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

分散型匿名化処理によるプライバシープリザーブドAI基盤構築

研究開発代表者： 斎藤　英雄　　慶應義塾大学･理工学部情報工学科　教授

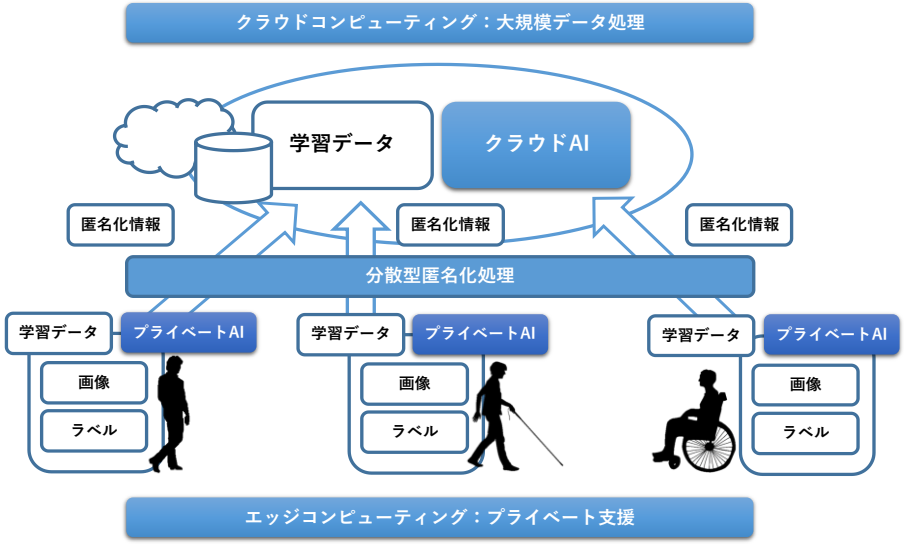
共同研究機関： 早稲田大学，カーネギーメロン大学，日本IBM

目的： プライバシー保護を行いながらプライベートAIとクラウドAIが学習データを共有する枠組みを構築し，クラウド上で大規模な学習データの蓄積を実現するとともに，実環境のユーザの行動支援に使用できることを示す．

研究概要： AI技術の革新のためには，大量の現実データにより学習されたAIを構築することが重要となる．特に，飛躍的に増加しているモバイル型デバイス等により撮影される大量の画像群による機械学習は有効であるが，個人的な特徴を含むデータをクラウド上で共有することはプライバシー保護の観点から問題があり難しい．

本研究では，撮影した画像からプライバシー性を自動判定し，プライバシー性の度合いを階層的に制限した画像を生成するメディア処理技術を研究する．そして，それをカメラの接続されたエッジ側のデバイスのみで実施できるプライベートAI群と，そこから集約されるプライバシー情報を含まない大規模な学習データを共有するクラウドAIにより構成される集合的ネットワークモデルを構築する．

さらに，プライバシー保護を行ったAIによって，障害者の視覚や高齢者の記憶力の補助により社会的行動が支援可能であることを実証する．



Innovative AI technologies for sophisticated integration of cyber and physical world

Privacy preserved AI framework based on distributed anonymization

Project Leader : Hideo Saito
Professor, Department of Information and Computer Science, Keio University

R&D Team : Waseda University, Carnegie Mellon University, IBM Research - Tokyo

Summary : For the advancement of AI technologies, it is important to train engines from a large amount of real data. Though the rapid increase of photos taken by mobile devices helps such advancement, the difficulty to share data including personal features on a cloud given the privacy concerns inhibits broader applicability.

In this study, we will investigate a media processing techniques to automatically judge level of privacy and generate images without the privacy for the use of training data for AI. Then, we will implement collective network model composed of private AI group capable of the privacy preservation the edge devices with cameras, which are connected to cloud AI sharing large scale learning data without containing privacy information.

Also, we will demonstrate the power of AI with privacy protection by assisting missing visual cognition of the blind and declining memory of the elderly people.