セキュリティ基礎

情報セキュリティ

- データやシステムを含めた情報の状態を守る
- 情報セキュリティの CIA
  - 機密性（Confidentiality）：認められた人だけデータにアクセスできる状態を確保すること
  - 完全性（Integrity）：データが破損・改ざんされない状態を確保すること
  - 可用性（Availability）：必要なときにデータにアクセスできる状態を確保すること

セキュリティの必要性

- 脅威（Threats）：CIAの達成を脅かす何らかの事象
- セキュリティの前提：性悪説
  - 例え「〜」があったとしてもCIAを達成するための仕組み

技術的脅威

- プログラムが介在する脅威
- マルウェア，フィッシング詐欺，標的型メールなど，メールの偽装やプログラムの脆弱性を悪用する
- 主な原因
  - 脆弱性：情報セキュリティ上の欠陥（セキュリティホール）
- 対策
  - 「手口」を理解し，悪用されるようなプログラムを作成しない
  - セキュリティパッチの適用

- SQLインジェクション
  - フォームから不正な値を入れることでシステムの内部情報を漏洩させる
- クロスサイト・スクリプティング（XSS）
  - Webサイトにアクセスすることで不正なプログラムが実行され情報が漏洩する

人的脅威

- 人の操作によって引き起こされる脅威
- メール誤送信，内部関係者によるデータの抜き取りなど，操作ミス，内部からの情報漏えい
- 主な原因
  - ヒューマンエラー，ソーシャルセキュリティ
- 対策
  - 運用ルールの規定
  - 操作ミスを減らす運用（機能の限定）

物理的脅威

- 物理的な破損による脅威
- 主な原因
  - 経年による故障，災害などに機器の破損
- 対策
  - データ保全ルールの規定
  - 運用によるリスク低減

セキュリティポリシー

- 基本方針
- ガイドライン
- 実施手順

- 機密性の確保
  - 情報資産を正当な権利を持った人だけが使用できる状態にしておく
  - 情報漏えい防止，アクセス権の設定，暗号の利用などの対策
- 完全性の確保
  - 情報資産が正当な権利を持たない人により変更されていないことを確実にしておく
  - 改ざん防止，検出などの対策
- 可用性の確保
  - 情報資産を必要なときに使用できる
  - 電源対策，システムの二重化，バックアップ，災害復旧計画などの対策