

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

渡辺 一樹¹ 長友 誠¹ 油田 健太郎² 岡崎 直宣² 朴 美娘¹

概要：電子的に鍵の開閉を行うスマートロックがある。その認証方式として、指紋認証方式や顔認証方式ではドアの前で数秒間立ち止まらなくてはならないという煩わしさがある。そこで、我々は歩行時の行動的特徴を用いて認証を行う方式に着目した。歩行認証は、スマートフォンの加速度センサや角速度センサを用いた研究が行われてきたが認証精度に課題があった。本研究ではスマートフォンとウェアラブル端末の二つの端末の加速度センサを用いて歩行認証を行うモデルを提案する。また、各端末のセンサから取得した加速度データから 31 個の特徴量を抽出し機械学習を用いて本人認証率を計算する。

キーワード：歩行認証, スマートロック, 機械学習, ウェアラブル端末, 加速度センサ

A Study on Smart Lock Authentication Using Smart Phone and Wearable Device Acceleration Sensor

KAZUKI WATANABE¹ MAKOTO NAGATOMO¹ KENTARO ABURADA² NAONOBU OKAZAKI²
MIRANG PARK¹

Abstract: Recently, smart lock products that electronically open doors are used. But they have a kind of troublesomeness. People have to stop for several seconds in front of door, in a fingerprint or face authentication method. Therefore, we focused on a user authentication method using walking behavioral features. Conventional gait-based authentication method using an acceleration sensor or angular velocity sensor of a smart phone has a problem in authentication accuracy. In this paper, we propose a gait-based authentication method using acceleration sensors of two terminals, a wearable device and a smart phone. In addition, 31 features are extracted from the acquired acceleration data, and the individual authentication rate is calculated using machine learning.

Keywords: gait-based authentication, smart lock, machine learning, wearable device, acceleration sensor

1. はじめに

近年、モノとインターネットがつながる IoT(Internet of Things) 製品が多く開発されている。IoT 製品は年々増加傾向にあり情報通信白書 [1] によると 2021 年には約 350 億台にも増加すると予測されている。IoT 製品にはインターネットと家電がつながるスマート家電や、音声でインター

ネット上のコンテンツとつながるスマートスピーカーなど様々な製品が開発されている。その中で、スマートロックと呼ばれる IoT 製品がある。スマートロックは家のドアの鍵などに取り付け、電子的に鍵の開閉を行う IoT 製品である。2015 年はスマートロック元年と言われ、現在までに、Qrio[2] や Akerun[3], August[4] など、様々なスマートロック製品が販売されている。スマートロックにおける認証方式として、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がある。これらの問題点を解消する方式として人間の身体的特徴や行動的特徴を用いて認証を行う生体認証方式がある。しか

¹ 神奈川工科大学
Kanagawa Institute of Technology
² 宮崎大学
University of Miyazaki

し、スマートロックにおける生体認証方式として、例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無くすことができていない現状がある。そこで、本論文ではユーザが所持している端末のセンサから得られる歩行状態の行動的特徴を用いて認証を行う歩行認証に着目する。通常生活で行う歩行を用いることでユーザが意識することなく認証が行われ、さらにドアの数メートル前から加速度計測を開始し、ドアのすぐ手前で加速度計測を終了し自動的に認証を行うことでスマートロックにおける認証の煩わしさを解消できると考える。

先行研究では、スマートフォンに搭載された加速度センサを用いた歩行認証の研究が行われてきた [5],[6],[7]。ここでは認証の際に、端末の向きを同じにしなければならないという煩わしさや、認証精度の課題がある。また、体に身に付けた複数のセンサを用いた歩行認証の研究もある [8]。単一のセンサを用いた認証より、認証精度が向上しているが、大量のセンサを身につけなくてはならないため、ユーザにとって望ましい認証とは言えない。

一方、体に身に付け持ち歩く端末であるウェアラブル端末として、メガネ型のスマートグラスや腕時計型のスマートウォッチなどの製品が開発されている。ウェアラブル端末は年々増加傾向にあり情報通信白書 [9] によると 2020 年には約 3 億台にも増加すると言われ、多くの人がウェアラブル端末を所持すると予測される。

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二つの端末を用いた歩行認証を提案する。本論文では、スマートロックを想定したスマートフォンとウェアラブル端末を用いた歩行認証のシステムモデルを提案する。また、実験として腕に身に付けるウェアラブル端末であるスマートウォッチから歩行状態の腕の振りによる個人の特徴を抽出し、さらにポケットに入れるスマートフォンから足の動きによる個人の特徴を抽出することで歩行認証を行いその有効性を確認する。

以降、2. では歩行認証の関連研究について示す。3. ではスマートロックを想定したスマートフォンとウェアラブル端末の二つの端末を用いた歩行認証の提案システムモデルを示す。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示す。4. では実装と実験について述べる。5. では提案方式の識別率や認証に貢献する特徴量について示す。6. ではまとめと今後の課題を示す。

2. 関連研究

2.1 スマートフォンに搭載されたセンサを用いた歩行認証

彭ら [5] は、スマートフォンに搭載された加速度センサか

ら取得される 3 軸加速度 x, y, z を用いた歩行認証を提案している。認証には機械学習の分類を用い、歩行時の加速度データから、平均値や標準偏差、絶対標準偏差、平均合成加速度、ピーク間の時間、ビン分布を用いた 43 個の特徴量を抽出し識別率を調べている。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、FAR(False Acceptance Rate) が 0.6%、FRR(False Rejection Rate) が 8.7%であり、NeuralNetwork を用いた場合の FAR は 0.3%、FRR が 3.8%であった。また、平均値のみ、標準偏差のみ、平均絶対偏差のみ、平均合成加速度のみ、ピーク間の時間のみのみ、ビン分布のみ、平均値なしの 7 パターンから FAR、FRR を調べることで認証に貢献する特徴量や認証に貢献しない特徴量を挙げている。認証に貢献した特徴量としては 3 軸それぞれの平均値が挙げられ、認証に貢献しない特徴量として平均合成加速度やピーク間の時間が挙げられている。さらに、データマイニングソフトである WEKA の 56 個の分類アルゴリズムを用い識別率を計算し、分類アルゴリズムによって精度が大きく変わることを示している。しかし、各 x, y, z の 3 軸加速度データから特徴量を抽出したため、端末の向きを考慮しなくてはいけないという課題が残っている。

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。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。ここでは、端末の向きやポケットなど実際の環境を想定した歩行認証を課題としている。

2.2 加速度センサが搭載された端末の所持位置を考慮した歩行認証

岩本ら [7] は、ユーザの歩行状態の推定 (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) を行った上で、ユーザの推定を行う歩行認証のモデルを提案している。被験者 5 名に対して実験を行い、状態推定に関しては 99.7%、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。所持位置推定の結果から、同じ体に身に付けた端末でも所持位置によって異なったデータを取得できると考えられ、複数の異なった部位にセンサを身に付けることで歩行認証の精度向上が期待できる。

2.3 複数のセンサを体に装着した歩行認証

Mondal ら [8] は、体の関節 8 箇所 (右肩、左肩、右腕、左腕、右腰、左腰、右足、左足) に角度センサを装着し、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。体の 8 箇所に装着された角度センサから得られる信

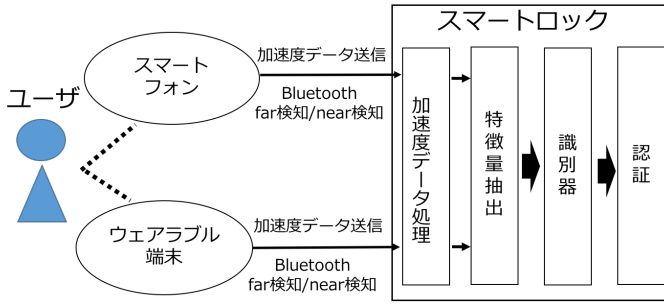


図 1 提案システムモデル

号を計測し NeuralNetwork などを用い、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言えない。

本研究では、多くの人が身に付けることが予測されるウェアラブル端末やスマートフォンを異なった体の部位に装着し加速度データを取得することで、端末の向きを考慮せずに歩行認証を行う場合でも、高い識別率を得ることを目的とする。

3. 提案方式

3.1 システムモデル

スマートフォンとウェアラブル端末の二つの端末の加速度データを用いてスマートロックの認証を行う。システムモデルを図 1 に示す。提案システムモデルは、加速度センサが搭載されたスマートフォンとウェアラブル端末、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ている。スマートフォンとウェアラブル端末は Bluetooth の iBeacon を用いてスマートロックとの近接検知を行う。iBeacon では immediate(約 2cm 未満), near(約 2cm～約 1m), far(約 1m～約 50m) の 3 つの近接検知を行うことができ、本提案では 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。提案システムモデルの認証手順を以下に示す。

- (1) 二つの端末がそれぞれ iBeacon の far 検知を行う。
- (2) 二つの端末がそれぞれ加速度計測を開始する。
- (3) 二つの端末がそれぞれ iBeacon の near 検知を行う。
- (4) 二つの端末がそれぞれ加速度計測を終了する。
- (5) 二つの端末がそれぞれ加速度データをスマートロックへ送信する。
- (6) スマートロック内で、手順 (5) で取得した加速度データを用いてユーザの認証を行う。

スマートロックには、あらかじめ複数人の歩行データを登録しておき、登録フェーズで歩行データの登録を行う。また、認証フェーズでは登録されたデータを基に本人認証を行う。手順 (6) において、スマートフォンとウェアラブル端末の加速度データを受信したスマートロックはデータの処理を行い、そのデータから特徴量を抽出する。通信の遅延や近接検知の精度の差などから加速度データを取得す

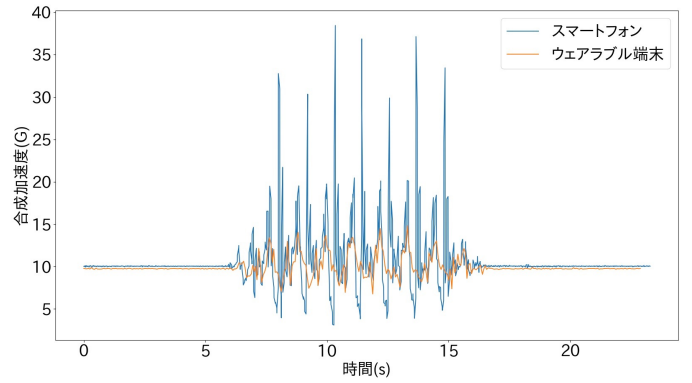


図 2 合成加速度データ

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最大値などの特徴量を抽出する。特徴量を抽出した後、識別器でユーザを判定し認証を行う。識別器には、機械学習の教師あり学習を用いる。

3.2 加速度データの処理

スマートフォンとウェアラブル端末の加速度センサから測定されたデータをスマートロックで受信しユーザの特徴量を抽出するため加速度データの処理を行う。本研究では、合成加速度を用いることで端末の向きを考慮せずに歩行認証を行う。ここで、スマートフォンとウェアラブル端末の合成加速度 r_i^1, r_i^2 を次のように示す。なお、取得した x, y, z 軸の加速度データをスマートフォンでは x_i^1, y_i^1, z_i^1 と表しウェアラブル端末では x_i^2, y_i^2, z_i^2 で表す。

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

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

スマートフォンとウェアラブル端末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、計測開始から終了までに取得したデータ数を n_1, n_2 で表すと、スマートフォンとウェアラブル端末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。

$$d_1 = \{(t_i^1, r_i^1) | i \in \{1, \dots, n_1\}\} \quad (3)$$

$$d_2 = \{(t_i^2, r_i^2) | i \in \{1, \dots, n_2\}\} \quad (4)$$

二つの端末の合成加速度データの例を図 2 に示す。青い波形は右ポケットに入れたスマートフォンの合成加速度データを示し、オレンジ色の波形はウェアラブル端末であるスマートウォッチを左腕に装着した場合の合成加速度データを示す。ここで、二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を確認できた。そこで、二つのデータを比較するため二つの端末のサンプル数を合わせる。その方法として、二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わせる。例えば、2 つの

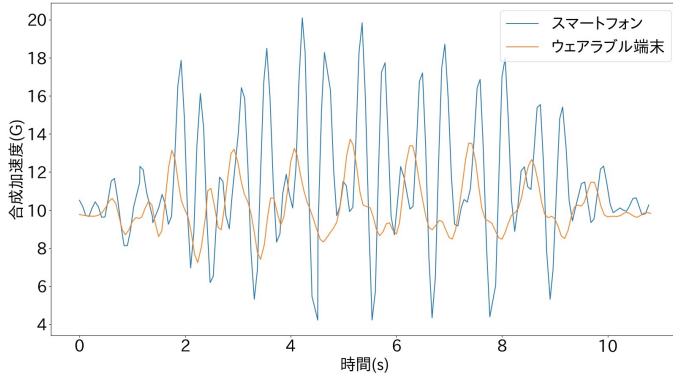


図 3 加速度処理後の合成加速度データ

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。

$$d'_1 = \{(t_i^1, r_i^1) | i \in \{1, \dots, n_2\}\} \quad (5)$$

$$d'_2 = \{(t_i^2, r_i^2) | i \in \{1, \dots, n_2\}\} \quad (6)$$

ここで、 t_i^1, r_i^1 は以下の式で計算される。

$$t_i^1 = t_1^1 \arg \min_{j \in \{1, \dots, n_1\}} (|t_j^1 - t_i^2|) \quad (7)$$

$$r_i^1 = r_1^1 \arg \min_{j \in \{1, \dots, n_1\}} (|r_j^1 - r_i^2|) \quad (8)$$

また、静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。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の処理を行ったあとの波形を示す。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。

3.3 特徴量抽出

ユーザ識別のため合成加速度データの平均値、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、類似度を用いた特徴量を抽出する。本提案ではスマートフォンとウェアラブル端末の二つの端末を用いるため、端末それぞれの値や二つの端末の差などを計算することにより個人の特徴量の抽出を行う。類似度の特徴量は、二つの端末の加速度データを時間軸方向にずらし、最も高い類似度の値を特徴量とする。その類似度を算出する方法として、テンプレートマッチングを用いる。使用したテンプレートマッチングは絶対値の差から計算する SAD (Sum of Absolute Difference)、二乗和から計算する SSD (Sum of Squared Difference)、相関係数から計算する NCC (Normalized Cross Correlation) の 3 つを用いる。3 つの類似度を算出する式を式 (9)~(11) に示す。た

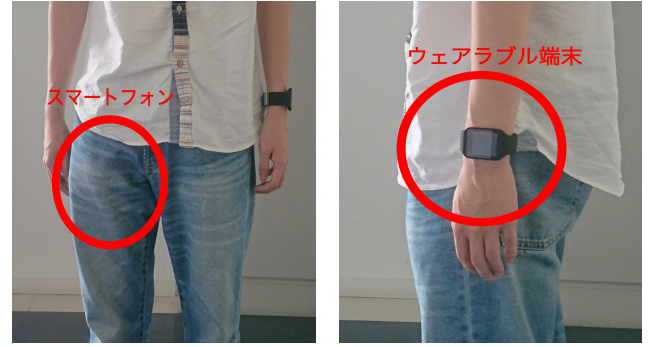


図 4 スマートフォンを用いた例 図 5 ウェアラブル端末を用いた例

だし、式 (5), (6) でそろえたサンプル数を n とした場合、2 つの合成加速度データを n まですらすと類似度を比較するサンプル数が少なくなってしまうため、ずらす個数を $k \in \{1, \dots, \frac{2}{3}n\}$ とする。

$$SAD = \min_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{1}{n-k} \sum_{i=1}^{n-k} |r_i^1 - r_{i+k}^2| \quad (9)$$

$$SSD = \min_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{1}{n-k} \sum_{i=1}^{n-k} (r_i^1 - r_{i+k}^2)^2 \quad (10)$$

$$NCC = \max_{k \in \{1, \dots, \frac{2}{3}n\}} \frac{\sqrt{\sum_{i=1}^{n-k} r_i^1 r_{i+k}^2}}{\sqrt{\sum_{i=1}^{n-k} (r_i^1)^2} \sqrt{\sum_{i=1}^{n-k} (r_{i+k}^2)^2}} \quad (11)$$

また、DP (Dynamic Programming) マッチングの 1 つである最小コスト弾性マッチングを用いる類似度も特徴量とする。その類似度を算出する式を次に示す。

$$\text{コスト} : C = |r_i^1 - r_j^2|$$

$$DP(i, j) = \min \begin{cases} DP(i-1, j-1) \\ DP(i-1, j) + C \\ DP(i, j-1) + C \end{cases} \quad (12)$$

なお、 $i, j \in \{1, \dots, n\}$ とした場合、 $DP(n, n)$ を特徴量とする。以上の計算を用いて特徴量の抽出を行う。

本提案では、スマートフォンとウェアラブル端末それぞれの二つの平均値、二つの中央値、二つの標準偏差、二つの分散、二つの最大値、二つの最小値、二つの極大値間隔の中央値、二つの極小値間隔の中央値、二つの周期、また、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, SSD, NCC, DP の 31 個の特徴量を用いて、識別器で分類することによってユーザの分類を行う。

4. 実装と実験

本研究で示したシステムモデルの評価を行うため実装を行った。システムモデルの加速度データを取得する端末として、スマートフォンに Sony XperiaXZs、ウェアラブル端末に Sony SmartWatch3 を用い、二つの端末の Android

表 1 スマートフォンを用いた場合の識別率

機械学習			
SVM	NaiveBayes	RandomForest	NeuralNetwork
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 2 スマートウォッチを用いた場合の識別率

機械学習			
SVM	NaiveBayes	RandomForest	NeuralNetwork
特徴量			
中央値	平均値	平均値	中央値
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			
47.3%	69.3%	76.0%	51.3%

システムから加速度センサのデータを取得するプログラムを JAVA で作成する。また、スマートロックの代わりにサーバを用意し、加速度データを受信しそのデータを基に機械学習を行い識別率を計算するプログラムを Python で作成する。データの送受信には Bluetooth を使い、加速度の計測開始命令および計測終了命令を各端末に送信することで加速度計測を行う。機械学習には Python モジュールの scikit-learn[10] を使い、分類アルゴリズムとして SVM, NaiveBayes, RandomForest, NeuralNetwork を用い識別率を計算する。

次に、提案したスマートフォンとウェアラブル端末を用いた歩行認証の有効性を確認するため実験を行なった。被験者には図 4 のようにスマートフォンを右ポケットに入れ、図 5 のようにウェアラブル端末を左腕に装着した状態で約 10m の廊下を 20 回歩行してもらう。被験者は神奈川工科大学の学生 15 名である。実験の手順を以下に示す。

- (1) 二つの端末がそれぞれ加速度計測を開始する。
- (2) 被験者は 5 秒間その場で静止する。
- (3) 被験者は廊下を 10m 歩行する。
- (4) 被験者は 5 秒間その場で静止する。
- (5) 二つの端末がそれぞれ加速度計測を終了する。

表 3 二つの端末を用いた場合の識別率

機械学習			
SVM	NaiveBayes	RandomForest	NeuralNetwork
特徴量			
平均値	標準偏差	中央値	平均値
中央値	最小値	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%

表 4 特徴量最頻出順

機械学習	
NaiveBayes	RandomForest
頻出数	
最小値 (2 回)	極大値間隔 (363 回)
NCC(2 回)	最小値 (342 回)
極大値間隔 (2 回)	中央値 (332 回)
極小値間隔 (2 回)	極小値間隔 (317 回)
平均値 (1 回)	NCC(281 回)
標準偏差 (1 回)	SSD(197 回)
最大値 (1 回)	DP(197 回)
SSD(1 回)	周期 (194 回)
DP(1 回)	最大値 (184 回)
中央値 (0 回)	SAD(184 回)
分散 (0 回)	標準偏差 (181 回)
SAD(0 回)	中央値 (176 回)
周期 (0 回)	分散 (173 回)

なお、手順 (2), (4) では、手順 (3) の歩行状態を正確に抽出するため 5 秒間の静止を行う。以上の手順で得られた加速度データからユーザの分類を行い識別率を確認する。

5. 評価

上記の実験で得られた 300 個の加速度データを基に識別率を計算する。また、半分のデータを機械学習の学習データとし、残りのデータをテストデータとする。なお、識別率は正しく分類できたデータ数から全てのテストデータ数を割った値を百分率で算出する。まず、端末を身に付ける場所による違いを確認するため、右ポケットに入れたスマートフォンのみを用いた場合の識別率、左腕に装着したウェアラブル端末のみを用いた場合の識別率をそれぞれ計算する。

スマートフォンのみを用いる場合、二つの端末の値の差や二つの合成加速度の類似度を特徴量とすることができない。そのため、スマートフォンの平均値、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する. 表 1 にスマートフォンのみを用い, 最も高い識別率とその場合に使用した特徴量を機械学習別で示す. 右ポケットに入れたスマートフォンの加速度データのみを特徴量とした際, RandomForest を用い特徴量に平均値, 中央値, 最大値, 最小値, 極大値間隔, 極小値間隔を用いた場合, 最も識別率が 76.7% であった.

次に, 左腕に装着したウェアラブル端末のみを用いた場合, スマートフォンのみを用いた場合と同様に, ウェアラブル端末の加速度データから特徴量を抽出し, 識別率を計算する. 表 2 にウェアラブル端末のみを用い, 最も高い識別率とその場合に使用した特徴量を機械学習別で示す. 左腕に装着したウェアラブル端末から得られる加速度データを特徴量とした際, RandomForest を用い, 特徴量に平均値, 中央値, 分散, 最大値, 最小値, 極大値間隔, 極小値間隔, 周期を用いた場合に最も識別率が 76.0% であった. スマートフォンから取得される加速度データのみで識別を行なった場合より, 左腕につけたスマートウォッチのみを用いた場合の方が識別率が低い結果となった. スマートフォンから取得される足の動きの特徴量は, 個人の足の長さの違いなどにより歩幅が変わり個人差が大きいと考えられ, 腕に装着するスマートウォッチから取得される腕の動きの特徴量は, 腕の長さなどによって腕の振りによる影響が少ないため, このような結果になったと考えられる.

次に, スマートフォンとウェアラブル端末の二つの端末を用いた場合の歩行認証の有効性を確認するため, 二つの端末から特徴量を抽出し識別率を確認する. 全ての特徴量の組み合わせに対して識別率を計算すると, 計算量が多くなってしまう. そのため, 特徴量を 13 グループ (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) に分割する. 例えば, 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, ウェアラブル端末の加速度データの平均値, 二つの端末の平均値の差をそのグループとする. 表 3 に二つの端末を用い, 最も高い識別率とその場合に使用した特徴量のグループの組み合わせを機械学習別で示す. 二つの端末を用いた場合の最も高い識別率は機械学習に RandomForest を用い, 特徴量に中央値, 分散, 最小値, SSD, NCC, 極大値間隔, 極小値間隔, 周期のグループを用いた場合の 95.3% であった. 表 1 と表 2, 表 3 から, 一つの端末を用いた場合より二つの端末を用いた場合の方が識別率が上がるのがわかった. また, 表 4 に識別率 90% を超えた機械学習で使用された特徴量を再頻出順で示す. この結果から, 今回の提案では, 極大値間隔や最小値, 極小値間隔などは認証に貢献し, 分散や中央値, 標準偏差などは認証に貢献しないことがわかった.

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二つの端末を用いた歩行認証のシステムモデルを提案した. 認証には機械学習の分類を用い, 二つの端末を所持した歩行時に得られる加速度データを基に抽出する 31 個の特徴量を示した. 実験として, 被験者 15 名に 10m の廊下を歩行してもらい識別率を確認した. 結果として, 一つの端末を用いた場合より二つの端末を用いた場合の方が識別率が向上し, 機械学習に RandomForest を用い, 特徴量に中央値, 分散, 最小値, SSD, NCC, 極大値間隔, 極小値間隔, 周期を選択した場合 95.3% という識別率となった. さらに, 識別率が 90% 以上になった機械学習で使われた特徴量を再頻出順で示し, 認証に貢献する特徴量として, 極大値間隔や最小値, 極小値間隔が挙げられ, 認証に貢献しない特徴量として, 分散や中央値, 標準偏差が挙げられた.

今後は, 提案システムモデルを実際の環境でも行えるか確認するためシステムの開発を行う予定である. また, 眼鏡型のウェアラブル端末など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を行う予定である.

参考文献

- [1] 総務省: IoT 化する情報通信産業 爆発的に増加する IoT デバイス, 平成 29 年度版 情報通信白書, 入手先 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/pdf/n3300000.pdf> (2017).
- [2] Qrio: Qrio Smart Lock, (<https://qrio.me/smartlock>) (2018/08/02 参照).
- [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, (<https://akerun.com/feature>) (2018/08/02 参照).
- [4] august: August Smart Lock, (<https://august.com>) (2018/08/02 参照).
- [5] 彭 龍, 渡邊 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 2013, 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] S. Mondal, A. Nandy, P. Chakraborty, et al.: Gait Based Personal Identification System Using Rotation Sensor, Journal of Emerging Trends in Computing and Information Sciences, Vol.3, No.3, pp.395-402 (2012).
- [9] 総務省: ウェアラブルデバイス ウェアラブルデバイスが注目されている背景, 平成 28 年度版 情報通信白書, 入手先 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n3100000.pdf> (2016).
- [10] scikit-learn: scikit-learn machine learning in Python scikit-learn 0.19.1 documentation, (<http://scikit-learn.org/stable/index.html>) (2018/08/02 参照).