単元 9

セキュリティ

情報セキュリティの概要

学習内容

情報セキュリティ、機密性、完全性、可用性、脅威、脆弱性、リスク
人的脅威、技術的脅威、物理的脅威、情報セキュリティマネジメント、ISMS

情報セキュリティとは？

情報セキュリティは、情報をさまざまな**脅威**から保護することである。また、**日本工業規格**（JIS）では、次の七つの特性を維持するように定めている。

特　性	概　要
機密性	利用が認められた者だけが情報にアクセスできること
完全性	情報が改ざんされていないこと
可用性	決められた時間帯に情報にアクセスできること
真正性	利用者や情報が本物であると証明できること
責任追跡性	誰が情報にアクセスしたか、過去にさかのぼって確認できること
否認防止	利用者による情報へのアクセスを後で否認できないようにすること
信頼性	情報システムの動作結果が期待したものと常に同じであること

- **脅威**　顧客情報・営業情報・技術情報などの**情報資産**に損失を発生させる原因。
- **脆弱性**　情報の**漏えい**・**紛失**・**改ざん**などが発生・拡大する要因となる弱点や欠陥。
- **リスク**　脅威と脆弱性によって情報資産に発生する損失。

情報資産 × 脅威 × 脆弱性 ＝ リスク


重要データ


マルウェア


マルウェア対策ソフトの未導入


マルウェア感染

リスクマネジメントとは？

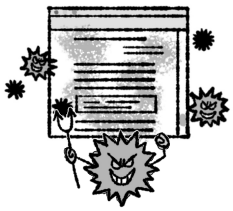
リスクマネジメントは、将来、起こるかもしれないリスクに対して、あらかじめ対応を決めて管理することである。これは、次の手順で進める。

①リスクアセスメント（リスク特定 → リスク分析 → リスク評価）

情報資産について、どのようなリスクが存在するのか、調査して洗い出し、その発生頻度や発生時の影響の大きさ（被害や損失の大きさ）を評価する。

リスク特定

マルウェア対策ソフトがインストールされていないPCが複数台存在している。
もしPCがマルウェアに感染したら、顧客情報が漏えいしてしまうかもしれない。



リスク分析

顧客情報の漏えいは、わずかなものであっても、企業にとって大きなダメージになる。
刑事／民事上の責任を負う可能性もある。

リスク評価

このリスクに、早急に対応する必要がある。
マルウェア対策ソフトは価格が安く、PCに簡単にインストールできる。

②リスク対応

リスクの対応の優先順位を決めて、損失と対応費用の関係から、リスクへの対応策を決定・実施する。その後、①に戻る。

- リスク回避　脅威発生の要因を停止あるいは全く別の方法に変更すること。
- リスク共有
  - リスク移転　アウトソーシングなどで、リスクを他社に移すこと。
  - リスク分散　損害保険をかけるなどで、リスクを他社に分散すること。
- リスク保有　リスクを許容範囲内として受容すること。

脅威の分類

①人的脅威　人の行為が原因となる脅威。過去の情報セキュリティ事故・事件において、人の行為が原因であったケースが最も多い。

- **漏えい**　情報を第三者に漏らすこと。「意図的な情報の漏えい」と「意図的でない情報の漏えい」がある。
- **紛失**　情報が保存されているPCやUSBメモリを置き忘れたり、盗まれたりして、なくしてしまうこと。
- **誤操作**　操作を間違えて情報を消去したり、上書きしてしまうこと。電子メールの宛先を間違えて、重要な情報が漏えいしてしまうこと。
- **ソーシャルエンジニアリング**
  なりすまし（本人であるかのように装って、暗証番号やパスワードなどを聞き出す行為）や**盗み見**（暗証番号やパスワードを入力している人の、キーボード操作や画面に表示された情報を盗み見る行為）がある。

②技術的脅威　悪意をもった第三者がコンピュータを利用して**サイバー攻撃**してくる脅威。

- **マルウェアによる攻撃**
  コンピュータウイルスによる攻撃（コンピュータに何らかの被害を与える攻撃）や**DoS攻撃**（コンピュータに過剰な負荷をかけて、サービス提供を妨害する攻撃）がある。
- **パスワードクラック**
  辞書攻撃（辞書ファイルを用いて単語の組合せを試して、パスワードを不正に解読する攻撃）や**総当たり攻撃**（あらゆる文字の組合せを試して、パスワードを不正に解読する攻撃）がある。

③物理的脅威　機器や、機器が設置された建物に対する脅威。

- **災害**　自然災害（地震、洪水など）や人的災害（火災など）によって機器が使えなくなったり、機器がなくなってしまうこと。
- **破壊**　悪意をもった第三者による**破壊行為**や**妨害行為**によって、機器が使えなくなること。