

久留米工業高等専門学校		開講年度	平成31年度 (2019年度)	授業科目	情報セキュリティ	
科目基礎情報						
科目番号	3S19		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	制御情報工学科		対象学年	3		
開設期	前期		週時間数	2		
教科書/教材	教科書: 菊池他 共著, IT Text ネットワークセキュリティ, オーム社 参考書: 八木他 共著, コンピュータネットワークセキュリティ, コロナ社					
担当教員	請園 智玲					
到達目標						
1. サイバーセキュリティの重要性の理解 2. サイバー攻撃の具体的驚異を知る 3. ネットワークセキュリティの具体的手法を知る						
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	
サイバーセキュリティの重要性を理解	サイバーセキュリティの重要性を理解し, 的確に説明できる.		サイバーセキュリティの重要性を理解し, 説明できる.		サイバーセキュリティの重要性を理解できない.	
サイバー攻撃の具体的驚異を知る	サイバー攻撃の方法を知り, 的確に説明できる.		サイバー攻撃の方法を知り, 説明できる.		サイバー攻撃の方法を理解できない.	
ネットワークセキュリティの具体的手法を知る	ネットワークセキュリティによる防御方法を知り, 的確に説明できる.		ネットワークセキュリティによる防御方法を知り, 説明できる.		ネットワークセキュリティによる防御方法を理解できない.	
学科の到達目標項目との関係						
教育方法等						
概要	コンピュータネットワークが普及する現在, セキュリティの専門家だけでなく, すべての技術者がネットワークセキュリティに関する基礎的な知識を習得する必要がある. 特に, 情報処理に携わる技術者は常に情報セキュリティの保全を念頭に置いておく必要がある. この授業ではネットワークセキュリティの基礎として, ソフトウェアの脆弱性や, サイバー攻撃の具体例を紹介すると同時に, その対処法である防御手段を併せて紹介する.					
授業の進め方・方法	教科書と参考書に沿って講義を行う. 関連科目: デジタル通信, 情報通信実験					
注意点	(1) 点数配分: 中間試験50%, 期末試験50%とする. (2) 評価基準: 100点法で評価し, 60点以上を合格とする. (3) 再試: 再試は行わない.					
授業計画						
		週	授業内容	週ごとの到達目標		
前期	1stQ	1週	情報システムとサイバーセキュリティ	情報システムの驚異とセキュリティの3要素を理解できる.		
		2週	ファイアウォール1	ポートスキャンとバッファオーバーフローを理解できる.		
		3週	ファイアウォール2	パケットフィルタリング, NAT, DMZを理解できる.		
		4週	マルウェア	マルウェアの定義とボットネットを理解できる.		
		5週	共通鍵暗号	共通鍵暗号の概念とセキュアハッシュを理解できる.		
		6週	公開鍵暗号1	公開鍵アルゴリズムの基礎と安全性を理解できる.		
		7週	公開鍵暗号2	DH鍵共有, RSA暗号が理解できる.		
		8週	公開鍵暗号3	デジタル署名を理解できる.		
	2ndQ	9週	認証技術	パスワード認証とデバイスを用いた生体認証を理解できる.		
		10週	PKIとSSL/TLS	PKI, SSL/TLSの原理と安全性が理解できる.		
		11週	電子メールのセキュリティ	電子メールの暗号化と認証が理解できる.		
		12週	Webセキュリティ1	Webシステムの脆弱性が理解できる.		
		13週	Webセキュリティ2	Webシステムの脆弱性対策が理解できる.		
		14週	コンテンツ保護とFintech	放送型暗号, 電子透かし, 暗号通貨技術が理解できる.		
		15週	プライバシー保護技術	匿名加工, プライバシー保護技術が理解できる.		
		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	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	情報技術の進展が社会に及ぼす影響、個人情報保護法、著作権などの法律について説明できる。	3	前1
			高度情報通信ネットワーク社会の中核にある情報通信技術と倫理との関わりを説明できる。	3	前1	
専門的能力	分野別の専門工学	情報系分野	情報通信ネットワーク	プロトコルの概念を説明できる。	4	
				プロトコルの階層化の概念や利点を説明できる。	4	
				ローカルエリアネットワークの概念を説明できる。	4	
				インターネットの概念を説明できる。	4	前12,前13
				TCP/IPの4階層について、各層の役割を説明でき、各層に関係する具体的かつ標準的な規約や技術を説明できる。	4	
主要なサーバの構築方法を説明できる。	4	前4				

				情報通信ネットワークを利用したアプリケーションの作成方法を説明できる。	4	前4
				ネットワークを構成するコンポーネントの基本的な設定内容について説明できる。	4	
				無線通信の仕組みと規格について説明できる。	4	
				有線通信の仕組みと規格について説明できる。	4	
				SSH等のリモートアクセスの接続形態と仕組みについて説明できる。	4	
				基本的なルーティング技術について説明できる。	4	
				基本的なフィルタリング技術について説明できる。	4	前2,前3
			その他の学習内容	コンピュータウイ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,前5,前11,前12,前13,前14
				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,前2,前3,前5,前11,前12,前13,前14,前15
				基本的な暗号化技術について説明できる。	4	前5,前6,前7,前8,前9
				基本的なアクセス制御技術について説明できる。	4	
				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4
				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。	1	前14,前15

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	100	0	0	0	0	0	100
基礎的能力	0	0	0	0	0	0	0
専門的能力	100	0	0	0	0	0	100