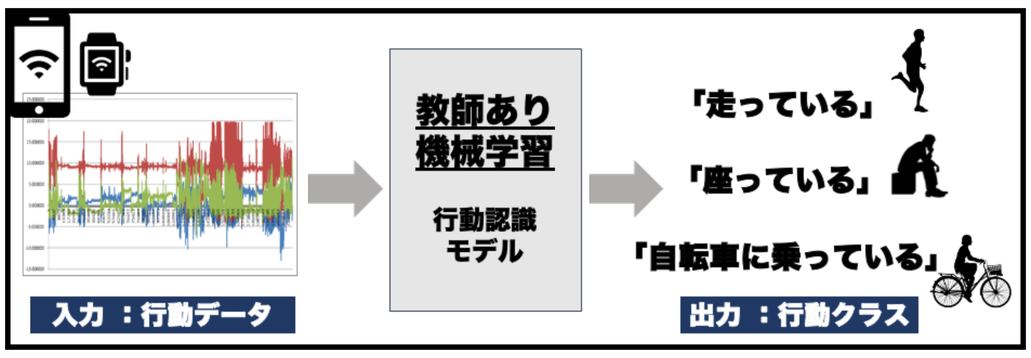
SecHack365

プライバシー保護と高い認識精度を両立可能な行動認識システム

研究駆動コース　安達康平

行動認識とは

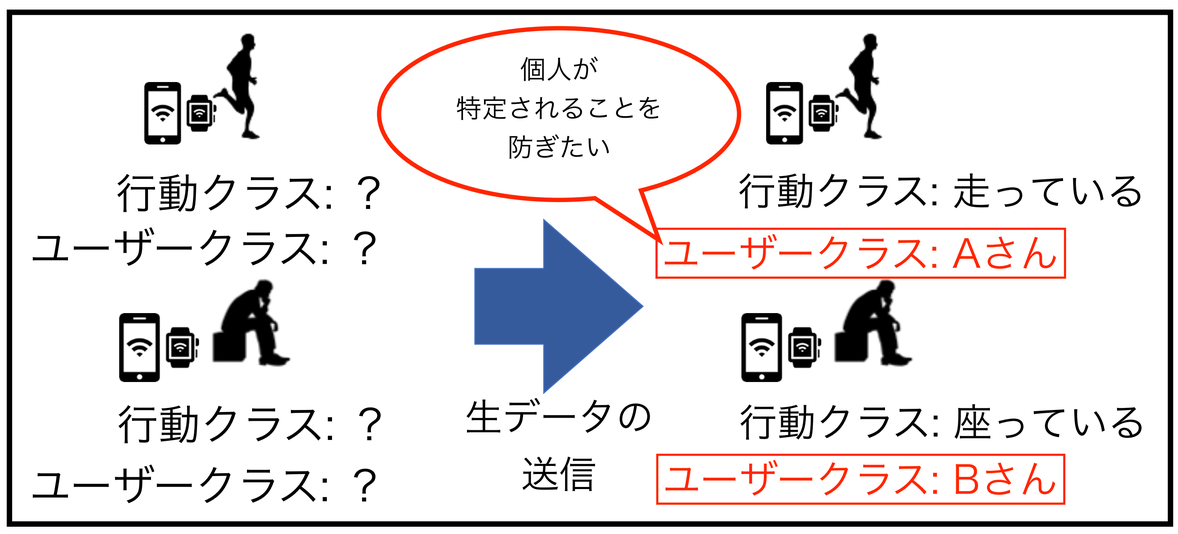
行動認識とはスマートフォンなどに搭載されている
センサを用いて人が人の行動を認識する技術である.
現在使われている行動認識システムでは，デバイス上から
取得したセンサデータを生データの状態で送信している.
一方でセンサデータを用いることで人の身長，性別，身
長・体重を予測する研究が多くされている.



行動認識

本研究の目的

生データの状態でサーバに送信していた場合，行動認識を
行うことができる一方で，サーバ上からデータがリーク
した際に**ユーザーの識別が行われるリスク**がある.
本研究では，ユーザー認識の精度を抑えることによる
プライバシー保護と高い行動認識の精度を両立可能な
行動認識システムの構築を目指す.

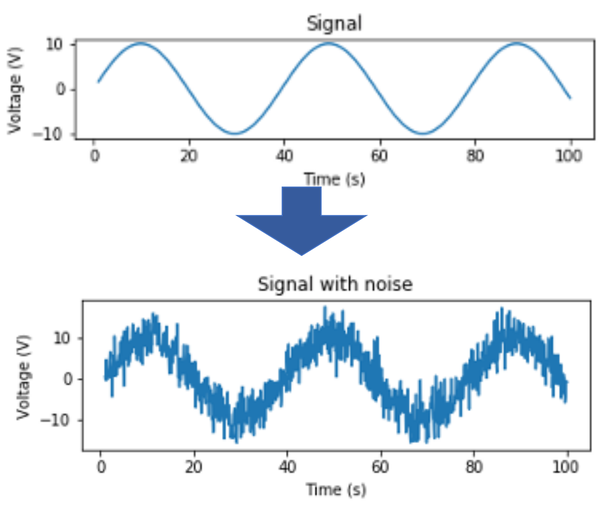


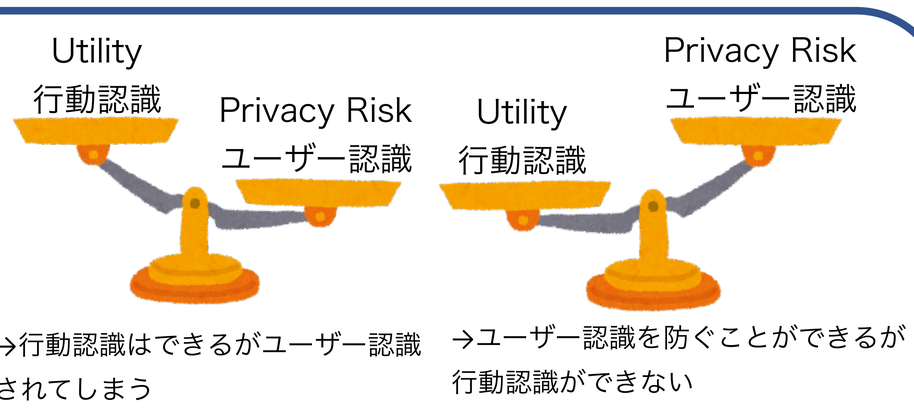
提案手法

Utility(行動認識)とPrivacy Risk(ユーザー認識)は**トレードオフの関係である**ため，それぞれのバランスを考慮しなければならない.
本研究では，**①センサデータにノイズを付加**と**②特徴量重要度に基づく特徴量選択**を行った．その後，①と②を組み合わせた.

①センサデータにノイズを付加

Additive white Gaussian noiseを用いたノイズの付加





→行動認識はできるがユーザー認識されてしまう

→ユーザー認識を防ぐことができるが行動認識ができない

②特徴量重要度に基づく特徴量選択

ユーザー認識の特徴量重要度	行動認識の特徴量
特徴量A	~~特徴量A~~
特徴量B	~~特徴量B~~
特徴量C	~~特徴量C~~
特徴量D	~~特徴量D~~
特徴量E’	特徴量E
特徴量F’	特徴量F

ユーザー認識の特徴量重要度上位の特徴量を
行動認識の特徴量から削除

結果

10分割交差検証を用いてユーザー認識および行動認識の
それぞれの精度をAccuracy及びF1-Scoreを用いて評価

	ユーザー認識 Accuracy	ユーザー認識 F1-Score	行動認識 Accuracy	行動認識 F1-score
BaseLine	0.972 ± 0.066	0.972 ± 0.065	0.917 ± 0.013	0.791 ± 0.032
①ノイズ	0.521 ± 0.057	0.507 ± 0.058	0.723 ± 0.060	0.543 ± 0.044
②特徴量選択	0.857 ± 0.125	0.853 ± 0.126	0.899 ± 0.016	0.762 ± 0.033
ノイズ + 特徴量選択	0.192 ± 0.036	0.144 ± 0.037	0.552 ± 0.060	0.373 ± 0.045

考察

人の識別は，行動のペースやリズムに関連し
ておりノイズを加えることで周波数領域の
特徴量に影響が出たと考えられる

今後の課題

- 行動認識精度の低下をさらに抑える
- 被験者数を増やした場合の検証

NICT 国立研究開発法人 情報通信研究機構

GitHub: github.com/KohheiAdachi/Privacy-Preserving-HAR-Project