

情報セキュリティ (Information Security)		4 年・後期・1 学修単位 (β)・必修 情報工学科・担当 岡村 真吾	
〔準学士課程(本科 1-5 年) 学習教育目標〕 (2)	〔システム創成工学教育プログラム 学習・教育目標〕 B-2 (80%), D-1 (20%)	〔JABEE 基準〕  (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、原理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。また、情報セキュリティに関する事例についても適宜紹介する。			
〔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〕 後期中間試験：各種暗号技術の原理や安全性について理解する。 学年末試験：組織の情報セキュリティを確保するための仕組みや、個人に期待される情報セキュリティリテラシーについて理解する。			
〔評価方法〕 定期試験の成績（75%）とレポート等の課題（25%）により評価する。 （ただし、課題の出題がなかった場合は定期試験の成績（100%）で評価する。）			
〔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	共通鍵暗号	共通鍵暗号について学ぶ。	
第4週	公開鍵暗号（1）	RSA 暗号について学ぶ。	
第5週	公開鍵暗号（2）	DH 鍵共有と ElGamal 暗号について学ぶ。	
第6週	デジタル署名	デジタル署名について学ぶ。	
第7週	秘密分散法	秘密分散法について学ぶ。	
第8週	バイOMETリック認証	生体認証について学ぶ。	
第9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10週	アクセス制御	アクセス制御技術について学ぶ。	
第11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12週	セキュリティ管理	評価制度やセキュリティポリシーについて学ぶ。	
第13週	情報セキュリティリテラシー	個人に期待されるリテラシーについて学ぶ。	
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。	
学年末試験			

\* 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）