| 情報セキュリティ<br>(Information Security) | ４年・後期・１学修単位（β）・必修<br>情報工学科・担当　岡村 真吾 |
|---|---|

| 〔準学士課程(本科 1-5 年)<br>学習教育目標〕 | 〔システム創成工学教育プログラム<br>学習・教育目標〕 | 〔JABEE 基準〕 |
|---|---|---|
| (2) | B-2(80%), D-1(20%) | (c), (d-2a) |

〔講義の目的〕

情報機器や情報ネットワークが発達し、多くの情報が発生し交換される現代において、技術者が身につけておくべき情報セキュリティに関する基本的な技術や知識について学ぶ。

〔講義の概要〕

本科目では、暗号技術やアクセス制御技術といった技術に加え、組織の情報セキュリティを確保するための仕組みや情報セキュリティに関する法制度など、情報を守るための手段について広く学ぶ。各種技術について、理論の説明に加えて具体例の紹介や演習問題を行い、理解を深めていく。

〔履修上の留意点〕

教科書には載っていない内容を扱うこともあるため、ノートを取ることをお薦めする。ただし、単に板書をそのまま書き写すのではなく、内容を理解し、自分なりに要約や補足をすること。
レポートは、参考文献や他人の意見の単なるコピーではなく、自分自身による考えや作業の結果などが含まれるようにすること。

〔到達目標〕

中間試験：各種暗号技術の原理や安全性について理解する。
期末試験：情報ハイディングやアクセス制御などの技術や、組織の情報セキュリティを確保するための仕組みについて理解する。

〔自己学習〕

各講義終了後速やかに、講義内容において理解できたことと理解できなかったことを整理すること。理解できなかったことについては、次回の講義までに解決しておくこと。

〔評価方法〕

試験の成績（100%）で評価する。ただし、本科目への取り組み姿勢に問題がある場合（講義時間中に取り組むべき演習問題に取り組んでいない、レポート等の課題が未提出、提出物の内容が不十分、など）は最大 61%減点することがある。

〔教科書〕

「情報セキュリティの基礎」、佐々木良一 監修、手塚悟 編著、共立出版

〔参考書〕

「情報セキュリティ」、宮地充子、菊池浩明 編著、オーム社
「暗号とセキュリティ」、神保雅一 編著、オーム社
「情報セキュリティの対策と要点」、持田敏之、船曳信生 編著、コロナ社
「情報社会・セキュリティ・倫理」、辻井重男 著、コロナ社

〔関連科目〕

情報数学、計算機ネットワーク、情報理論

講義項目・内容

| 週数 | 講義項目 | 講義内容 | 自己評価＊ |
|---|---|---|---|
| 第 1 週 | イントロダクション | 本科目で扱う内容を概観する。 | |
| 第 2 週 | 暗号の基礎 | 暗号技術の基礎について学ぶ。 | |
| 第 3 週 | 秘密分散法 | 秘密分散法について学ぶ。 | |
| 第 4 週 | 共通鍵暗号（１） | DES や AES について学ぶ。 | |
| 第 5 週 | 共通鍵暗号（２） | ブロック暗号の操作モードについて学ぶ。 | |
| 第 6 週 | 公開鍵暗号（１） | RSA 暗号について学ぶ。 | |
| 第 7 週 | 公開鍵暗号（２） | DH 鍵共有と ElGamal 暗号について学ぶ。 | |
| 第 8 週 | ディジタル署名 | ディジタル署名と PKI について学ぶ。 | |
| 第 9 週 | バイオメトリック認証 | 生体認証について学ぶ。 | |
| 第 10 週 | 情報ハイディング | 電子透かしやステガノグラフィについて学ぶ。 | |
| 第 11 週 | アクセス制御 | アクセス制御技術について学ぶ。 | |
| 第 12 週 | 不正プログラム対策 | 不正プログラムへの対策について学ぶ。 | |
| 第 13 週 | セキュリティ評価 | 評価制度やセキュリティポリシーについて学ぶ。 | |
| 第 14 週 | 法制度 | 情報セキュリティに関する法制度について学ぶ。 | |
| 第 15 週 | デジタルフォレンジック | 電磁的証拠の保全と解析について学ぶ。 | |
| 期末試験 | | | |

＊４：完全に理解した，３：ほぼ理解した，２：やや理解できた，１：ほとんど理解できなかった，０：まったく理解できなかった．
（達成） （達成） （達成） （達成） （達成）