# 行動変容支援サービスにおけるユーザ保護と有用性を両立する重み付き $\epsilon$-差分プライバシーの提案

藤本 隆晟 [†1]　中村 優吾 [†2]　荒川 豊 [†3]
九州大学　九州大学　九州大学

## 1. はじめに

センサや機械学習アルゴリズムの技術革新により，ユビキタスコンピューティングやヒューマンコンピュータインタラクション分野では人間の行動認識（Human Activity Recognition: HAR)[1] に関する研究が進んでいる．行動認識は運動・健康支援や娯楽，セキュリティ等，幅広い分野で応用されており，近年では加速度やジャイロセンサ，GPS 等，複数のセンサを搭載したスマートデバイスの普及によって，人の行動認識に基づく行動変容支援サービスが多く開発されている．これは行動変容支援サービスの実装には多くの行動データを集めることが必須となるからである．しかし，スマートデバイスから収集したセンサデータにはユーザのプライバシーが含まれているため，そのデータの取り扱いにはプライバシーへの配慮が要求されている．

プライバシーの保護技術としては従来からユーザ ID の削除や k-匿名化が存在する．前者は利用するデータベースのレコードから個人が特定される ID を削除するという単純な手法だが，Ji らの研究 [2] によると脱匿名化攻撃に対して脆弱であることが証明されている．後者はデータベース内に同じ準識別子を持つレコードが k 件以上存在する，という k-匿名性 [3][4] を満たすようにデータ加工する技術である．しかし，この技術によってプライバシーが保証されるのはデータベースの複数属性を組み合わせることで個人を特定しようとするリンケージ攻撃に限られる [5]．そこで，これら従来の脆弱性を克服するために提唱されたプライバシー保護技術が「差分プライバシー」である [6]．差分プライバシーとは個人のプライバシーをどの程度守ることができるかを定量的に示す枠組みであり，数学的に厳密なプライバシー保護を満たす基準を定めている．差分プライバシーを実現するにはプライバシー保護メカニズム（関数・統計処理や機械学習モデルの生成等）[7] によって，データにノイズを加算する．その代表的なメカニズムとして「Laplace メカニズム」と呼ばれる手法よくが用いられる [8]．しかし，差分プライバシーに基づくプライバシー保護メカニズムはデータに対して統計的なノイズ加算を用いるため，プライバシーを保証すると同時にデータの有用性が下がってしまう．つまり，ユーザのプライバシーとデータ有用性の間にはトレードオフの関係があり，これを両立させるのが様々な行動変容支援サービスにとっての課題である．行動変容支援サービスにおいて，センシングデータの有用性を妨げずにユーザのプライバシーを保護するための適切なメカニズムにおけるプライバシーパラメータ（$\epsilon$）は未だ明らかになっていない．そこで本研究では，行動変容支援サービスにおいて適切なプライバシーパラメータ $\epsilon$ について検証し，ユーザ保護と有用性を両立したプライバシー保護メカニズムの提案と評価を行った．

本研究で想定する行動変容支援サービスはライフロギングによる運動促進システムである．ユーザのスマートフォンから収集されるデータを行動認識モデルによって分類し，その結果の行動ラベルと行動に基づく報酬をユーザにフィードバックすることで行動データを記録するとともに運動増進を促すことを目的とする．またこのシステムにおける脅威は，ライフロギングシステムのデータベースに対して攻撃者による推論攻撃が行われ，攻撃者の背景知識に基づくユーザ認識モデルによって個人が特定されることである．ここで，行動認識モデル，ユーザ認識モデルは機械学習アルゴリズムの 1 つである Random Forest を用いて学習モデルを構築した．

本研究におけるプライバシー保護メカニズムの提案手法では，Laplace メカニズムと差分プライバシーの合成定理に基づき，想定している攻撃者のユーザ認識モデルの構築において重要な特徴量に対してのみノイズを多く加え，その他の特徴量に対しては一様のノイズを加える．この提案手法を 2 つの認識モデルにおいて 10 分割交差検証法にて，行動認識精度（サービスの有用性）と，ユーザ認識精度（プライバシー保護）を F 値を用いて評価した．

本稿では，2 章で関連研究を紹介し，本研究の位置づけを明らかにする．3 章では本研究で想定しているライフロギングシステム構成とその脅威モデルについて述べ，行動変

---

A Proposal for Weighted $\epsilon$-Differential Privacy to Realize User Protection and Availability in Behavior Change Support Service

[†1] RYUSEI FUJIMOTO, Kyushu University
[†2] YUGO NAKAMURA, Kyushu University
[†3] YUTAKA ARAKAWA, Kyushu University

容支援サービスにおけるサービス要求とプライバシー要求を定義する．4 章では本研究における提案手法について述べ，5 章でその結果を評価する．最後に 6 章で行動変容支援サービスにおけるユーザ保護とサービスの有用性を両立するプライバシー保護メカニズムについて考察し，今後の展望について述べる．

## 2. 関連研究

本章では本研究に関連する既存研究について述べる．まず，$\epsilon$-差分プライバシーについての定義や動向について述べる．次に差分プライバシーを保証した HAR に関する研究におけるプライバシー保護メカニズムについて述べる．

### 2.1. $\epsilon$-差分プライバシー

前章でも述べた通り，ユーザ ID の削除や k-匿名化では，特定の攻撃手法のみのプライバシーしか保証されない．そこで特定の攻撃のみではなく，任意の攻撃に対してプライバシーが保証することを目的とし，個人のプライバシーがどの程度保証されるかを定量的に示した差分プライバシーが提唱された [5]．差分プライバシーではアプリケーションで利用されるデータベースへのクエリ処理に対し，そのクエリ結果にノイズを加えるプライバシー保護メカニズム $\mathcal{M}$ とそのプライバシー強度を表すパラメータ $\epsilon$ によって，以下のように定義される [6]．

**定義 1.**（$\epsilon$-差分プライバシー）$\mathcal{D}$ をデータベースのドメインとし，$D_1$ と $D_2$ は 1 レコードのみ異なる任意の隣接したデータベースとする（$D_1, D_2 \in \mathcal{D}$）．このとき，プライバシー保護メカニズム $\mathcal{M} : \mathcal{D} \to \mathcal{R}$ が式（1）を満たすならば，$\mathcal{M}$ は $\epsilon$-差分プライバシーを保証する．ここで，$\mathcal{S}$ は $\mathcal{M}$ の出力空間 $\mathcal{R}$ の任意の部分空間とする（$\mathcal{S} \subseteq \mathcal{R}$）．

$$P(\mathcal{M}(D_1) \in \mathcal{S}) \leq e^{\epsilon} P(\mathcal{M}(D_2) \in \mathcal{S}) \tag{1}$$

上記の定義より，プライバシー保護メカニズム $\mathcal{M}$ が $\epsilon$-差分プライバシーを満たすならば $\epsilon$ の値が小さいほどプライバシーをより厳格に保証することが可能である．そのため，プライバシー保護メカニズム $\mathcal{M}$ は $\epsilon$ の値が小さいほどノイズを多く加算する．本稿では $\epsilon$ をプライバシーパラメータとして扱う．また，プライバシー保護メカニズムは必ずしも 1 つである必要はなく，下記の定理によって複数の差分プライバシーを満たすメカニズムを合成した場合にも差分プライバシーは保証される [9]．

**定理 1.**（合成定理）$\epsilon_i$-差分プライバシーを満たすプライバシー保護メカニズム $\mathcal{M}_i\,(i \in \{1, 2, \ldots, n\})$ があり，$\mathcal{M}$ を $\mathcal{M}(D) = (\mathcal{M}_1(D), \mathcal{M}_2(D), \ldots, \mathcal{M}_n(D))$ と定義する．このとき，$\mathcal{M}$ は $\sum_{i=1}^{n} \epsilon_i$-差分プライバシーを満たす．

### 2.2. 差分プライバシーを保証する VR インターフェイスでの文書分類に関する研究

ヒューマンコンピュータインタラクション分野では，VR ヘッドセットに搭載されるアイトラッキング技術によってユーザ情報の識別を防ぐためのプライバシーに配慮した VR インタフェースの提案とその有用性に関する研究 [10] で差分プライバシーが導入されている．この研究の実験では被験者が VR ヘッドセッドを装着し，目の前に浮かぶ文書（3 種類）を読むことでその眼球運動を記録した．記録された時系列データから眼球運動の特徴量を 52 個抽出し，特徴量ごとに異なるプライバシー保護メカニズム（指数メカニズム）を適用させた．つまり，この研究では**定理 1** に基づき，特徴量 $f_i$ ごとのプライバシーパラメータ $\epsilon_i$ の合計値がプライバシー強度となる．このノイズを加えた特徴量を用いてサポートベクターマシン分類器で 3 つの文書，2 つの性別，20 人のユーザを分類した．評価結果としては $\epsilon = 15$ とすることで偶然性と同様のプライバシー保護を実現しつつ，目的である文書のタイプ分類の実用性を約 70% 維持した．つまり，この研究によって視線データに基づく文書のタイプ分類においては，ユーザやその性別情報を保護しつつ，有用性も両立できることを示している．

### 2.3. 差分プライバシーを保証するスマートフォンのセンサデータに基づく HAR に関する研究

近年，行動変容支援サービスを実現するにあたっては，スマートフォンやスマートウォッチ等に搭載されたセンサによってセンシングした行動データが活用されている [11][12]．しかし，これらのデータは有益である反面，ユーザのプライバシー情報を多く含んでいるため，それを保護する研究が進められている．Garain らの研究 [13] ではスマートフォンの 3 軸加速度センサのデータに対し，差分プライバシーに基づくプライバシー保護メカニズムを適用する HAR フレームワークの提案によってプライバシー保護と行動認識の精度のトレードオフ関係について調査している．提案手法では収集された加速度センサの RAW データを 3 次元ベクトルと捉え，以下の手順で特徴量抽出前と特徴量抽出後にプライバシー保護メカニズムを用いる．

(手順 1) 加速度ベクトルないしはその特徴量ベクトルに一様なノイズ $\boldsymbol{p} = (p, p, p)$ を加えて，ベクトルを回転させる．($p \in \mathbb{R}$)

(手順 2) ノイズを加算したベクトル空間におけるベクトルの大きさを一定にするために，手順 1 で生成したベクトルをスカラー倍する．

(手順 3) 上記手順のメカニズムが**定義 1** を満たすとき，そのプライバシーパラメータ $\epsilon$ を算出する．

提案手法では，HAR フレームワークに Deep Multi Layer Perceptron (DMLP) を用いており，ノイズを加える特徴量選択の際に，ノイズを加えない場合と 9 つの特徴量それぞれにノイズを加えた場合の 10 パターンについて 10 分割交差検証を行った．その結果として，スマートフォンにおける z 軸加速度データの標準偏差値にノイズを加えることは行動認識に大きな影響を及ぼすことなくユーザ認識精度を下げることができると判明した．HAR フレームワークの評価結果としては 8 人の被験者によるデータセットに対し，差分プライバシー導入前では行動認識精度が約 96%，ユーザ認識精度が約 95% だったが導入後は行動認識精度が約 96%，ユーザ認識精度が約 49% となり，行動認識精度を維持してユーザ認識精度を下げることに成功している．

しかし，先行研究の手法では行動変容支援サービスにおいてユーザ認識精度はまだ偶然性と同様のレベル（プライバシー要求）には程遠い．そこで本研究では，ユーザ認識精度をプライバシー要求を満たし，行動認識精度もサービス要求を満たすような差分プライバシーに基づくプライバシー保護メカニズムを提案し，行動変容支援システムにおけるユーザのプライバシー保護とサービス有用性のトレードオフについて考察する．

## 3. 行動変容支援サービス

本章では，まず本研究で想定する行動変容支援サービスとしてライフロギングシステムについての概要を述べる．次に行動変容支援サービスにおける脅威やその脅威の原因となりうる背景知識について述べる．最後にサービスの構成や脅威を踏まえて，本サービスで求められるサービス要求とユーザ保護で求められるプライバシー要求について定義する．

### 3.1. 行動変容支援サービス概要

本研究では，行動変容支援サービスとしてライフロギングによる運動促進システムを対象とする．ライフログとは人間が生活する上での行動を記録することであり，システムとしては私生活における行動のセンシングデータに対し行動（歩く，座る等）がラベル付けされ，それを記録する．本研究におけるシステム構成図を図 1 に示す．構成として，ユーザはスマートフォンに搭載された加速度センサ，ジャイロセンサとライフログを確認できるアプリケーションを利用する．そして，アプリケーションではそれぞれのセンサでセンシングされた RAW データのみをサーバに送信する．送信されたデータは特徴量抽出され，特徴量データがサーバのデータベースに保存される．ここで，データベースにはユーザ ID は含まれないとする．次に，ユーザの行動情報を含む特徴量データを行動認識モデルに入力することで行動を分類し，データに行動ラベルを付与する．最後に付与された行動ラベルと行動に基づく報酬をフィードバックすることでユーザの運動増進を促す．本研究において分類する行動は「座る，立つ，寝る，歩く，階段を登る，階段を降りる」の 6 種類である．

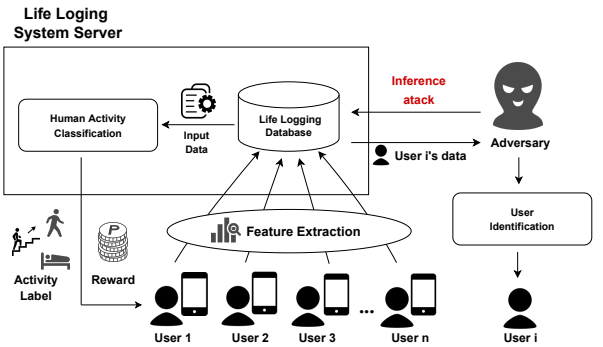



図 1　ライフロギングシステムとそれを襲う脅威モデル
Figure 1　Life logging system and the threat models that attack it

### 3.2. 脅威モデル

次に，本研究で想定する行動変容支援サービスにおける脅威について考える．このライフロギングシステムにおける脅威とは，攻撃者の背景知識と攻撃手法によって構成される．また本サービスでの攻撃者の目的は行動データからユーザを特定することとする．まず攻撃者の背景知識については最悪のケースを想定する．攻撃者は差分プライバシーの**定義 1** に基づき，サービスにおける行動認識モデルを構築する際のデータセットと高々 1 レコード異なるデータセットを保持しているとし，さらにはサービスを利用するユーザの ID とデータセットに含まれる匿名化されたユーザ ID の対応付けが可能であるとする．攻撃手法としては，図 1 に示すライフロギングシステムのデータベースに対し，攻撃者はクエリを実行することで，あるユーザの行動データを取得する．そして，背景知識に基づいて構築されたユーザ認識モデルによって個人の特定を行う．この状況下において差分プライバシーを導入し，想定する脅威からユーザ保護を実現することが本研究の目的である．

### 3.3. サービス要求とプライバシー要求

差分プラバシーの概念を行動変容支援サービスに導入するにあたって考えるべき問題は，ユーザのサービスの有用性とプライバシー保護がトレードオフ関係になっているということである．そこで，想定するサービスを実現するに

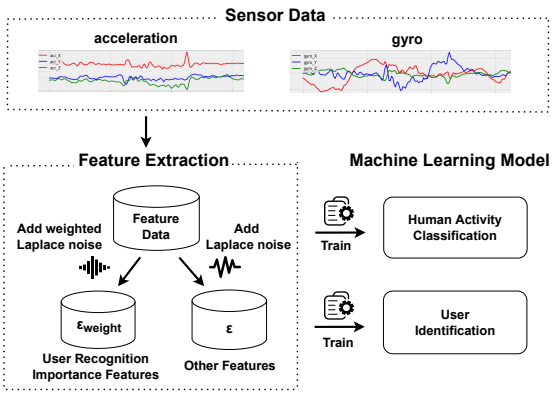



図 2　重み付き $\epsilon$-差分プライバシーによる学習モデル構築
Figure 2　Learning Model building with Weighted Epsilon-Differential Privacy

あたり，ユーザから求められるユーザ保護とサービス有用性を両立するためのプライバシー要求とサービス要求について考える．まずプライバシー要求については，2 章で紹介した先行研究 [10] で偶然的にユーザが特定される確率と定義している．本研究においてもこれに倣い，偶然的にユーザが特定される確率として，$\frac{1}{\text{利用ユーザ数}}$ をプライバシー要求の指標として利用する．次にサービス要求について説明する．今回分類する行動は「座る，立つ，寝る，歩く，階段を登る，階段を降りる」の 6 種類であり，これは静的動作である「座る，立つ，寝る」と動的動作「歩く，階段を登る，階段を降りる」の 2 つに大きく分けることができる．そこで，サービス要求の指標としてはこの 2 つの動作を正確に分類することができるとする．

しかし，ユーザによってはプライバシー漏洩について考慮せずサービス有用性を求める場合や，完全にプライバシーが保護された上でのサービス提供を要求する場合もあり，考え方は各ユーザに依存してしまう．そこで，5 章ではこの指標を基準とした場合における従来手法と提案手法を比較し，提案手法が行動変容支援サービスにおけるサービス有用性を保ちながらもプライバシーを十分保護できることを示す．

## 4.　提案手法（重み付き $\epsilon$-差分プライバシー）

### 4.1.　学習モデルとデータセット

本研究では，ライフロギングシステムで利用する行動認識モデル，攻撃者が保持するユーザ認識モデルの 2 つの学習モデルを構築する．学習モデルの構築は，先行研究 [14] でスマートフォンに搭載したセンサデータを用いた行動認識において精度が最も高かった機械学習アルゴリズムである Random Forest を利用した．また学習モデル構築における学習・テストデータには，19 歳から 48 歳までの 30 人の被験者を対象とした，スマートフォン (Samsung Galaxy S II) に搭載された加速度センサとジャイロセンサのオープンデータセットである UCI HAR[15] に含まれる RAW データを利用した．提案手法においては，時系列 RAW データから時間領域と周波数領域の特徴量を抽出したデータセットでの 10 分割交差検証によってモデルの評価を行う．特徴量抽出の手法については 4.2 節で述べる．モデルの評価指標には F 値を用いており，Precision（適合率）と Recall（再現率）の調和平均として，下記の式（2) で表される．

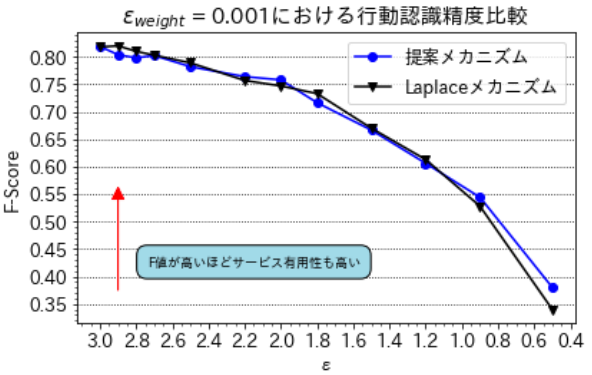
$$F\text{-}Score = 2 \cdot \frac{Recall \cdot Precision}{Recall + Precision} \tag{2}$$

### 4.2.　特徴量抽出

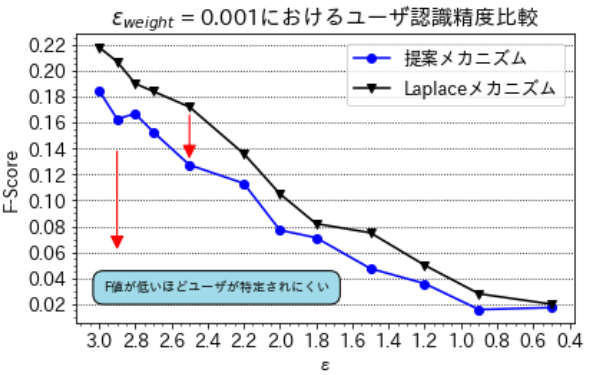
最初に，一定間隔（50Hz）で計測されている時系列 RAW データに対して，ノイズフィルタによる前処理を施し，データに含まれるノイズを除去した．その後，加速度データに関してはカットオフ周波数が 0.3Hz のバターワース型ローパスフィルタを用いることで静加速度と動加速度に分離した．次に動加速度とジャイロセンサで取得した角速度の信号データを時間微分することにより，ジャークを導出した．ここで，動加速度と角速度，ジャークの信号においては，高速フーリエ変換（FFT）を適応させることで周波数領域における信号データも取得した．これらの時間領域，周波数領域における信号データはオーバーラップ 50% で 2.56 秒のスライディングウィンドウによりデータをサンプリング（128 data/window）し，特徴量を 640 個抽出した．最後に抽出した特徴量データに対して行動と匿名ユーザ ID のラベル付けを行なった．

### 4.3.　プライバシー保護メカニズムの提案

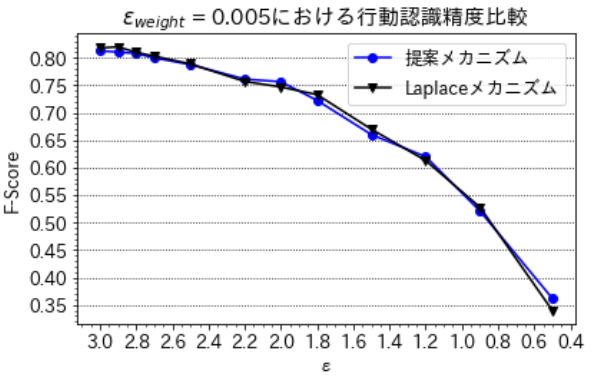
本研究で提案する差分プライバシーを満たすプライバシー保護メカニズムについて説明する．4.1 節，4.2 節で述べた通り被験者 30 人, 特徴量 640 個のデータセットを用いる．本研究の目的としては行動認識精度を維持しつつ，ユーザ認識精度を低下させることである．そこで，本研究では学習モデルの構築時の行動認識，ユーザ認識における特徴量重要度に基づいてノイズの加算方法を変化させた．具体的には，まず学習モデル構築に利用する機械学習アルゴリズムである Random Forest のジニ係数によって行動認識モデル，ユーザ認識モデルの各特徴量重要度を求める．そして，各特徴量重要度の高い上位 n 個の特徴量において重複率が最も低い n を求め，ユーザ認識モデルの特徴量重要度が上位 n 個の特徴量に対しノイズを多く加算する．提案手法でのプライバシー保護メカニズムを図 2 に示す．ノイズを多く加算するということはプライバシーパラメータ $\epsilon$ を小さくする必要があり，$\epsilon$ の値は小さいほどプライバシーはより厳格に保証される．そのため，この提案メカニズム



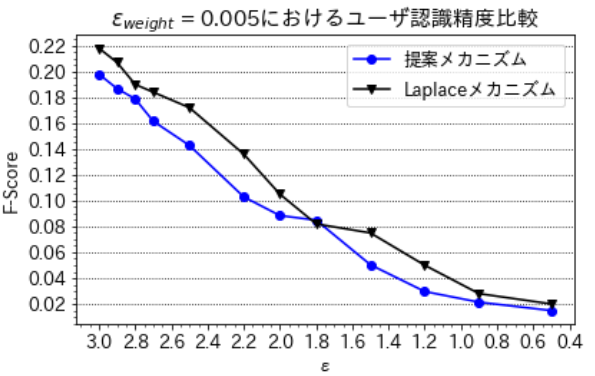

(a) $\epsilon_{weight} = 0.001$ における行動認識モデルの評価結果




(b) $\epsilon_{weight} = 0.001$ におけるユーザ認識モデルの評価結果




(c) $\epsilon_{weight} = 0.005$ における行動認識モデルの評価結果




(d) $\epsilon_{weight} = 0.005$ におけるユーザ認識モデルの評価結果

図 3　プライバシー強度を比較指標にした場合のモデル評価結果

Figure 3　Model evaluation results when privacy strength is used as a comparative measure

はユーザ認識において重要な特徴量には重み付けされたプライバシーパラメータ $\epsilon_{weight}$ のノイズを加算し，その他の特徴量には一様の $\epsilon$ のノイズを加算する ($\epsilon_{weight} < \epsilon$)．ここで，ノイズ加算には Laplace メカニズムを利用した．この提案するプライバシー保護メカニズムは**定理 1** に基づき，$(\epsilon_{weight} + \epsilon)$-差分プライバシーを満たす．

5 章では従来の Laplace メカニズムで一様にノイズを加算した場合と提案するプライバシー保護メカニズムによって重み付けしてノイズを加算した場合における行動認識精度，ユーザ認識精度の評価を行う．

## 5.　評価実験

本章では，本研究で提案するプライバシー保護メカニズムを利用したモデル評価実験の内容について述べる．その後，従来手法と提案手法を比較し，その評価結果について述べる．

### 5.1.　実験内容

本実験の目的は，提案手法がサービス要求とプライバシー要求を同時に満たすことができるプライバシー保護メカニズムであるかを従来手法と比較し，評価することである．

実験前に，まずノイズなしの特徴量を学習させた行動認識モデル，ユーザ認識モデルにおける各特徴量重要度を算出し，各特徴量重要度の高い上位 n 個の特徴量において重複率が最も低い n を求めた．本実験では $n = 119$ となり，ユーザ認識モデルの特徴量重要度が高い 119 個の特徴量に重み付けした Laplace ノイズを加算することにする．

本実験では，提案するプライバシー保護メカニズムにおける $\epsilon$ と $\epsilon_{weight}$ のパラメータを変化させて，特徴量によって重み付けした Laplace ノイズを加えた際の行動認識とユーザ認識モデルの F 値を評価する．ここで重み付けを行うパラメータ $\epsilon_{weight}$ については，$\{0.001, 0.005\}$ の 2 つの値で実験を行う．実験結果は Laplace メカニズムによるノイズ生成のランダム性を考慮し，2 つのパラメータの組み合わせに対して 5 回ずつ実験を行い，平均化した結果とする．

### 5.2. 評価結果

本研究の提案手法を評価するために比較対象を設定する．比較対象はノイズを加算しなかった場合と，従来の Laplace メカニズムで $\epsilon$ のパラメータを変化させて特徴量に対して一様の Laplace ノイズを加えた場合のモデル評価値とし，後者は同様に 1 つの $\epsilon$ に対して 5 回ずつモデル評価を行い，平均化したものを利用した．まず本研究の提案手法と従来手法について，プライバシー強度を比較指標とした場合の結果を図 3 に示す．図 3 の (a), (b) は $\epsilon_{weight} = 0.005$ における比較結果であり，(c), (d) は $\epsilon_{weight} = 0.001$ における比較結果である．これより比較指標をプライバシー強度とした場合は，提案するプライバシー保護メカニズムが，従来手法である Laplace メカニズムと同等の行動認識精度を維持，もしくは少し向上しつつ，ユーザ認識精度を一部を除き低下させるという結果になった．

また，次に比較指標をプライバシー要求にした場合について両者を比較する．3.3 節で述べたが，本研究ではプライバシー要求を偶然的にユーザが特定される確率と定義している．これより，本実験では被験者 30 人のデータセットを利用しているため，本研究におけるプライバシー要求は 3% と決定した．このプライバシー要求において提案手法と従来手法を比較した結果を図 4 に示す．図 4 における左のグラフはノイズを加算しなかった場合の認識精度である．ノイズなしの場合と比較すると，プライバシー要求 3% というのはユーザ認識精度を大幅に低下させていることになる．次に中央のグラフは従来手法である Laplace メカニズムによる一様にノイズを加算した際にプライバシー要求を満たす場合（$\epsilon = 0.9$）である．最後に右のグラフは提案手法による $\epsilon_{weight} = 0.005$ で重み付けをした際のプライバシー要求を満たす場合（$\epsilon = 1.2$）である．これよりプライバシー要求を評価指標とした場合においても，提案手法が従来手法より行動認識精度を約 10% 向上するという結果になった．また，本研究ではプライバシー要求を 3% と定義したが，別に定義した場合においても，ほとんどの場合で行動認識精度が従来手法に比べて向上した．

最後に，比較指標をサービス要求にした場合について両者を比較する．図 4 の Laplace メカニズムと提案メカニズムでノイズを加算した際の行動認識における混同行列を図 5 に示す．図 5(a) が従来手法による結果で図 5(b) が提案手法による結果である．本研究における行動変容支援サービスではサービス要求としてはこの 2 つの動作を正確に分類することができるとしている．その観点について，従来手法では動的動作を静的動作と分類している点が提案手法と比較すると少々見当たるがほとんど差異はない．そのため両者とも動的動作と静的動作の分類は問題なく行うことができる．しかし，提案手法が従来手法に比べて F 値が約 10% 向上していることもあり，図 5(a) と (b) を各行動で比較すると全体的に精度が向上している結果となった．このことから，サービス有用性は提案手法により十分向上していると言える．次章では以上の内容を踏まえて実験結果の考察を行う．

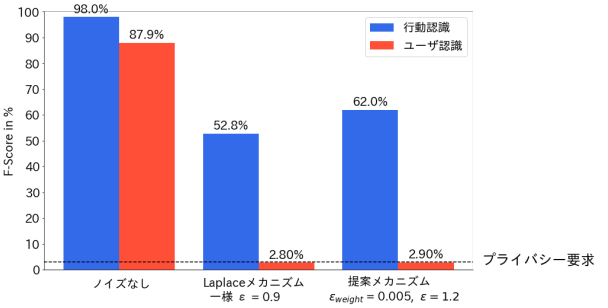
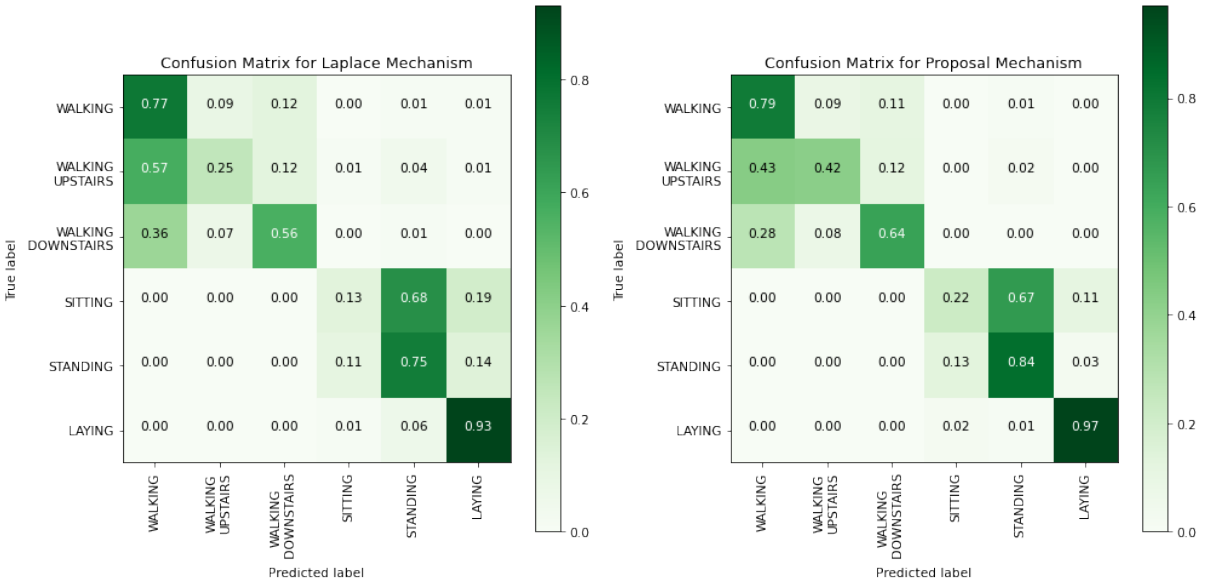



図 4　プライバシー要求を比較指標とした場合のモデル評価結果

Figure 4　Model evaluation results when privacy requirements are used as a comparative measure

## 6. 考察と展望

5 章より，従来の一様に Laplace メカニズムを適用する場合と比較して，提案手法がプライバシー要求を満たすようにユーザ保護を実現しつつ，サービス有用性を向上できることがわかった．これは適用する Laplace メカニズムを 2 つにしたことで**定理 1** より，単純に 1 つのメカニズムを適用した場合と比べて，微小だが制約を緩めることが要因として考えられる．またノイズを加算するものを特徴量の重要度で変化させたことも要因の 1 つだろう．一方，行動認識，ユーザ認識モデルの各特徴量重要度の重複率に基づいてノイズを重み付けする特徴量を選択したことにより，その特徴量の中には行動認識にとっても重要な特徴量が一部含まれてしまった．そのため，図 4 のようにプライバシー要求を満たしつつ，サービス有用性を向上するのには限界があり，先行研究 [13] のような精度の高さを実現するまでには至らなかった．しかし，今回の実験を通して，差分プライバシーの合成定理を用いてプライバシー保護メカニズムを組み合わせることでより有用性のあるメカニズムができることがわかった．応用するアプリケーションやシステムにはそれぞれに適切なメカニズムがあり，適切なメカニズム選択を行うことがより，サービス有用性を高める．今後の展望としては，行動変容支援サービスにとって十分な有用性を発揮するプライバシー保護メカニズムについて，さらに検討していきたいと考えている．またその際に，今回は 1 つのデータセットに限って実験を行ったが，他のデータセットでも検証を行い，一般的に利用できるような特徴




(a) Laplace メカニズムにおける行動認識モデルの混同行列　　(b) 提案メカニズムにおける行動認識モデルの混同行列

図 5　サービス要求を比較指標とした場合のモデル評価結果

Figure 5　Model evaluation results when service requirements are used as a comparative measure.

量選択アルゴリズムについても考えていく．

## 7. おわりに

本研究では，行動変容支援サービスにおけるユーザ保護と有用性を両立したプライバシー保護メカニズムの提案と評価を行った．結果としては，プライバシー要求を偶然的にユーザが特定される確率未満と定義した場合において，提案手法が従来手法に比べて約 10% の行動認識精度を向上させた．しかし，行動認識精度としては 62% 程度であり，静的動作，動的動作を分類することは可能だが正確に全行動を分類できるまでには至らなかった．

行動変容支援サービスを利用するユーザには，プライバシー保護よりサービス有用性の向上を要求するユーザもいれば，サービス有用性よりも完全にプライバシーが保護された状態を期待するユーザも存在する．そのため行動変容支援サービスにおいてトレードオフな関係にあるユーザのプライバシー保護とサービス有用性の具体的な基準を決めることは難しいが，それを踏まえ，各ユーザに適したプライバシー保護とサービスを提供できるようなプライバシー保護メカニズムの開発が求められる．今後は行動変容支援サービスにおける，より有用性の高いプライバシー保護メカニズムや特徴量選択アルゴリズムについて検討し，プライバシー要求を達成した上での行動認識精度の向上を目指していきたい．

**謝辞**　本研究の一部は，科学研究費補助金（19KT0020）および JST さきがけ（JPMJPR21P7）の助成を受けたものである．

## 参考文献

[1] Slim, S. O., Atia, A., Elfattah, M. M. and M.Mostafa, M.-S.: Survey on Human Activity Recognition based on Acceleration Data, *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 3 (online), 10.14569/IJACSA.2019.0100311 (2019).

[2] Ji, S., Mittal, P. and Beyah, R.: Graph Data Anonymization, De-Anonymization Attacks, and De-Anonymizability Quantification: A Survey, *IEEE Communications Surveys Tutorials*, Vol. 19, No. 2, pp. 1305–1326 (online), 10.1109/COMST.2016.2633620 (2017).

[3] Sweeney, L.: K-Anonymity: A Model for Protecting Privacy, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, Vol. 10, No. 5, p. 557–570 (online), 10.1142/S0218488502001648 (2002).

[4] 小栗秀暢, プライバシー保護データ流通のための匿名化手法, システム/制御/情報, Vol. 63, No. 2, pp. 51–57 (2019).

[5] 寺田雅之, 差分プライバシーとは何か，システム／制御／情報， Vol. 63, No. 2, pp. 58–63（オンライン），10.11509/isciesci.63.2$_5$8(2019).

[6] Dwork, C.: Differential Privacy, *Automata, Languages and Programming* (Bugliesi, M., Preneel, B., Sassone, V. and Wegener, I., eds.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 1–12 (2006).

[7] 寺田雅之, 差分プライバシの基礎と動向, 情報処理， Vol. 61, No. 6, pp. 591–599 (2020).

[8] Xue, W., Shen, Y., Luo, C., Xu, W., Hu, W.

and Seneviratne, A.: A differential privacy-based classification system for edge computing in IoT, *Computer Communications*, Vol. 182, pp. 117–128 (online), https://doi.org/10.1016/j.comcom.2021.10.038 (2022).

[9] Dwork, C. and Roth, A.: The Algorithmic Foundations of Differential Privacy, Vol. 9, No. 3–4, p. 211–407 (online), 10.1561/0400000042 (2014).

[10] Steil, J., Hagestedt, I., Huang, M. X. and Bulling, A.: Privacy-Aware Eye Tracking Using Differential Privacy, *Proceedings of the 11th ACM Symposium on Eye Tracking Research amp; Applications*, ETRA '19, New York, NY, USA, Association for Computing Machinery, (online), https://doi.org/10.1145/3314111.3319915 (2019).

[11] Vecchio, A., Mulas, F. and Cola, G.: Posture Recognition Using the Interdistances Between Wearable Devices, *IEEE Sensors Letters*, Vol. 1, No. 4, pp. 1–4 (online), 10.1109/LSENS.2017.2726759 (2017).

[12] Mekruksavanich, S. and Jitpattanakul, A.: Biometric User Identification Based on Human Activity Recognition Using Wearable Sensors: An Experiment Using Deep Learning Models, *Electronics*, Vol. 10, No. 3 (online), 10.3390/electronics10030308 (2021).

[13] Garain, A., Dawn, R., Singh, S. and Chowdhury, C.: Differentially private human activity recognition for smartphone users, *Multimedia Tools and Applications*, Vol. 81 (online), 10.1007/s11042-022-13185-4 (2022).

[14] Gupta, P. and Arora, R.: Human activity recognition system using smartphone based on machine learning algorithms, Vol. 2555, p. 040010 (online), 10.1063/5.0110384 (2022).

[15] Garcia-Gonzalez, D., Rivero, D., Fernandez-Blanco, E. and Luaces, M. R.: A Public Domain Dataset for Real-Life Human Activity Recognition Using Smartphone Sensors, *Sensors*, Vol. 20, No. 8 (online), 10.3390/s20082200 (2020).