

電気通信大学 平成17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	2005年度	開講年次	4年次
開講学期	7学期	開講コース・課程	昼間コース
授業の方法		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
ota@ice.uec.ac.jp	http://www.oklab.ice.uec.ac.jp/class/info-system/

<p>【主題および達成目標】</p> <p>主題：</p> <p>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。</p> <p>インターネット環境を想定して、これらの応用としてゼロ知識証明、秘密分散など、一見、不可能に思われるような性質をみたく暗号プロトコルを紹介する。</p> <p>達成目標：</p> <p>暗号理論で習得した「安全性証明技法」をもとにして、種々の「暗号プロトコル」が実現できることを学ぶ。</p>
--

<p>【前もって履修しておくべき科目】</p> <p>「暗号理論」（公開鍵暗号の概念を理解しておいてほしい。）</p>
--

<p>【前もって履修しておくことが望ましい科目】</p> <p>「情報ネットワーク」（インターネットの原理を知っていると理解が深まる。）</p>

<p>【教科書等】</p> <p>参考書</p>

電気通信大学 平成17年度シラバス

1. 「情報セキュリティの科学」太田,黒澤,渡辺,

講談社ブルーバックス, ISBN4-06-257055-6

2. 「暗号理論」太田, 國廣, 岩波書店, ISBN4-00-026871-6

【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「暗号プロトコル」を紹介する.

- ・ゼロ知識証明
- ・秘密情報分散
- ・匿名通信路
- ・プライバシー重視型の署名方式

など

【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.

【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、いくつかの「マジカル」な暗号プロトコルを理解できる。可能なら、自分で暗号プロトコルを設計してもらいたい。

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】

前年度までの講義内容とはまったく違うので注意すること。ネットワーク・セキュリティには言及しない。