

佐世保工業高等専門学校		開講年度	平成30年度 (2018年度)	授業科目	情報通信特論
科目基礎情報					
科目番号	0104		科目区分	専門 / 選択	
授業形態	講義		単位の種別と単位数	学修単位: 2	
開設学科	電子制御工学科		対象学年	5	
開設期	通年		週時間数	1	
教科書/教材	PDFファイルおよびWordファイルを配布				
担当教員	中村 嘉男, 兼田 一幸, 手島 裕詞, 佐当 百合野				
到達目標					
1. コンピュータネットワークに用いられるプロトコルの概要を説明できる. (A4) 2. ネットワーク社会における各種セキュリティの脅威を説明できる. (A4) 1. コンピュータネットワークに用いられるプロトコルの概要を説明できる. (A4) 2. ネットワーク社会における各種セキュリティの脅威を説明できる. (A4)					
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 (到達目標1)		コンピュータネットワークに用いられるプロトコルの概要を説明できる。	コンピュータネットワークに用いられるプロトコルの概要をほぼ、理解し説明できる。	コンピュータネットワークに用いられるプロトコルの概要をあまり理解していません、説明できない。	
評価目標2 (到達目標2)		ネットワーク社会における各種セキュリティの脅威をよく理解し、説明できる。	ネットワーク社会における各種セキュリティの脅威をほぼ、理解し説明できる。	ネットワーク社会における各種セキュリティの脅威をあまり理解していません、説明できない。	
"評価項目3 (到達目標3)"		認証、暗号利用技術、アクセス制御等情報セキュリティに必要な基礎技術をよく理解し、説明できる。	認証、暗号利用技術、アクセス制御等情報セキュリティに必要な基礎技術をほぼ、理解し説明できる。	認証、暗号利用技術、アクセス制御等情報セキュリティに必要な基礎技術をあまり理解していません、説明できない。	
"評価目標4 (到達目標4)"		情報セキュリティマネジメントの重要性と必要性についてよく理解し、説明できる。	情報セキュリティマネジメントの重要性と必要性についてほぼ、理解し説明できる。	情報セキュリティマネジメントの重要性と必要性についてあまり理解していません、説明できない。	
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に関する基本的な事項(プロトコル, ネットワークの分類など), インターネット社会における各種攻撃手法, データ解析手法等を学ぶ。				
授業の進め方・方法	予備知識: プログラミングの基礎があること。情報科学の基礎(データ構造とアルゴリズム, ネットワーク基礎, OS基礎, データベース基礎)を理解していること。 講義室: 選択授業講義室 授業形式: 講義と演習, 演習レポート 学生が用意するもの: ノート				
注意点	評価方法: 中間・定期試験により評価し, 60点以上を合格とする。 自己学習の指針: 与えられた課題を調べる。講義の内容を確実に把握する。 オフィスアワー: 中村(火, 金 午後4-5時)				
授業計画					
		週	授業内容	週ごとの到達目標	
前期	1stQ	1週	ネットワークの基礎	情報セキュリティを学習するうえで必要なネットワークの要素について理解し、説明できる。	
		2週	情報セキュリティの必要性と定義	ネットワーク社会における情報セキュリティの必要性と重要性を理解し、説明できる。	
		3週	情報セキュリティの必要性と定義	情報セキュリティの脅威と対策を理解し、利用できる。	
		4週	"情報セキュリティの要素技術(認証、アクセス制御、ソフトウェアのセキュリティ)"	情報セキュリティ技術の全体像を理解し、説明できる。	
		5週	情報セキュリティの要素技術(暗号、ログ管理)	暗号利用、PKI、ログ管理のための基礎技術を理解し、利用できる。	
		6週	ネットワークの基本的な構成、ネットワークの脆弱性とリスク	TCP/IPとネットワークの基本的な構成、課題とリスク等について理解し、説明できる。	
		7週	情報セキュリティにおけるファイアウォールの位置づけと機能	情報セキュリティ対策、ファイアウォールの役割と仕組みについて理解し、利用できる。	
		8週	中間試験		
	2ndQ	9週	ネットワークセキュリティを構成する要素技術	NAT機能、VPN機能、IDS/IPSの役割と仕組みについて理解し、利用できる。	
		10週	無線LAN環境(規格、暗号化、認証、その他の機能など)	利便性と問題点、セキュリティ技術の仕組みと必要性を理解し、説明できる。	
		11週	無線LANの脆弱性	wep, wpa, wpa2規格の脆弱性を理解し、より安全に使用する方法を説明できる。	
		12週	Webアプリケーションセキュリティ	Webアプリケーションのセキュリティ、仕組み及びセキュリティ対策の概要を理解し、説明できる。	
		13週	"Webアプリケーションに対する代表的な攻撃、SQLインジェクション攻撃"	Webアプリケーションに対する代表的な攻撃、SQLインジェクション攻撃を理解し、利用できる。	
		14週	クロスサイト・スクリプティング攻撃、Webアプリケーション開発時の対策	クロスサイト・スクリプティング攻撃、Webアプリケーションにおける設計・実装時の対策を理解し、利用できる。	
		15週	バッファオーバーフローによるデータ破壊の危険性	バッファオーバーフローの危険性を理解し、説明できる。	
		16週	期末試験		

後期	3rdQ	1週	情報セキュリティマネジメントシステムの基礎知識 1	情報セキュリティ対策の有効性評価および適合性の維持活動を理解し、説明できる。
		2週	情報セキュリティマネジメントシステムの基礎知識 2	情報セキュリティ対策の有効性評価および適合性の維持活動を理解し、説明できる。
		3週	情報セキュリティにおけるリスクアセスメントとリスク対応（総合演習）	"情報セキュリティの対策を効果的に導入および実践するため、リスクアセスメントとリスク対応方法について演習を通じて学習し、利用できる。"
		4週	サイバー攻撃におけるマルウェア感染	マルウェア感染を中心としたサイバー攻撃の概要、観測の重要性を理解し、説明できる。
		5週	ハニーポットでのデータ収集	サイバー攻撃の形態、攻撃の観測について学習し、説明できる。
		6週	ハニーポットの観測環境の手法とデータ解析について理解し、説明できる。	解析環境について理解し、利用できる。
		7週	ハニーポット環境におけるデータ収集	データ収集手法について理解し、説明できる。
		8週	中間試験	
	4thQ	9週	Webクライアントへの攻撃	Webクライアントへのマルウェア感染攻撃の特性を理解し、説明できる。
		10週	Webクライアントへの攻撃の観測・解析	Webクライアントへの攻撃の観測・解析方法を理解し、説明できる。
		11週	サーバへの攻撃とデータ解析	Webサーバに対する代表的攻撃を理解し、観測について説明できる。
		12週	パスワードクラッキング	辞書攻撃、フォースアタックの手法の理解と、安全なパスワードについて説明できる。
		13週	フォレンジックとは	デジタルフォレンジックの一般的手法について理解し、説明できる。
		14週	削除データ等の復元方法	HDD等の削除データの復元手法を理解し、説明できる。
		15週	各種ブラウザ等のオペレーション作業の復元	ブラウザ等のオペレーション作業の復元について理解し、説明できる。
		16週	期末試験	

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	70	0	0	0	0	30	100
基礎的能力	0	0	0	0	0	0	0
専門的能力	70	0	0	0	0	30	100
分野横断的能力	0	0	0	0	0	0	0