

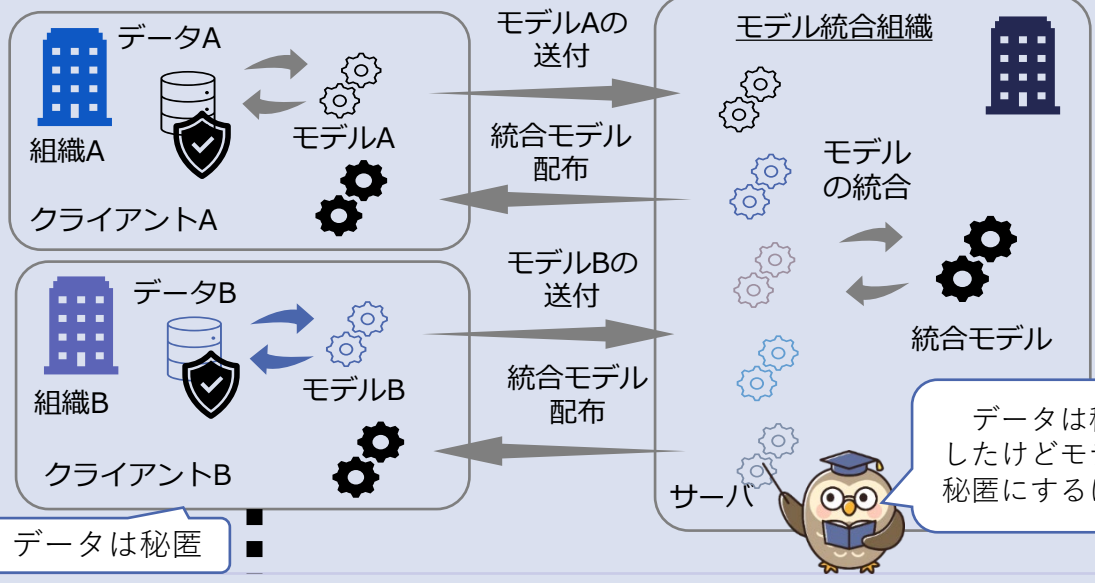
プライバシー保護とデータ活用の両立を目指して ～モデル蒸留に基づく連合学習～

広島市立大学大学院情報科学研究科智能工学専攻
データ科学講座・データ工学グループ・連合学習チーム

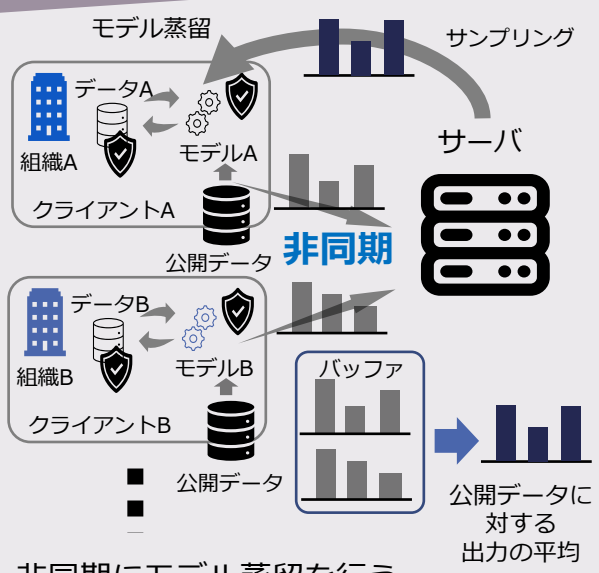
個人が持つデータを集めることなく機械学習を行う連合学習が注目されています。本展示では、データとモデルそのものも秘匿できるモデル蒸留に基づく連合学習とその応用について紹介します。

連合学習

個人が持つデータを集めることなく学習したモデルパラメータを集めることで機械学習を行う方法



非同期型のFedMD



FedMD: Federated Learning with Model Distillation

分散連合学習

データとモデルを秘匿にしたまま分散環境下で学習

