「マルチメディア，分散，協調とモバイル
(DICOMO2021) シンポジウム」 令和3年6月-7月

活動量と移動中のGPS/Wi-Fiログの相関を利用したライフスタイル認証手法

宮澤 晟[1]　トラン フン タオ[1]　山口 利恵[1]

概要：近年，従来の知識認証，所持物認証および生体認証に加わる新たな認証手法として，個人の行動履歴を複数組み合わせて認証に用いるライフスタイル認証が提案されている．これまでのライフスタイル認証の研究では，多要素認証の際に要素ごとのスコアを独立して計算し最終的な認証に用いることが多く，それぞれの要素の相関を用いてこなかった．我々は相関を活用することが有効と考え，現在広く普及しているデバイスである活動量計とスマートフォンから収集可能な歩行中の活動量と GPS 位置情報・周囲の Wi-Fi アクセスポイントの情報という異なる認証要素の相関を利用する手法を提案したが，先に提案した手法では GPS・Wi-Fi の計測が定期的に行えない場合に認証精度が極端に低下するという課題が存在した．この問題は，OS の制約上，ユーザの移動中のみしか位置情報の収集が行えない iOS 端末において，本手法を適用する際の大きな障壁となっていた．本論文では，移動中に収集した少数の GPS・Wi-Fi 情報のみを用いた場合でも認証精度が低下しないよう手法を改善し，この問題を解決した．ライフスタイル認証の実証実験である MITHRA プロジェクトで収集した iOS/Android ユーザ双方が含まれるデータに対して本手法を適用し，等価エラー率 (EER) が 0.13 と，先の提案手法と比較してほぼ同程度の認証精度を達成した．

Lifestyle Authentication Using a Correlation between Activity and GPS/Wi-Fi Data on Movement

AKIRA MIYAZAWA[1]　TRAN PHUONG THAO[1]　RIE SHIGETOMI YAMAGUCHI[1]

1. はじめに

近年，スマートフォン等のデバイスの普及に伴い，ますます多くのユーザがデジタルデバイスを使用し，その中で決済情報などの機密情報をやり取りするようになっている．そうした背景の中で，正規ユーザとそうでないユーザを識別し，不正なアクセスを防ぐ認証技術に対する関心がますます大きくなっている．

従来から存在する個人を識別するための認証手法として，パスワードなどの知識情報を用いた認証手法，キーカードなどの所持情報を用いた認証手法，指紋などの生体情報を用いた認証手法という 3 つの手法が存在する [1]．これら従来の 3 種の認証手法に加わる第 4 の認証手法として，個人の種々の行動データを用いて認証を行う行動認証や，それらを複数組み合わせて多要素認証を行うライフスタイル認証が近年提唱されている [2]．これらの認証手法は従来の認証手法と比較して認証情報の窃取が難しいという利点や，認証を行うためにユーザに明示的なアクションを求める必要がないという利点が存在する．

ライフスタイル認証や行動認証の例として，スマートフォンの操作や持ち方の個人差を認証に用いる手法 [3], [4]，活動量計によって計測した身体・行動情報の特徴を認証に用いる手法 [5], [6]，GPS や Wi-Fi のログを用いて行動情報を抽出し認証に用いる手法 [7], [8] といった複数の手法がこれまでに提案されてきた．

ライフスタイル認証や行動認証の研究では，認証対象者を識別するための手法として，認証対象者のみのデータを一定期間使用し個人の認証テンプレートを生成する手法 [7], [9], [10] と，認証を分類問題として捉え，認証対象者と他人のデータを両方用意して SVM (Support Vector

[1] 東京大学大学院 情報理工学系研究科 〒 113–8656 東京都文京区本郷 7-3-1

Machine) 等の教師ありの分類手法を用いて分類する手法 [6], [11] という 2 つの手法が主に用いられてきた．しかし，これらの手法はどれも大量の事前データを必要とするという課題があった．また，複数の認証要素を組み合わせる際，これまでは要素ごとのスコアを独立して計算し最終的な認証に用いることが多く，個別の認証要素間に存在するはずである相関を用いてこなかった．例えば，同一ユーザから収集した GPS 位置情報と加速度センサの情報の間にはある種の相関がある（ユーザが GPS 位置情報で移動中の場合，加速度情報にも変化が現れる等）と考えられるが，多くの既存研究ではこれらのセンサ情報を別個に扱い，認証スコアも別々に計算した上で最終的な認証判断に用いることが多かった．

先の研究 [12] では，スマートフォンから収集した GPS/Wi-Fi 情報と，同一人物から収集した活動量計の活動情報の間の相関を利用したライフスタイル認証手法を提案した．しかし，この手法では OS の制約上データの定期的な収集が難しい iOS 端末において，認証精度が極端に低下してしまうという問題が存在したため，実験では Android 端末のユーザのデータのみを使用していた．

本論文では，この手法を改良し，移動中に収集した少数の GPS/Wi-Fi 情報を基準に認証を行うよう変更することによって，GPS/Wi-Fi 情報の定期的な収集が難しい端末であっても，従来の提案手法と同程度の認証精度を実現できるライフスタイル認証の一手法を提案する．

2. 関連研究

2.1 行動認証

ライフスタイル認証，およびそれを構成する行動認証は知識情報，所持情報および生体情報を用いた従来型の認証手法に加わる第 4 の認証手法として提唱されている [2]．近年では，スマートデバイスの普及に伴い，こうした認証手法が積極的に研究されている [5], [11], [13]．以前は，個人の行動の特徴を収集するために専用のデバイスを身につけてもらう必要があり，実世界への応用という点で大きな障壁となっていた．しかし，現在では多種多様なセンサ類の搭載したスマートフォンやスマートウォッチといった機器が普及したため，個人への負担が殆どない形で各種行動データを収集することが可能となった．こうした背景により，今まで大きな課題であった実世界への応用も解決の兆しが見えるようになっている．

ライフスタイル認証・行動認証の既存研究について，認証要素・データの取得方式・認証結果の生成方式の 3 つの視点から分類し以下に述べる．

2.1.1 認証要素による分類

行動認証の既存研究は，利用している認証要素に着目して主に 3 つの種類（生体情報・デバイス操作・位置情報）に分けることができる．

生体情報

従来の生体認証は，指紋や虹彩といった個人で不変の特徴を，専用のセンサで読み取り認証を行うという手法であった．こうした手法は容易かつ精度良く個人を認証できる一方で，事前の登録プロセスが必要であるという課題や，プライバシーの懸念といった問題も存在している．行動認証における生体活動を用いた認証では，従来の生体認証で使用されるような時不変であると考えられる特徴を用いるわけではなく，時間を経て変動する特徴を用いて認証を行う．このような生体情報は，指紋等とは異なり，それ自体が個人を識別できる特徴ではないが，ある期間（例えば，1 日）の変動の特徴を用いることで，個人を識別することが可能となる．生体情報に着目した既存研究として，歩容に着目しているもの [9], [13] や複数種の活動データ（消費カロリー，歩数，心拍数等）を組み合わせるもの [6] が挙げられる．

デバイス操作

デバイス操作による認証では，個々人のデバイス操作の傾向の違いを用いて認証を行う．例えば，2000 年の Monrose ら [10] の研究では，PC のハードウェアキーボードのキーストロークの個人差から個人を識別する手法が提案されている．その後，スマートデバイスが普及したことで，スマートフォンにこうしたデバイス操作の個人差を用いて認証を行う手法が適用されるようになった．このような手法として，スマートフォンのキー入力の個人差を用いて認証を行う手法 [14] や，タッチ操作の個人差を用いて認証を行う手法 [3], [4] が提案されている．

位置情報

位置情報を用いた認証では，GPS データや Wi-Fi のアクセスポイント情報といった，直接的・間接的にユーザの位置情報と結びつく様々な情報を利用し，認証に活用する．一般に，毎日決まった場所を訪れるなど，人間の行動パターンには規則性があるため，こうした行動パターンを位置情報から取得することで個人認証が可能となる．こうした認証の例として，周囲の Wi-Fi アクセスポイントの状態に着目し，その傾向を用いてユーザの行動パターンを割り出し，認証に用いる手法が提案されている [7], [8]．また，GPS 位置情報とその位置情報に結びつく住所に着目し，その傾向を用いて認証を行う手法も提案されている [15]．さらに，位置情報を取得する手段として GPS や Wi-Fi の情報を利用するのではなく，周囲の IoT デバイスの情報を利用する手法も提案されている [16]．

2.1.2 データの取得方法による分類

データ収集の観点において，これまで提案されてきた行動認証の研究は，単一のデバイスから取得したデータを用いるものと，複数のデバイスから取得したデータを総合するものという 2 つの種類に大別できる．

単一のデバイスを用いたデータ取得は，スマートデバイスが普及する前から広く用いられており，例えばユーザのキー入力の傾向を認証に用いる研究 [10] や歩容パターンを認証に用いる研究 [9] など，比較的古い研究においてよく見られる手法である．一方で，ここ数年では複数種類のセンサを搭載した時計型のスマートデバイスが広く普及し，身につける人も次第に増加している．従来のスマートフォン等に搭載されたセンサによるデータに加えて，これらのウェアラブルデバイスに搭載されたセンサも用いて行動認証を行うことで，単一デバイスの場合と比べてより良い精度で行動認証を行うことができるようになると期待される．

そのため，近年ではこうした複数デバイスのセンサデータを用いた行動認証の研究も徐々に増えてきており，その例として，Lee ら [17] によるスマートフォンとスマートウォッチ双方の加速度センサとジャイロスコープを用いた行動認証の研究が挙げられる．[17] では，複数のデバイスに搭載されている同じ種類のセンサデータを認証に用いることで，単一のデバイスのデータのみを使うときと比べて認証精度が改善されたと結論づけている．この手法を更に発展させ，モデル生成に機械学習を取り入れて複数デバイスの認証を実現している手法 [18] も存在する．

2.1.3 認証結果の生成法による分類

行動認証では，一定期間のユーザの行動を記録したものを認証に活用するが，行動認証の既存研究における認証結果の生成手法には大きく分けて 2 種類の手法が存在する．

1 つ目の手法として，認証対象者のデータを認証開始前に一定期間収集し，それを基に個人の認証テンプレートを生成し，新たな入力と比較することで認証を行うという手法がある．このようなテンプレートベースの手法は，認証テンプレートの生成に認証対象者本人のデータのみしか必要としないため，実用化がしやすいというメリットがある．一方で，人の行動は時間によって移り変わる性質があるため，テンプレート生成後にどのようにテンプレートを更新していくかという問題が存在する．

2 つ目の手法として，認証結果の生成を分類問題として捉え，SVM やランダムフォレスト等の教師あり分類手法を用いて認証を行う手法が存在する．こうした手法はテンプレートベースの手法と比べて一般に認証精度が高く，またテンプレート生成のアルゴリズムを別途考える必要がないというメリットがある．一方で，こうした分類手法では，正解となる本人のデータだけでなく他人のデータも与えなければならないため実用化が難しいという問題や，学習に用いるデータセットの偏りの問題，学習に用いたデータセットに存在しない第三者が入力として与えられた場合の精度が予測できないといった問題が存在する．

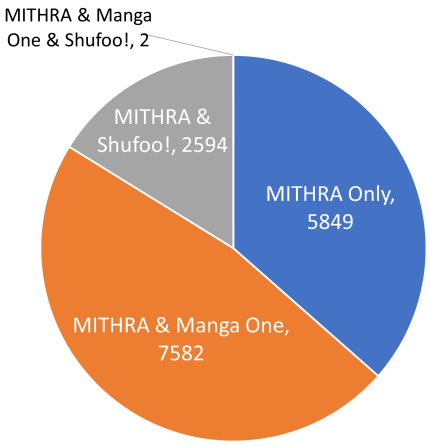

図 1　MITHRA プロジェクトでの実験参加者の概要

また，これらのいずれの手法においても，認証準備段階において大量のテンプレート生成用データ・学習用データを準備しなければならないという問題が存在しており，実用化の際の大きなハードルとなっている．

2.2 MITHRA プロジェクト

本研究では，著者らが所属する研究室が行ったライフスタイル認証の実証実験である MITHRA プロジェクトで収集されたデータ [19] を用いている．この実証実験は，2017 年 1 月 11 日から同年 4 月 26 日までの約 3 ヶ月半の間行われ，実験参加者から種々の行動データを収集した [20]．収集したデータの内容として，実験用スマートフォンアプリケーション（MITHRA アプリ）から集めた端末情報，IP アドレス情報，周囲の Wi-Fi の BSSID 情報ならびに GPS 位置情報がある．また，提携スマートフォンアプリケーションの利用履歴情報も収集した．

なお，MITHRA アプリによる端末情報の収集にあたっては，利用開始前に画面で利用者にプライバシーポリシーを表示し，利用者が同意した場合のみデータを収集するようにした．実験参加者は実験開始後においても，任意のタイミングで実験の参加・不参加を切り替えられるようにし，端末情報以外の個人情報（身長，年齢，体重など）は一切収集していない．

実験参加者の中から約 100 名の実験参加者に活動量計（オムロンヘルスケア製 HJA-750C）を身につけてもらい，日々の活動量の収集も行った．提携先アプリケーション及び活動量計のデータは，その大半を MITHRA アプリで収集した実験データと紐付けられる形で収集した．最終的な実験参加者の内訳を図 1 に示す（活動量計を身につけた参加者は，「MITHRA Only」の中に含まれている）．

なお，実験に先立ち，学内の倫理委員会の審査などを受け，然るべき許可を得てから実験を実施した．

3. 提案手法

3.1 概要

提案手法では，スマートフォンから収集される GPS 及び周囲の Wi-Fi アクセスポイントのデータ（以下位置情報データと呼ぶ）を基準として，活動量計から取得される活動履歴のデータ（以下活動履歴データと呼ぶ）との間にどれくらいの相関があるかを判定することで認証を行う．具体的には，活動履歴データから推測される活動種別（活動なし・生活活動・歩行）と，位置情報データから推測される移動速度との間にどれほどの相関があるかを判定することで認証対象者を識別する．

本手法では，認証に用いるデータは 1 日分のみで良いため，2.1.3 節で述べたテンプレートベースの手法，分類ベースの手法のいずれにおいても存在していた，事前に大量の学習用データを用意しなければならないという問題を緩和できる．

3.2 位置情報データ

本手法では，はじめにスマートフォンから取得した GPS の位置情報データ（緯度・経度情報）から，ある期間におけるユーザの移動速度を求めることでユーザが移動している時間帯を推定する．

ある時刻 t_1 で測定された位置情報（緯度・経度）を $l_1(\mathrm{lon}_{t_1}, \mathrm{lat}_{t_1})$ とすると，時刻 t_1 から時刻 t_2 までに移動した距離 $d\,[\mathrm{m}]$ は以下の式によって計算できる．ただし，r は赤道半径 $r = 6378137\,\mathrm{m}$ である．

$$\begin{aligned} d = r \arccos(&\sin \mathrm{lon}_{t_1} \sin \mathrm{lon}_{t_2} \\ &+ \cos \mathrm{lon}_{t_1} \cos \mathrm{lon}_{t_2} \cos(\mathrm{lat}_{t_2} - \mathrm{lat}_{t_1})) \end{aligned} \tag{1}$$

従って，時刻 $t_1 \le t \le t_2$ 間の平均移動速度 $v_{t_1}\,[\mathrm{m/s}]$ は $v_{t_1} = d/(t_2 - t_1)$ と表すことができる．

ここで，$W \in \{0, 1\}$ を 0 が静止状態，1 が移動状態を示す集合と定義する．また，W_{t_1} をデータ収集時刻 t_1 から次のデータ収集時刻 t_2 の間における移動状態と定義する．この時，$v_{t_1} \ge v_{\mathrm{thr}}$ であれば $W_{t_1} = 1$, そうでなければ $W_{t_1} = 0$ とする．

次に，$\mathrm{gcount}(W, t_a, t_b)$ を時刻 $t_a \le t \le t_b$ 間において，$W \in \{0, 1\}$ が出現する回数と定義する．また，$\mathrm{con}_{\max}(W, t_a, t_b)$ を，時刻 $t_a \le t \le t_b$ 間において，$W \in \{0, 1\}$ が連続して出現する最大の回数と定義する．このとき，以下の条件を全て満たすような最大の時間範囲のうち，$W = 1$ である期間のみを認証に用いる．

$$W_{t_a} = 1, W_{t_{a-1}} = 0 \tag{2}$$

$$\mathrm{gcount}(1, t_a, t_b) > 5 \tag{3}$$

$$\mathrm{con}_{\max}(0, t_a, t_b) < 3 \tag{4}$$

ただし，t_{a-1} は t_a の直前の計測時刻である．

スマートフォンを用いた GPS の位置情報の収集には一般に遅延が生じたり，実際には全く移動していない場合であっても位置情報に若干の変動が現れることがある．そのため，今回の実験ではこれらの誤差の影響を最小限にするため，移動中であると判定する移動速度 $v_{\mathrm{thr}} = 10\,\mathrm{m/s}$ とした．

また，ユーザが何らの理由で GPS をオフにしたり，GPS の位置情報ログを正しく取得できなかった場合でも認証精度の低下を抑えるため，GPS の移動速度が 0.001 m 未満かつ端末が Wi-Fi に接続していない場合，端末周囲の Wi-Fi アクセスポイントのデータが次に示す条件式 (5), (6) のいずれかを満たした時も移動中であると判定するようにした．ただし，W_{t_1}, W_{t_2} をそれぞれ時刻 t_1, t_2 で収集された Wi-Fi アクセスポイントの BSSID の集合，$n(W)$ を集合 W に含まれる要素の個数とする．

$$n(W_{t_1}) \neq 0 \ \wedge \ n(W_{t_2}) = 0 \tag{5}$$

$$n(W_{t_2}) \neq 0 \ \wedge \ \frac{n(W_{t_1} \cap W_{t_2})}{n(W_{t_2})} < 0.2 \tag{6}$$

3.3 活動履歴データ

本手法では，3.2 節で述べた位置情報データから推定される移動状態と，活動量計により計測した加速度データから導かれる活動種別を比較することによって認証を行う．一般に，加速度データから活動種別を推定する方法として，大河原らによる手法 [21] があり，本研究で用いている活動量計（オムロンヘルスケア製 HJA-750C）もこの手法により運動種別を推定している [22]．

大河原らの手法では，以下のような手順で加速度データから活動種別を推定する．まず，加速度センサデータをカットオフ周波数 0.7 Hz のハイパスフィルタに通した後の 3 軸の合成加速度を $\mathrm{ACC}_{\mathrm{fil}}$，ハイパスフィルタを通さずにそのまま求めた合成加速度を $\mathrm{ACC}_{\mathrm{unfil}}$ とする．これらの合成加速度をもとに，静止・生活活動・歩行の 3 状態を次のように識別する．

- 静止: $\mathrm{ACC}_{\mathrm{fil}} < 29.9\,\mathrm{mG}$
- 生活活動: $\mathrm{ACC}_{\mathrm{fil}} \ge 29.9\,\mathrm{mG} \ \wedge \ \mathrm{ACC}_{\mathrm{unfil}}/\mathrm{ACC}_{\mathrm{fil}} \ge 1.16$
- 歩行: $\mathrm{ACC}_{\mathrm{fil}} \ge 29.9\,\mathrm{mG} \ \wedge \ \mathrm{ACC}_{\mathrm{unfil}}/\mathrm{ACC}_{\mathrm{fil}} < 1.16$

本研究でも，この大河原らによる活動種別の判別手法をそのまま利用した．

3.4 認証の実行

本手法では，位置情報データを処理して得られた移動種別を基準とし，入力として与えられる活動履歴データの活動種別とどの程度の相関を持つかを比較・計算することによって最終的な認証を行う．具体的な手順の詳細を以下に述べる．

まず，$a_t \in \{\mathrm{stop}, \mathrm{live}, \mathrm{walk}\}$ を，時刻 t における活動

量計の記録から推定された活動形態と定義する．ただし，stop は静止，live は生活活動，walk は歩行を表す．また，$\mathrm{wcount}(a, t_a, t_b)$ を時刻 $t_a \leq t \leq t_b$ 間において，特定の活動種別 $a \in \{\mathrm{stop}, \mathrm{live}, \mathrm{walk}\}$ が出現する回数と定義する．

位置情報データについて，3.2 節の式 (2)〜(4) の条件を満たし，かつ $W = 1$ であるような計測期間のうちの 1 つを $\mathrm{gp}(t_1, t_2)$ と表す．この時，この位置情報の計測期間 $\mathrm{gp}(t_1, t_2)$ と $t_s \leq t \leq t_e$ 間の活動履歴データが以下の全ての条件を満たした時に，認証データが一致していると判定する．ただし，t_s は $t_s \leq t_1$ を満たす最大の活動履歴の計測時刻であり，t_e は $t_e \geq t_2$ を満たす最小の活動履歴の計測時刻である．

$$t_2 - t_1 \leq \mathrm{G_{int}}\ [\mathrm{min}] \tag{7}$$

$$v_{t_1} < v_{\mathrm{high}}\ [\mathrm{m/s}] \tag{8}$$

$$\mathrm{wcount}(\mathrm{walk}, t_s, t_e) > 0 \tag{9}$$

ただし，$\mathrm{G_{int}}$ 及び v_{high} は定数値である．これらの定数値は，実際に実験で用いたデバイスやデータ収集の間隔によって最適な値が変化する．$\mathrm{G_{int}}$ は位置情報の収集間隔が長過ぎることにより認証精度の低下が起きることを防止するための閾値である．今回の手法では，実験において最も良い結果が得られた数値として $\mathrm{G_{int}} = 10\,\mathrm{min}$ とおいた．また，v_{high} は位置情報データから推定される移動速度のうち，歩行による移動であると考えられる移動速度の上限値である．人間の一般的な歩行速度は分速約 75 m である [23] が，スマートフォンの GPS の精度にはゆらぎがあり，移動を開始したとしてもすぐには位置情報に反映されない場合がある．そのような場合，実際には歩行であったとしても，データ上は非常に速い速度で移動しているように見えたり，ほとんど移動していないように見えたりといった現象が生じる．そのため，本手法ではある程度の余裕をもたせ，実験で用いる値として $v_{\mathrm{high}} = 300\,\mathrm{m/s}$ とした．

一方で，他人の活動履歴データが入力された場合など，位置情報では移動している一方で，活動履歴では移動していないといったような矛盾のあるデータが認証システムに提示されることも考えられる．このような場合にペナルティを与えるため，位置情報データについて 3.2 節で認証に用いるとした計測期間において，式 (7), (8) をみたし，かつ以下の条件を満たす活動履歴データが与えられた場合に認証データが不一致であると判定する．

$$\frac{\mathrm{wcount}(\mathrm{stop}, t_s, t_e)}{\sum_a \mathrm{wcount}(a, t_s, t_e)} > \mathrm{M_{thr}} \tag{10}$$

ただし，$\mathrm{M_{thr}}$ はどの程度不一致であった場合にペナルティを与えるかを決める閾値であり，本手法では実験で最も良い結果を与えた値として $\mathrm{M_{thr}} = 0.5$ とおいた．

本手法では，最終的な認証結果の判定に 1 日分のデータを用いる．これは，人間の活動は一般に 1 日単位での周期性がみられるため，その周期全体の中に含まれる複数回の歩行期間での判定を行うことで認証精度を向上させるねらいがある．

認証対象日の 1 日の中で，3.2 節で示した条件を満たす認証対象となる位置情報データの計測期間の総数を $\mathrm{gp_{all}}$，そのうち活動履歴と一致すると判定された計測期間数からペナルティを与えると判定された計測期間数を引いた値を $\mathrm{gp_{ac}}$ とすると，一致率 P は以下の式によって表される．

$$P = \frac{\mathrm{gp_{ac}}}{\mathrm{gp_{all}}} \tag{11}$$

この一致率がある閾値 λ を上回った時に本人であると判定し，下回った時に他人であると判定する．

4. 実験

4.1 実験装置・データセット

今回の実験では，2.2 節で述べたライフスタイル認証の実証実験である MITHRA プロジェクト [19] で収集した行動データのうち，実験参加者のスマートフォンから収集した GPS/Wi-Fi のデータと，活動量計から収集した活動履歴データを使用した．

GPS/Wi-Fi のデータは，Android 端末では 5 分間隔（理想的な場合）で収集され，iOS 端末では OS が定めた基準に適合した場合に収集される．収集時には，収集時刻におけるスマートフォンの緯度・経度の情報，及び周囲に存在する Wi-Fi アクセスポイントの BSSID が記録される．また，活動量計のデータは 1 分間隔で収集され，各計測時刻における活動量（代謝当量: METs）及び 3.3 節で述べた方法で推定される活動形態が記録される．

4.1.1 データ選定

MITHRA プロジェクトに参加した被験者のうち，スマートフォンからの GPS 履歴と活動量計の双方を使用して実験に参加した被験者 64 人を抽出した．

上記被験者 64 人のうち，実験期間中に活動量計を 1 日 180 分以上装着していた日が 1 日以上存在する被験者 59 人を抽出し，本実験での利用対象とした．今回用いる活動履歴データにこのような制限を付けたのは，長時間活動量計を身につけている参加者のデータのみを抽出することで，提案手法の有効性を確実に判定するというねらいがある．

4.2 実験手順・実装

3 章で述べた手法を基に，Python（バージョン 3.9.4）を用いて認証スクリプトを実装した．4.1.1 節で選定したデータを用い，提案手法に従って本人拒否率 (FRR) 及び他人受入率 (FAR) を算出した．

本人拒否率と他人受入率の計算においては，(11) 式における一致率 P の閾値を $\lambda = 0$ から $\lambda = 0.99$ まで 0.01 きざみで変化させてそれぞれ計算した．なお，$\mathrm{gp_{all}} \geq 3$ を

表 1　提案手法と既存手法の精度比較．ACC は精度を示す．

著者	手法	事前データ数	EER	FAR	FRR	ACC
提案手法	相関	1728	13%	–	–	–
Gafurov et al. [9]	テンプレート	–	6%	–	–	–
Kobayashi & Yamaguchi [7]	テンプレート	8640	–	7.5%	9.9%	–
Sitová et al. [3]	テンプレート	8000	7%	–	–	–
Muaaz et al. [13]	テンプレート	3000	13%	–	–	–
Susuki & Yamaguchi [5]	分類	–	–	–	–	89%
Lee et al. [17]	分類	240000	–	7.5%	8.3%	–
Vhaduri & Poellabauer [6]	分類	11250	–	–	–	93%
Fridman et al. [11]	分類	1555200	2%	–	–	–
Monrose & Rubin [10]	テンプレート & 分類	–	–	–	–	92%

満たす日のみを判定に用いた．この gp_{all} の制限に関しては，認証に用いる位置情報データの総数が 1 日 3 回未満の場合，不十分なデータにより他人受入率が上昇してしまい，提案手法の有効性を正確に評価できなくなることが理由である．

4.3　実験結果

59 人の実験参加者で実験を行った結果は図 2 のようになった．この結果から，等価エラー率 (EER)，即ち本人拒否率 (FRR) と他人受入率 (FAR) が一致する値は約 0.130 となることが読み取れる．

なお，予測と正解が共に本人，共に他人であることを各々 TP, TN と表し，予測が本人で正解が他人，予測が他人で正解が本人であることを各々 FP, FN と表すと，$FAR = FP / (TN + FP)$, $FRR = FN / (TP + FN)$ である．

先の提案手法 [12] では，Android の実験参加者 16 人で実験を行った場合に EER が 0.12, そのうち理想的なデータが取得できた 14 人に対して実験を行った場合に EER が 0.08 という結果が得られていた．今回の実験では，Android/iOS のデータを両方用いて実験を行い，実験参加者も先の提案手法と比べて 59 人と増加している．その上で，本提案手法では EER が 0.130 となっているため，本手法は先の提案手法と比べて適用対象が広く，また認証精度もほぼ変わらない手法であると言える．

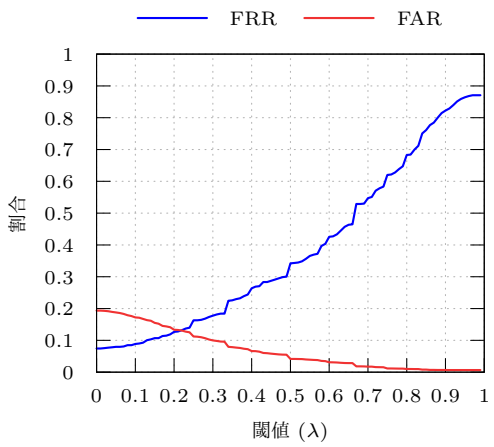

図 2　実験結果

また，一般に，既存のライフスタイル認証・行動認証の研究では EER は 0.1 程度であることが多い（表 1 参照）．ただし，$ACC = (TP + TN) / (TP + FP + FN + TN)$ である．これらの結果より，認証にデータ間の相関を用いる本提案手法が，既存のテンプレートベース・分類ベースの認証手法と同程度の認証精度を実現しているといえる．

5.　考察

5.1　提案手法の有効性

提案手法では，認証はユーザのスマートフォンから収集した GPS・Wi-Fi 情報と活動量計から収集した活動量の相関を用いて行われる．本手法では，スマートフォンからのデータ収集が定期的に行えない端末においても認証精度を保てるよう，認証の際に基準として用いるデータを活動履歴データから位置情報データに変更した．一方で，例えばユーザが片方のデバイスのみを身につけて行動した場合には認証精度が依然として低下する恐れがある．

しかし，提案手法はこの手法だけで完結する認証を提供するのではなく，ライフスタイル認証の一要素として，他のライフスタイル認証手法とも組み合わせて使用することを想定している．また，4.3 節でも述べたように，提案手法の等価エラー率はこれまで提案されてきた他の行動認証・ライフスタイル認証手法と比較しても遜色のない値となっている．従って，本提案手法はライフスタイル認証の一要素として有用な認証精度を実現できる手法であるといえる．

5.2　相関認証の応用

本提案手法では，スマートフォンから収集した位置情報データと活動量計から収集した活動履歴データの相関を持ちいて認証を行った．一般に，同一人物から収集したデータにおいて，何らかの相関を持つと考えられるデータは今回使用したデータの組にとどまらず，様々存在すると考えられる．実際，相関ベースの手法ではないものの，2 章でも述べたように，今回用いたセンサデータとは異なるセン

サデータを用いて行動認証手法を提案している論文は既に多く存在している．

例えば，スマートフォンから収集できる加速度センサやジャイロスコープといったセンサデータを用いれば，ユーザの移動状況を推定することができると考えられるため，こうしたデータを用いても相関ベースの認証ができると期待される．また，今回は複数のデバイスを用いて認証実験を行ったが，Wi-Fi と GPS のデータ間といったように，単一のデバイスから収集できる複数のセンサデータに対しても相関ベースの認証手法を適用できると考えられる．

このような他のセンサデータを用いる相関ベースの認証手法を本提案手法と組み合わせることによって，認証システム全体としての認証精度を向上できると期待される．

5.3 偽データへの対策

今回提案した手法は，位置情報データで移動している判断された期間において，活動履歴データ上で移動していないようなデータが与えられた場合，認証スコアを下げる（ペナルティを与える）ようになっている．従って，単純な偽データを与えるだけの攻撃は成立しにくいと考えている．

しかし，予備実験を行った際，偽データを与えた場合のほうが正規の他人のデータを与えた場合よりも他人受入率が高くなってしまう場合が存在することが判明した．偽データが与えられた場合の他人受入率をより低下させるために，ペナルティの値を調整したり，ペナルティを与える条件を変更したりすることが今後の課題として考えられる．

また，今回提案した手法は 1 日分のデータしか使用しないため，攻撃者が双方のデバイスを入手して 1 日が経過すると自動的に認証されてしまうという問題も存在する．この問題については，提案手法だけでは解決できないため，他のライフスタイル認証と組み合わせた多要素認証によって解決できると考えている．

6. 結論・今後の展望

本論文では，はじめに行動認証・ライフスタイル認証が第 4 の認証手法として提案されていることを説明した．また，行動認証・ライフスタイル認証の既存研究は，多くが大量の事前データを必要とすること，また異なる認証要素間の相関を用いて認証を行うものがほとんどないことを指摘した．さらに，先に提案した相関を用いる認証手法では，位置情報データの収集が定期的に行えない端末において認証精度が低下するため，実用化が難しいという課題が存在することを指摘した．

こうした背景を基に，既存手法の弱点を解消する，スマートフォンから収集した GPS・Wi-Fi データを基準として活動量計から収集した活動量を比較し，相関ベースの手法で認証を行うライフスタイル認証の新手法を提案した．提案手法を MITHRA プロジェクトで実世界のユーザから収集した実際の行動データを用いて評価し，先の手法で使用できなかった実験参加者も含めた等価エラー率 (EER) が 0.130 という結果を得た．この結果より，本手法が実世界のライフスタイル認証に適用可能であることを示した．

今後の課題として，他のライフスタイル認証手法と組み合わせて多要素認証を行うことや，今回用いたデータとは異なるデータ間の相関を用いたライフスタイル認証の研究を行うことが考えられる．また，今回の提案手法自体の認証精度の改善に関しては，加速度センサやジャイロスコープのデータを追加で使用することなどが考えられる．さらに，活動量計ではなく，心拍数などのセンサ類を搭載したスマートウォッチを提案手法で利用することも可能であると考えられる．こうした追加の活動データを利用することで，認証精度をより向上させることができると期待される．

参考文献

[1] O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication, *Proceedings of the IEEE*, Vol. 91, No. 12, pp. 2021–2040 (2003).

[2] Yamaguchi, R. S., Nakata, T. and Kobayashi, R.: Redefine and Organize, 4th Authentication Factor, Behavior, *2019 7th International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 412–415 (2019).

[3] Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P. and Balagani, K. S.: HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users, *IEEE Trans. Inf. Forensics Security*, Vol. 11, No. 5, pp. 877–892 (2016).

[4] Shen, C., Li, Y., Chen, Y., Guan, X. and Maxion, R. A.: Performance Analysis of Multi-Motion Sensor Behavior for Active Smartphone Authentication, *IEEE Trans. Inf. Forensics Security*, Vol. 13, No. 1, pp. 48–62 (2018).

[5] Susuki, H. and Yamaguchi, R. S.: Cost-Effective Modeling for Authentication and Its Application to Activity Tracker, *Information Security Applications* (Kim, H.-w. and Choi, D., eds.), Cham, Springer, pp. 373–385 (2016).

[6] Vhaduri, S. and Poellabauer, C.: Wearable device user authentication using physiological and behavioral metrics, *IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6 (2017).

[7] Kobayashi, R. and Yamaguchi, R. S.: A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User, *2015 Third International Symposium on Computing and Networking (CANDAR)*, pp. 463–469 (2015).

[8] Kobayashi, R. and Yamaguchi, R. S.: One hour term authentication for Wi-Fi information captured by smartphone sensors, *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 330–334 (2016).

[9] Gafurov, D., Helkala, K. and Søndrol, T.: Biometric Gait Authentication Using Accelerometer Sensor., *Journal of Computers*, Vol. 1, No. 7, pp. 51–59 (2006).

[10] Monrose, F. and Rubin, A. D.: Keystroke dynamics as a biometric for authentication, *Future Generation*

Computer Systems, Vol. 16, No. 4, pp. 351 – 359 (2000).
[11] Fridman, L., Weber, S., Greenstadt, R. and Kam, M.: Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location, *IEEE Syst. J*, Vol. 11, No. 2, pp. 513–521 (2017).
[12] 宮澤晟，トランフンタオ，山口利恵：活動量と GPS・Wi-Fi 情報の相関を利用したライフスタイル認証手法，SCIS2021 暗号と情報セキュリティシンポジウム，No. 2B4-2, pp. 1–8 (2021).
[13] Muaaz, M. and Mayrhofer, R.: Smartphone-Based Gait Recognition: From Authentication to Imitation, *IEEE Trans. Mobile Comput.*, Vol. 16, No. 11, pp. 3209–3221 (2017).
[14] Roh, J., Lee, S. and Kim, S.: Keystroke dynamics for authentication in smartphone, *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1155–1159 (2016).
[15] Thao, T. P., Irvan, M., Kobayashi, R., Yamaguchi, R. S. and Nakata, T.: Self-enhancing GPS-Based Authentication Using Corresponding Address, *Data and Applications Security and Privacy XXXIV* (Singhal, A. and Vaidya, J., eds.), Cham, Springer, pp. 333–344 (2020).
[16] Agadakos, I., Hallgren, P., Damopoulos, D., Sabelfeld, A. and Portokalidis, G.: Location-Enhanced Authentication Using the IoT: Because You Cannot Be in Two Places at Once, *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ACSAC '16, New York, NY, USA, Association for Computing Machinery, p. 251–264 (2016).
[17] Lee, W.-H. and Lee, R.: Implicit Sensor-Based Authentication of Smartphone Users with Smartwatch, *Hardware and Architectural Support for Security and Privacy 2016*, HASP 2016, New York, NY, USA, Association for Computing Machinery, pp. 1–8 (2016).
[18] Zhu, T., Qu, Z., Xu, H., Zhang, J., Shao, Z., Chen, Y., Prabhakar, S. and Yang, J.: RiskCog: Unobtrusive Real-Time User Authentication on Mobile Devices in the Wild, *IEEE Trans. Mobile Comput.*, Vol. 19, No. 2, pp. 466–483 (2020).
[19] 鈴木宏哉，小林良輔，佐治信之，山口利恵：ライフスタイル認証実証実験-MITHRA プロジェクト-，SCIS2017 暗号と情報セキュリティシンポジウム，No. 4D2-1, pp. 1–8 (2017).
[20] 鈴木宏哉，小林良輔，佐治信之，山口利恵：ライフスタイル認証実証実験レポート-MITHRA データセット-，マルチメディア、分散、協調とモバイル (DICOMO2017) シンポジウム，No. 1H-2, pp. 223–230 (2017).
[21] Ohkawara, K., Oshima, Y., Hikihara, Y., Ishikawa-Takata, K., Tabata, I. and Tanaka, S.: Real-time estimation of daily physical activity intensity by a triaxial accelerometer and a gravity-removal classification algorithm, *British Journal of Nutrition*, Vol. 105, No. 11, p. 1681–1691 (2011).
[22] Nakanishi, M., Izumi, S., Nagayoshi, S., Kawaguchi, H., Yoshimoto, M., Shiga, T., Ando, T., Nakae, S., Usui, C., Aoyama, T. et al.: Estimating metabolic equivalents for activities in daily life using acceleration and heart rate in wearable devices, *Biomedical engineering online*, Vol. 17, No. 1, p. 100 (2018).
[23] Knoblauch, R. L., Pietrucha, M. T. and Nitzburg, M.: Field Studies of Pedestrian Walking Speed and Start-Up Time, *Transportation Research Record*, Vol. 1538, No. 1, pp. 27–38 (1996).