

函館工業高等専門学校		開講年度	令和05年度 (2023年度)	授業科目	セキュリティ
科目基礎情報					
科目番号	0261		科目区分	専門 / 必修	
授業形態	授業		単位の種別と単位数	履修単位: 1	
開設学科	生産システム工学科		対象学年	5	
開設期	後期		週時間数	2	
教科書/教材	なし (テキスト配布)				
担当教員	小山 慎哉				
到達目標					
1. 情報セキュリティの概要について理解し説明できる。 2. 暗号技術および認証技術の原理を説明できる。 3. セキュリティに対する脅威 (ウィルス, 不正攻撃等) とその対策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	情報セキュリティの概要と, そのセキュリティ技術のフレームワークについて説明できる,	情報セキュリティの概要について説明できる.	情報セキュリティの概要について説明できない.		
評価項目2	暗号技術の暗号化と複合を理解し, 公開鍵暗号と共通鍵暗号, 各種認証技術の方式について説明できる.	暗号化の基本概念, 公開鍵暗号, 共通鍵暗号, 認証技術の概念について説明できる.	暗号化の基本概念, 公開鍵暗号, 共通鍵暗号, 認証技術の概念について説明できない.		
評価項目3	不正プログラムの内容とその脅威, 対策技術の方法を説明できる.	不正プログラムによるセキュリティ脅威とその対策技術を説明できる.	不正プログラムによるセキュリティ脅威とその対策技術を説明できない.		
学科の到達目標項目との関係					
函館高専教育目標 B					
教育方法等					
概要	情報化社会は人々の生活に大きな変化と飛躍をもたらす一方で, その重要な構成要素であるコンピュータやネットワークにおいて様々な脅威が発生し, 人々の生活に多大な影響を与えている. その脅威について考え, セキュリティを維持管理するための基本概念を理解し, 情報セキュリティ技術に関する知識を修得する. なお, 授業内容は公知の情報のみ限定されている.				
授業の進め方・方法	情報セキュリティに関する基礎技術と応用・運用管理技術について学習し, 情報理論を基に暗号技術の基礎を学習するとともに, 不正プログラムによるセキュリティの脅威とその対策について理解する. 関連科目: 情報ネットワーク基礎, 情報ネットワーク, Webシステム, 情報理論 なお, 授業の一部においては, 企業から派遣される現職エンジニアによる演習指導を行う予定である.				
注意点	教育到達目標評価: 中テスト (B,40%), 期末試験 (B,40%), レポート (B,20%)				
授業の属性・履修上の区分					
<input checked="" type="checkbox"/> アクティブラーニング		<input checked="" type="checkbox"/> ICT 利用		<input checked="" type="checkbox"/> 遠隔授業対応	
<input 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		
3rdQ	1週	・ガイダンス ・情報セキュリティ技術の概要	科目の位置づけ, 学習到達目標, 留意点を理解する 情報セキュリティ技術の概要を説明できる		
	2週	暗号技術の基礎	暗号化と復号の基礎となる情報数学を基に, 暗号技術の基礎を理解する		
	3週	共通鍵暗号方式とその応用例	DES, AESなどの共通鍵暗号方式について説明できる		
	4週	公開鍵暗号方式とその応用例	RSAなどの公開鍵暗号方式, およびハイブリッド方式について説明できる		
	5週	暗号技術に関する演習	演習を通じて暗号アルゴリズムを理解する		
	6週	電子署名とPKI, 認証の仕組み	電子署名とPKIについて説明できる		
	7週	情報ハイディング	情報ハイディングについて説明できる		
	8週	中テスト			
後期 4thQ	9週	答案返却・解答解説	試験問題を見直し, 間違った正答を求めることができる		
	10週	攻撃の種類	各攻撃の原理, 脆弱性の発見手法, および対策について理解できる		
	11週	トラフィックモニタリング	攻撃の解析手法について理解できる。またIDS/IPS機能を理解できる		
	12週	ネットワークの保護	AAAのコンセプト, IEEE802.1xの認証の仕組み, 脆弱性情報の管理について説明できる。		
	13週	トラフィックモニタリング演習	サーバログの解析手法について演習を通じて理解する。		
	14週	セキュリティポリシーと情報倫理	セキュリティポリシー, 情報倫理, 法制度について説明できる		
	15週	期末試験			
	16週	試験答案返却・解答解説	試験問題を見直し, 間違った問題の正答を求めることができる		
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
評価割合					

	試験	発表	相互評価	レポート	ポートフォリオ	その他	合計
総合評価割合	80	0	0	20	0	0	100
基礎的能力	40	0	0	10	0	0	50
専門的能力	40	0	0	10	0	0	50
分野横断的能力	0	0	0	0	0	0	0