豊田工業高等専門学校	開講年度	平成30年度 (2018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／「実践パケット解析」Chris Sanders（オライリージャパン）ISBN:978-4873115696_x000B_「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		

目的・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こと。

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理解できる。	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理解できない。
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理解できる。	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理解できない。
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、電子署名の基礎を理解できる。	共通鍵暗号、公開鍵暗号、ハッシュ関数、電子署名の基礎を理解できない。

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た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、それらのリスクを分析する方法を学習する。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習する。続いて、セキュリティ対策に必要な暗号の基礎を学習する。さらに、様々な問題の原因になっているマルウェアの仕組みと解析手法を学習する。最後に、法律的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。
授業の進め方と授業内容・方法	
注意点	演習にてノートパソコンを利用するので毎回持参すること。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

授業計画

		週	授業内容・方法	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（教科書　1章）	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　（教科書　2章）	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　（教科書　3章）：　セキュリティのCIA （機密性、完全性、可用性）、リスク分析	セキュリティのCIA （機密性、完全性、可用性）、リスク分析の基礎を理解できる。
		4週	情報セキュリティの技術的対策　（教科書　4章）	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	演習（1）：　ポートスキャンとOS推測、ファイアウォールの設定、Wireshark によるパケットの解析	ポートスキャンとOS推測、ファイアウォールの設定、Wireshark によるパケットの解析がおこなえる。
		6週	演習（2）：　ARPとDHCPのパケット解析、なりすまし攻撃への対策	ARPとDHCPのパケット解析でき、なりすまし攻撃への対策を理解できる。
		7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への対策、アクセスログの分析方法	OSコマンドインジェクション攻撃への対策、アクセスログの分析方法を理解できる。
		8週	ウェブアプリケーションのセキュリティ（2）：　SQLインジェクション攻撃への対策	SQLインジェクション攻撃への対策を理解できる。
	2ndQ	9週	ウェブアプリケーションのセキュリティ（3）：クロスサイトスクリプティング攻撃への対策	クロスサイトスクリプティング攻撃への対策を理解できる。
		10週	暗号（1）：　共通鍵暗号、 OpenSSLによる演習	共通鍵暗号について理解できる。
		11週	暗号（2）：　公開鍵暗号、ハッシュ関数、電子署名、 OpenSSL による演習	公開鍵暗号、ハッシュ関数、電子署名について理解できる。
		12週	マルウェア解析（1）：　マルウェア解析と脆弱性の報告	マルウェア解析手法（静的解析）と脆弱性の報告について理解できる。
		13週	マルウェア解析（2）：　逆アセンブラによる静的解析の演習	逆アセンブラによる模擬マルウェアの静的解析をおこなえる。

		14週	インターネット社会と法　（教科書　５章）、情報倫理教育へ向けて　（教科書　６章）	インターネット社会と関連する法律について理解できる。倫理の重要性を理解でき、インターネットを社会に役立つように活用する考え方を理解できる。
		15週	総まとめ	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