

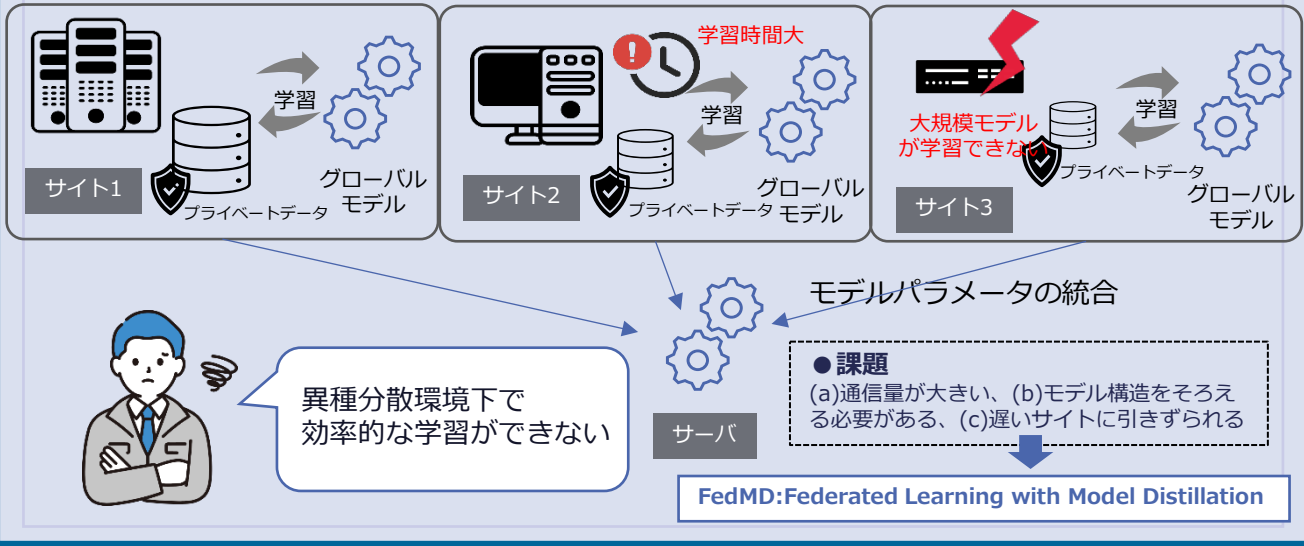
プライバシー保護とデータ活用の両立を目指して ～モデル蒸留に基づく連合学習～

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・連合学習グループ

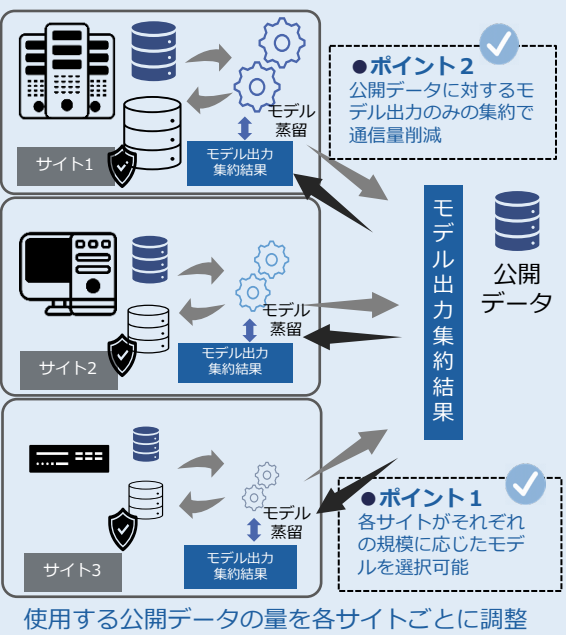
個人が持つデータを集めることなく機械学習を行う連合学習が注目されています。本展示では、データとモデルそのものも秘匿できるモデル蒸留に基づく連合学習とその応用について紹介します。

連合学習とその課題

連合学習：個人や組織が持つ機密性の高い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



FedMDとその効率化



非同期型のFedMD

