津山工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	0091	科目区分	専門 / 選択
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	総合理工学科(情報システム系)	対象学年	4
開設期	前期	週時間数	2
教科書/教材	令和03年 情報セキュリティマネジメント合格教本（技術評論社）		
担当教員	寺元 貴幸		

到達目標

学習目的：情報セキュリティに関して技術的な仕組みを含めて概要を学習する。また，具体的な攻撃手口や防御方法についても事例を含めて学習する。

到達目標
1．情報セキュリティの要素とその重要性と説明できる。
2．情報セキュリティの確保に必要な基礎知識を説明できる。
3．攻撃を検知し解析するための仕組みを具体的に説明できる。
4．情報セキュリティの管理について説明できる。

ルーブリック

	優	良	可	不可
評価項目1	情報セキュリティの要素とその重要性について具体的に説明できる。	情報セキュリティの要素とその重要性について概念を説明できる。	情報セキュリティの要素とその重要性について例示できる。	左記に達していない。
評価項目2	情報セキュリティの確保に必要な基礎知識を具体的に説明できる。	情報セキュリティの確保に必要な基礎知識の概要を説明できる。	情報セキュリティの確保に必要な基礎知識を例示できる。	左記に達していない。
評価項目3	攻撃を検知し解析するための仕組みを具体的に説明できる。	攻撃を検知し解析するための仕組みの概念を説明できる。	攻撃を検知し解析するための仕組みを例示することができる。	左記に達していない。
評価項目4	情報セキュリティの管理について具体的に説明することができる。	情報セキュリティの管理について概要を説明できる。	情報セキュリティの管理について例示することができる。	左記に達していない。

学科の到達目標項目との関係

教育方法等

概要	一般・専門の別：専門　学習の分野：情報システム・プログラミング・ネットワーク 基礎となる学問分野：工学／情報科学，情報工学およびその関連分野／情報セキュリティ関連 学習教育目標との関連：本科目は総合理工学科学習教育目標「③基盤となる専門性の深化」に相当する科目である。 授業の概要：前半は情報セキュリティ全般の概要を学習する。後半は具体的な攻撃手口や防御手法そして関連する法律等に関して学習する。
授業の進め方・方法	授業の方法：各学生にテキストの担当を与え，その内容をまとめてPowerPointを作成し，その内容を１０分程度で発表する。また，関連する諸技術にやできごとについても補足説明する。また，理解が深まるよう担当者が演習問題を作成し，それを他の学生が解くことで内容の確認を行う。発表後に学生間で議論を行い相互の理解を深める。 成績評価方法： 2回の定期試験の結果に重みを付けて評価する（60%，後中：後末＝１：１）。 ・各試験はノートの持ち込みを許可しない。 ・各定期試験の結果が60点未満の人には補習，再試験により理解が確認できれば，点数を変更することがある。ただし，変更した後の評価は60点を超えないものとする。 演習・レポート課題で評価する（40%）。
注意点	履修上の注意：本科目を選択した者は，学年の課程修了のために履修（欠課時間数が所定授業時間数の３分の１以下）が必須である。また，本科目は「授業時間外の学修を必要とする科目」である。当該授業時間と授業時間外の学修を合わせて，１単位あたり４５時間の学修が必要である。授業時間外の学修については，担当教員の指示に従うこと。 履修のアドバイス：教科書に出てくる用語の意味や定義をよく確認し正確に理解すること。また，例題や各章の最後に用意されている演習問題を一つずつ自分で解いて内容をよく確認すること。 事前に行う準備学習として，基礎科目である情報リテラシー（１），情報ネットワーク基礎（２）の内容を復習しておくこと。 基礎科目：総合理工基礎(１年)，情報リテラシー（１），情報ネットワーク基礎（２），ディジタル工学（３）など 関連科目：eビジネス（5年），ネットワークセキュリティ（４）など 受講上のアドバイス：基礎知識に加え，現代社会で使われている通信機器,無線機器についても学習するので，日常生活とも関わっている事を念頭に起き興味を持って学習すること。遅刻は授業時間（＝2コマ）の4分の1（＝0.5コマ）刻みで取り扱う。

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

履修選択

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	ガイダンスおよび情報セキュリティの必要性を理解する
		2週	情報のCIA	情報のCIAについて理解する
		3週	情報資産・脅威・脆弱性	情報資産・脅威・脆弱性について理解する
		4週	サイバー攻撃（１） 不正サクセス，盗聴，なりすまし	サイバー攻撃（不正サクセス，盗聴，なりすまし）について理解する

		5週	サイバー攻撃（2） サービス妨害，ソーシャルエンジニアリング，その他攻撃	サイバー攻撃（サービス妨害，ソーシャルエンジニアリング，その他攻撃）について理解する
		6週	暗号	暗号の基礎を理解する
		7週	認証	認証の基礎を理解する
		8週	前期中間試験	前期中間試験を受ける
	2ndQ	9週	前期中間試験返却・解説 リスク分析	前期中間試験の問題と解答を理解する リスク分析の仕組みを理解する
		10週	セキュリティポリシ	セキュリティポリシの仕組みを理解する
		11週	マルウェア対策	マルウェア対策の仕組みを理解する
		12週	不正アクセス対策	不正アクセス対策の仕組みにを理解する
		13週	情報漏えい対策	情報漏えい対策について理解する
		14週	アクセス管理	アクセス管理について理解する
		15週	前期末試験	前期末試験を受ける
		16週	前期末験の返却と解答解説	前期末試験の問題および解答を理解する

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
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	
				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。	4	
				基本的なアクセス制御技術について説明できる。	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。	4	

評価割合

	試験	発表	相互評価	自己 評価	課題	小テスト	合計
総合評価割合	60	0	0	0	40	0	100
基礎的能力	0	0	0	0	0	0	0
専門的能力	60	0	0	0	40	0	100
分野横断的能力	0	0	0	0	0	0	0