仙台高等専門学校	開講年度	平成31年度 (2019年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	0259	科目区分	専門 / 選択
授業形態	授業	単位の種別と単位数	学修単位: 2
開設学科	情報ネットワーク工学科	対象学年	5
開設期	後期	週時間数	2
教科書/教材	情報セキュリティの基本と仕組み，暗号技術入門		
担当教員	衣川 昌宏		

到達目標

1. コンピュータを扱っている際に遭遇しうる代表的な情報セキュリティのリスクおよび脅威についての分析ができる。
2. 代表的な脅威について、その技術的手法の理解およびその実践と対策ができる。
3. 情報セキュリティの持続可能なシステム化手法の基礎的な立案ができる。

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
情報セキュリティのリスク・脅威の分析	情報資産に対する情報セキュリティでのリスクを理解し，脅威の分析ができる。	情報資産に対する情報セキュリティでの基本的なリスクと脅威を理解している。	情報資産に対する情報セキュリティでのリスクと脅威を理解していない。
情報セキュリティの技術的対策の理解・実践・対策	リスクに対する技術的セキュリティ対策を正しく選択し，利用することができる。	リスクに対する技術的セキュリティ対策を理解している。	リスクに対する技術的セキュリティを理解していない。
情報セキュリティの持続可能なシステム化手法の立案	技術的セキュリティの評価手法を理解し，維持管理を行える。	技術的セキュリティの評価手法を理解している。	技術的セキュリティの評価手法を理解していない。

学科の到達目標項目との関係

学習・教育到達度目標 1 通信機器や情報通信システム構築に必要なハードウェア・ソフトウェアの知識と技術の習得

教育方法等

概要	この科目は企業で情報通信セキュリティに関する製品・サービスの設計を担当していた教員が、その経験を生かし、情報セキュリティについて講義形式で授業を行うものである。不正アクセスやコンピュータウィルスなどによるセキュリティ上の脅威と共に，ファイアーウォールやセキュリティプロトコルによるそれらへの対策技術を学習する。また，情報の盗聴・改ざん・なりすましに対処するための暗号技術と認証技術の基礎と活用法、さらにソフトウェアへの攻撃手法とその対策を修得する。
授業の進め方・方法	各回の授業で，前半は新しい知識の習得，後半は演習を行う。
注意点	「情報セキュリティ基礎」および「情報理論」での学習事項に関する実践手法を学習する。そのため，「情報セキュリティ基礎」および「情報理論」を履修していることが望ましい。また，前述教科で用いる教科書を参考書としており，学習補助資料として参照する。

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	情報システムの情報セキュリティと、組織のセキュリティ	情報システムに要求される安全性および、組織と体制作りについて説明できる。
		2週	情報の分類と管理および、情報セキュリティポリシー、リスクマネジメント	情報資産の分類と管理および、情報セキュリティポリシーの策定と実施手順を説明できる。また、リスク分析と対応および回避について説明できる。
		3週	暗号理論 1	情報セキュリティにおける暗号の役割を理解し、基礎的な暗号アルゴリズムについて説明できる。
		4週	暗号理論 2	基礎的な暗号アルゴリズムについて、ソフトウェアでの暗号化について設計指針を作成できる。
		5週	暗号理論 3	基礎的な暗号アルゴリズムについて、C言語で実装ができる。
		6週	暗号理論 4	ブロック暗号のモードについて理解できる。
		7週	暗号理論 5	ブロック暗号のモードについて、CBCモードのC言語実装ができる。
		8週	暗号理論 6	ハッシュ関数について理解できる。
	4thQ	9週	暗号理論 7	ハッシュ関数を用いた認証について理解できる。
		10週	法令遵守	代表的な情報セキュリティに関する法律を説明できる。
		11週	ネットワークソフトウェアセキュリティ 1	バッファオーバフロー攻撃とその実践、対策が理解できる。
		12週	ネットワークソフトウェアセキュリティ 2	バッファオーバフロー攻撃について、C言語で実践、対策ができる。
		13週	ネットワークソフトウェアセキュリティ 3	サーバソフトウェアのログから攻撃の状況を把握できる。ログの管理が理解できる。
		14週	ネットワークソフトウェアセキュリティ 4	様々なサーバソフトウェアのログから動作を解析できる。
		15週	期末試験	期末試験の実施
		16週	期末試験の返却	期末試験の答案返却と解説

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	情報リテラシー	情報リテラシー	情報セキュリティの必要性および守るべき情報を認識している。	4	後1,後2
				個人情報とプライバシー保護の考え方についての基本的な配慮ができる。	4	後2
				インターネット(SNSを含む)やコンピュータの利用における様々な脅威を認識している	4	後1

				インターネット(SNSを含む)やコンピュータの利用における様々な脅威に対して実践すべき対策を説明できる。	4	後1
専門的能力	分野別の専門工学	情報系分野	プログラミング	要求仕様に従って、いずれかの手法により動作するプログラムを設計することができる。	4	後4,後7,後12
				要求仕様に従って、いずれかの手法により動作するプログラムを実装することができる。	4	後5,後7,後12
			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1
				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1
				基本的な暗号化技術について説明できる。	4	後3,後4,後5,後6,後7,後8,後9
				基本的なアクセス制御技術について説明できる。	4	後11,後12,後13,後14
				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1
分野横断的能力	態度・志向性(人間力)	態度・志向性	態度・志向性	法令やルールを遵守した行動をとれる。	4	後10

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	その他	合計
総合評価割合	60	0	0	0	0	40	100
基礎的能力	20	0	0	0	0	20	40
専門的能力	40	0	0	0	0	20	60
分野横断的能力	0	0	0	0	0	0	0