「マルチメディア，分散，協調とモバイル
(DICOMO2019)シンポジウム」 令和元年7月

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

中鉢 かける[1]　中村 嘉隆[2]　稲村 浩[2]

概要：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．スマートホームのセキュリティに関するサービスとして，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 Wi-Fi や Bluetooth 経由で行う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，現在のユーザがデバイスの所有ユーザであるかどうかの認証は行っていないため，デバイス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存在する．そこで本研究では，ドアの前で自然に行える動作としてドアのノック動作に注目し，ユーザごとのドアのノック動作の癖などの特徴を用いてスマートロック解錠時におけるドアノック型認証方式の検討を行う．評価実験の結果，等価エラー率の小さな特徴量の選択が可能であることが示され，提案手法は個人認証方式として有効であることがわかった．

Door knock type person authentication method for smart lock system

KAKERU NAKABACHI[1]　YOSHITAKA NAKAMURA[2]　HIROSHI INAMURA[2]

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．スマートホームでは，外出先からスマートフォンを用いて自宅のエアコンを操作するサービスなどが提供される．このようなスマートホームサービスの１つとして，住宅の玄関のドアの施錠・解錠を物理的な鍵なしでスマートフォンアプリを用いて Wi-Fi や Bluetooth 経由で行うスマートロックと呼ばれる技術が存在する．スマートロックはすでに製品化が進んでいるものもあり，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）に外付けすることで，工事不要でスマートロック化できる製品が既に販売されている [1][2]．これらの製品には，スマートフォンアプリにより施錠・解錠する機能，利用者の位置情報を利用してドアに近くだけで解錠が可能なハンズフリー解錠機能や，家族や友人等，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を持つものがある．しかし，これらの機能は玄関ドアの施錠・解錠に関して利便性を向上できる一方，各機能がスマートフォン等のデバイスに紐付けられているのみであり，現在の利用者がデバイスの所有者であるかどうかの認証は行っていないため，デバイス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存在し，これへの対策としてドア付近における個人認証が必要となる．

ドアの前で用いることができると考えられる従来の一般的な認証技術として，所有物認証，知識認証，生体（バイオメトロニクス）認証等がある．所有物認証とは，物理的な鍵や IC カードなど，利用者本人所有の物理的デバイスを用いて認証を行う方法である．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方法である．また，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種類存在する．身体的特徴とは指紋や顔，虹彩などの人体に備わる特徴を用いたものである．行動的特徴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たものである．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

[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

的簡単に認証可能だが，盗難や紛失した場合には本人の認証が不可能となるばかりか，他人に認証を突破される危険もある．知識認証は現在スマートフォンのロック解除など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を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必要性はないが，身体的特徴の変更はほぼ不可能であるために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体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，普段人が意識せずに行っている動作を本人の特徴として用いるため，認証のための記憶負荷や心理的負担が小さい認証方法である．本研究では，行動的特徴としてドアの前で自然に行え，動作のための心理的負担が少ないと考えられるドアノック動作に注目し，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．

2. 関連研究

2.1 行動的特徴を用いた認証・識別

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．端末を用いて空間に文字を書いたり，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，行動的特徴を用いた生体認証としてリズム認証手法に関する研究も行われている [5][6]．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なっている．このように行動的特徴を用いた生体認証の中にも記憶負荷をかけるものが存在する．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せずに用いることでユーザへ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自然な動作中に含まれる個人特徴を用いることが可能である．

2.2 スマートドアロックシステム

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][15]．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操作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法を提案している．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り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やユーザ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 カメラを用いて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 回行なっているため，現状では認証速度が実用的なものではなく，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ものが多いため，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. 提案手法

3.1 アプローチ

本研究で提案するドアノック型個人認証方式は，ドアノック動作という行動的特徴を用いた生体認証に分類される．行動的特徴を用いた生体認証では，2.1 節で述べたように認証動作をパターン化させてしまうことにより，ユーザへ記憶負荷を与えてしまう場合があるため認証動作はできる限りパターン化させない方が望ましい．したがって，提案手法が解決すべき課題として以下の 2 つが挙げられる．

(1) ノックパターン以外のドアノック動作の個人特徴の抽出

(2) ドア側での特別なデバイス設置が不要な特徴検出

課題（1）について，ノック動作自体は利用者がドアの前で自然に行うことができる動作であるが，その際，ノック動作自体に個人の癖が含まれるため利用認証可能な特徴を抽出できる可能性がある．自然に行なったドアノック動作からは，個人によって異なるノック時の腕の動きと，振動パターンによる特徴量を得ることができ，これらは個人の癖による特徴であるため，意識せずとも記憶負荷をかけずに再現可能な特徴となる．

課題（2）について，特徴検出のためにユーザに何らかの機器を装着してもらう必要があるが，本研究では近年広く普及しているスマートフォンを用いてドアノック動作時の特徴を抽出する．

3.2 想定環境

提案手法では，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ノック動作の特徴を抽出し，ドアロック解錠のための認証に利用する．この際，ドアには，利用者の行動特徴を検出するためのセンサ等のデバイスを設置せず，スマートロックシステムで一般的に用いられるサムターン回転のためのデバイスのみを設置することを想定する．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 1 に示す．本研究で用いたスマートフォンの主な仕様を表 1 に示す．

3.3 ドアノック動作の取得

提案手法では，認証時に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う．この方法でドアノック動作をすることにより，ノック時の衝撃などを直接センシング可能であると考える．

表 1 スマートフォンの主な仕様

項目	仕様
機器	iPhone8
OS	iOS 12.1.4
重量	148g
サイズ	138.4mm × 67.3mm × 7.3mm
ディスプレイ	4.7 インチ
センサ	気圧計・3 軸加速度センサ・3 軸角速度センサ・接近センサ・照度センサ

3.4 特徴量の抽出

以上の環境のもとで得られるドアノック動作のデータから個人認証に有効な特徴量の抽出を行う．ドアノック動作は認証に用いることができる動作時間が短い傾向にあるため，短時間で個人差の大きい特徴量を用いる必要がある．

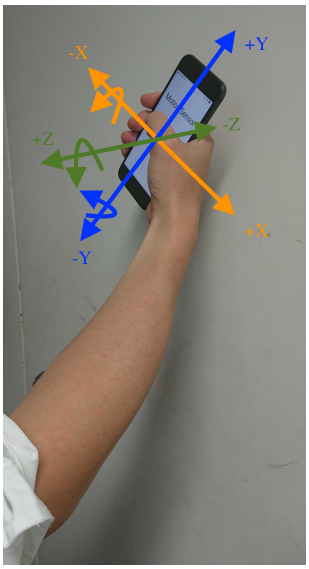

図 1 ドアノック動作の様子と各センサの軸方向

また，スマートフォン搭載のセンサを用いて特徴を検出できる必要がある．一般的なスマートフォンに搭載されているセンサとしては，気圧計，3 軸加速度センサ，3 軸角速度センサ，近接センサ，照度センサ等がある．このうち，動作を検出する際に有用と考えられるのは 3 軸加速度センサ，3 軸角速度センサであり，これらを用いて検出した特徴量について検討する．図 2〜図 7 はそれぞれ 2 名の被験者によるドアノック動作の加速度・角速度の変化を 3 軸加速度センサ，3 軸角速度センサで取得した結果である．3.2 節で述べたスマートフォン把持方法を採用した場合，加速度（図 2，図 3）については，被験者によらずノック動作時に Z 軸方向に大きなピークが見られている．また．各軸のグラフの形状については，被験者間にある程度の差異が見られている．一方，角速度（図 4，図 5）については，被験者ごとにグラフの形状に加え，大きなピークが見られる軸も異なっている．この結果より，各被験者のノック動作時における手首の回転等の癖が現れているといえる．図 6 図 7 は被験者 A から得られた別の加速度と角速度データである．図 2 と図 6 を比較するとノック時のピーク大きさやそのピークの頂点の出現間隔，各軸の波形が類似していることがわかる．角速度データである図 4 と図 7 を比較するとこちらも各軸の波形が類似していることがわかり，本人間ではノック動作ごとに類似した特徴が現れており，認証に用いることが可能であると考えられる．

次に，ノック動作時における加速度・角速度の各軸に出現しているピークについて検討する．これらのピークは一度のノック動作に伴って出現するため，このピークの間隔や大きさが個人を識別するための特徴量として用いることができる．実際のノック時の衝撃によるピークは直接加速度によって検出可能であると考える．以降，加速度のピークに着目し，加速度データに現れるノック動作時のピーク

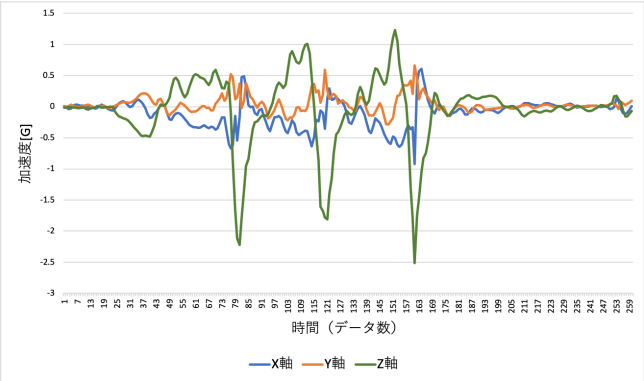

図 2　被験者 A の 3 軸加速度データ

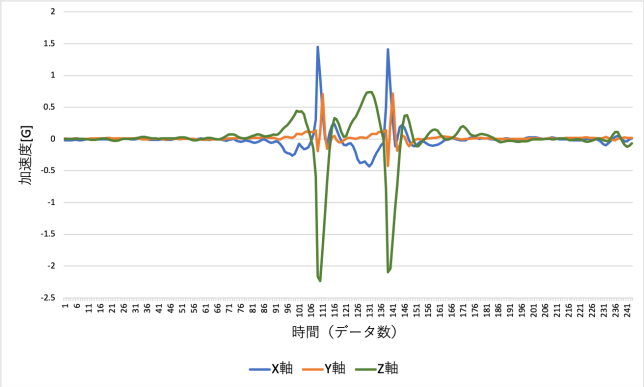

図 3　被験者 B の 3 軸加速度データ

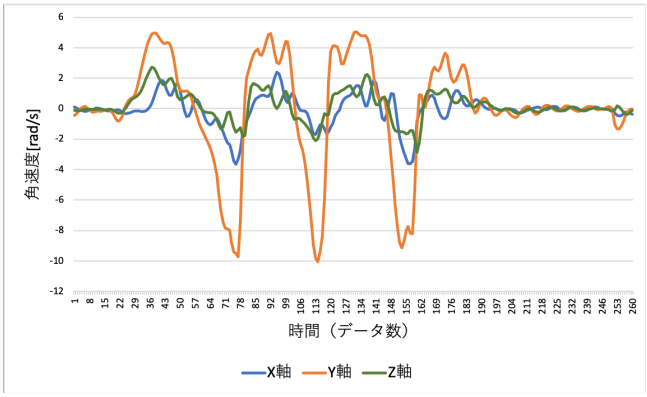

図 4　被験者 A の 3 軸角速度データ

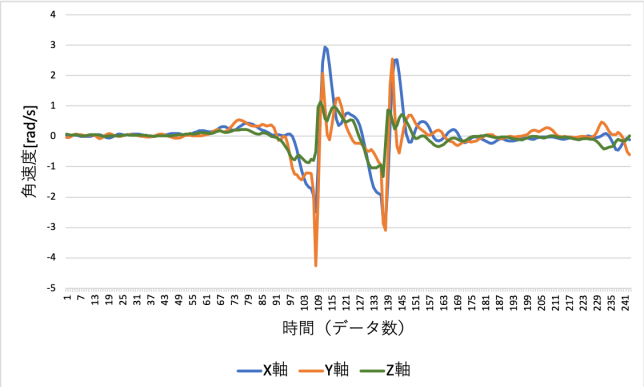

図 5　被験者 B の 3 軸角速度データ

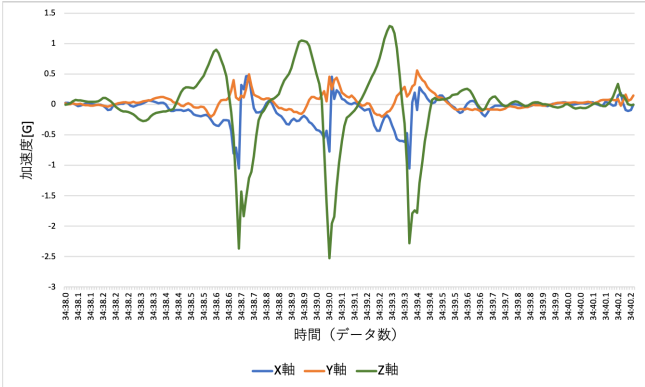

図 6　被験者 A の別の 3 軸加速度データ

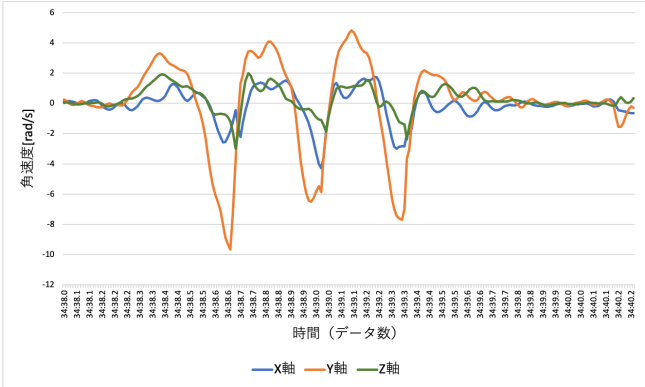

図 7　被験者 A の別の 3 軸角速度データ

をノックピークと呼ぶ．加速度センサから得られた加速度の時系列データからノイズなどのピークを排除してノックピークのみを抽出するために，村尾らが提案しているピーク抽出アルゴリズム [16] を用いる．このアルゴリズムでは，まず取得した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，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．3.3 節で取得した実験データから被験者 A の Z 軸加速度データをローパスフィルターにかけた上で，ピーク抽出アルゴリズムを適用した結果を図 8 に示す．

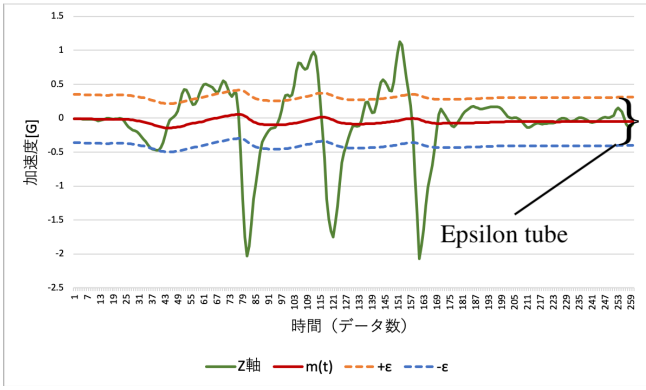

図 8　ピーク抽出アルゴリズム適用（被験者 A の 3 軸加速度データ）

また，利用者ごとにスマートフォンの持ち方が変わり，ノックピークが出現する軸が異なることが考えられる．3 軸の合成加速度データを用いることで考慮しなくても済むが，波形が複雑になりノックピークのみを検出することが困難になる．そこで，3 軸のどの軸のノックピークが最大であったかは，各軸データの分散値 $varX$，$varY$，$varZ$ をもとに，以下の (1) 式で算出する．

$$axis = max(varX, varY, varZ) \tag{1}$$

上記の被験者 A のデータでは $axis = varZ$ が得られる．

ピーク抽出アルゴリズムにより得られる特徴量を図 9 に示す．本稿では，ノックピークの高さ，幅，1 度ノックピークが出現してから次のノックピークが出現するまでの各ノックピークの頂点の間隔を特徴量として用いる．ノックピークの高さは波形が一度 Epsilon tube 域外に出てから再び Epsilon tube 内に戻るまでの間の頂点の値とし，ノックピークの幅はその時のデータ数とした．ノックピーク間隔はノックピークの頂点と次のノックピークの頂点が出現するまでのデータ数とした．加速度，角速度の 3 軸それぞれの最大値・最小値・平均値・分散値・標準偏差と，これらのノックピークの特徴量を要素として生成する特徴ベクトルを表 2 に示す．ノックピーク以外に用いる特徴量の選出には既存の研究 [9][8][10] を参考にして行なった．これにより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，特徴ベクトル x に対し，平均 0，分散 1 になるように正規化した．

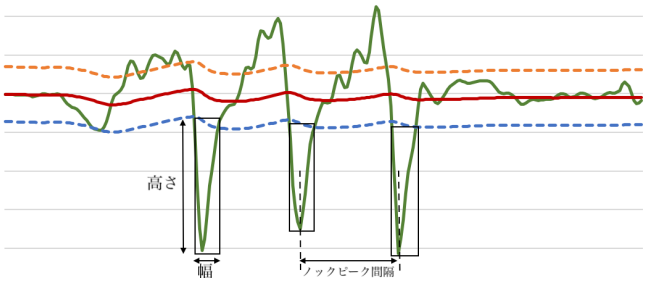

図 9　ピーク抽出アルゴリズムで得られる特徴量

表 2　特徴ベクトルの内容

特徴量	個数（個）
最大値（加速度 3 軸・角速度 3 軸）	6
最小値（加速度 3 軸・角速度 3 軸）	6
平均（加速度 3 軸・角速度 3 軸）	6
分散（加速度 3 軸・角速度 3 軸）	6
標準偏差（加速度 3 軸・角速度 3 軸）	6
ノックピーク数	1
ノックピーク高さ	ノックピーク数
ノックピーク幅	ノックピーク数
ノックピーク間隔	ノックピーク数 - 1

3.5　特徴ベクトル間の類似度算出方法

正規化後の特徴ベクトルを用いて，ベクトル間の類似度（距離）を算出する．本稿で扱う特徴ベクトルは表 2 で示したように，ノックピーク数に応じて次元数が異なってしまうため，片方の時系列データにおける一点をもう一方の時系列データの複数の点に総当たりに対応づけることで時間方向の非線形な伸縮が可能となる方法である DTW(Dynamic Time Warping)[8] を用いる．これにより，次元数の異なるベクトル同士の類似度の算出も可能である．この時，被験者ごとに動作登録として取得した動作データの中から認証時に用いるマスタデータを 1 つ選出する方法として石原ら [3] の提案している方法を参考にする．複数の動作データの中から i 番目の試行データから抽出した特徴ベクトルを $M_i(i = 1, 2, \cdots, 10)$ とする．M_i と $M_j(j = 1, 2, \cdots, 10)$ の DTW の距離を D_{ij} とし，それぞれの試行データとの DTW 距離の二乗和 $(\sum_{j=1}^{10} D_{ij}^2(i \neq j))$ を最小とする M_i をマスタデータとする．DTW で算出した特徴ベクトル間の類似度が事前に定めた閾値よりも低ければ認証成功とし，閾値よりも高ければ認証失敗とする．

4.　評価実験

4.1　実験環境

提案したドアノック型認証から得られる特徴量の中から有効な特徴量の組み合わせを評価するため，20〜23 歳の男子大学生 8 名に対して評価実験を行なった．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なってもらった．ノックの回数，リズム，強さは被験者ごとに自然な動作で行なってもらった．

ノック動作は短い時間で行われる動作であり，従来の認証方式と比較すると高い認証精度を出すのが困難であることが予想される．そこで，本人間でノックのやり方が大きく異なると他人と判断される可能性が高くなることが考えられるため，2〜10 回目の試行では 1 回目の試行とノックのやり方を意図的に大きく変えずに行なってもらうように指示した．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データの計測を終了するまでは 1 秒ほど静止してもらうように指示した．

上記の実験を，図 10 に示す公立はこだて未来大学内のある鉄製ドアに対して行い，同一スマートフォンの各センサのサンプリングレートを 200Hz として動作データを取得した．

4.2　実験結果および考察

実験の結果得られた被験者ごとのノック数を表 3 に示す．被験者全体で 2，3，4 回の 3 パターンでドアノック動作をしたことがわかった．ノックの回数が異なる被験者同

図 10　実験に用いたドア

士では個人認証が容易になると考えられる．被験者 A とその他の被験者との DTW 距離の比較を図 11 に示す．被験者 A はノック動作を 3 回しており，同じ 3 回ノック動作をしていた被験者 B との DTW 距離は他の被験者と比べると類似した動作となり，DTW 距離が近くなっている．またノック動作回数が異なる被験者 C〜H と比較すると，被験者 B と比較して DTW 距離が離れることがわかった．

また，被験者 D〜H のノック動作回数は 2 回と共通しているため，被験者 E と他のノックを 2 回行なった被験者との試行回数ごとの DTW 距離の比較を図 12 に示す．

表 3　被験者ごとのノック動作回数

被験者	A	B	C	D	E	F	G	H
ノック数	3	3	4	2	2	2	2	2

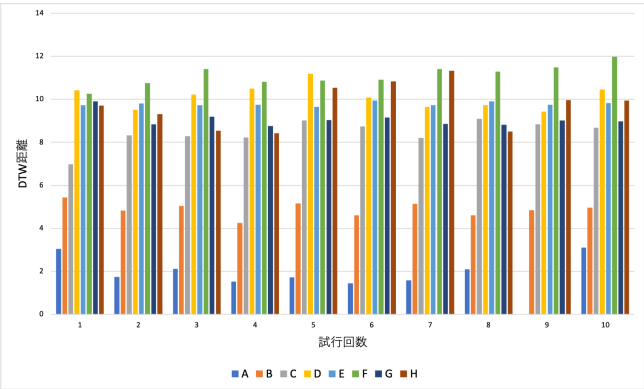

図 11　被験者 A と他の被験者との DTW 距離の比較

同じ 2 回ノック動作をした被験者同士でも本人と他人では大きな差異があることがわかった．したがって，図 12 に現れた差にはノック数以外の特徴量が有効に働いている

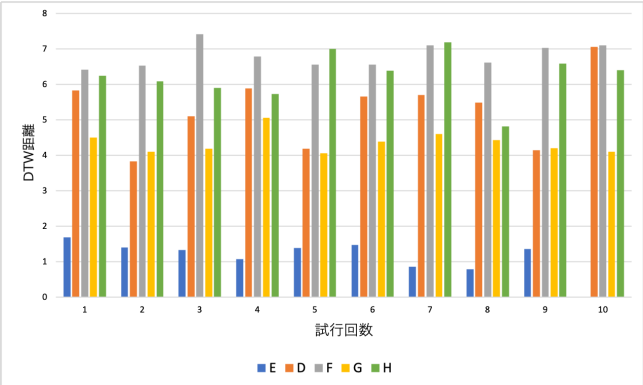

図 12　被験者 E と同一ノック回数の他の被験者との DTW 距離比較

と考えられる．

認証では，本人拒否率（FRR:False Reject Rate）と他人受入率（FAR:False Accept Rate）および FRR と FAR が等しくなる等価エラー率（EER:Equal Error Rate）を求めることができる．FRR とは，同一人物同士の類似度を算出した際に閾値よりも大きくなる割合であり，認証動作を行なったのが本人であるにも関わらず他人と判断して認証失敗としてしまう割合のことである．EER は生体認証の研究においてその手法の精度を評価する際に一般的に使われる指標であり，値が小さいほど認証精度は高い．特徴量ごとの認証精度とどの特徴量が有効であるかを確認するため，表 4 に示す特徴量パターンごとに EER を算出し，結果を表 5 に示す．

表 4　特徴ベクトルの内容

特徴量パターン	特徴量
1	3 軸加速度（最大値・最小値・平均・分散・標準偏差）
2	3 軸角速度（最大値・最小値・平均・分散・標準偏差）
3	3 軸加速度・3 軸角速度
4	ノックピーク（数・高さ・幅・間隔）
5	3 軸加速度・ノックピーク
6	3 軸角速度・ノックピーク
7	3 軸加速度・3 軸角速度・ノックピーク

表 5　特徴量ごとの EER

		特徴量パターン							平均
		1	2	3	4	5	6	7	
被験者	A	0.15	0.12	0	0.20	0.11	0.13	0	0.10
	B	0.07	0.07	0.04	0.12	0.10	0.08	0	0.07
	C	0.14	0.16	0	0	0	0	0	0.04
	D	0	0.21	0.10	0.27	0.27	0.30	0.22	0.20
	E	0.06	0.05	0.02	0.04	0.03	0.22	0	0.06
	F	0	0.11	0.11	0.05	0.02	0	0.01	0.04
	G	0	0	0	0.30	0.02	0	0	0.05
	H	0.07	0.13	0.13	0.19	0.21	0.08	0.07	0.13
平均		0.06	0.11	0.05	0.15	0.1	0.1	0.04	

全体的に見ると被験者と特徴量パターンによっては EER の値が 0 になっている箇所があり，ドアノック動作が認証として有効であることが示唆された．特徴量パターンごと

の被験者間の平均 EER を見ると，特徴量パターン 7 を採用した際に，最小 EER0.04 が得られた．既存の個人認証に関する研究 [18] では EER0.05 以下は他人に模倣されにくいと評価される数値であり，特徴量パターン 7 は本人認証に対して有効である．特徴量パターン 7 の次に被験者全体で平均 EER が小さかったのは加速度と角速度のデータを含んだ特徴量パターン 3 であった．このため，ノック動作の加速度および角速度には本人認証に有効な情報が潜在的に含まれていると言える．一方，特徴量パターン 4 のノックピークのみの特徴量を特徴ベクトルとして用いた時が一番 EER が大きくなり，ノックピーク単体のデータだけでは高い認証精度を出すために用いることは難しいことがわかった．しかし，ノックピークのみを除いた特徴量を特徴ベクトルとした特徴量パターン 3 よりもノックピークも含んだ特徴量パターン 7 の方が EER の値が小さかったことから，ノックピークを特徴量として加速度と角速度のデータと組み合わせる特徴ベクトルは個人認証に有効であると考えられる．

4.3 今後の課題

本実験では被験者から得られたノック数が 2，3，4 回であり，その中でもノック数ごとに被験者の偏りがあったため，今後被験者を増やした上，ノック数ごとに被験者の偏りを無くして再度，正確に特徴量の分析をする必要がある．また，今回は各被験者がノック数を固定して実験を行なったが，ユーザが日常で認証を行う際に登録時と認証時ではノック数が異なることが考えらるため，その時の認証精度に関する実験が必要である．

ドアノック動作によるスマートロック解錠は，スマートフォンのロック解除の認証と比べて頻度が低く，一度の認証の重要度が極めて高いと考えられ，FRR よりも FAR を低く抑えることが重要である．そのため，認証判定に用いる閾値の導出には KinWrite[19] の手法のように，その時点で得られているデータの中の全ての本人データと他人データを比較し，一番 DTW の距離が小さいものを閾値とすることで，その時点では FAR を 0 にする方法を用いることが考えられる．

また，被験者を増やした上で，FRR と FAR の評価や特徴量ごとの重要度の算出，覗き見られた場合のなりすまし攻撃による耐性，経年変化によるノック動作の再現性に関する調査などが課題としてあげられる．

5. おわりに

本研究では，スマートロック解錠のためにユーザへ物理的な鍵が不要で記憶負荷や心理的負担がない認証方式としてドアノック型認証方式を提案した．ユーザは自然に行えるノック動作で認証が可能なため，パスワードを入力するなどの記憶負荷や，認証動作に対する心理的負担が少ない．悪意のある他者にスマートフォンを盗難された場合もノック動作を完全に模倣されなければ住居への侵入を防ぐことが期待できる．本手法では，一般的に認証で用いられる加速度・角速度の特徴量の他に，ユーザがスマートフォンを把持した手でノック動作をして得られた加速度データからノックによるピーク（ノックピーク）のみを抽出して特徴量として用いて特徴ベクトルを生成し，DTW により類似度を算出した．ノックピークから抽出される特徴量として，ノックピークの数・高さ・幅・間隔を用いた．

評価実験の結果，平均 EER が 0.04 を達成する特徴量パターンが得られ，ドアノック動作が認証動作として有効であることが示唆された．

今後の課題として，今回はノック数ごとに被験者の偏りがあったため，今後は被験者を増やした上，ノック数ごとに被験者の偏りを無くして再度特徴量の分析や認証精度の評価をする必要がある．また，今回は各被験者がノック数を固定して実験が行なったが，ノック数を変えた場合の認証精度を確認する必要がある．他には，ノック動作を覗き見られた場合のなりすまし攻撃による耐性や，経年変化によるノック動作の再現性に関して調査することなどがあげられる．

参考文献

[1] Qrio Lock(オンライン), 入手先 ⟨https://qrio.me/smartlock/⟩（参照 2019-03-09）.

[2] CANDY HOUSE SESAMI(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 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-MBL-70, 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, pp109-122(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 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] Y. T. Park, P. Sthapit, and J. Pyun: Smart digital door

lock for the home automation, Proceedings of the IEEE TENCON 2009 Singapore, pp.1-6(2009).
[12] K. Dhondge, K. Ayinala, B. Choi, and S. Song,: Infrared Optical Wireless Communication for Smart Door Locks Using Smartphones, Proceedings of the 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN 2016), pp.251-257(2016).
[13] M. S. Hadis, E. Palantei, A. A. Ilham, and A. Hendra: Design of smart lock system for doors with special features using bluetooth technology, Proceedings of the International Conference on Information and Communications Technology 2018 (ICOIACT 2018), pp.396-400(2018).
[14] F. Aman and C. Anitha: Motion sensing and image capturing based smart door system on android platform, Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS 2017), 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] 村尾和哉，クリストフファンラールホーフェン，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, 情報処理学会論文誌, Vol.51, No.3, pp.1068-1077(2010).
[17] 西郷里拓，川本淳平，櫻井幸一：加速度センサを用いたスマートフォンの筆跡認証の性能向上, 火の国情報シンポジウム, Vol.2015, pp.1B–1(2015).
[18] 飛世速光，村尾和哉，寺田努，磯俊樹，塚本昌彦，堀越力：圧力センサを用いた把持ジェスチャによる携帯端末の個人認証手法, マルチメディア、分散協調とモバイルシンポジウム 2014 論文集, Vol.2014, pp.1027-1034(2014).
[19] J.Tian, C.Qu, W.Xu, and S.Wang: KinWrite: Handwriting-Based Authentication Using Kinect, Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS Symposium 2013), (online), available from ⟨https://www.ndss-symposium.org/wp-content/uploads/2017/09/10_2_0.pdf⟩ (2013).