久留米工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	3S19	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	履修単位: 1
開設学科	制御情報工学科	対象学年	3
開設期	後期	週時間数	2
教科書/教材	教科書：(独)情報処理推進機構，情報セキュリティ読本 五訂版，実教出版　スライド：(独)高専機構K-SEC，座学と演習で学ぶサイバーセキュリティ		
担当教員	小田 幹雄		

到達目標

1．情報セキュリティリスクとリスクアセスメントの説明ができる。
2．暗号理論を説明できる。
3．ネットワークセキュリティに関する攻撃方法とその対策を説明できる。
4．ソフトウエア・ハードウエアに関するセキュリティ上の問題を説明できる。

ルーブリック

	理想的な到達レベルの目安	標準的な到達レベルの目安	未到達レベルの目安
評価項目1	情報セキュリティに関する脅威，脆弱性，攻撃などのリスクとそのリスクの評価法について詳細で正確に説明ができる。	情報セキュリティに関する脅威，脆弱性，攻撃などのリスクとそのリスクの評価法について説明ができる。	情報セキュリティに関する脅威，脆弱性，攻撃などのリスクとそのリスクの評価法について説明ができない。
評価項目2	代表的な暗号化法の理論について詳細で正確に説明できる。	代表的な暗号化法の理論について説明できる。	代表的な暗号化法の理論について説明できない。
評価項目3	ネットワークを利用する時の情報セキュリティに関する代表的な攻撃方法とその対策方法について詳細で正確に説明できる。	ネットワークを利用する時の情報セキュリティに関する代表的な攻撃方法とその対策方法について説明できる。	ネットワークを利用する時の情報セキュリティに関する代表的な攻撃方法とその対策方法について説明できない。
評価項目4	情報処理装置等を構成するソフトウエアやハードウエアに関する情報セキュリティ上の代表的な問題点について詳細で正確に説明できる。	情報処理装置等を構成するソフトウエアやハードウエアに関する情報セキュリティ上の代表的な問題点について説明できる。	情報処理装置等を構成するソフトウエアやハードウエアに関する情報セキュリティ上の代表的な問題点について説明できない。

学科の到達目標項目との関係

教育方法等

概要	PCやスマートフォン等の情報処理機器が，常時インターネットに接続され，広範囲な社会活動に利用されるに伴い、扱う情報に対するセキュリティ対策は，利用者にとって身近な問題であり，技術者にとっては，重要な技術的課題である。本授業では，これら情報セキュリティに関わる基礎的な知識と技術的な対応方法について修得することを目的とする。具体的には，情報セキュリティに関する脅威，脆弱性，攻撃などのリスクとそのリスクの評価法，代表的な暗号化理論，サイバー攻撃方法とその対策方法および情報処理機器を構成するソフトウエアやハードウエアに関わる情報セキュリティ上の問題点について理解する。
授業の進め方・方法	教科書とスライドを用いた講義を行う。教科書を用いて授業内容の概要を理解し，スライドを用いて詳細な事例を紹介することにより理解を深める。情報系技術者として知っておくべき基本的な情報セキュリティに関する事例や技術を幅広く説明する。授業中の演習やレポートにより、自学自習の機会を与えるが，授業外でも予習または復習に取り組むことを推奨する。 関連科目：計算機ネットワーク，オペレーティングシステム，情報通信実験
注意点	定期試験（80%）、レポート(20%)とし、100点法により総合成績を評価する。 総合成績が不合格の場合は、総合成績が上限60点の再試験を実施する。 評価基準：60点以上を合格とする。 授業終了時に示す課題のレポートを作成するとともに、授業内容の予習復習に努めること。

授業の属性・履修上の区分

□ アクティブラーニング	☑ ICT 利用	□ 遠隔授業対応	□ 実務経験のある教員による授業

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	情報とそのセキュリティリスク（1）	情報とそのセキュリティリスクを説明できる。
		2週	情報とそのセキュリティリスク（2）	情報とそのセキュリティリスクを説明できる。
		3週	情報セキュリティマネジメント（1）	情報セキュリティのマネジメント方法を説明できる。
		4週	情報セキュリティマネジメント（2）	情報セキュリティのマネジメント方法を説明できる。
		5週	暗号理論（1）	暗号理論を説明できる。
		6週	暗号理論（2）	暗号理論を説明できる。
		7週	演習（1）	演習課題に取り組み報告できる。
		8週	中間試験	
	4thQ	9週	ネットワークセキュリティ（1）	ネットワークセキュリティを説明できる。
		10週	ネットワークセキュリティ（2）	ネットワークセキュリティを説明できる。
		11週	ネットワークセキュリティ（3）	ネットワークセキュリティを説明できる。
		12週	ソフトウエアセキュリティ	ソフトウエアセキュリティを説明できる。
		13週	ハードウエアセキュリティ	ハードウエアセキュリティを説明できる。
		14週	情報セキュリティと法制度	情報セキュリティと法制度を説明できる。
		15週	答案返却と問題解説	
		16週		

モデルコアカリキュラムの学習内容と到達目標

分類	分野	学習内容	学習内容の到達目標	到達レベル	授業週

基礎的能力	工学基礎	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	技術者倫理(知的財産、法令順守、持続可能性を含む)および技術史	情報技術の進展が社会に及ぼす影響、個人情報保護法、著作権などの法律について説明できる。	3	後14
専門的能力	分野別の専門工学	情報系分野	その他の学習内容	コンピュータウィルスやフィッシングなど、コンピュータを扱っている際に遭遇しうる代表的な脅威について説明できる。	4	後9,後10
				コンピュータを扱っている際に遭遇しうる脅威に対する対策例について説明できる。	4	後9,後10
				基本的な暗号化技術について説明できる。	4	後5,後6
				基本的なアクセス制御技術について説明できる。	4	後9,後10
				マルウェアやフィッシングなど、コンピュータを扱っている際に遭遇しうる代表的な脅威について説明できる。	4	後9,後10

評価割合

	試験	レポート	合計
総合評価割合	80	20	100
専門的能力	80	20	100