

No.	実施大学	授業科目名	担当教員	単位数	開講区分	曜日	予定回数	時間	実施場所	定員
6	東京工科大学	情報セキュリティ	宇田 隆哉 コンピュータサイエンス学部 講師	2	前期	火	14	10:45～12:25	東京工科大学 八王子キャンパス	若干名

【到達目標】

公開鍵暗号の仕組みについて理解する。(実学に基づく専門能力、論理的な思考能力)
 共通鍵暗号の仕組みについて理解する。(実学に基づく専門能力、論理的な思考能力)
 ネットワークのフィルタリングについて理解する。(実学に基づく専門能力、論理的な思考能力)
 情報セキュリティに関する知識を深める。(実学に基づく専門能力)
 これらの仕組みや専門知識は、論理的な構造を伴うものであり、目標に到達する過程で、実学に基づく専門能力、論理的な思考能力を養う。

【授業の概要】

本講義は情報セキュリティについての理解を深めることを目的とする。ネットワークを介した不正攻撃、コンピュータウイルスの仕組みや対策、ファイアウォールの原理などのネットワークセキュリティ、共通鍵暗号、公開鍵暗号、ハッシュなどの暗号技術、暗号理論を応用した認証技術、電子透かし技術、匿名化通信、IoT セキュリティについての解説を行う。

この授業では主に論理的な思考能力を身につけることを目的としている。さらに、実学に基づく専門能力を鍛えることを目指している。

【授業内容】

第1回:情報セキュリティの目的、技術的対策方法について概要を学ぶ	第8回:認証技術を応用した SSL、S/MIME、PGP、VPN、WEP の仕組みについて学ぶ
第2回:不正攻撃に対するコンピュータの脆弱性、攻撃手法と対策について学ぶ	第9回:PKI の基礎について学ぶ
第3回:代表的コンピュータウイルスの種類と機能、対策について学ぶ	第10回:PKI の詳細について学ぶ
第4回:ファイアウォールの仕組み、NAT、DMZ について学ぶ	第11回:電子透かしの技術について学ぶ
第5回:共通鍵暗号、ハッシュの技術について学ぶ	第12回:匿名化通信について学ぶ
第6回:公開鍵暗号の技術について学ぶ	第13回:IoT セキュリティについて学ぶ
第7回:電子署名、タイムスタンプなどの認証技術について学ぶ	第14回:総復習を行う

【成績評価方法】

数回の課題レポートおよび期末試験により成績評価を行う。期末試験結果とレポートは、およそ 10 対 3 の比率で総合成績に反映する。
 Moodle 小テストの得点はこれにおよそ最大 15%の割合で加算される。

【教科書】

宮地充子、菊池浩明編著、「IT Text 情報セキュリティ」、オーム社(2003年)

【参考書、教材等】

情報セキュリティ標準テキスト編集委員会編、「情報セキュリティ標準テキスト」、オーム社(2006年)
 佐々木良一、吉浦裕、手塚悟、三島久典共著、「インターネット時代の情報セキュリティ・暗号と電子透かし」、共立出版(2000年)

【履修上の注意】

学内外問わず、受講者はノート PC 必携とする。受講者は全員、本講義の開始日までに学内ネットワークに接続可能な環境を整えておくこと。コンピュータ概論 I、コンピュータ概論 II を修得していることが履修の前提となる。予習・復習を十分に行うこと。提出方法を守らないレポート、および、やむを得ない事情無く期日に遅れて提出されたレポートは受理しない。

【準備学習】

コンピュータ概論 I、コンピュータ概論 II の内容を理解していることを前提に講義を行うので、これらの科目の単位取得有無にかかわらず、本講義の開始日までにその内容を理解していること。
 予習として、次の回の授業に必要な前提知識を、コンピュータ概論 I、コンピュータ概論 II の教科書を使って再確認する。
 復習として、その回の授業における Moodle の小テストで不正解となった項目について、講義資料と照らし合わせて確認する。

※ この授業は、4/14(火)が初回です。