

佐世保工業高等専門学校		開講年度	平成30年度 (2018年度)		授業科目	情報処理Ⅱ
科目基礎情報						
科目番号	0085		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: 1		
開設学科	機械工学科		対象学年	5		
開設期	後期		週時間数	1		
教科書/教材	K-SEC高学年共通教材					
担当教員	中浦 茂樹					
到達目標						
1. 機械工学分野における情報セキュリティ対策の課題を指摘できる。 2. 情報セキュリティの基盤技術である、情報通信の基礎技術を理解し説明できる。 3. 情報セキュリティを体系的に理解し、攻撃や事故の事例を体系に則って説明できる。						
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		
評価項目1 (到達目標 1)		機械工学分野における特定のケースでの情報セキュリティの課題を指摘することができ、是正するための情報技術分野を特定することができる。	機械工学分野における特定のケースでの情報セキュリティの課題を指摘することができる。	機械工学分野における特定のケースでの情報セキュリティの課題を指摘することができない。		
評価項目2 (到達目標 2)		TCP/IPネットワークと、その背景となるコンピュータの仕組みを説明することができる。 ネットワーク：(良)に加え、生じがちな基本的接続トラブル（物理配線，WiFi設定，IPアドレス設定）の対処法を説明できる。 コンピュータの仕組み：(良)に加え、生じがちなPCトラブル（ドライバ等のハードウェア接続トラブル，ハードディスク障害，メモリ不足，パフォーマンス劣化，OSとアプリケーションの不適合）の対処や予防の方法を説明できる。	TCP/IPネットワークと、その背景となるコンピュータの仕組みを説明することができる。 ネットワーク：インターネットの閲覧の流れを，TCP/IPプロトコルモデル（階層）に沿って説明できる。 コンピュータの仕組み：五大装置，OSとプログラムの役割を，実際の機器に照らし合わせて説明できる。市販されている機器の商品カタログを見て，特徴を説明できる。	TCP/IPネットワークと，その背景となるコンピュータの仕組みを説明することができない。 ネットワーク：インターネットの閲覧の流れを説明できない。 コンピュータの仕組み：実際の機器が果たしている役割を説明することができない。		
評価項目3 (到達目標 3)		(良)に加え，セキュリティ事故の事例や攻撃手法と，その対策技術を説明することができる。（7つ以上説明できることが望ましい。）	情報セキュリティ関連の用語（資産，脅威，脆弱性，気密性，完全性，可用性）を説明できる。 1つ～2つの代表的なセキュリティの脅威の説明と，その対策の特定をすることができる。	情報セキュリティ関連の用語（資産，脅威，脆弱性，気密性，完全性，可用性）を説明できない。 代表的なセキュリティの脅威の説明と，その対策の特定ができない。		
学科の到達目標項目との関係						
教育方法等						
概要	情報セキュリティの基本的な技術・知識を習得する。 （1）機械工学分野における，情報セキュリティの課題を特定し，対処や対策を適切に取れるようにする。【導入】 （2）そのために，情報セキュリティの定義や用語を知り，事故や攻撃に対するセキュリティ技術を理解する。【1～2章，10～11章】 （3）（2）を理解するためには，その基礎技術であるIT技術（コンピュータ基礎，ネットワーク技術）を習得する必要がある。【3～9章】 （4）情報システムを俯瞰できるように，システム運用や新しい技術であるクラウドコンピューティングを紹介している。【12～15章】					
授業の進め方・方法	予備知識：これまでに学習してきた，情報セキュリティ基礎の知識 講義室： 授業形式：講義，グループワーク 学生が用意するもの：可能であれば，BYOD端末があるとよい					
注意点	評価方法：各章毎の確認テストを50%，グループワークとして行う活動等での態度・内容をそれぞれ25%により評価し，60点以上を合格とする。 自己学習の指針：授業後の復習をしっかりと行い，各章ごとの確認テストを独力で取り組む。これらの自己学習時間は，十分確保することが望ましい。 オフィスアワー：月曜日と金曜日の17:00～，その他時間が空いている時はいつでも可					
授業計画						
		週	授業内容	週ごとの到達目標		
後期	3rdQ	1週	機械工学分野ケーススタディ（K-SEC高学年分野別教材 1～4）	分野別教材のケーススタディにより，機械工学分野における情報セキュリティの課題を認識できる。		
		2週	グループワーク（機械工学分野の情報セキュリティの課題を調査，発表）	グループで課題を調査し，プレゼンテーションができる。		
		3週	セキュリティの概要（K-SEC高学年共通教材 1章）	情報セキュリティの用語や定義を理解できる。		
		4週	セキュリティの概要（K-SEC高学年共通教材 2章）	セキュリティ事故と結びつけて，攻撃の種類を理解できる。		
		5週	グループワーク（セキュリティ事故の事例を調べ，発表。脆弱性や脅威について認識する。）	グループで事例を調査し，プレゼンテーションができる。		
		6週	コンピュータ基礎（K-SEC高学年共通教材 3～4章）	コンピュータの五大機能と，対応している装置とその特徴，プログラムの実行との関連を理解できる。		
		7週	コンピュータ基礎（K-SEC高学年共通教材 4～5章）	コンピュータの五大機能と，対応している装置とその特徴，プログラムの実行との関連を理解できる。		

	4thQ	8週	グループワーク (コンピュータの分解・組立, コマンドプロンプト操作)	グループで作業を分担し, コミュニケーションがとれる.
		9週	ネットワーク基礎 (K-SEC高学年共通教材 6～7章)	OSI参照モデル, TCP/IPモデルを理解できる. 接続機器の種類を理解できる. MACアドレスを理解できる. 無線LANの注意点を理解できる.
		10週	ネットワーク基礎 (K-SEC高学年共通教材 8～9章)	IPアドレスの仕組みを理解できる. ネットワークアドレスとホストアドレスを理解できる.
		11週	グループワーク (ネットワークの接続, MACアドレスの確認, IP関連コマンドの実行)	グループで作業を分担し, コミュニケーションがとれる.
		12週	セキュリティ対策 (K-SEC高学年共通教材 10～11章)	代表的なセキュリティ技術を理解できる. 個人と組織の取り得るセキュリティ対策を理解できる.
		13週	グループワーク (セキュリティ対策に関するディスカッション)	グループでディスカッションを行い, プレゼンテーションができる.
		14週	情報システムとサーバ, クラウド (K-SEC高学年共通教材 12～13章)	社会の中での情報システムの位置付けを知り, そのための運用があり, サーバが存在することを理解できる.
		15週	情報システムとサーバ, クラウド (K-SEC高学年共通教材 14～15章)	仮想化とクラウドの特徴を理解できる.
		16週		

評価割合

	確認テスト	態度	発表内容	合計
総合評価割合	50	25	25	100
基礎的能力	0	0	0	0
専門的能力	50	25	25	100
分野横断的能力	0	0	0	0