2023 年度年次報告書
AIP 加速課題
2023 年度採択研究代表者

松谷 宏紀

慶應義塾大学 理工学部
教授

適応性と信頼性を両立するオンデバイス学習技術の確立

主たる共同研究者:
岡本 球夫（パナソニックホールディングス(株) プロダクト解析センター 課長）
吉田 康太（立命館大学 理工学部 助教）

研究成果の概要

2023 年度は、主として、オンデバイス学習と連動したコンセプトドリフト検知の信頼性向上（研究項目 A1）、オンデバイス学習におけるセキュリティリスクの解析（研究項目 A2）、適応性と信頼性を両立するオンデバイス学習技術の電気火災予知への応用（研究項目 B2）を実施した。研究項目 A1 は、計算資源の限られた IoT デバイス上で動作するコンセプトドリフト検知アルゴリズムの研究である。メモリ使用量の少ない逐次アルゴリズムを用いたコンセプトドリフト検知を開発し、同じく逐次アルゴリズムであるオンデバイス学習アルゴリズムと併せて Raspberry Pi Pico 上で動作させた。回転機械などを対象とした異常検知データセットを用いて評価した結果、従来手法よりも少ないメモリ量、計算コストで従来手法に比肩する検知性能を実現できた。研究項目 A2 は、オンデバイス学習を対象としたセキュリティリスクの解析である。IoT デバイスを対象としたオンデバイス学習によって、デバイスが置かれた現場に合わせてモデルを再学習できるというメリットがあるが、同時に、意図せぬ再学習による誤動作や悪意のあるユーザによる攻撃といったリスクが生じうる。オンデバイス学習の信頼性向上が本研究のゴールであるが、その前段階として立命館大グループが中心となって異常検知器を対象としたポイズニング攻撃を実証した。また、攻撃検知手法の研究も開始した。研究項目 B2 では、パナソニックグループが中心となってオンデバイス学習技術を実用化するうえでの課題を検討している。具体的には AI の処理フローを 1)データ取得・前処理、2)学習、3)推論、4)後処理、5)入力管理、6)リスク監視・ヘルスチェック、7)アップデート・メンテナンスに分類したうえでオンデバイス学習特有の課題について検討した。検討した課題への対策についていくつか前倒しで研究開発を進めた。

【代表的な原著論文情報】

1) Kazuki Sunaga, Masaaki Kondo, Hiroki Matsutani, "Addressing Gap between Training Data and Deployed Environment by On-Device Learning", IEEE Micro, Vol.43, No.6, pp.66-73, Nov/Dec 2023.

2) Takahito Ino, Kota Yoshida, Hiroki Matsutani, Takeshi Fujino, "A Feasibility Study of Data Poisoning against On-device Learning Edge AI by Physical Attack against Sensors", RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing, 4 pages, Feb/Mar 2024.