仙台高等専門学校	開講年度	令和03年度 (2021年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	0107	科目区分	専門 / 必修
授業形態	授業	単位の種別と単位数	学修単位: 2
開設学科	総合工学科 I 類	対象学年	4
開設期	後期	週時間数	2
教科書/教材	CISCO CCNA Cyber OPSによるオンライン学習		
担当教員	和泉 諭		

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

JABEE (A) 実践技術者としての高度でかつ幅広い基本的能力・素養

教育方法等

概要	この科目はCISCO CCNA Cyber Operations のインストラクター資格を持つ教員が、その経験を生かし、情報セキュリティについてオンライン教材を使用し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、さらに情報資産への攻撃手法とその対策の基礎を学修する。
授業の進め方・方法	オンライン教材を使用し、各自のペースで学習を行うマスタリーラーニングの手法で行う。受講生は事前に教材ページを読んで学習を行う。講義では教材ページに関する詳細や保続を説明することでその理解を深める。また事後学習として各章ごとに用意されたオンライン課題を受講する。
注意点	CISCO networking academyを使用した講義になるので、各自、予習復習が必須である。

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	ガイダンス	サイバーセキュリティの置かれた現状について理解します。
		2週	サイバーセキュリティとSOC	この章では、誰が、なぜ、どのようなサイバー攻撃を仕掛けるのかについて学習します。さまざまな人がさまざまな理由でサイバー犯罪を実行します。セキュリティ オペレーション センターは、サイバー犯罪と闘っています。セキュリティ オペレーション センター（SOC；Security Operations Center）で働くためには、認定資格を取得し、正式な教育を受け、雇用サービスを利用してインターシップ体験や仕事を得て、備えます。
		3週	Windowsオペレーティングシステム	オペレーティング システムの仕組みや Windows エンドポイントを保護するために使用されるツールなど、Windows の基本的な概念について説明します。
		4週	Linuxオペレーティングシステム	Linux の基本的な操作と、管理およびセキュリティ関連タスクを実行する方法を学習します。
		5週	ネットワーク プロトコルとサービス	TCP/IP プロトコル スイートのプロトコルと、SSHなどのコンピュータ ネットワークでタスクを行うための関連サービスの説明を通して、ネットワークが通常どのように動作するのかその概要を示します。
		6週	ネットワーク インフラストラクチャ	有線および無線ネットワーク、ネットワーク セキュリティ、およびネットワークの設計など、ネットワーク インフラストラクチャの基本的な操作について説明します。
		7週	ネットワーク セキュリティの原則	攻撃者がネットワーク攻撃を開始するために使用する各種ツールおよび方法について説明します。
		8週	ネットワーク攻撃：詳細	トラフィック モニタリングの重要性およびその方法について説明します。この後に、IP、TCP、UDP、ARP、DNS、DHCP、HTTP、電子メールなどのネットワーク プロトコルやサービスの脆弱性について詳しく説明します。
	4thQ	9週	ネットワークの保護	ネットワーク セキュリティ防衛のアプローチ、アクセス制御方法、およびサイバーセキュリティ アナリストが脅威インテリジェンスで頼りにするさまざまなソースについて説明します。
		10週	暗号化と公開キー インフラストラクチャ	ネットワーク セキュリティ モニタリングへの暗号化の影響を説明します。

		11週	エンドポイントのセキュリティと分析	エンドポイントの脆弱性と攻撃を調査する方法について説明します。
		12週	セキュリティの監視	セキュリティの監視で使用されるセキュリティ テクノロジーおよびログ ファイルについて学習していきます。
		13週	侵入データの分析	ネットワーク セキュリティ アラートのレポート、評価、エスカレート、および証拠保存の方法について説明します。
		14週	インシデントの対応と処理	インシデント対応および処理のモデルと手順について説明します。これらには、サイバー キル チェーン、ダイヤモンド モデル、VERIS スキーマ、および NIST 発行の Computer Security Incident Response Team（CSIRT）の構造とインシデント対応プロセスのガイドラインなどが含まれます。
		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
専門的能力	分野別の専門工学	情報系分野	情報通信ネットワーク	SSH等のリモートアクセスの接続形態と仕組みについて説明できる。	4	後5
			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

評価割合

	試験	毎週の課題	合計
総合評価割合	70	30	100
基礎的能力	10	10	20
専門的能力	40	10	50
分野横断的能力	20	10	30