

電気通信大学 平成19年度シラバス

授業科目名	ネットワークセキュリティ論1		
英文授業科目名	Network Security 1		
開講年度	2007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	小林 欣吾		
居室	総合研究棟921		

公開E-Mail	授業関連Webページ
kingo@ice.uec.ac.jp	

【講義の狙い，目標】
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。

【内容】
<ul style="list-style-type: none"> ・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。

【教科書，参考書】
教科書は使用しない．参考書，参考文献は必要に応じて指示する．

【予備知識】
離散数学，情報理論など

【演習】

電気通信大学 平成19年度シラバス

【成績評価方法及び評価基準】

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。

【その他】

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。