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	ﾊｰﾄﾞｳｪｱｾｷｭﾘﾃｨ Ⅰ

科目基礎情報

科目番号	I5015	科目区分	専門 / 必修
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	前期	週時間数	2
教科書/教材	教科書は使わず、随時、授業資料等を配布する。		
担当教員	山田 隆行		

到達目標

1. IoTによって繋がれる様々な機器への脅威、脆弱性について理解する。
2. 代表的なハードウェアへの攻撃手法について理解する。
3. スマートカードのセキュリティについて知る。
4. 著作権保護技術として使用される電子透かしについて理解する。

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	IoTによりさまざまな機器がインターネット化されることを理解し、説明できる。	IoTによりさまざまな機器がインターネット化されることを理解できる。	IoTによりさまざまな機器がインターネット化されることを理解できる。
評価項目2	スマートカードの機能と役割を知り代表的なハードウェアへの攻撃手法を理解し、説明できる。	スマートカードの機能と役割を知り代表的なハードウェアへの攻撃手法を理解できる。	スマートカードの機能と役割や代表的なハードウェアへの攻撃手法を理解できない。
評価項目3	著作権保護技術として使用される電子透かしについて理解し、説明できる。	著作権保護技術として使用される電子透かしについて理解できる。	著作権保護技術として使用される電子透かしについて理解できない。
評価項目4	アルゴリズムを理解しプログラムを作成して、画像にデジタルデータを埋め込むことができる。	簡単なプログラムを作成して、画像にデジタルデータを埋め込むことができる。	プログラムの内容が理解できない。

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	現代社会では、IoTにより様々なモノがインターネット化され、収集されたビックデータがデジタル化され仮想化されることから、フィジカル（実世界）とサイバー（仮想世界）が融合した社会環境でのセキュリティを考える必要がある。本講義では、前半でフィジカル面でのセキュリティとして、IoT機器への脅威と脆弱性の事例について説明し、具体的なハードウエアへの攻撃としてサイドチャネル攻撃を上げ、スマートカードにおけるセキュリティについて考察する。後半では、サイバー空間でのセキュリティの考え方を示し、実習を通じて著作権保護技術として使用される電子透かしについて説明する。
授業の進め方・方法	座学による講義により知識を与え、実習に取り組むことで知識の理解を深め定着を図る。 実習では、LINUX上での基礎的なプログラム作成に取り組んでもらう。
注意点	【履修上の注意】 この科目を履修するにあたり、これまで他科目等で学んできた基礎的な知識並びにプログラミング能力の習得が望まれる。

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
前期	1stQ	1週	講義概論	本講義で扱う、ハードウェアセキュリティの概要とシラバスについて説明する。
		2週	IoTとその脅威、脆弱性についての事例	IoTの構成や動向、脅威事例及びIoTに感染するウイルス等について理解する。
		3週	ハードウェアへの攻撃 破壊攻撃	破壊攻撃と非破壊攻撃について学び具体的な破壊攻撃としてブートの破壊やチップセットの焼切りについて理解する。
		4週	非破壊攻撃	テンペスト攻撃とサイドチャネル攻撃の違いについて学び、代表的な非破壊攻撃手法について理解する。
		5週	スマートカードにおけるセキュリティ	スマートカードの機能と役割について学び、RSAに対する電力解析の事例について理解する。
		6週	サイバー空間でのセキュリティの考え方	情報のデジタル化とIoTによるモノのインターネット化について理解する。
		7週	デジタルデータの著作権保護	ディジタルデータの著作権を保護する電子透かしの概要と代表的な手法等について理解する。
		8週	UNIX上での画像（RAW画像）処理について	UNIX環境での画像の取り扱いについて、RAW画像の作成や画像の画素値の表示などのプログラムを作成する。
	2ndQ	9週	輝度分布、基本統計量	画像の輝度分布や基本統計量についてのプログラムを作成する。
		10週	画質の評価	透かし画像の評価（SN比）を計算するプログラムを作成する。
		11週	マスク処理	画像の特定の部分のみを表示するマスク処理を行うプログラムを作成し、透かしの埋込み量と画質について考察する。
		12週	画像の埋込み１	画像の埋込みの概要とアルゴリズムについて理解する。
		13週	画像の埋込み２	画像の埋込みプログラムを作成する。

		14週	画像の埋込み３	作成したプログラムの解説を聞き、アルゴリズムの理解を深め、プログラミング技術の向上を図る。
		15週	電子透かし（パッチワーク法）への攻撃	統計量を用いた電子透かし画像に対する攻撃及び復元法について理解する。
		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	情報リテラシー	情報リテラシー	コンピュータのハードウェアに関する基礎的な知識を活用できる。	4	
専門的能力	分野別の専門工学	情報系分野	計算機工学	整数・小数をコンピュータのメモリ上でディジタル表現する方法を説明できる。	4	
				基数が異なる数の間で相互に変換できる。	4	
				整数を2進数、10進数、16進数で表現できる。	4	
				小数を2進数、10進数、16進数で表現できる。	4	
				基本的な論理演算を行うことができる。	4	
				基本的な論理演算を組合わせて、論理関数を論理式として表現できる。	4	
				論理式の簡単化の概念を説明できる。	4	
				簡単化の手法を用いて、与えられた論理関数を簡単化することができる。	4	
				論理ゲートを用いて論理式を組合せ論理回路として表現することができる。	4	
				与えられた組合せ論理回路の機能を説明することができる。	4	
				組合せ論理回路を設計することができる。	4	
				フリップフロップなどの順序回路の基本素子について、その動作と特性を説明することができる。	4	
				レジスタやカウンタなどの基本的な順序回路の動作について説明できる。	4	
				与えられた順序回路の機能を説明することができる。	4	
				順序回路を設計することができる。	4	
				コンピュータを構成する基本的な要素の役割とこれらの間でのデータの流れを説明できる。	4	
				プロセッサを実現するために考案された主要な技術を説明できる。	4	
				メモリシステムを実現するために考案された主要な技術を説明できる。	4	
				入出力を実現するために考案された主要な技術を説明できる。	4	
				コンピュータアーキテクチャにおけるトレードオフについて説明できる。	4	
				ハードウェア記述言語など標準的な手法を用いてハードウェアの設計、検証を行うことができる。	3	
				要求仕様に従って、標準的なプログラマブルデバイスやマイコンを用いたシステムを構成することができる。	3	
			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	前1
				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	前1
				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	前5
				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	前2
				メディア情報の主要な表現形式や処理技法について説明できる。	4	
				ディジタル信号とアナログ信号の特性について説明できる。	4	
				情報を離散化する際に必要な技術ならびに生じる現象について説明できる。	4	

評価割合

	意欲	課題等	試験	合計
総合評価割合	10	10	80	100
基礎的能力	0	0	0	0
専門的能力	10	10	80	100