



総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策-実践編:社員・職員全般

社員・職員全般のための情報セキュリティ対策-実践編

企業や組織内のコンピュータには、業務で利用するためのさまざまな情報資産が格納されています。ここでは、それらの情報資産をさまざまな障害から防御するために、社員や職員が実践すべき情報セキュリティ対策について説明します。

なお、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。

ウイルス対策の実践	2
ソフトウェアの更新	5
💡 パスワードの検討	6
定期的なバックアップの実行	8
コンピュータやメディアの廃棄	10

※特に重要な項目には 💡 マークがついています。



総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策-実践編:社員・職員全般

ウイルス対策の実践

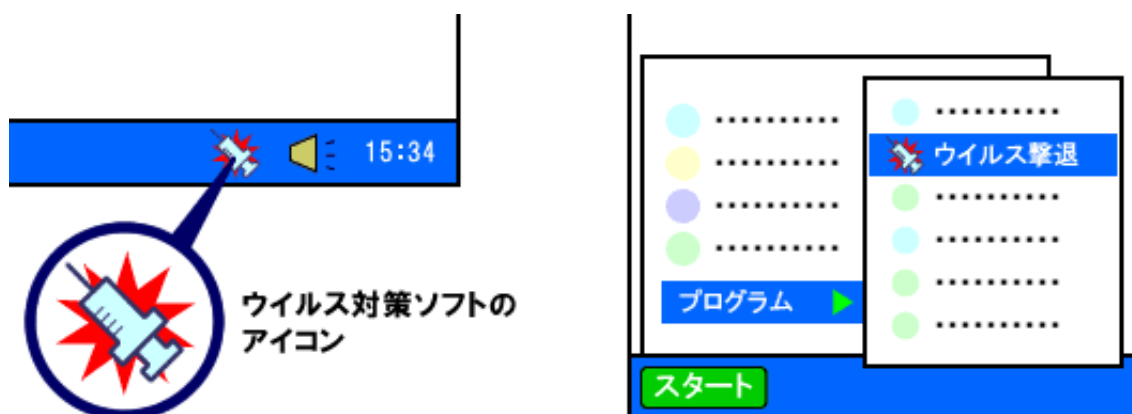
ウイルスに感染しないようにすることは、コンピュータにおける情報セキュリティとしてもっとも大切な対策のひとつです。最近のウイルスは、電子メールを見ただけで感染したり、ホームページを見ただけで感染したりするウイルスばかりではなく、勝手にインターネットやネットワークを通じて感染するワーム型というタイプのウイルスも出現してきています。

また、企業や組織のネットワークにコンピュータが接続されている場合には、自分の使用しているコンピュータに対するウイルス対策を怠るだけで、ネットワーク全体にウイルスを蔓延させてしまうこともあります。企業や組織内の情報資産やコンピュータをウイルスから防御するためには、すべてのコンピュータにウイルス対策ソフトを導入しなければなりません。

■ウイルス対策ソフトの確認

ウイルス対策ソフトがコンピュータにインストールされている場合には、通常、コンピュータのタスクバーと呼ばれる領域にウイルス対策ソフトが動作していることを示すアイコンが表示されます。または、コンピュータのプログラムの一覧で、ウイルス対策ソフトが含まれているかどうかを確認するという方法もあります。

自分の使用しているコンピュータにウイルス対策ソフトがインストールされていない場合には、情報管理担当者に確認してみましょう。





■ウイルス検知用データの更新

ウイルス対策ソフトが新しいウイルスに対応するためには、常にウイルス検知用データを最新のものに更新しておかなければなりません。コンピュータにウイルス対策ソフトがインストールされていても、ウイルス検知用データが古いままでは、新しいウイルスに感染してしまう危険性があります。一般的なウイルス対策ソフトでは、購入してから約1年ごとに、ウイルス検知用データをダウンロードするための契約を更新する場合があります。

自分のコンピュータのウイルス対策ソフトがどのような契約内容になっているかということを確認し、契約が切れてしまっている場合には、新たに契約を延長するか、新規にウイルス対策ソフトを購入しなければなりません。ウイルス検知用データの更新方法や契約方法については、情報管理担当者に確認してください。

ヒント

ウイルス検知用データは、ウイルス対策ソフトによって、パターンファイル、ウイルス定義ファイルなどの名前と呼ばれています。

■定期的なウイルススキャンの実行

ウイルス対策を万全にするためには、ウイルス対策ソフトを導入して、ウイルス検知用データを更新するだけでなく、定期的なウイルススキャンを実行することが大切です。ほとんどのウイルス対策ソフトでは、指定したスケジュール（毎週金曜日の夜8時など）で、システム全体に対するウイルススキャンを実行することができるようになっています（ただし、その時刻にコンピュータの電源が入っていない場合には実行されません）。お昼休みや定例の会議の時間など、自分の予定に合わせて、スケジュールを設定しておくといでしょう。

■ウイルス対策サービスの利用

企業や組織によっては、プロバイダが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していることがあります。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、プロバイダがウイルス検知用データを自動的に更新します。詳細は、情報システム部門や情報管理担当者に確認してください。



総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策－実践編：社員・職員全般

■ USB 媒介ウイルスへの対策

USB 媒介ウイルスは、USB メモリの自動実行機能を利用して、コンピュータにUSB メモリを差し込んだだけで感染するウイルスです。USB 媒介ウイルスへの対策として、許可されていないUSB メモリや持ち主の分からないUSB メモリを使用しないようにしてください。また、USB メモリを差し込んだときには、フォルダやファイルを開く前に必ずウイルスチェックを行うようにするとよいでしょう。可能であれば、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しておく、さらに安心して利用できるようになります。

注意

所属する企業や組織の情報セキュリティポリシーで、個人のコンピュータのネットワークへの接続が禁止されていない場合であっても、ウイルス対策ソフトが導入されていないコンピュータは絶対に社内や組織内のネットワークに接続してはいけません。たった1台だけであったウイルスに感染したコンピュータを接続してしまうと、ネットワークに接続している他のコンピュータやサーバーにウイルスを感染させてしまうことがあります。

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。

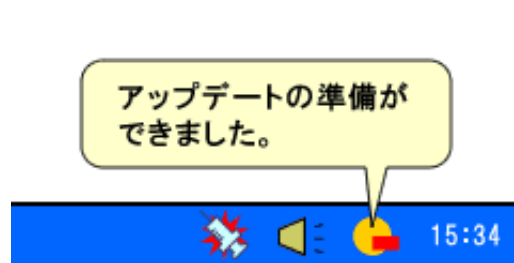
ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード / インストールしたりしないようにしてください。



ソフトウェアの更新

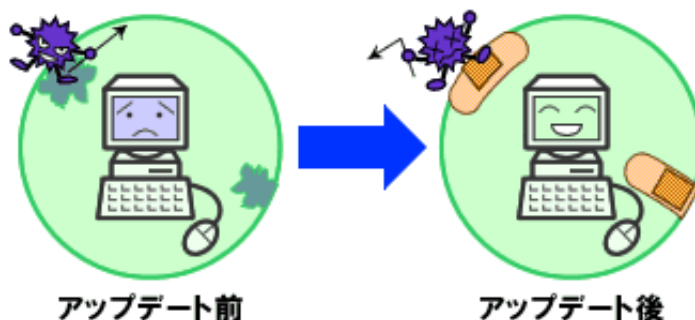
近年では、OS、Web ブラウザや電子メールソフト、Office アプリケーションなど、あらゆるタイプのソフトウェアにセキュリティホールが見つかっています。これらのセキュリティホールを修正したり、情報セキュリティ上の問題を解決したり、さまざまな不具合を解消したりするために、メーカーから修正プログラムが提供されることがあります。インターネットに接続された環境でコンピュータを利用する場合には、これらの修正プログラムを定期的に適用して、できる限りすべてのソフトウェアを最新の状態に保つように心がけなければなりません。

最近では、パッケージソフトなどの利用者の多いソフトウェアを始めとして、修正プログラムの有無を定期的に確認したり、自動的に適用したりするための自動アップデート機能が導入されることが増えてきました。このような自動アップデート機能を利用すると、修正プログラムの適用を忘れてしまうことがなくなります。自動アップデート機能を利用できる場合には、「アップデートの準備ができました」などのメッセージが表示されるため、そのメッセージをクリックして、画面上の指示に従って操作してください。



ソフトウェアのアップデートを知らせるアイコンとメッセージ

自動アップデート機能が用意されていないソフトウェアについても、情報セキュリティ上の問題などで、修正プログラムが提供されることがあります。これらについても、コンピュータにインストールされているソフトウェアを確認して、それぞれのメーカーのホームページなどで定期的にチェックしてみてください。また、最近では、ソフトウェアのメーカーに登録をしておくと、プログラムが更新された場合に、電子メールで連絡が来る場合があります。そのため、普段使用しているソフトウェアについては、できるだけユーザー登録をしておいた方がよいでしょう。





総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策-実践編:社員・職員全般

パスワードの検討



重要!

自分のコンピュータにログオンしたり、企業や組織のネットワークに接続したり、業務データが格納されているデータベースシステムにログオンしたりする際において、なりすましを防ぐための情報セキュリティ対策には、一般的にパスワードが利用されています。そのため、企業や組織でコンピュータを利用するユーザーにとって、いかに適切にパスワードを管理するかということが、とても重要なことと言えます。

適切なパスワード管理には、次の3つの要素があります。

- 安全なパスワードを作成すること
- 適切な方法でパスワードを保管すること
- 定期的にパスワードを変更すること

安全なパスワード





総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策-実践編:社員・職員全般

安全なパスワードは、以下のような条件を満たしていなければなりません。

● 個人情報からは推測できないこと

- ✕ 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)

● 英単語やよくある名称などをそのまま使用しないこと

- ✕ password、baseball、soccer、monkey、dragon

● 適切な長さの文字列であること

- ✕ gf、ps

● 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

- ✕ 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)

このような条件を満たすパスワードを作ることが困難な場合には、インターネットでダウンロードできるパスワード生成ソフトを利用するという方法も検討してください。パスワード生成ソフトは、指定した条件からランダムなパスワードを作り出してくれる機能を持つソフトウェアです。

ヒント

現在の一般的なOSのスクリーンセーバーでは、元の操作画面に復帰する際にパスワードの入力を促す設定を行うことができます。このように設定することで、離席中に不正なユーザーがそのコンピュータを操作することを防ぐことができるようになります。ただし、スクリーンセーバーが起動するには一定の時間が必要です。

さらに情報セキュリティを強化するためには、離席する際にログオフを行ない、パスワードを入力してログオンしなければコンピュータを操作できないようにするなど、ユーザーが自発的にロックする方法が有効です。





定期的なバックアップの実行

業務で作成した情報は、たとえ自分で使用しているコンピュータが壊れてしまったとしても、いつでも他のコンピュータで利用できるようにバックアップしておかなければなりません。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。クライアントのバックアップに利用できる代表的な記憶媒体（メディア）には、以下のものがあります。

CD-R

1 枚のメディアに、640MB 以上のファイルを格納することができます。ただし、一度書き込むと、後からファイルを追加することはできませんが、書き換えることができません（CD-RW というメディアでは、繰り返し書き換えて利用することが可能です）。書き込んだ CD-R メディアは、大部分の CD-ROM ドライブで読み出すことができるため、ほとんどの場合、他のコンピュータへの復元がもっとも簡単です。



DVD-R、DVD+R

一度だけ書き込むことができる DVD メディアです。現在普及している規格では、片面で 4.7GB のファイルを格納することができます。DVD-R や DVD+R は追記型のメディアであるため、一度書き込んだデータを消去することはできませんが、DVD-RAM、DVD-RW、DVD+RW といった書き換え可能な DVD メディアも登場しています。



外付けのハードディスク

外付けのハードディスクをバックアップ用のデバイスとして使用する方法もあります。他のメディアに比べて高速であるということと、必要に応じた容量のハードディスクを選択できるというメリットがあります。



オンラインストレージ

オンラインストレージは、インターネット上で利用できるファイル保管サービスです。Web ブラウザや専用のソフトウェアを利用して、インターネット上の領域とクライアントのディスクとの間でデータをやり取りすることができます。複数のユーザーでファイルを共有化できるサービスもあります。





総務省

国民のための情報セキュリティサイト



「企業・組織」の情報セキュリティ対策-実践編:社員・職員全般

バックアップを実行する上でもっとも大切なことは、「どのファイルをバックアップするか」ということと、「いつバックアップするか」ということです。

保有している情報を漏れなくバックアップするためには、常にドキュメントをハードディスク上にわかりやすく保存しておくことが大切です。また、電子メールの送受信データやよく利用するホームページのURL アドレスなども、忘れずにバックアップしなければなりません。

バックアップを実行するタイミングは、保有する情報の重要性や更新の頻度などにもよりますが、少なくとも1週間に1回程度は実行するように、自分なりのルールを決め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。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。



コンピュータやメディアの廃棄

最近、廃棄されたコンピュータやメディアから情報が漏洩するという事件が発生しています。そのため、コンピュータやメディアを廃棄する場合には、記憶されているデータを復元不可能な方法で抹消しなければなりません。コンピュータやメディアを廃棄する際に、以下の方法を検討してください。

- データ消去用のソフトウェアを利用する。

データ消去用のソフトウェアを使用すると、ハードディスクやメディアのファイルを復元できないように完全に消去することができます。なお、データ消去用のソフトウェアは、パソコンショップや家電販売店などで販売されています。



- 専門業者のデータ消去サービスを利用する。

サービスを提供している業者は、インターネットの検索エンジンで探すことができます。「データ消去サービス」などのキーワードで検索してください。



- ハードディスクやメディアを物理的に破壊する。

ただし、ハードディスクの場合には、外側のケースだけを破壊しても、中にあるディスクが破損していない場合には、ディスクを取り出してデータを復元することも可能なので注意してください。



専門業者に依頼する場合には、できる限り、依頼先の会社の信頼度やその会社におけるプライバシーポリシーのあり方にも考慮して選定しなければなりません。

また、コンピュータを修理する場合にも、作成したドキュメントや電子メールなどのデータを破棄してから依頼するようにしましょう。

なお、情報セキュリティポリシーに廃棄の規定が定められている場合は、あらかじめ情報セキュリティポリシーを確認しておきます。また、組織内に情報管理担当者がいる場合には、コンピュータを廃棄する前に、不明な点や廃棄方法を相談するようにしてください。