特別講義

明治大学 国際交流基金事業「Researcher Mobility Grant」

“Private and Secure AI: Learning from Sensitive Data Without Exposing It”

2026年5月27日 水 5限

17:10～18:50

明治大学　中野キャンパス　高層棟3階302教室

講演詳細（使用言語は英語です）

This talk explains the core ideas of privacy-preserving machine learning: how to train models on sensitive data while keeping individual records hidden. I will give intuitive examples (data staying on local devices instead of being centralized, adding controlled noise to protect users) and discuss what still goes wrong in practice: attacks that can recover information, security weaknesses, and the ethical questions that appear when AI is deployed in real systems.

講師紹介　Ghazaleh Khodabandelou博士

Dr. HDR Ghazaleh Khodabandelou is a Professor of Computer Science at the University of Paris-Est Créteil (UPEC), affiliated with the **Laboratoire Images, Signaux et Systèmes Intelligents (LISSI)**. She holds a **Ph.D. in Artificial Intelligence** from Paris 1 Panthéon-Sorbonne University and an **HDR (Habilitation à Diriger des Recherches) in Artificial Intelligence** from Université Paris-Est. Her research focuses on **advanced artificial intelligence methodologies**, including **multimodal deep learning, large language models, neuro-symbolic reasoning, and advanced optimization techniques**.

主催：明治大学　総合数理学部専任教授／菊池　浩明

共催：明治大学　国際連携本部

問い合わせ先：　kikn@meiji.ac.jp（菊池　浩明）