電気通信大学　平成16年度シラバス

授業科目名	社会情報システム学特論１		
英文授業科目名	Advanced Topics in Information Systems 1		
開講年度	2004年度	開講年次	
開講学期	前学期	開講コース・課程	博士前期・後期課程
授業の方法		単位数	2
科目区分	情報システム学研究科-情報システム運用学専攻-特論科目		
開講学科・専攻	情報システム運用学専攻		
担当教官名	森田　光(藤村　考)		
居室	ＮＴＴサ-ビスインテグレ-ション基盤研究所		

公開E-Mail	授業関連Webページ
morita@isl.ntt.co.jp	http://ntt.ohta.is.uec.ac.jp

【講義の狙い，目標】

・狙い：高い視点から物の見方を捉え，社会的な要請に応じて技術を構築する方法論を学ぶ.
・目標：情報科学分野における情報セキュリティと電子商取引の技術を習得する.
・対象とする学生：発展中の若い情報科学分野に興味のある人.

【内容】

現代社会は，情報通信システム技術を基盤の一つとして構成されている．本特論では，社会情報システムの要素となっている技術に関して，選定した事項について，理論，機能，評価，構造，高度化，応用等を論じる.

関連図に担当分担を示す.

【教科書，参考書】

教科書は利用しない．必要に応じて，ＯＨＰを使用すると共に，資料配布と参考図書紹介を行う.

【予備知識】

専門的な基礎知識は前提としない．数学的知識は高校数学習得済を前提とする.

【演習】

必要があれば演習問題を提示するが，演習の時間は取らない.

【成績評価】
レポート．但し，評価には出席状況を加味する．

【その他】
・基礎事項と最新技術を分かりやすく講義することを心がける．情報理論，計算量理論，離散数学などからなる基礎的な情報科学ばかりでなく，数学（主に数論），暗号学，確率論，演算工学を横断的に幅広く駆使するが，社会的状況に応じて変化する動向もカバーする． ・学生諸君には，活発な質問・議論を行おうとする高い参加意識を期待する．

電気通信大学　平成16年度シラバス

関連図1

・情報セキュリティ: 以下の項目から特論1は基礎面中心に，特論2は応用面中心に講義を行う(森田担当分)．

基礎項目	技術応用項目	社会応用項目
共通鍵暗号・暗号解読法，公開鍵暗号が基盤とする数学的問題(素因数分解・離散対数)，電子署名，ハッシュ関数(一方向性関数)，楕円曲線上の暗号・認証	秘匿通信，鍵配送，メッセージ認証，相手認証，セキュアプロトコル(ビットコミットメント，マルチパーティセキュア計算，匿名通信路)	電子投票・電子くじ，電子決済(電子マネー，電子クレジットを含む)，輸出管理と鍵復元，著作権保護と鍵管理，標準化(de facto vs. de jure)

関連図2

No Image

関連図3

・電子商取引: 以下の項目から応用面中心に講義を行う(藤村担当分)．

基礎項目	技術応用項目	社会応用項目
証明書とトラストモデル（PGP, SPKI, PKIX，電子チケット、セキュアDNS等)、信用と評判の形成モデル	モバイルコマースの動向(赤外線，BlueTooth, ICカード等の利用技術)，マーケットプレイス構築術	ビジネスモデルと知的財産保護，標準化とオープンソース，販売促進技法，商品格付サービス

関連図4

No Image