総務省 安心してインターネットを使うために

国民のためのサイバーセキュリティサイト

基礎知識

ここでは、インターネットを使った身近なサービスの仕組みや、インターネットの利用に伴う危険、インターネットを安全に使うための基本的な対策などについて説明します。

基礎知識

I.　インターネットを使ったサービス

ここでは、情報セキュリティ対策を立てるための基礎知識として、インターネットや、インターネットを使ったサービスの仕組みについて説明します。

インターネットって何？

インターネットは、世界中のコンピュータなどの情報機器を接続するネットワークです。1990年ごろから、世界的に広く使われ始め、近年はその利活用が目覚しく進展してきました。現在では、私たちの生活や仕事などのさまざまな場面で使われる、不可欠な社会基盤（インフラ）となっています。

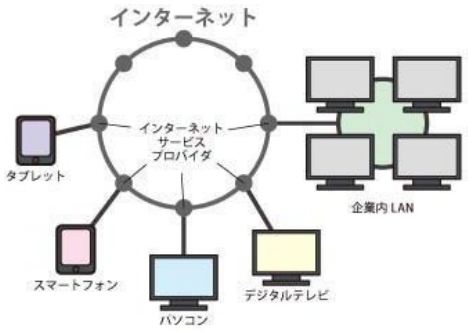
私たちがインターネットを利用するためには、さまざまな方法があります。家庭や学校、職場で利用する場合には、インターネットサービスプロバイダ（光回線、ADSL回線、ケーブルテレビ回線などを通じて、インターネットに接続してくれるサービス事業者）と契約することによって、インターネットに接続できるようになります。携帯電話会社と契約することで、携帯電話回線を通じてインターネットを利用することもできます。

次のページでは、インターネットの仕組みについて説明します。

インターネットの仕組み

複数のコンピュータを、ケーブルや無線などを使ってつなぎ、お互いに情報をやりとりできるようにした仕組みをネットワークと呼びます。

インターネットは、家や会社、学校などの単位ごとに作られた1つ1つのネットワークが、さらに外のネットワークともつながるようにした仕組みです。外のネットワークと接続するために、ルータと呼ばれる機器や、インターネットサービスプロバイダと呼ばれる通信事業者のサービスを利用します。世界規模でコンピュータ同士を接続した、最も大きいネットワークといえます。



ネットワーク上で、情報やサービスを他のコンピュータに提供するコンピュータをサーバ、サーバから提供された情報やサービスを利用するコンピュータをクライアントと呼びます。私たちが普段使うパソコンや携帯電話、スマートフォンなどは、クライアントにあたります。

インターネット上には、メールサーバやWebサーバといった、役割の異なる多数のサーバが設置されています。それらのサーバが、クライアントからの要求に従って、情報を別のサーバに送ったり、持っている情報をクライアントに渡したりすることで、電子メールを送信したり、Webブラウザでホームページを見たりすることができるようになっているのです。

インターネットでは、コンピュータ同士が通信を行うために、TCP/IP（ティーシーピー・アイピー）という標準化されたプロトコルが使われています。プロトコルとは、コンピュータが情報をやりとりする際の共通の言語のようなものです。この仕組みのおかげで、インターネット上で、機種の違いを超えて、さまざまなコンピュータが通信を行うことができるようになっています。

インターネットで、情報の行き先を管理するために利用されているのが、それぞれのコンピュータに割り振られているIPアドレスと呼ばれる情報です。このIPアドレスは、世界中で通用する住所のようなもので、次の例のように表記されるのが一般的です。

IPアドレスの例：198.51.123.1

ところが、このIPアドレスは、コンピュータで処理するのには向いていますが、そのままでは人間にとって扱いにくいので、ホームページや電子メールを利用するときには、相手先のコンピュータを特定するために、一般的にドメイン名が使われています。

ドメイン名を使用した記述方法では、例えばホームページのアドレスでは“www.soumu.go.jp”のように指定します。ネットワーク上には、これらのドメイン名とIPアドレスを変換する機能を持つサーバ（DNSサーバ）があり、ドメイン名をIPアドレスに自動的に変換することで、電子メールの送り先や

ホームページの接続先を見つける仕組みになっています。

【コラム】

近年、インターネットに接続する情報機器が爆発的に増えてきたことで、IPアドレスが足りなくなってきていることが問題になっています。使えるIPアドレスの数を増やすために、IPアドレスの桁数を増やしたIPv6という規格が徐々に導入されてきています。

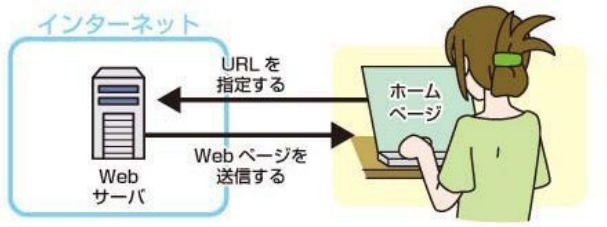
IPv6方式のIPアドレスは、例えば「2001:db8:bb5c:8008:2013:a219:2210:8103」のように表記します。

ホームページの仕組み

インターネット上で情報を公開する仕組みを、ホームページと言います。ホームページのコンテンツ（内容）は、インターネット上に点在する、Webサーバというホームページ公開専用のコンピュータのなかに保存されています。私たちの端末から、そのパソコンに命令を出し、情報を送ってもらうことで、ホームページを見ることができます。

ここでいうホームページとは、Webサイトと呼ばれるインターネット上のひとまとまりのWebページのことです。元々は、Webサイトの入り口のページをホームページと呼んでいましたが、日本ではWebサイトと同じ意味で使われるようになりました。

ホームページを閲覧する場合には、Webブラウザという専用のソフトウェアでURLを指定します。URLを指定すると、Webブラウザがインターネット上のWebサーバを探して、目的のホームページをコンピュータの画面上に表示します。



URLは、「https://www.soumu.go.jp/joho_tsusin/joho_tsusin.html」のように指定します。「https」は、ホームページの閲覧に使用されるHTTPSというプロトコルを表しています。「www.soumu.go.jp」はWebサーバを指定しています。その後の「/joho_tsusin/joho_tsusin.html」がWebサーバの中のホームページの情報が保存されている場所を表しています。このようなURLをWebブラウザで指定することで、自分が見たいWebサイトへ接続できるのです。

URLの最後には「.htm」や「.html」という表記がよく見られますが、これはそのホームページが、主にHTML形式のファイルで作られていることを表しています。このHTMLファイルの中には、画像や動画、音声などのマルチメディア情報を指定することができ、これにより、ホームページ上で多彩で動きのあるコンテンツを利用することができるようになります。

また、Webページを見るのに、1つ1つちがうURLをWebブラウザに入力するのは大変です。そこで、Webページの中のテキストやイラスト、図などにURLの情報を埋め込んで、ここをクリックしてもらうことで、利用者を別のWebページに誘導することができます。この仕組みはハイパーリンク（リンク）と呼ばれています。これにより、現在見ているWebページから、関連する他のWebページやWebサイトに移動することができるようになります。

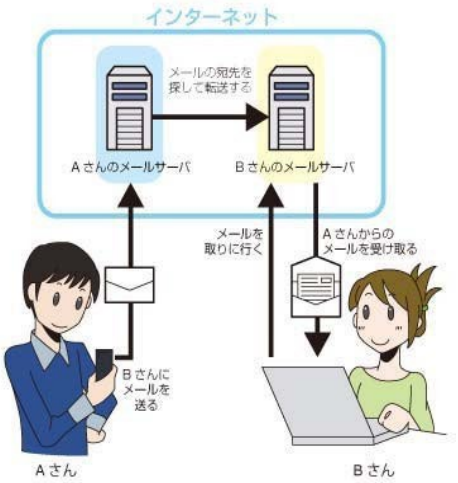
電子メールの仕組み

電子メール(e-mail)とは、パソコンや携帯電話、スマートフォンなどの情報機器同士が、専用のメールソフトを使って、インターネットなどのネットワークを利用して情報をやりとりする機能です。やりとりできる情報は文章（テキスト）だけでなく、文書ファイルや画像などを添付ファイルとして扱うことができます。

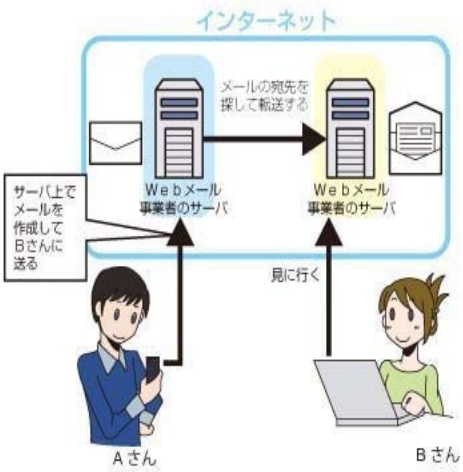
電子メールを送る際には、送り先のコンピュータを指定するためにアドレスを使います。電子メールのアドレスは、一般的に”xxx@example.co.jp”のように表記されます。@の後には、所属する組織や利用しているインターネットサービスプロバイダなどの事業者のドメイン名が一般に使われます。また、一般的なメールソフトを使うのではなく、Web上でWebブラウザを使って送受信を行うWebメールという方式もあり、フリーメールサービスとして広く普及しています。

電子メールの送受信は、インターネット上の多くのメールサーバが連携することによって実現しています。

電子メールを送信すると、契約しているインターネットサービスプロバイダ、学校や会社にあるメールサーバにデータが送られます。電子メールを受け取ったメールサーバは、宛先として指定されているインターネットサービスプロバイダなどのサーバに、そのデータを転送します。電子メールを受け取ったサーバは、受取人が電子メールを取りにくるまで、サーバ内にデータを保管するようになっています。
電子メールの受取人は、契約しているインターネットサービスプロバイダのメールサーバにある自分のメールボックスに自分宛の電子メールを取りに行きます。



Webメールでは、送受信された電子メールがサーバに蓄積されます。利用者は、WebサーバにWebブラウザで接続することで、受信したメールの閲覧や、新規メッセージの作成・送信などができるようになります。



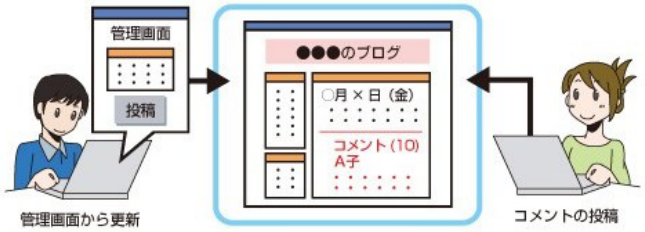
ブログの仕組み

ブログは、自分の考えや社会的な出来事に対する意見、物事に対する論評、他のWebサイトに対する情報などを公開するためのWebサイトのことです。当初は、個人サイトで利用されていましたが、最近では企業でも自社の情報を公開したり、新しい商品やサービスの情報を公開したりする場合に利用されることが増えてきました。基本的に、ブログはこれまでのホームページを公開する技術をそのまま利用しているため、閲覧する側は通常のWebブラウザだけで見ることができます。

ブログという用語は、「Weblog」（ホームページの履歴の意味）から派生した言葉であると言われています。そして、ブログで情報を発信する人のことをブロガー（blogger）と呼んでいます。なお、ブログという言葉は、明確に決められた使い方をされているわけではなく、日記風に情報を追加しているホームページもブログに含むことがあります。

これまでのホームページでは、新しく情報を追加する場合に、自分のコンピュータで変更するWebページのHTMLファイルを編集して公開していました。これに対して、ブログではインターネット上の管理者用のWebサイトに新しい情報を登録するだけで、自動的に日記風に情報を追加することができるようになっています。

このような技術を採用することにより、HTMLファイルの知識やホームページ作成ソフトの利用方法を知らなくても、簡単に情報を公開するWebサイトを構築することができることから、新たな利用者層がブログを利用するようになりました。



ブログのシステムでは、管理者が書き込んだ情報はデータベースに保存され、閲覧者がブログを訪問すると、データベースに保存されている情報から毎回ホームページを生成し直すので、追加された情報をすぐに見ることができます。

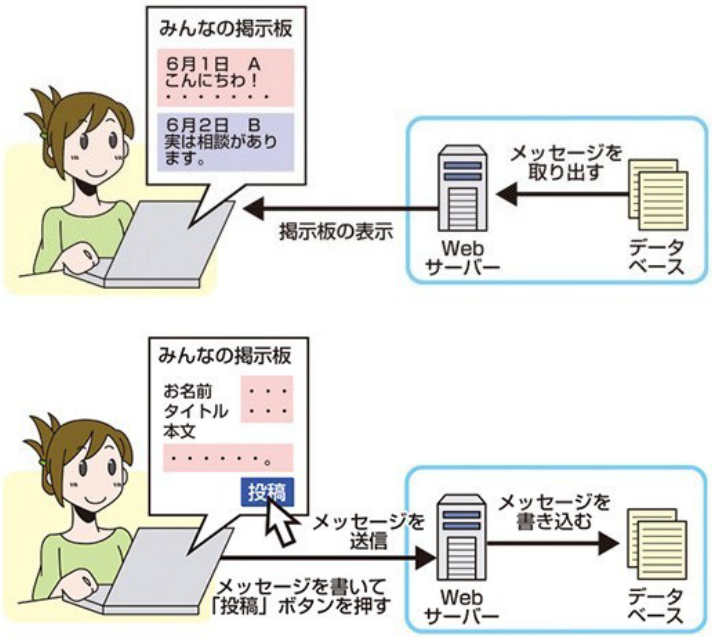
さらに、ブログの多くは、書き込まれた情報に対して、「コメント」を登録できるようになっています。コメントはこれまでの電子掲示板に近い技術ですが、ブログに登録されたそれぞれの情報に対して、閲覧者が意見や追加の情報を書き込むことができるようになっています。このコメントの機能により、ブログは、発信された情報や意見に対するディスカッションを行う目的にも利用できるようになり、新しいコミュニケーションの場所として活用されています。

一方で、近年のブログでは、アフィリエイトと呼ばれる、ブログを書いている人が、ある企業やその製品の紹介をすることで報酬を受ける仕組みが導入されている例も多くあります。このような場合、ブログから情報を得る際には、書かれている情報をそのまま鵜呑みにすることなく、閲覧側がその内容の信憑性を判断するなどの注意も必要になります。

電子掲示板の仕組み

電子掲示板とは、インターネット上で記事（スレッドやトピックなどと呼ばれています）を書き込んだり、閲覧したりできる仕組みです。単に「掲示板」と呼んだり、「BBS」(Bulletin Board Systemの略語)とも呼ばれたりしています。個人が開設するものや企業の中だけに限定したものなど小規模なものから、多数の電子掲示板を集めて一つのWebサイトとして発展させた大規模なものまで、さまざまな電子掲示板が存在します。大規模なものは、投稿された記事の内容が社会的な影響を与えることもあります。

電子掲示板では、書き込まれたメッセージはWebサーバ経由でデータベースに蓄積され、別の訪問者が記事を参照すると、新たなメッセージが追加された状態で表示されます（コメントやレスと呼ばれています）。このような仕組みによって、ホームページの内容が常に最新のデータに自動更新されるため、駅の伝言板のような利用が可能になります。



電子掲示板には、使用しているプログラムによってさまざまなタイプのものがあります。その中でももっとも一般的な表示方法は、伝言板型とツリー型です。

伝言板型は、駅の伝言版に書き込むような使い方ができる簡単なものです。書き込まれたメッセージは、新しい順に連続して表示されます。

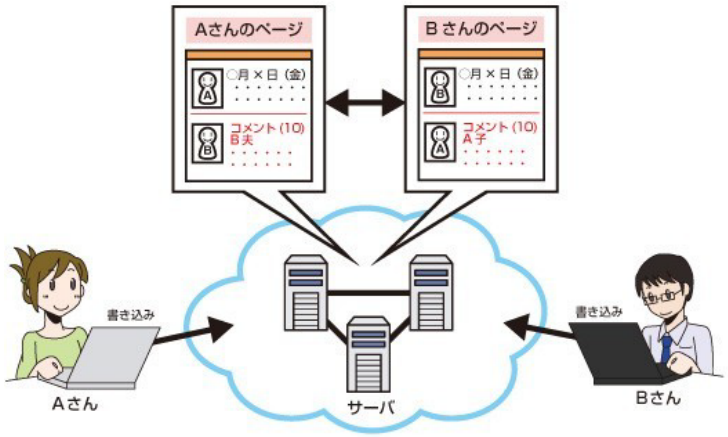
ツリー型は、特定の話題ごとに個別のまとまりで表示する電子掲示板です。それぞれのメッセージに対する返事を書き込むことで、自動的にメッセージのツリーができあがります。この形式は、特定の情報に対して、討論を繰り返す場合などに有効な表示方法です。

電子掲示板では、多くの場合、本名ではない名前（ハンドルネームやニックネームと呼ばれます。）で書き込みが行われます。そのために、面白半分で他人の書き込みに対して挑発や反論をする「荒らし」行為や、特定の個人のプライバシー情報を書き込むなどの行為が行われることがあり、他にも不用意な書込みにより多くの人から非難を浴びるような状況である「炎上」が起こることもあります。利用の際には、書き込む内容に注意をすることが必要です。

SNS（ソーシャルネットワーキングサービス）の仕組み

SNSは、ソーシャルネットワーキングサービス（Social Networking Service）の略で、登録された利用者同士が交流できるWebサイトの会員制サービスのことです。友人同士や、同じ趣味を持つ人同士が集まったり、近隣地域の住民が集まったりと、ある程度閉ざされた世界にすることで、密接な利用者間のコミュニケーションを可能にしています。最近では、会社や組織の広報としての利用も増えてきました。

多くのSNSでは、自分のホームページを持つことができ、そこに個人のプロフィールや写真を掲載します。ホームページには、公開する範囲を制限できる日記機能などが用意されていたり、アプリケーションをインストールすることにより、機能を拡張したりすることもできます。その他、Webメールと同じようなメッセージ機能やチャット機能、特定の仲間の間だけで情報やファイルなどをやりとりできるグループ機能など、多くの機能を持っています。さらに、これらの機能はパソコンだけではなく、携帯電話やスマートフォンなど、インターネットに接続できるさまざまな機器で、いつでもいろいろな場所で使うことができます。



最近では、SNSの1つとして提供されることもある、利用者同士が交流しながら遊べるソーシャルゲームも普及しています。

SNSは、とても身近で便利なコミュニケーション手段であると言えますが、最近ではアカウントの不正利用や、知り合い同士の空間であるという安心感を利用した詐欺やウイルス配布の被害にあうなどの事例が発生しているため、注意が必要です。

また、友人間のコミュニケーションを目的としてSNSを利用している場合であっても、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。

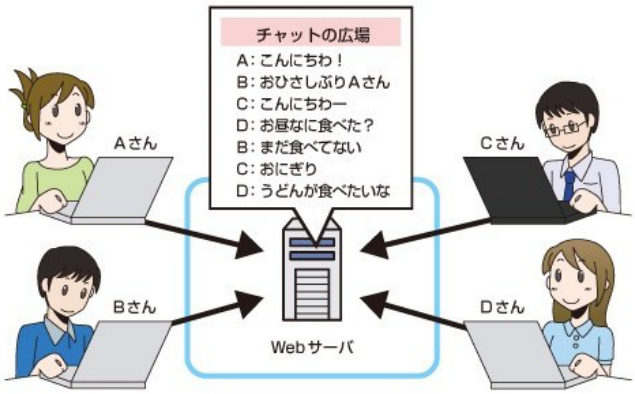
チャットの仕組み

チャット（chat）は、インターネットでよく利用されるサービスのひとつで、本来は“おしゃべり”という意味の言葉です。インターネットでは、複数の利用者がリアルタイムにメッセージを送信するためのシステムをチャットと呼びます。

チャットをする場合は、一般にインスタントメッセンジャーと呼ばれるアプリケーションを使ってやりとりします。現在のチャットシステムでは、チャットサーバに接続すると、参加者が入力したテキストのメッセージがリアルタイムに表示される仕組みを提供していることが多いようです。

システムとしては、電子掲示板と非常によく似ていますが、誰かがメッセージを入力すると、即座にすべての参加者に送信されるため、数人の友だちの間で会話をするように使うことができます。

最近では、パソコンやスマートフォンで使える無料通話アプリケーションやSNSを通じて、チャットをしている利用者も増えています。

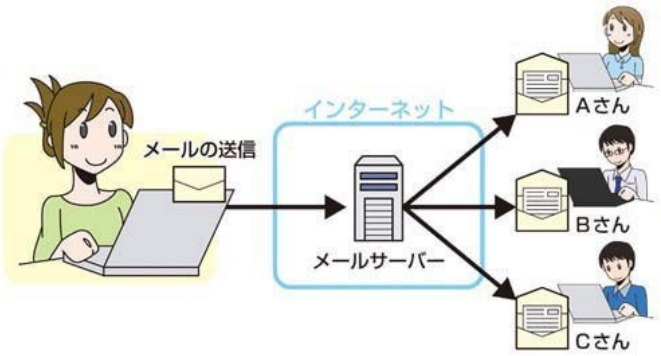


メーリングリストの仕組み

メーリングリストは、電子メールを利用したコミュニケーションツールです。通常の電子メールで複数の相手に電子メールを送る場合には、全員分のメールアドレスを指定して送信しますが、メーリングリストでは専用のメールアドレスに送信することで、そのメーリングリストに登録されているすべてのメールアドレスに同時に送信することができます。

メーリングリストでは、投稿した電子メールは全員に送信されるため、特定の相手に対して返信したつもりでも、すべての参加者にその電子メールが送信されることになります。

また、最近はメーリングリストにウイルス付きの電子メールが投稿されて、参加者全員にウイルスが配信されてしまうというトラブルが発生しています。メーリングリストに参加する場合には、他の利用者に対する責任があるということを認識しておかなければなりません。



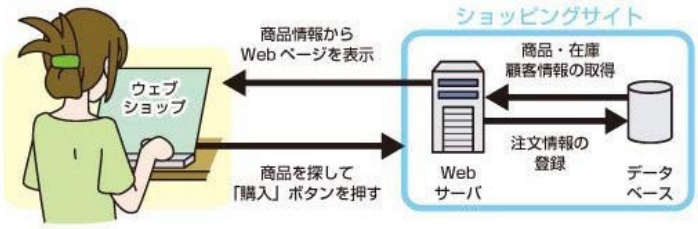
ショッピングサイトの仕組み

ショッピングサイトは、インターネット上で買い物ができるホームページです。ほとんどのショッピングサイトでは、Webサーバとデータベースサーバが連携して動作しています。データベースサーバには、顧客情報、商品情報、在庫情報、販売情報などが保管され、Webサイトの訪問者が入力した情報が、リアルタイムにデータベースに書き込まれ、更新されます。

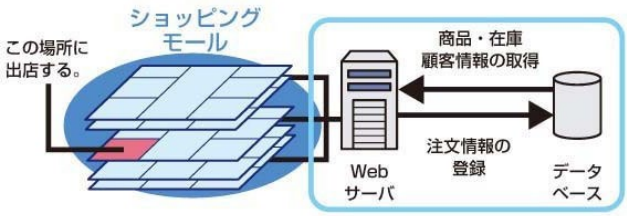
実際のショッピングサイトでの購入の流れは、以下のようになります。

まず、訪問者が商品を購入すると、購入情報（購入者の顧客情報や購入商品とその在庫情報）がデータベースに登録されます。すると、ショッピングサイト側は、利用者に購入受付が完了したことをホームページの画面上または電子メールなどで通知し、受注情報をショップの管理者側に通知します。ショップの管理者は、この情報から受注・決済などの処理（在庫確認、受付通知、入金確認など）をします。さらに、受注処理をもとにデータベースの情報処理経過や在庫数更新など）を更新し、これらの処理の経過状況を購入者に電子メール等で通知します。そして、商品の発送処理（発送準備、発送など）や請求処理を行い、購入者に商品が届けられることになります。

こうしてショップの管理者は、データベースに保存された情報をもとに注文を受けてから発送完了までをショッピングサイトのプログラムを通して情報を更新しながら、並行して実際の処理をしていく流れになります。



また、ショッピングモールと呼ばれるショッピングサイト群があり、ここではその管理会社がWebサーバやデータベースサーバを用意して、ショッピングサイトの仕組みを提供しています。そのため、ショッピングサイトは、このような仕組みを利用するだけではなく、自身で開設することもできます。個人や中小の商店でも、所定のホームページを作成するだけで、簡単にショッピングサイトを開設できるようになっています。



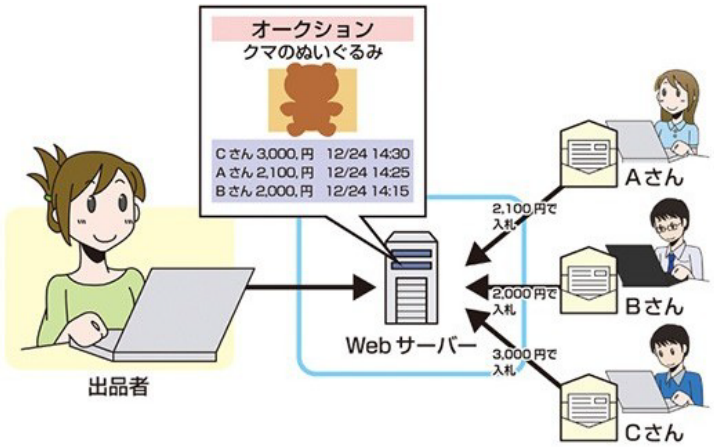
一般にショッピングサイトでは会員登録が必要となります。これにより、購入者は都度自分の発送先や決済情報の登録をせず利用ができ、ショップの管理者側は顧客管理などが効率的に行うことができます。しかし、これはお互いにとって重要な情報を預けたり預かったりすることでもあります。預ける側は提供する情報の内容について、預かる側は保存し利用する情報の厳重な管理について注意が必要になります。

ネットオークションの仕組み

ネットオークションとは、インターネット上で行われるオークションのことです。出品されている商品の中から、気に入った品物を自分の指定した金額で入札することができます。

一般的なオークションサイトでは、現在の最高価格が表示されており、その価格よりも高い金額であれば入札できるといった仕組みを設けています。そして、あらかじめ決められた期間、入札を受け付けて、最終的にもっとも高い金額をつけた利用者がその商品を購入できます。

また、オークションサイトによっては、参加者が自分の商品を出品することもできるようになっており、新しい形のフリーマーケットとして多くの人に利用されるようになってきました。



ただし、ネットオークションでは、盗品や違法な薬物などが出品されたり、ブランド品などを架空出品して代金をだまし取るなどの詐欺行為が行われることがあるほか、利用者同士のやりとり上のトラブルが発生しています。

一般的な商店での購入と異なり、販売者の顔が見えないため、怪しげな出品にだまされないよう、オークションサイトでの販売者の過去の取引評価などを参考にしながら、慎重に利用しましょう。

インターネットバンキングの仕組み

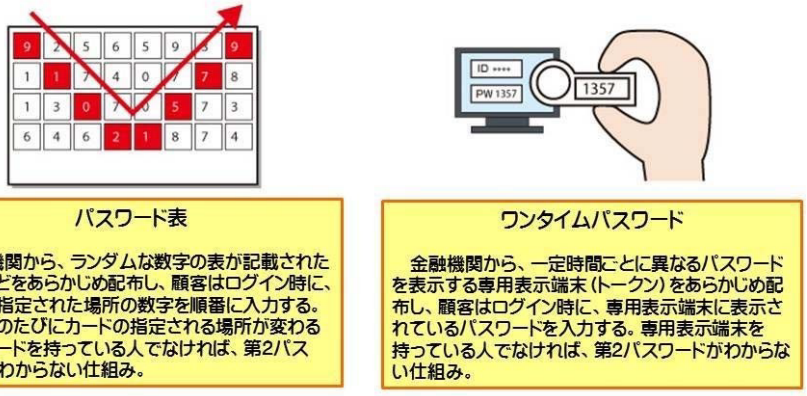
インターネットバンキングは、インターネットを利用した銀行などの金融取引のサービスです。オンラインバンキングとも呼ばれることがあります。パソコンだけでなく、携帯電話やスマートフォンなどからも利用できるサービスが多くなっています。

インターネットバンキングでは、銀行の窓口やATMに行かなくても、自宅や外出先などで、銀行の営業時間を気にすることなく振込や残高照会などをすることができます。このような便利さから、インターネットバンキングの利用は急速に拡大しています。

インターネットバンキングでは、利用者を識別するために、ATMでよく使われているキャッシュカードや暗証番号の代わりに、ID（契約者番号など）とパスワードでサービスを利用します。第2パスワードなど複数のパスワードや、専用機器やスマートフォンアプリによって表示されるワンタイムパスワードなどの多要素認証が導入され、なりすましなどの不正がないように管理されています。

しかし、利用の拡大に伴い、危険性も増大しています。特に、フィッシング詐欺では、このインターネットバンキングという利用形態が最も狙われているサービスの1つとなっています。代表的な手口としては、電子メールで金融機関を名乗り、利用者のIDやパスワードなどアカウント情報の確認や更新を要求し、情報を盗み取ろうとするものや偽のページに誘導しIDやパスワードの入力を要求し情報を盗み取ろうとするものがあります。

第2パスワードの例

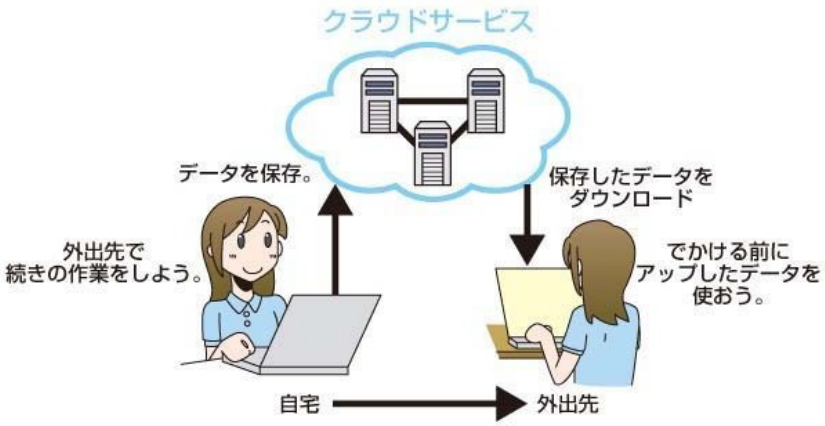


このような手口による被害にあわないよう、金融機関を名乗ってパスワード等の入力を求める電子メールや偽のページに対しては、決して情報を入力してはいけません。その金融機関のWebサイトや問合せ窓口で確認するなどの注意をするようにしましょう。また、最近ではインターネットバンキングを狙ったウイルスへの感染による被害も拡大しているため、注意が必要です。

クラウドサービスとは？

クラウドサービスは、従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、サービスとして利用者に提供するものです。利用者側が最低限の環境（パーソナルコンピュータや携帯情報端末などのクライアント、その上で動くWebブラウザ、インターネット接続環境など）を用意することで、どの端末からでも、さまざまなサービスを利用することができます。

これまで、利用者はコンピュータのハードウェア、ソフトウェア、データなどを、自身で保有・管理し利用していました。しかし、クラウドサービスを利用することで、これまで機材の購入やシステムの構築、管理などにかかるとされていたさまざまな手間や時間の削減をはじめとして、業務の効率化やコストダウンを図れるというメリットがあります。



クラウドサービス（特に、以下の分類でいうIaaS）では、主に仮想化技術が使われています。仮想化技術とは、実際に存在する1台のコンピュータ上に、ソフトウェアの働きにより、何台もの仮想のコンピュータがあるかのような働きをさせることができる技術です。逆に複数台のコンピュータをあたかも1台であるかのように利用することもできます。この技術により、利用者は、クラウドサービス事業者が保有するコンピュータの処理能力を、柔軟に必要な分だけ利用することができます。利用者から見て、インターネットの先にある自分が利用しているコンピュータの形態が実際にどうなっているのか見えづらいことを、図で雲のかたまりのように表現したことから、「cloud＝雲」という名称がついたと言われています。

クラウドサービスは、主に以下の3つに分類されています。

■ SaaS（サース、サーズ：Software as a Service）

インターネット経由での、電子メール、グループウェア、顧客管理、財務会計などのソフトウェア機能の提供を行うサービス。以前は、ASP（Application Service Provider）などと呼ばれていました。

■ PaaS（パース：Platform as a Service）

インターネット経由での、仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うサービス。

IaaS（アイアース、イアース：Infrastructure as a Service）

インターネット経由で、デスクトップ仮想化や共有ディスクなど、ハードウェアやインフラ機能の提供を行うサービス。HaaS（Hardware as a Service）と呼ばれることもあります。

クラウドサービスは、企業が情報資産を管理する手段として急速に普及しています。また、個人が利用するインターネット上のさまざまなサービスが、意識するかどうかにかかわらず、クラウドサービス上で稼働するようになっています。

クラウドサービスを利用する場合には、データがクラウドサービス事業者側のサーバに保管されているということ、インターネットを介してデータなどがやりとりされることなどから、十分な情報セキュリティ対策が施されたクラウドサービスの選択が重要であるということを理解した上で利用することが大切です。

スマートフォンとは？

従来の携帯電話に代わって、スマートフォンが急速に普及しています。従来の携帯電話とスマートフォンでは、デザインだけでなく、機能にもいろいろな違いがあります。

スマートフォンとは、従来の携帯電話に比べてパソコンに近い性質を持った情報機器です。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たり、アプリケーションを追加することによって機能を自由に追加したりすることができます。また、タッチパネルを使い、画面の拡大やスクロールなど直感的な操作が可能です。

外出先でもさまざまな機能を使うことができる便利なスマートフォンですが、スマートフォンには危険なアプリケーションをダウンロードすることなどで、ウイルスに感染する危険性があります。もともと携帯電話には、アドレス帳やメールの内容など、さまざまなプライバシー情報が保存されています。さらに、スマートフォンでは、大切な仕事上のデータや位置情報などが蓄積されるようになってきているため、情報漏洩（ろうえい）を引き起こすウイルスなどに感染しないよう、よりいっそう利用にあたって注意することが大切です。

スマートフォンのメリットとデメリット

また、スマートフォンと同様に普及しているものにタブレット端末があります。タブレット端末は、スマートフォンと同様にタッチパネルでの操作、アプリケーションの追加などができますが、スマートフォンよりもさらに大きな画面での操作が可能です。また、スマートフォン以上の機能も備えており、それ単体でパソコンに近い処理能力を備えている情報機器です。

スマートフォンやタブレット端末で利用するアプリケーションは、より便利なサービスを提供するために、利用者側の連絡先情報や位置情報などを使っているものも多くあります。そうしたアプリケーションは、利用者自身が事前に利用範囲の承認をするようになっていますが、便利なサービスを利用できる代わりに、プライバシー漏洩などにつながる危険性が高くなるということを知っておかなければなりません。

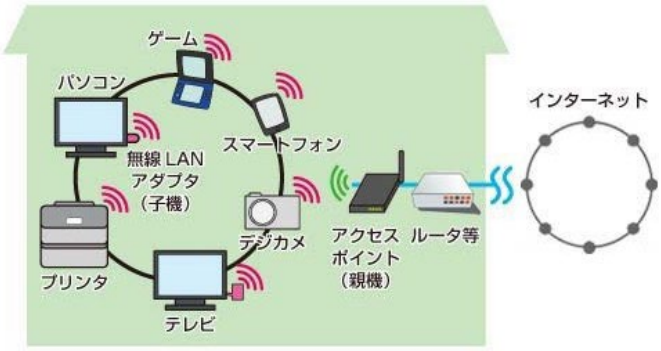
このほか、スマートフォンは、携帯電話会社のネットワーク以外に、無線LANを使ってもインターネットに接続することができます。無線LANは、適切な設定をしないまま使用すると、通信を傍受されるなどの危険性がありますので、情報セキュリティ対策をしっかり取ることが大切です。

無線LANの仕組み

無線LANとは、電波でデータの送受信を行う構内通信網（LAN：Local Area Network）のことです。LANとは、会社内や家庭内などでパソコンやプリンタなどをつないで、データをやりとりできるようにしたネットワークのことです。ケーブルの代わりに無線通信を使うのが無線LANです。

Wi-Fi（ワイファイ、Wireless Fidelity）とも呼ばれますが、これは無線LANの普及促進を行う業界団体Wi-Fi Allianceから相互接続性などの認証を受けた機器のことです。現在はWi-Fi認証を得た製品が増えたことから無線LAN全般を「Wi-Fi」と呼ぶことが多くなりました。

無線LANを利用することにより、ケーブルを気にすることなく、どこでも好きな場所に移動してインターネットに接続し、気軽にWebサイトの閲覧やメールの利用ができるようになりました。また、最近は公衆無線LANの整備も進み、駅、空港などの公共の場でも無線LANが利用できるようなっています。さらに最近ではスマートフォンやタブレット端末の利用者の増加により、急増するトラフィックを軽減するためのオフロード対策の一つとして注目されています。



無線LANを利用するためには、親機（アクセスポイント）と、パソコンなどの端末に装着する子機が必要ですが、最近はほとんどの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いるため、親機があれば無線LANが利用できます。

【コラム】

無線LANの子機同士が、アクセスポイントを介さずに直接通信を行うこともできます。これはアドホック・モードと呼ばれ、携帯型ゲーム機で対戦型のゲームをする際などに利用されています。

参照 一般利用者が安心して無線LANを使用するために
企業等が安心して無線LANを導入・運用するために

Ⅱ.どんな危険があるの？

インターネットにはどんな脅威があるのでしょう。

まず、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。

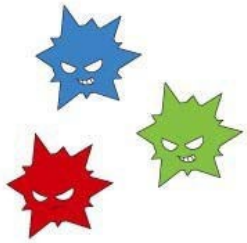
その他にも、コンピュータやソフトウェアの不具合などによる障害、社員や職員の過失などによる事故、火災や台風など自然災害など、インターネットにおける危険性は多くあります。

ここでは、インターネットにおける主な危険性について説明していきます。

ウイルスとは？

ウイルスは、人が病気になるときの病原体のひとつですが、コンピュータの世界のウイルスとはどのようなものなのでしょうか。

ここでは、情報セキュリティの対策を立てる上で避けては通れないウイルスについて、その動作、過去に発生したウイルスの解説、その対策について説明します。



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。狭義のウイルスは、医学上のウイルス同様、コンピュータに侵入して増殖する動きをしますが、利用者が意図しない（大抵は被害を及ぼす）特殊なプログラムには、ボット、ランサムウェア、キーロガー、スパイウェア、トロイの木馬などの種類があり、これらをまとめて「広義のウイルス」と呼ぶこともあります。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。

ウイルスの中には、何らかのメッセージや画像を表示するだけのものもありますが、危険度が高いものの中には、ハードディスクに保管されているファイルを消去したり、コンピュータが起動できないようにしたり、パスワードなどのデータを外部に自動的に送信したりするタイプのウイルスもあります。

そして、何よりも大きな特徴としては、「ウイルス」という名前からも分かるように、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自身の機器のソフトウェアを最新の状態にしておく必要があります。またウイルス対策ソフトを導入するといった手段もあります。ウイルス対策ソフトは、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更新しておかなければなりません。

ウイルスの感染経路と主な活動

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。

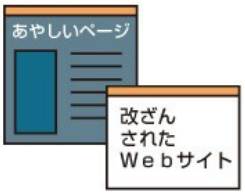
ここでは、主なウイルスを感染経路と活動方法によって分類してみましょう。

ウイルスの感染経路　　ウイルスの主な活動

ウイルスの感染経路

ホームページの閲覧

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。

信頼できないサイトで配布されたプログラムのインストール

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。

電子メールやメッセージ

電子メールやメッセージもウイルスの感染経路として一般的です。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、文書を閲覧するソフトウェアの脆弱性を狙い、添付されてきた文書ファイルを開くことでウイルスに感染させる例もありました。利用しているソフトウェアを更新せず脆弱性が残っているものはこのような危険もあります。
さらに、ファイルが添付されていなくても、電子メールやメッセージの本文中のURLにアクセスさせて、ウイルスをダウンロードさせる事例もありますので留意が必要です。

USBメモリからの感染

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による感染

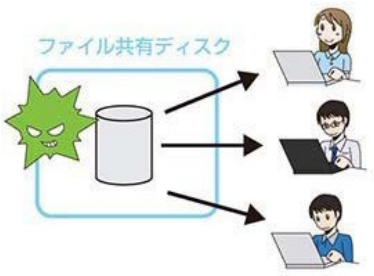
ファイル共有ソフトとは、インターネットを利用して他人とファイルをやり取りするソフトウェアのことです。自分が持っているファイルの情報と、相手が持っているファイルの情報を交換し、お互いに欲しいファイルを送り合ったりすることから、ファイル交換ソフトとも呼ばれています。

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。

電子メールのHTMLスクリプト

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。

ネットワークのファイル共有



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

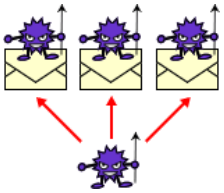
のファイル形式など、ある条件で探し出したファイルに感染していくタイプのものがあります。このようなウイルスは組織内のネットワークを通じて、他のコンピュータやサーバにも侵入して感染を拡げる可能性があります。とても危険度が高く、完全に駆除することが難しいのが特徴です。

■ マクロプログラムの実行

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。

ウイルスの主な活動

■ 自己増殖



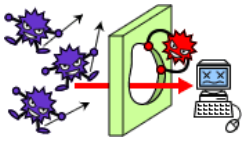
ウイルスの中には、インターネットやLANを使用して、他の多くのコンピュータに感染することを目的としているものがあります。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルとして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、利用者の操作を介さずに自動的に増殖していきます。

■ 情報漏洩（じょうほうろうえい）

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。

■ バックドアの作成



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。

■ コンピュータシステムの破壊

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。

■ メッセージや画像の表示

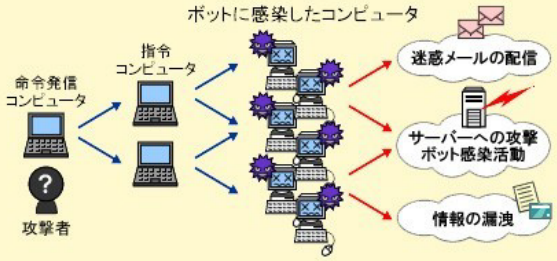
いたずらを目的としたウイルスは、一定期間コンピュータ内に潜伏して、ある日時に特定のメッセージや画像を表示することがあります。ただし、最近はこのようないたずらを目的としたウイルスは減ってきています。

【コラム】ボットとは？

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ボットネットを形成し、その一員として動作するようになります。そして、インターネットを通じて、悪意のある攻撃者が、ボットに感染したコンピュータを遠隔操作します。外部から自由に操るという動作から、このような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、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」も行うことがあります。ボットは旧来のウイルスのように愉快犯的な行為で作られたものではなく、不正な金銭的利益のために作られているという点で、手口が巧妙化しています。このような目的から、旧来のウイルスと比べると、感染しているという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。

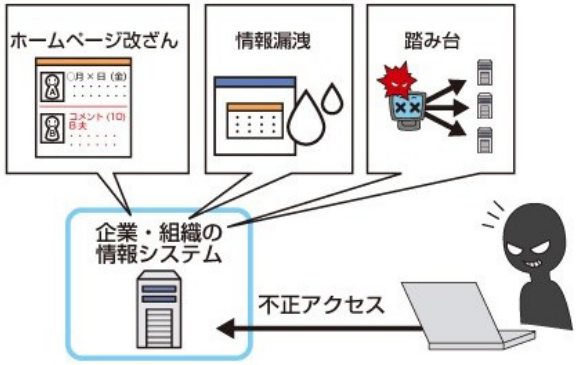
もし、あなたのコンピュータがボットに感染した場合、あなたはもちろん被害者なのですが、あなたのコンピュータが迷惑メールを送信したり、別のサイトを攻撃したりするため、攻撃の標的となったコンピュータから見ると、あなたのコンピュータは加害者になってしまいます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことなのです。



不正アクセスとは？

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。



- ホームページやファイルの改ざん
- 他のシステムへの攻撃の踏み台に

ホームページやファイルの改ざん

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（ろうえい）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。

他のシステムへの攻撃の踏み台に

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。

詐欺等の犯罪

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ログインID・パスワード、メールアドレスやクレジットカード番号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。

事故・障害

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」や情報通信技術の使いこなし能力（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（ぜいじゃくせい）とは？

脆弱性（ぜいじゃくせい）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。

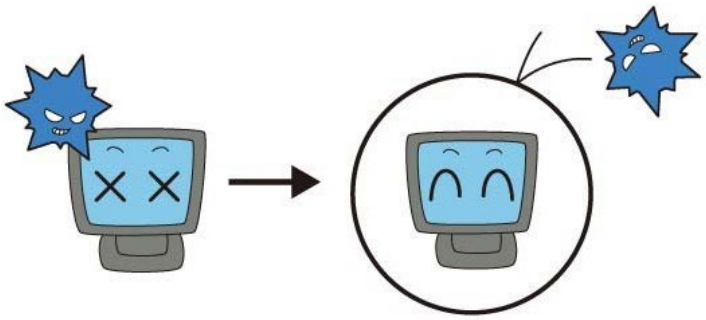
このような脆弱性が発見されると、多くの場合、ソフトウェアを開発したメーカーが更新プログラムを作成して提供します。しかし、脆弱性は完全に対策を施すことが困難であり、次々と新たな脆弱性が発見されているのが現状です。

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。
近年では、PCやスマートフォンに限らず、インターネットに接続される機器（家電製品やカーナビゲーションなど）も増えましたが、これらの機器もコンピュータで動いており、ソフトウェアに脆弱性があると被害を受けるリスクが生じることは変わりありません。

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。



情報発信に関するトラブル

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。

インターネットにおけるプライバシーの考え方

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。

個人に関する情報とは

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、同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。

基礎知識

Ⅲ.インターネットの安全な歩き方

インターネットには、さまざまな脅威があります。そのような脅威に晒され、大きな被害や影響を受けないためには、どのようなことをすればよいのでしょうか。

ここでは、そのための主な方法を説明します。

IDとパスワード

ここでは、インターネット上でのサービス利用時に広く使われている認証の仕組みと、ID、パスワードなどのアカウント情報の適切な管理について説明します。

認証の仕組みと必要性　　設定と管理のあり方

認証の仕組みと必要性

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。

設定と管理のあり方

他人に自分のユーザアカウントを不正に利用されないようにするには、適切なパスワードの設定と管理が大切です。

適切なパスワードの設定・管理には、以下の3つの要素があります。

■ 安全なパスワードの設定

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。
理想的には、ある程度長いランダムな英数字の並びが好ましいですが、覚えなければならないパスワードの場合は、無関係な（文章にならない）複数の英単語をつなげたり、その間に数字列を挟んだりしたものであれば、推測されにくく、覚えやすいパスワードを作ることができます。

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ひとつだけ
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。

パスワードの保管方法

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

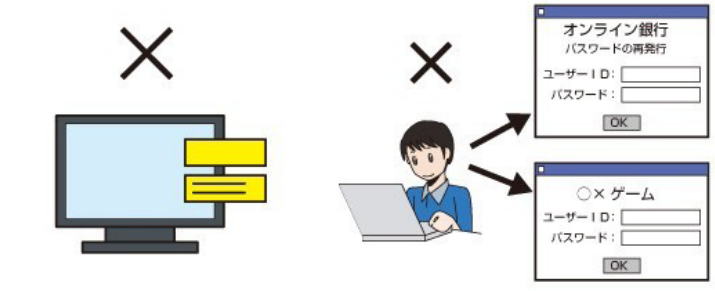
なお、各サービスごとに異なる充分に安全なパスワードを覚えておくのは大変なので、パスワード管理ツールやサービスの利用も一考です。もちろん、充分に信頼できる安全なツールやサービスを利用することは重要です。
これらのツールやサービスは、マスターパスワード（覚えられる充分に安全なもの）や、利用デバイス（スマートフォンなど）のロック（生体認証など）で守る必要があります。

パスワードを複数のサービスで使い回さない（定期的な変更は不要）

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）からネットワークビギナーのための情報セキュリティハンドブックとして、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）NISTSP800-63B（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

【コラム】生体認証とは？

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。

ウイルスに感染しないために

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。

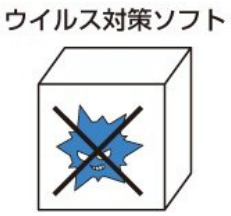
1.ソフトウェアを更新する

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。

参照どんな危険があるの？：脆弱性（ぜいじゃくせい）とは？

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。

参照 どんな危険があるの？：ウイルスの感染経路

【コラム】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。

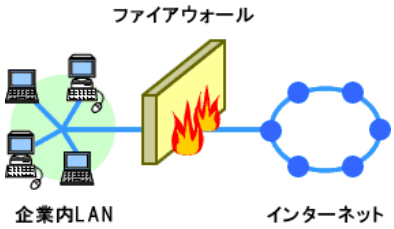
不正アクセスに遭わないために

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。



詐欺や犯罪に巻き込まれないために

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。

また、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・障害への備え

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。

情報発信の心得

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・プライバシー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。

また、匿名だからと安易に考えるのも禁物です。上記の通り公開されている情報から特定されるケースもありますし、司法機関によるプロバイダーに対する開示請求によって発信者の情報が提供される場合もあります。

インターネットに匿名はないと考えたほうがいいでしょう。

参照 SNS利用上の注意点

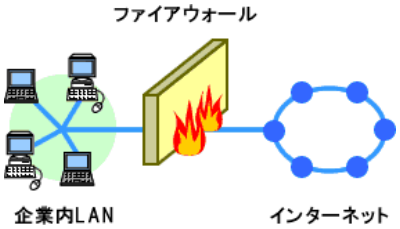
基礎知識

Ⅳ.情報セキュリティ関連の技術

ここでは、情報セキュリティ対策に使われる代表的な技術と、反対に情報セキュリティ上の脅威となる技術などを紹介します。

ファイアウォールの仕組み

ファイアウォールは、ネットワークの通信において、その通信をさせるかどうかを判断し許可するまたは拒否する仕組みです。しかし、その通信をどう扱うかの判断は、通信の送信元とあて先の情報を見て決めており、通信の内容は見ていません。これを荷物の配送にたとえると、送り主とあて先などの情報は見ているが、その荷物の中身は見ていないということになります。



ファイアウォールとは、元々は火災などから建物を防御するための防火壁のことをいいます。火災のときに被害を最小限に食い止める防火壁のような役割を果たすことから、インターネットの世界では、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を、ファイアウォールと呼ぶようになりました。

現在のファイアウォールには、大きく分けて2種類あります。ひとつは家庭などで利用する、単体のコンピュータを防御することを目的としたパーソナルファイアウォールで、もうひとつは、企業や家庭のネットワーク全体を防御するファイアウォールです。

パーソナルファイアウォールは、クライアントのコンピュータに導入するソフトウェアです。パーソナルファイアウォールは、そのコンピュータに対して、インターネットからの不正な侵入を防いだり、ウイルスの侵入を防御したり、自分のコンピュータを外部から見えなくしたりすることが可能になります。ソフトウェアのメーカーによっては、ウイルス対策ソフトと組み合せて販売されています。

企業などのネットワークに使用するファイアウォールは、インターネットと社内のLANとの間に設置するものです。この場合のファイアウォールの基本的な機能は、外部からの不正なアクセスを社内のネットワークに侵入させないことです。具体的には、外部からの不正なパケットを遮断する機能や、許可されたパケットだけを通過させる機能を持っています。

また、インターネットサービスプロバイダが自社の接続サービスを利用している利用者を対象として、ファイアウォールをサービスとして提供している場合もあります。自分が利用しているインターネットサービスプロバイダで、サービスが提供されているかどうか確認し、利用を検討してみるとよいでしょう。

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は、必須と言える情報セキュリティ対策です。ただし、ファイアウォールを設置しても、それがネットワークに関する完全な情報セキュリティ対策になるわけではありません。あくまでも、ネットワークに対する攻撃や不正アクセスに関する情報セキュリティ対策のひとつとして考える必要があります。

暗号化の仕組み

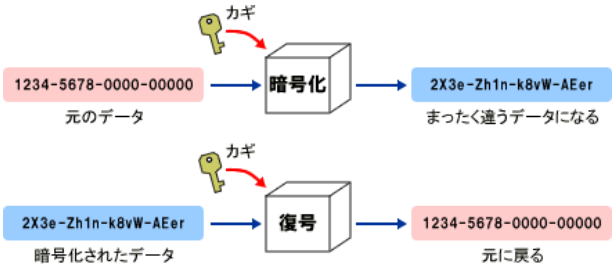
暗号化とは、データの内容を他人には分からなくするための方法です。たとえば、コンピュータを利用する際に入力するパスワードが、そのままの文字列でコンピュータ内に保存されていたとしたら、そのコンピュータから簡単にパスワードを抜き取られてしまう危険性があります。そのため、通常パスワードのデータは、暗号化された状態でコンピュータに保存するようになっています。

暗号化の仕組みは、以下のとおりです。

まず、元のデータを暗号のシステムを使い暗号化します。この時に暗号鍵と呼ばれるデータを使用します。このような仕組みで暗号化をすると、元のデータは、まったく違うデータになります。

暗号化されたデータは、同じように暗号のシステムを使い元のデータに戻します。これを復号と呼び、この際に暗号化の時と同じように暗号鍵を使って行います。

つまり、暗号化をするときに使う暗号鍵が非常に重要な役割を果たします。これが他人に渡ってしまうと、暗号化したデータが読まれてしまうことになります。そのため、この暗号鍵は暗号化通信に関係のない人に渡ったりすることがないよう厳重に管理しなければなりません。



Webページの送受信データ、電子メール、無線LANによる通信データにおいても、データを利用者以外にはわからなくするために、さまざまな暗号化技術が使われることがあります。

暗号技術を応用した仕組みとして、電子署名や電子証明書があります。

電子署名を利用することにより、情報の送信元のなりすましやメッセージの改ざんが行われていないことを確認することができます。

電子証明書は、電子署名技術を用いて、Webサイトや電子メールが正しいものであるかを証明するものです。Webブラウザやメールソフトに表示される鍵のマークをクリックして、「証明書の表示」を選択することにより、そのWebサイトや電子メールが正しいものであるかどうかを確認できます。

但し、近年では偽サイトや詐欺サイトが電子証明書を設置する例があります。サイト証明書があっても安全とは限らないことには注意が必要です。

SSL/TLSの仕組み

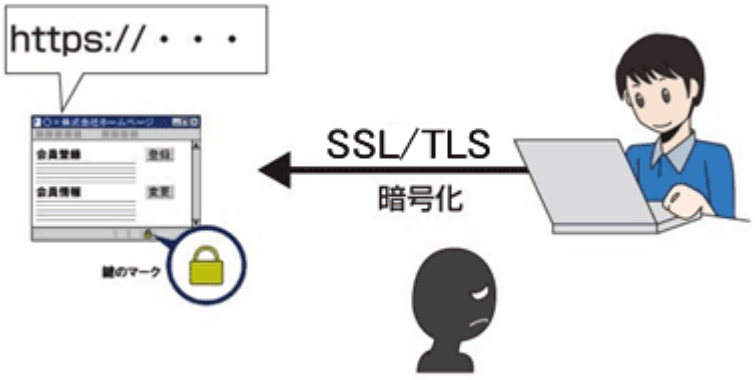
SSL（Secure Socket Layer）/TLS(Transport Layer Security)とは、インターネット上でデータを暗号化して送受信する仕組みのひとつです。クレジットカード番号や、一般に秘匿すべきとされる個人に関する情報を取り扱うWebサイトで、これらの情報が盗み取られるのを防止するため、広く利用されています。また、SSL/TLSは暗号化に加え、電子証明書により通信相手の本人性を証明し、なりすましを防止するなど、今日のインターネットの安心・安全を支えています。

なお、過去にはSSLが使われていましたが、脆弱性が発見されたためにTLS（v.1.2以降）への移行が進んでおり、今ではSSLは使われなくなってきています（SSL全バージョンと、TLSv1.1以前に脆弱性があります）。しかし、歴史的経緯でSSLの用語が広く普及しているため、本サイトでは「SSL/TLS」と表記しております。

SSL/TLSは、WebサーバとWebブラウザとの通信においてやりとりされるデータの暗号化を実現する技術です。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などは、このSSL/TLSを使ったホームページが使われます。ここで入力された情報は暗号化され、金融機関のWebサーバに送られるのです。これにより、通信の途中で情報が盗み見られることを防いでいます。

Webブラウザにより、SSL/TLSを使ったサイトに接続するには、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。SSL/TLS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。これらにより、SSL/TLS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。

電子証明書などの詳細な情報を確認できます。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ますので、普段、使用しているWebブラウザではどこにどのようなマークが出るかということを、あらかじめ確認しておくのがよいでしょう。



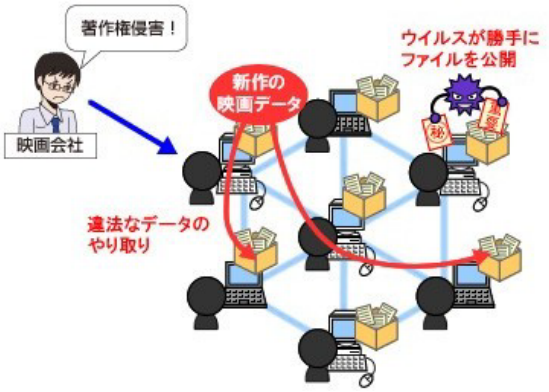
ファイル共有ソフトとは？

ファイル共有ソフトとは、インターネットで不特定多数の利用者とファイルをやり取りするためのソフトウェアのことです。ファイル共有ソフトの仕組みはソフトウェアによって少しずつ異なりますが、その多くはファイルのやり取りをクライアント同士で行うP2P（Peer to Peerーピア・トゥー・ピア）型というタイプのものです。

P2P型のファイル共有は、通常の社内のネットワークで利用するファイル共有とは異なり、ファイルを提供するサーバが固定されているわけではありません。ファイル共有ソフトによるファイル共有では、どのファイルがどこのコンピュータに存在するかというインデックス情報（ソフトウェアによって呼び方は異なります。）が必要であり、ソフトウェアによって、中央に配置した専用のサーバで管理したり、それぞれのコンピュータ（クライアント）が保有したりしています。このインデックス情報を元に、ファイルを保管しているコンピュータを特定して、欲しいファイルを直接コピーするという仕組みになっています。つまり、インデックス情報を共有化することによって、網の目のように張り巡らされたクライアント同士のネットワークで、ファイル共有システムを実現しているというわけです。

最初のファイル共有ソフトは、1990年代後半に米国で登場しました。その後、日本でも多くのファイル共有ソフトが登場し、ブロードバンド通信の普及に伴い、多くの利用者に利用されました。しかし、そこで共有されるデータも、著作権違反の音楽データ、映画、テレビ番組、漫画、ゲームソフトのファイルといったものが多く、社会問題となっています。また、ファイル共有ソフトが接続するネットワークでは、非常に多くのウイルスが流れており、これにより感染したり、さらなる情報漏洩（ろうえい）を引き起こしたりする危険性があります。

また、現在ではファイル共有ソフトをターゲットにしたウイルスにより、企業や組織の機密情報がインターネット上に漏洩してしまうという事件が数多く発生しています。ファイル共有ソフトはできるだけ使わないことが望ましいといえます。また、自分ではファイル共有ソフトを使っていないつもりでもいつの間にか家族の誰かが勝手にインストールし、情報が漏洩してしまう事件も起こっています。ファイル共有ソフト使用の方針については家族にも徹底が必要です。



このテキストに関する問い合わせ先

総務省 サイバーセキュリティ統括官室
Email:kokumin-security@ml.soumu.go.jp

○ 国民のためのサイバーセキュリティサイト
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

○ キッズページ
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/

○ このテキストの利用規約
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/guide.html