Vol.2021-SPT-41 No.16
2021/3/1

継続的な認証及び異なる歩行速度での二つの端末を用いた異常検知による歩行認証の研究

渡辺 一樹[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二つの端末の加速度による歩行認証を提案する．提案する歩行認証では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，機械学習を用いて本人認証率を計算する．本論文では，継続的な歩行認証の有効性を確認するため日にちを開け定期的に歩行実験を行った．その結果，平均 FAR が 18.6%, 平均 FRR が 13.8%という認証率となった．さらに，様々な歩行速度での認証率の確認を行うため，早歩き，普段歩き，遅歩きの三つの速さを学習させ，平均 FAR が 18.8%で平均 FRR が 15.0%という結果となった．日にちを開けた実験や速さを変えた歩行では歩行認証の認証率が悪いという結果となったが，より良い特徴量の計算や選択によっては認証精度の向上が期待できる．

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 Continuous and at Different Walking Speeds Using Two Devices

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

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 using machine learning. In order to confirm the effectiveness of the continuous gait-based authentication, we conducted walking experiments periodically on different days. As a result, the average FAR is 18.6% and the average FRR is 13.8%. Furthermore, in order to check the authentication rate at various walking speeds, we trained three speeds: fast, normal, and slow. As a result the average FAR is 18.8% and the average FRR is 15.0%.

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) 機器の開発が盛んに進んでいる．例えば，インターネットと繋がる自動車やインターネットと繋がる AI スピーカーなど多くの 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呼ばれる製品がある．2015 年はスマートロック元年と言

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

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，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つか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など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挙げられる．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，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などから行動的特徴を抽出し認証を行う生体認証方式の一つであり，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．さらにドアの数メートル前から開始し，ドアのすぐ手前で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．

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 [5] 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．また，行動的特徴を用いる認証方式では，本人の行動を常に再現することが難しく認証制度に課題がある．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 [6], [7], [8], [9]．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着ける必要がある等の課題点がある．

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体に身に着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 5300 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着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二つの端末を用いた歩行認証システムモデル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二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 の異常検知モデルを用いる．また，提案方式の有効性を確認するため，実装・実験を行った．本研究では，継続的な歩行認証及び異なる速度での歩行認証の有効性を確認するため，8 名の学生に日にちを開け，早歩き，普通歩き，遅歩きの三つの速さで実験を実施する．結果として，日にちを開けた普段の速度での歩行のみの認証率では，平均 FAR が 18.6%，平均が 13.8% となった．また，異なる速度を学習させた場合の認証率は，平均 FAR が 18.8%，平均 FRR が 15.0%という結果となった．機械学習アルゴリズムの中には日にちを開けずに行った実験と認証率があまり変わらないアルゴリズムもあり，特徴量の抽出方法によって継続的な歩行認証及び異なる速度での歩行認証の認証率向上が期待できる．

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二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示す．4 章では，実装について述べ，5 章で実験について述べる．6 章では，歩行認証の継続的な認証及び異なる速度での認証についての評価を行う．7 章では，おわりとして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 [6] 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 FAR が 0.6%，FRR が

表 1 異常検知を用いた歩行認証の FAR と FRR

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%

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挙げ，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挙げている．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 加速度センサ及び角速度センサを用いた歩行認証

今野ら [7] 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．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，その上で 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率の確認を行なっていた．認証には機械学習には SVM を用いることで評価を行い結果として，提案手法では 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いけない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挙げている．

2.3 端末の所持位置を考慮した歩行認証

岩本ら [8] は，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．また，ユーザの状態推定では特徴量に最大値や最小値，高速フーリエ変換 (FFT) スペクトルを用い，携帯電話の所持位置推定には特徴量に最大値や最小値，軸毎の平均値，変化量を用いている．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．

2.4 複数の加速度センサを使用した歩行認証

Mondal ら [9] 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．体に装着した 8 箇所に装着された角度センサから得られる信号を計測し，結果として識別器に NeuralNetwork 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言えない．

2.5 二つの端末を用いた歩行認証

以前我々は，二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]．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 10m の廊下を歩行しユーザの分類を行った．まず，一つの端末での識別率を確認するためスマートフォンのみの特徴量を用いた識別率の確認を行った．結果として，最も高い識別率は機械学習に RandomForest 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．次に，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 RandomForest 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．これらの結果を踏まえ提案した二つの端末を用いた場合の識別率を行った．結果として，機械学習に RandomForest を用い中央値，分散，最小値，SSD(Sum of Squared Difference)，NCC(Normalized Cross Correlation)，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．この結果から，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言えない．

そこで，未知のデータに対して有効な歩行認証を行うため，機械学習の異常検知を用いた歩行認証の提案を行なった [12]．実験では，11 名の学生に 10m の廊下を 50 回普段の速度で歩行してもらい，歩行中の加速度データを取得した．学習器には本人のデータのみを学習させ，実験で取得した 50 データのうち 30 データを学習させた．また，本人の学習データ以外の 20 データをテストデータとし，他の被験者の歩行データを異常データとすることで認証率の確認を行った．表 1 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み合わせと，平均 FAR，平均 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平均 FAR と平均 FRR が小さくなるように調整した．結果として，GMM や Isolation Forest を用いた場合に FAR と FRR が低くなり，GMM を用いた場合に平均 FAR が 13.6%，平均 FRR が 3.6%であり，Isolation Forest を用い場合に平均 FAR が 8.3%，平均 FRR が 9.5%であった．異常検知アルゴリズムごとに最適な特徴量の組み合わせが異なり，認証精度に差があることが確認できた．

3. 提案方式

本研究では，加速度センサを搭載した二つの端末を用いた歩行認証の提案を行う．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．提案する歩行認証では，二つの端末から取得した加速度データから極大値間隔や二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．スマートロックと二つの端末間の通信方式には Bluetooth を用い，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，及び取得終了を行い，加速度計測を行う．

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二つの端末，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．スマートロックと二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二つの端末との近接検知を行う．iBeacon では Immediate(約 2cm 未満)，Near(約 2cm 1m)，Far(約 1m 約 50m) の 3 つの近接検知を行うことができ，本提案システムモデルでは Near と Far の二つの近接検知を用いて加速度データの計測を行う．二つの端末は，以下の手順で認証を行う．

(1) iBeacon の Far 検知
(2) 二つのデバイスの ID 送信
(3) スマートロック 内で二つのデバイスの ID 確認
(4) 加速度データの計測開始
(5) iBeacon の Near 検知
(6) 加速度データの送信
(7) スマートロック内で受信した二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，二つの端末は 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．次に二つの端末の加速度データを計測し (5) 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，二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他人か判定し，認証を行う．

3.2 ID 確認

提案システムモデルでは，歩行認証の認証率の課題を解消するため，二つの端末に 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，一つの端末だけでなく二つの端末から ID を認証することで，例えば一つの端末が盗難された場合でももう一つ

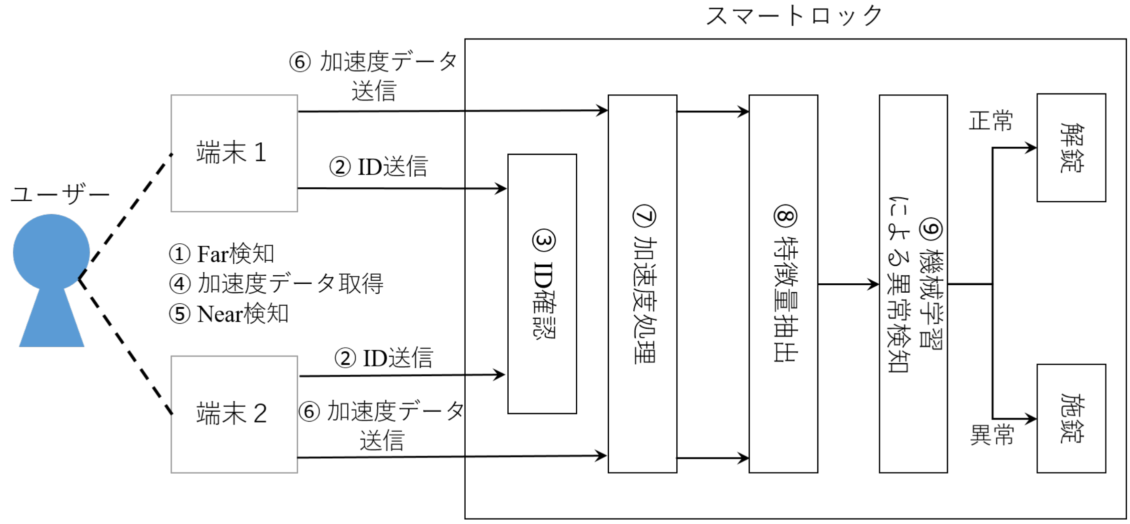

図 1 提案システムモデル

の端末を持っていない限り認証を行うことが出来ない．そのため，同時に二つの端末を盗難され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，二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二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，二つの端末の合成加速度 r_i^1,r_1^2 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．

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

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

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．算出した二つの合成加速度データの例を図 2 に示す．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が確認できる．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．その方式として，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時のデータの集合を d'_1, d'_2 で表すと次のようになる．

$$d'_1 = \left\{(t_i'^1, r_i'^1) | i \in \left\{1, ..., n_2\right\}\right\} \tag{5}$$

$$d'_2 = \left\{(t_i'^2, r_i'^2) | i \in \left\{1, ..., n_2\right\}\right\} \tag{6}$$

ここで，$t_i'^1$，$r_i'^1$，$t_i'^2$，$r_i'^2$ は以下の式で計算される．

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

$$r_i'^1 = r^1_{\underset{j \in \{1,...,n_1\}}{\arg\min}(|t_j^1 - t_i^2|)} \tag{8}$$

$$t_i'^2 = t_i^2 \tag{9}$$

$$r_i'^2 = r_i^2 \tag{10}$$

また，歩行状態を抽出するため，一定区間の加速度データで標準偏差が高い区間を歩行データとして抽出する．その後，特徴量を抽出しやすくするため，フーリエ変換を用いたローパスフィルタで加速度データのノイズを除去する．**図 2** に上記の加速度データ処理を行った後の波形データを示す．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，加速度処理が行われ，歩行状態が抽出されたことが確認できる．

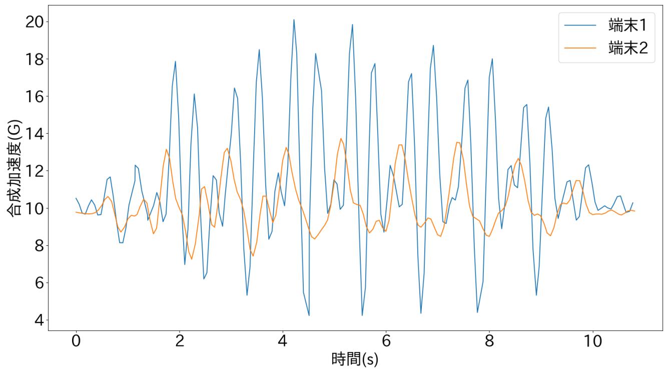

図 2　加速度処理後の合成加速度データ

3.4　特徴量抽出

機械学習を用いた歩行認証を行うため，二つの端末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．特徴量抽出には二つの端末の特徴量の差や二つの端末の加速度データの類似度などを用い，一つ端末だけでは取得できない特徴量の抽出も行う．以下に抽出する特徴量を示す．

- 平均値 (端末 1，端末 2)
- 二つの端末の平均値の差
- 標準偏差 (端末 1，端末 2)
- 二つの端末の標準偏差の差
- 最大値 (端末 1，端末 2)
- 二つの端末の最大値の差
- 最小値 (端末 1，端末 2)
- 二つの端末の最小値の差
- 極大値間隔の中央値 (端末 1，端末 2)
- 極小値間隔の中央値 (端末 1，端末 2)
- 類似度 (SSD: Sum of Squared Difference)

$$SSD = \min_{k \in \{1,\ldots,\frac{2}{3}n\}} \frac{1}{n-k} \sum_{i=1}^{n-k} (r_i'^1 - r_{i+k}'^2)^2 \tag{11}$$

- 類似度 (NCC: Normalized Cross Correlation)

$$NCC = \max_{k \in \{1,\ldots,\frac{2}{3}n\}} \frac{\sqrt{\sum_{i=1}^{n-k} r_i'^1 r_{i+k}'^2}}{\sqrt{\sum_{i=1}^{n-k} (r_i'^1)^2} \sqrt{\sum_{i=1}^{n-k} (r_{i+k}'^2)^2}} \tag{12}$$

- 類似度 (DTW: Dynamic Time Warping)

$$DTW = f(n, n)$$

$$f(i,j) = |r_i'^1 - r_j'^2| + min \begin{cases} f(i-1, j-1) \\ f(i-1, j) \\ f(i, j-1) \end{cases} \tag{13}$$

なお，サンプル数を n とし，$i, j \in 1, ..., n$ とする．また，SSD と NCC の類似度算出に関して二つの端末の動かし方が似ているかを特徴とするため，二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，二つの端末の合成加速度をサンプル数の数ず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 $k \in \{1, ..., \frac{2}{3}n\}$ 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．

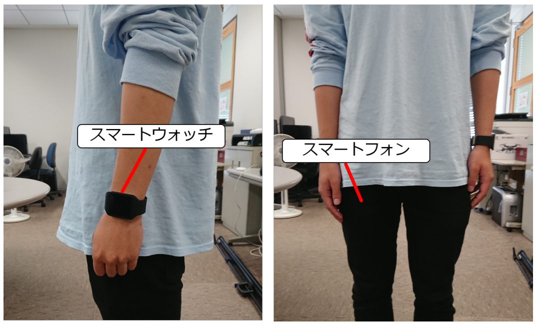

図 3　実験の様子

4.　実装

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 Android 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．実験では，スマートロックの代わりに加速度データを取得するため加速度の開始及び終了命令を送信するためのサーバを用意し，サーバから加速度データ取得開始命令を端末 1，端末 2 がそれぞれ受信した場合に，それぞれの端末で加速度データの計測を開始する．その後，サーバから加速度データ取得終了命令を受信したそれぞれの端末は，加速度計測を終了し，サーバに加速度データを送信する．これらを繰り返すことで加速度データの計測を行う．

次に，機械学習ではより良い特徴量選択を行うため，Exhaustive Feature Search を用いて全ての特徴量の組み合わせに対して認証率を計算し，それぞれの機械学習モデルに適した特徴量の選択を行う．特徴量選択によってえらば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率を計算し，最適なパラメータ及び閾値を決定する．機械学習には Python モジュールの scikit-learn[13] 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率を計算し評価を行う．

5.　実験

実験として，被験者は図 3 のようにスマートフォン (Sony

XperiaXZs) を右ポケットに入れ，ウェアラブル端末 (Sony SmartWatch3) を左腕に装着した状態で約 10m の廊下を歩行してもらう．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用意し，そのパソコンでデータを受信することで実験を行う．継続的な歩行認証の有効性及び異なる速度での歩行認証の有効性の確認を行うため，8 名の学生に 1 日に 10m の廊下を早歩き 10 回，普通歩き 10 回，遅歩き 10 回の歩行を行い，それぞれ日にちを開け 5 日間実施した．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) 被験者はその場で 5 秒間静止する．
(3) 被験者は廊下を 10m 歩行する．
(4) 被験者はその場で 5 秒間静止する．
(5) 二つの端末がそれぞれ加速度計測を終了する．

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学習器を作成し，認証率の確認を行う．

6. 評価

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を用いて認証率の確認を行う．機械学習には Elliptic Envelope，GMM，Isolation Forest，KDE，LOF， One Class SVM の 6 つの異常検知アルゴリズムを用いて評価を行う．評価では，継続的な歩行認証の評価普段及び，異なる速度での歩行認証の評価を示す．

6.1 継続的な歩行認証の評価

継続的な歩行認証の評価では，実験で得た 5 日間の普段の速度でのデータを基に評価を行う．機械学習を行うための学習データには，1 日 10 回データの内 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．そのため一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率を計算する．特徴量には，表 1 と同様の機械学習アルゴリズムごとの最適な特徴量の組み合わせを用い，学習を行なった．その結果を表 2 に示す．結果として，最も良かった認証率は機械学習に KDE を用いた場合の平均 FAR が 18.6%，平均 FRR が 13.8%であった．認証率は，表 1 の結果と比べ軒並み悪くなった．しかし，大きく認証率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率に変化のないアルゴリズムもあり，例えば日にちを開けずに行った歩行に比べ KDE では，FAR が+3.4%，FRR が-3.9%とそこまで変わらないという結果となった．この結果から，より良い特徴量の計算や加速度処理により，継続的な歩行認証でも認証精度の向上が期待できる．

6.2 異なる速度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，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率の確認を行う．認証率の確認では，継続的な歩行認証の評価と同様に表 1 で選択した機械学習アルゴリズムごとの最適な特徴量の組み合わせを用い学習を行う．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率の確認を行った．その結果を表 3 に示す．結果として，最も良かった識別率は機械学習に GMM を用いた場合の平均 FAR が 18.8%であり，平均 FRR が 15.0%であった．こちらも，認証率は軒並み悪くなるという結果となったが，大きく FAR や FRR が悪くなったが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様々な歩行速度を行った場合でも，認証精度の向上が期待できる．

7. 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システムモデルの提案を行い，継続的な歩行認証及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二つの端末の 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う．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，歩行認証の認証率の課題を低減することが期待できる．提案歩行認証では，まず歩行時に得られた二つの端末の加速度データを特徴量が抽出しやすいように加速度データの処理を行った．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う．特徴量抽出では，二つの端末それぞれの合成加速度から，極大値間隔や二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率の計算を行った．実験では，日付を開けた場合の継続的な歩行認証及び異なる速さでの歩行認証の有効性を確認するため，8 名の学生に 10m の廊下を早歩き 10 回，普通歩き 10 回，遅歩き 10 回を行ってもらい日にちを開け 5 日間実験を実施した．まず，日にち

表 2 継続的な歩行認証の認証率

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%

表 3 異なる速度での歩行認証の結果

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%

を開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．認証率は，日にちを開けずに行った結果に比べ軒並み悪くなった．しかし，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，例えば KDE では，FAR が+3.4%，FRR が-3.9%とそこまで認証率が変わらないという結果となった．この結果から，別の特徴量や加速度処理により継続的な歩行認証でも精度の向上が期待できる．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，認証率は軒並み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，認証精度の向上が期待できる．今後の課題としては，認証率の向上のためより良い特徴量の抽出や，より良い特徴量選択の方法などが挙げられる．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することが挙げられる．

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, ⟨https://qrio.me/smart lock⟩ (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, ⟨https://akerun.com/feature ⟩ (参照 2020-12-20).
[4] august: August Smart Lock, ⟨https://august.com⟩ (参照 2020-12-20).
[5] M. Muaaz, R. Mayrhofer: Smartphone-Based Gait Recognition: From Authentication to Imitation, IEEE Transactions on Mobile Computing, Vol. 16, No. 11, (2017).
[6] 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).
[7] 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).
[8] 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).
[9] 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).
[10] Gartner: Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019, ⟨https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow- ⟩ (参照 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，Computer Security Symposium, pp.173-178 (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).
[13] scikit-learn: scikit-learn machine learning in Python scikit-learn 0.19.1 documentation, ⟨http://scikit-learn.org/stable/index.html⟩ (参照 2020-12-20).