

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
2	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 准教授	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】

1. 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
2. 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
3. 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
4. ファイアウォールの仕組み、NAT、DMZについて学ぶ
5. 共通鍵暗号、ハッシュの技術について学ぶ
6. 公開鍵暗号の技術について学ぶ
7. 電子署名、タイムスタンプなどの認証技術について学ぶ
8. 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
9. PKIの基礎について学ぶ
10. 電子透かしについて学ぶ
11. ブロックチェーン技術について学ぶ
12. バイオメトリクスについて学ぶ
13. IoTセキュリティについて学ぶ
14. 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、100対27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期末試験の最大15%の割合で加算される。

レポートおよび小テストのフィードバックはMoodleにて行う。

【教科書】

宮地充子、菊池浩明編著、「IT Text 情報セキュリティ 改訂2版」、オーム社（2022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）

岡田仁志著、「決定版 ビットコイン&ブロックチェーン」、東洋経済新報社（2018年）

松井俊浩著、「IoTセキュリティ技術入門」、日刊工業新聞社（2020年）

※ この授業は、4/18（火）が初回です。