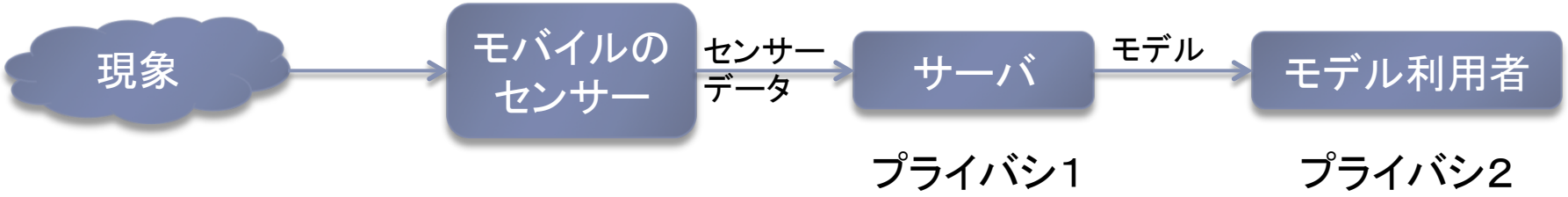
T-13

クラウドセンシングにおける差分プライバシーを保証する線形回帰モデル学習

チャン クワン カイ[*1], 福地 一斗[*1], 佐久間 淳[*1*2]
*1 筑波大学システム情報工学研究科コンピュータサイエンス専攻, *2 JST CREST

クラウドセンシングにおけるモデル学習のフレームワーク



- 動機
  - ✓ クラウドセンシングにより交通渋滞や空気汚染などの大規模な現象を観測する
  - ✓ 収集してきたデータを用いて現象の予測モデルを学習する
- 問題
  - ✓ センサーデータには位置情報などの個人情報が入っている
  - ✓ プライバシ1：サーバは個人情報を開示するリスク
  - ✓ プライバシ2：モデル利用者は公開モデルから個人情報を開示するリスク
- 貢献
  - ✓ 初めてプライバシ1とプライバシ2の保護を同時に保証する入力摂動法
    - サーバに対して正規乱数による摂動に基づくプライバシを保証する
    - モデル利用者に対して差分プライバシーを保証する
  - ✓ 学習モデルの汎化損失は既存手法と同程度でO(1/n)のサンプル複雑度を持つ