The Smartphone authentication using holding behavior

把持動作の特徴を用いたスマートフォン個人認証手法

浜崎 琢司*　小高 知宏*　黒岩 丈介**　白井 治彦*** 諏訪 いずみ**

The smartphone authentication using holding behavior

Takushi HAMASAKI*,　Tomohiro ODAKA*, Jousuke KUROIWA**, Haruhiko SHIRAI***
and Izumi SUWA **

(Received February 2, 2018)

In this study, the purpose is to establish an individual authentication system based on the smartphone holding behavior. We developped a system measured how one holds with the smart phone. Using this, we collected the smartphone holding data from 9 participants during operationg the specified application. The data was classified for each participant by machine learning, and calculated FRR (False Rejection Rate) and FAR (False Acceptance Rate). It found to be 0.130 and 0.106 on average. For some users, both FRR and FAR were less than 0.05. For this reason, we think this method is useful for some users

Key words : Smart Phone, Biometrics, Holding behavior

1. はじめに

現在，スマートフォンの総利用者数は若年層を中心に増加している．フィーチャーフォンと比較してタッチパネルが大きいため直感的な操作が容易であること，機能が充実していることなどが人気の理由として挙げられている．そのためスマートフォン上に重要なデータを保持していることが多く，一度紛失してしまうとデータが盗まれていた，という事例が少なくない．それを防ぐため，様々な認証方法でスマートフォンをロックしている．

どのスマートフォンでも用いられている認証方法として，PIN 認証やパターン認証が挙げられる．PIN 認証とは数字を 4 桁から 8 桁までをパスワードとして入力する認証方法で，パターン認証とは縦横 3 点の合計 9 点ををどのようになぞるかをパスワードとする認証方法である．どちらも簡単にパスワードを設定できるが PIN 認証は総当り攻撃に対して弱く，パターン認証はタッチスクリーン上の指紋の汚れや覗き見などでパスワードが推測されやすいという欠点も存在する．そのため所有者以外の人間には破られにくい認証方法についての研究が盛んに行われている．

その認証方法の一つに，バイオメトリクス認証を用いて所有者を確認する手法がある．バイオメトリクス認証とは人間が持っている身体的，または行動的特徴を用いた認証方法である．身体的特徴を用いたバイオメトリクス認証では，指紋や虹彩などその個人特有の身体的特徴を用いて認証を行う．特徴を計測するためのカメラやセンサをスマートフォンに搭載することで，スマートフォン上でも認証を行うことが可能となる．既に実用化されており高い認証精度を誇っているが，別途特別に機材が必要となりコストがかかるというデメリットも存在する．行動的特徴を用いたバイオメトリクス認証では，例えば筆跡や歩行時の姿勢など個人の行動や癖から特徴を抽出し，それらを元に認証を行う．行動や癖を特徴として用いるという特性上，認証を行った形跡が残らない，又は他人に認証動作を覚えられにくいというメリットがある．

* 大学院工学研究科 原子力・エネルギー安全工学専攻
** 大学院工学研究科 知能システム工学専攻
*** 工学部技術部
* Nuclear Power and Energy Safety Engineering Course, Graduate School of Engineering
** Human and Artificial Intelligence Systems Course, Graduate School of Engineering
*** Technical Division

スマートフォン上での行動的特徴を用いた認証システムの例として，タッチジェスチャーやフリック操作から個人を特定する研究が行われている [1][2][3][4]．同様に，タッチスクリーンを用いた入力自体にも個人による特徴が表れているという研究結果が報告されている [5][6]．これらはスマートフォンに備え付けられているタッチスクリーンや加速度センサなどから特徴量を取得しているため，追加で機材を必要としないが，まだ精度の面で向上の余地があると考えられる．

しかし，これらの認証は主にログイン時での使用を目的としたものが多く，仮に攻撃者に突破された際でも継続的に本人確認を行うような仕組みの認証システムがスマートフォン上で実装されている例は少ない．

本研究では，スマートフォンの持ち方がユーザによって異なることに着目し，それを行動的特徴として捉えた．ここで，ユーザによって異なるスマートフォンの持ち方をスマートフォン把持動作と呼称する．把持動作を用いて，スマートフォンのログイン認証を破られた後のことを念頭に置いた認証手法を提案する．

本研究のためにスマートフォン把持動作の特徴計測システムを加速度センサを用いて構築した．本システムは加速度センサをバックグラウンドで起動し，その間スマートフォンの加速度センサの値を記録し続ける機能を有する．それを用いることで，ユーザがスマートフォンを操作している間の把持動作を調査することができる．得られたデータを機械学習によってユーザ毎に分類し，それらを元に FAR / FRR 値を算出した．本研究の実験を通して，把持動作でユーザを分類することが可能なのか，他ユーザに攻撃された際に有効なのかどうかを検証する．

2. バイオメトリクス技術を用いた侵入検知システムの構築

本研究ではユーザのスマートフォン把持動作を用いて，スマートフォン操作中も連続的に認証を行うシステムを構築する．本手法で構築するシステムの概要図を図 1 に示す．本システムを構築するためには大きく分けて，スマートフォン把持動作を取得する処理と，得られた把持動作データを学習し，それを元に正規ユーザかどうかを識別する処理の 2 つが必要である．把持動作取得処理はスマートフォン上で行い，得られたデータを PC 側に送信することでオフラインで解析を行った．なお，得られたデータは k 近傍法を用いてユーザ分類を試みる．本章では計測に用いたシステムの概要とその設計について述べる．2.1 節では把持動作取得処理について，2.2 節では取得した把持動作データからユーザ分類を行う処理について述べる．

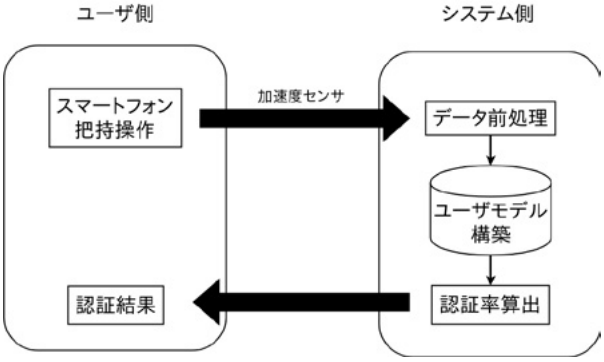

図 1 本手法の概要図

2.1 把持動作取得処理

把持動作を取得するためには様々な方法が考えられる．例えば，先行研究ではタッチスクリーンへの入力によって得られるタッチ位置やその圧力の大きさによって把持動作を判断している [6]．本研究ではユーザ毎の把持動作によって変化するスマートフォンの 3 軸方向の傾きを加速度センサで検出する．これは，歩行状態の検出等，ユーザの運動状態を検知するには有効な方法であることが理由である [7][8]．

また，ユーザがスマートフォンを把持している際，スマートフォンが受け取っている加速度を記録するためのアプリケーションが必要となる．計測を行う際は，なるべくユーザが操作に集中できるよう，使い慣れたアプリと併用して実験を行った方が良いと考えた．把持動作取得システムでは，他のアプリと併用して計測を行うことができるような機能があることが望ましい．つまり，バックグラウンドでも稼働する機能が必要である．以上より，把持動作取得処理には以下の 2 つの機能を搭載した．

- バックグラウンド稼働機能
- 加速度値記録機能

このアプリケーションは対象 OS を Android とし，開発言語は Java を用いている．

把持動作取得処理の概要を図 2 に示す．この処理では，ユーザが任意のアプリケーションを操作する際，バックグラウンドでユーザの把持動作の加速度データをテキスト形式で保存している．テキストは，x 軸方向の加速度，y 軸方向の加速度，z 軸方向の加速度，計測時間の順で毎行書き込まれる．この時の

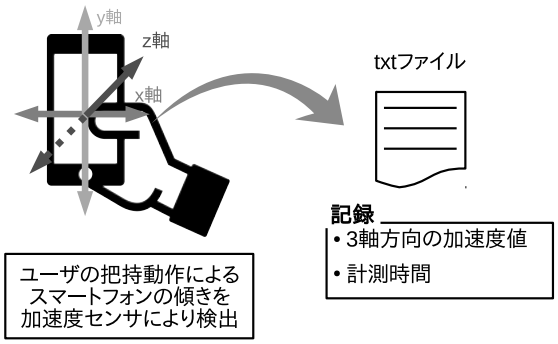

図 2 把持動作取得処理の概要

サンプリングレートは 50ms とした．処理が終わった後，PC 側に送信し，オフラインで解析する．

2.2 ユーザの認証方法

次に，得られた把持動作データを解析し，ユーザを正規ユーザかそうでないか分類する処理について述べる．先ほど取得したスマートフォン把持動作について，タッチを用いたスマートフォン個人認証だと「タッチ操作中」，筆跡認証だと「サイン中」が動作区間となるため，これらと比較すると動作区間が大きくなる可能性が非常に高い．また，スマートフォン把持動作はユーザや使用されるアプリケーションによって計測時間が左右される可能性が高い．そこで，安定しない計測時間の中からユーザの特徴を抽出できる解析手法が必要である．

本研究では，ユーザの特徴を解析する手法として機械学習を用いる．本研究では，正規ユーザの把持動作データを取得できる環境であるため，機械学習の一種である教師あり学習を用いる．そうすることによって，定式化できないユーザの把持動作の特徴を計算する．

教師あり学習の基本的な処理の流れをまとめると以下のようになっている．まず，取得した把持動作データの前処理を行う．続いて，選択したアルゴリズムを基に学習モデルを構築する．最後に，その学習モデルに検査データを与え，このモデルの評価を行う．以下でそれぞれの段階について順に説明する．

2.2.1 加速度データ前処理

この処理では，ユーザから取得した加速度データを加工し，機械学習のアルゴリズムを上手く動作させやすくする．まず，3 軸方向の加速度データと計測時間を記録したファイルから，計測時間を取り除く．そして，残った 3 軸加速度のデータの尺度を揃えるため，標準化を行う．標準化とは，各列のデータについて，平均値 $\mu = 0$，分散 $\sigma^2 = 1$ となるように変換する処理である．以下のような計算式 (1)，(2) で表される．

$$a^{std} = \frac{a-\mu}{\sigma} \quad (1)$$

$$\sigma = \sqrt{\frac{1}{n-1}\sum(a-\mu)^2} \quad (2)$$

計算式 (1)，(2) の a は各軸方向の加速度データ，μ はその平均，σ は標準偏差を表す．

この処理により，加速度の外れ値の検出も容易になる．また，標準偏差の商を取っているため，加速度データは無次元量となる．よって，平均値や単位の違うデータ同士でも比較することが可能になる．

2.2.2 分類アルゴリズムの選定

続いて，先ほど前処理したデータを学習するアルゴリズムを選定する．本研究の目標は，スマートフォンを使用しているユーザが正規か非正規かを分類することであるため，分類問題に適したアルゴリズムを選択する必要がある．

本研究では k 近傍法 (k-Nearest Neighbor algorithm) を用いてユーザの分類を行う．k 近傍法とは，検査データの近くにある訓練データを k 個取得し，その多数決により検査データのラベルを予測するというアルゴリズムである．アルゴリズムはシンプルだが，他の教師あり学習アルゴリズムと異なり，訓練データからパラメータを決定するような仕組みはなく，訓練データそのものを暗記する．訓練データをそのまま暗記するため，他のアルゴリズムと違って分類器のモデル構築に時間をかける必要がない．そのため、新しい訓練データにすぐに適応することができる．

このアルゴリズムを選んだ理由について，いくつか挙げられる．まず，本研究で扱う問題はスマートフォン把持動作によるユーザ分類であり，それを取得するために用いた特徴は 3 軸方向の加速度 (a_x, a_y, a_z) の 3 次元データである．このデータ量ならば，k 近傍法のようなシンプルなアルゴリズムでも良い分類結果が得られるだろうと判断したためである．また，先行研究が少ないため，スマートフォン把持動作を用いてユーザ分類を行った場合，どれほどの認証精度を記録するのかという指標となるようなデータが少なかった．そのため，他の複雑な分類アルゴリズムを用いた場合の認証精度ではなく，まずシンプルな分類ア

ルゴリズムを使用した場合の認証精度を把握する必要があったためである．

この際，ユークリッド距離と標準ユークリッド距離，マハラノビス距離を用いて訓練データと検査データの距離判定を行い，どれが良い精度を示すか比較する．用いた計算式はそれぞれ次の通りである．

$$De(x_{test}, x_{train}^{(i)}) = \sqrt{\sum (x_{test} - x_{train}^{(i)})^2} \quad (3)$$

$$Dse(x_{test}, x_{train}^{(i)}) = \sqrt{\sum \left(\frac{x_{test} - x_{train}^{(i)}}{\sigma_x} \right)^2} \quad (4)$$

$$D_m(x_{test}, x_{train}^{(i)}) = \sqrt{(x_{test} - x_{train}^{(i)})^T \Sigma_{(i)}^{-1} (x_{test} - x_{train}^{(i)})} \quad (5)$$

ここで，x_{test} は検査データの 3 軸加速度ベクトル，x_{train} は訓練データの 3 軸加速度ベクトル，i は各ユーザの番号を示す．また計算式 (5) の Σ^{-1} はユーザ i の加速度データで計算された逆共分散行列を示す．

ユークリッド距離は，普段，実生活上で距離を計測される時に用いられている距離測定法である．

標準ユークリッド距離は，その名の通りユークリッド距離を標準化したものである．標準ユークリッド距離とユークリッド距離との相違点は，各次元の差の累乗和の平方根をその分散で割る点である．この計算によって，各次元の単位を無視することができ，また各次元の尺度を揃える働きがある．

マハラノビス距離は，各次元のデータ同士に相関が見られる場合に用いられる．ユークリッド距離や標準ユークリッド距離との違いは，各次元のデータの分散を考慮できるという点である．ユークリッド距離ではどの特徴も均一な尺度で距離を計測するため，各次元の分散によって尺度を変更していない．標準ユークリッド距離では各次元毎に尺度を揃えているが，次元間での相関までは計算されていない．マハラノビス距離では，分散が小さい次元では距離が大きくなり，分散が大きい次元では距離が小さくなる．また，この時，逆共分散行列 Σ^{-1} が単位行列ならばユークリッド距離と等しくなり，対角成分以外を 0 にした場合，標準ユークリッド距離と等しくなる．これは対角成分に残っている数値は各次元データ毎の分散のみであり，各次元同士の共分散が 0 となるためである．

以上の距離測定法を用いて，出力された結果と付与されているラベルデータを比較することで，分類結果の正答率を調査できる．

2.2.3 k 分割交差検証法による学習モデル評価

教師あり学習の最後の段階として，構築した学習モデルの評価を行う必要がある．本研究の場合，学習モデルに対して未知のデータを与えた時，どれだけの精度でユーザを分類できるかを確認することで評価を行う．教師あり学習を用いて分類問題を解く場合，取得した訓練データ・検査データの分布が偏っていないか注意する必要がある．訓練データの分布が偏って居た場合，分類器そのものの性能が向上せず，検査データが偏っていた場合，正当な分類結果を示すことは難しい．また，訓練データを検査データとして使用しないように注意することも重要である．訓練データを検査データとして使用した場合もちろん正しく分類することが可能だが，未知のデータに対しても同じ結果であるのか分からない．つまり，実際使用した時の分類結果と違う精度を示す可能性がある．教師あり学習の評価段階では，未知のデータに対する分類性能を示すことが重要である．この未知データに対する分類性能のことを汎化性能と呼ぶ．また，学習データに対して過度に適応してしまい，未知データに対して性能が向上しないことを過学習と呼ぶ．

本研究では k 分割交差検証法 (k-fold cross-validation) と呼ばれる手法を用いて学習モデルの評価を行う．

k 分割交差検証法の手法について図 3 を用いて説明する．k 分割交差検証法では，まず取得したデータセットを k 個に分割する．なお，図の例では k=10 としている．次に，分割されたデータセットのうち，先頭のデータを検査データ，残りを訓練データという風に分別する．この訓練データを入力した分類器を用いて，検査データの分類結果 $result_1$ を算出する．続いて，先頭から 2 番目のデータを検査データ，残りを

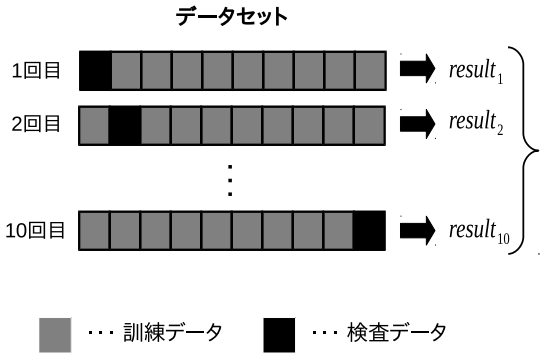

図 3 k 分割交差検証

訓練データとして，再び分類結果 $result_2$ を得る．これを末尾のデータまで k 回計算を繰り返す．今回の例では 10 回の計算になり，分類結果は $result_{10}$ の 10 個得られることになる．最後に，全ての分類結果の平均を算出することで，今回の分類結果の性能が示される．

k 分割交差検証法を用いるメリットとして，集められたデータが少数である場合でも全て有効に使うことができる点が挙げられる．k の値を大きくすることで，各検査データについて分類結果を算出するときの訓練データ数を増加させることができ，訓練データ不足による学習不足となる事態になりにくくなると考えられる．しかし，大きくし過ぎると，k 分割交差検証法による計算量が増大し，各訓練データセットも似通ってくるため，過学習に陥りやすくなる．データセットが大きい場合，k の値を小さくすることで分類器の学習と評価のための計算量を削減しつつ，学習モデルの平均性能を評価することが可能である．

以上のユーザ分類処理のための計算は Python を用いて処理する．Python は汎用のスプリクト言語の一種であり，数値解析や機械学習のライブラリが豊富に揃っているためデータサイエンスの分野でよく用いられている．本研究では，オープンソースの機械学習ライブラリである scikit-learn を用いてユーザ認証処理を実装している．それと同時に，数値計算ライブラリである Numpy と Scipy も使用している．

3. スマートフォン把持動作を用いた個人認証による実験

本章ではその提案手法を用いて実際にユーザの分類結果を算出し，本手法の精度の確認を行う．本実験では，提案手法による分類結果の汎化性能の確認や，スマートフォン上で使用するアプリの違いで把持動作に違いは表れるのか，表れるとしたらどのようになるのかを検証した．3.1 節では実験に用いた機材や実験を行う上での条件等を含めた実験環境について述べる．3.2 節では取得されるデータセットを用いた認証結果の算出方法について詳しく述べる．取得した把持動作データセットの扱いについては 3.3 節で述べる．

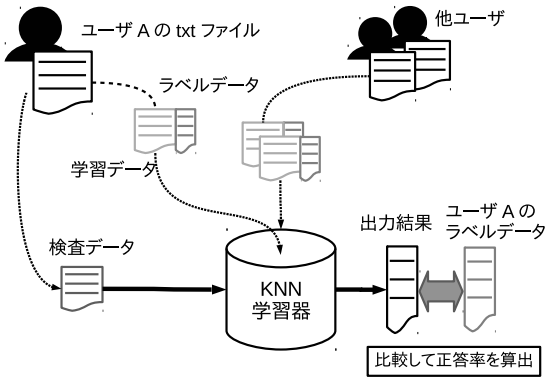

図 4 分類結果算出までの過程

3.1 本実験の評価方法

本実験では被験者は大学生 9 名で行い，全員スマートフォンを使用した経験があることを確認している．被験者には着席したままスマートフォンを縦向きに保持し指定したアプリケーションを 5 分間操作してもらい，その操作を 3 セットずつ行ってもらった．本実験ではアプリケーションとして，ブラウザとパズルゲームを選択した．なお，ブラウザでは閲覧するサイトによって把持動作が変化する可能性もあるため，全被験者に同じニュースサイトを閲覧してもらうよう指示している．計測されたデータは PC 側に送信され，k 近傍法により被験者毎の分類結果を算出した．

3.2 認証率の算出方法

本研究では k 近傍によるユーザの分類結果を FAR（False Acceptance Rate : 他人受入率），FRR（False Rejection Rate : 本人拒否率）を用いて評価する．FRR は正規ユーザであるにも関わらず認められない割合を表し，FAR は非正規ユーザを正規ユーザと認めてしまう割合を表す．どちらも誤った分類の比率を表しており，0 に近いほど精度が良いことを示す．ここで，分類結果を算出するまでの過程を図 4 に示す．各ユーザから得られた把持動作データを計算式 (1) を用いて標準化し，訓練データと検査データに分割する．全ユーザの訓練用データにユーザ毎に割り振られた固有の番号であるラベルデータを付与し，kNN 分類器に読み込ませることで学習を行う．最後に，学習させた kNN 分類器に検査データを読み込ませて，その検査データがどのユーザに最も近かったのかをユーザ番号で出力する．この際，ユークリッド距離と標準ユークリッド距離，マハラノビス距離をそれぞれ用いて訓練データと検査データの距離判定を行う．なお，用いるデータセットには前処理として計算式 (1) を用いた標準化に加え，前処理を行わない生データの 2 種類を使用する．従って，計 6 パターンの分類結果を示す，

FRR を算出するために，kNN 分類器に調査したいユーザの検査データを読み込ませ，そのユーザのラ

ベルデータと出力結果を比較し，その正答率を FRR として算出している．FAR は，同じく kNN 分類器に本人以外の全ユーザの検査データを読み込ませ，本人と間違った割合を FAR として算出する．

3.3 実験データセット

取得した把持動作データセットの作成方法について，図 5 に示す．まず，使用したアプリケーション毎に把持動作データは分けておく．初めに，1 セット目の把持動作データを検査データとして用いる時，他セットの把持動作データを訓練データとして使用する．続いて，各ユーザの認証率を算出する時，FRR をそのユーザの検査データ，FAR をそれ以外のユーザの検査データを用いる．なお，距離判定に用いる逆共分散行列はそのユーザから得られた訓練データから算出される．この操作を全ユーザに対して行う．これを 3 セット分繰り返し行うことで交差検証を行う．それぞれ算出された認証率の平均をグラフ化することで本手法の認証精度を図る．訓練データ数は，全被験者の 3 軸方向加速度データ計 108,000 個，検査データ数は，FRR 算出時は同データ 6,000 個，FAR 算出時は同データ 48,000 個を用いている．これは，サンプリングレート 50ms の加速度データが 5 分間分蓄積されたデータ量が 6,000 個であり，訓練データは 9 名の被験者のデータを 2 セット分，検査データは FRR 算出時では被験者 1 名のデータを 1 セット分，FAR 算出時は被験者 8 名のデータを 1 セット分使用されていることから導かれる．

4. 実験結果と考察

本手法において，それぞれのアプリケーションにおいて最も認証精度が良いものを図 6，図 7 に示す．

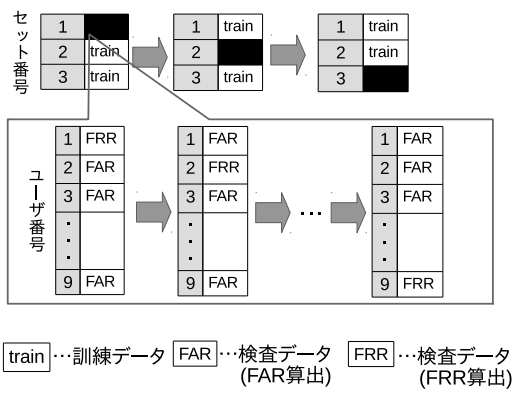

図 5 データセットの作成方法

各グラフの縦軸は FRR·FAR の認証率，横軸は k 近傍法のパラメータ k の値を示している．FRR·FAR のどちらも 0 に近いほど認証率が良いということを示す．なお，本実験の FRR·FAR はパラメータ k が 10，50，100，500，1000，5000，10000 の場合の認証率を算出している．実線が FRR，点線が FAR の値を示す．

本実験で最も良い分類結果を示したのは，ニュースサイト閲覧時は標準ユークリッド距離での距離判定 (図 6) であり，パラメータ k=10000 の時，FRR=0.130，FAR=0.106 であった．パズルゲーム時では，マハラノビス距離での距離判定 (図 7) であり，パラメータ k が 10000 の時，FRR=0.168，FAR=0.090 であった．全体の結果を見て，FRR が大きく FAR が小さいグラフが示されたことから，他人のなりすましには強いが本人拒否も起こりやすい認証システムであると言える．

2 つのアプリケーション間で全ユーザ平均の認証精度を比較すると，ニュース閲覧時の方が良い認証精度を示しているが，大きな差は見られなかった．ユーザ別に見ると，ニュース閲覧時は FAR=0.012，FRR=0.008，パズルゲーム時は FRR=0.080，FAR=0.007 を記録しているユーザが見られた．これは，パズルゲームでの操作方法では把持動作データの分散が大きくなる傾向にあり，そのため k 近傍法による分類が若干困難になったと考えられる．

どちらのアプリケーションを使用した実験，また距離判定方法の違いによらず共通していることは，生データのまま k 近傍法を試みても，特に全ユーザ平均の FRR が 0.5 以上となる結果が多く見られたことである．このことから，生データでの認証処理では認証精度が向上しないということが分かる．これは，使用している 3 軸の加速度データ (a_x, a_y, a_z) の各軸の特徴を抽出することができなかったためであると考える．例えば，被験者によって y 軸方向の加速度 a_y の平均値や標準偏差が異なっていることが分かっているが，標準化等の前処理を行っていないデータだとそれらの数値を抜き出すことができない．そのため，取得した加速度の値が単純に近かった被験者同士で誤認識しやすくなり，その結果認証率が向上しなかったと考えられる．

また，どちらのアプリケーション使用時でも，ユークリッド距離での距離判定を用いた場合，標準化を行ったデータセットでも認証率が向上しなかった．特に，計算式 (1) を用いたデータセットの場合の方が認証率が悪化していた．これは，他の距離判定方法では見られなかった傾向である．理由として，ユークリッド距離は本手法で取り上げた他の距離判定方法と異なり，各軸の特徴量に重み付けを行うような操作をせず

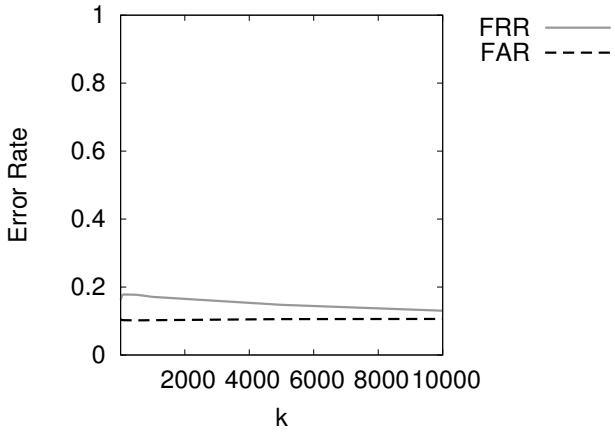

図 6 ニュース閲覧時の認証結果

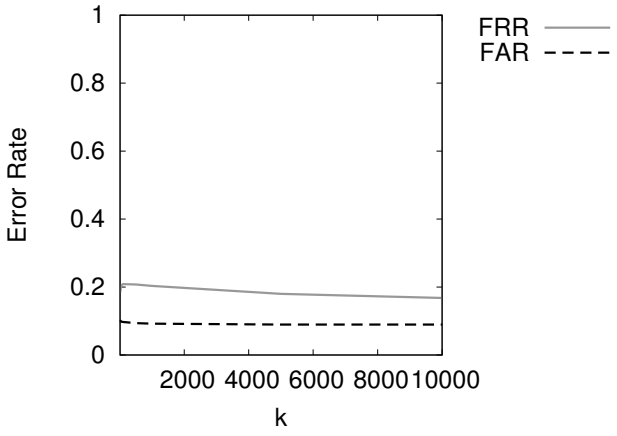

図 7 パズルゲーム時の認証結果

等しく距離計算を行っていることが挙げられる．計算式 (1) による標準化は，全ての特徴量を平均値 $\mu = 0$，分散 $\sigma^2 = 1$ に変換するため，見かけ上検査データの近傍に類似した訓練データが多数出現することになる．ユークリッド距離では，単純に近くの訓練データと同じラベルのユーザであると判断してしまうため，ユーザで異なる特徴量の標準偏差等を考慮できなかったことが原因であると考えられる．

それ以外の距離判定方法では，計算式 (1) を用いた標準化でのデータセットでの認証精度は大きく向上していた．マハラノビス距離と標準ユークリッド距離は，各特徴量の標準偏差，つまり各被験者の特徴量ごとのバラつきを考慮できるため，上手く分類することが可能であったと考えられる．

本実験前の予想では，マハラノビス距離の方が標準ユークリッド距離よりも良い結果を示すだろうと考えていた．これは，マハラノビス距離では各特徴量同士の共分散まで考慮することができ，これは標準ユークリッド距離ではここまで考慮されていないため，認証精度に差が出るであろうと考えたためである．しかし，結果としては予想通りマハラノビス距離の方が良い認証精度を示した実験もあったが，標準ユークリッド距離の方が良い結果を示した実験もあった．この 2 つの距離判定法について，マハラノビス距離の計算に用いられている共分散行列 Σ の非対角成分を 0 にしたものが標準ユークリッド距離の計算方法であるため，類似した計算を行っていると言える．本実験では，被験者はスマートフォンを縦向きに持ってもらうという条件で各アプリケーションを操作しているため，3 軸方向のうち標準偏差が大きくなる軸もあれば，小さくなる軸も見られる．そのため，共分散を計算しても距離判定に大きな影響を及ぼさない数値が算出されていることが原因に挙げられる．また，計算コストに関して，標準ユークリッド距離の方が計算コストが小さいため，よりリアルタイム性が必要になる場合は標準ユークリッド距離を選択する方が良いと考える．

本実験では被験者が椅子に座っているという状況下において，加速度センサを用いてスマートフォン把持動作を取得した場合の認証結果が得られた．このことから，スマートフォンが盗難されパスワード等のログイン認証を突破された際にも一定の効果があり，ユーザの行動的特徴も得られていると考えられる．スマートフォンを持つだけで行動的特徴を取得することのできる手軽さは長所であると考えられる．ただし，立ち状態や電車内での使用等，使用状況を固定しない場合では，加速度センサから得られる値は大きく変化し，認証精度が悪化することが予想される．今後は，把持動作からユーザの体勢や状態に左右されにくい特徴を抽出すること，もしくはそのような外乱に強い認証アルゴリズムを考案することが課題として挙げられる．

また，本手法ではバックグラウンドでスマートフォンの使用ユーザを監視できることから，他の認証システムとの組み合わせも容易である．このことから，複数の認証方法と組み合わせることで認証精度を向上させることができるのではないかと考える．

本手法の認証精度を改善するためには取得する特徴量を増加させることが考えられるが，それを行うことで計算コストが膨大になるというリスクもある．本手法で用いている k 近傍法でも，パラメータ k=1 ならば計算も時間はあまり掛からないが，良い認証

結果を示していた k=10000 の時その何倍もの計算時間を要した．マハラノビス距離や標準ユークリッド距離でもユークリッド距離での距離判定時と比べて計算コストが増大するため，比較的計算に時間を要するという問題があった．そこで，学習モデル構築に時間を要するが計算コストの少ない SVM や線形判別等の教師ありアルゴリズムでの認証システムを試すことが改善案として考えられる．

5. まとめ

本研究ではスマートフォン把持動作を用いて継続的に本人認証を行うシステムの手法を提案した．加速度センサから把持動作を取得し，それを k 近傍法によりユーザ識別を行うことで，本手法の精度を確認した．実験結果は，最も良い精度を記録したのはニュース閲覧時で FRR=0.130，FAR=0.106，パズルゲーム時で FRR=0.168，FAR=0.090 であった．結果をユーザ別に見ると，FAR，FRR 共に 0.05 以下となるユーザが存在したことから，本手法は一部ユーザに有用であったと考えられる．

2 つのアプリケーション間で全ユーザ平均の認証精度を比較すると大きな差は見られなかったがユーザ別に見ると，ニュース閲覧時は FAR=0.012，FRR=0.008，パズルゲーム時は FRR=0.080，FAR=0.007 を記録しているユーザが見られた．これは，パズルゲームでの操作方法では把持動作データの分散が大きくなる傾向にあり，そのため k 近傍法による分類が若干困難になったと考えられる．

また，実験結果から，データ前処理を行った方が認証精度が向上する傾向にあることが示された．同様に，ユークリッド距離を用いた場合よりも，標準ユークリッド距離やマハラノビス距離を用いた場合の方がユーザ分類の精度が高かった．理由として，ユークリッド距離は本手法で取り上げた他の距離判定方法と異なり，各軸の特徴量に重み付けを行うような操作をせず等しく距離計算を行っていることが挙げられる．マハラノビス距離と標準ユークリッド距離は，各特徴量の標準偏差，つまり各被験者の特徴量ごとのバラつきを考慮できるため，上手く分類することが可能であったと考えられる．

今後の改善策として，取得する特徴量を増やすことで認証精度向上を図ることや計算コストの削減等が挙げられる．

参考文献

[1] 山田健一朗 , 納富一宏 , 斎藤恵一 . スマートフォン操作時における行動的特徴量を利用した個人識別手法. バイオメディカル・ファジィ・システム学会誌 , Vol. 16, No. 1, pp. 4148, 2014.

[2] 渡邊裕司 , 市川俊太ほか . スマートフォンにおけるタッチ操作の特徴を用いた継続的な個人識別システムの検討 . コンピュータセキュリティシンポジウム 2012 論文集 , Vol. 2012, No. 3, pp. 797804, 2012.

[3] Tao Feng, Jun Yang, Zhixian Yan, Emmanuel Munguia Tapia, and Weidong Shi. Tips: Context-aware implicit user identification using touch screen in uncontrolled environments. In Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, p. 9. ACM, 2014.

[4] 渡邊裕司:スマートフォンにおけるタッチ操作の特徴による個人認証, 高精度化する個人認証技術, 株式会社エヌ・ティー・エス, pp. 193200 (2014).

[5] Kolly, S. M., Wattenhofer, R. and Welten, S.: A personal touch: Recognizing users based on touch screen behavior, Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones, ACM, p. 1 (2012).

[6] Goel, M., Wobbrock, J. and Patel, S.: GripSense: using built-in sensors to detect hand posture and pressure on commodity mobile phones, Proceedings of the 25th annual ACM symposium on User interface software and technology, ACM, pp. 545554 (2012).

[7] 彭龍, 渡邊裕司ほか:スマートフォンの加速度センサを用いた歩行時の認証に関する一考察, コンピュータセキュリティシンポジウム 2013 論文集, Vol. 2013, No. 4,

[8] 倉沢央 , 川原圭博 , 森川博之 , 青山友紀ほか . センサ装着場所を考慮した 3 軸加速度センサを用いた姿勢推定手法 . 情報処理学会研究報告ユビキタスコンピューティングシステム (UBI), Vol. 2006, No. 54 (2006-UBI-011),pp. 1522, 2006.