

2026 年度 授業計画(シラバス)

学 科	専攻科医療秘書専攻		科 目 区 分	基礎分野	授業の方法	講義
科 目 名	AI特論Ⅲ		必修/選択の別	必修	授業時数(単位数)	15 (1) 時間(単位)
対 象 学 年	1年		学期及び曜時間	後期	教室名	PCルーム
担 当 教 員	BSC	実務経験と その関連資格				
《授業科目における学習内容》						
コンピューターの基本的な仕組みやインターネットの基礎を理解し、ネットワークの構成要素や通信の基本的な仕組みを学ぶ。さらに、OSI参照モデルやTCP/IP、各種通信プロトコルの役割を理解するとともに、DNSやSSL/TLSなど安全なインターネット通信の仕組みについて理解を深める。						
《成績評価の方法と基準》						
出席(20%)、平常点(10%)、課題・小テスト点(70%)						
《使用教材(教科書)及び参考図書》						
ネットワークとセキュリティ基礎(仮名)						
《授業外における学習方法》						
自宅等にインターネットにつながったPCがあれば、イーラーニングで自習できます。 欠席した場合は次の週までに課題を済ませて下さい。						
《履修に当たっての留意点》						
出席することが一番重要ですので、欠席しないように受講してください。						
授業の方法	内 容			使用教材	授業以外での準備学習 の具体的な内容	
第1回	講義形式	授業を通じての到達目標	コンピューターの基本的な仕組みを理解できるとネットワークの周りを理解できる	ネットワークとコンピューター	イーラーニングテキストで講義の内容を確認しておくこと。	
		各コマにおける授業予定	プロトコルとネットワーク機器/OSI参照モデル/IPアドレスとMACアドレス			
第2回	講義形式	授業を通じての到達目標	セキュリティ脅威の概要を理解できる	セキュリティ1	イーラーニングテキストで講義の内容を確認しておくこと。	
		各コマにおける授業予定	脅威とは/攻撃の種類/マルウェア			
第3回	講義形式	授業を通じての到達目標	セキュリティ脆弱性の概要を理解できる	セキュリティ2	イーラーニングテキストで講義の内容を確認しておくこと。	
		各コマにおける授業予定	脆弱性とは/脆弱性の種類			
第4回	講義形式	授業を通じての到達目標	組織としてセキュリティを守る方法を理解できる	セキュリティ3	イーラーニングテキストで講義の内容を確認しておくこと。	
		各コマにおける授業予定	リスク管理とアセスメント/セキュリティポリシー/技術的・人的・物理的セキュリティ			
第5回	講義形式	授業を通じての到達目標	インシデントの管理と対応の概要について理解できる		イーラーニングテキスト	

5 回	授 業 形 式	各コマに おける 授業予定	インシデントとは/インシデント管理/インシデント対応/BCP	セキュリティ4	で講義の内容を確認し ておくこと。
授業の 方法		内 容		使用教材	授業以外での準備学習 の具体的な内容
第 6 回	講 義 形 式	授業を 通じての 到達目標	セキュリティ対策の具体例を理解できる	セキュリティ5	イーラーニングテキスト で講義の内容を確認し ておくこと。
		各コマに おける 授業予定	エンドポイントでの防御/FW(ファイアウォール)/IPS/IDS/監視と ログ		
第 7 回	講 義 形 式	授業を 通じての 到達目標	Canvaを使って資料を作成できる	CANVA資料作成	イーラーニングテキスト で講義の内容を確認し ておくこと。
		各コマに おける 授業予定	生成AIとの会話/生成AIで自己紹介を作成/Canvaの紹介 /Canvaの使い方/Canvaで資料作成		
第 8 回	講 義 形 式	授業を 通じての 到達目標	AIを使ってショート動画を作成できる	ショート動画作成	イーラーニングテキスト で講義の内容を確認し ておくこと。
		各コマに おける 授業予定	リール台本をCopilotで制作/Canvaで動画作成		