北九州工業高等専門学校	開講年度	令和02年度 (2020年度)	授業科目	専攻科特論II

科目基礎情報

科目番号	0089	科目区分	専門 / 選択
授業形態	演習	単位の種別と単位数	学修単位: 2
開設学科	生産デザイン工学専攻	対象学年	専2
開設期	前期	週時間数	2
教科書/教材	実施機関が指定または準備する教材		
担当教員	松久保 潤		

到達目標

講師が設定した目標を達成し、定められた基準により合格の評価を得ること。

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	不正アクセスの手法について、現実的な問題を把握し、課題について議論できる。	著名な不正アクセスの手法について理解できる。	著名な不正アクセスの手法について理解できない。
評価項目2	マルウェアを用いた不正アクセス法について理解し、種類ごとの適切な解析手法が分かる。	マルウェアの脅威について理解し、マルウェアの一般的な構造が分かる。	マルウェアの脅威について理解できず、マルウェアの一般的な構造が分からない。
評価項目3	不正アクセス対策の実際と運用について理解し、近年の認証技術の課題について議論できる。	従来の不正アクセス対策について理解し、従来の認証技術について説明できる。	従来の不正アクセス対策について理解できず、従来の認証技術について説明できない。

学科の到達目標項目との関係

専攻科課程教育目標、JABEE学習教育到達目標 SB① 共通基礎知識を用いて、専攻分野における設計・製作・評価・改良など生産に関わる専門工学の基礎を理解できる。
専攻科課程教育目標、JABEE学習教育到達目標 SC① 専門工学の実践に必要な知識を深め、実験や実習を通じて、問題解決の経験を積む。
専攻科課程教育目標、JABEE学習教育到達目標 SC② 機器類（装置・計測器・コンピュータなど）を用いて、データを収集し、処理できる。
専攻科課程教育目標、JABEE学習教育到達目標 SD① 専攻分野における専門工学の基礎に関する知識と基礎技術を総合し、応用できる。
専攻科課程教育目標、JABEE学習教育到達目標 SD② 専攻分野の専門性に加え、他分野の知識も学習し、幅広い視野から問題点を把握できる。
専攻科課程教育目標、JABEE学習教育到達目標 SE② 実験・実習・調査・研究内容について、日本語で論理的に記述し、報告・討論できる。
専攻科課程教育目標、JABEE学習教育到達目標 SF② 工業技術と社会・環境との関わりを理解し、社会・環境への効果と影響を説明できる。

教育方法等

概要	OSおよび各種アプリケーションソフトウェアおよびネットワークにおけるセキュリティを確保するだけでなく、暗号や認証プロトコルのセキュアな運用方法、および技術を習得することを目的とする。さらに制御システムやIoT、そして特に車載ネットワークのセキュリティ技術のついても詳解する。具体的には、サービス妨害（DoS攻撃）、脆弱性検査（ポートスキャン等）、侵入行為、ルート権限奪取、不正プログラム設置および実行（トロイの木馬等）等の不正アクセス方法、さらにマルウェア、特にボットやランサムウェア等およびそれらの対策手法としてのファイアーウォール、IDS、IPS、脆弱性検査システム、それらを統合したUTMの技術、SOCでの運用等の技術的要因だけでなく、ソーシャルエンジニアリング等の社会的、人的要因についても議論する。
授業の進め方・方法	地域連携による共同教育の講座で学修した結果、その成果が2単位に相当すると認められる場合には、専攻科特論Ⅱを学修したものとし2単位を認定する。設定された講座、レクチャーの内容により、本講座の場合、情報、通信、制御系の基礎が必要である。従って、参加者の専攻分野が限定されることがある。
注意点	企業における実習では社内規則を厳守しマナーに注意する事。

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	セキュリティインシデント対応演習	机上模擬実験でインシデントへの対応を行い、セキュリティ対策の基礎的な考え方を学ぶ。
		2週	概論（リスク、脅威、脆弱性、資産）	最近の事例、特に情報漏えいや不正アクセス事例について、その手口と原因について解説する。
		3週	ネットワークインフラセキュリティ（TCP/IP、ルータ/SW、FW等）	ネットワーク通信に用いられる基盤技術がもつ性質とセキュリティとの関係について学ぶ。
		4週	ネットワークセキュリティ（侵入検知、マルウエア対策、VPN等）	ファイアウォール、IDS、IPSの構造について解説する。
		5週	暗号	暗号システムの理論、および認証技術について詳解する。
		6週	セキュリティ運用・ログ運用管理	セキュリティリスク管理の手法を詳解する。また、インシデント対応時の手がかりとなるログの管理方法について詳解する。
		7週	セキュリティツール実習	ぜい弱性対策、開発支援などを目的としたセキュリティツールを用いて実習を行う。
		8週	セキュリティ監査・検査	具体的な対策法を用いて脆弱性を排除し、一定のセキュリティレベルを確保する活動について解説する。
	2ndQ	9週	インシデント対応(1)	インシデント発生時の対応を迅速かつ適切に行うためのプロセスについて詳解する。策
		10週	インシデント対応(2)	9週の続き
		11週	脆弱性管理	ソフトウェアの脆弱性を識別、分類、優先順位付け、修正、および緩和する手法について解説する。
		12週	セキュア開発(1)	システムの要件定義、設計、開発段階から全体の安全性を高める開発手法を学習する。
		13週	セキュア開発(2)	12週の続き
		14週	セキュア開発(3)	13週の続き
		15週	CTF、まとめ	サイバー攻撃への対処を学習する。加えて、講義全体のまとめを行う。
		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					
			レポート	合計	
総合評価割合			100	100	
基礎的能力			100	100	