熊本高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	情報セキュリティ特論

科目基礎情報

科目番号	AE1122	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	電子情報システム工学専攻	対象学年	専1
開設期	前期	週時間数	2
教科書/教材	教科書=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=齋藤孝道、「マスタリングTCP/IP情報セキュリティ編」、オーム社、その他オンライン学習システム等		
担当教員	藤井 慶		

到達目標

1. 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。
2. 共通鍵暗号、公開鍵暗号の仕組みをそれぞれ説明できる。そして公開鍵暗号をユーザ認証等に活用できる。
3. 生体認証の仕組みについて説明できる。
4. ネットワークやセキュリティの基本的な設定を適切に行える。

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
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説明できない。
ネットワーク上の脅威と対策	ネットワーク上の主要な脅威とその対策について深く理解し、説明できる。	ネットワーク上の主要な脅威とその対策について概ね理解し、説明できる。	ネットワーク上の主要な脅威とその対策を説明できない。
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説明できない。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説明できない。
ネットワーク設定、セキュリティ設定	適切かつ効率よくネットワーク設定、セキュリティ設定を行える。	適切にネットワーク設定、セキュリティ設定を行える。	一定時間内に適切にネットワーク設定、セキュリティ設定を行えない。

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、サイバー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、半期で完結するものではないが、本科目では教科書とオンライン学習コンテンツとを併用し、その一端を学ぶ。 本科目に関連の深い資格としてIPA情報処理技術者試験の「情報セキュリティマネジメント試験「基本情報技術者試験」がある。
授業の進め方・方法	授業は講義形式と演習形式とで行う。いずれの形式でも主にOneNote class Notebookを用いるため、ノートPCを持参すること。演習の場所や内容は適宜指示する。演習の成果はレポートや小テストで評価する。
注意点	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たり法や学則を犯す技術にもなり得る。そのため学習者は倫理観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欠落が認められた場合、たとえ知識・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。 演習・事前/事後学習は主にオンラインで行う。演習内容によっては管理権限を必要とすることがある。その際には管理権限を持つPCを各自用意する必要がある。 本科目は2単位の学修科目である。規定授業時間は30時間であり、1単位あたり30時間程度の自学学習が求められる。

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	ガイダンス、情報セキュリティの基礎(1)	情報セキュリティを学ぶ意義を理解できる。 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。 情報セキュリティに関する基礎用語について説明できる。
		2週	情報セキュリティの基礎(2)	同上
		3週	ネットワーク設定演習(1)	UNIXマシンを適切に設定し、ネットワークに接続できる。
		4週	暗号技術(1)	共通鍵暗号の概要、運用モード、バーナム暗号の仕組みについて説明できる。
		5週	暗号技術(2)	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。
		6週	暗号技術(3)	同上
		7週	認証技術(1)	公開鍵暗号に基づく認証基盤PKIとSSL/TLSの原理について説明できる。
		8週	認証技術(2)	二要素認証、生体認証、指紋認証の原理について説明できる。
	2ndQ	9週	ネットワーク設定演習(2)	パケットフィルタリングによるパーソナルファイアウォールを適切に設定できる。

		10週	ネットワーク上の脅威と対策(1)	既存の通信サービスに対する主な攻撃について説明できる。 ファイアウォールをはじめとする、サーバ運用に必要なセキュリティ技術について説明できる。
		11週	ネットワーク上の脅威と対策(2)	同上
		12週	ネットワーク上の脅威と対策(3)	同上
		13週	ネットワーク上の脅威と対策(4)	同上
		14週	監視、分析	ネットワークの監視法や侵入検知法について説明できる。 代表的な通信サービスのログの基本的な読み方が分かる。
		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

評価割合

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