

登録コード	T2022300	開講年度	2026	県内大学開放授業				
授業科目	情報セキュリティ(16T以降)					担当教員	岡崎 裕之 他	
英文授業名	Information Security					副担当		
単位数	2	講義期間	後期	曜日・時限	水曜・2時限		対象学生	電子情報システム工学科3年生
講義室	工W2-101教室			授業形態	講義	遠隔授業科目	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】	
	2 5Tカリ, 2 3Tカリ							
	【22T〜】専門分野における専門的学力が身についている。					⇔	・基本的な暗号技術, それらのセキュリティプロトコルへの応用, 認証技術, Webアプリケーションへの多様化する攻撃手法の知識と対策技術を身に付けることができる。	
(2)授業で学べる「テーマ」	その他							
(3)全学横断特別教育プログラム								
(4)授業の概要	講義において, 前半では先ず, 情報セキュリティの分類や脅威の範囲, セキュリティを構成する要素や動向などを概説した後, 暗号技術の基礎, 共通鍵暗号化技術, 公開鍵暗号化技術, 認証技術と認証プロトコルの実例および関連技術を解説する。続いてセキュア通信で不可欠な公開鍵証明基盤, 認証局などPKIに関係する各種技術について説明し, 更にSSL/TLS, IPsecといったインターネット標準化されたセキュリティプロトコルについて解説する。 後半では, システムセキュリティ領域として, ホストセキュリティ, ネットワークセキュリティ, IDS, ファイアウォール, Webセキュリティ, 更にはXSS攻撃, SQLインジェクションなどの攻撃の実例などを説明する。 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。							
(5)授業計画	担当: 岡崎裕之 第1回 情報セキュリティ概論(教科書 第1章) 第2回 暗号技術(1)(教科書 第2章) 第3回 暗号技術(2)(教科書 第2章) 第4回 認証技術(1)(教科書 第3章) 第5回 認証技術(2)(教科書 第3章) 第6回 PKI(教科書 第4章) 第7回 セキュリティプロトコル(教科書 第5章) 第8回 演習課題I 第9回 ホストのセキュリティ(教科書 第6章) 第10回 ネットワークセキュリティ(教科書 第7章) 第11回 Webセキュリティ(教科書 第8章) 第12回 情報セキュリティマネジメント(1) 第13回 情報セキュリティマネジメント(2) 第14回 演習課題II 第15回 小テスト, 授業アンケート 第16回 定期試験							
(6)成績評価の方法	・第15回にて小テストを行う。 ・定期試験と小テストの成績に基づいて総合的に評価する。 ・定期試験の実施が困難な場合にはレポートを課し評価する。							
(7)成績評価の基準	小テストの成績が一定水準に達したうえで, 定期(筆記)試験において, 授業で示した例題と同レベルの問題が解ければ「水準にある」, 応用問題が解ければ「やや上にある」, やや難しい応用問題が解ければ「かなり上にある」, 例題からは難しい応用問題が解ければ「卓越している」とする。 なお, IPAの応用情報技術者試験の午後のセキュリティ問題"単体"に挑める程度が「水準にある」と想定している。							
(8)事前事後学習の内容	・予習は不要, 復習は授業中およびeALPSにて指示する。							
(9)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。							
(10)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。 岡崎 okazaki@cs.shinshu-u.ac.jp							
(11)その他	・コンピュータネットワーク, 符号理論をあわせて履修することが望ましい(必須ではない)							
【教科書】	・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 ISBN 978-4274228797							
【参考書】	・Ivan Ristic著, 齋藤孝道 監訳「プロフェッショナルSSL/TLS」ISBN: 978-4-908686-00-9 ・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/ (著者自身によりPDF版公開中) ・IPA「情報セキュリティ白書」授業開講時での最新版							

【参考書】	・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）
-------	---