国民のための
サイバーセキュリティサイト

総務省

サイバーセキュリティの基礎知識

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・脅威等、について説明します。

目次

インターネットを利用したサービス

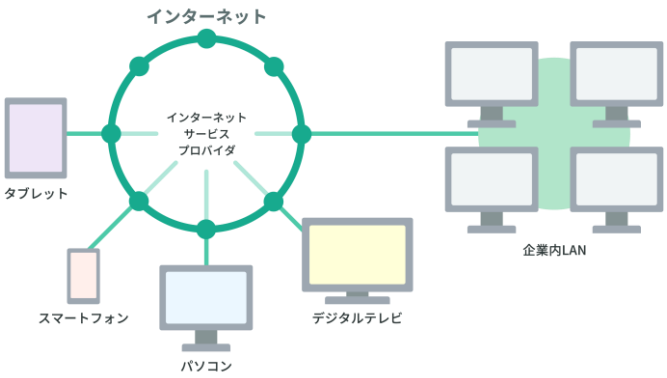
ここでは、サイバーセキュリティ対策を立てるための基礎知識として、インターネットや、インターネットを使ったサービスの仕組みについて説明します。

インターネットの仕組み

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。



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スマートフォン、タブレットなどは、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（IP アドレスの例：198.51.100.1）は、世界中で通用する住所のようなものです。

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を“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 という規格が導入されています。

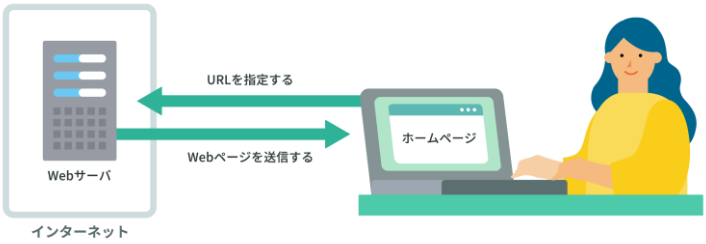
IPv6 方式の IP アドレスは、例えば
「2001:db8:bb5c:8008:2013:a219:2210:8103」のように表記します。

Web サイトの仕組み

インターネット上で情報を公開する場所を Web サイトと呼びます。Web サイトのコンテンツ

(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中に保存されています。私たちの端末から、そのコンピュータに命令を出し、情報を送ってもらうことで、Web サイトを見ることができます。

ここでいう Web サイトとは、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。Web サイト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 Web サイト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、Web サイト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 Web サイトが、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、Web サイト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 つ異なる 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 サイトに簡単に移動することができるようになります。

Web サイトには、ショッピングサイトやネットオークションサイトといったものも存在し、商品の売買を行うこともできます。

電子メールの仕組み

電子メール(e-mail)とは

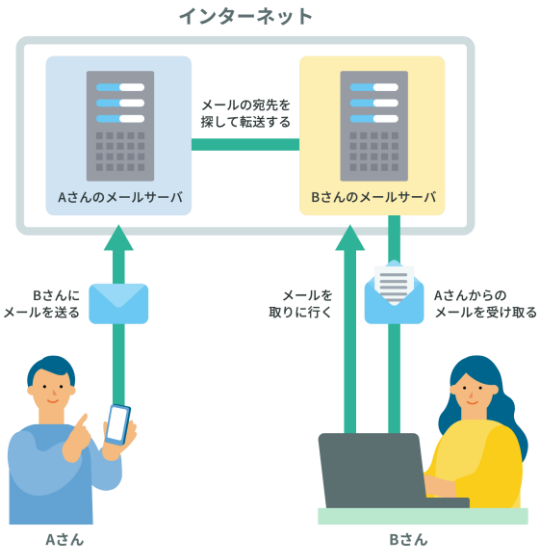
パソコンやスマートフォン、タブレットなどの情報機器同士が、専用のメールソフトを使って、インターネットなどのネットワークを利用して情報をやりとりする機能です。やりとりできる情報は文章(テキスト)だけでなく、文書ファイルや画像などを添付ファイルとして扱うことができます。

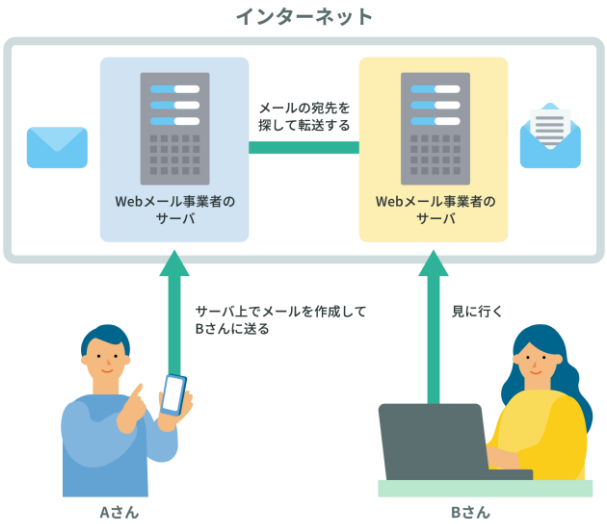
電子メールを送る際には、送り先のコンピュータを指定するためにアドレスを使います。電子メールのアドレスは、一般的に”xxx@example.co.jp”のように表記されます。@の後には、所属する組織や利用しているインターネットサービスプロバイダなどの事業者のドメイン名が一般に使われます。また、一般的なメールソフトを使うのではなく、Web 上で Web ブラウザを使って送受信を行う Web メールという方式もあり、フリーメールサービスとして広く普及しています。

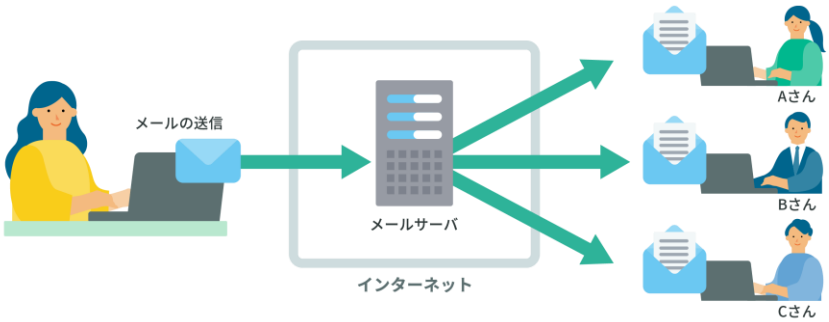
電子メールの送受信は、インターネット上の多くのメールサーバが連携することによって実現しています。

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など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 メールの場合、送受信された電子メールは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。


インターネット
メールの宛先を
探して転送する
Aさんのメールサーバ
Bさんのメールサーバ
Bさんに
メールを送る
メールを
取りに行く
Aさんからの
メールを受け取る
Aさん
Bさん


インターネット
メールの宛先を
探して転送する
Webメール事業者の
サーバ
Webメール事業者の
サーバ
サーバ上でメールを作成して
Bさんに送る
見に行く
Aさん
Bさん


メールの送信
メールサーバ
インターネット
Aさん
Bさん
Cさん

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。

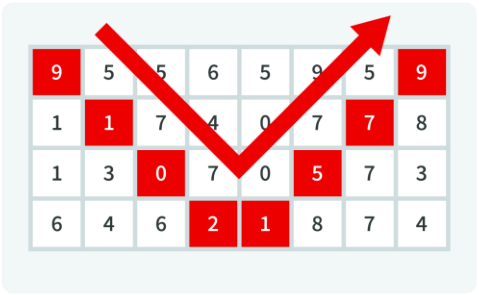
インターネットバンキングでは、銀行の窓口や ATM に行かなくても、自宅や外出先などで、銀行の営業時間を気にすることなく振込や残高照会などをすることができます。このような便利さから、インターネットバンキングの利用は急速に拡大しています。

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。

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。

第2パスワードの例



パスワード表

金融機関から、ランダムな数字の表が記載されたカードなどをあらかじめ配布し、顧客はログイン時に、
カードの指定された場所の数字を順番に入力する。
ログインのたびにカードの指定される場所が変わるので、カードを持っている人でなければ、第２パスワードがわからない仕組み。

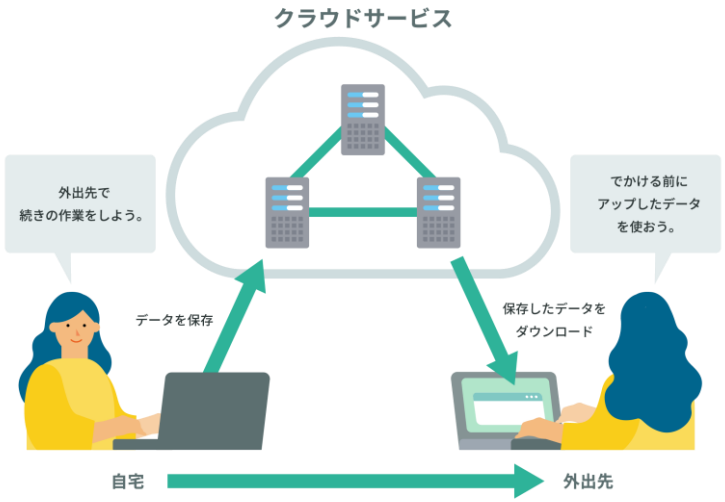
ワンタイムパスワード

金融機関から、一定時間ごとに異なるパスワードを表示する専用表示端末(トークン)をあらかじめ配布し、顧客はログイン時に、専用表示端末に表示されているパスワードを入力する。
専用表示端末を持っている人でなければ、第２パスワードがわからない仕組み。

クラウドサービスの仕組み

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、十分なサイバー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。

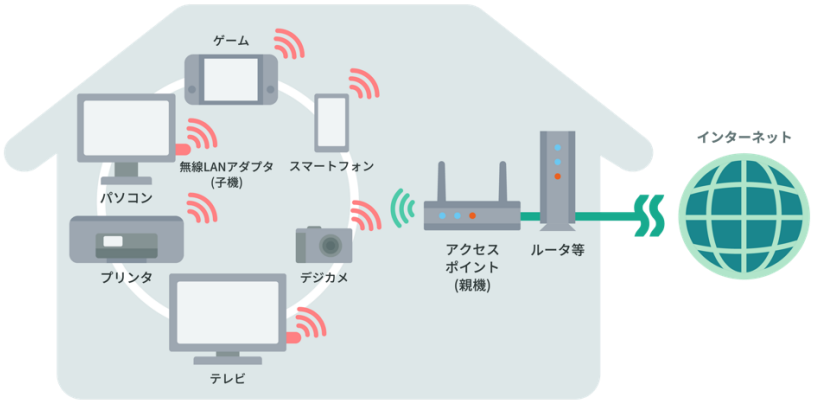
無線 LAN(Wi-Fi)の仕組み

LAN は、構内通信網(LAN:Local Area Network)といい、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。その中でも無線 LAN はケーブルの代わりに無線通信のことを言います。。

無線 LAN は 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。

Wi-Fi 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無線通信(ワイヤレス)で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出来るようになりました。

当初 Wi-Fi は職場や家庭のパソコン等をワイヤレスでインターネットに接続する手段として普及しましたが、スマートフォンやタブレット等の普及により利用がさらに拡大しました。一般の利用においては自宅で利用する自宅 Wi-Fi と空港や駅、ホテル、学校、図書館といった様々な場所で使える公衆 Wi-Fi の提供も増えております。



コラム:災害時にも活躍する無線 LAN(Wi-Fi)

公衆 Wi-Fi は災害時の通信手段としても活用されています。
2011 年の東日本大震災の際に、通信事業者が公衆 Wi-Fi を無料開放して被災地の通信手

段確保に貢献しました。これをきっかけに、「00000JAPAN（ファイブゼロ・ジャパン）」という取組が進められ、近年では地震や風水害等の災害発生時やモバイル通信事業者の大規模な障害の発生時に Wi-Fi サービスの無料開放が行われています。
開放されると、ネットワーク名（SSID）が「00000JAPAN」でサービスが提供され、誰でも、パスワードを入力することなく接続して、安否確認等の情報の共有や入手に利用することができます。
※ただし、利便性を最優先して一切の認証なし・暗号化なしで提供されます。そのため、情報入手等のための利用にとどめるなど、利用に当たっては十分ご留意ください。災害時に限られた通信手段を譲り合って利用する観点からも、必要最小限の利用にとどめるようにしましょう。

インターネットに潜む脅威

インターネットにはどんな脅威があるのでしょう。

脅威にはそれを引き起こす者がいます。悪意を持って意図的に攻撃をする人や、悪意は持ってなかったとしても設定ミスや操作ミス等で偶発的に被害が発生してしまう場合もあります。

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。

マルウェア(ウイルス等)とは？

ウイルスは、電子メールやホームページなどを閲覧などを介し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、利用者が気づかないうちに勝手に活動する(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。

マルウェアは、USB メモリなどの記憶媒体の利用や、電子メール、ホームページの閲覧など、さまざまな方法で侵入します。侵入したマルウェアは、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。

ウイルスに感染しないためには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。マルウェア(ウイルス等)対策ソフトを導入するといった手段も有効ですが、最新のウイルスに対応できるよう、常に更新しておくことが重要です。

マルウェア(ウイルス等)はどこから来るの？

インターネットの普及以前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、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、ユーザが何もしなくても、ユーザが何かをしなくても、ネットワークからウイルスが感染する事例も発生しています。 以下が代表的なマルウェアの感染経路です。

No.	主な感染経路	内容
1	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させるため、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（ぜいじゃくせい）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可能性があります。
2	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	代表的な手口としては、無料のマルウェア（ウイルス等）対策ソフトのように見せかけて、マルウェアをインストールさせようとする「偽セキュリティソフト」の被害があります。具体的には、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、利用者を偽のマルウェア（ウイルス等）対策ソフトを配布するWebサイトに誘導します。
3	電子メールやメッセージ、添付ファイルの開封	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、それがマルウェア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。
4	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。
5	USB メモリからの感染	USB メモリをコンピュータに差し込んだだけで自動的にマルウェア悪意のあるプログラムが実行されてしまう危険性があります。
6	ファイル共有ソフトによる感染	ファイル共有ソフトでは、不特定多数の人に自由にファイルを公開することができるため、正規のファイルに偽装するなどの方法で、いつの間にかマルウェアを実行させられてしまうことがあります。マルウェアが仕込まれた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。
7	ネットワークのファイル共有	マルウェアによっては、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。
8	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、特定の操作をプログラムとして登録できるマクロという便利な機能があります。このマクロ機能を悪用して感染するタイプのマルウェアが知られており、マクロウイルスと呼ばれています。
9	IoT 機器（ルータ含む）の感染	ルータや Web カメラ等の IoT 機器が外部へ公開されていることでマルウェア（mirai 等）に感染し、攻撃者に悪用されてしまうことがあります。

マルウェアはどんなことをするの？

マルウェアは、増殖するための仕組みや他のコンピュータに感染するための機能があります。

例えば、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。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、利用者がホームページを見るだけで感染するものも多く、世界中にマルウェアが蔓延する大きな原因となっています。マルウェアが実施できる主な活動は、以下の通りです。

No.	主な活動	内容
1	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。
2	情報漏洩（じょうほうろうえい）	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。
3	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、いつでも攻撃者から遠隔操作できてしまう可能性があるため極めて危険です。

4	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。
5	遠隔操作	コンピュータを外部からの踏み台として遠隔操作するためのウイルスをボット（BOT）と呼びます。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、攻撃の踏み台として利用することがあります。
6	ランサムウェア	ランサムウェアとは、感染したPC上に保存しているファイル（PC からアクセス可能なネットワーク上のファイルも含みます。）を暗号化して使用ができない状態にするマルウェアです。攻撃者は、復旧させることと引き換えに身代金を要求するため、ランサム（身代金:ransom）ウェアと呼ばれています。 ただし、身代金を支払っても復旧されない可能性があることや、金銭を支払うことで犯罪者に利益供与を行ったと見なされてしまうこともあるため、支払いに応じることは推奨されません。 また、これまでは暗号化して身代金を要求するケースが多かったものの、攻撃者が「より手軽に」身代金を得るため、「暗号化」を行わず、盗み取ったデータの公開を対価に身代金を要求する「ノーウェアランサム」攻撃による被害も増加しています。

フィッシング詐欺とは？

フィッシング詐欺とは、送信者を詐称した電子メールを送りつけたり、偽の電子メールから偽のホームページに接続させたりするなどの方法で、クレジットカード番号、アカウント情報（ユーザ ID、パスワードなど）といった重要な情報を盗み出す行為のことを言います。なお、フィッシングは phishing という綴りで、魚釣り（fishing）と洗練（sophisticated）から作られた造語であると言われています。

最近では、電子メールの送信者名を詐称し、もっともらしい文面や緊急を装う文面にするだけでなく、接続先の偽の Web サイトを本物の Web サイトとほとんど区別がつかないように偽造するなど、ますます手口が巧妙になってきており、ひと目ではフィッシング詐欺であるとは判別できないケースが増えてきています。

さらに、最近ではパソコンだけでなく、スマートフォンでも同様に電子メールや SMS などのメッセージ機能からフィッシングサイトに誘導される手口が増えています。

フィッシング詐欺の手口としては以下のようなものが挙げられます。

電子メールやメッセージ機能でフィッシングサイトに誘導

典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールなどで、巧みにリンクをクリックさせ、あらかじめ用意した本物のサイトにそっくりな偽サイトに利用者を誘導します。
そこでクレジットカード番号や口座番号などを入力するよう促し、入力された情報を盗み取ります

SNS などの情報でフィッシングサイトに誘導

電子メールやメッセージだけではなく、SNS の投稿サイトに、URL を記載してアクセスさせ誘導する手口です。

表示されている URL を本物の URL に見せかけてアクセスさせる手口

電子メールや SNS に投稿された URL を実在する URL に見間違えるような表示にすることで誘導する手口です。

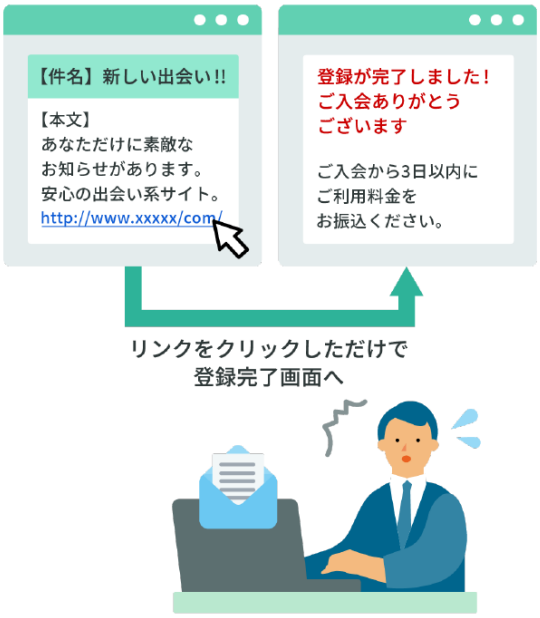
例えば、アルファベットの一文字の（オー）o を数字の 0 にしたり、アルファベットの大文字の（アイ）I を小文字の（エル）l にしたりして、閲覧者が見間違えたり、信用させたりする手口もあります。

対策としては、最低限以下の点に注意しましょう。

- 正しい URL や正規のアプリケーションを用いてアクセスする
  金融機関の ID・パスワードなどを入力する Web ページにアクセスする場合は、金融機関から通知を受けている URL を Web ブラウザに直接入力するか、普段利用している Web ブラウザのブックマークに金融機関の正しい URL を記録しておき、毎回そこからアクセスするようにするなど、常に真正のページにアクセスすることを心がけましょう。 事業者が提供している正規のスマホアプリを利用することも有効です。スマホアプリをダウンロードする際は正規の提供元（Google Play や AppStore）から入手してください。

ワンクリック詐欺とは？

ワンクリック詐欺とは、Web サイトや電子メール、SMS などのメッセージに記載された URL を一度クリックしただけで、一方的に、サービスへの入会などの契約成立を宣言され、多額の料金の支払いを求められるという詐欺です。



フィッシング詐欺が情報をだまし取るのに対し、不安を煽るなどして直接金銭を支払わせようとするものがワンクリック詐欺です。ワンクリック詐欺の手口には、以下のようなものがあります。

- 利用者の興味を引きそうな電子メールや電子掲示板などを利用して、利用者をおびき寄せる。アダルト系、出会い系など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。多くの Web サイトでは利用者が間違って契約してしまったように思わせる仕組みや、わざとわかりにくいところに利用規約などを表示して、利用者が気付きにくいような細工をしている。
- 料金請求の際、携帯電話の個体識別番号や、パソコンの固有識別番号、利用しているインターネットサービスプロバイダの情報などを表示させ、利用者の情報が“複雑な技術によって”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、法的措置を講ずるといった脅迫的な内容で、利用者に支払いを迫る。

ワンクリック詐欺に対する対処方法としては、以下があげられます。

- 不用意に Web サイトにアクセスせずに、電子メールや電子掲示板の文面をきちんと読んで、利用しましょう。特に、利用規約などが記載されている場合には注意が必要です。場合によってはこの利用規約を非常に長文にしたり、Web ブラウザから 1～2 行しか表示できないように工夫したりなどして、利用者が利用規約を読まずにクリックさせるような手口のサイトもあります。
- あたかも個人が特定されたような表現で、「お支払い頂けない場合には、自宅にまで伺います」といった脅し文句が書かれていても、真に受けないようにして、どうしても心配であれば、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。
- 「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」では、「電子消費者契約に関する民法の特例」として、消費者がコンピュータの操作ミスなどで、契約する意志がなく申し込んだ場合における救済措置がとられています。間違ってクリックした場合や、意図せずこうした Web サイトを閲覧して、料金を請求された場合は、解約手続きや、連絡などはせずに無視しましょう。
- 利用状況や支払理由などを確認するために業者に連絡を取るということは、相手に自分の連絡先などの情報を渡すことにつながります。決して連絡をしないようにしましょう。
- ワンクリック詐欺はいわゆる迷惑メールなど知らない人から送信されるメールが発端になる場合が多いので、できるだけ知人以外からの電子メールを受け取った際に安易にURLをクリックしないようにしましょう。
- また、サイト検索結果に詐欺サイトに誘導するものが含まれる場合があります。日常利用しているサービスは、検索せず、過去にアクセスしたことがあるブックマークを利用する方が安全です。
- トラブルになりそうなときには、表示されているデータを保存したり、画面を印刷したりしておくことも必要です。また、自分の行った手順をメモしておくとよいでしょう。（[いいえ]を選択したが、登録完了画面が表示された時など）。

最近では、ホームページを表示した際に、自動的にウイルスを埋め込む悪質な Web サイトも増えてきているため、知らない Web サイトを訪問する場合には、それらの危険性もきちんと認識しておくようにしましょう。

サポート詐欺とは？

サポート詐欺とは、悪意のある Web サイトを訪問した利用者に偽の警告画面を表示し、画面上に表示しているなりすましサポートセンターに電話をさせて金品をだまし取る詐欺です。

マルウェア感染やパソコンのセキュリティに問題があると偽装した警告メッセージが表示され、警告音が鳴るケースもあります。次々に警告ウィンドウが開き、パソコンのスキャンを装ってマルウェアが発見される画面を表示するなどして利用者の不安を煽ります。画面上のなりすましサポートセンターに電話をかけると有償サポートへ誘導され、プリペイドカードなどによる支払いを求められます。

偽の警告画面はウイルスの感染有無に関わらず繰り返し表示されているのみであり、偽の警告画面を閉じるのみで問題の解消が可能です。偽の警告画面が表示されたら、表示されているサポートセンターへの連絡や、アプリやソフトウェアのインストールは決してせずに、ブラウザを終了するようにしましょう。
サポート詐欺では Web サイトの遷移を伴いますから、怪しげな広告やリンクをクリックして上記のような画面が開いた場合、いったん立ち止まって冷静に対処することが大切です。

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

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パスワード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したり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、ボットと呼ばれるウイルスを攻撃者によって送り込まれ、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。

脆弱性とは？

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サイバー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サイバーセキュリティ上の大きな問題のひとつになっています。

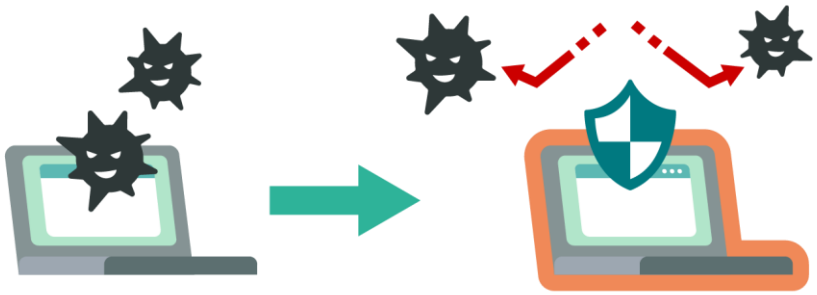
脆弱性はクライアントとサーバ、どちらのコンピュータにおいても重要な問題ですが、特にインターネットに公開している場合には、脆弱性を利用した不正アクセスによって、ホームページが改ざんされたり、他のコンピュータを攻撃するための踏み台に利用されたり、ウイルスの発信源になってしまったりするなど、攻撃者に悪用されてしまう可能性があるため、脆弱性は必ず塞いでおかなければなりません。

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。



プライバシーの侵害とは？

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”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 SNS 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、万全なサイバー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。

サイバーセキュリティ関連の法律・ガイドライン

サイバーセキュリティに関する我が国の法律には、どのようなものがあるのでしょうか。また、どのような行為が違反とされるのでしょうか。

　ここでは、代表的な法律とインターネットを利用した法律違反の事例を紹介します。なお、法律については、五十音順に列記し、関連条文のみを記載しています。

刑法

刑法とは「犯罪と刑罰に関する法律である」と定義されます。ここでは、コンピュータやインターネットを利用した事件の中から、刑罰に該当した刑法の条文を抜粋して紹介します。

■用語：電磁的記録
第七条の二 この法律において「電磁的記録」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。

（電磁的記録不正作出及び供用）
第百六十一条の二　人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、五年以下の懲役又は五十万円以下の罰金に処する。
２　前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、十年以下の懲役又は百万円以下の罰金に処する。
３　不正に作られた権利、義務又は事実証明に関する電磁的記録を、第一項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同一の刑に処する。
４　前項の罪の未遂は、罰する。

（不正指令電磁的記録作成等）
第百六十八条の二　正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
２　正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
３　前項の罪の未遂は、罰する。

（不正指令電磁的記録取得等）
第百六十八条の三　正当な理由がないのに、前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。

（わいせつ物頒布等）
第百七十五条　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若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。

（名誉毀損）
第二百三十条　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。
２　死者の名誉を毀損した者は、虚偽の事実を摘示することによってした場合でなければ、罰しない。

（電子計算機損壊等業務妨害）
第二百三十四条の二　人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。
２　前項の罪の未遂は、罰する。

（詐欺）
第二百四十六条　人を欺いて財物を交付させた者は、十年以下の懲役に処する。
２　前項の方法により、財産上不法の利益を得、又は他人にこれを得させた者も、同項と同様とする。

（電子計算機使用詐欺）
第二百四十六条の二　前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する。

第二百五十条　この章の罪の未遂は、罰する。
（※第二百四十六条から第二百四十九条までの罪）

サイバーセキュリティ基本法

「サイバーセキュリティ基本法」は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定しています。

（目的）
第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法（令和三年法律第三十五号）第二条に規定する情報通信技術（以下「情報通信技術」という。）の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

（国民の努力）
第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

著作権法

「著作権法」は、著作物などに関する著作者等の権利を保護するための法律です。

（差止請求権）
第百十二条 著作者、著作権者、出版権者、実演家又は著作隣接権者は、その著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

2 著作者、著作権者、出版権者、実演家又は著作隣接権者は、前項の規定による請求をするに際し、侵害の行為を組成した物、侵害の行為によって作成された物又は専ら侵害の行為に供された機械若しくは器具の廃棄その他の侵害の停止又は予防に必要な措置を請求することができる。

（侵害とみなす行為）
第百十三条　次に掲げる行為は、当該著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為とみなす。
一　国内において頒布する目的をもって、輸入の時において国内で作成したとしたならば著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害となるべき行為によって作成された物を輸入する行為

二　著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為によって作成された物（前号の輸入に係る物を含む。）を情を知って頒布し、又は頒布の目的をもつて所持する行為

2　プログラムの著作物の著作権を侵害する行為によって作成された複製物（当該複製物の所有者によって第四十七条の二第一項の規定により作成された複製物並びに前項第一号の輸入に係るプログラムの著作物の複製物及び当該複製物の所有者によって同条第一項の規定により作成された複製物を含む。）を業務上電子計算機において使用する行為は、これらの複製物を使用する権原を取得した時に情を知っていた場合に限り、当該著作権を侵害する行為とみなす。

3　侵害著作物等利用容易化ウェブサイト等の公衆への提示を行っている者（当該侵害著作物等利用容易化ウェブサイト等と侵害著作物等利用容易化ウェブサイト等以外の相当数のウェブサイト等とを包括しているウェブサイト等において、単に当該公衆への提示の機会を提供して

いるに過ぎない者（著作権者等からの当該侵害著作物等利用容易化ウェブサイト等において提供されている侵害送信元識別符号等の削除に関する請求に正当な理由なく応じない状態が相当期間にわたり継続していることその他の著作権者等の利益を不当に害すると認められる特別な事情がある場合を除く。）を除く。）又は侵害著作物等利用容易化プログラムの公衆への提供等を行っている者（当該公衆への提供等のために用いられているウェブサイト等とそれ以外の相当数のウェブサイト等とを包括しているウェブサイト等又は当該侵害著作物等利用容易化プログラム及び侵害著作物等利用容易化プログラム以外の相当数のプログラムの公衆への提供等のために用いられているウェブサイト等において、単に当該侵害著作物等利用容易化プログラムの公衆への提供等の機会を提供しているに過ぎない者（著作権者等からの当該侵害著作物等利用容易化プログラムにより提供されている侵害送信元識別符号等の削除に関する請求に正当な理由なく応じない状態が相当期間にわたり継続していることその他の著作権者等の利益を不当に害すると認められる特別な事情がある場合を除く。）を除く。）が、当該侵害著作物等利用容易化ウェブサイト等において又は当該侵害著作物等利用容易化プログラムを用いて他人による侵害著作物等利用容易化に係る送信元識別符号等の提供が行われている場合であって、かつ、当該送信元識別符号等に係る著作物等が侵害著作物等であることを知っている場合又は知ることができたと認めるに足りる相当の理由がある場合において、当該侵害著作物等利用容易化を防止する措置を講ずることが技術的に可能であるにもかかわらず当該措置を講じない行為は、当該侵害著作物等に係る著作権、出版権又は著作隣接権を侵害する行為とみなす。

4　前二項に規定するウェブサイト等とは、送信元識別符号のうちインターネットにおいて個々の電子計算機を識別するために用いられる部分が共通するウェブページ（インターネットを利用した情報の閲覧の用に供される電磁的記録で文部科学省令で定めるものをいう。以下この項において同じ。）の集合物（当該集合物の一部を構成する複数のウェブページであつて、ウェブページ相互の関係その他の事情に照らし公衆への提示が一体的に行われていると認められるものとして政令で定める要件に該当するものを含む。）をいう。

5　プログラムの著作物の著作権を侵害する行為によって作成された複製物（当該複製物の所有者によって第四十七条の三第一項の規定により作成された複製物並びに第一項第一号の輸入に係るプログラムの著作物の複製物及び当該複製物の所有者によって同条第一項の規定により作成された複製物を含む。）を業務上電子計算機において使用する行為は、これらの複製物を使用する権原を取得した時に情を知っていた場合に限り、当該著作権を侵害する行為とみなす。

6　技術的利用制限手段の回避（技術的利用制限手段により制限されている著作物等の視聴を当該技術的利用制限手段の効果を妨げることにより可能とすること（著作権者等の意思に

基づいて行われる場合を除く。）をいう。次項並びに第百二十条の二第一号及び第二号において同じ。）を行う行為は、技術的利用制限手段に係る研究又は技術の開発の目的上正当な範囲内で行われる場合その他著作権者等の利益を不当に害しない場合を除き、当該技術的利用制限手段に係る著作権、出版権又は著作隣接権を侵害する行為とみなす。

なお、「著作権法の一部を改正する法律」が、通常国会において平成 24 年 6 月 20 日に成立し、同年 6 月 27 日に平成 24 年法律第 43 号として公布されました。本法律は、一部の規定を除いて、平成 25 年 1 月 1 日に施行されています。

電気通信事業法

「電気通信事業法」は、電気通信の健全な発達と国民の利便の確保を図るために制定された法律で、電気通信事業に関する詳細な規定が盛り込まれています。

特に、第四条では、何人も電気通信事業者の取扱中の通信を侵してはならない旨の条文があり、通信の秘密が保護されています。
また、第五二条では端末設備の接続の技術基準が定められており、それを受けた端末設備等規則において、IoT 機器のセキュリティ基準等について定められております。

（秘密の保護）
第四条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

２　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

（端末設備の接続の技術基準）
第五十二条　電気通信事業者は、利用者から端末設備（電気通信回線設備の一端に接続される電気通信設備であつて、一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む。）又は同一の建物内であるものをいう。以下同じ。）をその電気通信回線設備（その損壊又は故障等による利用者の利益に及ぼす影響が軽微なものとして総務省令で定めるものを除く。第六十九条第一項及び第二項並びに第七十条第一項において同じ。）に接続すべき旨の請求を受けたときは、その接続が総務省令で定める技術基準（当該電気通信事業者又は当該電気通信事業者とその電気通信設備を接続する他の電気通信事業者であつて総務省令で定めるものが総務大臣の認可を受けて定める技術的条件を含む。次項並びに第六十九条第一項及び第二項において同じ。）に適合しない場合その他総務省令で定める場合を除き、その請求を拒むことができない。
２　前項の総務省令で定める技術基準は、これにより次の事項が確保されるものとして定められなければならない。
一　電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること。
二　電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること。
三　電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすること。

第百七十九条　電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信並

びに同条第四項及び第五項の規定により電気通信事業者の取扱中に係る通信とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号ロの通知及び認定送信型対電気通信設備サイバー攻撃対処協会が取り扱う同項第二号ロの通信履歴の電磁的記録を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

2 電気通信事業に従事する者（第百六十四条第四項及び第五項の規定により電気通信事業に従事する者とみなされる認定送信型対電気通信設備サイバー攻撃対処協会が行う第百十六条の二第二項第一号又は第二号に掲げる業務に従事する者を含む。）が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

3 前二項の未遂罪は、罰する。

端末設備等規則

（インターネットプロトコルを使用する専用通信回線設備等端末）
第三十四条の十　専用通信回線設備等端末（デジタルデータ伝送用設備に接続されるものに限る。以下この条において同じ。）であつて、デジタルデータ伝送用設備との接続においてインターネットプロトコルを使用するもののうち、電気通信回線設備を介して接続することにより当該専用通信回線設備等端末に備えられた電気通信の機能（送受信に係るものに限る。以下この条において同じ。）に係る設定を変更できるものは、次の各号の条件に適合するもの又はこれと同等以上のものでなければならない。ただし、次の各号の条件に係る機能又はこれらと同等以上の機能を利用者が任意のソフトウェアにより随時かつ容易に変更することができる専用通信回線設備等端末については、この限りでない。
一　当該専用通信回線設備等端末に備えられた電気通信の機能に係る設定を変更するためのアクセス制御機能（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第三項に規定するアクセス制御機能をいう。以下同じ。）を有すること。
二　前号のアクセス制御機能に係る識別符号（不正アクセス行為の禁止等に関する法律第二条第二項に規定する識別符号をいう。以下同じ。）であつて、初めて当該専用通信回線設備等端末を利用するときにあらかじめ設定されているもの（二以上の符号の組合せによる場合は、少なくとも一の符号に係るもの。）の変更を促す機能若しくはこれに準ずるものを有すること又は当該識別符号について当該専用通信回線設備等端末の機器ごとに異なるものが付されていること若しくはこれに準ずる措置が講じられていること。
三　当該専用通信回線設備等端末の電気通信の機能に係るソフトウェアを更新できること。
四　当該専用通信回線設備等端末への電力の供給が停止した場合であつても、第一号のアク

セス制御機能に係る設定及び前号の機能により更新されたソフトウェアを維持できること。

電子署名及び認証業務に関する法律

「電子署名及び認証業務に関する法律」は、電子商取引などのネットワークを利用した社会経済活動の更なる円滑化を目的として、一定の条件を満たす電子署名が手書き署名や押印と同等に通用することや、認証業務（電子署名を行った者を証明する業務）のうち一定の水準を満たす特定認証業務について、信頼性の判断目安として認定を与える制度などを規定しています。

電子データが存在していたことと、それ以降改ざんされていないことを証明し、情報の信頼性を担保するためにタイムスタンプという技術があります。タイムスタンプを利用することで、当該電子データがある時刻に存在していたことを示すことができ、また当該電子データについて改変が行われていないかどうか確認することができます。

　このタイムスタンプ技術の利用拡大や海外とのデータ流通を容易にするために、「時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）」が制定されており、時刻認証業務（電子データに関わる情報にタイムスタンプを付与する役務を提供する業務）について、総務大臣による認定制度が置かれています。

電波法

電波は、テレビや携帯電話、アマチュア無線などさまざま場面で利用されています。「電波法」はこの電波の公平かつ能率的な利用を確保するための法律で、無線局の開設や秘密の保護などについての取り決めが規定されています。

（秘密の保護）
第五十九条 何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第四条第一項又は第百六十四条第三項の通信であるものを除く。第百九条並びに第百九条の二第二項及び第三項において同じ。を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。

（罰則）
第百九条 無線局の取扱中に係る無線通信の秘密を漏らし、又は窃用した者は、一年以下の懲役又は五十万円以下の罰金に処する。

特定電子メールの送信の適正化等に関する法律

「特定電子メールの送信の適正化等に関する法律」は、利用者の同意を得ずに広告、宣伝又は勧誘等を目的とした電子メールを送信する際の規定を定めた法律です。

（特定電子メールの送信の制限）
第三条 送信者は、次に掲げる者以外の者に対し、特定電子メールの送信をしてはならない。
一 あらかじめ、特定電子メールの送信をするように求める旨又は送信をすることに同意する旨を送信者又は送信委託者（電子メールの送信を委託した者（営利を目的とする団体及び営業を営む場合における個人に限る。）をいう。以下同じ。）に対し通知した者
二 前号に掲げるもののほか、総務省令で定めるところにより自己の電子メールアドレスを送信者又は送信委託者に対し通知した者
三 前二号に掲げるもののほか、当該特定電子メールを手段とする広告又は宣伝に係る営業を営む者と取引関係にある者
四 前三号に掲げるもののほか、総務省令で定めるところにより自己の電子メールアドレスを公表している団体又は個人（個人にあっては、営業を営む者に限る。）
2 前項第一号の通知を受けた者は、総務省令で定めるところにより特定電子メールの送信をするように求めがあったこと又は送信をすることに同意があったことを証する記録を保存しなければならない。
3 送信者は、第 1 項各号に掲げる者から総務省令で定めるところにより特定電子メールの送信をしないように求める旨（一定の事項に係る特定電子メールの送信をしないように求める場合にあっては、その旨）の通知を受けたとき（送信委託者がその通知を受けたときを含む。）は、その通知に示された意思に反して、特定電子メールの送信をしてはならない。ただし、電子メールの受信をする者の意思に基づき広告又は宣伝以外の行為を主たる目的として送信される電子メールにおいて広告又は宣伝が付随的に行われる場合その他のこれに類する場合として総務省令で定める場合は、この限りでない。

（表示義務）
第四条 送信者は、特定電子メールの送信に当たっては、総務省令で定めるところにより、その受信をする者が使用する通信端末機器の映像面に次に掲げる事項（前条第三項ただし書の総務省令・内閣府令で定める場合においては、第二号に掲げる事項を除く。）が正しく表示されるようにしなければならない。
一 当該送信者（当該電子メールの送信につき送信委託者がいる場合は、当該送信者又は当該送信委託者のうち当該送信に責任を有する者）の氏名又は名称
二 前条第 3 項本文の通知を受けるための電子メールアドレス又は電気通信設備を識別する

ための文字、番号、記号その他の符号であって総務省令で定めるもの
三 その他総務省令で定める事項

（送信者情報を偽った送信の禁止）
第五条 送信者は、電子メールの送受信のために用いられる情報のうち送信者に関するものであって次に掲げるもの（以下「送信者情報」という。）を偽って特定電子メールの送信をしてはならない。
一 当該電子メールの送信に用いた電子メールアドレス
二 当該電子メールの送信に用いた電気通信設備を識別するための文字、番号、記号その他の符号

（架空電子メールアドレスによる送信の禁止）
第六条 送信者は、自己又は他人の営業のために多数の電子メールの送信をする目的で、架空電子メールアドレスをそのあて先とする電子メールの送信をしてはならない。＜

総務省が迷惑メールに対して行っている取り組みについては、迷惑メール関係施策を参照してください。

総務省では、平成 23 年 4 月 1 日から、お使いのパソコンにインストールすることで、メールソフトからの情報提供がワンクリックで可能になるプラグインソフトを配布しています。

詳しくは以下のホームページをご確認ください。

迷惑メール情報提供用プラグイン ダウンロードサイト（総務省）
特定電子メールの送信の適正化等に関する法律のポイント（総務省）

不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）は、不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止する法律です。

識別符号とは、情報機器やサービスにアクセスする際に使用する ID やパスワード等のことです。不正アクセス行為とは、そのような ID やパスワードによりアクセス制御機能が付されている情報機器やサービスに対して、他人の ID・パスワードを入力したり、脆弱性（ぜいじゃくせい）を突いたりなどして、本来は利用権限がないのに、不正に利用できる状態にする行為をいいます。

（目的）
第一条 この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

（定義）
第二条 1～3 略
4 この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。
一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）
二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）
三 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特

定利用をし得る状態にさせる行為

（不正アクセス行為の禁止）
第三条 何人も、不正アクセス行為をしてはならない。

（他人の識別符号を不正に取得する行為の禁止）
第四条 何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。

（不正アクセス行為を助長する行為の禁止）
第五条 何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。

（他人の識別符号を不正に保管する行為の禁止）
第六条 何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

（識別符号の入力を不正に要求する行為の禁止）
第七条 何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。
一 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為
二 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

（罰則）
第十一条 第三条の規定に違反した者は、三年以下の懲役又は百万円以下の罰金に処する。

第十二条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

一　第四条の規定に違反した者

二　第五条の規定に違反して、相手方に不正アクセス行為の用に供する目的があることの情を知ってアクセス制御機能に係る他人の識別符号を提供した者

三　第六条の規定に違反した者

四　第七条の規定に違反した者

第十三条　第五条の規定に違反した者（前条第二号に該当する者を除く。）は、三十万円以下の罰金に処する。

有線電気通信法

「有線電気通信法」は、有線電気通信の設備や使用についての法律で、秘密の保護や通信妨害について規定されています。

（有線電気通信の秘密の保護）
第九条　有線電気通信（電気通信事業法第四条第一項　又は第百六十四条第二項　の通信たるものを除く。）の秘密は、侵してはならない。

（罰則）
第十三条　有線電気通信設備を損壊し、これに物品を接触し、その他有線電気通信設備の機能に障害を与えて有線電気通信を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。
２　前項の未遂罪は、罰する。

第十四条　第九条の規定に違反して有線電気通信の秘密を侵した者は、二年以下の懲役又は五十万円以下の罰金に処する。
２　有線電気通信の業務に従事する者が前項の行為をしたときは、三年以下の懲役又は百万円以下の罰金に処する。
３　前二項の未遂罪は、罰する。
４　前三項の罪は、刑法（明治四十年法律第四十五号）第四条の二　の例に従う。

第十五条　営利を目的とする事業を営む者が、当該事業に関し、通話（音響又は影像を送り又は受けることをいう。以下この条において同じ。）を行うことを目的とせずに多数の相手方に電話をかけて符号のみを受信させることを目的として、他人が設置した有線電気通信設備の使用を開始した後通話を行わずに直ちに当該有線電気通信設備の使用を終了する動作を自動的に連続して行う機能を有する電気通信を行う装置を用いて、当該機能により符号を送信したときは、一年以下の懲役又は百万円以下の罰金に処する。