

経営者のための学校情報

太陽 ASG 拝啓理事長先生

第 214 号 この資料は全部お読みいただいて 3 分 00 秒です。

今回のテーマ： IT の管理と情報セキュリティ

学校の教育活動や事務業務で PC が活用され、学内ネットワークを構築するなど、近年は IT が欠かせないものとなっています。たくさんの情報を処理できるので大変便利ですが、その反面で情報流出の危険性が常につきまといまいます。IT の管理は情報セキュリティの確保でもあります。

以下に主な IT の利用に関するチェックポイントを掲載しています。IT の管理体制を確認してください。

チェックポイント

■IT の管理責任者はいますか？

管理担当者と管理責任者を配置し、学内の IT の構築状況と利用状況を定期的に点検しましょう。

管理責任者は IT の利用上のルールを策定し、教職員にルールを遵守させるとともに、情報セキュリティの重要性を認識させましょう。

■ID とパスワードを設定し、管理していますか？

PC・ソフトウェア・学内ネットワーク等、各種の利用に ID とパスワードを要求することで、アクセス権を与えられた者だけが利用できるようにします。ID 保有者は誰か、退職者の ID が有効なままになっていないかという点に気をつけましょう。ID とパスワードを複数名で共有しないようにするとともに、パスワードを定期的に変更しましょう。

■ウイルス対策ソフトやデータの暗号化ソフト等のセキュリティソフトを利用していますか？

セキュリティソフトの利用により、ウイルスの侵入や PC への不正アクセスを防ぎます。製品によっては情報が流出しても容易に読み取れないようにできるものもあります。セキュリティソフトは日々進化していますので、プログラムの更新やバージョンアップをこまめに行いましょう。

■PC を業務外の目的で使用していませんか？

安易なフリーソフトのダウンロードやインターネットの私的利用により、外部からの不正アクセスやウイルス侵入の危険性が高まります。業務目的にのみ使用するようにしましょう。

■私有の PC を学内で使用していませんか？

一般的に、私有 PC には高度なセキュリティ対策が取られていないと考えられます。その状態で学内システムに接続すればウイルス侵入の可能性があります。また情報を PC に保存して外部に持ち出すこともできます。私有 PC の学内における使用を制限しましょう。

■情報が入った PC や USB 等を学外に持ち出してはいませんか？

PC や USB を外部に持ち出すことで、紛失や盗難による情報流出の危険性が高まります。

学外への持ち出しに承認制度を採用し、外部持ち出しを制限しましょう。

■システムやデータのバックアップを取っていますか？

バックアップがあれば、データの紛失やシステム故障が起きても、それらを復旧することができます。バックアップデータが入った機器は施錠可能な場所で厳重に保管しましょう。

また、サーバールームがある建物とは別の建物に保管することが災害対策に有効です。

お見逃しなく！

IT のクラウド化という、インターネット上にネットワークやサーバーを仮想化することが話題となっています。物理的な設備を必要としないため、自然災害にあまり影響されないと言われていますが、インターネットを利用するのでセキュリティ面で注意が必要です。

導入する場合には、いかにしてセキュリティを確保するかを十分検討してください。