

大阪情報コンピュータ専門学校 授業シラバス (2021年度)

専門分野区分	ネットワーク	科目名	ネットワークセキュリティⅡ				科目コード	T1432A1		
配当期	後期	授業実施形態	通常				単位数	4 単位		
担当教員名	白石 雅義	履修グループ	4A(SN)				授業方法	演習		
実務経験の内容	システムエンジニアとしてIT企業でLinux サーバの設計・構築・運用のフェーズにおける15年の各実務経験を活かし、設計に始まり運用に至るまでのインフラ構築の全てのフェーズのネットワークの現場の在り方を俯瞰的に見渡してきた豊富な実績を元に、ネットワーク通信の”イロハ”について、実務に即した実践的な形式で講義を実施する									
学習一般目標	ネットワーク上からのさまざまな攻撃手法や防御方法について学び、「インターネットを通じた攻撃の種類および防御方法の研究」、「インターネットを利用する上で安全に運用するために必要なセキュリティの研究」を学んでいきます。また、実機を用いた実習を用いることにより、学生の関心・学習意欲を高めていきます。サーバOSにWindows、Linuxを活用し、ネットワーク環境構築を行っていき、現場で使える知識を学ぶ事を目標とします。									
授業の概要および学習上の助言	サイトなどの情報を元に学生自身がネットワークセキュリティに関して興味を持つていくことで、積極的な態度で授業に臨んでもらえるよう工夫を行っています。適宜質疑を重ねながら理解を進めてください。毎回講義に対しての理解した内容を書き出す形式でレポートを課します。									
教科書および参考書	様々なサイトや資料を用いますが、特定の教科書はありません。									
履修に必要な予備知識や技能	ネットワークセキュリティに関する興味やここ数年の1PA発表の「10大驚異」を事前に眺めておくとう望ましい									
使用機器	5-A端末やネットワーク機材。									
使用ソフト	都度準備を進め、提供していきます。									
学習到達目標	学部DP(番号表記)	学生が到達すべき行動目標								
	1/2	ネットワークセキュリティの基礎知識について理解する								
	1/2	Firewallの概要・機能・操作方法を学び 実際の企業を想定した構築ができる								
	1/2	OSのセキュリティ設定 を理解し、構築できる								
	1/2	インターネットを利用した攻撃の種類を理解し、実際に防御する手法を学ぶ								
	5	情報セキュリティ分野に関心を持ち意欲をもって取り組めることができる								
達成度評価	評価方法	試験	小テスト	レポート	成果発表(口頭・実技)	作品	ポートフォリオ	その他	合計	
	学部DP	1.知識・理解			40					40
		2.思考・判断			40					40
		3.態度								
		4.技能・表現								
		5.関心・意欲							20	20
総合評価割合				80				20	100	
評価の要点										
評価方法	評価の実施方法と注意点									

試験	試験は行わず、出席率とレポート提出で評価を行う。
小テスト	
レポート	
成果発表(口頭・実技)	
作品	
ポートフォリオ	
その他	授業への出席、取り組みなどを含め総合的に判断する

### 授業明細表

授業回数	学習内容	授業の運営方法	学習課題(予習・復習)
第1回	セキュリティの腕を磨く鍵は「答えは一つじゃない」	実習	数回の講義の中で、学生のみなさんの理解度を把握しながら講義内容を変えていきます
第2回	zabbix1	実習	
第3回	zabbix2	実習	
第4回	zabbix3	実習	
第5回	snmp	実習	
第6回	情報漏洩事故	実習	
第7回	ネットワーク目線からのデータベースのセキュリティ	実習	
第8回	自動運転とネットワークセキュリティ	実習	
第9回	メールとセキュリティ	実習	
第10回	ISMSとPマークを紐解く	実習	
第11回	ゼロトラストネットワーク	実習	
第12回	IDS/IPSを改めて理解する	実習	
第13回	10大驚異2021を振り返る	実習	
第14回	その機器は本当にセキュアな状態か？に気付く	実習	
第15回	まとめ	実習	