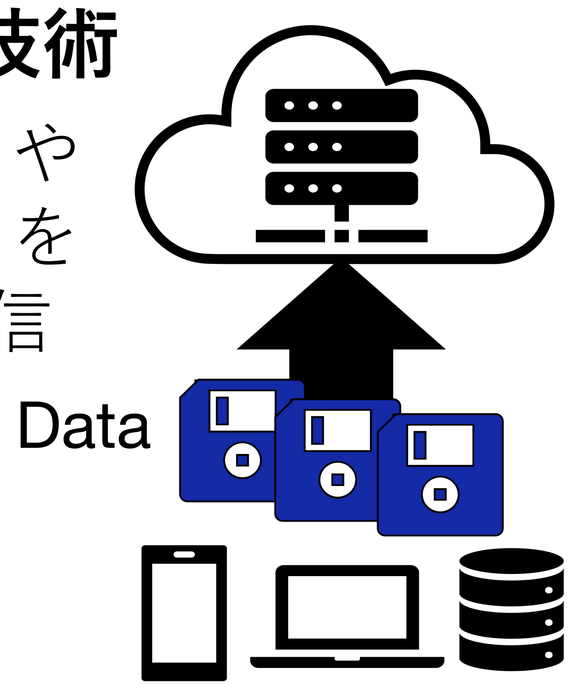
プライバシ保護型エッジAI技術

東京工業大学西尾研究室　代表:西尾理志 (nishio@ict.e.titech.ac.jp)

特徴: 入力データを社外に出さずにエッジでAIを利用可能

従来のエッジAI技術

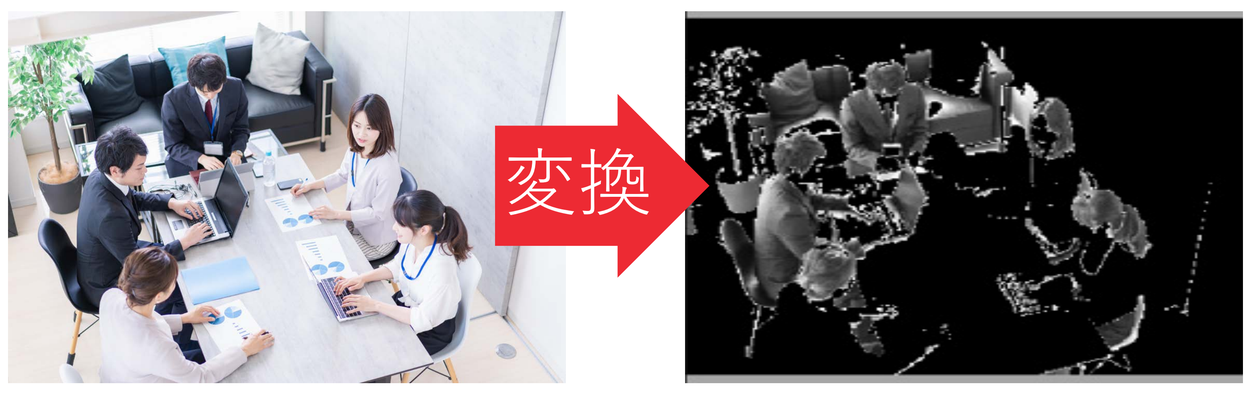
入力となる画像やテキストデータをエッジサーバに送信



データ漏洩や不正利用のリスク

プライバシ保護型エッジAI

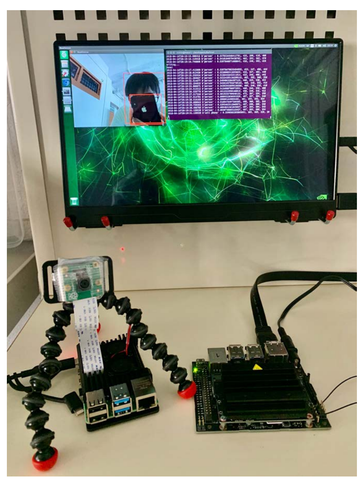
個人情報が除去された中間データのみを送信することで入力データを秘匿



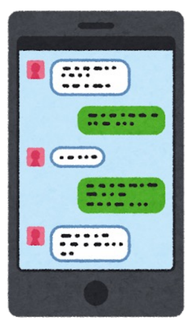
特徴: 幅広い応用が可能（※機械学習モデルは別途準備が必要）

応用例

- 人流計測
- 侵入検出
- 見守り



- テキスト生成
- 自動応答
- 大規模言語モデル



- 画像生成

- 音声認識

技術展示: エッジAIによる物体検出

画像そのものはラズパイからエッジサーバに送信せずにリアルタイムかつ高精度な物体検出を実現

技術詳細: Split Computing

大規模機械学習モデルを利用者とサーバで分散処理。モデルを分割し、利用者（データ入力者）はモデルの入力側 (HN: Head network)を保持し、クラウドには出力側を配置。処理した中間データを送信することで、入力データを秘匿可能