

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	情報工学実験Ⅱ
科目基礎情報					
科目番号	I4069		科目区分	専門 / 必修	
授業形態	実験・実習		単位の種別と単位数	履修単位: 4	
開設学科	SD 情報セキュリティコース		対象学年	4	
開設期	通年		週時間数	4	
教科書/教材	教材はオリジナルのものを随時配布する				
担当教員	高木 和久, 浦山 康洋, 立川 崇之, 長谷川 長一				
到達目標					
<ol style="list-style-type: none"> Linuxサーバの脆弱性およびその脆弱性が引き起こす脅威を確認することができる。 プラットフォーム診断を行い、脆弱性を発見することができる。 発見された脆弱性に対し、適切な対処をすることができる。 修復後のサーバに対し、既知の脆弱性がないことを保証することができる。 レポート(報告書)の作成方法を理解し、実践できる。 					
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		Linuxサーバの脆弱性およびその脆弱性が引き起こす脅威を確認し、説明できる。	Linuxサーバの脆弱性およびその脆弱性が引き起こす脅威を確認できる。	Linuxサーバの脆弱性およびその脆弱性が引き起こす脅威を確認できない。	
評価項目2		プラットフォーム診断を行い、脆弱性を発見し、説明できる。	プラットフォーム診断を行い、脆弱性を発見できる。	脆弱性を発見できない。	
評価項目3		発見された脆弱性について理解し、適切に対処できる。	発見された脆弱性に対し、適切に対処できる。	発見された脆弱性に対し、適切に対処できない。	
評価項目4		修復後のサーバに対し、既知の脆弱性がないことを保証し、説明できる。	修復後のサーバに対し、既知の脆弱性がないことを保証できる。	修復後のサーバに対し、既知の脆弱性がないことを保証できない。	
評価項目5		レポート(報告書)の作成方法を理解・実践し、論理的なレポートを作成できる。	レポート(報告書)の作成方法を理解し、実践できる。	レポート(報告書)の作成方法を理解できない。	
学科の到達目標項目との関係					
学習・教育到達度目標 (E)					
教育方法等					
概要	情報セキュリティ技術者として必須となるサーバおよびネットワークの構築技術や関連する情報セキュリティ技術についての学習および実践を行う。 本実験を通じて、サーバおよびネットワークへの理解を深め、サーバやネットワークのよりセキュアな構築・運用するために必要なモラル・知識と技術を培うことが目標である。 また、本科目では、セキュリティ実務およびセキュリティ教育への従事経験がある講師(長谷川長一氏 [株式会社ラック, JNSA教育部WGリーダー])による実践的な演習も実施する。				
授業の進め方・方法	与えられたテーマ(課題)について、個人もしくはグループで実習を行い、レポート(自己評価・報告書など)を提出する。 実習はRaspberryPi、およびデスクトップPC、ノートPCを用いて行う。 実施する実験のトピックは、状況により順序、内容が入れ替わることがある。				
注意点	<p>【成績評価の基準・方法】 レポート(報告書)評価を70%、課題評価を30%の割合で総合的に評価する。成績評価は中間と期末の各期間の評価の平均とする。学年の評価は学年末(後学期末)の評価とする。 レポート・課題については、実施内容の進行度および理解度を重視し、「与えられた仕様にしたがったサーバが構築できているか」「サーバが正しく稼働しているか」など到達目標に対する達成度を評価する。レポートは全ての回のものを提出しなければ単位を認めない。</p> <p>【事前・事後学習】 事前学習としては前回までに与えられた課題・実習の内容をサーバなどに構築して授業に臨むこと。また、事後学習として授業内で指示した課題・実習を次の授業までに完了しておくこと。</p> <p>【履修上の注意】 この科目を履修するにあたり、2年生のプログラミング基礎、3年生のプログラミング・コンピュータネットワーク・情報工学実験Ⅰの内容を十分に理解しておくこと。</p>				
授業の属性・履修上の区分					
<input type="checkbox"/> アクティブラーニング		<input checked="" type="checkbox"/> ICT 利用		<input type="checkbox"/> 遠隔授業対応	
<input checked="" type="checkbox"/> 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	実習環境構築 1	実習を行うための環境を構築できる。	
		2週	実習環境構築 2 情報セキュリティにまつわる法令および事例	実習を行うための環境を構築できる。 情報セキュリティにまつわる法令および事例について理解し、説明できる。	
		3週	情報モラルについて	情報セキュリティ技術者として持つべき情報モラルについて理解し、説明できる。	
		4週	サーバ監視1	ソフトウェアおよびツールを利用してサーバを攻撃することができる。	
		5週	サーバ監視2	ソフトウェアおよびツールを利用してサーバへの攻撃を監視することができる。	
		6週	パケットキャプチャ・解析	パケットキャプチャについて理解し、実践できる。また、キャプチャしたパケットの解析方法について理解し、実践できる。	
		7週	パケットキャプチャ実践 1	与えられた環境において、パケットキャプチャおよびパケット解析を実践できる。	
		8週	パケットキャプチャ実践 2	パケット解析結果を基に自作したパケットを用いて、通信(コマンド実行)できる。	

後期	2ndQ	9週	脆弱性診断ツール	脆弱性診断ツールの導入と基本的な操作を理解し、実践できる。
		10週	SQLインジェクション1	SQLインジェクションの概要について理解し、説明および診断ができる。
		11週	SQLインジェクション2	SQLインジェクションの対処方法について理解し、実践できる。
		12週	クロスサイトスクリプティング1	クロスサイトスクリプティングの概要について理解し、説明および診断できる。
		13週	クロスサイトスクリプティング2	クロスサイトスクリプティングの対処方法について理解し、実践できる。
		14週	OSコマンドインジェクション1	OSコマンドインジェクションの概要について理解し、説明および診断できる。
		15週	OSコマンドインジェクション2	OSコマンドインジェクションの対処方法について理解し、実践できる。
		16週		
	3rdQ	1週	Webサーバへの同時アクセス1	Webサーバの同時アクセスについて理解し、説明および診断ができる。
		2週	Webサーバへの同時アクセス2	Webサーバの同時アクセスの対処方法について理解し、実践できる。
		3週	SSHによる大量アクセス診断1	SSHによる大量アクセスについて理解し、説明および診断ができる。
		4週	SSHによる大量アクセス診断2	SSHによる大量アクセスの対処方法について理解し、実践できる。
		5週	セキュアなサーバ構築1	セキュアなWebサーバを構築することができる。
		6週	セキュアなサーバ構築2	セキュアなデータベースサーバを構築することができる。
		7週	マルウェア1	マルウェア（ランサムウェア）について理解し、説明することができる。
		8週	マルウェア2	マルウェア（ランサムウェア）について、実践（開発）でき、その対処方法を理解する。
4thQ	9週	不正アクセス1	不正アクセスについて理解し、診断できる。	
	10週	不正アクセス2	フォーマットにしたがって、不正アクセスに関する報告書を作成できる。	
	11週	外部講師（長谷川長一氏）による情報セキュリティ演習1	実践的な演習を通して、セキュリティの実務についての理解を深める。	
	12週	外部講師（長谷川長一氏）による情報セキュリティ演習2	実践的な演習を通して、セキュリティの実務についての理解を深める。	
	13週	外部講師（長谷川長一氏）による情報セキュリティ演習3	実践的な演習を通して、セキュリティの実務についての理解を深める。	
	14週	外部講師（長谷川長一氏）による情報セキュリティ演習4	実践的な演習を通して、セキュリティの実務についての理解を深める。	
	15週	レポート指導	レポート（報告書）の作成方法を理解し、実践できる。	
	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	工学実験技術(各種測定方法、データ処理、考察方法)	物理、化学、情報、工学における基礎的な原理や現象を明らかにするための実験手法、実験手順について説明できる。	3	
			実験装置や測定器の操作、及び実験器具・試薬・材料の正しい取扱を身に付け、安全に実験できる。	3	
			実験データの分析、誤差解析、有効桁数の評価、整理の仕方、考察の論理性に配慮して実践できる。	3	
			実験テーマの目的に沿って実験・測定結果の妥当性など実験データについて論理的な考察ができる。	4	
			実験ノートや実験レポートの記載方法に沿ってレポート作成を実践できる。	4	
			実験データを適切なグラフや図、表など用いて表現できる。	4	
			実験の考察などに必要な文献、参考資料などを収集できる。	4	
			実験・実習を安全性や禁止事項など配慮して実践できる。	4	
			個人・複数名での実験・実習であっても役割を意識して主体的に取り組むことができる。	4	
			共同実験における基本的ルールを把握し、実践できる。	4	
レポートを期限内に提出できるように計画を立て、それを実践できる。	4				
専門的能力	分野別の専門工学	情報系分野	代入や演算子の概念を理解し、式を記述できる。	4	
			プロシージャ(または、関数、サブルーチンなど)の概念を理解し、これらを含むプログラムを記述できる。	4	
			変数の概念を説明できる。	4	
			データ型の概念を説明できる。	4	
			制御構造の概念を理解し、条件分岐を記述できる。	4	
			制御構造の概念を理解し、反復処理を記述できる。	4	
			与えられた問題に対して、それを解決するためのソースプログラムを記述できる。	4	

			ソフトウェア生成に必要なツールを使い、ソースプログラムをロードモジュールに変換して実行できる。	4	
			与えられたソースプログラムを解析し、プログラムの動作を予測することができる。	4	
			主要な言語処理プロセッサの種類と特徴を説明できる。	2	
			ソフトウェア開発に利用する標準的なツールの種類と機能を説明できる。	3	
			プログラミング言語は計算モデルによって分類されることを説明できる。	2	
			主要な計算モデルを説明できる。	2	
			要求仕様に従って、標準的な手法により実行効率を考慮したプログラムを設計できる。	4	
			要求仕様に従って、いずれかの手法により動作するプログラムを設計することができる。	4	
			要求仕様に従って、いずれかの手法により動作するプログラムを実装することができる。	4	
			要求仕様に従って、標準的な手法により実行効率を考慮したプログラムを実装できる。	4	
	分野別の工学実験・実習能力	情報系分野【実験・実習能力】	情報系【実験・実習】	与えられた問題に対してそれを解決するためのソースプログラムを、標準的な開発ツールや開発環境を利用して記述できる。	4
ソフトウェア生成に利用される標準的なツールや環境を使い、ソースプログラムをロードモジュールに変換して実行できる。				4	
ソフトウェア開発の現場において標準的とされるツールを使い、生成したロードモジュールの動作を確認できる。				4	
フローチャートなどを用いて、作成するプログラムの設計図を作成することができる。				4	
問題を解決するために、与えられたアルゴリズムを用いてソースプログラムを記述し、得られた実行結果を確認できる。				4	
与えられた仕様に合致した組合せ論理回路や順序回路を設計できる。				3	
基礎的な論理回路を構築し、指定された基本的な動作を実現できる。				3	
論理回路などハードウェアを制御するのに最低限必要な電気電子測定ができる。				3	
標準的な開発ツールを用いてプログラミングするための開発環境構築ができる。				4	
要求仕様にあったソフトウェア(アプリケーション)を構築するために必要なツールや開発環境を構築することができる。				4	
要求仕様に従って標準的な手法によりプログラムを設計し、適切な実行結果を得ることができる。				4	

評価割合			
	レポート(報告書)	課題	合計
総合評価割合	70	30	100
基礎的能力	40	15	55
専門的能力	30	15	45
分野横断的能力	0	0	0