第 18 回研究科セミナー
（次世代デジタル社会基盤研究領域）

テーマ

「AI セキュリティの最前線 Frontiers in AI Security」

講演者：株式会社 KDDI 総合研究所

KDDI Research, Inc.

エキスパート　披田野 清良　氏

Expert, Seira Hidano

コアリサーチャー　長谷川 健人　氏

Core Researcher, Kento Hasegawa

日　時：令和 7 年 12 月 12 日（金）15：00～16：30

場　所：情報科学研究棟 3 棟 5 階 コラボレーションルーム 7

及びオンライン

講演要旨：

本講演では、AI セキュリティ領域の最前線の取り組みを 2 つ紹介します。まず Security for AI の領域について、AI のセキュリティ情報を一元化して発信する「AI セキュリティポータル」の取り組みを通じて、AI 自体への攻撃・防御だけでなく社会影響と対策技術について紹介します。次に AI for Security の領域について、システムの設計から運用に関わるセキュリティにおける AI 活用の研究を紹介します。設計時の LLM による検証や運用時の強化学習によるレッドチーミング等の取り組みを通じ、セキュリティ分野における AI 応用の課題と解決のアプローチを紹介します。

講演者略歴：

【披田野 清良 氏】

2007 年 3 月　早稲田大学理工学部コンピュータ・ネットワーク工学科卒業
2012 年 3 月　早稲田大学理工学術院基幹理工学研究科情報理工学専攻博士後期課程修了
2011 年 4 月　早稲田大学理工学術院基幹理工学部助手
2013 年 4 月　KDDI 株式会社　入社
2014 年 4 月　株式会社 KDDI 研究所（後に株式会社 KDDI 総合研究所と改称）配属

【長谷川 健人 氏】

2016 年 3 月　早稲田大学 基幹理工学部 情報理工学科 卒業
2017 年 3 月　早稲田大学大学院 基幹理工学研究科 情報理工・情報通信専攻 修士課程 修了
2020 年 3 月　早稲田大学大学院 基幹理工学研究科 情報理工・情報通信専攻 博士後期課程 修了（博士（工学））
2020 年 4 月　KDDI 株式会社 入社。同年に株式会社 KDDI 総合研究所に出向し、現職

お問合せ先：准教授　BEURAN, Razvan Florin（Email: razvan@jaist.ac.jp）