Tokuyama College	Year	2022	Course Title	Information Systems and Engineer ethics

Course Information

Course Code	0084	Course Category	Specialized / Compulsory
Class Format	Lecture	Credits	Academic Credit: 1
Department	Department of Computer Science and Electronic Engineering	Student Grade	4th
Term	Second Semester	Classes per Week	1
Textbook and/or Teaching Materials	（独）情報処理推進機構：情報セキュリティ読本　五訂版。他に，講義用のプリントを配布する。		
Instructor	Nitta Takayuki		

Course Objectives

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。

Rubric

	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。

Assigned Department Objectives

到達目標 A 1 到達目標 A 2
JABEE d-1

Teaching Method

Outline	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。
Style	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。
Notice	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。

Characteristics of Class / Division in Learning

☐ Active Learning	☐ Aided by ICT	☐ Applicable to Remote Class	☐ Instructor Professionally Experienced

Course Plan

			Theme	Goals
2nd Semester	3rd Quarter	1st	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。情報資産について、どのようなものがあるのか説明できる。
		2nd	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。 機密性，完全性，可用性について，それぞれの特性を区別して考えることができる。
		3rd	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。 ISMSのPDCAにおけるPlanにあたることであることを認識できる。
		4th	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。リスクアセスメントの実施手順を説明できる。
		5th	ISMSのフェーズ2(その２) 【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。
		6th	ISMSのフェーズ3とISMS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。
		7th	情報セキュリティの全体像 【事前事後学習の内容(0.5時間)】復習	ISMSにおけるPDCAの具体例を説明できるようになる。
		8th	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。
	4th Quarter	9th	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。

		10th	稼働率 【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。稼働率の計算の仕方を説明できる。
		11th	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	中間試験前までに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。
		12th	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。
		13th	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。
		14th	セキュリティに関する周辺技術 【事前事後学習の内容(1時間)】予習0.5時間，復習0.5時間	セキュリティに関連する周辺技術（ネットワーク，システムの構成方法）について，説明できる。
		15th	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。
		16th	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。

Evaluation Method and Weight (%)

	試験	発表	相互評価	態度	ポートフォリオ	その他	Total
Subtotal	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