徳山工業高等専門学校	開講年度	令和02年度 (2020年度)	授業科目	情報システムと技術者倫理

科目基礎情報

科目番号	0125	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: 1
開設学科	情報電子工学科	対象学年	4
開設期	後期	週時間数	1
教科書/教材	（独）情報処理推進機構：情報セキュリティ読本　四訂版。他に，講義用のプリントを配布する。		
担当教員	新田 貴之		

到達目標

現在、情報セキュリティに対する倫理観とそれに基づいた能力が求められていることを理解できる。
この社会的状況を理解するための技術的側面や運用的側面を理解できる。
それに加え、状況を他者に説明する能力や、技術者としてどのように臨むかを各自が確立できる。

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
セキュリティの確立方法（ISMSの確立方法）	情報セキュリティについて、セキュリティの確保の方法について、理解し説明できる。	情報セキュリティについて、脅威と脆弱性の関係について理解することができる。	情報セキュリティについて、脅威や脆弱性について理解できない。
セキュリティの確立方法（技術的側面）	情報セキュリティについて、セキュリティの確保の方法について、理解し説明できる。	情報セキュリティについて、脅威と脆弱性の関係について理解することができる。	情報セキュリティについて、脅威や脆弱性について理解できない。
技術者倫理	情報セキュリティについて、技術者に求められていることを理解でき，妥当な方法を選択できる。	情報セキュリティについて、技術者に求められていることを理解できる。	情報セキュリティについて、技術者に求められていることを理解できない。

学科の到達目標項目との関係

到達目標 A 1 到達目標 A 2
JABEE d-1

教育方法等

概要	近年、情報システムの社会的役割が大きくなっているが、それにつれて、新聞報道になるような各種の問題が生じている。現在は、情報漏洩・システムの大規模な不具合が大きな話題であろう。この授業では、これらの諸問題に対し、体系的なセキュリティの確保方法と、それを支える技術的な側面を学習する。
授業の進め方・方法	授業は、講義形式で進める。前半までは、情報セキュリティの確立方法として、ISMSを勉強する。後半では、具体的な数値やシステムについて講義を行う。シラバスの内容を軸に授業を展開するが、セキュリティの事故については、日々の話題に意識を持って欲しいために，その時々の話題を使う。進行に若干の前後が生じることについては、了承されたい。
注意点	授業では、「システムの利用者として常識的な事項」は、知っていることを前提として進めるため、可能な限り予習を中心に行うことを期待する。予習不足（前提の知識不足）の場合には、どのような知識が必要であったかを考えながら、復習を行うこと。 【関連科目】本科：情報通信工学(４年)、ネットワークアーキテクチャ(５年)、知的財産権(３年) 【評価法】 最終評価点＝（後期中間＋後期末）／2 備考：2019年度までは，社会情報システムという授業科目名で実施していた科目である。従前の授業は，セキュリティに関する事故を取り扱い，技術者としてどうあるべきかという話題提供を行い，それに対する技術の習得という形式であった。今年度からは，セキュリティエンジニアとしての『基本的な態度・素養』を問う問題も出題予定である。

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 【事前事後学習の内容(0.5時間)】復習	情報とは何かを考えることができる。
		2週	情報セキュリティの概要 【事前事後学習の内容(1時間)】復習	情報セキュリティの現状を知り、セキュリティを確立するための方法や組織を知り，説明できる。
		3週	ISMSのフェーズ1 【事前事後学習の内容(1.5時間)】予習1時間（ISMSの全体像を予習すること）復習0.5時間	領域の策定や基本方針の策定の概要を説明できる。
		4週	ISMSのフェーズ2(その１) 【事前事後学習の内容(0.5時間)】復習	情報資産に対する格付けを説明できる。
		5週	ISMSのフェーズ2(その２) 【事前事後学習の内容(0.5時間)】復習	リスクアセスメントの実施手順を説明できる。
		6週	ISMSのフェーズ2(その３) 【事前事後学習の内容(2時間)】フェーズ２の全体の復習	管理策の種類と選択方法を説明できる。
		7週	ISMSのフェーズ3と前半のまとめ 【事前事後学習の内容(2時間)】中間までの全体の復習	リスクに対する考え方を説明できる。
		8週	中間試験	ISMSを用いた情報セキュリティの確立について出題された問題を解答できる。
	4thQ	9週	前半の復習・後半のガイダンス 【事前事後学習の内容(1時間)】復習	前半で学んだセキュリティの確立について、再確認し，後半に向けて、必要な知識を整理できる。
		10週	RASISの概念と現在のセキュリティ 【事前事後学習の内容(1時間)】予習0.5時間，復習0.5時間	前半で学んだセキュリティの確立と技術的な話との関連性を説明できる。
		11週	稼働率（その１） 【事前事後学習の内容(1時間)】予習0.5時間，復習0.5時間	稼働率の向上を行うためのシステム構成を説明できる。
		12週	稼働率（その２） 【事前事後学習の内容(1時間)】予習0.5時間，復習0.5時間	稼働率の計算の仕方を説明できる。

		13週	認証技術 【事前事後学習の内容(1時間)】予習0.5時間，復習0.5時間	パスワードの管理法やその重要性を説明できる。
		14週	暗号化技術 【事前事後学習の内容(２時間)】復習	暗号の使い方について説明できる。
		15週	期末試験	用語の確認とRASISの考え方とその具体例（稼働率、認証、暗号化）を中心に確認する出題を解答できる。
		16週	答案返却など	試験に対する解説と来年以降の授業に対しての心構えを確認できる。

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	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	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。	3	後1,後2
		情報リテラシー	情報リテラシー	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	後1,後2
				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	後1,後2
				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	後2,後10
				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	後2,後10
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10,後13,後14
				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10,後13,後14
				基本的な暗号化技術について説明できる。	4	後14
				基本的なアクセス制御技術について説明できる。	4	後13
				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13,後14

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	100	0	0	0	0	0	100
基礎的能力	0	0	0	0	0	0	0
専門的能力	100	0	0	0	0	0	100
分野横断的能力	0	0	0	0	0	0	0