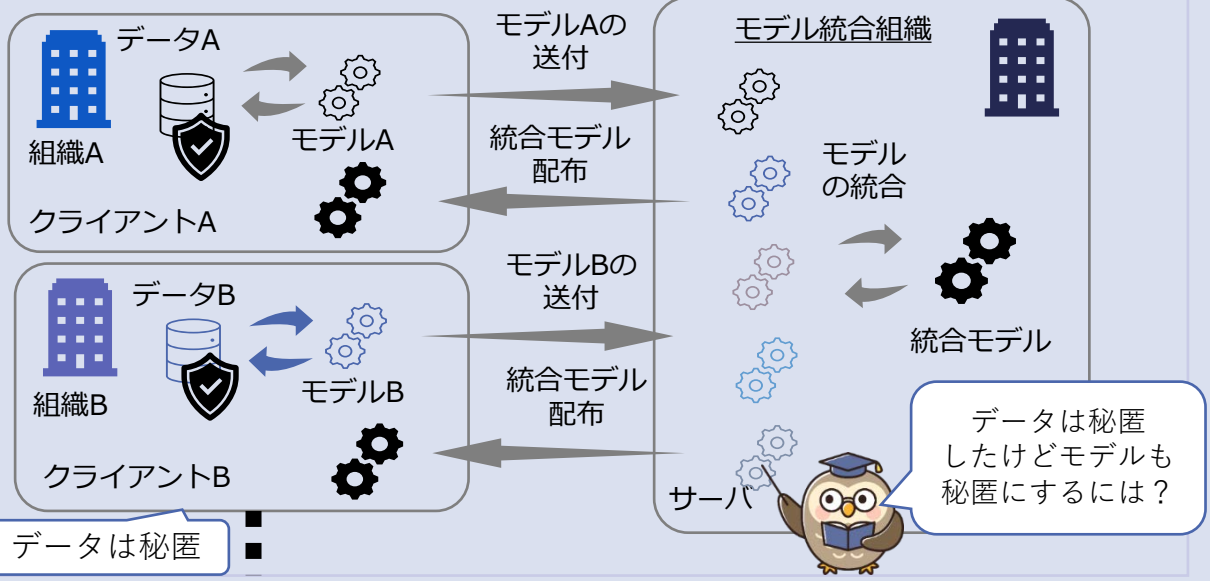
プライバシー保護とデータ活用の両立を目指して
～モデル蒸留に基づく連合学習～

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

データを集めることなく機械学習を行う方法である連合学習の機密性を高めるためにデータフリーモデル蒸留(DFMD)に基づく連合学習とその分散化について研究開発を行っています。

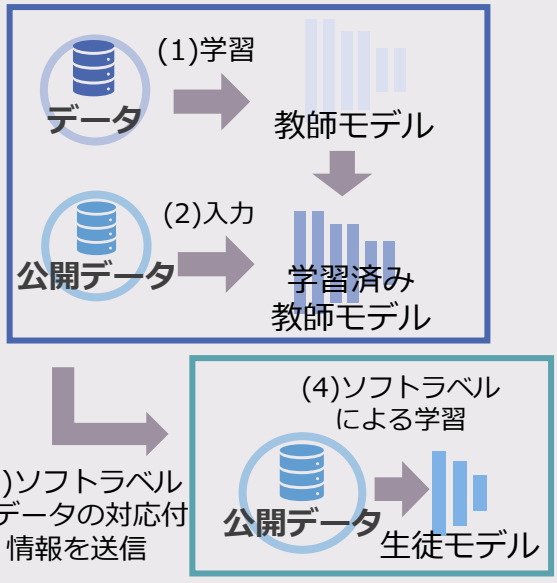
連合学習

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



データフリーモデル蒸留

モデルを秘匿にしたまま知識を転送



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