コース名	専門人材特化型コース				
講座名	社会人向けサイバーセキュリティ人材育成講座(九州大学SECKUN)（共同事業）				
科目名	AIセキュリティ特論				
必修・選択	―	単位	ー		
概要・目的	近年急速に発展しているAIにおいて、そのセキュリティ対策を理解することは非常に重要である。本講座では、機械学習及び生成AIに関する攻撃手法及びその対策に関する知識を習得する。さらに発展的な内容である AIシステムに対する脅威モデリング演習を行うことにより、AIシステムに対する脅威を理解するとともに脅威モデリングの手法を習得する。				
到達目標	機械学習及び生成AIに対する攻撃手法とその対策について理解し説明できる。 また、脅威モデリングの手法について理解し、実施できる。				
授業方法	講義＋演習	実施形態	対面＋遠隔同期＋遠隔非同期		
評価方法	出席状況、レポート等の結果を総合的に判断し、評価する。			実施形態	同期日
授業項目	1	はじめに		対面 +遠隔同期 +遠隔非同期	10/26
	2	機械学習とは			
	3	機械学習に対する攻撃手法とその対策			
	4	機械学習に対する攻撃手法とその対策		対面 +遠隔同期 +遠隔非同期	11/1
	5	生成AIに対する攻撃手法とその対策			
	6	生成AIに対する攻撃手法とその対策			
	7	生成AIに対する攻撃演習		対面 +遠隔同期	11/30
	8	生成AIに対する攻撃演習			
	9	生成AIに対する攻撃演習			
	10	脅威モデリングとは		対面 +遠隔同期	12/7
	11	AI脅威モデリング演習			
	12	AI脅威モデリング演習			
	13	AI脅威モデリング演習		対面 +遠隔同期	12/14
	14	AI脅威モデリング演習			
	15	おわりに			
使用教材	スライド Pythonスクリプト				
特記事項	1日あたり3コマ実施予定 第1回と第2回講義の様子は録画し後日配信するため、実施日以降も申込可能(11/20まで) 第3回受講開始までに第1回および第2回の講義参加、あるいは講義動画を視聴しておく必要あり				