第 3 回安全性とセキュリティ研究会（SIG-SEC）

人工知能学会合同研究会 2024 論文募集

■ 開催概要

- 日時：2024 年 12 月 21 日(土)
- 開催形式:会場およびオンライン(Zoom 使用)のハイブリッド開催
- 会場：慶應義塾大学日吉キャンパス 来往舎 大会議室（G 会場）
    - 神奈川県横浜市港北区日吉 4-1-1

■ 重要日程

- 発表申込締切：2024 年 11 月 ~~15 日(金)~~→ 22 日(金) ※延長しました
- 原稿提出締切：2024 年 ~~11 月 29 日(金)~~ → 12 月 2 日(月)※延長しました
- 参加申込締切：2024 年 12 月 6 日(金)

■ Web サイト

- 公式 HP:
    - https://ai.iisec.ac.jp/sig-sec/
    -
- 発表申込 URL:
    - https://www.ai-gakkai.or.jp/sig-system/confusers/presenter_add/sigais2024/sec
-

■ 開催主旨

近年、Al 技術を利用した多くの製品やサービスが世の中に浸透してきており、Al の意思決定が人々の生命や多くの産業に影響を与えるものになっています。AI による自律的な意思決定から人間が徐々に排除されていく中で、設計原理として AI のセキュリティを考慮する必要性が高まっています。本セッションでは、Al のセーフティとセキュリティに関する誤動作、攻撃、防御、追跡、分析を含む新しいアイデアを広く模索し、研究を深めることを目的としています。

人工知能学会の会員でなくても発表･参加していただけます．皆様の積極的なご投稿･ご参加をお待ちしております．

■ 募集テーマ

- Deepfake/生成 AI の信頼確保やプライバシーに関連する研究
- 機械学習モデルの脆弱性,強靭性.安全性,プライバシーに関連する研究
- Al/機械学習システムの品質·安全性·信頼性·マネジメントに関する研究
- Al/機械学習を用いた情報システムへの攻撃,防御,プライバシー保護に関する研究など

■ 発表申込方法

- 発表申込締切日までに下記の SIG-SEC 合同研究会発表申込フォームからお申し込みください.
  - https://www.ai-gakkai.or.jp/sig-system/confusers/presenter_add/sigais2024/sec
  - 会場での現地発表か Zoom 遠隔発表を選択いただきます.

■ 論文執筆方法

- 人工知能学会研究会スタイル・ファイルをご利用ください．原稿は 8 頁以内として下さい.
- http://www.ai-gakkai.or.jp/sig/sig-style/
- 原稿提出締切日までに SIG-SEC 合同研究会発表申込フォームからアップロードして下さい
  - https://www.ai-gakkai.or.jp/sig-system/confusers/presenter_add/sigais2024/sec
- 投稿論文の著作権について
  - 本研究会に投稿された論文は，**人工知能学会著作権規定**において人工知能学会二種研究会の論文として扱われます．投稿された論文の著作権は著者に帰属しますが，投稿された論文を学会が Web サイト(J-Stage 等)で開示すること等を許諾して頂きます.

■ 発表時間

- 予定：1 件 25 分(発表 20 分，質疑 5 分)
- 発表件数などにより時間を多少変更することがあります

■ 表彰

- 年度ごとに優秀な論文を選定し、安全性とセキュリティ研究会より人工知能学会研究会優秀賞（JSAIIncentiveAward）に推薦します.
- https://www.ai-gakkai.or.jp/about/award/jsai_award-sig/

■ **参加費：無料**

- 参加のみの方の参加登録：以下の URL から登録して下さい.
- https://www.ai-gakkai.or.jp/sigais2024/registration/

■ **問い合わせ先**

ai-sig-sec@conferenceservice.jp