パソコン利用時のリスク管理

# はじめに

このマニュアルでは、パスワードの管理やパソコンの盗難対策、データのバックアップなどパソコン利用時のリスク管理について解説します。

# 第1章　情報を守る

パスワードを設定することで、パソコンに保存された情報を守ることができます。しかし、安易なパスワードでは、他人に見破られてしまう場合があります。

パスワードを管理する場合には、次のような点に注意します。

## （1）パスワードの設定

1. 身近な情報をパスワードに使わない  
   名前や生年月日、電話番号など、本人の個人情報から簡単に推測できるものや、辞書に載っている単語などは使わないようにします。
2. 一度でも使ったことのあるパスワードは使わない  
   過去に使ったことのあるパスワードは使わないようにします。
3. パスワードを同じにしない  
   パスワードは様々な場面で使用します。パソコンを利用するときやLANを利用するとき、インターネットを利用するときなど、それぞれ異なるパスワードを設定します。
4. 複数の文字の種類を組み合わせる  
   英字の大文字や小文字、数字、記号などを組み合わせて複雑なものにします。
5. 適切な長さの文字数で付ける  
   短いパスワードは見破られる可能性が高いので、8文字以上のパスワードを設定します。文字列が長いほど安全性が高くなります。

## （2）パスワードの管理

1. 初期値のパスワードを変更する  
   初期値のパスワードはシステム管理者から与えられます。初期値のパスワードでシステムにアクセスしたあとは、必ずパスワードを変更します。
2. 定期的にパスワードを変更する  
   パスワードを見破られる可能性もあるので、定期的にパスワードを変更するようにします。
3. パスワードを入力しているところを他人に見られないようにする  
   パスワードを入力しているところを見られただけでさとられる場合もあるので、入力時は注意します。
4. 手帳などに記入しない  
   パスワードは手帳など誰かに見られる可能性があるものには記入しないようにします。
5. 他人に漏らさない  
   パスワードは他人に教えないようにします。また、パスワードを尋ねるような不審な問い合わせには応じないようにします。

# 第2章　盗難からの保護

しっかりとした盗難対策をしておかないと、簡単にパソコン自体が盗まれる場合があります。重要な情報が保存されているパソコンが盗難されると、業務に支障が出るばかりでなく、機密情報が漏えいしてしまう可能性があり、企業の信用問題に発展しかねません。また、機密情報をもとに恐喝されたり、機密情報を売買されたりする可能性もあります。

これらの対策として、次のようなことがあげられます。

## （1）侵入者対策

運送業者や清掃業者などを装って、事務所内に不正に侵入する場合があります。また、従業員の多い事務所では、社員か外部の人間かの区別がつきにくい場合があります。このような偽装者による不正侵入対策として、次のことを実施します。

* 社員証(IDカード)を着用する
* 訪問者は受付で訪問記録を残してもらう
* 訪問者はゲスト用のIDカードを着用してもらう

## （2）盗難防止

パソコン本体にも盗難対策をします。重要なCPUやハードディスクを守るために本体カバーが開閉しないように施錠したり、セキュリティワイヤーで机などに固定したりして盗難を防止します。また、普段使用しないパソコンは、鍵のかかるロッカーなどに保管し、重要なデータが保存されているパソコンは、鍵のかかる部屋や監視カメラの設置してある部屋に置くようにします。

# 第3章　落雷や停電からの保護

落雷や停電によって、パソコンが破壊されたり、重要なデータが壊れて使用できなくなったりする可能性があります。

これらの対策として、次のようなことがあげられます。

## （1）施設・設備の管理

1. サージプロテクト機能のあるOAタップの使用  
   近くに落雷があった場合、コンセントに接続しているパソコンなどの電気製品は雷サージといわれる異常電流を受け、壊れてしまう場合があります。サージプロテクト機能のあるOAタップを使用することで、落雷による雷サージを防ぐことができます。
2. 無停電電源装置の使用  
   無停電電源装置は電力を蓄えておくバッテリーのようなものです。停電が発生すると電源を蓄電池に切り替えて、電力を供給します。電力の供給可能な時間は無停電電源装置の性能により様々ですが、速やかに作業中のデータを保存したり、システムを停止したりする必要があります。

## （2）データのバックアップ

機器の故障、ウイルスやクラッカーによる攻撃、人災や天災によるデータの消失は、多大な損害につながります。この危険性を最低限に抑えるためにデータのバックアップを取っておきます。バックアップがあれば、データを復旧することができます。

1. バックアップの対象データ  
   パソコンには様々な種類のデータが格納されています。すべてのデータをバックアップするには、多大な時間と全データを保存できる記憶媒体が必要になります。OSやアプリケーションソフトなどは、再度インストールすれば初期の状態に戻せます。バックアップの対象にするファイルは、ユーザーが作成したファイルや動作環境を設定したファイルなどにします。
2. バックアップの記憶媒体  
   パソコン本体やハードディスク自体が壊れてしまうと、ハードディスクに保存してあるデータを開くことができなくなります。データのバックアップをとる場合は、ハードディスク障害にも対応できるように、ハードディスク以外の別の記憶媒体にバックアップします。記憶媒体は、データの容量にあわせて選択するとよいでしょう。
3. バックアップの注意点  
   バックアップは定期的に行い、日常業務に支障がない時間にスケジューリングします。
4. バックアップデータの保管先  
   バックアップした記憶媒体は、内容の消失や記憶媒体の紛失を回避するために大切に保管します。保管先は磁気の影響のない場所などを選択します。