大分工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	R04AES110	科目区分	専門 / 選択
授業形態	授業	単位の種別と単位数	学修単位: 2
開設学科	専攻科電気電子情報工学専攻	対象学年	専1
開設期	前期	週時間数	前期:2
教科書/教材	K-SEC 高学年共通教材，K-SEC 高学年分野別教材		
担当教員	霸 浩二		

到達目標

(1) 情報化社会における,情報セキュリティ技術の重要性を説明できる.(定期試験と課題)
(2) 暗号技術に関する理論と実際の応用例を説明でき，自主的・継続的に学習できる.(定期試験と課題)
(3) ネットワークセキュリティ技術と不正アクセスに対する対処法を説明できる.(定期試験と課題)
(4) セキュリティシステムを構築するための装置,システム,評価方法を説明できる.(定期試験と課題)

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
評価項目1	情報化社会における,情報セキュリティ技術の重要性を詳しく説明できる	情報化社会における,情報セキュリティ技術の重要性を説明できる	情報化社会における,情報セキュリティ技術の重要性を説明できない
評価項目2	暗号技術に関する理論と実際の応用例を説明でき，自主的・継続的に学習できる	暗号技術に関する理論と実際の応用例を説明でき，継続的に学習できる	暗号技術に関する理論と実際の応用例を説明でき，継続的に学習できない
評価項目3	ネットワークセキュリティ技術と不正アクセスに対する対処法を詳しく説明できる	ネットワークセキュリティ技術と不正アクセスに対する対処法を説明できる	ネットワークセキュリティ技術と不正アクセスに対する対処法を説明できない
評価項目4	セキュリティシステムを構築するための装置,システム,評価方法を詳しく説明できる	セキュリティシステムを構築するための装置,システム,評価方法を説明できる	セキュリティシステムを構築するための装置,システム,評価方法を説明できない

学科の到達目標項目との関係

学習・教育目標 (E1)
JABEE 1.2(d)(1) JABEE 1.2(g)

教育方法等

概要	本授業では,情報を安全に管理,運用するための技術として情報セキュリティを学ぶ.情報セキュリティとして必要な暗号理論,ネットワークセキュリティ,個人認証技術,耐タンパデバイスについて理論と応用技術を習得する.また,実際の導入例など具体的なセキュリティ技術を適宜紹介することにより,実践的な知識を養う (科目情報) 教育プログラム　第3学年　○科目 ネットワークアーキテクチャ, 情報理論(E科),通信工学Ⅰ・Ⅱ(S科)
授業の進め方・方法	授業は教科書に沿って進め、適宜最新の技術情報を紹介する．暗号技術に関しては、数学を用いて演習を行う． （事前学習） 授業の前に，前回の授業範囲の復習を行っておく．また，教科書の今回の授業範囲を事前に読んで，予習をしておく．
注意点	(履修上の注意) 講義の途中でもわからなくなったら,何時でも質問してよいことにする 課題提出には，プログラミング（C言語）が必要となることがあるので復習しておくこと （自学上の注意） 5課題×3時間以上の自宅学習と試験準備2回×8時間で合計30時間以上の自学自習が必要 (参考書) 宮地充子,菊池浩明,「情報セキュリティ」（オーム社）など，情報セキュリティ，暗号技術に関する本

評価

(単位修得の条件について)
総合評価60点以上を単位修得の条件とする
(総合評価)
総合評価 = （中間試験）×0.4 +（期末試験）×0.4 + (課題平均[10点満点])×2.0
(再試験について)
再試験は原則として行わない

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
前期	1stQ	1週	情報セキュリティ技術 ・セキュリティへの脅威，対策	情報化社会における,情報セキュリティ技術の重要性を理解する
		2週	共通鍵暗号 ・ブロック暗号の構造	ブロック暗号を理解する
		3週	.共通鍵暗号 ＤＥＳ，ＡＥＳ	.共通鍵暗号であるＡＥＳの仕組みと方法を理解する
		4週	公開鍵暗号 必要な数学的知識	公開鍵暗号を理解するのに必要な数学的知識を学ぶ
		5週	公開鍵暗号 初等整数論	公開鍵暗号方式の仕組みを学ぶ
		6週	素因数分解の困難性に基づく公開鍵暗号（ＲＳＡ）	RSAについて仕組みを学ぶ
		7週	ディジタル署名	ディジタル署名について学ぶ
		8週	前期中間試験	

	2ndQ	9週	前期中間試験の解答と解説 暗号プロトコル	暗号プロトコルについて学ぶ
		10週	ゼロ知識証明と社会システム	ゼロ知識証明と社会システムについて学ぶ
		11週	ネットワーク・インターネットセキュリティ	ネットワーク・インターネットセキュリティについて学ぶ
		12週	ネットワークセキュリティ演習	KIPS教材を用いた演習を行う
		13週	不正アクセス ・ウイルス・ファイヤーウォール ・不正侵入検出技術	不正アクセスについての対処方法について学ぶ
		14週	耐タンパ・バイオメトリクス	耐タンパ・バイオメトリクスについて学ぶ
		15週	前期期末試験	
		16週	前期期末試験の解答と解説	

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

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	課題	合計
総合評価割合	80	0	0	0	0	20	100
基礎的能力	40	0	0	0	0	10	50
専門的能力	40	0	0	0	0	10	50
分野横断的能力	0	0	0	0	0	0	0