福島工業高等専門学校	開講年度	令和02年度 (2020年度)	授業科目	情報科学論

科目基礎情報

科目番号	0008	科目区分	専門関連 / 必修
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	専攻科（各専攻共通：一般科目・専門関連科目）	対象学年	専1
開設期	後期	週時間数	2
教科書/教材	プリント配布		
担当教員	小泉 康一		

到達目標

①情報量、エントロピーの意味が理解し、簡単な確率システムのエントロピーが計算できる。②グラフ理論を通してアルゴリズムの概念を理解する。③コンピュータネットワークの基礎について理解する。④情報セキュリティのための暗号システムの基礎概念を理解する。

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
情報量、エントロピーの意味が理解し、簡単な確率システムのエントロピーが計算できる。	各授業項目の内容を理解し、応用できる。	各授業項目の内容を理解している。	各授業項目の内容を理解していない。
グラフ理論を通してアルゴリズムの概念を理解する。	各授業項目の内容を理解し、応用できる。	各授業項目の内容を理解している。	各授業項目の内容を理解していない。
コンピュータネットワークの基礎について理解する。	各授業項目の内容を理解し、応用できる。	各授業項目の内容を理解している。	各授業項目の内容を理解していない。
情報セキュリティのための暗号システムの基礎概念を理解する。	各授業項目の内容を理解し、応用できる。	各授業項目の内容を理解している。	各授業項目の内容を理解していない。

学科の到達目標項目との関係

教育方法等

概要	広く一般のエンジニア、研究者等として知っておくべき情報理論、数学的な情報の解析法の基礎について解説する。情報通信理論の話題についても取り上げる。
授業の進め方・方法	期末試験を実施する。単位追認試験は、小テストをすべて受験し授業内に明示する規定点数に達した者のうち、試験日までに実施する数回の指導をすべて受けた者のみ受験できる。この科目は学修単位科目のため、事前、事後の学習の確認として、定期的に小テストを実施する。
注意点	数学的な内容を多く含むので、復習をして、各事項を一つ一つ確実に理解していくことが重要である。 自学自習の確認方法：定期的に小テストを行う。 参考書 ・情報理論入門，アブラムソン（宮川洋訳），好学社. ・インターネット工学，後藤滋樹，外山勝保，コロナ社. ・工学のための離散数学，黒澤馨，数理工学社.

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	情報量とエントロピー1	対数と確率論の基礎，それらの計算法の復習 完全情報系、情報量の定義
		2週	情報量とエントロピー2	情報源とエントロピー
		3週	情報数学1 （情報量とｴﾝﾄﾛﾋﾟｰの小ﾃｽﾄ）	グラフとは何か オイラー閉路
		4週	情報数学2	ハミルトン閉路，木
		5週	情報数学3	全域木，根つき木 最短路，DIJKSTRAアルゴリズム1
		6週	情報数学4 ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ1	DIJKSTRAアルゴリズム2 OSI参照モデルとプロトコル
		7週	ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ2 （グラフ理論の小テスト）	LANにおける通信
		8週	ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ3	ルータと経路制御
	4thQ	9週	ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸ4	インターネットの応用 TCP/IPの概要
		10週	暗号理論 （ｺﾝﾋﾟｭｰﾀﾈｯﾄﾜｰｸの小テスト）	秘密鍵暗号方式と公開鍵暗号方式の違い シフト暗号の暗号化、復号化
		11週	整数論 1	剰余環Znについて mod演算，ユークリッド互除法とその演習
		12週	整数論 2 公開鍵暗号 1	拡張ユークリッド互除法を使った逆数導出法 RSA暗号系
		13週	公開鍵暗号 2 量子暗号　1	RSA暗号系とその演習 量子暗号BB84の理論について
		14週	量子暗号　2	敵がいる場合の量子暗号について
		15週	まとめ （暗号理論の小テスト）	授業内容のまとめ
		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

評価割合

	試験	小テスト	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	60	40	0	0	0	0	100
基礎的能力	30	40	0	0	0	0	70

専門的能力	30	0	0	0	0	0	30
分野横断的能力	0	0	0	0	0	0	0