社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

活動量計とスマートフォンGPSログの相関を利用したライフスタイル認証手法(1)

宮澤　　晟† 　トランフン タオ† 　山口　利恵†

† 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
E-mail: †{sgong,tpthao}@yamagula.ic.i.u-tokyo.ac.jp, ††yamaguchi.rie@i.u-tokyo.ac.jp

あらまし　近年，これまでのパスワードなどの知識情報を用いた認証手法，セキュリティキー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に代わる新たな認証手法として，個人の行動履歴を用いて認証を行うライフスタイル認証が提案されている．従来では，ライフスタイル認証の手法として，一つのデバイスから取得した単一のセンサデータを認証に用いる手法や，一つのデバイスをから取得した複数のセンサデータをフュージョンして認証に用いる手法が主に提案されてきた．本報告では，活動量計で計測した活動履歴とスマートフォンで計測した GPS の移動履歴の相関を用いたライフスタイル認証の新手法を提案し，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実際の個人の行動データを用いて本手法の有効性を検証する．
キーワード　ライフスタイル認証，GPS，活動量計，MITHRA プロジェクト

Lifestyle authentication using the correlation between activity and GPS logs (1)

Akira MIYAZAWA†, Tran PHUONG THAO†, and Rie SHIGETOMI YAMAGUCHI†

† Graduate School of Information Science and Technology, The University of Tokyo
7-3-1 Hongo, Bunkyo, Tokyo, 113–8656 Japan
E-mail: †{sgong,tpthao}@yamagula.ic.i.u-tokyo.ac.jp, ††yamaguchi.rie@i.u-tokyo.ac.jp

Abstract　In recent years, lifestyle authentication, which uses personal activity logs to authenticate individuals, has been introduced as an alternative for knowledge-based authentication such as passwords, ownership-based authentication such as physical security keys and inherence-based authentication such as fingerprints. In previous lifestyle authentication studies, most of them used one sensor data retrieved from one device, or multiple sensor data from one device with data fusion methods as a means of individual identification. In this technical report, we propose a new method of lifestyle authentication, which utilizes and combines personal activity data from activity trackers and GPS location data from smartphones, and uses their correlation as an authentication factor. We implemented this method and conducted experiments with real-world individual activity data which was collected by MITHRA project, which is a demonstration experiment of lifestyle authentication.
Key words　Lifestyle authentication, GPS, Activity tracker, MITHRA project

1. はじめに

1.1 研究の背景・目的

近年，デジタルデバイスやサービスがかつてないほど普及し，それに伴ってユーザのサイバーセキュリティに対する意識も高まっている．その中でも，正規のユーザからのアクセスを識別し，不正な利用からユーザを守る認証技術への関心はますます大きくなっている．

個人を識別する認証の手法として，パスワードなどの知識情報を用いた認証手法，セキュリティキー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つの手法が従来から存在する [1]．これに加えて，第 4 の認証手法として，個人の行動を用いて認証を行う行動認証が近年提唱されている [2]．行動認証では，これまで存在していた3つの認証手法と異なり，ユーザに認証の存在を意識させずに認証を完了させることができ，利便性の向上が期待される．

行動認証の例として，これまで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提案されてきた．なお，行動認証の中でも 1 日単位など，比較的長い周期での

ユーザの行動を用いて認証を行うものをライフスタイル認証といって区別することがあり，本報告でもそのように区別する．

これらの研究はいずれも単一のデバイスを用いて，1 つ或いは複数のセンサデータから個人認証を行う手法である．しかし，現在では 1 人のユーザがスマートフォンと活動量計など，複数のデバイスを同時に身につけて行動することが珍しくなくなっている．複数のデバイスからのデータを総合して行動認証をすることにより，単一デバイスでの認証と比べてより頑強で高精度な認証が行えると期待される．

このような複数デバイスを用いた行動認証では，異なるデバイスから取得した同種類のセンサデータ（例えば，加速度データ）を比較して認証する手法が提案されてきた [9]．本研究では，ライフスタイル認証の実証実験である MITHRA プロジェクトにおいて，同一の被験者から収集した活動量計の活動履歴とスマートフォンの GPS の移動履歴という種類が異なる 2 つのデータを用いて，これら 2 つのデータの相関から個人を認証するライフスタイル認証の新手法を提案する．

1.2 本報告の構成

本報告は以下のように構成されている．2. 章では，行動認証の関連研究について述べる．また，今回の実験で用いるデータを収集した MITHRA プロジェクトについても述べる．3. 章では，今回の提案手法である GPS の位置情報データと活動量計の活動量データの相関を用いた認証手法について，それぞれのデバイスから収集したデータの処理方法や認証手法について述べる．4. 章では，提案手法を評価するために行った実験の構成や結果について説明する．5. 章で提案手法や今後の課題について実験結果を踏まえながら考察し，最後に 6. 章で本報告のまとめとする．

2. 関 連 研 究

この章では，個人の行動を認証に用いる行動認証の分野における関連研究について述べる．

2.1 行 動 認 証

先の章でも述べたように，行動認証は従来の知識情報を用いた認証，所持情報を用いた認証，生体情報を用いた認証に代わる第 4 の認証手法として提唱されている [2]．

行動認証が近年盛んに研究されている背景には，スマートデバイスの普及がある．従来は，個人の行動パターンを取得するためには専用の機器を身につける必要があり，実世界への応用という点で大きな障壁があった．しかし，スマートフォンやスマートウォッチといったセンサ類を大量に搭載したデバイスが広く普及したことで，専用の機器を用いずとも，行動データを個人の負担がほとんど無い形で取得することができるようになり，実世界への応用も容易になった．

これまで提案されてきた行動認証は，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．それぞれの方針における関連研究を以下に述べる．

2.1.1 単一のデバイスを用いた行動認証

単一のデバイスを用いた行動認証は，歩容といった生体情報の延長としての個人の行動の特徴を利用するものと，GPS や Wi-Fi の接続履歴といった個人の移動の特徴を利用するものとに大別される．

歩容認証

歩容認証は，人間の歩行パターンが個人間で異なることを利用し，その傾向を加速度センサやジャイロスコープなどのセンサ類で測定し認証に用いる手法である．この手法は，スマートデバイスが普及する前から，行動認証の一手法として広く研究されている．例えば，2006 年の Gafurov らの研究では，加速度センサを被験者の足首に取り付け，マイコンを用いて収集するという手法で歩容認証を行い，約 5% の EER という高い精度の認証結果を得ている [10]．その後，スマートフォンやスマートウォッチの普及に伴い，それらに搭載された加速度センサーやジャイロセンサーを用いて歩容認証を行う手法も提案されている [11]．近年では，歩容の違いを識別するために CNN 等の機械学習手法を用いているものもある [12]．

デバイス操作による認証

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．この手法も，スマートデバイスが普及する前から研究が行われている．例えば，2000 年の Monrose らの研究では，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 [13]．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．

生体活動を用いた認証

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確実に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特徴を用いるわけではなく，活動量や心拍数といった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．スマートウォッチを用いた認証の例として，日々の活動量の傾向を認証に用いる手法 [5]，活動量や心拍数といったスマートウォッチから取得できる種々のセンサ情報を組み合わせて，活動傾向から個人を認証する手法 [6] といった手法が存在する．

行動履歴を用いた認証

行動履歴を用いた認証では，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種々の情報を利用し，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．行動履歴を用いた認証の例として，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，他の手法として GPS の位置情報（と Web ブラウジングの履歴等のデバイス操作の情報）を用いて認証を行う手法 [15] といった手法も存在する．

2.1.2 複数のデバイスを用いた行動認証

行動認証では，前節で述べたように単一のデバイスを用いて認証を行う手法が大半である．これは，スマートウォッチや活動量計といったウェアラブルデバイスが普及するまで，個人が持ち歩くセンサを搭載したデバイスは事実上スマートフォンしかなかったということが大きな理由として考えられる．

一方で，ここ数年では加速度計や心拍数センサを備えたスマートウォッチや活動量計が広く普及し，時計として日々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．また，認証精度が向上するだけではなく，それぞれのデバイスが搭載するセンサの性能や測定漏れによる制約といった問題も，複数デバイスのセンサデータを用いることである程度克服することができるようになると期待される．

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関連研究として，Lee ら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ある [9]．Lee らの研究では，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有意に認証精度が改善されたと結論づけている．この Lee ら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も存在する [16]．

また，キーストロークを用いた認証において，キーストローク自体だけでなく，ユーザの手首の動きも用いて認証を行う手法も提案されている [17]．更に，この手法をマウスの動きに応用し，マウスの動きと手首の動きを用いて認証を行う手法も提案されている [18]．

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を用いている [19]．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 情報がある．

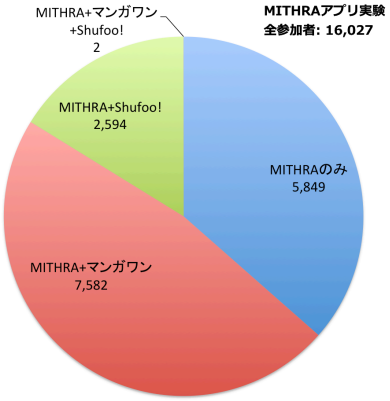

図 1　MITHRA プロジェクト参加者内訳

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．

MITHRA アプリでの端末情報の収集に加えて，提携先アプリケーションの漫画閲覧履歴（マンガワン）及び電子チラシ閲覧履歴（Shufoo!）も収集した．また，さらに約 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 のみ」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

2.1.2 節でも述べたように，複数のデバイスから収集したセンサデータを総合して行動認証を行う手法は，近年提唱されてきているものの，単一デバイスで行動認証を行う手法と比べてごく少数である．また，複数デバイスのデータを用いる手法でも，デバイス間の同種のセンサデータを利用して認証を行うものが大半である．本研究では，複数デバイスで収集した異なるセンサデータの相関を用いて認証を行う新手法を提案する．

3.1 概　　要

提案手法では，データソースとしてスマートフォンから収集される GPS 位置情報のデータ（以下位置情報データと呼ぶ）と，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）の相関を用いて認証を行う．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形態（静止・歩行による移動・乗り物による移動）がどれほど一致しているかで本人のデータか他人のデータかを識別する．

2.1.1 節でも述べたように，移動履歴を行動認証に用いる研究は既に多く存在しているが，それらはどれも過去の行動パターンを基にテンプレートを生成し，そのテンプレート情報と認証対象となる行動データがどれほど似ているかを計算して認証を行うといったものであった．こうした手法と比較すると，本手法は事前のテンプレート生成を必要としないため，認証対象者が過去の行動パターンと異なる行動をとったとしても正しく認証できることが利点である．

なお，本研究の現段階では，悪意のあるユーザが意図的に本人の行動パターンに似せたデータを提示した場合の対策について考慮しないものとする．

3.2 位置情報データ

本手法では，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移動形態を判定する．

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 [m] は以下の式によって計算できる．ただし，r は赤道半径 $r = 6378137$ [m] である．

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

人間の一般的な歩行速度は分速約 75 m である [21] 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，今回の手法では，毎分 5 m 以上 300 m 未満の移動を歩行による移動とし，それ以下は静止，それ以上は乗り物による移動とした．

3.3 活動履歴データ

本手法では，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用いて認証に利用する．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 [22] 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 [23]．

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: $\mathrm{ACC}_{\mathrm{fil}} < 29.9$ [mG]
- 生活活動: $\mathrm{ACC}_{\mathrm{fil}} \geq 29.9$ [mG] $\wedge$ $\mathrm{ACC}_{\mathrm{unfil}}/\mathrm{ACC}_{\mathrm{fil}} \geq 1.16$
- 歩行: $\mathrm{ACC}_{\mathrm{fil}} \geq 29.9$ [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，3.2 節において GPS データを処理して得られた移動種別と，3.3 節において活動量計によって得られた歩行履歴とがどの程度の相関を持つかを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．

3.4.1 歩行期間の抽出

3.3 で述べた手法を基に，活動種別を 3 種類にラベル付けしたデータから，一連の歩行動作を抽出する．

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 は歩行を表すこととする．

次に，$\mathrm{ex}(a, t_1, t_2)$ を，時刻 $t_1 \leq t \leq t_2$ において，活動形態 $a \in \{\mathrm{stop}, \mathrm{live}, \mathrm{walk}\}$ 以外の活動が連続して現れる最大の時間範囲と定義する．

一般に，一連の歩行の間には信号待ち等による小休止が存在すると考えられるので，時刻 t_1 から t_2 までの一連の歩行 $\mathrm{wp}(t_1, t_2)$ とは，以下の条件を全て満たすような時間範囲の中で最大の範囲であるとする．

$$a_{t_1}, a_{t_2} = \mathrm{walk} \tag{2}$$

$$t_2 - t_1 \geq 5 \text{ [min]} \tag{3}$$

$$\mathrm{ex}(\mathrm{walk}, t_1, t_2) < 3 \text{ [min]} \tag{4}$$

なお，計測装置の誤作動により意図せず歩行と認識されてしまう場合を除くため，認証に使う歩行期間は (3) 式にあるように 5 分以上継続しているものに限定している．

3.4.2 GPS の移動データとの比較

3.4.1 で求めた歩行期間と，3.2 で求めた GPS データから推定した移動種別を比較することで認証を行う．

まず，時刻 $t_1 \leq t \leq t_2$ の間に得られた GPS の計測サンプル数を $\mathrm{gcount}(t_1, t_2)$ と定義する．ある歩行期間 $\mathrm{wp}(t_1, t_2)$ において，対応する GPS データが以下の式の条件を満たした場合にのみ，この歩行期間を認証に用いる．ただし，t_s は $t_s \leq t_1$ を満たす最大の GPS 計測時刻であり，t_e は $t_e \geq t_2$ を満たす最小の GPS 計測時刻である．

$$\frac{t_e - t_s}{\mathrm{gcount}(t_e, t_s)} \leq 10 \text{ [min]} \tag{5}$$

このような制限を設けているのは，活動量計による活動量の計測と異なり，スマートフォンを用いた GPS 位置情報の計測は決まった周期で行われることが保証されないためである．

OS やアプリケーションの制約により指定した計測間隔で計測が行われず，次の計測まで長い時間が経過した場合，3.2 で求めた平均移動速度によって移動種別を判別すると誤差が大きくなると考えられる．そのため，今回の手法では (5) で示されるような制約を用いて，誤差による認証精度の低下を抑えている．

歩行期間 $\mathrm{wp}(t_1, t_2)$ と計測時刻 $t_s \leq t \leq t_e$ における GPS によ

る移動種別が一致するか否かの判定は，以下の条件式によって行う．ただし，v_{t_n} は GPS 計測時刻 t_n から次の計測時刻 t_{n+1} までの間の平均移動速度を表す．

$$\exists v_{t_n},\ 5[\mathrm{m/min}] < v_{t_n} < 300[\mathrm{m/min}]\ (t_s \leq t_n < t_e) \qquad (6)$$

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 日の中での独立した歩行期間の総数を $\mathrm{wcount}_{\mathrm{all}}$，そのうち (6) 式を満たす歩行期間の数を $\mathrm{wcount}_{\mathrm{ac}}$ とすると，一致率 P は以下の式によって表される．

$$P = \frac{\mathrm{wcount}_{\mathrm{ac}}}{\mathrm{wcount}_{\mathrm{all}}} \qquad (7)$$

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

3. で述べた手法を基に，実データを用いた実験を行った．この章では，実験手法とその結果について説明する．

4.1 実験装置・データセット

今回の実験では，2.2 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 の移動履歴データと，活動量計から収集した活動履歴データを使用した．

GPS の移動履歴データは 5 分間隔（理想的な場合）で収集され，各計測時刻におけるスマートフォンの緯度・経度の情報が記録される．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 で述べた方法で推定される活動形態が記録される．

実験に使用したスマートフォンアプリ（MITHRA アプリ），及び活動量計は図 2 のとおりである．

(1) MITHRA アプリケーション

(2) 活動量計 HJA-750C

図 2　実 験 装 置

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，Android 端末を利用し，かつ活動量計を 1 日 180 分以上装着していた日が 10 日以上存在する被験者 16 人を抽出し，本実験での利用対象とした．

今回用いるデータにこのような制限を付けたのは，iOS 端末では OS の制限により，一定間隔での GPS の位置情報の収集が難しく，データの欠落が頻繁に発生するためである．また，活動量計の制限については，確実に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ねらいがある．

4.2 実験手順・実装

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

なお，本人受入率と他人受入率の計算においては，(7) 式における一致率 P の閾値を $\lambda = 0.75$ に固定し，$\mathrm{wcount}_{\mathrm{all}} \geq 3$ を満たす日のみを判定に用いた．なお，$\mathrm{wcount}_{\mathrm{all}}$ の制限に関しては，1 日 3 回未満の歩行期間しかないデータを用いると判定に用いる歩行期間の数が不足し，他人受入率が上昇することが理由である．また，λ の制限に関しては，最低 3 回以上歩行期間と GPS の記録が一致するデータのみを本人として受け入れるようにするというねらいがある．

また，今回実験に用いた 16 人のうち 5 人はスマートフォンから収集したデータと活動量計から収集したデータに一貫性のないものが多く含まれていたため（4.3 で詳述），今回の実験では全員（16 人）の結果とともに，これらの参加者を除いた 11 人の結果についても検討した．

4.3 実 験 結 果

4.1.1 で抽出した 16 人のデータを用いて認証を行った結果は図 3 のようになった．

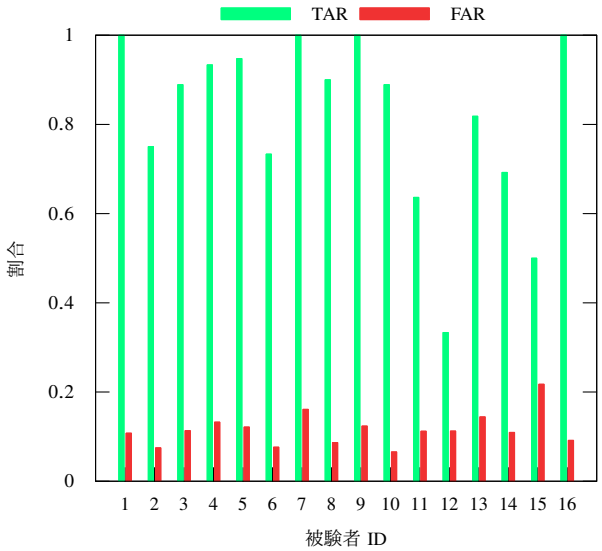

図 3　16 人全員での実験結果

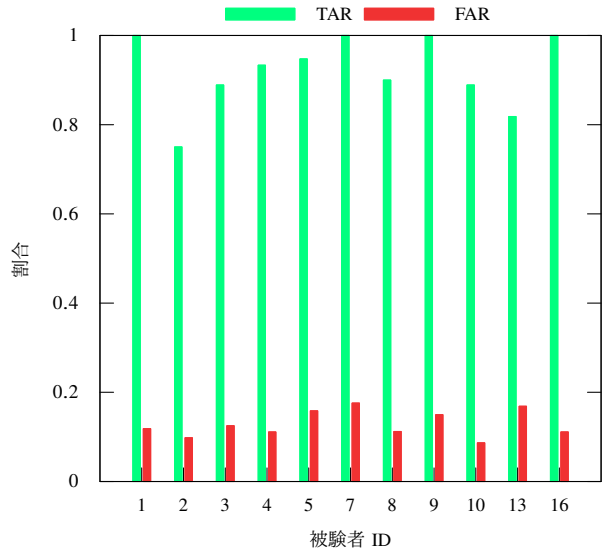

図 4　11 人での実験結果

表 1　平均 TAR 及び FAR

	TAR	FAR
全員 (16 名)	0.814	0.116
11 名	0.921	0.129

結果を見ると，ほとんどの実験参加者の TAR が 80% を超える一方，例えば被験者 ID が 11 番や 12 番の被験者では，TAR が他の実験参加者と比べて著しく悪くなっている．これらの被験者から収集した実際の認証に使われた GPS ログデータを解析すると，誤って他人だと判定された日のうち，多くの日において実験参加者の GPS 位置情報が 1 日を通して全く変化していないといった現象や，活動量計が歩行と判定してから，実際に GPS の測定結果に反映されるまでに遅延が生じていると考えられるような現象が発生していた．

このようなデータが収集された理由として，ユーザが屋内にスマートフォンをおいたまま外出したことが考えられる．また，OS の制約により，アプリケーションで収集した位置情報データが更新されずに古い情報が記録されたことや，端末の GPS 測位に時間がかかり，結果として位置情報データが遅れて反映されたことも原因として考えられる．

こうした一貫性のない GPS データが多く確認された 5 人のユーザを除いて，再度認証実験を行ったところ，結果は図 4 のようになった．図 4 を見ると，GPS データが正しく取得できたユーザの本人受入率は平均して 90% を超えており，良好な認証結果を得られていることが確認できる．

被験者全員の平均 TAR 及び FAR は表 1 のようになった．16 人全員の結果と，GPS データが概ね正しく取得できた 11 人の結果を比較すると，TAR が大きく改善している一方で，FAR の悪化は抑えられている．除いた 5 人の中に見られる 1 日を通して全く変化しない GPS データは，提案手法における他人受入率を低下させる方向に寄与すると考えられるが，このようなデータを除いた場合も FAR が大きく悪化していない．従って，本手法は実データにおいて良い性能を有しているといえる．

5. 考　　察

4.3 節で得られた結果を基に，本章では提案手法の有効性と今後の展望について考察を行う．

5.1 提案手法の有効性

提案手法ではユーザのスマートフォンの GPS 位置情報データと活動量計の活動履歴データの相関を用いて認証を行うため，4.3 節で述べたように，ユーザが片方のデバイスのみを身につけて行動したり，何らかの理由で GPS 位置情報の取得に遅延が生じたりすると認証精度が低下する恐れがある．

一方で，表 1 からも読み取れるように，双方のデバイスを正しく身につけ，GPS のデータにも遅延がほとんど見られなかったユーザ間では，TAR が約 92%, FAR が約 13% と，比較的高い認証精度を得ることができている．

今回提案した手法は，それ単体で完全な認証を提供するものではなく，ライフスタイル認証の一要素として，他の手法と組み合わせて簡便な認証手法を提供することを目的としている．そのため，本手法はその点において十分な認証精度を有していると考えられる．

5.2 認証精度が低下するユーザへの対策

片方のデバイスのみを身につけて外出することが多いユーザの場合，本手法の認証精度を高めることは難しいと考えられる．一方で，スマートフォンの性能その他の理由により，GPS 位置情報の反映に遅延が生じたり，GPS 位置情報が正しく記録されなかったユーザの認証精度をあげる方法はいくつか考えられる．

最も簡便な方法として，GPS の緯度経度の情報に加えて，GPS の精度情報も用いて認証を行う手法が考えられる．GPS の精度情報とは，取得した緯度経度から半径何 m 以内にデバイスの真の位置が存在しているかを示す情報のことである[1]．GPS の精度情報が悪い場合は，その時間帯は認証に用いないようにしたり，精度情報から求められる誤差まで含めて移動速度を計算したりすることで，不正確な GPS 位置情報による認証精度への影響を最小限に抑えることができると考えられる．

より正確な認証ができると期待される方法として，スマートフォンの GPS 位置情報に加えて，周囲の Wi-Fi アクセスポイント情報も用いるという手法が考えられる．GPS 位置情報は，例えば地下街やビル内など，GPS 信号が届かない場所では当然ながら使用できない．また，それだけでなく，屋内から屋外に移動した際は測位開始まで時間がかかる場合がある．

一方で，Wi-Fi のアクセスポイント情報は受信可能範囲が数十〜数百 m と狭いため，ユーザが移動すれば，それがたとえ屋内であっても大きく異なる測定結果を得ることができる．従って，GPS の測定精度が悪い場合は，周囲の Wi-Fi アクセスポイントの情報を比較することで，ユーザが移動したか否かを判定することができる可能性がある．ただし，Wi-Fi のアクセスポイント情報を第一の要素として用いてしまうと，電車

(注 1)：厳密には，Android の場合 68% の確率でその範囲内に存在するような円の半径を返す

に乗っているなどの乗り物による移動と，歩行による移動を区別できなくなってしまうため，あくまで GPS の位置情報を使用できない場合の補助的な要素として用いるのが正しいと考えられる．

5.3 攻撃への対策

本手法の現段階では，悪意のある攻撃者が意図的に偽のデータを提示した場合の対策については評価の対象外としたが，本節では攻撃の可能性とその対策について簡単に検討する．

まず，攻撃者が 1 日を通して歩行をしているような GPS データを提示するといった方法が考えられる．本手法では，活動量計で歩行と判定された時間範囲において，提示された GPS データにおいても歩行しているかどうかを比較することで認証を行っているため，1 日を通して歩行しているような GPS データを提示された場合，常に本人であるという判定結果となる．

このような攻撃を防ぐ方法として，活動量計で歩行と判定された時間範囲の他に，静止していると判定された時間範囲において，確かに GPS ログデータも静止しているかも認証対象にすることが考えられる．一般に，攻撃者が攻撃対象者の行動を逐一監視しない限り，対象者の歩行期間を正確に把握することは難しいと考えられるので，歩行時だけでなく静止時も認証対象とすることで，偽データによる攻撃の影響を最小限に抑えることができると期待される．

また，本手法では 1 日分のデータを認証に用いているため，攻撃者がスマートフォンと活動量計の両方を手に入れて 1 日以上が経過すると，自動的に認証されてしまうという問題も考えられる．この問題に関しては，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で，影響を抑えることができると期待される．

5.4 今後の展望・課題

今後の展望として，5.2 で述べた精度低下や 5.3 で述べた攻撃への対策として，他のライフスタイル認証手法を組み合わせた多要素認証への応用が考えられる．

例えば，本手法に Wi-Fi の要素を加えるのではなく，周囲の Wi-Fi アクセスポイントの傾向から個人を認証する既存手法 [7], [8] の認証結果を組み合わせて使用することも考えられる．複数の認証手法の認証スコアをスコアレベルフュージョンにより統合し，最終的な認証判断に用いることで，単一の認証手法と比べて TAR や FAR を改善することが可能になると期待される．

また，本研究では活動量計を使用しているが，より多くのセンサ類を搭載しているスマートウォッチを利用し，活動量や活動種別だけではなく，心拍数などの他の生体情報も組み合わせて用いることも考えられる．特に，心拍数に関しては個人の行動パターンと密接に結びついていると考えられ，既存手法でもスマートウォッチから取得した心拍数データから個人の識別を行うものが多く存在する．これらの追加の生体情報も認証手法に組み込むことで，より精度の高い認証手法になると考えられる．

6. おわりに

本報告では，初めに既存の知識認証，所有物認証，生体認証に代わる第 4 の認証手法としての行動認証・ライフスタイル認証について述べた．その上で，多くの行動認証に関する既存研究が単一デバイスから取得したセンサデータを用いて認証するものであることを指摘した．

それらの背景をふまえ，本報告ではスマートフォンの GPS 位置情報データと，活動量計の活動履歴データという，複数のデバイスから取得したデータ間の相関を用いてライフスタイル認証を行う新たな手法を提案した．

提案手法を基に，ライフスタイル認証の実証実験である MITHRA プロジェクトにおいて収集した実際の個人の行動データを用いて実験を行った．結果として，被験者全員の場合で平均 TAR / FAR が各々約 81%, 12% となり，理想的なデータが取得できた被験者に限ると約 92%, 13% という高い認証精度を得ることができた．これらの実験を通して，提案手法がライフスタイル認証の一要素として十分な認証精度を有することを確認した．

5. 章でも述べた通り，本提案手法は GPS の位置情報の精度が低下するような状況では認証精度が悪くなるという弱点が存在するが，これを改善するため，GPS のログデータに加えて Wi-Fi アクセスポイントのデータを組み合わせることで精度を高めることができる可能性があることを指摘した．今回考察で指摘したこれらの手法を実際に実装し，提案手法の認証精度を更に向上させることが今後の課題となる．

文　献

[1] K. Abhishek, S. Roshan, P. Kumar, and R. Ranjan, “A comprehensive study on multifactor authentication schemes,” Advances in Computing and Information Technology, eds. by N. Meghanathan, D. Nagamalai, and N. Chaki, pp.561–568, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[2] R. Shigetomi Yamaguchi, T. Nakata, and R. Kobayashi, “Redefine and organize, 4th authentication factor, behavior,” 2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW), pp.412–415, 2019.

[3] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K.S. Balagani, “Hmog: New behavioral biometric features for continuous authentication of smartphone users,” IEEE Transactions on Information Forensics and Security, vol.11, no.5, pp.877–892, 2016.

[4] C. Shen, Y. Li, Y. Chen, X. Guan, and R.A. Maxion, “Performance analysis of multi-motion sensor behavior for active smartphone authentication,” IEEE Transactions on Information Forensics and Security, vol.13, no.1, pp.48–62, 2018.

[5] H. Susuki and R.S. Yamaguchi, “Cost-effective modeling for authentication and its application to activity tracker,” Information Security Applications, eds. by H.-w. Kim and D. Choi, pp.373–385, Springer International Publishing, Cham, 2016.

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

[7] R. Kobayashi and R.S. Yamaguchi, “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] R. Kobayashi and R.S. Yamaguchi, “One hour term authentication for wi-fi information captured by smartphone sensors,” 2016 Interna-

tional Symposium on Information Theory and Its Applications (ISITA), pp.330–334, 2016.
[9] W.-H. Lee and R. Lee, “Implicit sensor-based authentication of smartphone users with smartwatch,” Proceedings of the Hardware and Architectural Support for Security and Privacy 2016, pp.1–8, HASP 2016, Association for Computing Machinery, New York, NY, USA, 2016.
[10] D. Gafurov, K. Helkala, and T. Søndrol, “Biometric gait authentication using accelerometer sensor.,” Journal of Computers, vol.1, no.7, pp.51–59, 2006.
[11] M. Muaaz and R. Mayrhofer, “Smartphone-based gait recognition: From authentication to imitation,” IEEE Transactions on Mobile Computing, vol.16, no.11, pp.3209–3221, 2017.
[12] M. Gadaleta and M. Rossi, “Idnet: Smartphone-based gait recognition with convolutional neural networks,” Pattern Recognition, vol.74, pp.25–37, 2018.
[13] F. Monrose and A.D. Rubin, “Keystroke dynamics as a biometric for authentication,” Future Generation Computer Systems, vol.16, no.4, pp.351–359, 2000.
[14] J. Roh, S. Lee, and S. Kim, “Keystroke dynamics for authentication in smartphone,” 2016 International Conference on Information and Communication Technology Convergence (ICTC), pp.1155–1159, 2016.
[15] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, “Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location,” IEEE Systems Journal, vol.11, no.2, pp.513–521, 2017.
[16] T. Zhu, Z. Qu, H. Xu, J. Zhang, Z. Shao, Y. Chen, S. Prabhakar, and J. Yang, “Riskcog: Unobtrusive real-time user authentication on mobile devices in the wild,” IEEE Transactions on Mobile Computing, vol.19, no.2, pp.466–483, 2020.
[17] B. Li, H. Sun, Y. Gao, V.V. Phoha, and Z. Jin, “Enhanced free-text keystroke continuous authentication based on dynamics of wrist motion,” 2017 IEEE Workshop on Information Forensics and Security (WIFS), pp.1–6, 2017.
[18] B. Li, W. Wang, Y. Gao, V.V. Phoha, and Z. Jin, “Hand in motion: Enhanced authentication through wrist and mouse movement,” 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp.1–9, 2018.
[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，vol.1，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，vol.1，no.1H-2，pp.223–230，2017.
[21] R.L. Knoblauch, M.T. Pietrucha, and M. Nitzburg, “Field studies of pedestrian walking speed and start-up time,” Transportation Research Record, vol.1538, no.1, pp.27–38, 1996.
[22] K. Ohkawara, Y. Oshima, Y. Hikihara, K. Ishikawa-Takata, I. Tabata, and S. Tanaka, “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.
[23] M. Nakanishi, S. Izumi, S. Nagayoshi, H. Kawaguchi, M. Yoshimoto, T. Shiga, T. Ando, S. Nakae, C. Usui, T. Aoyama, 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.