

<p>情報セキュリティ (Information Security)</p>	<p>4 年・後期・1 学修単位 (β)・必修 情報工学科・担当 岡村 真吾</p>	
<p>〔準学士課程(本科 1-5 年) 学習教育目標〕 (2)</p>	<p>〔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%)</p>	<p>〔JABEE 基準〕 (c), (d-2a)</p>
<p>〔教育方法等〕 概要： 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。 授業の進め方と授業内容・方法： 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。 注意点： 関連科目 情報数学、計算機ネットワーク、情報理論 学習指針 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。 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。</p>		
<p>〔教科書〕 「情報セキュリティの基礎」共立出版 佐々木良一 監修 手塚悟 編著 〔補助教材・参考書〕 「情報セキュリティ」オーム社 宮地充子 菊池浩明 編著 「暗号とセキュリティ」オーム社 神保雅一 編著 「情報セキュリティの対策と要点」コロナ社 持田敏之・船曳信生 編著 「情報社会・セキュリティ・倫理」コロナ社 辻井重男 著</p>		
<p>〔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。</p>		
<p>〔評価割合〕 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。</p>		

授業計画

	週	授業内容・方法	到達目標	自己評価*
後 期	1 週	暗号の基礎	暗号技術の基礎を理解する。	
	2 週	秘密分散法	秘密分散法を理解する。	
	3 週	共通鍵暗号	DES や AES を理解する。	
	4 週	公開鍵暗号（１）	RSA 暗号を理解する。	
	5 週	公開鍵暗号（２）	DH 鍵共有と ElGamal 暗号を理解する。	
	6 週	デジタル署名	デジタル署名と PKI を理解する。	
	7 週	中間試験	授業内容を理解し、正しく解答することができる。	
	8 週	試験返却と解説	自身の答案を見直し、理解が不十分な点を解消する。	
	9 週	バイオメトリック認証	生体認証を理解する。	
	10 週	情報ハイディング	電子透かしやステガノグラフィを理解する。	
	11 週	アクセス制御	アクセス制御技術を理解する。	
	12 週	不正プログラム対策	不正プログラムへの対策を理解する。	
	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を理解する。	
	14 週	法制度	情報セキュリティに関する法制度を理解する。	
	15 週	期末試験	授業内容を理解し、正しく解答することができる。	
	16 週	試験返却と解説	自身の答案を見直し、理解が不十分な点を解消する。	

* 4：完全に達成した， 3：ほぼ達成した， 2：やや達成できた， 1：ほとんど達成できなかった， 0：まったく達成できなかった