

埼玉大学産学官連携協議会

データサイエンス研究会

第4回 対面開催

2026年

9月17日(木)

14:00-17:00

生成AI・AIエージェントの評価とセキュリティ ～代表的な論文、事例から学ぶ～

生成AIやAIエージェントを安全に活用するには、出力品質をどう評価し、どのような攻撃や情報漏えいに備えるべきでしょうか。本研究会では、生成AI評価の基本と、プロンプトインジェクションやRAGからの意図しない情報開示などのセキュリティ課題について、最新の研究動向を代表的な論文と具体的な事例から解説します。また、参加者からの事例紹介と、体験型グループワークを通して、実務への適用方法と今後の課題について意見交換を行います。

会場



埼玉大学 大学会館2階 ラーニングコモンズB（裏面にMAPあり）

内容



14:00-15:00 生成AI評価の基本／生成AI・AIエージェントのセキュリティ入門
15:00-15:30 事例ライトニングトーク(参加者からの導入事例、失敗事例の紹介)
15:30-16:30 グループワーク：意図しない情報開示を実際に体験
16:30-17:00 質疑・意見交換・交流

講師



埼玉大学 教育機構 基盤教育研究センター 市川 裕介 教授

対象



埼玉大学産学官連携協議会の会員企業・団体にご所属の方、学部生・院生

埼玉大学産学官連携協議会 データサイエンス研究会

E-mail: s-kyougikai@gr.saitama-u.ac.jp TEL: 048-858-9064

埼玉大学産学官連携協議会

第4回データサイエンス研究会

申込方法 ▶ 申込フォームよりお申し込みください。

QRコードまたはURLよりアクセスし、
必要事項をご入力の上、ご登録ください。



<https://forms.cloud.microsoft/r/mhdwm8cYHy>

申込期限 ▶ 2026年9月11日(金)

※ 参加希望者が多数の場合は、早期に締め切らせていただく場合がございます。

参加対象 ▶ 埼玉大学産学官連携協議会の会員企業・団体にご所属の方、
学部生・院生

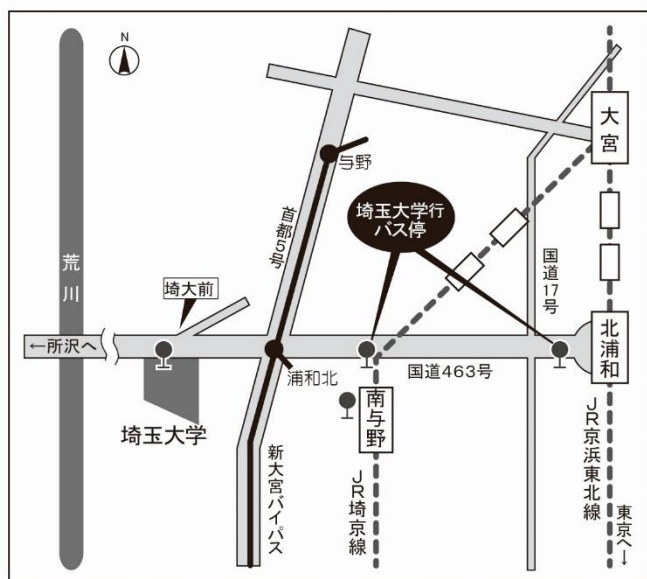
問合せ先 ▶ 埼玉大学産学官連携協議会 事務局

TEL: 048-858-9064 E-mail: s-kyougikai@gr.saitama-u.ac.jp

埼玉大学への交通案内

- 東京駅 → JR京浜東北線(快速35分) 北浦和駅西口
→ バス(埼玉大学行き 約15分・3.5km)
- 新宿駅 → JR埼京線(34分) 南与野駅
→ バス(埼玉大学行き 約10分・約2.2km)

※交通事情により到着時間に遅れが生じる場合があります。ご了承ください。



キャンパスマップ

お車で越しの方は、正門前守衛所で
入構手続きをお願いします。

