情報セキュリティ管理と監査

日本公認会計士協会　IT委員会
ITアシュアランス専門委員会　専門委員長
監査法人トーマツ　和貝　享介

2003/5/23

情報セキュリティとは

- 情報の機密保持、インテグリティ、可用性を維持すること

  - 機密保持（Confidentiality）
    - 情報へのアクセスが許された者のみに限られること。
  - インテグリティ（Integrity）
    - 情報が正確に過不足なく処理、保存されること。
  - 可用性（Availability）
    - 情報が必要な時いつでも利用できること。

情報セキュリティへの脅威

- 盗聴・漏洩
  - 正当又は不正アクセス手続を通じて、情報関連施設・組織の内部者又は外部者が機密情報を取得、他者に提供する。
- 改ざん・破壊
  - 正当又は不正アクセス手続を通じて、情報を異常更新する。
- システムダウン
  - 災害等により端末機、ネットワーク、コンピュータの運用が停止する。

情報セキュリティ管理

- 人的な管理
  - 教育・研修による管理 ・・・セキュリティ教育・研修
  - 規程による管理 ・・・セキュリティポリシー・スタンダード・マニュアルの策定・遵守
- 物的な管理
  - アクセス管理 ・・・建物、設備、ネットワーク、データ、プログラムのアクセス者の限定
  - 暗号化 ・・・漏洩した情報の判読不能化
  - バックアップ管理 ・・・データ、プログラム、コンピュータ、ネットワーク、要員、電源の二重化

情報セキュリティ監査

- 情報セキュリティ管理の整備・運用の有効性は、運営主体自身でない第三者が保証することで信頼性が付与され、安心して情報を利用できる。

- 情報セキュリティ監査のポイント
  - セキュリティの仕組みは適切か
  - セキュリティの仕組みを支える組織・手続は適切か
  - セキュリティの仕組み・組織・手続は適切に運用されているか
- 情報セキュリティ外部監査の例
  - 金融庁「システムリスク監査」
  - 経済産業省「情報セキュリティ監査制度」
  - 総務省「住民基本台帳ネットワークシステムのシステム運営監査」