豊田工業高等専門学校	開講年度	令和06年度 (2024年度)	授業科目	サイバーセキュリティ

科目基礎情報

科目番号	34236	科目区分	専門 / 選択
授業形態	講義	単位の種別と単位数	学修単位: 2
開設学科	情報工学科	対象学年	4
開設期	後期	週時間数	2
教科書/教材	毎回プリントを配布する。		
担当教員	平野 学		

到達目標

(ア) セキュリティの概念とガバナンス、法と規制、リスク管理とセキュリティ設計原則を説明できる。
(イ) 暗号の基礎、公開鍵基盤とその応用、ID管理とアクセス制御を説明できる。
(ウ) 脆弱性・ネットワーク・ウェブアプリケーションに対する攻撃と防御、セキュリティアセスメントを説明できる。
(エ) セキュリティオペレーション、インシデントレスポンス、ソフトウェア開発セキュリティを説明できる。

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 (ア)	セキュリティの概念とガバナンス、法と規制、リスク管理とセキュリティ設計原則を詳細に説明できる。	セキュリティの概念とガバナンス、法と規制、リスク管理とセキュリティ設計原則を説明できる。	セキュリティの概念とガバナンス、法と規制、リスク管理とセキュリティ設計原則を説明できない。
評価項目 (イ)	暗号の基礎、公開鍵基盤とその応用、ID管理とアクセス制御を詳細に説明できる。	暗号の基礎、公開鍵基盤とその応用、ID管理とアクセス制御を説明できる。	暗号の基礎、公開鍵基盤とその応用、ID管理とアクセス制御を説明できない。
評価項目 (ウ)	脆弱性・ネットワーク・ウェブアプリケーションに対する攻撃と防御、セキュリティアセスメントを詳細に説明できる。	脆弱性・ネットワーク・ウェブアプリケーションに対する攻撃と防御、セキュリティアセスメントを説明できる。	脆弱性・ネットワーク・ウェブアプリケーションに対する攻撃と防御、セキュリティアセスメントを説明できない。
評価項目 (エ)	セキュリティオペレーション、インシデントレスポンス、ソフトウェア開発セキュリティを詳細に説明できる。	セキュリティオペレーション、インシデントレスポンス、ソフトウェア開発セキュリティを説明できる。	セキュリティオペレーション、インシデントレスポンス、ソフトウェア開発セキュリティを説明できない。

学科の到達目標項目との関係

学習・教育到達度目標 A3 コンピュータネットワークの動作を通信理論の観点から数理的に解析できる.
JABEE d 当該分野において必要とされる専門的知識とそれらを応用する能力
本校教育目標 ① ものづくり能力

教育方法等

概要	この科目では情報通信システムの運用で必要とされるサイバーセキュリティの概念とガバナンスを理解し、法と規制、リスク管理、セキュリティ設計原則に基づいて、技術的・組織的・物理的・人的な管理策（コントロール）を選択、実装する方法を学ぶ。具体的には暗号の基礎、公開鍵基盤とその応用、ID管理とアクセス制御、脆弱性・ネットワーク・ウェブアプリケーションに対する攻撃と防御、セキュリティアセスメント、セキュリティオペレーション、インシデントレスポンス、そしてソフトウェア開発セキュリティの基礎的事項の学習を通して、組織がサイバーセキュリティリスクを低減するために用いる管理策（コントロール）を学ぶ。この科目は企業でインターネットサービスを開発していた教員がその経験を生かし、サイバー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。
授業の進め方・方法	毎週プリントを配布し、プリントにノートを記入していく形式で授業を進める。本講義の演習は受講者のノートパソコン上の「サンドボックス化された（外部から隔離された）仮想環境」でおこなう。自学自習用の教材として Cisco 社の eラーニング教材 CCNA Cybersecurity Operations（ネットワーキングアカデミー https://www.netacad.com）を提供する。
注意点	継続的に授業内容の予習・復習を行うこと。授業内容について、決められた期日までの課題（レポート）提出を求める。ノートパソコンを持参すること。 サイバーセキュリティ技術者育成トレーニングにはサイバー攻撃とその防御を理解するための実践的な演習が含まれる。本講義の演習は「サンドボックス化された（外部から隔離された）仮想環境」の中だけで行う。受講者は演習に先立ちサイバー犯罪に適用される刑法ならびに関係する法律を学ぶ。日本を含む多くの国では不正アクセスは犯罪であり犯人の動機に関係なく厳罰を伴う。受講者は本講義で利用したツールや脆弱性を、倫理的な方法でのみ、かつ「サンドボックス化された（外部から隔離された）仮想環境」でのみ使用する必要があること、知り得た知識やツールを倫理的ではない目的に悪用しないことを約束する誓約書を提出する。

選択必修の種別・旧カリ科目名

選択必修３，規制技術に含まれるものはない。

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

必履修

授業計画

		週	授業内容	週ごとの到達目標
後期	3rdQ	1週	セキュリティの概念とガバナンス：セキュリティの三要素、セキュリティガバナンス、セキュリティ管理策（コントロール）フレームワーク （自学自習内容）ケース分析、課題の提出	セキュリティの概念とガバナンスを説明できる.
		2週	法と規制：サイバーセキュリティ関連の法（刑法、不正アクセス禁止法、個人情報保護法、プロバイダ責任制限法等）、規制（PCI-DSS等） （自学自習内容）ケース分析、課題の提出	サイバーセキュリティ関連の法と規制を説明できる。
		3週	リスク管理とセキュリティ設計原則：資産の特定と管理、リスクの管理と定量的評価、災害復旧と事業継続計画、セキュリティ設計原則（多層防御、最小権限、職務分離等） （自学自習内容）ケース分析、課題の提出	リスク管理とセキュリティ設計原則を説明できる。

		4週	暗号の基礎：暗号で用いられる数学、暗号の種類、対称暗号アルゴリズム、鍵配布問題、ハッシュ関数 （演習）OpenSSLを用いた対称暗号アルゴリズムによる暗号化、ハッシュ関数の利用、ツールを用いた暗号解読攻撃と防御 （自学自習内容）課題の提出	暗号の基礎、対称暗号とハッシュ関数を説明できる。
		5週	公開鍵基盤とその応用：非対称暗号アルゴリズム、DH鍵交換、電子署名、通信プロトコルへの応用（TLS、IPsec）、公開鍵基盤、政府認証基盤と電子申請 （演習）OpenSSLを用いた非対称暗号アルゴリズムによる暗号化と電子署名の利用 （自学自習内容）課題の提出	公開鍵基盤とその応用を説明できる。
		6週	ID管理とアクセス制御：AAAサービスの要素、認証要素と多要素認証、IDのライフサイクル、シングルサインオン、アクセスコントロールモデル（DAC、RBAC、MAC等） （演習）Linux と Windows でのID管理とアクセス制御 （自学自習内容）課題の提出	ID管理とアクセス制御を説明できる。
		7週	脆弱性に対する攻撃と防御：脅威モデリング（STRIDE等）、マルウェアとAPT、サイバーキルチェーン、脆弱性とCVE、ゼロデイ攻撃、アップデートの重要性 （演習）権限昇格攻撃と防御 （自学自習内容）課題の提出	脆弱性に対する攻撃と防御を説明できる。
		8週	ネットワークに対する攻撃と防御（１）：OSIモデルとTCP/IPモデル、通信の解析、境界防御、ファイアウォール、ウェブアプリケーションファイアウォール（WAF）、プロキシ、リモートアクセスとVPN （演習）ファイアウォールの設定 （自学自習内容）課題の提出	ネットワークに対する攻撃と防御（境界防御）を説明できる。
	4thQ	9週	ネットワークに対する攻撃と防御（２）：IPアドレスとドメイン名、ドメイン名システム（DNS）、権威DNSサーバとキャッシュDNSサーバ、フィッシングサイト （演習）DNSキャッシュポイズニング攻撃と防御 （自学自習内容）課題の提出	ネットワークに対する攻撃と防御（通信プロトコルの脆弱性）を説明できる。
		10週	ネットワークに対する攻撃と防御（３）：ブロードキャストドメインとLAN、セグメント分割とVLAN、中間者攻撃 （演習）ARPキャッシュポイズニング攻撃と防御 （自学自習内容）課題の提出	ネットワークに対する攻撃と防御（通信プロトコルの脆弱性）を説明できる。
		11週	ウェブアプリケーションに対する攻撃と防御：インジェクション攻撃（SQLインジェクション、コマンドインジェクション、クロスサイトスクリプティング等）、OWASPが公開するセキュリティ情報 （演習）SQLインジェクション攻撃と防御 （自学自習内容）課題の提出	ウェブアプリケーションに対する攻撃と防御を説明できる。
		12週	セキュリティアセスメント：ネットワーク探索スキャン、脆弱性スキャン、ペネトレーションテストと法令順守 （演習）nmap と Metasploit を用いたセキュリティテスト （自学自習内容）課題の提出	セキュリティアセスメントを説明できる。
		13週	セキュリティオペレーション：セキュリティ設計原則の適用、資産の特定と管理、構成管理とパッチ管理、ロギング、セキュリティモニタリング （演習）ログを用いたセキュリティモニタリング （自学自習内容）課題の提出	セキュリティオペレーションを説明できる。
		14週	インシデントレスポンス：インシデントの予防と検知、ロギングとモニタリング、インシデントレスポンスの手順、証拠収集とフォレンジック、MITRE ATT&CK と攻撃元特定 （演習）インシデントレスポンス （自学自習内容）課題の提出	インシデントレスポンスを説明できる。
		15週	ソフトウェア開発セキュリティ：プログラミング言語、ライブラリ、入力検証、エラーハンドリング、ロギング、ソフトウェア開発ライフサイクル、テスト、コード署名 （演習）ライブラリの脆弱性に関する攻撃と防御 （自学自習内容）課題の提出	ソフトウェア開発セキュリティを説明できる。
		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
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	基本的なフィルタリング技術について説明できる。	4	後8
			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,後3,後7
				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,後3,後7
				基本的な暗号化技術について説明できる。	4	後4,後5
				基本的なアクセス制御技術について説明できる。	4	後6
				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,後3,後7

評価割合			
	定期試験	課題	合計
総合評価割合	50	50	100
専門的能力	50	50	100