講義科目名称： 情報セキュリティC　C5-C42-30　　科目コード： 19260

英文科目名称： Information Security

開講期間	配当年	単位数	科目必選区分
3年前期	3	2	選択（教職「情報」は必修）
担当教員			
大石　和臣			
添付ファイル			

講義概要	情報セキュリティは現代社会において最も重要で必要不可欠な概念の一つである．情報セキュリティとそれに関連する概念について説明し，技術的な対策について詳しく解説する．セキュリティ評価制度や組織における運用や管理についても説明し，情報セキュリティを踏まえた情報リテラシーを学ぶ．この科目は、情報セキュリティ技術分野の実務経験のある教員が担当する科目である。
授業計画	1　イントロダクション，情報セキュリティ概論 カリキュラムにおける本講義の位置づけ（ステップ4，コース、分野科目）を説明する．講義概要をシラバスを使って説明する．現代における情報セキュリティの重要性と具体的なリスクを例示する．AL①。講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)．AL①. 準備：シラバスを読んでくること. 課題：今回の復習および次回の講義内容を予習. 2　暗号の基礎，共通鍵暗号 暗号に基礎について，整数論や計算量理論を踏まえて学ぶ．共通鍵暗号について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 3　暗号(公開鍵暗号，ハッシュ関数，ディジタル署名) 公開鍵暗号とハッシュ関数，ディジタル署名について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 4　公開鍵証明書，暗号プロトコル 公開鍵証明書の概念と実例，認証局とその階層構造，暗号プロトコルの実例について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)．AL①. 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 5　サイドチャネル攻撃，秘密分散，量子暗号 ICカードを対象とするサイドチャネル攻撃，暗号鍵を管理する手法である秘密分散，量子コンピュータが実現しても破られない量子暗号について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 6　アクセス制御，UNIXパスワード，PBC ユーザ認証とアクセス制御について学びUNIXパスワードの具体的な仕組みを学ぶ．パスワードに基づく暗号化プログラムの構造を学習する．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 7　バイオメトリクス 指紋や虹彩などの生体情報を用いるバイオメトリック認証について学ぶ．講義の最後に簡単な演習を行う. 準備：今回の講義内容を予習してくること(iLearnあるいはMicrosoft Formsを活用する場合がある). 課題：今回の復習および次回の講義内容を予習. 8　前回の演習の回答と解説，質疑応答，中間試験 前回の演習の回答と解説を行う．前回までの講義について質疑応答をする．AL①．その後に中間試験を行う. 準備：前回までの講義内容を復習してくること. 9　ネットワークセキュリティ,Web セキュリティ ネットワークセキュリティとWebセキュリティについて学ぶ．ファイアウォール，NAT等の具体的技術を学習する．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 10　マルウェア（コンピュータウイルス，ワーム，シェルコード他) Webセキュリティに関連してマルウェアについて学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある). 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習. 11　マルウェア対策（アンチウイルス，ハニーポット，セキュアコーディング） マルウェア対策の技術について，最新技術も含めて学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)．AL①. 準備：今回の講義内容を予習してくること. 課題：今回の復習および次回の講義内容を予習.

	12　プライバシ保護，匿名性，匿名通信，RFID プライバシ保護，匿名性，匿名通信，RFIDの背景と具体的技術について学ぶ．中間試験の回答と解説．AL①．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)． 準備：今回の講義内容を予習してくること． 課題：今回の復習および次回の講義内容を予習． 13　情報ハイディング（電子透かし，ステガノグラフィー），ディジタルフォレンジック 電子透かしやステガノグラフィー等の情報ハイディング技術とハードディスクの解析等のディジタルフォレンジック技術について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)． 準備：今回の講義内容を予習してくること． 課題：今回の復習および次回の講義内容を予習． 14　評価制度（ISO/IEC15408，JISEC，JCMVP），ISMS 技術的な評価と組織的な評価に関する評価制度について学ぶ．講義の最後に簡単な演習を行う(iLearnあるいはMicrosoft Formsを活用する場合がある)． 準備：今回の講義内容を予習してくること． 課題：今回の復習および次回の講義内容を予習． 15　セキュリティインシデントや関連技術の事例紹介，まとめ，総合演習 最新の研究紹介やいままでの講義内容についての質問を受け付ける．AL①． 準備：今回の講義内容を予習してくること． 課題：いままでの講義内容を復習し，定期試験に備える． 16　定期試験
授業形態	講義と演習（課題） アクティブラーニング：①:6回,②:0回,③:0回,④:0回,⑤:0回,⑥:0回
達成目標	1）情報セキュリティの脅威と対策を理解する． 2）要素技術（暗号，認証，マルウェア対策等）の知識を得る． 3）要素技術の特徴と限界を理解して適切に使用できるようになる． 4）情報セキュリティに関する法律や制度（運用）を理解する． 5）情報セキュリティを踏まえた情報リテラシーを身に着ける．
評価方法・フィードバック	演習・課題40%，総合演習60%の配点で評価する．各回に行う演習は次回に解説を行い，課題（宿題）は採点して返却し、結果をフィードバックする。
評価基準	100～90：秀，89～80：優，79～70：良，69～60：可，60未満：不可 達成目標の100～90%に到達した場合は秀， 達成目標の89～80%に到達した場合は優， 達成目標の79～70%に到達した場合は良， 達成目標の69～60%に到達した場合は可， 達成目標の59～0%に到達した場合は不可．
教科書・参考書	教科書：指定しない． 参考書：いくつかの書籍を以下に示す． 1. 独立行政法人情報処理推進機構，情報セキュリティ白書2019，独立行政法人情報処理推進機構，2019 年． 2. 辻井重男，情報社会・セキュリティ・倫理，コロナ社，2012 年． 3. 映像情報メディア学会編，半谷精一郎編著，バイオメトリクス教科書：原理からプログラミングまで，コロナ社，2012 年． 4. 佐々木良一監修，手塚悟編著，情報セキュリティの基礎，共立出版，2011 年． 5. 独立行政法人情報処理推進機構，情報セキュリティ読本四訂版-IT 時代の危機管理入門-，実教出版株式会社，2009 年． 6. 黒澤馨，尾形わかは，現代暗号の基礎数理，コロナ社，2004 年． 7. 松井甲子雄，岩切宗利，情報ハイディングの基礎―ユビキタス社会の情報セキュリティ技術，森北出版，2004 年．
履修条件	符号・暗号理論1を履修済み，符号・暗号理論2を履修中あるいは履修済みが望ましい．
履修上の注意	なし
準備学習と課題の内容	1回の講義につき2時間程度の予習・復習を行って授業にのぞむこと．予習として，授業計画の各内容に関して，参考書の該当する章を読むことあるいはインターネットで調べて準備することが望ましい．復習として，講義のスライドやノートを読み返して講義内容を理解し，参考書の該当する章を読むことあるいはインターネットで調べて理解を深めることが望ましい．演習や課題（宿題）を繰り返し解くことは有効な復習および試験対策になる．
ディプロマポリシーとの関連割合（必須）	知識・理解:40%,思考・判断:40%,関心･意欲:10%,態度:5%,技能・表現:5%
DP1 知識・理解	
DP2 思考判断	
DP3 関心意欲	
DP4 態度	
DP5 技能・表現	