鈴鹿工業高等専門学校		開講年度	令和06年度 (2024年度)	授業科目	情報セキュリティ概論
科目基礎情報					
科目番号	0056		科目区分	専門 / 必修	
授業形態	授業		単位の種別と単位数	履修単位: 1	
開設学科	材料工学科		対象学年	3	
開設期	前期		週時間数	2	
教科書/教材	教科書: なし (適宜資料を配布する). 参考書: 授業内で適宜紹介する.				
担当教員	桑野 一成				
到達目標					
情報の重要性を理解し, 情報セキュリティの基礎, 技術, 必要性を理解, 導入, 周知できる.					
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		
評価項目1	情報セキュリティ技術の必要性について, 理解し, 導入, 周知することができる.	情報セキュリティ技術の必要性について, 理解することができる.	情報セキュリティ技術の必要性について, 理解することができない.		
評価項目2	情報セキュリティ技術について, 理解することができ, 応用や適用について説明できる.	情報セキュリティ技術について, 理解することができる.	情報セキュリティ技術について, 理解することができない.		
評価項目3	コンピュータシステムについて, 内部構造も含めて説明できる.	コンピュータシステムについて, 理解することができる.	コンピュータシステムについて, 理解することができない.		
評価項目4	ネットワーク技術について, 理解することができ, 構築や利用ができる.	ネットワーク技術について, 理解することができる.	ネットワーク技術について, 理解することができない.		
学科の到達目標項目との関係					
教育方法等					
概要	情報の重要性を理解し, 情報セキュリティの基礎, 技術, 必要性を理解, 導入, 周知できる.				
授業の進め方・方法	- 全ての内容が学習・教育到達目標(B)<基礎>に対応する. - 本教科は演習を中心に行っていく. 後半ではグループワークも行う.				
注意点	<到達目標の評価方法と基準> 「到達目標」1～11を中間試験, 期末試験, 課題で確認する. これらの合計得点が満点の60%以上であれば, 授業の目標を達成したと判定する. <学業成績の評価方法および評価基準> - 中間試験, 期末試験の結果の合計70%, 課題の評価30%として, 100点満点換算した結果を学業成績とする. ※定期試験の成績が60点未満の者には再試験を実施する. また, 課題点が60%未満の者には追加課題を実施する. <単位修得要件> - 学業成績で60点以上を取得すること. <レポート等> - 適宜課題を課す. 詳細は授業時に説明する. <備考> - 本教科は後に学習する「情報処理応用」の基礎となる科目である. - 特に指示が無い限り, 情報処理センター演習室で講義を実施する. - 授業の進行状況に応じて, 授業内容を一部省略, 追加することがある.				
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		
前期	1stQ	1週	ガイダンス, 情報セキュリティと関連する脅威	1. 情報セキュリティの必要性とその脅威について説明できる.	
		2週	ネットワークの仕組みその1 (通信, コンピュータの識別)	2. コンピュータの構成, ハード・ソフトの役割, 構築されるシステムについて説明できる.	
		3週	ネットワークの仕組みその2 (プロトコル, OSI参照モデル)	3. ネットワーク技術, 構成, システムとの繋がりについて説明できる.	
		4週	情報セキュリティの重要性	4. 情報セキュリティの重要性を理解し, 説明できる. 上記. 1	
		5週	情報セキュリティ技術の概要	5. 情報セキュリティ技術について, 意味と効果を説明できる.	
		6週	暗号技術	6. 公開鍵暗号と共通鍵暗号の仕組みを理解し, 説明できる. 上記. 5	
		7週	1～6週までの復習	上記. 1～6	
		8週	中間試験	これまで学習した内容に対して説明ができる.	
	2ndQ	9週	情報セキュリティ関連法規その1 (名誉棄損, プライバシー権)	7. 情報セキュリティに関連する法律について, 内容を理解し, 説明できる.	
		10週	情報セキュリティ関連法規その2 (著作権, 不正アクセス)	上記. 7	
		11週	情報セキュリティ対策その1 (マネジメントゲーム)	8. 情報セキュリティマネジメントの必要性を理解し, 説明できる.	
		12週	情報セキュリティ対策その2 (分野別)	9. 所属学科の分野と情報セキュリティとの関係が理解できる. 上記. 8	

	13週	メディアリテラシーその1 (生成AIとフェイクニュース)	10. 情報の真偽を判別するための基本的な考え方を理解し, 実践できる.
	14週	メディアリテラシーその2 (統計的思考)	11. データを読み取る際の注意点を理解し, 適切に分析できる. 上記. 10
	15週	まとめ	これまで学習した内容に対して説明ができる.
	16週		

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	計算機工学	コンピュータを構成する基本的な要素の役割とこれらの間でのデータの流れを説明できる。	4	
				プロセッサを実現するために考案された主要な技術を説明できる。	4	
				メモリスistemを実現するために考案された主要な技術を説明できる。	4	
				入出力を実現するために考案された主要な技術を説明できる。	4	
			コンピュータシステム	ネットワークコンピューティングや組込みシステムなど、実用に供せられているコンピュータシステムの利用形態について説明できる。	4	
				デュアルシステムやマルチプロセッサシステムなど、コンピュータシステムの信頼性や機能を向上させるための代表的なシステム構成について説明できる。	4	
				集中処理システムについて、それぞれの特徴と代表的な例を説明できる。	4	
				分散処理システムについて、特徴と代表的な例を説明できる。	4	
			システムプログラム	コンピュータシステムにおけるオペレーティングシステムの位置づけを説明できる。	4	
				プロセス管理やスケジューリングなどCPUの仮想化について説明できる。	4	
				排他制御の基本的な考え方について説明できる。 記憶管理の基本的な考え方について説明できる。	4 4	
			情報通信ネットワーク	プロトコルの概念を説明できる。	4	
				プロトコルの階層化の概念や利点を説明できる。	4	
				ローカルエリアネットワークの概念を説明できる。	4	
				インターネットの概念を説明できる。	4	
			その他の学習内容	TCP/IPの4階層について、各層の役割を説明でき、各層に関係する具体的かつ標準的な規約や技術を説明できる。	4	
				コンピュータウイルスやフィッシングなど、コンピュータを扱っている際に遭遇しうる代表的な脅威について説明できる。	4	
				コンピュータを扱っている際に遭遇しうる脅威に対する対策例について説明できる。	4	
				基本的な暗号化技術について説明できる。 基本的なアクセス制御技術について説明できる。	4 4	
						マルウェアやフィッシングなど、コンピュータを扱っている際に遭遇しうる代表的な脅威について説明できる。

評価割合

	試験	課題	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	70	30	0	0	0	0	100
基礎的能力	50	20	0	0	0	0	70
専門的能力	10	5	0	0	0	0	15
分野横断的能力	10	5	0	0	0	0	15