情報処理学会論文誌 Vol.62 No.12 2011–2023 (Dec. 2021)

# スマートロックにおける2端末による機械学習を用いた歩行認証に関する研究

朴 美娘[1,a)] 渡辺 一樹[1] 油田 健太郎[2] 岡崎 直宣[2]

受付日 2021年3月8日, 採録日 2021年9月9日

**概要**：電子的に鍵の開閉を行うスマートロックの認証方式として，従来の所持認証方式では通常の鍵と同様に紛失や盗難の危険性があり，指紋認証方式ではドアの前で数秒間立ち止まる必要がある．そこで，本研究ではスマートフォンとウェアラブル端末の 2 つの端末の合成加速度による歩行認証を提案する．歩行距離の差による影響の少ない 19 個の特徴量を抽出し，代表的な機械学習アルゴリズムを用いて他人受入れ率（FAR）および本人拒否率（FRR）の観点から認証精度を比較した．その結果，最も良かった認証精度は機械学習アルゴリズムに Isolation Forest を用いた場合の FAR が 8.3%，FRR が 9.5%であった．次に，継続的な歩行認証の評価のため日にちを空け定期的に歩行実験を行った．その結果，FAR が 18.6%，FRR が 13.8%という認証精度となった．さらに，様々な歩行速度での認証精度の確認を行うため，早歩き，普段歩き，遅歩きの 3 つの速さを学習させ，FAR が 18.8%で FRR が 15.0%という結果となった．また，被験者ごとの認証精度や機械学習アルゴリズムごとの認証精度を分析することで，同じ被験者でも認証精度が良くなる識別器が異なることが確認できた．

**キーワード**：スマートロック，歩行認証，加速度センサ，機械学習

# A Study of Gait-based Authentication by Using Two Devices in Smart Lock

Mirang Park[1,a)] Kazuki Watanabe[1] Kentaro Aburada[2] Naonobu Okazaki[2]

Received: March 8, 2021, Accepted: September 9, 2021

***Abstract:*** As an authentication method for smart locks, the conventional possession authentication method poses the risk of loss or theft, while the fingerprint authentication method requires the user to stand still in front of the door for several seconds. In this paper, we propose a gait-based authentication system based on the acceleration of two devices: a smartphone and a wearable device. The proposed gait-based authentication method extracts 19 features and calculates the authentication rate, that is, the false acceptance rate (FAR) and the false rejection rate (FRR), using some typical machine learning algorithms. As a result, when using Isolation Forest algorithm, FAR and FRR are 8.3% and 9.5%, respectively. Next, in order to evaluate of the continuous gait-based authentication, we conducted walking experiments periodically on different days. In this case, FAR and FRR are 18.6% and 13.8%, respectively. Furthermore, in order to check the authentication rate at various walking speeds, we trained three speeds: fast, normal, and slow. As a result, FAR is 18.8% and FRR is 15.0%. We found that the better algorithm of anomaly detection of FAR and FRR is different depending on the subjects.

***Keywords:*** smart lock, gait-based authentication, accelerometers, machine learning

## 1. はじめに

近年，様々なモノがインターネットにつながる IoT（Internet of Things）機器の開発がさかんに進んでいる．たとえば，インターネットとつながる自動車やインターネットとつながる AI スピーカ等，多くの IoT 機器が開発されている．このような IoT 機器は年々増加傾向にあり，情報通信白書 [1] によると 2022 年には約 348 億台にも増加すると予測されている．その IoT 機器の中に，電子的に個人の認証を行い家のドア等の鍵の開閉を行うスマートロックと

[1] 神奈川工科大学
Kanagawa Institute of Technology, Atsugi, Kanagawa 243–0292, Japan
[2] 宮崎大学
University of Miyazaki, Miyazaki 889–2192, Japan
[a)] mirang@nw.kanagawa-it.ac.jp

呼ばれる製品がある．2015 年はスマートロック元年といわれ，現在までに，Qrio [2] や Akerun [3]，August [4] 等，様々なスマートロック製品が開発されている．しかし，スマートロックにおける個人認証方式として，従来のパスワード方式ではパスワードが推測されやすくユーザに記憶負荷がかかるという問題点や，毎回記憶したパスワードを端末に入力する必要があり日常的に使う鍵の開閉を行うための個人認証方式としては煩わしさが残る．また，IC チップの埋め込まれたカードや事前に認証を済ませた端末等を持ち歩くことで認証を行う所持認証と呼ばれる方式があるが，スマートロックにおける所持認証方式では，従来の鍵と同様に紛失や盗難等の危険性が課題としてあげられる．これらの課題点を解消する方式として人間の身体的特徴を用いて認証を行う生体認証方式がある．しかし，スマートロックにおける生体認証方式として，たとえば指紋認証方式では，家の前で数秒間立ち止まらなくてはならず，手袋をつけていればそれを外す必要がある．また，顔認証方式においてもドアの前で数秒間立ち止まる必要があり，マスクや帽子等を身に付けていればそれらを外さなくてはならないという煩わしさがある．

以上のように，スマートロックにおける認証の煩わしさを完全に排除できていない現状がある．そこで，本論文ではユーザの行動から得られる行動的特徴を用いた歩行認証に着目した．歩行認証とは，歩行時の加速度データや角速度データ等から行動的特徴を抽出し認証を行う生体認証方式の 1 つであり，日常的に行われる歩行を用いることでユーザが意識することなく認証を行うことができる利便性があると考えられる．しかし，行動的特徴を用いる認証方式では，本人の行動をつねに再現することが難しく認証精度に大きな課題がある．これまでも歩行認証は認証精度向上のため多くの研究が行われている [5], [6], [7], [8]．これらの研究では，機械学習や複数のセンサを用いることで認証精度の向上のための研究を行っている．しかし，認証の際に端末の向きを同じにしなくてはならないという煩わしさや，複数の同一センサを身につける必要がある等の課題点がある．

また，行動的特徴を用いる認証方式には行動を他人に真似され不正なユーザに認証されてしまうという問題点がある．この問題点に対して Muaaz ら [9] は，スマートフォンから取得した加速度データを基に歩行認証を行い，なりすまし攻撃に対して有効か確認を行っている．実験では，他人になりきり演技をすることを専門としている，俳優学校の学生に攻撃者として登録者の歩行を真似してもらい，認証が成功してしまうか実験を行っている．結果として，ほとんどの場合に攻撃者は認証を成功させることができず歩行認証がなりすまし攻撃に対して有効であることを示している．

そこで我々は，近年開発が進んでいるウェアラブル端末に着目した．ウェアラブル端末とは普段から身につける時計や眼鏡等の形をしたデバイスであり，主にヘルスケアやスマートフォンの補助デバイスとして開発が進んでいる．このウェアラブル端末は，年々増加傾向にあり Gartner [10] によると 2022 年には，約 4 億 5,300 万台にも増加すると予測され，将来多くの人が体にウェアラブル端末を身につけることが予測される．そこで本研究では，ユーザになるべく負荷がかからないようウェアラブル端末とスマートフォンの 2 つの端末を用いた歩行認証システムモデルを提案し，認証精度の評価を行うことを目的とする．提案する方式では，それぞれの端末から取得される加速度データから極大値間隔や 2 つの端末の類似度等の特徴量を計算し機械学習を用いて認証を行う．機械学習には，GMM（Gaussian mixture model：ガウシアン混合モデル）や Isolation Forest，Elliptic Envelope，KDE（Kernel Density Estimation），LOF（Local Outlier Factor），One Class SVM（Support Vector Machine）の異常検知モデルを用いる．

以降，2 章では，歩行認証についての関連研究について示す．3 章では，スマートロックを想定した 2 つの端末を用いた歩行認証の提案システムモデルについて示す．また，認証に用いる加速度データの処理や特徴量の抽出について述べる．4 章では，提案方式の実装・実験について述べる．5 章では，異常検知アルゴリズムを用いた提案方式の評価と実験結果から考えられる認証精度について考察を行う．最後に 6 章では，まとめと今後の課題を示す．

## 2. 関連研究

### 2.1 スマートフォンの加速度センサを用いた歩行認証

彭ら [5] は，スマートフォンの加速度データをもとに，$x$，$y$，$z$ の 3 軸加速度データからそれぞれ平均値（3 軸），標準偏差（3 軸），平均絶対偏差（3 軸），平均合成加速度，ピーク間の時間（3 軸），ビン分布（3 軸 $\times$ 10 個）の合計 43 個の特徴量を抽出し機械学習を用いて分類を行っている．機械学習にはデータマイニングソフトである WEKA を用い，正解率の確認を行っている．また，特徴量ごとの正解率を確認し認証に貢献する特徴量や貢献しない特徴量について確認を行っている．結果として，機械学習の分類アルゴリズムに決定木 J48 を用いた場合は他人受入れ率（FAR）が 0.6%，本人拒否率（FRR）が 8.7%であり，分類アルゴリズムにニューラルネットワーク（Neural Network）等を用いた場合は FAR が 0.3%，FRR が 3.8%であった．また，認証に貢献する特徴量としては平均値をあげ，認証に貢献しない特徴量としては平均合成加速度やピーク間の時間をあげている．しかし，この研究では 3 軸加速度データをそれぞれ用いた特徴量の抽出を行っているため，端末の向きを考慮しなくてはならないという問題点がある．

### 2.2 加速度センサおよび角速度センサを用いた歩行認証

今野ら [6] は，スマートフォンに搭載された加速度センサと角速度センサの 2 つのセンサを用いた歩行認証を提案しその識別率を示している．認証システムへ入力されたセンサのデータと，事前に登録されたデータとの距離を計算し，その距離を基に機械学習でユーザの識別を行っている．まず，予備実験を行いフィルタの最適な点数と，各センサの振幅正規化方法および，距離計算方法を決定し，そのうえで 50 名の被験者に約 70 秒間歩行してもらい取得したデータを基に認証精度の確認を行っていた．ここでは機械学習の SVM（Support Vector Machine）を用いることで評価を行い，結果として EER（Equal Error Rate）が 0.8%となった．

この研究では，端末の向きを同じにしなくてはならないという問題や同じズボンを着用した条件下での実験であったため，実際の環境を想定した歩行認証を課題としてあげている．

### 2.3 3 軸加速度センサを用いた歩行者推定

岩本ら [7] は，携帯電話の 3 軸加速度センサを用いて，ユーザの状態推定（静止状態，歩行状態，走行状態）と，端末の所持位置の推定（前ポケット，後ろポケット，胸ポケット，端末の画面を見る，腕を振る）を行ったうえで，ユーザの推定を行う歩行認証のモデルを提案している．ここで，ユーザの状態推定では最大値や最小値，高速フーリエ変換（FFT）したスペクトルの特徴量を用い，携帯電話の所持位置推定には最大値や最小値，軸ごとの平均値，変化量を特徴量に用いている．さらに，ユーザの推定ではそれぞれの携帯電話の所持位置推定に合わせた特徴量を用い認証を行っている．実験として被験者 5 名に対して実験を行い，結果としてユーザの状態推定に関しては 99.7%，端末の所持位置推定については 93.1%と高い識別率を得ることができ，ユーザの推定に関しては 95.8%となっている．しかし，一般的にユーザの状態と端末の所持位置が変わる場合のユーザの推定に関しては実験が実施されず，課題があると考えられる．

### 2.4 複数の加速度センサを使用した歩行認証

Mondal ら [8] は，体の関節 8 カ所（右肩，左肩，右腕，左腕，右腰，左腰，右足，左足）にそれぞれ角度センサを装着し歩行認証を行っている．実験では，被験者 30 名に歩行してもらうことでその認証精度を示している．結果として，体の 8 カ所に装着された角度センサから得られる信号を計測し，識別器にニューラルネットワーク等を用い，100%の精度で識別を行っている．しかし，体に大量のセンサを装着するため，ユーザにとって望ましい認証方式とはいえない．

### 2.5 2 つの端末を用いた歩行認証

以前我々は，2 つの端末の合成加速度を用いて歩行認証を行う方式の提案を行った [11], [12], [13]．この研究では，2 つの端末から取得した加速度を用いて合成加速度を計算し，平均値や極大値間隔等の 31 個の特徴量を抽出する．評価には機械学習の教師あり学習の識別を用いてユーザの識別率の確認を行った．実験では，15 名の学生の左腕にスマートウォッチ，右ポケットにスマートフォンを入れた状態で 10 m の廊下を歩行しユーザの分類を行った．また，提案した 2 つの端末を用いた場合の識別率の評価を行った．結果として，機械学習に Random Forest を用いた場合は 95.3%であった．この結果から，1 つの端末を用いた場合より 2 つの端末を用いた場合の方が，識別率が上がることを示した．しかし，評価に用いた機械学習の教師あり学習分類では，登録ユーザ以外のデータが入力された場合でも登録ユーザのいずれかに分類されてしまうため，未知のデータに対して有効とはいえない．

## 3. 提案方式

本研究では，加速度センサを搭載した 2 つの端末を用いた歩行認証システムモデルの提案と評価を行う．提案システムモデルでは，事前に登録した端末の ID による所持認証を行うことで歩行認証の認証精度の課題を解消することを目的とする．加速度センサの計測では，iBeacon による近接検知を行うことによって加速度データの取得開始・終了の判定を行う．また，2 つの端末から取得した加速度データから極大値間隔や 2 つの端末の類似度等の特徴量を抽出することで，学習器を作成しスマートロックの認証を行う．学習器には，機械学習の異常検知モデルを用い，本人のデータのみを学習させ，正常データの場合は鍵を開錠し，異常データの場合は施錠することで認証を行う．

### 3.1 システムモデル

提案システムモデルは，加速度センサが搭載された 2 つの端末，加速度データを受信しユーザの認証を行うスマートロックで構成される．提案システムモデルを**図 1** に示す．スマートロックと 2 つの端末の通信方式には Bluetooth を用い，iBeacon によりスマートロックと 2 つの端末との近接検知を行う．iBeacon では Immediate（約 2 cm 未満），Near（約 2 cm〜1 m），Far（約 1 m〜約 50 m）の 3 つの近接検知を行うことができ，本提案システムモデルでは Near と Far の 2 つの近接検知を用いて加速度データの計測を行う．

2 つの端末は，以下の手順で認証を行う．

(1) iBeacon の Far 検知
(2) 事前登録した 2 つの端末の ID 送信
(3) スマートロック内で 2 つの端末の ID 確認
(4) 2 つの端末での加速度データの計測開始

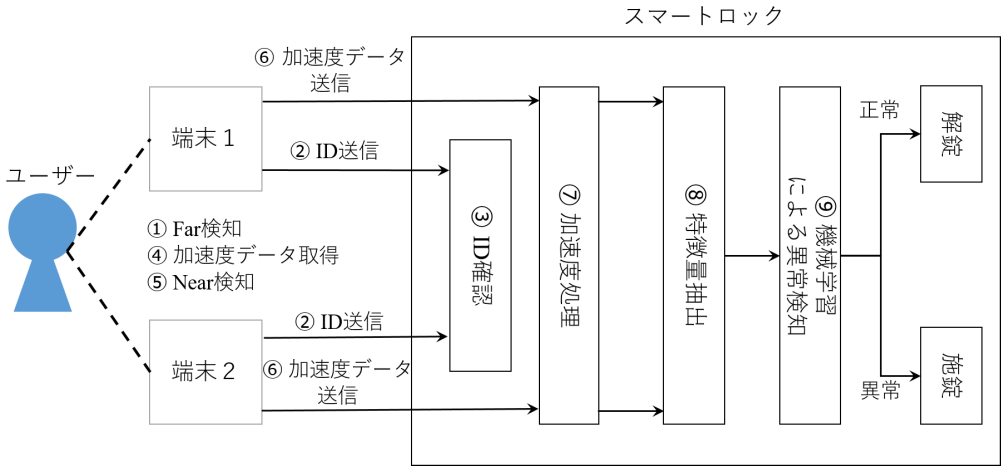


**図 1** 提案システムモデル
**Fig. 1** Proposed system model.

(5) iBeacon の Near 検知
(6) 計測した加速度データをスマートロックへ送信
(7) スマートロック内で受信した 2 つの端末の加速度データを処理
(8) 加速度データから特徴量抽出
(9) 機械学習による異常検知を行い正常データなら解錠，異常データなら施錠

認証では，まずスマートロックと端末の近接検知を行い Far が検知された場合に，2 つの端末は ID をスマートロックへ送信する．ID を受信したスマートロックは ID の確認を行い，その端末 ID を用いて所持認証を行う．次に 2 つの端末の加速度データを計測し，iBeacon で Near を検知した場合に，スマートロックへ加速度データを送信し加速度処理を行う．その後，2 つの端末の加速度データから特徴量を抽出する．ここで，通信の遅延や端末の近接検知の精度差などから加速度データを取得する時間や歩行距離が異なることが予測されるため，特徴量にはそれらの影響が少ない平均値や極大値間隔などの特徴量を抽出する．特徴量を抽出した後，機械学習の異常検知を行い，異常データを検知することで本人か判定し認証を行う．

### 3.2 ID 確認

提案システムモデルでは，歩行認証の認証精度の課題を解消するため，2 つの端末に ID を付与し，所持認証を行う．歩行認証を行う前に，端末の ID による所持認証を行うことで登録された端末を持っていないユーザの認証を受け付けず，他人に認証されるリスクの低減が期待できる．ここで，1 つの端末だけでなく 2 つの端末から ID を確認することで，たとえば 1 つの端末が盗難された場合でももう 1 つの端末を持っていない限り認証を行うことができない．そのため，同時に 2 つの端末が盗難にあわない限り認証が行われることがないため盗難における鍵の開錠のリスクを減らすことができる．本提案システムモデルの ID 確認では，事前に端末 1，端末 2 にそれぞれ ID を付与し，ID を事前にスマートロックに登録しておく．認証の際に，2 つの端末から暗号化した ID をスマートロックに送信し，ID を受け取ったスマートロックはそれぞれの ID を確認し認証を行う．

### 3.3 加速度処理

本節では，ユーザの特徴量を抽出するため 2 つの端末の加速度センサから計測される加速度データの処理について述べる．本研究では，端末の向きを考慮せずに歩行認証を行うため合成加速度を用いる．ここで，2 つの端末の合成加速度 $r_i^1$，$r_i^2$ を以下の式で示す．なお，取得した $x$，$y$，$z$ 軸の加速度データを端末 1 では $x_i^1$，$y_i^1$，$z_i^1$ と表し，端末 2 では $x_i^2$，$y_i^2$，$z_i^2$ で表す．

$$r_i^1 = \sqrt{(x_i^1)^2 + (y_i^1)^2 + (z_i^1)^2} \tag{1}$$

$$r_i^2 = \sqrt{(x_i^2)^2 + (y_i^2)^2 + (z_i^2)^2} \tag{2}$$

端末 1 と端末 2 の加速度データの計測開始から $i$ 番目にデータを取得した時刻を $t_i^1$，$t_i^2$ とし，計測開始から計測終了までに取得したデータ数を $n_1$，$n_2$ で表すと，端末 1 と端末 2 から取得した合成加速度データの集合 $d_1$，$d_2$ は次のようになる．

$$d_1 = \left\{(t_i^1, r_i^1) | i \in \{1, \ldots, n_1\}\right\} \tag{3}$$

$$d_2 = \left\{(t_i^2, r_i^2) | i \in \{1, \ldots, n_2\}\right\} \tag{4}$$

加速度センサから得られた $x$，$y$，$z$ それぞれの加速度データから式 (1)，(2) で合成加速度を算出する．算出した 2 つの合成加速度データの例を**図 2** に示す．ここで，2 つの端末の性能差や計測時間の違いからサンプル数が異なることが確認できる．そこで，2 つのデータを比較するため 2 つの端末のサンプル数を合わせる．その方式として，2 つの端末の加速度データを取得した時刻差からサンプル数を合

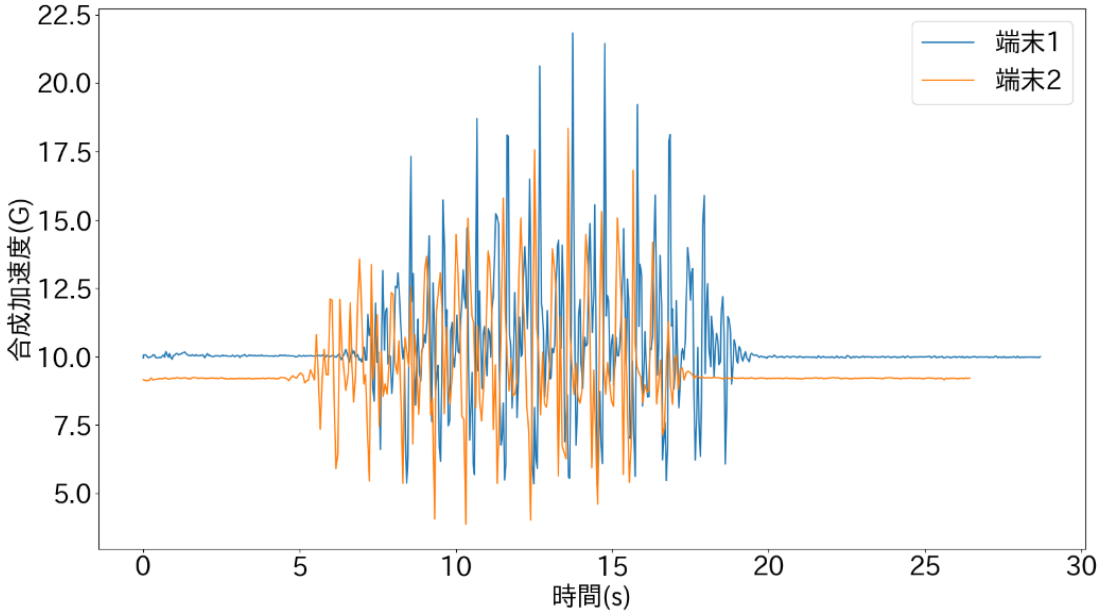


図 2 2 つの端末の合成加速度
**Fig. 2** Composite acceleration of two devices.

わせる．たとえば，2 つのサンプル数の大小関係が $n_1 > n_2$ であった場合の，サンプル数を合わせたときのデータの集合を $d'_1$，$d'_2$ で表すと次のようになる．

$$d'_1 = \left\{(t'^1_i, r'^1_i) | i \in \{1, \ldots, n_1\}\right\} \tag{5}$$

$$d'_2 = \left\{(t'^2_i, r'^2_i) | i \in \{1, \ldots, n_2\}\right\} \tag{6}$$

ここで，$t'^1_i$，$r'^1_i$，$t'^2_i$，$r'^2_i$ は以下の式で計算される．

$$t'^1_i = t^1_{\underset{j \in \{1,\ldots,n_1\}}{\arg\min}\ (|t^1_j - t^2_i|)} \tag{7}$$

$$r'^1_i = r^1_{\underset{j \in \{1,\ldots,n_1\}}{\arg\min}\ (|t^1_j - t^2_i|)} \tag{8}$$

$$t'^2_i = t^2_i \tag{9}$$

$$r'^2_i = r^2_i \tag{10}$$

また，停止状態では加速度データのばらつきが少なく，歩行状態ではデータのばらつきが多いため，一定区間の加速度データの標準偏差が高い位置を探し，その区間を歩行状態とする．具体的には，一定区間の区間幅を $p$，歩行状態を判断する加速度データの標準偏差の閾値を $\sigma_w$ とするとき，区間 $i \sim i+p-1$ の加速度データの標準偏差 $\sigma_i$ が式 (11) を満たすとき，$i \sim i+p-1$ 番目のデータを歩行状態とする．ここで，$p$ および $\sigma_w$ の値は，実験で得られたデータから上記の式で歩行状態を判定するのに適した値を選び，本実験では $p = 15$ および $\sigma_w = 0.05$ とした．

$$\sigma_i = \sqrt{\frac{1}{p}\sum_{k=i}^{i+p-1}(x_k - \bar{x})^2} \geq \sigma_w \tag{11}$$

その後，ローパスフィルタで加速度データのノイズの除去を行う．**図 3** に上記の加速度データ処理を行った後の波形を示す．ここで，加速度データ処理を行うことでサンプル数の差を解消することができ，歩行状態の加速度データを抽出されたことが確認できる．

### 3.4 特徴量抽出

機械学習を用いた歩行認証を行うため，2 つの端末の歩行区間全体（歩行状態）から得られる加速度データをもとに特徴量の抽出を行う．特徴量抽出には 2 つの端末の標準偏差が高い区間の合成加速度の特徴量の差や 2 つの端末の加速度データの類似度などを用い，1 つの端末だけでは取得できない特徴量の抽出も行う．

まず，各端末からは次の特徴量を抽出する．

- 平均値
- 標準偏差
- 最大値
- 最小値
- 極大値間隔の中央値
- 極小値間隔の中央値

次に，各端末から取得した特徴量から以下に示す特徴量を導出する．

- 2 つの端末の平均値の差
- 2 つの端末の標準偏差の差
- 2 つの端末の最大値の差
- 2 つの端末の最小値の差
- 類似度（SSD：Sum of Squared Difference）

$$SSD = \min_{k \in \{1,\ldots,\frac{2}{3}n\}} \frac{1}{n-k}\sum_{i=1}^{n-k}\left(r'^1_i - r'^2_{i+k}\right)^2 \tag{12}$$

- 類似度（NCC：Normalized Cross Correlation）

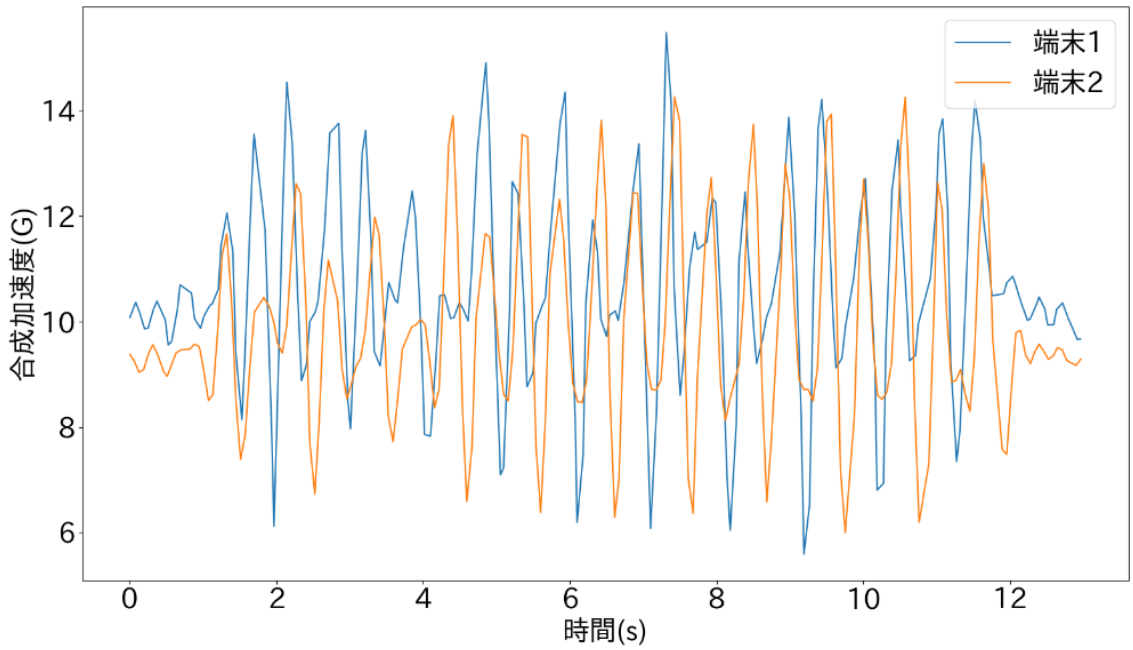


図 3 加速度処理を行った後の 2 つの端末の合成加速度
**Fig. 3** Composite acceleration after acceleration processing.

$$NCC = \max_{\{k\in 1,\ldots,\frac{2}{3}n\}} \frac{\sqrt{\sum_{i=1}^{n-k} r_i'^1 r_{i+k}'^2}}{\sqrt{\sum_{i=1}^{n-k}(r_i'^1)^2}\sqrt{\sum_{i=1}^{n-k}(r_{i+k}'^2)^2}} \tag{13}$$

- 類似度（DTW：Dynamic Time Warping）

$$DTW = f(n,n)$$
$$f(i,j) = \left|r_i'^1 - r_j'^2\right| + \min\begin{cases} f(i-1,j-1) \\ f(i-1,j) \\ f(i,j-1) \end{cases} \tag{14}$$

なお，サンプル数を $n$ とし，$i,j \in \{1,\ldots,n\}$ とする．また，SSD と NCC の類似度算出に関して 2 つの端末の動かし方が似ているかを特徴とするため，2 つの加速度データを時間軸方向にずらしたときの最も高い類似度を特徴量とする．ここで，2 つの端末の合成加速度の類似度を比較するサンプル数を確保するため，ずらす個数を $k \in \left\{1,\ldots,\frac{2}{3}n\right\}$ とする．本提案では上記の特徴量を用い機械学習の異常検知を用いて本人か他人かを検知し認証を行う．

## 4. 実装と実験

### 4.1 実装

本節では提案方式の評価実験を行うため，スマートフォンやスマートウォッチ，機械学習等の実装について述べる．

#### 4.1.1 加速度を取得する端末

提案システムモデルの加速度データを取得する端末として，端末 1 にスマートフォン Sony Xperia XZs を用い，端末 2 にウェアラブル端末 Sony SmartWatch3 を用い実装を行う．それぞれの端末のアンドロイドシステムから加速度センサのデータを取得するためのプログラムを JAVA で作成する．また，スマートロックの代わりに Linux OS をインストールしたパソコンをサーバとして用意し，各端末から加速度データを取得するため加速度の開始および終了命令を送信するためのプログラムを実装する．

#### 4.1.2 機械学習

サーバの加速度を取得するためのプログラムによって，取得された加速度データを用いて機械学習による評価を行う．実装したプログラムでは，まずより良い特徴量選択を行うため，すべての特徴量の組合せに対して認証精度（FAR および FRR）を計算し，それぞれの機械学習モデルに適した特徴量の選択（以降 Exhaustive Feature Selection という）を行う．次に，選択された特徴量を用いて，機械学習モデルを作成しそれぞれの機械学習のパラメータの調整や異常度を算出しその異常度の閾値を調整することで認証精度を計算し，最適なパラメータおよび閾値を決定する．機械学習には Python モジュールの scikit-learn [16] を用い，異常検知アルゴリズムとして，Elliptic Envelope，GMM，Isolation Forest，KDE，LOF，One Class SVM を用いそれぞれの認証精度を計算し評価を行う．

認証精度に関しては，FAR と FRR の 2 つの観点から評価する．その算出方法は次のようになる．

$$\text{FAR} = \frac{\text{他人が誤って本人として識別された回数}}{\text{他人による試行回数}}$$
$$\text{FRR} = \frac{\text{本人が誤って他人として識別された回数}}{\text{本人による試行回数}}$$

### 4.2 実験

提案方式の識別率と認証精度を評価するための実験を行

表 1 実験で使用した機器
**Table 1** Experimental equipment specifications.

| システム構成 | 使用機器 | OS | サイズ |
|---|---|---|---|
| 端末 1（スマートフォン） | Sony XperiaXZs | Android | 51mm×36mm |
| 端末 2（スマートロック） | Sony SmartWatch3 | Android | 146mm×72mm |
| スマートロック（サーバ） | ASUS X200M | Ubuntu | |

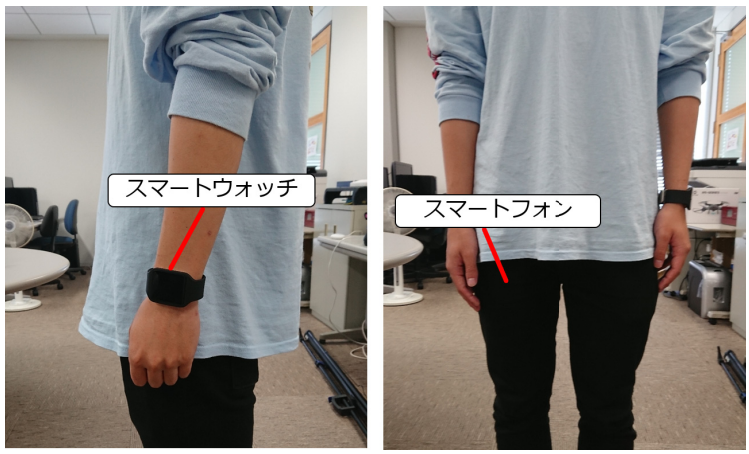


図 4 2 つの端末の所持位置
**Fig. 4** Experiment conditions.

う．実験の目的は，次のようになる．

- 2 つの端末を用いた場合の識別率を確認すること
- 普段の速さの歩行での認証精度を確認すること
- 異なる速さでの歩行認証精度を確認すること

#### 4.2.1 実験方法

上記の目的を達成するために，次の 3 種類の実験を行う．

① 予備実験

まず，機械学習の教師ありアルゴリズムを用いて 1 つの端末を用いた場合より 2 つの端末を用いた方が歩行認証の識別率が向上するかを確認する．ここでの識別率は，すべての試行回数中の正しく分類された回数の割合とする．

② 普段の速度での歩行実験

次に提案方式が日常の歩行に適用できるかどうか確認するため，機械学習の異常検知を用いた認証精度の確認実験を行う．ここでは，日にちを空けずに普段どおりの速度で歩行してもらう．

③ 異なる速さの歩行実験

異常検知を用いた歩行認証の継続的な認証および異なる速度での歩行認証の適用可能性を確認するため，日にちを空け早歩き，普通歩き，遅歩きの 3 種類の速さでの歩行実験を行う．

実験に使用した機器を**表 1** に示す．今回の実験では，近接無線通信規格である Bluetooth の通信距離内である 10 m の距離を想定し実験を行った．被験者は**図 4** のようにスマートフォンを右ポケットに入れ，スマートウォッチを左腕に装着した状態で約 10 m の廊下を歩行してもらう．なお，使用した機器の BLE の iBeacon では，約 1 m 未満で Near 検知，約 1 m 以上を Far 検知することができる．

#### 4.2.2 予備実験

実験では，15 名の学生に 10 m の廊下を 10 回歩行してもらい，収集したデータ（150 回）の半分（75 回）を学習データ，残りの半分をテストデータとして，機械学習の教師あり分類を用いて評価を行う．機械学習の分類アルゴリズムには SVM（Support Vector Machine），Naïve Bayes，Random Forest，Neural Network を用い識別率の確認を行う．

まず，1 つの端末を用いた場合の識別率を確認するため，1 つの端末から取得できる加速データのみを用い，平均値，中央値，標準偏差，分散，極大値間隔の中央値，極小値間隔の中央値，周期を特徴量として抽出し，Exhaustive Feature Selection により特徴量選択を行ったうえで識別率の確認を行う．スマートフォンのみを用いた場合の結果を**表 2** に示し，スマートウォッチのみを用いた場合の結果を**表 3** に示す．結果として，スマートフォンのみを用いた場合の最も高い識別率は機械学習に Random Forest を用い平均値，中央値，最大値，最小値，極大値間隔，極小値間隔の特徴量を選択した場合の 76.7%であった．また，スマートウォッチのみを用いた場合の識別率を確認した結果，機械学習に Random Forest を用い平均値，中央値，分散，最大値，最小値，極大値間隔，極小値間隔，周期の特徴量を選択した場合の 76.0%であった．

次に，2 つの端末を用いた歩行認証の識別率の確認を行

表 2 スマートフォンのみを用いた場合の識別率
**Table 2** Identification accuracy obtained using only smartphone for various classifiers.

| 機械学習 | | | |
|---|---|---|---|
| SVM | Naïve Bayes | Random Forest | Neural Network |
| 特徴量 | | | |
| 平均値 | 平均値 | 平均値 | 平均値 |
| 中央値 | 中央値 | 中央値 | 中央値 |
| 標準偏差 | 分散 | 最大値 | 標準偏差 |
| 分散 | 最大値 | 最小値 | 分散 |
| 最大値 | 最小値 | 極大値間隔 | 最大値 |
| 極大値間隔 | 極大値間隔 | 極小値間隔 | 最小値 |
| 極小値間隔 | 極小値間隔 | | 極大値間隔 |
| 周期 | | | 極小値間隔 |
| | | | 周期 |
| 識別率 | | | |
| 57.0% | 71.3% | 76.7% | 64.7% |

表 3 スマートウォッチのみを用いた場合の識別率
**Table 3** Identification accuracy obtained using only smartwatch for various classifiers.

| 機械学習 | | | |
|---|---|---|---|
| SVM | Naïve Bayes | Random Forest | Neural Network |
| 特徴量 | | | |
| 中央値 | 平均値 | 平均値 | 平均値 |
| 標準偏差 | 中央値 | 中央値 | 標準偏差 |
| 最大値 | 標準偏差 | 分散 | 分散 |
| 最小値 | 最大値 | 最大値 | 最大値 |
| 極大値間隔 | 最小値 | 最小値 | 最小値 |
| 極小値間隔 | 極大値間隔 | 極大値間隔 | 極大値間隔 |
| 周期 | 極小値間隔 | 極小値間隔 | 極小値間隔 |
| | | 周期 | |
| 識別率 | | | |
| 47.0% | 69.3% | 76.0% | 51.3% |

うため，1 つの端末のみを用いた特徴量に加え，2 つの端末を用いることで抽出できる，平均値の差，中央値の差，標準偏差の差，分散の差，最大値の差，最小値の差，極大値間隔の差，極小値間隔の差，周期の差，SAD（Sum of Absolute Difference），SSD，NCC，DP（Dynamic Programming）の特徴量を抽出し識別率の確認を行う．また，ここではすべての特徴量に対して Exhaustive Feature Selection により特徴量選択を行うと計算量が多くなりすぎるため，抽出した 32 個の特徴量を平均値，中央値，標準偏差，分散，最大値，最小値，極大値間隔，極小値間隔，周期，SAD，SSD，NCC，DP の 13 グループに分割する．たとえば，平均値のグループでは，スマートフォンの加速度データの平均値，スマートウォッチの加速度データの平均値，2 つの端末の平均値の差をそのグループとする．その結果を**表 4** に示す．結果として，2 つの端末を用いた場合に最も良かった識別率は機械学習に Random Forest を用い中央値，分散，最小値，SSD，NCC，極大値間隔，極小値間隔，周期の特徴量を選択した場合の 95.3%であった．これらの結果から，1 つの端末を用いた場合より 2 つの端末を用いた場合の方が，識別率が上がることが確認できる．

しかし，評価に用いた機械学習の教師あり学習分類では，登録ユーザ以外のデータが入力された場合でも登録ユーザのいずれかに分類されてしまうため，未知のデータに対して有効とはいえない．そのためこの予備実験を基に，次に機械学習の異常検知を用いた認証精度の確認実験 2 つを行う．

#### 4.2.3 普段の速度の歩行実験

提案する歩行認証の認証精度を評価するため，日常の歩行を想定し，普段どおりの速度で廊下を歩行してもらう実験を行う．実験では，認証するユーザとして 11 名の学生

表 4 2 つの端末を用いた場合の識別率
**Table 4** Identification accuracy obtained using both smartphone and smartwatch for various classifiers.

| 機械学習 | | | |
|---|---|---|---|
| SVM | Naïve Bayes | Random Forest | Neural Network |
| 特徴量 | | | |
| 平均値 | 標準偏差 | 中央値 | 平均値 |
| 中央値 | 中央値 | 分散 | 中央値 |
| 標準偏差 | NCC | 最小値 | 標準偏差 |
| 分散 | DP | SSD | 分散 |
| 最大値 | 極大値間隔 | NCC | 最大値 |
| 最小値 | 極小値間隔 | 極大値間隔 | 最小値 |
| SAD | | 極小値間隔 | SSD |
| NCC | | 周期 | NCC |
| 極大値間隔 | | | 極小値間隔 |
| 極小値間隔 | | | |
| 識別率 | | | |
| 86.7% | 90.0% | 95.3% | 83.3% |

に 10 m の廊下を 50 回，異常データとして認証するユーザ以外の 10 名の学生に 10 m の廊下を 20 回歩行してもらい，歩行中の加速度データを取得することで実験を行う．実験の手順を以下に示す．

(1) スマートロック用のサーバが 2 つの端末に加速度データ取得開始を送る．
(2) 2 つの端末がそれぞれ加速度計測を開始する．
(3) 被験者はその場で 5 秒間静止する．
(4) 被験者は廊下を 10 m 歩行する．
(5) 被験者はその場で 5 秒間静止する．
(6) スマートロック用のサーバが 2 つの端末に加速度データ取得終了を送る．
(7) 2 つの端末がそれぞれ加速度計測を終了する．

上記の手順 (3)，(5) で 5 秒間の静止を行う理由は，手順 (4) の歩行状態をより正確に抽出するためである．以上の手順で得られた加速度データから学習器を作成し，認証精度の確認を行う．

#### 4.2.4 異なる速さの歩行実験

次は日にちを空け実験を行い，早歩き，普通歩き，遅歩きの 3 種類の速度での歩行を行うことで，継続的な歩行認証の有効性および異なる速度での歩行認証の有効性の確認を行う．実験では，8 名の学生が 1 日に 10 m の廊下を早歩き 10 回，普通歩き 10 回，遅歩き 10 回の歩行を行った．これを，それぞれ日にちを空け 5 日間実施した．実験は 4.2.3 項で述べた実験の手順と同様に行う．日にちを空けた場合の継続的な歩行認証の認証精度を評価するため，この実験で得られた普段の速度の歩行データを用い学習器を作成し異常データを検知することで認証精度の確認を行う．また，異なる歩行速度での歩行認証の有効性の確認のため，早歩き，普通歩き，遅歩きの 3 つの速度のデータを学習させた学習器を作成し，異常検知により認証精度の確認を行う．これら実験結果については，以降 5 章で示す．

## 5. 評価と考察

上記の 2 つの認証精度の確認実験で得られた加速度データをもとに機械学習の異常検知アルゴリズムを用いたアルゴリズムごとの結果に基づく評価と考察を示す．

### 5.1 普段の速度での認証精度

ここでは，特徴量選択による認証精度向上の確認のため，抽出した 19 個の特徴量を 13 グループ（平均値，平均値の差，標準偏差，標準偏差の差，最大値，最大値の差，最小値，最小値の差，極大値間隔の中央値，極小値間隔の中央値，SSD，NCC，DTW）に分割し，それぞれの特徴量の組合せに対して FAR と FRR を算出する．たとえば，平均値のグループでは端末 1 の平均値，端末 2 の平均値をそのグループとする．学習器には，認証するユーザごとに学習器を作成し，実験で 1 人あたり取得した 50 データのうち学習データとして 30 データを学習させた．また，認証するユーザ以外の異常データとして実験した 10 名 × 20 データの歩行データを異常データとすることで認証精度の確認を行った．**表 5** に学習アルゴリズムごとの最も認証精度が良くなった特徴量の組合せと，FAR，FRR を示す．ここで，機械学習のパラメータや異常度の閾値にはこの FAR と FRR が小さくなるように調整した．すなわち，最急降下法を用いて FAR+FRR の値ができるだけ小さくなるようパラメータを決定した．結果として，異常検知アルゴリズムごとに最適な特徴量の組合せが異なり，認証精度に差があ

表 5 普段の速度での提案歩行認証の認証精度
**Table 5** FAR and FRR of the proposed system using anomaly detection.

| 機械学習（異常検知） | | | | | |
|---|---|---|---|---|---|
| Elliptic Envelope | GMM | Isolation Forest | KDE | LOF | One Class SVM |
| 特徴量の選択 | | | | | |
| 標準偏差の差 | 平均値 | 平均値 | 平均値 | 標準偏差の差 | 平均値 |
| 最大値 | 平均値の差 | 標準偏差 | 平均値の差 | 最大値 | 平均値の差 |
| 最大値の差 | 標準偏差 | 標準偏差の差 | 標準偏差 | 最大値の差 | 標準偏差 |
| 最小値の差 | 標準偏差の差 | 最大値 | 標準偏差の差 | 最小値 | 最大値 |
| DTW | 最大値 | 最小値 | 最小値 | 最小値の差 | 最大値の差 |
| 極大値間隔 | 最小値 | 最小値の差 | 最小値の差 | 極大値間隔 | 最小値 |
| | 最小値の差 | SSD | NCC | 極小値間隔 | 最小値の差 |
| | SSD | NCC | DTW | | SSD |
| | NCC | DTW | 極大値間隔 | | NCC |
| | 極大値間隔 | 極小値間隔 | | | 極大値間隔 |
| FAR | | | | | |
| 7.8% | 13.6% | 8.3% | 15.2% | 12.4% | 6.4% |
| FRR | | | | | |
| 12.2% | 3.6% | 9.5% | 17.7% | 13.1% | 17.2% |

表 6 日にちを空け普段の歩行を行った結果
**Table 6** Results of opening the date.

| 機械学習（異常検知） | | | | | |
|---|---|---|---|---|---|
| Elliptic Envelope | GMM | Isolation Forest | KDE | LOF | One Class SVM |
| FAR | | | | | |
| 22.9% | 29.6% | 19.0% | 18.6% | 70.8% | 15.5% |
| FRR | | | | | |
| 18.1% | 4.3% | 18.8% | 13.8% | 13.1% | 21.9% |

ることが確認できた．また，GMM や Isolation Forest を用いた場合に FAR と FRR が低くなり，GMM を用いた場合に FAR が 13.6%，FRR が 3.6%であり，Isolation Forest を用いた場合に FAR が 8.3%，FRR が 9.5%であった．

### 5.2 異なる速さでの認証精度

日にちを空けた継続的な歩行認証の評価のため 5.1 節で示した普段の速度での歩行認証と同様の方法で認証精度を計算する．また，異なる速度での歩行認証の評価を行うため，早歩き，普通歩き，遅歩きでの 3 つの速度の歩行を学習させた学習器を作成し，その学習器を基に異常検知を行い本人か他人かを判定しその認証精度の計算を行う．

#### 5.2.1 継続的な歩行認証の評価

日にちを空けて実施した歩行認証の認証精度と，日にちを空けずに実施した歩行認証の認証精度を比較するため，5.1 節で選択した学習器ごとの特徴量を用い評価を行う．学習データには，1 日 10 回データのうち 6 回の歩行を学習データとし残りの 4 回を本人データとする．それを同様に 5 日分のデータに対して学習を行う．そのため 1 人のユーザの学習データは 6 回 × 5 日分の 30 データ，テストデータは 4 回 × 5 日分の 20 データとなる．また，他のユーザの普段の歩行を異常データとし機械学習の異常検知を行うことで本人か他人かを判定し認証精度を計算する．その結果を**表 6** に示す．結果として，最も良かった認証精度は機械学習に KDE を用いた場合の FAR が 18.6%，FRR が 13.8%であった．ここでは，大きく認証精度が悪くなった機械学習のアルゴリズムもあればあまり認証精度に変化のないアルゴリズムもあることを確認した．たとえば，日にちを空けずに行った歩行に比べ KDE では，FAR が +3.4%，FRR が −3.9%とそれほど変わらないという結果となった．

#### 5.2.2 異なる速さでの歩行認証の評価

次に，日によって早歩きの場合や普通の速度での場合，

表 7 早歩き普通歩き遅歩きを行った実験の結果
Table 7 Results of different speeds.

| 機械学習（異常検知） | | | | | |
|---|---|---|---|---|---|
| Elliptic Envelope | GMM | Isolation Forest | KDE | LOF | One Class SVM |
| FAR | | | | | |
| 46.8% | 18.8% | 34.5% | 20.0% | 75.5% | 37.3% |
| FRR | | | | | |
| 11.0% | 15.0% | 16.0% | 20.6% | 9.1% | 14.4% |

表 8 被験者ごとの認証精度
Table 8 FAR and FRR of each subject.

| | 機械学習（異常検知） | | | |
|---|---|---|---|---|
| | GMM | | Isolation Forest | |
| | FAR | FRR | FAR | FRR |
| 被験者 A | 6.0% | 5.0% | 4.0% | 10.0% |
| 被験者 B | 42.5% | 0.0% | 16.5% | 0.0% |
| 被験者 C | 28.5% | 0.0% | 6.5% | 25.0% |
| 被験者 D | 0.0% | 10.0% | 0.0% | 5.0% |
| 被験者 E | 21.5% | 0.0% | 3.5% | 5.0% |
| 被験者 F | 2.5% | 0.0% | 7.5% | 5.0% |
| 被験者 G | 0.0% | 5.0% | 0.0% | 0.0% |
| 被験者 H | 0.5% | 0.0% | 13.0% | 10.0% |
| 被験者 I | 37.5% | 15.0% | 23.0% | 20.0% |
| 被験者 J | 8.5% | 5.0% | 9.5% | 25.0% |
| 被験者 K | 3.0% | 0.0% | 8.5% | 0.0% |

遅歩きでの場合など異なる速さでの歩行が予測されるため，歩行の速さを変えた場合での歩行認証の認証精度の確認を行う．ここでは，5.1 節で選択したそれぞれの学習器ごとの特徴量を用い評価を行う．学習データには，本人のデータのみを学習させ，1 日の早歩き 10 回，普通歩き 10 回，遅歩き 10 回のデータのうちそれぞれ 6 回 × 3 の 18 データを 5 日分，合計 90 データを学習器に学習させた．また，学習データ以外の 4 回 × 3 の 12 データを 5 日分，合計 60 データを本人データとし，他の被験者の歩行データを異常データとし認証精度の確認を行った．その結果を**表 7** に示す．結果として，最も良かった識別率は機械学習に GMM を用いた場合の FAR が 18.8%であり，FRR が 15.0%であった．全体的に，普段の速さで行った場合に比べ認証精度は軒並み悪くなった．

### 5.3 考察

今回実施した実験の結果から考えられるユーザごとの認証精度とアルゴリズムごとの認証精度について簡単にまとめる．

#### 5.3.1 被験者ごとの認証精度

提案方式では，学習に本人のデータのみを学習させるため，個人の歩行のばらつきによって認証精度が大きく異なることが予測される．そこで，ユーザごとの認証精度の違いを確認するため他の異常検知アルゴリズムに比べ認証精度の良かった，GMM と Isolation Forest を用いた場合の被験者ごとの FAR と FRR の確認を行った．

**表 8** に被験者ごとの FAR と FRR を示す．ここで，同じ識別器の作成方法でも，被験者ごとに認証精度に差があることが分かる．さらに，同じ被験者でも認証精度が良くなる識別器が異なることが確認できる．以上より，複数の異常検知アルゴリズムの結果をもとに異常を判定することによって，認証精度を向上させることができると考えられる．

#### 5.3.2 機械学習アルゴリズムごとの認証精度

今回行った，3 つの歩行認証実験の認証精度をアルゴリズムごとにまとめると**図 5** のようになる．ここで，BER（Balanced Error Rate）は FAR と FRR の平均である．アルゴリズムごとに日にちを空けずに行った実験に比べ，日にちを空けた継続的な歩行認証や，異なる速度を学習させた歩行認証の認証精度が悪くなっている．しかし，KDE の

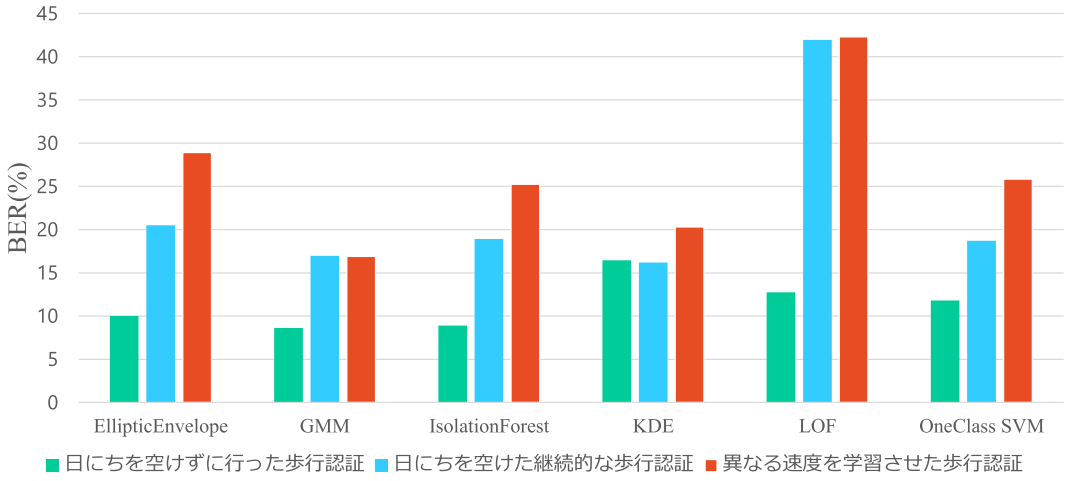


図 5 歩行実験結果の比較

**Fig. 5** Comparison of experimental results.

場合は日にちを空けずに行った場合の BER は 16.4%，日にちを空けた継続的な歩行認証の場合は 16.2%，日にちを空け異なる速度での場合は 20.3%で，認証精度に変化がないことが分かる．したがって，他のアルゴリズムにおいても特徴量の抽出方法や加速度処理の方法によって，日にちを空けずに行う歩行認証の認証精度を高めることができれば継続的および異なる速度での歩行認証の認証精度の向上にもつながると考えられる．

## 6. おわりに

本研究ではスマートロックにおける，スマートフォンとウェアラブル端末の 2 つの端末を用いた歩行認証システムモデルの提案を行い，継続的な歩行認証および異なる速度での歩行認証の有効性を確認するための実験を行った．提案システムモデルでは，事前にスマートロックに 2 つの端末の ID と歩行データを登録しておくことで，認証の際にまず ID を確認し所持認証を行った．歩行認証を行う前に，所持認証を行うことで端末を所持していないユーザの認証を拒否することができ，歩行認証の認証精度の課題を低減させることが期待できる．また加速度処理では，端末の向きを考慮せずに認証を行うため 3 軸加速度の合成加速度を計算し，この合成加速度を基に特徴量の抽出を行った．特徴量抽出では，2 つの端末それぞれの合成加速度から，極大値間隔や 2 つの端末の類似度等の 19 個の特徴量を抽出しそれを 13 グループに分割することで，特徴量選択を行い機械学習の異常検知を用いて認証精度の計算を行った．実験では，日にちを空けた場合の継続的な歩行認証および異なる速さでの歩行認証の有効性を確認するための実験を実施した．まず，日にちを空けた場合の普段の速度での歩行認証の有効性を確認するため，学習データには本人のデータのみを学習させ，評価を行った．結果として，最も良かった識別率では機械学習に KDE を用いた場合の平均 FAR が 18.6%，平均 FRR が 13.8%であった．ここでは，大きく悪くなった機械学習のアルゴリズムもあればあまり変化のないアルゴリズムもあり，たとえば KDE では，FAR が +3.4%，FRR が −3.9%とそれほど認証精度が変わらないという結果となった．次に，異なる速度での歩行認証の有効性を確認するため，学習データには異なる速度の歩行データを学習させ，評価を行った．結果として，最も良かった識別率は機械学習に GMM を用いた場合の FAR が 18.8%であり，FRR が 15.0%であった．こちらも，認証精度は悪くなるという結果となったが，大きく FAR や FRR が悪くなってしまった機械学習アルゴリズムもあれば変化の少ないアルゴリズムもあり，特徴量の抽出方法や加速度処理の方法によっては，認証精度を向上させることができると考えられる．

最後に，今回の実験で使用したデータの数は十分とはいえない．データが少ないことによって生じうる影響として，学習データにいつもと違う歩行データが混ざってしまった場合にそのデータに影響を受けてしまい FRR が高くなってしまう可能性が考えられる．ほかにも，データが少ないことにより他人との境界をつけにくく FAR も高くなってしまうと考えられる．今後の課題としては，認証精度向上のためより幅広い年代の十分なデータでの分析，より良い特徴量の抽出や，より良い特徴量選択の方法等があげられる．また，眼鏡型のウェアラブル端末等，様々なウェアラブル端末から歩行状態の加速度データを取得した場合でも高い精度で認証を行うことができるか確認することがあげられる．

**謝辞** 本研究は JSPS 科研費 JP20K11801 の助成を受けたものです．

## 参考文献

[1] 総務省：5G が促すデジタル革命と新たな日常の構築，令和 2 年度版情報通信白書，入手先 ⟨https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.

pdf⟩ (2020).
[2] Qrio: Qrio Smart Lock, 入手先 ⟨https://qrio.me/smartlock⟩ (参照 2020-12-20).
[3] 株式会社フォトシンス：入退室管理システムなら Akerun オフィス向けスマートロック，入手先 ⟨https://akerun.com/feature⟩ (参照 2020-12-20).
[4] August: August Smart Lock, available from ⟨https://august.com⟩ (accessed 2020-12-20).
[5] 彭 龍，渡邉裕司：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，*Computer Security Symposium*，pp.21–23 (2013).
[6] 今野慎介，中村嘉隆，白石 陽，高橋 修：複数のウェアラブルセンサを用いた歩行動作による本人認証法の精度向上，情報処理学会論文誌，Vol.57, No.1, pp.109–122 (2016).
[7] 岩本健嗣，杉森大輔，松本三千人：3 軸加速度センサを用いた歩行者推定手法，情報処理学会論文誌，Vol.55, No.2, pp.734–749 (2014).
[8] Mondal, S., Nandy, A., Chakraborty, P., et al.: Gait Based Personal Identication System Using Rotation Sensor, *Journal of Emerging Trends in Computing and Information Sciences*, Vol.3, No.3, pp.395–402 (2012).
[9] Muaaz, M. and Mayrhofer, R.: Smartphone-Based Gait Recognition: From Authentication to Imitation, *IEEE Trans. Mobile Computing*, Vol.16, No.11 (2017).
[10] Gartner: Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019, available from ⟨https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow-⟩ (accessed 2020-12-20).
[11] 渡辺一樹，長友 誠，油田健太郎，岡崎直宣，朴 美娘：スマートロックにおける二端末の加速度を用いた歩行状態による本人認証の検討，FIT2018（第 17 回情報科学技術フォーラム），第 4 分冊，pp.137–140 (Sep. 2018).
[12] 渡辺一樹，長友 誠，油田健太郎，岡崎直宣，朴 美娘：スマートフォンとウェアラブル端末の加速度センサを用いたスマートロックにおける歩行認証，コンピュータセキュリティシンポジウム（CSS2018）論文集，pp.173–178 (Oct. 2018).
[13] Watanabe, K., Nagatomo, M., Aburada, K., Okazaki, N. and Park, M.: Gait-Based Authentication for Smart Locks Using Accelerometers in Two Devices, *The 22nd International Conference on Network-Based Information Systems* (*NBiS2019*), *Advances in Networked-based Information Systems 1036*, pp.281–291, Springer (2019).
[14] 渡辺一樹，長友 誠，油田健太郎，岡崎直宣，朴 美娘：スマートロックにおける異常検知を用いた二つの端末の加速度による歩行認証の提案，マルチメディア分散協調とモバイルシンポジウム 2019 論文集，pp.1155–1160 (2019).
[15] Watanabe, K., Nagatomo, M., Aburada, K., Okazaki, N. and Park, M.: Gait-Based Authentication using Anomaly Detection with Acceleration of Two Devices in Smart Lock, *Proc. 14th International Conference on Broad-Band Wireless Computing, Communication and Applications* (*BWCCA-2019*), Lecture Notes in Networks and Systems 97, pp.352–362, Springer (2019).
[16] scikit-learn: scikit-learn machine learning in Python scikit-learn 0.19.1 documentation, available from ⟨http://scikit-learn.org/stable/index.html⟩ (accessed 2020-12-20).

**朴 美娘** （正会員）

1983 年漢陽大学工学部電子工学科卒業．同年同大学工学部助手．1993 年東北大学大学院工学研究科情報工学専攻博士後期課程修了．同年同大学電気通信研究所助手．1994 年三菱電機株式会社入社．2010 年神奈川工科大学情報学部教授．博士（工学）．ネットワークセキュリティ，暗号プロトコル設計，認証等の研究に従事．IEEE，電子情報通信学会，日本セキュリティ・マネジメント学会各会員．

**渡辺 一樹** （学生会員）

2021 年 3 月神奈川工科大学工学研究科博士前期課程修了．在学中，個人認証方式の研究に従事．現在，アルプスシステムインテグレーション株式会社在籍．

**油田 健太郎** （正会員）

2003 年宮崎大学工学部情報システム工学科卒業．2005 年同大学大学院工学研究科情報工学専攻博士前期課程修了．2006 年熊本県立大学総合管理学部助手．2009 年宮崎大学大学院工学研究科システム工学専攻博士後期課程修了．同年大分工業高等専門学校助教．2012 年同講師．2017 年宮崎大学工学部情報システム工学科准教授．博士（工学）．コンピュータネットワークに関する研究に従事．電子情報通信学会，電気学会各会員．

**岡崎 直宣** （正会員）

1986 年東北大学工学部通信工学科卒業．1991 年同大学大学院工学研究科電気及び通信工学専攻博士後期課程修了．同年三菱電機株式会社入社．2002 年宮崎大学工学部助教授．2007 年同大学准教授を経て，2011 年同大学工学教育研究部教授．博士（工学）．通信プロトコル設計，ネットワーク管理，ネットワークセキュリティ，モバイルネットワーク等の研究に従事．電子情報通信学会，IEEE 各会員．