豊田工業高等専門学校	開講年度	令和04年度 (2022年度)	授業科目	ネットワークセキュリティ

科目基礎情報

科目番号	95025	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	情報科学専攻	対象学年	専2
開設期	前期	週時間数	2
教科書/教材	「情報セキュリティ入門　情報倫理を学ぶ人のために（改訂版）」 佐々木良一監修，会田和弘（共立出版）ISBN:978-4-320-12376-2／（参考書）「実践パケット解析」Chris Sanders（オライリージャパン）ISBN:978-4873115696／（参考書）「アナライジングマルウェア」新井悠 他（オライリージャパン）ISBN:978-4873114552		
担当教員	平野 学		

到達目標

(ア)インターネット社会が抱える問題に対する倫理の重要性を理解できる。
(イ)TCP/IPネットワークのレベルでのセキュリティ対策を理解できる。
(ウ)ウェブアプリケーションのセキュリティ対策を理解できる。
(エ)共有鍵暗号、公開鍵暗号、ハッシュ関数、電子署名の基礎的な考え方を理解できる。
(オ)マルウェアの仕組みと解析手法を理解できる。
(カ)情報セキュリティの法制度の基礎を理解できる。

ルーブリック

	理想的な到達レベルの目安	最低限の到達レベルの目安(良)	未到達レベルの目安
評価項目(ア)	インターネット社会が抱える問題に対する倫理の重要性とセキュリティに関する法律を理解でき、自分の言葉で具体的な事例について説明できる。	インターネット社会が抱える問題に対する倫理の重要性とセキュリティに関する法律を説明できる。	インターネット社会が抱える問題に対する倫理の重要性とセキュリティに関する法律を説明できない。
評価項目(イ)	TCP/IPネットワーク、ウェブアプリケーションのセキュリティ対策を理解でき、応用的な対策についても説明できる。	TCP/IPネットワーク、ウェブアプリケーションのセキュリティ対策を説明できる。	TCP/IPネットワーク、ウェブアプリケーションのセキュリティ対策を説明できない。
評価項目(ウ)	共通鍵暗号、公開鍵暗号、ハッシュ関数、電子署名の基礎を理解でき、実際の社会での応用事例についても説明できる。	共通鍵暗号、公開鍵暗号、ハッシュ関数、電子署名の基礎を説明できる。	共通鍵暗号、公開鍵暗号、ハッシュ関数、電子署名の基礎を説明できない。

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	この講義の目的はインターネットによって生じる様々な社会問題を技術、倫理、法律のそれぞれの観点から正しく理解することである。まず、インターネット社会が抱える問題を説明し、そのリスク評価手法を学ぶ。そして、法律の観点からインターネット社会を健全に維持する仕組みを学び、最後に技術者としての倫理の重要性を学習する。技術的観点からは、TCP/IPレベルでのセキュリティ対策を学習し、その後にウェブアプリケーション特有のセキュリティ対策を学ぶ。続いて、セキュリティ対策に必要な暗号の基礎を学ぶ。最後に、様々なセキュリティ事件の原因となり得るマルウェアの仕組みとその解析手法を学習する。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、インターネットサービス構築の際に考慮すべきセキュリティ上の脅威と対策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	授業では各自のノートパソコンに仮想マシンをインストールし、その環境のなかでサイバー攻撃とその防御機構を構築する演習をおこなう。本講義はサイバー攻撃を模擬するセキュリティ検査ツールを利用する。よって演習を開始する前に必ず受講生はサイバーセキュリティ関連の法律を学び、さらに法律でカバーできない範囲の行動基準として「倫理」の重要性も学ぶ。
注意点	毎週、ノートパソコンを持参すること。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。

選択必修の種別・旧カリ科目名

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	シラバスの説明 インターネット社会と情報倫理（１章） （自学自習内容）最新のサイバーセキュリティ事件に関する調査	インターネット社会と情報倫理を理解できる。
		2週	インターネット社会が抱える問題（２章） （自学自習内容）クッキーを用いた広告トラッキングに関する調査	インターネット社会が抱える問題を理解できる。
		3週	情報セキュリティとは（３章） セキュリティのCIA （機密性、完全性、可用性）、リスク分析 （自学自習内容）セキュリティ事件のリスクの評価	セキュリティのCIA （機密性、完全性、可用性）、リスク分析を理解できる。
		4週	情報セキュリティの技術的対策（４章） （自学自習内容）情報セキュリティの技術的対策の復習	情報セキュリティの技術的対策の概要を理解できる。
		5週	インターネット社会と法（５章） 情報倫理教育へ向けて（６章） （自学自習内容）不正アクセス禁止法の条文の理解	インターネット社会と法を理解できる。情報倫理教育の重要性を理解できる。
		6週	演習（１）：　ポートスキャンとOS推測、Wiresharkによるパケットの解析 （自学自習内容）演習内容をまとめて課題として提出	ポートスキャンとOS推測を理解できる。

		7週	演習（2）： ファイアウォール、ARPスプーフィング攻撃と対策、Wireshark によるパケットの解析 （自学自習内容）演習内容をまとめて課題として提出	ファイアウォール、ARPスプーフィング攻撃と対策を理解できる。
		8週	ウェブアプリケーションのセキュリティ（1）： OSコマンドインジェクション攻撃と対策、アクセスログの分析 （自学自習内容）演習内容をまとめて課題として提出	OSコマンドインジェクション攻撃と対策、アクセスログの分析を理解できる。
	2ndQ	9週	ウェブアプリケーションのセキュリティ（2）： SQLインジェクション攻撃と対策 （自学自習内容）演習内容をまとめて課題として提出	SQLインジェクション攻撃と対策を理解できる。
		10週	ウェブアプリケーションのセキュリティ（3）： クロスサイトスクリプティング攻撃と対策 （自学自習内容）演習内容をまとめて課題として提出	クロスサイトスクリプティング攻撃と対策を理解できる。
		11週	暗号（1）： 共通鍵暗号、ハッシュ関数、 OpenSSLによる演習、パスワード解析ツールによる演習 （自学自習内容）演習内容をまとめて課題として提出	共通鍵暗号、ハッシュ関数を理解できる。
		12週	暗号（2）： 公開鍵暗号、RSAアルゴリズムによる暗号化と電子署名、 OpenSSL による演習 （自学自習内容）演習内容をまとめて課題として提出	公開鍵暗号、RSAアルゴリズムによる暗号化と電子署名を理解できる。
		13週	マルウェア解析（1）： 不正プログラムの特徴、マルウェア解析の手順、脆弱性の報告、逆アセンブラ IDA Pro の使い方 （自学自習内容）IDA Pro の使い方を復習	不正プログラムの特徴、マルウェア解析の手順、脆弱性の報告、逆アセンブラ IDA Pro の使い方を理解できる。
		14週	マルウェア解析（2）： 逆アセンブラ IDA Pro による模擬マルウェアの静的解析 （自学自習内容）演習内容をまとめて課題として提出	逆アセンブラ IDA Pro による模擬マルウェアの静的解析を理解できる。
		15週	総まとめ （自学自習内容）これまでの授業の復習と定期試験の対策	総まとめ
		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

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