社員・職員全般のための情報セキュリティ対策

企業や組織の一員であるユーザーには、どのような情報セキュリティ対策が要求されるのでしょうか。ここでは、企業・組織における社員・職員のための情報セキュリティ対策について説明します。

なお、企業や組織において、実施する情報セキュリティ対策の方針や行動指針を明確にした情報セキュリティポリシーを策定しているケースが増えています。情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、ならびに情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。

所属する企業や組織において、情報セキュリティポリシーが策定されている場合には、以下の内容と共に、組織内の情報セキュリティポリシーを参照してください。

※特に重要な項目には マークがついています。

安全なパスワード管理

重要!

他人に自分のユーザー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管理が大切です。適切なパスワード管理には、以下の 3 つの要素があります。

■安全なパスワードの作成

安全なパスワードとは、他人に推測されにくく、ハッキングツールなどの機械的な処理で割り出しにくいものを言います。

安全なパスワードの作成条件としては、以下のようなものがあります。

- 名前などの個人情報からは推測できないこと
- 英単語などをそのまま使用していないこと
- アルファベットと数字が混在していること
- 適切な長さの文字列であること
- 類推しやすい並び方やその安易な組み合わせにしないこと

逆に、危険なパスワードとしては、以下のようなものがあります。

- ✗ 自分や家族の名前、ペットの名前
- ✗ 電話番号や郵便番号、生年月日など、他人から類推しやすい情報
- ✗ 社員コード
- ✗ 辞書に載っているような一般的な英単語
- ✗ “aaaaa”など、同じ文字の繰り返し
- ✗ ユーザー名と同じ文字列
- ✗ 短かすぎる文字列

インターネットなどで配布されているハッキングツールの中には、機械的にパスワードを推測する機能を持つものがあります。それらのハッキングツールでは、辞書に載っている英単語や簡単な英数字の繰り返し（123 や abc、aaa など）を自動的に組み合わせることで、パスワードを探し出そうとします。このようなハッキングツールでパスワードを割り出されないようにするためには、機械的に推測しやすい文字列を使わないようにすることが大切です。

■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
●ユーザー名や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作ったり、ディスプレイにそのメモを貼ったりしないこと
●パスワードを Web ブラウザなどのソフトウェアに記憶させないこと

■パスワードの定期的な変更

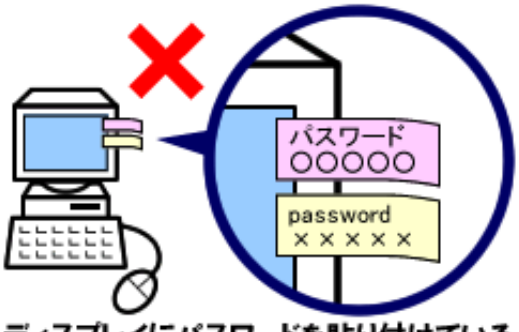
安全なパスワードを作成し、パスワードの保管方法も徹底したとしても、同一のパスワードを長期間使い続けることは避けなければなりません。定期的にパスワードを変更するようにしましょう。また、定期的な変更といっても、2 つか 3 つのパスワードをあらかじめ決めて、使いまわすのも避けるようにした方が良いでしょう。

パスワードを定期的に変更しなければならない理由には、以下のようなものがあります。

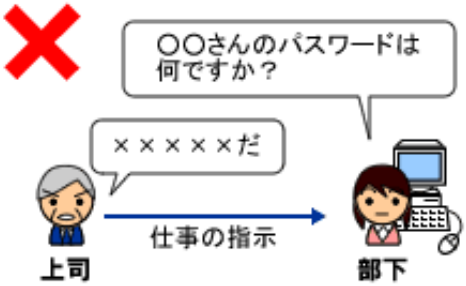
●他人に推測されにくいパスワードでも、ハッキングツールを使って長時間かければパスワードが割り出されてしまうこと
●仮にパスワードが割り出されてしまっても、なりすましなどの被害を受け続けることを避けることができること

企業・組織におけるパスワードは、ユーザー名と組み合わせることで、企業内の情報資産へのアクセスレベルを決める重要なものです。安易なパスワードを設定したり、自分のパスワードを同僚が知っていたりする状態で、機密情報の流出や、なりすましにより自分が承認していない支出行為が実行される事態が起こったら、自身の管理責任を問われることもあります。

パスワードの重要性を再認識して、適切なパスワード管理を心がけましょう。



ディスプレイにパスワードを貼り付けている



他のユーザーにパスワードを教えている

ウイルスからの防御

自分のコンピュータや社内のネットワークを防御するためには、まず第一にウイルスへの適切な予防が必要です。

従来のウイルスは、ほとんどが不用意に添付ファイルを開かないといった対策だけでも十分でしたが、最近のウイルスは、電子メールをプレビューしたり、Web ブラウザでホームページを閲覧したりするだけで感染するなど、その仕掛けはますます複雑で狡猾なものになってきています。ウイルスに感染したときの活動内容も、電子メールをやり取りした相手のメールアドレスを探し出して、何十通ものウイルス付きの電子メールを自動的に送信したり、LAN に接続している他のコンピュータに感染したりするなど、以前に比べて被害規模が急速に拡大し、感染速度も速まってきています。

ウイルス感染の予防対策として、必ず行わなければならないことは、コンピュータにウイルス対策ソフトをインストールして、ウイルス検知用データを常に最新のものに更新しておくことです。

次に行わなければならないことは、企業や組織での情報システム部門などからのウイルスに関する連絡に注意を払い、もしおかしいなと思った電子メールが届いた場合は、情報システム部門などにすぐに相談することです。また、Web ブラウザの設定についても、情報システム部門に問い合わせするなどして適切な設定に変更するという方法を取ることも大切です。

万一ウイルスに感染してしまった場合は、コンピュータの LAN ケーブルを抜くなどの方法で、社内のネットワークからコンピュータを切り離すことを心がけてください。その上で社内の情報システム部門などに相談しましょう。

ウイルスに感染してしまうと、インターネットに個人情報や機密情報が漏洩してしまったり、盗み出されてしまったりする危険性もあります。また、取引先の方にウイルスが含まれた電子メールが送られてしまったという話を聞くこともあると思います。これらのような事態が発生した場合には、企業・組織として信用を大きく落とすことになります。今後も、より一層悪質で強力なウイルスが発生し続けることは間違いありません。そのため、ひとりひとりのユーザーがウイルスに対する正しい知識を持って対応することが、企業・組織における情報セキュリティにとっては何よりも大切なことであると言えます。

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。

悪意のあるホームページ

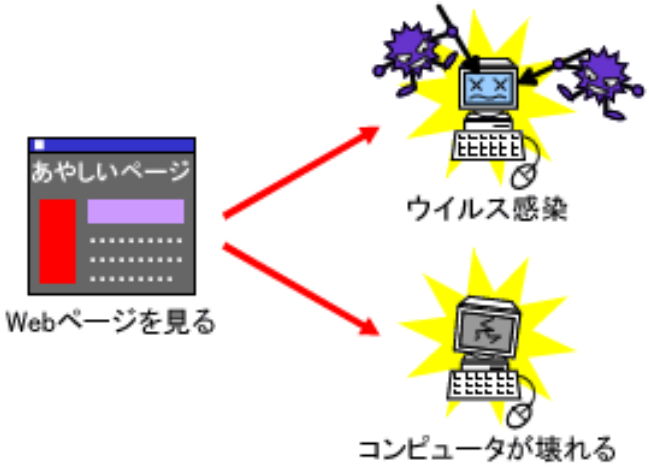
インターネットにはさまざまなホームページが公開されていますが、それらの中には個人情報を収集することや、いやがらせが目的のものもあります。また、ホームページによっては、閲覧しただけで、ウイルスに感染したり、コンピュータシステムを破壊されたりしてしまうものもあります。

まず第一に心がけなければならないのは、悪意を持ったホームページが存在するということを認識することです。信用できないホームページには個人情報を書き込まないようにするなどの対策が必要です。また、ホームページによってはCookieを利用して、閲覧時に入力した情報をWebブラウザに保管させることがありますが、ここにパスワードなど、重要な個人情報が含まれることもあるため、必要に応じてWebブラウザの設定を見直すことも検討すべきです。Webブラウザの設定変更の方法については、情報システム部門などに相談してください。

このようなホームページの被害を受けないために、まずはウイルス対策ソフトを導入するか、プロバイダによるウイルス対策サービスを利用するようにしてください。その上で、怪しいホームページはできる限り閲覧しないことが大切です。特に、不特定多数のユーザーが利用する電子掲示板では、いやがらせのためにこのような動作をするホームページへのリンクを貼り付ける場合があるので、むやみにリンクをクリックせずに慎重に利用するようにしましょう。

最近では悪意を持たないホームページであっても、ホームページ開設者の知らないうちにWebページが改ざんされてしまい、別の悪意のあるサイトの一部が見えないように埋め込まれていたり、自動的に別のサイトに誘導されたりすることが増えています。このような改ざんされたホームページから身を守るためにも、やはりしっかりとしたウイルス対策が必要です。また、パッチ等の修正プログラムを確実に適用し、Webブラウザは常に最新の状態を保つようにしてください。

悪意のあるスクリプトが自動的に実行されないようにするには、Web ブラウザの設定を変更して、JavaScript の実行時に警告を出すようにする、もしくは信頼できる Web サイト（信頼済みサイト）以外では JavaScript を実行させないといったことを実施してください。



ソフトウェアの情報セキュリティ対策

Web ブラウザや電子メールソフト、OS、Office アプリケーションなどのソフトウェアには、時間の経過とともに、セキュリティホールと呼ばれる不具合が発見されることがあります。

セキュリティホールは、プログラムの不具合や設計ミスに起因して起こるものですが、それらを修正するためにパッチなどの修正プログラムがメーカーから配布されています。

セキュリティホールを放置していると、たとえウイルス対策ソフトを入れて、最新版のウイルス検知用データに更新していたとしても、ウイルスに感染してしまったり、ウイルス付きの電子メールが他の人に自動的に送られてしまったり、悪意のあるホームページを見ただけでコンピュータシステムが破壊されてしまったりすることがあります。

セキュリティホールを修正するための修正プログラムは、メーカーのホームページなどで配布されることがあるので、自分が使っているソフトウェアの製品名やメーカー名を調べた上で、定期的に修正プログラムを適用するようにしましょう。

また、情報セキュリティ対策としては、企業や組織で許可されていないソフトウェアをコンピュータにインストールしないことも大切です。インターネットなどからダウンロードできるソフトウェアの中には、悪意のあるプログラムが含まれているものや、セキュリティホールが存在しているものがあります。業務の都合上、許可されていないソフトウェアをインストールする必要がある場合は、事前に情報システム部門などに相談してから行うようにしましょう。

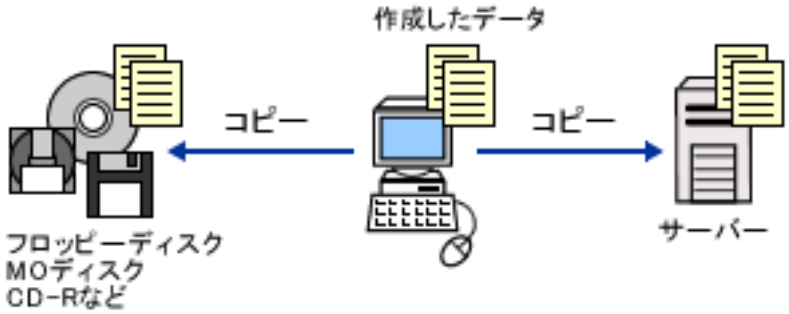
バックアップ

安全にコンピュータを利用するためには、定期的なバックアップが不可欠です。クライアントのコンピュータでは、ワープロソフトや表計算ソフトなどで作成したドキュメントファイルだけでなく、送信した電子メールや受信した電子メール、よく利用するホームページのＵＲＬアドレスなども、バックアップしておかなければなりません。

バックアップには、バックアップ用のファイルサーバーやインターネット上のオンラインストレージ、外付けのハードディスクにコピーする方法、ＣＤ-Ｒ やＤＶＤ メディアなどの外部の記憶媒体を利用する方法などがあります。まず、どのようなバックアップ方法を推奨しているかということを、情報管理担当者や情報システム部門などに確認するか、情報セキュリティポリシーや社内ルールで確認した上でバックアップ方法を決定してください。

バックアップするファイルの数が多いときには、手動でファイルをコピーするのはとても大変な作業になってしまいます。その場合には、ＯＳ に付属しているバックアップツールや市販のバックアップソフトの導入を検討してみるとよいかもしれません。

なお、外部の記憶媒体にバックアップされた情報は、たとえ個人のコンピュータ内の情報だからといって外に持ち出したり、机の上に放置したりすることは避けなければなりません。企業・組織にとって重要な情報が含まれる場合がありますので、鍵のかかる場所に保管するなど、適切な保管方法をとるべきです。



注意

最近は機密情報や個人情報の漏洩を防止するため、情報セキュリティポリシーで、個人による外部の記憶媒体の利用を禁止または制限している企業が増えてきています。バックアップ用に外部の記憶媒体を利用する場合には、事前に情報管理担当者や情報システム部門などに相談するか、情報セキュリティポリシーをよく確認してから行うようにしてください。

ソーシャルエンジニアリングの対策

重要!

ソーシャルエンジニアリングとは、ネットワークに侵入するために必要となるパスワードなどの情報を、コンピュータを使用せずに盗み出す方法です。ソーシャルとはsocial、つまり社会を表す言葉で、IT 技術を利用したハッキングではなく、実社会において情報を盗み出すことと考えるとわかりやすいかもしれません。

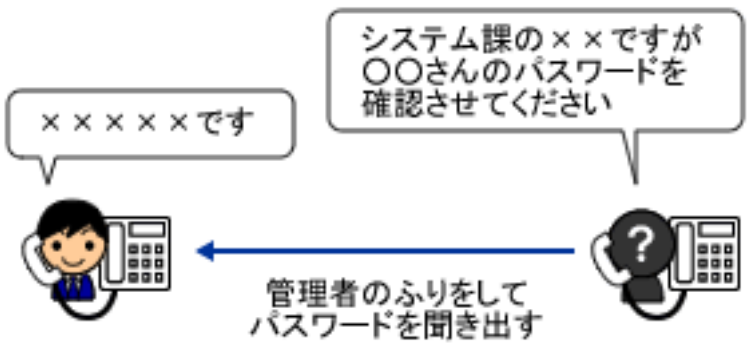
ソーシャルエンジニアリングにはさまざまなやり方がありますが、ここでは代表的な方法と対策を紹介します。

自分のユーザー情報が漏洩するということは、組織全体のセキュリティを脅かすということをきちんと認識して、ソーシャルエンジニアリングに対する適切な対策を心がけるようにしましょう。

■電話でパスワードを聞き出す

電話を利用したソーシャルエンジニアリングは、昔からある代表的な方法です。何らかの方法でユーザー名を入手したら、そのユーザーのふりをして、ネットワークの管理者に電話をかけ、パスワードを聞き出したり、パスワードの変更を依頼したりします。また、逆に管理者になりすまして、直接ユーザーに利用しているパスワードを確認するといったこともあります。これらの対策としては、あらかじめ電話ではパスワードなどの重要な情報を伝えないというルールを決めておくしかありません。

なお、この方法はキャッシュカードの暗証番号を調べるために使われることも多く、ほとんどの金融機関では「当行では電話でお客様の暗証番号をお聞きすることはありません」という案内を出しています。



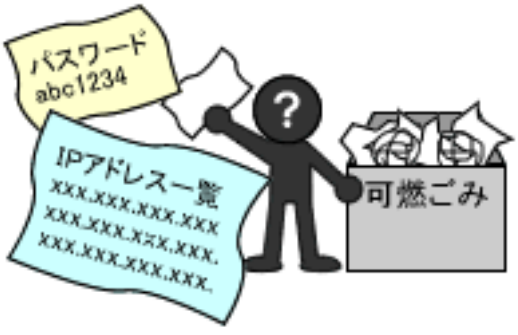
■肩越しにキー入力を見る（ショルダハッキング）

パスワードなどの重要な情報を入力しているところを後ろから近づいて、覗き見る方法です。肩越しに覗くことから、ショルダ（shoulder ＝肩）ハッキングと呼ばれています。たとえオフィス内であっても、パスワードやクレジットカードの番号など、キーボードで重要な情報を入力する際には、周りに注意しなければなりません。

■ごみ箱を漁る（トラッシング）

外部からネットワークに侵入する際に、初期の手順として行われることが多いのがトラッシングです。ハッキングの対象として狙ったネットワークに侵入するために、ごみ箱に捨てられた資料から、サーバーやルーターなどの設定情報、ネットワーク構成図、ＩＰ アドレスの一覧、ユーザー名やパスワードといった情報を探し出します。

面倒なようですが、やはり社内ネットワークや個人情報に関連する資料は必ずシュレッダーを使用して、裁断してから捨てるようにしなければなりません。



ごみ箱の紙くずから情報を探し出す

廃棄するコンピュータやメディアからの情報漏洩

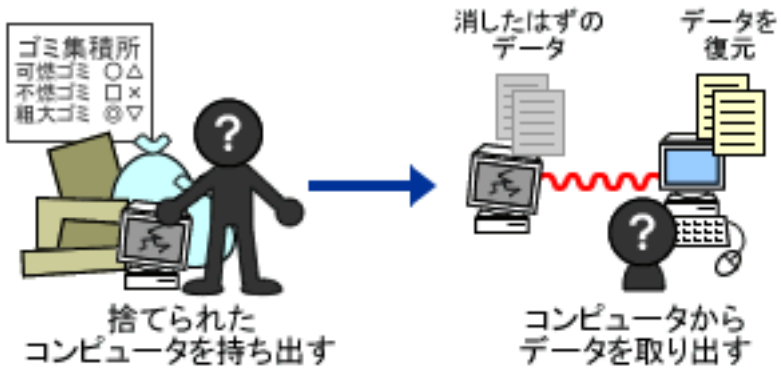
企業や組織の情報が漏洩するのは、ネットワーク経由とは限りません。コンピュータを廃棄したり、他人に譲渡したりする場合に、搭載されているハードディスクから情報が漏洩する可能性があります。中古のコンピュータに前の所有者が利用しているデータがそのまま残されていたというトラブルが発生しているだけでなく、企業で利用していた形跡のある中古のコンピュータを意図的に購入して、そこに保存されているデータを探し出すという方法で機密情報を入手するという手口も実際に使われているようです。

特に注意が必要なのは、格納されているデータを削除したり、ハードディスクをフォーマットしただけで、コンピュータを処分してしまう場合です。画面上でデータが消えているように見えても、実際にはハードディスク上にデータが残されたままになっていることがあり、特殊なソフトウェアを利用することで、削除されたはずのファイルを復元することが可能です。

不要になったコンピュータのハードディスクの処理方法には、以下のようなものがあります。

- データ消去用のソフトウェアを利用する。
- 専門業者のデータ消去サービスを利用する。
- コンピュータのハードディスクを取り出して、物理的に破壊してしまう。

これらの方法を企業・組織の情報資産の重要度に応じて組み合わせて、最適な方法を取るようにしましょう。また、当然のことですが、CD-ROM や CD-R、DVD メディアといった記憶媒体、外付けのハードディスク、USB メモリなどを廃棄する場合にも、同様の処理を心がけなければなりません。



持ち運び可能なノートパソコンを利用する上での危険性と対策

重要!

最近では、外出先でもインターネットが利用できるようなインフラが整ってきたこともあり、持ち運び可能なノートパソコンを利用するケースが増えてきています。しかし、外部に持ち出したノートパソコンに関する情報セキュリティ対策を怠っていたがために、情報の漏洩を起こしてしまった事例が多数報告されています。

外部にノートパソコンを持ち出した場合には、以下のような事例による情報漏洩の危険性が考えられます。

- 喫茶店等へ置き忘れることによるノートパソコンの紛失
- 電車の網棚等へ置き忘れることによるノートパソコンの紛失
- 車上荒らしによるノートパソコンの盗難
- 自宅や外出先にてノートパソコンをインターネットに接続することによるウイルス感染

ノートパソコンを外部に持ち出した際の情報漏洩に対するリスクを軽減するためには、次のような対策が考えられます。

- 盗難、紛失に備えて、持ち運ぶ必要のない機密情報、個人情報は格納しない。
- ハードディスクには、できるだけファイルを暗号化して保存する。
- 容易に推測されにくいログオンパスワードを設定して、他人には利用できないようにする。もしくは、指紋認証などの生体認証付きのノートパソコンを使用するのもよい。ただし、生体認証の情報セキュリティ対策機能は、緊急時の対策用にパスワードによるログオンも可能にしていることが多いため、やはり容易に推測されにくいパスワードを設定しておくことが不可欠であるという認識が大切である。
- 扱うデータの重要性によっては、OS だけでなく、BIOS やハードディスクにもパスワードを設定するなどの方法で、より強固な対策を検討する。

ただし、これらの対策はいずれも情報漏洩に対するリスクを軽減するだけのものであり、万全な対策にはなり得ません。やはり外部にノートパソコンを持ち出した場合には、情報セキュリティ上の危険性があるということを常に念頭に置いておくことが大切です。

■ＢＩＯＳのパスワードとハードディスクのパスワード

ＢＩＯＳとは、Ｂａｓｉｃ Ｉｎｐｕｔ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍの略で、コンピュータの電源を入れたときに最初に起動するプログラムです。また、ＢＩＯＳには、キーボードやマウス、ハードディスク等を制御するプログラムが含まれており、ＯＳがこれらの機器とやり取りするための基本的な機能を提供しています。

ＢＩＯＳパスワードとは、このＢＩＯＳに対して、設定できるパスワードのことで、コンピュータを起動したときにパスワードの入力を要求するものと、ＢＩＯＳの設定変更画面を利用するときにパスワードの入力を要求するものとがあります。コンピュータの起動時にパスワードの入力を要求する場合は、ＯＳのパスワードとは別にパスワードの入力が必要になるため、コンピュータに不正にログオンされる危険性を減らすことができます。また、ＯＳの再インストールなどの操作もできなくなることから、ＯＳのログオンパスワードだけを設定した場合に比べて、１段階上の強固な対策を施すことができるようになります。ただし、ＢＩＯＳのパスワードを忘れてしまった場合には、コンピュータの製造元に依頼しなければ解除できないという問題もあるため、注意が必要です。

ハードディスクのパスワードとは、コンピュータに内蔵されているハードディスクに設定できるパスワードのことです。ハードディスクのパスワードを設定してしまえば、コンピュータが分解されてハードディスクを他のコンピュータにつなげられてしまっても、ハードディスクに保存されているデータを読み取ることは困難になります。

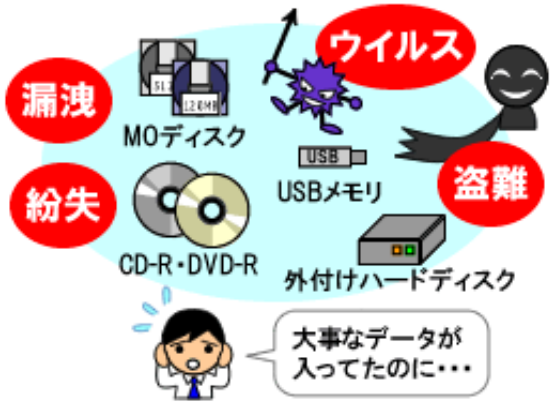
なお、ＢＩＯＳとハードディスクのパスワードについては、使用するコンピュータによって、装備されていなかったり、機能が異なったりすることがありますので、コンピュータの説明書やメーカーのホームページなどで確認してください。

持ち運び可能なメディアを利用する上での危険性と対策

重要!

最近、手の中に隠れるほど小さなサイズのUSBメモリの人気が高まっており、自宅や取引先とのデータのやり取りにUSBメモリを利用するケースが増えてきています。USBメモリは、コンピュータのUSB端子に接続するだけで手軽に利用でき、多くのユーザーに支持されています。

しかし、小さくて持ち運びが楽であるため、紛失してしまう危険性が高いという点に注意しなければなりません。また、データをそのままメディアに記録していた場合、紛失時にメディア内の情報が漏洩する危険性が非常に高くなります。もちろん、このことは外付けハードディスク、CD-R、DVD-R、MOディスクなど、持ち運び可能なメディア全般について言えることです。



これらの持ち運び可能なメディアを外部へ持ち出した際には、以下のような危険性が考えられます。

- メディアを入れたカバンを置き忘れることにより紛失して情報漏洩
- ワイシャツのポケットなどに気軽に入れておいたために紛失して情報漏洩
- USB媒介ウイルスによりウイルスに感染
- 自宅のパソコンにデータを移して作業。その後、ウイルスに感染して情報流出

可搬性のあるメディアを利用する際の情報漏洩に対するリスクを軽減するためには、次のような対策が考えられます。

●盗難、紛失に備えて、持ち運ぶ必要のない機密情報、個人情報は格納しない。
●ファイルは、できるだけ暗号化して保存する。
●USB メモリや外付けハードディスクでは、製品に情報セキュリティ対策機能の仕組みやソフトウェアが装備されているものも多いので、外部に持ち出すために利用する場合にはできるだけそのような製品の購入を検討する。
●USB メモリでは、指紋認証などの生体認証付きの機器を使用するのもよい。ただし、生体認証の情報セキュリティ対策機能は、緊急時の対策用にパスワードによるログオンも可能にしていることが多いため、容易に推測されにくいパスワードを設定しておくことが不可欠である。
●コンピュータの設定を変更して、USB メモリの自動再生機能を停止する。
●USB メモリを差し込んだときには、ファイルを開く前に必ずウイルスチェックを行う。
●家庭で利用している自分のUSB メモリや持ち主の分からないUSB メモリを使用しない。

ただし、これらの対策はいずれも情報漏洩に対するリスクを軽減するだけのものであり、万全な対策にはなり得ません。やはり外部にメディアを持ち出した場合には、情報セキュリティ上の危険性があるということを念頭に置いておくことが大切です。

注意

最近は機密情報や個人情報の漏洩を防止するため、情報セキュリティポリシーで、個人による外部の記憶媒体の利用を禁止または制限している企業が増えてきています。外部の記憶媒体を利用する場合には、事前に情報管理担当者や情報システム部門などに相談するか、情報セキュリティポリシーをよく確認してから行うようにしてください。

ボットの危険性と対策

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、ボットに感染したコンピュータはボットネットワークの一部に組み込まれてしまいます。悪意のあるハッカーは、ボットネットワーク上のコンピュータをインターネットから遠隔操作することで、持ち主の知らないうちに「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個人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、迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点が手口の巧妙化の要因のひとつとなっています。そのため、旧来のウイルスと比べると、感染しているということに気付きにくくしているというのも特徴のひとつです。なお、ボット対策プロジェクト「Cyber Clean Center（サイバークリーンセンター）」が2008年6月に国内のボット感染者数を調査したところ、ブロードバンドユーザー約3000万人のうち約30万人（感染率約1％）と推計されています。

ボットに感染したコンピュータは大量に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、被害を受け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が加害者に見えます。あなたやあなたの所属する企業・組織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と言えます。

ボットへの対策としては、以下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

なお、これらの対策の具体的な実施方法について不明な点があれば、情報管理担当者や情報システム部門などに確認してください。