

旭川工業高等専門学校		開講年度	令和02年度 (2020年度)		授業科目	情報セキュリティ概論	
科目基礎情報							
科目番号	0032		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	生産システム工学専攻		対象学年		専2		
開設期	前期		週時間数		2		
教科書/教材	「サイバーセキュリティ人材育成事業(K-SEC)」により作成された教育コンテンツ(K-SEC教材) など						
担当教員	笹岡 久行						
到達目標							
1. 情報セキュリティの三大要素を説明することができる。 2. 代表的な暗号化アルゴリズムを説明することができる。 3. ファイヤーウォール等の情報セキュリティ機器の働きを説明することができる。 4. 最新のセキュリティ技術に関心を持ち、自ら情報収集することができる。							
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三大要素自らを説明することができる。		情報セキュリティの三大要素について関心を持ち、資料を見ながら説明することができる。		情報セキュリティの三大要素について説明することができない。		
評価項目2	代表的な暗号化アルゴリズムについて説明し、自ら暗号化・復号化することができる。		代表的な暗号化アルゴリズムについて説明することができる。		代表的な暗号化アルゴリズムについて説明することができない。		
評価項目3	情報セキュリティ機器に関心を持ち、自ら説明することができる。		情報セキュリティ機器に関心を持ち、資料を見ながら説明することができる。		情報セキュリティ機器について説明することができない。		
評価項目4	最新のセキュリティ技術に関心を持ち、自ら情報収集することができる。		資料や教材にあるセキュリティインシデントについては説明することができる。		資料や教材にあるセキュリティインシデントについては説明することができない。		
学科の到達目標項目との関係							
学習・教育到達度目標 (生産システム工学専攻の教育目標) 学習・教育到達度目標 (専攻科の教育目標) JABEE D-1 JABEE D-2 JABEE基準 (d)							
教育方法等							
概要	暗号化アルゴリズムやセキュリティ機器に関心を持ち、それらに関する基礎事項を身につける。						
授業の進め方・方法	教科書や配布資料を用いて、代表的な定理を説明する。さらに例題を通して各種手法を説明する。その定着のため、演習問題を解いてもらう。また、プログラミング言語「Python」によりコンピュータを用いた演習を行う。						
注意点	・教育プログラムの学習・教育到達目標において該当する項目は、D-1、D-2とする。 ・自学自習時間(60時間)は、日常の授業(30時間)に対する予習復習、レポート課題の課題作成時間、試験のための学習時間を総合したものとする。 ・評価については、合計点数が60点以上で単位修得となる。その場合、各到達目標項目の到達レベルが標準以上であること、教育プログラムの学習・教育到達目標の各項目をみたしたことが認められる。 ・単に授業に出席するだけでなく、演習問題等を積極的に自分の力で解くようにすること。これにより、種々の手法が身に付き、各種定理等の意味の理解が一層深くなる。また、単に計算方法を覚えるだけでなく、導出された値が意味していることを深く考察する姿勢が必要である。 ・「サイバーセキュリティ人材育成事業(K-SEC)」により作成された教育コンテンツ(K-SEC教材)を使用する。						
授業計画							
		週	授業内容		週ごとの到達目標		
前期	1stQ	1週	1次元データの整理		平均値や中央値を算出することができる。コンピュータを利用してデータを整理する方法を説明することができる。		
		2週	推測統計の基本 1次元の離散型確率変数		簡単な離散型の確率の演習問題を解くことができる。		
		3週	ベイズの定理		ベイズの定理を説明することができる。		
		4週	情報量		自己情報量、平均情報量および相互情報量の計算をすることができる。		
		5週	情報セキュリティとは		情報セキュリティの三大要素について説明することができる。		
		6週	セキュリティ要素技術①		共通鍵暗号方式と公開鍵暗号方式の違いについて説明することができる。		
		7週	セキュリティ要素技術②		RSA暗号方式について計算方法を説明することができる。		
		8週	中間試験		学んだ知識の確認ができる。		
	2ndQ	9週	試験答案の返却と解説 通信方法①		学んだ知識の再確認と修正ができる。 SSLの仕組みについて説明することができる。		
		10週	通信方法②		SSHについて説明することができる。		
		11週	通信方法③		無線LANのセキュリティの問題点について説明できる。		
		12週	マルウェア対策		マルウェア対策の基本的な方法について説明することができる。		
		13週	演習①		Pythonのプログラムを用いたセキュリティ演習を実施することができる。		
		14週	演習②		Pythonのプログラムを用いたセキュリティ演習を実施することができる。		
		15週	期末試験		学んだ知識の確認ができる。		
		16週	試験答案の返却と解説		学んだ知識の再確認と修正ができる。		

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	レポート	合計	
総合評価割合		60	40	100	
基礎的能力		0	0	0	
専門的能力		60	30	90	
分野横断的能力		0	10	10	