教員	落合秀也 准教授	研究場所	本郷	研究分野	分散AI, IoT, セキュリティ, エネルギー

落合研究室は，これからの時代の情報システムの在り方を研究しています．2010年代は Big Data の時代と呼ばれていましたが，AI半導体技術の進化やプライバシー意識の高まりなどに後押しされて，(1) 分散AI，(2) IoT制御システムの新時代を迎えようとしています．また，混迷化する情報システム社会の中で (3) IoT/LANセキュリティの研究需要が高まっています．

1. 分散AI – 自律分散協調学習

機械学習と言えば，サーバに集約されたユーザデータを題材として，モデルを学習するものでしたが，近年は連合学習（Federated Learning）のように，ユーザからデータを集めることなく，モデルを学習できるようになってきました．この分散学習システムを，落合研究室では完全分散化（サーバレス化）し，Peer-to-Peer型の分散AIを実現することに成功しています．様々な機械学習モデルに対して，完全分散化を実現することが今後の目標であり，この分野を今後，急速に開拓していく必要があります． 関連サイト: https://github.com/jo2lxq/wafl/

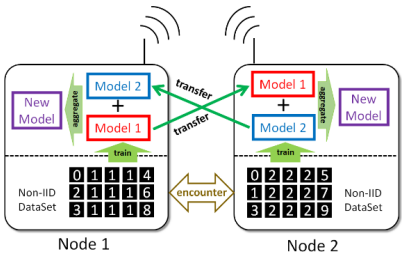

図1: 最も基本的なPeer-to-Peer型 連合学習

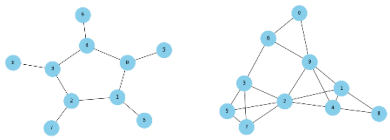

図2: Peer-to-Peer型 連合学習のトポロジー

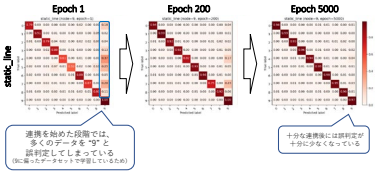

図3: 学習が成功している様子

2 . AIによるIoT制御システム

AIの進化は目覚ましく，我々の物理的な世界（空間）もAIが関与する時代となってきています．落合研究室では制御ロジックを書かないIoTシステムを研究開発しています．

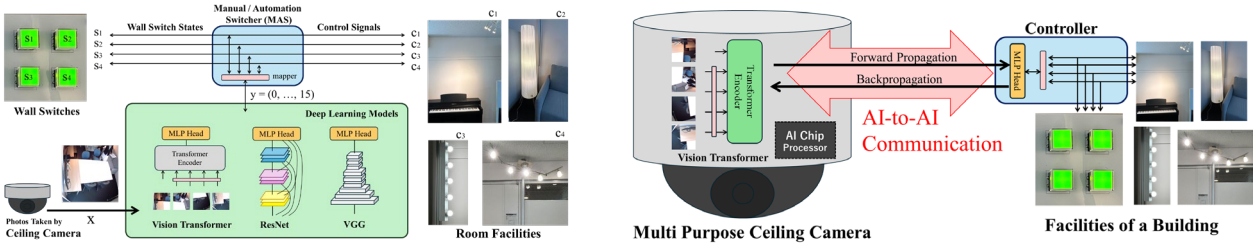

図4: AIによるビル制御システム (Logic Free Building Automation) 左，とその分散化 右

3. IoT/LAN セキュリティ

コンピュータネットワークの末端であるLAN (Local Area Network)には，IoT機器を含む多様な端末が接続されますが，近年のコンピュータシステムの複雑化に伴い，巧妙化するサイバー攻撃により，LAN内部での不審活動が見受けられます．2018年からマルウェア感染が深刻な東南アジア地域の大学と協力し，そのような不審活動の収集を行い，LAN内攻撃種別の体系化を進めています．また，OT (Operational Technology)に対する攻撃をいち早く検知するための，検知技術の開発も進めています．

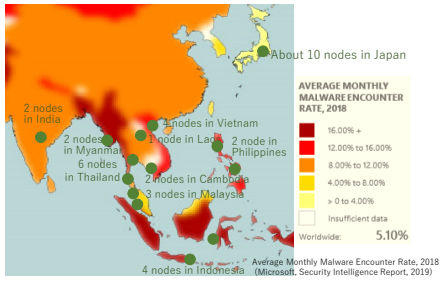

図5: マルウェア感染が深刻な東南アジア地域に構築した観測網

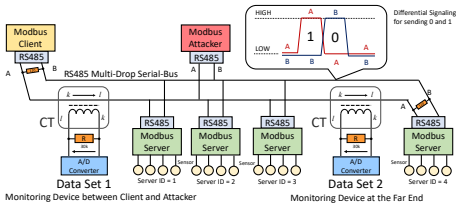

図6: OTセキュリティ監視システム