苫小牧工業高等専門学校	開講年度	令和06年度 (2024年度)	授業科目	情報セキュリティ演習

科目基礎情報

科目番号	0026	科目区分	専門 / 必修
授業形態	演習	単位の種別と単位数	履修単位: 1
開設学科	創造工学科（情報科学・工学系共通科目）	対象学年	4
開設期	後期	週時間数	2
教科書/教材	特になし．必要に応じ資料を提示あるいは配布する．		
担当教員	土居 茂雄		

到達目標

MCCにおける
V-D-4 コンピュータシステム＞コンピュータシステム
V-D-6 情報通信ネットワーク＞階層化プロトコル，ローカルエリアネットワークとインターネット
V-D-8 その他の学習内容＞セキュリティ
Ⅶ-B PBL教育＞情報収集・分析，問題発見
Ⅷ-C 情報活用・収集・発信力

ルーブリック

	理想的な到達レベルの目安(優)	標準的な到達レベルの目安(良)	未到達レベルの目安(不可)
V-D-4 コンピュータシステム＞コンピュータシステム	ネットワークコンピューティングや組込みシステムなど、実用に供せられているコンピュータシステムの利用形態について詳細に説明できる。	ネットワークコンピューティングや組込みシステムなど、実用に供せられているコンピュータシステムの利用形態について説明できる。	ネットワークコンピューティングや組込みシステムなど、実用に供せられているコンピュータシステムの利用形態について説明できない。
V-D-6 情報通信ネットワーク＞階層化プロトコル	プロトコルの概念を詳細に説明できる。	プロトコルの概念を説明できる。	プロトコルの概念を説明できない。
V-D-6 情報通信ネットワーク＞階層化プロトコル	プロトコルの階層化の概念や利点を詳細に説明できる。	プロトコルの階層化の概念や利点を説明できる。	プロトコルの階層化の概念や利点を説明できない。
V-D-6 情報通信ネットワーク＞ローカルエリアネットワークとインターネット	インターネットの概念を詳細に説明できる。	インターネットの概念を説明できる。	インターネットの概念を説明できない。
V-D-8 その他の学習内容＞セキュリティ	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詳細に説明できる。	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。	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ない。
V-D-8 その他の学習内容＞セキュリティ	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代表的な対策について詳細に説明できる。	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代表的な対策について説明できる。	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代表的な対策について説明できない。
Ⅶ-B PBL教育＞情報収集・分析，問題発見	集められた情報をもとに、状況を適確に分析することができる。	集められた情報をもとに、状況を分析することができる。	集められた情報をもとに、状況を分析することができない。
Ⅶ-B PBL教育＞情報収集・分析，問題発見	与えられた目標を達成するための解決方法を的確に考えることができる。	与えられた目標を達成するための解決方法を考えることができる。	与えられた目標を達成するための解決方法を考えることができない。
Ⅷ-C 情報活用・収集・発信力	ICTやICTツール、文書等を自らの専門分野において情報収集や情報発信に適切に活用できる。	ICTやICTツール、文書等を基礎的な情報収集や情報発信に活用できる。	ICTやICTツール、文書等を基礎的な情報収集や情報発信に活用できない．

学科の到達目標項目との関係

Ⅰ　人間性 1 Ⅰ　人間性
Ⅱ　実践性 2 Ⅱ　実践性
Ⅲ　国際性 3 Ⅲ　国際性
CP2　各系の工学的専門基盤知識，および実験・実習および演習・実技を通してその知識を社会実装に応用・実践できる力 5 CP2　各系の工学的専門基盤知識，および実験・実習および演習・実技を通してその知識を社会実装に応用・実践できる力
CP4　他者を理解・尊重し，協働できるコミュニケーション能力と人間力 7 CP4　他者を理解・尊重し，協働できるコミュニケーション能力と人間力

教育方法等

概要	情報セキュリティは学問としてはまだ日が浅い領域であり，課題解決志向の領域でもあります． 本演習では，情報セキュリティは何かを実際の演習を通して学びます． 本演習は，企業で「ソフトウェアの研究開発」を担当していた教員が，その経験を活かし，「ソフトウェアのセキュリティ」を中心にした内容を「演習」形式で担当します．
授業の進め方・方法	ディスカッションや実習を中心に進めていきます． 自学自習のための課題やレポートを提示しますので，期限までに提出してください．
注意点	本科目では，高専サイバーセキュリティ人材育成事業(K-SEC)と高専機構が協定を結んでいるシスコ合同会社のCyberOPs 教材を利用します． 外部講師による講演は実施時期が確定したら連絡します(調整次第では実施しない可能性もあります)．確定後，シラバスの修正等が行われますので承知おきください．

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	情報セキュリティ概論	情報セキュリティとは何かを俯瞰し，なぜ対策が必要かを理解する．
		2週	リスクマネジメント演習	実際の事例を対象に，情報資産の特定やリスク管理を行うことができる．
		3週	サイバーセキュリティにおける倫理	サイバーセキュリティ技術を習得するうえで必要となる倫理を実践することができる．

		4週	OSINT	インターネットにある情報から目的の情報を抽出することができる.
		5週	RSA暗号	RSA暗号アルゴリズムを実装し，平文を暗号化および暗号化文を復号することができる.
		6週	RSA暗号	RSA暗号アルゴリズムを実装し，平文を暗号化および暗号化文を復号することができる.
		7週	外部講師による講演・演習	外部講師による講演・演習を通し，実際にどのようにセキュリティを維持するかを理解できる.
		8週	ログ解析演習	リダイレクトやパイプを駆使して，サーバのログから攻撃の痕跡を抽出することができる.
	4thQ	9週	ログ解析演習	リダイレクトやパイプを駆使して，サーバのログから攻撃の痕跡を抽出することができる.
		10週	ログ解析演習	リダイレクトやパイプを駆使して，サーバのログから攻撃の痕跡を抽出することができる.
		11週	可用性・多層防御	可用性を上げるためのシステムの構成法や多層防御の仕組みを理解し説明できる.
		12週	セキュアプログラミング	プログラミングで起こりうる脆弱性を理解し，脆弱性を埋め込まない設計や実装を説明できる.
		13週	セキュアプログラミング	プログラミングで起こりうる脆弱性を理解し，脆弱性を埋め込まない設計や実装を説明できる.
		14週	セキュアプログラミング	プログラミングで起こりうる脆弱性を理解し，脆弱性を埋め込まない設計や実装を説明できる.
		15週	セキュアプログラミング	プログラミングで起こりうる脆弱性を理解し，脆弱性を埋め込まない設計や実装を説明できる.
		16週		

評価割合

	課題	合計
総合評価割合	100	100
基礎的能力	0	0
専門的能力	100	100