電気通信大学　平成21年度シラバス

授業科目名	情報セキュリティシステム		
英文授業科目名	Information Security Systems		
開講年度	2009年度	開講年次	４年次
開講学期	前学期	開講コース・課程	昼間コース
授業の方法	講義	単位数	2
科目区分	専門科目-学科専門科目-選択科目		
開講学科・専攻	情報通信工学科		
担当教官名	太田　和夫		
居室	総合研究棟928		

公開E-Mail	授業関連Webページ
なし	http://www.oslab.ice.uec.ac.jp/class/information_security_systems/

【主題および達成目標】

主題：
セキュリティ技術を応用した「より安全性の高い」暗号プロトコルの設計法について概説する．まず，概論として暗号，認証の基本的な概念を解説する．

今年度は，公開鍵暗号の安全性の定義と，その定義を実現する具体的な方式について紹介する．

達成目標：
暗号理論で習得した「安全性証明技法」を，情報を秘匿する「暗号方式」にまで拡張して，いくつかの数論仮定の下で安全性を証明する．

【前もって履修しておくべき科目】

「暗号理論」（公開鍵暗号の概念を理解しておいてほしい．）

【前もって履修しておくことが望ましい科目】

離散数学第一（証明と論理について，理解しておいてほしい．）

【教科書等】

教科書は用いない．参照すべき論文や解説記事は講義中に指示する．

【授業内容とその進め方】

暗号技術，認証技術，技術動向等を概説したのちに，いくつかの「暗号方式」を紹介する．

・ElGamal 暗号
・RSA-OAEP 暗号
・Cramer-Shoup 暗号
・KEN-DEM 暗号
など

【授業時間外の学習（予習・復習等）】

参照すべき論文を予習することで，講義の内容の理解は深まります．暗号の本質を理解したい人は，論文を読み込んで講義に臨んでください．

【成績評価方法及び評価基準(最低達成基準を含む)】

出席，レポート等にもとづく． 授業中の講義への参加の状況も考慮する．

【オフィスアワー：授業相談】

特に設けない．質問等は事前にメールでアポイントメントを取ること．

【学生へのメッセージ】

本講義は，3年生の後期の講義「暗号理論」の続編であり，非常に難しい内容を含んでいるので，その点に留意して履修すること．頑張って講義についてくれば，情報を秘匿するという意味での暗号を理解できるように講義を行いたいです．

学生には活発な質問・議論などによる講義への参加を強く期待する．

【その他】

なし