■募集情報

募集番号	2022-12
部署名	サイバーセキュリティ研究所
インターンシップ課題名	深層学習モデルの頑健性に対する研究開発
インターンシップ内容の概要	近年、深層学習の目覚ましい発展によりサイバーセキュリティ分野での応用が進んでいる。その一方で、モデル反転攻撃やモデル抽出攻撃、敵対的サンプルなど深層学習に対する様々な攻撃も提案されており、モデルの頑健性の評価はセキュリティ上重要である。本インターンではセキュリティ分野で応用されている有力な深層学習モデルの頑健性の評価を行うために、当該モデルの脆弱性を利用した攻撃の検討や既知の攻撃に対する頑健性の評価を行う。
課題に関する問い合わせ先	サイバーセキュリティ研究所 サイバーセキュリティ研究室 副室長　高橋健志 takeshi_takahashi@nict.go.jp
応募条件	・応募者区分：高専、大学、大学院 いずれも可 ・学年：大学 4 年生以上 ・その他：機械学習及び深層学習モデルの頑健性に関する知見がある方を優先的に採択する。
実施場所	サイバーセキュリティリカレントエボリューションセンター(CYREC)　（東京都武蔵野市）
実施期間	2022 年 9 月 1 日～2023 年 3 月 31 日の間で 30 日間程度 (休・祝日を除く)
受入予定人数	1 名
選考課題	過去の発表論文
備考	