石川工業高等専門学校	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	20339	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	履修単位: 1
開設学科	電子情報工学科	対象学年	5
開設期	後期	週時間数	2
教科書/教材	情報セキュリティ基礎講義（コロナ社）		
担当教員	長岡 健一		

到達目標

1．情報セキュリティとその動向について概説できる。
2．セキュリティ脅威，マルウェアについて説明できる。
3．暗号化技術について理解し，説明できる。
4．ディジタル署名について理解し，説明できる。
5．サイバー攻撃手法について理解し，説明できる.
6．ネットワークセキュリティ技術について理解し，説明できる。
7．セキュリティ管理について理解し，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
到達目標 項目1	情報セキュリティとその動向について概説し，起こりうる課題について議論できる.	情報セキュリティとその動向について概説できる。	情報セキュリティとその動向について概説することが困難である.
到達目標 項目2	セキュリティ脅威，マルウェアについて説明でき，応用課題について考察することができる.	セキュリティ脅威，マルウェアについて説明できる.	セキュリティ脅威，マルウェアについて説明することが困難である.
到達目標 項目3, 4	暗号化技術とディジタル署名について理解し，説明できるとともに，応用課題について考察することができる.	暗号化技術とディジタル署名について理解し，説明できる.	暗号化技術とディジタル署名について理解し，説明することが困難である.
到達目標 項目5, 6	サイバー攻撃手法とネットワークセキュリティについて理解し，説明でき，応用課題について考察することができる.	サイバー攻撃手法とネットワークセキュリティについて理解し，説明できる.	サイバー攻撃手法とネットワークセキュリティについて理解し，説明することが困難である.
到達目標 項目7	セキュリティ管理について理解し，説明でき，応用課題について考察することができる.	セキュリティ管理について理解し，説明できる.	セキュリティ管理について理解し，説明することが困難である.

学科の到達目標項目との関係

本科学習目標 1 本科学習目標 2 本科学習目標 3
創造工学プログラム B1専門(電気電子工学&情報工学)

教育方法等

概要	情報通信技術の進展と普及が進む一方で，情報セキュリティの重要性がますます高まっている．本授業では情報セキュリティとは何か，またその動向について概説し，セキュリティに関する技術やセキュリティ管理手法について詳説する．このように，情報セキュリティ分野における応用的学力と専門知識を身につけ，課題解決について意欲的に取り組むことができるようになることなどを目標とする。
授業の進め方・方法	WebClassやteamsで配布する資料に基づき座学で授業を行う．また，適宜課題・演習を行う. 【事前事後学習】到達目標の達成度を確認するため，適宜，演習課題を与える。 【関連科目】情報通信I，情報通信II，情報通信III，電子情報工学実験V 【MCC対応】Ⅳ-B　技術者倫理および技術史，Ⅳ-C 情報リテラシー，V-D-6 情報通信ネットワーク，V-D-8 その他の学習内容，情報教育対応科目
注意点	平常時の予習・復習が大事です。課題のレポートは必ず提出すること。ただ事項を暗記するのではなく，仕組みを理解し理論的に説明できるようにすること。並行して実施される電子情報工学実験V「情報セキュリティ」にて演習を行うので，そちらも参考にすること．なお，毎時間WebClassおよびteamsにて資料を配布するので，各自授業開始時までにダウンロードし準備しておくこと。また，適時オンラインで講義することがある. 【評価方法・評価基準】成績の評価基準として60点以上を合格とする。 中間試験（35%），期末試験（35%），課題（30%）

テスト

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	情報セキュリティとは	情報セキュリティとは何か理解し，説明できる.
		2週	情報セキュリティの最新動向	情報セキュリティの最新動向について説明できる.
		3週	セキュリティ脅威	セキュリティ脅威について理解し，説明できる.
		4週	マルウェア	マルウェアについて理解し，説明できる.
		5週	暗号化技術1（古典暗号）	暗号化技術とは何か，古典暗号について理解し，説明できる.
		6週	暗号化技術2（共通鍵，公開鍵暗号基盤）	共通鍵，公開鍵暗号基盤について理解し，説明できる.
		7週	暗号化技術3（SSL）	SSLの動作，仕組みを理解し，説明できる.
		8週	ディジタル署名（メッセージダイジェスト，MD5，SHA）	ディジタル署名について理解し，説明できる.
	4thQ	9週	サイバー攻撃手法1（SQLインジェクション，クロスサイトスクリプティング）	SQLインジェクション，クロスサイトスクリプティングを理解し，説明できる.

		10週	サイバー攻撃手法2（パスワードクラック，DoS，標的型攻撃）	パスワードクラック，DoS，標的型攻撃について理解し，説明できる.
		11週	サイバー攻撃手法3（DNSハイジャック，経路ハイジャック）	DNSハイジャック，経路ハイジャックについて理解し，説明できる.
		12週	ネットワークセキュリティ1（ファイアウォール，パケットフィルタリング，無線LANセキュリティ）	ファイアウォール，パケットフィルタリング，無線LANセキュリティについて理解し，説明できる.
		13週	ネットワークセキュリティ2（VPN，認証）	VPN，認証方式（IPSec，IEEE802.1X）について理解し，説明できる.
		14週	セキュリティ管理（セキュリティポリシー，CSIRT）	セキュリティ管理の概要と，セキュリティポリシー，CSIRTについて理解し，説明できる.
		15週	試験前復習	
		16週	前期復習	

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	
				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	
				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	
				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	
専門的能力	分野別の専門工学	情報系分野	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	
				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	
				基本的な暗号化技術について説明できる。	4	
				基本的なアクセス制御技術について説明できる。	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	

評価割合

	試験	レポート	合計
総合評価割合	70	30	100
基礎的能力	0	0	0
専門的能力	70	30	100
分野横断的能力	0	0	0