熊本高等専門学校	開講年度	令和06年度 (2024年度)	授業科目	情報セキュリティ

科目基礎情報

科目番号	HI1505	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: 1
開設学科	人間情報システム工学科	対象学年	5
開設期	前期	週時間数	1
教科書/教材	OneNote class NotebookやWebClass等で提示する。 参考書1=菊池浩明、上原哲太郎、「IT Text ネットワークセキュリティ」、オーム社。 参考書2=齋藤孝道、「マスタリングTCP/IP情報セキュリティ編」。		
担当教員	藤井 慶		

到達目標

1. UNIXでの基本的なサーバ・クライアント設定、セキュリティ（フィルタリング）設定を行える。
2. サイバーセキュリティ、特にネットワークセキュリティの主要なトピックについて説明できる。
3. 共通鍵暗号、公開鍵暗号の仕組みを説明できる。そして公開鍵暗号をユーザ認証等に活用できる。
4. 認証の仕組みについて説明できる。

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
ネットワーク設定	UNIXを使って適切かつ効率良くサーバ設定、セキュリティ設定を行える。	UNIXを使って適切に基本的なサーバ設定、セキュリティ設定を行える。	UNIXを使って適切に基本的なサーバ設定、セキュリティ設定を行えない。
サイバーセキュリティ、特にネットワークセキュリティ	サイバーセキュリティ、特にネットワークセキュリティの主要な事柄について深く理解し、説明できる。	サイバーセキュリティ、特にネットワークセキュリティの主要な事柄について概ね理解し、説明できる。	サイバーセキュリティ、特にネットワークセキュリティの主要な事柄を理解できない。
暗号技術	各種暗号技術の仕組みについて深く理解し、説明できる。そして公開鍵暗号をユーザ認証等に活用できる。	各種暗号技術の仕組みについて概ね理解し、説明できる。そして公開鍵暗号をユーザ認証等に活用できる。	各種暗号技術の仕組みを理解できない。公開鍵暗号をユーザ認証等に活用できない。
認証技術	認証の仕組みについて深く理解し、説明できる。	認証の仕組みについて概ね理解し、説明できる。	認証の仕組みについて理解できない。

学科の到達目標項目との関係

教育方法等

概要	ICTが社会基盤の一つになった現在、サイバーセキュリティの役割はますます重要になっている。サイバーセキュリティの知識はネットワーク運用をはじめとした様々な場面で必須であり、セキュリティ技術者の需要も増えている。サイバーセキュリティの分野は広く、本科目では講義および演習によってその一部の事柄を学ぶ。 全15週のうち第14週の授業については、情報セキュリティを業務とする企業より講師を招聘し、業界の最新の知識・技術についての講義を受ける。
授業の進め方・方法	授業は主に講義形式でOneNote class Notebookを用いて行う。また、時折演習を行う場合がある。演習場所や内容は適宜指示する。演習の成果は主にレポートで評価するが、進度に応じて小テストを行う場合がある。また定期試験については主に評点の低い学生を対象に別途再評価試験や追加課題を行う場合がある。
注意点	【大前提として】 セキュリティに関する知識・技術は他者から自分を守るためのものだが、攻撃と防御は表裏一体であり、使い方を誤ると他者に迷惑をかける技術にもなり得る。そのため学習者は倫理観（情報モラル）を適切に備えていることが大前提である。万が一看過できないほどの倫理的な欠落が認められた場合、たとえ技術的な理解が十分であったとしても、評価に値しないと見做し厳しく減点する可能性がある。 【自学・自習について】 本科目は1単位の学修科目であり、30時間(15コマ)の授業に加えて15時間の自学・自習が求められる。自学・自習では、一般的な予習・復習・試験勉強に加え、各単元の課題レポート作成などを求める。加えて、本科目はあくまでも基礎的な知識の概要に触れるまでのものであることから、より細かい所や授業で詳細に触れなかった所については自主的に補完することが望ましい。 【関連する資格・科目について】 本科目は4年情報ネットワークに深く関係するため、基礎用語や概念をよく復習しておくこと。また本科目に関連の深い資格として「情報セキュリティマネジメント」「基本情報技術者試験」がある。情報系の基盤となる知識を押さえやすい資格であるため、取得を推奨する。

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
前期	1stQ	1週	情報セキュリティの基礎	情報セキュリティの3要素、主要な脅威について説明できる。
		2週	ネットワーク、セキュリティ設定(1)	基本的なネットワーク設定、セキュリティ設定を行える。
		3週	ネットワーク、セキュリティ設定(2)	基本的なネットワーク設定、セキュリティ設定を行える。
		4週	ネットワークセキュリティとマルウェア対策(1)	代表的な不正アクセスとその対策法について説明できる。
		5週	ネットワークセキュリティとマルウェア対策(2)	マルウェアについて説明できる。
		6週	ネットワークセキュリティとマルウェア対策(3)	ファイアウォールの仕組みを説明できる。
		7週	暗号技術(1)	共通鍵暗号の概要、バーナム暗号の仕組みについて説明できる。
		8週	暗号技術(2)	代表的な運用モードについて説明できる。

	2ndQ	9週	暗号技術(3)	公開鍵暗号の仕組みについて説明できる。公開鍵と秘密鍵のペアを生成し、公開鍵暗号を使った暗号化・復号処理や遠隔ログインができる。
		10週	PKI	PKIについて説明できる。
		11週	認証技術	主な認証技術について説明できる。
		12週	ログ解析(1)	webやメールなどの代表的なログを読み解くことができる。
		13週	ログ解析(2)	webやメールなどの代表的なログを読み解くことができる。
		14週	セキュリティの動向	近年のセキュリティの動向について把握できている。
		15週	定期試験	これまで学習した事柄についての理解が定着できている。
		16週	定期試験答案返却	

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。	3	前1
				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。	3	前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を認識している	3	前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。	3	前1
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	前2,前3,前4
			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	前2,前3,前4
				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	前2,前3,前4
				基本的な暗号化技術について説明できる。	4	前5,前6,前7
				基本的なアクセス制御技術について説明できる。	4	前2,前3,前4
				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	前2,前3,前4

評価割合

	試験	小テスト・報告書・演習	合計
総合評価割合	60	40	100
基礎的能力	30	20	50
専門的能力	30	20	50
分野横断的能力	0	0	0