履歴書・研究業績書

大塚馨　Kaoru Otsuka

沖縄科学技術大学院大学（OIST）博士課程（5 年一貫制）
機械学習・データ科学（MLDS）ユニット（山田誠）
kaoru06135@gmail.com　/ kaoru.otsuka@oist.jp
https://roppinhoppin.github.io/

2026 年 11 月 17 日現在

研究概要

通信量や計算機の速度差を考慮し、攻撃や故障があっても安定して学習を進められる分散・連合学習の手法を研究している。通信効率と頑健性を両立するアルゴリズムを設計し、その収束や攻撃耐性を理論と実験の両面から検証する。

査読付き国際会議論文

1. Delayed Momentum Aggregation: Communication-efficient Byzantine-robust Federated Learning with Partial Participation

Kaoru Otsuka, Yuki Takezawa, Makoto Yamada
ICML 2026 掲載済み／筆頭著者
Proceedings of Machine Learning Research, Vol. 306, pp. 95020–95050, 2026.

各回の学習に一部の端末だけが参加する連合学習において、その回に参加しない端末から過去に得た情報も活用する手法 DeMoA を提案。通信量を抑えつつ、端末が毎回参加するとは限らない状況での攻撃耐性を、一定の仮定の下での理論解析と実験により示した。

公式掲載情報（PMLR）　| OIST 公式紹介記事（2026 年 7 月 9 日）

2. Shepherd: High-Precision Coverage Inference for Response-guided Blackbox Fuzzing (Registered Report)

Takuya Shimizu, Ryuichi Yoshizawa, Kaoru Otsuka, Yudai Fujiwara, Yuichi Sugiyama
ISSTA Companion 2025, pp. 105–115, 2025.
https://doi.org/10.1145/3713081.3731719

プレプリントおよび投稿中論文

3. Robustifying Asynchronous SGD via Soft Throttling

Kaoru Otsuka*, Maxime Meyer*, Yuki Takezawa, Makoto Yamada,
Anastasia Koloskova
ICLR 2027 投稿中／共同第一著者
arXiv:2609.39357（2026 年 9 月 30 日公開）

計算が終わった端末から順に更新を反映する非同期 SGD では、速い端末が大量の更新を送り、学習全体に過度な影響を与える危険がある。同じ端末から繰り返し届く更新の重みを段階的に下げる THROTTLE を提案し、攻撃耐性を理論と実験で検証した。攻撃者がいない実験条件でも、通常の非同期 SGD より性能が向上することを確認した。

https://arxiv.org/abs/2609.39357
* Kaoru Otsuka と Maxime Meyer は共同第一著者。本論文は投稿中であり、採択済みではない。

学歴

2025 年 5 月〜現在　沖縄科学技術大学院大学（OIST）

博士課程（5 年一貫制）。研究領域：計算機科学。
機械学習・データ科学（MLDS）ユニット（山田誠）所属。

2021 年 4 月〜2025 年 3 月　慶應義塾大学環境情報学部

学士。GPA：3.78 / 4.00。金沢篤研究室（純粋数学）および川島英之研究室（データプラットフォーム）で研究・学術活動に参加。

2022 年 9 月〜2023 年 6 月　University of California, San Diego

交換留学（非学位課程）。数学を中心に、計算機科学を副専攻として履修。GPA：3.8 / 4.0。抽象代数、実解析、位相空間論・代数的位相幾何学、複素解析、暗号学を履修。大学院生が主催するリー群・リー代数のセミナーに参加。

研究歴・職歴

2023 年 11 月〜2024 年 9 月　統計数理研究所　研究インターン

指導：日野英逸。情報幾何と機械学習にまたがる研究に従事。

2020 年 3 月〜2021 年 12 月　Ricerca Security　Student Researcher

未踏プロジェクトで開発したファザーを拡張し、実用化に向けて開発。チームで開発した手法をオープンソースのファジングツール AFL++ に組み込んだ。
関連技術記事：ARMored CoreSight

2019 年 4 月〜2020 年 3 月　IPA 未踏 IT 人材発掘・育成事業

担当 PM：首藤一幸。プロセッサトレースを用いた組み込み機器向けファザーを開発。ARM のトレース機能とファジングにより、システムソフトウェアのバグ・脆弱性を効率的に検出。
プロジェクト概要

講演・教育活動

2017 年 11 月　CODE BLUE　講演者

当時公開されていた脆弱性を利用した Apple iOS カーネルの脱獄手法を解説し、実演。

2019 年 8 月　IPA セキュリティ・キャンプ　ティーチングアシスタント

マルウェア解析および Linux カーネルの脆弱性利用に関する講義を補助。教材用の仮想環境の準備と受講者からの質問への対応を担当。

受賞・研究支援

- **文部科学省 AI for Science SPReAD 1000（2026 年度採択）**。研究費予定額：直接経費 486.6 万円、間接経費 145.9 万円、計 632.5 万円。e-Rad に登録された予定額。交付決定額・契約額は未登録。
- **JASSO 海外留学支援制度奨学金（2022 年）**：UC San Diego への交換留学に際して受給。
- **IPA 未踏 IT 人材発掘・育成事業（2019 年度）**：委託金 230.4 万円（確定額）。
- **IPA 未踏スーパークリエータ**：2019 年度採択プロジェクト（2020 年認定）。