インターネットって何？

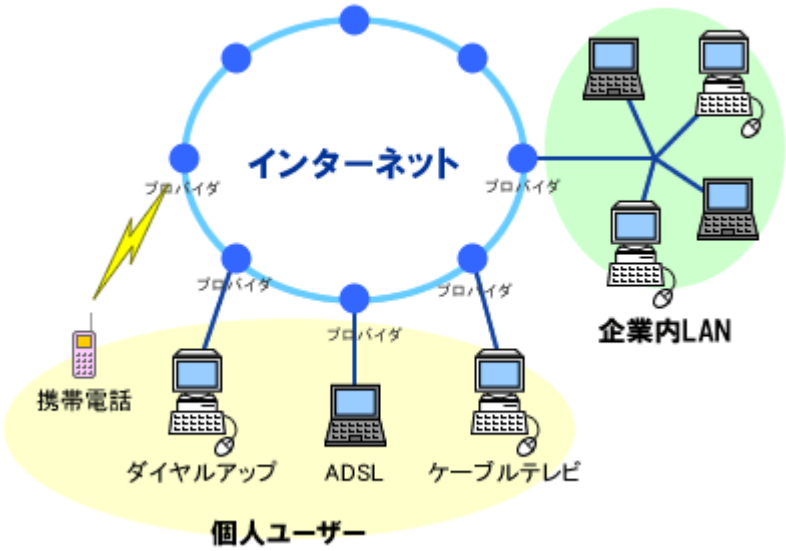
インターネットは、米国国防総省が構築した、ARPAnet（Advanced Reserch Projects Agency net）を起源とする、分散型のコンピュータネットワークです。1990年代に、商用ネットワークとして利用可能になるとともに、世界中で利用者が急激に増大し、電子メールやホームページの閲覧など、さまざまな用途で幅広く活用されています。

ここでは、情報セキュリティの対策を立てるために最低限必要な知識として、インターネットの仕組みやインターネットでできることを説明します。

インターネットの仕組み

インターネットは、世界中のネットワークが接続されたネットワークです。会社や学校などのネットワークが、それぞれの契約しているプロバイダによって、インターネットに接続されています。

インターネットには、メールサーバーやWebサーバーのように、クライアントから送られる要求に対して、決められた動作を行うように設定されたサーバーがあります。それらのサーバーが互いに連絡を取り合うことで、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数字です。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、下記の例のような数字の組み合わせによって表記されるのが一般的です。

IPアドレスは、各国ごとに設置された機関がIPアドレスを利用者に配布しています。日本では社団法人日本ネットワークインフォメーションセンター（JPNIC）という組織が、このIPアドレスを管理しています。

IPアドレスの例

127.0.0.1

通常、電子メールでは“mail.soumu.go.jp”、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。これはドメイン名を使用した記述方法で、これらのアドレスを受け取ったDNSサーバーが、IPアドレスに自動的に変換することで行き先を見つける仕組みになっています。

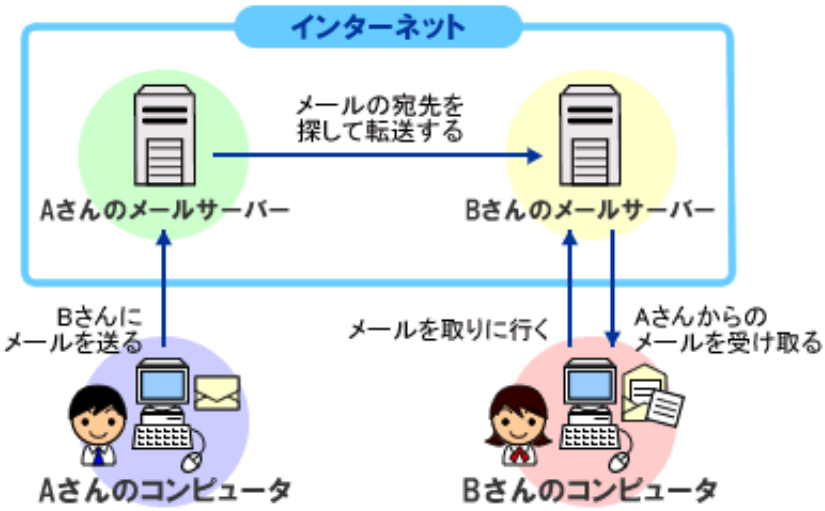
電子メールの仕組み

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ーが連携することによって動作しています。

電子メールを送信すると、契約しているプロバイダや、学校や会社にあるメールサーバー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ーは、宛先として指定されているプロバイダなどのサーバーに、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ーは、受取人が電子メールを取りにくるまで、サーバー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、契約しているプロバイダのメールサーバーに自分宛ての電子メールを取りに行き、届けられた電子メールを受け取ります。

一般的に電子メールの送信や他のサーバーへの転送にはSMTPサーバーが、電子メールの受信にはPOP3サーバーが使用されています。

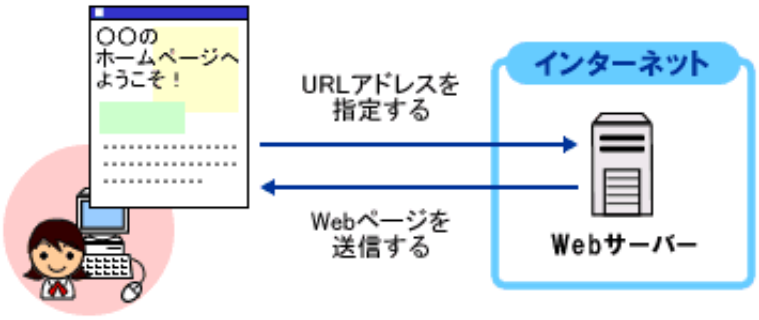


なお、電子メールをやり取りする際には、メールサーバーに接続するために、インターネット上にあるDNSサーバーを利用して、対象とするメールサーバーのIPアドレスを取得するようになっています。

ホームページの仕組み

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、IE（Internet Explorer）やNetscapeなどのWebブラウザでURLアドレスを指定します。URLアドレスを指定すると、Webブラウザがインターネット上のWebサーバーを探して、目的のホームページを自分のコンピュータに表示します。



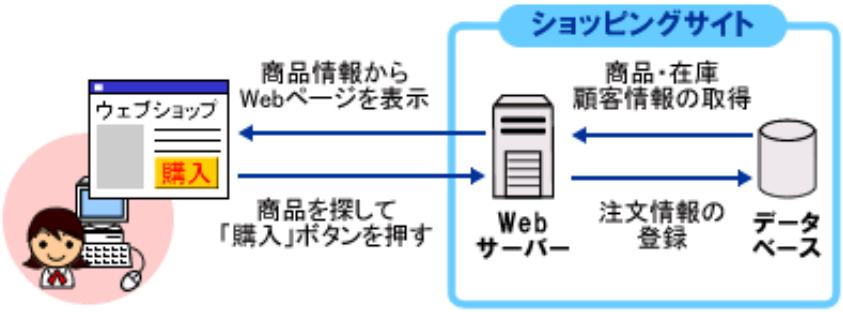
URLアドレスは、「http://www.soumu.go.jp/joho_tsusin/joho_tsusin.html」のように指定します。「ｈｔｔｐ」はホームページの閲覧に使用されるＨＴＴＰというプロトコルを表しています。「www.soumu.go.jp」はWebサーバーを指定しています。その後の「/joho_tsusin/joho_tsusin.html」がホームページの場所と名前を表しています。

実際に、このようなURLアドレスで示されているWebサーバーに接続するためには、インターネット上にあるDNSサーバーを利用して、対象とするWebサーバーのIPアドレスを取得するようになっています。

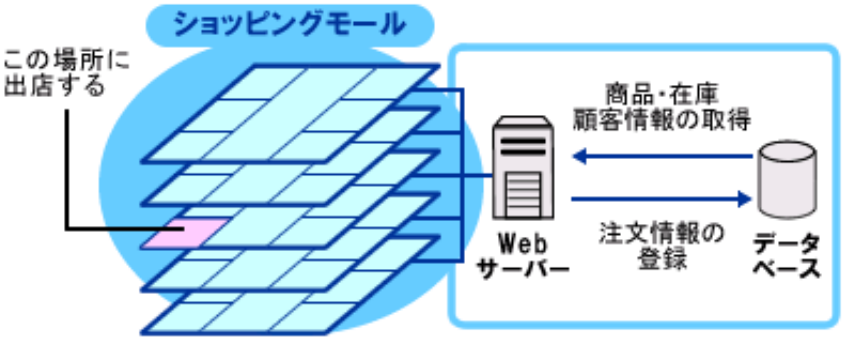
ホームページの表示には、主にHTML形式のファイルが使用されます。このファイルの中には、画像や動画、音声などのマルチメディア情報を指定することができます。また、テキストやイラスト、図などにハイパーリンクを埋め込むことによって、ユーザーを別のWebページに誘導することができます。

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 サーバーとデータベースサーバーが連携して動作しています。データベースには、顧客情報、商品情報、在庫情報、販売情報などが格納され、Web サイトの訪問者が購入した情報はリアルタイムにデータベースに書き込まれます。ショッピングサイトの管理者は、データベースに格納された販売情報を元にして、商品の発送や請求の手続きを開始します。



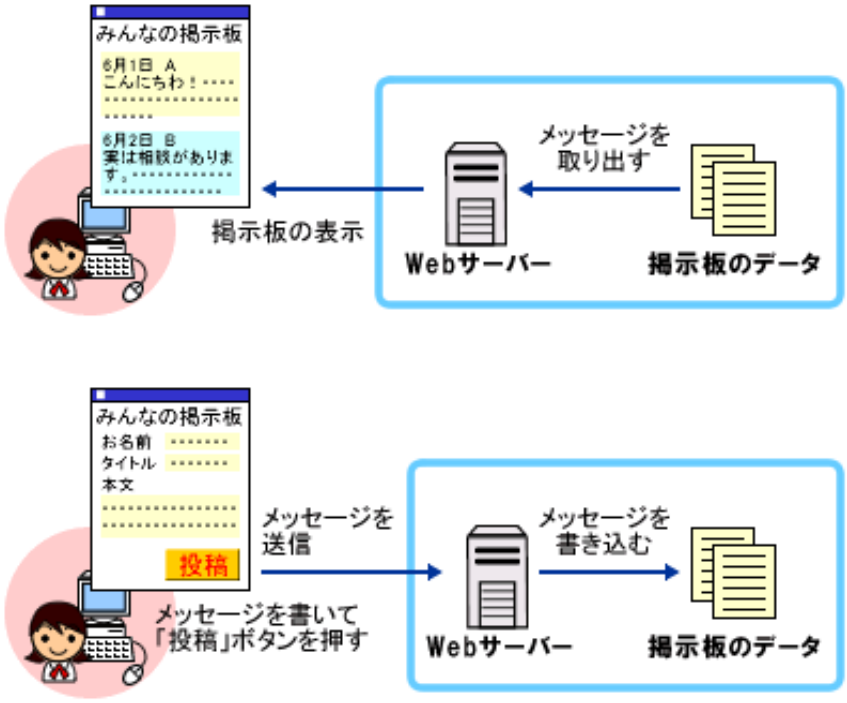
また、モールと呼ばれるショッピングサイト群では、管理会社がWebサーバーやデータベースサーバーを用意して、ショッピングサイトの仕組みをお店や会社に貸し出しています。そのため、小さなお店や会社でも、決められた料金を支払えば、特定の形式の Web ページを作成するだけで、簡単にショッピングサイトを開設できるのです。



電子掲示板の仕組み

電子掲示板は、ホームページで利用できる代表的な機能のひとつです。電子掲示板では、Webサーバーに保管されているデータを利用して、最新のメッセージを表示するようになっています。一般的な電子掲示板では、書き込みフォームにメッセージを入力すると、Web サーバーのデータにメッセージを追加することができます。

そして、その後、別の訪問者がこの電子掲示板を参照すると、新たなメッセージが追加された状態で表示されます。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。

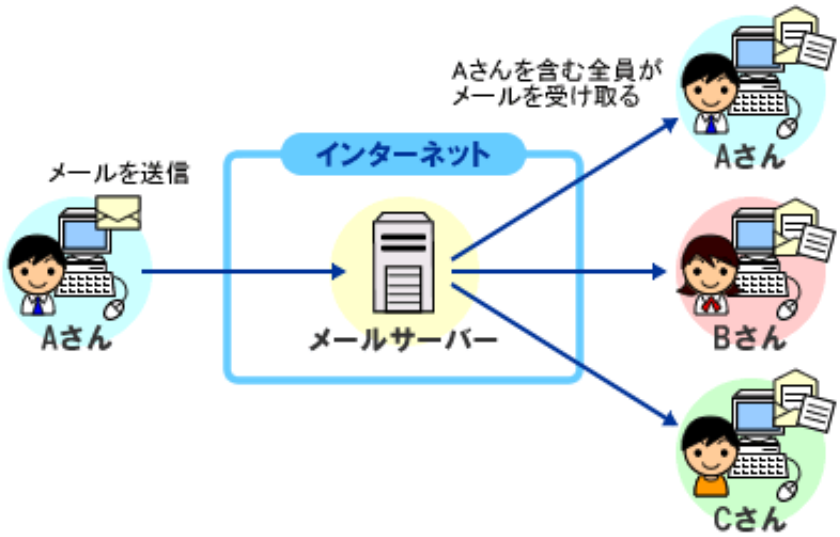
ツリー型は、特定の話題ごとに個別のまとまりで表示する電子掲示板です。それぞれのメッセージに対する返事を書き込むことで、自動的にメッセージのツリーができあがります。この形式は、特定の情報に対して、討論を繰り返す場合などに有効な表示方法です。

伝言板型の例

ツリー型の例

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ユーザー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。

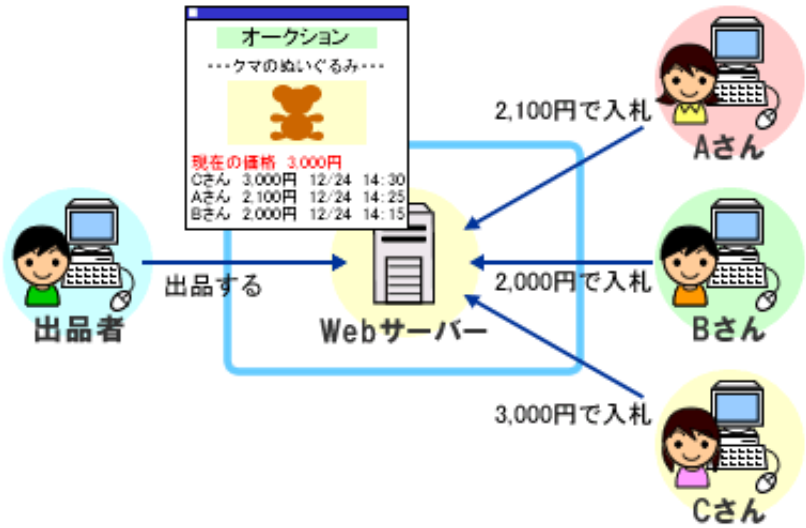
また、最近はメーリングリストにウイルス付きの電子メールが投稿されて、参加者全員にウイルスがばらまかれてしまうというトラブルが発生しています。メーリングリストに参加する場合には、他のユーザーに対する責任があるということを認識しておかなければなりません。

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ユーザー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。

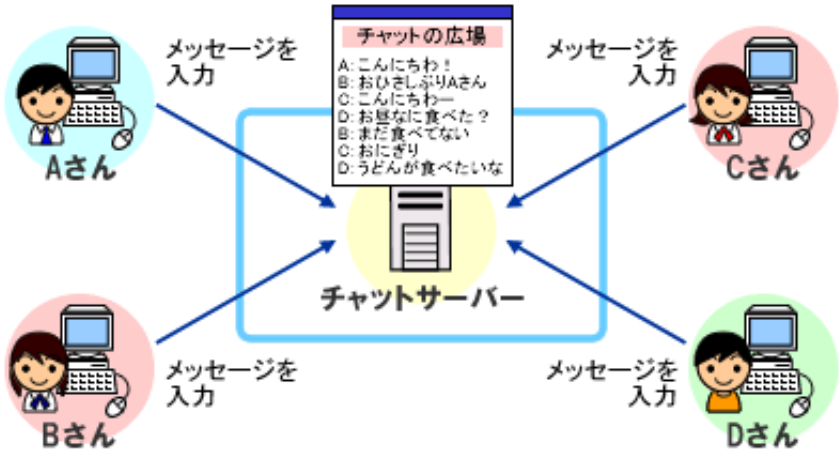


ただし、ネットオークションでは、盗品や違法な薬物などが出品されたり、代金を支払っても商品が送付されてこないなどの違法行為が行われることがあります。一般的な商店での購入と異なり、販売者の顔が見えないため、オークションサイトでの販売者の過去の取引評価等を参考にしながら、慎重に利用しましょう。

チャットの仕組み

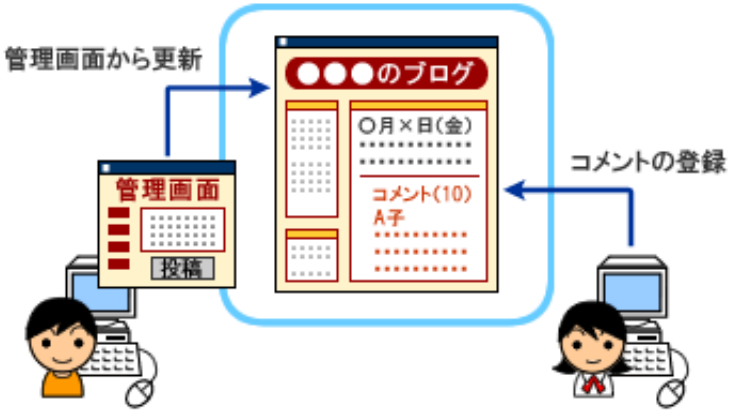
チャット（chat）は、インターネットでよく利用されるサービスのひとつで、本来は“おしゃべり”という意味の言葉です。インターネットでは、複数のユーザーがリアルタイムにメッセージを送信するためのシステムをチャットと呼びますが、現在のチャットシステムでは、チャットサーバーに接続すると、参加者が入力したテキストのメッセージがリアルタイムに表示される仕組みを提供していることが多いようです。

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。



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。



新しく情報を追加する場合に、これまでのホームページでは、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たのに対して、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。

ブログのシステムでは、その多くがデータベースを利用して、書き込まれた情報を格納するようになっています。つまり、管理者が書き込んだ情報はデータベースに格納され、閲覧者がブログを訪問すると、データベースに格納されている情報から毎回ホームページを生成し直すといった仕組みです。

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、新たなユーザー層がブログを利用し始めています。

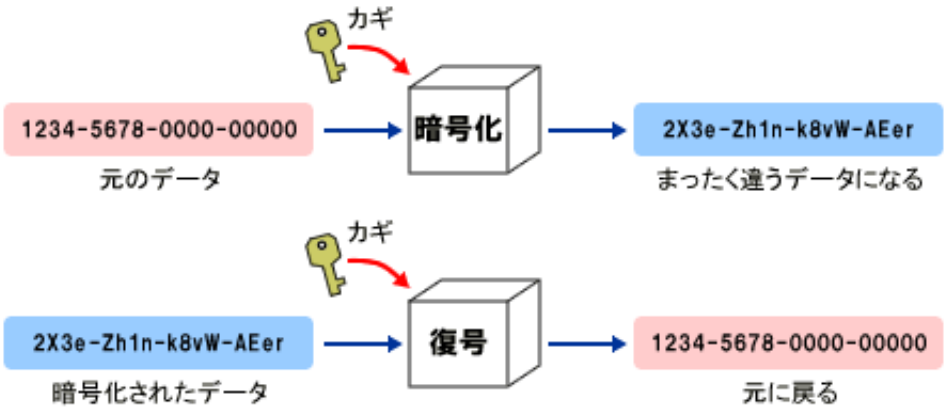
さらに、ブログの多くは、書き込まれた情報に対して、「コメント」を登録できるようになっています。コメントはこれまでの電子掲示板に近い技術ですが、ブログに登録されたそれぞれの情報に対して、閲覧者が意見や追加の情報を書き込むことができるようになっています。このコメントの機能により、ブログは、発信された情報や意見に対するディスカッションを行う目的にも利用できるようになり、新しいコミュニケーションの場所として活用されています。

ブログという用語は、「Web log」（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。

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格納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格納するようになっています。

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。これらの用途の場合には、データの受信側が暗号化データを復号と呼ばれる処理で元のデータに戻して利用できるようになっています。



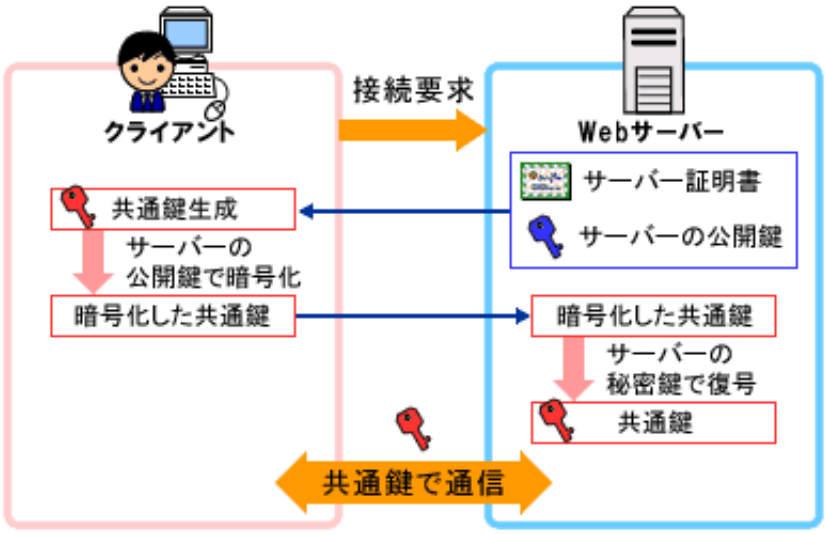
SSLの仕組み

SSL（Secure Socket Layer）とは、インターネット上でデータを暗号化して送受信する方法のひとつです。

通常、インターネットでは、暗号化されずにデータが送信されています。そのため、通信途中でデータを傍受されると、情報が第三者に漏れてしまう可能性があります。また、相手のなりすましに気付かずに通信すると、データがなりすましの相手に取得されてしまう可能性があります。

現在、クレジットカード番号や個人情報を扱う多くのホームページでは、通信途中での傍受やなりすましによる情報漏洩を防ぐ目的で、SSL を利用しています。

利用者がSSLを利用できるサーバーとデータをやり取りする場合には、Webサーバーと利用者のコンピュータが相互に確認を行いながらデータを送受信するようになるため、インターネットにおける通信内容の暗号化及びなりすましの防止が実現されます。



IE（Internet Explorer）やNetscapeなどのSSLに対応したWebブラウザを利用して、SSLで保護されたサイトに接続すると、通信相手の認証が行われ、通信データが自動的に暗号化されるようになります。このとき、主なWebブラウザでは、ステータス欄に鍵のマークが表示されます。たとえば、IEでは、SSL接続を行っている場合には、右下のステータス欄に鍵のマークが表示されるようになっています。なお、この鍵のマークをダブルクリックすると、サーバー証明書の詳細情報を確認することができます。

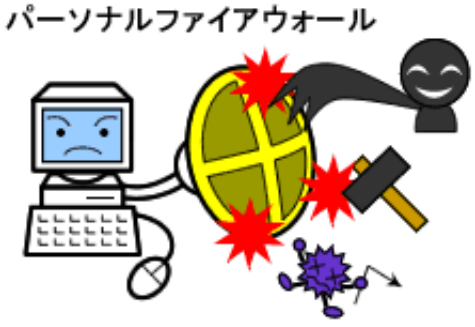
ファイアウォールの仕組み

ファイアウォールとは、本来火災などから防御するための防火壁のことを言います。火災のときに被害を最小限に食い止めることから、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。

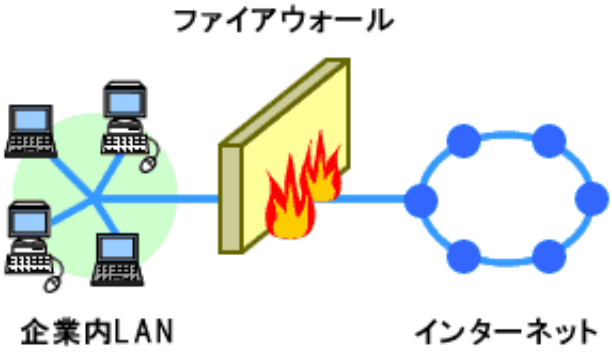
現在のファイアウォールには、主に2通りのものがあります。ひとつは家庭など、1台のコンピュータを防御することを目的としたパーソナルファイアウォールで、もうひとつは、企業や家庭のネットワーク全体を防御する本来のファイアウォールです。

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を導入すると、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していることも多いようです。



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。このようなファイアウォールは、ソフトウェアとして提供されているものと、機器として提供されているものがあります。また、最近では、ルーターにファイアウォールの機能が装備されているものが多くなっています。



また、プロバイダが自社の接続サービスを利用しているユーザーを対象として、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。そのサービスの内容は、ウイルス対策機能を含めた統合的なセキュリティサービスなど、プロバイダによって異なります。ファイアウォールのサービスの提供の有無や、サービスの提供内容などについては、プロバイダのホームページで確認するか、プロバイダに問い合わせてください。

ファイアウォールの主要な機能には、以下のようなものがあります（これらの機能は、機種によって異なります）。

■フィルタリング機能

不正なパケットを遮断して、許可されたパケットだけを通過させます。

■アドレス変換機能

外部のネットワークと内部のネットワークにおいて、相互に IP アドレスを割り当てる機能です。

■遠隔操作、監視機能

別のコンピュータからファイアウォールの設定を行ったり、ログを確認したりできる機能です。

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対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対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。

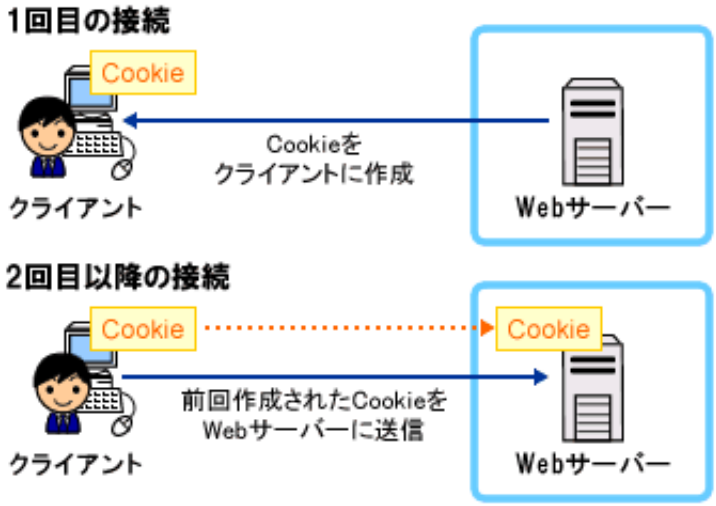
Cookieの仕組み

Cookie（クッキー）とは、Webサーバーがクライアントコンピュータに預けておく小さなファイルのことです。

クライアントコンピュータが、あるWebサーバーに初めて接続した際に、Webサーバーがクライアントコンピュータの中に、そのWebサーバー専用のCookieファイルを作成します。

そして、次回、クライアントコンピュータがWebサーバーに接続したときには、Webブラウザがそのcookieをwebサーバーに送信します。このような仕組みによって、Webサーバーは、個々のクライアントコンピュータが前回使用していた情報を読み取ることができるようになります。

Cookieには、Webサーバーによってどのような情報でも格納できますが、多くの場合は、ユーザー名などの接続情報、ショッピングサイトなどで購入する商品を一時的に保管する“買い物かご”の情報、氏名や住所、電話番号などの一度登録した会員情報といった管理に利用されています。



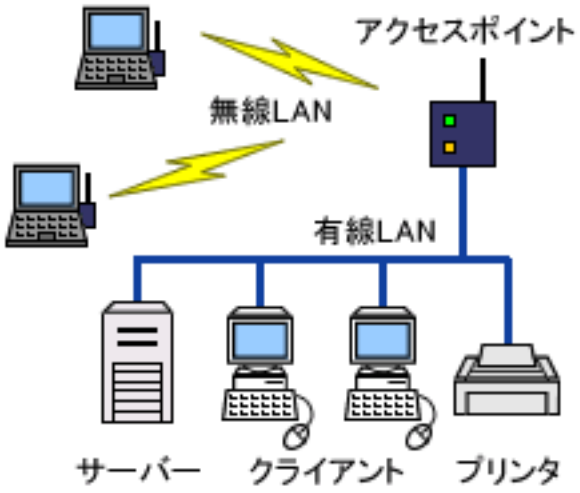
Webサイトによっては、Cookieに個人情報などの重要なデータが格納されている可能性もあります。しかし、本来は取得できないはずの別のWebサーバー用のCookieの情報を取得できてしまうというWebブラウザのセキュリティホールが過去に発見されたこともあったため、現在Cookieはクライアントコンピュータにおける情報セキュリティ上のひとつの懸念事項になっています。

なお、現在のWebブラウザではセキュリティの設定やプライバシーの設定といった機能によって、Webサイトごとに Cookieの利用を指定することができるようになっています。ショッピングサイトなどでは、Cookieを利用しなければWebサイト自体が利用できないこともあるため、自分の信頼するWebサイトにだけCookieの使用を許可するのがもっとも現実的な利用方法と言えます。

無線LANの仕組み

無線 LAN とは、有線 LAN のケーブルを無線に置き換えたものです。無線 LAN の機器にはさまざまな種類のものがありますが、無線 LAN のアクセスポイントと無線 LAN アダプタを利用して、有線の LAN に接続するために無線 LAN を利用する方法が一般的です。

無線 LAN のアクセスポイントとは、有線 LAN と接続して使用するもので、無線 LAN アダプタとの送受信を行う役割を果たします。無線LANアダプタは、コンピュータに接続して使用するもので、主にノートパソコンに使用できるPCカードタイプのものと、デスクトップコンピュータで使用できるPCI カードタイプ、USB 接続タイプのものがあります。最近では、無線 LAN を使用できる環境が増えたこともあり、あらかじめ無線 LAN アダプタが内蔵されているノートパソコンも多くなってきました。



配線の必要がないため、LAN ケーブルを這わすことが困難な環境や、レイアウトの変更が多いオフィスなどでは、無線 LAN は非常に便利なものです。しかし、現在の無線 LAN の標準的な規格では、情報セキュリティ対策の機能が万全ではないと言う弱点もあるため、必ず適切な情報セキュリティ設定を行った上で利用するようにしてください。

セキュリティホールとは？

セキュリティホールとは、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。セキュリティホールが残された状態でコンピュータを利用していると、ハッキングに利用されたり、ウイルスに感染したりする危険性があります。

代表的なセキュリティホールに、バッファオーバーフローがあります。バッファオーバーフローとは、OSやアプリケーションソフトのプログラムが処理に利用しているメモリのバッファに、入りきらない量のデータが渡されることで、予期しないような動作が実行されたり、システムが停止してしまったりすることです。

バッファオーバーフローは、コンピュータで実行されているプログラムが、内部で利用するバッファを適切に管理することで解決しますが、プログラム内の一部にでもそのような対策を怠った箇所が残されていた場合に、重大なセキュリティホールになってしまう可能性があるというわけです。

このようなセキュリティホールが発見されると、多くの場合、ソフトウェアを開発したメーカーがパッチと呼ばれる修正プログラムを作成して提供します。しかし、バッファオーバーフローの問題は、完全に対策を施すことが困難であり、次々と新たなセキュリティホールが発見されているのが現状です。

バッファオーバーフローのセキュリティホールが放置されているコンピュータでは、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。

セキュリティホールはクライアントとサーバー、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ーの場合には、セキュリティホールを利用したハッキングによって、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、ハッカーに悪用されてしまう可能性があるため、必ずセキュリティホールを塞いでおかなければなりません。

セキュリティホールを塞ぐには、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セキュリティホールを塞ぐことができます。ただし、一度セキュリティホールを塞いでも、また新たなセキュリティホール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セキュリティホールが発見されたときに、メーカーがパッチ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パッチ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、対応パッチを適用するまでの間は十分な注意が必要です。

スパイウェアとは？

スパイウェアとは、コンピュータ内部からインターネットに対して情報を送り出すソフトウェアの総称です。一般的には、そのようなソフトウェアがインストールされていることや動作していることにユーザーが気付いていない状態で、自動的に情報を送信するソフトウェアをスパイウェアと呼んでいます。

これらのすべてが悪質なソフトウェアというわけではありませんが、スパイウェアの中には、明らかに情報を盗み取ることを目的として、ユーザー名やパスワード、メールアドレスといった個人情報を送信する機能を持つものもあり、インターネットに接続しているコンピュータにとって、大きな情報セキュリティ上の問題となっています。

スパイウェアは、主に次の 2 種類に分類することができます。

- ユーザーがインストールしたソフトウェアに組み込まれているもの
- ユーザーの知らないうちに、自動的にインストールされてしまうもの

このうち、ユーザーがインストールするソフトウェアに組み込まれている場合には、そのソフトウェアの開発会社に、ユーザーの利用状況や障害情報などを送信することを目的としていることが多く、個人情報を収集することが目的ではないため、ユーザーにとってはそれほど大きな脅威になることはないかもしれません。また、この場合のほとんどは、ソフトウェアの「エンドユーザー使用許諾契約」に情報を送信する機能を組み込むといった旨の説明が記載されています。

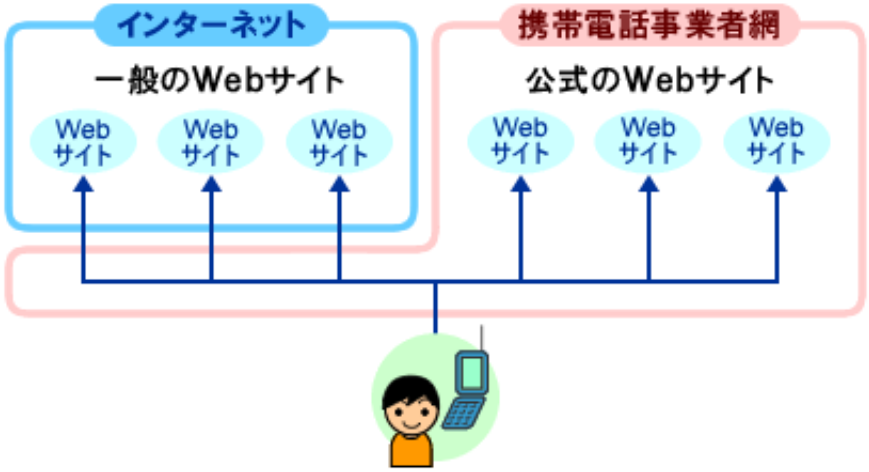
しかし、インターネットで公開されているフリーウェアなどと共に、知らないうちにスパイウェアをインストールしてしまうソフトウェアや、ホームページを閲覧しただけでダウンロードされてしまう ActiveX コントロールなどのスパイウェアについては、ユーザーは自分のコンピュータに含まれるどのような情報が誰に対して送信されているかということさえ分からない可能性があります。

現在では、このようなスパイウェアから防御するために、スパイウェアを除去するためのソフトウェアが登場してきています。また、一般ユーザー向けの統合的な情報セキュリティソフトでは、ウイルス対策機能、パーソナルファイアウォールに加えて、スパイウェアの除去機能を搭載したものもあるため、これらのソフトウェアを導入するという方法も検討してください。

携帯電話によるインターネット利用

現在の携帯電話の多くは、通話だけでなく、電子メールの利用やホームページの閲覧も行うことができるようになっています。これらの機能の多くが、インターネットを利用して実現されています。

携帯電話を利用して閲覧できるホームページには、大きく分類して、一般のWebサイトと携帯電話会社が提供する公式のWebサイトがあります。一般のWebサイトとは、パソコンでも接続できるインターネット上のホームページのことで、携帯電話で閲覧ができるような大きさにコンテンツが調整されていることもあります。これに対して、公式のWebサイトとは、それぞれの携帯電話会社がさまざまな会社と提携して用意している携帯電話専用のホームページのことです。公式のWebサイトは携帯電話事業者網の中にあるため、基本的には安全と言えますが、一般のWebサイトを閲覧する場合には、パソコンと同様に注意が必要です。

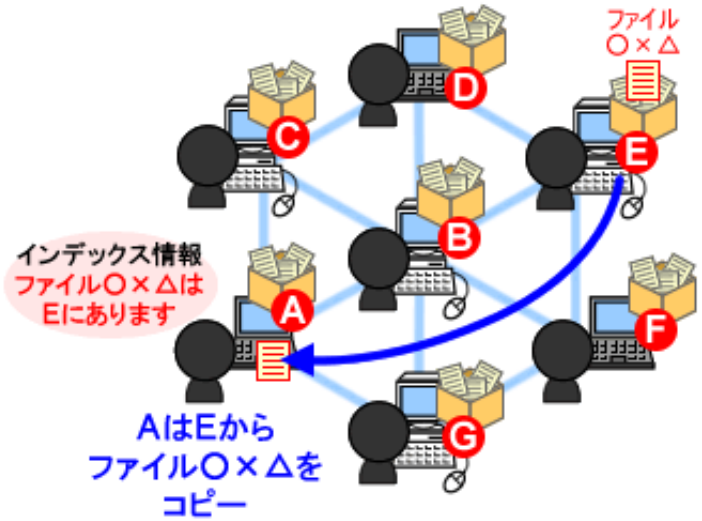


現在の携帯電話は、パソコンと同様に、Javaなどのプログラム実行用のプラットフォームが用意されていて、後からインストールしたアプリケーションが動作するようになっています。そのため、悪意のあるプログラムを動作させてしまうと、携帯電話の情報（電話帳やスケジュールなど）が盗み取られたり、消去されたりする危険性があることが指摘されています。また、アプリケーションが実行できるということは、携帯電話であってもウイルスに感染する危険性があるということを意味しています。特に、携帯電話には共通のアドレス帳などが整備されており、悪質なウイルスが発生した場合には、パソコン以上に急速に感染が広まる危険性があると言われています。

このようなこともあり、携帯電話だからといっても、信用のできないホームページを訪問しないようにするなど、情報セキュリティ対策への意識を持つことが必要と言えます。

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ユーザー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 －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ー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ーで管理したり、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。

最初に登場したファイル共有ソフトは、米国で1999年に発表されたNapster（ナップスター）です。Napsterは、サーバーでインデックス情報とユーザーの接続だけを管理し、インデックス情報を元にして、クライアント間でファイルを転送する仕組みを持っていました。

Napsterは音楽ファイル専用のファイル共有ソフトでしたが、やり取りされるコンテンツの多くが音楽CDから違法に複製されたものであったことから、大きな社会問題となり、最終的には音楽関連団体の訴えにより運営が差し止められました。また、そのコンテンツの内容だけでなく、Napsterのファイル転送量がインターネット回線を占有してしまうことも多く、大学などではNapsterの利用を禁止するところもありました。

その後、日本でもWinnyやWinMXといったファイル共有ソフトが登場し、ADSLなどのブロードバンド通信の普及に伴い、多くのユーザーに利用されました。しかし、そこで共有されるデータも、違法な音楽データ、映画、テレビ番組、ゲームソフトのファイルといったものが多く、著作権法違反幇助容疑でWinnyの開発者が逮捕されるという事件にまで発展しました。

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。

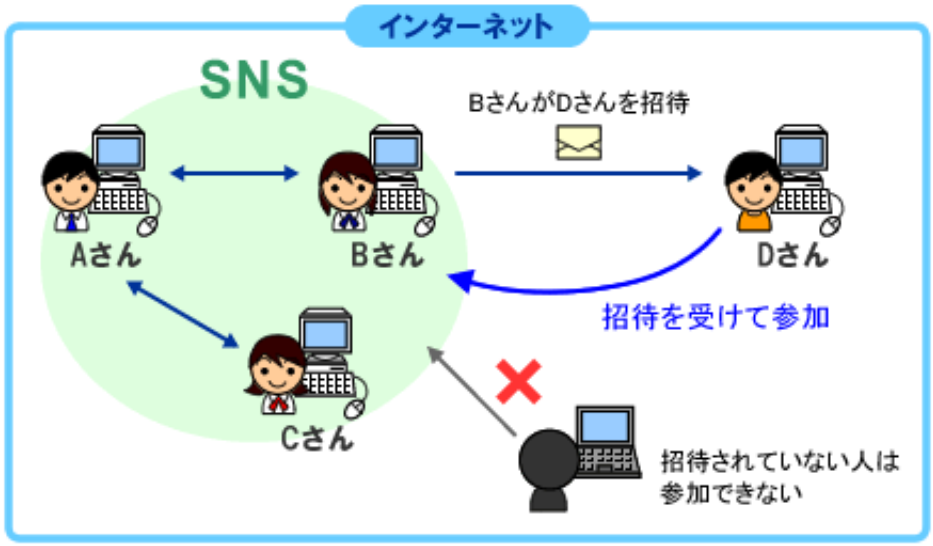
SNS(ソーシャルネットワーキングサービス)の仕組み

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、限られたユーザーだけが参加できるWebサイトの会員制サービスのことです。友人同士が集まったり、同じ趣味を持つユーザーが集まったり、近隣地域のユーザーが集まったりと、ある程度閉ざされた世界にすることで、密接なユーザー間のコミュニケーションを可能にしています。

そのため、SNSでは登録制や招待制という形にすることで、ユーザーを登録する仕組みを採用しています。招待制のSNSの場合には、既にSNSに登録しているユーザーが別の友人を招待することで、その友人がユーザー登録できる権利を獲得します。

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した日記機能などが用意されていたり、自分のホームページへの訪問者の履歴を参照する機能などが提供されています。また、自分だけのアドレス帳を管理して、SNSに参加しているメンバー情報を管理することもできます。

友人や趣味仲間などと利用できる場としてのSNSは、とても有効的かつ効率的なコミュニケーション手段であると言えますが、最近では詳細なプロフィールを掲載していたユーザーの個人情報の漏洩事件や、簡単なパスワードが設定されていたため、不正ログオンの被害に遭い、未公開情報を入手されてしまうなどの問題も発生しています。そのため、SNSであっても、やはりインターネット上に情報が公開されているということを念頭に置いて利用することが大切であると言えます。



招待制のSNSの場合

ボットとは？

ボット（BOT）とは、コンピュータを外部から遠隔操作するためのコンピュータウイルスです。そして、インターネットを通じて、悪意のあるハッカーが、常駐しているボットにより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、このような常駐型の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。

ボットに感染させたハッカーは、その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ーへの攻撃」、「感染活動」などの迷惑行為や犯罪行為を行ないます。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を操作した情報を盗み出す「スパイ活動」も行なうことがあります。

ボットに感染したコンピュータとそのコンピュータの持ち主はもちろん被害者なのですが、感染した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、迷惑メールを受け取ったり、攻撃されたりしたコンピュータから見ると、ボットに操られた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です。

ボットへの対策として、日常的に適切な情報セキュリティ対策を心がける必要があります。まず、ボットはウイルスとして侵入してくることが多いため、基本的にはウイルス対策がもっとも重要と言えます。しかし、最近ではさまざまな手口の侵入方法が考えられているため、以下のような対策を心がけるようにしてください。

- ウイルス対策ソフトの導入とウイルス検知用データの更新
- セキュリティホールを塞ぐための OS やソフトウェアのパッチの適用
- パーソナルファイアウォールの導入