仙台高等専門学校	開講年度	平成29年度 (2017年度)	授業科目	情報セキュリティ基礎

科目基礎情報

科目番号	0256	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	4
開設期	前期	週時間数	2
教科書/教材	教科書：「図解入門 よくわかる最新情報セキュリティの基本と仕組み―基礎から学ぶセキュリティリテラシ」相戸浩志(秀和システム)		
担当教員	速水 健一		

到達目標

セキュリティに対する考え方について学び，分類やリスクの見積もり，対策方法について考えることができる。脅威について，どのようなものがあるか理解し，意識できるようになる。代表的な暗号技術について理解し，セキュリティへの応用について考えることができるようになる。技術面や，人的な面，法的な面によるセキュリティ対策として，どのようなものがあるのかを理解し，現状でのそれらの効力，問題点について理解し，ある程度の対策を考えることができるようになる。

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	セキュリティの６要素について分類，説明できる。代表的な脅威について説明できる。	セキュリティの６要素を区別できる。代表的な脅威について知識がある。	セキュリティの基本要素や，代表的な脅威についての理解が不足している。
評価項目2	代表的な暗号技術の分類や仕組み、応用例を説明できる。その他の技術面でのセキュリティ対策に関する知識がある。	代表的な暗号技術の分類や、応用例を説明できる。その他の技術面でのセキュリティ対策に関する知識がある。	代表的な暗号技術を分類や、応用例を説明できない。その他の技術面でのセキュリティ対策に関する知識が不十分である。
評価項目3	人的な面や法的な面でのセキュリティ対策があることを知っており，対策を評価する方法や法体系について説明できる。	人的な面や法的な面でのセキュリティ対策があることを知っており，対策を評価する方法や法体系についての知識がある。	人的な面や法的な面でのセキュリティ対策があることへの知識が不十分である。

学科の到達目標項目との関係

教育方法等

概要	情報の信頼性と信ぴょう性，セキュリティポリシー，個人情報や知的財産権に関する法律，不正アクセスなどに関する法律と犯罪の現状などについて学習する。また，インターネットなどの我々が普段利用する情報システムにおける情報セキュリティ全般についての基礎と仕組みを理解する。
授業の進め方・方法	定期試験(60%)，及び提出物と小試験(40%)により，総合評価する。
注意点	・1学年で学修した「コンピュータリテラシ」中の「インターネットの基礎」や，3学年で学修した「ネットワークシステム基礎」の内容の一部が基礎になっており，授業概要とねらいに記した内容について，より詳しく学び直す。 ・また，この科目は，「情報セキュリティ」や，「情報社会学」，「通信法規」の基礎となるため，復習予習の双方を行い，理解度を極力上げるように心がけることが，関連科目全般にもよい結果をもたらすことになる。

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	ガイダンス 1. セキュリティの考え方	・セキュリティの6要素について理解する。 ・セキュリティを時系列や，管理方法，リスクコントロール，リスク管理といった観点から見た場合の対策方法が解る。 ・リスクと損失について考えることができる。
		2週	1. セキュリティの考え方	
		3週	2. 脅威	・資産に対する意識と，それらへの脅威が解る。 ・脅威を分類することができる。 ・代表的な侵入の手口が解る。 ・代表的な攻撃手法の名称と，どのようなものであるかとが解る。
		4週	2. 脅威	
		5週	2. 脅威	
		6週	3. 暗号技術	・共通鍵暗号と公開鍵暗号についての知識がある。 ・暗号技術を応用した代表的な手法について説明できる。
		7週	3. 暗号技術	
		8週	4. 技術面でのセキュリティ対策	・技術面での対策には，どのようなものがあるか代表的なものが解る。 ・ファイアウォールの種類，機能，構成，弱点について解る。 ・代表的なセキュリティ対策技術の名称と，どのようなものであるかとが解る。
	2ndQ	9週	4. 技術面でのセキュリティ対策	
		10週	4. 技術面でのセキュリティ対策	
		11週	5. 人的な面でのセキュリティ対策	・情報セキュリティポリシーの概念と，記述，策定について解る。 ・情報資産の洗い出しと，リスク評価，脅威分析，貧弱性分析ができる。
		12週	5. 人的な面でのセキュリティ対策	
		13週	5. 人的な面でのセキュリティ対策	

		14週	6. 法的な面でのセキュリティ対策	・情報セキュリティの国際基準にどのようなものがあるのか解る。 ・プライバシーマーク制度について説明できる。 ・個人情報保護法の内容を説明でき，保護すべき内容が解る。 ・コンピュータ犯罪に対する法律について知っている。 ・情報セキュリティ監査制度について知っている。
		15週	6. 法的な面でのセキュリティ対策	
		16週	答案返却，及び解説	

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
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	変数とデータ型の概念を説明できる。	1	
				代入や演算子の概念を理解し、式を記述できる。	1	
				制御構造の概念を理解し、条件分岐や反復処理を記述できる。	1	
				プロシージャ(または、関数、サブルーチンなど)の概念を理解し、これらを含むプログラムを記述できる。	1	
				ソフトウェア開発に利用する標準的なツールの種類と機能を説明できる。	1	
			ソフトウェア	ソフトウェアを中心としたシステム開発のプロセスを説明できる。	2	
			計算機工学	整数・小数を2進数、10進数、16進数で表現できる。	2	
				基本的な論理演算を行うことができる。	2	
				コンピュータを構成する基本的な要素の役割とこれらの間でのデータの流れを説明できる。	1	
			コンピュータシステム	処理形態の面でのコンピュータシステムの分類である集中処理システムと分散処理システムについて、それぞれの特徴と代表的な例を説明できる。	1	
				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。	1	
			システムプログラム	コンピュータシステムにおけるオペレーティングシステムの位置づけを説明できる。	2	
				プロセス管理やスケジューリングなどCPUの仮想化について説明できる。	1	
			情報通信ネットワーク	プロトコルの概念を説明できる。	2	
				プロトコルの階層化の概念や利点を説明できる。	2	
				ローカルエリアネットワークの概念を説明できる。	2	
				インターネットの概念を説明できる。	2	
				TCP/IPの4階層について、各層の役割を説明でき、各層に関係する具体的かつ標準的な規約や技術を説明できる。	3	
				主要なサーバの構築方法を説明できる。	2	
				情報通信ネットワークを利用したアプリケーションの作成方法を説明できる。	2	
			情報数学・情報理論	ブール代数に関する基本的な概念を説明できる。	2	
				情報源のモデルと情報源符号化について説明できる。	1	
				通信路のモデルと通信路符号化について説明できる。	1	
			その他の学習内容	少なくとも一つの具体的なコンピュータシステムについて、起動・終了やファイル操作など、基本的操作が行える。	3	
				少なくとも一つの具体的なオフィススイート等を使って、文書作成や図表作成ができ、報告書やプレゼンテーション資料を作成できる。	2	
				少なくとも一つのメールツールとWebブラウザを使って、メールの送受信とWebブラウジングを行うことができる。	2	
				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。	3	
				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。	3	
				メディア情報の主要な表現形式や処理技法について説明できる。	1	

評価割合

	定期試験	提出物と小試験					合計
総合評価割合	60	40	0	0	0	0	100
専門的能力	60	0	0	0	0	0	60
基礎的能力	0	40	0	0	0	0	40
	0	0	0	0	0	0	0