

電気通信大学 平成20年度シラバス

授業科目名	符号化の数理		
英文授業科目名	Mathematics of Information and Coding		
開講年度	2008年度	開講年次	
開講学期	前学期	開講コース・課程	博士前期課程
授業の方法	講義	単位数	2
科目区分	電気通信学研究科-情報通信工学専攻-基礎科目		
開講学科・専攻	情報通信工学専攻		
担当教官名	小林 欣吾、山口 和彦		
居室	総合研究棟921(小林)、総合研究棟919(山口)		

公開E-Mail	授業関連Webページ

<p><b>【主題および達成目標】</b></p> <p>多利用者の存在するネットワークシステムを流れる「情報」を眺めるための数理的視点を確立して、効率性、信頼性、安全性を高めるための符号化について理解を深める。</p> <p>「情報」の収集，伝送，加工に必然的に伴う符号化の数理的構造を解説する．数論，離散数学などの知識をもとにしたデータ変換法やその符号理論・暗号理論等への応用，乱数生成，秩序生成などをトピックスとして講義する．</p> <p>データ圧縮，データ探索，ソーティングなどをとおして情報理論と計算機科学の関連が理解できるようにし，「情報」を眺める数理的視点を確立することが目標である．とくに，組み合わせ的情報構造の数え上げの手法と，その符号化法に焦点をあてて解説する．</p>
--

<p><b>【前もって履修しておくべき科目】</b></p> <p>なし</p>
--

<p><b>【前もって履修しておくことが望ましい科目】</b></p> <p>離散数学，情報理論など</p>
--

<p><b>【教科書等】</b></p> <p>H20年度は K. J. Ray Liu他著</p>
--

## 電気通信大学 平成20年度シラバス

Multimedia Fingerprinting Forensics for Traitor Tracing, Hindawi Publishing などを利用する

### 【授業内容とその進め方】

#### (a) 授業内容

- ・符号化の数理的構造
  - ・暗号・セキュリティの問題を理解するための数学的基礎、
  - ・数論的暗号理論、情報理論的暗号理論、共通鍵暗号、公開鍵暗号
  - ・ネットワーク符号化（効率化とセキュリティ）
  - ・盗聴通信路問題、セキュリティプロトコル、署名認証技術、
  - ・暗号セキュリティ応用、標準化、ネットワークセキュリティ技術、
  - ・ステガノグラフィと電子透かしの基礎、
- 等から話題を選び講義する。

H 2 0 年度は主に山口が担当し電子透かし、電子指紋なかでも結託耐性符号について講義する。

#### (b) 授業の進め方

授業中に演習を行うことがある、レポート用紙を持参すること

#### (c) 授業時間外の学習（予習・復習等）について

- ・予習は指示があった場合に行えばよい。
  - ・授業内容の復習は必須である。
- 通常の大学院生の場合、宿題レポートと合わせて授業時間の2倍程度の時間が見込まれる。

### 【成績評価方法及び評価基準(最低達成基準を含む)】

教室での議論，レポートで判断する．必要であれば試験をする．

- ・電子透かしを取り巻く情報セキュリティ分野の社会的な状況を理解し，自分の意見を含めて論じられること．
- ・各種方式，プロトコルの機能特徴と，具体的なアルゴリズムがほぼ理解できていること

が合格の基準である．

### 【オフィスアワー：授業相談】

月曜日 - 金曜日12:30 - 16:30の在室時が望ましい。  
会えない場合は、E-mailなどで事前にアポイントを取ること。  
訪問可能な日時をできるだけ多く指定すること。

### 【学生へのメッセージ】

本質的なことは美しく単純であるが，その理解に至るまでには集中した論理的演繹力が要求される．

電気通信大学 平成20年度シラバス

【その他】