Vol.2020-DPS-182 No.45
Vol.2020-CSEC-88 No.45
2020/3/13

スマートロックのためのドアノック型個人認証方式の精度向上に関する検討

中鉢 かける[1]　中村 嘉隆[2]　稲村 浩[2]

概要：IoT（Internet of Things）技術の発展に伴い，住人により快適な暮らしを実現するスマートホームと呼ばれる住宅が注目されている．スマートホームには住宅の玄関ドアの施錠・解錠を物理的な鍵を用いず，スマートフォンを用いて行うことが可能なスマートロックと呼ばれる技術が存在する．玄関ドアの施錠・解錠に関して利便性を向上できる一方，その利用者がスマートフォンの所有者であるかどうかの認証は行っていないため，スマートフォンの盗難等によって悪意のある他者の住居への侵入を許す危険性がある．そこで我々はこれまでにドアの前で自然に行うことができる動作としてドアノック動作から得た行動的特徴を用いた個人認証方式に着目してきた．本稿では，ドアノック動作から取得できる種々の特徴量に対し，機械学習における各種異常検知アルゴリズムを用いた場合の F 値，適合率，再現率を算出することで，提案する認証方式の性能評価を行った．

キーワード：スマートホーム，スマートロック，ドアノック，個人認証

1. はじめに

近年，IoT（Internet of Things）技術の発展に伴い，住人により快適な暮らしを実現するスマートホームと呼ばれる住宅が注目されている．スマートホーム対応家電やデバイスを設置することで，例えばスマートフォンを用いて外出先から自宅のエアコン等の家電を操作するサービスが実現されている．このようなスマートホームのサービスの 1 つとして，住宅の玄関ドアの施錠・解錠を物理的な鍵を用いず，スマートフォンアプリを用いて行うスマートロックと呼ばれるサービスが存在する．スマートロックは既に製品化が進んでいるものもあり，その中には従来のドアのサムターン（ドアの室内側に付いている鍵のツマミ部分）に外付けすることにより，特別な工事が不要でスマートロック化できる製品が販売されている [1] [2]．主機能としてはスマートフォンからの施錠・解錠機能であるが，他にも，利用者の位置情報を利用してドアに近づくだけで解錠が可能なハンズフリー解錠機能や，家族や友人など，利用者本人以外もドアの解錠が可能になるアクセス権シェア機能がある．これらの機能により，従来の物理的な鍵を用いた玄関ドアの施錠・解錠に関して利便性を向上できる．一方，現状のスマートロックサービスの各機能はスマートロック製品とスマートフォンの事前のペアリングに基づいて実行され，その利用者がスマートフォンの所有者であるかどうかの認証は行っていない．そのため，事前に住所を知られている人物によってスマートフォンを盗難された場合や，運転免許証など住所などが記載された個人情報と一緒にスマートフォンの盗難にあった場合は悪意のある他者の住居への侵入を許す危険性が存在し，これらへの対策として，ドア付近における個人認証が必要である．

ドアの前での利用が可能な従来の認証技術として，所有物認証，知識認証，生体認証（バイオメトリクス）認証などがある．所有物認証とは，物理的な鍵や IC カードなど，利用者本人が所有する物理的デバイスを用いて認証を行う技術である．知識認証とは，あらかじめ登録したパスワードを入力して認証するなど，人の脳内にある知識を用いる認証技術である．生体認証には，身体的特徴を用いたものと行動的特徴を用いたものの 2 種類が存在する．身体的特徴を用いた生体認証では人間の指紋や顔，虹彩などの人体に備わる特徴を用いる．行動的特徴を用いた生体認証とは，歩行動作やキーボードの打鍵動作，ドアの開閉動作などの人の行動に現れる特徴を用いる．これらの認証技術にはそれぞれ利点・欠点が存在する．所有物認証の場合，ユーザは認証する際に，物理的な鍵や IC カードを用いて比較的簡単に認証可能だが，それらの機器を盗難に遭った場合や紛失した場合には本人の認証が不可能になるばかりか，他

[1] 公立はこだて未来大学大学院 システム情報科学研究科
[2] 公立はこだて未来大学 システム情報科学部

人に認証を突破される危険もある．知識認証はスマートフォンのロック解除など現在幅広く用いられている認証技術であるが，パスワードなどの記憶負荷が生じる．また，ショルダーハッキングなどによりパスワードが盗難された場合の危険性も高い．身体的特徴を用いた生体認証は，既に人体に備わっている特徴を用いるため，パスワードなどを記憶する負荷はないが，身体特徴の変更はほぼ不可能であるため，指紋の偽造などにあった場合は対応が不可能となる．また，専用のデバイスによって身体情報の一部を特徴として登録する必要があるため，人への心理的負担が大きいという面もある．行動的特徴を用いた生体認証は，人が行う動作からその人固有の特徴を抽出するため，他人に全く同じ動作をされない限り認証を突破されないので，なりすまし攻撃に対する耐性は高いと考えられるが，特徴の選び方によっては十分な認証精度を得ることが難しい．しかし，歩行認証のように利用者に意識させることなく，認証のための特徴を暗黙のうちに取得し，認証できるという利点がある．

現在の製品化されているスマートロックでは，基本的に利用者が事前にスマートロック製品とペアリングによって紐付いたスマートフォンを所持し，ドアに近づいて Bluetooth などを通して近距離で施錠・解錠を行う．従来のドアの施錠・解錠と比較すると，スマートロック製品が鍵穴，スマートフォンがその鍵穴に対応する鍵と見なすことができ，所有物認証を行っており，所有物認証の欠点を抱えているといえる．

本研究では，行動的特徴としてドアの前で自然に行え，動作のための負担が少ないと考えられるドアノック動作に注目する．ドアノック動作に検出される個人特徴をベースに生体認証を可能とすることで，スマートロックの解錠を可能にするドアノック型個人認証方式を提案する．提案方式により，既存のスマートロックが行う所有物認証と行動的特徴を用いた生体認証を組み合わせる 2 要素認証にすることで，セキュリティ強度を高めることが期待できる．

2. 関連研究

2.1 行動的特徴を用いた認証・識別に関する研究

従来の行動的特徴を用いた個人認証・識別に関する研究として，携帯端末や腕時計型端末の加速度センサを用いて空間動作を検知することによる認証手法 [3] [4] が存在する．専用の端末を用いて空間に文字や図形を描いたり，左フックパンチなどの空間に対するパターン化された動作を認証動作としている．また，リズム認証手法に関する研究 [5] [6] も行われている．利用者に対してあらかじめ楽曲を聞かせて，その楽曲に応じたパターン化されたリズムを登録させ，認証時に利用者にそのリズムパターンを再現させることで認証を行っている．このように行動的特徴を用いた生体認証の中にも利用者へ認証時に登録時のパターンを想起させることで記憶負荷をかける手法が存在する．利用者への利便性を考えたとき，この記憶負荷は排除するほうが望ましい．これに対し，歩行動作 [7] やキーボードの打鍵動作 [8]，ドアの開閉動作 [9]，トイレットペーパーの巻き取り動作 [10] など日常生活における自然な動作をパターン化させずに用いることで認証時に利用者への記憶負荷をかけずに個人を認証・識別する方法が存在する．提案手法で用いるドアノック動作でも認証のために定めた不自然なノックリズムなどをパターン化させて用いることはせず，日常生活における自然なノック動作中に含まれる個人特徴を用いることで利用者への認証時に登録時のパターンを想起させる記憶負荷を排除する．

2.2 スマートドアロックシステムの認証に関する研究

スマートロックに関する研究では，スマートドアロック（SDL:Smart Door Lock）システムについてのものが多く進められている [11] [12] [13] [14]．これらのシステムではそれぞれ独自のドアロックを行うハードウェアと解錠のための手法を提案している．ドアにタッチパネルを搭載した SDL システム [11] では，利用者がドアを解錠する際の認証としてタッチパネルにパスワードを入力する認証方式を提案している．また，ログインしたスマートフォンアプリケーションからワンタイムパスワード方式によるドアロックを解錠する SDL システム [12] なども提案されている．これらはドアロックを解錠する際に，知識認証を用いているためユーザへの記憶負荷が大きい．アクセス権のある端末が設定エリア内に入ると自動的にドアロックを解錠する SDL システム [13] では，ユーザへ認証のための動作を意識させずにシームレスなドアの解錠を実現している．しかし，登録されているアクセス権のある端末を紛失した場合には，Web アプリケーションにログインし，登録端末を削除する必要があり作業が煩雑となる．また，指紋認証を用いてユーザを認証し，ドアロックを解錠する機能も同時に提案されているが，身体的特徴を用いているため，偽造された際の危険性があり，指紋を取得するための特別なデバイスを用いることによる利用者への心理的負担が大きい．ドアに設置した PIR（Passive Infared Ray）モーションセンサを用いてドアの前に人が来たことを検知し，ドアの管理者に通知することで管理者によってドアロックを解錠する SDL システム [14] ではドアの前にいる利用者に認証動作を行わせずドアロックを解錠可能にしているが，既存のドアにセンサを取り付ける設置コストや，通知を受け取った利用者は毎回解錠許可を与えなくてはならない手間がある．佐藤らは，ドアノブに設置した Web カメラを用いた掌紋認証を装備したインジェントドアノブシステムと呼ばれる SDL システムを提案している [15]．これにより，利用者に認証動作を意識させずにシームレスなドアロックの解錠を可能にしている．しかし，一度の認証に対して

SIFT（Scale Invariant Feature Transform）と呼ばれる計算を 150 回行っているため，現状では認証速度が実用的でなく，Web カメラをドアノブに設置するコストも発生する．このように既存の SDL システムでは，利用者の記憶負荷・心理的負担の点や設置コストに問題がある手法が多いため，できる限り利用者の負担が少なく特別な機器の設置が不要な認証方法が必要である．

3. ドアノック型個人認証方式

3.1 提案方式

提案方式では，利用者によるドアノック動作から得られる 3 軸加速度データ，3 軸角速度データを受信して図 1 に示す一連の処理を経て，複数の機械学習における異常検知アルゴリズムを用いて本人を認証する．本稿ではその中から，最適な異常検知アルゴリズムを選択して用いる．認証時は，自宅に設置されたスマートロックと事前に Bluetooth でペアリング済みのスマートフォンが BLE（Bluetooth Low Energy）の近接検知を用いてドアノック動作を取得する．BLE の距離測定を用いることでスマートフォンとスマートロック間の距離が 1m 以上のとき（Far），約 1m のとき（Near），1m 未満のとき（Immediate）を区別して検知することが可能であるため，提案方式では BLE が Immediate を検知した場合にのみドアノック動作による認証を許可する．取得したドアノック動作データはノイズ除去などの前処理を経て，認証のための特徴量の抽出が行われた後，異常検知アルゴリズムによって正常と判断された場合のみ本人として認証する．スマートロックの解錠は利用者が認証された場合のみ行う．提案方式によって，従来のスマートロックの事前にスマートロックと紐付いたスマートフォンを用いて解錠する所有物認証の要素に加え，ドアノック動作による行動的特徴を用いた生体認証の要素を付け加えることで 2 要素認証となるため，認証を強固とすることが可能である．提案方式では，利用者への認証時の記憶負荷を排除するため，従来の行動的特徴を用いた生体認証の研究手法にあるような動作をパターン化させることはせず，日常的に行う自然なドアノック動作から本人固有の特徴量を抽出することで利用者が認証時に登録パターンを想起させる記憶負荷を排除することを目指す．

3.2 想定環境

提案方式では，解錠時のみに着目し，利用者の把持するスマートフォンからドアノック動作の特徴を抽出して，スマートロック解錠のための認証に利用する．この際，ドアには利用者の行動的特徴を検出するためのセンサなどのデバイスを設置せず，近年一般的に広く普及しているスマートフォンに内蔵されているセンサを用いる．身近に存在し，日常的に持ち運ぶデバイスを用いることで，提案方式による新たな専用デバイスを用意する手間や導入コストが削減可能である．スマートフォンでは，3 軸加速度センサと 3 軸角速度センサのデータを取得する．ドアノック動作の様子と各センサの各軸の方向を図 2 に示す．提案方式で用いたスマートフォンの主な仕様を表 1 に示す．動作取得のための Android アプリケーションを Kotlin を用いて開発した．サンプリングレートは 200Hz とした．

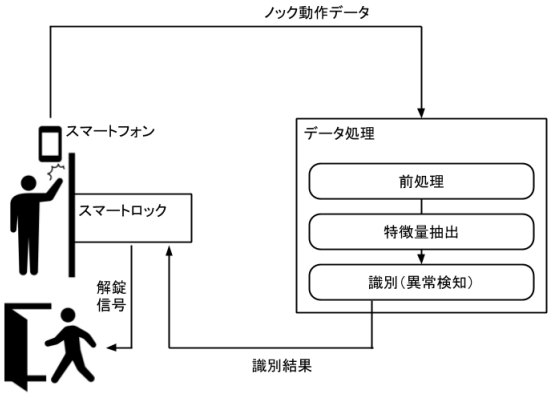

図 1　システム概要図

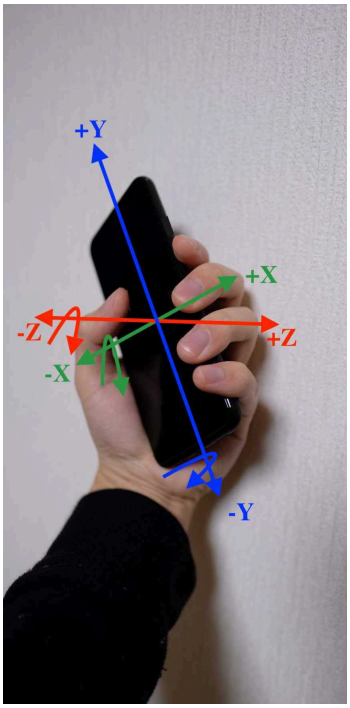

図 2　ドアノック動作の様子と各センサの軸方向

表 1　スマートフォンの主な仕様

項目	仕様
機器	VAIO Phone JCI VA-10J
OS	Android 5.0.2
重量	130g
サイズ	71.3mm x 141.5mm x 7.95mm
センサ	3 軸加速度センサ・3 軸角速度センサ
ディスプレイ	5 インチ
サンプリングレート	200Hz

3.3 前処理

前処理ではまず，実際に動作したデータ以外のノイズを除去するため取得した 3 軸加速度データ，3 軸角速度データの前後のデータの切り取りを行った．その後それぞれローパスフィルターを適用して実際の動作データに含まれる微小なノイズを除去した．その結果を図 3 に示す．

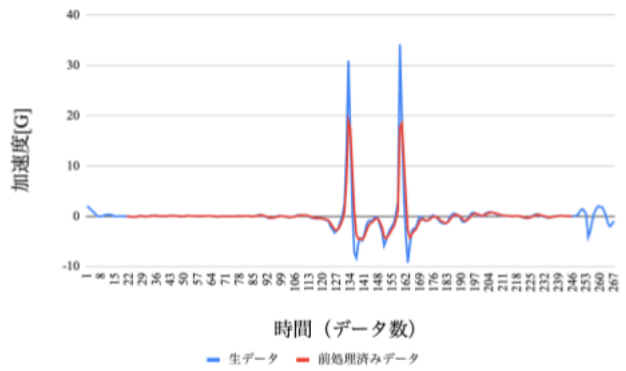

図 3 前処理結果

3.4 特徴量抽出

以上の環境のもとで得られるドアノック動作データから個人認証に有効な特徴量の抽出を行う．我々はこれまでに特別なパターン化させない自然なドアノック動作から個人固有の特徴量を抽出可能であることを示している [16]．結果として，3 軸加速度と 3 軸角速度データから得られる最大値・最小値・平均・標準偏差の基本統計量と加速度データに現れるドアノック時の衝撃ピークであるノックピークから得た特徴量が有効であることがわかっている．しかし，ノックピークから得る特徴量としてノックの数や 1 回毎のノックの高さ・幅などの値をそのまま扱っていることによって特徴ベクトルの次元数が変化するため，特徴ベクトルの分析の仕方によっては同じ利用者でも登録時と認証時でノック数を変えると他人と認証されてしまう可能性が高いと考えられる．提案方式では，ノック時に現れるノックピークのそれぞれの高さ・幅・ノックピーク間の間隔のそれぞれについて平均・標準偏差の値として扱うことでノック数が変更された場合も対処可能にする．ノックピークの抽出には村尾らが提案しているピーク抽出アルゴリズム [17] を用いる．ピーク抽出アルゴリズムを適用した結果を図 4 に示す．ピーク抽出アルゴリズムでは，加速度時系列データの現在時刻 t から過去 Δt 秒間（ウィンドウ）における平均値 $m(t)$ を計算する．これに対し，図 4 に示したように,$m(t)$ の上下に Epsilon tube と呼ばれる領域を $m(t) \pm \epsilon$ の幅で設け，加速度の値が一度 Epsilon tube 域外に出てから再び Epsilon tube 領域内に戻るまでの波形をピークとして抽出する．ドアノック動作では，利用者にスマートフォンの画面を手前にするように把持して行っても

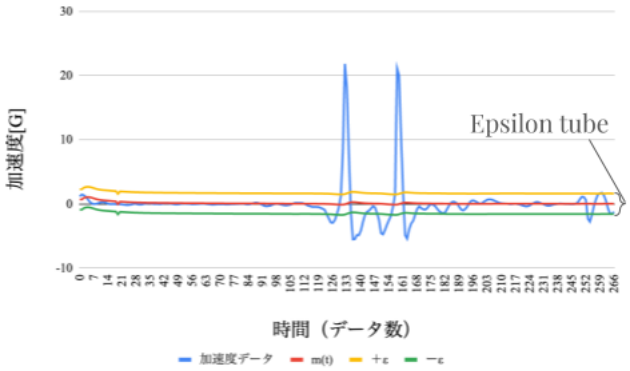

図 4 ピーク抽出アルゴリズム適用

らうため，加速度の z 軸に直接ドアノック時のピークが出現することから z 軸に対してピーク抽出アルゴリズムを適用する．本研究では，それぞれのノックピークの幅と高さの平均・標準偏差と間隔をノックピークからの特徴量として抽出する．加えて，スマートフォンの把持の仕方によって本人を誤って他人と認証してしまうことを防ぐため，3 軸合成加速度データから得られた基本統計量も特徴量として抽出し，3 軸合成加速度データを高速フーリエ変換した周波数スペクトルも特徴量として抽出する．提案方式で用いる可能性のある特徴量の種類を表 2 に示す．これらの特徴量を組み合わせて最終的に表 3 に示す特徴ベクトルパターンを作成してそれぞれ識別に用いる．生成した特徴ベクトルの各要素はスケールが異なり等価に扱うことができないため，それぞれの特徴ベクトルに対し，平均 0，分散 1 になるように正規化した．

表 2 特徴量の種類

特徴量名	特徴量	個数（個）
3 軸加速度	3 軸加速度（最大値・最小値・平均・標準偏差）	12
3 軸角速度	3 軸角速度（最大値・最小値・平均・標準偏差）	12
ノックピーク	ノックピーク幅・高さ・間隔（平均・標準偏差）	6
3 軸合成加速度	3 軸合成加速度（最大値・最小値・平均・標準偏差）	4
周波数スペクトル	3 軸合成加速度の周波数スペクトル	100

3.5 識別

識別では，機械学習の異常検知アルゴリズムを用いる．本人の特徴ベクトルのみを学習した識別器に未知の特徴ベクトルを入力として与えたときに正常（本人）と判断するか異常（他人）と判断するかで認証を行う．提案方式では，異常検知アルゴリズムとして One Class SVM，Elliptic Envelope，Gaussian Mixture Model，Isolation Forest の 4 種類を用いる．

表 3　特徴ベクトルパターン

パターン	特徴量
1	3 軸加速度・3 軸角速度・ノックピーク
2	3 軸加速度・3 軸角速度
3	3 軸加速度
4	3 軸角速度
5	3 軸合成加速度
6	3 軸合成加速度・3 軸角速度・ノックピーク
7	周波数スペクトル
8	3 軸合成加速度・3 軸角速度・周波数スペクトル
9	3 軸加速度・3 軸角速度・周波数スペクトル
10	3 軸合成加速度・3 軸角速度・ ノックピーク・周波数スペクトル
11	3 軸加速度・3 軸角速度・ ノックピーク・周波数スペクトル

4. 評価実験

4.1 実験方法

提案したドアノック型個人認証から得られる特徴量の有効性と，用意した 11 種類の特徴ベクトルパターンと 4 種類の機械学習の異常検知アルゴリズムの最適な組み合わせを評価するため，被験者を用いた実験を行った．実験は，21 歳〜23 歳の男子大学生 7 名に対してそれぞれ 60 試行してもらった．被験者にはスマートフォンを把持したままの手でドアノック動作を行ってもらい，認証を意識した特別なドアノック動作ではなく，日常生活で行う自然なドアノック動作をするように教示して行った．ノック数に関しては我々が過去に行った実験 [16] からドアノック動作についての教示を与えずドアノック動作をしてもらったところ，2 回ノックをする被験者が多く見られたことから，全員全試行でノック数を 2 回に固定して行った．ドアノック時はスマートフォンをノック時の体制に構えてからノック動作を始め，データの計測を開始してからドアノック動作を開始するまでとドアノック動作を終了してからデータの計測を終了するまでは 1 秒程度静止してもらうように指示した．

上記の実験を，公立はこだて未来大学内に設置してある鉄製のドアに対して行い，動作データを取得した．取得した動作データから前述した 11 種類の特徴ベクトルパターンを抽出し，それぞれに対して学習させる異常検知アルゴリズムを 4 種類変えて最適な特徴ベクトルパターンとアルゴリズムの組み合わせと最適な特徴量を評価する．異常検知アルゴリズム 4 種類それぞれに対して全被験者の 11 種類の特徴ベクトルパターンをそれぞれ学習させたときの平均 F 値（F-measure），適合率（Precision），再現率（Recall）で提案手法を評価する．F 値，適合率，再現率は識別器に未知のデータを入力として与えたときの識別器の予測結果によって表 4 に示す TP（True Positive），FN（False Negative），FP（False Positive），TN（True Negative）を用いてそれぞれ式（1），（2），（3）で算出する．本実験においては TP は識別器が本人と予測したデータが実際に本人である数，FN は識別器が他人と予測したデータが実際は本人であった数，FP は識別器が本人と予測したデータが実際は他人であった数，TN は識別器が他人と予測したデータが実際に他人である数を表す．適合率は，識別器が本人と予測したデータのうち実際に本人である割合，再現率は実際に本人であるデータのうち，識別器が本人と予測したデータの割合を表す．F 値はこれらの調和平均を算出した値である．機械学習の異常検知アルゴリズムに設定するパラメータは事前に平均 F 値が最小となるようにチューニングし，本人の試行データ 60 個のうち 40 個を学習用として用いた．

表 4　識別器の予測結果

		予測したクラス	
		本人	他人
実際の	本人	TP	FN
クラス	他人	FP	TN

$$F-measure = \frac{2*(Precision*Recall)}{Precision+Recall} \tag{1}$$

$$Precision = \frac{TP}{TP+FN} \tag{2}$$

$$Recall = \frac{TP}{TP+FP} \tag{3}$$

4.2 実験結果および考察

動作データから抽出した 11 種類の特徴ベクトルパターンにそれぞれ 4 種類の機械学習の異常検知アルゴリズムを適用したときの平均 F 値，適合率，再現率を表 5 に示す．実験の結果，最も精度の良い平均 F 値を算出したのは 3 軸加速度の基本統計量を用いた特徴ベクトルパターン 3 を Gaussian Mixture Model に学習させたときの 0.796 であった．このときの平均適合率は 0.970，平均再現率は 0.752 であった．次に平均 F 値が高かったのは，3 軸加速度，3 軸角速度の基本統計量と 3 軸合成加速度を高速フーリエ変換して得られた周波数スペクトルを用いた特徴ベクトルパターン 9 を Gaussian Mixture Model に学習させたときの 0.764 であった．このときの平均適合率は 0.907，平均再現率は 0.748 であった．このことから，異常検知アルゴリズムとして Gaussian Mixture Model を採用し，特徴量を 3 軸加速度データから抽出すると平均 F 値が高く算出されやすいことがわかった．適合率だけに着目するとどちらも 0.9 台が得られ，識別器が本人と予測したデータ中の本人データの割合が高いことから，他人を誤って認証してしまう可能性は低いと考えられる．実際にスマートロックの認証に利用する際，他人を本人と誤って認証することは住居への悪意のある他人の侵入を許すことにも繋がるためこ

表 5　各特徴ベクトルパターンと異常検知アルゴリズムごとの平均 F 値，適合率，再現率

	One Class SVM			Elliptic Envelope			Gaussian Mixture Model			Isolation Forest		
パターン	F 値	適合率	再現率	F 値	適合率	再現率	F 値	適合率	再現率	F 値	適合率	再現率
1	0.587	0.781	0.500	0.014	0.143	0.007	0.244	0.547	0.169	0.548	0.550	0.714
2	0.558	0.721	0.471	0.051	0.286	0.029	0.205	0.272	0.170	0.559	0.554	0.714
3	0.480	0.543	0.536	0.311	0.876	0.200	0.796	0.970	0.752	0.532	0.459	0.743
4	0.411	0.442	0.436	0.351	0.920	0.221	0.176	0.498	0.137	0.521	0.452	0.764
5	0.322	0.224	0.807	0.380	0.432	0.557	0.673	0.862	0.576	0.442	0.406	0.693
6	0.585	0.733	0.564	0.066	0.429	0.036	0.336	0.541	0.318	0.520	0.482	0.714
7	0.160	0.198	0.414	0.079	0.571	0.043	0.645	0.931	0.535	0.207	0.181	0.714
8	0.581	0.711	0.543	0.000	0.000	0.000	0.432	0.530	0.425	0.261	0.160	0.821
9	0.532	0.776	0.464	0.040	0.286	0.021	0.764	0.907	0.748	0.384	0.268	0.814
10	0.538	0.727	0.471	0.000	0.000	0.000	0.622	0.678	0.587	0.351	0.279	0.800
11	0.585	0.804	0.479	0.063	0.286	0.036	0.420	0.708	0.350	0.418	0.325	0.821

の値は認証に有効であるといえる．平均再現率に着目すると，どちらも 0.7 台であり，このときの平均適合率と比較すると低い結果となった．低い再現率は利用者の認証を否認する割合に繋がるため，実際に認証として利用する場合は利用者への再認証が多くなり利便性に支障が出る．しかし，提案方式のドアノック型認証方式では実験の結果，ほとんどの被験者が前後の静止する時間を含めて認証動作を 3 秒以内に終了していたため，例えばポケットからスマートフォンを取り出してから認証動作を行った場合に認証動作のみを取り出すことができれば認証にかかる時間を削減できる．これは，再認証に関する利用者への負担を従来の行動的特徴を用いた生体認証と比較してごくわずかな負担となり数回の再認証であれば許容できる．

今後は実験の結果から得られた認証に有効な特徴量を手がかりに，更に認証精度の高い特徴量の選択と再認証における利用者の負担に関する再認証回数の限界調査などが課題として挙げられる．また，提案方式ではスマートフォンを把持した手で認証動作を行なったが，ポケットやかばんからスマートフォンを取り出す手間と動作のしにくさが存在することがわかった．今後はこれらを解決するため，近年普及しているスマートウォッチを用いた認証動作の取得とそれに応じた特徴量選択を行っていくことを検討する．スマートウォッチを用いた場合でも今回有効であるとわかった 3 軸加速度データを用いることで同程度の認証精度が得ることができると考えられる．行方らの研究 [4] では加速度センサを搭載した腕時計型端末を用いて腕の動きを認証のための動作として認証を行っている．しかし，この手法では登録時に利用者に認証のための特別な動作を登録させ，認証時にそれを再現させることを前提としている．そこで，提案方式の結果を利用し，利用者の記憶負荷を取り除いた形で実現可能な方式を検討する．

5. おわりに

本研究では，スマートロック解錠のために利用者へ動作をパターン化せずに記憶負荷を無くし，認証時の動作に対する心理的負担を減らした行動的特徴を用いた生体認証としてスマートフォンの 3 軸加速度センサと 3 軸角速度センサを用いたドアノック型認証方式を提案した．本提案手法を用いることで現在スマートロックが行っているスマートロックにペアリングしたスマートフォンによる所有物認証に加えて行動的特徴を用いた生体認証を組み合わせた 2 要素認証とすることで，従来のスマートロック解錠時の認証におけるセキュリティ強度を高めることが期待できる．提案方式では取得した動作データから 11 種類の特徴ベクトルパターンを作成し，それぞれ 4 種類の異常検知アルゴリズムに学習させることで，未知のデータを入力として与えたときに正常（本人）データか異常（他人）データか予測することで認証を行う．

被験者を用いた実験の結果，異常検知アルゴリズムに Gaussian Mixture Model を，特徴量に 3 軸加速度から抽出した基本統計量を用いたとき平均 F 値 0.796，平均適合率 0.970，平均再現率 0.752 が得られた．今後は，実験結果から得られた認証に有効な特徴量を手がかりに，更に認証精度の高い特徴量の選択とスマートフォンを取り出す手間などを排除するためにスマートウォッチを用いた認証動作の取得を検討する．

参考文献

[1] Qrio: Qrio Lock, Qrio（オンライン），入手先 ⟨https://qrio.me/smartlock/⟩（参照 2019-03-09）.
[2] CANDYHOUSE: セサミスマートロック，CANDYHOUSE（オンライン），入手先 ⟨https://jp.candyhouse.co/⟩（参照 2019-03-09）.
[3] 石原　進，太田雅敏，行方エリキ，水野忠則：端末自体の動きを用いた携帯端末向け個人認証，情報処理学会論文誌，Vol. 46, No. 12, pp. 2997–3007 (2005).
[4] 行方エリキ，太田雅敏，石原　進，水野忠則：加速度センサ搭載腕時計型端末を用いた腕の動きによる個人認証，情報処理学会研究報告，Vol. 2003, No. 94(2003-HI-105), pp. 21–26 (2003).
[5] 市村亮太，納富一宏，斎藤恵一：覗き見攻撃耐性を考慮したスマートフォンにおけるリズム認証手法- 楽曲の主旋

律を用いた際の認証精度評価-，マルチメディア、分散協調とモバイルシンポジウム 2013(DICOMO2013) 論文集，Vol. 2013, pp. 230–233 (2013).
[6] 喜多義弘，神里麗葉，朴　美娘，岡崎直宣：マルチタッチ操作を利用したリズム認証方式の検討，情報処理学会研究報告，Vol. 2014-UBI-41, No. 19, pp. 1–7 (2014).
[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] 伊藤駿吾，白石　陽，今野慎介：手首装着型センサを用いた打鍵動作特徴による個人認証手法，マルチメディア，分散協調とモバイルシンポジウム 2016(DICOMO2016) 論文集，Vol. 2016, pp. 1165–1171 (2016).
[9] 光来出優大，林　健太，石田繁巳，田頭茂明，福田　晃：ドアの開閉動作に基づく人物識別手法の提案と初期評価，情報処理学会研究報告，Vol. 2019-UBI-61, No. 32, pp. 1–6 (2019).
[10] 倉橋真也，村尾和哉，寺田　努，塚本昌彦：トイレットペーパの回転に基づくトイレ使用者識別手法，情報処理学会論文誌，Vol. 58, No. 1, pp. 237–248 (2017).
[11] Park, Y. T., Sthapit, P. and Pyun, J.: Smart digital door lock for the home automation, *Proc. 2009 IEEE Region 10 Conference(TENCON2009)*, pp. 1–6 (2009).
[12] Dhondge, K., Ayinala, K., Choi, B. and Song, S.: Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones, *Proc. 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, pp. 251–257 (2016).
[13] Hadis, M. S., Palantei, E., Ilham, A. A. and Hendra, A.: Design of smart lock system for doors with special features using bluetooth technology, *Proc. 2018 International Conference on Information and Communications Technology (ICOIACT2018)*, pp. 396–400 (2018).
[14] Aman, F. and Anitha, C.: Motion sensing and image capturing based smart door system on android platform, *Proc. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pp. 2346–2350 (2017).
[15] 佐藤公則，野間悠希，鹿嶋雅之，渡邊　睦：掌紋認証を装備したインテリジェントドアノブシステムの開発に関する研究，画像の認識・理解シンポジウム (MIRU2011) 論文集，Vol. 2011, pp. 580–585 (2011).
[16] 中鉢かける，中村嘉隆，稲村　浩：スマートロック操作のためのドアノック型個人認証方式の検討，マルチメディア，分散協調とモバイルシンポジウム 2019(DICOMO2019) 論文集，Vol. 2019, pp. 1433–1440 (2019).
[17] 村尾和哉，KristofVanLaerhoven，寺田　努，西尾章治郎：センサのピーク値を用いた状況認識手法とその評価，情報処理学会研究報告，Vol. 2009-UBI-22, No. 11, pp. 1–8 (2009).