未来社会創造事業　探索加速型探索研究
事後評価結果

1．　領域

「超スマート社会の実現」領域

2．　重点公募テーマ

サイバーとフィジカルの高度な融合に向けた AI 技術の革新

3．　研究開発課題名

エッジ AI のハードウェアセキュリティに関する研究

4．　研究開発代表者名（機関名・役職は評価時点）

藤野 毅 （立命館大学 理工学部 教授）

5．　評価結果

評点： A （優れている）

総評：

本研究開発課題は、AI 処理特有のセキュリティ攻撃と対策技術を網羅的に検討し、安全性と信頼性が保証されたセキュリティを持つエッジ AI ハードウェアの開発を目指すものである。

探索研究期間では、エッジ AI への悪意ある攻撃を、回避攻撃（Adversarial Examples 攻撃）、ポイズニング攻撃、モデル反転攻撃、抽出攻撃に大別し、車載・監視カメラ用途を想定した画像処理エッジ AI 処理を FPGA や MPU に実装したエッジ AI ハードウェア上で、それらの夫々の攻撃が可能であること、および、幾つかの攻撃への対策の有効性を実証したことを評価する。

また、当初目標としていたハードウェアセキュリティだけでなく、オペレーティングシステム上でのエッジ AI セキュリティへの対策も検討し、オペレーティングシステムから隔離された信頼できる実行環境 TEE（Trusted Execution Environment）上でエッジ AI 処理を実行する際の問題点を抽出し、基本的な解決策を評価する等、優れた成果が認められた。

今後は、RISC-V 等のオープンプラットホームを用いた汎用性の高いエッジ AI ハードウェアを開発し、セキュリティ技術の標準化に向けて研究開発が発展することを期待する。

以上