2-1 情報セキュリティとは

情報セキュリティとは、パソコンやサーバ、CDやDVDのようなメディアなどに記録された、さまざまな情報資産の安全性を保持することです。国際標準化機構（ISO）と国際電気標準会議（IEC）は、大学や企業などの組織におけるISMS（情報セキュリティマネジメントシステム）の仕様を定めた規格として、ISO/IEC 27002 を策定しました。組織にとってのリスクの分析と対応、情報資産の管理、アクセス制御などの項目があります。

情報は組織にとって、非常に重要な資産です。ISO/IEC 27002のようなISMSを参考に、組織として情報セキュリティへの取り組みを検討する必要があります。

1. 情報セキュリティの定義

情報セキュリティはISO/IEC 27002で「情報の機密性、完全性、可用性を確保すること」と定義されています。機密性、完全性、可用性とは次のような意味です。

- **機密性（Confidentiality）**
  アクセスを許可されている者だけが、その情報にアクセスできる状態
- **完全性（Integrity）**
  情報を破壊、改ざん、消去されない状態
- **可用性（Availability）**
  アクセスを許可されている者が、必要に応じて情報にアクセスできる状態

上の3つの頭文字をとって、「情報セキュリティのCIA」といいます。CIAは情報セキュリティの基本3要素です。

また、CIAのほかに次の要素を加えることもあります。

- **真正性（Authenticity）**
  なりすましや虚偽の情報でないことが保証される状態
- **責任追跡性（Accountability）**
  アクセスログなどから、ユーザやシステムの振る舞い、責任が説明できる状態
- **信頼性（Reliability）**
  システムが矛盾なく正常に動作する状態
- **否認防止（Non-Repudiation）**
  事後になってから事実を否定することができないように証拠が残された状態

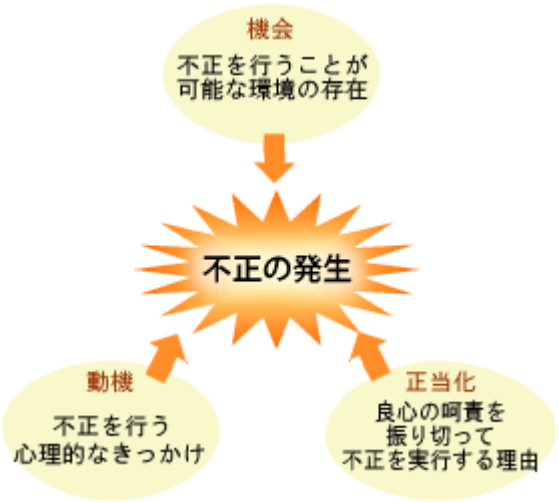
これら4つの要素を含めて「情報セキュリティの3要素・7要素」といいます。

2. 不正のメカニズム

不正の発生要因は、「機会、動機、正当化」の3つです。これは、米国の組織犯罪研究者D.R.クレッシーによって提唱された「不正のトライアングル」という理論です。

- **機会（Opportunity）**
  不正を行うことが可能な環境の存在
- **動機（Pressure/Incentive）**
  不正を行う心理的なきっかけ
- **正当化（Justification）**
  良心の呵責を振り切って不正を実行する理由

情報セキュリティを保持するため、組織としてこれらの3要素が発生しないような環境を作ることが重要です。



2-2 セキュリティポリシー

「ユーザ アカウント が書かれた用紙の紛失」「大学の サーバ に対する 不正アクセス 」「 ウィルス 感染」など、情報資産を利用する学校ではさまざまなトラブルが発生します。対処を誤ると、被害が全学に拡散したり、信用を失うような問題に発展する場合があります。よって、このような事態に対処する危機管理体制のガイドラインが必要です。

1. 情報セキュリティのガイドライン

組織の セキュリティ に関するガイドラインは次の3つで構成されます。

- セキュリティポリシー（情報セキュリティに関する方針、対策、手順などをまとめたもので、最も根幹をなす指針、モラルなど）
- セキュリティ運用管理基準（部署やシステムごとにセキュリティを実現するための具体的方法）
- セキュリティ手順（それぞれの部署や業務にかかわる人ごとに適用されるマニュアル）

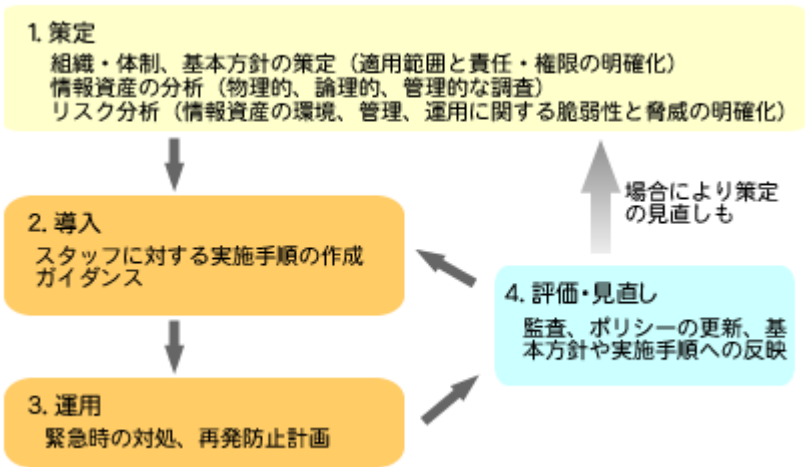
セキュリティポリシーはそのなかで最上位の方針となります。

セキュリティポリシーに従って管理・運営を行うには、まず、学校における情報資産とそのリスクを分析し、ガイドラインを明確化しておく必要があります。

セキュリティポリシーの策定については、イギリスのセキュリティマネジメント規格（A Code of Practice for Information Security Management）「BS7799」をもとにすることが多くなっています。日本ではこの規格を参考にして作られた「ISMS適合性評価制度」があります。

セキュリティポリシーは、状況に応じた見直しが必要になります。具体的に出てきた問題や、新たに考えられるリスクを分析し、定期的な見直しを行うことも業務の一部に入れておきましょう。

また、効果的な運用を行うため、教職員に対する教育も重要です。危機意識は個人差があり、一部の無責任な行動からシステム全体を揺るがす事件に発展することも十分考えられます。したがって、スタッフで研修会を開いて、部署ごとに ウィルス対策ソフト を導入しているか、業務に無関係なソフトが インストール されていないかなど、日頃からチェックを行う体制を作りましょう。

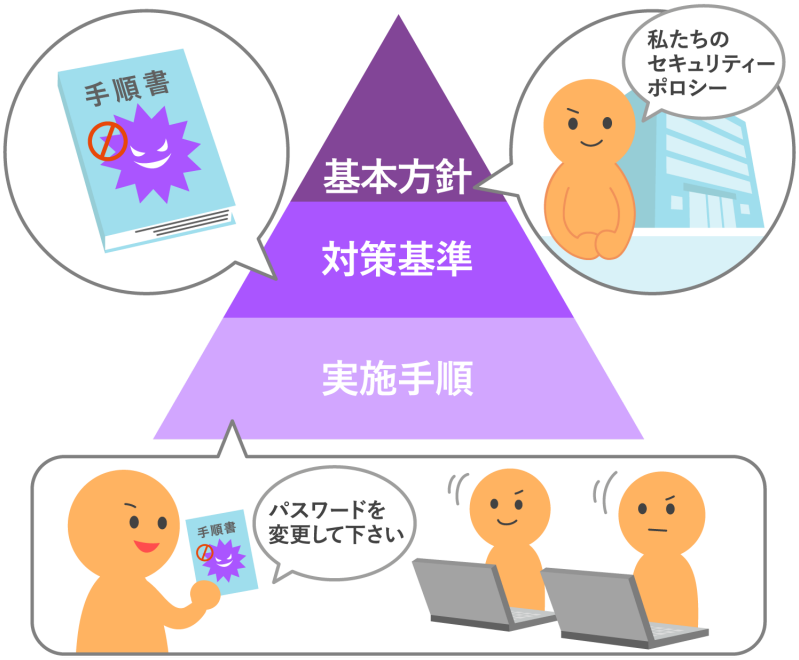


2. 情報セキュリティポリシーの内容

情報セキュリティに関する方針と対策、手順などをまとめたものをセキュリティポリシー（Security Policy）といいます。学校で扱われる個人情報の管理、さまざまなリスクに対する管理などについて、根幹となる指針を文書化したものということができます。

情報セキュリティポリシーは、一般に「基本方針」「対策基準」「実施手順」で構成されます。

- **基本方針**：情報セキュリティの基本的な方針に関して、代表者による宣言が記述されます。「情報セキュリティの必要性」「個人情報の扱いについての方針」など、セキュリティの根幹にかかわる部分が含まれます。
- **対策基準**：情報セキュリティ対策の指針が記述されます。どのような対策を行うのかという規定を記述します。
- **実施手順**：情報セキュリティ対策に関して、各対策基準について詳細で具体的な手順が記載されます。



3. テレワークに関するセキュリティポリシーの見直し

2020年、新型コロナウィルス感染拡大防止のため、テレワークを導入する大学が多く見られます。通常、学内で行っていた業務を自宅に行うことになるため、セキュリティポリシーを見直しておく必要があります。

セキュリティ対策の実施について、具体的な手順をスタッフに対して示しましょう。以下は、テレワークを行う場合の基本的な注意事項です。

- **デバイスやメディアの持ち出し**
  ノートPC、タブレットなどのデバイスを持ち出す場合、紛失・盗難に注意する。

USBメモリ、CD・DVDなどの小型メディアで情報を持ち出す必要がある場合も、紛失・盗難に注意する。また、メディアのファイルを暗号化する。

- **添付ファイルの誤送信**
  電子メールで添付ファイルを送信する場合、誤って個人情報などのファイルを送信しないように注意する。
- **無線LANの盗聴**
  テレワークを自宅で行う場合、必ず無線LANルータを暗号化し、盗聴を防止する。
  喫茶店などで暗号化されていない無線LANに接続しない。
- **出先での作業**
  出先から学内のサーバにアクセスする場合は、不特定多数が利用するパソコンで、パスワードなどの機密情報を入力しないようにする。
- **マルウェア対策**
  業務に使用するデバイスには、必ずウィルス対策ソフトをインストールし、最新状態にする。また、OSやアプリケーションのアップデートを行う。

4. 教育情報セキュリティポリシーに関するガイドライン

2017年に文部科学省が、「教育情報セキュリティポリシーに関するガイドライン」を策定し公表しました。教育機関における情報セキュリティポリシーの策定や見直しついて、その考え方や内容を示しました。概要を以下に示します。

1. 組織体制を確立すること
2. 児童生徒による重要性の高い情報へのアクセスリスクへの対応を行うこと
3. 標的型および不特定多数を対象とした攻撃等のリスクへの対応を行うこと
4. 教育現場の実態を踏まえた情報セキュリティ対策を確立させること
5. 教職員の情報セキュリティに関する意識の醸成を図ること
6. 教職員の業務負担軽減及びICTを活用した多様な学習の実現を図ること

近年、GIGAスクール構想で１人１台端末を所持するようになり、ICTの環境整備が急ピッチで進んでいます。このような状況下で、2021年にガイドラインの改定が行われました。
主な改正点は以下です。

- 1人1台端末におけるセキュリティ（学習用端末のID管理）
- クラウドサービス利用におけるセキュリティ
- 事業者に対して行うべきプライバシー保護

今後も情報セキュリティがより重要性が増してきますので、ガイドラインを参考にセキュリティポリシーを策定し、随時見直しを繰り返しましょう。