

大島商船高等専門学校		開講年度	令和05年度 (2023年度)	授業科目	セキュリティマネジメント
科目基礎情報					
科目番号	0082		科目区分	専門 / 選択	
授業形態	授業		単位の種別と単位数	履修単位: 1	
開設学科	情報工学科		対象学年	5	
開設期	後期		週時間数	2	
教科書/教材	「徹底攻略 情報セキュリティマネジメント教科書 令和5年度」, 瀬戸美月他 (著), インプレス. 情報セキュリティ人材育成事業・セキュリティ教材. 参考図書 「マスタリング TCP/IP 情報セキュリティ編」 齋藤孝道 (著) オーム社, 「暗号と認証のしくみと理論がしっかりわかる教科書」 光成滋生 (著) 技術評論社.				
担当教員	高橋 芳明				
到達目標					
現代社会において、情報技術と通信ネットワーク技術は広く普及し、あらゆる場面でIT及びインターネットを活用することが当たり前になってきた。クレジットカードを使って買い物したり、大切な情報をクラウドに預けたりする機会も増えており、安全に情報をやりとりするための仕組みである暗号と認証について理解することは、情報技術者にとって必須となっている。また、近年、企業をはじめ様々な組織がサイバー攻撃を受け、情報漏洩やシステム障害などが頻繁に発生している。このような情報セキュリティの問題は、技術による対策で十分と思われがちであるが、適切な情報管理体制の整備や、社員の意識改善が重要であり、管理面の対策にも注力する必要がある。そこで本授業では、暗号と認証の技術及びセキュリティマネジメントに関する知識を学び、情報技術者として不可欠な安心・安全な情報セキュリティの技術と知識を修得することを目的とする。					
ループリック					
	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基本的な考え方を理解し、マルウェア、各種攻撃などの脅威を詳細に説明できる。	情報セキュリティの基本的な考え方を理解し、マルウェア、各種攻撃などの脅威を説明できる。	情報セキュリティの基本的な考え方を理解し、マルウェア、各種攻撃などの脅威を説明できない。		
評価項目2	共通鍵暗号、公開鍵暗号、認証のしくみを理解し、詳細に説明できる。	共通鍵暗号、公開鍵暗号、認証のしくみを理解し、説明できる。	共通鍵暗号、公開鍵暗号、認証のしくみを理解し、説明できない。		
評価項目3	情報セキュリティ対策、法務、マネジメントについて理解し、詳細に説明できる。	情報セキュリティ対策、法務、マネジメントについて理解し、説明できる。	情報セキュリティ対策、法務、マネジメントについて理解し、説明できない。		
評価項目4	学んだ知識を活用して、情報セキュリティに関する演習問題を解くことができる。	学んだ知識を活用して、情報セキュリティに関する初歩的な演習問題を解くことができる。	学んだ知識を活用して、情報セキュリティに関する演習問題を解くことができない。		
学科の到達目標項目との関係					
JABEE J(05) 本校 (1)-a 情報 (4)-a					
教育方法等					
概要	暗号と認証の技術及びセキュリティマネジメントに関する知識を学び、情報技術者として不可欠な安心・安全な情報セキュリティの技術と知識を修得することを目的とする。				
授業の進め方・方法	講義中心に行う。				
注意点	授業中は配布プリントの書込みを確実にし、次の授業までに復習すること。				
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 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		
後期	3rdQ	1週	情報セキュリティの基礎知識	情報セキュリティの目的と考え方、脅威と脆弱性、情報セキュリティ技術を理解し、説明できる。	
		2週	アルゴリズムと安全性	暗号におけるアルゴリズムと安全性について理解し、説明できる。	
		3週	共通鍵暗号、ワンタイムパッド	共通鍵暗号とワンタイムパッドについて理解し、説明できる。	
		4週	ストリーム暗号	ストリーム暗号について理解し、説明できる。	
		5週	ブロック暗号、AES	ブロック暗号とAESについて理解し、説明できる。	
		6週	鍵共有、公開鍵暗号	鍵共有、公開鍵暗号について理解し、説明できる。	
		7週	前半のまとめ	第1週～6週までの内容を理解し、説明できる。	
		8週	中間試験		
	4thQ	9週	RSA暗号	RSA暗号について理解し、説明できる。	
		10週	楕円曲線暗号	楕円曲線暗号について理解し、説明できる。	
		11週	ハッシュ関数	ハッシュ関数について理解し、説明できる。	
		12週	認証	情報セキュリティにおける認証について理解し、説明できる。	
		13週	情報セキュリティ管理と対策	情報セキュリティマネジメント、リスク分析と評価、情報セキュリティ対策について理解し、説明できる。	
		14週	法務、マネジメント	情報セキュリティ関連法規、システム監査について理解し、説明できる。	
		15週	まとめ	第1週～14週までの内容を理解し、説明できる。	
		16週	学年末試験		
評価割合					

	試験	提出物	合計
総合評価割合	70	30	100
基礎的能力	0	0	0
専門的能力	70	30	100
分野横断的能力	0	0	0