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

科目基礎情報

科目番号	7141	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	ソーシャルデザイン工学専攻	対象学年	専1
開設期	後期	週時間数	2
教科書/教材	教材は適宜配布する		
担当教員	立川 崇之		

到達目標

1. 暗号技術および暗号に関わる数学について理解し説明できる。
2. 階層型通信プロトコルの基本概念とネットワークセキュリティ技術を理解し、説明できる。
3. マルウェアの動作、およびマルウェアの被害を防止する手法について理解し、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	暗号技術、暗号に関わる数学について理解し、適切な暗号の利用方法を説明できる。	暗号技術、暗号に関わる数学について説明できる。	暗号技術、暗号に関わる数学について説明できない。
評価項目2	階層型通信プロトコルの基本概念とネットワークセキュリティ技術を理解し、目的に応じた安全なネットワーク構成を提案できる。	階層型通信プロトコルの基本概念とネットワークセキュリティ技術を説明できる。	階層型通信プロトコルの基本概念とネットワークセキュリティ技術を説明できない。
評価項目3	マルウェアの動作、およびマルウェアの被害を防止する手法について理解し、具体的な実現方法を提案できる。	マルウェアの動作、およびマルウェアの被害を防止する手法について説明できる。	マルウェアの動作、およびマルウェアの被害を防止する手法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 (C)

教育方法等

概要	現代社会において、安全な情報通信を実現するために情報セキュリティ技術は必須である。特に情報を暗号化し他者に見られないようにする暗号技術、ネットワーク上での安全な通信を行うためのネットワークセキュリティ、悪意あるプログラムによる被害を防止するためのマルウェア検知、解析技術は重要である。本講義はこれらの高度なセキュリティ技術について理解する。
授業の進め方・方法	授業は主に e-learning を活用して行う。教材は Web サイトなどを通じて配布する。授業に関して分からないことがあれば教員に質問するほか、自主的に調査することも推奨する。
注意点	【成績評価の基準・方法】 本授業は他の教育機関の授業を遠隔で受講するものであり、成績評価の基準は授業を実施する教育機関に準じて行う（2021年度は課題にて評価を行った）。 【事前・事後学習】 事前学習として本科で学ぶレベルの基礎的な内容を復習した上で授業に臨むこと。また、事後学習として授業内で取り扱った項目について練習問題を解いたり、教材を熟読したりして理解を深めること。 【履修上の注意】 本科目は高知高専情報セキュリティコースの「情報代数」「暗号理論」「コンピュータネットワーク」「ネットワークセキュリティI, II」「情報工学実験II」の内容を理解している前提で進める。十分に理解していない者は、受講前に復習しておくことを強く勧める。

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	イントロダクション 暗号の歴史と概要	古典的暗号の歴史と概要について理解する。
		2週	暗号数学	合同式、フェルマーの小定理など初等整数論について理解する。
		3週	共通鍵暗号とデータ暗号化 公開鍵暗号と認証技術	共通鍵暗号、公開鍵暗号の技術について理解する。
		4週	暗号計算のソフトウェア、ハードウェア実装	ソフトウェア、ハードウェアに暗号を実装する技術について理解する。
		5週	暗号実装に対する脅威と対策技術	ソフトウェア、ハードウェアに暗号を実装した場合の脅威と対策技術について理解する。
		6週	通信における様々な脅威と安全に通信するための暗号技術	通信において安全に通信を行うための暗号技術について理解する。
		7週	データリンク層セキュリティ	階層型通信プロトコルのうち、データリンク層におけるセキュリティ技術について理解する。
		8週	ネットワーク層セキュリティI	階層型通信プロトコルのうち、ネットワーク層におけるセキュリティ技術について理解する。
	4thQ	9週	ネットワーク層セキュリティII	階層型通信プロトコルのうち、ネットワーク層におけるセキュリティ技術について理解する。
		10週	トランスポート層セキュリティ	階層型通信プロトコルのうち、トランスポート層におけるセキュリティ技術について理解する。
		11週	マルウェア感染	悪意あるソフトウェアであるマルウェアについて、その概要を理解する。
		12週	侵入検知	悪意ある者、あるいはソフトウェアがシステムに侵入したことを検知する技術について理解する。

		13週	メモリ破壊の脆弱性	不正なメモリの書き換えやメモリ操作である、メモリ破壊の脆弱性について理解する。
		14週	アクセス制御	適切に情報を管理するためのアクセス制御について理解する
		15週	マルウェア解析	悪意あるソフトウェアであるマルウェアに対する解析技術を理解する。
		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

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	15	45
分野横断的能力	10	0	0	0	0	5	15