人工知能学会 合同研究会 2022 安全性とセキュリティ研究会(SEC) 論文募集

日時: 2022 年 11 月 23 日 (水・祝)

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 矢上キャンパス 12 棟 106 教室（オンラインとのハイブリッド開催）
〒223-8522 神奈川県横浜市港北区日吉 3-14-1

- 今後の COVID-19 の感染状況を受けて，開催形態は変更となる可能性があることをご了承ください．

■ 重要日程

* 発表申込締切: 2022 年 10 月 12 日 (水)
* 原稿提出締切: 2022 年 11 月 15 日 (土)
* 参加申込締切: 2022 年 11 月 21 日 (月)

■ 開催主旨

近年、AI 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、AI 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、AI 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

・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
・AI/機械学習システムの品質・安全性・信頼性に関する研究
・AI/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/sigconf2022/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/sigconf2022/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, 以下の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, 投稿された論文を学会が Web サイトで開示すること等を許諾して頂きます.

https://www.ai-gakkai.or.jp/pdf/sig/sig_copyright.pdf

■ 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

合同研究会自体は 22～23 日の 2 日間開催となりますが, SIG-SEC は 23 日の開催です。

■ 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（JSAI Incentive Award）に推薦します.

https://www.ai-gakkai.or.jp/about/award/jsai_award-sig/

■ 参加費：無料

■ 参加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/sig-system/confusers/add/sigconf2022

■ 問い合わせ先

sig-sec@ai.iisec.ac.jp

■ 主査

- 櫻井 幸一（九州大学）

■主幹事

- 大塚 玲（情報セキュリティ大学院大学）

■幹事(五十音順)

- 菅和聖 （日本銀行金融研究所）
- 榊 剛史（株式会社ホットリンク）
- 櫻井祐子（名古屋工業大学）
- 高橋健一（鳥取大学）
- 溝口誠一郎(DNV ビジネス・アシュアランス・ジャパン)
- 宮地充子（大阪大学）

■顧問

浦本直彦（三菱ケミカルグループ株式会社）

■ 研究会 URL

https://conferenceservice.jp/www/ai-sig-sec/