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 I

科目基礎情報

科目番号	R04G111	科目区分	一般 / 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	一般科目	対象学年	1
開設期	前期	週時間数	2
教科書/教材	（教科書）なし／（参考図書）K-SEC教材などのe-learning教材		
担当教員	樋口 勇夫		

到達目標

(1) 情報リテラシーの基本的な内容について理解し説明できる(定期試験と課題)
(2) 情報ネットワークの構成と仕組みを理解し，必要に応じた設定ができる(定期試験)
(3) 情報セキュリティの必要性や対策について説明できる(定期試験と課題)
(4) サイバー攻撃や情報を扱ううえでのリスクを理解し，その防御・対策について説明できる(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
目的・到達目標(1) の評価指標：情報基礎	情報リテラシーの基礎となる内容を理解し，情報伝達について状況に沿った説明ができる.	情報リテラシーの基礎となる内容について説明できる.	情報リテラシーの基礎となる内容について理解できない.
目的・到達目標(2) の評価指標：ネットワーク	ネットワークの構成と仕組みを理解し，状況を踏まえた設定ができる.	ネットワークの構成と仕組みを理解し，基本的な設定ができる.	ネットワークの構成や仕組みを理解できない.
目的・到達目標(3) の評価指標：情報セキュリティ	状況に合わせたセキュリティ対策を説明できる.	情報セキュリティの必要性や対策について説明できる.	情報セキュリティの必要性や対策を説明できない.
目的・到達目標(4) の評価指標：サイバー攻撃とリスク管理	サイバー攻撃や情報リスクに対して状況に合わせた対策を選択し，説明できる.	サイバー攻撃や情報リスクとその対策について説明できる.	サイバー攻撃や情報リスクについて説明できない.

学科の到達目標項目との関係

学習・教育目標 (B2)

教育方法等

概要	（科目情報） ・数理・データサイエンス・AI教育プログラム科目 数理・データサイエンス・AIに関するリテラシーレベルの基礎的な内容として，情報学の基礎についてオンライン授業で学ぶ.
授業の進め方・方法	最初にBYOD端末でオンライン受講するための基礎知識を学び，それ以降はオンラインでの受講を原則とする. (事前学習) 可能であればネットワークの設定をしておくこと.
注意点	(自学上の注意) 復習をしっかりすること．わからないことはそのままにせず質問すること. (履修上の注意) 場合によっては情報演習室なども活用すること.

評価

（総合評価）
総合評価=(中間試験と期末試験の平均)×0.6+(オンライン課題・小テスト)×0.4
最終評価60点以上を合格とする.
(再試験)
不合格者には再試験を行う.

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	BYOD端末の取り扱い e-learningの進め方	BYOD端末でネットワークに接続できる. Moodleにログインできる.
		2週	情報システムとその利用形態 オペレーティングシステム	代表的な情報システムとその利用形態について理解できる．コンピュータの構成とオペレーティングシステム(OS)の役割を理解し，基本的な取り扱いができる．(MCC Ⅳ-C, 数理)
		3週	データベースの意義と概要	データベースの意義と概要について説明できる．(MCC Ⅳ-C, 数理)
		4週	データの表現方法 アナログ情報とデジタル情報	コンピュータ内におけるデータ(数値，文字等)の表現方法について説明できる．アナログ情報とデジタル情報の違いについて説明できる．(MCC Ⅳ-C, 数理)
		5週	社会におけるネットワークの役割 ポートとサービス	社会における情報通信ネットワークの役割を説明できる．基礎的なネットワークの構成と仕組みを理解できる．(MCC Ⅳ-C, 数理)
		6週	OSI参照モデル ネットワークデバイスの設定	情報通信ネットワークの仕組みや構成要素，プロトコルの役割や技術（OSI参照モデル）について理解できる．一般的なネットワークデバイス（パソコン，家庭用レベルのルーター等）の設定ができる．(MCC Ⅳ-C, 数理)
		7週	前半のまとめ	
		8週	前期中間試験	目的・到達目標(1)(2)
	2ndQ	9週	中間試験の解説 情報セキュリティの必要性 情報セキュリティ対策	情報セキュリティの必要性について説明できる．情報セキュリティ対策について説明できる．(MCC Ⅳ-C, 数理)

		10週	情報セキュリティの3要素 アクセス制限や認証方式	情報セキュリティの３要素（機密性，完全性，可用性）について説明できる．情報へのアクセス制限や認証方式について説明できる．(MCC Ⅳ-C, 数理)	
		11週	暗号技術の必要性 サイバー攻撃の形態と実例	基礎的な暗号技術とその必要性（HTTPS，VPN等）について説明できる．主要な攻撃の形態や実例について説明することができる．(MCC Ⅳ-C, 数理)	
		12週	攻撃に対する防御 情報に関するリスク	攻撃に対する防御方法（予防と対処）について知っている．情報を取り扱う上でのリスクを洗い出し，適切に取り扱う方法を知っている．(MCC Ⅳ-C, 数理)	
		13週	インシデントととるべき対応 脅威と対策	インシデント発生時にとるべき行動を説明できる．脅威（意図的脅威，偶発的脅威）を理解し，その危険度と対策を知っている．(MCC Ⅳ-C, 数理)	
		14週	後半のまとめ		
		15週	前期末試験	目的・到達目標(3)(4)	
		16週	前期末試験の解説	わからなかったところを復習する.	

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
基礎的能力	工学基礎	情報リテラシー	情報リテラシー	情報を適切に収集・処理・発信するための基礎的な知識を活用できる。	3	前3,前4
				情報伝達システムやインターネットの基本的な仕組みを把握している。	3	前2,前5,前6
				情報セキュリティの必要性および守るべき情報を認識している。	3	前9,前10
				個人情報とプライバシー保護の考え方についての基本的な配慮ができる。	3	前13
				インターネット(SNSを含む)やコンピュータの利用における様々な脅威を認識している	3	前11,前12
				インターネット(SNSを含む)やコンピュータの利用における様々な脅威に対して実践すべき対策を説明できる。	3	前12,前13

評価割合

	試験	課題	合計
総合評価割合	60	40	100
基礎的能力	40	20	60
専門的能力	0	0	0
分野横断的能力	20	20	40