まとめ

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

情報技術の特性

- 情報技術の特性
  - 無体物 (物理実体なし)、非占有、非可逆的拡散など
- 情報技術による先鋭化
  - 時間・距離の短縮
- 技術そのものの変化の速さ
- 技術、社会、法制度、倫理
  - 社会や制度が情報技術に追いつかない
  - グローバルな影響

情報システムとインターネット

- インターネットの基本
  - 防御のための基礎知識が必要
  - IP address, port, netmask, etc.
- 分散情報システム
  - 関連システムが連携して動く
  - ネットワークを介したデータ連携等
- web 型情報システム
  - サービスの標準化
  - プロトコルの基本の理解が必要
    connection-less, cookie, etc.

- 仮想化
  - 物理的サーバとサービスの分離
  - サービスのソフトウェア化
  - サービスを複製できる
- クラウドサービス
  - SaaS
  - PaaS
  - IaaS
  - etc.

情報セキュリティの概念

- 機密性
  - 権限のある者だけが、生成、閲覧、変更、削除できる
  - 秘密を守る
- 完全性
  - 必要とするときに正しい情報を取得できる
- 可用性
  - 必要とするときに情報・装置を利用できる
- 公開情報にもセキュリティの概念がある
  - 完全性、可用性の重要性を再確認

情報資産とリスク

- 情報資産: 情報に関わる様々な資産
- 有形資産
  - コンピュータ本体
  - ネットワーク機器
  - データを保管する媒体
  - 紙の図面
- 無形資産
  - ソフトウェア
  - データ
  - ノウハウ
  - バックアップが必要
- リスク: 破損、紛失、漏洩、システム停止
  - 発生確率と損害の積

情報セキュリティへの視点

- 個人として
  - 被害者にならないために
  - 加害者にならないために
- 組織人として
  - 組織のポリシーの理解
  - 公私の区別
- 技術者として
  - 情報収集と報告
  - 対策実施
- 経営者として
  - 情報セキュリティの重要性への理解

情報セキュリティ技術

- 暗号
  - 共有鍵方式、公開鍵方式、電子証明書
- アクセス制御
  - ネットワーク、サービス等の各層
- 認証: 利用者の特定
  - 認証要素
  - 多要素認証
  - FIDO
  - パスワードの課題
- マルウェア対策
  - ウィルス対策アプリケーション
  - IPS (Intrusion Protection System)
- ログ分析

情報セキュリティの設計

- 機能要件と非機能要件
- 仕様書に情報セキュリティ要件を記載
  - アクセス制限
  - 認証
  - 暗号化
  - 資格要件、作業要件等
- 情報セキュリティに関する基準
  - 認証制度 (ISMS など)
- セキュリティポリシー
  - 統一基準

事後対策

- セキュリティインシデントは必ず起こる
- インシデント発生を想定した対策
  - 被害拡大を抑止する
  - インシデント予兆を把握する
- インシデント発生時の対策準備
  - 応急措置の体制
  - 連絡・報告の体制
- 再発防止
- CSIRT

情報セキュリティに関する法制度

- 刑法の中での情報技術: 無体物であることの困難さ
- 不正アクセス防止法
- 電子署名法
- 個人情報保護法
- 著作権
- Creative Commons

情報セキュリティと人間

- 人間の特性を考慮したセキュリティ対策
  - 内部からの情報漏洩
  - 対策を無効化する行動
  - リテラシー、教育の重要性
- 組織的情報セキュリティ対策
- 情報倫理