日本工学院専門学校	開講年度	2019年度	科目名	情報セキュリティ

科目基礎情報

開設学科	パソコン・ネットワーク科	コース名	ネットワーク・セキュリティコース	開設期	後期
対象年次	1年次	科目区分	必修	時間数	30時間
単位数	2単位			授業形態	講義
教科書/教材	実習資料は毎回配布する。関連する資料等についてはそれぞれの実習内で紹介する。				

担当教員情報

担当教員	東堂　隼平	実務経験の有無・職種	有・システムエンジニア

学習目的

本講義を受講する学生は、ネットワークを介した不正攻撃、コンピュータウイルスの仕組みや対策、ファイアウォールの原理などのネットワークセキュリティ、共通鍵暗号、公開鍵暗号、ハッシュなどの暗号技術、暗号理論を応用した認証技術、電子透かし技術、セキュリティ監査およびセキュリティの標準、法規についての知識を身に着け、セキュリティマネジメント手法や対策など実学に基づく専門能力として社会で活用できるようになることを目的とする。

到達目標

セキュリティ技術の基本として暗号化、フィルタリングなどの知識を深め、セキュリティマネジメント、セキュリティ対策等の応用や活用例を知り、実社会において理解、活用ができるようになることを目標とする。また、近年のサイバー攻撃事例を学び、セキュリティに関連する話題、ニュース記事を理解し、興味を持ち、常にセキュリティ関連のトレンドを追いかけることができるようにする。

教育方法等

授業概要	本講義では、セキュリティ技術の基本を学び、管理策（マネジメント手法）についても学び、社会で活用できるようにする。また、近年のサイバー攻撃事例の調査、発表を行う。学生が主体的に学ぶことができるよう、グループワークを採り入れる。他人が発する情報をどのように受けとめ、理解するか、さらにそれをどのように伝えていくかを意識しながら、講義を進める。
注意点	本講義では学生の主体性を重視し、定期的に課題の提出を実施する。また、グループで考え、発表する作業があるため全員が積極的に参加し、時間内で効果的に作業を進める意識が肝要である。社会への移行を前提とした受講マナーで参加し、講義中の私語や受講態度などには厳しく対応する。（詳しくは初回の講義で説明する。）理由のない遅刻や欠席は認めない。パソコン、教科書を忘れずに持参すること。授業時数の4分の3以上出席しない者は定期試験を受講することができない。

評価方法	種別	割合	備考
	試験・課題	50%	試験と課題を総合的に評価する
	小テスト	0%	
	レポート	20%	授業内容の理解度を確認するために実施する
	成果発表（口頭・実技）	20%	授業時間内に行われる発表方法、内容について評価する
	平常点	10%	積極的な授業参加度、授業態度によって評価する

授業計画（1回～15回）

回	授業内容	各回の到達目標
1回	ガイダンス	ガイダンスにて情報セキュリティの授業の重要性を知り、本講義の取り組み方、姿勢を身に着ける
2回	基礎学習(1)	暗号技術（公開鍵、秘密鍵、ハイブリッド）を学び、仕組みを理解できる
3回	基礎学習(2)	暗号技術の理解の下、PKI運用管理技術を学び、仕組みを理解できる
4回	基礎学習(3)	ディジタル署名などの認証技術について学び、仕組みを理解できる
5回	基礎学習(4)	コンピュータウィルス、マルウェアの種類を知り、対策手法を理解できる
6回	基礎学習(5)	ネットワークセキュリティ手法、フィルタリング等について学び、活用できる
7回	管理策(1)	情報セキュリティマネジメント手法を学び、活用できる
8回	管理策(2)	リスクファクターについて知り、リスクマネジメント手法を学び、活用できる
9回	管理策(3)	セキュリティ評価、分析手法を学び、定量的、相対的にデータに基づいて評価できる
10回	応用学習(1)	サイバー攻撃の種類を学び、セキュリティ支援組織について学び、理解できる
11回	応用学習(2)	セキュリティ監査と脆弱性検査について学び、理解できる
12回	事例解析(1)	グループでのサイバー攻撃事例解析演習を通して、トレンドを知り、能動的な調査ができる
13回	事例解析(2)	サイバー攻撃事例解析演習発表を通して、知識整理を行い発表することができる
14回	事例解析(3)	サイバー攻撃事例解析演習発表を通して、知識整理を行い発表することができる
15回	事例解析(4)	サイバー攻撃事例解析演習発表を通して、知識整理を行い発表することができる