

2023 年度年次報告書

信頼される AI システムを支える基盤技術

2021 年度採択研究代表者

高前田 伸也

東京大学 大学院情報理工学系研究科
准教授

D3-AI: 多様性と環境変化に寄り添う分散機械学習基盤の創出

主たる共同研究者:

今泉 允聡 (東京大学 大学院総合文化研究科 准教授)

木谷 友哉 (静岡大学 学術院 准教授)

高瀬 英希 (東京大学 大学院情報理工学系研究科 准教授)

吉岡 健太郎 (慶應義塾大学 理工学部 専任講師)

研究成果の概要

チーム全体では、グループ間の共同研究、および産官学の連携や別 CREST 領域との合同ワークショップ等を通じて、分野横断型の研究を促進した。高前田 G は、連合学習の信頼に関わる成果として、新たなバックドア攻撃手法を発見し、より頑健な連合学習を実現するための方策を考察した。また、ロバストで扱いやすい連合学習を実現する技術として、組込みデバイス向け軽量オンライン学習方式と、クライアント間の分布差を測るクラスタリング連合学習アルゴリズムの開発を進めた。吉岡 G は、信頼される分散機械学習ハードウェアで必要となる要素技術として、コンピュータインメモリ(CIM)に適した新たな確率的近似計算アルゴリズムを開発した。本方式に基づく CIM ハードウェアを開発し、大幅に電力効率が向上することを示した。今泉 G は、(i) ニューラルネットワークの量子化の影響を記述する理論開発、および、(ii) 公平性を制御する連合学習手法の開発と理論評価を行なった。(i)では、レプリカ法を用いて量子化の際の数および量子化範囲の相転移現象を発見し、それに基づいたパラメータ選択の尺度を与えた。(ii)では、公平性指数を導入した分布外汎化法を活用した連合学習手法を開発し、実効性を評価した。高瀬 G は、非同期・非中央集権型の分散システムについて、ローカル学習とモデル更新の順序を考慮した連合学習方式を開発した。また、連合学習の信頼性を評価するための分散シミュレータの開発を開始した。仮想技術を用いた実証的評価環境については、情報世界と物理世界の時間同期を効率的に実現する通信技術の開発を進めた。木谷 G は、道路や土木フィールドのダイナミックセンシングに関して、地元産業界と協力し、計測手法の研究開発と実証を行った。また、モビリティメーカーやライフサイエンス関連組織と協力し、デジタルインフラデータの利活用と更新・維持管理のニーズについて議論を重ね、必要な研究開発項目を明らかにした。

【代表的な原著論文情報】

- 1) Masayoshi Tsutsui, Tatsuya Kaneko, and Shinya Takamaeda-Yamazaki, “Poison Egg: Scrambling Federated Learning with Delayed Backdoor Attack”, 3rd International Conference on Ubiquitous Security 2023 (UbiSec-2023), November 2023, https://doi.org/10.1007/978-981-97-1274-8_13.
- 2) Kotaro Shimamura, and Shinya Takamaeda-Yamazaki, “FS-Boost: Communication-Efficient Federated Subtree-based Gradient Boosting Decision Trees”, IEEE Consumer Communications and Networking Conference 2024 (CCNC 2024), January 2024, <http://dx.doi.org/10.1109/CCNC51664.2024.10454880>.
- 3) Yuki Hirayama, and Shinya Takamaeda-Yamazaki, “Scalable Moment Propagation and Analysis of Variational Distributions for Practical Bayesian Deep Learning”, IEEE Transactions on Neural Networks and Learning Systems, Early Access, January 2024, <https://doi.org/10.1109/TNNLS.2024.3367363>.
- 4) Yung-Chin Chen, Shimpei Ando, Daichi Fujiki, Shinya Takamaeda-Yamazaki, and Kentaro Yoshioka, "OSA-HCIM: On-The-Fly Saliency-Aware Hybrid SRAM CIM with Dynamic Precision Configuration", 29th Asia and South Pacific Design Automation Conference (ASP-DAC 2024), January 2024, <https://doi.org/10.1109/ASP-DAC58780.2024.10473966>.
- 5) Kentaro Yoshioka, “A 818-4094 TOPS/W Capacitor-Reconfigured CIM Macro for Unified

Acceleration of CNNs and Transformers”, 2024 IEEE International Solid-State Circuits Conference (ISSCC 2024), February 2024, <https://doi.org/10.1109/ISSCC49657.2024.10454489>.