登録コード	TSJ15500	開講年度	2026

授業科目	情報セキュリティ学特論					担当教員	岡﨑　裕之
英文授業名	Information Security and Cryptology					副担当	
単位数	2	講義期間	後期	曜日・時限	金曜･３時限	対象学生	総合理工学研究科 情報数理・融合システム分野　修士課程１，２年生
講義室	工W1-115教室			授業形態	講義	備考	
信大コンピテンシー	非該当						

(1)授業の達成目標	【授業で得られる「学位授与の方針」要素】	⇔	【授業の達成目標】
	２６TSカリ，２５TSカリ，２４TSカリ，２３TSカリ		
	【専攻】工学分野の研究者・技術者として科学・技術を発展させるための幅広い見識と健全な倫理観	⇔	・独立行政法人 情報処理推進機構（IPA）や、内閣サイバーセキュリティセンター（NISC）から公表される情報セキュリティに関する技術報告を理解し、実務に生かせるようになる。

(2)授業の概要	講義において、先ず情報セキュリティの概要を解説する。セキュリティ対策技術のみならず、マネジメント、関連法規などについても理解する。 さらに学外講師によるソフトウェア開発現場でのセキュリティ対策について学習する。それらのなかでの暗号技術の果たす役割について理解する。 次に、暗号技術のベースとなる数学知識、計算機科学知識を学ぶ。また、証明可能安全性、形式的安全性検証技術についても学習する。 講義内容に基づく演習において課題を課す。最後に、定期試験を実施する。
(3)授業計画	第１回　履修ガイダンスと情報セキュリティ概論 第２回　情報セキュリティの最近の動向 第３回　情報セキュリティマネジメント 第４回　情報セキュリティインシデント事例紹介 第５回　ネットワークセキュリティ 第６回　ブロックチェーン関連技術 第７回　演習１（レポート第1回） 第８回　個人情報保護と認証 第９回　暗号技術総論 第10回　現代暗号理論に必要な数学概要 第11回　高度な暗号技術 第12回　証明可能安全性 第13回　演習２（レポート第2回） 第14回　形式的安全性検証技術 第15回　演習３、授業アンケート 第16回　定期試験
(4)成績評価の方法	・講義内容に基づく演習ではレポート課題を課す．成績は，レポート課題（2回：各40%）とテスト、確認問題等（20%）の成績に基づいて総合的に評価する． レポート評価基準 内容の正しさ、体裁、論理展開、記述方法についてそれぞれで技術報告書として許容できる場合にのみ成績評価を行う。 課された全てのレポートが提出されない場合は成績判定されない。
(5)成績評価の基準	情報セキュリティに関する基礎知識を習得すること。 合格基準はIPAの情報処理技術者試験、応用情報技術者区分のセキュリティに関連する問題の合格基準と同程度とする。
(6)事前事後学習の内容	学部3年次後期の「情報セキュリティ」の発展的な講義を行うため、同科目を履修していることが望ましい。
(7)履修上の注意	・担当教員から提示される授業eALPSページならびに電子掲示板は逐次更新されるので注意して見ておくこと． ・暗号プロトコル安全性形式的検証ツールを利用する場合があるため、事前に指示のあった場合にはノートPCを持参すること。 （Windowsを想定しています。Linux,Mac等でもツールは利用できますがインストール作業等については自己責任でお願いします）
(8)質問,相談への対応	質問は原則として授業中に直接聞くのが望ましい．不在時には，電子メールにて受け付ける．アドレスは以下の通り． okazaki@cs.shinshu-u.ac.jp
(9)その他	
【教科書】	・光成 滋生「クラウドを支えるこれからの暗号技術」秀和システム(2015)　ISBN978-4798044132 https://herumi.github.io/ango/
【参考書】	・齋藤孝道「マスタリングTCP/IP 情報セキュリティ編(第２版)」オーム社 ISBN9784274228797 ・上記の参考書とともに，担当教員から随時提示提供されるコンテンツを使用する（Web，電子メール添付ファイルを含む）