奈良工業高等専門学校	開講年度	令和03年度 (2021年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	0073	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	情報工学科	対象学年	4
開設期	後期	週時間数	2
教科書/教材	「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		
担当教員	岡村 真吾		

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】
認証技術、情報ハイディング技術、アクセス制御技術、不正プログラム対策、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。

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	未到達レベルの目安
暗号技術	暗号技術に関する定義や性質を理解し、基本的な暗号方式による暗号化や復号の計算ができる。	暗号技術に関する定義や性質を理解している。	暗号技術に関する授業への取り組みができていない。
認証技術	認証技術に関する定義や性質を理解し、基本的な認証手法について説明できる。	認証技術に関する定義や性質を理解している。	認証技術に関する授業への取り組みができていない。
情報ハイディング技術	情報ハイディング技術に関する定義や性質を理解し、基本的な情報埋め込み手法について説明できる。	情報ハイディング技術に関する定義や性質を理解している。	情報ハイディング技術に関する授業への取り組みができていない。
アクセス制御技術	各種アクセス制御技術を理解し、基本的なアクセス制御技術について説明できる。	各種アクセス制御技術の存在を理解している。	アクセス制御技術に関する授業への取り組みができていない。
不正プログラム対策	各種不正プログラムを理解し、基本的な不正プログラムについてその性質や対策を説明できる。	各種不正プログラムの存在を理解している。	不正プログラム対策に関する授業への取り組みができていない。
情報セキュリティを確保するための仕組み	評価制度、情報セキュリティポリシー、法制度などの、情報セキュリティを確保するための仕組みを理解し、基本的な制度や仕組みについて説明できる。	評価制度、情報セキュリティポリシー、法制度などの、情報セキュリティを確保するための仕組みの存在を理解している。	情報セキュリティを確保するための仕組みに関する授業への取り組みができていない。

学科の到達目標項目との関係

準学士課程（本科１～５年）学習教育目標 （２）
JABEE基準 (c) JABEE基準 (d-2a)
システム創成工学教育プログラム学習・教育目標 B-2 システム創成工学教育プログラム学習・教育目標 D-1

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・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	【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 「サイバーセキュリティ入門」、猪俣敦夫 著、共立出版 「現代暗号のしくみ」、中西透 著、共立出版 「情報社会・セキュリティ・倫理」、辻井重男 著、コロナ社 これらの他にも、次のページに挙げられている本校の蔵書も参考となる。 https://www.info.nara-k.ac.jp/security/books.html 【関連科目】 情報数学、計算機ネットワーク、情報理論、計算理論 【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。 【事前学習】 規則正しい生活を送り、体調を整えておくこと。余力があれば教科書に目を通しておくこと。 【事後展開学習】 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。

学修単位の履修上の注意

講義時間中に提示する演習問題や教科書に掲載されている演習問題を自学自習時間に解くこと。演習問題の類似問題を試験で出題し、試験の成績として自学自習内容を評価する。

授業の属性・履修上の区分

□ アクティブラーニング	□ ICT 利用	□ 遠隔授業対応	□ 実務経験のある教員による授業

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	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	ディジタル署名	ディジタル署名と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。
		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。
	4thQ	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。
		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。

モデルコアカリキュラムの学習内容と到達目標

分類		分野	学習内容	学習内容の到達目標	到達レベル	授業週
専門的能力	分野別の専門工学	情報系分野	情報数学・情報理論	離散数学に関する知識をアルゴリズムの設計、解析に利用することができる。	4	後2,後3,後4,後5,後6

評価割合

	試験	合計
総合評価割合	100	100
専門的能力	100	100