高知工業高等専門学校	開講年度	令和05年度 (2023年度)	授業科目	情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄ

科目基礎情報

科目番号	I5010	科目区分	専門 / 選択
授業形態	講義	単位の種別と単位数	履修単位: 1
開設学科	SD 情報セキュリティコース	対象学年	5
開設期	後期	週時間数	2
教科書/教材	教材はオリジナルのものを作成し配布する．購入必須ではないが参考書としてISO27001に関する文献を授業中に紹介する．		
担当教員	立川 崇之		

到達目標

1. 情報セキュリティリスクの分析・評価・対応について説明できる。
2. 情報セキュリティの継続的改善についての具体的な方策について説明できる。
3. 国内における情報セキュリティ組織・機関とその役割について説明できる。
4. 情報セキュリティマネジメントに関する法律やガイドラインについて説明できる.

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	情報セキュリティリスクの分析・評価・対応について説明でき，対応の優先度をつけられる．	情報セキュリティリスクの分析・評価・対応について説明できる．	情報セキュリティリスクの分析・評価・対応について説明できない．
評価項目2	情報セキュリティの継続的改善についての具体的な方策について説明でき，計画書を作成できる．	情報セキュリティの継続的改善についての具体的な方策について説明できる．	情報セキュリティの継続的改善についての具体的な方策について説明できない．
評価項目3	国内における情報セキュリティ組織・機関とその役割について説明でき，それらを活用して情報収集ができる．	国内における情報セキュリティ組織・機関とその役割について説明できる．	国内における情報セキュリティ組織・機関とその役割について説明できない．
評価項目4	情報セキュリティマネジメントに関する法律やガイドラインについて説明でき，運用改善の方法を提案できる．	情報セキュリティマネジメントに関する法律やガイドラインについて説明できる．	情報セキュリティマネジメントに関する法律やガイドライン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・教育到達度目標 (C)

教育方法等

概要	組織において情報システムを運用するためには、組織における情報資産のセキュリティを管理するための枠組みである情報セキュリティマネジメントシステム (ISMS) について理解しておく必要がある。ISMS を策定し実施することが、情報セキュリティマネジメントである。 情報の機密性、完全性、可用性を維持し、またリスクを適切に監視できている状態を保つことを目的とする。
授業の進め方・方法	本授業はISMS を規定した ISO/IEC 27001:2013 に基づいた授業である。ISO/IEC 27001:2013 で取り扱う内容は多岐にわたるため、特に重要と思われる部分を抜粋した教材を使う予定である。講義の状況により、授業の内容や順序を入れ替えることがある。 単に講義を行うだけなく、情報セキュリティの対策手順やリスク評価などを受講者に考えてもらう課題を出題する。情報セキュリティマネジメントの重要事項を問う定期試験も実施する。
注意点	【成績評価の基準・方法】 試験の成績を70%，課題を30%の割合で総合的に評価する．成績評価は中間と期末の各期間の評価の平均とする．学年の評価は後学期末の評価とする．技術者が身に着けるべき専門科目として，上記の到達目標に対する達成度を試験等において評価する． 【事前・事後学習】 事前学習としてシラバスに沿って資料を読んだ上で，理解が難しかった部分を整理して授業に臨むこと．また，事後学習として授業内で取り扱った項目について，関連した事例を調査して理解を深めること． 【履修上の注意】 本科目は，情報システムを構築する技術者ではなく，運用管理や利用者サポートを行う技術者の立場に置かれたときの行動を検討する科目である．卒業後に情報システムを運用する立場に置かれたときの事を想定して，前向きに受講していただきたい．

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
後期	3rdQ	1週	ガイダンス 情報セキュリティマネジメントシステム (ISMS) とは	情報セキュリティマネジメントシステム (ISMS) を導入する意義を理解する．
		2週	ISO/IEC 27001 と関連規格、法制度、ガイドライン，用語の構成	ISMS の国際規格である ISO/IEC 27001 と関連事項を理解する．ISO/IEC 27001 における用語の構成と意味を理解する．
		3週	情報セキュリティ機関	国内外の情報セキュリティ機関とその役割を理解する．
		4週	管理策I	ISO/IEC27001附属書Aに記載されたセキュリティリスク管理策を理解する．
		5週	管理策II	ISO/IEC27001附属書Aに記載されたセキュリティリスク管理策を理解する．
		6週	管理策III	ISO/IEC27001附属書Aに記載されたセキュリティリスク管理策を理解する．
		7週	管理策IV	ISO/IEC27001附属書Aに記載されたセキュリティリスク管理策を理解する．
		8週	ISMS 運用検討	ISMS を運用するにあたっての計画，管理法などを理解する．

	4thQ	9週	ISMS 組織の状況	ISMS を導入するにあたり，適用する組織への考慮点を理解する.
		10週	リスク対応I	情報セキュリティのリスクについて分類と対策を理解する.
		11週	リスク対応II	情報セキュリティのリスクについて分類と対策を理解する.
		12週	ISMS 導入支援	ISMS を適用予定の組織への物的，人的支援について評価法を理解する.
		13週	ISMS パフォーマンス評価，改善	ISMS を実施するにあたっての評価法を理解する. ISMS の短期的，長期的な改善方法について理解する.
		14週	ISMS 導入事例I	ISMS を導入している国内外の事例を理解する.
		15週	ISMS 導入事例II	ISMS を導入している国内外の事例を理解する.
		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
基礎的能力	工学基礎	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	説明責任、製造物責任、リスクマネジメントなど、技術者の行動に関する基本的な責任事項を説明できる。	3	後1,後2,後3
				現代社会の具体的な諸問題を題材に、自ら専門とする工学分野に関連させ、技術者倫理観に基づいて、取るべきふさわしい行動を説明できる。	3	後1,後2,後3
				技術者倫理が必要とされる社会的背景や重要性を認識している。	3	後1,後2,後3
				社会における技術者の役割と責任を説明できる。	3	後1,後2,後3
				情報技術の進展が社会に及ぼす影響、個人情報保護法、著作権などの法律について説明できる。	4	後1,後2,後3
				高度情報通信ネットワーク社会の中核にある情報通信技術と倫理との関わりを説明できる。	4	後1,後2,後3
				環境問題の現状についての基本的な事項について把握し、科学技術が地球環境や社会に及ぼす影響を説明できる。	3	後1,後2,後3
				環境問題を考慮して、技術者としてふさわしい行動とは何かを説明できる。	3	後1,後2,後3
				国際社会における技術者としてふさわしい行動とは何かを説明できる。	3	後1,後2,後3
				過疎化、少子化など地方が抱える問題について認識し、地域社会に貢献するために科学技術が果たせる役割について説明できる。	3	後1,後2,後3
				知的財産の社会的意義や重要性の観点から、知的財産に関する基本的な事項を説明できる。	3	後1,後3
				知的財産の獲得などで必要な新規アイデアを生み出す技法などについて説明できる。	3	後1,後3
				技術者の社会的責任、社会規範や法令を守ること、企業内の法令順守(コンプライアンス)の重要性について説明できる。	4	後1,後2,後3
				技術者を目指す者として、諸外国の文化・慣習などを尊重し、それぞれの国や地域に適用される関係法令を守ることの重要性を把握している。	4	後1,後2,後3
				全ての人々が将来にわたって安心して暮らせる持続可能な開発を実現するために、自らの専門分野から配慮すべきことが何かを説明できる。	3	後1,後2,後3
				技術者を目指す者として、平和の構築、異文化理解の推進、自然資源の維持、災害の防止などの課題に力を合わせて取り組んでいくことの重要性を認識している。	3	後1,後2,後3
				科学技術が社会に与えてきた影響をもとに、技術者の役割や責任を説明できる。	3	後1,後2
				科学者や技術者が、様々な困難を克服しながら技術の発展に寄与した姿を通し、技術者の使命・重要性について説明できる。	3	後1,後2
		情報リテラシー	情報リテラシー	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。	4	後1
				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。	4	後1,後4,後5,後6,後7
				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。	4	後1,後4,後5,後6,後7
				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	4	後1,後4,後5,後6,後7
				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。	4	後1,後4,後5,後6,後7
専門的能力	分野別の専門工学	情報系分野	その他の学習内容	コンピュータウィ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	後4,後5,後6,後7
				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	後4,後5,後6,後7
				基本的な暗号化技術について説明できる。	4	後4,後5,後6,後7
				基本的なアクセス制御技術について説明できる。	4	後4,後5,後6,後7
				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。	4	後4,後5,後6,後7

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	70	0	0	0	0	30	100
基礎的能力	30	0	0	0	0	10	40
専門的能力	30	0	0	0	0	10	40
分野横断的能力	10	0	0	0	0	10	20