情報理論 (Information Theory)	４年・通年・２学修単位（β）・必修 情報工学科・担当　岡村 真吾

〔準学士課程(本科 1-5 年) 学習教育目標〕	〔システム創成工学教育プログラム 学習・教育目標〕	〔JABEE 基準〕
(2)	B-2(80%), D-1(20%)	(c), (d-2a)

〔講義の目的〕

シャノンの通信理論に基づく理論体系について学ぶ。さらに、符号理論や暗号理論の基礎についても学ぶ。

〔講義の概要〕

本科目では、情報や通信の数学的な扱い方について学ぶ。各種理論の説明に加え、具体例の紹介や演習問題を行い、理解を深めていく。

〔履修上の留意点〕

本科目の内容は確率論を基礎とするが、確率論についての説明は応用数学での内容との重複を避けるためにここでは省略する。応用数学でしっかりと勉強しておくこと。また、一部教科書には載っていない内容も扱うため、ノートを取ることをお薦めする。ただし、単に板書をそのまま書き写すのではなく、内容を理解し、自分なりに要約や補足をすること。レポートは、参考文献や他人の意見の単なるコピーではなく、自分自身による考えや作業の結果などが含まれるようにすること。

〔到達目標〕

前期中間試験：情報量とエントロピーについて理解する。
前期期末試験：通信路のモデル、通信路容量、高効率の符号化について理解する。
後期中間試験：誤り検出と誤り訂正について理解する。
学年末試験：連続量の情報量と暗号の基礎について理解する。

〔評価方法〕

定期試験の成績（75%）とレポート等の課題（25%）により評価する。
（ただし、課題の出題がなかった場合は定期試験の成績（100%）で評価する。）

〔教科書〕

「わかりやすいディジタル情報理論」、塩野充 著、オーム社

〔参考書〕

「ビギナーズガイド情報理論」、井上純一 著、プレアデス出版
「通信の数学的理論」、クロード・E. シャノン、ワレン・ウィーバー 著、植松友彦 訳、筑摩書房

〔関連科目〕

応用数学で学ぶ確率論が本科目の基礎となる。本科目で学んだ内容は、信号処理やパターン情報処理につながる。

講義項目・内容

週数	講義項目	講義内容	自己評価＊
第 1 週	情報量	情報量の定義について学ぶ。	
第 2 週	エントロピー（1）	エントロピーについて学ぶ。	
第 3 週	エントロピー（2）	結合エントロピーと条件付きエントロピーについて学ぶ。	
第 4 週	相互情報量	相互情報量について学ぶ。	
第 5 週	通信系のモデル	シャノンの通信系のモデルについて学ぶ。	
第 6 週	情報源	マルコフ情報源について学ぶ。	
第 7 週	通信路	通信路のモデルについて学ぶ。	
第 8 週	通信路容量（1）	通信路容量の定義について学ぶ。	
第 9 週	通信路容量（2）	通信路容量の計算について学ぶ。	
第 10 週	符号化の基礎知識（1）	冗長度について学ぶ。	
第 11 週	符号化の基礎知識（2）	一意的復号可能と瞬時復号可能について学ぶ。	
第 12 週	符号化の基礎知識（3）	符号化の効率について学ぶ。	
第 13 週	高効率の符号化（1）	シャノン・ファノの符号化法について学ぶ。	
第 14 週	高効率の符号化（2）	ハフマンの符号化法について学ぶ。	
第 15 週	高効率の符号化（3）	シャノンの第１基本定理について学ぶ。	
	前期期末試験		
第 16 週	雑音のある場合の符号化（1）	シャノンの第２基本定理について学ぶ。	
第 17 週	雑音のある場合の符号化（2）	誤り検出、誤り訂正の原理について学ぶ。	
第 18 週	誤り訂正可能な符号化法（1）	長方形符号と三角形符号について学ぶ。	
第 19 週	誤り訂正可能な符号化法（2）	ハミング符号について学ぶ。	
第 20 週	誤り訂正可能な符号化法（3）	巡回符号の生成手順について学ぶ。	
第 21 週	誤り訂正可能な符号化法（4）	巡回符号の誤りの検出と訂正について学ぶ。	
第 22 週	連続量の情報（1）	連続量のエントロピーについて学ぶ。	
第 23 週	連続量の情報（2）	連続量の相互情報量について学ぶ。	
第 24 週	暗号系のモデル	暗号系のモデルについて学ぶ。	
第 25 週	暗号の安全性	暗号の安全性について学ぶ。	
第 26 週	暗号系の分類	秘密鍵暗号、公開鍵暗号について学ぶ。	
第 27 週	ディジタル署名	ディジタル署名について学ぶ。	
第 28 週	暗号の例（1）	素因数分解問題の困難性に基づく暗号について学ぶ。	
第 29 週	暗号の例（2）	離散対数問題の困難性に基づく暗号について学ぶ。	
第 30 週	秘密分散法	秘密分散法について学ぶ。	
	学年末試験		

＊4：完全に理解した，3：ほぼ理解した，2：やや理解できた，1：ほとんど理解できなかった，0：まったく理解できなかった．
（達成） （達成） （達成） （達成） （達成）