電気通信大学　平成20年度シラバス

授業科目名	ネットワーク基礎論2		
英文授業科目名	Mathematical Foundations of Network and Information 2		
開講年度	2008年度	開講年次	
開講学期	後学期	開講コース・課程	博士前期・後期課程
授業の方法	講義	単位数	2
科目区分	情報システム学研究科-情報ネットワークシステム学専攻-専門科目		
開講学科・専攻	情報ネットワークシステム学専攻		
担当教官名	小川　朋宏		
居室	IS-821		

公開E-Mail	授業関連Webページ
ogawa@is.uec.ac.jp	

【講義の狙い，目標】

(a) 狙い：情報理論は，通信の効率・信頼性・安全性に関する数学的理論として，60 年前にシャノンによって創始された．情報理論を基礎として，データ圧縮・誤り訂正・暗号は，現代の情報化社会において必須の技術となっている．例えば，コンピュータ，携帯電話などの情報通信機器の動作には，誤り訂正技術が不可欠である．また，テキスト，動画などの保存・効率的配信のために，様々なデータ圧縮技術が用いられている．この科目では，情報理論に基づく暗号理論の解説を目標にして，ややアドバンストな情報理論のコースを提供する．

(b) 目標：情報理論の基礎を習得し，データ圧縮，誤り訂正符号などの様々な符号化の効率が，エントロピーをはじめとする情報量によって規定されることを学ぶ．さらに，暗号の安全性について，情報理論に基づく暗号と，計算量理論に基づく暗号の違いを理解し，代表的な情報理論的暗号プロトコルについて学ぶ．

【内容】

1. 情報量とその性質
- エントロピー，相対エントロピー，相互情報量
- チェインルール，情報量の単調性，十分統計量
2. データ圧縮
- 系列のタイプ，標準系列
- 固定長符号化，情報源符号化定理とエントロピー
- （可変長符号化，語頭符号，クラフトの不等式，可変長情報源符号化定理）
3. 情報理論と大偏差理論
- 大偏差理論，Sanovの定理
- 仮説検定，Steinの補題と相対エントロピー
4. 通信路符号化
- 通信路容量，通信路符号化定理と相互情報量

- （誤り訂正符号）
5. 情報理論的暗号理論
- 秘密鍵暗号と公開鍵暗号，（量子暗号）
- 情報理論に基づく暗号と計算量理論に基づく暗号
- 盗聴通信路符号化定理
- 秘密分散法，ビットコミットメント

ただし，（）内は適宜省略する．

【教科書，参考書】

教科書は指定しない．参考書として，例えば以下の文献を挙げる．
韓太舜・小林欣吾，情報と符号化の数理，培風館，1999.
T. M. Cover, J. A. Thomas, Elements of Information Theory, Wiley, 2006.
岡本龍明・山本博資，現代暗号，産業図書，1997.

【予備知識】

確率論に関する初歩的知識

【演習】

【成績評価方法及び評価基準】

レポート，出席状況などにより評価する．

【その他】

注意：基礎科目の「情報ネットワーク学基礎２」と名称が似ていますが，こちらは専門科目なので混同しないように注意してください．

情報理論は統計学，学習理論，計算機科学，制御理論，物理学などの様々な分野と関係しています．自身の研究への応用も考えてみましょう．