旭川工業高等専門学校	開講年度	令和04年度 (2022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	「入門サイバーセキュリティ 理論と実験」（面 和成 著，コロナ社）「Pythonでいかにして暗号を破るか」（Al Sweigart著，ソシム社），「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	情報機器や通信プロトコルに関心を持ち，自ら説明することができる。	情報機器や通信プロトコルに関心を持ち，資料を見ながら説明することができる。	情報機器や通信プロトコル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)

教育方法等

概要	情報セキュリティ、特に暗号化アルゴリズムに関心を持ち，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」などを用いてコンピュータを用いた情報セキュリティ演習を行う。
注意点	・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はなく，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。 ・「サイバーセキュリティ人材育成事業(K-SEC)」により設置されたサイバーセキュリティ演習室の設備を使用する。

授業の属性・履修上の区分

☑ アクティブラーニング	☑ ICT 利用	☑ 遠隔授業対応	□ 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
前期	1stQ	1週	Pythonの基礎（1）	プログラミング言語「Python」の基本的な文法を説明することができる。
		2週	Pythonの基礎（2）	この後の演習を円滑にすすめるにあたり，簡単なプログラムを作成することができる。
		3週	1次元データの整理 1次元の離散型確率変数	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。
		4週	情報量とエントロピ	平均情報量を計算することができる。また、情報通信において必要になる結合エントロピや相互情報量を計算することができる。
		5週	ネットワークプロトコル　1	TCP/IPの特徴を説明することができる。OSI参照モデルについて説明することができる。IPアドレスについて、説明することができる。
		6週	ネットワークプロトコル　2	各ネットワークサービスの概要を説明することができる。
		7週	セキュリティ要素技術　1	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。
		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 セキュリティ要素技術　2	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。
		10週	暗号１「シーザー暗号」「転置式暗号」	シーザー暗号化のアルゴリズムを説明することができる。転置暗号化のアルゴリズムを説明することができる。
		11週	暗号２「ファイルの暗号化と復号」	転置暗号化を応用し，ファイルの暗号化・復号化などに利用することができる。

		12週	暗号３「素数の検索と生成」	暗号化における素数の重要性を知り，素数生成のアルゴリズムを説明することができる。
		13週	暗号４「公開鍵暗号の鍵生成」	公開鍵暗号における「鍵」のアルゴリズムを説明することができる。与えられたプログラムを読み解き，鍵を生成することができる。
		14週	情報セキュリティ演習	情報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