情報セキュリティ

九州産業大学
情報科学部
宮崎明雄

情報セキュリティとは

- ネットワーク社会とインターネット
- ネットワーク社会の問題点
- 情報倫理・モラル
- ネットワーク社会のルールとマナー
- プライバシー・個人情報・著作権の保護
- 情報システム・ネットワークの安全性（セキュリティ）

情報セキュリティ技術の概要

- ネットワーク社会とセキュリティへの脅威
  - ーセキュリティに対する脅威の分類
- ネットワーク社会のセキュリティを守る技術の概要
  - ーアクセス管理技術
  - ー暗号技術
  - ー電子透かし技術
  - ーその他の対策
    （コンピュータウィルス用ワクチン、・・・）

アクセス管理技術

- アクセス管理技術の分類
- ユーザ認証技術
- クライアント認証技術
- リモートユーザ認証技術
- アクセス制御
- ファイアウォール
- セキュリティ評価基準

暗号技術　ー暗号とはー

- 暗号の歴史
- 簡単な暗号からより強い暗号へ
- 究極の暗号
- 暗号で署名する
- ネットワーク暗号

暗号技術　ー共通鍵暗号方式ー

- 共通鍵暗号方式
- DES (Data Encryption Standard)
- 暗号攻撃
- DESからトリプルDES（T-DES）へ
- AES (Advanced Encryption Standard)
- ブロック暗号の使い方

暗号技術
－鍵配送方式と公開鍵暗号方式－

- 古典的鍵配送方式
- 公開鍵暗号方式
- 耐タンパー装置を用いたIDに基づく暗号方式
- RSA暗号
- さまざまな公開鍵暗号方式（DH鍵共有方式とエルガマル暗号など）
- 公開鍵暗号方式の安全性
- 公開鍵暗号で何ができるのか

暗号技術
－デジタル署名と認証方式－

- デジタル署名
- デジタル署名の安全性とハッシュ関数
- さまざまなデジタル署名方式
- IDに基づくデジタル署名
- メッセージ認証
- 相手認証

暗号技術
－ネットワーク暗号に向けて－

- ネットワーク暗号
- 公開鍵認証基盤 (PKI)
- IDに基づく方式
- 鍵事前配布方式 (KPS)
- 暗号の応用（秘密分散、ネットワークコイン投げ、電子投票、電子マネー、電子入札、タイムスタンプサービス）

電子透かし技術

- インターネット社会におけるデジタル情報の保護
- 暗号によるマルチメディアのプロテクトとその問題点
- 電子透かし
  ～マルチメディアのニュープロテクト技術～
- 電子透かし技術の紹介
- 電子透かし技術の実用化に向けて