情報システム論

第11回

今日の話題

- 情報セキュリティ

情報セキュリティの必要性

- JIS Q 27002 (ISO/IEC 17799)
  - 情報は、他の重要な事業資産と同様、組織事業の基礎を成すものであり、したがって、適切に保護する必要がある。
  - 企業
    - 競争力、キャシュフロー、収益性、法的遵守、企業イメージの維持に不可欠
  - 官民
    - 電子政府、電子ビジネスの構築、関連リスクの回避・低減

情報に対する脅威

- 不正行為
- 妨害行為
- 破壊行為
- 自然災害
- 機器障害
- 故意・過失

情報セキュリティとは

- 情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

- 機密性
  - 認可されていない個人，エンティティ又はプロセスに対して，情報を使用不可又は非公開にする特性
- 完全性
  - 資産の正確さ及び完全さを保護する特性
- 可用性
  - 許可されたエンティティが要求したときに、アクセス及び使用が可能である特性

- 真正性
  - ある主体又は資源が、主張どおりであることを確実にする特性
- 責任追跡性
  - あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性
- 否認防止
  - ある活動又は事象が起きたことを、後になって否認されないように証明する能力
- 信頼性
  - 意図した動作及び結果に一致する特性

情報セキュリティマネジメント

- 技術的な手段には限界
- 適切な管理と手順とによって支持

JIS Q 27002 (ISO/IEC 17799)

- 情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範
  - 組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則について規定

JIS Q 27001 (ISO/IEC 27001)

- 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項
  - 情報セキュリティマネジメントシステム(ISMS)を確立、導入、運用、監視、レビュー、維持及び改善するためのモデルを提供するために作成

資産の管理

- 資産に対する責任
  - 資産目録
  - 資産の管理責任者
  - 資産利用の許容範囲

人的資源のセキュリティ

- 雇用前
- 雇用期間中
- 雇用後

物理的および環境的セキュリティ

- セキュリティを保つべき領域
  - 物理的セキュリティ境界
  - 物理的入退管理策
  - オフィス、部屋および施設のセキュリティ
  - 外部および環境の脅威からの保護
  - セキュリティを保つべき領域での作業
  - 一般の人の立ち寄り場所及び受渡場所

物理的および環境的セキュリティ

- 装置のセキュリティ
  - 装置の設置及び保護
  - サポートユーティリティ
  - ケーブル配線のセキュリティ
  - 装置の保守
  - 構外にある装置のセキュリティ
  - 装置の安全な処分又は再利用
  - 資産の異動

通信及び運用管理

- 第三者が提供するサービスの管理
- 悪意のあるコード及びモバイルコードからの保護
- バックアップ
- ネットワークセキュリティ管理
- 媒体の取扱い
- 情報の交換
- 電子商取引サービス
- 監視

アクセス制御

- 利用者のアクセス管理
  - 利用者登録
  - 特権管理
  - 利用者パスワードの管理
  - 利用者アクセス権のレビュー

アクセス制御

- 利用者の責任
  - パスワードの利用
  - 無人状態にある利用者装置
  - クリアデスク・クリアスクリーン方針

アクセス制御

- ネットワークのアクセス制御
  - 外部から接続する利用者の認証
  - ネットワークにおける装置の識別
  - ネットワークの領域の分割
  - ネットワークの接続制御
  - ネットワークルーティング制御

アクセス制御

- オペレーティングシステムのアクセス制御
  - セキュリティに配慮したログイン手順
  - 利用者の識別及び認証
  - パスワード管理システム
  - システムユーティリティの使用
  - セッションのタイムアウト
  - 接続時間の制限

情報システムの取得、開発及び保守

- 業務用ソフトウェアでの正確な処理
- 暗号による管理策
- システムファイルのセキュリテイ
- 開発及びサポートプロセスにおるセキュリテイ
- 技術的脆弱性管理

その他

- 情報セキュリティインシデントの管理
- 事業継続管理
- 順守

ISMSの確立

- ISMSの適用範囲及び境界を定義
- ISMSの基本方針を定義
- リスクアセスメントの取組方法を定義
- リスクの特定
- リスクの分析と評価
- リスク対応
- 管理目的と管理策の選択
- 残留リスクの承認
- 適用宣言書の作成