

# リズム感の違いを利用した個人認証方式の開発と評価

高瀬 由梨<sup>1,a)</sup> 野本 一輝<sup>1</sup> 飯島 涼<sup>1</sup> 森 達哉<sup>1,2,3</sup>

**概要:** スマートフォン等のモバイル端末は、公的サービス等の社会インフラにアクセスするために欠かせないものであり、個人認証技術の導入が必要不可欠である。一方、これらの端末において、多様なユーザーのニーズを満たす単一の個人認証方式は存在しない。例えば、高次脳機能障害を持つユーザーは、知識ベースの個人認証技術を使うことは困難である。また、ブルカやニカブを着用して顔を隠すスリムの女性は、公の場で顔認証技術を利用することはできない。本研究は、上述したような従来の個人認証技術の利用に困難を抱える人を含む、広く多様なユーザーにとって使いやすい、包摂的な個人認証技術の開発を試みる。提案する個人認証技術のアイデアは、個々のユーザーが持つ「リズム感」の違いを活用することにある。リズム感の違いを指先を用いたタップで表現する個人認証方式「リズムタップ」を開発し、その認証精度とユーザビリティを評価する。7人の実験協力者が参加した実験の結果、平均 99.8% の精度で認証が成功した。

**キーワード:** ユーザ認証, スマートフォン, リズム, ユーザビリティ

## Development of a Personal Recognition Scheme Using Differences in the Senses of Rhythm

**Abstract:** Mobile devices such as smartphones have become indispensable for accessing social infrastructures such as public services, making the introduction of personal recognition technology essential. On the other hand, there is no single personal recognition method that meets the needs of a wide variety of users of these devices. For example, there are users who have difficulty using widely used fingerprint and face recognition technologies for various reasons. In this study, we attempt to develop a personal recognition scheme that is inclusive and easy to use for a wide variety of users. The idea of the proposed personal recognition scheme is to take advantage of the differences in "sense of rhythm" that each user has. We develop a personal recognition scheme named "Rhythm Tap," which expresses the difference of rhythm sense by tapping with a fingertip, and evaluate the accuracy and usability of the recognition. We evaluated the proposed method on seven normal participants, and found that the proposed method succeeded in authentication with an average accuracy of 99.8%.

**Keywords:** User recognition, Smartphones, Rhythm, Usability

### 1. はじめに

2008年のスマートフォン国内販売から15年が経過し、商品やサービスの購入、SNSの利用、マイナンバーカードを用いた公的サービスへのアクセスなど、スマートフォンは社会的基盤として必要不可欠なものになった。スマートフォンの利用率は2022年時点で90%を超え、世代を問わず幅広いユーザーに利用されている[1]。スマートフォンに

は、SNSやメールをはじめとするメッセージ内容、カメラや動画画像など、多くの個人情報が格納されているため、個人認証方式の導入が必要不可欠である。現在、スマートフォンに用いられる個人認証方式として、Personal Identification Number (PIN)、パターンロック、パスコード、指紋認証、顔認証などがある[2], [3], [4], [5], [6]。

前述した個人認証方式は、必ずしもすべてのユーザーにとって使いやすいとは限らない。例えば、PINやパスワード方式は、指定された箇所への入力に時間がかかることが報告されている[7]。スマートフォンでは、ランダムな文字列のパスワードを入力するのに7.5秒かかり[8]、スマート

<sup>1</sup> 早稲田大学 / Waseda University

<sup>2</sup> 情報通信研究機構 / NICT

<sup>3</sup> 理化学研究所 革新知能統合研究センター / RIKEN AIP

<sup>a)</sup> yuri@nsl.cs.waseda.ac.jp

フォン利用に慣れていない人にとって、望ましいシステムとは言えない。また、高次脳機能障害を持つユーザにとって、パスワードを記憶することは困難である。四肢障害などの身体的な理由、あるいはブルカやニカブを着用したムスリムの女性など、宗教的な利用により、指紋認証や顔認証などのバイオメトリクス認証の利用が困難であるケースは多数存在する。

本研究は既存の個人認証方式を使うことが困難である人を含む、多くのユーザにとって使いやすい、包摂的な個人認証技術の開発を目的とする。本研究が提案する個人認証技術「リズムタップ」は、指先のタップを用いる行動バイオメトリクス認証である。リズムタップの技術的アイデアは、個々のユーザが持つ「リズム感」の違いを活用することにある。リズム感には個人差があることが報告されており [9]、その個人差を個人識別に利用することができると期待される。リズムタップの個人認証においては、はじめにユーザは複数のリズムパターンを、画面や背面などをタップすることによって登録する。認証は、以下に示すようなチャレンジレスポンス方式である。ユーザからの認証要求を受けると、システムはリズムパターンをランダムに選択し、その一部をユーザに提示する（音や振動として再生）。ユーザは提示されたリズムパターンに続くリズムパターンを応答としてタップし、システムは入力されたパターンと予め登録されたパターンを照合する。

リズムパターンの精度およびユーザビリティを評価するために、22 歳から 54 歳までの実験協力者 7 名によるユーザスタディを実施した。この結果、99.8% の高い精度で個人認証が実現できることを明らかにした。また、System Usability Scale (SUS) [10] を用いたユーザビリティ評価の結果、平均スコアが 72 となり、Rank B に相当する比較的高いユーザビリティを達成することがわかった。

## 2. 背景

本章では、はじめに現在使われている個人認証技術の概略を示す。つぎに、それらの個人認証技術に共通する課題を論じる。

### 2.1 個人認証技術の概略

現在、スマートフォンや PC といったモバイル端末において認証を行なう際によく利用されている個人認証方式はさまざまである [11]。例えば、最も一般的な個人認証方式として、パスワード認証があり、数桁の英数字や記号を組み合わせることで認証を行なう。また、SMS 認証、ワンタイムパスワードといった一時的なパスワードを利用した認証を行うこともある。生体認証としては、指紋認証があり、指紋センサーにユーザが直接触れることで認証を行なうことができ、指紋の縞模様を特徴量として利用する照合

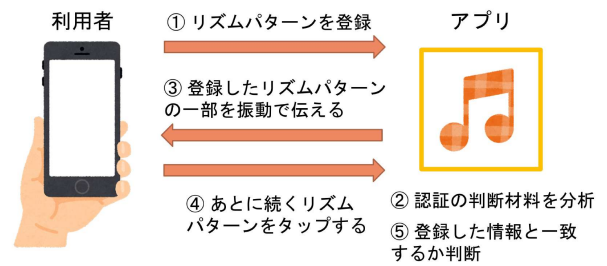


図 1 概要イメージ図

方式が一般的である [12]。その他、顔認証、虹彩や静脈を使った認証方式も利用される。

### 2.2 個人認証技術の課題

パスワードや PIN コードを用いた認証では、人間が複雑な情報を正しく記憶できることが前提になっている。様々な文字種を含み、十分な長さがあり、辞書的な意味を一切もたないランダムに構成されたパスワードが強度が高いパスワードであるが、そのようなパスワードを記憶することは容易ではない。年齢や高次脳機能障害などにより、情報の記憶が困難なユーザには、知識ベースの個人認証技術を使うことは難しい。また、前章で議論したように、バイオメトリクスは知識の記憶を必要としないユーザビリティが高い個人認証技術として広く普及しているものの、身体的、あるいは宗教的な理由により、その利用が困難であるユーザは少なくない。広く、多様なユーザが便利に個人認証技術を使うためには、上記の課題を解決する包摂的な個人認証方式を開発する必要がある。

## 3. 提案手法

本章では、2 章で論じた個人認証技術の課題を解決することを狙いとして、多様なユーザにとって使いやすい個人認証方式リズムタップを提案する。リズムタップは端末の要求に応じて応答が変化するチャレンジレスポンス認証方式を採用している。

### 3.1 概要

リズムタップ認証の概要イメージ図を図 1 に示す。はじめに、ユーザが自分の好きなリズムパターンでスマートフォンの画面、側面、背面をランダムにタップすることで、システムに認証情報を登録する。認証を行なう際には、登録したリズムパターンの一部が振動でユーザに伝えられるので、その後続くリズムパターンを登録したときと同じようにユーザがタップする。このとき、タップしたリズムパターンが登録されたリズムパターンと一致すれば、認証成功となり、一致しない場合は、認証失敗となる。

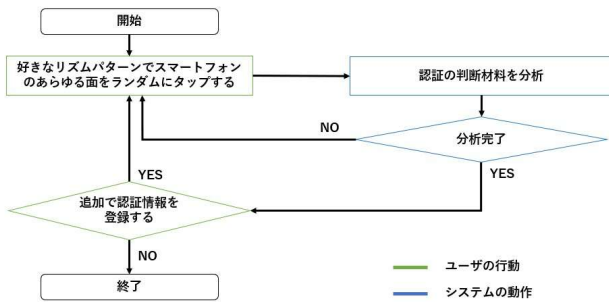


図 2 登録手順

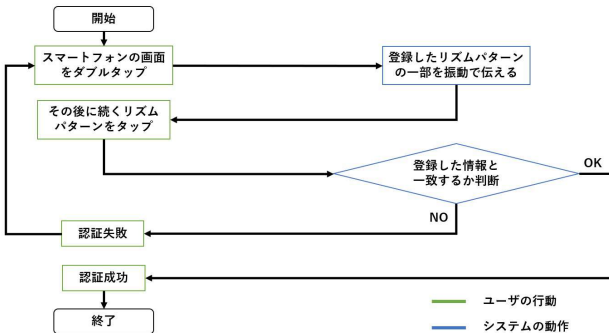


図 3 認証手順

表 1 ユーザごとの実験条件

ユーザ	条件	タップした面
User1	A	画面
User2	A	画面
User3	A	画面
User4	B	画面
User5	B	画面
User6	B	画面
User7	B	画面

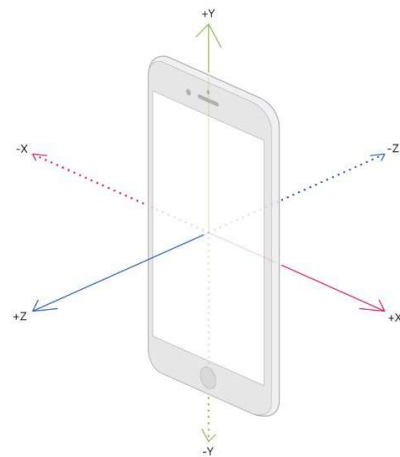


図 4 加速度の軸方向

### 3.2 システム概要

リズムタップは認証情報の登録フェーズと認証の試行フェーズの 2 段階に分けられる。

(1) 認証情報の登録フェーズ：ここでは、ユーザが自身で考えたリズムパターンでスマートフォンの画面、側面、背面を自由にタップすることで認証情報の登録を行なう。提案手法では、曲のリズムパターンが認証情報となる。登録手順は図 2 に示す。なお、図 2 の左側がユーザの動作、右側がシステムの動作を表す。まず、ユーザ側が曲の数フレーズのリズムパターンでスマートフォンの画面、側面、背面をランダムにタップする。すると、システム側はそのユーザがタップした際の重力を除く加速度の値を常時取得し、さらに、各音符と休符をタップする長さを分析する。システム側の分析が終了するまで、ユーザは繰り返し同じようにタップを行なう。分析することで、その情報を認証の判断材料 (タップする強さ、タップするタイミング、タップする角度) として利用する。なお、認証情報は最低 2 パターン、最大 5 パターン登録することが可能である。

(2) 認証の試行フェーズ：リズムタップは、登録フェーズでユーザが登録したリズムパターンを用いて、チャレンジレスポンス認証による認証を行なう。ユーザは複数のリズムを登録し、システムはその内どれかをランダムに選んでユーザに一部を提示することで、チャレンジレスポンス認証を実現する。認証手順は図 3 に示す。まず、ユーザが認証を開始したいタイミングで、スマートフォンの画面をダブルタップするとシステムが起動する。すると、開始音が鳴り、予め登録されたリズムパターンのうち、あるリズ

ムパターンの一部がスマートフォンから振動でユーザに伝えられる。その後ユーザは、システムから伝えられたリズムパターンの後に続くリズムパターンを実際に登録した際と同じようにタップする。そして、タップしたリズムパターンが登録されたリズムパターンと一致すれば、認証成功となり、完了音が鳴る。一致しない場合は、認証失敗となり、失敗音が鳴るので、再度スマートフォンの画面をダブルタップし、もう一度認証を行なう。

## 4. 認証精度評価実験

本章では、リズムタップの認証精度を評価する。

### 4.1 実験概要

実験にあたり、重力を除く加速度と経過時間を収集するアプリを実装した。参加者を募り、実装したアプリを用いて、リズムパターンをタップした際の加速度データを収集した。得られた結果から、加速度のピークなどの情報を検出し、目的を達成するために分析を行なう。

システムの実装環境は Andorid Studio で言語は Kotlin を使用した。実験で使用したスマートフォンは Huawei 社の Android 端末で、機種は HUAWEI P20 lite である。

参加者は健康者 7 人を対象とし、内訳は男性 4 人、女性 3 人で、年齢の幅は 22 から 54 歳であった。7 人のうち 4 人が大学生、1 人が主婦、2 人が会社員である。

参加者を以下の 2 つのグループに分け、それぞれ異なる

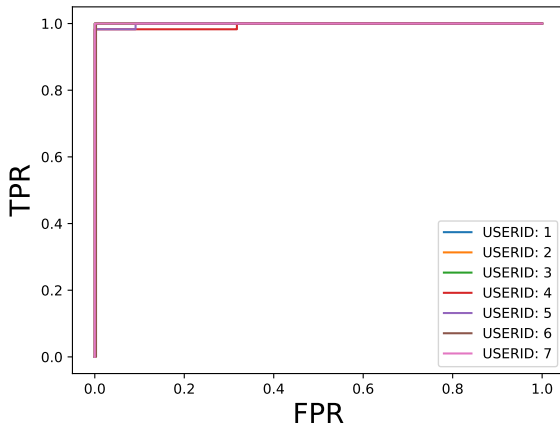


図 5 ROC 曲線

タスクの実験を行った。

- (A) ユーザはある曲の指定された箇所のリズムパターンをタップする
- (B) ユーザは自由に決めた曲の箇所のリズムパターンをタップする

A グループでは、ユーザごとに小節数の等しいリズムパターンが指定される。B グループでは、ユーザは自由に曲を決めることができ、自由にリズムパターンを決めることもできる。なお、参加者は表 1 に示したように割り振って実験を行なった。

実験手順は以下の通りである。

- (1) ユーザが対象となる音声データ (曲) を最大 5 回聞く。
- (2) ユーザがタップする曲のリズムパターンを自分自身が納得のいくまで練習する。
- (3) ユーザの練習が終わったらシステムを起動し、そのリズムパターンを 1 日に 200 回計測する。

タップしている際には、システムが X 軸方向と Z 軸方向の重力を除く加速度の値を常時取得する。スマートフォンとそれぞれの軸の関係を図 4 に示す。ユーザが画面、背面をタップした際は Z 軸方向に、側面をタップした際は X 軸方向に加速度のピークが現れる [13]。

各ユーザがリズムパターンをタップする際に使用したスマートフォンの面を表 1 に示す。今回は全員画面のみの 1 箇所でのリズムパターンをタップした。そして、得られた結果から特徴量を抽出し、モデルを作って評価を行なった。

#### 4.2 SVM による識別精度の評価

認証精度を評価するため、機械学習モデルの一種である SVM による識別方法を適用した。取得した Z 軸方向の加速度データから tsfresh を利用して特徴量を抽出する [14]。tsfresh は、時系列およびその他の連続データから特徴量を抽出するためのツールであり [15]、さまざまな時系列の長さをサポートしている。3 つの scikit-learn 互換トラン

表 2 Z 軸方向の加速度データから抽出する特徴量一覧

フレーム数
中央値
平均値
最大値
最小値
最大絶対値
データの長さ
標準偏差
最初に現れる最大値の位置
最後に現れる最大値の位置
最初に現れる最小値の位置
最後に現れる最小値の位置
サンプルエントロピー
0 次~9 次の自己相関係数
サポート 1, 3, 5, 10, 50 のピーク数

表 3 SVM によるユーザごとの識別精度

ユーザ ID	Accuracy Score	F1 Score	AUC	EER	EER threshold
1	1.0000	1.0000	1.0000	0.0000	0.5300
2	1.0000	1.0000	1.0000	0.0000	0.7529
3	1.0000	1.0000	1.0000	0.0000	0.8207
4	0.9976	0.9913	0.9945	0.0166	0.0893
5	0.9929	0.9734	0.9984	0.0166	0.0778
6	0.9976	0.9915	0.9972	0.0028	0.6467
7	0.9976	0.9915	1.0000	0.0000	0.5128
平均	0.9980	0.9925	0.9986	0.0051	0.4865

スフォーマーが含まれており、時系列からの特徴抽出と特徴選択を既存の機械学習パイプラインに簡単に組み込むことができる。抽出した 27 個の特徴量を表 2 に示す。サンプルエントロピーは、近似エントロピーを修正したもので、時系列データの複雑さの尺度である [16]。自己相関係数は、指定されたラグの自己相関を計算したものである。ある時系列データと数タイムステップずらしたそのデータの間の相関を自己相関といい、例えば 1 次の自己相関係数は 1 タイムステップずつずれたデータの自己相関係数である。ピーク数は、時系列データのピーク数を計算したものである。今回は時系列データの少なくともサポート 1, 3, 5, 10, 50 のピークの数抽出した。

特徴量を抽出したデータセットに正解ラベル (1) と不正解ラベル (0) を追加し、70% を学習データ、30% をテストデータに分割する。また、グリッドサーチを利用して linear カーネル、RBF カーネルのハイパーパラメータを最適化する。その後、学習データを SVM に入力して、モデルを作成する。この操作を参加者ごとに行い、最終的に 7 個のモデルを作成した。そして、テストデータをそれぞれのモデルに入力して認証テストを行い、正解率 (Accuracy Score), Area Under the Curve (AUC), Equal Error Rate (EER), EER threshold といった評価指標を算出した。算出した評価指標を表 3 に示す。Accuracy Score は平均で 0.9980、つまり 99.8% の精度でユーザを認証できた。AUC は平均で 0.9986 となり、モデルによる予測性能が非常に高いといえる。AUC を算出する際に描いた Receiver Operatorating Characteristic (ROC) 曲線は図 5 に示す。EER は平均で 0.0051 となり、他人受入率 (FAR)

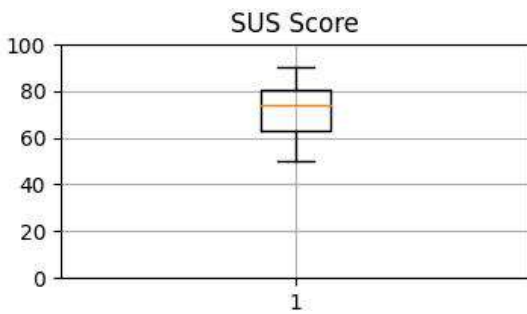


図 6 ユーザごとの SUS スコア

と本人拒否率 (FRR) の値が小さいほど良いため、EER は小さいほど性能が良いといえる。また、適合率と再現率のトレードオフ関係に着目し、モデルの品質を評価するため、2つの値を調和平均 F1 Score も算出した。平均で 0.9915 となり、性能が非常に良いといえる。算出した評価指標については 6.4 節で議論している。

## 5. ユーザビリティ評価

本章では、リズムタップのユーザビリティを評価する。選択式の設問と自由回答から構成される質問紙を作成した。性能評価実験に参加した参加者を対象に質問紙を用いた調査を行なった。

### 5.1 ユーザビリティ評価方法

本研究はシステムのユーザビリティを評価する手法として System Usability Scale (SUS) [10] を採用する。SUS は、肯定的な質問と否定的な質問を交互に繰り返し、総合的にユーザビリティを測定する方法である。実験参加者は各質問に対して 5 段階 (1: まったくそう思わない - 5: まったくそう思う) で回答する。得られた回答から、肯定的な質問の場合は、ユーザのスコアから 1 を引く。否定的な質問の場合は、5 からユーザのスコアを引く。そして、各質問の点数を計算し、これらの総計に 2.5 を掛けることで、100 を基準とした SUS スコアを算出する。

ユーザビリティ評価の参加者は認証精度評価実験の参加者 7 名の内、6 名であった (男性 4 人、女性 2 人、年齢は 22 - 54 歳)。調査では、本実験の内容ならびにリズムタップの認証フェーズについて評価した。

### 5.2 ユーザビリティ評価結果

ユーザ毎に得られた SUS スコアの箱ひげ図を図 6 に示す。なお、User1 は開発者自身であるため、ユーザビリティ評価には参加していない。平均解答時間は 5 分だった。SUS スコアの最小値は 50、最大値は 90 で、平均が 72 であった。SUS の標準スコアは 68 であり [17]、リズムタップは満足度の高い結果を得られたといえる。

図 7 に設問に対する回答の統計を示す。質問ごとの結果を見ていくと、No.1 「この提案方式をしばしば利用したい

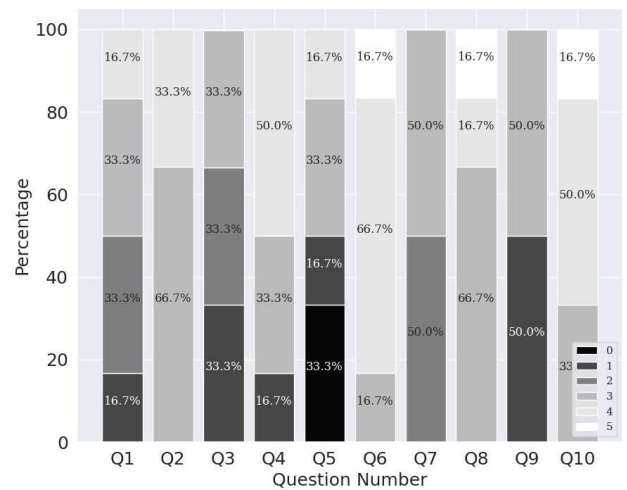


図 7 回答状況

と思う」や No.3 「この提案方式は容易に使いこなすことができると思った」という質問に対しては、回答にバラつきがあった。また、音楽に携わった経験がある、あるいは音楽が好きな参加者が多く、No.9 「この提案方式を利用できる自信がある」に対してポジティブな回答をする傾向が高かった。自由記述式の設問では、リズムタップに対する意見として、「自分のリズム感がどれくらい通用するのか気になる」という回答もあった。このような回答に対しては、同じようにタップできていることをフィードバックする仕組みを振動などによって設けることで、ユーザの懸念を払拭できると考えている。以上のように、ユーザが本認証方式を採用する基準として、リズムに対する親しみやすさなどの要素により個人差があることが示唆される。個人差はあるものの、「スマートフォンの習熟度による親しみやすさ、使いやすさの差異」は見られないことから、本方式は、お年寄りや子どもなど、スマートフォンを使いこなすのが困難な子どもにも利用可能な個人認証として普及が可能であると考えている。習熟度とユーザビリティに関する調査は、今後の課題とする。このようなギャップをより詳細に理解し、ギャップを埋める方式を開発することは今後の課題である。

## 6. 議論

### 6.1 制限事項

以下では、本研究の内容における制約事項を述べる。

実験参加者：リズムタップは、多様なユーザにとって使いやすい個人認証方式であることを目的としている。本研究の実験およびユーザビリティ評価の参加者は全員健常者であり、従来の個人認証技術に困難を抱えるユーザ (障害者等) に参加していただくことが出来なかった。また、日頃からスマートフォンを頻繁に利用している 20 代が過半数以上を占め、年齢層にも偏りがあった。今後は障害者を持つ方を含む、従来の認証技術の利用に困難を抱える幅広

い世代の参加者を対象に実験を実施する予定である。  
実験で使用したシステム： 今回の実験は、スマートフォンをタップすることによって加速度センサの値を取得し、単純な認証精度を評価することに焦点を当てて研究を実施した。そのため、チャレンジレスポンス認証としての実装は行わずに実験を行っている。また、ユーザビリティ評価の時点においても、リアルタイムで認証・フィードバックができる形での実装となっていなかった。しかし、実際は通知音によるナビゲーションやチャレンジレスポンス認証の要素なども踏まえて評価していただくべきであるため、本研究では、リズムタップの認証方法や利用方法をアンケート前に説明することでユーザビリティ評価を実施した。

具体的には、参加者が SUS の質問項目に目を通す前に、リズムタップについての説明書を読んでいただくことで、実験の内容に加えてリズムタップの内容にも目を通してもらった。そして、リズムタップへの理解度を確認し、参加者はリズムタップの認証方法や利用方法を理解した上でユーザビリティを評価した。今後は、リズムタップの実装を進め、実際にナビゲーション等を搭載した個人認証技術を用いてユーザビリティ評価を行なっていく。

提案手法の評価方法： リズムタップの評価において、考慮不足な点について議論する。例えば、騒音の中やユーザの移動中に、認証を行なう場合、ユーザのリズム感に影響が出る可能性がある。また、ユーザはスマートフォンの振動からリズムを正しく感じられるか、第三者がタップ動作を盗み見することで、認証情報を推測できるかについて検討する必要がある。そして、今回は、参加者ごとに条件を統一するため、画面のみの 1 箇所ではリズムパターンをタップした際の加速度データによる評価を行なった。実際は側面や背面をタップするユースケースもデザイン段階で検討していることから、他の場所をタップした際の加速度データを考慮する必要がある。上記の課題について、今後、実験を行なって評価する。

また、リズムタップのシステムの機能にもいくつか課題が挙げられる。まず、ユーザのタップによる加速度とは異なる、外的要因による加速度が計測されてしまう可能性がある。例えば、電車や車などの乗り物の揺れなどである。上記の問題を解決するためには、加速度データのうち、ノイズとなる成分を除去する手法を検討する必要がある。また、ユーザごとにリズム感が異なるため、タップするタイミングの許容範囲をどこまで設けるかを個人ごとに最適化することが好ましいと考えている。さらに、取得した加速度データはシステムに入力する前に、最初のピーク値を揃える必要がある。本研究では、この作業を手動で行っていたため、今後自動化を検討する。例えば、Scipy の `find_peaks` 関数のように、ピーク検出が行える関数を用いて最初のピークを検出し、セグメント化を行うアプローチが考えら

れる。ピーク検出を行う際のしきい値の決定法の確立、別のピークを誤って検知することを回避するノイズ除去の適用は今後の課題である。

## 6.2 提案手法のユーザビリティ評価

リズムタップのユーザビリティ評価を SUS を用いて行ない、5章で述べた通り、スコアの平均は 72、標準偏差は 14.63 であった。しかし、自由記述式の設問では、「急いでいるときには別の個人認証手法を利用したい」という回答もあった。リズムタップは比較的多くの人にとって使いやすいものの、利用する基準は人によって大きく差があると考えられる。そして、SUS のスコア自体にもバラつきがあったため、すべてのユーザのニーズを満たすためには、さらなる改善が必要であることが分かった。

## 6.3 提案手法の利点

以下ではリズムタップの利点を考察する。まず、リズムタップはタップできる範囲が限定されていないため、認証に利用できるデバイスの箇所が広く使いやすいと考えられる。また、リズムベースのチャレンジレスポンス認証を適用することで、認証に用いる音楽(チャレンジ)を変更してレスポンスの変更が可能であること、個人差が大きいリズムという特徴を用いることで模倣データの用意が難しいことから、セキュリティ強度も高められる可能性がある。そして、自分の好きな曲をリズムパターンに用いればパスワードを覚える労力を軽減することも可能である。さらには、ユーザが自分の好きな曲のリズムパターンでスマートフォンの画面、側面、背面をランダムにタップするため、他人が正確に模倣することは困難である。また、使用される曲やフレーズ、それに伴うリズムパターンは無数に考えられるため、推測は困難である。もし万が一盗作された場合でも登録情報(リズムパターン)の変更は容易である。上記した利点はいずれも仮説を含む。実験を通じた仮説の検証は今後の課題である。

## 6.4 提案手法の認証精度評価結果

リズムタップの認証精度を評価した結果、99.8% の高い精度でユーザを認証できることを示した。しかし、表 3 に示した通り、User4, 5 は EER threshold の値がそれぞれ 0.0893, 0.0778 と他のユーザに比べて極端に低かった。そのため、実利用の際には他人受入率が高い可能性が高く、模倣攻撃が成功しやすい可能性がある。実際、User1 の新たに取得したデータを各ユーザのモデルに入れてみたところ、User1 のモデル以外に User4, 5, 6 のモデルでも本人と識別された。認証の可否のしきい値を EER の点ではなく、FAR が低くなる点に変更するなどの対策が考えられる。また、実験参加者の人数が足りず、得られたデータ

数が十分でなかったため、学習データが少ないことから、表 3 に示した通り、極端に良い結果が得られている可能性が高い。また、取得したデータの切り出しを手動で行なったため、タップ以外の部分が特徴として反映されている可能性がある。今後は、実験参加者の数を増やしてさらに多くのデータを収集し、データの切り出しを自動化したうえで SVM を適用し、認証精度を評価する。

本研究は、tsfresh を利用して特徴量を自動抽出した。これらの特徴量はリズムタップにおけるデータの時系列の特徴を反映していないものが多数である。今後は既存研究を参考にし、タップする強さ、タップするタイミング、タップする角度といった認証の判断材料となり得る特徴量を作成したうえで認証精度を評価する [18]。

## 6.5 倫理的配慮

ユーザスタディを行った際、個人名が第三者に特定されることがないこと、参加は自由意志であり拒否における不利益はないこと、ならびに本研究の目的と内容を参加者に対して事前に説明し、同意を得た上で調査と実験を実施した。

## 7. タップを用いた既存の個人認証方式

著者らの知る限り、タップを認証した方式は研究事例が少なく、唯一 Chen ら [19] の研究が挙げられる。Chen らは、ユーザがデバイスの画面上で一連のリズム的なタップ、スライドを用いた個人認証方式を提案した。Chen らの個人認証方式と比較した、リズムタップ認証の大きな利点は、加速度データなど、よりタップの違いを細かく表現できるアナログ量を利用している点である。Android SDK から得られるタップ情報、スライド情報など、Chen らの提唱するデジタル量を利用した個人認証と比較して、ユーザごとのリズム表現の差が現れやすい。本研究では、今後ジャイロセンサなどの値を導入することで、さらに細かく個人ごとの差を抽出できるよう工夫を行う。さらに、本研究では、画面上のタップ情報を利用しないため、画面がオフの状態でも、加速度センサの値をバックグラウンド取得することにより認証を利用することができる利点がある。従来の個人認証方式のほとんどは、認証を開始するために画面をオンにする必要があり、電源ボタンの確認に手間がかかる状態であった。

## 8. まとめ

本研究は、多様な人々に使いやすい個人認証技術として、「リズムタップ」を開発した。リズムタップのアイデアは、個々のユーザが持つ「リズム感」の違いを活用することである。リズムタップを Android アプリとして実装し、7人の協力者が参加した実験の結果、平均 99.8% の高い精

度で認証が成功することを明らかにした。また SUS を用いたユーザビリティ評価の結果、SUS の平均スコアが 74 となり、Rank B に相当する比較的高いユーザビリティが確認された。本研究は包括的な個人認証技術の確立を目指したものであり、1 章で述べたような個人認証技術の利用にあたって様々な困難を抱えているユーザにとっても使いやすい技術であることを狙いとしている。実際にそのような困難を抱えるユーザを対象とし、ユーザスタディを通じてリズムタップの有効性を評価すること、およびデータの登録から、リアルタイムの認証まで End-to-End で動作する個人認証システムとしてリズムタップを実装することは今後の課題である。

謝辞 本研究の一部は JSPS 科研費 22K19782 の助成を受けたものです。

## 参考文献

- [1] 総務省. 令和 3 年版 情報通信白書. <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd111100.html>, jul 2022.
- [2] Nathan L Clarke, Steven M Furnell, Philip M Rodwell, and Paul L. Reynolds. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, Vol. 21, No. 3, pp. 220–228, 2002.
- [3] 石黒司, 福島和英, 清本晋作, 三宅優ほか. モバイル端末のロック解除向けパターン認証の安全性評価. 研究報告コンピュータセキュリティ (CSEC), Vol. 2012, No. 41, pp. 1–6, 2012.
- [4] L. O’Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, Vol. 91, No. 12, pp. 2021–2040, 2003.
- [5] 笹川耕一. 指紋による個人認証. *生体医工学*, Vol. 44, No. 1, pp. 15–19, 2006.
- [6] 今岡仁, 早坂昭裕, 森下雄介, 佐藤敦, 広明敏彦. 顔認証技術とその応用. *NEC 技報*, Vol. 63, No. 3, pp. 26–30, 2010.
- [7] Shuqi Liu, Wei Shao, Tan Li, Weitao Xu, and Linqi Song. Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, Vol. 125, pp. 103–120, 2022.
- [8] Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, NordiCHI ’14, p. 461–470. Association for Computing Machinery, 2014.
- [9] 郡未来, 松田浩一, 海賀孝明, 長瀬一男ほか. 地域伝統舞踊におけるリズム感の個人差抽出. 第 68 回全国大会講演論文集, Vol. 2006, No. 1, pp. 103–104, 2006.
- [10] Georgia Gallavin. System usability scale (sus): Improving products since 1986. <https://digital.gov/2014/08/29/system-usability-scale-improving-products-since-1986/>, feb 2022.
- [11] パナソニック EW ネットワークス株式会社. 認証方式の種類を比較! それぞれの仕組みや選び方を解説. <https://panasonic.co.jp/ew/pewnw/solution/column/network/025.html>, nov 2022.
- [12] 日本電気株式会社. 指紋認証・指静脈認証とは : 指紋・指静脈認証 — nec.

- <https://jpn.nec.com/biometrics/fingerprint/about.html>,  
aug 2022.
- [13] Apple. Getting raw accelerometer events.  
[https://developer.apple.com/documentation/coremotion/  
getting\\_raw\\_accelerometer\\_events](https://developer.apple.com/documentation/coremotion/getting_raw_accelerometer_events), aug2022.
- [14] Read the Docs. tsfresh.  
<https://tsfresh.readthedocs.io/en/latest/>, feb 2021.
- [15] Maximilian Christ, Nils Braun, Julius Neuffer, and Andreas W. Kempa-Liehr. Time series feature extraction on basis of scalable hypothesis tests (tsfresh – a python package). *Neurocomputing*, Vol. 307, pp. 72–77, 2018.
- [16] Joshua S. Richman, Douglas E. Lake, and J.Randall Moorman. Sample entropy. In *Numerical Computer Methods, Part E*, Vol. 384 of *Methods in Enzymology*, pp. 172–184. Academic Press, 2004.
- [17] Hadi Alathas. How to measure product usability with the system usability scale (sus) score.  
<https://uxplanet.org/how-to-measure-product-usability-with-the-system-usability-scale-sus-score-69f3875b858f>, nov 2018.
- [18] Hongliang Bi, Yuanyuan Sun, Jiajia Liu, and Lihao Cao. Smartear: Rhythm-based tap authentication using earphone in information-centric wireless sensor network. *IEEE Internet of Things Journal*, Vol. 9, No. 2, pp. 885–896, 2022.
- [19] Yimin Chen, Jingchao Sun, Rui Zhang, and Yanchao Zhang. Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. In *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2686–2694, 2015.