行わなければなりません。
- なお、近年はゼロデイ攻撃と呼ばれる脅威が増加しています。ゼロデイ攻撃とは、OSやソフトウェアに対する脆弱性が発見されたときに、メーカーが修正プログラムを配布するまでの間に、その脆弱性を利用して行われる攻撃です。脆弱性が公開されてから、メーカーが対応策を検討して修正プログラムを開発することも多いため、完全な対策は困難と言わざるを得ません。そのため、指摘された脆弱性の内容を確認し、危険となる行為を行わないなど、修正プログラムを適用するまでの間は十分な注意が必要です。

- インターネットの普及により、私たちが自由に情報を発信できる場所や機会が大幅に増えてきました。これは便利なことである反面、発信のしかたを誤るとトラブルを引き起こす原因にもなります。
- 情報発信のしかたを誤ることにより、重要情報が漏洩（ろうえい）したり、企業・組織のブランドやイメージを大きく低下させたり、自分のプライバシーを必要以上に公開してしまったり、他人のプライバシーを侵害してしまったり、などのトラブルが起こってしまいます。

- プライバシーとは、一般に、“他人の干渉を許さない、各個人の私生活上の自由”をいうと考えられています。インターネットにおいても、実社会と同様に、プライバシーは守られなければなりません。インターネットでは、不特定多数の利用者が接続する可能性があるため、特に注意を払ってプライバシーに関する情報を管理しなければなりません。
- まず、ひとりひとりの利用者にとって最も大切なことは、自分や知人の個人に関する情報を不用意に公開しないことです。たとえば、インターネット上の電子掲示板やホームページなどへの氏名、住所、電話番号、メールアドレスなど個人に関する情報の公開は、プライバシーを守るということから考えて、本当に問題のない行為であるかどうかをよく検討すべきです。
- また、ホームページ開設者や企業において、アンケートサイトなどを用意している場合には、収集した情報の管理について、責任があるということを認識しなければなりません。特に、プライバシーに関する情報を収集する場合には、万全な情報セキュリティ体制のもとで管理する義務があると言えます。近年、ホームページで登録したプライバシーに関する情報の漏洩が多く発生していますが、ほとんどのケースでは不適切な情報管理が原因となっています。

- 一般に個人情報と総称される、個人に関する情報としては、氏名、住所、生年月日、性別、電話番号、メールアドレス、写真などの情報があげられます。これらの個人に関する情報については、プライバシー保護のために注意して取り扱わなければなりません。
- なお、法律上の定義では、個人情報とは、「生存する個人に関する情報で、特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（個人情報の保護に関する法律第２条）をいいます。
- 企業などが個人情報を事業活動に利用する場合、その取り扱い方法などについては、「個人情報の保護に関する法律」の義務対象となりますので、司法や各省庁の定めるガイドラインに従って適切に取り扱う必要があります。

- インターネットでは、通信している相手が本人かどうかを確認する手段として認証と呼ばれる方法がとられます。
- インターネットの認証は、利用者を識別する情報と、それを確認する情報を組み合わせることで行われます。利用者を識別する情報には、IDが一般的に使用されます。IDとは、情報機器やサービスの提供者が、一人ひとりの利用者を区別して割り振る符号です。IDと組み合わせて確認する情報として、パスワードが使用されます。パスワードとは、そのIDを割り振られた本人だけが知る情報で、それを入力することでIDを持つ本人であることを確認するための符号です。パスワード以外では、カードや生体（指紋や網膜などの、バイオメトリクス情報）などが使われることもあります。

- IDとパスワードは、パソコンなどの情報機器や、インターネット上のサービスを利用する際に、許可された者であるかを識別し、本人を確認するための重要な情報です。
- 利用者の範囲が制限されている情報機器やインターネットサービスに、IDとパスワードを入力して、その機器やサービスを利用できる状態にすることをログインといいます。この確認のやりとりのことを認証と呼んでいます。利用を終了して、機器やサービスから離れる行為のことはログアウトといいます。

- このような認証の仕組によって、ネットワークや情報機器を利用する際に、利用する権限のない第三者の利用を防止します。しかし、IDやパスワードなど認証で使っている情報（アカウント情報）が不適切な管理や、攻撃などで盗まれてしまうと、なりすましなどの不正行為が行われてしまう危険性もあります。
- このような手口による被害にあわないよう、認証の仕組みと重要性を理解し、IDやパスワードなどのアカウント情報は厳重に管理するようにしましょう。

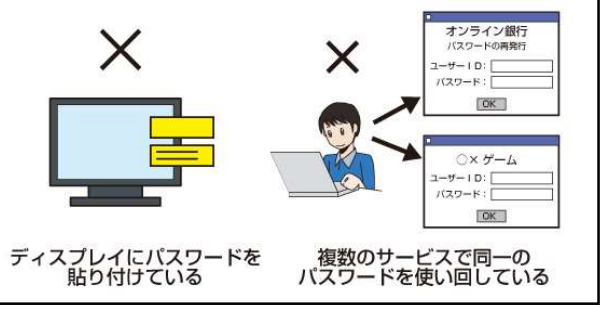
- 安全なパスワードとは、他人に推測されにくく、ツールなどで割り出しにくいものを言います。
  - (1) 名前などの個人情報からは推測できないこと
  - (2) 英単語などをそのまま使用していないこと
  - (3) アルファベットと数字が混在していること
  - (4) 適切な長さの文字列であること
  - (5) 類推しやすい並び方やその安易な組合せにしないこと

- 逆に、危険なパスワードとしては、以下のようなものがあります。このような危険なパスワードが使われていないかどうか、チェックをするようにしましょう。
  - (1) 自分や家族の名前、ペットの名前
    - yamada、tanaka、taro、hanako（名前）
    - 19960628、h020315（生年月日）
    - tokyo、kasumigaseki（住所）
    - 3470、1297（車のナンバー）
    - ruby、koro（ペットの名前）
  - (2) 辞書に載っているような一般的な英単語
    - password、baseball、soccer、monkey、dragon
  - (3) 同じ文字の繰り返しやわかりやすい並びの文字列
    - aaaa、0000（同じ文字の組み合わせ）
    - abcd、123456、200、abc123（安易な数字や英文字の並び）
    - asdf、qwerty（キーボードの配列）
  - (4) 短すぎる文字列
    - gf、ps
- この他、電話番号や郵便番号、生年月日、社員コードなど、他人から類推しやすい情報やユーザIDと同じものなどは避けましょう。

- せっかく安全なパスワードを設定しても、パスワードが他人に漏れてしまえば意味がありません。以下が、パスワードの保管に関して特に留意が必要なものです。
  - パスワードは、同僚などに教えないで、秘密にすること
  - パスワードを電子メールでやりとりしないこと
  - パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと
- やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

- またパスワードはできる限り、複数のサービスで使い回さないようにしましょう。あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。
- なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

- これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです（※１）。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています（※２）。
  - （※1） NIST SP800-63B（電子的認証に関するガイドライン）
  - （※2） https://www.nisc.go.jp/security-site/handbook/index.html



ディスプレイにパスワードを貼り付けている

複数のサービスで同一のパスワードを使い回している

- 生体認証（バイオメトリクス認証）とは、IDとパスワードの代わりに、身体的または行動的特徴を用いて個人を識別し認証する技術です。
- 生体認証に用いられる身体的な特徴として、指紋、顔、静脈、虹彩(瞳孔周辺の渦巻き状の文様)などが、行動的特徴として、声紋(音声)、署名(手書きのサイン)などがあります。 生体認証は、広く個人認証として用いられているパスワードによる認証やICカードによる認証と比較して、パスワードの記憶やICカードの管理が不要なため利便性が高く、また、記憶忘れや紛失によるトラブルもないという長所があります。
- その一方で、生体認証の種類によっては、以下の課題があります。
  - 安定性の課題(人の成長、老化などによる身体的特徴の変化によって、認証が正しく行われないなど)
  - 秘匿性の課題(サインなどの行動的特徴を盗み見られてなりすまされるなど)
  - 識別性能の課題(双子など身体的特徴が似ている人を誤認識するなど)
  - 認証情報の変更の課題(パスワードやICカードと異なり身体的特徴は、意図的に変更できないなど)
- なお、これらの課題に対策を施した製品も出てきています。

- ウイルス感染を防止するためには、次の３つが基本の対策になります。
  - 1. ソフトウェアを更新する。
  - 2. ウイルス対策ソフトを導入する。
  - 3. 怪しいホームページやメールに注意する。
- １．ソフトウェアを更新する
  - ソフトウェアの更新は、脆弱性（ぜいじゃくせい）をなくすためにとても重要です。

- ２．ウイルス対策ソフトを導入する
  - 次に、コンピュータにウイルス対策ソフトを導入する必要があります。ウイルス対策ソフトは、一般的にコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取ったり送ったりするデータを常時監視することで、インターネットやLAN、記憶媒体などからコンピュータがウイルスに感染することを防ぎます。
  - ただし、ウイルス対策ソフトは、これまでに発見されたウイルスに対応するウイルス検知用データからウイルスを見つけ出す仕組みになっているため、新しいウイルスは検知できないことがあります。そのため、ウイルス検知用データはいつでも最新のものに更新しておかなければなりません。最新のウイルス検知用データは、ウイルス対策ソフトメーカーが、インターネットなどを通じて配布しています。

- 有料のウイルス対策ソフトの場合、契約期間内であれば、通常、自動的に更新されるか、更新の通知が来るように設定されています。また、最近では、ウイルス検知用データを毎回ダウンロードする必要のないクラウドサービス型のウイルス対策ソフトも登場してきています。
- ウイルス対策ソフトの契約期間が切れて、ウイルス検知用データが更新できなくなってしまうと、コンピュータを十分に保護することができなくなってしまいます。ウイルス対策ソフトは、コンピュータを使用する上での必要な投資と考え、必ず継続的に更新するようにしましょう。

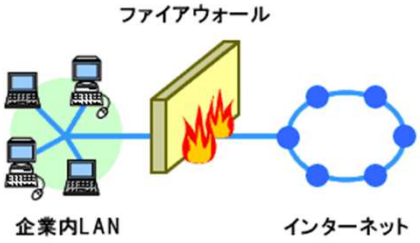
- また、ウイルス対策ソフトを導入する以外にも、インターネットサービスプロバイダなどが自社の接続サービスの利用者向けに提供しているウイルス対策サービスを利用する方法もあります。ウイルス対策サービスの内容などについては、インターネットサービスプロバイダのホームページで確認するか、加入しているインターネットサービスプロバイダに問い合わせてください。なお、インターネットサービスプロバイダのウイルス対策サービスを利用する場合には、インターネットサービスプロバイダがウイルス検知用データを自動的に更新するため、利用者による更新作業は不要になります。

- ３．怪しいホームページやメールに注意する
  - ウイルスは悪性のホームページなどで配布されていたり、メールに添付されていたりなど、さまざまな経路でコンピュータに侵入してきます。悪性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、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。最近では、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おり、これにも注意が必要です。

- 偽のウイルス対策ソフトに注意
  - 最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、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」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Webサイトに誘導して、ウイルスをインストールさせる方法です。
  - ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード/インストールしたりしないようにしてください。

- インターネットに接続したパソコンには、外部から自分の意図しない攻撃の通信が送られてくる場合があります。こうした不正アクセスをさせないためには、まず外部からの不要な通信を許可しないことが大切です。そのためには、通信の可否を設定できるファイアウォールを導入し、運用することが重要になります。
- 最近では、ノートPCなどを外部に持ち出すなどの機会が増えたため、利用者のPCが直接の不正アクセスの対象になっています。このような被害を防ぐためには、パーソナルファイアウォールを導入し、運用するようにしましょう。

- ファイアウォールなどによって、権限のない者の通信を防いでいても、権限を悪用されると、不正アクセスをされることになってしまいます。そのようなことがないよう、アカウント情報（ID、パスワードなど）の管理を十分に行い、権限を奪われることがないように注意しなければなりません。
- その他、不正アクセスをされる原因となる脆弱性（ぜいじゃくせい）への対策も必要になります。脆弱性（ぜいじゃくせい）が報告され、修正プログラムが配布されたら、速やかに適用するようにしましょう。



- インターネットを利用した詐欺や犯罪は、次々に新しい手口が登場しています。利用者の心構えとしては、普段からインターネットにおける詐欺や犯罪などの手口を知り、その対策について知識を深めておくことが大切です。
- まず、インターネット上のやりとりで、少しでも不審な点を感じたら、その情報の発信元や真偽を確認する姿勢が重要です。

- インターネットには、違法な有害情報や、法律に抵触しているようなサイトが多くあります。こうしたサイトを利用して、知らない間に、犯罪行為をしてしまっていた、というようなケースもあります。このような犯罪に巻き込まれないようにするためには、どのような行為が犯罪にあたるのかを知っておくことも大切です。インターネットの世界では利用者を誘惑したり、だましたりして犯罪行為に加担させるというケースもありますので、普段から、怪しいもうけ話などの誘惑に乗らないように行動するよう心がけましょう。

- 事故や障害が完全に発生しないようにすることは困難です。しかし、その発生確率を下げたり、発生した場合を想定した事前の対策により、被害を最小限に抑えることは可能です。
- 過失を防ぐために、まずはひとりひとりが注意することが大事ですが、事前の対策としては、例えば、パソコンやスマートフォン・携帯電話などを紛失してしまったり、盗難にあったりしたとしても、情報を保護できるための対策が必要になります。そのためには、情報をパスワードや暗号化などで保護したり、使用している機器にロックをかけておくなどして、情報を読まれたり、機器を悪用されたりすることを防ぐようにしましょう。

- 企業や組織においては、過失がある前提で事故への備えをすることが重要になります。過失による事故を未然に防ぐために、組織での情報セキュリティポリシーを整備し、利用や運用のルールを定めるなどの対策はもちろん、人の過失に備えて、例えば二重の確認チェックなどを行うなど、こうした事故への対策をしましょう。
- 障害への対策としては、例えばクラウドサービスなど、外部業者のサービスを使っていた場合は、その業者側での障害で影響を受けることもあります。こうした障害や自然災害が起こった場合には、情報を保護する対策も必要になります。そのため、利用するサービスを選ぶ際に、なるべく信頼性の高いサービスを選ぶこと、盗難や紛失への備えと同様に、ファイルの保護を行うこと、それでもファイルが失われた場合に備え、重要情報のバックアップを行いましょう。

- インターネットで情報発信をする際には、掲示板、SNSなどに機密情報・個人情報を書き込まない、誹謗中傷しないことが重要です。これは自分のものだけでなく、家族や友達などの情報も同様です。インターネットに書かれた情報は広く公開されるため、その情報が悪用され思わぬ被害を受けたり、プライバシー侵害が起こったりするためです。
- そのほか、不注意な発言により、多くの人から非難を受けたり、自分や所属する組織の評判を失墜させたりする事態を招くこともあります。
- 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起こりえるか、常に意識をしながら、情報発信をするよう心がけましょう。

- SNSには本人確認が徹底していないサービスもあり、実在の人物・組織の名前を使った偽のアカウントや、架空のアカウントで投稿されているケースもあります。偽のアカウントや架空のアカウントを悪用して、不正リンクの投稿などが行われる事例もありますので、SNSで関わるアカウントの相手が本物であるかどうかは、慎重に確認する必要があります。
- SNSサービスによっては、本人確認が行われた上で公式アカウントとして登録されているものもあります。特に公的機関や企業、著名人などの情報を購読する場合には、まず公式アカウントが存在するかを、それぞれの機関のホームページなどで確認してみるとよいでしょう。直接の知人や公式アカウント以外のアカウントで、本人確認ができない場合には、安易にフォロー（購読）したり、友達になったりしないようにしましょう。

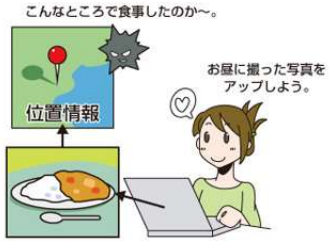
- 短縮URLは、SNSで文字数の制約上URLを短縮して表示する外部のサービスです。本来のURLよりも文字列が短くなり、見た目にも扱いやすくなります。しかし、一見しただけではどのようなサイトにリンクされているかわからないことから、この機能を悪用してフィッシング詐欺やワンクリック詐欺などの悪性ホームページに誘導する手口が確認されていますので、短縮URLをクリックする際には注意が必要です。心配な場合、短縮URLを元のURL表示に戻して確認することのできるWebサービスも提供されています。

- SNSのアプリケーションの中には、インストールの際に、連絡先情報へアクセスする許可を求めてくるものがあります。このようなアプリケーションの中には、個人の連絡先情報を収集して、収集したメールアドレスに迷惑メールなどを送りつけることなどを目的としているものもあります。連絡先情報へアクセスするアプリケーションで、作成者の身元やその利用目的がよくわからないものは、使用を避けるようにした方が良いでしょう。

- プライバシー情報の書き込みに注意しましょう
- 友人間のコミュニケーションを目的としてSNSを利用しているであっても、プライバシー設定が不十分であったり、友人から引用されることなどにより、書きこんだ情報が思わぬ形で拡散する危険性もあります。インターネット上に情報が公開されていることに変わりはないということを念頭に置いて、書き込む内容には十分注意をしながら利用することが大切です。

- 最近のGPS機能のついたスマートフォンやデジタルカメラで撮影した写真には、設定によっては、目に見えない形で、撮影日時、撮影した場所の位置情報（GPS情報）、カメラの機種名など、さまざまな情報が含まれている場合があります。SNSに、こうした位置情報付きの写真をよく確認せずに掲載してしまうと、自分の自宅や居場所が他人に特定されてしまう危険性があり、迷惑行為やストーカー被害などの犯罪の被害に遭う可能性もあるため、十分注意が必要です。

- 写真にどのような情報が含まれているか調べる方法はいくつかありますが、これらを表示するための専用のアプリケーションを利用すると、事前に確認ができます。写真に含まれている情報を編集・削除できるアプリケーションもあります。位置情報もプライバシー情報であるということを十分理解して、むやみに位置情報をつけて写真を投稿しないように心がけましょう。



- SNSの怪しい投稿のリンクに注意しましょう
- SNSは誰でも投稿することができることから、怪しいリンク（ワンクリック詐欺、フィッシング詐欺など）に誘導される危険性があります。投稿した人が実在の信頼できる人であったとしても、他の人が投稿した内容をそのまま再投稿する場合もありますので、元々の情報の発信元の信頼性を意識することが大切です。

- インターネットでは、動画を共有するサイト、リアルタイムで動画を配信しながらチャットやメッセージを交換するサイト、音楽配信サイトや、音声番組をポッドキャストで配信するサイトなど、多数のサービスが存在しています。こうしたサービスは利用者にとって大変魅力的ですが、それらのWebサイトの中には、法令違反になりかねない著作権侵害の音楽や動画が掲載されていたり、悪意のあるサイトへ誘導するものもありますので、利用する場合は注意が必要です。
- 著作権法違反のリスクに注意しましょう
- 違法な動画配信サイトには、権利者に無断でアップロードした動画や、音楽が存在します。こうした著作権法違反の動画や音楽ファイルを、違法性を認識しながらダウンロードする行為も、著作権法違反となります。

- 利用者を悪性ホームページに誘導しようとする攻撃者は、利用者にとって魅力的なサイトを構築して、利用者のアクセスを誘おうとします。例えば、主要な検索サイトで音楽を検索する際に、「Free(無料)」という言葉を追加すると、検索結果が上位に表示されるように細工して、多くの利用者の関心を誘い、ウイルスに感染させる手口が報告されています。
- こうしたサイトでは、動画の再生画面やクリックボタンを模した偽の画像に、悪性サイトへのリンクを仕込み、巧妙に利用者のクリックを誘って、悪性サイトへ誘導する手口も確認されています。実際、動画配信サイトとそっくりに設計された、マルウェアを配信するＷｅｂページは多数報告されています。音楽ばかりでなく、大きな事件や人気スポーツ、映画などのキャッチフレーズで利用者を誘惑し、マルウェア配信サイトに誘導する例もありますので注意が必要です。

- オンラインゲームは、パソコンやスマートフォン・タブレット端末、ゲーム専用機器などから、インターネットを経由して、他のコンピュータとデータを交換しながらゲームを進めるという、コンピュータゲームの一形態です。オンラインゲームにはさまざまなサービス形態のものがありますが、一般的に、パッケージソフトとして購入するゲームと比較すると、オンライン上で複数の人が同時に参加・交流しながらゲームを進めることができる、最初に購入対価を支払うのではなく、月額料金やプレイ内容に応じて課金されることが多い、といった特徴があります。こうしたゲームでは、さまざまなトラブルや危険性も増えています。
- 例えば、子どもが親のパソコンやスマートフォンを使ってオンラインゲームをし、無料だと勘違いして有料のアイテムを購入してしまい、後になって高額な料金が請求される事例が発生しています。
- また、ゲーム内で知らない人にアイテムを売って欲しいと言われ、アイテムのデータを送ったものの、相手から代金の振込がないなどのトラブルもあります。

- 子どもを持つ保護者の方は、子どもがインターネットの世界でどのような行動をしているのかを理解し、目を配るようにしてください。家庭内で、オンラインゲームを含めたインターネットの利用方法についてのルールを定め、年齢に見合った利用の制約を設けることも必要です。

- ゲームの課金の仕組みを理解する。
- ゲームの利用登録は無料でも、ゲームの進行によって、アイテムが有料になるなど、料金が発生する場合がありますので、課金の仕組みをよく理解しましょう。有料課金のゲームを子どもに使わせる場合には、携帯電話やクレジットカードの暗証番号、パスワードを子どもに教えず、親が管理するなどの利用方法を検討してください。
- 知らない人との取引をしない。
- ゲーム内で知り合った人とのアイテムの交換や売買は、特に子どもの場合、その仕組みや代金の徴収方法などを理解しておらず、だまされてアイテムを窃取される場合があります。そもそも多くのゲーム運営会社では、利用規約でゲーム内での通貨やアイテムの取引を禁止しており、禁止行為を行った場合には、ゲーム自体の利用者アカウントが停止するなどの措置を取っています。

- オンラインゲームの詐欺行為に注意しましょう。
- オンラインゲームではチャット機能を使って、悪性サイトに誘導されたり、オンラインゲームのファンサイトが改ざんされ、同じオンラインゲームをしている人がウイルスに感染したり、オンラインゲームの利用者のアイテムを窃取するなどのウイルスに感染する可能性もあります。アカウントが盗まれてアイテムが窃取されるなどの被害も多く発生していますので、こうした詐欺行為には十分注意しましょう。
- チャット機能に注意する。
- オンラインゲーム中のチャット機能はリアルタイムに情報を交換したり、ゲームの方法などを教えあったりする場合に非常に便利な機能です。しかし、子どもたちの間でこうしたチャット機能を使って、発言のやりとりや、アイテムの交換などを行っている場合には、友達同士のトラブルになるケースもありますので、注意が必要です。また、やり取りの中で、出会い系サイトに誘導されるなど、犯罪に巻き込まれることもあるので気軽に自分の個人情報やプライバシー情報を教えることはやめましょう。

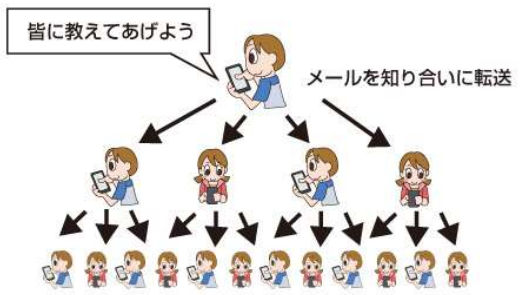
- 受信者が望んでいないにもかかわらず、一方的に送信されてくる電子メールのことを迷惑メールと呼んでいます。いわゆる「出会い系サイト」やドラッグなどの商品の宣伝などを内容とする電子メールが多く、スパムメールとも呼ばれます。
- これらの電子メールは、昼夜を問わずに届けられ、電子メールをダウンロードするために時間がかかるなど、受信者側に大きな負担をかけるため、最近では社会問題のひとつになっています。また、いやがらせのために送りつけられる大量の無意味な電子メールも、迷惑メールの一種といえます。
- 迷惑メールの対策としては、ホームページのアンケートや電子掲示板などにメールアドレスをむやみに掲載しないことや、使用するメールアドレスは、わかりにくいものにするなどが考えられます。
- さらに注意が必要なのは、このような迷惑メールで送信される内容をうかつに信用してはいけないということです。これらの電子メールの中には、無限連鎖防止法に抵触するもの（いわゆるねずみ講）や詐欺行為を目的としているものもあります。

- 最近では、携帯電話やSNSのメッセージでの迷惑メールの急増が問題化しています。このような迷惑メールを受信しないようにするためには、
- 長く複雑なメールアドレスを使用する。
- 指定したドメインやメールアドレスからの電子メールのみ受信するように設定する。
- 必要以上に自分のアドレスを他人に漏らさない。
- SNSのメッセージでの迷惑メールの場合は、利用しているSNSサービスの機能を使って、メッセージを拒否する、もしくは相手をブロックする。
- など、利用者側でできる自衛策も大変有効です。携帯電話による迷惑メール対策の一環として実施してみましょう。
- 携帯電話番号を使って送られてくるSMS（ショートメッセージサービス）の迷惑メールの場合は、携帯電話会社のサービスを使って、電話番号によるブロック設定をすることが有効です。

- パソコンの場合には、以下のような対応策が考えられます。
- インターネットサービスプロバイダでメール受け取りの拒否条件設定による受信制限をかける。
- インターネットサービスプロバイダによる迷惑メールフィルタを使用する。
- 統合セキュリティ対策ソフトによる迷惑メールフィルタを使用する。
- 迷惑メールフィルタを使用すると、電子メールの内容を分析して、迷惑メールと判断された場合には、件名に「SPAM」や「MEIWAKU」などの文字列が追加されます。電子メールソフトで、件名にこれらの文字列が付けられた電子メールを自動的に分類する設定を行うことで、迷惑メールを通常の受信用ボックスから除外することが可能になります。ただし、迷惑メールフィルタは、定められたロジックや蓄積された情報によって迷惑メールであると判定するため、常に正しい判断が行われるわけではないという点に注意しなければなりません。

- 受信者の望んでいない広告メールを送信する際には、「今後送信を必要としない場合にはこちらのメールアドレスまでご連絡ください」といった内容を記載することが法律で義務付けられていますが、その意思を伝える際には、相手側に氏名・住所などの個人情報をむやみに開示しないように気を付けましょう。悪意を持って、迷惑メールを送信してくる業者は、このような意思を伝えた際に、その送信元の電子メールアドレスが使われていることを確認できることにもなります。そして、その後も迷惑メールが送信され続けるという被害も起こっています。

- チェーンメールとは、電子メールを受け取った人が次々に知人に電子メールを転送することで、ねずみ算式に広まっていく電子メールのことです。多くの場合、チェーンメールには、「すぐに友達に教えてあげてください」や「できるだけ多くの人に広めてください」「すぐに10名に転送しないと、あなたは不幸になります」などのように、電子メールの転送を促す言葉が付いています。
- チェーンメールの内容は、ほとんどがデマ情報やいたずらであったり、「あるテレビ番組の企画です」、「すぐにお金儲けができます」など詐欺的な内容のものですが、募金の呼びかけや輸血のお願いなど、本来は善意の電子メールがいつの間にかチェーンメールとして広まってしまうケースもあります。最近では、SNSでも同様に、リツイートやシェアなどの機能で、デマ情報が広まってしまうケースが出ています。



- チェーンメールへの対策としては、身に憶えのないメールや不審なメールが送りつけられてきたら、まず次のことはしないように心掛けましょう。
- メールのURLはクリックしない
- メールの添付ファイルは開かない
- メールに返信しない
- メールは転送せず、削除する。
- こうしたチェーンメール対策は、自分自身が被害にあわないようにするとともに、被害をそれ以上広げないための重要なマナーです。相手にメールの転送を強要する行為は、メールの内容にかかわらず、迷惑行為であるといわざるをえません。人間関係や信用に傷がつくことにもなりかねませんので、勇気を持って転送しないようにしましょう。

- 電子メールはメッセージやデータを簡単に交換できる利便性の高いサービスですが、送り先を間違えてしまうと、他人にメールが届き、結果的に情報漏洩（ろうえい）につながってしまう危険性もあります。また、複数の相手に同時にメールを送る際に、操作を誤って、本来は秘密にしなければならないそれぞれのメールアドレスが見える状態で送ってしまった場合も、やはり個人情報の漏洩につながります。

- 電子メールを送る場合、まずは TO: 、CC: 、BCC: の違いを理解する必要があります。 TO: や CC: は、電子メールを受け取った人には、自分以外の誰宛てに送信されたメールかがわかります。このため一度に複数の人宛てに送る場合で、他の人のメールアドレスがわかると困る場合は BCC: を使います。この利用方法を間違えると、関係のない第三者にメールアドレスが知られてしまい、個人情報の漏洩事案となってしまう可能性があります。

- 電子メールの誤送信の対策は、以下の通りです。
- メールアドレスの宛先（TO: 、CC: 、BCC:）の設定を間違えないように利用する。
- 個人情報やプライバシー情報が含まれた電子メールを安易に送信しない。
- 誤送信した場合に第三者に電子メールを見られる可能性があるため、添付ファイルなどを送る場合は、ファイルを暗号化したり、添付ファイルにパスワードを設定する。
- メールアドレスの誤入力など、意図しない宛先に電子メールが送信されてしまうことを防ぐため、送信する際に宛先などを確認する画面を開くように、あらかじめ電子メールソフトに設定する。